The subject of the invention is a procedure for diversifying a basic code and for authenticating a thus diversified code as having been generated from a predetermined basic code, and a system for using the procedure.

Such a procedure enables, in particular, secret codes recorded in portable media, such as smart cards, to be diversified.

The rapid development of applications which use portable objects such as cards is essentially due to the advent of smart cards, one essential characteristic of which is that they contain processing circuits. Said circuits generally comprise a microprocessor which performs calculations not only on data entered externally, but particularly on internal data inaccessible from outside.

Such cards are distributed to users by issuing bodies which offer services via devices or terminals available to the public and to which the user temporarily connects his card.

In general, any device will not provide the requested service until it has checked that the card was indeed originally set up to be able to provide access to said service.

In fact, it is necessary at all costs to prevent a card set up to access service (A) also being able to access service (B), or to prevent a fraudulent person being able to design or simulate a forged card providing access to service (A) and/or (B).

Said aims are generally achieved by first setting up an information interchange in the form of a dialogue between the card and the device.

One type of dialogue, as described in the applicant's American patent 4 471 216, corresponding to its French patent 2 469 760, includes a secret code, known only to the issuing body and

recorded in both the card and the device. By way of example, the card calculates a result which is a function of its secret code and the device calculates a similar result which is a function of its secret code. The results are compared by the device which will not authorise access to the requested service unless said results are equal or agree. Said condition may not be fulfilled unless the codes of the card and the device are identical.

Thus, any device designed to provide a given service is capable of identifying all the cards which have been issued by an issuing body in order to gain access to said service.

However, for a single secret code recorded in a device, there are n cards of the same family with said secret code (n may reach several million, particularly in banking applications). If a fraudulent person succeeds in cracking the secret of said code, he is able to manufacture and distribute forged cards which will, however, be identified as valid by the devices. Such a consequence would be catastrophic and would require the secret code to be changed and new cards to be distributed.

In order overcome said disadvantage, the invention is intended to diversify the secret codes of cards from a single basic code, whilst enabling the devices to identify them as having been generated from the same secret code. Thus, each card will have a specific secret code which is different to the codes allocated to the other cards.

The invention, therefore, offers a procedure for diversifying a basic code by means of an initialisation system, each diversified code being recorded in a memory of a subject device, and for identifying, by means of an operating system, that the diversified code of a subject device has indeed been generated from a predetermined basic code, characterised in that it consists:

- in order to diversify a basic code Sb prerecorded in a memory of the initialisation system:
of calculating, by means of the processing circuits of said system, a diversified code Sd, by subjecting the basic code Sb and a diversification parameter Du specific to each subject device to a commutative one-to-one combinational transformation (T), such that Sd = Du (T) Sb,

- of recording the diversified code Sd thus calculated in the memory of the subject device,

- and to have the diversified code Sd of a subject device identified as having been generated from a basic code Sb:
of connecting the subject device to an operating system having a memory in which the basic code Sb is recorded, and calculating, by means of the processing circuits of said system, an intermediate parameter Pu, by subjecting a data element Cu specific to each subject device and the aforementioned diversification parameter Du to the transformation (T), such that Pu = Cu (T) Du,

and of calculating, on the one hand by means of the operating system, a first code authentication R1 which is a function of an external data element Ex and a first code K1, such that R1 = f3 (K1, Ex),

and K1 = Sb (T) Pu

and, on the other hand by means of the subject device, a second code authentication R2, which is a function of the external data element Ex and a second code K2, such that R2 = f4 (K2, Ex)
and K2 = Sd (T) Cu

the two code authentications (R1, R2) being identical if the diversified code Sd of the subject device has indeed been

calculated from the same basic code Sb as that recorded in the operating system.

According to one characteristic of the procedure, the transformation (T) is an exclusive-OR function.

According to another characteristic of the invention, an initialisation system for using the procedure according to the main claim is characterised in that, in order to initialise a subject device with a diversified code Sd, it comprises:

- means of connection with the subject device, - a memory in which a basic code Sb and a program are recorded, - processing circuits for calculating the diversified code Sd by executing the program which applies a commutative one-to-one combinational transformation (T) to the basic code and to a diversification parameter Du specific to each subject device, such that Sd = Sb (T) Du.

According to another characteristic, an operating system for using the procedure according to the main claim is characterised in that, in order to identify the diversified code Sd recorded in a subject device, it comprises:

- means of connection with the subject device,

- a memory in which a program is recorded and processing circuits for calculating an intermediate parameter Pu by executing the program which applies a commutative one-to-one combinational transformation (T) to a diversification parameter Du specific to each subject device and to a data element Cu specific to each subject device, such that Pu = Du (T) Cu,

- a memory in which a basic code Sb and a program are recorded, and processing circuits for calculating a code authentication R1 by executing the program, in which:

$$R1 = f3\ (K1,\ Ex)$$

and $$K1 = Sb\ (T)\ Pu$$

where Ex is an external data element.

Other advantages, characteristics and details are described in the following explanatory description, provided with reference to the appended drawings, given by way of example.

- figure 1 is a diagrammatic representation of an initialisation system in order to illustrate the first phase of the procedure according to the invention,

- and figure 2 is a diagrammatic representation of an operating system in order to illustrate the second phase of the procedure according to the invention.

In general, the procedure according to the invention may be broken down into an initialisation phase and an operating phase.

The initialisation phase consists:

- of calculating a diversified code from a predetermined basic code by means of an initialisation system,

- and of recording said secret code thus diversified in a memory of a portable object.

Said first phase is carried out by an issuing body, which then gives the portable object to a user, each portable object having a different secret code. Each user may then request access to the services using his portable object, although such access operations may not be authorised until a check has been carried out on the basis of the identification of the diversified code recorded in the portable object. Said check is the subject of the second phase or operating phase which is described below.

The initialisation system (1) shown in figure 1, is broken down, in particular, into a source device (CM1), an intermediate device (DI2), an input device such as a keyboard (CL) and an input-output interface (IO).

The source device (CM1) consists in particular of a memory (M1), processing circuits (T1) such as a microprocessor, and an input-output interface (I1). All said circuits are interconnected by a data bus (b1).

At least the following data is recorded in the memory (M1) of the source device (CM1):

- an intermediate secret code (Sm),

- and a calculation program (P1), the function of which is explained below.

The intermediate device (DI2) consists in particular of a memory (M2), processing circuits (T2) such as a microprocessor and an input-output interface (I2). All said circuits are interconnected by a data bus (b2).

The memory (M2) of the intermediate device (DI2) contains the following data:

- a predetermined basic code (Sb), - and a program (P2), the function of which is explained below.

The interfaces (I1, I2) of the source device (CM1) and of the intermediate device (DI2) are linked together, as are the keyboard (CL) and the initialisation interface (1), by a data bus (b0).

A portable object (CU3) to be initialised consists in particular of a memory (M3), processing circuits (T3) such as a

microprocessor and an input-output interface (I3). All said circuits are interconnected by a data bus (b3).

According to a preferred embodiment, the portable object (CU3) or user card consists of a smart card as described in American patents 4 211 919 and 4 382 279, which correspond respectively to the applicant's French patents 2 401 459 and 2 461 301.

The user card (CU3) is connected to the initialisation system via a transmission line (L) which links the interfaces (I0, I3). Such a line (L) is described in particular in the American patent 4 556 958, which corresponds to the applicant's French patent 2 483 713.

The function of the initialisation system (1) is therefore to calculate a diversified code (Sd) from a predetermined basic code (Sb).

The principle of said calculation is as follows. Firstly, a diversification parameter (Du) is calculated from data specific to each user card to be initialised and from an intermediate basic code (Sm). Secondly, the diversified code (Sd) is calculated from the diversification parameter (Du) and the predetermined basic code (Sb).

In a first embodiment, the diversification parameter (Du) is calculated by the source device (CM1) and the diversified code (Sd) is calculated by the intermediate device (DI2).

More precisely, the processing circuits (T1) of the source device (CM1) execute the aforementioned program (P1) in order to calculate a diversification parameter (Du) such as:

$$Du = f1\ (Sm, Eu, Cu)$$

where (Sm) is the aforementioned intermediate basic code recorded in the memory (M1), (Eu) is a data element specific to the user card (CU3) entered at the keyboard (CL) and recorded in the memory (M3), and (Cu) is a diversification data element specific to the user card (CU3), which is either external and entered at the keyboard (CL) before being recorded in the memory (M3), or internal and already prerecorded in the memory (M3).

Then, the intermediate device (DI2) calculates a diversified code (Sd) from the predetermined basic code (Sb) recorded in its memory (M2) and from the diversification parameter (Du) calculated by the source device (CM1) and transmitted by the bus (b0) to the intermediate device (DI2).

The diversified key (Sd) is calculated by the processing circuits (T2) which execute the program (P2) which uses a one-to-one combinational transformation (T) such as:

$$Sd = Sb\ (T)\ Du$$

By way of example, said transformation is an EXCLUSIVE-OR function.

Finally, the diversified code (Sd) thus calculated is recorded in the memory (M3) of the card (CU3).

It should be noted that the memory (M3) of the user card (CU3) is advantageously divided into at least two zones (Z1, Z2). The memory zone (Z1) is such that once the data has been recorded, it is inaccessible from outside, and accessible only by the processing circuits (T3). The memory zone (Z2) is such that the recorded data may be read but not modified from outside. Such memory access operations are described, in particular, in the applicant's American patent 4 211 919, which corresponds to his French patent 2 401 459.

Since memory zone (Z1) enables the recorded data to be kept secret, the diversified code (Sd) is recorded in said zone, whilst the data (Eu, Cu) specific to the user are recorded in zone (Z2).

The initialisation phase thus described is generally supplemented by writing several other data elements specific to each application to the memory (M3) of the card (CU3).

A user card thus initialised by an issuing body is given to a user who may then access any service authorized by his card, by connecting it to a device or terminal responsible for providing said service and managed by the issuing body.

Before providing said service, the device must check that the presented card has an authentic secret code, i.e. that said card has indeed been calculated from the basic code specific to the requested service and prerecorded in all devices responsible for providing said service. If this is not the case, the device will have detected either a forged card, or a genuine card, but one which has not been initialised to obtain the service provided by said device.

Said check is the subject of the second phase of the procedure or operating phase as described with reference to figure 2.

The operating system (4) is made up of a checking device (CM4), an intermediate device (DI5), an input device (CL) such as a keyboard, for example, and an input/output interface (I0).

The checking device (CM4) is made up, in particular, of a memory (M4), processing circuits (T4) such as a microprocessor, and an input/output interface (I4). All said circuits are interconnected by a data bus (b4).

The following data at least is recorded in the memory (M4):

- the secret codes (Sm, Sb) used during the initialisation phase,
- the program (P1), which is also used during the initialisation phase for calculating the diversification parameter (Du),
- and a program (P3), the function of which is explained below.

The intermediate device (DI5) is made up, in particular, of a memory (M5), processing circuits (T5) such as a microprocessor, and an input/output interface (I5). All said circuits are interconnected by a data bus (b5).

The memory (M5) of the intermediate device (DI5) contains at least the same program (P2), the function of which is explained below.

The interfaces (I4, I5) of the checking device (CM4) and the intermediate device (DI5) are linked together and to the keyboard (CL) and to the interface (I0) of the operating system (4) by a data bus (b0).

Let a user card (CU3) be initialised as described above and temporarily connected to the operating system (4). Said connection is obtained by means of a transmission line (L) of the type specified above, which links the interface (I0) of the system (4) and the interface (I3) of the card (CU3).

Firstly, the checking device (CM4) recalculates a diversification parameter (Du) by executing the program (P1) via the processing circuits (T4). Said parameter (Du) is such that:

$$Du = f1\ (Sm, Eu, Cu)$$

where the parameters (Eu, Cu) have been fetched from the memory (M3) of the user card (CU3).

Once it has been calculated, the diversification parameter is sent to the intermediate device (DI5), the processing circuits (T5) of which will execute the program (P2) in order to obtain a parameter (Pu) such that:

$$Pu = Du\ (T)\ Cu$$

where (Cu) is the parameter fetched from the memory (M3) of the user card (CU3).

At this stage of the procedure, it is important to note an original feature of the invention. The checking device (CM4) and the intermediate device (DI5) do not directly recalculate a diversified code (Sd) from the basic code (Sb) in order to then compare it to the one recorded in the user card (CU3). Thus, the diversified code (Sd) is even better protected.

However, in order to enable the diversified code (Sd) recorded in the user card (CU3) to be identified, the checking device (CM4) and the card (CU3) will each calculate the result known as the code authentication. Said code authentications will be identical if the diversified code (Sd) of the card (CU3) has been calculated from the same basic code (Sb) as the one recorded in the memory (M4) of the checking device (CM4). Identity of the two code authentications is based on the relationships which exist between the secret codes (Sb, Sd) and the parameters (Pu, Du) as explained below.

A first code authentication or result (R1) is calculated by the processing circuits (T4) of the checking device (CM4) by executing the program (P3) recorded in the memory (M4). Said result (R1) is such that:

$$R1 = f3\ (K1,\ Ex)$$

and

$$K1 = Sb\ (T)\ Pu$$

where (Sb) is the basic code recorded in the memory (M4), (Pu) is the parameter calculated by the intermediate device (DI5), and (Ex) is an external data element entered at the keyboard (CL), for example, by an operator or by the user.

For their part, the processing circuits (T3) of the user card (CU3) execute the program (P4), which is prerecorded in the memory (M3) during the initialisation phase in order to obtain a second code authentication or result (R2) such that:

$$R2 = f4\ (K2,\ Ex)$$

and

$$K2 = Sd\ (T)\ Cu$$

where (Sd) is the diversified code recorded in the memory (M3), (Cu) is the parameter fetched from the memory zone (Z2), and (Ex) is the aforementioned external data element.

If the diversified code (Sd) has indeed been calculated from a basic code (Sb) identical to the one recorded in the checking device (CM4), the two results (R1, R2) will be identical for the following reasons:

- the intermediate parameter (K2) for calculating the result (R2) is such that:

$$K2 = Sd\ (T)\ Cu$$

thus: $Sd = Sb\ (T)\ Du$

hence: $K2 = Sb\ (T)\ Du\ (T)\ Cu$

thus: $Pu = Cu\ (T)\ Du$

hence: $K2 = Sb\ (T)\ Pu = K1$ (intermediate parameter used for calculating the result (R1).

All said equalities are satisfied since the transformation (T) used is a commutative transformation.

Of course, if at least one of said equalities is not satisfied, the diversified code (Sd) of the subject device (CU3) is not identified as being authentic and the dialogue is interrupted.

It follows from the above that the source device (CM1) and the intermediate device (DI2) of the initialisation system (1), and the checking device (CM4) and the intermediate device (DI5) of the operating system (4), contain data which must remain secret in order to prevent fraud, which might consist of simulating forged user cards (CU3), which are identified as being genuine by the checking device (CM4).

It is, therefore, essential to implement safety measures to protect access to the data contained in the memories (M1, M2, M4 and M5).

A first solution consists of implementing physical or material protection measures which make said memories difficult to access.

A second solution consists, once the data has been written, of locking the memory access operations in such a manner as to render them inaccessible from outside, and accessible only by the processing circuits allocated respectively to said memories.

Said second solution is fulfilled if the memories correspond to the memories of portable objects, such as the user cards (CU3). More precisely, the memory (M1) and the processing circuits (T1) of the source device (CM1) of the initialisation system (1) on the one hand, and the memory (M4) and the processing circuits (T4) of the checking device (CM4) of the operating system (4) on the other hand, are integrated into a user-type card in which each memory (M1, M4) is divided into at least two memory zones (Z1, Z2).

A third solution consists of combining the source device (CM1) and the intermediate device (DI2) of the initialisation system

(1) into the same device designed, for example, in the form of an integrated circuit package with the same memory access characteristics as an aforementioned card. Said solution also applies to the checking device (CM4) and to the intermediate device (DI5) of the operating system (4).

As a variant of said third solution, the aforementioned integrated circuit package is included in a portable object and, particularly, in an aforementioned smart card.



Claims

1. Procedure for diversifying a basic code by means of an initialisation system, each diversified code being recorded in a memory of a subject device, and for identifying, by means of an operating system, that the diversified code of a subject device has indeed been generated from a predetermined basic code, characterised in that it consists:

- in order to diversify a basic code Sb prerecorded in a memory (M2) of the initialisation system (1):
of calculating, by means of the processing circuits (T1, T2) of said system (1), a diversified code Sd by subjecting the basic code Sb and a diversification parameter Du specific to each subject device (CU3) to a commutative one-to-one combinational transformation (T), such that Sd = Du (T) Sb,

- of recording the diversified code Sd thus calculated in the memory (M3) of the subject device (CU3),

- and to have the diversified code Sd of a subject device (CU3) identified as having been generated from a basic code Sb:
of connecting the subject device (CU3) to an operating system (4) having a memory (M4) in which the basic code Sb is recorded, and of calculating by means of the processing circuits (T4, T5) of said system (4) an intermediate parameter Pu, by subjecting a data element Cu specific to each subject device (CU3) and the aforementioned diversification parameter Du to the transformation (T), such that Pu = Cu (T) Du,

and of calculating, on the one hand by means of the operating system (4), a first code authentication R1 which

is a function of an external data element Ex and a first code K1, such that R1 = f3 (K1, Ex),

and K1 = Sb (T) Pu

and, on the other hand by means of the subject device (CU3), a second code authentication R2, which is a function of the external data element Ex and a second code K2, such that R2 = f4 (K2, Ex)

and K2 = Sd (T) Cu

the two code authentications (R1, R2) being identical if the diversified code Sd of the subject device (CU3) has indeed been calculated from the same basic code Sb as that recorded in the operating system (4).

2. Procedure according to claim 1, characterised in that it consists of calculating by means of the initialisation system (1), the aforementioned diversification parameter Du by executing a program (P1) recorded in its memory (M1) and which includes a data element (Eu) specific to the subject device (CU3).

3. Procedure according to claim 2, characterised in that the aforementioned program (P1) also includes an intermediate code (Sm) prerecorded in the memory (M1) of the initialisation system (1).

4. Procedure according to claim 1, characterised in that it consists of calculating, by means of the operating system (4), the aforementioned diversification parameter Du by executing a program (P1) recorded in its memory (M4) and which includes a data element (Eu) specific to the subject device (CU3).

5. Procedure according to claim 4, characterised in that the aforementioned program (P1) also includes an intermediate

code (Sm) prerecorded in the memory (M4) of the operating system (4).

6. Procedure according to claim 1, characterised in that it consists of using an EXCLUSIVE-OR function for the aforementioned transformation (T).

7. Initialisation system for using the procedure as defined according to one of claims 1 to 6, characterised in that, in order to initialise a subject device (CU3) with a diversified code Sd, it comprises:

- means of connection (I0, I3, L) with the subject device (CU3), - a memory (M2) in which a basic code Sb and a program (P2) are recorded, processing circuits (T2) for calculating the diversified code Sd by executing the program (P2) which applies a commutative one-to-one combinational transformation (T) to the basic code and to a diversification parameter Du specific to each subject device (CU3), such that Sd = Sb (T) Du.

8. System according to claim 7, characterised in that it also comprises processing circuits (T1) for calculating the aforementioned diversification parameter Du by executing a program (P1) recorded in a memory (M1) and which includes at least one data element (Eu) specific to the subject device (CU3).

9. System according to claim 8, characterised in that the aforementioned program (P1) also includes an intermediate code (Sm) prerecorded in the memory (M1).

10. System according to one of claims 7 to 9, characterised in that the processing circuits (T1) and the aforementioned memory (M1) are integrated into a portable object such as a smart card (CM1).

11. System according to one of claims 7 to 9, characterised in that the processing circuits (T1, T2) and the memories (M1, M2) are integrated into an integrated circuit package.

12. System according to claim 11, characterised in that the aforementioned package is mounted in a portable object, such as a smart card.

13. Operating system for using the procedure as defined according to one of claims 1 to 6, characterised in that, in order to identify the diversified code Sd recorded in a subject device (CU3), it comprises:

- means of connection (I0, I3, L) with the subject device (CU3),

- a memory (M5) in which a program (P2) is recorded, and processing circuits (T5) for calculating an intermediate parameter Pu by executing the program (P2) which applies a commutative one-to-one combinational transformation (T) to a diversification parameter Du specific to each subject device (CU3) and to a data element Cu specific to each subject device (CU3), such that Pu = Du (T) Cu,

- a memory (M4) in which a basic code Sb and a program (P3) are recorded, and processing circuits (T4) for calculating a code authentication R1 by executing the program (P3), in which:

$$R1 = f3\ (K1, Ex)$$

and

$$K1 = Sb\ (T)\ Pu$$

where Ex is an external data element.

14. System according to claim 13, characterised in that the aforementioned memory (M4) also contains a program (P1)

executed by the processing circuits (T4) in order to calculate the aforementioned diversification parameter Du and which includes at least one data element (Eu) specific to the subject device (CU3).

15. System according to claim 14, characterised in that the aforementioned program (P1) also includes an intermediate code (Sm) prerecorded in the memory (M4).

16. System according to one of claims 13 to 15, characterised in that the memory (M4) and the processing circuits (T4) are integrated into a portable object (CM4), such as a smart card.

17. System according to one of claims 13 to 15, characterised in that the memories (M4, M5) and the processing circuits (T4, T5) are integrated into an integrated circuit package.

18. System according to claim 17, characterised in that the aforementioned package is mounted in a portable object, such as a smart card.

19. System according to one of claims 13 to 15, characterised in that the memory (M3) of the subject device (CU3) connected to the said system contains a program (P4) executed by the processing circuits (T3) in order calculate a code authentication R2 in which:

$$R2 = f4\ (Ex,\ K2)$$

and:

$$K2 = Sd\ (T)\ Cu$$

where Ex is the aforementioned external data element, said code authentication R2 having to be identical to the aforementioned code authentication R1 calculated by the said system.

20. System according to one of claims 13 to 19, characterised in that the subject device (CU3) is a portable object such as a smart card.