The invention relates to a method for generating a random number in a system with electronic portable objects such as cards with memory and microcircuits, and to a system for implementing this method.

The rapid development in applications implementing portable objects, such as cards with memory and microcircuits, is essentially due to the fact that these cards have processing circuits that generally comprise a microprocessor that can perform calculations, not only on data entered externally, but also on internal data that is inaccessible from outside.

Such cards are distributed to users by authorised bodies which offer to provide services through equipment or terminals made available to the public and to which the user temporarily couples the portable object that has been given to him, at the time of requesting the provision of a service.

Depending on the nature of the service rendered with the aid of a given portable object, it may be necessary for data travelling between the portable object and the terminal to retain a degree of confidentiality and, in consequence, systems using portable objects, such as microcircuit cards, are arranged so that they are able to encode (also known as encrypt) these data in transit. For this purpose, encoding programs are recorded inside the processing circuits of the portable objects, and similarly encoding programs are recorded inside the circuits of the associated terminals. Furthermore, these programs generally use keys for encoding the data and, consequently, the secret encoding keys are generally recorded in the portable objects and in the associated terminals. These keys are described as secret when they are accessible only via the processing circuits of the device of the system in which they are recorded. On the other hand, the processing circuits of the portable objects and the terminals have to memorise corresponding decoding programs.

Furthermore, numerous functions which allow these transactions to take place in complete security have been envisaged and are described and protected by a number of patents in the name of the applicant. For example, methods making it possible to check that a decoded datum actually corresponds to the original datum,

and that there has been no alteration during transmission, have been envisaged; reciprocal methods for the authentication of the terminal by the portable object to which it is connected, and of the portable object by the terminal, have also been envisaged, so that, on the one hand, the terminal can be certain that the portable object connected to it has indeed been provided for the service in question, or so that the portable object can check that it is indeed connected to a terminal intended for the service.

These various functions often require, for their implementation, secret data specific to the application in question, which cannot be decoded from outside.

The various functions that have just been mentioned can be used when a portable object has been put into circulation by a service provider, and also before the portable objects are put into service, during what is known as the customisation phase of these portable objects which consists of introducing, into their memory, the data specific to the application for which the object could be used, some of which data are secret. At the time of customisation, encoding operations therefore have to be performed, and the checking functions mentioned also have to be implemented.

Furthermore, in some cases the encoding of data is subject not only to the taking into account of a secret encoding key, but also the taking into account of a random number, which means that, when any one datum that takes account, inter alia, of different random numbers is encoded, a different encoded message appears. Thus, a person intending to commit fraud who observed the datum entered would have difficulty in simulating in advance the result of encoding.

Numerous patent applications in the name of the applicant or of third parties, including French patent application published under number 2 601 535 in the name of the applicant, mention systems using algorithms for encoding and decoding data, and demonstrating various ways of using random numbers, particularly in systems with microcircuit cards.

In such systems, the term 'random number' is in fact generally used to denote the result of a calculation performed on predetermined parameters, which can be contained in certain memory zones of the portable object. As a result, if the parameters used for calculating a random number should be identical for two different calculations, then the result of these two calculations is the same.

Thus, a competent person intending to commit fraud who, each time a random number was drawn, observed the value of the parameters used as the basis for calculating said number and noted the random number obtained for each combination of parameters, would be in a position to determine in advance what the next random number calculated would be, if the parameters used to calculate it were to take a value identical to a value that the defrauder had observed previously. Consequently, the person intending to commit fraud would be in a position to determine in advance the result of encoding a datum previously encoded with the same random number.

For this reason, in order for the system to be as reliable as possible, the probability of any one combination of parameters being identical when these systems are used should be reduced as far as possible, or even nullified, in order to limit the risk of fraud as far as possible.

In certain operating methods, the random number is calculated by the portable object by using, in order to obtain it, parameters or data that are contained in the memory of the portable objet.

For example, the French patent application published under number 2 601 535, in the name of the applicant, envisages a random number being obtained on the basis of parameters sampled from the control zone of the memory, that is, the memory zone where the content is modified each time the card is used, for example, to store fraudulent attempts at use, or errors, or any other type of control operations required by the particular use for which the portable object in question might be intended. More specifically, the word in the control zone that was modified at the last use is sampled from the control zone of the memory. The random number may be

produced by encoding this word in the control zone, modified at the time of the last use. However, in order to save memory, the control zone is generally modified bit by bit, and not word by word. As a result, since a memory is normally divided into words of n bits, each word being located at a different address, the content of a word located at a given address is capable of being modified n times, such that the content of a word located at a given address in the control memory can be used n times to constitute the random number, its value changing each of these n times such that, at each change, the resulting random number becomes unforeseeable.

However, this solution is not totally satisfactory since, at the end of these n changes, the random number will be obtained by sampling a word located at a different address in the control zone. However, the content of this word located at a different address is capable of taking on, successively, the configurations of the word at the preceding address, such that the same random numbers can be found. Consequently, a person intending to commit fraud who had observed the preceding series of random numbers would be in a position to determine the result of subsequent encoding, in the event that a random number already used were to be used once again to encode the same datum. For this reason, in this application, it has been envisaged that use is made not only of the content of a word in the control zone located at a given address, but also an element that takes into account the value of the address itself, such that the random number is obtained from a calculation taking into account the value of the word and its address.

This solution proves satisfactory from the point of view of memory consumption, since the random number is calculated from data necessary for the operation of the system.

However, in certain applications, the control zone can be modified only once at a session, that is, between the moment when the portable object is connected to the terminal and the moment when it is disconnected, whereas at the time of the current session, the processing circuits of the system may make several requests to use a random number. In such a case, the successive calculations of a random number would give the same result, since the parameters would not have evolved.

The objective of the invention is therefore to overcome these disadvantages, by proposing a method by which, in a microcircuit card system, numbers can be obtained that can be qualified as random, when they are considered by an outside observer, in so far as the combination of the parameters used to calculate them does not occur twice identically when the system is used. The method according to the invention also has to allow random numbers to be obtained as many times as necessary, whether at any one session, or at different sessions, without substantially affecting the memory consumption.

To this end, the invention concerns a method for generating a random number in a system with portable objects, such as cards with electronic memories and microcircuits, of the type comprising causing the processing circuits (TC) of a portable object to generate each random number required at the time of the data processing, when the portable object is connected to a processing apparatus, said method consisting in executing a calculation program recorded in the circuits of the objet and taking into account, for each demand for a random number at a session, at least a first parameter (PA1) constituted by the datum of a field (RB) of a memory zone of the object, said datum being modified following each demand for a random number during one session, and a second variable parameter (PA2). Such a method is known from EP-A-231 702. According to the invention, said memory zone is volatile and the second parameter is constituted by a datum of another memory zone of the object, said datum being modified at least once during each session and being preserved between the end of one session and the next session, this other zone moreover being such that the second parameter (PA2) is incapable of having the same value twice in the course of the life of the card.

In a preferred embodiment of the invention, the first parameter is constituted by the value of the content of a field having a specific address, of a volatile memory zone of the card, this field being used for memorising the latest random number calculated during the current session. Given that the field in question is a volatile memory zone, it loses its content when the circuits of the card are disconnected from voltage, such that, after the reinitialisation of the circuits of the card when

voltage is reconnected, the content of the field in question is identical from one session to another.

This is of no importance since, from one session to another, the second parameter, which is sampled from a memory zone that is nonvolatile between sessions, is modified such that, even if the first parameter has an identical value at the start of each session, the result is that the first random number calculated at a session is not foreseeable, since it depends on the value of at least two parameters, one of which (the second) cannot have the same value twice during the life of the card.

In one embodiment, the second parameter is read from a specific memory zone that is not volatile from one session to the next, but contents of which can be modified on request from the microprocessor incorporated in the card, for example after the reinitialisation of the circuits following the connection of voltage at the start of a session. In consequence, said specific memory zone, which contains the second parameter, is for example an electrically erasable and reprogrammable memory (EEPROM-type memory) zone, and the second parameter is constituted by the content of a specific field of this zone.

In a preferred embodiment, in order that the second parameter does not have the same value twice during the life of the card, its value is controlled by incrementing it from one session to another.

Preferably, at least one of the elements taken into account for calculating a random number is secret. Preferably, the secret element is one of the parameters used in the calculation. This precaution makes it possible to prevent a person intending to commit fraud from having at his disposal all the elements taken into account for calculating the random number, and from being able to simulate in advance the result of a subsequent calculation.

The invention also concerns a portable electronic object, such as a card with memory (MC) and processing microcircuits (TC), for implementing the method according to the invention, arranged so as to execute a program for calculating the

random number, memorised in a nonvolatile memory zone by taking into account, for each demand for a random number at the time of a session, at least a first parameter (PA1) constituted by the datum from one field (RB) of a memory zone of the object, said datum being modified following each demand for a random number at the time of a session, and a second variable parameter (PA2). According to the invention, said memory zone is volatile and the second parameter is constituted by a datum in another memory zone of the object, said datum being modified at least once at the time of each session and being preserved between the end of one session and the following session, this other zone being moreover such that the second parameter (PA2) is incapable of having the same value twice in the course of the life of the object.

Other characteristics and advantages will become apparent from the following description, given with regard to the attached figures in which:

- Figure 1 is a basic diagram of a system for implementing the invention;
- Figure 2 illustrates a variant for organising the memory of a portable object for implementing the invention;
- Figure 3 illustrates the principle for calculating a random number;
- Figures 4 and 5A and 5B illustrate a way in which the second parameter can be modified;
- Figures 6A-6B and 7A-7B illustrate two variants for organising the memory of a portable object.

Figure 1 illustrates the minimum elements necessary for a card with a memory to be able to function and be used. The present invention can be used to generate a random number whatever the phase in the life of the card. Hence the invention can be applied to the generation of a random number when the card is customised, that is, during a phase immediately following the manufacture of the card, which consists of entering data, secret or otherwise, which will be necessary for using the card in question.

It also applies when the card has been given to an end user, since it is necessary to generate random numbers when the card is used.

To be used, a memory-type card (1) must be connected to an apparatus (2) which may be a terminal or a transaction apparatus. The card (1) and the apparatus (2) are connected via a transmission link (3). The link can be electric and, in this case, the card is provided with contact regions that are intended to be interconnected with the corresponding contact regions of a connector incorporated into the apparatus (2); the connection could also be optical, magnetic, or other, without departing from the scope of the invention.

One type of transmission link that can be used in such a system is described in French patent no. 2 483 713, in the name of the applicant, entitled: "Dispositif pour la transmission de signaux entre deux stations de traitement de l'information" [apparatus for transmitting signals between two information processing stations] (this French patent corresponds to US patent no. 4 556 958).

The card (1) contains at least one memory (MC) and data processing circuits (TC), making it possible to process the data contained in the memory (MC) of the card, or data from outside, for example data coming directly from the apparatus (2), or relayed by it, where the system comprises several interconnected apparatuses forming a network.

In a manner known in itself, the memory (MC) of the card can be partitioned in several different memory zones, which are distinguished from one another by their electronic nature. Each zone also has a certain number of memory words that can each be identified by their address in the zone.

Hence the memory (MC) of the card (1) can contain a first ROM memory zone (11), that is, a nonvolatile memory zone, which contains in particular the data constituting the instructions of a program (PC) that can be executed by the processing circuits (TC) of the card. This first nonvolatile memory zone (11) is programmed once and for all.

The memory (MC) can also contain a second nonvolatile memory zone (12), which can however be programmed throughout the life of the card, for example under the control of the processing circuits (TC) of the latter, while respecting the access conditions that are managed by the program (PC). This second zone (12) is of the PROM type. It is in this zone that the customisation information or data of each card are recorded, such as the serial number, secret codes giving access to the system, after the checking of a corresponding code entered on a keyboard of a transaction apparatus, such as the apparatus (2), and in general all types of data, secret or otherwise, that might appear during the use of the card, and which it would be necessary to preserve throughout its remaining life. For example, in certain applications, the card is supplied to its end user with a secret code predetermined by the service provider which supplies him with this card. In some cases, the user is authorised to modify his secret code, in order to introduce one which he has made up deliberately. A modified code of this kind is memorised in this second, PROM-type zone (12). It is also in this zone that the status memory, mentioned in the preamble to the present application, can be constituted, which memory serves for storing attempts at access or the number of operations performed with the card (1) since its first use, for example.

As mentioned previously, this second memory zone (12) can contain information that has to remain secret from the outside, such as access codes, which means that only the processing circuits (TC) of the card will be able to exploit this information, whereas other parts of this second zone are accessible in read and/or write mode indiscriminately by the processing circuits (TC) of the card or by the processing circuits (TA) of the apparatus (2). This structure is well known in the prior art, and has been implemented in particular for many years on the applicant's products.

A card for implementing the method of the present invention comprises a third EEPROM-type memory zone (13), that is, a memory that is nonvolatile when there is no electric supply to the card, but which can nevertheless be modified on request from the processing circuits, or on a request from outside, either word by word, or in part, or else in its totality. Such a memory zone is commonly known as an electrically erasable and reprogrammable memory zone.

In a preferred embodiment, the present invention exploits the presence of this third zone in a particularly advantageous manner, to obtain random numbers without excessive consumption of memory.

It should be noted that the use of EEPROM-type memory zones has been envisaged for some time already, in memory-type cards, to increase the period of use of these cards. Indeed, although possibilities of integrating components with higher and higher performance are being achieved, nevertheless the memory capacity of portable objects, such as cards with microcircuits, is limited. A memory-type card is an information medium containing information that has to remain permanent, such as information allowing the cardholder to be identified, and/or information that may be only temporarily of use. Thus, in banking or monetary applications, information such as the balance of an account is information that evolves. In the first kinds of memory-type cards, it was envisaged that such information could be recorded in the PROM-type memory zone, that is, the memory zone that could be recorded but was not subsequently volatile. Consequently, when a new balance had to be recorded, the preceding balance was preserved, which used up the memory unnecessarily. For any one type of use, that is, banking or monetary use, the use of an EEPROM-type memory allows the memorising of this type of information, which is not of use during the whole life of the card, but which nevertheless has to be preserved temporarily.

In all types of applications, there is information and data which do not have to be preserved eternally, and an EEPROM-type memory is particularly suitable in this case.

The management of this memory zone, particularly the determination of the moment when all or some of the fields it contains have to be erased in order to be reused, does not form the subject-matter of the present invention, but depends mainly on the type of application for which the portable object is intended. However, a much more precise explanation will be given later of how the invention takes advantage of the presence of this EEPROM-type memory zone (13).

The card memory (MC) can also contain a fourth, RAM-type volatile memory zone (14), that is, a memory zone in which the data it contains are lost as soon as electric power is disconnected from the card. This zone can be used to store information or data which are known in advance not to be necessary from one session to another. Furthermore, this fourth memory zone (14) is used at the time that the third, EEPROM-type zone is erased, for the temporary storage of certain data from this third zone which will have to be re-recorded after it has been erased.

For example, in banking applications, the balance of a customer account that was recorded in the third EEPROM zone would have to be transferred to this fourth (RAM-type) memory zone (14), before the EEPROM-type zone is erased, and then it would once again be transferred from the fourth zone (14) to the third (13).

The present invention also takes advantage of the presence of this fourth memory zone (14) when random numbers are calculated.

Finally, the memory (MC) of the portable object (1) can comprise a fifth, EEPROM-type memory zone (15), that is, a zone that is nonvolatile when electric power to the portable object is disconnected, but which can nevertheless be erased totally, for example by subjecting it to exposure to ultraviolet radiation.

An apparatus (2) for exchanging data or information with a card (1), and for the complete or partial processing of this information, has a structure known in itself. Reference may be made to numerous patents in the name of the applicant in this field, and in particular French patent no. 2 601 535, to name but one. Such an apparatus (2), which can be a transaction terminal, or an element in a customisation machine, comprises in particular data processing circuits (TA), which can execute appropriate programs, the instructions (PA) of which are recorded in a memory (MA) incorporated in, or associated with, said apparatus. The memory (MA) of the apparatus can be much larger than that (MC) of the card (1), and can be built up from electronic elements and/or from peripheral memories, such as floppy disks, or other media known in the field. The memory (MA) of the apparatus can contain a nonvolatile zone, with secret data that will be used during different transactions, and

in the processes of checking the validity of cards connected thereto. Such processes are known as authentication processes.

The secret data and the program (or at least part of it) of the apparatus can be incorporated into an integral security module, more commonly known in the field by the abbreviation MCS.

Figure 2 illustrates a variant for organising the memory of the object allowing a random number to be obtained in such a system implementing the present invention.

A random number is obtained by applying a algorithm for calculating at least two parameters, the first of which (PA1) is constituted by a datum in a memory field (RB) of the card or the portable object, the content of which is modified each time a random number is requested in a session, and the second of which (PA2) is constituted by a datum in another memory field (RI), the content of which is modified at least once at each session. Furthermore, the second parameter is chosen in such a way that it is not capable of having the same value twice during the life of the portable object or the card with memory and microcircuits.

In a preferred embodiment, the first parameter (PA1) is constituted by the value of the latest random number calculated during the current session. In order to allow the use, for a subsequent calculation, of the latest random number calculated during the current session, it is necessary to provide, in the memory of the portable object or card, a memory field (RB) in which this latest number is memorised. As in any information processing system, each of the memory zones can be split into several fields or words, which can be identified by their addresses. In accordance with the present invention, in order to allow the storage of the latest random number calculated at a session, the fourth (14) RAM memory zone, that is, the one where the content is destroyed each time the portable object is disconnected, is provided with the field (RB) for memorising the latest random number calculated during the current session. When a random number is calculated, this field (RB) is filled with said random number which constitutes the first parameter (PA1) at a subsequent

calculation. At a subsequent calculation, the new random number calculated is substituted for the random number that had been calculated and stored previously. The address or the position in memory where the random number has to be stored can be fixed once and for all, or else determined during a session by the processing circuits of the portable object. This aspect is not of capital importance, the only important aspect being that the processing system is in a position to determine the location in memory (14) of the last random number calculated.

Each time the circuits of the portable object or the card are connected to voltage, the first parameter is capable of having an identical value, since it is stored in a memory zone, the content of which is erased each time the circuits are connected to voltage, which zone is reinitialised each time voltage is reconnected. This has no importance, since this program for calculating a random number takes account not only of this first parameter, but also of a second parameter, the value of which is not capable of being identical twice during the life of the card.

This embodiment is particularly economical of memory, since only one memory field, containing a number of bits corresponding to the format of the random number that one wishes to calculate, needs to be provided in the volatile (RAM) memory zone (13), and since, each time a random number is calculated, it is sufficient to replace the value contained by this field at the end of the preceding calculation, or on reconnection of voltage to the circuits, by the new number calculated.

By way of example, the various memory zones of a card with memory and electronic microcircuits, in credit card format, comprise words of 32 bits. In a preferred embodiment of the invention, the calculation of random numbers is performed on 64 bits, such that it is sufficient to reserve two 32-bit words in the fourth volatile memory (RAM) zone (14) of the memory of the card or the portable object in order to constitute the memory field (RB) for memorising the random numbers calculated in succession at a session.

Figure 2 illustrates what has just been described. It shows in greater detail a memory of a portable object for implementing the invention. Thus, the fourth volatile

memory zone (14) has been shown with several fields. In the field (RB) there is a broken line to signify that the field (RB) could be constituted of one or more words, which is the case when the random number is calculated on 64 bits, whereas the memory contains words of 32 bits.

Figure 2 also illustrates which other parts of the memory are capable of being used when calculating and generating a random number. In particular, in the fourth memory zone (14), that is, the volatile zone, a field (ZT) has been shown, constituted on the basis of several memory words (ZT1, ZT2), which is used during the phase of modifying the second parameter from one session to another, as will be explained below.

The third memory zone (13) contains a field (RI) that can also be constituted of several words (PA21, PA22). It is the overall content of this field that constitutes the second parameter (PA2) used for calculating a random number.

The program for calculating a random number is preferably recorded in a nonvolatile part of the memory. It can be recorded in the first memory zone (11) of the read-only type (ROM), at the time that this is masked, or it can be recorded after the card or portable object has been put into use, within the second, PROM-type zone (12).

This calculation program makes use of a function (F) which can be more or less complex. To calculate the random number, the processing circuits of the portable object read and sample the content (PA1) of the field (RB) of the fourth memory zone; they read the second parameter (PA2) contained in the field (RI) of the third zone (13), and the function (F) for calculating the random number is applied, such that a random number (RN) is a function of the two parameters:

RN = F (value of PA1, value of PA2).

Next, after a random number has been calculated, the operating program of the card or the portable object is such that the processing circuits (TC) of the card or the portable object record the result of this calculation in the field (RB), so that it can be

used for any subsequent calculation of the random number during the current session.

Of course, when a random number is calculated for the first time in a session, the content of the field (RB) is not a function of the result of a preceding calculation, since the field (RB) is located in a volatile memory zone. As has already been mentioned, this is of no importance, since the content of the field (RB) constitutes only one of the parameters taken into account for calculating a random number, the other parameter (PA2) being constituted by the content of a field (RI) in the third memory zone (13). Now, the content (PA2) of this field (RI) is modified once during each session, such that, from one session to another, it does not have the same value.

The content of the field (RI) of the third zone (13), constituting the second parameter (PA2) taken into account when a random number is calculated, is preferably modified at the start of each session, before a random number has been calculated. The modification of the content (PA2) of this field (RI) immediately follows, for example, the reinitialisation of the circuits of the card of the portable object, after connection to voltage. This systematic modification, after reinitialisation, or at least before the first calculation of a random number, means that the problems of fraud can be avoided. Indeed, if this precaution has not been taken, a person intending to commit fraud could very well disconnect his card before the content (PA2) of the field (RI) had been changed during a session, such that, at the start of the next session, the second parameter would have the same value. Since, *a priori*, at the start of each session the first parameter contained in the field (RB) is identical after the reinitialisation of the circuits, the result would be that, by observing the calculations that had taken place during the preceding session, it would be possible to predetermine the results of the next session. This precaution is therefore particularly useful.

In one embodiment, the second parameter (PA2), contained in the field (RI) of the third memory zone (13), is modified by incrementing the value of this parameter, with the aid of the processing circuits of the card or the portable object. Since this

parameter is contained in an electrically erasable and reprogrammable zone, the operating program for the processing circuits of the portable object or the card with a memory and microcircuits is such that only the content (PA2) of said field (RI), or of part of it, can be modified from one session to another, without the need for intervention in the other fields of this zone (13). This does not constitute a disadvantage, since it is quite possible, with EEPROM-type memories, to modify only the content of given fields of these memories, without modifying the rest of said memories.

In a preferred embodiment, the function used to calculate a random number uses an encoding algorithm such as the algorithm known and commonly denoted by its initials (DES), from its English name "Data Encryption System", or only some of the functions usually comprised by this algorithm.

Furthermore, the generation of a random number preferably takes into account at least a third parameter (PA3) which makes it possible to diversify the results of calculation from one portable object, or card, to another. Indeed, assuming that a person intending to commit fraud wanted to deceive the system and has two identical cards, and given that the programs used are the same, then if the first parameter of a first card were identical to the first parameter of a second card, and if at the same time the second parameter of the first card were identical to the second parameter of the second, then the results of calculating random numbers applied to these two cards would be identical. A person intending to commit fraud could take advantage of this aspect in order to try and deceive the system, by transposing the observations made from a first card to a second one. For this reason, in this preferred embodiment, the third parameter (PA3) is for example a parameter unique to each of the cards, which is recorded after manufacture in a nonvolatile memory zone for the whole life of the card. This parameter (PA3), which has been shown in Figure 2 in a memory field of the second nonvolatile zone (12) of the card, could also be installed in an EEPROM-type memory zone, that is, a zone corresponding to the third zone (13) in Figures 1 or 2, as long as the operating program of the card is such that, should this third parameter be installed in an EEPROM memory zone, it cannot be erased at any time in the life of the card.

Hence it can be envisaged that the serial number of the card, or any other key or datum specific to each of the cards, in so far as they exist, could be used as the third parameter (PA3). Indeed, it has been said previously that random numbers could be requested at any phase in the life of the card, that is, during the manufacturing phase, the precustomisation phase or the customisation phase, or else when the card has been given to its end user.

Cards can be encountered in which, during the manufacturing or precustomisation phases, there are as yet no data distinguishing between the various cards in the same batch, such that it is impossible, or difficult, to obtain different random numbers between two cards in the same batch. This is not very important since, at the end of these phases, which are carried out under the direct control of the manufacturer, that is, under maximum security conditions, a moment is very soon reached when the various cards in any one batch contain at least one data distinguishing one from another.

During the manufacture of the components a manufacturer key is recorded, that is, a datum specific to the manufacturer of a batch of cards. Each random number requested during the manufacturing and precustomisation phases, after this manufacturer key has been recorded, will be obtained by using this manufacturer key as a third parameter (PA3). At the end of these manufacturing and precustomisation phases and during the customisation and use phases, use will be made of either a customisation key or the serial number, or else a combination of these various keys or specific data, to constitute the third parameter (PA3).

In Figure 2, the fifth, EPROM-type zone (15) does not contain any of the parameters used for calculating random numbers. It is however possible for the third parameter (PA3), or all or some of the customisation data, to be recorded in this fifth EPROM-type zone (15) instead of being recorded in the second PROM-type zone (12). This can be the case for example when provision is made for the service provider to "refresh" the portable object during its life by modifying the customisation data recorded in it.

Finally, in a variant not shown, the third parameter (PA3) or, in general, all or some of the customisation data, are recorded in the third EEPROM-type zone (13).

Figure 3 illustrates a complete basic diagram of the calculation of a random number, and Figure 4 illustrates a procedure for incrementing the second parameter (PA2), where each of the memory zones is composed of 32-bit words and where 64 bits, that is, two words, are used, at least for calculating the random number, and where this second parameter (PA2) is memorised in an EEPROM-type memory zone.

Preferably, an algorithm such as (DES) is implemented by memorising the data involved in the calculation in a buffer memory specific to (DES). This is what has been illustrated in Figure 3, which shows this specific buffer memory, known by the name (DES BUFFER). In a first phase (31), the content of the field (RI) containing the second parameter (PA2), in the third, EEPROM-type zone (13), is loaded into the buffer memory of the DES (DES BUFFER). Next, the content of this buffer register or memory and the content of the field (RB), constituting the first parameter, are combined together (phase 32), so as to obtain a 64-bit word, in the example considered, which is then memorised in the buffer register of (DES) (phase 33). The operation, performed between the content of the field (RB) and the content of the buffer register (DES) during phase (32), is a logic operation such as EXCLUSIVE OR, AND, etc., which makes it possible to combine the content of the buffer register of (DES) and the content of the field (RB). A more complex operation may also be involved, but one resulting in an intermediate parameter, the size of which is compatible with the memory size of the buffer register of DES (DES BUFFER).

This Figure 3 illustrates the case where random number generation takes into account not only the first two parameters, but also a third parameter (PA3), such as a specific key as mentioned previously. In one phase (34), for example, the algorithm (DES), or all or part of it, or any other algorithm allowing encoding to be carried out, is applied to the new content of the register of (DES), coming from the result of the operation carried out during phase (32), and to the specific key that has been mentioned and which is, for its part, sampled from the memory zone in which it is stored. The result of the operation carried out during this phase (34) is then

recorded in the register of DES (DES BUFFER), before being recorded in the field (RB) of the fourth volatile memory zone of the card or the portable object. Thus, a new random number is immediately stored in the appropriate field, with a view to possible subsequent calculation.

So that the notion of random number is total, and any risk of fraud is obviated, in a preferred embodiment additional precautions are taken, applying in all the variant ways of distributing the different parameters among the various zones.

Indeed, everything described above shows that the invention makes it possible to prevent any one combination of parameters from recurring during the life of the card, so that simple observation or knowledge of the parameters will not make it possible immediately to deduce the random number that will be obtained. However, knowledge of these parameters and the calculation algorithm would allow a competent person intending to commit fraud, who had the appropriate equipment, to calculate in advance the future random number.

This could be the case with the use of an algorithm such as DES or part thereof, since this algorithm is in the public domain.

For this reason, in a preferred embodiment, at least one of the elements taken into account when calculating random numbers is secret, thus preventing competent persons intending to commit fraud from predicting in advance the results of subsequent calculations.

Preferably, the secret element is one of the parameters used during the calculation. Given that the first parameter (PA1) sampled from the field (RB) of the fourth memory zone is the random number calculated previously, this first parameter cannot be secret since it is intended to be transmitted from the card to the apparatus (2) to which the card is connected. Thus there remains the possibility of making the second parameter (PA2) and/or the third parameter (PA3) secret when account is taken of said parameter during calculation.

There are known methods, which the applicant moreover uses in a number of its products, to keep secret the information contained in given memory zones. One of the best known methods consists in associating a locking bit with the words intended to be protected in read mode with respect to external circuits, said locking bit being set to a predetermined state indicating to the processing circuits (TC) of the portable object (1) whether or not the information in question has to remain secret with respect to external circuits.

In the particular case of the present invention, the second parameter (PA2) or else the third parameter (PA3), can thus be made accessible in read and write mode solely by the processing circuits (TC) of the portable object, by associating with these parameters at least one bit indicating to the processing circuits that the value of the parameter must not be transmitted externally. This bit is preferably set to an appropriate value at the end of the manufacture of the portable object. In a variant, it is the management program of the portable object, stored in ROM or in PROM, that manages access to the memory zones.

Of course, it is necessary that neither the parameters (PA2) and (PA3), nor the parameter (PA1), can be modified on request from outside. Indeed, if a person intending to commit fraud knew the algorithm and managed to give the value he wanted to the parameters, he could deceive the system. For this reason, all the parameters used for calculating the random number are protected externally in write mode, and their content can only be modified under the control of the processing circuit (TC) of the portable object. This protection can also be given by locking bits, or by the management program of the object itself.

As mentioned before, the second parameter (PA2) contained in the field (RI) of the third memory zone (13) is modified by incrementation at each session. In a preferred embodiment of the invention it is provided that, on customisation of the memories of the portable objects, the second parameter (PA2) is not initialised to the same value in each of the portable objects. This precaution proves useful for applications in which only a first (PA1) and a second (PA2) parameter are taken into account. In that case, if the second parameter were identical in each of the cards

or portable objects, after manufacture, then a person intending to commit fraud who procured several cards could, on the basis of observations made on a first card, deceive the system by using other cards he had at his disposal.

In one embodiment, this initialisation to different values of the second parameter (PA2) is carried out on the customisation of the portable object (1). The value of the second parameter is calculated or extracted from the processing circuits (TA) of the customisation apparatus, and is then recorded within the field (RI) of the third zone (13), while said third zone is not yet write-protected with respect to the outside. During this customisation phase, when the initial value of the second parameter (PA2) has been recorded, then the bit for write-protection with respect to external circuits is set as appropriate.

The initial value of the second parameter (PA2) that must be recorded in each of the cards can be determined by a calculation performed either in the processing circuits (TC) of the card, when it is connected to the customisation machine, or in the processing circuits (TA) of the customisation machine. When the calculation is performed by the processing circuits (TC) of the portable object (1), it can take account of the value of the serial number of the object, since this differs from one object to another, such that the initial value of the second parameter (PA2) is highly likely to differ from one portable object to another.

When the calculation is performed by the processing circuits (TA) of the customisation apparatus, the value of the second parameter to be recorded in the memory of the portable object can be obtained following a calculation taking account of a random number generated at the level of the customisation apparatus, or it can be a value of a register of the memory (MA) of the customisation apparatus, incremented each time a new portable object is introduced.

Other solutions can be envisaged for initialising the second parameter at the end of manufacturing the portable object, the essential factor being that a person who might commit fraud knows, in the event that he has several portable objects, that they do not necessarily have the same initialisation values and that, consequently,

he cannot simulate in advance the results he will obtain with each of the objects he possesses.

When a third parameter (PA3) is used for calculating a random number, as was envisaged before, this parameter (PA3) has to be secret, when the parameter (PA2) is not, and when it is desired to offer the maximum degree of security. Of course, when the second parameter (PA2) is secret, it is not necessary for the third parameter (PA3) to be so. On the other hand, when the third parameter (PA3) is secret, then the second parameter (PA2) does not necessarily have to be secret.

As has been mentioned, the third parameter (PA3) can be the serial number of the portable object, or a specific key recorded when the portable object is customised. In general, the serial number has to remain accessible in read mode by any processing circuit (TA) of an external apparatus (2) for processing data contained in the memory of the portable object. In this case, when the third parameter used is the serial number, then the second parameter (PA2) must be inaccessible in read mode to the processing circuits (TA) of an external apparatus (2). On the other hand, any other diversified, secret datum specific to a given portable object can constitute the third parameter (PA3), and it is not necessary to provide a specific one for calculating random numbers.

Figure 4 illustrates a procedure for incrementing the second parameter when it is constituted by two memory words, for example two 32-bit words, such that the second parameter comprises 64 bits. More specifically, Figure 4 shows a flow chart of the operations that can be used to perform this incrementation.

Figure 4 can be understood by referring also to Figure 2, the elements of which, that were not described previously, are described now.

As shown in Figure 2, in such a case, the field (RI) of the third zone (13) containing the second parameter (PA2) is constituted by two sub-fields (PA21 and PA22) each constituted by one memory word.

Furthermore, in the volatile memory (14), a buffer field (ZT) has been provided, also comprising two sub-fields (ZT1 and ZT2) which are used during this incrementation phase which, as will be recalled, takes place after each reinitialisation of the circuits of the card or the portable object, after reconnection to voltage, that is, after the portable object or card (1) has been put into communication with the appropriate transaction apparatus (2).

A first phase consists in loading the content of the first sub-field (PA21) of the third zone (13) into the first sub-field (ZT1) of the fourth zone (14). Then the content of the second sub-field (PA22) of the third zone (13) is loaded into the second sub-field (ZT2) of the fourth zone (14).

As a result, following these loading operations, the buffer field (ZT) of the fourth zone (14) has the same content (PA2) as the field (RI) of the third zone (13), that is, it contains the second parameter.

Following these loading operations, a test is made between the content of the sub-fields (ZT1 and ZT2) of the fourth zone (14), in order to check whether the value of the content of the first sub-field (ZT1) is greater than or equal to the value of the content of the second (ZT2).

If it is, then the value of the first sub-field (ZT1) of the fourth zone is incremented, and the second sub-field (PA22) of the third zone (13), that is, the one where its content was loaded into the second sub-field (ZT2) of the fourth zone (14), is erased, and the new value of the first sub-field (ZT1) of the fourth zone (14) is recorded in the second sub-field (PA22) of the third (13), such that the new second parameter is constituted as follows: content of the first sub-field (PA21) identical to that of the preceding session, and content of the second sub-field (PA22) corresponding to the content of the first (PA21) incremented in comparison with the preceding session.

When the test mentioned before reveals that it is in fact the content of the second sub-field (ZT2) that is greater than that of the first (ZT1), which means that in fact

the content of the second sub-field (PA22) is greater than that of the first sub-field (PA21), then the content of the second sub-field (ZT2) of the fourth volatile zone (14) is incremented, and then the content of the first sub-field (PA21) of the third zone (13) is erased and replaced with the content of the second sub-field (ZT2) obtained after incrementation.

Naturally, the procedure that has just been described is not limiting, and any other procedure could have been chosen. In particular, if one had wanted to make do with random numbers, of a length corresponding to the length of the words in the memory, then it would have been sufficient for the second parameter (PA2) to have been constituted only by a single word, and the incrementation procedure would have been much simpler, since it would have been done in the same way as in a counter.

The procedure that has just been described is therefore particularly suitable when it is desired that the random number be large enough to be sufficiently significant.

With the procedure that has just been described it will be noted that, when the second parameter (PA2) is constituted by two memory words, the evolution of this parameter (PA2), on successive incrementations from one session to another, is such that each of the words constituting this parameter is modified once every two times, and that the modification of a word consists in replacing this word by the other word after it has been incremented.

However, the fact that the second parameter is constituted by two words each having a number N of predetermined bits does not significantly increase the number of possible combinations in order to constitute this second parameter. As has been mentioned before, this constitution with the aid of two or more words simply makes it possible to adapt the format of the parameter (PA2) to the desired random number format.

Indeed, since each word constituting the second parameter is modified once in two times, it will be noted that the total number NT of different second parameters (PA2)

that can be obtained is calculated as follows: $NT = 2^N + 1$. If the parameter (PA2) had been constituted with the aid of a single word of N bits, then the total number NT' would have been: $NT' = 2^N$. This is illustrated by Figures 5A and 5B which show how the second parameter (PA2) evolves when it is composed of one three-bit word (Figure 5A), or of two three-bit words (Figure 5B) incremented as described with respect to Figure 4. In Figure 5A, it will be noted that there are only eight possibilities for the second parameter (PA2), when said second parameter is constituted of only a single three-bit word while, in Figure 5B, it will be seen that there are nine possibilities.

In one embodiment, the second parameter (PA2) is constituted by two 32-bit words, and it is then determined that it can take around 4,300 million different values. This is ample since, assuming that the card is connected permanently to a terminal, and that one random number is calculated every second, there would have to be a permanent connection lasting 136 years in order to exhaust the possibilities, also assuming that the initial value of the second parameter (PA2) is zero (binary 0) and that each incrementation involves one unit. Indeed, in a number of practical applications, the life or period of use is intentionally restricted to a few years.

When the present invention applies to a portable object or a card possessing an EEPROM-type memory zone, it is possible to generate random numbers in a particularly memory-saving way, as has just been illustrated.

However, not all applications use cards or portable objects with an EEPROM-type memory. The invention nevertheless applies to systems using cards or portable objects that do not have such an EEPROM-type memory zone, as illustrated by Figures 6A to 7B.

Figure 6A illustrates a first variant of a system that does not comprise an EEPROM-type memory, and Figure 6B illustrates more particularly how the parameters (PA1, PA2, PA3) are stored in the memory.

A system such as that illustrated in Figure 6A comprises a portable object (100) such as a card with a memory (MC) and circuits (TC) for processing data in the memory. The system also comprises at least one apparatus or transaction machine (200), identical or similar to that illustrated in Figure 1, and therefore comprising processing circuits (TA) and a memory (MA), part of which is used to store an operating program (PA).

The memory (MC) of the portable object (100) comprises a first ROM-type memory zone (110), in which the operating program (PC) of the portable object can be recorded. Such a memory would also comprise a second, PROM-type zone (120), that is, a programmable nonvolatile zone, and finally a third, RAM-type zone (140).

Figure 6B illustrates the way in which the parameters are managed and distributed among the various memory zones (MC) of the portable object.

The first parameter (PA1) is stored in a field (RB) of the RAM-type zone (140). Preferably, as was the case with the variant illustrated in the preceding Figures 1 to 5, the first parameter (PA1) is the latest random number calculated during the current session. This first parameter (PA1) can also occupy several memory words, which is illustrated by a broken line passing through the field (RB) in Figure 6B.

As in the variants illustrated with regard to Figures 1 to 5, the third parameter (PA3), which can also occupy several memory words, is stored in a field of the PROM-type memory zone (120). This third parameter can be the serial number of the portable object, or a secret diversified datum specific to that object.

The difference between the variant illustrated by these Figures 6A and 6B and the variants illustrated by the preceding figures lies in the fact that, because of the absence of an EEPROM-type memory zone, the second parameter, modified at each session, has to be stored and managed in a different way. In this case, the second parameter (PA2) is constituted by a datum in the PROM-type memory zone (120), that is, the one that also contains the third parameter. As has been indicated with regard to Figures 1 and 2, the PROM-type memory zone is the one, at least

part of which is used as a control memory, that is, the one used for memorising events arising during the life of the portable object. In fact, the control memory is constituted by a number of words in the zone, and it is modified under the control of the processing circuits (TC) of the portable object. As has been explained in the preamble to the present application, a word in the control memory can be modified as many times as it comprises bits, in so far as each modification involves one bit. In other words, if each word of the control memory comprises eight bits then, in theory, each word is capable of recording eight different control operations before the following word in the control memory starts to be modified. In practice this is not absolutely true, since certain control operations are encoded over several bits, for example, two or three bits. However, it is easy to understand that it will be very rare for a word in the control memory to be modified on a single occasion. Thus, while there are still bits available in a word of the control memory, that is, bits that have not been modified in comparison with their original state, between the last bit modified and the end of the word in which this last modified bit is located, then it is possible to reuse this word. However, as has been explained, also in the preamble to the present application, a word in the control memory can take the same binary configuration as another word previously modified in this memory, and this is why, in a preferred embodiment, the second parameter (PA2) is constituted by the latest word modified in the control memory, and by the address in memory of this word.

Thus, by taking into account not only the value of the latest word modified in the control memory, that is, a word known to have been modified relative to the preceding session, but also the value of the address of this word, it is certain that the second parameter (PA2) cannot have the same value twice in the life of the card.

This solution is economical of memory, since it avoids having to provide a specific memory zone for constituting the second parameter (PA2), taking advantage of the existence of a portion of memory where the data are capable of changing from one session to another.

In a variant, which could be used in cases where the memory (MC) of the portable object (100) does not comprise a control memory, or in cases where the control memory is likely not to be modified at each session, then part of the PROM-type zone (120) is reserved in order to constitute the second parameter. More specifically, a certain number of words in this zone are reserved and can be modified, for example, bit by bit. The modification of this zone, in order to cause the second parameter to evolve over successive sessions, can be carried out as follows: each word in the part of the PROM-type memory zone (120) allocated to the second parameter (PA2) can be modified bit by bit such that, at the start of a session, after the reinitialisation of the processing circuits of the portable object, one bit of a word is modified and, at the next session, the following bit of the same word is modified. When all the bits of any one word have been modified, then the following modification affects the first bit of the next word in this part of the zone. In this way, each time a random number is requested at a session, the second parameter is constituted at least by the latest word modified in this part of the zone and by the address in memory of this latest word modified. This means that, when the word taken into account changes, the second parameter does not revert to a value it has already had, since account is also taken of the address.

This solution is somewhat more memory-consuming, since part of the zone is reserved specifically for the second parameter, but the additional consumption is fairly relative. Indeed, assuming a portable object, the memory of which was constituted of 32-bit words, the life of which was intentionally limited by the service-provider to two years, and which was used for two sessions a day, 46 words would have to be reserved in the PROM-type memory zone (120), which corresponds to 184 bytes of memory. This is relatively little compared with the usual size of memory of portable objects of this type.

In general, the control memory has to be accessible in read mode from outside and, where the second parameter is constituted by the latest word modified in the control memory, it cannot be secret. In this case, it is the third parameter (PA3) that must be secret and, for this third parameter (PA3), a datum specific to the portable object in question is chosen.

On the other hand, when the second parameter is constituted by the latest word modified in a specific part of the PROM-type memory (120), it is possible to make it secret and, in this case, the third parameter (PA3) is not necessarily secret and can be constituted simply by the serial number, or by any other datum specific to the portable object in question.

Figure 7A illustrates another variant of the invention in which the memory (MC) of the portable object (100) does not have an EEPROM-type memory zone. This variant differs from that in Figure 6A in that, in addition to the zones described with regard to Figures 6A and 6B, it has an EPROM-type memory zone (150), that is, a nonvolatile zone that is nevertheless erasable, for example by exposure to ultraviolet. In contrast with EEPROM-type zones, it is not possible to select the parts of the zone that are capable of being erased, so that erasing affects the whole zone.

The variant illustrated in Figure 7A allows the second and third parameters to be memorised in and sampled from the PROM-type zone (120), as was the case in the variants illustrated by Figures 6A and 6B, the first parameter itself always being stored in the (RAM)-type memory zone (140). Furthermore, the second parameter can be constituted by the latest word modified in the control zone, when it is present, and by the address of this latest word modified, or by a latest word modified, and its address in a specific part of this PROM-type zone (120). The third parameter (PA3) can be constituted by the serial number of the portable object, or by any other datum specific to the portable object in question, whether secret or not, according to whether or not the second parameter (PA2) is secret.

On the other hand, it is perfectly possible for the presence of the EPROM-type zone (150) to be profitably employed in order to store the second and/or third parameter, with the same criteria as those defined with regard to Figures 6A and 6B. This is what is illustrated by Figure 7B, in which the field (RI) containing the second parameter has been shown in the EPROM-type memory zone (150).

This field containing the second parameter (PA2) can be the control memory, or a specific field such as that described previously with regard to Figures 6A, 6B and 7A.

The calculation of a random number in a system that did not comprise an EEPROM-type memory zone would nevertheless be identical to that illustrated by Figure 3 and described in the corresponding part of the description.

Naturally, the invention is not limited to the embodiments described, but also extends to all equivalents within the scope of the person skilled in the art.

* C L M S *

CLAIMS

1. A method for generating a random number in a system with portable objects, such as cards with electronic memories and microcircuits, of the type comprising causing the processing circuits (TC) of a portable object (1, 100) to generate each random number required at the time of the data processing, when the portable object is connected to a processing apparatus (2, 200), said method consisting in executing a calculation program recorded in the circuits of the objet and taking into account, for each demand for a random number at the time of a session, at least one first parameter (PA1) constituted by the datum of a field (RB) of a memory zone (14) of the object, said datum being modified following each demand for a random number during one session, and a second variable parameter (PA2), characterised in that said memory zone (14) is volatile and the second parameter is constituted by a datum in another memory zone (120,13, 150) of the object, said datum being modified at least once during each session and being preserved between the end of one session and the next session, this other zone (13) moreover being such that the second parameter (PA2) is incapable of having the same value twice in the course of the duration of the life of the card.

2. A method for generating a random number according to Claim 1, characterised in that it consists in providing, in the volatile memory zone (14), a specific field (RB) for memorising each random number calculated successively at the time of a session, the new number being substituted for the old in this field, and that the first parameter (PA1) is constituted by the datum contained in this specific field (RB).

3. A method for generating a random number according to Claim 1, characterised in that the second parameter (PA2) is kept inaccessible, for reading and writing, to the processing circuits (TA) of an apparatus (2, 200) for processing the data contained in the portable object (1, 100).

4. A method for generating a random number according to Claim 3, characterised in that each portable object intended for the same application is initialised such that the second parameter that it contains is not the same in the set of said portable objects.

5. A method for generating a random number according to Claim 1, characterised in that it consists in causing at least one third parameter (PA3), constituted by a datum specific to the portable object in question, to be taken into account, in addition to the two aforementioned parameters (PA1, PA2).

6. A method for generating a random number according to Claim 5, characterised in that the third parameter (PA3) is kept inaccessible, for reading and writing, to the processing circuits (TA) of an apparatus (2, 200) for processing the data contained in the portable object (1, 100).

7. A method for generating a random number according to Claim 1, characterised in that the second parameter (PA2) is modified at the beginning of each session, after the reinitialisation of the circuits of the portable object (1, 100), following its connection to the appropriate processing apparatus (2).

8. A method for generating a random number according to any one of the preceding Claims 1 to 7, characterised in that, each memory zone of the portable object being divided into words, the second parameter (PA2) is constituted by at least one word of a memory zone (120, 13, 150) that is nonvolatile between two sessions, and that the modification of this second parameter consists in incrementing the value of at least one of its constituent words (PA21, PA22).

9. A method for generating a random number according to Claim 8, characterised in that the second parameter (PA2) is constituted by the latest word modified and its address in memory, in a portion of a PROM- or EPROM-type zone (120, 150), the contents of one of the words of which are modified at least once during each session.

10. A method for generating a random number according to Claim 9, characterised in that said portion of the zone (120, 150) is the control memory of the portable object, and that the second parameter (PA2) is constituted by the latest word modified of this control memory during the current session, and by the address in memory of this word.

11. A method for generating a random number according to Claim 9, characterised in that said portion of the zone (120, 150) is a specific portion, the contents of which are modified upon request of the processing circuits (TC) of the portable object, after the reinitialisation of the electronic circuits of this object, and that each modification of this portion affects a different bit of one of the words of this portion.

12. A method for generating a random number according to Claim 8, characterised in that the second parameter is constituted by two words (PA21, PA22) of a field (RI) of the other zone (13); that this zone is of the electrically erasable and reprogrammable type (EEPROM); and that, to increment this second parameter (PA2), its two binary words (PA21, PA22) are memorised in a buffer memory field (ZT) of the volatile memory zone (14); that, in this buffer memory, the one of the two words (ZT1, ZT2) having a value higher than the other is detected; that the word having a higher value is incremented; and that, in the EEPROM memory zone (13), the word thus incremented is substituted for the word that had the lowest value (PA21) or (PA22).

13. A portable electronic object, such as a card with memory (MC) and processing microcircuits (TC), for implementing the method according to one of Claims 1 to 12, arranged to execute a program for calculating the random number, memorised in a nonvolatile memory zone (11, 12) by taking into account, for each demand for a random number at the time of a session, at least one first parameter (PA1) constituted by the datum of one field (RB) of a memory zone (14) of the object, said datum being modified following each demand for a random number at the time of a session, and a second variable parameter (PA2), characterised in that said memory zone is volatile and the second

parameter is constituted by a datum of another memory zone (120, 13, 150) of the object, this datum being modified at least once at the time of each session and being conserved between the end of one session and the following session, this other zone (13) being moreover such that the second parameter (PA2) is incapable of having the same value twice in the course of the duration of the life of the object.

14. A portable electronic object according to Claim 13, characterised in that the other zone intended to memorise the second parameter (PA2), is a PROM-type (120) or EPROM-type (150) memory zone.

15. A portable object according to Claim 13, characterised in that the other zone (13) for memorising the second parameter (PA2) is of the EEPROM type, and that the volatile memory zone (14) serving to memorise the first parameter (PA1) further comprises a field (ZT) reserved for temporarily memorising the second parameter (PA2) at the time of its modification.

16. A portable object according to Claim 13, characterised in that it comprises, memorised in a nonvolatile memory zone (12, 13), at least one datum specific to the portable object in question, constituting a third parameter (PA3) taken into account at the time of the generation of the random number.

17. A portable object according to Claim 16, characterised in that the third parameter (PA3) is constituted by the serial number of the portable object.

18. A portable object according to Claim 16, characterised in that the third parameter (PA3) is constituted by a secret diversified datum belonging to the portable object.

19. A portable object according to Claim 13, characterised in that the first parameter (PA1) memorised in the field (RB) of the volatile zone (14) of the memory, following each calculation of a random number, is the random number itself.

20. A data processing system for implementing the method defined by one of Claims 1 to 12, characterised in that it comprises a portable object (1) according to one of Claims 13 to 19, and a processing apparatus (2) to which the portable object can be connected.