



Method for generating cryptographic half-keys, and associated system

The present invention relates to a method for generating cryptographic half-keys and its implementation system. It applies notably to the creation of several keys for access to a secure apparatus.

5

An apparatus designed for handling sensitive information may be made secure by encrypting this information with the aid of a cryptographic key composed of several distinct elements. Such a key is thus conventionally defined by a pair of half-keys stored separately from one another. For example, a first half-key is stored within the secure apparatus while a second half-key is recorded on a medium external to the apparatus. When this external medium is connected to the apparatus, the two half-keys are combined to form the access key for the apparatus and thus allow its use. An example of such a securing method is designated by the acronym CIK for "Crypto Ignition Key". The acronym CIK designates in a general manner the principle of use of a cryptographic key allowing the booting of a cryptographic apparatus. With a view to simplification, a recording medium external to the secure apparatus and able to store a CIK half-key will be designated by the expression "CIK plug". A CIK plug may be allocated to a particular user or to a group of users and thus, in addition to allowing the unlocking of the secure apparatus, make it possible to identify a user, and to identify his role (administrator, maintenance agent, operator, etc.).

Conventionally, the complete initialization of a CIK plug necessitates its connection to the apparatus, the creation of a pair of half-keys, one of which is stored solely on the apparatus and the other of which is transmitted and recorded on the CIK plug, and then a configuration phase, for example to configure the access rights in respect of the user for whom the CIK plug is intended. Hence, when several users need to use a secure apparatus, it becomes necessary to initialize several CIK plugs, for example one plug per user, sometimes with different configurations from one CIK plug to another. The initialization of a series of CIK plugs therefore requires the execution of multiple cycles of connection / configuration / disconnection which render the manipulations lengthy and repetitive, and consequently also sources of errors, more particularly when the apparatus has no ergonomic



means for transmitting instructions to it, for example no man-machine interface, no screen, no keyboard and no mouse. Moreover, the apparatus may be placed in a cramped space, for example on board a vehicle or an aircraft, thus making it difficult to access the connectors of the apparatus that
 5 are designed to receive the plugs, yet further complicating the task of the operator responsible for initialization, and immobilizing the vehicle for a certain period.

A first solution for simplifying the initialization of these media
 10 consists in installing on the apparatus to be secured a graphical interface and means of interaction with a user such as, for example, a keyboard. However, the apparatuses to be secured do not always lend themselves to the setting up of a graphical interface or to the connecting of user input/output means. For example, an onboard facility for encrypted radiocommunications is not
 15 designed to accommodate such upgrades. Moreover, a keyboard may not be usable within certain contexts of employment (notably with the use of gloves or mittens). Likewise, for example, a back-lit screen cannot be employed at night when it is desired to maintain a certain discreetness of use.

A second solution for simplifying the procedure for initializing the
 20 CIK plugs is to use a generic key-setup system. However, this type of system is very complex to implement, therefore very expensive.

An aim of the invention is to propose an inexpensive scheme making it possible to initialize CIK plugs readily, in particular when the latter are employed on apparatuses having no ergonomic man-machine interface. For
 25 this purpose, the subject of the invention is a method for generating n pairs (K_1^i, K_2^i) , $1 \leq i \leq n$, of cryptographic half-keys, each of said pairs making it possible to reconstruct an access key K_{PL} specific to a secure apparatus, said method being characterized in that it comprises at least the following steps:

- 30
- generating and storing, with the help of a management center distinct from said apparatus, a first series of n half-keys K_1^i on a recording medium;
 - supplying the apparatus with said recording medium so as to generate, with the help of said access key K_{PL} and of the n half-keys

K_1^i stored on said medium, a second series of n half-keys K_2^i making it possible to form said n pairs (K_1^i, K_2^i) .

The apparatus can thus be initialized by n pairs of different half-keys. Indeed, the association of the half-keys belonging to each of the n pairs
 5 (K_1^i, K_2^i) formed with the two series of half-keys makes it possible to reconstruct the local key K_{PL} .

According to an implementation of the method for generating pairs of cryptographic half-keys according to the invention, a file of commands is produced by the management center, said file of commands being stored on
 10 the recording medium, said file containing instructions to be read by the apparatus so as to command the generation by the secure apparatus of the second series of half-keys K_2^i . Such a recording medium is more commonly designated by the term "Fill Gun".

According to an implementation of the method for generating pairs
 15 of cryptographic half-keys according to the invention, the apparatus does not have any ergonomic input means to allow a user to transmit instructions. For example, there may be no keyboard or mouse installed on said apparatus.

The management center may be a personal computer linked to a bank of connectors adapted for the connection of a medium storing a half-key
 20 K_1^i , said computer being provided with software for generating half-keys.

According to an implementation of the method according to the invention, each of the media storing one or more half-keys K_1^i is allocated to a user or a group of users of the secure apparatus, the method comprising a step of defining access rights in respect of each of said media, via a
 25 graphical interface installed on the management center.

Each of the n half-keys K_1^i of the first series may be stored on a removable medium external to the apparatus, the n half-keys K_2^i of the second series being recorded on the apparatus. The removable medium containing a half-key K_1^i may be associated with a user, so that each user
 30 entitled to access the secure apparatus possesses his own access half-key.

The apparatus may be a system for encrypted radiocommunications, an apparatus endowed with cryptographic means or more generally any system necessitating the protection of certain sensitive data.

The subject of the invention is also a system for generating n pairs (K_1^i, K_2^i) , $1 \leq i \leq n$, of cryptographic half-keys, each of said pairs making it possible to reconstruct an access key K_{PL} specific to a secure apparatus, the system comprising a management center provided with a bank of connectors
 5 able to receive removable media adapted for the recording of one or more half-keys K_1^i , the system comprising a recording medium to be connected up to the secure apparatus and adapted for the implementation of the method such as described above.

In contradistinction to a conventional initialization method in the
 10 course of which the two half-keys of a pair (K_1^i, K_2^i) are created at the same time with the help of the secure apparatus, the method according to the invention dissociates the creation of these two half-keys K_1^i, K_2^i , which are nevertheless tightly related mathematically.

15 Other characteristics will become apparent on reading the following nonlimiting detailed description given by way of example in regard to appended drawings which represent:

- Figure 1, elements implemented during the execution of a method according to the invention,
- 20 - Figure 2, a schematic illustrating the steps of a method according to the invention.

Figure 1 presents elements implemented during the execution of a method according to the invention. The method applies to the initialization of
 25 media 111, 112, 113, in the example CIK plugs, able to connect up to a secure apparatus 121 to allow its unlocking. To perform this initialization, a device 213 for injecting files into the apparatus 121 and a management center 131 are used. As explained further on, the management center 131 is linked to a bank 132 of connectors able to receive the media 111, 112, 113.

30 Figure 2 presents a schematic illustrating the steps of a method according to the invention. The example developed in the figure relates to the creation of n pairs of half-keys allowing, for example, n different users to access a secure apparatus.

During a first step 201, a CIK plug 211 with administrator rights is
 35 connected to a secure apparatus. This secure apparatus is for example a

high-security radiocommunications terminal, an IP encrypter, a file encryption system. The apparatus is unusable as long as a cryptographic access key K_{PL} has not been reconstructed. It should be noted that in order to execute the method according to the invention, it is therefore necessary that an
5 already initialized CIK plug be previously available. Stated otherwise, it was necessary firstly to perform a conventional initialization of a CIK plug — that of the administrator, in the example — so as to be able to initialize the other CIK plugs afterwards.

Connecting the CIK plug 211 to the apparatus therefore makes it
10 possible to reconstruct the cryptographic access key K_{PL} for this apparatus, by combining the half-key present on the CIK 211 and the associated half-key present on the apparatus. The apparatus therefore remains usable as long as the CIK plug 211 remains connected to the apparatus. This connection may be carried out by physically joining the plug up with the
15 apparatus or by any other means.

During a second step 202, a qualified person, for example an administrator, utilizes a management center to create n half-keys, each intended for a different CIK plug, the CIK plugs being able to unlock the same apparatus or different apparatuses. The management center is, for example,
20 a personal computer, advantageously placed in an ergonomic and secure environment, furnished with a graphical interface allowing the administrator to create a new user number for someone entitled to possess a CIK plug for accessing the apparatus, said graphical interface also making it possible, for example, to allocate more or less extensive rights to future users of the CIK
25 plugs. The personal computer is linked to connection means for CIK plugs, for example, a bank comprising ten or so connectors.

Firstly, n virgin CIK plugs to be initialized are therefore connected to a bank, which is linked to a personal computer. Furthermore, a device 213 for injecting files into the apparatus is also connected to the computer, this
30 type of device sometimes being designated by the term "Fill Gun". For example, the device 213 is linked to the computer and to the apparatus by standard interfaces, of RS232, RS485, USB type. Thereafter, the administrator 215 creates, for example via a man-machine interface executed by the computer, a number n of plugs to be considered and a number p of
35 secure apparatuses to which access is required. The computer then creates

n half-keys K_1^i , $1 \leq i \leq n$, one for each CIK plug to be initialized. Each of these half-keys K_1^i is transmitted to a CIK plug 217 connected to the bank and the n half-keys K_1^i are transmitted to the file injection device 213. The administrator 215 can also allocate different access rights in respect of each
 5 CIK plug. Finally, a file of commands is created on the injection device 213, this file containing instructions comprehensible to the secure apparatus in order to complete the initialization, as explained further on, during a third step 203 of the method.

On termination of the second step 202, each CIK plug 217 records
 10 an identifier of the apparatus to which it allows access and its half-key K_1^i , and the file injection device 213 contains a file of commands and, for each association between a CIK plug and the apparatus to which it allows access, the half-key K_1^i of the CIK plug and the access rights associated with this CIK plug.

15 One and the same CIK plug may be used for several different apparatuses; in this case, several different half-keys are recorded on one and the same CIK plug.

Moreover, the first step 201 and the second step 202 may be inverted, without prejudice to the result obtained by the method according to
 20 the invention.

During a third step 203, the file injection device 213 is connected to the secure apparatus. The file of commands generated during the second step 202 is read by the apparatus and the latter, with the help of the cryptographic access key K_{PL} and of the n half-keys K_1^i contained in the file
 25 injection device 213, produces a second series 219 of n half-keys K_2^i to be stored on the secure apparatus. To each half-key K_1^i of the first series 217 there corresponds a half-key K_2^i of the second series 219. Stated otherwise, n pairs of half-keys (K_1^i, K_2^i) are formed, each of these pairs making it possible to reconstruct the cryptographic access key K_{PL} for the apparatus,
 30 the half-keys of each pair being stored on distinct media (apparatus and CIK plug). Preferably, once a half-key K_2^i of the second series 219 has been created, the corresponding half-key K_1^i in the first series 217 is erased from the file injection device 213. Moreover, the user numbers present on the file injection device 213 as well as the rights associated with these users are also

transmitted to the apparatus. The apparatus thereafter interprets what these levels of right represent.

On termination of this third step 203, the secure apparatus is
5 ready 220 to be used via any of the initialized CIK plugs. When a user connects his CIK plug to the locked apparatus, the apparatus reconstructs the cryptographic access key K_{PL} and grants the privileges initially configured for this user.

Except for the prior connection indispensable to the initialization of
10 an administrator CIK plug 211, a single connection to the apparatus has therefore been necessary (that of the file injection device 213), when the prior art required n connections of CIK plugs to an apparatus to generate n half-keys. Thus, when $n \geq 2$, lengthy and repetitive manipulations are avoided, thereby decreasing the risk of error in the generation of the half-keys.

15 When a CIK plug is lost, it must be possible to deactivate it within the apparatus, which, conventionally, makes it necessary to tell the apparatus which CIK plug is lost, and therefore to have plug identifiers. Now, in order that the apparatus can know these identifiers, it must be possible to
20 enter them and therefore the apparatus must have for example a keyboard.

The method according to the invention allows the use of a file of commands which is subsequently injected into the apparatus so as to order it to delete all the CIK plugs, or to delete all the plugs except the one which is connected. Thus, no need for CIK plug identifier or keyboard.

25 The method according to the invention exhibits notably the advantage of reducing threats related to erroneous initialization of the apparatus, while preserving a high level of security.

Another advantage of the method according to the invention is that
30 it is upgradable, since the procedure put in place at the management center level may be refined, on account of the possibilities of adaptation.

CLAIMS

1. A method for generating n pairs (K_1^i, K_2^i) , $1 \leq i \leq n$, of cryptographic half-keys, each of said pairs making it possible to reconstruct an access key K_{PL} specific to a secure apparatus, said method being characterized in that it comprises at least the following steps:
 - generating (202) and storing, with the help of a management center (131) distinct from said apparatus (121), a first series (217) of n half-keys K_1^i on a recording medium (213);
 - supplying (203) the apparatus with said recording medium (213) so as to generate, with the help of said access key K_{PL} and of the n half-keys K_1^i stored on said medium (213), a second series (219) of n half-keys K_2^i making it possible to form said n pairs (K_1^i, K_2^i) .
2. The method for generating pairs of cryptographic half-keys as claimed in claim 1, characterized in that a file of commands is produced by the management center (131), said file of commands being stored on the recording medium (213), said file containing instructions to be read by the apparatus so as to command the generation by the secure apparatus of the second series of half-keys K_2^i .
3. The method for generating pairs of cryptographic half-keys as claimed in claim 1 or 2, characterized in that the apparatus (121) does not have any ergonomic input means to allow a user to transmit instructions.
4. The method for generating pairs of cryptographic half-keys as claimed in one of the preceding claims, characterized in that the management center (131) is a personal computer linked to a bank (132) of connectors adapted for the connection of a medium (111, 112, 113) storing a half-key K_1^i , said computer being provided with software for generating half-keys.
5. The method for generating pairs of cryptographic half-keys as claimed in claim 4, each medium storing one or more half-keys K_1^i being allocated to a user or a group of users of the secure apparatus, the method being

characterized in that it comprises a step of defining access rights in respect of each of said media (111, 112, 113), via a graphical interface installed on the management center (131).

- 5 6. The method for generating pairs of cryptographic half-keys as claimed in one of the preceding claims, characterized in that each of the n half-keys K_1^i of the first series (217) is stored on a removable medium (111, 112, 113) external to the apparatus (121), the n half-keys K_2^i of the second series (219) being recorded on the apparatus.
- 10 7. The method as claimed in one of the preceding claims, characterized in that the apparatus (121) is a system for encrypted radiocommunications or an apparatus endowed with cryptographic means.
- 15 8. A system for generating n pairs (K_1^i, K_2^i) , $1 \leq i \leq n$, of cryptographic half-keys, each of said pairs making it possible to reconstruct an access key K_{PL} specific to a secure apparatus, the system being characterized in that it comprises a management center (131) provided with a bank (132) of connectors able to receive removable media (111, 112, 113) adapted for
 20 the recording of one or more half-keys K_1^i , the system comprising a recording medium (213) to be connected up to the secure apparatus and adapted for the implementation of the method as claimed in one of the preceding claims.