CENTRALISED CRYPTOGRAPHIC SYSTEM AND METHOD WITH HIGH CRYPTOGRAPHIC RATE

This invention concerns a centralised cryptographic procedure and system, particularly intended for applications that need high flux cryptographic.

In a service system distributed as, for example, pay-television, payment by credit card or by means of Internet, the information exchanged between the operating centre and the user modules uses cryptographic means to guarantee the authenticity and confidentiality of the data.

Depending on the type of application, the number of user modules can be high, and each of these modules sends the information by means of a concentrator to one or several operating centres in charge of authentifying and carrying out the transactions. These operations are based on encrypted communications and need cryptographic means, on the one hand for the user modules and on the other hand for the operating centre. It can easily be imagined that if a great number of user modules have to be processed, the cryptographic means of the operating centre will have to be very powerful, while those of the user modules, being particular of each user, do not have the same needs.

For this reason, while a processor contained in a smart card is capable of processing these data at the user module level, powerful computers have to be installed at the operating centre.

A fundamental point concerns the cryptographic keys. At the operating centre the cryptographic operations take place in a specialised cryptographic module, where particular attention is paid to security. These modules consist of a high capacity processor, which carries out the cryptographic operations, and a memory that contains the keys. For security reasons, these modules are either situated in a protected enclosure, such as a safe or a closed room, or they are encapsulated in a box, which, if opened by whatever means, will erase the sensitive data.

Although these measures have undeniable qualities, these modules suffer weaknesses in their electronic structure, and can be vulnerable to an operator with bad intentions. In fact, the employee who has the key to the door of the room where

the cryptographic modules are situated can easily gain access to the memory where the cryptographic keys are stored. Such a damage can be catastrophic for the system's security and for the credibility of the supplier of the service.

Furthermore, although these cryptographic modules have a great processing capacity, they are not flexible when higher capacities are needed. For example, a 10% power increase involves the doubling of the cryptographic module, which in fact means increasing the capacity by 100%. Another aspect concerns the updating of these modules, which is difficult for a card especially developed for this purpose.

It is known to use more than one smart card for the decoding operations in the subscriber module, and this configuration is described in WO 96/07267 and in EBU Review Technical N¼ 266 "Functional Model of a Conditional Access System". However, the presence of these multiple cards on the receiver's side is due to the fact that it is necessary to decode several sources using different keys, even different cryptographic functions. The presence of these cards does not solve the problem of processing an important flux of data, it only ensures the compatibility with various standards.

This invention intends to solve the problem of finding a cryptographic module that offers high security against intrusion, both at the physical and logical level, a great flexibility depending on the cryptographic flux necessities, and that allows an easy updating.

This objective is totally achieved by a centralised cryptographic system, comprising a control module and at least one cryptographic module, characterised in that each cryptographic module comprises one or several interface modules on which are one or several monolithic security units.

A monolithic security unit is a unit that includes all the necessary elements for the cryptographic operations located on a single support in order to ensure security. They generally consist of a single electronic smart card that has a mechanical or electronic anti-intrusion protection. However, other structures consisting of, for example, two electronic chips are also included in the denomination "monolithic" as long as they are intimately linked and supplied by the distributors as a single element.

According to the invention, the cryptographic module comprises a first control module in charge of administrating the entry/exit of the data to be processed. It allows to determine the cryptographic flux that is desirable and knows the cryptographic capabilities that are available. This control module can be material or logical. It has one or several interface modules on which are monolithic security units in order to process the data. Each of these units consist of a cryptographic calculating unit, a memory containing at least a part of the cryptographic keys and means to communicate with the interface module. The keys appear decoded only in the security units, which have, as indicated previously, a high level of security. This level is achieved by the fact that they consist of a single standardised card designed for this purpose. Their structures do not allow them to achieve high processing capacities. For this reason the increase in cryptographic flux is ensured by using a great number of these units. The more the necessary flux of the cryptographic system increases, the more the number of these working units will increase.

This configuration allows to ensure a great flexibility as to the cryptographic flux of the system by adding security units depending on the needs. This configuration allows to attend the demand by adding the necessary security units.

According to one embodiment, the monolithic security units are set on the interface modules in an removable way. This allows an easy updating of the latter, as technology progresses rapidly. Another advantage of this solution is their cost, because these security units are manufactured in large quantities and thus have attractive prices.

According to one embodiment, the security units are smart cards following the norms ISO 7816.

The present invention includes also a method of centralised cryptographic processing of data consisting in transmitting the data to be processed to a cryptographic module, said module comprising one or several interface modules and transmitting the data by means of said interface modules to one or several monolithic security modules in charge of the cryptographic operations according to the flux of the data.

According to this method, the number of security units in service depend on the flux of the data required to the cryptographic module. In fact, because each unit has not

enough power to process a great number of cryptographic operations in a short time it is necessary to use several security units. The control module and the interface module allow the parallel processing of the resources of the security units.

One of the functions of the interface module is the administration of the resources that are further available. The interface module carries out in an initialisation phase the inventory of the security units that are attached to it, as well as their characteristics. This resource file will be able to direct the requests according to the characteristics of these units.

According to another embodiment of the invention, this method consists in executing the same cryptographic operations by means of several security units and comparing the various results. If the results are different, the control module sends an error message to the console. This console can react in different ways, for example, establishing which of the security units is responsible of the error, by using either a reference security unit or several security units and detecting which unit sends a different result.

The result of this test will be notified to the resource list so that the defective unit or units are not used any more.

In the hypothetical case that the error is not in one of the security units but concerns all the units of a same interface module, the parallel cryptographic operations are executed by two security units situated in two different interface modules. In fact, some parameters are stored on the interface module, and their modification can produce a malfunction of all the security units.

In order to ensure a good functioning of the various modules, it is possible to execute test operations on the security units that are not being used. These tests can be carried out with reference data of which the result is known in advance, or they can be executed by testing in parallel several modules with randomly generated data and comparing the results.

The invention will be better understood with the following detailed description that makes reference to the annexed figures, which are given as a non-limiting example, in which:

- Figure 1 represents a centralised cryptographic system according to the state of the art;

- Figure 2 represents a cryptographic system according to the invention;

In Figure 1 are represented diagrammatically the various blocks of the system that is responsible for the encryption in the operating centre. The data to be encrypted are on the bus, which communicates the various information that are necessary for the functioning of the operating centre. When such an operation is required by the operating centre, the specialised cryptographic system is used, which is represented here by the control module block CM and the cryptographic module block EM. The mission of the control module CM is to filter the access to the cryptographic module EM, that is to say, it offers protection against attacks coming from the exterior by means of the communication bus. It is not conceived to resist a local attack, be it physical or "programming", for example, of the operator.

This control module CM, after having filtered the data, sends them to the cryptographic module EM to be processed. As mentioned above, it has powerful cryptographic means in order to satisfy the high flux of the central bus. To achieve this, it has clear readable keys in its memory. In this example, the module is situated in a physically protected enclosure in order to prevent any non-authorised person from taking out the keys or from modifying the software in his/her own benefit.

In Figure 2 the architecture of the system according to the invention is represented. We find again the control module CM that works as a software filter against external damage. As indicated in Figure 2, this module communicates with several interface modules IM. These modules have a software protection, that is to say, a certain number of operations (for example, the reading) are simply not possible. These modules, on the other hand, are not physically protected. This function is left to the security units PIM. Each interface module IM has a certain number of these PIM units in order to increase the cryptographic flux.

Another task of this CM module is to direct the requests coming from the central bus towards the security units. When the desired operation is finished (for example, the coding) the result is transmitted to the CM module, which informs the entity that has required this operation. In order to ensure the distribution of the requests, the CM

module has a list of the available resources. When an error has been detected, the unit that is responsible for the error is disabled in the resource list.

It is not necessary that all the security units be of the same type. Some may have a cryptographic calculation unit based on a different algorithm than the other units. In this example, some units have, for example, a unit of the type RSA; others have a unit of the type DES or IDEA.

These information are contained in the resource list stored in the CM module. This module directs the requests depending on the availability and the capability of the security units.

According to another embodiment, the interface modules are cards of the PCI type and the security units are smart cards of the ISO 7816 type.

Although this invention concerns in the first place the coding of data, the architecture described above is equally applicable to the decoding of a flux of data. In fact, it is possible that during an emission purchase many users accede the operating centre, generating in this way an important flux to be decoded. The security units are then used for data decoding operations.

CLAIMS

1. A centralised high cryptographic rate system localised in an operating centre and intended to process data to be transmitted to a plurality of user modules, comprising a control module (CM) and at least one cryptographic module (EM), characterised in that each cryptographic module comprises at least one interface module (IM) on which are connected in parallel, a plurality of monolithic security units (PIM).

2. A system according to Claim 1 characterised in that the security unit comprises at least one calculation unit for the cryptographic functions, a memory containing the cryptographic keys, and communication means to the interface module.

3. A system according to Claims 1 or 2 characterised in that the security unit is set in an removable way on the interface module.

4. A system according to Claims 1 to 3 characterised in that the security unit is in the form of a smart card.

5. A system according to Claim 4 characterised in that said smart card follows the norms ISO 7816.

6. A system according to any of the preceding Claims characterised in that the monolithic security units (PIM) have cryptographic calculation units of a different type, such as RSA, DES, T-DES, or IDEA.

7. A system according to any of the preceding Claims characterised in that the control module (CM) has a resource list of the monolithic units comprising the available number, their state, their version, and their cryptographic capability.

8. A centralised encryption/decryption method of data transmitted between an operating centre and a plurality of user units, consisting in transmitting, by the operating centre, data to be encrypted or decrypted to a control module (CM), said module comprising at least one interface module and transmitting by means of said interface modules the data to be coded or decoded to a plurality of monolithic security units connected in parallel, in charge of cryptographic operations depending on the flux of the data.

9. A cryptographic processing method according to Claim 8 characterised in that it consists in transmitting to several security units the same data to be processed, comparing the data when returning from the security units, and informing an external entity if their values differ.

10. A cryptographic processing method according to Claim 9 characterised in that it consists in transmitting the data to be processed to security units situated on different interface modules.

11. A cryptographic processing method according to Claim 8 characterised in that it consists in carrying out test operations on one or several security units that are not currently in use and comparing the result with a reference result.

12. A cryptographic processing method according to Claim 8 characterised in that it consists in carrying out test operations on at least three security units that are not currently in use and comparing the results in order to determine if these units are operative.

13. A cryptographic processing method according to Claims 8 to 12 characterised in that it consists in administrating the security units by means of a resource list situated in the control module (CM), this list comprising the number of available units, their state, their version, and their cryptographic capacity.