



G00002

METHOD FOR STORING ENCRYPTED DATA

The present invention concerns the encryption of data, particularly the transmission of encrypted data on open networks.

5

When we want to guarantee that only the authorised addressees can exploit the data transmitted on open networks (cable, satellite, hertz wave, or Internet) the most appropriate means is to encrypt these data and to ensure that only the authorised addressees have the means for decrypting them.

10

Despite the used algorithms it is admitted that it is possible for a third person that has important calculus power to decrypt these data.

15

This is why the present systems integrate a key changing mechanism that frequently discourages the potential assailants. Each attack then only acts on a small portion of data and only allows access, after decryption, to a few seconds of transmission.

20

This method is used for the broadcasting of pay television, the key called "control word" only having a duration of a few seconds. These data are called "for immediate consumption" and the corresponding key is sent paralelly.

25

The apparition of storing means and the possibility of viewing (or exploiting) these data at any given moment has modified little the situation.

30

In order to further satisfy clients it is from now on possible to send encrypted data on a distribution network comprising a great number of users, data that are stored in the storing unit of the user unit. These data are accompanied by a file containing the encryption keys, this file also being encrypted according to an algorithm and keys contained in a security module of the user.

This security module generally is in the form of a smart cart having in its memory its own keys to decrypt the data.



159159

For the following exposition the data defining the product subject to conditional access will be named "product data". By "product data" we can understand a film, a sports broadcast, a game, or a software.

- 5 We will consider the fact that a great number of user units contain in their storing unit the same "product data" and a file of keys.

If the user decides to buy this product, the security module will receive the necessary instructions to decrypt the keys file and to supply in useful time the
10 keys to decrypt the "product data".

A bad intentioned third person will then attack the keys file that is encrypted by the specific key while the "product data" are encrypted by a great number of
15 keys.

Furthermore, the size of the keys file is small compared with the size of the product data. For information, the size of a film in encrypted form is about 1 Gigabyte; in decrypted and decompressed form the same can represent a size
20 of 10 Gigabytes.

In this way when this third person manages to decrypt the keys file this information can circulate easily on the Internet for example allowing thus other persons by means of a modified decoder to decrypt the "product data".

25 It should be known that the decoder receives a flux of data whose format is property of the broadcaster. This means that it is very difficult to isolate the different packages of information to obtain the "product data" in encrypted form at this stage. This is why the attack is made on the storing unit or hard disk, which for economic reasons is of a standard type (IDE for example). This disk is
30 then transferred to a personal computer to receive by other channels the keys file.

In the similar objective of allowing the storing of a product on a hard disk and of viewing it later, a first approach is described in the document FR 2 732 537.

The problem that this document seeks to solve is the duration of limited validity of the keys transmitted with the data. This is why the proposed solution is to decrypt the file containing the keys (CW) and to re-encrypt them with a local key to allow thus the use of the data at any time. It should be noted that the data in themselves are stored in the same state as when they entered the decoder.

The embodiment described in the document EP 0 912 052 varies in the sense that the local re-encryption key is stored in a smart card.

These two documents do not allow to solve the problem of the vulnerability of the data when they are stored on a support with easy access.

The objective of the present invention is to prevent the decryption of a keys file or of data from allowing many bad intentioned users benefiting illegally from "product data".

This objective is achieved by a storing method of data extracted from an encrypted data flux sent to a decoder connected to a security module and to a storing unit (DB), method consisting in re-encrypting the encrypted data before they are transferred to the storing unit (DB) by at least one specific key (K1, K2).

In this way, the data of each storing unit are specific to the considered decoder and the decryption of a keys file only allows to decrypt the "product data".

The data flux entering the decoder is firstly interpreted to isolate the parts that constitute the "product data". These are encrypted by a first key that is contained in the decoder.

From the fact that the decoder is not considered as inviolable it is possible to use instead of or additionally to the first key, a key contained in a security module.

The present invention will be better understood with the help of the annexed figures, taken as a non-limiting example, in which:

- Figure 1 illustrates the different components of a decoder,
- 5 - Figure 2 illustrates the operations according to the invention.

Figure 1 illustrates the flux entering EF in the decoder STB for processing. The data that are to be stored are isolated according to the format specific to the data destined for memorisation and sent to an encryption module before being
10 transferred. This module uses the key K1 supplied by the security module SM, generally in the form of a smart card connected to the decoder. This card is reputed inviolable and the different exchanges between the latter and the decoder STB are encrypted by a key specific to these two elements. From then on it is not possible to read the information exchanged to feed a modified
15 decoder for example. Once the data are encrypted they are transmitted by the channel FF to the storing unit DB.

The key K1 delivered by the security module SM can be combined with a second key K2 specific to the decoder. From this fact the deviation of the
20 security module SM with the content of the data stored DB does not allow to decrypt these data.

These keys are specific, that is that each decoder or security module uses a different key. Depending on the chosen generation mode this key is generated
25 randomly during an initialisation phase or is sent by the operating centre of the system.

Figure 2 represents in the form of a diagram the same processing with the entering flux EF that passes through a first filter Sdata. This filter isolates the
30 data destined for storing; the data serving other aims are directed to other processing by the outlet EX.

A first stage of encryption $NK(K1)$ is then accomplished with a first key K1 coming from the security module SM. These data are then sent to a second

encryption module NK(K2) fed by a second key K2 coming from the decoder STB.

5 These keys supplied by the decoder STB and the security module SM are used in any given order.

According to one embodiment the encryption module is placed directly in the interface between the decoder and the storing module. In this way it is at a low logical level that this encryption is carried out and in a way that is independent
10 of the central management software of the decoder.

According to another embodiment the security module SM has encryption means powerful enough to receive the data flux to be encrypted and to return the data in encrypted form. In this case it is the security module SM only that
15 contains and uses the encryption key.

The encryption of the data can be executed a first time on the base of a first key K1 coming from the security module SM then on the base of a second key K2 coming from the decoder STB. Furthermore, according to the capacities of
20 the storing module the latter can also supply a key K3 allowing to encrypt the data with this key.

It will then be necessary to collect these three elements so that the decryption is possible.
25

This principle can be understood for all the elements capable of storing their own key, this key then being used by a new encryption layer of data.

In most cases the use of stored data according to the method described above
30 is subject to obtaining a right. This right is obtained from the operating centre and can be acquired before or after the downloading of the "product data". This right contains a describer of the product and a decryption key for the control words.

According to our invention at least one stage of the encryption is subject to a key contained in the security module (SM) where there are also the rights for the use of the data. During the decryption operation of the stored data on the storing means, the key K1 is only supplied to the decryption module if the
5 verification of the right of use is positive. In this way the data DB will only recover their original encrypted form as sent if the user has the right of use.

According to this embodiment the data DB are accompanied by a describer in plain text describing the necessary rights for these data. The security module
10 SM, before decrypting with the key K1, verifies this information with that contained in its secured memory.

CLAIMS

1. A storing method of data extracted from an encrypted data flux sent to a decoder (STB) connected to a security module (SM) and to a storing unit (DB), method consisting in securely re-encrypting the encrypted data before they are transferred to the storing unit (DB) by at least one specific key (K1, K2).
2. A method according to Claim 1, characterised in that it consists in using as a single key a key (K1) specific to the security module (SM).
3. A method according to Claim 1, characterised in that it consists in using as a single key a key (K2) specific to the decoder (STB).
4. A method according to Claim 1, characterised in that it consists in successively encrypting the data by several keys, either the key (K1) of the security module and the key (K2) of the decoder or inversely.
5. A method according to Claims 1 to 4, characterised in that it consists in encrypting the data destined to the storing unit (DB) by an encryption key (K3) contained in the storing unit (DB).
6. A method according to one of the Claims 1 or 2, characterised in that the data to be encrypted are sent to the security module (SM) to be encrypted, the encrypted data are then directed towards the storing unit (DB).
7. A method according to one of the Claims 1 to 3, characterised in that it consists in executing the encryption or the decryption in a low level interface located between the storing unit (DB) and the decoder (STB).