

PRE-PAYMENT PAY-TV SYSTEM

The present invention concerns the domain of receivers/ decoders of conditional access services, in particular an access system to an encrypted data stream calculated by a unit of time.

5 As an example of such data stream, we mean an information service about the stock exchange, weather forecast, general interest television, a sports event or others. These contents can be broadcasted on user units such as a pay-TV decoder, a computer, a portable phone, a "palm-top", a PDA, a radio, a television, or a multimedia terminal.

10 The digital stream is encrypted in order to be able to control use and define conditions for such use. This encryption is carried out thanks to control words, which are changed at regular intervals (between 5 and 30 seconds) in order to dissuade any attack aiming to find such a control word.

In order to allow the user unit to decode the stream encrypted by a control word, the
15 latter is sent to it independently of the stream, in a control message (ECM) encrypted by a key suitable for the transmission system between the managing center (CAS) and the security module of the user unit.

In fact, the security operations are carried out in a security module (SC), which is generally in the form of an inviolably reputed microchip card. This unit can be either
20 of a removable type or directly integrated to the user unit dealing with signals such as a paying TV decoder or a DAB receiver. In fact, the functioning of the invention authorizes the use of a user unit without a removable security module.

At the time of decrypting the control message (ECM), it is verified, in the security module (SC), that the right to accede to the considered stream is present.

25 This right can be managed by authorization messages (EMM), which load such a right into the unit (SC). Other possibilities are also possible such as the sending of decrypting keys.

The accounting of the use of such contents is today based on the principle of subscription, of purchasing events or of paying by time unit.

5 The subscription allows defining a right associated to one or several diffusion channels and allows the user to obtain these channels unscrambled if the right is present in his security module.

At the same time, it is possible to define rights specific to some contents, such as a film or a football match. The user can acquire this right (purchase for example) and these contents will be specifically managed by this right. This method is known under the denomination "pay-per-view" (PPV).

10 With regard to payment by the time unit, the security user unit comprises a credit that is debited according to the real consumption of the user. So for example, a unit will be debited each minute to this credit whichever the watched channel. It is possible according to the technical implementations, to vary the accounting unit, either in length, or in value per allowed time, even by combining these two parameters to
15 adapt the invoicing to the kind of transmitted product.

At the time of decrypting the control words, it will be verified if an associated right to access conditions is present in the security module.

The control word is returned in a decrypted form to the user unit only when the comparison is positive.

20 This way of functioning demands that the managing center knows the user, his physical address, his bank details as well as all the payment traffic which allows him to renew his rights.

In fact, the principle of the subscription is based on the renewal obligation that is to say that a right cancels itself if it is not renewed. This way of proceeding avoids that
25 anyone who subscribes to all the channels available terminates their subscription and arranges it so that the termination message does not ever reach its user unit. That is why such a right includes a time limit and its right for all the channels, if it is not renewed, cancels automatically at the end of a month for example.

One imagines thus the work necessary to follow the thousands of subscribers who regularly settle their invoices and to whom it is necessary to send a renewal message each month. Furthermore, such a message must be repeated for several days because the managing system does not know if the user unit is powered on.

- 5 It frequently happens that a user who was on holiday and who had switched off his apparatus finds on his return his user unit blocked. It is then necessary for him to call the managing center so that a personalized renewal message is sent to him.

So, a great part of the resources and the costs connected to the management of a center is allocated to the management of the subscribers.

- 10 A first solution using an electronic purse is described in document US 6282293. The chip card contains a credit that is debited when an encrypted content is accessed. The accounting information is included in the transmitted signal and allows this accounting. To reload the credit, the user unit calls a managing center in order to send the consumed events and to reload the credit according to the terms agreed
15 with this user, for example through a credit card.

- In a large number of cases, on the one hand the user unit has no communication channel towards a managing center and on the other hand, one wish to avoid recording all users in a database with their payment means. thus, this document do not allow to solve the aims of the invention, namely the creation of a set of user units
20 without back channel and without the knowledge of each unit's owner.

The aim of this invention is to propose an innovating way of offering access to paying TV to a large clientele and thus by drastically reducing the costs connected to the management of the subscribers.

- This aim is reached by a system having a managing center transmitting a data
25 stream encrypted by control words (CW), these control words being included in control messages (ECM), this data stream is intended to be received by at least one user unit linked with a security module identified by a unique address, this security module containing a credit, which is decreased according to the purchase of products or to the consumption of the data stream, characterized in that the security module
30 includes means to decrease the credit of a amount relating to a product or to a

amount relating to a duration, this amount and/or this duration being defined in the control message (ECM) or in a management message (EMM), the user having user unit independent means to transmit an identifier representative of the unique address and a value code representing an amount of the reload credit to the managing
5 center, the managing center having means to deal with and verify the value code and to transmit an encrypted message having the unique address and the amount of the credit to reload to the security module.

Thus, according to the invention, the credit reloading means are independent from the user unit while keeping the managing center as supervisor of the reloading
10 operations. Moreover, the transmission of this value code allows suppressing the invoicing of the user because this value code already contains the information proving that the user has acquired the rights to this value. According to other solutions of the prior art, the managing center handles in an independent way the customer's credit (invoicing, credit card) and transmits the reloading instructions
15 through the modem.

According to the invention, the value code is transmitted through one of the modes described below and the reloading instruction is sent in the encrypted data stream, in a management message for example.

This value code (VC) can have several forms:

20 1.) A unique number is contained on a card to scrape off and defines a pre-paid credit. These cards are sold in shops and have a part hidden by a layer that is easy to remove with a fingernail or a coin. The number revealed is a single number generated by a cryptographic system, that is to say that it must respect strict rules in its format. It is not possible in this way (or with very few probabilities) to generate
25 such a number that is recognized as valid by the managing center. To this number is associated a value which is what the user has paid for to acquire this card. Once this number is used, it is not possible to present it again to the managing center.

2.) A bank account or credit card number and the amount to reload. According to the terms accepted by the managing center and in agreement with the banking
30 institutions, the user can transmit his banking card number and the amount desired to be debited from his account. In this option, it is possible to use a removable security

module and insert it in a terminal for that purpose. This terminal allows one either to receive ready cash (banknotes for example) or to read a bankcard (even a credit card). Once the amount desired by the user has been duly checked (either by the notes introduced in the slot of the terminal, or by the authorization of the banking organization), the terminal contacts the managing center and a message of the credit reloading is sent to the terminal that transfers it to the security module. During this operation, it is possible to collect data about the consumption of the user, data that is conserved in his security module.

3.) A phone number or wireless telephony identifier number and the amount to reload. The user can simply send the desired amount to reload to the address of the managing center. In this message the sender's number is automatically comprised and according to the agreements between the telephony operator and the managing center, the reloaded amount is debited on the phone account.

According to the operating procedure chosen, the user communicates the value code to the managing center accompanied by the identifier of his user unit. In this kind of application, the unique address of the security module will be considered as the number of the group formed by the user unit and the security module. For simplification reasons, it is possible to generate a representative simplified code of the unique address. In fact, this unique address is generally a number comprising a large number of digits, which are necessary for the system (creation dates, version etc.) but not indispensable to identify a unit. This is why a shortened number of the user unit (STB) may be displayed but sufficient to differentiate each unit.

According to a particular embodiment, it is possible for the user to transmit another number to the managing center in place of the number shortened in a procedure of initialization.

For example it can be about a user's phone number. The managing center verifies that this new number is unique and associates this number to the unique address (UA). Consequently, it will be possible to replace the identification of the user unit with the phone number.

To reload his credit, the user can use a voice server and a classic phone that sends signals by DTMF. After having bought a value card (solution 1 of the value code), he

calls the voice server of the managing center. He is asked to introduce its unique address (UA) and the value code affixed to the card.

This operation does not take much time; the managing center checks the conformity of the value code and the identifier and if those data are correct, it prepares a
5 destination message of this user unit.

The message is transmitted by the diffusion channel in encrypted form and only the security module has the means to decrypt this message. Each security module receiving this message checks if the unique address contained in the message corresponds to its address and if not, ignores it.

10 For the unit responding to the unique address (UA), the amount of the credit contained in this message is added to the remaining credit.

The term "managing center" is to be understood extensively. In fact, in practice this entity is subdivided into several modules that can be located in different places. These modules are the control messages (ECM) encryption unit, the management
15 messages (EMM) encryption unit responsible for recharging the credit. The unit for dealing with value codes can be situated in a banking establishment if one considers variant 2, namely the connection with a credit center or on the premises of a phone operator if one considers variant 3, namely the sending of a short message by their portable phone. Once the value code is recognized and dealt with, a secured
20 connection allows the encryption unit to be informed that a management message, in charge of sending the reload message, should be sent to his recipient.

The user disposes of means to display the credit remaining on his television at all times.

According to the mode using the portable phone, a simple short message (SMS)
25 containing the value code and the identifier of its unit, allows his credit to be reloaded. If, furthermore, one has replaced his identifier by his phone number, only the value code is to be sent, the phone number being automatically transmitted to the addressee.

When the credit in the security module (SC) is sufficient, several operating modes are
30 possible namely:

- impulsive subscription: the user decides to use all or part of his credit to buy a subscription for one or several channels. So, a new right is created in the unit for the reception of said channels without any new action on his credit being necessary.

5 - impulsive purchase: the user can decide to buy a transmission or a transmission group (a series or a retrospective) and a corresponding right is created in the security module.

- deduction as time goes by: the user can decide to pay only what he actually consumes and the credit is consumed according to a payment method by a time unit.

10 The first two modes are preferably managed by the management messages (EMM) because they create a right inside the security module. While the third mode can only work with the control messages (ECM) in which one places the unit value as well as the acquired duration.

15 When a control message (ECM) is presented to the security module, the rights are checked according to a hierarchy starting from the largest right to the narrowest. So for example first one checks if the user has a subscription for these rights, then, if not if a right for impulsive purchase exists and as a last resort, one debits the credit by time unit.

In Figure 1, an embodiment is disclosed. It is about the variant 3 of the value code. The managing center (CG) is disclosed by several elements such as a phone
20 operator (TO), a data (DTA) encryption module (ENC), a encryption keys (CW) control module (ECME) responsible for generating the control messages (ECM) and a managing module (EMME) responsible for generating the credit reload messages towards the security modules. Each decoder (STB) comprises a security module (SC) that memorizes the credit (CR) of the user.

25 According to the example of the value code in the form of a card to scrape, having a unique number, the user uses his portable phone (TP) to transmit this unique number by connection to the telephony operator (TO). This operator receives this information and transmits it to the managing module (EMME) with the user's phone number. The validity of this number is verified thanks to a database (DB) of the valid numbers and

if this is the first time this number is used, the corresponding value (TA) is returned by the database. This number is then irrevocably invalidated.

Thanks to the phone number provided by the phone operator, the managing module (EMME) deduces the unique address (UA) of the security module and a
5 corresponding message can be sent by the classic transmission channel (cable, radio, etc.). This message is generally repeated during several days. For this purpose, it is useful to add that the security module comprises means to process the message only once. This is assured by an identifier of the message that is also encrypted by transmission keys. This identifier is memorized in the security module
10 therefore only such a message is received and processed. The security module from then on expects a different or upper identifier.

According to this way of proceeding, the database conserves a trace of the amount reloaded for each security module. It is possible to verify the consumption of each unit and detect fraud attempts. Furthermore, the sum of the reloaded amounts must
15 always be lower than the sum of the value cards in circulation.

CLAIMS

1. System comprising a managing center (CAS) transmitting a data stream encrypted by control words (CW), these control words being included in control messages (ECM), this data stream is intended to be received by at least one user unit (STB) linked with a security module (SC) comprising a unique address (UA), this security module (SC) containing a credit (CR) which is decreased according to the purchase of products or to the consumption of the data stream, characterized in that the security module (SC) includes means to decrease the credit of an amount (M1) relating to a product or to an amount (M2) relating to a duration (T), this amount (M1, M2) and/or this duration (T) being defined in the control message (ECM) or in a management message (EMM), the user having user unit (STB) independent means to transmit an identifier representative of the unique number (UA) and a value code (VC) representing an amount (TA) of credit to reload (CR) to the managing center (CAS), the managing center having means to deal with and verify the value code (VC) and to transmit an encrypted message having the unique address (UA) and the amount (TA) to reload the credit (CR) to the security module (SC).
2. System according to claim 1, characterized in that the value code (VC) comprises a bank account or credit account number and the reload amount (TA).
3. System according to claim 1, characterized in that the value code (VC) is a unique code and is pre-established by the managing center and complying with the cryptographic composition rules, and in that the managing center comprises means to check this code and extract the value which will be credited in the security module (SC).
4. System according to claim 1, in which the user disposes of a phone number (TN), characterized in that the user has means to associate the unique address (UA) to his phone number (TN) and in that the value code (VC) is transmitted to the managing center with the phone number (TN), said center having means to transmit the research message to the user unit (SC) whose unique address (UA) is associated to this phone number.

5. System according to one of the previous claims, characterized in that the product is a paying TV subscription for a determined duration or a transmission or transmission group for impulsive purchase.