CONDITIONAL ACCESS SYSTEM FOR DIGITAL TV: THE EUROCRYPT STANDARD

D. PELLERIN
PHILIPS ELECTRONIQUE GRAND PUBLIC

ABSTRACT

Digital compression of video signals will provide a breakthrough in TV broadcasting market by enabling the transmission of several TV programmes per channel. Moreover the digital technology for transmission will allow to provide the consumer with various services such as:

- *TV programmes with several stereo sounds.*
- *Stereo sound radio programmes.*
- *Data transmission...*

The tremendous increase in number and type of services will require a permanent use of conditional access. In Europe, the EUROCRYPT standard has been defined for the MAC transmission requiring conditional access. The module in charge of the conditional access function is a Smart Card.

The EUROCRYPT system offers the usual types of access modes. Those are:

- Subscription: Access is given for a certain type of programme for certain period of time.
- Pre-booked Pay per View: The user asks in advance for the access to one or several programmes.
- Impulse Pay per View (IPPV): If a user wants to access this type of programme, he will have to accept to buy the programme. The cost of the programme will then be debited from the credit in his Smart Card. In this case, the user watches what he pays for.

To get a personal control of his Smart Card, the user is given the possibility to define:

- Personal maturity rating
- Secret code to get access to IPPV programmes and programmes under maturity rating

Some facilities are also offered to the broadcaster to control the audience:

- Blackout with replacement under geographical and/or subject basis
- Fingerprinting to ensure that no misuse of video recordings from his programme are made.

The following pages describe the current implementation with the Smart Card and the way it will be extended from MAC (Multiplexed Analogue Components) to digital TV.

SYSTEM ASPECTS

The system can be split into two parts [see fig. 1]: The receiver side and the transmission side. The receiver side is made out of a receiver which incorporates the descrambler. A Smart Card performs the conditional access function. The transmission side has to manage the following functions:

- The encoding of the signal
- The scrambling function of video, sound, data ...
- Transmission of conditional access information related to scrambling using a master Card.

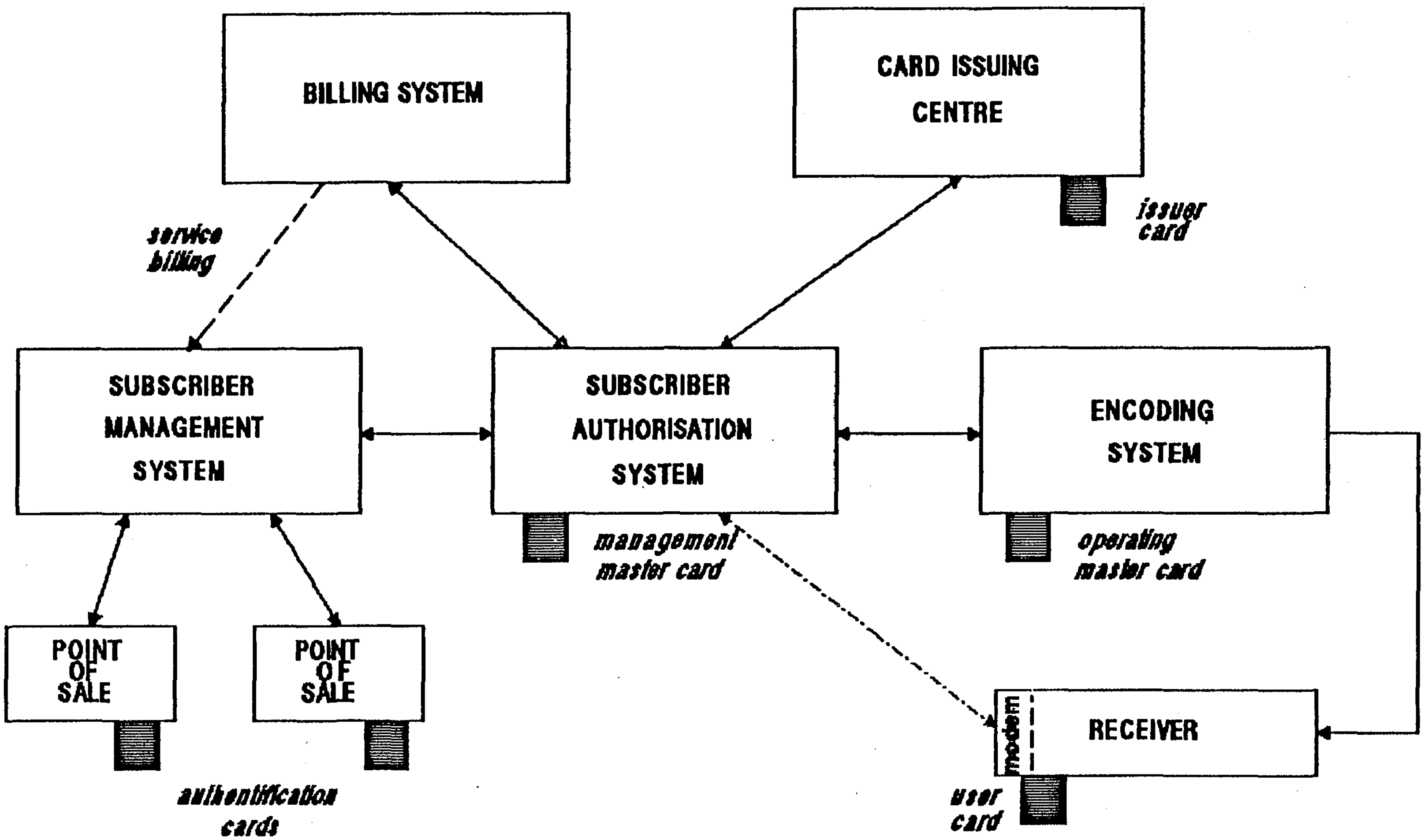

fig. 1

EUROCRYPT SYSTEM

- . Transmission of entitlements related information using a master Card.
- . Handling of the Commercial, Billing and Subscriber data base.

SMART CARD

The Smart Card is the part which is in charge of the conditional access and which handles all the entitlements and secrets of the conditional access system. The Smart Card is similar to a credit card with a built in chip. The Smart Card offers high protection against piracy:

- . The chip includes protections versus physical piracy.
- . The built in component is a monolithic chip which means no easy access to the internal bus.
- . The microprocessor of the Smart Card controls the interface with the external world. No sensitive information can be read in the Smart Card through this interface.
- . No secret information appear in clear on the Smart Card interface. There is no use in monitoring this interface for secret information.

The Smart Card is built up in two major parts [see fig. 2]:

- . The program part which contains the software to manage the Smart Card and also the algorithm to decrypt messages.
- . The memory which contains all the information related to the services (e.g. the name), the keys used by the broadcasters to encrypt the messages and also the entitlements the user has for his programmes.

The master Card is a specific card for the broadcaster who has the capability to encrypt messages.

EUROCRYPT allows several broadcasters or "Service Entities" to share the same Smart Card. An authority called "Issuer Entity" supervises the whole Smart Card and attributes to each Service Entity memory to write his data. The Issuer Entity will also supply the Service Entity with his first secret key.

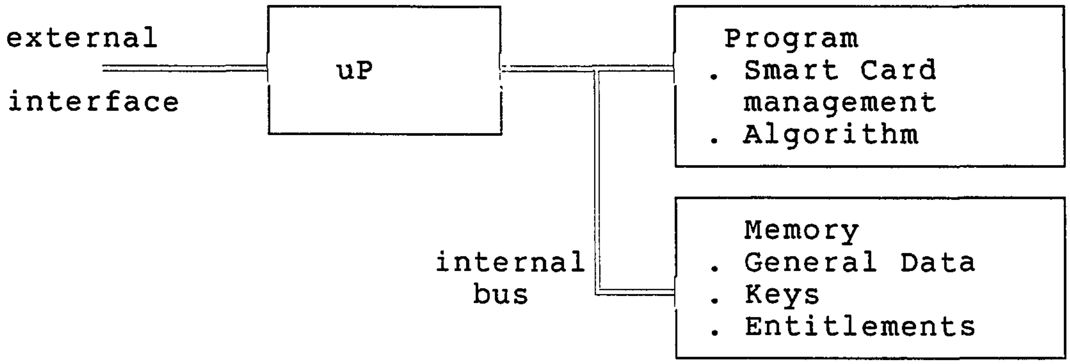

fig. 2

The current version of EUROCRYPT Smart Cards used in Europe can contain around 2000 entitlements of any type. This of course depends on the number of Service Entities in the Smart Card. The new version with EEPROM will be erasable which means that it could theoretically last for ever.

One of the most obvious advantages of a Smart Card is portability. A user who has to travel can take his Smart Card with him and insert it in the receiver available in his room at e.g. a hotel. The receiver is not specific for each user: It contains no secret key. When a problem occurs with the entitlements the Smart Card can be taken to a shop and checked or loaded with some special entitlements. Furthermore, if by any chance someone could pirate the Smart Card, the broadcasters would only have to replace the Smart Cards instead of complete receivers which from a price point of view is a big advantage.

DIGITAL TV APPLICATION

The data in the digital transmission, like in MAC, are organized in packets and each component can be selected and extracted from the packet multiplex by filtering its packet address.

The scrambling in a digital system consists, as in the digital part of MAC, in adding a binary pseudo random sequence to the bit information extracted from the signal. This scrambling is totally symmetrical (identical operation on transmission and reception side) and does neither give any consistent information about the initial signal nor about the scrambling sequence itself.

The receiver is in charge of the demultiplexing of the data, the recovery of the components (video, sound, data...) and also of the descrambling of the components which are under conditional access.

The scrambling sequence is the output of a complex Pseudo Random Generator initialized by a Control Word and the frame counter of the video. The Control Word is generated (e.g. randomly) on the transmitter side and transmitted in a encrypted form to the receiver side. If the user did subscribe, the conditional access will deliver the decrypted Control Word to the receiver which will load them in the pseudo random generator. The user will then get a clear signal.

Each component part of the transmission (sound, video, data ...), can be scrambled with different Control Words, which means that each can be accessed separately.

Concerning a Control Word:

- It has to be long enough to prevent pirates from trying all possible combinations. In the case of EUROCRYPT this Control Word is 60 bit. This means that trying all the combinations, say one per NTSC frame, would take around 1 billion years.

- It has to be changed rather often to prevent subscribers from distributing the Control Words to e.g. neighbors. In the MAC application the Control Word can be changed every 256 frames (about every 10 seconds in MAC).

Two types of messages are defined for transmission of conditional access data: One for control Words (ECM) and the other type is for entitlements transmission (EMM).

ECM MESSAGES

The Control Word is sent in the TV signal itself in a special message called Entitlement Checking Message: ECM. This ECM is transmitted every half a second to offer a quick descrambling of the signal. This message does not require significant data capacity of the signal.

An ECM message contains:

. PPID (Programme Provider IDentifier): reference of the broadcaster or Service Entity in the Smart Card. This field gives also the reference of the key to be used for decrypting the following data. This information is of course not encrypted.

. The access modes of the programme: The authorization valid to get access to this programme, the maturity level, etc. This information is not encrypted.

. The Control Words in Encrypted format: The current one to get access immediately to the programme and the one for the next 256 frames period.

. The HASH parameter which is the signature of any sensitive parameter of the message. This is to guarantee the integrity of the message, that is that nobody has tried to modify for example the access modes part.

EMM MESSAGES

The user also needs to get his entitlements from the broadcaster. The message used for this purpose is the Entitlement Management Message: EMM. This message can contain several types of information:

. Initialization of a Service Entity
. Keys
. Entitlements
. Replacement or fingerprinting data

This message is sent within the transmission. The receiver can filter the messages for a specific user at the user address present in the message. The user addresses are memorized in the Smart Card and passed on to the receiver. There are four types of EMM:

. EMM_U: Uses a Unique address which means that this message is intended for one particular user. This unique address is 36 bits (around 64 billion potential users). A Unique Address EMM is used to send entitlements to one user. Using the capacity of one sound channel at mono medium quality in MAC, around 250 customers can be addressed their entitlements per second.

. EMM_S: Uses a Shared address which means that this type of message can be addressed to several users. This type of EMM can be used when the users having the same address are asking for the same entitlements. This address is 24 bits (about 16 million possibilities). The audience is split into groups of 256 subscribers. The entitlement itself is sent in the EMM_G and this entitlement is registered in the conditional access system only if the information available in the EMM_S for the user indicates to do so. Using the equivalent capacity of one mono medium quality sound in MAC, 1 million users can have their entitlement updates within 20 seconds.

. EMM_C: Uses the Collective address. In the current application of EUROCRYPT, only the value 0 of the address is defined. The Collective EMM is used to send replacement or fingerprinting information. These are not used for addressing entitlements and do not require a big capacity of the channel.

. EMM_G: Uses no address at all. These message are intended for the whole audience. The General EMM is received by all the users. This type of EMM is used in combination with an EMM_S for addressing a large amount of people at the same time. It is also used to send free entitlements for customers who are subscribing to the channel for the first time. The user will be able to watch some programmes during which he will receive the entitlements he paid for.

Only the secret information such as keys are encrypted in an EMM message. The entitlement for example is sent in clear format or at most scrambled to guarantee confidentiality. A HASH field as in the ECM ensures that no fraudulent operation was performed on the message.

CONCLUSION

EUROCRYPT has proved to be reliable and secure in the current applications in Europe. EUROCRYPT can fit for new applications like Digital TV.

The EUROCRYPT standard offers many advantages for the development of Digital TV. The Digital TV will require very soon a conditional access function which EUROCRYPT could supply today. The market development of Digital TV with conditional access is also dependant on the price the customer will have to pay. With the Smart Card, the user will not have to pay for several specific receivers. The same neutral receiver, produced in large quantities at a low price, will be used by all customers for all conditional access programmes. If the broadcasters have to change the conditional access system, they just have to change the Smart Cards. These are some of the reasons why EUROCRYPT is the solution for conditional access in digital TV.

REFERENCE:

- Système d'accès conditionnel pour la famille MAC/paquet: EUROCRYPT

D. PELLERIN
PHILIPS ELECTRONIQUE GRAND PUBLIC
24, Quai Galliéni
92156 SURESNES Cedex
FRANCE