REPORT 1079-1

GENERAL CHARACTERISTICS OF A CONDITIONAL-ACCESS BROADCASTING SYSTEM

(Question 37/11)

(1986-1990)

1. Introduction

The present Report presents principles for conditional-access systems worked out by the EBU for application to satellite television by France and the United Kingdom, where the principles have been applied to teletext services. Some details of these applications are given in Table I at the end of the Report.

The principles may also be applied to conventional television and sound broadcasting systems as well as to additional services other than the teletext services listed in Report 802.

2. Components of a conditional access system

There are two distinct and in many cases independent components:

2.1 *Scrambling**

This is the process of rendering a service of no value to unauthorized users by changing certain of its characteristics under the control of the conditional access system at the sending end.

2.2 *Access control**

This is the provision of information to enable authorized users to descramble the service. The availability of this information is controlled by transmitting it in encrypted* form.

3. The requirements to be satisfied by a conditional access system

3.1 *Security*

The security of the system is the degree of difficulty encountered by an unauthorized user in attempting to gain access to the service.

There are two aspects:

- descrambling the signal without reference to the access control process. This is a function of the nature of the services and the scrambling method;
- obtaining the access control key* in an unauthorized manner. This is a function of the security of the algorithms used and the method of key distribution.

3.2 *Access modes*

A conditional access system will be more effective if there is a range of access modes.

Examples are:

- period availability – authorization runs from a starting time to a finishing time;
- programme or service item – availability is for a specific service item, whether or not it is completely used;
- service charge (commonly called "pay per view") – the charge or use of credit is proportional to the duration of use and/or the value of the service involved.

* See Annex I for definitions.

The access modes need to be variable with respect to several parameters, for example:

- time;
- various segments of the service;
- groups of intended users.

3.3 *Equipment standardization*

To provide maximum economy of manufacturing scale for receiving equipment and to simplify management and maintenance:

- common equipment should be standardized so that it can cater for as many service options as possible;
- the "secret" components should be within a secure module with a standardized interface**.

3.4 *Access management*

The definition of conditional access is based on the formal concept of *entitlement* to access, which can be implemented in various forms. An entitlement gives to its holder an *authorization* to access the related service.

3.5 *Avoidance of impairments to the service*

Three types of impairment are significant:

- impairment to the finally available service due to the scrambling/descrambling process;
- impairments due to faulty or unreliable acquisition of the access control data;
- uneconomic use of the resources due to the management or transmission overheads involved.

3.6 *Interaction with digital processing*

It should be noted that certain scrambling processes may conflict with some operations of digital signal processing techniques, for instance bit-rate reduction.

4. General description of a conditional access system

4.1 *General*

Conditional access requires that the information must be *scrambled* before it is broadcast. This process is under the control of a scrambling sequence obtained from a *pseudo-random generator.*

The descrambling process at the receiving end requires the same sequence (in this case the descrambling sequence) to recover the original signal.

To provide this sequence and to ensure synchronism between the sending and receiving processes, the starting condition of the pseudo-random bit stream generator is controlled by an *initialization word.*

** This subject has already been discussed in the EBU in connection with the specifications for conditional access for the broadcasting-satellite service (BSS) (see Report 1073).

To achieve security, access-related information permitting recovery of the initialization word is transmitted in an encrypted form, according to the access modes in use (see Fig. 1). The detailed structure of this process is given in Fig. 2 and in the following sections.

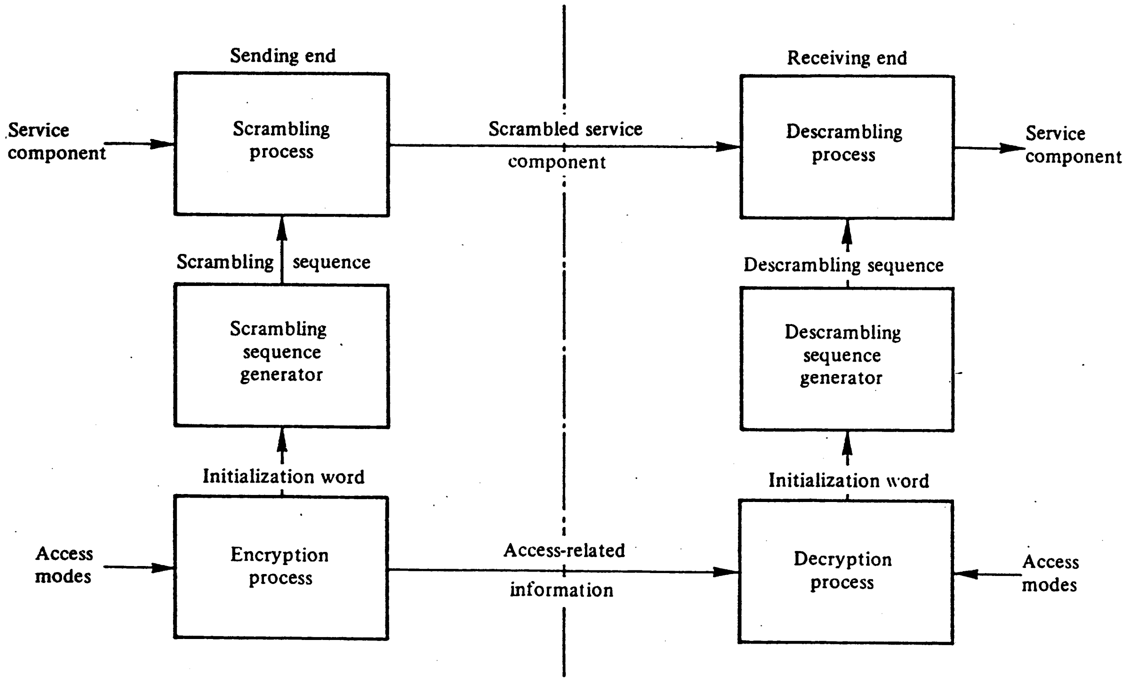


FIGURE 1 – *Basic conditional access system*

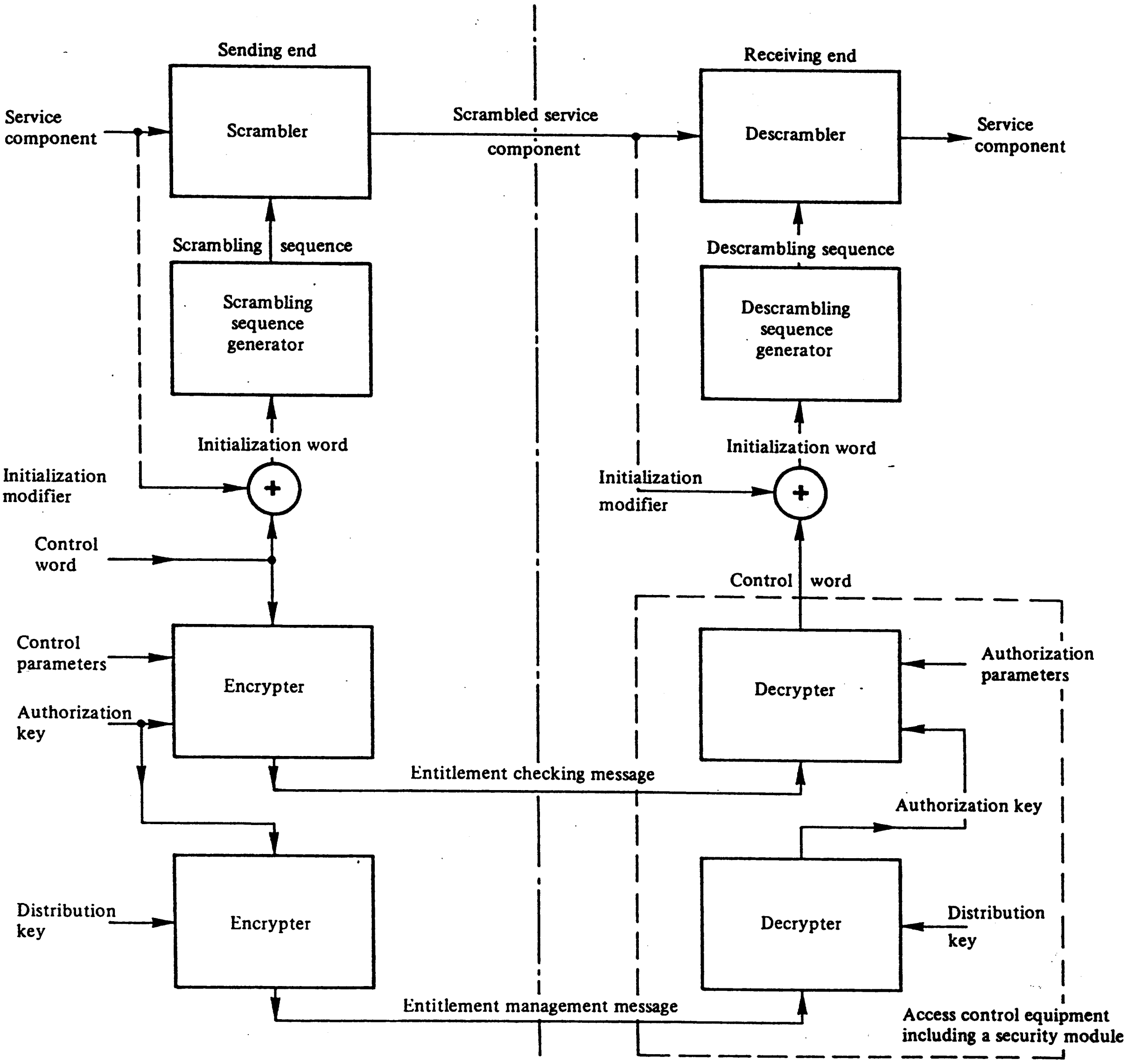


FIGURE 2 – *Functional description of a conditional access system*

Note. – Two encrypters and decrypters are shown in this figure for clarity. In practice, only one of each may be necessary if the encryption algorithm controlled by the authorization key and the one controlled by the distribution key are the same.

4.2 *Initialization word*

Conditional access to a service component is in fact equivalent to conditional access to the initialization word, which has two components: the *control word* and the *initialization modifier.*

4.3 *Control word*

The control word is the basic element of security. Its value is chosen arbitrarily and it may be changed during the service operation to enhance security.

The control word is communicated to the receiver as follows:

- at the sending end, according to the access mode in use, an encryption algorithm supplies encrypted versions of the control word, which are transmitted in special records. These are the *access entitlement checking messages*;
- at the receiving end, the access control equipment applies the inverse algorithm to regenerate the control word.

4.4 *Initialization modifier*

The initialization modifier is used in order to impose sufficiently short scrambling sequences to provide security, while avoiding the need for too frequent calculation of the control word. Thus, the use of different initialization modifiers for each structural unit of scrambled information causes the initialization word to change sufficiently frequently.

4.5 *Control word index*

To operate a segmented service, it is necessary to manage several related control words. These are identified by means of *indices.* The control word index used to access a unit of scrambled information must be obtainable from the transmitted signal.

5. Access entitlement checking messages

Each of these messages comprises:

- the control word index;
- . a control word change flag: a change of state indicates a change of value of the control word;
- an *authorization pointer* which identifies the authorization key located in the receiver security module to which the message is addressed;
- a *control parameter* which supplies value (e.g. date, price, etc.) for comparison limits set to these values, in the receiver security module, called the *authorization parameters*;
- the encrypted control word.

In order to descramble a unit of information, the receiver must previously have acquired the control word from an access entitlement checking message bearing the appropriate index.

For optimum efficiency, access entitlement checking messages relating to the same control word but corresponding either to different user groups or to different types of access control equipment should be grouped under the same index. Although this is not its only application, the indexing system described above enables the advance transmission of entitlement checking messages.

The conditional access equipment creates a table of active control words which is updated by the access entitlement checking messages independently of the scrambled data. To identify the correct control word, the descrambling device supplies the access control equipment with the corresponding index. The management of this table is a part of the facilities provided at the interface between the descrambler and the access control equipment.

6. Access entitlement management messages

The processing of an access entitlement management message validates or provides the entitlement. This process takes place within the security module associated with a cryptographic calculation involving a *distribution key.* This distribution key is used to encrypt and decrypt messages and/or authorization keys addressed to individual receivers. The corresponding cryptograms constitute the validation signal and are carried as part of the access entitlement management message.

In conditional access broadcasting systems, the access management messages may be broadcast. This is known as "over-air addressing". The cycle time associated with the distribution of over-air keys may be significantly reduced by the application of the principles of shared key encryption (see section 2 of Annex II). The access management messages may also be distributed by other media.

In the case of payment, per unit of time or per programme, the management messages convey an encrypted cost code, transmitted as part of the service. The credit held in the receiver may take the form of encrypted money tokens which are transmitted as part of an over-air addressing service (see section 3 of Annex II). Alternatively credit may take the form of stored money tokens distributed by other means. Payment consists of decrementing the stored credit according to the received cost code.

7. Access control equipment

This equipment includes a security module that is supplied with entitlement checking messages. This module may be buried or detachable (for example, smart card). The access control equipment communicates with the descrambler through a physical interface and logic circuits. The standardization of this interface is important in order to permit:

- the independence of the security module and the descrambling function built into the receiver;
- further development of the access control equipment.

If the security module contains an authorization with the same identifier as the authorization pointer in the entitlement checking message, it provides a control word if, in addition, the control parameters fulfil the conditions of the received authorization parameters. These may include:

- a date requirement, with the date in the control parameter falling between the starting and expiry dates in the authorization parameter;
- a price requirement by which an authorization may be provided only if a charge is accepted by the security module.

A transaction involving the security module may include three distinct stages:

- preliminary instructions, if present (e.g. password, user acceptance, etc.);
- operating instructions using the security module;
- result processing (e.g. delivery of control word).

Because a variety of security modules may be used, it would be desirable for the access control equipment to be independent of specific transactions. This independence can be provided if the access control equipment can interpret a sequence of instructions arranged in a specific language and transmitted within specific messages.

8. Applications

Conditional access techniques have been applied to some page organized teletext systems, to the use of independent data broadcasting systems (see Recommendation 653), satellite-broadcasting systems (see Report 1073) and terrestrial broadcasting systems (see Report 802). Some examples are given in Table I.

TABLE I

Examples of implementation of a conditional-access system

Reference in this Report	Page organized teletext systems		Data broadcasting systems .		MAC/packet family (Report 1073, C-MAC/packet and D2-MAC/packet)
	Teletext system A [CCIR, 1982-86, Part I, Chapter 5]	Teletext system B [CCIR, 1982-86, Part II]	Independent data lines in teletext system B	Layers 1 to 4 of teletext system C adopted in France	
Scrambling process § 4.1	Exclusive-OR combination of the data bytes with the bytes of a pseudo-random generator. An interpretation byte in the header indicates whether the record is scrambled or not. See § 3.1	Exclusive-OR combination of the data bytes with the bytes of a pseudo-random generator. Packet 27 links designate the page as scrambled. See § 20.1	Exclusive -OR combination of the data bytes with bytes from a scrambling stream generator. Regular occurrence of user-data-key blocks designates the service as being scrambled.	Exclusive -OR combination of the data bytes with the bytes of pseudo-random generator. A byte in the initialization modifier indicates whether the data group is scrambled or not Data groups with GT=0 or 1 are not scrambled.	*Picture:* double cut component rotation or single cut line rotation under the control of a pseudo-random generator *Sound:* exclusive-OR combination bit by bit of the data bits with the bits of a continuously running pseudo-random generator
Pseudo-random generator § 4.1	Combination of three multi-stage linear feedback shift register. See Annex I	Use of one-way function employing cipher feedback algorithm. See Notes to § 20	Scrambling stream generator uses deciphering algorithm connected in output feedback mode (ISO DIS 8372).	Combination of three multi-stage line feedback shift register.	*Picture:* two multi-stage linear feedback shift registers *Sound:* two multi-stage linear feedback shift registers initializing a further multi-stage linear feedback shift register
Pseudo-random generator synchronization § 4.1	First byte following the first US-X-Y sequence of the record. See § 2.3	First data byte of packet 0 of a designated page. See § 20	First byte of user data in user data block.	First byte following the initialization modifier.	Start of each picture frame
Initialization word § 4.2	12 bytes, see § 2.3	56 bits page key. See § 20.1	Scrambling stream initial variable is single byte at start of data block replicated eight times.	12 bytes	60 bits
Control word § 4.3	8 random bytes, see § 2.1	56 bits current system key. See § 20.1.3	64-bit user key	8 random bytes	60 bits being either randomly chosen or a cryptogram of the 256 frames counter
Initialization modifier § 4.4	4 bytes following the record header. See § 2.3	Not applicable	Not applicable.	4 bytes following the data group header.	The 8 bits frame-count

Entitlement checking messages (ECM) § 5	Designated records with classification numbers FFF and Y_{11} = 1; byte Y_{12} gives the index of the control word. Each message is introduced by the sequence US-3/F-3/F and comprises: – 3 bytes for the authorization pointer – 3 bytes for the control parameter – 16 bytes for the encrypted control word. See § 3.2	Designated packets include 22 bits authorization and control parameters, 112 bits encrypted control word. See § 20.1.3	One type of control block carries a user-data-key to all users who have a valid system key which enables them to decipher it.	Data groups for which GT (data group type, see Recommendation 653, Table Ia point 4.1) is equal to 14. The data groups are constituted of commands, each command identified by a command identifier and a command length identifier and composed of parameters identified by parameter identifier and parameter length identifier; two types of commands are defined: CI –0 reference to the security module to use; CI ≠ 0: entitlement checking command where each parameter carries an ECM and comprises: - 3 bytes for the authorization printer - 3 bytes for the control parameter - 16 bytes for encrypted control word	Packets designated in the service identification channel. In the conditional access system for D2-MAC/packet used among others, on the French direct broadcasting satellite system TDF1-TDF2, packet coding is in accordance with the provisions of the specifications in "EUROCRYPT conditional-access system for the MAC/packet family" (March 1989) [CCIR, 1986-90a] In the United Kingdom where D-MAC/packet has been adopted, British Satellite Broadcasting will commence BSS operations using the "EuroCypher a conditional access system for use with the MAC/packet family of transmission formats" [CCIR, 1986-90b]
Control word index § 4.5	Byte Y_{16} of scrambled record for descrambling and byte Y_{12} of ECM for updating. See § 3.1 and 3.2	Not applicable	Not applicable.		Not applicble
Change of control word and flag § 5	Bit b_8 of byte Y_{12} of ECM. See § 3.2	Current and new key words included in a designated packet of the user addressing See § 20.2	The correct versions of keys are identified by matching lable keys sent with the keys and the data blocks requiring these keys	Bit b 8 of parameter identifier of entitlement checking command	A new control word is transmitted every 256 frames and becomes the current control word when the frame count equals 0

Entitlement management message (EMM) § 6	Entitlement is currently managed by a Videotex system on a telecommunication network. See § 1.3	Entitlement is managed by over-air addressing of receiving equipment using shared and unique user addressing packets. See § 20.2	Entitlement managed by over-air addressing of access control module using shared and uniquely addressed data blocks. Data blocks for over-air addressing are multiplexed into same channel as message data.	Not yet standardized. Entitlement may be managed by a videotex system on a telecommunication network.	Packets designated in the SI channel. For conditional access to D2-MAC/packet services used among others on the French direct broadcasting satellite system, TDF1-TDF2 the packets are encoded in accordance with the provisions of the specifications in "EUROCRYPT conditional access system for the MAC/packet family" (March 1989) [CCIR, 1986-90a] In the United Kingdom where D/MAC/packet has been adopted, British Satelllite Broadcasting will commence BSS operations using the "EuroCypher a conditional access system for use with the MAC family of transmission formats" [CCIR, 1986-90b]
Access control equipment § 7	Built into the receiver and including a smart card reader. See § 1.3	Built into the receiver or functionally separate at service provider choice	Completely contained within security module. Accepts serial data from packet decoder and provides deciphered serial data to user.	Built into the receiver and including a smart card reader.	Functionally separated from the other parts of the receiver, by means of an interface to be standardized
Security module § 7	Smart card, with interface proposed for ISO standardization [ISO, 1986]	Built-in or detachable module or smart card	Microprocessor based unit loaded with application software to perform all data protocol handling and deciphering algorithms.	Smart card with interface proposed for ISO standardization.	Two solutions are proposed: – the smart card or – a built-in module

REFERENCES

ISO [1986] TC97/SC17/WG 4/N97 Integrated circuit card with contacts, Part III, Electronic signals and exchange protocols.

CCIR Documents

[1982-86]: 11/422 (Rev. 1) (Specification of teletext systems. Provisional Descriptive Booklet).

[1986-90]: a. JIWP 10-11/3-116 (France), b. JIWP 10-11/3-117 (UKIBA).

BIBLIOGRAPHY

BECKER, H. and PIPER, F. *Cypher Systems. The Protection of Communications.* Northwood Books, ISBN 719825717.

BRADSHAW, D.J. and WRIGHT, D.T. [1986] - BBC Datacast - Conditional Access Operation, IERE Publication No. 69, pp. 99-105, London, 16th-17th September, 1986.

DENNING, D. *Cryptography and Data Security.* Addison Wesley. ISBN 0-201-101-50-5.

GUILLOU, L. [November, 1980] Radiodiffusion à péage pour application au télétexte Antiope. Congrès international sur les systèmes et services nouveaux de télécommunications, Liège, Belgium.

GUILLOU, L. [April, 1984] Smart card and conditional access. Eurocrypt 1984, La Sorbonne, Paris, France.

ISO/TC97/SC17/WG [1987] 4 Identification cards. Integrated circuits with contact. ISO Dis 7816.

MASON, A. G. [1985] A pay-per-view over-air addressing system specified for direct broadcasting by satellite. IERE Publication No. 62.

WRIGHT, D.T. and EDWARDSON, S.M. [1986] - Key Management in Broadcast Conditional Access Systems, IEE Conf. Pub. 269, pp. 104-109, London, 27th-28th October, 1986.

CCIR Documents

[1982-86]: 11/139 (EBU); 11/307 (France); 11/308 (France); 11/379 (Canada).

[1986-90]: 11/35 (United Kingdom); 11/36 (United Kingdom); 11/40 (United Kingdom); 11/122 (France).

ANNEX I

SOME TERMS AND DEFINITIONS RELATED TO CONDITIONAL-ACCESS BROADCASTING SYSTEMS

Scrambling [in broadcasting] (Embrouillage, aleatorización)

Alteration of the characteristics of a broadcast vision/sound/data signal in order to prevent unauthorized reception of the information in a clear form. This alteration is a specified process under the control of the conditional-access system (sending end).

Descrambling [in broadcasting] (Désembrouillage, desaleatorización)

Restoration of the characteristics of a broadcast vision/sound/data signal in order to allow reception of the information in a clear form. This restoration is a specified process under the control of the conditional-access system (receiving end).

Note 1. – The terms scrambling and descrambling are applicable to both analogue and digital signals.

Note 2. – The terms should not be used to describe processes such as energy dispersal in a satellite system.

Conditional access control

The function of the conditional-access control at the sending end is to generate the scrambling control signals and the "keys" associated with the service.

The function of the conditional-access control at the receiving end is to produce the descrambling control signals in conjunction with the "keys" associated with the service.

Note. – The word "key" is used in the above definitions in a general sense equivalent to that of Question 37/11.

Encryption and *decryption* are terms used for methods which are used to protect (and interpret) some of the information within the "access-related messages" which have to be transmitted from the sending end to the receiving end of the conditional-access control functions.

BIBLIOGRAPHY

CCIR Documents

[1982-86]: 11/139 (EBU); 11/228 (Working Group on Terminology).

ANNEX II

CONDITIONAL-ACCESS BROADCASTING SYSTEMS: EXAMPLES OF THE PRINCIPLES OF SHARED KEY ENCRYPTION SYSTEMS FOR DIRECT BROADCASTING SATELLITE SERVICES AND DATA BROADCASTING SERVICES INCLUDING TELETEXT

1. Description of conditional access system using over-air addressing used in the United Kingdom

1.1 Over-air addressed conditional-access systems

The basic functions in an over-air addressed direct broadcasting satellite television encryption system are shown in figure 1. A control word (CW) which changes, typically every 10 seconds is used to control the scrambling process of the television signal A. This forms the scrambled signal, CW(A). The control word is transmitted to the receiver after its encryption with the supplementary key S. This cryptogramme which also includes data concerning the programme, e.g. price, is transmitted in an ECM packet /EBU, 1986/. The supplementary key S is common to all subscribers but unlike the control word changes infrequently, typically once per month. The long intervals between the changes of the S key allow time for it to be transmitted to each subscriber by means of the over-air addressing process. The S key together with subscriber entitlement messages (M) are encrypted with each subscribers distribution key D. These cryptogrammes are sent in EMM packets which are individually addressed to separate receivers. A full description is given in /Mason, 1986/

1.2 Reduction of the validation cycle time - the shared cryptogramme

Figure 2 shows the format of a shared cryptogramme that reduces the total number of bits needed to be transmitted in the subscriber validation cycle. 23 subscribers are included in the cryptogramme of figure 2 and these represent a subscriber group. Each member of the group shares the same main address which is used to access the cryptogramme, and the same distribution key which is used to unlock the cryptogramme. Since the 56 bit supplementary key is needed by each member of the group to recover the television signal, its 'overhead' in bits is shared amongst 23 subscribers. The same is true for the 4 bit mode word and the 24 bit main address. The total of 84 bits is sent to the entire group rather than to each subscriber individually. Thus for a group of 23 members, only 3.65 bits per subscriber need to be transmitted. This budget allows for a 12 bit subscriber word which can cater for 12 independent basic subscription services, 6 independent tiered services or pay-per-view tokens. These latter may be used for any services provided that they are all managed by a common service operator. The mode word identifies which option is being transmitted. If less bits are used for the subscriber word, e.g. a basic single service subscription system would only require one bit. This would enable the subscriber validation cycle time to be reduced by a much larger factor, for example the use of a 12 bit subscriber word typically reduces the cycle time by a factor of 6.5, whereas a the use of 1 bit subscriber word reduces the cycle time by a factor of 20.

1.2.1 Strategy for eliminating stolen distribution keys

If a subscriber is identified as having became a pirate, that key must be removed. A method is required to avoid disabling other subscribers who share the same key.

This is achieved by storing two secret keys in the receiver security device, rather than just one. The first key is the shared distribution key and the second is a unique key (U) which is not shared but is different for each subscriber. When a pirate is detected a new shared distribution key (D_{new}) is individually sent to each of the remaining genuine subscribers by encrypting it with their unique key (U), see figure 3. As an example, X, Y and Z are the subscribers in a given group sharing the distribution key (D_{old}) and X is identified as a pirate. Subscribers Y and Z are sent the key (D_{new}) by transmitting UY (D_{new}) and UZ(D_{new}). Clearly the format for the transmission of U(D) is much less efficient than the shared key but this is not important since only a small number of subscribers are involved. A broadcaster can be confident that the genuine subscribers have received the new shared distribution key (D) by transmitting U(D) until the subscribers have returned two subscription payments. Since the cycle time is likely to be less than one minute the broadcaster can be confident that the new shared key has been received. This confidence relies on the assumption that each subscriber of the group will be watching the programmes for more than one minute during a subscription period that has been purchased.

1.3 Over-air credit and programme price transmission for pay-per-view

High security must be provided for the over-air transmission of credit for a full pay-per-view service. This can be achieved with confidence if the appropriate principles are followed.

1.3.1 Over-air credit information

The value of a sum of money cannot be sent over-air encrypted with a key K in the form K(MONEY). This is very insecure since the message MONEY is not unique. Assume that MONEY is a transmitted code which represents a monotonically increasing sum of money and that the transmission of the value "all zeros" for the code represents zero credit for a subscriber. Encrypting this code with the key K produces some bit pattern for K(MONEY). A pirate can add money to the credit stored in the receiver without knowing the key K by simply altering the bit pattern of K(MONEY). When the receiver decrypts this new message with the secret key K the plaintext must be non-zero. This is because there can only be one mapping of the ciphertext to the plaintext. Since the original ciphertext meant "zero credit" any change must mean "non-zero credit". The pirate can thus add credit but does not know the amount.

This problem is avoided by appending a key to the money, without recognition of which the receiver will not accept it. This is achieved by sending the signal D(M,S) where D is the distribution key and S the supplementary key. For the receiver to validate the money bits (M) with key S it must be certain that the supplementary key S has been correctly received. For this purpose the signal S(P,CW,S) is transmitted, see section 1.3.4.

1.3.2 Transmission of money tokens

Since the validation cycle repeats, a method of transmitting the money tokens must be used which allows the receiver to accept a new payment but prevents it from continuously accumulating the same payment at each repetition of the cycle. Equally, local "replays" of old ciphertext must be incapable of deceiving the security device in the receiver into accepting previous payments more than once. Since the broadcast channel permits only one way communication, these requirements must be fulfilled when the rate of making payments is not in step with the rate at which the security device receives them.

The only known method of achieving these essential criteria is to transmit the total sum of all payments ever sent to the broadcaster on the signal (M_T). The security device stores the total sum of all payments it has ever received (M_R) and the payment value (M_P) separately in its money stores. M_P is the difference between M_T and M_R:

payment made $M_P = M_T - M_R$ for M_P greater than zero.

In this way payments can never be missed and replays of old payments will not cause M_P to increase because each time a payment is accepted M_R is set to the received M_T value. Thus a payment is only accepted if $M_T - M_R$ greater than zero. In order to keep the cycle time short a limit must be placed on the number of bits used to transmit the value M_T. The MAC/packet system specification /EBU, 1986/ uses 12 bits for MT providing for up to 4096 tokens.

1.3.3 Programme pricing

The programme related data (P) may represent the price of a programme. One method of pricing causes the money store to decrement every 10 seconds by a given value as the programme is received. An alternative is to request a single payment at the begining of the programme for its complete purchase. If the alternative method is used an identification number is stored when the programme is purchased in order to prevent the programme from being purchased twice, if for example the receiver is switched off during its transmission.

The programme related data (P) is "signed" as being correct by the supplementary key (S) in the same manner as for the subscriber money bits. This "signing" is by including the S key in the plaintext of the signal S(P,CW,S). It only requires the receiver to check that the S key has been correctly received in order to verify both the programme related data (prices) and the subscriber messages (money), see section 3.4.

1.3.4 Knowledge ot correct supplementary key

The security check on the supplementary key (S) is performed by means of the signal S(P,CW,S). This signal has the property that the S key is both contained in and also used to encrypt the plaintext. The security check in the receiver first obtains the key that appears to be the correct supplementary key S by decrypting the validation signal D(M,S). It then uses this received key S to decrypt the signal S(P,CW,S). Provided that the security device can decipher the signal S(P,CW,S) and obtain the same value for the supplementary key S, within the plaintext, there is a high degree of certainty that it has received the correct supplementary key S.

The probability that the security device will give false information is approximately 2^{-n} where n is the number of bits used for the S key. The system of /EBU, 1986/ uses 56 bits for the S key which gives a probability of false detection of 10^{-17}.

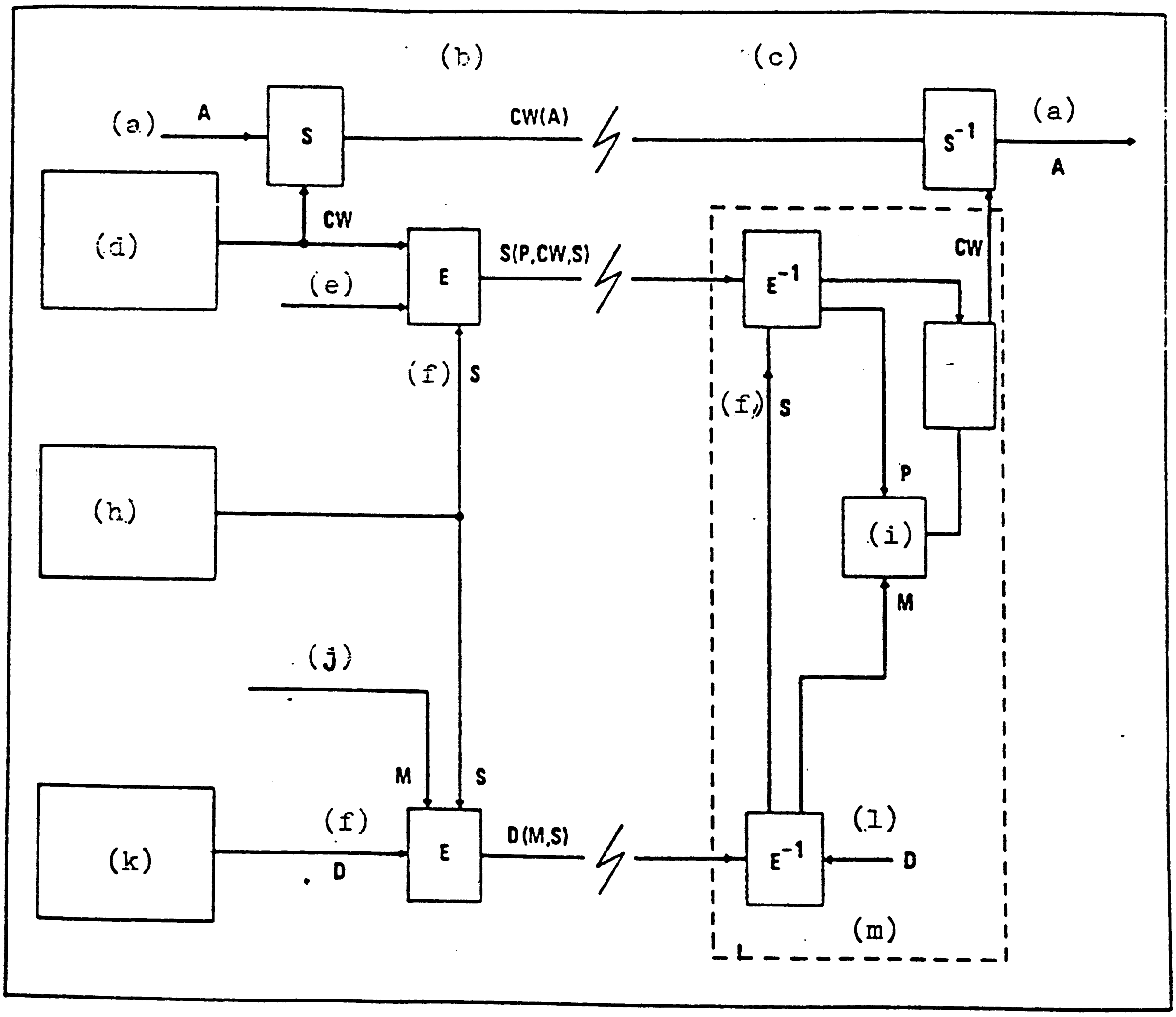


FIGURE 1 - Basic encryption system

(a) television signal
(b) transmitter
(c) receiver
(d) control word CW. changed every 10 seconds
(e) programme data P
(f) key
(g) gate
(h) supplementary key S. changed each month, say
(i) store
(j) customer message
(k) customer distribution key D
(l) secret customer key
(m) security devices

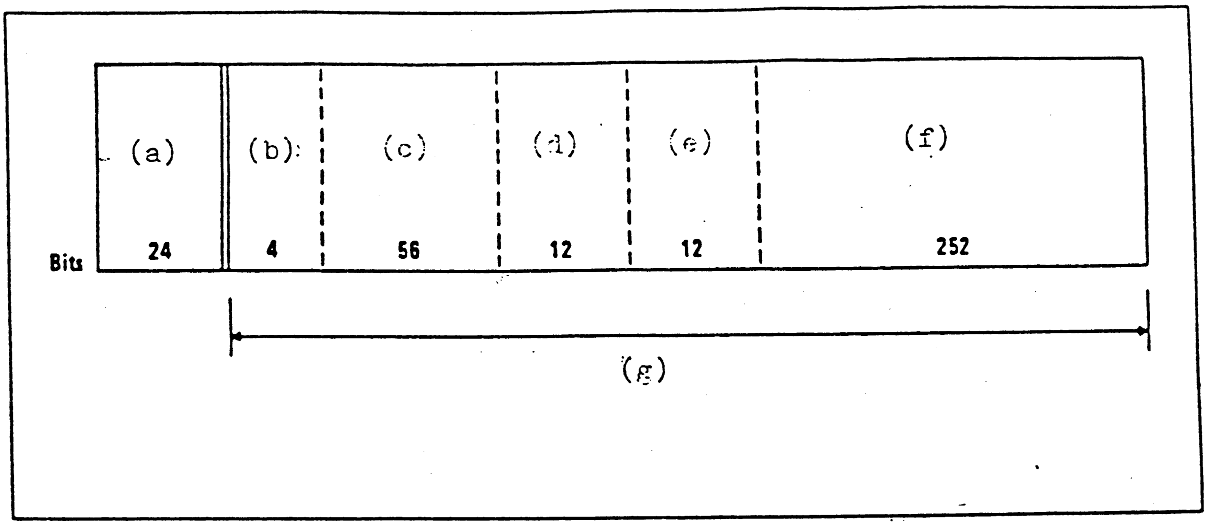


FIGURE 2 - Shared validation block

(a) shared address (b) mode (c) supplementary key S
(d) customer 1 (e) customer 2 (f) customers 3-23
(g) shared block encrypted with the shared distribution key D
Note. Error protection (not shown) - thirty (24,12)Golay code words

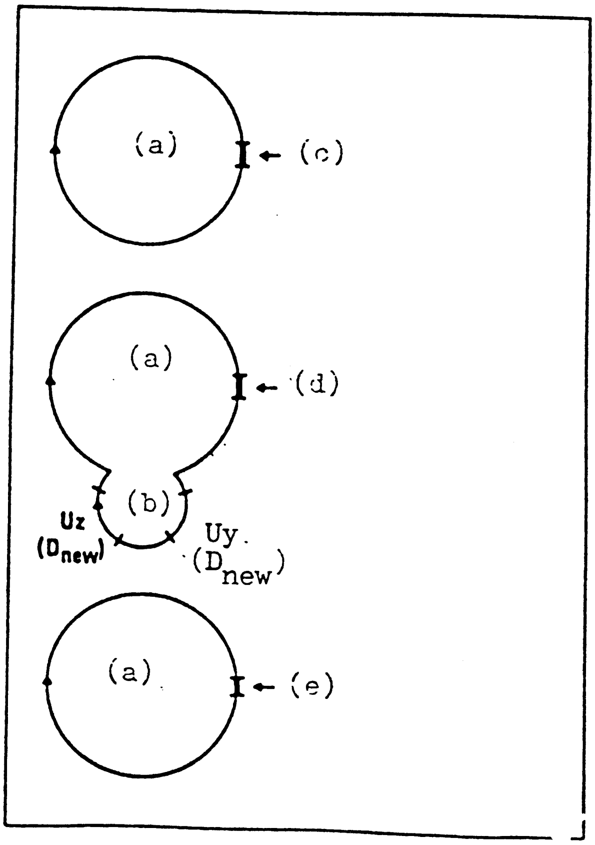


FIGURE 3 - Replacement of shared D key

(a) D cycle
(b) U cycle
(c) D_{old} customers X,Y,Z, share key D_{old}
(X,Y,Z)
(d) D_{new} X becomes a pirate and is eliminated
(Y,Z)
(e) D_{new} the broadcaster is sure that Y and Z have received D_{new}
(Y,Z) because they have both sent two subscriptions "

2. Description of a conditional access system using over-air addressing the Eurocrypt system

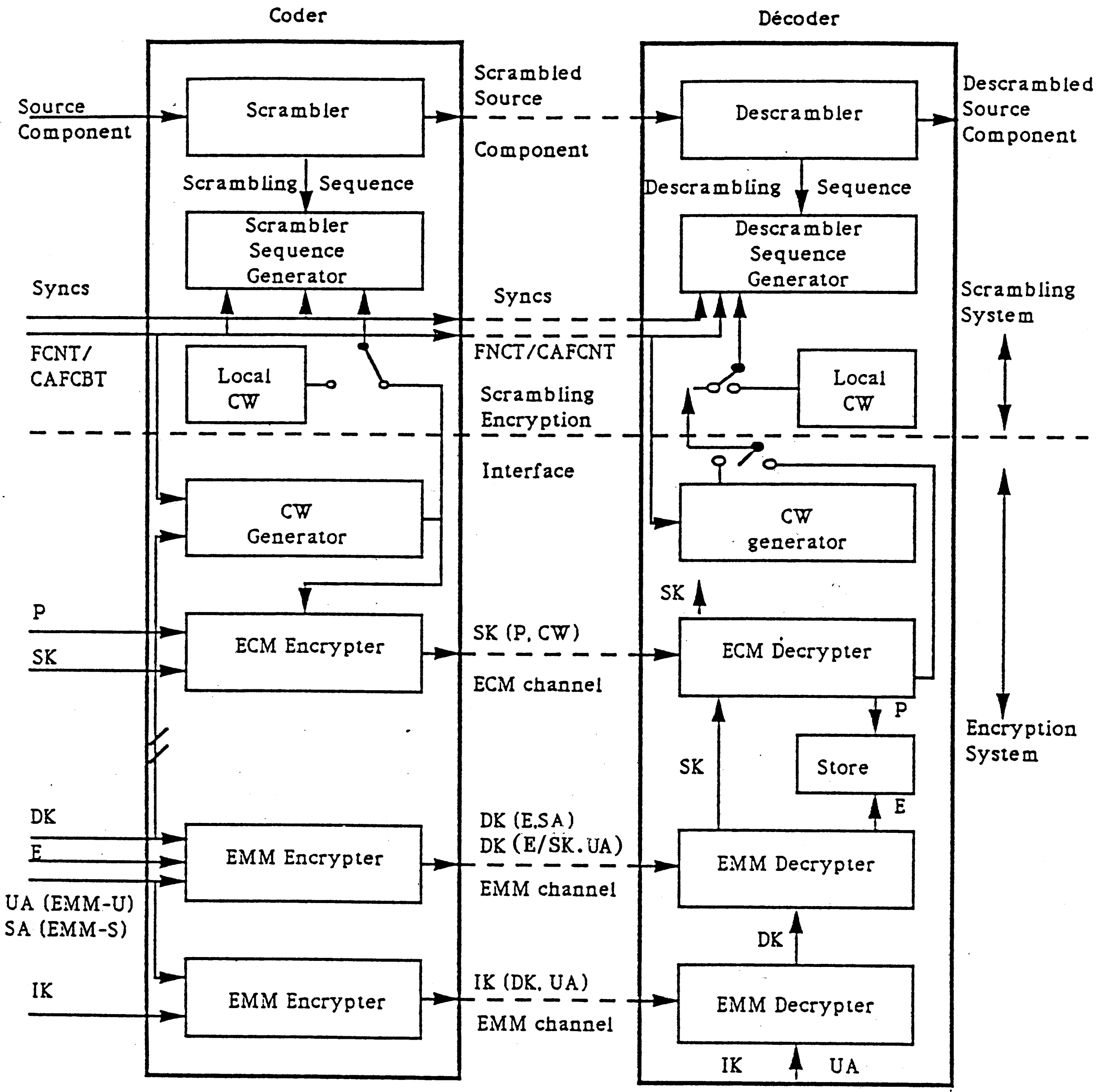
2.1 The scrambling and encryption systems

With reference to Figure 4, a control word (CW) is used to initialize the scrambling/descrambling sequence generator.

The control word is sent, encrypted by the session key (SK), in entitlement checking messages (ECM). Data relevant to the conditional access mode of the programme are also present in the ECM. The contents of the ECM is protected against falsification by a signing procedure. The session key (SK) is a secret information stored in a security processor. If the authorization parameters (entitlements) of the receiver are recognized by the security processor to match with conditional access parameters of the programme, the session key (SK) can be used to decrypt the CW.

The session key is a common to all users. The entitlements are updated periodically (every month for example) ; the session key can be changed under exceptionnal circumstances. Both, entitlements and session keys, may be sent to the users using over-air addressing methods in entitlement management messages (EMM). The session keys are sent encrypted with a distribution key DK specific to the program supplier. The contents of the EMM is (as for ECM) protected using a signing procedure. The distribution key may be specific to each user or to groups of users (or even to the entire audience). If the distribution key is specific to the user, then it may be used only to send entitlements or keys to a unique user referenced by his unique address (UA) in an unique EMM (called EMM-U). If the distribution key is common to a group of users, it may be used to send entitlements to the all group of users using a common shared EMM (called EMM-S). Since this would allow for a data rate reduction in the EMM messages it is used preferably to the first one. The first method would be best suited to the rare case where a change of the shared distribution key is needed.

The first distribution key of a programmer itself is also sent in EMM, encrypted with the issuer key IK. This key has the highest priority in the key system and is the only able to open the access for a new programmer in the security processor. The issuer key is specific for each user and is used in EMM-U.



ECM	: Entitlement checking Msg
EMM	: Entitlement Management Msg
CW	: Control Word
SK	: Service Key (or session Key)
FNCT	: Frame Count (from line 625)
CAFCNT	: Conditionnal Access from Frame Count (from line 625)
E	: Customer Entitlements
IK	: Issuer Key
UA	: Unique Receiver Address
P	: Program Data
SK (P;CW)	: P and CW encrypted with SK
DK (E;S)	: E and S encrypted with DK
IK(DK;UA)	: SK encrypted with IK
DK	: Distribution Key
SA	: Shared Receiver Address

Figure 4 : General Block Diagram Showing the key hierarchy of the Conditionnal Access System

2.2 Key hierarchy and key update

The functional use of the different keys are illustrated in Figure 5.

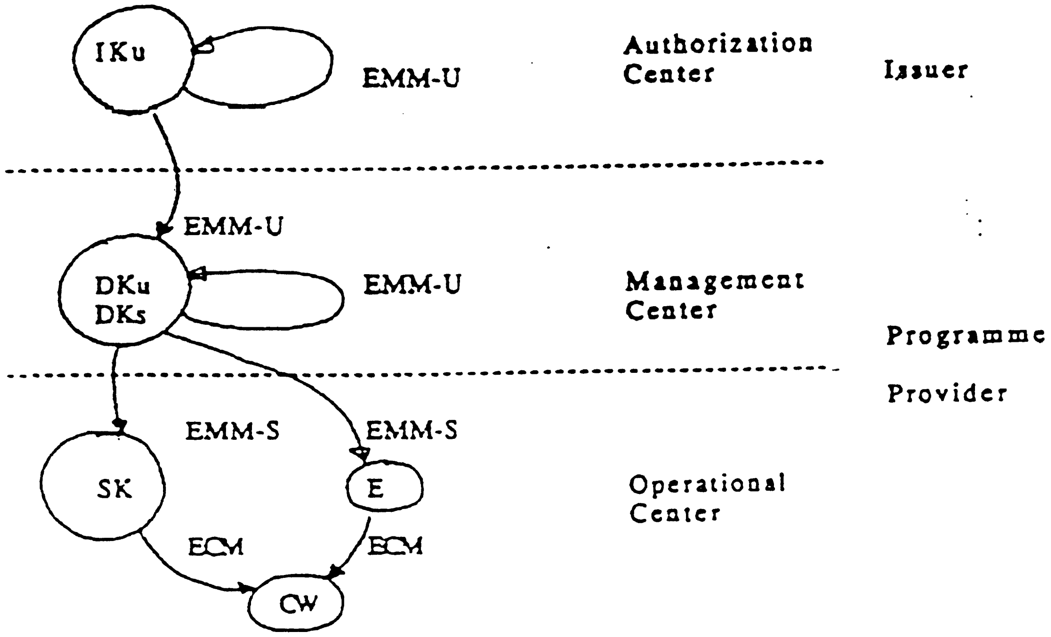


Figure 5 : Key hierarchy

2.2.1 Issuer key

- the issuer key sets and updates any kind of secret keys (DKu, DKs, SK, IKu).
- the issuer key is only able to open an access for a new programme provider in the security processor, by loading the first distribution key
- the issuer key is used only in unique messages (EMM-U).

2.2.2 Distribution key

- The DKu (unique distribution key) may update the DKs of the service via the EMM-U.
- the DKs (shared distribution key) sets or updates the session key (SK) and the entitlements E via EMM-S ; DKu may also be used for that purpose with EMM-U, but it is of less interest because of the overhead on data rate.

2.2.3 Session key

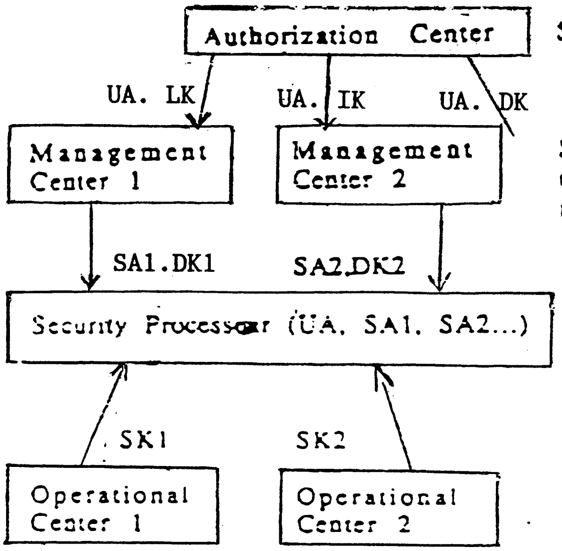
- SK is used to sign ECM and to encrypt the control words.

2.2.4 -Organization of key hierarchy

Two main scenarii are possible :

- the authorization center is in charge of the management of the secret keys (set and update) :
  - . the issuer sets and updates DKs and SK with IKu
  - . the programme provider updates the entitlements E with DKs.
- the authorization center is in charge of initialization of the programme provider but delegates afterwards the management of the keys belonging to the service :
  - . the issuer sets DKu (using IKu)
  - . the programme provider sets and updates DKs, SK and E.

The flowchart of operations may be summed up by :



Set of Distribution key

Set of Session key, Update of entitlements (rarely update of session or distribution key)

Storage of the session keys SK1 SK2... and of the entitlements

Compute of CW

2.3 Security of the system

2.3.1 Integrity of ECM and EMM

Two levels of data are transmitted in ECM or EMM :

- the secret data that will be transmitted in an encrypted form (CW, secret key)
- the non secret data whose content should have a high degree of protection (conditional access parameters, entitlements, address unique or shared) and which uses a "signing" procedure.
  For national regulation reasons, it may be necessary to send the entitlements in a confidential way. In that case, the entitlement contents is scrambled; this function is optional.

The structure of the message is then a clear text, followed eventually by an encrypted field and ended by a hashing field which signs all the message.

Structure of EMM :

user address (UA, SA) entitlement	[secret key]	hashing
scrambled * or clear text	encrypted	signature

[secret key] : optional
* The scrambled text is optional and applies only to entitlement description. This option may be chosen for national regulation reasons.

Structure of ECM :

conditional access parameters	CW	hashing
clear text	encrypted	signature

The modification of any field is barred through the hashing check.

2.3.2 Security through key hierarchy

The security of the system is achieved by introduction of two different levels of keys : the unique key and the shared key. The possession of the keys for a service is the first condition to get access to it ; the second condition is that the entitlements (subscription, pay-per-view credit...) must fit with the access conditions of a programme to allow the use of the session key SK. When a subscriber is removed the keys need not be changed and the entitlement will no longer be updated. Only when session keys are discovered by pirates will DKs be used to update. The use of unique keys (IKu or DKu) is exceptional and is reserved to update DKs. The update of DKs takes more data capacity because it needs EMM-U for individual addressing to all members of the group. Although the piracy of a unique key is of less interest because it applies only to one user ; this key may be also updated.

2.3.3 Security through the security processor

The security processor should provide secret data storage capability including an algorithm to decode encrypted fields and to check the integrity of the data. The system is flexible enough to upgrade the security processor changing the algorithm, increasing the processing capacity (introducing a new access condition)... without the need to change the receivers. This feature is made more easy if the security processor is present in a detachable form (smart card...). The software of the security processor should be designed in away to avoid any other use of the security mechanism than those it is built for.

2.3.4 security of transmission

The integrity of transmission of all the parameters describing the entitlement (theme/level, dates, credit, programme number...) is achieved through the hashing method. It is then impossible to modify successfully one or more bits of the message because of the failed checking.

For transmission of the credit, two methods have been retained :

- transmission of the total amount of credit acquired for an element of service. This total amount of credit is stored in the security processor. The purchase of any new programme is possible only if the remaining credit (total amount of credit - total amount of cost) is superior or equal to the cost of the programme. The total amount is transmitted together with an accreditation date.

- Transmission of a supplement of credit for an element of service. This supplement of credit is added to the total amount in the card. This supplement of credit is associated to an accreditation date to be sure that the same credit has not been added more than once in the security processor.

2.4 Shared messages EMM-S

The aim of the EMM-S is to reduce in a consequent way the data rate for management messages. Users of the same group receive the same update of their entitlement.

Supposing that an entitlement E must be sent to update a subscription to users, the message will be :

- a general EMM (EMM-G), interpreted by any receiver, to describe the common entitlement

- EMM-S messages to address groups of users.

EMM-G	entitlement E		
EMM-S	SA1	ADF1	Hashing 1
EMM-Sn	SAn	ADFn	Hashing n

Where :
- E is the entitlement to be renewed
- SA1 is the shared address of the group of 256 users
- ADF1 is the address field (256 bits) where one bit is allocated per user (if bit equal 1 then the entitlement is updated, if bit equal 0 then entitlement is not updated)
- Hashing is the signature of E, SAi, ADFi using the distribution key DKi.

This method allows a consequent reduction of data rate, 256 users sharing the same message (to be compared with EMM-U where 1 message is used per user).

REFERENCES

EBU [1986] Specification of the systems of the MAC/packet family - EBU Tech.3258.

MASON, A. [1986] The principles of the over air addressed pay-per-view encryption system for direct broadcasting by satellite and teletext. IERE Conference publication No. 69, September 1986.

BIBLIOGRAPHY

U.K. Department of Trade and Industry, London [1987] World system teletext and data broadcasting specification.