RECOMMENDATION ITU-R BT.810*

Conditional-access broadcasting systems

(1992)

The ITU Radiocommunication Assembly,

considering

a) that there is a growing demand in several countries to protect broadcast programmes against unauthorized reception;

b) that an efficient way of ensuring such a protection is to implement conditional-access broadcasting systems;

c) that examples of conditional-access broadcasting systems have been designed and are operated for terrestrial, cable and satellite television, as well as Teletext and data services;

d) that it is desirable to limit the number of different conditional-access systems while taking into account the different requirements of various broadcast services and transmission systems;

e) that putting as much common elements of conditional access as possible into the receivers at the outset would give the greatest potential to the general public to access protected services at a reduced equipment cost;

f) that copyright owners, programme suppliers and service providers desire highly secure broadcast/distribution networks to allow protection of their programmes through access control,

recommends

that conditional-access systems for broadcasting services should:

– be highly secure,

– share the largest number of common elements in the receiver, and

– be designed according to the fundamental principles listed in Annex 1.

---

* Radiocommunication Study Group 6 made editorial amendments to this Recommendation in 2002 in accordance with Resolution ITU-R 44.

ANNEX 1

Fundamental principles for conditional-access broadcasting systems

1 Introduction

The following principles apply generally to the delivery of current and future television services, sound programme services as well as Teletext and data broadcasting services. These principles apply for broadcast/delivery to consumers over terrestrial, cable, satellite, pre-recorded and other alternative media.*

2 Component of a conditional-access system

There are two distinct, and in many cases independent, components in a conditional-access system, each of which is a distinct information process. These two components are introduced below and are defined in Appendix 1.

2.1 Scrambling

This is the process of rendering the content of a service to have no value to unauthorized users by changing certain of its characteristics under the control of the conditional-access system at the sending end. The content of a service may be programme or other content such as data.

2.2 Access control

This is a provision of information to enable authorized users to descramble the service. The availability of this information is controlled by the conditional-access system.

Between the transmitter and the receiver(s), this information is structured in secure messages multiplexed with the signal itself.

At the receiving end(s), these messages are interpreted by the access control system in order to control the descrambling of the signal in the authorized receiver(s).

3 The requirements to be satisfied by a conditional-access control system

3.1 Quality

The scrambling and descrambling processes must not alter perceptibly the quality of the received picture, sound and data signals.

---

* Examples of implementation of conditional-access systems specifically applied to television satellite broadcasting in France, the United Kingdom and Japan are given in Appendix 2.

3.2 Security

The security of a system is the degree of difficulty encountered by an unauthorized user in attempting to gain access to the service. Security may be breached in two ways representing two aspects of difficulty:

– *descrambling the signal without reference to the access control process*. This is a function of the nature of the services and the scrambling method. Future television, sound and data broadcasting services are likely to be predominantly digital in nature and thus will allow for highly secure scrambling processes;

– *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.

3.3 Universal conditional access

Access is made available, to any authorized user meeting the conditions for access, via a common or universal scrambling algorithm. Universal conditional access simply means that everyone has access by using common processes and equipment, following common and user-friendly rules and procedures in order to comply with the access conditions set by a producer, provider or distributor. This will encourage the wider application of conditional-access services through simple, low cost, and flexible consumer equipment. Universal conditional access implies that descrambling would be common to all receivers, based on a standard scrambling algorithm, independent of delivery media used, and would still allow competition through company-specific implementations.

3.4 End-to-end content protection

End-to-end protection in distributing television, sound and data broadcasting services is the protection of content (programme or otherwise) and of access-related information (control or data) from origination to end, throughout delivery. Protection begins at point of origination and is maintained through to point of presentation* to consumer. This avoids the defeat of highly secure transmission systems through too easy a recording of programme content at home.

Thus, from any point of origination, end-to-end protection ensures that information, once concealed, remains concealed throughout all intermediary stages of the distribution system until it reaches the receiver where access will depend on a user meeting the conditions imposed by the originator or service distributor. In transit or in storage, protected content or other information never appears clear at any point or at any time until accessed by an authorized user. Thus, all transmittal and storage of content will be “as is”. This imposes no constraint on any intermediaries implementing their own “protection envelope” around the “protected” information provided they maintain its integrity, i.e., keep it intact “as is”. As content entering a point of origination may only be scrambled once, the scrambled content is sent as is. The scrambling key, however, is sent under control of a key distribution strategy, typically encrypted by a distribution key and sent to a consumer’s receiver to be stored encrypted with scrambling keys from various points of origination.

---

* See Appendix 1 for definitions.

3.5 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.

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

– time;

– various segments of the service;

– groups of intended users.

3.6 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;

– a consumer's receiver architecture must be flexible to implement distribution key and session key encryption/decryption facilities as well as descrambling key facilities in configurations ranging from buried and detachable processing units in the receiver to a portable personal intelligent security module (or smart card) with built-in secret session keys and personal code recognition logic.

3.7 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. Uneconomic use of the resources due to management or transmission overheads should be avoided.

3.8 Avoidance of impairments to the service

The following two 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.

3.9 Interaction with digital processing

It should be noted that scrambling processes may severely limit the possibility for further processing including bit-rate reduction.

3.10 Effect control

The system could allow for a range of signal intelligibility at the choice of the programme supplier as part of his marketing strategy.

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*.

The detailed structure of this process is given in Fig. 1.

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 is multiplexed with the signal itself. These are the access entitlement checking messages;

– at the receiving end, the access control equipment applies the inverse algorithm to regenerate the control word if all the access conditions have been met. The security module(s) in the receiver(s) could also perform cryptographic checksum computation and verification for ensuring integrity.

4.4 Initialization modifier

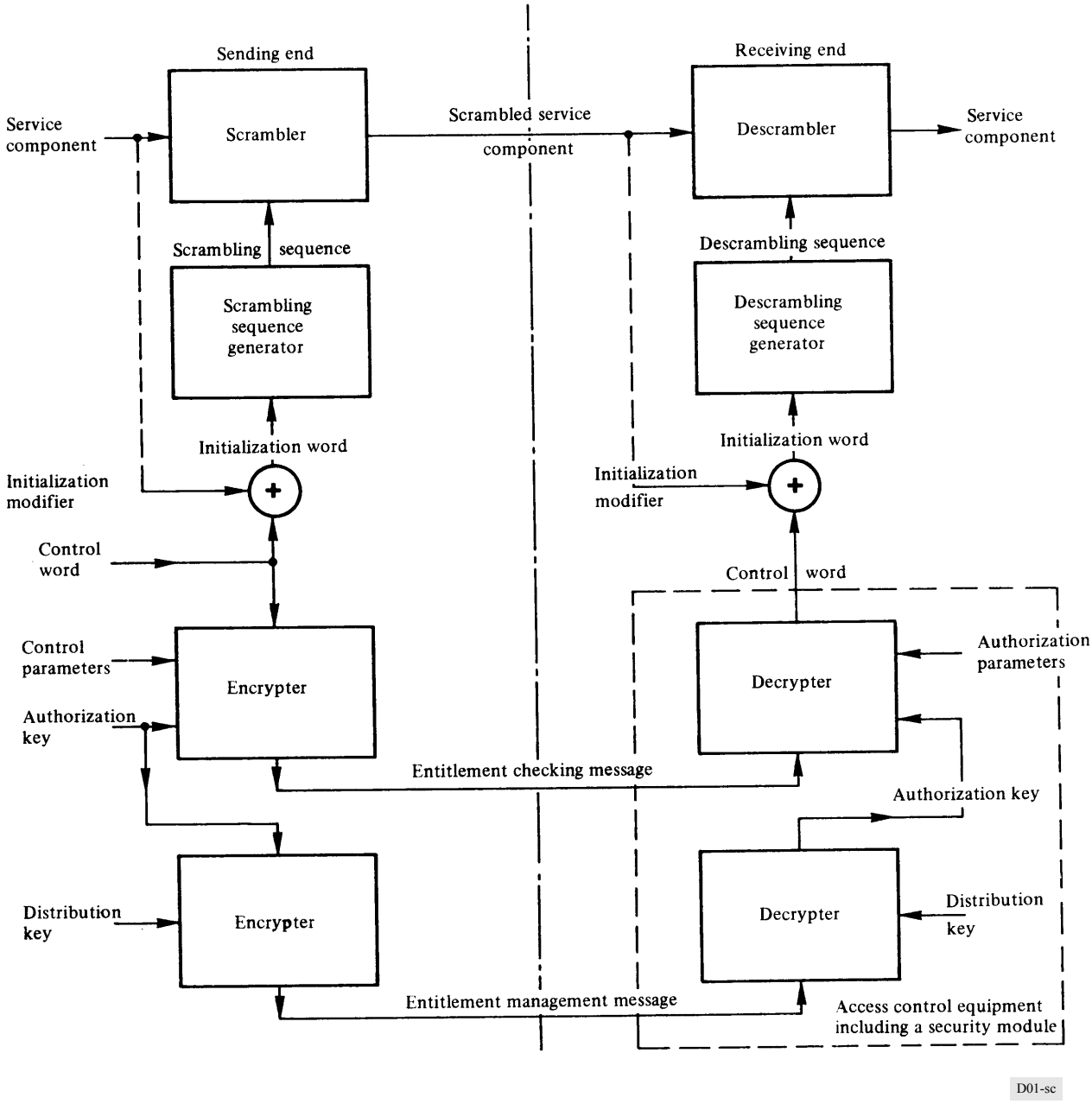
The initialization modifier is used in order to impose sufficiently short scrambling sequences to provide security, while avoiding the need for too frequent calculation of the control word. Thus, the use of different initialization modifiers for each structural unit of scrambled information causes the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

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.

FIGURE 1

Functional description of a conditional-access system



Note 1 – 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.

Note 2 – At the receiving end, the security mechanisms are performed inside the security module(s).

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. The access management messages may also be distributed by other media.

An example of operation is as follows. In the case of payment, per unit of time or per programme, the management messages can convey an encrypted cost code, transmitted as part of the service. The credit may be held in the receiver and may take the form of encrypted money tokens which are transmitted as part of an over-air addressing service. 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 (both allowing down loadable decryption algorithms). In the former case, access is permitted on a receiver basis whereas in the case of the detachable module (for example, smart card) access does not need to be constrained to a specific television set. The access control equipment communicates with the descrambler through a standardized 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.

APPENDIX 1

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

A user accesses a protected service by interacting via a receiver security module, secure module or decoder. If, in session, all the access conditions are met, authorization occurs, the scrambling key is released, and the content is descrambled.

Subscriber authentication, account confirmation, and validation of service availability or other programme control parameters activates the session encryption/decryption key to let the session conclude the authorization process.

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.

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.

Point of origination

This is the point in a distribution system where programme or other content first becomes a signal in its final broadcasting/distribution format. It marks the start of end-to-end protection. Entry content may be any form, not necessarily a humanly sensible form. The content input need not itself be intelligible.

Point of presentation

This is the point where programme or other content last occurs as a signal in a distribution system before it exists in a humanly sensible form at the receiver's screen and speakers. It marks the output from end-to-end protection.

NOTE 1 – The copyright owners, service providers, and distributors form a huge hierarchy of many possible points of origination in a flow of information to a consumer and thus in the flow of scrambled content and encrypted keys to a consumer. The point of origination ought to begin with a copyright holder or producer. In practice, most points of origination will be simply the points of entry wherever they may be in the system for business and operational reasons. While there may be many such points of entry, each is a unique and independent point from which the information can be consistently maintained in whatever format it may be input all the way through to a consumer.

APPENDIX 2

Examples of implementation of a conditional-access system

Reference in Annex 1	Page organized Teletext systems		Data broadcasting systems		MAC/packet family (C-MAC/packet and D2-MAC/packet)	Digital sub-carrier/NTSC
	Teletext system A	Teletext system B	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	Exclusive-OR combination of the data bytes with the bytes of a pseudo-random generator. Packet 27 links designate the page as scrambled	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 a 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	*Picture:* line rotation, line permutation, or a combination of the two methods controlled by 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 registers	Use of one-way function employing cipher feedback algorithm	Scrambling stream generator uses deciphering algorithm connected in output feedback mode (ISO DIS 8372)	Combination of three multi-stage line feedback shift registers	*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	Non-linear combination of the output of three multi-stage linear feedback shift registers (13, 11, 8 stages each)

APPENDIX 2 (*continued*)

Reference in Annex 1	Page organized Teletext systems		Data broadcasting systems		MAC/packet family (C-MAC/packet and D2-MAC/packet)	Digital sub-carrier/NTSC
	Teletext system A	Teletext system B	Independent data lines in Teletext system B	Layers 1 to 4 of Teletext system C adopted in France		
Pseudo-random generator synchronization § 4.1	First byte following the first US-X-Y sequence of the record	First data byte of packet 0 of a designated page	First byte of user data in user data block	First byte following the initialization modifier	Start of each picture frame	A timing signal is transmitted as a part of the sound frame control codes. Picture scrambling is started from the picture frame immediately after the timing signal, and sound scrambling is started from the sound scramble frame immediately after the timing signal
Initialization word § 4.2	12 bytes	56 bits page key	Scrambling stream initial variable is single byte at start of data block replicated eight times	12 bytes	60 bits	32 bits
Control word § 4.3	8 random bytes	56 bits current system key	64 bit user key	8 random bytes	60 bits being either randomly chosen or a cryptogram of the 256 counter	32 bits being randomly chosen (the same as the initialization word)
Initialization modifier § 4.4	4 bytes following the record header	Not applicable	Not applicable	4 bytes following the data group header	The 8 bits frame-count	Not applicable
Effect Control § 3.10	Not applicable	Not applicable	Not applicable	Not applicable	Not applicable	*Picture:* applicable *Sound:* not applicable

APPENDIX 2 (*continued*)

Reference in Annex 1	Page organized Teletext systems		Data broadcasting systems		MAC/packet family (C-MAC/packet and D2-MAC/packet)	Digital sub-carrier/NTSC
	Teletext system A	Teletext system B	Independent data lines in Teletext system B	Layers 1 to 4 of Teletext system C adopted in France		
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	Designated packets include 22 bits authorization and control parameters, 112 bits encrypted control word	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 ITU-R BT.653, Table 1a 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). 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"	Packets transmitted by the data channel within the digital sound frame. The meaning of each bit is defined, but the details are specified by the service provider
Control word index § 4.5	Byte Y_{16} of scrambled record for descrambling and byte Y_{12} of ECM for updating	Not applicable	Not applicable		Not applicable	Not applicable

APPENDIX 2 (*continued*)

Reference in Annex 1	Page organized Teletext systems		Data broadcasting systems		MAC/packet family (C-MAC/packet and D2-MAC/packet)	Digital sub-carrier/NTSC
	Teletext system A	Teletext system B	Independent data lines in Teletext system B	Layers 1 to 4 of Teletext system C adopted in France		
Change of control word and flag § 5	Bit b_8 of byte Y_{12} of ECM	Current and new key words included in a designated packet of the user addressing	The correct versions of keys are identified by matching label 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	A control word is renewed by the timing signal. The minimum renewal interval is 1 s
Entitlement management message (EMM) § 6	Entitlement is currently managed by a videotex system on a telecommunication network	Entitlement is managed by over-air addressing of receiving equipment using shared and unique user addressing packets	Entitlement is 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).	Packets transmitted by the data channel. They can also be distributed using IC cards. The meaning of each bit is defined, but the details are specified by the service provider

APPENDIX 2 (*end*)

Reference in Annex 1	Page organized Teletext systems		Data broadcasting systems		MAC/packet family (C-MAC/packet and D2-MAC/packet)	Digital sub-carrier/NTSC
	Teletext system A	Teletext system B	Independent data lines in Teletext system B	Layers 1 to 4 of Teletext system C adopted in France		
Entitlement management message (EMM) (*continued*)					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 family of transmission formats"	
Access control equipment § 7	Built into the receiver and including a smart card reader	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	Functionally separated from the other parts of the receiver, by installing it in an IC for exclusive use
Security module § 7	Smart card, with interface proposed for ISO standardization	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 standar-dization	Two solutions are proposed: – the smart card or – a built-in module	Built-in module