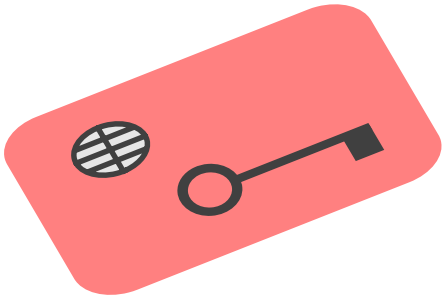


Functional model of a conditional access system

EBU Project Group B/CA

EBU Project Group B/CA has developed a functional model of a conditional access system for use with digital television broadcasts. It should be of benefit to EBU Members who intend to introduce encrypted digital broadcasts; by using this reference model, Members will be able to evaluate the different conditional access systems that are available.

The model is not intended as a specification for a particular system. Rather, it provides a framework for defining the terms and operating principles of conditional access systems and it illustrates some of the conflicts and trade-offs that occur when designing such systems.

1. Introduction

A conditional access (CA) system comprises a combination of *scrambling* and *encryption* to prevent unauthorized reception. Scrambling is the process of rendering the sound, pictures and data unintelligible. Encryption is the process of protecting the secret keys that have to be transmitted with the scrambled signal in order for the descrambler to work. After descrambling, any defects on the sound and pictures should be imperceptible, i.e. the CA system should be transparent.

The primary purpose of a CA system for broadcasting is to determine which individual receivers/set-top decoders shall be able to deliver particular programme services, or individual programmes, to the viewers. The reasons why access may need to be restricted include:

- to enforce payments by viewers who want access to particular programmes or programme services;
- to restrict access to a particular geographical area because of programme-rights considerations (territorial control can be enforced if the receiver has a built-in GPS system);

Original language: English
Manuscript received 6/10/95.

Glossary

Access Control System/Conditional Access System: The complete system for ensuring that broadcasting services are only accessible to those who are entitled to receive them. The system usually consists of three main parts – signal scrambling, the encryption of the electronic "keys" needed by the viewer, and the subscriber management system which ensures that viewers entitled to watch the scrambled programmes are enabled to do so.

Algorithm: A mathematical process (e.g. DES, RSA) which can be used for scrambling and descrambling a data stream.

Bouquet: A collection of services marketed as a single entity.

Conditional Access Sub-System (CASS): The part of the decoder which is concerned with decoding the electronic keys, and recovering the information needed to control the descrambling sequence. It is now usually implemented, all or in part, as a smart card.

Control Word: The key used in the descrambler.

Descrambling: The process of undoing the scrambling to yield intelligible pictures, sound and/or data services.

Electronic key: A general term for the data signals used to control the descrambling process in the decoders. There are several different levels of key, identifying the network which the subscriber is entitled to access, the services within that network that are available to the subscriber and the detailed control information to operate the descrambler. The ECMs are one component of this "key" data; all levels must be correctly decrypted in order to view the programme.

Encryption: The method of processing the continually-changing electronic keys needed to descramble the broadcast signals, so that they can be securely conveyed to the authorized users, either over-the-air or on smart cards.

Entitlement Control Message (ECM): A cryptogram of the control word and the access conditions. An ECM is a specific component of the electronic key signal and over-the-air addressing information. The ECMs are used to control the descrambler and are transmitted over-air in encrypted form.

Entitlement Management Message (EMM): A message authorizing a viewer to descramble a service. An EMM is a specific component of the electronic key signal and over-the-air addressing information. The EMMs are used to switch individual decoders, or groups of decoders, on or off and are transmitted over-air in encrypted form.

Event: A grouping of elementary broadcast data streams with a defined start and time (e.g. an advert or a news flash).

Impulse Pay-Per-View: Impulse Pay-Per-View requires no pre-booking. This rules out some Pay-Per-View methods (e.g. issuing smart cards for specific programmes). Smart card debit, or electronic banking via telephone line, both support impulse Pay-Per-View. Over-the-air addressing *can* support impulse PPV, provided that the time taken to process the request is sufficiently small (this implies a relatively large capacity for over-the-air addressing data in the transmission channel.

Multiplex: An assembly of all the digital data that is carrying one or more services within a single physical channel.

Pay-Per-View (PPV): A payment system whereby the viewer can pay for individual programmes rather than take out a period subscription. Pay-Per-View can work by debiting electronic credit stored in a smart card, by purchasing smart cards issued for special programmes, or by electronic banking using a telephone line to carry debiting information from the home to the bank.

Period Subscription: The most popular payment system, in which the viewer subscribes to a programme service for a calendar period (e.g. one year).

Piracy: Unauthorized access to controlled programmes. Common methods of piracy include the issue of counterfeit smart cards and decoders which bypass all or part of the access control system. The use of video cassette recorders to record descrambled pictures for distribution among friends/colleagues is also a simple method of piracy.

Programme: A television (or radio) presentation produced by programme providers for broadcasting as one of a sequence. A programme is a grouping of one or more events.

Scrambling: The method of continually changing the form of the broadcast signal so that, without a suitable decoder and electronic key, the signal is unintelligible.

Service: A sequence of events, programmes or data, based on a schedule, assembled by a service provider to be delivered to the viewer.

SimulCrypt: A system for allowing scrambled picture/sound signals to be received by decoders using different access control systems. The principle of the system is that the different ECMs and EMMs needed for the various access control systems are sent over-air together. Any one decoder picks out the information it needs and ignores the other codes. It is analagous to providing multiple front doors to a large house, each with a different lock and its own door key.

Smart Card: A device that looks rather like a credit card; it is used as a token of entitlement to descramble broadcast signals. Most of the major European access control systems use smart cards. Other systems that bury the same functionality inside the decoder do not usually allow the system to be changed to combat piracy or to add new services. Smart cards can be issued by the Subscriber Management System which can validate them by pre-programming them with keys to authorize access to certain tiers of programmes and/or data services. As part of the same issuing and validation process, the card may be personalised to make each one valid for one particular decoder only.

Subscriber Authorization System (SAS): The centre responsible for organizing, sequencing and delivering EMM and ECM data streams under direction from the Subscriber Management System.

Subscriber Management System (SMS): The business centre which issues the smart cards, sends out bills and receives payments from subscribers. An important resource of the Subscriber Management System is a database of infromation about the subscribers, the serial numbers of the decoders and information about the services to which they have subscribed. In commercial terms, this information is highly sensitive.

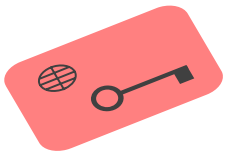


Figure 1
Vertically-integrated
CA system.

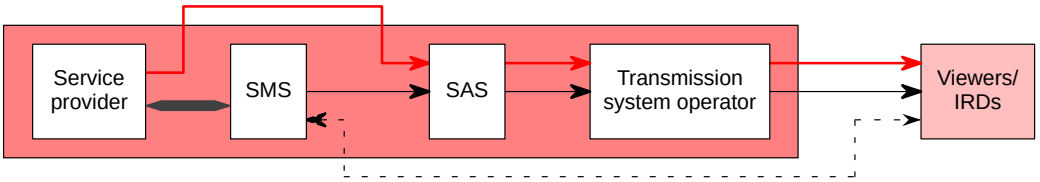


Figure 2
Devolved CA system.

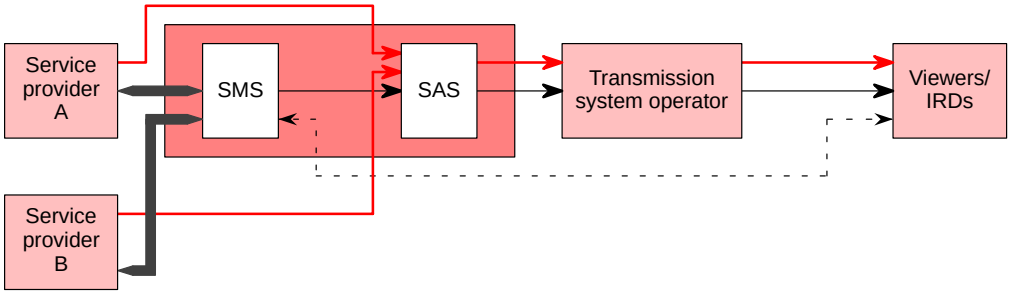
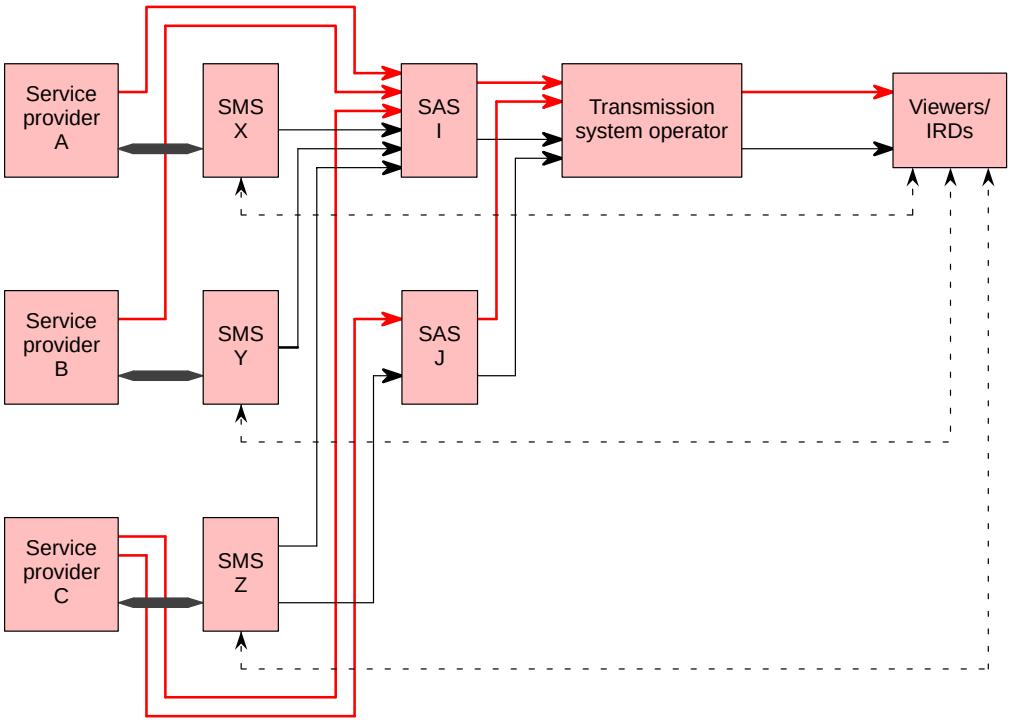
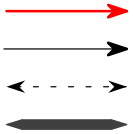


Figure 3
Devolved/shared/common
CA system.



KEY:



Programmes
Entitlements to view
Money, addresses and bills
Money and addresses

SMS = Subscriber Management System
SAS = Subscriber Authorization System
IRD = Integrated Receiver Decoder

– to facilitate parental control (i.e. to restrict access to certain categories of programme[2]).

2. Transactional models

Transactional models can be used to illustrate the underlying commercial transactions that take place in a conditional access broadcasting system, in a way which is independent of the technology employed. A similar analogy is sometimes used for the sale of goods to the public through retail and wholesale chains: in that situation, there is a flow of goods and services in one direction – from the manufacturers to the end customers – and a flow of money in the reverse direction.

A model of a vertically-integrated CA system is shown in *Fig. 1*. Here, the service provider is also the network operator and the CA system operator. Historically, CA systems originated in this form and the model remains true for many cable systems today: the cable operator acts as the service provider (usually by purchasing the rights to show programmes made by third parties) and also as the carrier and the CA system operator. In such circumstances, and especially where – as in most cable systems – the cable operator supplies and owns the decoders, a single proprietary system is acceptable, because there is no requirement to share any part of the system with competitors.

A model of a devolved CA system is shown in *Fig. 2*. In this case, the functions of the service provider, network operator and CA system operator are split. Indeed, there are two separate service providers, A and B, who share a common delivery system (owned and operated by a third party) and a common CA system which is owned and operated by a different third party. Thus all billing and collection of money is carried out by the CA system operator who then passes on payments in respect of programme rights back to the appropriate service providers. This model is true for many analogue satellite systems today and also applies to a retail market in which there is only one retailer. Note how the CA system operator has information about the names, addresses and entitlement status of all viewers; programme providers, on the other hand, have access only to the names, addresses and entitlement status of viewers to their own services.

An alternative model of a devolved CA system is shown in *Fig. 3.* Here, there are two independent CA Subscriber Authorization System (SAS) operators, I and J (see *Section 5.3.*). System J is used by service provider C only, whereas system I is used by all three service providers. Conversely, service providers A and B use system I only, whereas service provider C uses systems I and J. Thus, viewers to the services provided by C can use a decoder which is appropriate for either system I or J. A further feature of this model is that the billing and the money flow is directly between the viewers and the Subscriber Management System (SMS) operators (see *Section 5.3.*); it does not pass via the SAS operators or the transmission system operators. Consequently, sensitive information about the names and addresses of subscribers is known only to the appropriate service provider.

3. Functional model of a CA reference system

A functional model of a hypothetical CA reference system is now described. The model is loosely based on the *Eurocrypt* conditional access system but its principles of operation are expected to apply to CA systems generally.

3.1. Conditional Access Sub-System

A Conditional Access Sub-System (CASS) is a detachable security module which is used as part of the CA system in a receiver. It is also possible to embed the security module in the receiver itself, in which case each receiver will typically have its own secret individual address. Replacement of the CASS is one means of recovering from a piracy attack. Replacement of the CASS also enables new features to be added to the system as and when they are developed.

For analogue systems and some digital systems, the CASS is typically a *smart card* [1]. For digital systems which use the Common Interface (see *Section 3.6.*), the CASS will be a PCMCIA[3] module and this may have an associated smart card.

2. This is generally a Service Information (SI) function. However, regulators might specify that programmes should be scrambled where parental control is required. In current analogue systems, parental control often uses the CA system.

3. Personal Computer Manufacturers Computer Interface Association.

3.2. Scrambling and descrambling

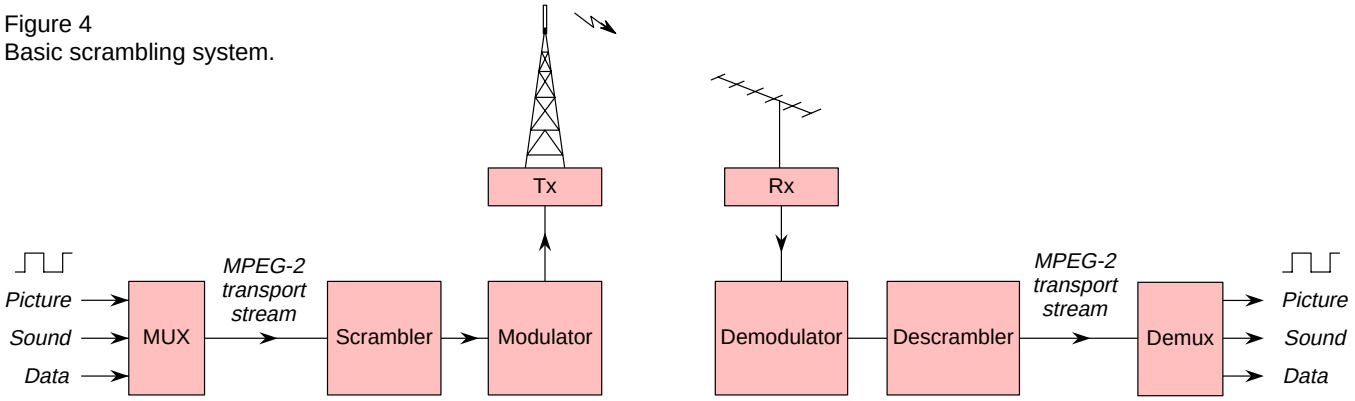
The basic process of scrambling and descrambling the broadcast MPEG-2 transport stream [2] is shown in *Fig. 4*. The European DVB Project has defined a suitable, highly-secure, Common Scrambling Algorithm.

3.3. Entitlement Control Messages

The generation, transmission and application of Entitlement Control Messages (ECMs) – which are used to recover the descrambling control word in the decoder – is illustrated in *Fig. 5*. The ECMs are combined with a service key and the result is decrypted to produce a control word. At present, the control word is typically 60 bits long and is updated every 2-10 seconds.

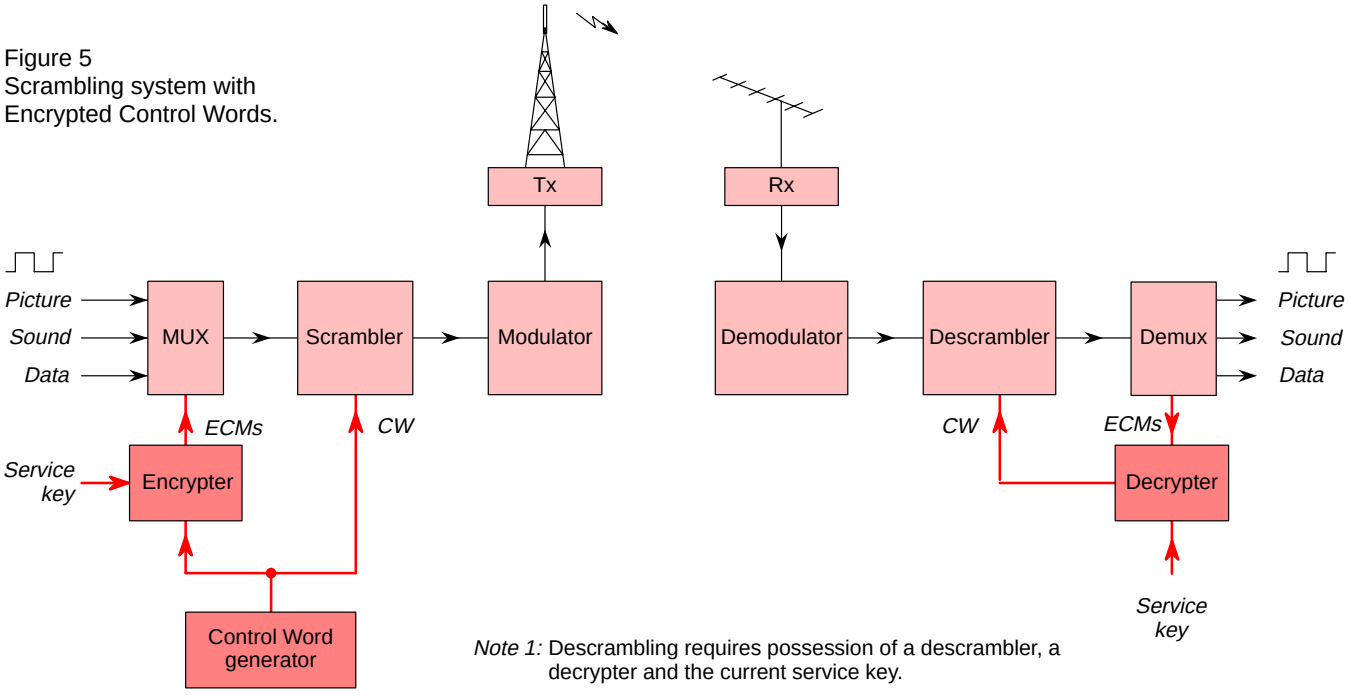
If the access conditions are to be changed at a programme boundary, it may be necessary to update the access conditions every frame, which is much more frequently than is required for security reasons. Alternatively, a change in access condi-

Figure 4
Basic scrambling system.



Note: In such a basic scrambling system, possession of a descrambler gives permanent entitlement to view.

Figure 5
Scrambling system with Encrypted Control Words.



Note 1: Descrambling requires possession of a descrambler, a decrypter and the current service key.

Note 2: Decryption recovers the descrambling Control Words (CW) from the Entitlement Control Messages (ECMs).

tions could be made frame-specific by sending out a change in entitlements in advance and then instigating the change with a flag. A third method would be to change the control word itself at a programme boundary. However, the second and third approaches would not allow a programme producer to change the access conditions instantaneously.

3.4. Entitlement Management Messages

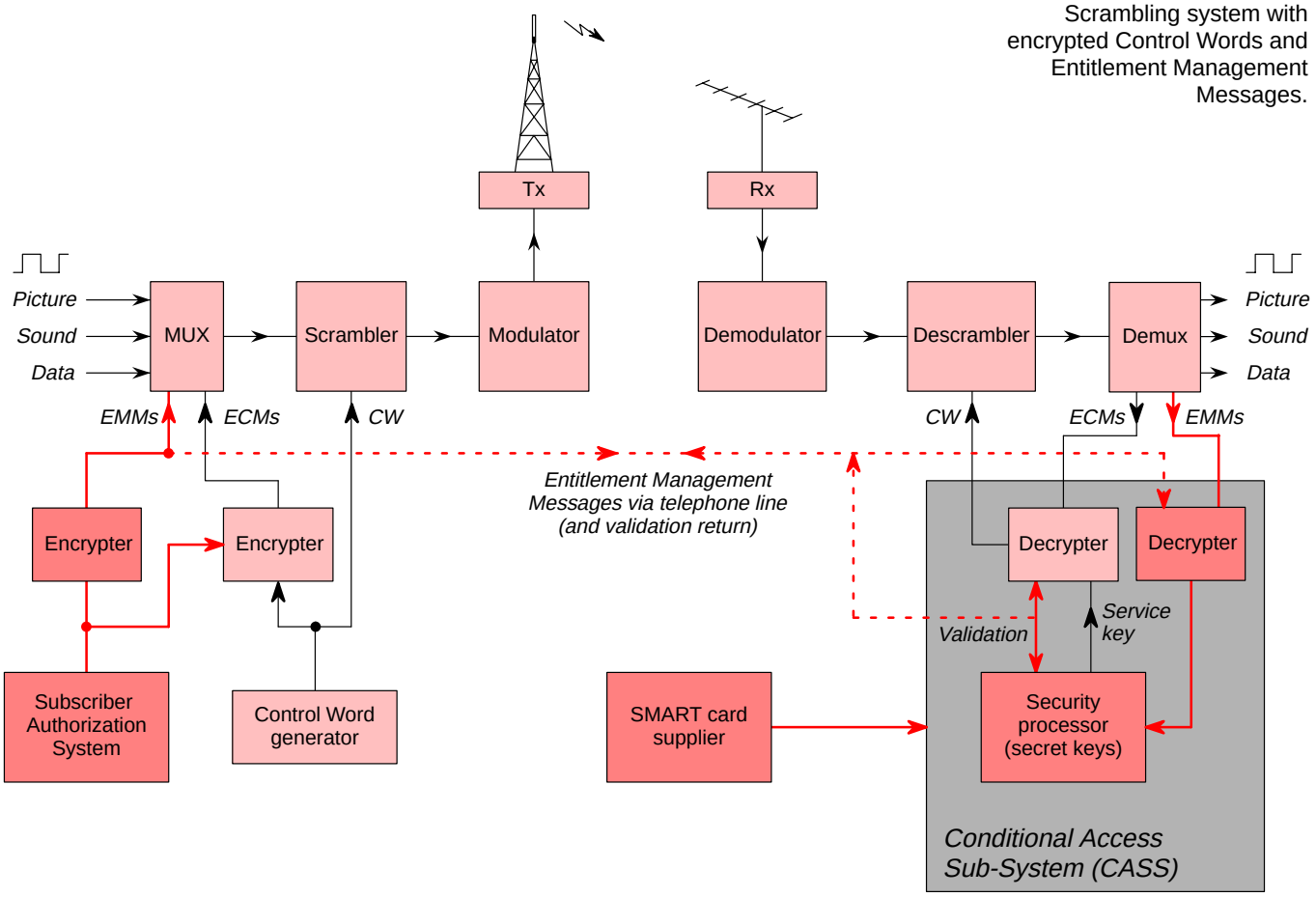
The generation, transmission, and application of Entitlement Management Messages (EMMs) by the Subscriber Authorization System is illustrated in *Fig 6.*

The card supplier provides the CASS (usually a smart card) and then the SAS sends the EMMs over-air or by another route, e.g. via a telephone line. To retain the confidentiality of customer information, it is best that the card supplier delivers the smart cards direct to the Subscriber Management System (or another business centre which guarantees confidentiality) for mailing to the viewer (see *Section 3.5.*).

It is possible to supply the cards through retail outlets as well, provided the retailer can guarantee confidentiality. In this situation, considerable care has to be taken if the cards have been pre-authorized by the SAS, because such cards will be a worthwhile target for theft.

When using the CA Common Interface [3], in conjuction with a PCMCIA module acting as the CASS, the descrambler is also situated in the CASS.

Figure 6
Scrambling system with encrypted Control Words and Entitlement Management Messages.



Note 1: Descrambling requires possession of a descrambler, a decrypter and the current service key.

Note 2: Decryption requires the Entitlement Management Messages (EMMs) for the current programme – which usually involves secret keys stored in a detachable Conditional Access Sub-System (CASS).

3.5. Subscriber Management System

As shown in *Fig 7.*, the reference model is completed by the addition of a Subscriber Management System (SMS), which deals with the billing of viewers and the collection of their payments. The control word need not be a decrypted ECM; it can be generated locally (e.g. from a seed) which means that the control word could be changed very quickly.

3.6. Common Interface

The European DVB Project has designed a Common Interface for use between the Integrated Receiver Decoder (IRD) and the CA system. As shown in *Fig. 8*, the IRD contains only those elements that are needed to receive clear broadcasts.

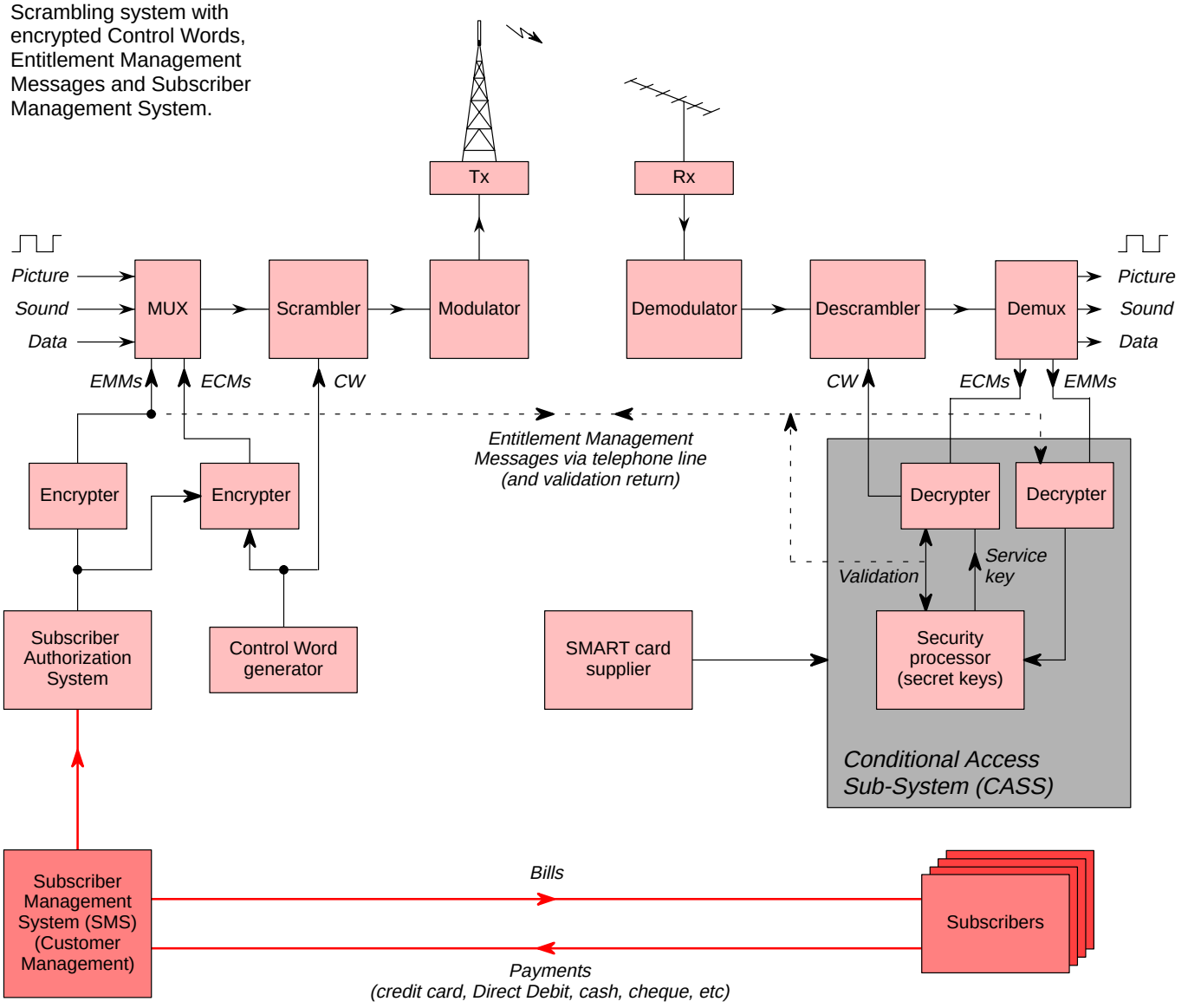
The CA system is contained in a low-priced, proprietary module which communicates with the IRD via the Common Interface. No secret conditional access data passes across the interface.

The Common Interface allows broadcasters to use CA modules which contain solutions from different suppliers, thus increasing their choice and anti-piracy options.

4. General requirements of a CA system

To be acceptable for use by EBU members, a conditional access system needs to meet the following general requirements, some of which conflict.

Figure 7
Scrambling system with encrypted Control Words, Entitlement Management Messages and Subscriber Management System.



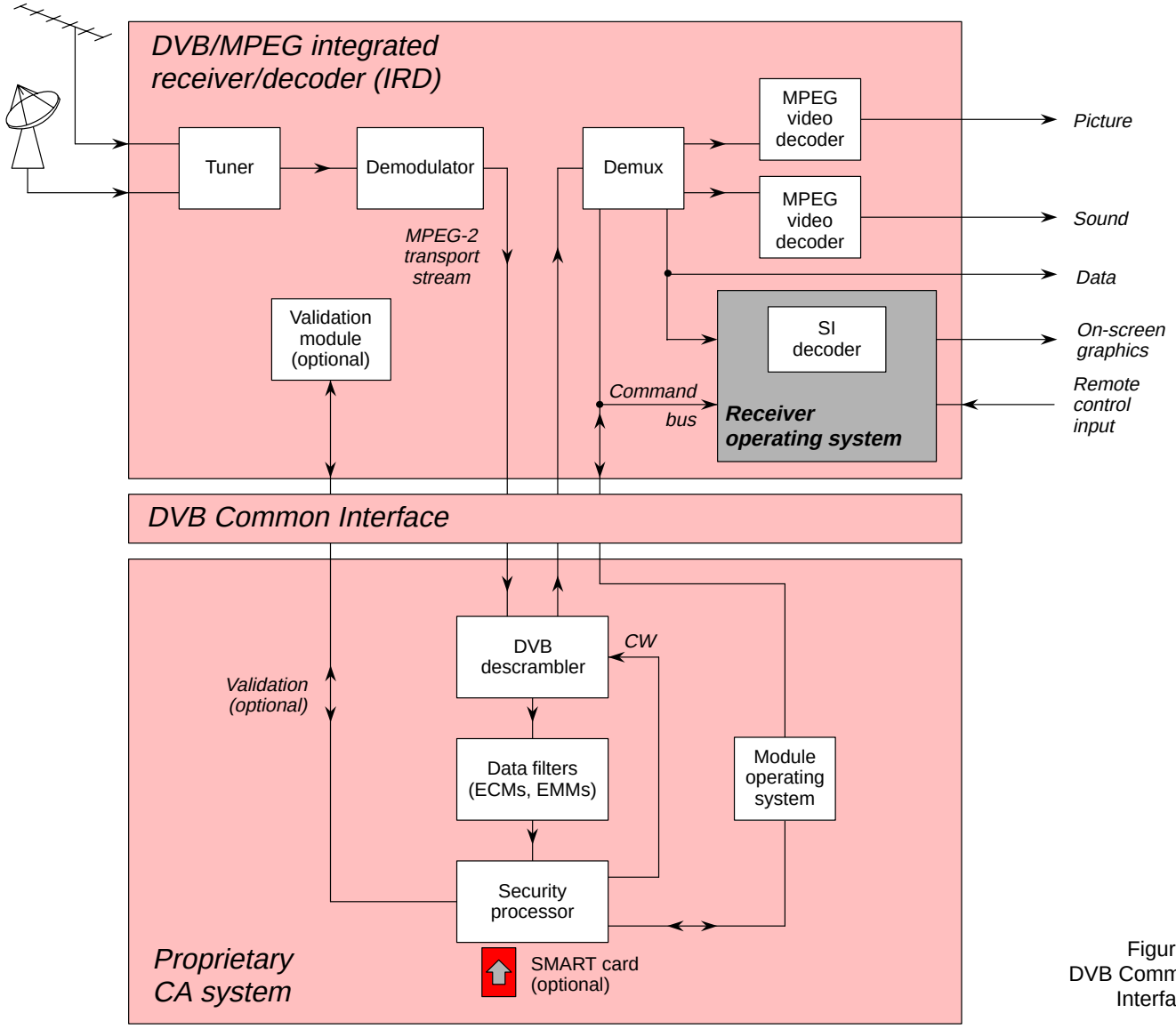


Figure 8
DVB Common Interface.

4.1. Convenience for viewers

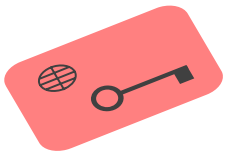
The CA system should impose a minimum of burden on the authorized viewer at any stage in the transaction. In particular it should not require special action when changing channels (e.g. swapping a smart card or keying in a Personal Identification Number) nor should it significantly delay presentation of picture and sound when "zapping" (a sensible upper limit on the "zapping" time is 1 second).

Furthermore, it should be easy to gain initial access to the broadcasts, requiring the minimum of equipment, outlay and effort. Ideally, the complete system would be integrated into the television set which would be able to access any combination of programme services to which individual viewers had subscribed.

It should be easy for the viewer to pay the necessary fees to the programme supplier. Payment methods should include all forms of monetary transaction including cash, direct debits and credit cards. The viewer might prefer to receive a single bill for any combination of services provided over a period of time. It may therefore be desirable, but not a necessity, for different CA system operators to share the use of smart cards.

4.2. Security

The CA system must be effective in preventing piracy, i.e. unauthorized viewing by people who are not entitled to access particular programmes or services. Although no CA technology can deliver per-



fect security, the overall system – combined with appropriate anti-piracy legislation and evasion-deterrent measures – must make piracy sufficiently difficult and/or uneconomic that the levels of evasion are kept small. Smart cards or payment cards must be resistant to tampering. For Pay-Per-View services in particular, the counting mechanism which indicates the remaining credit should be immune to resetting by unauthorized parties.

It is very important that the relationship between the service provider and the CA system operator is well defined so that, for example, a CA system operator can be compelled to act when piracy reaches a certain level. There are a number of ways to recover from a piracy attack. It is possible to initiate electronic counter measures over-air, whereby pirate cards are disabled or subtle changes are made in the operation of genuine CASSs. Alternatively, by issuing new CASSs, large changes can be made to the conditional access system.

4.3. Open marketing of digital receivers

The viewers should be able to benefit from a large choice of digital receivers or set-top boxes, produced by a wide range of manufacturers competing in an open market. Such an open market ideally requires that the complete digital broadcasting system, excluding the CA system, be fully described in open standards which are fully published by the appropriate organization (e.g. the ETSI[4] or the ISO[5]). The terms of licensing any Intellectual Property Rights (IPR) included within a standard must be regulated by the appropriate standards organization. (For example, in the case of an ETSI standard, licensing is open to all manufacturers on an equitable basis.)

It is undesirable for the CA system to be standardized: instead, the flexibility offered by the DVB Common Interface should ensure that a plurality of CA systems may be adopted (see *Section 3.6.*).

4.4. Open marketing of programme services

Authorized programme services should be accessible to any viewer whose IRD conforms to the relevant standard and who has the relevant CA entitlements issued solely under the control of the service provider. It must also be ensured that all approved service providers have fair access to a suitable delivery system.

4.5. Autonomy of the service provider's business

The primary contract should be between the service provider and the viewer. Although third parties (such as common carriers and/or CA system operators) may necessarily be involved in the broadcasting process, the CA system (and any other part of the system) should not require the service provider to share commercially-sensitive information with rival service providers, e.g. the identities of customers and their entitlements to view.

4.6. Low entry and operating costs

The cost of setting up and operating the CA system is significant but must not be prohibitive. In particular, it should be capable of being scaled to allow low start-up costs when the subscriber base is very small.

The system should not pose a constraint on the ultimate number of households that can be addressed; this could reach many tens of millions. The costs of upgrades to the CA system and of recovering from security breaches should be minimized by selecting a reliable and secure system.

5. Functional requirements of a CA system

5.1. Payment schemes

It is important that the CA system supports a wide range of charging and payment schemes.

These include:

– *Subscription (*pre-payment for a time period of viewing);

– *Pay-Per-View* (payment for a programme or group of programmes);

– *Impulse Pay-Per-View* (payment for a programme or group of programmes without advance notice).

Pay-Per-View (PPV) and Impulse Pay-Per-View (IPPV) often require the provision of a return path from the viewer to the CA system operator: in many systems this is implemented using a telephone connection and a modem built into the IRD. The return path can be used to record viewing history, which is important when considering the programme rights issues.

The acceptability and rules of operation for such a telephone return-path need further study. In par-

4. European Telecommunications Standards Institute.
5. International Organisation for Standardisation.

ticular, a system must exist for those viewers who do not have a telephone connection. One possible method would be to purchase credits in advance and to store them as viewing tokens on a smart card or CA module. The card or module could be re-authorized at a trusted dealer when information on past viewing could be transferred to the system operator. Provided security was not compromised, it would also be possible to have the smart card or module credited over-air with tokens which could be initiated by a telephoned (voice) request from the viewer. There must be a method to ensure that all service providers are paid fairly for the programmes provided, in proportion to the total number of viewer hours.

5.2. Multiple-decoder households

The question must be addressed as to whether payment authorizes:

1. the use of only one decoder to receive and decode the services;
2. use throughout a household, which may have multiple receivers/decoders and a VCR;
3. use by one individual anywhere within a household, in which case the entitlement needs to be transferable from one IRD to another, probably using a detachable security element such as a smart card.

In the third case given above, there is a conflict with the requirement to validate the security device for use with a particular decoder only. Therefore, each decoder should have its own CASS and the records of multiple CASSs within a household should be grouped together in the SMS to permit appropriate and reasonable billing.

5.3. Sharing of the CA system

In order to provide a fair and open market for CA broadcasts to develop, it is important that elements of the CA system can be shared. These include the following.

5.3.1. Receivers/decoders

One generic receiver/decoder should be capable of receiving and decoding CA broadcasts from a number of different broadcasters, perhaps using different delivery media (e.g. cable, satellite, terrestrial). This may imply that the decoder can support simultaneous use of multiple security devices, or that one security device can be shared between different service providers. In the latter case, the security device needs to be partitioned into independent zones so that operators have access to write to and read from only those zones which contain information about entitlements to view their own services. Where operators share a security device, it is important to resolve who issues and, more importantly, who re-issues the security device – especially in the case of a breach of security requiring a change of security device.

A particularly important and difficult requirement which arises from the need to share decoders is that of allowing the IRD to be tuned to broadcasts which do not necessarily carry the same over-air entitlement messages. It is worthwhile monitoring as many EMM data streams as possible, even when the receiver is in standby mode.

In some instances (for example, message broadcasting), it is necessary for the broadcaster to be able to address large numbers of decoders in a short period of time. In these situations, it is worth using shared keys to reduce the access time for large audiences. The audience is subdivided into groups of viewers; each person within a particular group has the same shared key which forms a part of the overall control word. Also, different messages intended for the same viewer can be combined together.

5.3.2. Delivery system

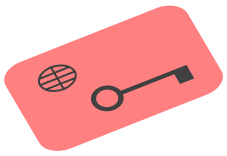
It is obvious that any one delivery medium (e.g. cable network, satellite transponder or terrestrial broadcast channel) should be capable of being shared between different and perhaps rival broadcasters. Less obvious, but perhaps equally important, is that any one transport stream should be capable of being decoded by different types of decoder, so that one broadcast can simultaneously use different kinds of CA system. This is the SimulCrypt concept (see *Section 7.1.1.*).

5.3.3. CA Systems

When considering the sharing of CA systems at the sending end, it is important to be able to divide the system into two separate functional elements:

a) *Subscriber Management System (SMS)*

The SMS is primarily responsible for sending out bills and receiving payments from viewers. It does not need to, and should not, be specific to a particular CA system. The SMS necessarily holds commercially-sensitive information such as the database of subscribers names and addresses and their entitlement status. Sharing of the SMS between rival broadcasters is possible if, and only if, it is operated by a trusted third party and only if adequate “firewalls” are pro-



vided so that any one service provider can access information only about subscribers to his or her own services. Although sharing an SMS may be seen as undesirable, it must be recognised that setting up and running an SMS is expensive, perhaps prohibitively so for services with a small number of subscribers at the outset.

The work of the SMS can be contracted out to a trusted third party (TTP), e.g. a secure and reliable organization such as a bank. There should be a subscriber database and the system must deal with changes to subscription details, installation difficulties, marketing, billing and card distribution. The SMS also manages the system installers and sends Entitlement Management Messages (to authorize viewers) to the Subscriber Authorization System queue.

To ensure the privacy of customer database information, the SMS could mail replacement smart cards and CA modules to the viewers. These could be provided pre-authorized by the conditional access system operator or could be authorized over-air by the Subscriber Authorization System using virtual addresses provided by the SMS.

At the moment, cable companies often send out a tape of customer usage to another company, at the end of the month, for billing.

b) *Subscriber Authorization System*

The Subscriber Authorization System (SAS) is primarily responsible for sending out the over-air entitlement messages and for validating security devices. The SAS needs a unique serial number (address) for each IRD security device but should not need access to commercially-sensitive information such as the names and addresses of subscribers. Hence it should be easily possible for rival broadcasters to share an SAS, although there are issues to be resolved concerning the queuing times for messages. Smart cards can be indirectly authorized over-air by the SAS.

The SAS generates a scrambler control word, encrypts the conditional access data, queues and prioritises the Entitlement Management Messages from the Subscriber Management System, and scrambles the pictures and sound. New messages from the SMS join the immediate queue, to be transmitted as soon as possible, and also join a regular cyclic queue where they stay until they expire. The frequency of transmission depends on the length of the queue and messages are expired by category. There will be a maximum limit on response time beyond which the system will not be usable. Disable messages may have an indefinite lifetime whereas enable messages may have a lifetime of a month or so. For security reasons, communication between the SMS and the SAS can be encrypted although this may not be necessary if all systems are in a secure environment.

5.4. Transcontrol at media boundaries

It will often be the case that a broadcast signal may travel via two or more different delivery media in tandem; for example the broadcast may be carried on a satellite and then conveyed into some homes via a cable system. In such cases it is often desirable to change the entitlement control at the media boundary without needing to descramble and rescramble completely. (This is possible with the use of the Common Scrambling Algorithm.) However, this method may present a security risk because one CA system operator would have to present the control word to another CA system operator inside the transcontrol equipment.

In practice it may be more secure (though more expensive) to descramble and rescramble at the media boundary. Descramblers and rescramblers from different CA system manufacturers could potentially be built into different PCMCIA modules.

Changing the entitlement control at the media boundary enables the end-transmission-system-operators to maintain direct control over each of their subscribers for all services provided. This means that the viewer only has to operate the CA system used by the end-transmission-system-operator. However, this approach also means that the service providers and the other transmission-system-operators that have supplied services to the end-transmission-system-operator cannot have direct and exclusive interaction with the subscribers.

Another approach would be to have no transcontrol at media boundaries. The viewer would have access to all services using either the SimulCrypt or MultiCrypt approaches. This has the disadvantage to the end-transmission-system-operator that all control is handed over to the original CA system operator and it therefore requires a good working relationship between all parties.

6. Operational requirements of a CA system

For security reasons it is important to include at least the following functions in a CA system:

– *Disable/enable decoder*

  Individual decoders or groups of decoders are prevented from descrambling any service, regardless of the authorizations stored in the smart card or other security device.

– *Disable/enable card*

  Individual smart cards, or groups of smart cards (or other security devices), need to be capable of being enabled or disabled over-air.

– *Disable/enable programme service*

  Individual smart cards, or groups of smart cards, need to be capable of being enabled or disabled over-air to decode any one particular programme service.

– *Send message to decoder*

  A text message is sent to individual decoders or groups of decoders for display on the screen; alternatively, the over-air message may comprise a display command and address of a message which is pre-stored in the decoder or smart card, e.g. to warn of imminent expiry or to request the viewer to contact the SMS because of account difficulties.

– *Send message to decoder for individual programme service*

  A text message is sent to individual decoders or groups of decoders in the same way as above, but is displayed only when the receiver/decoder selects the relevant programme service.

– *Show customer's ID card*

  The serial number of the smart card, or other means of identification (ID), is displayed on the screen. This is not the secret ID contained within the card, but is an unprotected ID which could be printed on the card. This function is useful for maintenance procedures.

– *Alter switching and drop-dead dates*

  An important security feature is that the algorithms used to decrypt the over-air entitlement messages and derive the descrambling control words can be changed. To allow smooth transition from one set of algorithms to the next, it is helpful if the smart card (or other security device) can store both algorithms and a date for switching from one to the other; this switching date can be alterable over-air. There should also be a "drop dead" date beyond which the card will cease to function at all. Note that not all CA systems perform these functions in this way and the implementation may be very system-dependent.

7. System implementation

7.1. Satellite transmission

The DVB Project has given its backing to two CA approaches for the transmission of digital television via satellite, namely *SimulCrypt* and *MultiCrypt*. These approaches are also relevant in cable and terrestrial transmission.

7.1.1. SimulCrypt

In the case of SimulCrypt, each service is transmitted with the entitlement messages for a number of different proprietary systems, so that decoders using different conditional access systems (in different geographic areas) can decode the service. SimulCrypt requires a common framework for signalling the different Entitlement Message streams. Access to the system is controlled by the system operators. Operation of the system requires commercial negotiations between broadcasters and conditional access operators. A code of conduct has been drawn up for the operation of SimulCrypt.

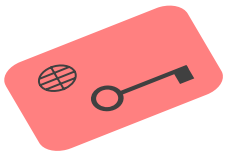
The philosophy behind the system is that in one geographical area, it will only be necessary to have a single smart card or CA module and a single decoder to receive the local service. If one wanted to descramble the service of a neighbouring area, one could subscribe to, and use the smart card/module for that service. Consequently, it is only necessary to have a single Subscriber Management System for a given area. When a viewer wants to watch services from two neighbouring areas, it is necessary for both services to carry the entitlement messages for that viewer. Therefore it is necessary to have secure links between the different Subscriber Management Systems of the different operators to allow transfer of the entitlement messages between operators.

7.1.2. MultiCrypt

MultiCrypt is an open system which allows competition between conditional access system providers and Subscriber Management System operators. MultiCrypt uses common receiver/decoder elements which could be built into television sets. The Common Conditional Access Interface can be used to implement MultiCrypt. Conditional access modules from different system operators can be plugged into different slots in the common receiver/decoder, using the common interface.

7.2. Return path

For most home installations, a return path could be set up between the set-top decoder and the Sub-



scriber Management System using a modem and the telephone network or a cable TV return. For example, calls could be initiated by the customer using a remote control unit which auto-dials a number delivered over-air. Also, the broadcaster may want the customer's decoder box to contact the SMS. This process could be initiated by commands sent over-air or (less likely) the SMS could dial up the customer's decoder box and interrogate it directly.

7.2.1. Reasons for using a return path

There are a number of reasons for using a return path:

a) *Enhanced security;*

The return path establishes a one-to-one link between the broadcaster and each decoder box. Communication via the return path should be encrypted.

b) *Payment billing;*

Pre-booked Pay-Per-View (PPV) and impulse PPV could be registered using the return path. Also, electronic viewing tokens could be purchased via the return path. A central server with a gateway would be necessary as a buffer for the large numbers of requests that would be expected as part of a Pay-Per-View service. These payment billing services could also be obtained by the viewer dialling up the SMS using his conventional telephone and having a conversation with an operator at the SMS. However this approach would be more time-consuming and costly to both the viewer and the SMS.

c) *Interactive TV;*

The return path could be used for audience participation (for example voting, games playing, teleshopping and telebanking). The return path could also be used for message delivery from the SMS to the decoder, although its limited bandwidth means that it is not very suitable for more complicated procedures such as Video-On-Demand (VOD). The return path could be used to deliver to the SMS diagnostic information such as measurements of signal strength and bit error rate (BER) to help solve transmission problems, and other information such as a record of programmes watched to provide statistical information to the broadcaster.

d) *Transmission of entitlement messages.*

For large shared networks, the capacity for transmission of entitlement messages may be inadequate and additional capacity may be achieved by using the telephone network. The return path could also be used to check that the decoder is tuned to the correct channel when giving authorization over-air. This could reduce the number of over-air signals that had to be repeated perpetually.

7.2.2. Reasons for not using a return path

There are also a number of reasons for not using a return path, as follows:

a) *Increased decoder cost;*

b) *Installation difficulties;*

The customer may not have a telephone at all, or may not have a telephone in the relevant room (in which case an extension socket would have to be fitted or a "cordless" connection would have to be used which would increase costs).

c) *Reliability of the telephone;*

In some areas, the reliability of the telephone service may be an issue.

d) *Blocking of normal calls;*

When the decoder is communicating, it will not be possible to make or receive normal telephone calls, unless there is more than one telephone line to the house.

e) *Telephone tapping.*

Depending on how the communication system works, there is a potential for reduced system security due to telephone tapping. Ideally, to overcome this problem, it is recommended that the Subscriber Management System should return the calls made by the IRD (although this will increase the costs to the SMS), the communication should be encrypted, and the Subscriber Management System should be able to identify individual IRDs.

Overall, the benefits of using a return path far exceed the costs. In situations where the return path does not exist but alternative facilities exist for performing some of its functions, decoders should be manufactured which are capable of implementing the return path. Cheaper decoders could be sold which do not have this option installed.

7.3. Home video recorders

If the viewer wants to watch one programme while recording another, then decisions will have to be made about the payment approach for the service. When using the Common Interface of the CA system, it should be possible to descramble two channels on the same multiplex (one to watch and the

other to record), using one PCMCIA module. To descramble two channels on different multiplexes, one would need two PCMCIA modules, two tuners and two MPEG-2 decoders.

One approach would be to view the descrambled picture from one channel and to record the scrambled picture from another channel. The recorded picture could then be descrambled at viewing time and the appropriate charges could be made in a Pay-Per-View system. Copy protection could be set for the digital recording. However, if the DVTR does not record the encrypted data associated with scrambling or, if the encryption mechanism would prevent successful descrambling at the later replay time, it would be possible to record an altered, but fixed, key. On replay, the picture could be descrambled using the fixed key, which would be specific to a particular recorder. This would help to ensure copyright protection by preventing a scrambled picture on a tape from one video recorder being descrambled by another video recorder.

Two descramblers could be used to permit the descrambling and recording of one programme whilst watching another. This has the disadvantage of added cost and complexity. Copy protection should be set for the original digital recording to hinder further digital recordings being made.

The question then arises as to whether to locate the second conditional access module in the IRD or in the video recorder. There are arguments in favour of both options and there is no need to standardize on one approach. In the end, the decision will be made by decoder and video recorder manufacturers. When costs fall sufficiently, it is likely that top-of-the-range IRDs and video recorders will have descramblers installed. (If the initial costs of digital video recorders are very high, it may also be possible to buy analogue video recorders with built-in descramblers).

The second descrambler/conditional access module could be installed either in the existing IRD box, or in the VCR. There are arguments in favour of both approaches:

In the existing IRD box

a) Having two complete descramblers in the IRD box, rather than one in the IRD box and one in the video recorder, would reduce the cost and complexity of the overall system but only by a relatively small amount;

b) The second descrambler could also be used if the viewer only owned an analogue video recorder.

In the video recorder

a) The video recorder could be used on its own, without the need for a separate IRD box to record programmes;

b) Any number of video recorders could be used without the need for multiple IRD boxes.

To reduce costs, the second descrambler could initially be available as an optional add-on to the IRD box.

8. Conclusions and recommendations

A basic set of transactional and functional models of CA systems for use with digital video broadcasting systems has been outlined. These models are intended to help EBU Members to understand and evaluate practical CA systems for use with future DVB services and, in particular, to understand the functionality, technical terms, and trade-offs in these systems. The specification or evaluation of a practical CA system requires considerably more depth and detail than could be included in this outline. In particular, an evaluation of security issues requires a careful analysis of the overall system security, including non-technical issues such as the theft of data.

Acknowledgements

EBU Project Group B/CA acknowledges a particular debt of gratitude to Dr. S.R. Ely and Mr. G.D. Plumb of BBC Research and Development Department for their considerable contribution to the development of the reference model.

Bibliography

[1] ISO 7816: **Identification Cards, Parts 1–6.**
(This ISO Standard describes “smart cards”).

[2] ISO/IEC 13818-1: **Generic coding of moving pictures and associated audio systems.**
(This ISO/IEC Standard describes “MPEG-2”).

[3] **Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications.**
DVB Document A007, July 1995.