Common Characteristics of CA Systems

1. GENERIC CA SYSTEM

1.1 Introduction

The primary purpose of a CA system is to ensure that there is an auditable means of ensuring that payment is received in return for the consumption of broadcasting programme rights. The technical system that enables this process to take place is called a conditional access system – access to certain programming is made conditional upon payment for the consumed content.

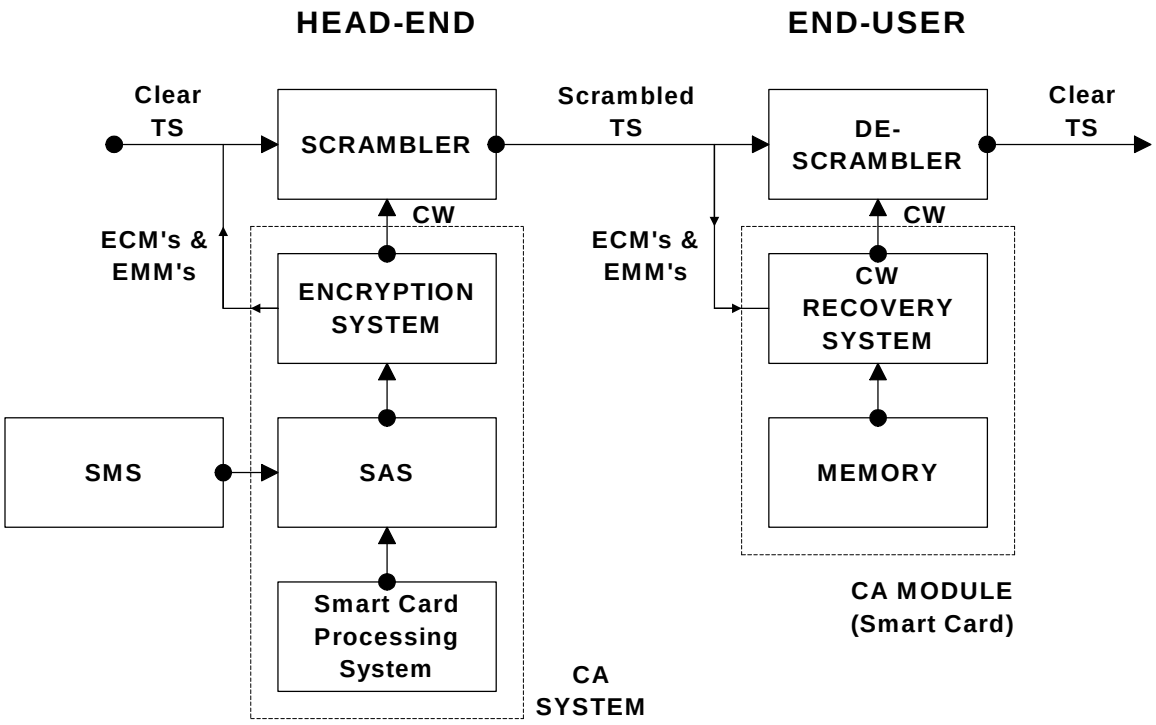
The reasons for implementing a CA system could include the following:

- To enforce payment, by the end-user, for consumed broadcasting programmes or programme services
- To restrict access to the programming to a particular geographical area, because of programme rights considerations
- To facilitate parental control i.e. to restrict access to certain categories of programming

1.2 Essential Components of a CA System

A typical CA system consists of three components: signal scrambling, the encryption of the electronic "keys" required by the end-user terminal, and the Subscriber Management System (SMS) that ensures that viewers entitled to consume the scrambled programmes are enabled to do so. These key components of a CA system, within a hypothetical broadcasting chain, are detailed in the diagram overleaf.

COMPONENTS OF A GENERIC CA SYSTEM



1.3 Scrambling & Descrambling

The digitised broadcasting stream, also known as a Transport Stream (TS), is applied to the scrambler. This stage contains a powerful algorithm that is designed to minimise the likelihood of an illegal ("pirate") attack over a long period of time. It scrambles the TS when it is "primed" or "seeded" by a Control Word. After each packet in the TS has been scrambled, the packet header is modified to indicate that it has been scrambled.

The output of the scrambler is applied to the distribution medium (cable, satellite or terrestrial) for delivery to the end-user. The CW is recovered from the encrypted keys in the scrambled TS and the keys stored on the smart card and is applied to a matching de-scrambling algorithm to recover the original programme content.

Common Scrambling Algorithm

The Digital Video Broadcasting (DVB) organisation, a structure based in Europe has developed a standardised Common Scrambling Algorithm (CSA) for the scrambling and de-scrambling operations mentioned above. It has become the *de facto* scrambling algorithm that is used in most current digital broadcasting CA systems around the world. To date, 117 licences have been granted for the descrambling technology (largely to STB manufacturers), while 55 licences have been granted for the scrambling technology (mainly to manufacturers of scramblers).

The CSA is comprised of the Common Descrambling System and Scrambling Technology. The specification for each section is distributed separately under arrangements with the European Telecommunications Standards Institute (ETSI), which acts as Custodian for the four companies that developed the CSA.

The Common Descrambled System is licensed to manufacturers of STB's and IRD's and their components, and to providers, designers and other entities engaged in conditional access. The Scrambling Technology is licensed to manufacturers of scramblers, who in turn sub-licence the purchasers of scramblers.

The CSA technology is made available to any interested party in good standing and upon signature of a licence agreement. The custodian of the CSA may be contacted at:

ETSI
Head of Administration Department
F-06921 SOPHIA ANTIPOLIS CEDEX
FRANCE

Fax: +33.4.9365-4716

1.4 Encryption & Decryption of Keys

The CA system at the head-end of the broadcasting operation generates the control word for the scrambler and also generates and encrypts special scrambling keys, the ECM's and EMM's. These encrypted keys are used in conjunction with the entitlements stored on the smart card in the STB, to recover the control word for descrambling the TS. ECM's are related to the programme content at a given time and are used for recovering the control word. The CA sub-system in the STB will decrypt the control word only when authorised to do so-that authority is sent to the STB in the form of an EMM. EMM's thus convey information related to the status of the subscription. This layered approach is fundamental to the operation of all proprietary CA systems in use today.

The Subscriber Access System (SAS) stores information in its database that is related to the smart card (serial number, unique identifier, entitlements) and other house-keeping information. The smart card management system provides the SAS with information on smart cards that have been processed for use in the pay-broadcasting operation.

1.5 Subscriber Management System (SMS)

The SMS contains a complete data base of all the subscribers in the pay-broadcasting network. It is capable of performing accounting operations on this data as well as issuing commands to the CA system to enable or disable subscribers for products. It is also responsible for requesting the return path manager, in an interactive system, to collect each subscriber's IPPV information.

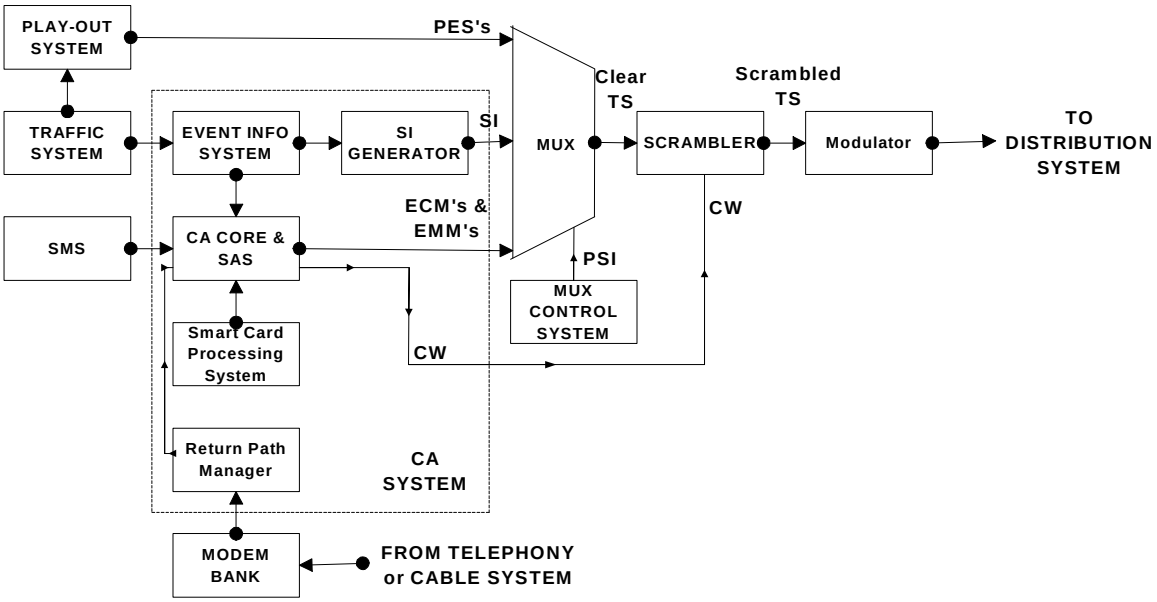
The smart card's serial number must be registered on the SAS before it is possible to enable that smart card via the SMS. The SMS does not need any other information from the smart card, other than its serial number, for normal pay-broadcasting operation.

2. HEAD-END CA COMPONENTS

2.1 Overview

The diagram below depicts the important components of a generic CA system at the head-end of a DVB pay-broadcasting operation. Brief explanations are offered of the key components relating to the CA system in the following sections.

CA COMPONENTS:
HEAD-END



2.2 Play-Out System

This is the facility where the broadcast material intended for the subscriber is assembled, stored, processed (sub-titling, teletext, advertisement switching etc.), played out, encoded and compressed into MPEG-2 format Packetised Elementary Streams (PES's).

2.3 Traffic Management System

This system controls the automation systems associated with the play-out of the services. It performs this task according to a broadcasting schedule.

2.4 SI Generator

The Service Information (SI) protocol is an important DVB-specified set of tables that assist the STB and the end-user adapt to the dynamics of the received DVB programme stream. The SI generator is driven by schedule information from the

traffic management system.

2.5 SMS

The Subscriber Management System contains a complete database of subscribers. It is capable of performing accounting operations on this data, as well as of issuing commands to the CA system to enable or disable products for subscribers.

2.6 SAS

The Subscriber Authorisation System is a database that is tightly coupled to the CA system. This database is changed by commands from the SMS.

2.7 CA Core

This system generates the control word for scrambling the multiplexed transport stream as well as the encrypted keys (ECM's and EMM's) used to enable the subscriber's smart card to descramble the scrambled transport stream.

2.8 Smart Card Processing System

This system processes entitlement information into the smart cards used in the system. It also provides a means for registering processed cards with the SAS.

2.9 Return-Path Management System

This system acts as the return-path link interface between the CA system and the STB. This system collects information on PPV consumption by the subscriber.

2.10 Multiplexer (MUX)

The multiplexer aggregates all the data streams from the above systems into a single Time Division Multiplexed (TDM) transport stream.

2.11 MUX Control System

The MUX control system, in addition to dedicated MUX control functions, also generates the MPEG-2 specified Programme Specific Information (PSI), a set of 4 tables that are fundamentally important to the successful operation of the STB.

2.12 Scrambler

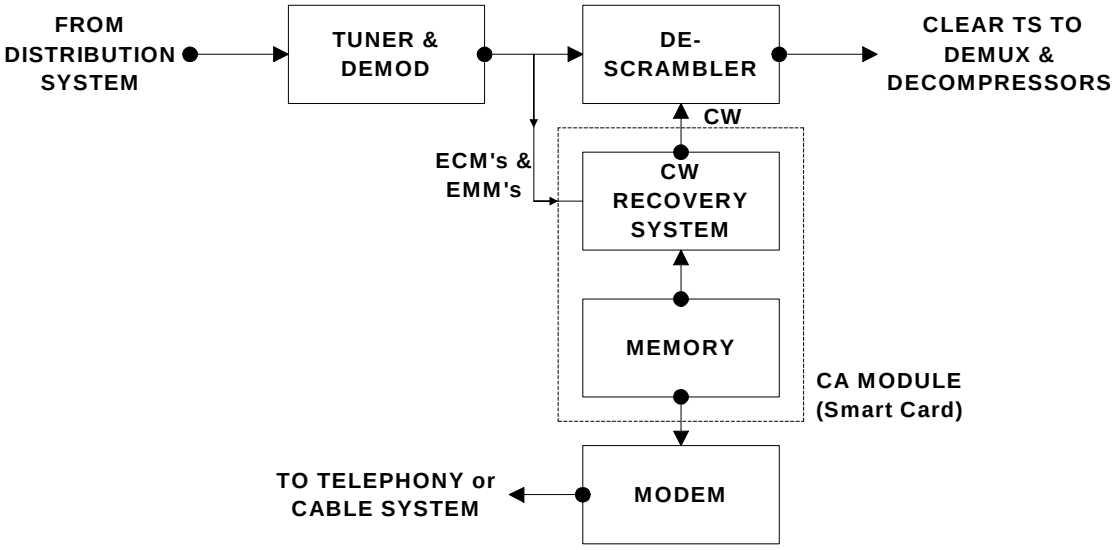
This device scrambles the multiplexed transport stream. It contains a powerful algorithm and is "seeded" by the control word generated by the CA system. In DVB systems, the scrambler implements the Common Scrambling Algorithm (CSA).

3. SET TOP BOX (STB) CA COMPONENTS

3.1 Overview

The diagram below depicts the generic CA components associated with the STB of a subscriber to a DVB pay-broadcasting operation. Brief explanations are offered of the key components relating to the CA system in the following sections.

CA COMPONENTS: STB



3.2 Descrambler

This device descrambles the scrambled transport stream. It contains a powerful algorithm and is "seeded" by the control word recovered by the STB's CA module . In DVB systems, the descrambler implements the Common Descrambling Algorithm (CDA).

3.3 CA Module

This system regenerates the control word that is required to "seed" the descrambling algorithm. It is fed by the ECM's and EMM's recovered from the scrambled transport stream. It may be in the form of a smart card or a plug-in module. The smart card should comply with the ISO 7816 standard.

3.4 Modem

The STB modem establishes a means to convey PPV consumption data from the smart card to the head-end.

4. PROPOSED REQUIREMENTS FOR A CA SYSTEM

4.1 Overview

Objectives of a CA System

The overall objectives of a CA system are:

- To ensure that restricted broadcasting programme rights are complied with in the delivery of this material to end-users;
- To ensure that there is an auditable trail of payments back to the rights holders of the material that has been broadcast;

Current International Situation on CA Systems

CA systems are almost by definition not capable of being standardised – a great deal of intellectual property is associated with CA systems, the disclosure of which could compromise the commercial integrity of existing and future broadcasting operations, as well as that of CA system vendors. In view of this, the standards bodies associated with digital broadcasting in Europe (the DVB) and in the USA (the ATSC) have consciously not mandated a CA standard for their digital broadcasting platforms. These standards bodies have instead established certain boundary requirements and promoted the development of standards that permit different CA systems to inter-operate on the same broadcasting platform, without inconvenience to the end-user.

The flexibility offered by this open standards approach to CA, ensures that multiple CA systems can be implemented on the same broadcasting platform in a fair, reasonable and non-discriminatory manner.

Some authorities may additionally wish to control the security elements of CA systems operating within their areas of jurisdiction. This implies that all operating CA systems will need to comply with any directive on CA systems issued by such authority.

4.2 General Requirements

Viewer Convenience

The CA system should impose a minimal burden on an authorised viewer at any stage in the transaction. In particular, it should not require special action when changing channels nor should it significantly delay the presentation of picture and sound when “zapping” or “surfing” across programmes.

Furthermore, it should be easy to gain initial access to broadcasts, requiring a 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 service supplier. Payment methods should include all forms of monetary transaction including cash, direct debits and credit cards. The viewer may prefer to receive a single bill for a combination of services provided over a period of time.

Security

The CA system must be effective in preventing piracy i.e. the unauthorised viewing by those not entitled to access particular programmes or services. Although no CA technology can deliver perfect 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 must be resistant to tampering. For PPV services in particular, the counting mechanism that indicates the remaining credit on the smart card, should be immune to resetting by unauthorised parties.

It is very important that the relationship between the service provider and the CA system operator be well defined so that, for example, a CA system operator can be compelled to act when piracy reaches a certain level.

Certain administrations may wish to extend their jurisdiction to the control of the secure elements within a CA system. This should be provided for in the CA system, without infringing the CA vendor's IPR.

Open Marketing of STB's and idTV's

Viewers should benefit from being able to be exposed to a choice of Set Top Boxes (STB's) or Integrated Digital Television sets (idTV's) produced by a range of manufacturers competing in an open market. This has the societal benefit of offering choice to meet individual requirements while at the same time offering market efficiencies.

Such an open market ideally requires that the complete digital broadcasting system, excluding the CA system, be fully described in open standards that are published by appropriate organisations.

Entry & Operating Costs

The cost of setting up and operating a 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 small.

The CA system should not impose a constraint on the ultimate number of end-users that can be addressed. The costs of upgrades to the CA system and of recovering from security breaches should be minimised by selecting a reliable and secure CA system.

4.3 Functional Requirements

Payment Schemes

The CA system should support a wide range of charging and payment schemes such as:

- Subscription: Pre-payment for a period of viewing
- Pay Per View (PPV): Payment for a programme or group of programmes
- Impulse Pay Per View (IPPV): Payment for a programme or group of programmes without advance notice

PPV and IPPV often require the provision of a return path from the viewer to the CA system operator: in many systems this is implemented by means of a telephone connection and a modem built into the STB. The return path can also be used to record viewing history.

The acceptability and rules of operation of such a telephone return-path system require careful study. In particular, a system should exist for those viewers who do not have a telephone connection. One possible method could be to purchase credits in advance and store them as viewing tokens on a smart card or CA module. The card or module would be re-authorised at a trusted dealer, when information on past viewing could be transferred to the system operator. Provided that security was not compromised, it could also be possible to have the smart card or module credited over-the-air with tokens that 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 hours viewed.

Sharing of the System

In order to promote the development of a fair and open market for CA broadcasting, it is worthwhile considering if the following components of CA systems could be shared:

- **Set Top Boxes (STB's)**

This item is addressed in a related white paper on the inter-operability of CA systems.

- **Delivery System**

It is cost effective for any one delivery medium i.e. the cable network to be shared between different and perhaps rival broadcasters. Equally important, is that any scrambled transport stream should be capable of being decoded by any type of STB.

- **CA Systems**

a) Subscriber Management System (SMS)

The SMS is primarily responsible for issuing accounts and receiving payments from viewers. It does not need to, nor should it be specific to a particular CA system. The SMS necessarily holds commercially sensitive information such as the subscriber database. Sharing of the SMS between rival broadcasters is possible if it is operated by a trusted third party and only

if “firewalls” are provided, so that any one service provider can access information only about the subscribers to his own services.

b) Subscriber Authorisation System (SAS)

The SAS is primarily responsible for generating the over-the-air entitlement messages and for validating the security devices in the CA system (smart cards or CA modules). The SAS needs a unique serial number for each smart card but does not need access to commercially sensitive information. In practice however, the SAS is normally tightly integrated into vendors’ CA system implementations and sharing of this resource is normally not possible.

4.4 Operational Requirements

The following features offer a listing of the minimum operational requirements of a CA system:

Enable/disable Smart Card

Individual smart cards, as well as groups of smart cards, need to be capable of being enabled or disabled over-the-air.

Enable/disable Programme Service

Individual smart cards, as well as groups of smart cards, need to be capable of being enabled or disabled over-the–air, to descramble any one particular programme service.

Send Message to STB

When this command is activated, a text message is sent to individual STB’s for display on the screen of the TV set it is connected to. Alternatively, the over-the-air message may comprise a display command and address of a message that is pre-stored in the STB i.e. to warn the subscriber of an expiring subscription or of an account in arrears.

Show Smart Card

The serial number of a smart card is displayed on the screen of the TV set attached to the STB and the respective smart card by invoking this feature of the CA system. This is not the specially encrypted card’s identity number, but an unprotected identity number used for administrative purposes. This feature is useful in maintenance and tracing piracy.

Regional Black-outs

The CA system should provide for the ability to limit reception within certain specified areas. This is a useful feature to prevent local reception of a locally staged event that is dependent on crowd attendance e.g. sports events.

Parental Control

The CA system should provide the ability to restrict programme content to minors by means of a parent-initiated password-controlled system.

Code Downloads

The CA system should support code downloads, the process of conveying software over-the-air, to STB's.