Digital Video Broadcasting Conditional Access Architecture

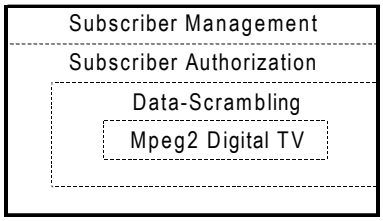
Introduction

Digital Video Broadcasting (DVB) is a standard defining a one-to-many unidirectional data network for sending digital TV programs over satellite, cable, and other topologies. The standard enables the broadcasting industry to offer hundreds of pay-TV channels to consumers. The expanded capacities make the broadcast signals more valuable and attractive to signal thefts [1]. To protect a DVB data-network, the DVB standard integrates into its broadcasting infrastructure an access control mechanism, commonly known as *Conditional Access*, or CA for short [3].

This report is an overview of the DVB-CA architecture. The approach is to provide a full picture of a typical DVB-CA deployment in operation. First, each of the major components is individually described. Then, an operational walk-through is given to show how the different components work together. Throughout the report, the architecture's enabling technologies are mentioned. However, the technical details are not elaborated but instead deferred to references.

Functional Partitions

The DVB-CA architecture manages end-users' access to protected contents with three elements: *data scrambling*, a *subscriber authorization system* (SAS), and a *subscriber management system* (SMS) [5]. Together, they form three layers around the protected contents:



Data scrambling encrypts the digital-TV contents at the center. The subscriber authorization system controls the data-scrambling element by handling the secured distribution of descrambling keys to authorized subscribers. Knowing which subscribers entitle to what contents, the subscriber management system delivers access permissions to the SAS for enforcement.

The protection scope of the DVB-CA architecture ends at the boundary where protected contents are legitimately descrambled. Thus, DVB-CA offers no protection when a legitimate subscriber wires up a receiver to tap out the descrambled contents.

Data-Scrambling

The data-scrambling element is the encryption of TV contents. To avoid confusion, the DVB-CA specification uses the terms *scrambling* and *descrambling* to mean the encrypting and decrypting of TV contents, differentiating other uses of cryptography in the broader DVB infrastructure [4] [7]. The broadcast center does the scrambling, and receivers perform the descrambling.

Subscriber Authorization System

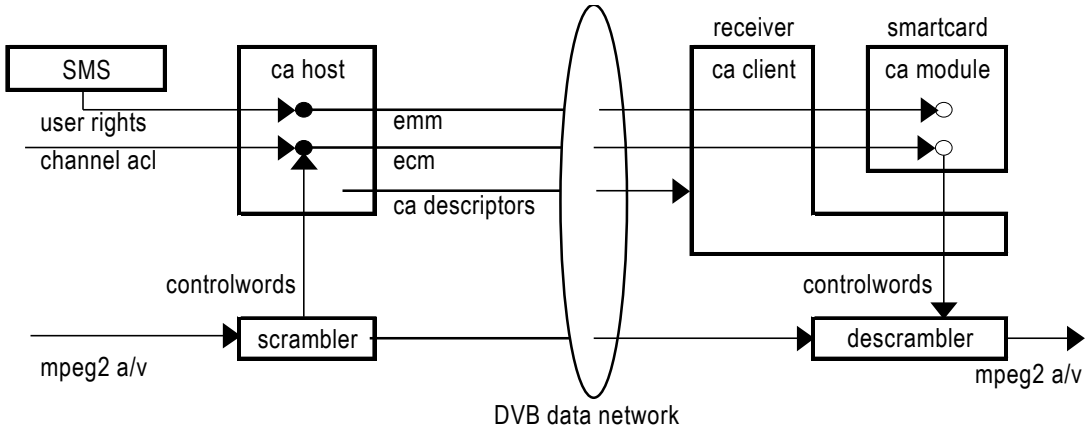
The SAS element implements the access-control protocol. It enforces end-users' access rights by allowing only authorized subscribers to descramble the contents [5]. SAS uses cryptography extensively, and the system is designed to be renewable inexpensively as a strategy to contain damage from being compromised.

Subscriber Management System

The SMS element grants access rights. Operating from the business operation center, the SMS maintains a database of subscribers. For each subscriber, the SMS database records subscription level, payment standing, and a unique ID inside the subscriber's smart card. The SMS uses the information to decide which TV channels a subscriber is entitled to view, and the access permissions are given to the subscriber authorization system for enforcement [6].

System Architecture

The next picture depicts the major components of the DVB-CA architecture and their relations [9]:



The scrambler and descrambler implement the data-scrambling element, and c*ontrol words* are the cipher keys. *CA-Host*, *CA-Client*, and *CA-Module* are the three distributed components of the SAS element, and they use *CA descriptors* and *CA messages* (*EMM* and *ECM*) for communication.

Scrambler and Descrambler

The data-scrambling cipher is called DVB Common Scrambling Algorithm (DVB-CSA) [4]. The algorithm is a combination of 64-bit block cipher followed by a stream cipher, with a key-size of 64 bits [7]. However, the detail is kept secret and disclosed to equipment manufacturers under non-disclosure agreement. For performance and obscurity, the algorithm is implemented in hardware.

At the broadcast center, the scrambler generates control words to scramble the contents, and it passes the control words to the CA-Host for secured distribution to descramblers via ECM CA messages [3]. Control words change about every ten seconds, and the scrambler synchronizes the descrambler to key switching using a specific bit in data-packet headers [4]. As a defense strategy, different TV channels are scrambled with different stream of control words.

CA Messages

CA messages are encrypted command-and-control communications from CA-Host to CA-Modules. The DVB-CA architecture categorizes CA messages into Entitlement Control Messages (ECM) and Entitlement Management Messages (EMM) [4]. ECMs carry channel-specific access-control list and control words. EMMs deliver subscriber-specific entitlement parameters [8]. As a strategy of defense in depth, a secret cipher different from data scrambling is used, and the details on the message formats are closely guarded secrets.

CA Descriptor

CA descriptors are data records associating a protected channel to its ECMs [4]. Since different stream of control words are used to scramble different channels, there is no need to keep the relations secret. Thus, the CA descriptors are sent in clear via the electronic channel guide, which is transmitted continuously in the broadcast traffic.

CA-Host

The CA-Host is the control center of the access protection [9]. It is responsible for encrypting all CA messages to CA-Modules and securely distributing CA messages' cipher keys to CA-Modules.

CA-Client

A CA-Client is the access-control coordinator at a receiver [9]. It passes CA messages from the CA-Host to its CA-Module. It delivers the control words from the CA-Module to the descrambler. When the viewer selects a channel, the CA-Client uses the channel's CA descriptor to filter the associated ECMs and passes them to the CA-Module. If the channel is a pay-per-view, the CA-Client also walks the viewer through GUI dialogs to confirm purchases.

CA-Module

A CA-Module (CAM) is the access-control guard at a receiver [9]. Each CA-Module has a unique CAM-ID for identifying the subscriber [2]. The CA-Module authenticates and decrypts EMMs to establish a subscriber's entitlement parameters, which are stored in the CAM's non-volatile and secured memory and never leave the CAM. The CA-Module also authenticates and decrypts ECMs to receive a channel's control words and access parameters from the CA-Host. If the access parameter in an ECM is consistent with the entitlement parameters stored in the CA-Module, the CA-Module returns the control word to the CA-Client for setting up the descrambler.

Since it is important for CA-Modules to be temper-resistant and easily replaced when damaged or compromised, they are often implemented as smart cards [2].

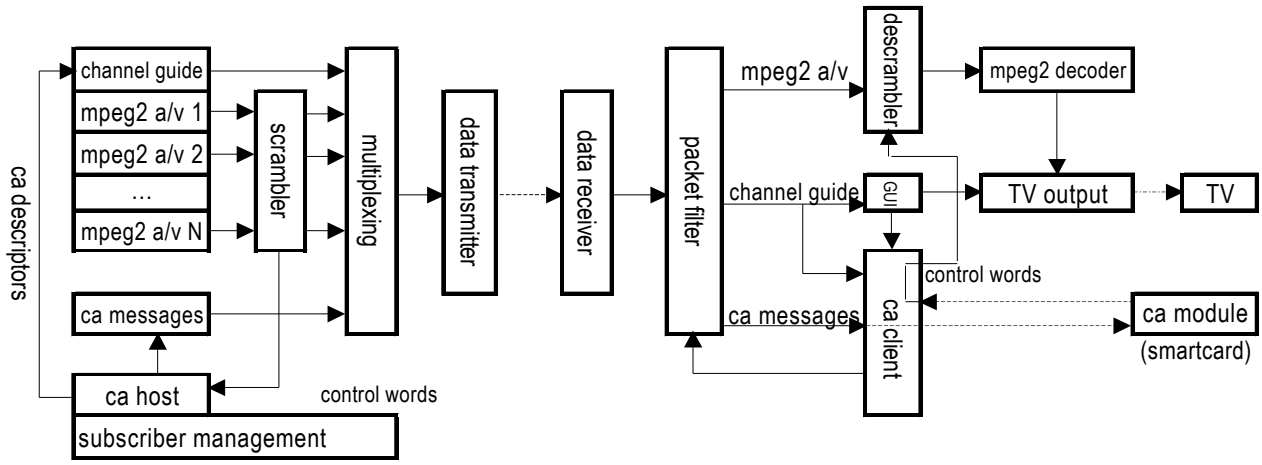
Subscriber Management System

The SMS is the business manager determining each subscriber's rights of channel access [5]. It uses CAM-IDs to link subscribers to the subscriber authorization system. As a subscriber's

subscription level and payment standing change, the SMS modifies the access rights by instructing the CA-Host to send new EMMs to the CA-Module having the subscriber's CAM-ID [9].

Network Integration

The next picture shows where the components of the DVB-CA architecture are integrated into a DVB data network:



To illustrate the interaction between the components in the DVB-CA architecture, a walk-through of the operations behind the following access scenario is presented next.

A subscriber is currently entitled to only basic services, without access to premium sports channels. In an evening, the subscriber browses through the on-screen channel guide and decides to watch a boxing event. Tuning to the channel, the subscriber is presented an on-screen message instructing the viewer to call the customer service center to upgrade subscription level. After going through the conversation of service upgrade, the customer representative confirms the subscriber's request to upgrade. Within a few seconds, the on-screen message is replaced by the boxing show.

Behind the scene, the CA-Client receives the channel-tuning request from the GUI. From the channel number of the boxing event, the CA-Client looks up the parameters from the channel-guide to set up the data receiver and packet filter for receiving the show's digital audio and video streams. More importantly, the CA-Client looks up the CA descriptor and extracts parameters to set up the packet filter for receiving ECM packets associated with the channel. When the ECMs arrive, the CA-Client passes them to the CA-Module and waits for response.

When the CA-Module receives an ECM, it authenticates and decrypts the ECM to extract the control word and access parameter of the tuned channel. Comparing the access parameter to the stored entitlement parameter, CA-Module finds that the service belongs to a subscription level higher than that of the subscriber. Thus, the CA-Module returns a status code of "below service level" to the CA-Client. The CA-Module continues to return the same status code for every ECM passed from the CA-Client since the subscriber's entitlement remains unchanged.

Receiving a response status of "below service level", the CA-Client displays a message on the TV screen, asking the subscriber to call the customer service center for service upgrade. The message

remains on screen for as long as the CA-Module returns the same response to all ECMs passed from the CA-Client.

As instructed by the on-screen message, the subscriber calls the customer service center to request service upgrade. After confirming the request and obtaining online credit approval, the customer representative enters the new subscription level to the SMS. Upon receiving the upgrade, the SMS provides the new subscription level and the subscriber's CAM-ID to the CA-Host. The CA-Host encapsulates the new subscription level into an EMM, tags it with the subscriber's CAM-ID, signs and encrypts it, and inserts the EMM into the broadcast traffic.

Back at the receiver site, the CA-Client receives the EMM tagged with the subscriber's CAM-ID and passes it to the CA-Module. After authenticating and decrypting the EMM, the CA-Module stores the new subscription level into its internal secured storage. When a subsequent ECM from the boxing channel comes along, the CA-Module finds that the subscriber is entitled to the channel. Consequently, CA-Module returns the control word.

Receiving a valid control word from the CA-Module, the CA-Client sets up the descrambler, and the digital audio and video data are descrambled, decoded, and shown on the TV set. Seeing the boxing event, the subscriber is happy and ends the conversation with the customer representative.

From this point on, the CA-Client continuously feeds the channel's ECMs to the CA-Module, which returns new control words as they change.

Summary

The DVB conditional access architecture manages end-users' rights to access contents of a DVB digital TV network. The architecture separates functions into subscriber management, subscriber authorization, and data scrambling. The same broadcast network is used for content delivery and access control. To defend against attacks, the architecture relies on secret designs, cryptography, and temper-resistant hardware to achieve its objectives. Furthermore, system components are carefully partitioned for damage management, where critical parts can be inexpensively replaced when security is compromised. The architecture is adopted by many broadcasting networks around the world and serves as a reference model for many other deployments of digital TV broadcasting.

References

[1] M Carter, "Pay TV Piracy: Lessons Learned," in *Digital Rights Management Workshop* (2000), at http://www.eurubits.de/drm/drm_2000/slides/carter.pdf.

[2] Donvito.dk, "Sat-Lexicon," at http://www.donvito.dk/Sat-Lexicon.htm.

[3] P Delogne, "CONCERTATION MEETING No 44," meeting report; at http://media.it.kth.se/SONAH/ANALYSYS/race/pl4/concert/meet_rep/rcm44.htm.

[4] ETSI, "Digital Video Broadcasting (DVB); Support for Use of Scrambling and Conditional Access (CA) within Digital Broadcasting Systems," ETR 289 (1996).

[5] EUTELSAT, "Technical Guide: Annex B - Overview of DVB," at http://www.eutelsat.com/satellites/pdf/tvservices/annex_b_DVB.pdf.

[6] EUTELSAT, "Technical Guide: Annex C - Guide to Further Information," at http://www.eutelsat.com/satellites/pdf/tvservices/annex_c_DVB.pdf.

[7] MG Kuhn, "The New European Digital Video Broadcast (DVB) Standard," at http://www.cl.cam.ac.uk/~mgk25/dvb.txt.

[8] J Ribés, "Glossary of Terms," at http://www.tele.ucl.ac.be/CAS/glossary/main_f_js.html.

[9] BJ Rijinsoever, JP Linnartz, "Interoperable Content Protection for Digital TV," in *IEEE International Conference on Multimedia & Expo* (2000), at http://buffy.eecs.berkeley.edu/~linnartz/articles/opima.pdf.

Digital Video Broadcasting Conditional Access Architecture

A Report Prepared
for

CS265-Section 2, Fall 2002
Prof. Stamp

By
Tong Ho