Simulcrypt: History, Functionality and DVEO Simulcrypt Support

Application Note
(Rev 1.1)
Introduction to Conditional Access

Conditional Access Systems (CAS, or CA systems) are deployed by pay-TV operators to control access to pay-TV services (programming) that require subscriber payment, whether on a periodic basis (referred to as Subscription Pay-TV) or per event (Pay-per-View). The most common use of CA systems is to protect the content during transport from the video head-end to the client device, and to restrict access to pay-TV services to authorized subscribers only, by using authenticated receivers.

CA system designs generally are highly secretive, and hence proprietary, by virtue of managing the crucial pay-TV “secret keys.” These keys form the basis of protecting content from piracy (unauthorized distribution or viewing), and therefore ultimately securing the revenue (actually, the business) of operators and content rights owners. It follows that CA systems are incompatible with each other.

Simulcrypt

The DVB-Simulcrypt specification is a Digital Video Broadcasting (DVB) protocol and standard published by ETSI (European Telecommunications Standards Institute) for use in broadcast television head-ends¹. The standard was introduced by the DVB Project in 1997 and has been adopted by the vast majority of video head-end vendors around the world (the one glaring exception being the U.S. cable industry).

The Simulcrypt standard defines how CA systems should interface to certain head-end components in order to exchange keys and CA-specific messages for the purpose of scrambling the content prior to transmission, and descrambling the content in the receivers such as set-top boxes (STBs). It specifies the system architecture, timing relationships, messaging structures, extended interoperability and control.

The Simulcrypt standard also addresses the requirements for the co-existence of two or more CA systems at a head-end with the objective of sharing a single broadcast environment. This is based on the concept of a shared scrambling and descrambling method while allowing each CA system to perform its proprietary and secret key management through a common protocol of end-to-end CA messaging.

Simulcrypt Adoption beyond DVB

Originally the DVB Common Scrambling Algorithm (DVB-CSA) was used in conjunction with Simulcrypt for DVB satellite, cable and terrestrial pay-TV operations. However, since the introduction of commercial IPTV services more than 10 years ago by telecommunications companies (“telcos”) using their managed networks, Simulcrypt deployments that utilize the Advanced Encryption Standard (AES) algorithm are also common. While adopted by telcos around the world for managed services, Simulcrypt is not used by Over-the-Top (OTT) operators for a variety of reasons that need not be discussed here.

Simulcrypt is independent of scrambling algorithm and network type, but one and the same algorithm must be used when two or more CA systems share a broadcast network.

In short, Simulcrypt enables:

1. Interoperability between multiplexers / scramblers and CA Systems
2. Dual CAS strategies: Use of more than one CAS in the a deployment, with unique STBs per CAS
3. CAS swap strategies: Like Dual CAS, but one CAS is gradually replacing the other, STB by STB

¹ ETSI TS 103 197: Digital Video Broadcasting (DVB) - Head-end implementation of DVB Simulcrypt. www.etsi.org
The components within the system architecture represent functional units. Specifically, the yellow components are provided by the video head-end, while the blue as CAS components. The boundaries between physical units are not required to match the boundaries between functional units. For example, it is possible that the SCS could reside inside the MUX equipment, or the SCS and MUX could be independent pieces of equipment. Not all head-end and CA systems support all the functions.

**Entitlement Control Message**

Contrary to common belief, the Simulcrypt standard does not define or perform encoding, decoding or content scrambling. It is solely a mechanism for providing keys originating from the Control Word Generator (CWG; i.e. scrambling key generator) to the connected CA systems via the Simulcrypt Synchronizer (SCS). CWG is essentially a random number generator providing CWs to the scrambling process as required. A new CW is typically generated every 10 seconds to ensure that the scrambling key is changed with that frequency for each program stream consisting of video, audio and data.
The CW distribution is time sensitive since the STB must be in possession of the next CW before it will be required to descramble the content. The SCS is tasked with ensuring key distribution in a timely manner.

The mux receives an Entitlement Control Message (ECM; containing the CW) from the CAS that it inserts in the MPEG-2 Transport Stream (TS) for transmission to the STB, where it will be used by the CAS client to descramble the program stream. The ECM itself is encrypted by the CAS and cannot be read by the mux. However, the exchange of ECMs between CAS and MUX is standardized by the ECMG interface and therefore a MUX may receive ECMs from several connected CA systems and insert them all in the TS. That is the mechanism by which several CAS can share a broadcast head-end and program streams.

**ECM Protection – The “Key” to CAS Design**

The ECM content (incl. the CW) must obviously be protected extremely well by each CAS – this is part of the *key management* process that each CAS performs. While the scrambling algorithm may be public knowledge, the ECM encryption and consequently the CW protection is, to state the obvious, the “key” to each CAS design. If the ECM protection is broken (“hacked”), keys can be recovered by pirates and provided to others, whether for free or against illicit payment. The many forms if piracy that pay-TV systems may suffer is beyond the scope of this document.

Most CA systems are designed to use an advanced *key hierarchy*, much like a set of Russian dolls where the opening of one leads to the discovery of another doll inside it, and so on.

The ECMG is the most commonly supported Simulcrypt component.

**Entitlement Management Messages**

Also, depending on each pay-TV operator situation, Entitlement Management Messages (EMMs; containing pay-TV "channel lineups" and other CA-specific keys), will be issued by each CAS, which will then be inserted into the MPEG-2 TS by the MUX. The EMMs are received by the STBs and the CAS client will use keys already in its possession to decrypt the EMM, which in turn will inform the STB which “channels” it will be allowed to descramble. Hence EMMs are associated with “channel lineups.”

In-band transmission of EMMs (i.e. in the MPEG-2 TS) is a requirement in one-way broadcast systems. The distribution has the inherent disadvantage that it will occupy bandwidth, and for large pay-TV systems that bandwidth will be substantial and may impact how much programming can be carried.

However, IPTV CA systems – when correctly designed – do not need to use in-band EMMs thus saving bandwidth. Instead, modern IPTV systems provide messages similar to EMMs out-of-band. Using the IP return channel, receivers will request the entitlement information from the video head-end, and after certain verifications have been performed, the requested information will be provided to the client.

**Set-top Box Clients**

In the STB, an embedded CA client reverses the scrambling process in order to present the content in the clear for output to a TV or other authorized receiving device (possibly the path between the STB and the receiver is protected by HDMI, especially for HD content). To do that, the client uses a key found in the EMM to unlock the ECM that contains the CW, which it then passes to the descrambler. This is an example of the key hierarchy mentioned earlier, where one key is used to unlock a message to recover another key and so on. Key hierarchies typically consist of multiple levels and are highly secret per CAS.
The CA client may reside in a so-called smart card, which was traditionally used in one-way broadcast systems without a return channel from the STB back to the video head-end and CAS. Smart card technology, which very profitable for the CAS vendors, is an operator headache in that the cards need to be replaced typically every 3 years to keep abreast of hackers. It adds both the recurring cost of card replacement and the associated logistics to distribute them, and to ensure subscribers start using them by a certain date lest their TVs go black.

In IPTV systems, a software based client has generally been the rule although some “legacy” (original DVB) CAS vendors also promoted smart cards early on, unsuccessfullly it should be added, until they realized the benefits of an IP two-way infrastructure that obviously lessens the need to store a lot of “secrets” in the STB — they can be fetched on-demand from the head-end when required. Software based clients more recently make use of embedded security feature in modern STB System-on-a-Chip (SOC) from major vendors such as Broadcom, Mstar, Ali, etc.

DVEO Simulcrypt Binary and Support for Third-party CAS

DVEO provides the MUX ECMG component and, in addition, includes embedded AES-128 encryption in its family of encoders/transcoders and streamers, and media servers. This includes the MultiStreamer, Gearbox, Brutus I-VI and Atlas Media Server.

DVEO has tested the ECMG functionality and confirmed its compatibility with the Verimatrix® Video Content Authority System (VCAS™), using the AES-128 encryption algorithm for managed IPTV networks (which is also used frequently for Hospitality, Campus and MDU systems).

Due to the virtue of this long established interface standard, DVEO will also be compatible with other major CA systems when using the AES-128 encryption algorithm. Some interface testing would be required, but based on experience of DVEO staff that have worked for several CAS vendors, such testing is usually confined to minor tweaking of ECMG parameters rather than troubleshooting and bug fixing.

This document has described Simulcrypt and associated DVEO support in general (non-NDA) terms. Another document, available under NDA, describes the DVEO Simulcrypt Binary that DVEO publishes and licenses for use exclusively on DVEO equipment. The DVEO software, which implements the Simulcrypt functionality, consists of a single binary. The user controls the actions of the binary solely via options specified in a configuration file, which must reside on the machine on which the binary runs.

For complete details, please refer to the document DVEO Simulcrypt Binary - Application Note.

Contact Us

For more information call DVEO at +1 858 613-1818 or visit www.dveo.com