

[News](#) > [Miscellaneous](#)

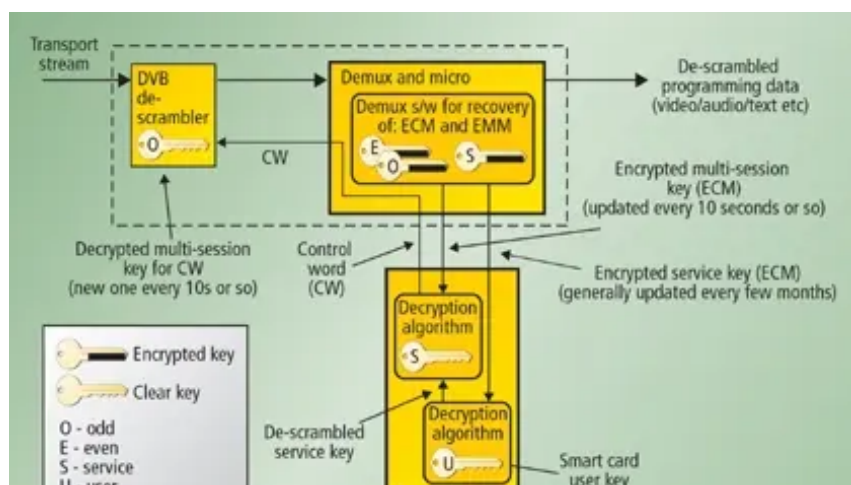
Advertisement

Conditional access

By [MARK MASSEL](#) published October 1, 2001



When you purchase through links on our site, we may earn an affiliate commission. [Here's how it works.](#)



Conditional access (CA) is a service that allows broadcasters to restrict certain programming products to certain viewers. The CA does this by encrypting the broadcaster's programs. Consequently, the programs must be decrypted at the receiving end before they can be decoded for viewing.

CA offers capabilities such as pay-per-view (PPV), interactive features such as video-on-demand (VOD) and games, the ability to restrict access to certain material (adult movies, for example) and the ability to direct messages to specific set-top boxes (perhaps based on geographic region).

Digital broadcast data

Maxell, Ltd.

Ex. 2032

Page 1 of 7_{1/7}

To understand how CA is used, we first need to look at the data it encrypts. Each individual program that a broadcaster provides is composed of many elements, such as video, audio and text. In digital television, these elements are converted into digital form using the MPEG-2 codec. The MPEG-2 data associated with each program are broken up into many packets, and the sum total of these packets for each program is called the program elementary stream (PES). The PES for each program is then multiplexed together with those of other programs. This stream of multiplexed programs is then broken up into 188-byte packets for transmission, at which point it is called the digital video broadcast (DVB) MPEG-2 transport stream (TS). The CA service can scramble the programming data either at the PES level or the TS level. (For digital terrestrial TV, however, the ATSC specifies that scrambling must take place at the TS level.)

The set-top box

At the receiving end, it is the job of the set-top box (STB) to descramble the CA encryption and decode the MPEG-2 data for viewing. Figure 1 is a block diagram of a typical set-top box. The main areas of the STB that are involved with conditional access are shown in yellow. The block labeled CA might be a dedicated, embedded CA module, or it might be one of the standard descramblers.

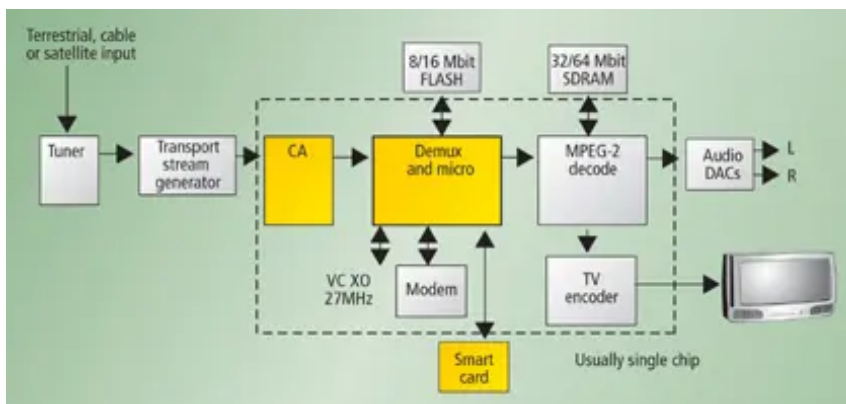


Figure 1. In this block diagram of a typical set-top box, the main areas of the STB that are involved with conditional access are shown in yellow.

Get the TV Tech Newsletter

The professional video industry's #1 source for news, trends and product and tech information. Sign up below.

SIGN ME UP

- ☐ Contact me with news and offers from other Future brands
- ☐ Receive email from us on behalf of our trusted partners or sponsors

By submitting your information you agree to the [Terms & Conditions](#) and [Privacy Policy](#) and are aged 16 or over.

Advertisement

MOST READ

- 1 **Telos Alliance To Feature Next Generation AERO DTV Audio Processors At IBC Show**
- 2 **Disney Streaming Operations Produce First Profits, Announce New Price Hikes**
- 3 **A New Take on Reflectors: Cine Reflect Lighting Systems**
- 4 **Finding The 'Boun-dairies' For AI In Media**
- 5 **Roku Launches Sports FAST Channel**

Maxell, Ltd.

Ex. 2032

Page 2 of 7 _{2/7}

The tuner portion of the STB receives the incoming signal, demodulates it and sends the resulting data to the transport stream generator. This part of the STB reconstitutes the transport stream, which contains many packets of information. Each packet has associated with it (in its header) a program identifier (PID). All packets with PID value hex 1 have not been encrypted and are used by the demux processor to construct the conditional access table (CAT). This table identifies all the PID values of the transport packets containing the entitlement management messages (EMMs). The demux processor also constructs the program map table (PMT) from non-encrypted packets and gives the PID values of all the transport streams associated with a particular program. Private data associated with the program can also be included in this table — for example, the PID value of the packet containing the entitlement control message (ECM). The data contained in these two messages (the EMM and the ECM) are vital in descrambling the encrypted programming material.

Figure 2 shows a DVB descrambling system. However, it should be noted that the standards don't specify the smart-card electronics or algorithms. Therefore, the system described here is a typical example. The EMM acquired by the demux processor is related to the authorization of services. It allows a particular set-top box, or a particular geographic region, to access services. It contains the encrypted service key. Typically, this key is changed every few months to discourage hackers. The encrypted multi-session key, carried by the ECM, is related to particular programming material. This key, once decrypted, actually becomes the control word that is fed into the DVB descrambler, allowing the transport stream to be descrambled so that the viewer can see a particular program or view the programming material for a particular session. As Figure 2 shows, the service key (EMM) is sent to the smart card, where it is decrypted with the help of the user key held inside the smart card. The descrambled service key is then used as the key to descramble the session key (ECM). This descrambling yields the control word (CW). It is this CW that is the key to the DVB transport-stream descrambler.

Figure 2. This block diagram shows a DVB descrambling system.

Middleware

With features such as video-on-demand (VOD) and games, the operating systems or middleware selected are important to the overall functionality of the system. The two main middleware programs being used today are OpenTV (originally developed by Sun Microsystems and Thomson MultiMedia) and Media Highways.

The future-proof promise

With the incorporation of the middleware, the overall solution came with the promise of being future-proof. This means that as more features become available on the STB silicon, the STB manufacturer need not change his software. New middleware software versions are generally needed to take advantage of the new features, but these operating systems or middleware are interpreted script languages. Alternative solutions, available from smaller, independent software houses, offer cheaper, more-efficient options.

Advertisement



It's Time to Renew

SPONSORED BY AMERICAN BAR ASSOCIATION

[Learn More](#)

Mark Massel works for STMicroelectronics in technical marketing and is author of “Digital television, DVB-T COFDM and ATSC 8-VSB,” available either at www.digitalTVbooks.com or from Amazon.com.

MARK MASSEL

LATEST



FCC Adopts New Alert Code for Missing and Endangered Persons ►



Wheatstone to Showcase Blade 4 at IBC 2024 ►



Disney Streaming Operations Produce First Profits, Announce New Price Hikes ►

SEE MORE LATEST ►

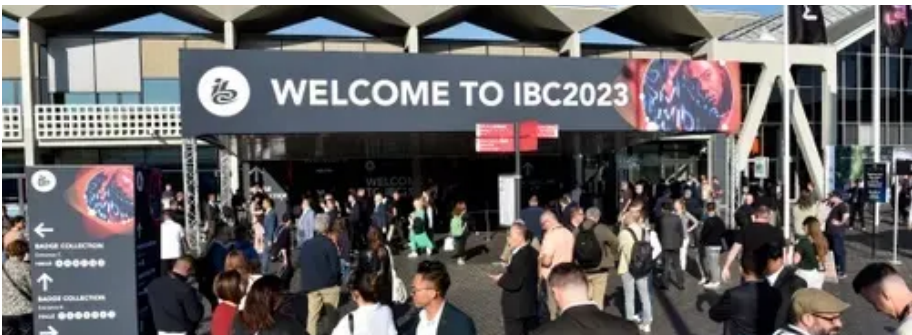
CATEGORIES

MISCELLANEOUS

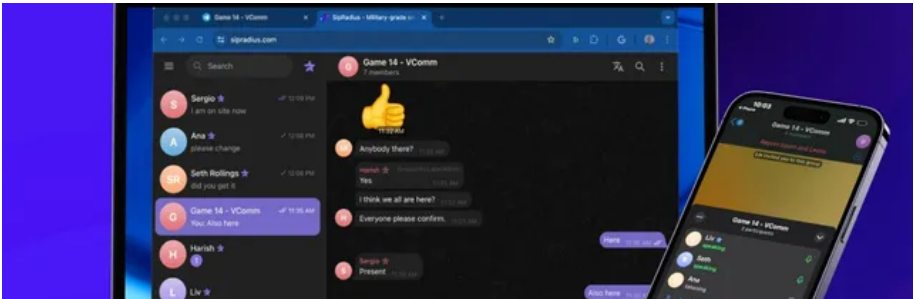
MOST POPULAR



M&E’s Embrace of AI Dampens Potential for Damage Mitigation



2024 IBC Show to Focus on AI, Business and Tech Innovation



New Report Offers Insight On How Marketers Can Make Best Use Of CTV



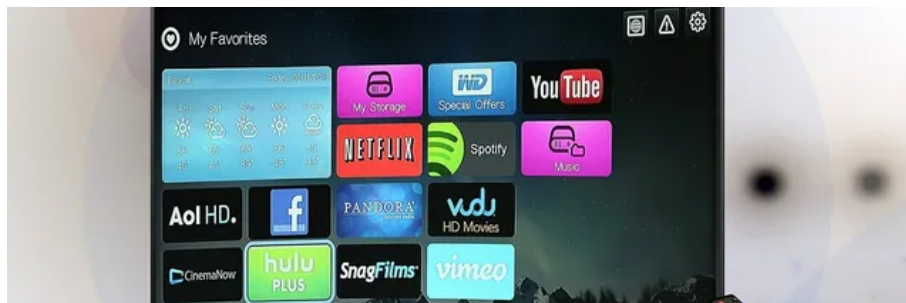
Mediaproxy To Show AI-Powered Captioning, Transcription for LogServer At IBC 2024



Kramer Buys ZeeVee To Expand AVoIP Portfolio



Univision Adds Two Affiliates in Indiana



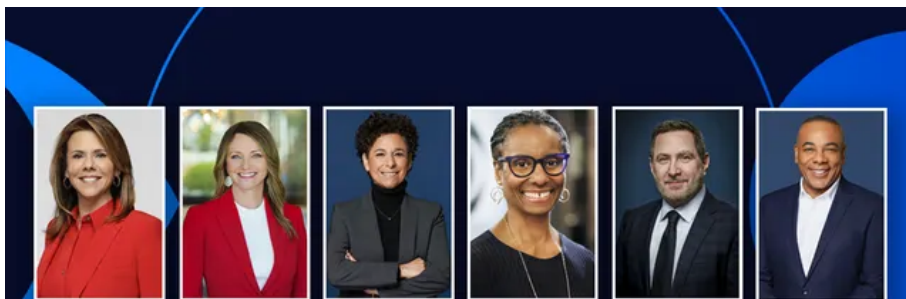
Study: Half of Viewers Begin Watching TV by Checking Smart TV Apps



EVS Invests in TinkerList



Kate Sims, Joe Marchitto Join ASG



Adrienne Roark and Jennifer Mitchell Get Expanded Roles at CBS News and Stations

TV Tech is part of Future US Inc, an international media group and leading digital publisher. [Visit our corporate site.](#)

[Terms and conditions](#)

[Contact Future's experts](#)

[Privacy policy](#)

[Cookies policy](#)

[Accessibility statement](#)

[Careers](#)

[Contact us](#)

[Advertise](#)

Do not sell or share my personal
information

© Future US, Inc. Full 7th Floor, 130 West 42nd Street, New York, NY 10036.