Algorithm: A mathematical function which, for the purposes of a broadcast system and conditional access system, is applied to data to produce a specific result. For example, encoding, compressing and encrypting video, audio and data streams.

Analog Signal: A method of signal transmission in which information is relayed by continuously altering the wave form of the electromagnetic current. The characteristics quantity representing information may at any instant assume any value within a continuous interval.

ATM: Asynchronous transfer mode. A network technology that supports real-time voice and video as well as data. The topology use switches that establish a logical circuit from end to end, which guarantees a quality of service (QoS) for that transmission. Unused bandwidth in ATM's logical circuits can be appropriated whenever available.

ATSC: Advanced Television Systems Committee. Establishes voluntary technical standards for advanced television systems, including digital high definition television (HDTV).

Go to Top

Blackout: Blackout restrictions can block viewers in a certain geographic area, or viewers who fit other criteria defined by the broadcaster, from watching certain programs.

Go to Top

Chaining: Chaining is a method of transferring subscriber entitlements from an old viewing card to a new card during card changeovers.

CMTS: Cable Modem Termination System, a headend component of the cable return path technology used in the DOCSIS standard.
Compression System: Responsible for compressing and multiplexing the video/audio/data bit streams, together with the authorization stream. The multiplexed data stream is then transmitted to the satellite, cable, or digital terrestrial headend.

CAS: Conditional Access Service ID: The identifier for a conditional access event. A single conditional access event can be divided into blocks with different types of access restriction (e.g., the first 5 minutes clear and purchasable; next 10 minutes scrambled and purchasable; the rest of the show scrambled).

Conditional Access: The security technology used to control the access to broadcast information, including video and audio, interactive services, etc. Access is restricted to authorized subscribers through the transmission of encrypted signals and the programmable regulation of their decryption by a system such as viewing cards.

Control Word: The key used in the encryption or decryption of a data stream.

Crypto-period: A crypto-period is a regular time interval during which a control word is valid. A crypto-period is typically only a few seconds long. Also called a Key Period.

Go to Top

Data Services: Data services provided over cable frequently include Internet and e-mail access, and can include delivery of a wide range of non-video information to subscribers.

DAVIC (Digital audio video council): The DVB-RC standard for cable return path, expected to be widely used in markets where DVB standards apply.
Digital Signal: A discretely timed signal in which information is represented by a finite number of defined discrete values that its characteristic quantities may take in time.

DOCSIS (Data over cable service interface specification): A standard for standalone cable modem communications, usually used with Internet or PCs, developed for the U.S. market.

DVB: Digital Video Broadcasting. A European project which has defined transmission standards for digital broadcasting systems using satellite (DVB-S), cable (DVB-C) and terrestrial (DVB-T) media, created by the EP-DVB group and approved by the ITU. Specifies modulation, error correction, etc.

Go to Top

Electronic Countermeasure: A security feature designed by NDS to combat piracy. Support for these security measures has been built-in to the conditional access software and viewing cards.

EPG: Electronic Program Guide: An on-screen guide to programs and services available to subscribers. The electronic program guide is a software application which runs inside the digital set-top box and is controlled by the use of a specially designed remote control. It allows the subscriber to view program schedule information, store favorite channels, 'book' programs for later viewing, purchase current and future pay-per-view events, read messages from the subscriber management system, and adjust set-top box settings.

Entitlement Control Message Generator: System component responsible for generating entitlement control messages and control words from conditional access information on the current programs; updating the entitlement control message and control word every crypto-period; and delivering them to the multiplexer.

Entitlement Control Message: A packet which contains information the viewing card needs to determine the control word (01 seed) which decrypts the picture.

ECM: Entitlement Management Message Generator: The component of the conditional access headend that delivers entitlements to the multiplexers. Acting on commands from the subscriber managemem system, it creates entitlement management messages for broadcast to the viewing cards or for relaying to cable operators. It then forwards the entitlement management messages to the multiplexers, The Entitlement Management Message Generator includes the subscriber database, which is a subset of the information held in to subscriber management system database.

EMM: Entitlement Management Message: A packet containing private conditional access information which specifies the authorization levels or the services of specific decoders. Entitlement management messages deliver viewing authorizations to the subscriber's card.

Go to Top

Fiat: Shamir Authentication: A zero-knowledge identification and signature scheme developed in 1986 by Amos Fiat and Adi Shamir. The request for a Fiat-Shamir zero-knowledge identification ensures that viewers use only valid viewing cards. When a request is broadcast, every smart card which is inserted in a set-top box is checked. If a card does not pass the check, that subscriber cannot view.

Go to Top

ICAM: Integrated Conditional Access Module. An optional chip included in the set-top box responsible for descrambling and packet filtering and reception. It also contains the physical interface to the subscriber's viewing card.

In-band channels: In-band channels or frequencies are those which contain content broadcast to subscribers. This can be audio, video, data, or other content.

INA: Interactive Network Adapter, a headend component of the cable return path technology used in the DAVIC standard.

IP: Internet Protocol.

IP Telephony: The ability to provide local telephone services via the cable infrastructure.

Go to Top

Macrovision: Copy protection system that allows consumers to view, but not record, programs that are distributed via digital STBs. The system adds a copy protection waveform to the video signal that is transparent on original program viewing, but causes copies made on VCRs to be degraded to the extent that they no longer have entertainment value.

Middleware: The layer of software that supports the user interface and interactive applications in the set-top box, and isolates the application from the particular hardware of a set-top box platform.

MPEG: Moving Pictures Experts Group. The name of the ISO/IEC working group which sets up the international standards for digital television source coding.
MPEG-2: Industry standard for video and audio source coding using compression and multiplexing techniques to minimize video signal bit-rate in preparation for broadcasting. Supersedes the MPEG-1 standard. The standard is split into layers and profiles defining bit-rates and picture resolutions.

MSO: Multiple Service Operator, a cable operator with several headends, perhaps across many geographic regions.

Go to Top

OOB Channels: Out-of-band channels are channels which are not used for broadcasting content to subscribers. The ability to broadcast entitlement information in OOB channels ensures that subscriber cards receive this information even if the set-top box is tuned to an analog signal.

OpenCable: A CableLabs® project aimed at obtaining a new generation of interoperable set-top boxes for the U.S. market, to enable a new range of interactive services to be provided to cable subscribers.

OpenCAS: A committee which is defining conditional access standards for the U.S. market. Its work has been submitted for review and approval to SCTE/DVS (Society of Cable Television Engineers/Digital Video Subcommittee).

Go to Top

Password: A four-digit number used to control access to programming and to set purchase limits.

POD Module: Point-of-deployment modules are removable conditional access devices which would make it possible for one set-top box to be used in many cable markets. All hardware and software required for the conditional access system is included inside this removable module rather than built into the set-top box.

PSIP: Program and System Information Protocol. ATSC term for the metadata used to describe events. Similar to DVB SI.

Go to Top

QAM: Quadrature Amplitude Modulation. A method of modulating digital signals which uses combined techniques of phase modulation and amplitude modulation. It is particularly suited to cable networks.

Go to Top

Report Back: An automatic function which reports IPPV purchases to the EMM Generator, via a telephone or cable modem connection.

Go to Top

Security Server: A computer that attaches a digital signature to each conditional access packet before that packet can be broadcast,
and provides scrambling control words. The signature is used to verify the validity of the packet.

Session-based Encryption: The ability to encrypt video-on-demand content per viewing session rather than per stream or in real-time. This enables cable operators to protect content, providing decryption rights to only a single viewer. The viewer can pause and resume viewing, if the video-on-demand server supports such functionality.

STB-Set-top Box: The receiver unit, with an internal decoder, which sits on top of the television set and is connected to the television set. It receives and demultiplexes the incoming satellite signal and decrypts it when provided a control word by the viewing card.

SI: Service Information (DVB term). Data used by the electronic program guide to display information about programs. Typically includes time of broadcast, title, etc. The ATSC is equivalent is PSIP (Program and System Information Protocol).

Simulcrypt: The co-existence of multiple conditional access systems on a single transmission service. In other words, using Simulcrypt, a cable operator can provide the same programming to two or more subscriber populations.
Smart Card : See Viewing Card.

SONET: Synchronous Optical NETwork. A fiber-optic transmission system for high-speed digital traffic. Employed by telephone companies and common carriers, SONET speeds range from 51 megabits to multiple gigabits per second. SONET is an intelligent system that provides advanced network management and a standard optical interface.

Subscriber Management System: A system which handles the maintenance, billing, control and general supervision of subscribers to conditional access technology viewing services provided through cable and satellite broadcasting.
Verifier : Conditional access software module embedded in a set-top box which handles the logical interface to the viewing card and passes entitlement control messages, entitlement management messages, and other conditional access and subscriber information to the card.

Go to Top

VOD: Video-on-demand : A method of providing video services to viewers under their control, permitting them to choose what they want to view and when. Video-on-demand often includes the ability to pause viewing and resume, even tuning to other channels before resuming viewing of the video-on-demand event.

Viewing Card: A credit-card sized programmable card. A conditional access security device in the subscriber's home, it receives and records entitlements from the broadcaster headend and checks these against the incoming program information in the entitlement control messages. If the subscriber is authorized by the to view the current program, the card provides the control word to the set-top box. (Also known generally as a smart card or subscriber access card.)

VPN: Virtual Private Network (VPN) : The ability to use the cable infrastructure for telecommuting. The subscriber can access a remote network, at the office, for example, using the cable connection.