

# 2

## Analysis of the World Smart-Card Based Pay TV Conditional Access Systems Market

### OVERVIEW AND DEFINITIONS

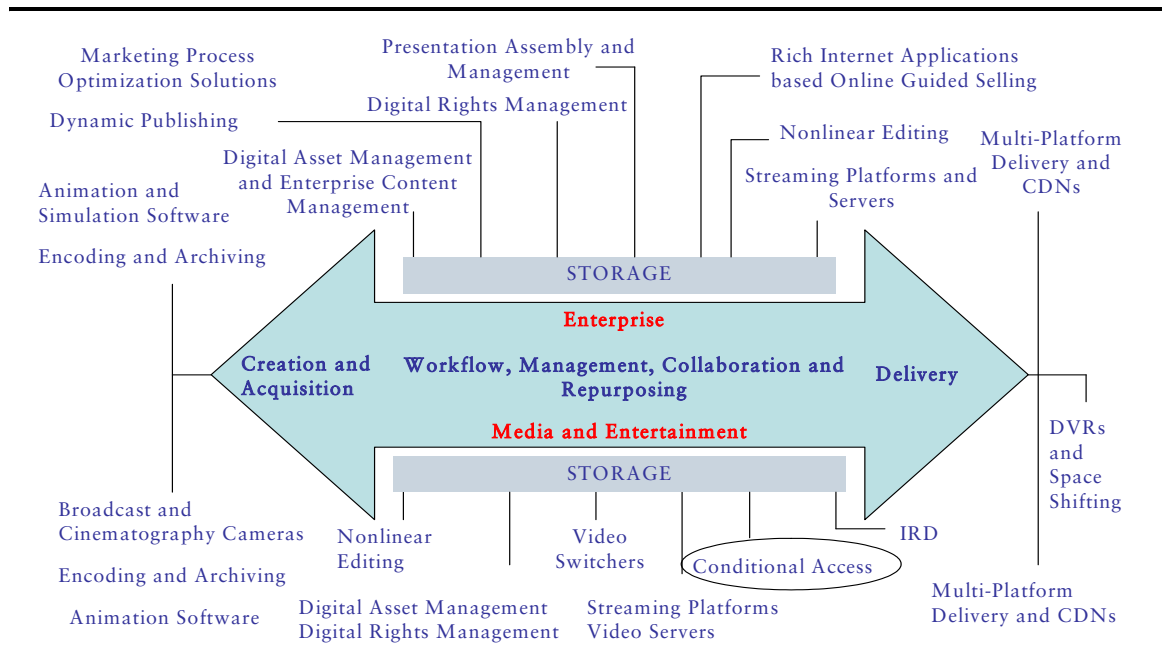
#### An Introduction to the World Smart-Card Based Pay TV Conditional Access System Market

This research service is part of the extensive Frost & Sullivan research subscription on digital media.

Chart 2.1 illustrates the components of the digital media value chain covered by the Frost & Sullivan analyst team.

CHART 2.1

Smart-Card Based Pay TV Conditional Access System Market: Digital Media Value Chain (World), 2008



Source: Frost & Sullivan

This value chain encompasses technologies that span the acquisition of content in a digitized format, through management of that content, to final delivery. Frost & Sullivan analyzes the digital media value chain primarily from an enterprise perspective, where it is largely used as a tool to facilitate marketing and corporate communications, as well as from the perspective of the media and entertainment market. Conditional access systems are at the heart of the pay TV digital content delivery and protection system, managing and controlling the delivery of premium broadcast content through distributors to end users.

This study is one in a series of Frost & Sullivan studies on digital rights management (DRM) and content protection. The forthcoming companion studies concern software based conditional access systems (Number), software DRM solutions, enterprise DRM solutions, and media & entertainment DRM solutions. Card-based conditional access (CA) systems are software and hardware systems used to protect digital content as it is delivered through the broadcasters, the broadcaster hubs, and on to consumer viewing devices.

#### DEFINITION

Frost & Sullivan defines the world smart-card based pay TV conditional access system market as the global card-based conditional access industry, including the vendors that design, manufacture, and sell card-based systems, the partnerships key to the delivery and distribution of the conditional access technologies, and the expanding global reach and impact of the industry. Conditional Access solutions are an integral part of the content management value chain, particularly at the point at which digital video content is delivered from the broadcasters to the consumer. Conditional access systems act as a gateway or filter, regulating and controlling both the access to content the consumer enjoys and the revenue streams the operators and owners command.

This study focuses on vendors that sell complete conditional access solutions, including head-end server software and hardware, smart-cards and software based client systems, and the other services related to fulfilling an operator's content delivery protection system needs. There are, of course, other players in the conditional access value chain, providing value added services, professional, implementation, and consultative services, component and hardware suppliers, and other OEM suppliers and service providers that feed into and add value to the industry. Although these suppliers may be integral to the entire picture, they do not per se either sell or focus on content delivery protections, and thus do not qualify as conditional access providers. When describing the video delivery ecosystem used to deliver television content within this study, the term "broadcaster" is loosely applied to cover over the air, terrestrial, cable, and satellite content delivery operators. IPTV and many modern cable providers actually multi-cast or uni-cast their content, yet in the interest of consistency and brevity, all digital video delivery providers are commonly termed "broadcaster" within this study.

Conditional access systems use encryption and signal scrambling software to protect digital content from unauthorized access, to protect the integrity of broadcast systems, and to ensure that content owners, broadcasters and distributors are able to collect usage fees and adequately monetize their content. This has allowed content owners to more confidently distribute their content through broadcasters, with assurances that it is protected from unauthorized access, replication and redistribution. Managed network operators, the hubs from which linear digital video broadcasting is delivered, also can leverage the security and integrity offered by CA systems to gain access to a greater variety of high quality content and additional channels and programming, and effectively inspire content creators and rights owners to generate additional high value broadcast content. The future of television and linear broadcasting as a whole rests to a large degree on the ability of operators to deliver any content any time to any consumer, with some level of targeted and interactive services, and reliable conditional access systems that ensure protection for the delivery and revenue generation for the content owners.

Frost & Sullivan estimates that there are approximately x.x billion households worldwide in which there are televisions. Approximately xxx million of those households currently subscribe to and pay for digital broadcast services, virtually all of it delivered through the use of set-top-boxes (STBs) and protected with conditional access systems. The remaining majority receive free or paid analog broadcasting content over terrestrial connections, including free over the air analog or digital terrestrial television (DTT) or basic cable connections that provide only basic content and programming, and rarely include conditional access protections.

Conditional access systems are similar in concept to digital rights management (DRM) in that both solutions protect digital content. Conditional access (CA) systems control and protect the point-to-point distribution of linear broadcasted digital content, ensuring the integrity and security of the delivery system and protecting the content from unauthorized access. CA systems are managed and controlled by broadcasters and managed network operators and are applied in the broadcaster to operator link, as well as the operator to consumer link. DRM solutions, on the other hand, are designed to preserve the rights of the content owner through the life of the content, protecting it from unauthorized duplication, reuse, redistribution, or other piracy related activities. DRM solutions are typically controlled by content rights owners and may include specific rules regarding how content is viewed, in what formats it may be rendered, how many times it may be viewed, if and how many times it may be copied, and how and when its protections may expire. CA and DRM solutions are in the same family of services and can and do often work in unison with each other, and each is a key element in the effort to protect digital content.

Consumers have many options these days in how they may receive digital broadcast content. The most common options are cable, broadband/telephone line, satellite, or over the air broadcasting connections. Modern consumers may also choose from among many viewing devices to capture and view content, including televisions, personal computers (PCs), personal media players (PMPs), MP3 players, mobile phones, personal digital assistants (PDAs), and virtually any other network connected device with an ability to display digital video content. In virtually all cases, conditional access systems are available to ensure the delivery and protection of the digital content, and can work across every part of the digitally connected home.

As an alternative content source, computers with built-in television tuners can receive live broadcasts as well, and display it on their screens. For the most part, this Internet TV solution is only able to receive premium content when the consumers download a software conditional access component or use an authorized CableCARD with their computer. This option is increasingly popular in homes with multiple access points.

It is important to distinguish that in regards to viewing video content on a computer however, online video content of the kind commonly found at CNN.com, MLB.com, YouTube.com, iTunes, Hulu and on-demand movie and television sites, such as Netflix.com, Amazon.com, BT Vision and other video-on-demand (VOD) web sites, does not qualify as linear broadcasting and is not protected by a conditional access system.

## Core Protections

Every year, conditional access systems in any form protect billions of dollars of revenue potential associated with digital broadcast content every year. It is difficult to monitor and measure total potential revenue losses due to CA system breaches and hacks, but Frost & Sullivan estimates that \$x billion or more in potential revenues were lost in 2008 due to illegal connectivity, system hacks, and content piracy. Conditional access systems are prime targets for hackers, content piracy and subscription fraud.

Content creators, rights owners, distributors, broadcasters and local operators rely on conditional access systems to protect the integrity of their delivery systems and their ability to effectively monetize and enable fee collection for the use of their content every day around the world. Conditional access vendors may offer additional peripheral solutions with their security systems, but it is their ability to consistently defend against and defeat hackers while maintaining a reliable revenue stream for their customers that is the core of their business, the basis of their reputations, and the reason they continue to grow and succeed.

Conditional access systems work by both scrambling broadcast signals and encrypting authorization codes. It is not uncommon for an operator to encrypt all of its broadcast channels, including its premium channels, movie/VOD channels, and HD channels prior to air. The conditional access system installed at the consumer's receiving device, either a smart card or software-based CA system, manages and authorizes access to the specific channels or content, based on the consumer's subscription and account status.

When, for example, a consumer requests access to a new channel or program, an authorization session or "virtual handshake" is initiated between the consumer's receiving device—the client device with a trusted card or software element—and the managed network operator's CA server system. If the consumer is authorized to access the content, based on the consumer's account status or an agreement on their part to pay for or be billed for the access, a communication is sent through the head-end to initiate an entitlement process.

Specifically, every couple of minutes, a unique entitlement management message (EMM) is sent to the STB or other receiving device. This EMM authorizes the STB/device CA system to decrypt entitlement control messages (ECMs)—a control word or phrase—that's been encrypted at the head-end and sent to the client CA device. The word must be successfully received, decrypted, and acknowledged prior to the system allowing the consumer access to the heretofore encrypted and protected content. This handshake/confirmation process is repeated hundreds of times in an hour and every time the consumer changes channels.

Although all vendors use similar encryption and key management processes, by design, each conditional access system uses different encryption systems and scrambling algorithms (some may use multiple simultaneous algorithms within a single system) that often change generation to generation, and operator to operator, and are diversified across all the different vendor systems. Many larger managed network operators use both different vendors and different generations of CA systems simultaneously within their networks. To alleviate the need to initiate multiple sessions with multiple control words and processes, operators commonly use a DVB standardized "SimulCrypt" system, which allows for a single session key or code word that can be used consistently across all of the CA systems in use.

## Connections and Carriers

Standard conditional access systems are composed of several physical and software based elements, including the head-end system, the receiving device with an installed conditional access receiver, and the software solutions that both manage the communications between the head-end and the device and provide additional relationship management, accounting, or consumer-interactive services.