

Next Generation Pay-TV Content Protection



Evolving Pay-TV Security Threats

All pay-TV operators share the fundamental objective to securely monetize content and specifically to protect content and services from piracy. They have a particular interest in securing their operations from various types of “revenue leakage” threats, such as theft of service, smart card piracy, etc. As pay-TV increasingly moves to digital delivery around the world, operators must prepare to address evolving security threats. The new delivery technologies, which offer opportunities for subscriber and revenue growth, also present new security challenges to the pay-TV world.

While security in analog cable TV systems is primarily focused on preventing theft of service, the threat scenarios are

entirely different and more complex when transitioning to digital TV services. Therefore, as cable operators plan for an analog to digital TV transition, they must address a unique set of complex issues. The goal is to ensure that the security path taken minimizes costs without sacrificing their ability to meet service requirements over the long term. The choice of security technology is fundamental to the overall competitiveness and prosperity of the pay-TV operator.

Digital TV Security Considerations

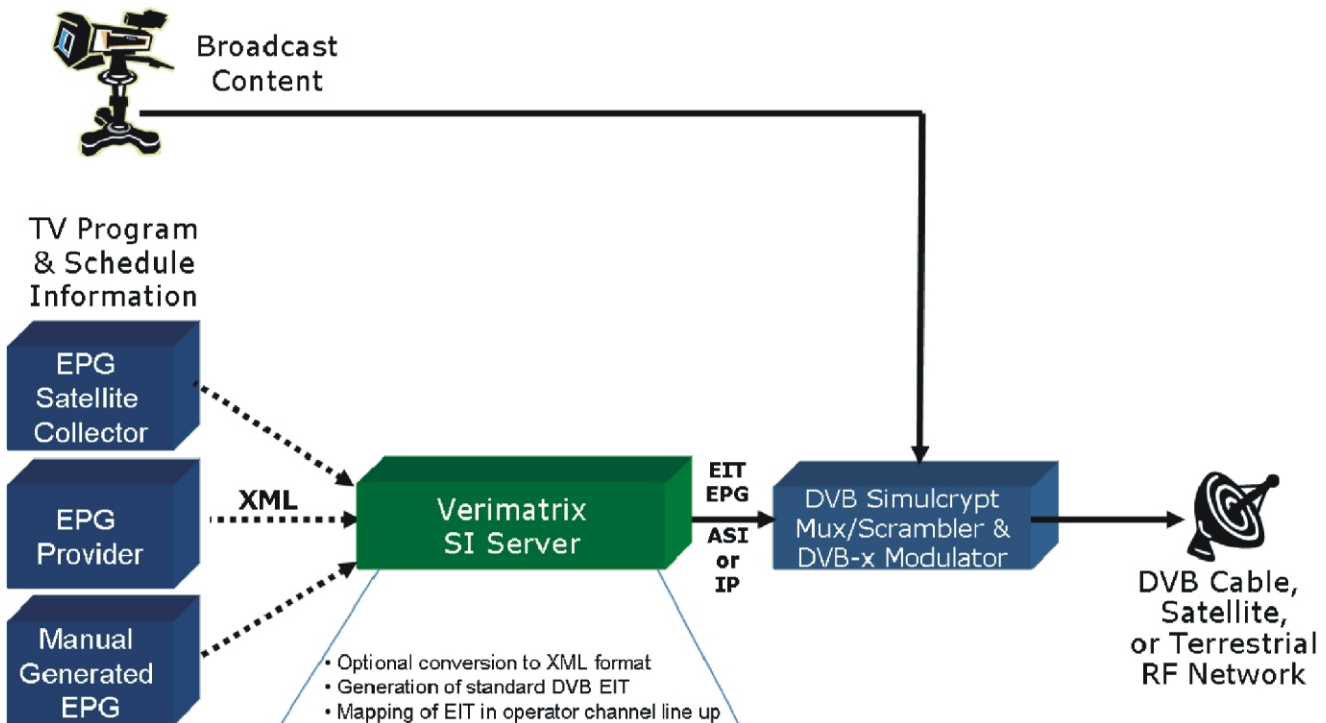
The evaluation of security options brings into play a slew of considerations concerning legacy video formats, the proportion of subscribers affected by the digital TV transition, the ages and types of

any set-top boxes (STBs) already in the field, managing the infrastructure logistics, and the service provider's longer-term business goals.

While cable operators contemplate significant changes in their service profiles, it behooves them to consider in parallel the value brought by digital TV security providers. These potential changes, viewed from a high-level perspective, include:

- Transitioning from analog to digital
- Choosing MPEG-2 or MPEG-4 video formats
- Offering standard definition (SD) services only, or including high definition (HD) from the outset
- Adding hybrid IP-based solutions to broadcast networks.

Pay-TV operators of all types, and at all stages of network development, realize that a



flexible and effective digital TV security architecture can be the essential enabler of innovative business models and improve their competitive positioning. The shape and flexibility of an overall security solution has therefore become a critical strategic decision. This consideration also moves the perspective of the security technology from basic content protection to the broader concept of revenue security.

There are many pay-TV security factors, not least financial, which need to be considered, such as:

- Initial purchase cost (CAPEX)
- Operational cost (OPEX)
- Cost of unresolved security breach (loss of revenue)
- Cost to overcome a security breach (security renewal)
- STB certification cost and lead time
- Choice and availability of STBs (competition among STB vendors)
- Ability to license premium content (trusted CA/DRM vendor).

Content Owners' Concerns

Licensing of content is the cornerstone of a pay-TV business. For the studios and content owners the threat of large-scale piracy, undermining the lifetime revenue potential of their product, is of major concern. Content owners focus on enforcing digital rights through technological and legal processes to ensure that a single distribution channel does not impact potential revenue in other geographic or release windows. Moreover, the commercial stakes for HD content are significantly higher than that of SD and now 3D content is added to the mix as well.

Content owners and operators alike expect digital TV security vendors to address the evolving challenges through a set of technologies and tools that encompass complete revenue security, during content creation, storage, delivery, and consumption and beyond.

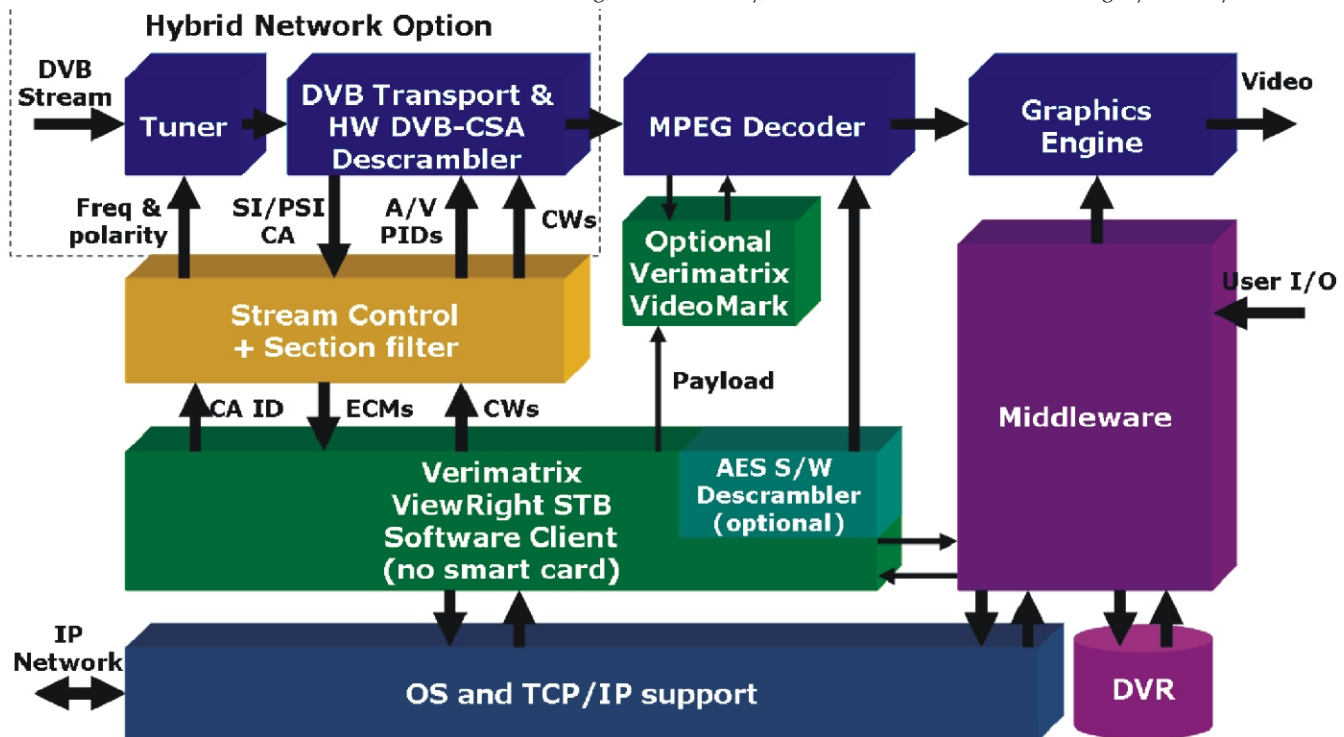
In this respect, the operator considering a digital transition will benefit from choosing a security vendor that is well known among, and trusted by, the content

providers. There is only one criterion that matters: a successful track record of pay-TV operator deployments around the world.

Legacy CA Systems

When digital TV was first introduced in Europe in the mid '90s, all broadcast networks were one-way in nature, i.e. they had no return channel from the STB to the head-end. The technology approach taken, which seemed a good idea at the time, was to protect the "pay-TV secrets," such as subscriber entitlements and decryption keys, in a "smart card" provided to the subscriber together with the STB. Service providers needed a robust security solution that did not depend on a physical connection between the network and set-tops, which was well-suited for smart card-based "conditional access" systems.

Unfortunately, piracy soon emerged and evolved into a sophisticated business, where analysis and reverse engineering of removable smart cards, or cracking their communication with the STB CPU, became common. All legacy CA systems were



hacked, one way or another.

This is the drawback of legacy systems: if the security is compromised, all smart cards have to be revoked and reissued. It has therefore become common practice among legacy vendors and operators to perform a card swap every three years or so.

Evolution of Set-Top Boxes

Jump forward to today and the entire video environment has changed. Cable and satellite service providers still use set-tops of course, but those boxes have far more intelligence and often much better connectivity than those of the past. Cable set-tops now typically have two-way connectivity, and operators are adding broadband capability in order to offer Video-on-Demand and interactive services.

Modern set-tops can do much more than their predecessors. Their processing power (for video decryption and decompression, as well as for displaying electronic program guides and running sophisticated interactive applications) rivals that of personal computers. They can do in software what used to require dedicated hardware, and it is that power that shifts the balance in favor of software-based security for set-tops. The vast majority of modern set-tops are perfectly capable of handling security functions using a combination of software and security features embedded in their CPUs, so the extra hardware cost of smart cards and their associated distribution logistics can be avoided.

Card-less Security

The card-less security of modern set-tops can either consist of very low-cost box with a highly obfuscated, software-based security module, or a sophisticated System-on-a-Chip (SOC) with embedded security features that enable the most robust and impenetrable pay-TV security possible

today. The security module is software-based but resides in a highly secure environment that cannot be penetrated by the tools traditionally used by smart card pirates. One major difference is that while a smart card can be removed from the box and analyzed in great detail, and even cloned, the SOC prevents such analysis by being embedded inside the box.

The secure SOC solution also solves the dreaded “control word sharing” piracy problem. In some legacy systems, the Control Word (content scrambling key) is passed in the clear between the smart card and the set-top descrambler. Pirates have found ways to intercept the key and share it with other (non-paying) subscribers over the Internet, and thus one hacked box can be used to help many others steal services. In the secure SOC environment, the key is never exposed in the clear outside the secure area, and hence the control word sharing threat is overcome.

Advantages of Software-based Security

As discussed, the cost and time required to replace a hardware-based security system can be substantial.

Renewability of security subsystems is thus a distinct advantage in a landscape of fast changing threats and business opportunities, making software-based security an attractive option. Content security is an arms race against pirates and fraudsters, so the security must be renewable. Software-based security, in combination with state-of-the-art secure SOC technology, offers flexible renewability options allowing operators to stay a step ahead.

Software-based security combines lower CAPEX and OPEX costs into a more favorable Total Cost of Ownership equation than hardware-based systems. Threats can be countered by over-the-air updates,

avoiding the dreaded “card swaps.”

Making the Right Digital TV Security Choice

Even if an analog cable operator today is merely considering the initial transition to digital, it is imperative to choose a security architecture that supports both the immediate requirements while also laying a sound foundation for the future—a future that may include delivery to PCs and Macs, games consoles, smart phones, web tablets and other mobile devices.

Service providers ultimately want to implement a security system that can serve as a single-source revenue security platform for services that are designed to reach multiple screens across multiple networks. They want a solution that can draw on the best of encryption, conditional access, digital rights management and video watermarking techniques to dynamically apply whatever types of security are appropriate to each service, no matter which delivery network is used, and no matter what type of subscriber device is used to access it.

Fortunately, software-based security systems now provide the flexibility to escape traditional CA system restrictions without compromising security or adding complications to the consumer's experience. In fact, software-based systems can provide new levels of security essential to new multi-device service models that would be impossible to achieve with legacy systems.

A unified, software-based pay-TV security system is a vital ingredient for operators looking to expand their service profiles, to meet contractual and service protection obligations. Most importantly though, a unified software-based security system, offering multi-layered protection, allows new business models to emerge and flourish.

