intertrust®

White Paper

ExpressPlay

Smart TV support for converged security–Upping the game for DVB broadcasters

Part 2

Why fully converged security is critical for smart TV OEMs and broadcasters

Contents

Introduction

Hybrid service strategies centered on the smart TV in DVB broadcaster markets provide OEMs and service providers alike major opportunities to cut costs and drive subscriber acquisitions.

This is possible by supporting converged security on core hardware, that enables a fully converged solution for pay TV subscribers to seamlessly access OTT streaming and over-the-air (OTA) broadcast TV content on the same device.

As described in Part 1, DVB broadcasters are pursuing more aggressive hybrid service strategies by exploiting the emergence of the smart TV as the dominant viewing platform in their markets. In Part 2 the focus swings to broadcasters' need for content protection that covers all legacy and OTT bases free of old approaches that required use of conditional access modules (CAMs) and set-top-boxes (STBs).

The advanced processing capabilities of the systems-on-chips (SoCs) powering today's smart TVs make it possible to do away with the costs and inconveniences imposed by previous approaches to securing legacy TV channels. But only one converged security solution eliminates the burdens imposed by continued reliance on legacy conditional access systems (CAS).

Unlike solutions developed by CAS suppliers, Intertrust's cloud-based ExpressPlay XCA security-as-a-service (SaaS) fully converges security on smart TV SoCs with no need for separate CAS support. It does this by orchestrating utilization of the open-standard Marlin DRM core, now embedded in nearly 500 million devices worldwide, to execute converged broadcasting and OTT streaming content protection.

That, combined with measures enabling manufacturers to self-certify platform compliance, has allowed OEMs and broadcasters to incur the lowest total cost of ownership (TCO) for content protection not only on smart TVs but across all other targeted devices as compared to every other multi-network and multi-screen security solution in the market today. This is why ever more OEMs, now including Vestel, Sony, and Hisense, are implementing ExpressPlay XCA with smart TVs sold in DVB markets.

ExpressPlay XCA eliminates the royalty or other fee structures attending reliance on legacy CAS. Of course, broadcasters offering encrypted legacy TV programming still must rely on the traditional CAS approach with older consumer premises equipment (CPE). By virtue of ExpressPlay XCA's compatibility with the DVB Simulcrypt standard, which enables simultaneous use of two or more CA systems from the same headend, broadcasters who rely on ExpressPlay XCA for protection on smart TVs and other connected devices can continue using their legacy CAS for as long as necessary.

Intertrust's client SDK and porting kit enable the device maker to meet the Enhanced Content Protection (ECP) specifications for UHD and other high-value content set by Hollywood studios' MovieLabs consortium. This includes support for the Compliance and Robustness framework as well as optional support for forensic watermarking when required by license holders.

On the DRM side, the ExpressPlay XCA SaaS works in concert with Intertrust's ExpressPlay multi-DRM cloud service to provide robust protection for OTT content delivered to all connected devices. ExpressPlay DRM, a widely deployed multi-DRM technology, is the only such service that supports all major DRMs, including Adobe Primetime, Apple FairPlay Streaming, Google Widevine and Microsoft PlayReady as well as Marlin. Consequently, broadcasters implementing ExpressPlay XCA are assured of having all the DRM protection they need whenever they transition from legacy TV to direct-to-TV (D2TV) broadcast delivery models.

Smart TV OEMs' ability to provide unified support for broadcast and OTT streaming protection modes represents a triple win benefitting broadcasters and consumers as well as manufacturers. Benefits to OEMs start with the fact that a smart TV supporting ExpressPlay XCA can be sold as a unified direct-to-TV viewing platform that can be used to receive services from any broadcaster that takes advantage of the ExpressPlay cloud service.

This allows smart TV OEMs to sell the devices without having to bind them to specific broadcasters. A major advantage is that TV OEMs can produce large quantities of smart TVs targeting an entire country or geographical region, lowering the manufacturing cost and speeding time to market. For broadcasters, the key advantage is that they can advise consumers to purchase smart TVs in retail, without becoming involved in the equipment acquisition and distribution process. Multiple broadcasters in the same country or region can address a common installed base of consumer-owned smart TVs without requiring additional equipment or security hardware. A broadcaster simply provides an Operator App and viewers then sign up for service with a single click of the remote immediately after connecting the TV set to the internet. A common advantage for both TV OEMs and broadcasters is that there is no CAS vendor lock-in. Moreover, ExpressPlay XCA's self-certification accelerates OEMs' time to market by avoiding tedious certification processes associated with a legacy CAS.

OEMs utilizing ExpressPlay XCA also gain from a marketing standpoint by providing an incentive for broadcasters to promote sales to consumers. Such promotions make sense because the more buyers of those brands there are, the larger the market base broadcasters have for delivering their services without incurring legacy CA costs.

For broadcasters, ExpressPlay XCA liberates them to pursue whatever business model suits their needs. They can employ the platform to provide protection for any combination of DVB one-way, DVB hybrid, or pure OTT services and, within those categories, service variations such as UHD or early-window movie releases that require different levels of protection.

By creating a single-client device stack for OTT and legacy programming, ExpressPlay XCA also relieves broadcasters of all the responsibilities associated with activating CA or DRM protection in device chipsets, managing keys and authenticating devices for use with specific services.

Along with saving money and time, broadcasters also benefit from the marketing exposure they get when their services are positioned on the smart TV UI with other options. Non-subscribers can sign up for new broadcast TV services with a simple click of the remote, similar to how they subscribe to OTT services such as Netflix or Amazon Prime. Moreover, consumers benefit from broadcasters' ability to offer more service options, such as free-to-air (FTA), free-to-view (FTV), pay-per-view (PPV), multi-tier subscriptions and other iterations.

In the sections that follow we begin with an assessment of what a consolidated security platform means to broadcasters and OEMs. Then we take a deeper look at how ExpressPlay XCA works and why, in terms of the benefits accruing to OEMs and broadcasters, it offers a consolidated security platform for enabling legacy and direct-to-TV services on smart TVs.

The need for a converged security solution

Clearly, the stars are aligned for broadcasters, and multichannel video programming distributors (MVPDs) as well, who want to take advantage of smart TVs to anchor new hybrid service strategies. The smart TV base has reached critical mass in DVB markets, and with broad support for HbbTV, broadcasters can now provide a large share of their customers ready access to both legacy and direct-to-TV content without requiring DVB receivers or STBs.

Getting beyond CAMs and STBs

In fact, the latest generation of SoCs used with smart TVs eliminates the need for CAMs as well. This is a major benefit to new direct-to-TV strategies, because, while the industry has partly succeeded in decoupling DVB receivers and STBs from a specific CAS through use of smartcards and CAMs supporting the DVB Common Scrambling Algorithm (DVB CSA), these devices don't provide an acceptable pathway to working in the hybrid services environment.

One problem has to do with the fact that CAMs and smartcards introduced security vulnerabilities that are out of step with ever more stringent content protection requirements imposed with current high-value content licensing policies. For example pirates have become adept at exploiting control words encrypted as entitlement control messages (ECM) unique to each CAS in the CAM or embedded CA card reader, which transmits authorization for decryption to the receiver via a CAS-specific entitlement management message (EMM). In some cases, they reverse-engineer the ECMs, which are much easier to defeat than the algorithms used to scramble the content. In other cases, they use "white-box" techniques that employ virtual machines such as logic analyzers to read electronic wave or power consumption patterns to enable emulation of the CA algorithm without having to break the code.

Apart from security concerns, there are serious issues related to the inconvenience and costs surrounding the use of CAMs and smartcards, starting with the fact that consumers have to obtain and install these security devices before they can gain access to the service, which defeats the click-and-subscribe convenience enabled by smart TVs.

The adoption of the second-generation CI Plus 2.0 standard, by enabling provision of security through USB CAM form factors, simplifies installation for consumers and lowers device costs. However, it still requires a conditional access system.

SoC-based content protection and the enduring CA problem

That issue can be surmounted in instances where Smart TV SoCs are used to perform the DRM and CA security processes independently, without the need for any extra CA hardware (see Fig. 1). These chipsets typically utilize Trusted Execution Environment (TEE) roots of trust conforming to the ETSI key ladder standard or its SMPTE variation, the Open Media Security key ladder, which configure how keys are embedded in hardware.

These steps, along with other measures supported by the Trusted Application (TA) running in the TEE, including sandboxing, firewalls, and other techniques providing enhanced security features, deliver hardware-level security that can be accessed by third parties with diverse security and operations systems.

These costs remain a significant expense in today's premium TV service operations, adding up to about $3 billion globally according to one tabulation.[1] Some cost elements may be reduced with card-free, chip-based CA protection, but fees related to CAS usage will remain, as will integration and certification costs in cases where SoCs haven't been pre-integrated with the chosen CAS. Moreover, with each advance in DVB's CI Plus standards, OEMs must choose whether to support the latest version and then communicate to buyers which models support what versions.

Rather than competing solely on the basis of innovation in their core areas of competence, OEMs must also compete on the basis of which CAS-based approach will resonate best with buyers in any given market. Guessing wrong can produce big losses with rollouts of new models. Moreover, OEMs take big hits in lost sales when they have perfectly good models sitting on retail shelves that have been outmoded by sets that conform to a new approach to CAS protection that is winning consumer support.

It's not hard to imagine the market appeal of TV sets that free consumers from STB and CAM installation of broadcast TV service. In such cases, they can be told that no matter where they live in the DVB marketplace, they can buy smart TV models and instantly connect to their choice of legacy and OTT premium service providers without having to deal with CAMs or STBs.

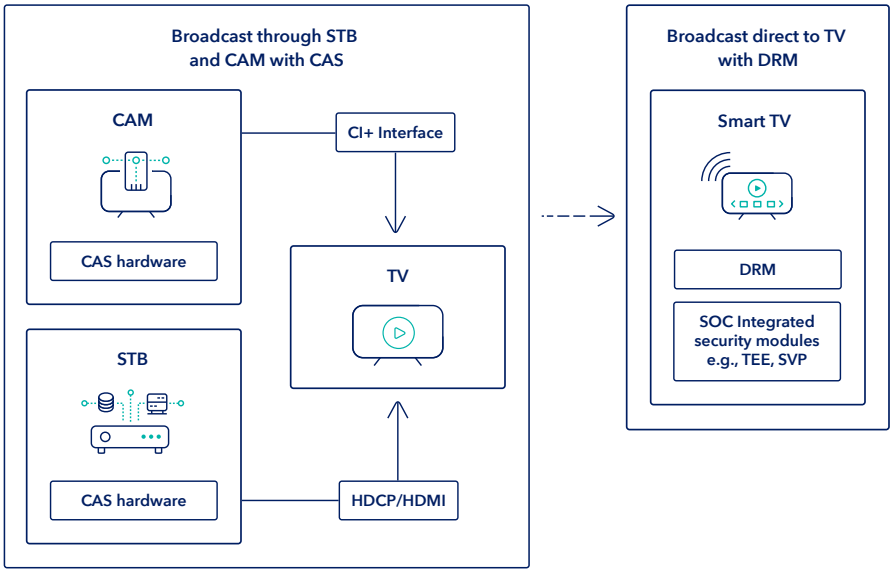


Fig. 1
Getting beyond CAM and STB using direct-to-TV broadcast security

1 1 Transparency Market Research, Conditional Access System Market to be Worth $5,381.2 Million by 2026, May 2018

The converged security solution for DVB broadcasters

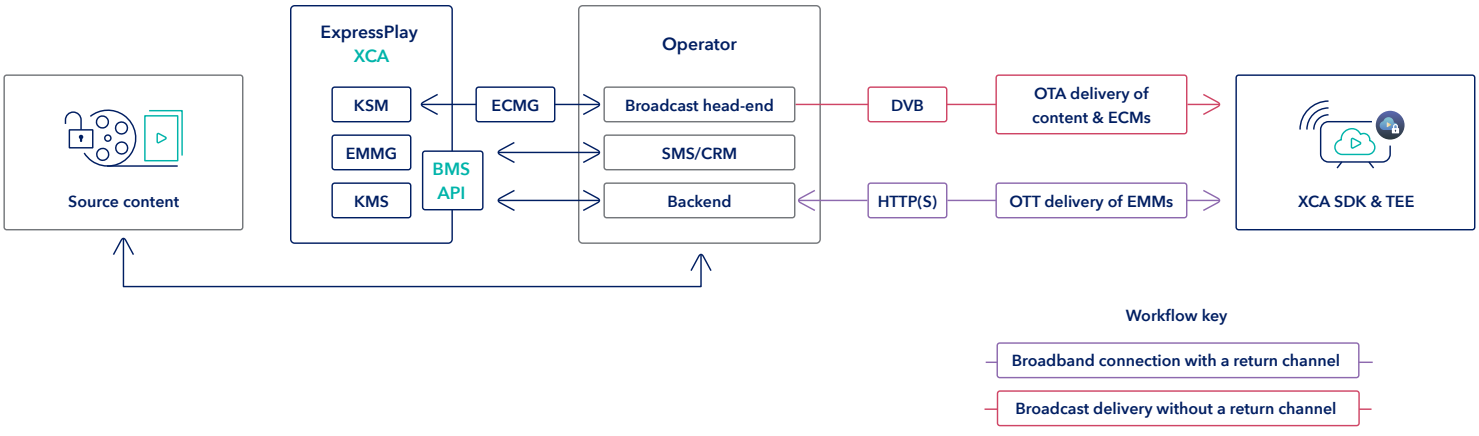
Given all the above, it makes sense that ever more OEMs are opting to support the one approach to utilizing their smart TV SoC resources that allows them to cover all security requirements without reliance on a traditional CAS. This is the ExpressPlay XCA platform, which Intertrust is operating to serve the DVB marketplace as a turnkey SaaS instantiated across the global Amazon Web Service (AWS) cloud footprint.

Global support for an open-standard platform

ExpressPlay XCA consolidates what is otherwise silo-based CAS and DRM security by utilizing the open-standard Marlin DRM engine to provide a unified content protection for any type of hybrid TV service that includes DVB channels (see Fig. 2).

At the backend, the XCA Broadcast Management System (BMS) serves as the interface for the operator CRM/SMS and head-end components. At the core processing center, the platform's Entitlement Management Message (EMM) Injector enables the DVB Simulcrypt compatible multiplexer to handle the EMM queue and cycles, and the Entitlement Control Messages (ECM) Generator generates and injects ECMs for the mux.

Fig. 2
Direct-to-TV broadcast delivery using ExpressPlay XCA



Marlin, now positioned as the native DRM in over 500 million devices worldwide, used as a DRM solution for protecting content from premium motion picture studios, TV networks and licensors worldwide, including UHD and other high-value content that requires adherence to MovieLabs' ECP Compliance and Robustness (C&R) framework.

Building on Marlin's longstanding integration with SoCs that support TEE and secure video paths (SVP) mandated by ECP, Intertrust has fostered pre-integration of the full ExpressPlay XCA client stack with a new generation of chipsets produced by Broadcom, MediaTek, RealTek, NovaTek, AmLogic, Alitech, Montage, and others.

This has enabled manufacturers to integrate ExpressPlay XCA with smart TVs representing approximately 50% of the global TV set market, including models produced by Sony, HiSense, TCL, and Vestel, with the latter serving as OEM for 150 brands worldwide.

ExpressPlay XCA has also been integrated at the HbbTV application layer with VEWD CORE, the dominant HbbTV middleware stack. This enables HbbTV applications to interact with ExpressPlay XCA client stack integrated by VEWD for HbbTV executions in the vast majority of smart TVs, 80% of which are integrated with VEWD middleware.

Freedom from legacy CAS and other benefits

Consolidating the content protection technologies for broadcast TV and OTT streaming on smart TVs will provide benefits equally to OEMs and broadcasters. By leveraging Intertrust's ExpressPlay XCA platform, OEMs are enabling broadcasters to achieve a truly converged approach to content protection that supports full realization of the hybrid service potential as an answer to the OTT challenge.

At the same time, these OEMs are able to free themselves from having to deal with the costs and complications of the legacy CAS marketplace. Multiple broadcasters can transmit their services to users who purchase a smart TV integrated with ExpressPlay XCA, while those XCA clients are compartmentalizing and maintaining the integrity of their operations.

Critically, broadcasters who want to take advantage of smart TVs' support for ExpressPlay XCA can do so while continuing to use their legacy CAS with deployed STBs and CAMs to whatever extent necessary.

Moreover, the ExpressPlay XCA service APIs make it easy for service providers to integrate the platform with virtually any subscriber management or content management system. Even better, it can support any distribution mode, including broadcast, adaptive streaming, multicast and progressive download, with support for offline playback, device-to-device side loading and time-shift applications (see Fig. 3).

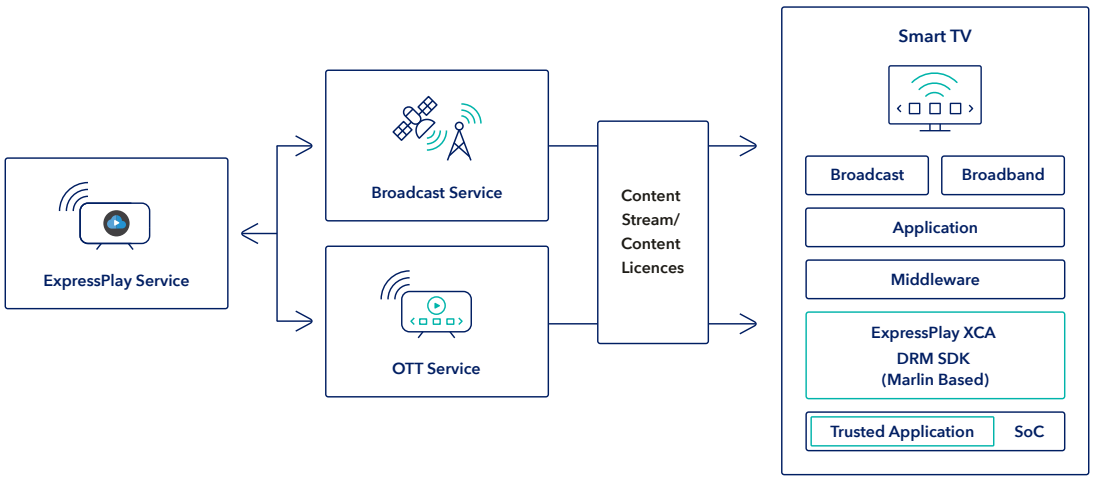
The protection versatility provided through ExpressPlay XCA makes it possible for service providers to issue, activate and deactivate content access rights in accord with different business models for virtually any use case.

Along with consolidating content protection free of legacy CAS requirements, the ExpressPlay XCA self-certification accelerates service providers' time to market, which, as mentioned, is an issue for certifications with legacy CAS.

When it comes to protecting the direct-to-TV side of the content portfolio, the DRM-related key management and other processes are incorporated into the ExpressPlay XCA SaaS through the Intertrust ExpressPlay DRM service, which can be extended beyond smart TVs to all connected devices.

The consolidation of security through ExpressPlay XCA also extends to the ever more common instances where content rights holders are calling for watermarking protection with high-value UHD 4K content and, in some cases, HD content as well. Leveraging Intertrust's partnerships with leading suppliers of watermarking platforms, ExpressPlay XCA makes it possible for customers to unify watermarking processes with live and on-demand content across all device platforms.

Fig. 3
Converged DRM-based security solution for Broadcast TV and OTT streaming



Attaining the lowest possible TCO

Looking at all these benefits from a financial perspective, the accrued savings results in a total cost of ownership (TCO) in the short and long runs that can't be matched through any other content protection approachsuited for a hybrid service strategy in the DVB marketplace.

This includes solutions that offer cloud-based consolidated security services that rely on legacy CAS technology, which don't have the integrated SoC presence in smart TVs that Intertrust has established for ExpressPlay XCA. Along with eliminating high CAS licensing fees and costs related to integration and certification, ExpressPlay capitalizes on the fact that the underlying principle behind industry adoption of Marlin was a commitment to an open-standard strategy with lower total cost of ownership (TCO). Carrying this through, ExpressPlay XCA is able to achieve multi-network content protection execution on a single platform that costs less than any other to license.

Costs are also mitigated by the fact that Intertrust is able to amortize the SaaS operating expenses across a rapidly expanding global customer base. This is another reason ExpressPlay XCA delivers by far the lowest TCO for securing broadcasters' hybrid services.

Conclusion

Across the DVB ecosystem, broadcasters and other providers of legacy TV services are capitalizing on the TV viewing experience being transformed by surging numbers of smart TV households everywhere.

By pursuing hybrid service strategies that offer consumers OTT streaming and direct-to-TV broadcast options alongside traditional premium programming, broadcasters are freeing themselves to leverage their local market strengths to maximum advantage.

This brings into play an opportunity to consolidate support for broadcasting and OTT streaming content protection on the advanced chipsets that have made smart TVs the driving force behind OTT content consumption. Intertrust is enabling this card-free future by leveraging the open-standard Marlin DRM core to handle processing for both types of protection, thereby eliminating the costs and inconvenience of utilizing legacy CAS.

Operating as a SaaS that takes care of all the key management and other processes related to executing converged multi-network content security, ExpressPlay XCA delivers by far the lowest TCO of any option in the converged security space with unmatched support from chipmakers and OEMs worldwide. With rapidly expanding OEM support, broadcasters leveraging the ExpressPlay XCA platform will be able to migrate at accelerating speed away from the costs and hassles of two-silo approaches to a unified security platform for hybrid services.

intertrust®

Building trust for the connected world.

Learn more at: expressplay.com/products
Contact us at: +1 408 616 1600 | onestopshop@expressplay.com

Intertrust Technologies Corporation
400 N McCarthy Blvd, Suite 220, Milpitas, CA 95035