intertrust®

White Paper

Media Solutions

The ideal path to converged content protection for hybrid TV services

Intertrust ExpressPlay XCA™ outperforms the competing options at the lowest TCO

Contents

Introduction

As hybrid TV service models that combine over-the-top (OTT) services with broadcast content take hold worldwide, broadcasters and multichannel distributors have more reason than ever to adopt a converged, cardless security approach in order to protect their content across the growing number of viewing platforms.

With the new generation of TV sets and their reduced dependence on factory integrated set-top boxes (STB) and legacy conditional access systems (CAS), the media and entertainment (M&E) industry and video service providers are on their way to eliminating the need for external security modules. However, these are just the interim steps toward what TV providers must now do to protect the OTT content that's delivered together with both broadcast programming to smart TVs and hybrid STBs.

The path forward involves the consolidation of security processing in the core client hardware, which enables a seamless orchestration of CA and digital rights management (DRM) protection on any device. Nevertheless, for many pay TV providers, determining whether a single-silo approach to content protection actually fits their service goals remains an open question. Conflicting vendor claims about the efficacy of the various approaches only further complicates the situation.

Converged security solutions that use a single client player to execute a legacy CAS, alongside DRM-based protection, retain traditional CA cost models and limit the service reach to only the devices with authenticated chip-level support for the specified CA.

Another DRM-based approach to converged content protection, enabled by Google's Widevine CAS, provides a single-player solution that only works with devices that support Android TV. However, with this approach, service providers are charged for any complex back-end integration and security management.

One exception to these limitations can be found in the converged approach to content protection, which is supported by the Intertrust ExpressPlay XCA security-as a service (SaaS) platform. ExpressPlay XCA eliminates the royalties and other fees associated with legacy CAS. ExpressPlay XCA utilizes the widely embedded open-standard Marlin DRM core to enable cardless CA and DRM protection.

Service providers can use ExpressPlay XCA for protection with virtually any type of hybrid TV service delivered to any DVB-compatible media gateway, STB, or smart TV regardless of the operating system. Because it's compliant with the DVB Simulcrypt standard, ExpressPlay XCA can be deployed alongside legacy CAS on one-way devices as well as interactive networks and facilitates non-disruptive transitions to hybrid services.

The ExpressPlay XCA SaaS also works in concert with Intertrust's ExpressPlay DRM service. It provides robust protection for OTT content delivered to smartphones and other online-connected devices with support for all the major DRMs including Google Widevine, Apple FairPlay, Microsoft PlayReady, and Adobe Primetime as well as Marlin. Both Intertrust services are optimized to support MovieLabs' Enhanced Content Protection (ECP) requirements, including the Compliance and Robustness (C&R) framework and forensic watermarking, which are increasingly required for the licensing of UHD and other high-value content.

The purpose of this paper is to provide information so that broadcasters and multichannel video programming distributors (MVPDs) can make informed decisions on maximizing their cost and DevOps efficiencies. It thoroughly explains and provides guidance on the various optimal approaches for protecting high-value video content in the converged OTT and legacy TV services marketplace, answering key questions on:

- Why is a ubiquitously deployable converged content protection solution essential for minimizing operational costs and maximizing the flexibility of service providers? How does it help them to innovate and keep pace with evolving marketplace requirements?
- How is ExpressPlay XCA (which is now widely integrated with media device chipsets, leading OEMs' smart TVs, and many other ecosystem device and management components) designed to deliver all the support that service providers need to protect their content across all modes of delivery and to every type of device?
- What are the differences between ExpressPlay XCA and the other approaches to converged content protection?

Part 1
Conditions calling for DRM-based converged content security

Both broadcasters and MVPDs are finding themselves in a vastly altered television hardware environment that requires an entirely new approach to fulfill the security requirements imposed by content rights holders. This is especially important in cases involving the delivery of both legacy TV and OTT content to TV sets.

It also applies to situations where legacy TV providers are streaming their content online to smartphones and other internet devices. Advances in device microprocessors, combined with the need to activate hardware-level security under the prescriptions of MovieLabs' ECP specifications, are best accommodated through a unified security approach.

The expanding device base for cardless security

The opportunity to eliminate the two-silo approach involves transitioning to a converged cardless security system for delivering hybrid TV services to TV sets. This can be done because virtually all chipsets handling core processing in smart TVs and recent vintage STBs and media gateways can support CA protection without the use of smartcards.

Today, this device ecosystem represents a huge global marketplace for the new converged security strategies. Various estimates put total smart TV penetration at about 30% of all TV households worldwide, with smart TV sets accounting for about 70% of all TV set sales in 2018.[1]

Counting hybrid STBs (which account for the lion's share of units installed since 2015), the penetration of devices capable of supporting converged cardless TV security most likely exceeds 50% of the world's TV households. With annual smart TV sales totals projected to increase from $157 billion in 2018 to $258 billion by 2024,[2] it won't be long before the chipset base for cardless TV security is almost universal.

These chipsets typically utilize hardware roots of trust conforming to the European Telecommunications Standards Institute (ETSI) key ladder standard or its Society of Motion Picture and Television Engineers (SMPTE) variation, the Open Media Security key ladder, which configures how keys are embedded in hardware. This provides hardware-level security that can be accessed by third parties with diverse security and operating systems. At the same time, the Trusted Execution Environment (TEE) utilizes sandboxes, firewalls, and other techniques to provide security features such as the integrity of trusted applications, confidentiality of assets, and independence from traditional middleware security to prevent the tampering with software-based security systems.

The sea change at the system-on-a-chip (SoC) level has very important implications for how broadcasters and MVPDs deliver their services to smart TV sets. Now, service providers have an opportunity to eliminate the need for STBs in smart TV households by making their services available to new subscribers with just a click of their remote.

By eliminating the need for STBs or CA modules (CAMs) in such instances, service providers reduce the impact of hardware costs on subscription prices. Therefore, the volume of smart TV sets that can be authenticated for use with a provider's TV service by virtue of pre-integration of the TV with a given converged protection platform becomes a major consideration when it comes to analyzing the cost benefits among competing security options.

Of course, the emergence of a new generation of SoCs capable of supporting converged cardless security doesn't eliminate the need to continue supporting deployed CPE that relies on legacy CAS. Service providers must be able to sustain these operations as they transition to a new converged security platform.

Drawbacks to using legacy CAS with cardless security

With the opportunity to make this transition now at the forefront, the next question is whether it makes sense to continue relying on legacy CAS technology. In a nutshell, it comes down to determining whether the CAS-related costs can be avoided through the use of a new solution that leverages DRM technology.

Certainly some CAS providers have adapted their solutions to exploit the new SoC environment using client players that execute DRM or CA processes, depending on the type of device and service configuration. But these solutions remain encumbered by many of the drawbacks associated with the reliance on legacy CAS technology.

Legacy CAS costs represent a significant component of today's premium TV service operations, which may continue according to several research studies. For example, a 2018 Transparency Market Research report states that the global CAS market, pegged at $2.9 billion in 2017, is growing at a 6.9% CAGR and is on course to reach $5.4 billion by 2026.[3]

The move to cardless, chip-based CA protection disrupts old CAS pricing models to some extent, but there is no reason to expect that the costs to distributors will go down. The rights to using CAS will be charged in the typical fashion whether it's through upfront charges, fixed monthly payments, per-user royalty fees, or some combination of these approaches.

Beyond the basic licensing charges, pay TV operators will have to bear the costs of integrations with any SoCs they want to use with their services that haven't already been integrated with their CAS. And regardless of whether the CAS is pre-integrated with targeted SoCs, service providers will incur the costs of integrating and certifying SoCs for use with their CAS-protected services.

Traditionally, these costs were reflected in STB and smartcard prices. In the new environment, integrations and certifications will be part of the CAS provider's SaaS service fee.

There is also a question of how CAS providers will recoup the revenue they're accustomed to generating from OEMs for use of their technology with operator- and consumer-purchased STBs and smartcards. Traditionally, CAS providers have derived a big share of their revenue from the licensing fees charged to STB and CAM manufacturers; or in the case of CAM modules, sometimes they market under their own brands. In the cardless chip-based CAS environment (to the extent CAS providers want to sustain traditional revenue levels), they will have to recoup lost hardware royalties through service and direct licensing charges to service providers.

Reliance on legacy CAS also brings into play the additional licensing costs of mounting the DRM side of the converged protection platform. By contrast, there's only a single licensing fee when a DRM core is used to support both CA and DRM protection.

As has always been the case, all these costs will ultimately be passed on to the consumer as part of their subscription fees. However, this presents a major problem for service providers who are under tremendous price pressure from OTT service providers who aren't burdened by traditional CAS costs.

Part 2
Defining the ideal converged security platform

TV providers can avoid all the drawbacks with the continued reliance on legacy CAS in the cardless security environment when they employ Intertrust ExpressPlay XCA SaaS. ExpressPlay XCA utilizes the open-standard Marlin DRM engine to provide CA and DRM functionality for any type of hybrid TV service delivered over DVB channels.

The ExpressPlay SaaS is hosted on Amazon Web Service (AWS) facilities to provide robust, redundant support with an extremely low latency across the DVB footprint. This encompasses broadcast and pay TV services throughout Europe, Russia, the Middle East, India, Indonesia, Australia, and much of Africa.

The Marlin advantage

With Marlin DRM as the anchor protection technology, ExpressPlay XCA provides the best possible solution for operating in today's converged legacy and OTT TV marketplace. It also positions service providers properly so there is a painless transition to the DRM protection regime that will take hold whenever they move to an all-IP mode of content distribution.

Launched as an industry standard in 2005 by Intertrust, Panasonic, Philips, Samsung, and Sony, Marlin provides a general-purpose rights management architecture that seamlessly delivers robust DRM protection across all connected devices and is compatible with all the major operating systems, codecs, file formats, and distribution networks.

Marlin is the recognized DRM solution used for protecting motion picture studios, TV networks and other licensor' content worldwide, including UHD and other high-value content that requires adherence to the ECP Compliance and Robustness (C&R) framework. Service providers are able to expedite C&R compliance because of Marlin's pre-integration with a vast ecosystem of chipsets that comport with TEE and the secure video paths (SVP) mandated by ECP.

Now serving as the native DRM on over 250 million devices, Marlin has been adopted as the certified DRM for a wide range of service platforms including the Japanese HTML5-based hybrid TV standard Japan Open IPTV; the Hollywood studios' UltraViolet; the U.K.'s YouView hybrid STB framework; the French HD Forum's TNT 2.0; and devices specified for use with Chinese OTT services such as iQIYI, Tencent, and PPTV.

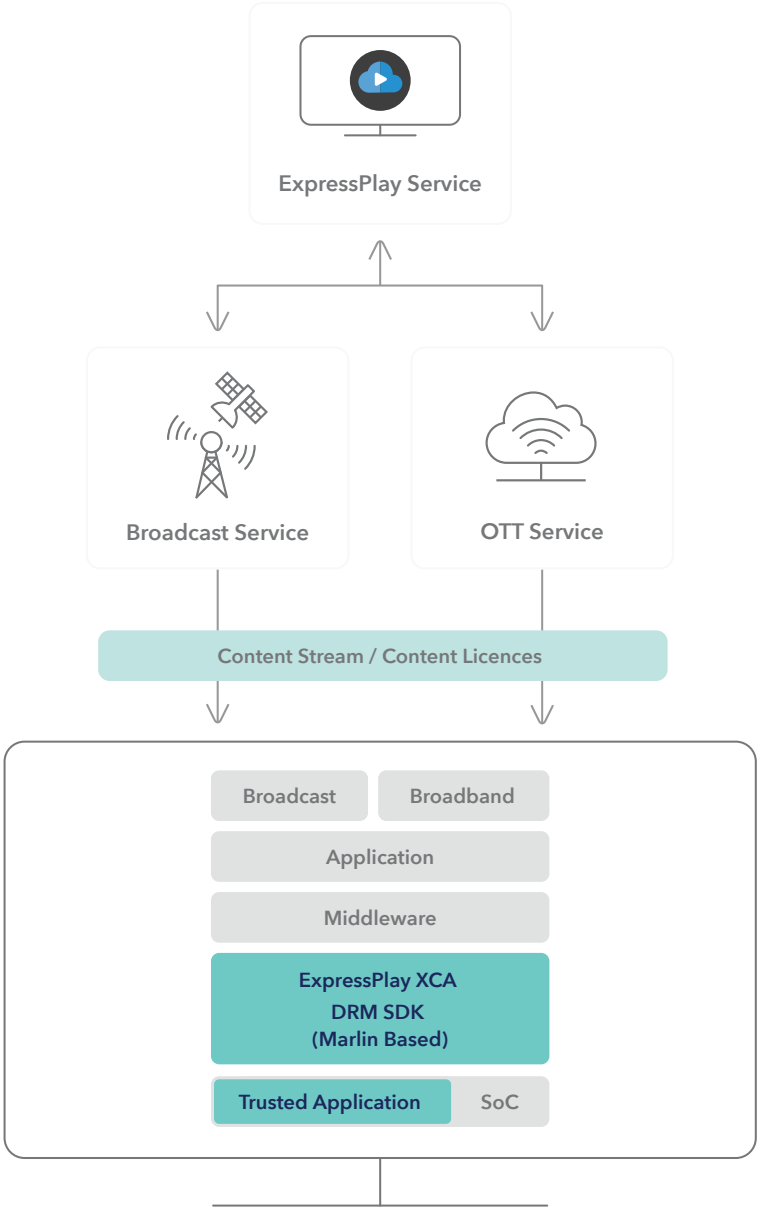
The mechanics of ExpressPlay XCA

The mechanics of ExpressPlay XCA as shown in Figure 1, pivot on three main areas:

- **Cloud architecture**
  An ExpressPlay (multi-DRM) operator can use the ExpressPlay XCA functionality without using dedicated on-premise hardware. This not only reduces costs, but it also speeds up the overall service deployment.
- **Single client stack for OTT and over-the-Air programming (OTA)**
  Combining the cloud deployment with a client that supports both OTA and OTT services from the outset, ExpressPlay XCA allows an operator to distribute content in various ways such as unicast/multicast and in multiple formats such as MPEG-2 TS with DVB CSA and MPEG-DASH with CENC. This will be completely transparent to the viewer.
- **Multi-tenant client**
  Since ExpressPlay XCA targets retail devices such as smart TVs, it's logical to assume that those devices are not bound to a specific broadcast operator. With ExpressPlay XCA, multiple operators can share the resources of the same device in a similar fashion to how OTT VOD services already do today. The ExpressPlay XCA client enables multiple broadcast operators to transmit their services to the same device, while the ExpressPlay XCA client takes care of the compartmentalization of the operator environments and the integrity of their operations.

Figure 1.

A unified security solution for broadcast and streaming services



Along with providing the appropriate mode of content protection in separate legacy pay TV and OTT scenarios, ExpressPlay XCA can be implemented as a trusted application (TA) with chipsets supporting Trusted Execution Environment (TEE) to provide protection for hybrid services distributed to smart TVs and STBs.

The ExpressPlay XCA architecture makes it possible for service providers to issue, activate, and deactivate content access rights in accordance with different business models for virtually any use case including free-to-air (FTA), free-to-view (FTV), pay-per-view (PPV), multi-tier subscription, and other iterations (see Figure 2).

For example, the Intertrust platform is providing content protection on content to over eight million European households served by the four free digital satellite broadcasters who comprise the Free TV Alliance. For example, important input for the ExpressPlay XCA functional and technical requirements have been defined together with the members of Free-to-View Alliance (FTVA), which is a group of satellite broadcasters including HD+ in Germany and Fransat in France. This opens a potential opportunity to address 10M+ households. More FTVA members are evaluating the ExpressPlay XCA security and cloud-based service, with major service launches anticipated in 2020.

Figure 2.

ExpressPlay XCA supported use cases

Free-to-view	Subscriptions	Pay-Per-View-Events	OTT
With Activation/Registration Groups of encrypted free-to-view channels that are only accessed once the devices have been registered.	**Subscriptions Groups** Encrypted pay-channels, which are only accessed once the services have been paid for by the consumer and the device is registered to the customer account. Some channels might support off-line registration and some require on-line registration to determine the location of the device through geo-tagging.	Encrypted channels that have pay-per-view events, which are encrypted and paid for. Only devices associated with the account that have paid to view the event will have access to the event.	Groups of encrypted free-to-view channels that are streamed through OTT pay-per-view. Groups of encrypted pay-per-view channels that are streamed through OTT.

The advent of TV-caliber OTT distribution has unleashed a wide range of use cases involving hybrid integration with legacy TV as well as pure-play OTT.

Each of these can be implemented in different ways. ExpressPlay XCA is designed to provide converged cardless protection with all versions of these use cases.

ExpressPlay XCA delivers protection suited to any distribution model including broadcast, adaptive streaming, multicast, and progressive download with support for offline playback, device-to-device side loading, and time-shift applications such as catch-up and network DVR. The platform can be deployed with one-way DVB broadcast-only devices as well as internet-connected DVB receivers.

ExpressPlay XCA is completely interoperable with existing CAS support infrastructures by virtue of its compatibility with the DVB Simulcrypt standard, which enables simultaneous use of two or more CA systems from the same headend. As a result, as service providers broaden the reach of protection supplied through ExpressPlay XCA, they can continue using any legacy CAS with deployed STBs and smartcards to whatever extent necessary until they are gradually replaced by the new TVs with embedded XCA security.

ExpressPlay XCA is implemented at all points in the protection architecture, including:

- **Client Device**
  ExpressPlay XCA client SDK and the TEE porting kit will enable device manufacturers to exceed the MovieLabs ECP requirements.
- **Backend**
  Broadcast Management System (BMS) serves as the interface for the operator CRM/SMS and head-end components.
- **Headend**
  Entitlement Management Message (EMM) Injector enables the DVB Simulcrypt compatible mux to handle the EMM queue and cycles and the Entitlement Control Messages (ECM) Generator generates and injects ECMs for the mux.

ExpressPlay XCA relieves service providers of all the responsibilities associated with activating protection in device chipsets, managing keys, and authenticating devices for use with specific services. These tasks are executed through the Intertrust Managed PKI platform, which has issued billions of cryptographic credentials to device makers and service providers. Moreover, the ExpressPlay XCA self-certification accelerates service providers' time to market, which as previously mentioned is an issue for certifications with legacy CAS.

ExpressPlay XCA can be used with Intertrust's ExpressPlay DRM service to extend unified protection to all connected devices. As described on the Intertrust website and the report, "Weighing the Buy Versus Build Options for Enabling Content Protection in the New OTT Video Market," ExpressPlay DRM is the only platform supporting all the major DRMs including Google Widevine, Apple FairPlay, Microsoft PlayReady, Adobe Primetime, and Marlin.

In conjunction with Marlin's support for the ECP C&R framework, both ExpressPlay XCA and DRM provide extensions for activating watermarking systems within their respective service domains. This makes it possible for ExpressPlay XCA customers to unify watermarking processes with live and on-demand content across all device platforms.

Ecosystem support for ExpressPlay XCA

Since its introduction in 2017, the full ExpressPlay XCA CA and DRM protocol stack has been pre-integrated with chipsets produced by Broadcom, MediaTek, RealTek, NovaTek, AmLogic, Alitech, Montage, and others. This has sparked wide adoption by major OEMs; notably, ExpressPlay XCA is now integrated with smart TVs produced by manufacturers representing approximately 50% of the global TV set market including Sony, Hisense, TCL, and Vestel, which serves as OEM for 150 brands worldwide.

ExpressPlay XCA, as a compatible security solution for Hybrid Broadcast Broadband TV (HbbTV) has also been integrated at the HbbTV application layer with VEWD CORE, the dominant HbbTV middleware stack. This positions ExpressPlay XCA for HbbTV executions with the vast majority of Android smart TVs, 80% of which are integrated with VEWD middleware.

Pre-integrations with vendor headends and cloud-based media services abound as well. Additionally, at the back-office level, the ExpressPlay XCA service APIs make it easy for service providers to integrate the platform with virtually any subscriber or content management system.

Part 3
Comparing converged security options

For broadcasters and MVPDs alike, when it comes to choosing a cardless converged security option for hybrid services, there are two fundamental questions to consider: Which options meet all the requirements for providing protection suited to achieving current and future service goals, and among those that do, which choice will deliver the lowest total cost of ownership (TCO)?

The case for ExpressPlay XCA versus legacy CAS-based solutions

Looking at how ExpressPlay XCA compares with a legacy CAS-based solution, the differences we covered explain the clear disadvantages of a legacy CAS.

Strategically, it's important to recognize that a key goal for any provider of hybrid legacy and OTT TV services is to maximize the opportunity to deliver content to smart TVs without the use of STBs or smartcards. Even if any given CAS-based solution offered as a service accomplishes security management and ECP fulfillment capabilities to the level of ExpressPlay XCA, such a solution will not have the integrated SoC presence in smart TVs that Intertrust has established for ExpressPlay XCA. OEMs that have integrated ExpressPlay XCA with current generations of smart TV sets account for 50% of the manufacturing base worldwide.

Turning to the TCO question (covered in Part 1), any SaaS using a legacy CAS is expected to incorporate the following cost factors in the recurring service charges:

- High licensing fees
- Additional licensing fees for DRM technology
- A comparatively high rate of integrations with SoC roots-of-trust
- Costly approaches to device certification with providers' services
- A need for the CAS provider to recoup revenue formerly collected from OEMs

Also, there are additional costs that are not part of the service charge that will impact service providers as well. These include time-to-market delays resulting from large SoC integration workloads, cumbersome device certification processes, and the lack of choice in choosing system components.

There are several reasons service providers can count on incurring a much lower TCO with ExpressPlay XCA than they will with a CAS-based approach.

One of the founding principles behind the development of Marlin was that royalty fees must be minimized in the interest of creating a low-cost DRM foundation that would spur the availability of the content essential for driving OEMs' IP-connected device sales. This was accomplished through use of open-standard technology to the fullest extent possible, in conjunction with the founding partners' agreement to set low fees for their own intellectual property contributions to the standard.

This mandate has been adhered to over the life of Marlin, resulting in very low per-device licensing costs. Moreover, users of ExpressPlay XCA only pay the costs of licensing a single protection platform as opposed to the two-platform licensing costs incurred with CAS-based converged protection services.

Adding to the cost advantage, ExpressPlay XCA customers are not burdened with the integration and time-to-market cost penalties from a more limited SoC base and slow certification processes.

Comparison of ExpressPlay XCA with Widevine CAS

Because ExpressPlay XCA is a better choice compared to a CAS-based platform, the decision-making process turns to an analysis of how ExpressPlay XCA compares in terms of strategic goal fulfillment and TCO with Widevine CAS, which is the other DRM-based hybrid service protection solution currently available to service providers. Figure 3 summarizes and compares the key technical points.

Figure 3.

Comparison of ExpressPlay XCA with Widevine CAS

ExpressPlay XCA	Widevine CAS
ExpressPlay XCA is the only broadcast content security solution on the market today that is based on the open-standard Marlin DRM. The open-standard approach guarantees transparency on how the core technology is defined and prevents a single player from monopolizing the technology.	Widevine CAS is based on proprietary technology defined by Google.
ExpressPlay XCA is available on various platforms including Linux and Android Open Source Project (AOSP) and Android TV.	Widevine CAS is available only for the Android TV platform and not for AOSP.
ExpressPlay XCA supports both internet connected devices as well as one-way broadcast devices.	Widevine CAS does not support one-way broadcast devices. There is a roadmap to support one-way broadcast devices in 2020.
ExpressPlay XCA supports all common broadcast TV business models including subscription, free-to-view, pay-per-view, etc.	Widevine CAS is based on Widevine DRM. Its policy setting enables many business rules.
ExpressPlay XCA is integrated on various chipsets (SoCs) that support TEE and SVP. The ExpressPlay XCA TEE Porting Kit allows potentially any chipset vendor to develop the Trusted Application for their TEE. ExpressPlay XCA is pre-integrated with the TEE environment of the following chipset vendors: MStar, MTK, Broadcom, Hisilicon, Realtek, Novatek.	Supported only on Google recommended SoC models. Widevine CAS only runs on Android TV starting from Android 9 "Pie." The SoC vendor of the STB or TV needs to implement at least OEMCrypto for Widevine CAS v14 and must complete the Widevine CAS specific Compliance Test Suite (CTS).
ExpressPlay XCA provides a cloud-based headend for broadcast management systems and ECMG/EMMG generation.	Widevine CAS only provides the basic entitlement functionality such as Widevine license service and ECMG. Other back end CAS components need to be licensed from third-party vendors. Widevine provides the following: • ECMG library for integration with the scrambler • CAS Proxy SDK for issuing entitlements and applying business rules

Figure 3. (Continued)

Comparison of ExpressPlay XCA with Widevine CAS

ExpressPlay XCA	Widevine CAS
Complies with Free TV Alliance (FTVA) requirements that include most broadcast operator use cases	Unknown
ExpressPlay XCA client security also supports an extension for watermarking.	While Widevine CAS comports with the TEE and SVP requirements of ECP C&R, Google has not specified an extension to enable use of watermarking with the platform.
ExpressPlay XCA provides a mechanism for each operator to manage the CAS logic in the client such as suspending or resuming a device.	Unknown
ExpressPlay XCA supports entitlement renewal through positive and negative addressing for both connected and unconnected cases.	Unknown
ExpressPlay XCA supports operator binding/unbinding from the HbbTV layer.	Unknown
ExpressPlay XCA supports secure device reset functionality (only available from a trusted reseller).	Unknown
ExpressPlay XCA clients are self-certified by device makers.	Since Widevine CAS is part of Android TV, it requires certification and compliance with hardware requirements.

Looking Beyond Android TV

The most dramatic difference demonstrating the limitations of Widevine CAS is the fact that this solution can only be applied for hybrid services targeting Android TV devices that run on the Android 9 Pie OS released August 2018. At the SoC level, only two chipmakers, Amlogic and HiSilicon, indicated they were producing devices supporting Widevine CAS with 9 Pie as of YE 2019, though Google listed Broadcom as another chipmaker that will be anchoring a new generation of Widevine CAS-capable Android TVs.

As noted earlier, ExpressPlay XCA has established a major presence in the smart TV ecosystem through integrations with OEMs worldwide. Adding to the breadth of support in the Android TV domain is the previously referenced ExpressPlay XCA support for integrations through the Android Open Source Program and its integration with VEWD's HbbTV middleware.

Other Technical Drawbacks to Avoid

In addition to the Android TV requirement, there are several other technical distinctions that favor use of ExpressPlay XCA. Perhaps most significantly, Widevine DRM, notwithstanding its royalty-free status and ubiquitous market presence, is a proprietary technology under a single entity's control that prevents the community visibility and input of an open standard.

Among other noteworthy differences, Widevine CAS does not support one-way broadcast devices as of YE 2019, though that could change in 2020. In addition, Widevine CAS doesn't lend itself to device self-certification and does not have an extension suited to implementing watermarking.

Addressing the Full Scope of TCO

Beyond such differences, any perception that Widevine CAS offers a TCO advantage over ExpressPlay XCA is easily dispelled when one examines the full range of tasks that must be undertaken either in-house or through third-party service support. Unlike ExpressPlay XCA, Widevine CAS is not operated as a comprehensive turnkey service.

As a component of Android 9 Pie and presumably future Android OSs, the DRM-based CAS merely provides the basic entitlement functionalities including licensing and policy formulations and sets the SoC integration and communications frameworks that enable implementation of the DRM for use with headend CA processes.

Service providers must work through third parties to provide essential components such as ECM Generator (ECMG), EMM Generator (EMMG), and a media player configured to work with the unified CAS/DRM system. All of these components must be integrated into the framework, which also must be integrated with the service provider's subscriber and content management systems.

Even if a service provider turns all this over to an outside party, there's still a significant amount of work involved with selecting a supplier and overseeing execution of the setup, including purchasing decisions. There will also be a need to cover ongoing operating costs either through engagement with a third party or assignment of personnel with the technical skills essential to working with chipmakers and OEMs and executing maintenance of the system components.

The ExpressPlay XCA SaaS ensures TCO is minimized through the amortization of costs across the cloud service customer base with a success-based pricing strategy that is directly tied to the volume of usage. Service providers gain the means to maximize hybrid service reach through expert management of interactions with manufacturers and turnkey support for all the primary use cases at a TCO far lower than can be found with any other option.

Conclusion

The transformation of the TV viewing experience enabled by smart TVs, hybrid STBs, and media gateways has resulted in a proliferation of hybrid legacy and OTT TV services worldwide. The trend is especially strong in Europe and other countries where standardized platforms built around DVB have created new ways to generate revenue.

To fully capitalize on these opportunities, broadcasters and MVPDs need a fully converged chip-level approach to content protection that supports all use cases on all classes of managed and unmanaged devices for a minimum cost. But this can't be done at acceptable cost levels without abandoning reliance on either legacy CAS or DRM technology.

Cardless security systems designed to unify OTT and legacy content protection on smart TVs, hybrid STBs, and media gateways with use of legacy CAS in conjunction with separate DRM components maintain a legacy cost structure that is unsustainable in today's intensely price-competitive video services market. No matter how charges are configured with service-based business models, service providers using these platforms will be saddled with paying licensing fees and other costs of running separate CA and DRM silos.

Starting in mid-2018 with the release of the 9 Pie Android OS, Google has attempted to create a more cost-effective approach to consolidating protection for hybrid TV services by using its Widevine DRM as a mechanism for providing CA protection with legacy content. But Widevine CAS can only be applied with services delivered to Android TV sets that run on Pie 9 and later versions of the Android OS, which adds up to a minor segment of the deployed smart TV base.

Intertrust has created an opportunity for TV service providers to avoid all these pitfalls by employing ExpressPlay XCA SaaS to deliver a low-cost converged protection solution based on the open-standard Marlin DRM.

Here is a summary of the attributes that contribute to the ExpressPlay XCA advantages over all the other options:

- Full support for both broadcast and OTT streaming use cases
- Built on top of Intertrust's industry-strength DRM SDKs and services
- Pre-integrated with major TV and STB brands
- Support for one-way DVB networks and unconnected devices
- Meets the MovieLabs requirements for UHD content
- Fully managed cloud-based service
- Optionally supports forensic watermarking for broadcast and OTT content

Through a SaaS model that amortizes costs across a rapidly expanding global customer base, ExpressPlay XCA delivers by far the lowest TCO of any option in the converged security space. Dual solutions relying on legacy CAS in combination with DRM support are far more expensive. Widevine CAS, with its limited reach and lack of support for integrations and operations, isn't a match for XCA when it comes to a realistic assessment of the total cost of ownership.

ExpressPlay XCA is designed from the outset to overcome the typical legacy CAS limitations with a future-proof hybrid DVB-OTT next-gen security solution. ExpressPlay XCA bridges the otherwise disparate worlds of CAS and DRM by supporting DVB one-way plus broadband and DVB-IP hybrid services.

The converged security client means that no client security hardware is required; there are no smart cards or DVB-CI/CAM modules, and, together with manufacturer self-certification, the costs are lowered for device makers and operators alike. This ensures that Intertrust offers the lowest TCO among all providers of multi-network and multi-screen content security.

About Intertrust

Intertrust provides trusted computing products for leading corporations – from mobile, CE and IoT manufacturers, to service providers, and enterprise software companies. These products include the world's leading digital rights management (DRM), software tamper resistance, and technologies to enable secure data exchanges for various verticals including energy, entertainment, retail, automotive, and fintech.

Intertrust is headquartered in Silicon Valley with regional offices globally. The company has a legacy of invention, with fundamental contributions in computer security and digital trust. Intertrust holds hundreds of patents that are key to internet security, trust, privacy management, mobile code, networked operating environments, web services, and cloud computing.

As a provider of robust multi-DRM services for media and entertainment companies, our security technology protects the content delivered to any screen and OS platform, over any network.

Intertrust ExpressPlay is the world's most complete multi-DRM security-as-a-service, enabling converged protection for broadcast television and over-the-top (OTT) streaming services.

Sources

1 Statista, Smart & Connected TVs – Statistics & Facts, January 2019

2 Inmarc Group, Smart TV Global Market Trends, July 2019

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

intertrust®

Building trust for the connected world.

Learn more at: intertrust.com/drm
Contact us at: +1 408 616 1600 | sales-xp@intertrust.com

Intertrust Technologies Corporation
920 Stewart Drive, Sunnyvale, CA 94085