Securing OTT Content with CryptoFirewall™ Security Cores

Flexible and robust multi-screen OTT content protection

Today, content protection in connected devices such as tablets and smart TVs is predominantly provided by software security. The level of protection achievable in software on these platforms today does not meet the latest studio requirements for premium content.

In order to provide stronger security while simplifying product development, system-on-chips (SoCs) used in Internet-enabled televisions and mobile devices have started to include integrated hardware security cores. Once designed into an SoC, these hardware security cores provide a significant increase in security without sacrificing user-friendliness, flexibility or cost.

The CryptoFirewall core is the leading hardware security core for TV/video distribution. It is designed to provide the multi-operator flexibility and robust security required for Over-the-Top (OTT) multi-screen distribution to connected devices.

THE OTT CHALLENGE

Throughout history, advances in technology that create new opportunities for delivering information have also been exploited by pirates. This applies to the Internet, including OTT video delivery.

In the pay TV industry, digital distribution is augmenting the established, centralized distribution models. OTT approaches enable users to acquire content from many sources and view it on an increasing array of tablets, laptops, smart TVs and other devices.

However, this shift removes critical controls that operators have traditionally relied upon to limit piracy. Unlike managed networks, the open Internet lacks centralized control over the security of endpoints, such as set-top boxes (STBs), as well as communications over the network itself. As a result, the operators influence over the devices used to decode, distribute or redistribute, and consume content is greatly reduced. Similarly, the shift from operator-defined endpoints to user-selected off-the-shelf products reduces operators' involvement in critical security decisions.

To make OTT distribution of premium content more secure, it is necessary for Internet-connected devices to have robust content protection capabilities. Major security issues can be addressed through effective hardware security, enabling content providers to be comfortable with releasing top-quality content to Internet-based distribution environments.

In addition to robustness, operators and device manufacturers must be able to:

- Maintain, or improve user flexibility – making it more convenient to acquire content legally than illegally
- Provide a compelling, secure library of content
- Support 'multi-operator' and 'multi-CAS' operation so that a single device model can support a range of different content sources and content protection technologies

CryptoFirewall Core Highlights

- Meets operator and studio security requirements
- Supports all distribution platforms – satelittle, cable, IPTV and OTT
- Delivers uniform security across managed and unmanaged devices
- Flexible, fast and robust multi-operator support
- Provides an idependent key engine within the device SoC
- Compliments CAS and DRM software security
- More secure than a downloadable software security app and easier to deploy
- Maintains scurity even if the remainder of the system is compromised
- Available now from leading SoC manufacturers (see **cryptography.com/paytv**)

Securing OTT Content with **CryptoFirewall** Security Cores

THE NEW DIRECTION IN SECURITY TECHNOLOGY

Hardware security cores – security blocks integrated into the SoCs in devices – are the new direction for securing Internet-connected and mobile devices. Most new STB chipsets, and an increasing number of mobile device SoCs, currently feature specialized hardware security cores.

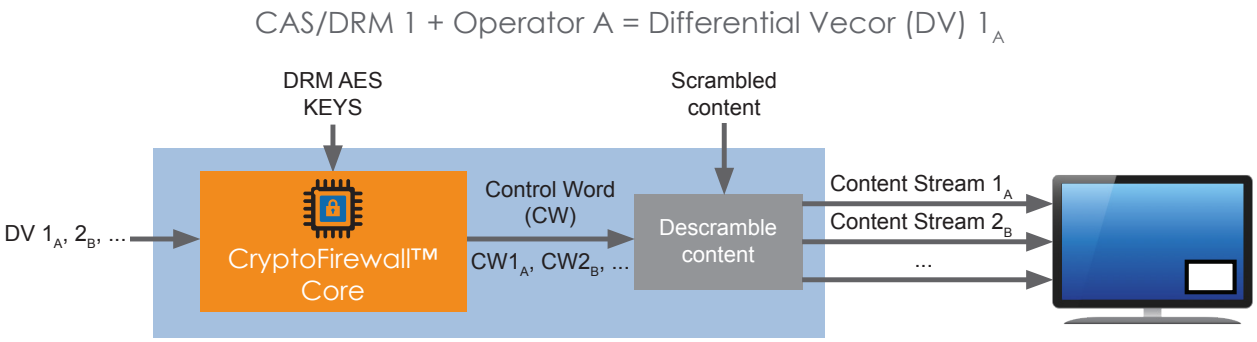
Well-designed hardware security cores separate security-sensitive processing and key storage from the processor and its software. Non-sensitive processing continues to be performed by software, but critical secrets and tasks are isolated from applications, operating system, device drivers, and other code.

This separation can deliver dramatic improvements in robustness, while accelerating time-to-market by relieving the software from rigid security and testing requirements. Modern SoC manufacturing processes enable hardware security cores to be added without significantly impacting costs, provided that cores have the flexibility to be used across a broad range of operators and security (CAS) architectures.

SECURE MULTI-OPERATOR SUPPORT

The CryptoFirewall™ core is an independent hardware security core specifically designed to protect digital content by protecting cryptographic keys and computations from attack. A leading solution for digital video decoding SoCs, the CryptoFirewall core has been integrated by vendors including Broadcom, ST, Entropic, ViXS, ALi, and MStar. Specifically for OTT applications, the CryptoFirewall core simplifies key management and provides a uniformly high level of security across devices and chipsets from different vendors.

To be used in securing video, the device needs to have a CryptoFirewall core in the SoC and a differentiation vector, a short secured data field that configures the core. The differentiation vector is an "ignition key" that readies the core for use with an operator and CAS or DRM system. Specifically, each differentiation vector is chip-specific and generated for a specific CAS/DRM + operator combination. Without the correct differentiation vector, the CryptoFirewall core cannot produce the correct control words for descrambling a service.



Single CryptoFirewall core simultaneously supports multiple CAS/DRM and operator combinations

With the differentiation vector, a CryptoFirewall core "joins" the security domain of a particular operator. If desired, multiple differentiation vectors (each for a particular CAS/DRM + operator combination) can be generated for use by the CryptoFirewall core in a particular device.

The CryptoFirewall core has the capability of loading different differentiation vectors for each new computation. Changing differentiation vectors takes about 5 milliseconds, so the rapid changes for picture-in-picture viewing of content from different operators are supported. Thus, a device can be simultaneously shared between multiple CAS/DRM systems and operators, if desired.

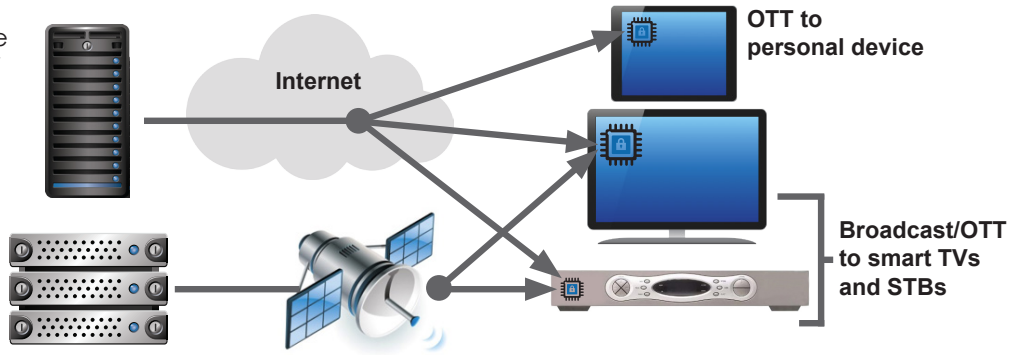
The overall result is ***flexible, fast and robust multi-operator support.***

Securing OTT Content with **CryptoFirewall** Security Cores

SECURE AND USER-FRIENDLY MULTI-SCREEN OPERATION

As CryptoFirewall cores are included in more types of devices, **highly-secure multi-screen operation can be enabled** as follows:

- For operator-managed devices, such as STBs or home-gateways, the media player and associated CAS/ DRM capabilities are pre-installed by the operator.
- For user-managed devices, such as most tablets, phones, and connected TVs, the user initiates a download of a media player application that provides the required capabilities.



Highly-secure multi-screen operation enabled with CryptoFirewall Security Cores

In both cases, the software serves as an untrusted conduit. In particular, the software retrieves differentiation vectors from the network and delivers them as needed to the security hardware, but the software cannot create, modify, or decrypt differentiation vectors. Likewise, the software cannot decrypt the video itself, but provides the hardware with the parameters needed to derive the video decryption keys.

If desired, devices may contain several media players for different operators, or several operators may share a single player app. In either case, the differentiation vector for the operator is sent to the device and received by the media player or other software that manages content rights.

In all cases, the operator obtains a uniform and high level of content protection across 'managed' and 'un-managed' devices in a very flexible way.

Once the CryptoFirewall core has been integrated into a device chipset, the device only needs a software app to manage playback, a differentiation vector to configure the core for a service, a rights keys authorizing access to specific programming the user has purchased, and the encrypted video stream. Content distribution is as flexible as software-only approaches, yet with the robustness of hardware security integrated directly in the SoC. From the user's perspective, downloading the appropriate app for use with a device that has the CryptoFirewall core is no more difficult than obtaining any other app. By combining ease of use, simple integration, low cost, and industry leading security, the CryptoFirewall core provides a user-friendly and convenient security solution for OTT.

cryptography.com/paytv