CryptoFirewall Content Protection Core

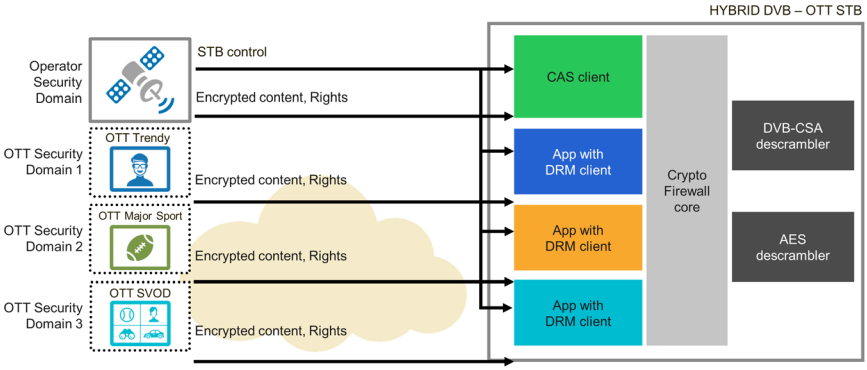
Our CryptoFirewall core secures digital entertainment content by protecting cryptographic keys and computations from attack.

Overview

The CryptoFirewall™ core is an independent hardware security core within the SoC that provides complete key management and secure video decryption. It works independently of the software and is designed to complement the existing security measures in any conditional access (CA) or digital rights management (DRM) systems.

Our CryptoFirewall solution supports a multi-domain security feature that is unique to our core and is based on an advanced hardware root-of-trust. With this multi-domain support, multiple broadcast or over-the-top (OTT) pay TV services can use the core's hardware security simultaneously, allowing premium content to flow securely from the cloud directly to pay TV devices like STBs and TVs. Our solution provides a secure foundation for convenient access to all pay TV content on one device. It enables new ways to distribute pay content, providing benefits to both operators and OTT distributors:

- Operators can provide their subscribers with instant individual choice of content on the STB or TV
- OTT distributors can deliver content directly and securely to operator STBs and TVs



CryptoFirewall core provides robust multi-domain security enabling STB devices to be included in multiple security domains

Highlights

Superior Security

- Provides robust hardware root-of-trust
- Protects against piracy and control word sharing attacks at the hardware level

Improved Profitability

- Cost-effective security
- Simplifies device validation
- Integrates easily into apps and HTML5 CDMs
- Enables new revenue with multi-domain security support

High Flexibility

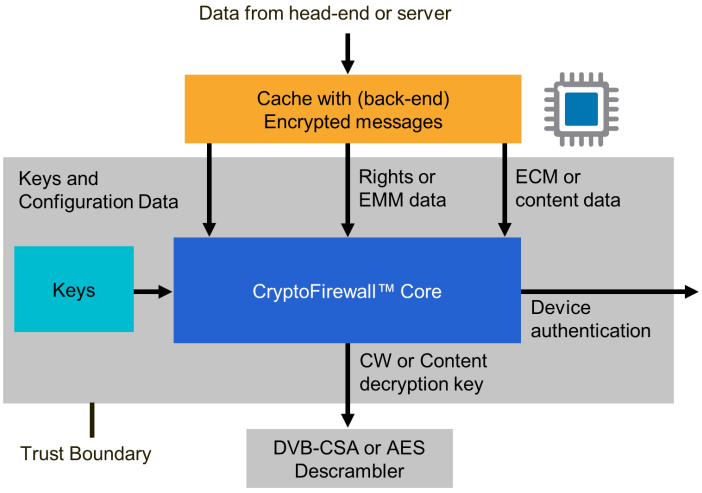
- Supports app-based content delivery to any device in any network

Use Cases

With a proven track record of more than 100 million devices in high-threat environments, our core supports numerous use cases.

- CAS used in one-way DVB/ATSC/ISDB operations
- Device authentication and content encryption key protection in 2-way IPTV/OTT operations
- Hybrid support: simultaneous access to two or more services using different CAS or DRM
- Multi-operator operation support for distribution of various OTT content to STBs

CryptoFirewall Content Protection Core



CryptoFirewall core operation

Security Features

- Provides the most robust hardware protection
- Supports multiple security domains
- Cost-effective security in the SoC — no external interface to attack
- Renders all software attacks as irrelevant as it does not include a CPU
- Protects against side-channel attacks
- Provides advanced logic to prevent glitching and fault injection
- Protects against reverse engineering by obfuscating and randomizing logic
- Provides secure integration with descramblers and key ladders
- Meets studio security requirements including UHD/4K content like MovieLabs ECP, facilitating licensing of premium content
- Includes advanced cryptography technology

Other Key Features

- Supports all major content distribution platforms - satellite, cable, IPTV, OTT, physical media
- Integrates easily — reference implementations and services available as needed
- Complements both software and smart card CA and DRM systems
- Compatible with MPEG2 and DVB transport, CENC, MPEG DASH, HTML5 EME, and more

Our Solution Supports Various Systems:

- **In broadcast systems**: the core receives the data it needs for operation in standard encrypted messages from the conditional access system.
- **In OTT systems**: data for the core is typically sent in license files during the provisioning of the device.
- **In CA systems**: the core can either derive or generate the control word and deliver it into the DVB-CSA descrambler. For derivation of the control word, the core delivers a key into the key ladder.
- **In DRM systems**: operation is similar to the CA system, except the key that is being derived is the content encryption key and is usually delivered to a bulk AES decryption engine. In both cases, generation and derivation of the control word or content encryption key is handled in secure, protected hardware.

rambus.com/cryptofirewall

© Rambus Inc. 1050 Enterprise Way, Suite 700
Sunnyvale, CA 94089 • rambus.com