



intertrust



ENHANCED HARDWARE CONTENT PROTECTION FOR 4K UHD & EARLY WINDOW CONTENT

Copy Protection Technical Group – January 27, 2016

Maximum Security

The maximum security for premium content



ExpressPlay™ DRM cloud system + CryptoFirewall™

Super-encrypted or wrapped keys are combined with a hardware-based device unique key that is only accessible within the CryptoFirewall core contained within the MStar chipset

Industry-leading hardware security core for smart TVs that complies with MovieLabs' requirements for the hardware root-of-trust



Enhanced Content Protection Requirements
UHD HDR early window

ExpressPlay is a full-featured and robust content protection platform for media distribution offering support for Marlin, PlayReady, Widevine and FairPlay DRM



Cloud Service

ExpressPlay Service is a secure cloud-based service that provides an easy to use API and web-based administration.



ExpressPlay SDK

The ExpressPlay SDK is available for iOS, Android, Mac OS X and Windows.



Distribution Modes

ExpressPlay supports media streaming, download-to-play, progressive download and side loading.

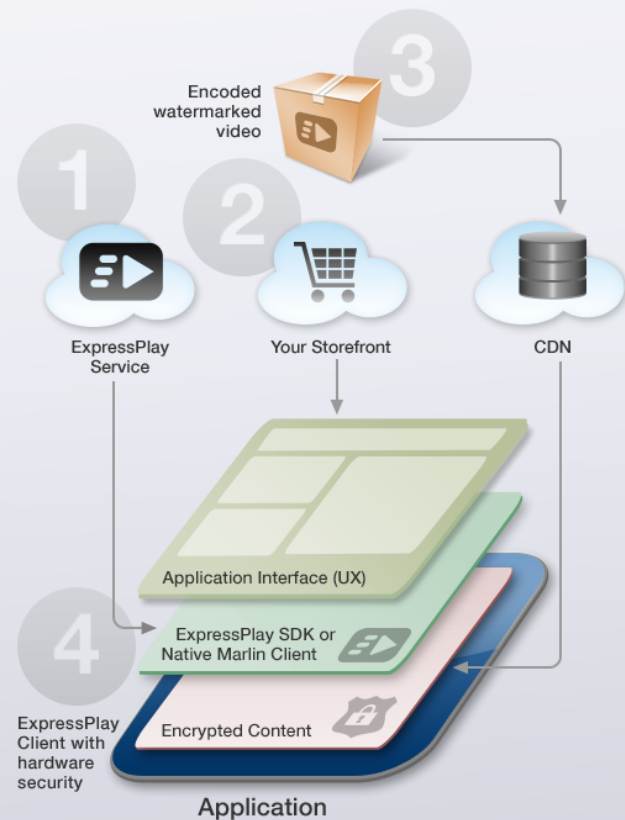


Tamper Resistant

The ExpressPlay SDK is protected by the Cryptanium code and data protection system.

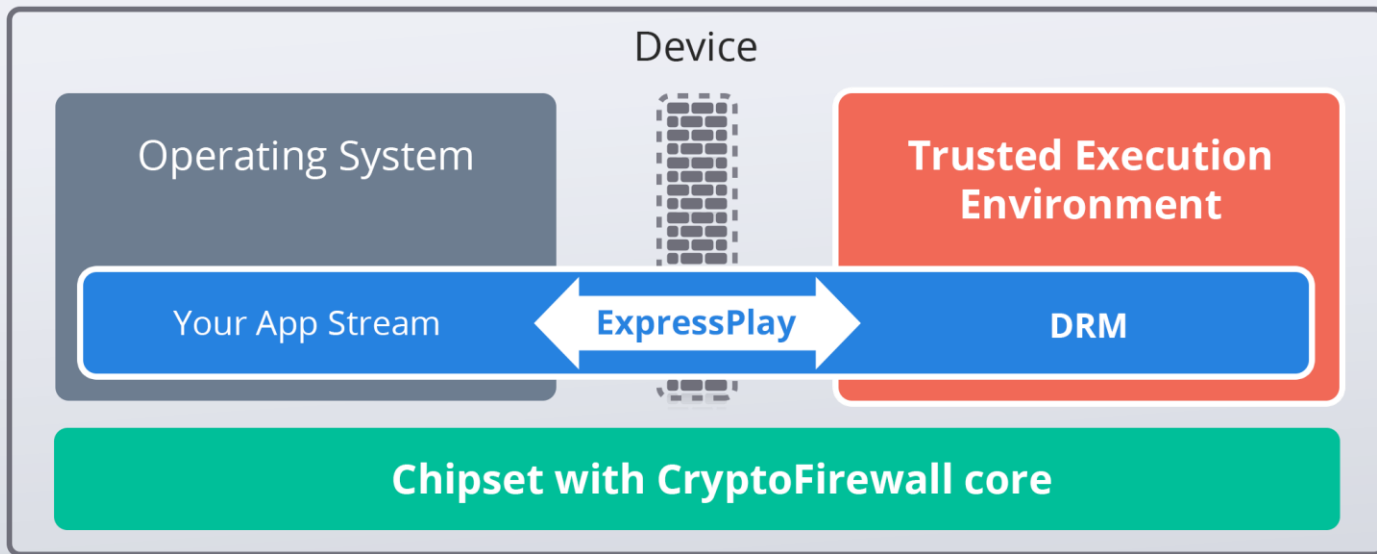
ExpressPlay UHD

ExpressPlay UHD offers service providers an unprecedented level of security by adding a hardware layer on compatible consumer devices



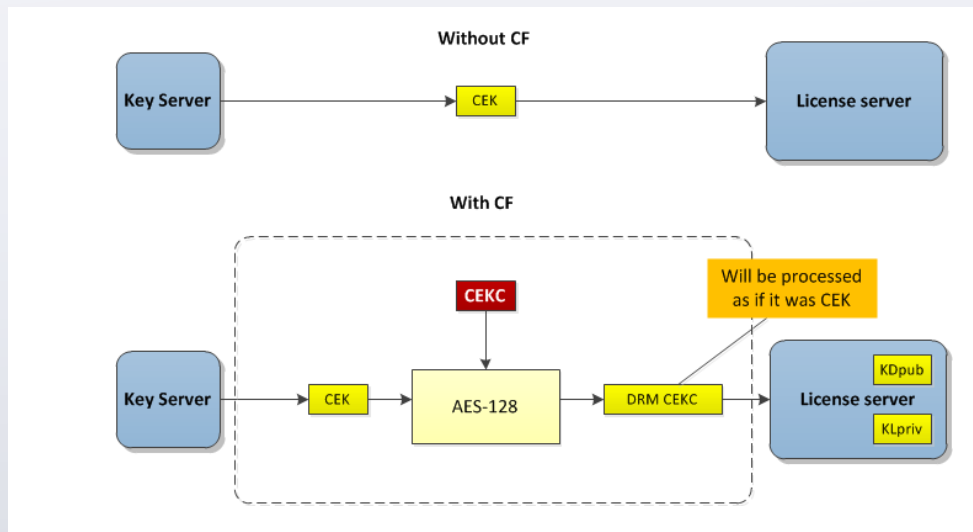
Hardware Root of Trust

CRI's **CryptoFirewall** hardware root of trust
protects content key in secure hardware



Additional Security Layer

Security at the CEK level, not at the public key cryptographic level
Encrypt CEK with CEKC using AES-128: $\text{AES-128}(\text{CEK})_{\text{CEKC}} = \text{DRM_CEKC}$



CryptoFirewall operates below the actual DRM Key Management level as an additional security layer providing hardware resistance

Content Key

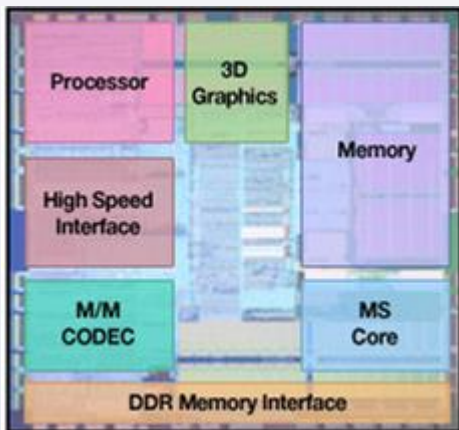
Server side

- The Content Key or CEK is encrypted with the CEKC resulting in the DRM_CEK
- CEKC is unique for each device and provided ahead of time to Intertrust
- DRM_CEK will replace the CEK in the Marlin license information and treated exactly like the CEK
 - e.g., the DRM_CEK will be encrypted in exactly the same way as the CEK.

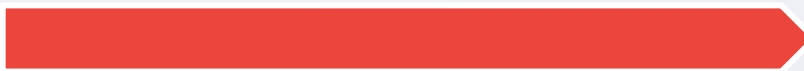
Client side

- DRM_CEK is ingested in the secure hardware of the device
- The CryptoFirewall (CF) core re-creates the CEKC in order to derive the final CEK
- CF is accessed via an API
- Caches to store the Encrypted Rights Key (ERK) and Differentiation Vector (DV) are implemented in the DRM client.

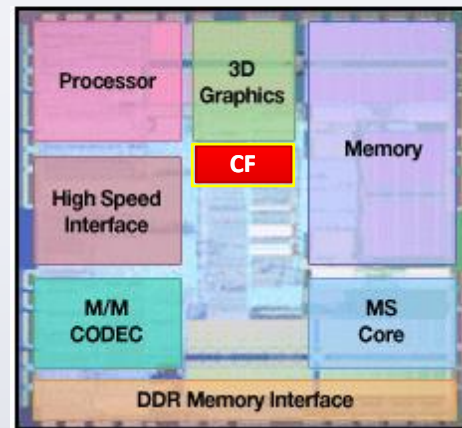
ExpressPlay UHD with CryptoFirewall



Chipset



- During chip manufacturing, each CryptoFirewall core gets a unique identity and set of keys programmed into the OTP memory (this identity is not tied to a specific DRM or operator)
- Once 'in the field', a CryptoFirewall core can be differentiated. A "diff vector" is sent to the CryptoFirewall core via software configuring CryptoFirewall for use with a specific DRM and a specific service provider



Chipset with
CryptoFirewall Core

Strongest Protection

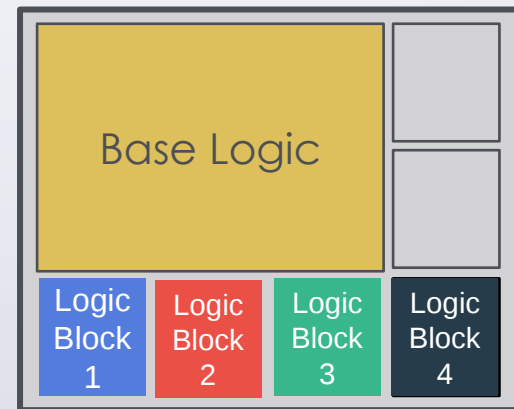
The CryptoFirewall core is designed to prevent the full range of attacks, including:

- Fault injection (glitching)
- Scan interface attacks
- Power analysis (SPA/DPA) and other external monitoring attacks
- Timing attacks
- Emulation
- Manufacturing/personalization facility compromise (insider attack)
- Probing of external buses
- Man-in-middle attacks
- Replay attacks
- Circumvention of security microcontrollers
- Die imaging and probing (e.g., microscopy, laser probing)
- Die modification, focused ion beam attacks
- Tearing and other attacks against NVM writes
- Corruption of nonvolatile memory or fuses
- NVM key extraction
- Key injection
- Algorithm cryptanalysis
- Exhaustive search (brute force)

CryptoFirewall cores are implemented in tamper-resistant secure ASIC hardware

CryptoFirewall Logic Blocs

- Each core is subdivided into distinct logic blocs
- Logic blocs can be assigned to a specific DRM and/or operator
- The assigned logic is cryptographically isolated from other logic blocks
- The CryptoFirewall core provides each distinct security system with its own hardware root of trust
- If there ever is a hack, another logic block within the CryptoFirewall core can be used...hackers have to start all over again, just like with a new smart card

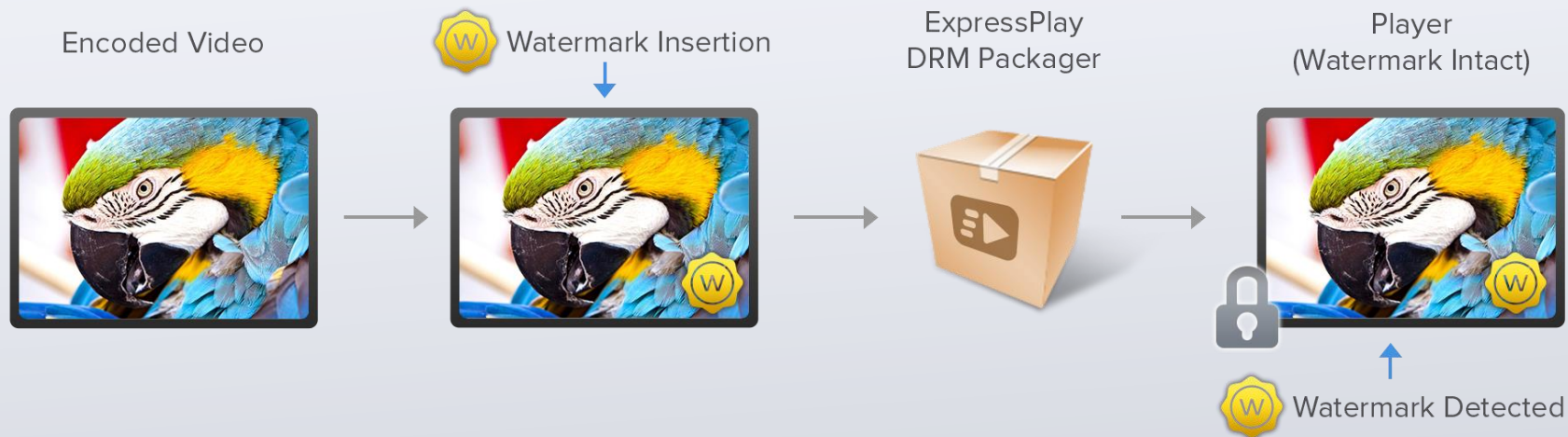


CryptoFirewall Core

ExpressPlay complies with the
HDCP 2.2 encryption standard

by securing the connection between the source and the display to transfer content keys and require a “locality check”

ExpressPlay supports Forensic and Transactional Watermarking



Availability



ExpressPlay with Marlin DRM is integrated with the CryptoFirewall core and is available today on the MStar 4K UHD TV chipset

Current customers
include:

FUNAI

HITACHI

JVC



Panasonic

RCA

SANYO

SHARP

TOSHIBA



MStar has the largest market share of any TV chip manufacturer
(45% worldwide market share)

Thank You

For more information, contact:

cryptofirewall@cryptography.com

info@expressplay.com

contact_taiwan@mstarsemi.com

Demand for premium Ultra HD content is rapidly growing

- 12 Million UHD TV units were shipped in 2014, and sales are expected to hit 100 Million by 2018
- Smart TVs reached 50% market share for the first time in 2014
- UHD TV shipments to exceed 30M in 2015, growing 147% YoY. While overall TV shipments fall 2%. (Source: Futuresource Worldwide TV Market Report)
- UHD TV forecasted to account for 13% of total YV market in 2015, up from 5% last year. (Source: Futuresource Worldwide TV Market Report)
- UHD accounts for 12% of global IP VOD traffic, up from .02% in 2013. Forecasted to account for 22% by 2018 as UHD content continues to grow. (Source: Cisco 2014 VNI Forecast)