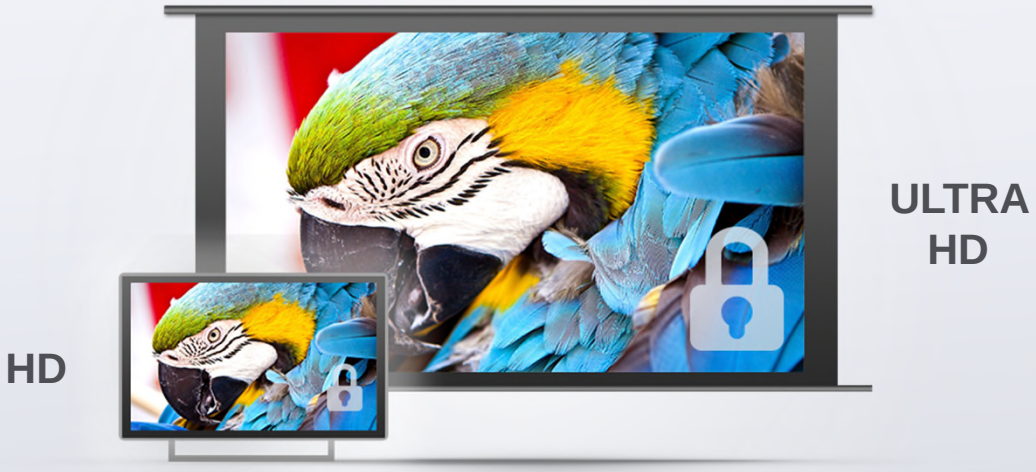
ENHANCED HARDWARE CONTENT PROTECTION FOR ULTRA HD & EARLY WINDOW CONTENT

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 TV chipset

Hollywood Compliant

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

Enhanced Content Protection Requirements

Ultra HD and early window

ExpressPlay

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.

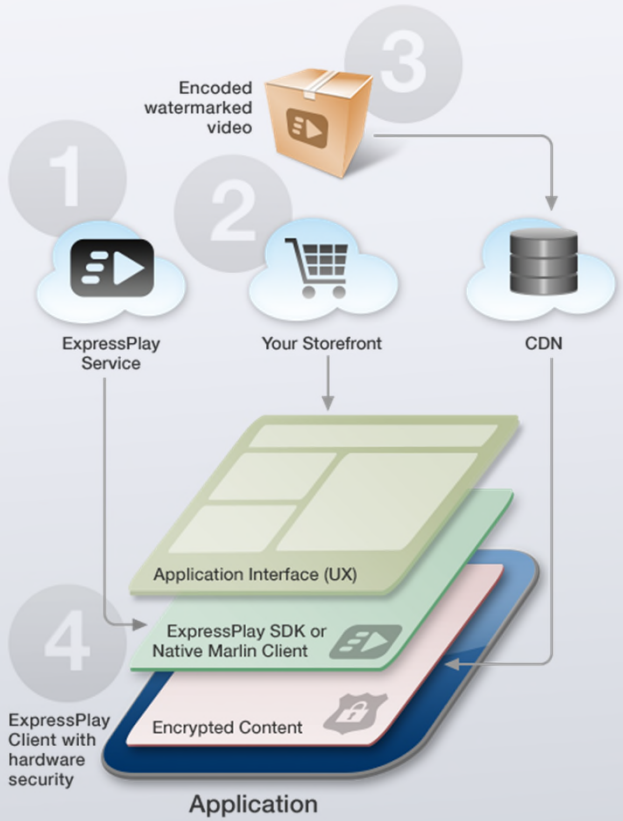
ExpressPlay SDK
The ExpressPlay SDK is available for iOS, Android, Mac OS X and Windows.

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.

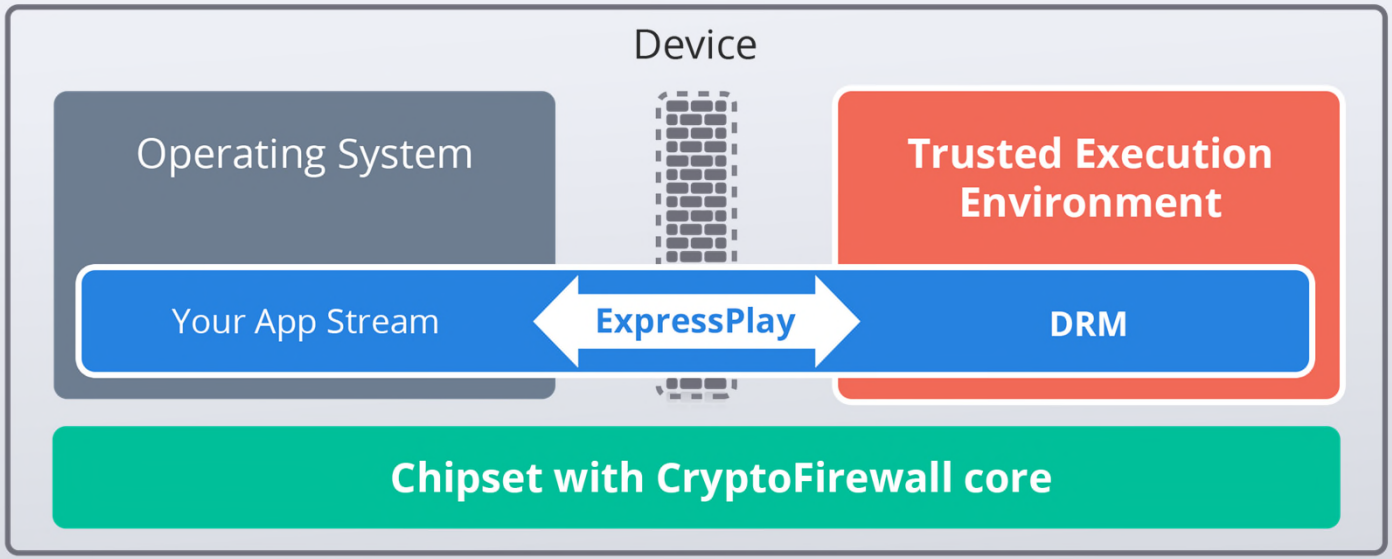
ExpressPlay UHD

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

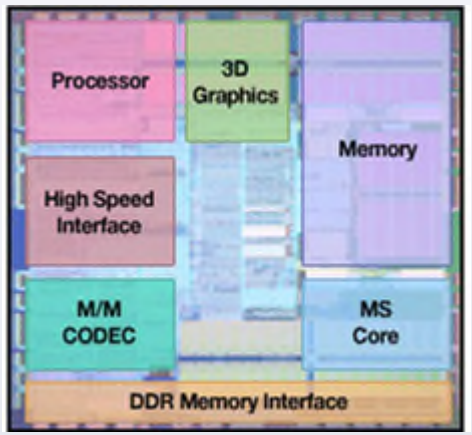


Hardware Root of Trust

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

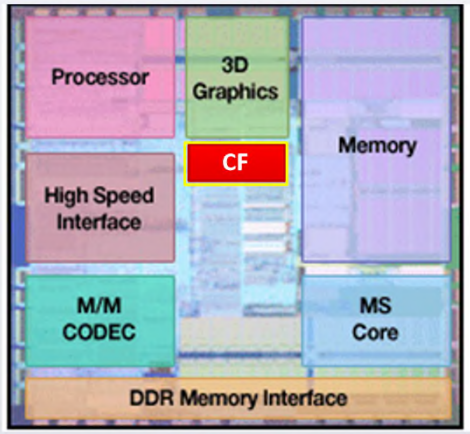


ExpressPlay Ultra HD with CryptoFirewall



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

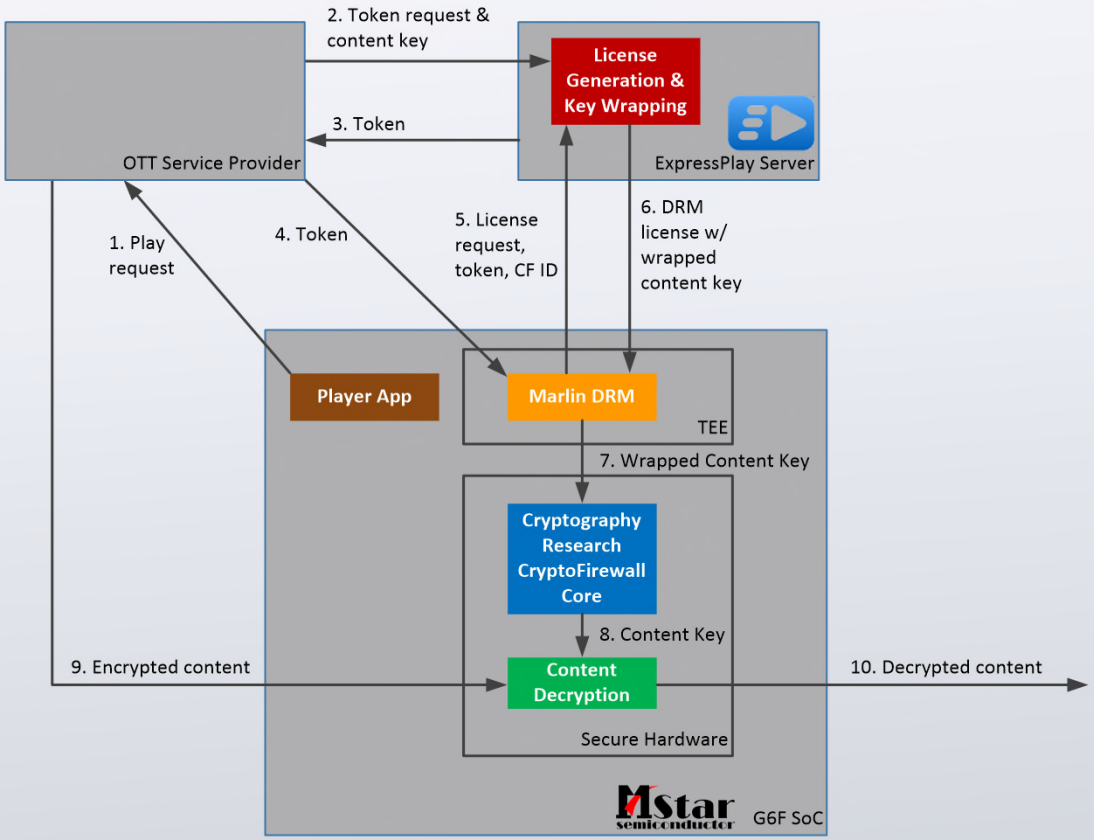
Strongest Protection

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

Overview of integrated security solution

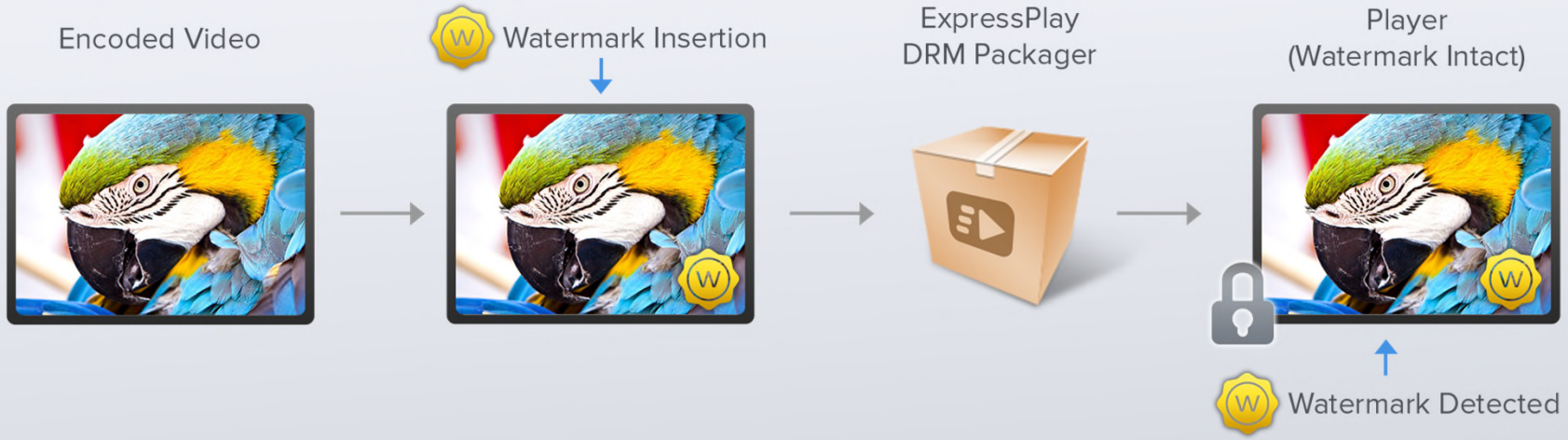


ExpressPlay UHD

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 UHD

ExpressPlay supports **Forensic Watermarking**



Availability

ExpressPlay with Marlin DRM is integrated with the CryptoFirewall core and is available today on the MStar Ultra HD TV chipset

Current customers include:

FUNAI HITACHI JVC

LG Panasonic RCA

SANYO SHARP TOSHIBA

MStar has the largest market share of any TV chip manufacturer

Thank You

For more information, contact:

cryptofirewall@cryptography.com

info@expressplay.com

contact_taiwan@mstarsemi.com