



How UHD Changes Revenue Security Landscape

November 2014

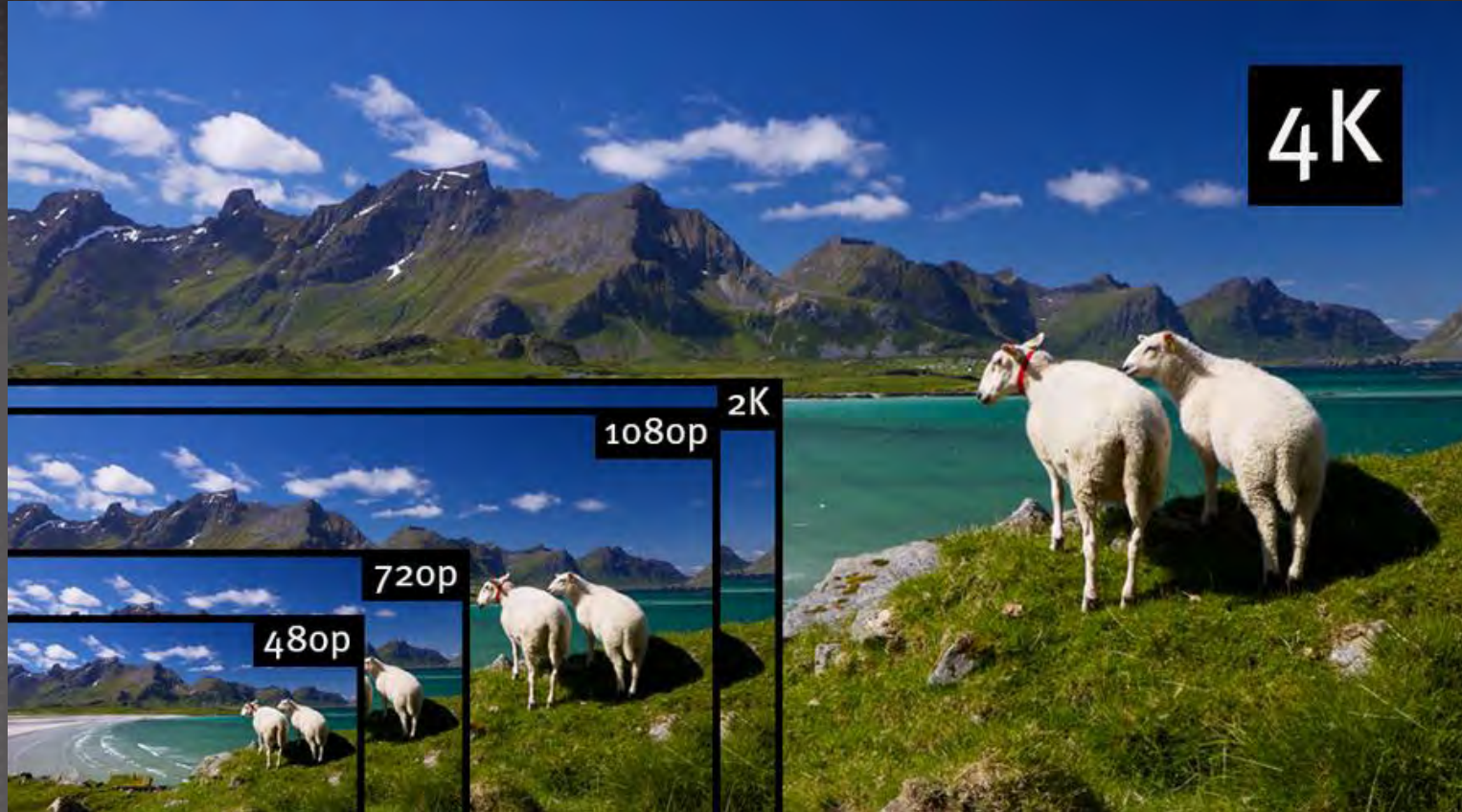


Background



- ❑ The pay-TV market is in the early stages of planning and deploying support for ultra high-definition (UHD) or “4K” content
- ❑ UHD content will be high-value premium programming, necessitating the highest level of protection
- ❑ As a market leader in pay-TV security, Verimatrix will fully support deployment of UHD pay-TV services and will ensure that our customers have access to the highest value studio content
- ❑ This presentation provides an overview of the security requirements for UHD content and the application of the VCAS solution for UHD service security

What Does 4K/UHD Mean?



4K

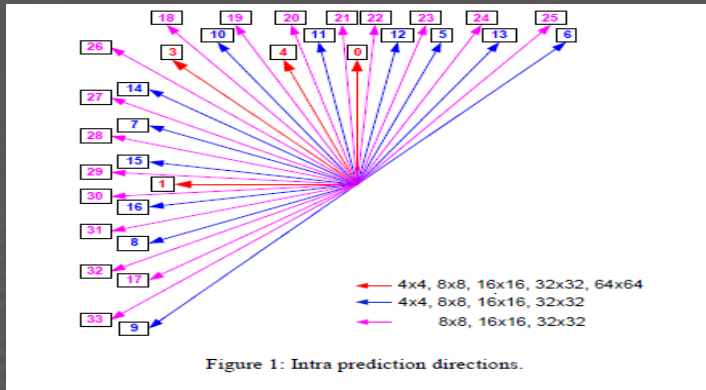
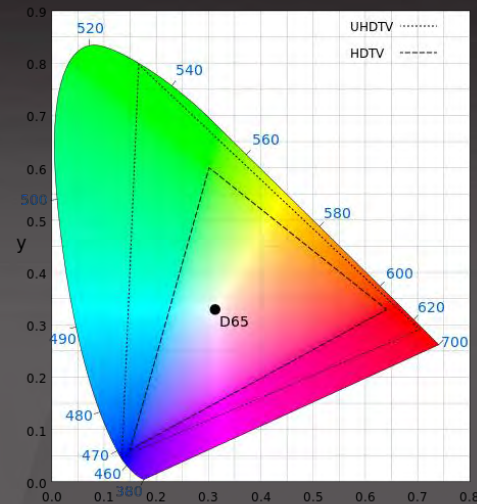
- ITU (Rec 2020) defines Ultra HD (UHD) as:
- 3840x2160 pixels
 - 16x9 format
 - Progressive scan only

Beyond More Pixels....

Richer color space:

10 or 12 bit color depth

Color space rendition far beyond that of HD



Increased encoding sophistication:

35 intra prediction directions in HEVC vs. 9 in H.264
50% bit-rate saving for H.265/HEVC vs H.264

Note – reference data courtesy of Elemental



UHD Security Requirements

4K/UHD – New Security Requirements

MovieLabs Specification Background



- ❑ Hollywood studios see 4K/UHD as their next opportunity to redefine security requirements for content protection
- ❑ When HD came out, the studios defined AACSS but it failed over time
- ❑ With UHD, the studios have defined broad requirements and will let the market develop the best content protection solutions
- ❑ Specs published as:
<http://www.movielabs.org/ngvideo/index.html>

Note that the specification is intended as a guide, with adherence to be decided independently by each studio

Threats

1. Availability and Distribution of Ripping Software
 - “hack one, hack all”
 - Breaking protection on one device, breaks it on a wide class of devices
2. Release Day Availability of Rips
 - Ripping a new release requires no additional information or technology than ripping a previous one.
3. Pre-Release Day Availability of Rips
 - Leaks in the supply chain
4. Output Capture
 - Secure video path
 - Output protection
 - Camcording

Cryptography

- 1. State of the art cryptography (e.g. AES128)**
 - Used by IPTV and OTT today, DVB moving to CSA3
- 2. Side channel attack resistance**
 - Mainly SoC feature
- 3. True Random Number Generation (TRNG)**
 - Most SoCs support today

HW Root of Trust

- 1. Secure chain of trust for trusted applications**
 - Must be securely provisioned (e.g. burned in factory)
 - Most SoCs support it today
- 2. Device-unique private key for protecting stored secrets**
 - Securely provisioned (e.g. Blackbox in factory)
 - Used to Identify and Authenticate device
 - Used to bind content to host or storage

Secure Computing Environment



- 1. Only authenticated code performs critical operations**
 - ❑ Supported via secure boot
 - ❑ Support for TrustZone/TEE or security processor
- 2. Secure OS, HW isolation mechanism for trusted code**
 - ❑ Supported via TrustZone/TEE, security processor, etc.
- 3. Memory protection**
 - ❑ Supported via SoC memory scrambling
 - ❑ Supported via TrustZone/TEE on-chip memory
- 4. Run-time integrity checks for secure applications**
 - ❑ Supported via TrustZone/TEE or security processor

Connectivity

- 1. License key delivery at a specified date (e.g. “street date”)**
 - ❑ Deliver content keys just-in-time and independent of movie file delivery
- 2. Copy/move mechanism using on-line key delivery**
 - ❑ DVR does not stores content keys – they are delivered on-line when needed; same process for copying
 - ❑ DVR re-encrypts content using local HW keys

Hack Containment

1. Key binding to device

- Content key protected by a unique SoC key
- Unique Device Certificate in TEE

2. SW diversity

- SW attacks should not be portable
- Vary by SW version, by Platform and by individual Installation

3. Title diversity

- Breach of one title does not make another title automatically available
- Each title is protected differently; mainly for optical media
- Custom Trusted Application (TA) in TEE/security processor

Revocation and Renewal

- 1. Revoke and renew versions of clients**
 - Support SW and TA upgrades
- 2. Revoke and renew code signatures of the root of trust chain**
 - Prevent SW version rollbacks and enforce server side checks
- 3. Revoke an individual device or a class of devices**
 - Revoke a device certificate
 - De-entitle an individual client
- 4. Proactive SW updates**
 - Upgrade client SW periodically or as a response to a breach

Secure Media Path and Output Control



1. Protect DRM keys and secrets

- SoC One-Time Programmable memory and/or TEE

2. Protect compressed video

- No access to video by non-authorized component; a.k.a. Secure Video Path

3. Protect decompressed video

- Secure Video Path; SoC feature

4. HDCP 2.2 or higher

- Signal minimum HDCP version

Watermarking

1. Forensic watermark

- ❑ Secure forensic marking on client or on server
 - ❑ Verimatrix VideoMark or StreamMark
- ❑ Robust against forensic information corruption
- ❑ Watermark must be guaranteed even on compromised devices

2. Playback watermark

- ❑ Detect Cinavia watermark (used in Digital Cinema)
 - ❑ Responsibility of the decoder/SoC

1. Certification by 3rd party and Trusted Implementers

- Merdan, Farncombe, etc.

2. Code signing keys not released until device certification is complete

- CA/DRM vendor typically owns signing keys and certifies STB implementations

3. Active breach monitoring

- IPTV clone detection
- Monitor the market, hacker websites, etc.
- Watermark extraction process (VideoMark Reveal)

4. Agreements must include rapid response provisions

- Turn on countermeasures at run-time as a response to a breach
- Download a new CAS client or a DRM TA as a response to a breach



Thank You!

info@verimatrix.com