Technology Presentation

DSTAC WG4 Face-to-Face Meeting
June 19, 2015

SONY

What is Passage?

A Sony derived method to allow for the simultaneous delivery of multiple DRM or CA encrypted content using the techniques of 1) selective multiple encryption of critical packets in a video stream, and 2) packet swapping

Passage is not a security system in and of itself. It is an enabler for overlaying one security system on top of another system. It is especially useful when Simulcrypt (key sharing between security systems) may not be possible or desirable.

SONY

What is selective multiple encryption?

A small amount of critical data, essential for decompressing digital media content, is duplicated and encrypted two different ways - DRM or CA.

Non-critical data is left unencrypted. Each device receives the same transport stream, selecting its respective encrypted data and sharing the remaining common content.

SONY

What is Packet Swapping?

A method for exchanging a primary digital content packet for an alternate digital content packet in a structured stream.

With Passage, it is the mere presence of the alternate packet that signals the deletion of the next primary packet. The end device can decrypt the alternate packet based on the appropriate CA or DRM.

SONY

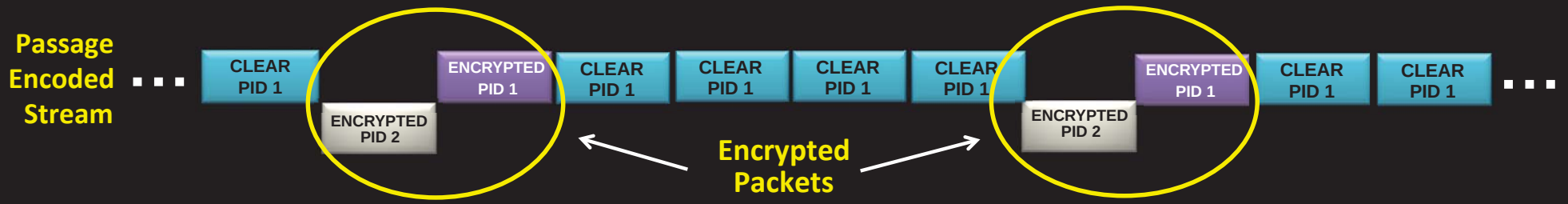
What is End to End DRM?

A method for ensuring the delivery of content rights established by the MVPD to the retail device as a replacement of legacy Copy Control Information (CCI) bits.

Allows for delivering advanced business and usage rules for expanded use cases. DRM can be used along with DTCP-IP and Whitelists for certain use cases.

Selective Multiple Encryption and Packet Swapping

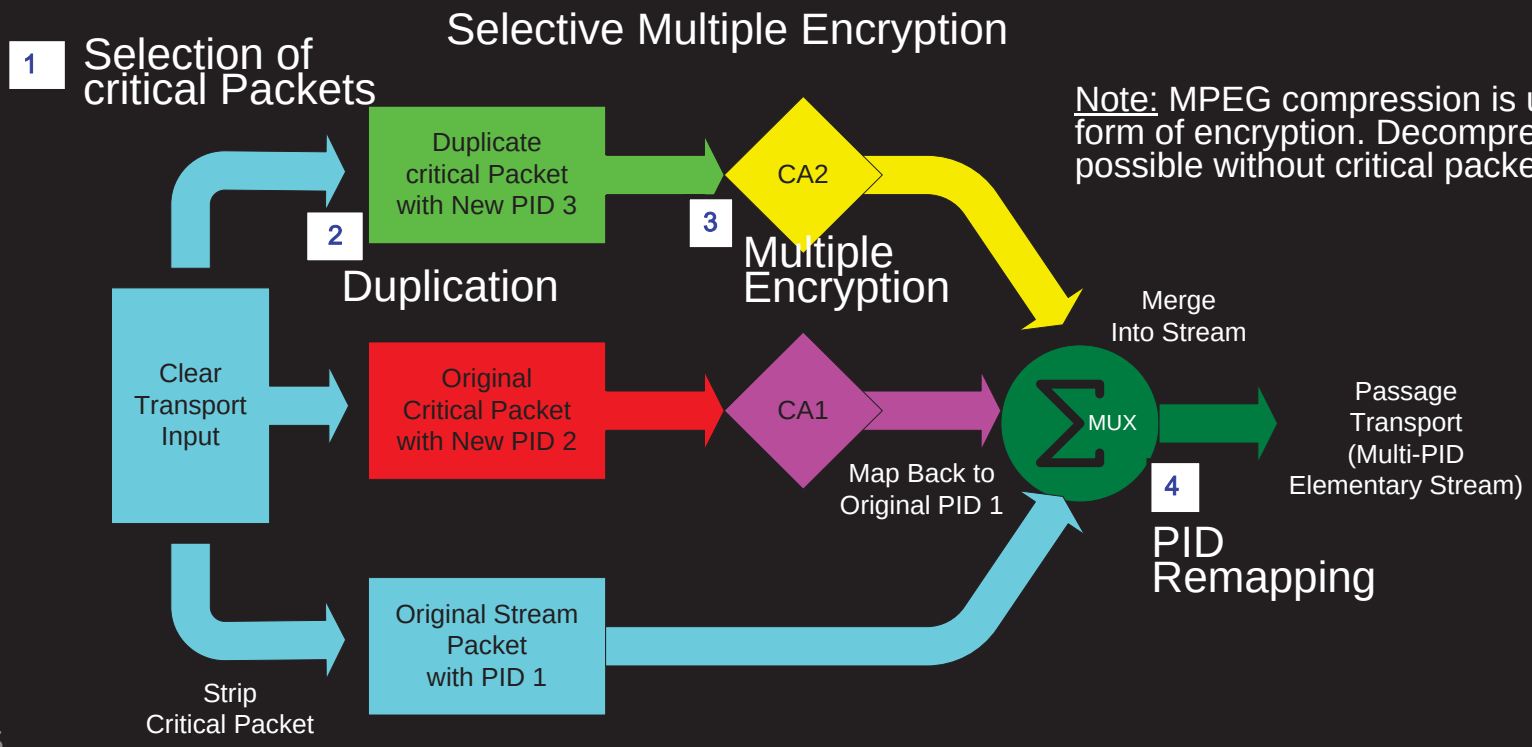
Selective Multiple Encryption: At the content distribution source, a small amount of critical data, essential for decompressing content is duplicated and encrypted at least two ways



Packet Swapping: Each device receives the same stream, selects its respective encrypted data and shares the remaining common content sent in the clear. “Packet swapping” is used to exchange the legacy CA packet for the alternately encrypted CA or DRM packet

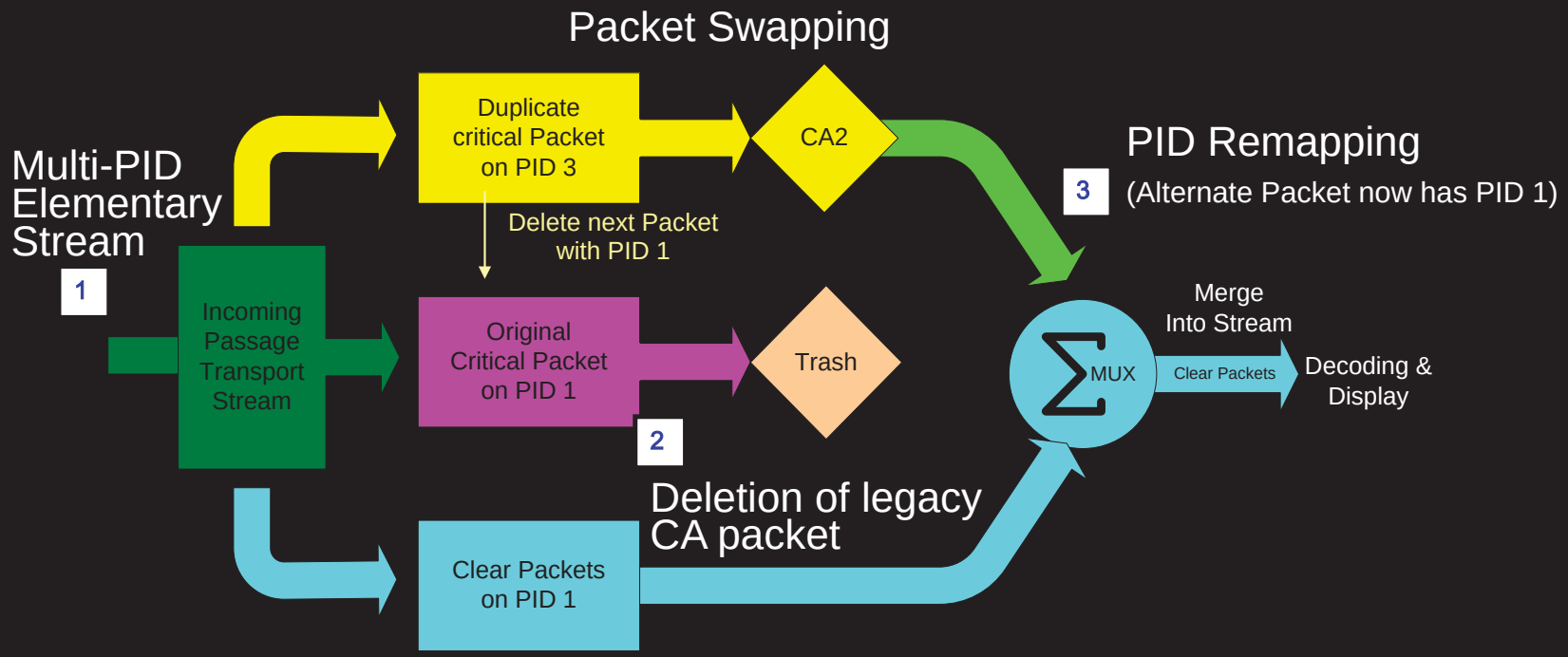
Passage Source Encoding: 4 Basic Techniques

1. Selection of critical packets (headers, etc.)
2. Duplication of selected packets
3. Multiple encryption of duplicated packets
4. Packet Identifier (PID) remapping



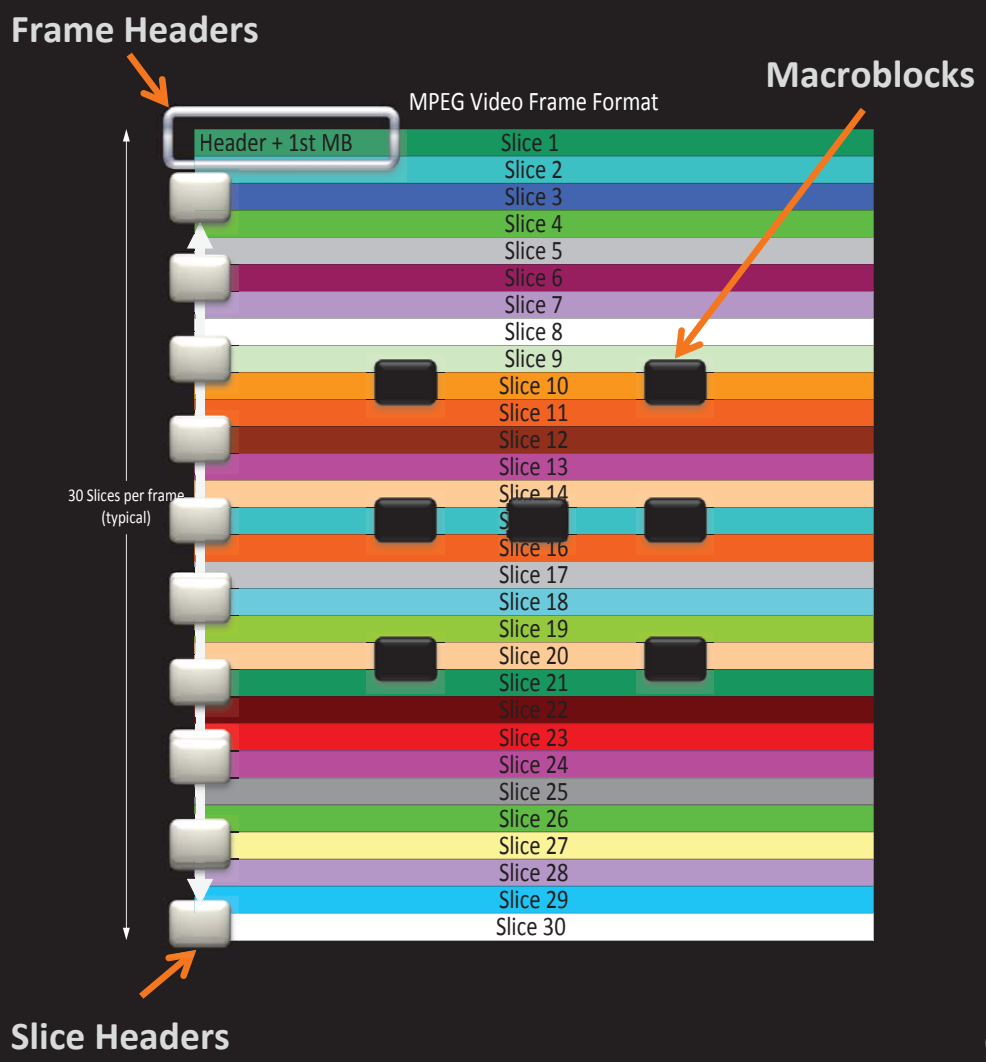
Passage Device Decoding: Three Basic Techniques

1. Receipt of structured, multi-PID elementary stream
2. Receive the alternate PID and delete the next legacy PID packet
   - Device parses Program Map Table to learn secondary PID
3. Decryption before Remapping of packet

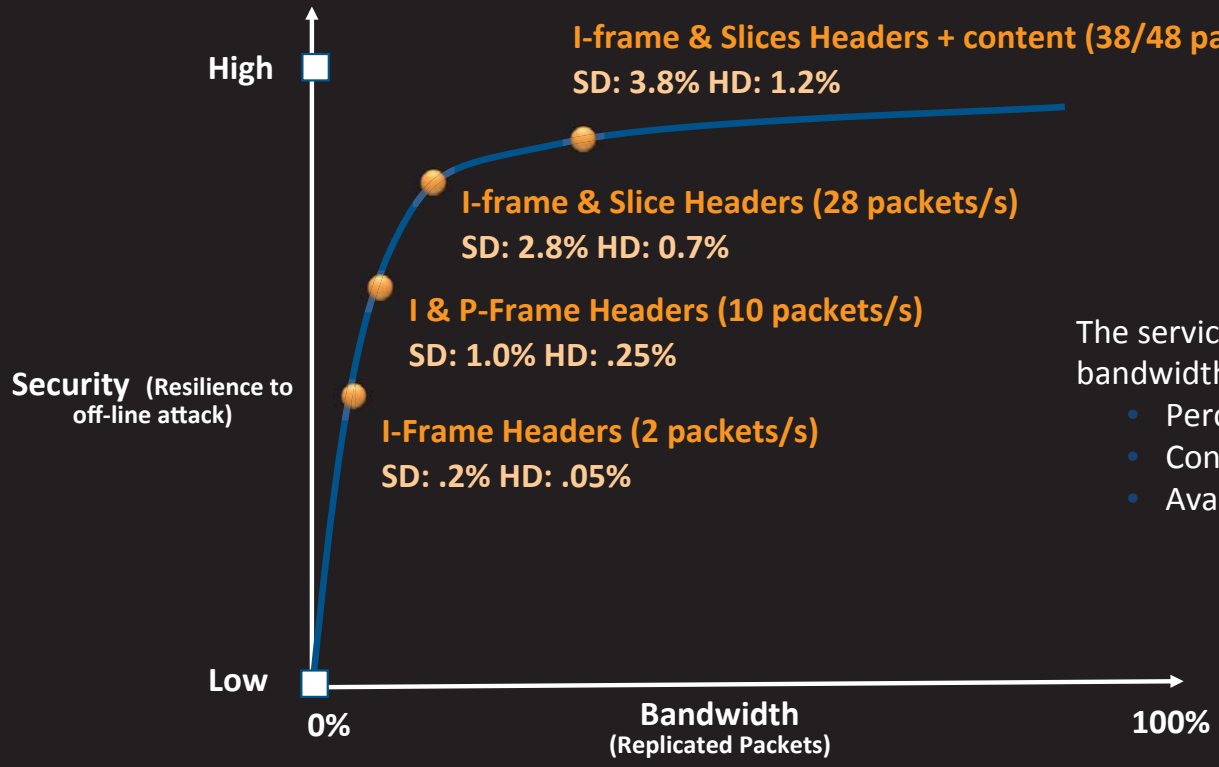


Critical Data

- Passage has various levels of security. Each uses different combinations of critical packets containing Sequence, GOP, Picture and Slice headers as well as individual macroblocks
- Passage has been approved by Merdan Associates and Sarnoff Laboratories – reports are available under NDA
- Selective encryption in the market:
  - Apple MPEG2 HTTP Live Streaming uses less than 10 % encryption using “skip encryption” without inspection of the compression. It enables decryption in software
  - Cisco CA Overlay uses 2.5%



Passage Bandwidth Usage



The service provider chooses the ***Passage*** bandwidth to use based upon:

- Perceived value of content
- Content provider requirements
- Available transport bandwidth

- No significant increase in robustness against offline (PVR) theft is gained when the total ***Passage*** replicated packet BW exceeds 3.8% SD 1.2% HD AVC
- Even the lowest level of ***Passage*** application provides complete coverage from real-time, casual theft of service from STBs

End-to-End DRM

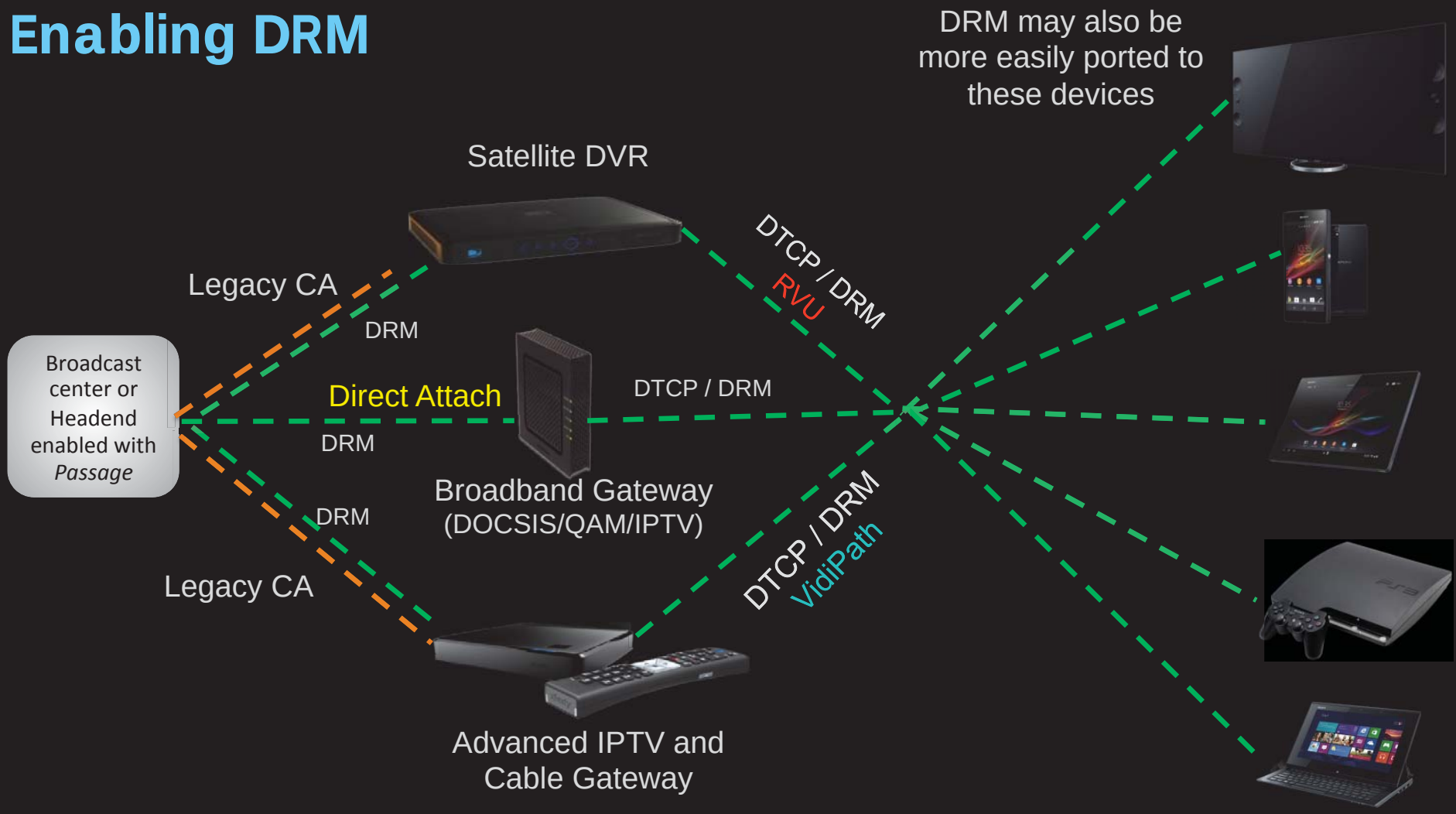
Content Distribution Sources:

- Back-haul Delivery Networks
  - Comcast Wholesale: HITS and Fiber
- Direct from Programmers
- Local content

Implementing Passage at a centralized location - at the point of distribution - means that NO NEW EQUIPMENT is needed at the headends except for locally generated content. Content rights can be distributed as part of DRM metadata at that of point of distribution

Multiple headend configurations are supported were existing equipment can be utilized – Only normal functions such as PID filtering, PID remapping, and packet encryption and re-encryption are needed

Enabling DRM



Use Cases

- Passage eliminates the need to support legacy CA in new devices for linear content
  - Since the alternate critical packets are encrypted independently, there is no dependency on the legacy CA vendor for know-how
    - No licensing is required for the legacy decryption algorithm (such as Initialization Vectors)
    - No secrets are shared as the legacy encrypted packet is not touched. The security of the installed base of set-top boxes is not put at risk!
    - Security Indemnity by the legacy CA vendor should not be an issue
  - CableCARD uses 2 Copy Control Information (CCI) bits with DFAST copy protection across the interface from the module to the host device
  - CAS-to-Copy protection bridging, e.g. DFAST , DTCP, etc. has limited usage rights:

    Copy Free, Copy Once, Copy Never, and Copy No More

Use Cases

- DRM enables rich rights expression and new use cases, new business opportunities and models
  - Persistent MVPD control over DRM encrypted content could enable ways to upsell to customers, to super-distribute content to peers, and create unique pairings of VOD-to-subscription business models

- DRM functionality might be more easily supported by both “Direct Attach” devices and home network devices, e.g. using DLNA VidiPath or RVU than legacy CA

SONY

Passage Overhead

- Requires a small amount of additional bandwidth for duplicated packets(.2 - 1%)
- Enabling a device for Passage requires modification of the parsing of Program Map Table (PMT) table to 1) signal the secondary CA Entitlement Control Message (ECM) Packet Identifier (PID) - similar to Simulcrypt- and 2) signal the secondary packet PID
- Many decoder ICs support Passage packet swapping, however, if not, then the transport processor embedded firmware (inside the decoder IC) needs to be upgraded. Packet swapping may also be done entirely in software by main CPU.
- Depending on the headend configuration, as with Simulcrypt, the plant may require additional control computers for the DRM security system (although most can be remotely deployed) , and Passage may require reconfiguration of exiting stream groomers and multiplexers

Passage Benefits

- Solution for broadcast linear streams, it allows for DRM interoperability with legacy CA
- Enables new use cases and devices based on new DRM rights expression
- DRM agnostic
- Unlike Simulcrypt, there is no dependency on the legacy CA vendor
- Uses modern AES-128 instead of CBC-DES with secret IVs which may be more conducive to software DRM implementations
- Legacy devices are completely unaffected
- Secure, proven technology with equipment, set-top box & chip support
- With a national roll-out and implementation at content distribution, headends would minimal changes (existing mux, stream groomer may be used)


SONY
Thank you