Passage at Content Distribution And End-to-End DRM

for DSTAC

March 14, 2015

Brant Candelore
Passage Architect / Security Specialist / Sr. Staff Member
UX Technology Center – San Diego
Sony Electronics Inc.
What is Passage

See Classic “Passage Technical Overview” PowerPoint presentation

Passage is an enabler - for new distribution paradigms - all while preserving the operators’ capital investment in legacy set-top boxes and distribution equipment!

Why Passage

a) Alternate scrambling of the critical packets, e.g. AES-128 vs. DES or CSA

b) Legacy CA can co-exist new CA or DRM
   - Alternate security (software vs. hardware-based CAS)
   - Alternative key management (content rights vs. entitlements)
   - Alternative Root of Trust (Crypto vs. Key Ladder vs. Software)
   - Alternative to key sharing (Simultcrypt) which may not be possible or desirable

Result: Linear content can be encrypted with DRM same as Web services which might help the transition to “all-IP” services
<table>
<thead>
<tr>
<th>Scenario</th>
<th>Encryption 1</th>
<th>Encryption 2</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Legacy CA</td>
<td>Alternate CA</td>
<td>“Classic” Passage</td>
</tr>
<tr>
<td>2</td>
<td>Legacy CA</td>
<td>DRM</td>
<td>End-to-End DRM</td>
</tr>
<tr>
<td>3</td>
<td>DRM</td>
<td>DRM</td>
<td>Multicast IP with independent keys</td>
</tr>
</tbody>
</table>
Enabling Sony Passage at the Point of Content Distribution

- Potential to facilitate Passage throughout content distribution ecosystem
Content Distribution

Content is currently delivered in the following ways to headends:

a) Back-haul Delivery Networks, e.g. Comcast Wholesale: HITS and Fiber
   - Networks get content from Programmers
b) Direct from Programmers
c) Local content

Methods a) and b) can benefit from doing Passage at the point of distribution. Existing headend equipment can be utilized. If Programmers, Method b) enabled Passage, then a) might accommodated. See following “Commercial Distribution” slides

c) must be Passage-encoded locally

There are a number of different types of headend systems which must be considered.

a) Digital Turnaround
b) Local Encryption (no Passage)
c) Remote Encryption (no Passage)
d) Local and Remote Encryption

All can be accommodated!
Commercial Distribution Scenario using Passage (3 Critical Packets)

**Step 1**
- **Harmonic**
- Packet Select, Dup x 2
- Critical 1 & 2, Alt
- PID Remapping
- Non-critical, Critical 1
- Encryption
  - Alt Critical

**Step 2**
- **Motorola**
- Encryption
  - Critical 2

**Step 3**
- **Harmonic**
  - Copy
  - Critical 2 to Critical 1
  - PID Remapping
  - Non-critical, Critical 1

**Headend**
- **Any IRD**
- Simply pass through

**Legend:**
*Critical Packet

Required for local re-encryption with Passage (Scenario D). # of Critical 2 packets do not need to match Critical 1 packets. Critical 2 could be I-Frame headers, while Critical 1, all Frame headers. Packet precludes need for double pass in Scenario D (see slide 5).

Ensures that all existing system will work without any changes whatsoever.
Sony Electronics Inc.
Confidential and Proprietary

Commercial Distribution Scenario using Passage (2 Critical Packets)

**Legend:**
*Critical Packet

---

**Step 1:**
- Harmonic
  - Packet Select, Dup
  - Critical, Alt Critical
  - PID Remapping
  - Non-critical
  - Encryption
  - Alt Critical

**Step 2:**
- Motorola
  - PID Encryption
  - Critical

**Step 3:**
- Harmonic
  - PID Remapping
  - Non-critical

**Step 1:**
- Any IRD
  - Simply Pass-through

**Step 2:**
- Motorola or DVB IRD (Passage)
  - Decrypt (Legacy CA IRD)
  - Critical 1
  - or
  - Passage and Decrypt (DVB IRD)
  - Alt Critical

**Step 3:**
- Harmonic
  - CA Decryption
  - Critical
  - or
  - Encrypted Critical

**Scenario requires 2 passes through Harmonic Equipment**

- Local Encryption
  - No Passage
  - Legacy CA or Alt CA

- Remote Encryption
  - No Passage
  - Alt CA

- HITS to Home
  - Remote Encryption
  - Passage System
  - Motorola, Alt CA

- SEM or Harmonic
  - Critical, Non-Critical

- Fiber or Satellite

---

Ensures that all existing system will work without any changes whatsoever
End-to-End DRM

- Treating linear content like IP-delivered DRM content
End-to-End DRM

- Capitalize on high quality linear content sent to legacy receivers
  - Customer buys inexpensive QAM tuner cards or QAM tuner USB stick

- Eliminate the need for CAS-to-DRM bridging. Bridging has the following issues:
  - OCUR/BOCUR solutions using CAS, e.g. CableCARD, are expensive
  - Rights and access criteria may be lost in “translation” using DTCP/IP and DLNA
  - Possible clear content or key trans-encryption exposure vulnerability

- DRM content (sent from linear programming) can be managed in the same way as that delivered strictly over IP

- Provides greater control over broadcast content

- Enables new business opportunities and models

- DRM packet could originate at Programmer Passage-enable facility. This minimizes the multiplexer changes at Distribution Networks and Headends
End-to-End DRM – To PC

Headend Scenarios
Selective Multiple Encryption

<table>
<thead>
<tr>
<th>CLEAR</th>
<th>LEGACY</th>
<th>WMDRM</th>
<th>Widevine</th>
</tr>
</thead>
<tbody>
<tr>
<td>not-encrypted PID 100</td>
<td>Critical CA encrypted PID 100</td>
<td>Critical encrypted PID 101</td>
<td>Critical encrypted PID 102</td>
</tr>
</tbody>
</table>

Storage & Distribution Scenarios

<table>
<thead>
<tr>
<th>CLEAR</th>
<th>Widevine</th>
</tr>
</thead>
<tbody>
<tr>
<td>not-encrypted PID 100</td>
<td>Critical encrypted PID 100</td>
</tr>
</tbody>
</table>

IP Distribution in the home, e.g. MOCA or Wi-Fi

- **AverMedia PCI CARD**
  - Clear QAM tuner to USB
- **Hauppauge 950Q USB2 QAM Tuner**
  - Clear QAM tuner to USB
- **SiliconDust Homerun Tuner**
  - Clear QAM tuner to IP

Direct reception by PC using existing PCI tuner board (decoding done by multi-core PC)
- No need for CA decryption and re-encryption
- Passage can be managed by client on PC, TV, or Tablet

PC browsing of MSO content

**AverMedia PCI CARD**
Clear QAM tuner to USB

**Hauppauge 950Q USB2 QAM Tuner**
Clear QAM tuner to USB

**SiliconDust Homerun Tuner**
Clear QAM tuner to IP

Direct reception by PC using existing PCI tuner board (decoding done by multi-core PC)
- No need for CA decryption and re-encryption
- Passage can be managed by client on PC, TV, or Tablet
SONY

End-to-End DRM

CA

DRM

TiVo Retail STB

PS4

Desktop PC

TV

SiliconDust

End-to-End DRM

Headend w/Passage

Arris or Cisco STB

CA

DRM

PS4

Desktop PC

TV

SiliconDust

Laptop

Tablets

Smart Phone

Wireless Router

Wireless Devices