BKK16-201 - PlayReady OPTEE Integration with Secure Video Path

Presented by
Zoltan Kuscsik, PhD

Date
BKK16-201 March 8, 2016

Event
Linaro Connect BKK16
Overview

The solution presented here integrates the following key components:

- W3C EME Working Draft
- Microsoft® PlayReady® DRM Porting Kit v3.0
- OP-TEE OS
- OpenCDM/OpenCDMI
- Chromium v45
Updates since SFO15

- Secure Data Path with OP TEE/Playready proof of concept on STM B2120 in progress.
- Secure Memory Allocator Framework (SMAF) integration - work in progress.
- EME with OP TEE on Hikey. We got Wayland/Chromium finally working!
- Moving to 4.5 Kernel and OP TEE master.
- AES OCDMI publicly available.
- Complete Playready TA implementation. We now support the Playready Interface For TEE (PRiTEE).
Supported boards

STM B2120

96boards - HiKey
Encrypted Media Extensions - Buffer decrypt

1. **Browser**
   - New session request

2. **CDM**
   - Load TA / Init Session
   - Send License Request
   - Update License
   - Update available keys
   - Allocate and Secure buffer using SMAF
   - Decrypt Buffer

3. **PlayReadyTA**
   - Key

4. **Secure Buffer**
   - Decrypt

5. **Encrypted Buf**
EME SW stack - what can be open?

- Chromium
- Android Framework
- OCDM
- Widevine PPAPI CDM
- DRM HAL
- PlayReady CDMI
- ClearKey CDMI
- Linux Kernel
- SMAF
- OPTEE Kernel Driver
- Playready TA
- HDCP TA
- ClearKey TA
- SMAF TA
- Policy Manager (?)
- OP TEE OS
- TEE

Closed Source
Open Source
Secure Memory Allocation Framework - CMA Allocator
Secure Memory Allocation Framework

Step 1: Allocate

Step 2: Request "set mem secure"

Step 3: Set memory secure
Secure Data Path
PlayReady has a CDMi interface as part of the PlayReady’s DRM Licensed product. This CDMi component provided is very close to the one that is required by the open source OpenCDMi project.

The Linaro secure media solution is an end-to-end DRM solution with a PlayReady license server. The client receives PlayReady encrypted content and communicates with a PlayReady server to request and receive a license and keys required to decrypt the content. The licence request is generated by PlayReady encapsulated by the CDMi, passed up to the to HTML5 application which initiates the licence acquisition from the Playready license servers.
Open CDM

The OpenCDM uses the platform's native RPC system to separate the CDM from the browser. The project has two main components:

1) A browser specific CDM integration layer and the communication interfaces for the CDM.

2) A CDMI service implementation.
## Implementation overview

<table>
<thead>
<tr>
<th>Feature</th>
<th>Chromium External Clear Key</th>
<th>Linaro Clear Key CDM with SSL</th>
<th>Linaro Clear Key CDM with OPTEE</th>
<th>Linaro CDM with TEE</th>
<th>Linaro CDM with software Playready</th>
<th>Linaro CDM with HW Playready</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPAPI CDM</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>OpenCDM</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>OP TEE and TrustZone®</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>PlayReady, other DRM support</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Compatibility</td>
<td>ARMv7, ARMv8, x86</td>
<td>ARMv7, ARMv8, x86</td>
<td>ARMv7, ARMv8</td>
<td>ARMv7, ARMv8</td>
<td>ARMv7, ARMV8</td>
<td>ARMv7, ARMV8</td>
</tr>
<tr>
<td>HiKey</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (in development)</td>
</tr>
<tr>
<td>Dragonboard</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
OpenSSL ClearKey CDM

- Works both on X86 and ARM Linux.
- Allows the testing and exercising the Open CDM implementation:
  
  https://github.com/linaro-home/open-content-decryption-module-cdmi

- Upstreamed to OpenCDM project
OP TEE ClearKey CDMI

- Needs OPTEE enabled HW with Chromium running
- ClearKey AES128 decryption in OP TEE:
  
  https://github.com/kuscsik/optee-clearkey-cdmi

- Works with upstream OCDM
Links

- OP TEE
  https://github.com/OP-TEE/optee_os
- Linaro OpenCDM
  https://github.com/kuscsik/linaro-cdmi