SFO15-205: OP-TEE Content Decryption with Microsoft PlayReady on ARM TrustZone
Introduction

Open source Linux project utilizing ARM TrustZone(R) for developing trusted applications. The project is maintained by Linaro and STMicroelectronics. OP TEE is compliant with the Global Platforms API specifications.

OP TEE OS:
https://github.com/OP-TEE/optee_os

OP TEE Client:
https://github.com/OP-TEE/optee_client

OP TEE Linux driver:
https://github.com/OP-TEE/optee_linuxdriver

Open CDM:
https://github.com/fraunhoferfokus/open-content-decryption-module
What is OP TEE?

Linux
- Linux Native App

OP TEE Client
- Global Platform TEE API
- TEE Supplicant
- OP TEE Linux Driver
- Storage

TrustZone / OP TEE OS
- Trusted App (DRM)
- OP TEE OS
- Secure Monitor
- TEE Core
- HAL

OP TEE Hello World:
https://github.com/jenswi-linaro/lcu14_optee_hello_world
Supported HW and Emulators

Architectures: ARMv7, ARMv8

Foundation FVP

ARMs Juno Board

QEMU

STMicroelectronics b2120 - h310 / h410

STMicroelectronics b2020-h416

Allwinner A80 Board

HiKey Board (HiSilicon Kirin 620)

MediaTek MT8173 EVB Board
Encrypted Media Extensions

W3C draft for playback protected content using the `HTMLMediaElement`. The standard doesn’t specify the DRM subsystem itself but provides an API to interface/select a DRM subsystem.

Supported by almost all browsers using various DRM platforms: Widewine, Adobe DRM, PlayReady.
CDM portability and interoperability?

- Support for internal and external CDM implementations.

- Chromium code is closely following the EME standard, however, the standard is still in draft.
Open CDM

Browser

OCDM

CDMI Service

RPC

cdmi.h
Interface for various key systems.

mock.drm
ClearKey/OpenSSL CDM
ClearKey OP TEE
PlayReady CDMI
# CDM implementations

<table>
<thead>
<tr>
<th></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</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPAPI CDM</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>
</tr>
<tr>
<td>OP TEE and TrustZone®</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PlayReady, other DRM support</td>
<td>No</td>
<td>No</td>
<td>No</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>
</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 - CDM

- Used as a baseline for integrating OP TEE with commercial DRMs.
- Decrypting and playback of protected webm/mp4 videos in Chromium.
- Support for MS PlayReady on ARM Linux.
- Support for STM B2120, Allwinner and 96boards.
Secure data path

Returning clear buffers to Linux space? Not very secure.