



connect

San Francisco 2015

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

Presented by

Zoltan Kuscsik, PhD

Date

Tuesday 22 September 2015

Event

SFO15

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

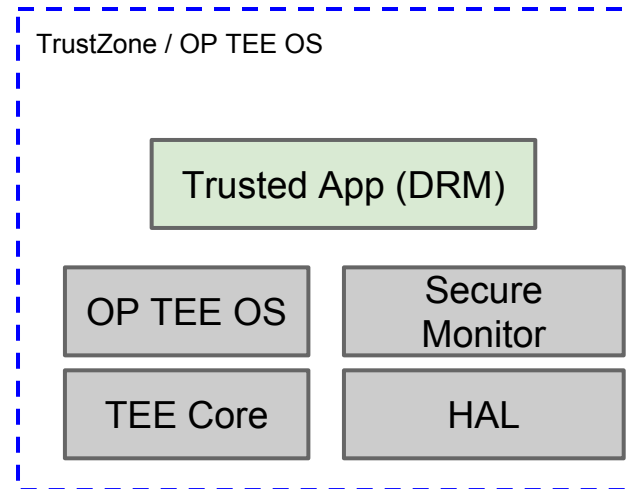
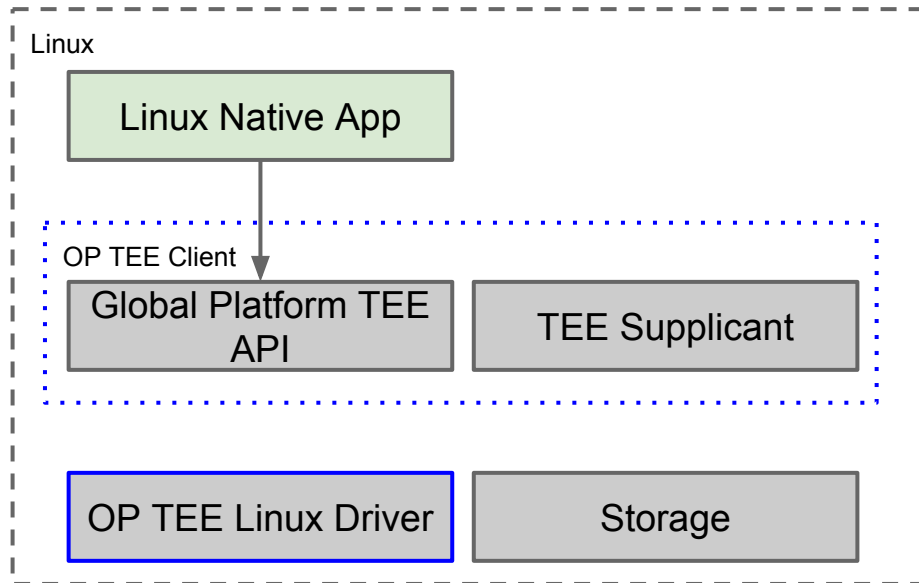
OP TEE Linux driver:

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

Open CDM:

<https://github.com/fraunhoferfokus/open-content-decryption-module>

What is OP TEE?



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

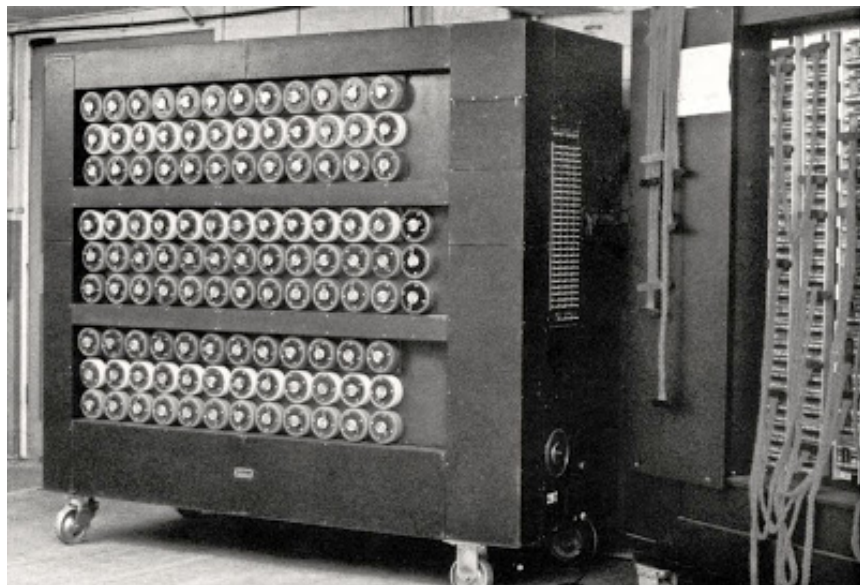
STMicroelectronics b2120 - h310 / h410

STMicroelectronics b2020-h416

Allwinner A80 Board

HiKey Board (HiSilicon Kirin 620)

MediaTek MT8173 EVB Board

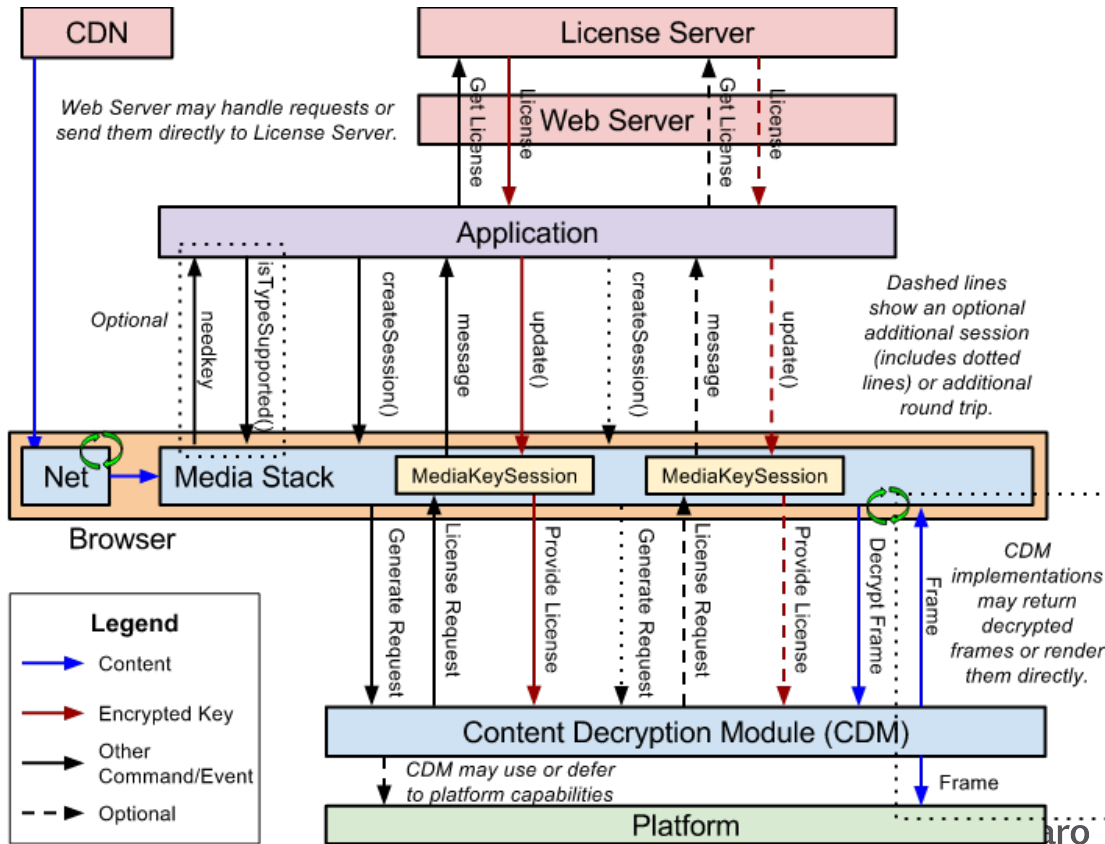


Encrypted Media Extensions

W3C draft for playback protected content using the **HTMLMediaElement**.

The standard doesn't specify the DRM subsystem itself but provides a API to interface/select a DRM subsystem.

Supported by almost all browsers using various DRM platforms: Widevine, Adobe DRM, PlayReady



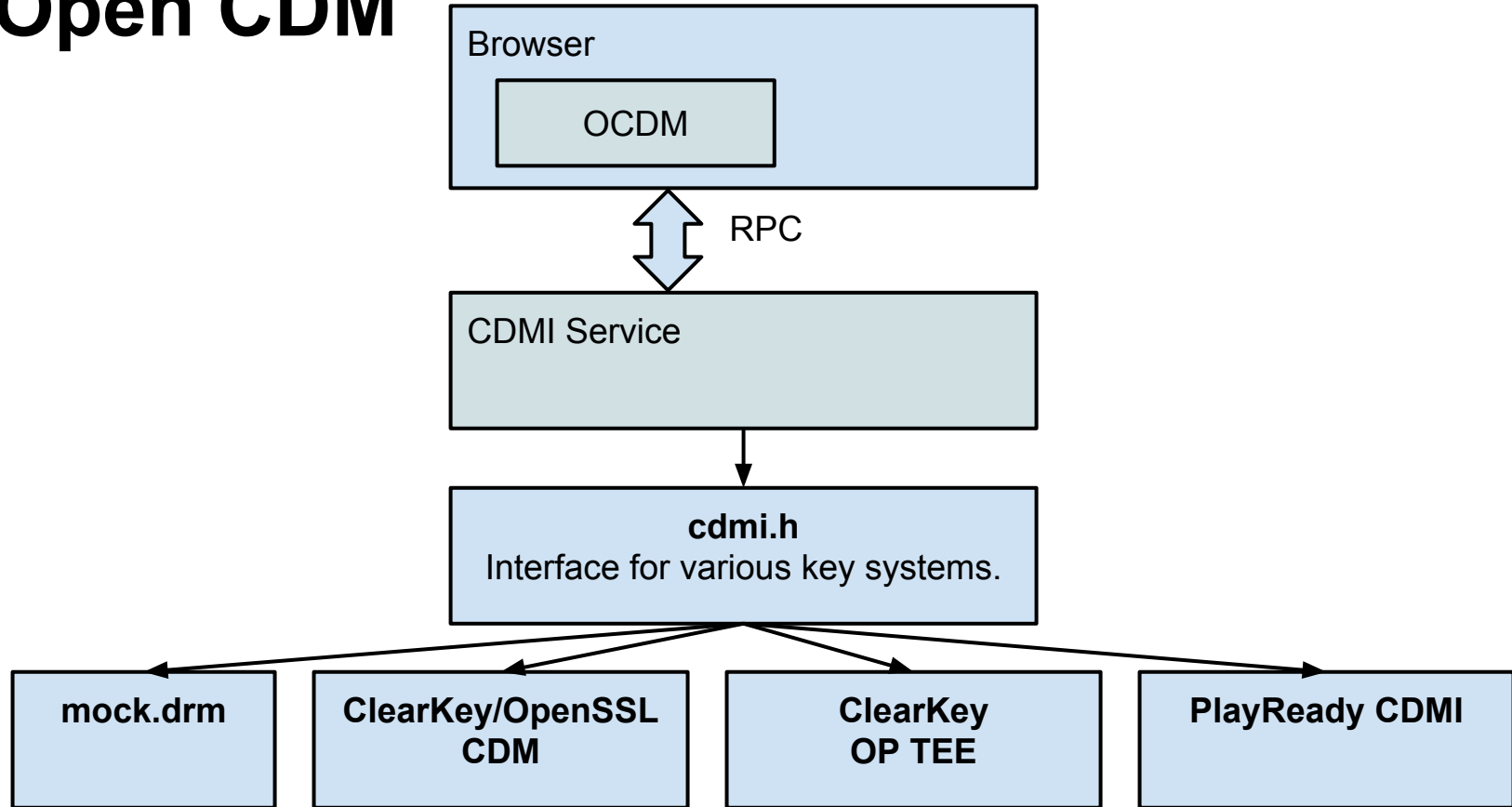
CDM portability and interoperability?

- Support for internal and external CDM implementations.
- Chromium code is closely following the EME standard, however, the standard is still in draft.



The screenshot shows a web browser window with the URL https://www.w3.org/Bugs/Public/show_bug.cgi?id=20944. The page title is "Bugzilla - Bug 20944". The navigation bar includes links for Home, New, Browse, Search, Reports, Requests, Help, and New Account. The main content area displays "Bug List: (1 of 16) First Last Prev Next Show last search results". The specific bug entry is "Bug 20944 - EME should do more to encourage/ensure CDM-level interop". Below the title, the status is "NEW" and the product is "HTML WG".

Open CDM



CDM implementations

	Chromium External Clear Key	Linaro Clear Key CDM with SSL	Linaro Clear Key CDM with OPTEE	Linaro CDM
PPAPI CDM	Yes	Yes	Yes	Yes
OpenCDM	No	Yes	Yes	Yes
OP TEE and TrustZone®	No	No	Yes	Yes
PlayReady, other DRM support	No	No	No	Yes
Compatibility	ARMv7, ARMv8, x86	ARMv7, ARMv8, x86	ARMv7, ARMv8	ARMv7, ARMv8

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.

