



Encrypted Media Extensions on OP TEE

Presented by

Zoltan Kuscsik, PhD

Date

July 2015

Contact:

zoltan.kuscsik@linaro.org

Introduction

Open source Linux project utilizing ARM TrustZone(R) for developing trusted applications. The project is maintained by Linaro and STMicroelectronic. 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

Linaro

Security

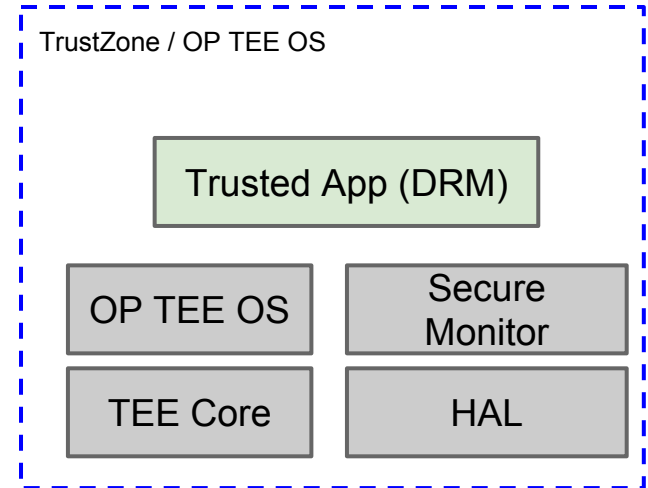
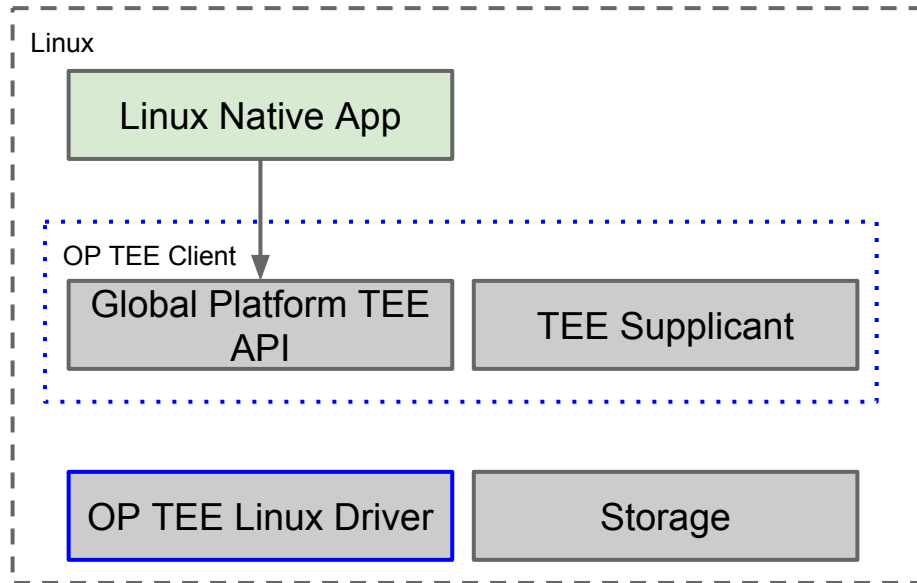
Working

group:

<https://wiki.linaro.org/WorkingGroups/Security/OP-TEE>



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

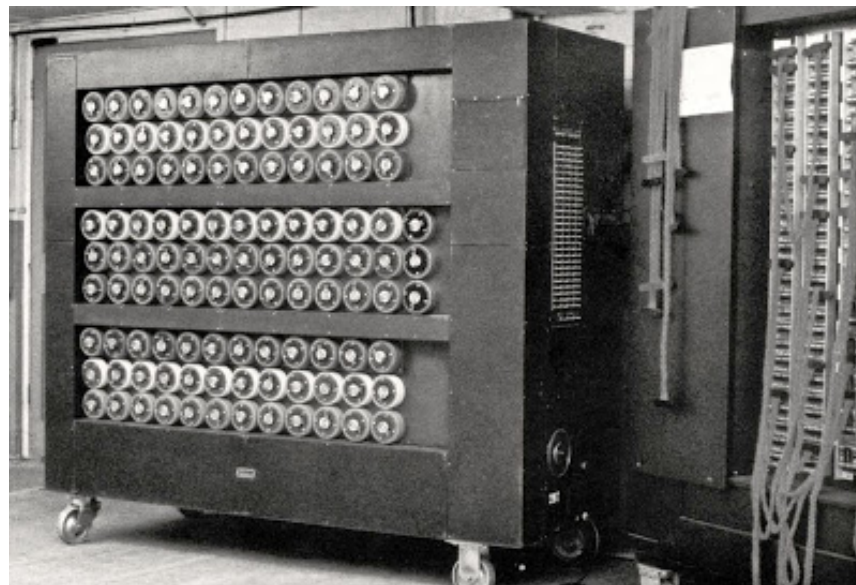
STMicroelectronics b2120 - h310 / h410

STMicroelectronics b2020-h416

Allwinner A80 Board

HiKey Board (HiSilicon Kirin 620)

MediaTek MT8173 EVB Board

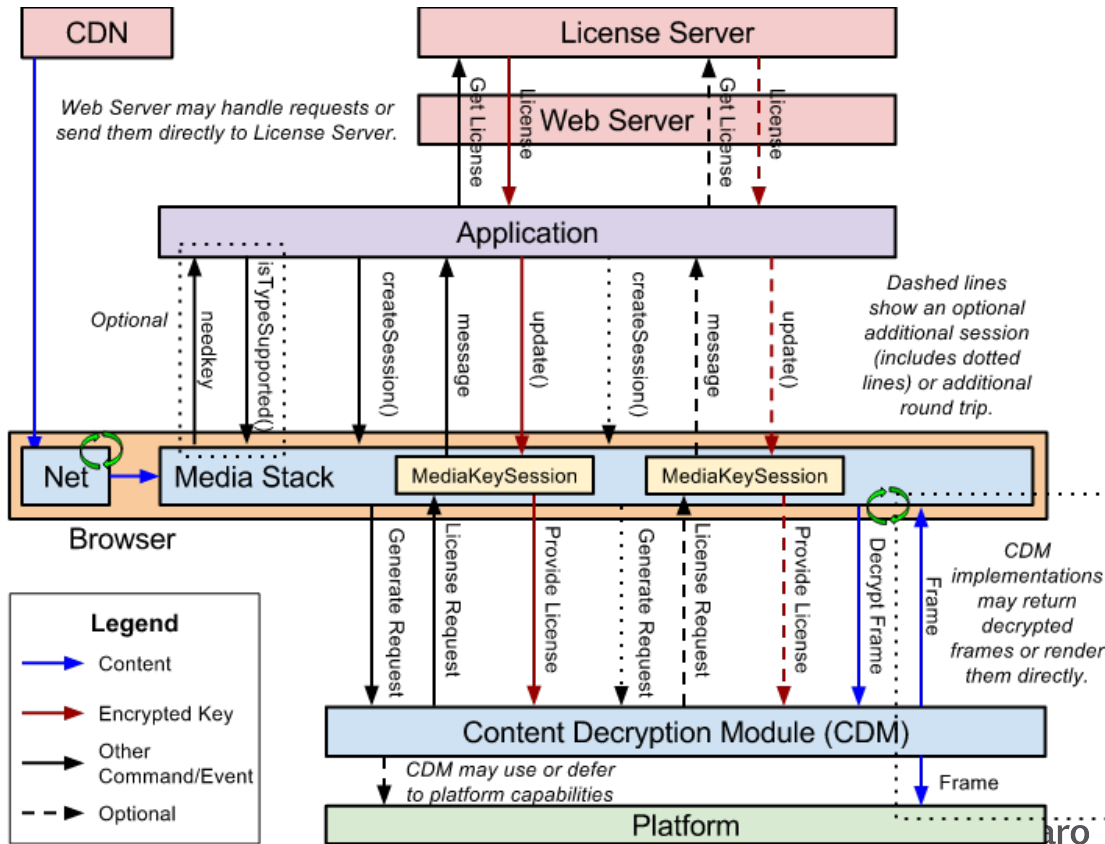


Encrypted Media Extensions

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



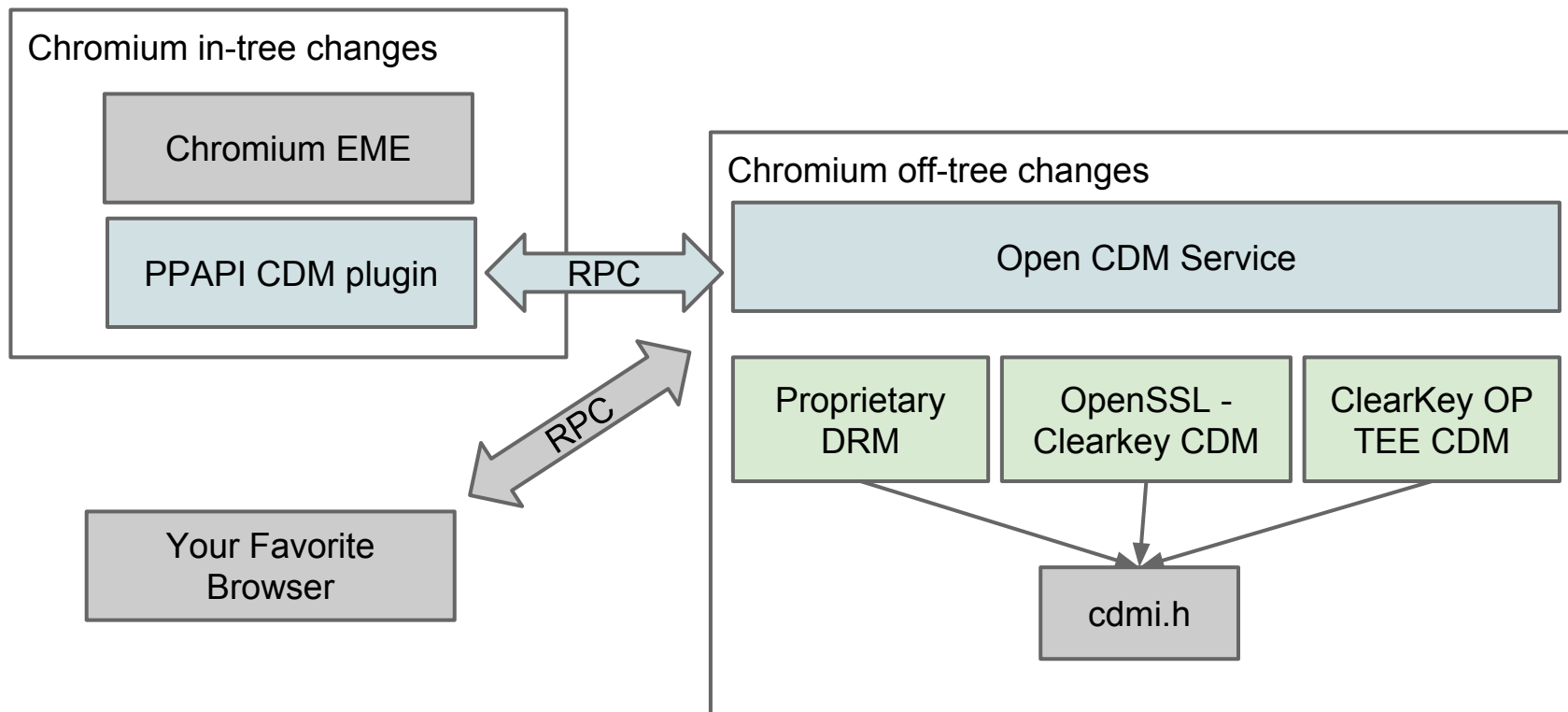
CDM portability and interoperability?

- 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" and the browser tab shows "EME". 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 "Status: NEW" and the product is "Product: HTML WG".

Open CDM



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-cdm>

- We are currently upstreaming top OpenCDM

OP TEE - CDM

- Used as a baseline for integrating OP TEE with commercial DRMs.
- Decrypting and playback of protected WEBM videos in Chromium.
- Public open source release in few weeks.
- Adding support for MS PlayReady on ARM Linux.
- Support for STM B2120, Allwinner and 96boards.

Secure Data Path

LKML.ORG

July 2015

30 1 2 3 4 5
7 8 9 10 11 12
14 15 16 17 18 19
21 22 23 24 25 26
28 29 30 31 1 2

Messages in this thread

First message in thread

Benjamin Gaignard



- *One Thousand Gnomes*

- *Denial Vector*

[[lkml](#)] [[2015](#)] [[May](#)] [[15](#)] [[last100](#)] [[RSS](#)]

Views: [[wrap](#)] [[headers](#)] [[forward](#)]

Date Tue, 5 May 2015 17:39:57 +0200

Subject [RFC] How implement Secure Data Path ?   0

From Benjamin Gaignard <>

Hello,

Since few months I'm looking for Linaro to how do Secure Data Path (SPD).
I have tried and implemented multiple thinks but I always facing architecture
issues so I would like to get your help to solve the problem.

Secure data path

Returning clear buffers to Linux space? Not very secure.

