# SECURE DATA PATH ON LINUX AND NXP I.MX 8M

PRODUCT PRESENTATION

MICR ADVANCED TECHNOLOGIES

Linaro connect

Linaro Multimedia Working Group
https://www.linaro.org/

LINARO CONNECT SAN DIEGO 2019

SECURE CONNECTIONS
FOR A SMARTER WORLD

# SECURE VIDEO PATH OVERVIEW

# I.MX 8MQ Secure Video Path with Android bsp – Hong Kong Connect 2018

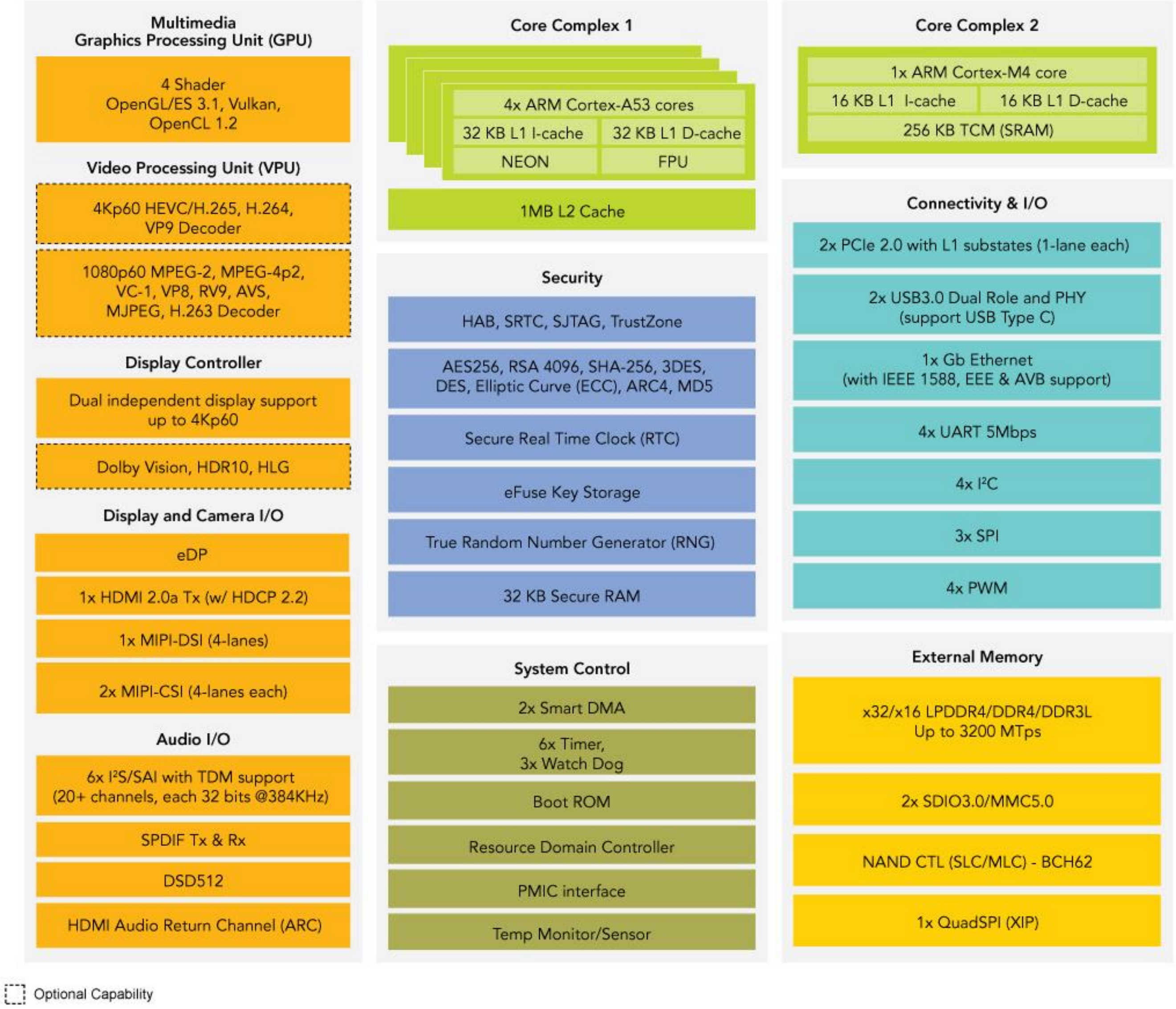
- Slides:

  https://www.slideshare.net/linaroorg/hkg18113-secure-data-path-work-with-imx8m

- Demos:

  https://www.youtube.com/watch?v=z27Tl5XkFJ4

# i.MX 8M : Voice and video processing applications processor



Multimedia Graphics Processing Unit (GPU)

4 Shader OpenGL/ES 3.1, Vulkan, OpenCL 1.2

Video Processing Unit (VPU)

4Kp60 HEVC/H.265, H.264, VP9 Decoder

1080p60 MPEG-2, MPEG-4p2, VC-1, VP8, RV9, AVS, MJPEG, H.263 Decoder

Display Controller

Dual independent display support up to 4Kp60

Dolby Vision, HDR10, HLG

Display and Camera I/O

eDP

1x HDMI 2.0a Tx (w/ HDCP 2.2)

1x MIPI-DSI (4-lanes)

2x MIPI-CSI (4-lanes each)

Audio I/O

6x I²S/SAI with TDM support (20+ channels, each 32 bits @384KHz)

SPDIF Tx & Rx

DSD512

HDMI Audio Return Channel (ARC)

Core Complex 1

4x ARM Cortex-A53 cores

32 KB L1 I-cache

32 KB L1 D-cache

NEON

FPU

1MB L2 Cache

Security

HAB, SRTC, SJTAG, TrustZone

AES256, RSA 4096, SHA-256, 3DES, DES, Elliptic Curve (ECC), ARC4, MD5

Secure Real Time Clock (RTC)

eFuse Key Storage

True Random Number Generator (RNG)

32 KB Secure RAM

System Control

2x Smart DMA

6x Timer, 3x Watch Dog

Boot ROM

Resource Domain Controller

PMIC interface

Temp Monitor/Sensor

Core Complex 2

1x ARM Cortex-M4 core

16 KB L1 I-cache

16 KB L1 D-cache

256 KB TCM (SRAM)

Connectivity & I/O

2x PCIe 2.0 with L1 substates (1-lane each)

2x USB3.0 Dual Role and PHY (support USB Type C)

1x Gb Ethernet (with IEEE 1588, EEE & AVB support)

4x UART 5Mbps

4x I²C

3x SPI

4x PWM

External Memory

x32/x16 LPDDR4/DDR4/DDR3L Up to 3200 MTps

2x SDIO3.0/MMC5.0

NAND CTL (SLC/MLC) - BCH62

1x QuadSPI (XIP)

Optional Capability

- Dedicated hardware for security

- Video quality with full 4K Ultra HD resolution and HDR (Dolby Vision, HDR10, and HLG)

- Hardware composer (4Kp60): DCSS (Display Controller Sub System)

- Highest levels of pro audio fidelity with more than 20 audio channels each @384KHz

- DSD512 audio capability

- Fully supported on NXP’s 10 and 15-year Longevity Program

# i.MX 8M SDP (Secure Data Path) at a glance

The i.MX 8M security subsystem is configured in a way that only hardware components involved in the decoding and the rendering of the stream have access to the decrypted data:

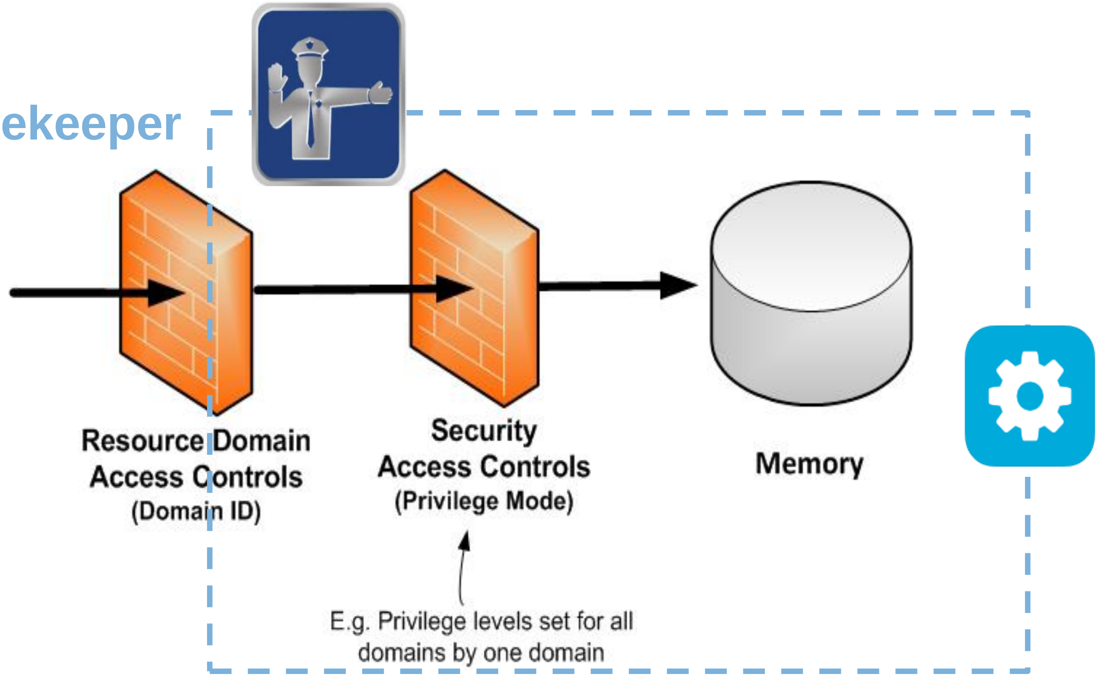
- High Assurance Boot (On Chip **ROM** with tamper detection). Authenticated and Encrypted boot
- ARM TrustZone/TEE and the Central Security Unit (CSU) split the processing between non-secure world running the rich OS, and the secure world running the trusted stack (ATF/OP-TEE from Linaro)
- RDC (Resource Domain Controller) to isolate CPU, VPU, GPU, DCSS and memory buffers, using **dedicated hardware**

  -> Application CPU cores won’t have physical access to decrypted video memory buffers
- CAAM (Cryptographic Acceleration and Assurance Module) to accelerate and isolate cryptographic operations, using **dedicated hardware**
- SNVS (Secure Non-Volatile Storage) and 32 KB of Secure RAM (tamper detection)

# Secure Data Path on i.MX 8M

# RDC: Resource Domain Controller

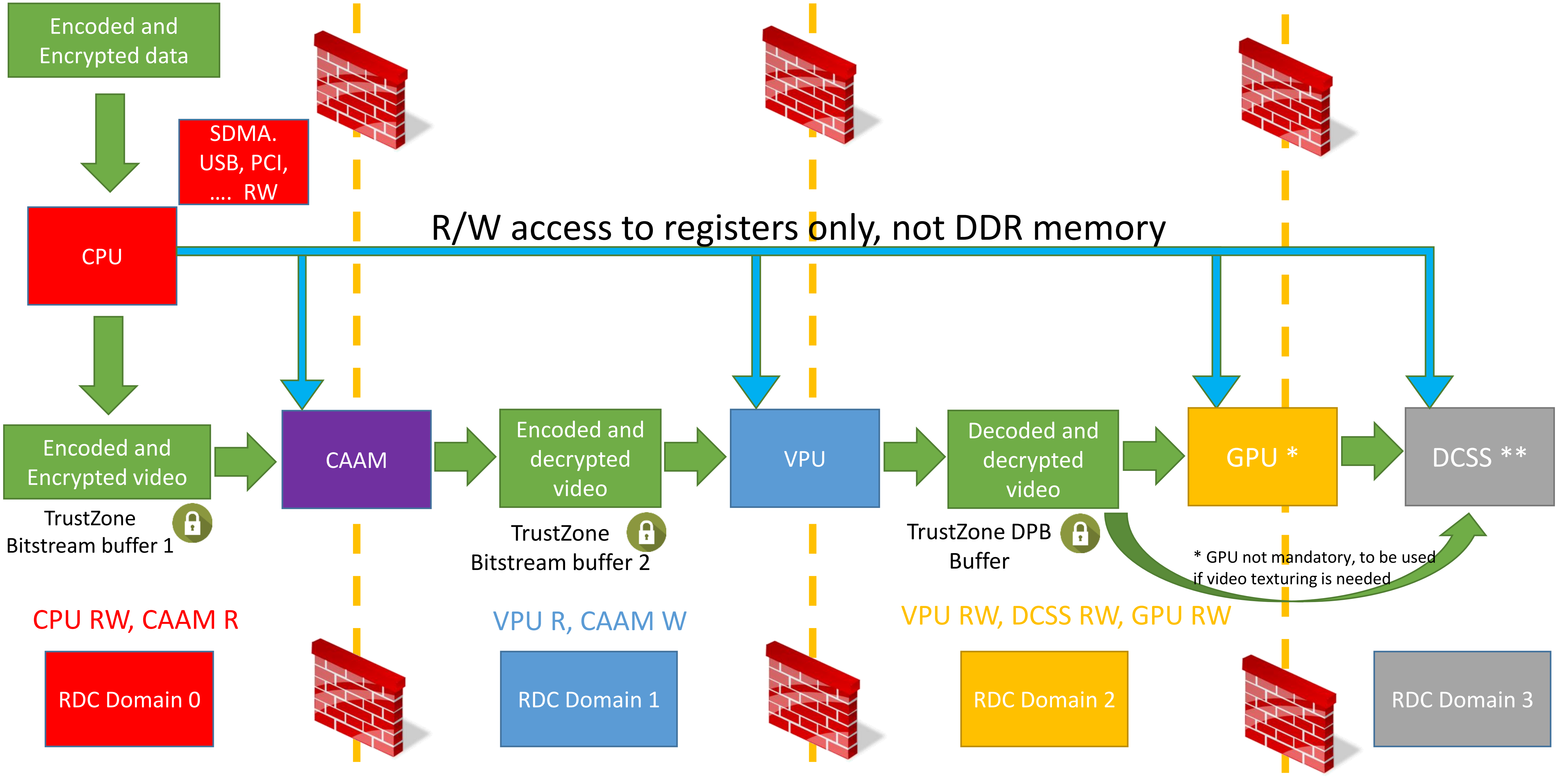
RDC the SDP gatekeeper



Use a configuration set at boot (within ATF)
Registers locked till next reset/reboot

- Assignment of cores and bus masters to a resource domain (4 domains, 27 bus masters)
- Peripherals and memory regions assigned right accesses based on domain IDs (118 Peripherals, 52 memory regions)
- Memory read/write access controls for each resource domain and region (up to 8 regions per domains)

# Secure Video Path on i.MX 8M



Encoded and Encrypted data

SDMA. USB, PCI, .... RW

CPU

R/W access to registers only, not DDR memory

Encoded and Encrypted video

TrustZone Bitstream buffer 1

CAAM

Encoded and decrypted video

TrustZone Bitstream buffer 2

VPU

Decoded and decrypted video

TrustZone DPB Buffer

GPU *

DCSS **

* GPU not mandatory, to be used if video texturing is needed

CPU RW, CAAM R

VPU R, CAAM W

VPU RW, DCSS RW, GPU RW

RDC Domain 0

RDC Domain 1

RDC Domain 2

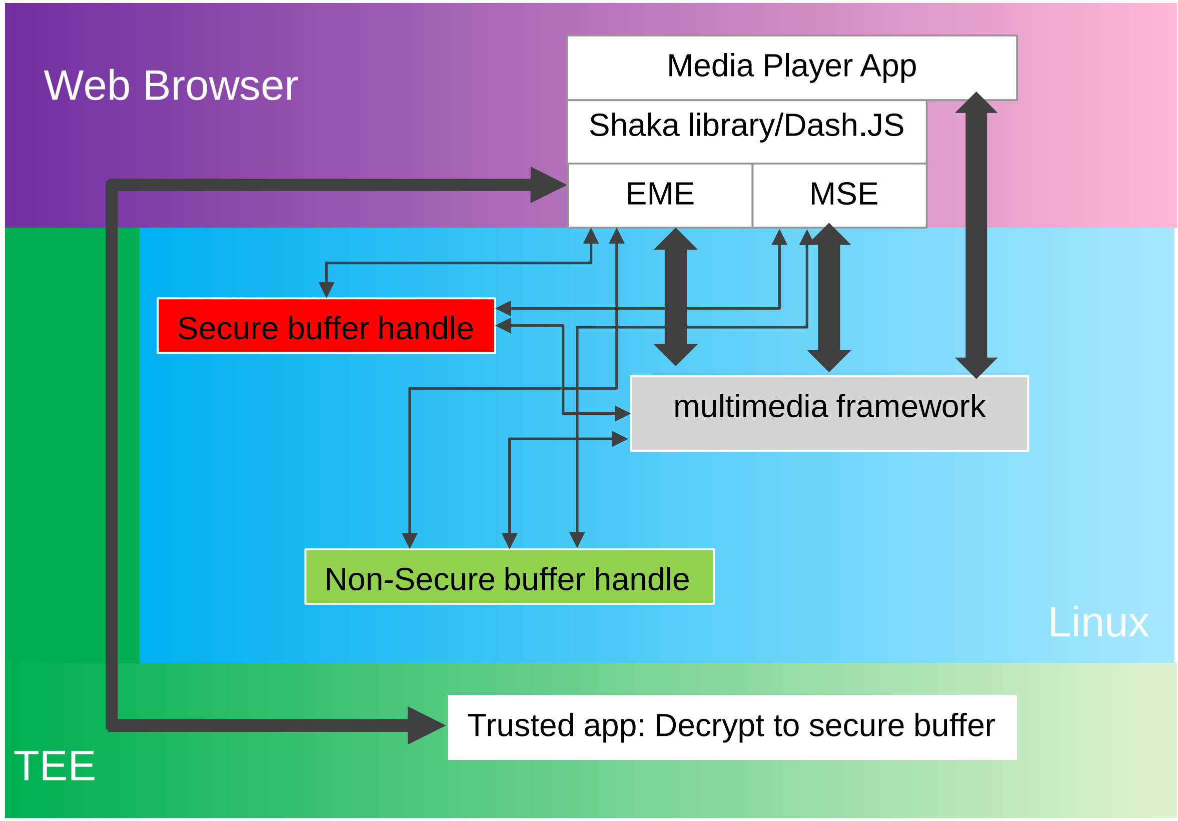
RDC Domain 3

** DCSS: Display Controller Sub System: to source up to three display buffers, on the fly composition (3 scalers, PIP) and drive display using HDMI 2.0a with HDCP 2.2

# LINUX SECURE VIDEO PATH

# i.MX 8MQ Linux DRM approach to support Secure Video Path

## High level design



- EME* (Encrypted Media Extension): API to allow Javascript to control playback of encrypted content.
- MSE** (Media Source Extension), API to allow Javascript to send bytes to media codecs. Compliant with EME
- Shaka Library ***/Dash.JS ****: API to allow Javascript to play Adaptive media format as DASH or HLS. Compliant with EME and MSE. CENC DRM support
- TEE: secure OS + Client and Trusted Applications for PlayReady and Widevine.
- i.MX 8M RDC and ARM TZASC to secure buffers
- We don’t support encrypted slice headers. CENC v2 and v3 suggests that only video data in slice NALs should be encrypted. other NAL types should be left in clear.

* https://www.w3.org/TR/encrypted-media/

** https://www.w3.org/TR/media-source/

*** https://github.com/google/shaka-player

**** https://dashif.org/dash.js/

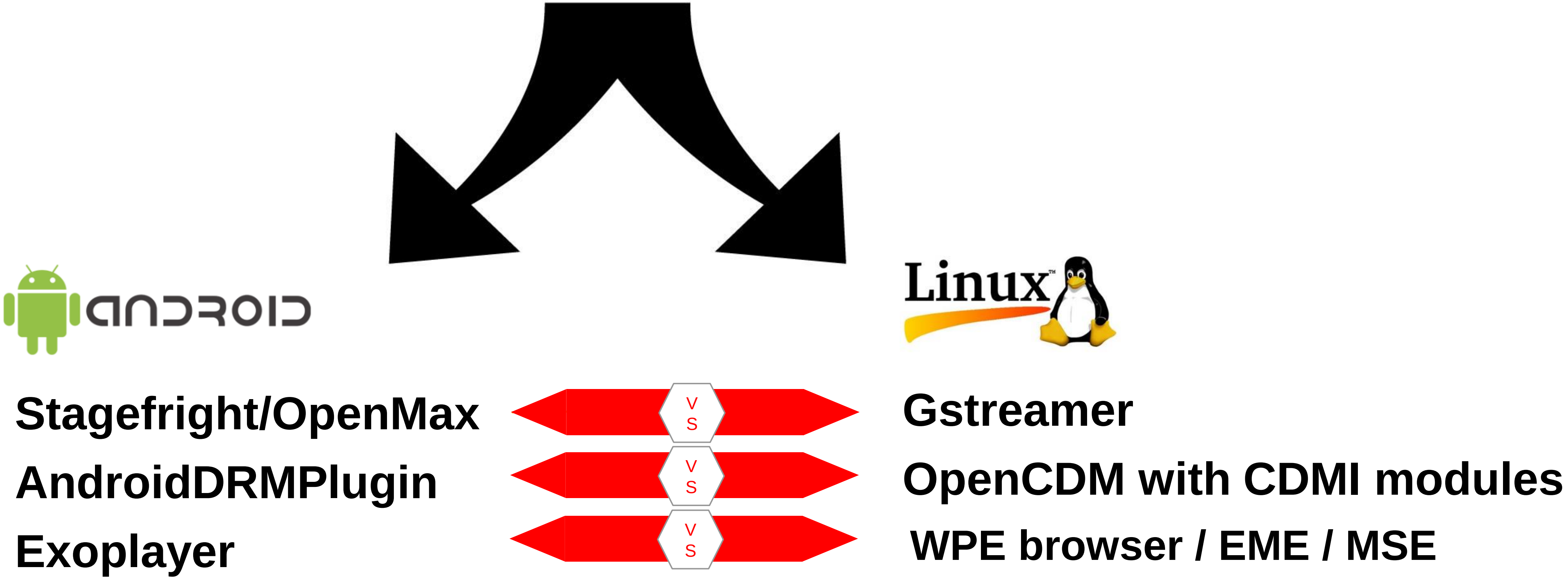
# Linux Secure Video Path vs Android Secure Data Path

Same OPTEE code

Same Trusted Applications for Widevine, PlayReady and Provisioning

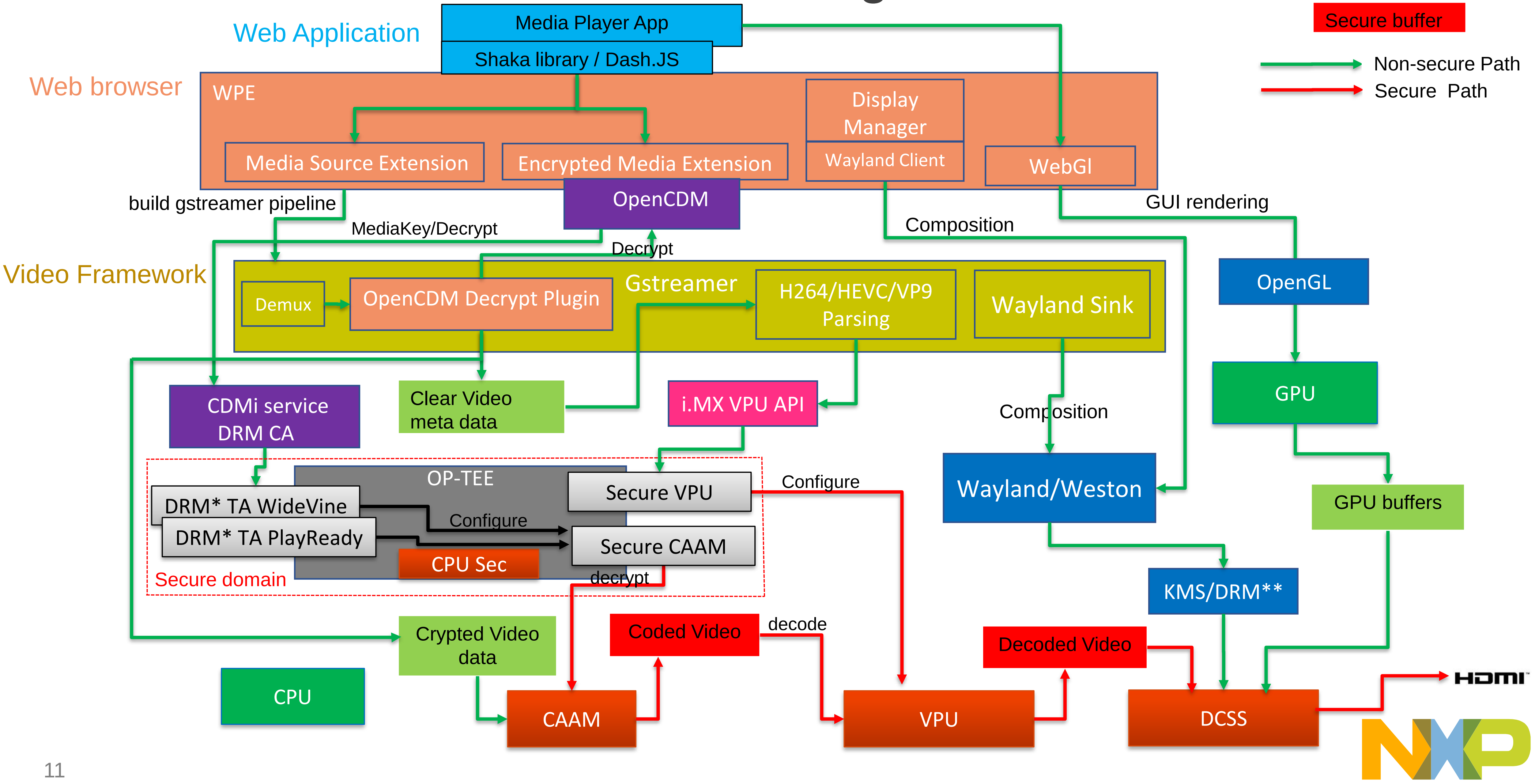
Same VPU,CAAM and DCSS drivers

ION unmapped buffers to manage secure buffers



| | | |
|---|---|---|
| **Stagefright/OpenMax** | VS | **Gstreamer** |
| **AndroidDRMPlugin** | VS | **OpenCDM with CDMI modules** |
| **Exoplayer** | VS | **WPE browser / EME / MSE** |

# Secure Data Path with WPE browser / gstreamer



DRM* Digital Right Management    DRM** Direct Rendering  Manager

# Secure Video Path with WPE browser / gstreamer : where Are we ?

Done:

- The SVP changes are based on the older OpenCDM architecture.
- WPE from metrological with Wayland Westeros, performs **PlayReady 1080p60 video playback**, ION unmapped buffers and GPU compositor, without TZASC/RDC protection, due to GPU compositor being used.

  ->Main contributor is **Alexandre Jutras** (NXP assignee)
- WPE from Igalia with Wayland Weston, performs **4Kp60 clear** video playback with gstreamer through secure VPU and DCSS compositor (Secure Video Path using secure ION unmapped buffer, protected by RDC and TZASC).

  -> Main contributor is **Alexandre Jutras** (NXP assignee)

On going:

- Move to the new OpenCDM architecture to support the latest EME specification
- WPE from metrological with Wayland Westeros, performs **Widevine** video playback without Secure Video Path, using shared Memory. **Peter Griffin** (Linaro employee)
- Add support of Wayland Weston to WPE from Metrological to benefit Secure Video Path with PlayReady and Widevine

  **Alexandre Jutras** (NXP assignee)

# WPE and Secure Video Path

-> WPE to use Wayland Weston (DCSS and HDCP support of i.MX 8MQ)

-> use ION buffer for decryption instead shared memory. Keep legacy mode with shared memory for audio. It supports legacy ION API <= Linux kernel 4.11 and new ION API.

-> Implement helper API to retrieve the ION heap ID from the heap name and to

configure the heap ID property for each ION allocators (video decrypted secure buffer and video decoded secure buffer)

# OpenCDM and Secure Video Path

-> OpenCMD: Open Source implementation of EME from Linaro and Metrological

-> Integrate ION buffer management in OPENCDM and CDMI for Secure buffer, in addition of shared Memory for non secure buffer.  Shared memory still used for non-secure buffer (audio)

-> At every decryption operation, OpenCDM allocates a 'secure' ION buffer from the ION heap specified at compilation.

Then, it communicates the corresponding file descriptor to the DRM layer via the CDMI service.

-> Modify the create media engine session RPC to communicate the socket channel ID. This ID is used by the Secure Data Path implementation to uniquely create a socket connection for each session. This is required to support multi-session in the SDP implementation.

-> Add the support for providing the sub-sample data to the CDMi service. Maintain the support for non-SDP and for SDP prototype.

# CDMI modules and Secure Video Path

-> Implement a socket server helper class

This socket server helper class allows the CDMI service to retrieve the secure (ION) file descriptor from the CDM browser plugin. The socket client helper class implements the plugin side of the communication. The helper class provides an API to accept a socket connection (typically when creating a media engine session) and to receive the file descriptor (typically at every decrypt operation).

-> Integrate secure ION buffer into CDMI service to implement Secire Video Path

When creating a media engine session, a socket connection is established with the OpenCDM browser plugin using the socket server helper class. This connection is used, at every decryption operation, to communicate the secure (ION) file description from the plugin to the CDMI service.

-> Multi-session is supported by creating a dedicated socket connection for each session.

# Gstreamer v1.14 and Secure Video Path

PlugInbase:

-> Add support of different IONS heaps for encode frames (VPU ION heap) and decode frames (display ION heap). Support of Legacy ION API <= Linux kernel 4.11 and new ION API

-> Separate clear video meta data and encrypted video data

GstIONAllocator is modified to support secure ION buffer. In addition to the ION file descriptor, the allocator maintains a shared buffer. It has the same size of the ION buffer and it is accessible by the CPU. When the map API is called, this shared buffer is mapped. In SDP's context, the shared buffer holds the unencrypted content of the stream. This allows the VPU plugin to access the stream's metadata.

gst-plugins-bad:

-> H264 support only till now. HEVC and VP9 still to be done

-> conversion from AVC (H264 Packetized stream) to H264 NAL byte-stream format before to be decrypted.

# QUESTIONS