NXP Semiconductors
Release Notes

Document Number: ADRMRN
2.3.1 Rev.0, 05/2020

Android™ DRM Release Notes

1. Release Description

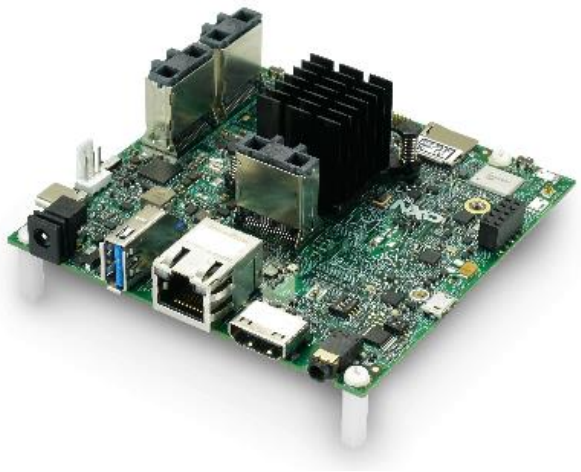
This document is an add-on to the Android **imx-p9.0.0_2.3.0_8m** release note, and targets **imx-p9.0.0_2.3.0_8m_drm-2.3.1** release**.**

The i.MX 8M Android DRM (Digital Rights Management) releases are a set of components allowing **demonstration** and **development** of DRM functionality using Secure Data Path on NXP i.MX 8M applications processors family.

This i.MX 8M Android DRM package includes all the necessary binaries and documents to assist users in setting up and running Google® Widevine® DRM demonstrators on NXP i.MX 8M platform, with Android BSP. This includes Exoplayer media application examples making usage of DRM schemes, related plugin libraries and trusted applications running in the TEE secure environment. The Android DRM package can be exercised on the i.MX 8M EVK platform (Evaluation Kit) platform.

Contents

i.MX 8M EVK platform



The Android DRM package includes elements allowing integration of the Android™ DRM components in a i.MX 8M platform, and targets Google Widevine DRM Security Level 1 support for video data. This release has an PRC qualification level and has not passed any DRM certification level. Only test keys are provided. There is a key provisioning mechanism included, but it has not passed certification level.

This release is based on Widevine oemcrypto v15.

Please note access to the Android DRM package is **restricted under license agreement.**

2. Release Content

Package content:

Google Widevine package: imx-p9.0.0_2.3.0_8mq_drm-wv-2.3.1

- imx-p9.0.0_2.3.0_8mq_drm-wv-2.3.1.tar.gz
- imx-p9.0.0_2.3.0_8mq_drm-wv-2.3.1_prebuilt.tar.gz
- Release Notes (ADRMRN), this document
- Android™ DRM Project User's Guide (ADRMPUG)

imx-p9.0.0_2.3.0_8mq_drm-wv-2.3.1 package is available through a moderated download site. To request access, the form at i.MX Software and Development Tool Resources should be filled up. Once access to the product is granted, download of the release package can be performed under your NXP Product list: NXP > Software & Support

The archives named with "_prebuilt" keyword correspond to precompiled images which can be flashed on the i.MX 8M EVK platform. Please refer to the Android™ Project User's Guide for flashing instructions.

The archives imx-p9.0.0_2.3.0_8mq_drm-wv-2.3.1.tar.gz correspond to the source code allowing to recompile the prebuilt image. Please refer to the Android™ Project User's Guide for compilation instructions.

In the following release content description, the supported target platforms and package types are as follow:

- TARGET_PLATFORM:
  - imx8mqevk: i.MX 8MQ
  - Android™ 9.0

3. Release Notes

DRM 2_3_ 1 release:

- Code complete
- Provisioning service based on OEMCrypto v15

DRM 2_2_ 0 release:

- Remove provisioning service based on OEMCrypto v11
- Upgrade from OEMCrypto v11 to OEMCrypto v15
- Fix Wifi regression from DRM 2_1_ 3

DRM 2_1_ 3 release:

- Add provisioning flags

DRM 2_1_ 0 release:

- Backporting of DRM 2_0_ cand20190515 to i.MX 8M EVK
- Rebase to Android 9 2.3.0 bsp
- VPU Trusted Application in OPTEE to support clear video content outside Secure Video Path.
- CTS/VTS and GTS bug fixing

DRM 2_0_ cand20190515 release:

- Add DRM support for i.MX 8M Mini EVK with ddr4 memory
- OPTEE to check if the Manufacturing Protection private key was reset
- ATF to manage SNVS register NPSWA_EN
- Add missing include path in u-boot for fsl/utils.h
- Fix suspend/resume issue

DRM 2_0_ cand20190419 release:

- Update Android bsp from Android 9 GA to Android 9 Post GA: p9.0.0_**2**.0.0-ga
- Based on **Private CAF**, not public CAF
- Add DRM support for i.MX 8M Mini EVK with ddr4 memory
- OPTEE to check if the Manufacturing Protection key protocol got already executed
- ATF to manage SNVS register NPSWA_EN
- Add missing include path in u-boot for fsl/utils.h

DRM 2_0_ cand20190405 release:

- Provisioning Service with RPMB filesystem support

DRM 2_0_ cand20190329 release:

- Keymaster Attestation support now functionnal

DRM 2_0_ cand20190315 release:

- Support secure storage using RPMB
- Android Verified Boot with secure storage of the rollback index (lock status not stored in

secure partition)
    - Trusted Keymaster 3 with OP-TEE
    - Attestation and Widevine Provisioning Library using AES-256-CCM

DRM 2_0_ cand20190222 release:
    - Widevine Provisioning API using AES-256-ECB for test purpose
    - Debug tool available to dump the Manufacturing Protection public key of the device.
    - Android Verified Boot without secure storage capability (stored rollback index is hardcoded to 0 and lock status is not security stored).

DRM 2_0_ cand20160215 release:
    - Widevine Provisioning API using AES-128-ECB for test purpose

DRM 2_0_ cand20190116 release:
    - Google Widevine DRM (Android DRM Plugin and Trusted Application through Secure Data Path) - Supports only Widevine test keys.
    - Exoplayer audio/video playback
    - HEVC and H264 codecs supported in Secure Data Path.
    - ARM® Trusted Firmware and OP-TEE OS with TZASC (TrustZone Address Space Controller) protection
    - Android 9.0 full treble support
    - Extra secure 92 MB ION heap, for decoded video data and graphics data, protected by RDC (Resource Domain Controller) against read and write CPU access, even in secure mode
    - Extra secure 32MB ION heap, for decrypted secure data, protected by RDC (Resource Domain Controller) against CPU Read access, even in secure mode
    - OpenMaxIL with secure ION buffer support
    - Hantro VPU driver with secure ION buffer support
    - Content decryption with CAAM acceleration
    - TZASC and RDC are used to secure decrypted video data and decoded video data.
    - Security fuses and OTP (One Time Programmable) flash partitions are not enabled

- Feature highlights from previous releases:
    - None

4. Limitations

Table 1. **Android™ features limitations with DRM image**

Limitation description	Remarks
VP9 and VP8 codecs are not supported in the Secure Video Path	
GPU is not yet part of the Secure Video Path. Video texturing is not secure.	JIRA MMIOT-56: Add GPU into Secure Data Path
No Secure Audio Path supported (not required by DRM Security Levels)	

Table 2. **Android™ VTS failing with DRM image**

Limitation description	Remarks
Below VTS test try to decode VP9 codec, not yet supported in Secure Video Path: **VtsHalMediaOmxV1_0Host#VideoDecHidlTest.DecodeTest.OMX.Freescale.std.video_decoder.vp9.hw-based_video_decoder.vp9_64bit**	JIRA MMIOT-91: Only HEVC and H264 codecs support secure data path.

Table 3. **Android™ CTS failing with DRM image**

Limitation description	Remarks
Below CTS tests try to playback VP9 content, not yet supported in Secure Video Path: **android.media.cts.DecoderTest#testCodecBasicVP9** **android.media.cts.DecoderTest#testCodecEarlyEOSVP9** **android.media.cts.DecoderTest#testCodecResetsVP9WithoutSurface** **android.media.cts.DecoderTest#testCodecResetsVP9WithSurface** **android.media.cts.DecoderTest#testEOSBehaviorVP9** **android.media.cts.DecoderTest#testVP9Decode30fps1280x720** **android.media.cts.DecoderTest#testVP9Decode320x180** **android.media.cts.DecoderTest#testVP9Decode60fps1920x1080** **android.media.cts.DecoderTest#testVP9Decode640x360** **android.media.cts.VideoDecoderPerfTest#testVp9Other0Perf0320x0180** **android.media.cts.VideoDecoderPerfTest#testVp9Other0Perf0640x0360** **android.media.cts.VideoDecoderPerfTest#testVp9Other0Perf1280x0720** **android.media.cts.VideoDecoderPerfTest#testVp9Other0Perf1920x1080** **android.media.cts.VideoDecoderPerfTest#testVp9Other0Perf3840x2160**	JIRA MMIOT-91: Only HEVC and H264 codecs support secure data path.

5. Known Issues

5.1. DRM 2.3.1 issues:

Table 4. **Known issues with DRM image**

Issue description	Remarks
Xtest from Linaro OPTEE test suite doesn't use ION buffer	JIRA MMIOT-119: xtest -aes-perf doesn't use ION buffer
Xtest from Linaro OPTEE test suite doesn't support RDC. Linaro needs to update the test, as with the current implementation the CPU needs access to the secure buffer	JIRA MMIOT-118: xtest sdp test doesn't support RDC
GPU is allocating memory in the same ION heap as VPU.	JIRA MMIOT-56: Add GPU into Secure Data Path
Minor issue in case widevine keys are not in the device.	JIRA MMIOT-44: Widevine fallback to level 3 produces major compression artifacts
android.media.cts.MediaCodecCapabilitiesTest#testGetMaxSupportedInstances	JIRA MMIOT-122: android.media.cts.MediaCodecCapabilitiesTest#testGetMaxSupportedInstances failed
android.media.cts.MediaRecorderTest#testRecorderCamera	JIRA MMIOT-123: android.media.cts.MediaRecorderTest#testRecorderCamera failed
android.media.cts.ResourceManagerTest#testReclaimResourceSecureVsNonsecure	JIRA MMIOT-124: android.media.cts.ResourceManagerTest#testReclaimResourceSecureVsNonsecure failed
android.media.cts.ResourceManagerTest#testReclaimResourceSecureVsSecure	JIRA MMIOT-125: android.media.cts.ResourceManagerTest#testReclaimResourceSecureVsSecure failed
android.os.cts.OsHostTests#testNonExportedActivities	JIRA MMIOT-126: android.os.cts.OsHostTests#testNonExportedActivities failed
record_cmd#dump_kernel_symbols	JIRA MMIOT-127**:** record_cmd#dump_kernel_symbols failed
VtsHalKeymasterV3_0Target.EncryptionOperationsTest.AesIncremental(default)_64bit	Investigation to be done
VtsHalKeymasterV3_0Target.VerificationOperationsTest.EcdsaAllDigestsAndCurves(default)_64bit	Investigation to be done
VtsHalKeymasterV3_0Target.VerificationOperationsTest.RsaAllPaddingsAndDigests(default)_64bit	Investigation to be done

How to Reach Us:

Home Page:
nxp.com

Web Support:
nxp.com/support

Document Number: ADRMRN
2.3.1 Rev.0
05/2020