NXP Semiconductors
Release Note

SECO FW release note

1. Revision History

VERSION	DATE	CHANGE DESCRIPTION
0.1	2020-02-18	Initial version
0.2	2020-02-26	Add version 2.6.0
0.3	2020-03-12	Add version 2.6.1
0.4	2020-04-20	Add versions 3.3.2, 3.5.7, 3.6.2
0.5	2020-06-10	Document SHE specification deviations in section 5
0.6	2020-07-30	Add version 3.7.0 Reformat release table
0.7	2020-09-10	Add version 3.7.1

2. Content

3. Release description

Each release is composed of one SECO Firmware (SECO FW) per supported System on Chip (SoC) hardware revision.

On each SoC revision, the corresponding SECO FW is loaded on the i.MX8 Secure Controller (SECO).

The SECO FW is available as binary only.

The release supports following hardware SoC revisions:

- i.MX8QXP B0
- i.MX8QXP C0
- i.MX8QM B0

3.1. Supported features

This release supports below features, as services provided by the SECO FW.

Here is a description of the SECO FW release numbering.

- The first digit corresponds to the anti-rollback protection.
- The second digit increases when major features are added.
- The third digit corresponds to minor fixes.

The SECO FW releases prior to 3.5.7 (patch release) and 2.6.0 are not suitable to support production SHE implementations.
The SHE feature is deprecated in the SECO FW releases 2.5.4 and 2.5.6.

Feature version	Anti rollback version	Incremental version	SECO FW version	SECO FW release type	SOC revision	Change description (please check the applicable SOC Revision for each change)
1.x	1	1.0	1.1.0	Mainline	QXP B0, QM B0	The support of the roll-back protection of the first two containers including the SECO FW and the SCFW has been added. The support of the SRK revocation for the two SRK sets, NXP and OEM, has been added. The support of the low power transitions has beed added. The support of the SECO FW attestation has been added.
		1.1	1.1.1	Patch of 1.1.0	QXP B0, QM B0	The support of the oscillator 32k trimming using fuses has been added.
					QXP B0	A USB SDP timer SCU ROM fix has been removed from the SCU patch and replaced in the SECO FW. *Note: This fix was not enough and has been updated in the versions 3.3.2, 3.5.7, 2.6.1.*
3.x	2	3.0	2.3.0	Mainline	QXP B0, QM B0	The support of the encrypted boot has been added. The encrypted boot makes use of AES 128, 192 or 256-bit keys. The support of the manufacturing protection has been added. The support of the message unit / device ID assignment has been added. The support of the VPU and IEE key handling has been added. The support of the SCU patch update has been added. The TRNG initialization sequence has been improved. Image integrity check failures generate events in OPEN configuration.
					QM B0	The support of the HDMI FW authentication has been added.
					QXP B0	A USB SDP timer SCU ROM fix has been removed from the SCU patch and replaced in the SECO FW. *Note: This fix was not enough and has been updated in the versions 3.3.2, 3.5.7, 2.6.1.*
	2	3.1	2.3.1	Mainline	QXP B0, QM B0	The support of the oscillator 32k trimming using fuses has been added.
	3	3.2	3.3.2	Patch of 2.3.1	QXP B0, QM B0	Manage the USB SDP boot disablement through the new SDP_DISABLE fuse.
					QXP B0	Update of the USB SDP timer fix.
4.x	2	4.1	2.4.1	Mainline	QXP B0, QM B0	**The support of the SHE specification has been added.**
5.x	2	5.3	2.5.3	Mainline	QXP B0, QM B0	The support of the SNVS tamper enablement has been added. Fix a low power issue introduced in 2.4.1.
		5.4	2.5.4	Mainline	QXP B0/C0, QM B0	The support of the i.MX8 QXP C0 hardware has been added. QXP C0 inherits from all features already delivered up to 2.5.3. Fix an issue with the request SHE_KEY_UPDATE that has been introduced in 2.5.3. ***Note: The SHE feature is deprecated in the SECO FW releases 2.5.4 and 2.5.6.***
					QM B0	The support of the HDCP 1.4 and 2.2 keys loading has been added.

		5.6	2.5.6	Mainline	QXP B0/C0, QM B0	***Note: The SHE feature is deprecated in the SECO FW releases 2.5.4 and 2.5.6.***
					QM B0	Fix an HDMI FW loading issue introduced in 2.5.4.
	3	5.7	3.5.7	Patch of 2.5.6	QXP B0/C0, QM B0	The SHE feature is available. Manage the USB SDP boot disablement through the new SDP_DISABLE fuse.
					QXP B0	Update of the USB SDP timer fix.
6.x	2	6.0	2.6.0	Mainline	QXP C0	**The support of the HSM feature set has been added.**
					QXP B0/C0, QM B0	The SHE feature is available. Permanent clearing of adm_caam_cg_inhibit to allow execution of DQS2DQ.
		6.1	2.6.1	Mainline	QXP B0	Update of the USB SDP timer fix.
	3	6.2	3.6.2	Mainline	QXP B0/C0, QM B0	Manage the USB SDP boot disablement through the new SDP_DISABLE fuse.
7.x	3	7.0	3.7.0	Mainline	QXP C0	Increase the TRNG entropy delay. Fix the memory leakage when handling the HSM key store.
					QXP B0/C0, QM B0	Fix an invalid attestation response when the SHE user in place.
		7.1	3.7.1	Mainline	QXP C0	**Candidate release for the FIPS 140-2 level 3 certification.** FIPS compliant TRNG configuration.

4. Delivery contents

The release is composed of the following artifacts:

File name	File desciption
mx8qmb0-ahab-container.img	SECO FW for i.MX8 QM B0
mx8qxb0-ahab-container.img	SECO FW for i.MX8 QXP B0
mx8qxc0-ahab-container.img	SECO FW for i.MX8 QXP C0

5. SHE specications deviations

The below deviations to the SHE Functional Specification v1.1 are documented.

Those deviations are applicable to i.MX 8X B0 silicon (known as QXP B0 in this document), i.MX 8X C0 silicon (known as QXP C0 in this document), and i.MX8QuadMax.

5.1. Unsupported commands

The SECO FW is not providing support for the following SHE commands:

- CMD_DEBUG : The SECO debug is not allowed in production life cycles, therefore the CMD_DEBUG is not supported in the current solution. To simplify the debug activity additional error codes are provided by the SECO API in case of error.
- CMD_CANCEL: the CMD_CANCEL is not handled by the SECO but by the SHE caller driver (e.g. seco_libs, CRYPTO Driver) requesting the SHE service to SECO. As result of the CMD_CANCEL the current command inputs and outputs are cleared
- CMD_SECURE_BOOT, CMD_BOOT_OK and CMD_BOOT_FAILURE are not supported: All boot images are authenticated using the i.MX8 boot process based on ECDSA signature verification.

5.2. Requirements deviations

We have deviations on the following requirements:

- Requirement: A non-volatile memory is required to store information that needs to be available after power cycles and resets of the microcontroller.

In the QXP/QM solution, the security subsystem implementing the SHE module doesn't own a non-volatile memory. The persistent keys are managed in the security enclave internal SECURE RAM and exported in the external NVM in an encrypted (chip-unique) format.

- Requirement: The latency of the AES must remain <2 us per encryption/decryption of a single block, including the key scheduler.

The latency of an AES encryption/decryption of a single block has been measured at 3,4 us (micro seconds).

- Requirement: The number of updates for a single memory slot is only limited by the width of the counter and the physical memory write endurance.

i.MX8 QXP/QM an OTP monotonic counter of 1920 bits is used as roll-back protection. The monotonic counter may be shared between the SHE and the generic-HSM services, a dedicated API is provided to configure these partitions

- Requirements: The facilities of SHE can be used to secure the boot process, i.e., to monitor the authenticity of the software on every boot cycle.

SHE secure boot is not supported by this solution, all boot images, included the SECO FW, are authenticated using the iMX8 boot process based on ECDSA signature verification

5.3. Additional requirements implemented

Moreover the solution implements the additional features required by the SHE+ extension.

- support of additional 40 general purpose keys
- support of the additional security flag: VERIFY_ONLY

How to Reach Us:

Home Page:

nxp.com

Web Support:

Information in this document is provided solely to enable system and software implementers to use NXP products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits based on the information in this document.

NXP reserves the right to make changes without further notice to any products herein. NXP makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does NXP assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. “Typical” parameters that may be provided in NXP data sheets and/or specifications can and do vary in different applications, and actual performance may vary over time. All operating parameters, including “typicals,” must be validated for each customer application by customer's technical experts. NXP does not convey any license under its patent rights nor the rights of others. NXP sells products pursuant to standard terms and conditions of sale, which can be found at the following address: nxp.com/SalesTermsandConditions.