Release Notes

for S32K3XX HSE Firmware 0.2.6.0

Rev. 1.0 — 9 December 2022 Release notes
COMPANY CONFIDENTIAL

1 Getting Started

IMPORTANT NOTES:

This is the Standard Package variant of the HSE Firmware for S32K312 device.

1.1 Package content

This package contains the NXP S32K3XX HSE Firmware 0.2.6.0:

- FULL MEM HSE Firmware: encrypted binary
- AB SWAP HSE Firmware: encrypted binary
- HSE Firmware interface files
- HSE Service API RM
- HSE_FW_S32K3XX_0_2_6_0_ReleaseNotes.pdf – this file
- The license.txt file and the `uninstall.exe` utility for removing the HSE Firmware binaries

NOTE:

Demo Application is provided separately and contains details on how to provision HSE Firmware on new device from factory and demonstrates common use cases of its security features. For this release RM can be provided On-Demand.

One can access via NXP DocStore (https://www.docstore.nxp.com) the following associated documentation:

- HSE Firmware Reference Manual VERSION 2.0

1.2 Installation

Follow the install steps in the demo application.

2 Release Details

This is the HSE Firmware 0.2.6.0 RTM (ready to market) release which can be used for production.

The provided example code shows how to setup and use the HSE Firmware and to perform basic cryptographic operations (refer to the documentation that comes with demo application). The examples will show how to:

- Boot the demo-application (secure mode)
- Install the Firmware
- Load the key(s)
- Perform cryptographic operations

This release was developed and tested using:

- Chip : E5 - P32K312NHVPBS
- Motherboard : X-S32K2XX-MB (700-31431 REV X3)
- Mini-Module :
  - X-S32K3X2CVB-Q257 (700-48307 REV X1)
  - S32K3XX-172MAXQFP (700-47255 REV X1)

Implemented Errata:

N/A

2.1 Supported Derivatives

The software described in this document is intended to be used with the following microcontroller devices of NXP:

- S32K312

2.2 Device Bricking scenario for HSE Firmware

- No bricking scenario identified in *CUST_DEL* lifecycle.

2.3 Security Aspects

Current release of HSE Firmware implements partial counter-measures against logical attacks (e.g. input parameter checking, address ranges). The code contained in this release was not subject to penetration testing / vulnerability attacks verification.

3 Changes in 0.2.6.0

Updated

- Firmware Update service for same Firmware Type in FULL MEM configuration will be allowed only if code size and sys image size is equal or higher than the current Firmware code size and sys-image size installed in the system.
- In the case of streaming mode, if firmware input length given has already exceeded the expected pink image length, then error will be thrown, and firmware update process will be terminated.
- In case there is firmware update request from standard to custom firmware for FULL MEM configuration, and there is change in sys image or code size, then also firmware update request will be allowed only in one shot mode.
- In case of change in sys image or code size change in new HSE Firmware image, then Firmware Update will be allowed only in one shot mode.

Issues Fixed

- Monotonic Counter Increment Service when run in parallel to Asymmetric Services (RSA & ECC) causes failures in both services and causes HSE FW to go into shutdown.
- Monotonic Counter Increment Service when ran in parallel to HASH/HMAC services causes failures in both services and causes HSE FW to go into shutdown.
- Fast CMAC without scatter gather given after Fast CMAC with scatter gather always fails with CAAM hardware error.
- HSE Firmware Update does not complete when XRDC is enabled by the host application. This issue is not applicable for S32K344 devices.

4 Changes in 0.2.1.0

Added

- Added the feature of calculating and verifying the GMAC using random IV in IVT, Base secure boot and secure recovery image
- Support for compressed ECC keys - hseEccKeyFormat_t
- Key verify service - hseKeyVerifySrv_t – generates a hash/MAC over a symmetric key from HSE key store
- AAD support for encrypted SMR - hseSmrDecrypt_t
- Enable the support of NXP ROM keys to allow the import of first user root key in secure manner. Please contact NXP support team for more details.
- Added support for Publish Sys Image and Attribute to allow user to program multiple keys in the flash once. This will help in reduction in time to store multiple keys in flash
- NVM Erase to be done in case junk data is present in the device and inform the status to the user.
- Added the support of software based HMAC-384 and HMAC-512 functionality.
- AES block mode mask as part of the AES key info. It restricts the usage of an AES key only to those specified by hseAesBlockModeMask_t member. If set to 0 then no restrictions apply
- Added the support of TLS RSA master secret key feature
- Enabled the support of Diffie-Hellman key exchange support.
- Added the support of address translation logic in SMR verification service for AB swap configuration. hseSmrVerificationOptions_t, hseSmrVerifySrv_t
- Added the support of scatter gather entries in service “HSE_SRV_ID_CMAC_WITH_COUNTER” - hseCmacWithCounterSrv_t
- The key derive copy restrictions on starting offset and number of bytes extracted - hseKeyDeriveCopyKeySrv_t

Updated

- Improve the flash programming check logic in interface level function. HSE Firmware will return an error at the time of accepting the request only when flash programming is in progress on the same code flash block where HSE Firmware is executing.
- Updated the comments in interface files.
- Minimum MAC length to 8 bytes for MAC service
- Include the MU instance in streaming context
- Policy on encrypted keys import/export. If encrypted, it must also be authenticated
- Minimum MAC length to 16 bytes for plain SMR initial authentication proof, authenticated key import/export and system authorization services
- RNG re-initialization is done for one time when first heavy job is requested after HSE Firmware initialization is completed.

Updated the ITCM and DTCM memory address range for output address for S32K314 device.

Issues Fixed

- HSE status and error bits are not updated on the application side (MU.FSR and MU.GSR) until HSE_STATUS_INIT_OK is set
- Flash Read while Write Issue is observed in Firmware if Flash Operation is ongoing on the device.

Removed

- XRDC configuration in SBAF to improve the boot time.
- Specific fatal error events for tamper violations - hseError_t
- SHA1 support for key derivation services
- HMAC and CMAC support as PRF for NXP key derivation scheme

5 Changes in 0.1.2.1 (hotfix)

Issues Fixed

- HSE goes into the exception due to RWW(read while write error) while handling watchdog ISR, if the Host is performing the flash operation (programming/ erase) on the same block on which HSE Firmware is executing. *(ASHF-4611)*

6 Changes in 0.1.2.0

Added

- Service *HSE_SRV_ID_IMPORT_EXPORT_STREAM_CTX*. This service is used for Import/Export streaming context for the symmetric operation.
- Enhanced the synchronization logic for the Flash read and write operation between the Host application and the HSE core. For every flash block, Status bit in the GPR register are provided which indicates to the Host application that HSE core is performing read or write operation on a specific block. For more details *(Refer to HSE Firmware reference manual V1.2)*
- Added the *HSE_RAM_PUB_KEY_IMPORT_POLICY_ATTR_ID* attribute which allows the importing of public keys in RAM without authentication.
- Added the SMR rollback protection feature.
- Added the support of glitch filter enablement for the Active Tamper.

Updated

- Interface comments.
- Key Import:
- Only authentication is required for importing the RAM provision keys. These keys can be used to import only RAM keys.
- NVM provisioning keys can be imported/updated without authentication only having SuperUser rights.
- Key Export:
- NVM keys cannot be exported using RAM provision keys.
- NVM and RAM symmetric keys can be exported only encrypted and authentication is optional.

Issues Fixed

- User Keys in the NVM are getting erased after giving a reset. *(ASHF-4435)*
- TLS 1.2 KDF output is not correct when secret key length is greater than the block size of the Hash Algo. *(ASHF-4303)*

7 Change logs in 0.1.1.0

Added

- Service *HSE_SRV_ID_IMPORT_EXPORT_STREAM_CTX*. This service is used for Import/Export streaming context for the symmetric operation.
- Enhanced the synchronization logic for the Flash read and write operation between the Application and the HSE core. For every flash block, Status bit in GPR are provided which indicates to host application that HSE core is performing read or write operation on a specific block. For more details (Refer to HSE Firmware reference manual V1.1)

Updated

- Interface comments.

8 Change logs in 0.0.12.0

Added

- Added the *HSE_RAM_PUB_KEY_IMPORT_POLICY_ATTR_ID* attribute which allows the importing the public keys in RAM without authentication.
- Added the SMR rollback protection feature.
- Added the support of glitch filter enablement in case of active tamper and updated the description for the same in interface file.

Updated

- Interface comments and enhancement. Some items have been moved to new headers (to decongest some headers).
- Key Import:
  - Only authentication is required for importing the RAM provision keys. These keys can be used to import only RAM keys.
  - NVM provisioning keys can be imported/updated without authentication only having SuperUser rights.
- Key Export:
  - NVM keys cannot be exported using RAM provision keys.
  - NVM and RAM symmetric keys can be exported only encrypted and authentication is optional.

9 Change logs in 0.0.10.0

Added

- Streaming support in HSE Firmware update service.
- The size of *HSE_MAX_RAM_STORE_SIZE* increased to 6144 bytes from 4096 bytes.
- Service *HSE_SRV_ID_FW_INTEGRITY_CHECK*. This service checks the integrity of active HSE Firmware in code flash area and backup image in data flash area.
- Service *HSE_SRV_ID_BURMESTER_DESMEDT*. This service implements the ECC Burmester-Desmedt Protocol to calculate the shared secret between multiple nodes i.e., more than 2.
- Service *HSE_SRV_ID_SBAF_UPDATE*. This service is used to update the SBAF on the device whenever the Firmware image is not compatible with SBAF present in the system.
- Service *HSE_SRV_ID_CMAC_WITH_COUNTER.* This service is used to calculate and verify the CMAC by appending the monotonic counter in input message.
- Handling of tamper violations: clock monitoring (CMU) and physical tamper.
- Service *HSE_SRV_ID_ON_DEMAND_CORE_RESET*. This service allows configuring CR entries and their associated SMR to be processed at run-time, on-demand
- Event *HSE_WA_SMR_PERIODIC_CHECK_FAILED*. This event signals the host that a periodic check SMR failed (the verification failed).
- Event *HSE_WA_DATA_FLASH_INTEGRITY_FAIL*. This event signals the host that valid backup of HSE Firmware is not present in data flash.
- Register HSE GPR for tamper status. This register is updated by HSE when a tamper is configured. It can be read by the host to check what tampers are configured.
- Prevention of the accesses to shared memory of other cores via HSE (see `hseAttrAllMuMemRegions_t` attribute).
- Service versioning using a byte from the service ID to encode the version for each service.
- Scatter-Gather support for RSA and ECDSA signature (refer to *hseSignSrv_t)*
- Added support for Adkp Provisioning via Key Handle.
- Added *HSE_CORE_RESET_RELEASE_ATTR_ID* attribute to configure the core release-from-reset strategy:
- all-at-once (cores are release all at once after all boot SMRs (Secure Memory Region) are verified).
- one-by-one (cores are release one by one as soon as the boot SMR(s) verification passed for that core)
- New HSE attributes (see *hseAttrId_t*):
- *HSE_PHYSICAL_TAMPER_ATTR_ID* – Enablement of physical tamper.
- *HSE_MEM_REGIONS_PROTECT_ATTR_ID* – Configure memory regions accessible through each MU.
- *HSE_SECURE_RECOVERY_CONFIG_ATTR_ID* – Enablement of the secure recovery mechanism.
- *HSE_CORE_RESET_RELEASE_ATTR_ID* – Release core from reset.

Updated

- Interface comments.
- The minimum value of Rollover Protection bits in monotonic counter is set to 32 bits and the size of Rollover Protection bits must be multiple of 8 bits.
- The configuration of monotonic counter can be done using only Super User rights.

- SHE keys catalog formatting must be configured for *HSE_KEY_OWNER_ANY* group owner.
- HSE_SRV_ID_GET_RANDOM_NUM macro value updated.
- Firmware is not functional if *HSE_FIRC_DIVIDER_CONFIG_ATTR_ID* is received with request to divide by 16.
- *HSE_ENABLE_BOOT_AUTH_ATTR_ID* attribute is not enabled if GMAC tag is not programmed in any of the IVT locations on the device.
- The *HSE_SRV_ID_ERASE_HSE_NVM_DATA* service does not require resetting the device to re-use the firmware services. This service is allowed only in CUST-DEL lifecycle.
- Secure Memory Regions (SMR) (see *hseSmrEntry_t*):
  - Added support for encrypted SMR. The SMRs can be encrypted using GCM or CTR.
  - Removed the SMR verification method field (*hseSmrVerifMethod_t*).
  - The SMR periodic tick has been updated from *10ms* to *100ms* (at 120 MHz frequency)
  - SMR version number added to provide the anti-rollback protection for the image against attacks during update.
- Core Reset (CR) (see *hseCrEntry_t*):
  - Included *PRE-BOOT*, *ALT_PRE_BOOT* and *POST-BOOT* SMR bit map in Core Reset entries.
  - Included *hseCrStartOption_t* option: auto-start (automatically release the core from reset at start-up) or on-demand (the core boot is triggered on demand by another application core)
  - For unsecure boot (BOOT_SEQ=0), the SMRs are not loaded at boot time. Application can use the *hseSmrVerifySrv_t* service to load and verify the SMR (for validation purpose)
  - Updated the SHE Secure Boot used with SMR entry#0 (see *hseSmrEntryInstallSrv_t* comments)
- Updated *hseSmrVerifySrv_t* service to: Verify any SMR using service ID *HSE_SRV_ID_SMR_VERIFY*.
- Fast CMAC:
  - Use input and tag length in bits
  - Included *HSE_FAST_CMAC_MIN_TAG_BIT_LEN_ATTR_ID* attribute to configure the minimum tag bit-length that can be used for Fast CMAC verify / generate.
- HSE errors reported to HOST are divided into warnings and errors.
- Error events reported by HSE (see *hseError_t*). To clear the errors, the host must read the MUB_GSR register and write back the register value (W1C)
- Application header for Basic Secure Boot: “tag address” and “key type” fields were removed; “core ID” field not used; core booted is specified by BOOT_TARGET in IVT; the tag must be placed after the application code (see *hseAppHeader_t*, *hseBootDataImageSignSrv_t*)
- Import/Export key to support GCM and CCM: AAD, Tag and IV should be specified in the AEAD scheme, and the keyInfo (key proprieties) must be within AAD (see *hseImportKeySrv_t*, *hseExportKeySrv_t*)
- HMAC to support key sizes greater than hash block size (updated *hseMacSrv_t* service)
- Erase service to delete the SHE keys only if system authorization was performed beforehand using MASTER_ECU key. Other keys (non-SHE keys) can be erased if the authorization operation was performed using any key type, including MASTER_ECU key (see *hseEraseKeySrv_t*)

- Load ECC service to save the ECC user-curve domain parameters in SYS-IMG (which needs to be published). The host needs Super User rights to be able to load an ECC user-defined curve. The loaded ECC user-defined curves must have the private key size equal to or greater than 192 bits
- SYS Authorization feature (see *hseSysAuthorizationReqSrv_t*) to perform the authorization using the *SHE MASTER_ECU_KEY*. SHE keys can be erased only if the host is authorized with MASTER_ECU_KEY.
- The host must call the *HSE_SRV_ID_ACTIVATE_PASSIVE_BLOCK service* to load new HSE Firmware after successful execution of the HSE Firmware update service in case of AB swap configuration.
- The SYS-IMG configured for 0.0.8.3 Firmware release is not compatible with this release. The Host must reconfigure the SYS-IMG.
- The size of HSE Firmware increased from 80KB to 128KB, the implications of this change would be:
- AB swap firmware cannot be installed through older version of Secure BAF (Boot Assist Flash).
- The Host must free up 40KB from DATA Flash out of 128KB. Hence, DATA Flash range that can be used by the Host is [0x10000000 – 0x10015FFF].
- The Host must free up 168KB from CODE Flash memory,
- Available CODE Flash range in FULL MEM configuration
  [0x400000 – 0x7D3FFF].
- Available CODE Flash range in AB SWAP configuration
  ACTIVE BLOCK: [0x400000 – 0x5D3FFF]
  PASSIVE BLOCK: [0x600000 – 0x7D3FFF]
- **Removed**
  - All TDES support.
  - IV Length parameter from symmetric cipher (see *hseSymCipherSrv_t*)
  - *HSE_KDF_SP800_108_FEEDBACK* and *HSE_KDF_SP800_108_PIPELINE* KDF SP800 modes. Only Counter Mode remained supported.
  - The restriction on allowing an SMR to be updated, in advanced life cycles (OEM_PROD, IN_FIELD), only if it is already verified successfully. *(ASHF-3433)*

10 Known Issues

- N/A

11 List of Limitations

- The HSE Firmware is operational when HSE_CLK is between 24MHz to 120MHz.
- User should restart the device once Firmware Update is completed in FULL_MEM configuration.
- Format Key catalogs service (*HSE_SRV_ID_FORMAT_KEY_CATALOGS*) returns success even if count of groups provided to the service is greater than *HSE_TOTAL_NUM_OF_KEY_GROUPS*. The number of groups provided to the service must be less than or equal to *HSE_TOTAL_NUM_OF_KEY_GROUPS*.
- The HSE FW goes into shutdown when HSE Firmware update service (*HSE_SRV_ID_FIRMWARE_UPDATE*) or SBAF Update service (*HSE_SRV_ID_SBAF_UPDATE*) is called with a pink image having an invalid entry pointer.
- The new HSE-B Firmware operates with restrictions with devices shipped prior to July 2022 with (old SBAF). All restrictions are removed once the SBAF is updated.

The restrictions are:

- The service computing GMAC over IVT, AppBL and recovery images (service structure hseBootDataImageSignSrv_t) will return an error
- The system attribute IVT_AUTH cannot be set to 1
- Advancing the life-cycle to OEM_PROD is not possible.

Older versions of HSE Firmware will not be allowed to be installed on devices with latest version of SBAF.

Important!

The HSE Firmware version 0.2.1.0 onwards is not compatible with older SBAF versions. To use all the services of Firmware, user must update the SBAF using service ID *HSE_SRV_ID_SBAF_UPDATE*.

Below table summarizes the compatibility between SBAF and HSE FW:

Table 1.

HSE-B SBAF	HSE-B FW	HSE-B FW operation	Recommended actions
Old	Old	Operates Normally	Update HSE FW first then Update SBAF
Old	New	Operates with limitations	Update SBAF
New	Old	HSE FW will not be installed	Install latest version of HSE FW
New	New	Operates Normally	None

For more details related to old and new FW and SBAF versions, refer to section “HSE Firmware and Secure BAF release version compatibility” in “HSE-B Firmware Reference Manual - V2.0”.

The demo security installer app provides the functionality to update the SBAF using Trace 32. Encrypted image of latest version of SBAF can be found in release package. Refer to chapter “SBAF Update” in demo app documentation on details to update the SBAF using demo app.

NXP application team can be contacted to get the standalone example code of SBAF update on host side.

12 HSE Firmware Version and S32K3XX Device compatibility

The Table below explains the HSE Firmware version number compatibility with the S32K3 family devices.

Table 2.

S.NO	HSE Firmware version number [<Configtype>_ <socTypeID>_ <fwTypeId>_ <majorVersion>_ <minorVersion>_ <patchVersion>]	Remarks	Applicable HSE Firmware reference manuals	Release Date
1	s32k3xx_hse_fw_0.5.0_0.8.3_pb200928.bin (FullMem) s32k3xx_hse_fw_1.5.0_0.8.3_pb200928.bin(AB Swap)	HSE Firmware Standard EAR release compatible with S32K344 Device. This release supports both Full Mem/AB Swap configuration.	HSE-B Firmware Reference Manual - V0 - Draft J	30th-Sep-2020
2	s32k3x4_hse_fw_0.5.0_0.10.0_pb210630.bin (FullMem) s32k3x4_hse_fw_1.5.0_0.10.0_pb210630.bin(AB Swap)	HSE Firmware Standard EAR2 release compatible with S32K344 Device. This release supports both Full Mem/AB Swap configuration.	HSE-B Firmware Reference Manual - V0 - Draft K	30th-June-2021
3	s32k3x2_hse_fw_0.13.0_0.11.0_pb210726.bin (FullMem) s32k3x2_hse_fw_1.13.0_0.11.0_pb210726.bin (AB Swap)	HSE Firmware Standard EAR release compatible with S32K312 Device. This release supports both Full Mem/AB Swap configuration.	HSE-B Firmware Reference Manual - V0 - Draft M	16th-Aug-2021
4	s32k3x4_hse_fw_0.5.0_0.12.0_pb210903.bin (FullMem) s32k3x4_hse_fw_1.5.0_0.12.0_pb210903.bin (AB Swap)	HSE Firmware Standard BETA release compatible with S32K344 Device. This release supports both Full Mem/AB Swap configuration.	HSE-B Firmware Reference Manual - V1.0	3rd-Sep-2021
5	s32k3x4_hse_fw_0.5.0_1.1.0_pb211004.bin (FullMem) s32k3x4_hse_fw_1.5.0_1.1.0_pb211004.bin (AB Swap)	HSE Firmware Standard RTM release compatible with S32K344 Device. This release supports both Full Mem/AB Swap configuration.	HSE-B Firmware Reference Manual - V1.1	13th-Oct-2021
6	s32k3x2_hse_fw_0.13.0_0.14.0_pb211207.bin (FullMem) s32k3x2_hse_fw_1.13.0_0.14.0_pb211207.bin (AB Swap)	HSE Firmware Standard EAR release compatible with S32K342/S32K341/S32K322 Devices. This release supports both Full Mem/AB Swap configuration.	HSE-B Firmware Reference Manual - V1.1	30th-Nov-2021

Table 2. *...continued*

7	s32k3x2_hse_fw_0.13.0_1.2.0_pb211228.bin (FullMem) s32k3x2_hse_fw_1.13.0_1.2.0_pb211228.bin (AB Swap)	HSE Firmware Standard BETA release compatible with S32K312 Device. This release supports both Full Mem/AB Swap configuration.	HSE-B Firmware Reference Manual - V1.2	18th-Jan-2022
8	s32k3x2_hse_fw_0.13.0_1.2.1_pb220205.bin (FullMem) s32k3x2_hse_fw_1.13.0_1.2.1_pb220205.bin (AB Swap)	HSE Firmware Standard hotfix release compatible with S32K312 Device. This release supports both Full Mem/AB Swap configuration.	HSE-B Firmware Reference Manual - V1.2	07th-Feb-2022
9	s32k3x4_hse_fw_0.5.0_2.1.0_pb220607.bin (FullMem) s32k3x4_hse_fw_1.5.0_2.1.0_pb220607.bin (AB Swap)	HSE Firmware Standard RTM release compatible with S32K344 Device. This release supports both Full Mem/AB Swap configuration.	HSE-B Firmware Reference Manual – V2.0	30th-June-2022
10	s32k3x2_hse_fw_0.13.0_2.6.0_pb221129.bin (FullMem) s32k3x2_hse_fw_1.13.0_2.6.0_pb221129.bin (AB Swap)	HSE Firmware Standard RTM release compatible with S32K312 Device. This release supports both Full Mem/AB Swap configuration.	HSE-B Firmware Reference Manual – V2.0	9th-Dec-2022

13 List of Services Available

All available HSE features/services are also listed in the *hse_b_config.h* file (from HSE Interface). All other features not listed in the table below (or enabled in *hse_b_config.h* file) **are NOT supported**. All available services applicable for both configuration device.

Table 3.

Service Class	HSE Service ID	Description/Notes
Administrative	HSE_SRV_ID_SET_ATTR	**Set an HSE attribute**. Attributes related to UTEST memory can be written only once (e.g. Debug Key) or can only be advanced (e.g. Life cycle). **Care must be taken.**
	HSE_SRV_ID_GET_ATTR	**Get an HSE attribute.**
	HSE_SRV_ID_CANCEL	**Cancel a one-pass or streaming service on a specific channel.** An HSE service request can be cancelled if it is in the processing queue and NOT passed to the hardware to be executed.
	HSE_SRV_ID_FIRMWARE_UPDATE	**HSE Firmware update** **This service covers the following things:** 1. Firmware update in FullMem configuration for Standard Firmware with one-pass/streaming mode 2. Firmware update in ABSwap configuration for Standard Firmware with one-pass/streaming mode
	HSE_SRV_ID_SBAF_UPDATE	**Secure-BAF update** in FullMem configuration for Standard Firmware with one-pass/streaming mode
	HSE_SRV_ID_SYS_AUTH_REQ	**SYS Authorization request** used to request the Super User rights (CUST/OEM).
	HSE_SRV_ID_SYS_AUTH_RESP	**SYS Authorization response** (response to SYS Authorization Request)
	HSE_SRV_ID_BOOT_DATA_IMAGE_SIGN	**Generate the signature on Boot Header & XRDC** image using ADKP
	HSE_SRV_ID_BOOT_DATA_IMAGE_VERIFY	**Verify the signature on Boot Header & XRDC** image using ADKP
	HSE_SRV_ID_IMPORT_EXPORT_STREAM_CTX	**Import and Export service for the crypto streaming context.**
	HSE_SRV_ID_ERASE_HSE_NVM_DATA	**Erase HSE Data Flash only in customer delivery lifecycle**
	HSE_SRV_ID_FW_INTEGRITY_CHECK	**Triggers the integrity check of HSE Firmware code flash and data flash area.**
	HSE_SRV_ID_PUBLISH_NVM_KEYSTORE_RAM_TO_FLASH	**Application requests the firmware to write the NVM keys from RAM mirrored keystore into the data flash. This service has no parameters.**
Key Management	HSE_SRV_ID_LOAD_ECC_CURVE	**Load the domain parameters for a Weierstrass ECC curve.** This service can be used to support additional Weierstrass ECC curves (Not supported by default). The loaded ECC curve domain parameters are persistent.
	HSE_SRV_ID_FORMAT_KEY_CATALOGS	**Format key application key catalogs (RAM & NVM).**

Table 3. *...continued*

Service Class	HSE Service ID	Description/Notes
	HSE_SRV_ID_ERASE_KEY	**Erase NVM/RAM key(s).** Erase key service depends on authorization rights. One or multiple keys can be erased. Selected key group can also be erased
	HSE_SRV_ID_GET_KEY_INFO	**Get key proprieties** (flags).
	HSE_SRV_ID_IMPORT_KEY	**Import a key**. Uses all algorithms supported by HSE firmware: * Plain form or AES / RSA encrypted. * MAC authenticated (refer to supported MAC algorithms) or RSA / ECDSA signed. * Import key restrictions depends on sys authorization rights. The restrictions are described by the service in the interface.
	HSE_SRV_ID_EXPORT_KEY	**Export a key.** Uses all algorithms supported by HSE firmware: * Plain form (only public keys) or AES / RSA encrypted. * MAC authenticated (refer to supported MAC algorithms) or RSA / ECDSA signed. * Export key restrictions depends on authorization rights. The restrictions are described by the service in the interface.
	HSE_SRV_ID_KEY_GENERATE	**Request to generate a symmetric/asymmetric key.** * Random symmetric key generation * RSA and ECC key pair generation
	HSE_SRV_ID_DH_COMPUTE_SHARED_SECRET	**ECC Diffie-Hellman Compute Key (shared secret)**: * SEC curves: SECP256R1, SECP384R1, SECP521R1 * Brainpool curves: BRAINPOOLP256R1, BRAINPOOLP320R1, BRAINPOOLP384R1, BRAINPOOLP512R1 * Montgomery curve: CURVE25519 * 1 user-defined ECC curves (see Load ECC curve service)
	HSE_SRV_ID_BURMESTER_DESMEDT	**ECC Burmester-Desmedt Protocol calculation (shared secret for more than 2 nodes):** * SEC curves: SECP256R1, SECP384R1, SECP521R1 * Brainpool curves: BRAINPOOLP256R1, BRAINPOOLP320R1, BRAINPOOLP384R1, BRAINPOOLP512R1 * Montgomery curve: CURVE25519 * 1 user-defined ECC curves (see Load ECC curve service)
	HSE_SRV_ID_KEY_DERIVE	**Perform a key derivation function:** * NXP Generic KDF, SP800_56C One Step, SP800_56C Two Step, ANSI_X963, SP800_108 (Only Counter Mode), ISO/IEC 18033 KDF1, ISO/IEC 18033 KDF2, PBKDF2HMAC, HKDF, TLS12PRF
	HSE_SRV_ID_KEY_DERIVE_COPY	**Extract a key from the derived key material to a key slot.**
	HSE_SRV_ID_KEY_VERIFY	**Computes a hash/MAC over a symmetric key inside HSE key store.**
	HSE_SRV_ID_SHE_LOAD_KEY	**Load a SHE key** using the SHE memory update protocol.
	HSE_SRV_ID_SHE_LOAD_PLAIN_KEY	**Loads SHE specification-based RAM key** as plain text.

Table 3. *...continued*

Service Class	HSE Service ID	Description/Notes
	HSE_SRV_ID_SHE_ EXPORT_RAM_KEY	**Exports RAM key as per SHE specification.**
	HSE_SRV_ID_SHE_GET_ID	**GETUID as per SHE specification.**
	HSE_SRV_ID_SHE_BOOT_ OK	The command is used to mark successful boot verification for later stages than CMD_SECURE_BOOT. For more details, see SHE specification
	HSE_SRV_ID_SHE_BOOT_ FAILURE	The command will impose the same sanctions as if CMD_SECURE_ BOOT would detect a failure but can be used during later stages of the boot process. For more details, see SHE specification.
ROM Keys	N/A	**Support for ROM keys (only AES keys).**
Cryptographic	HSE_SRV_ID_HASH	**Hash service (one-pass and streaming):** * SHA1 * SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256 * Miyaguchi-Preneel compression function (SHE specification support)
	HSE_SRV_ID_MAC	**Request to generate/verify a Message Authentication Code (MAC):** * AES-CMAC, AES-GMAC * HMAC_(SHA1, SHA_224, SHA_256, SHA_384, SHA_512)
	HSE_SRV_ID_FAST_CMAC	**Low latency, high performance CMAC generate/verify request**
	HSE_SRV_ID_CMAC_WITH_ COUNTER	**CMAC generate/verify with monotonic counter**
	HSE_SRV_ID_SYM_CIPHER	**Symmetric encryption/decryption (one-pass and streaming):** * AES-128/-192/-256: ECB, CBC, CTR, OFB, CFB
	HSE_SRV_ID_AEAD	**AEAD encryption/decryption**: * AES-CCM-128/-192/-256 (one-pass, **no streaming support**) * AES-GCM-128/-192/-256 (one-pass and streaming)
	HSE_SRV_ID_SIGN	**Request a Digital Signature Generation/Verification (one-pass and streaming):** * RSASAA_PSS (1024, 2048, 3072, 4096) * RSASAA_PKCS1-v1_5(1024, 2048, 3072, 4096) * ECDSA (all supported ECC curves) * EDDSA (for ED25519 curve)
	HSE_SRV_ID_RSA_CIPHER	**RSA encryption/decryption**: * RSAES-PKCS1-v1_5 (1024, 2048, 3072, 4096) * RSAES-OEAP (1024, 2048, 3072, 4096)
RNG	HSE_SRV_ID_GET_ RANDOM_NUM	**Get a random number.** AIS31 and FIPS 140-2 compliant
Counters	HSE_SRV_ID_INCREMENT_ COUNTER	**Incrementing Non-volatile counter.**
	HSE_SRV_ID_READ_ COUNTER	**Read Non-volatile counter.**
	HSE_SRV_ID_CONFIG_ COUNTER	**Configure the secure counter.**

Table 3. *...continued*

Service Class	HSE Service ID	Description/Notes
Advance Secure Booting (SMR/CR)	HSE_SRV_ID_SMR_ENTRY_INSTALL	**Install a Secure Memory Region (SMR) table entry.**
	HSE_SRV_ID_SMR_VERIFY	**Verify (on demand) a Secure Memory Region (SMR) table entry.**
	HSE_SRV_ID_CORE_RESET_ENTRY_INSTALL	**Install a Core Reset (CR) table entry.**
	HSE_SRV_ID_ON_DEMAND_CORE_RESET	**On-demand release a core from a reset after loading and verification.**

The service below is applicable only for **AB SWAP configuration device.**

Table 4.

Service Class	HSE Service ID	Description/Notes
Administrative	HSE_SRV_ID_ACTIVATE_PASSIVE_BLOCK	**Switch to passive area.** Using this service application can switch to passive area.

14 Legal information

14.1 Definitions

Draft — A draft status on a document indicates that the content is still under internal review and subject to formal approval, which may result in modifications or additions. NXP Semiconductors does not give any representations or warranties as to the accuracy or completeness of information included in a draft version of a document and shall have no liability for the consequences of use of such information.

14.2 Disclaimers

Limited warranty and liability — Information in this document is believed to be accurate and reliable. However, NXP Semiconductors does not give any representations or warranties, expressed or implied, as to the accuracy or completeness of such information and shall have no liability for the consequences of use of such information. NXP Semiconductors takes no responsibility for the content in this document if provided by an information source outside of NXP Semiconductors.

In no event shall NXP Semiconductors be liable for any indirect, incidental, punitive, special or consequential damages (including - without limitation - lost profits, lost savings, business interruption, costs related to the removal or replacement of any products or rework charges) whether or not such damages are based on tort (including negligence), warranty, breach of contract or any other legal theory.

Notwithstanding any damages that customer might incur for any reason whatsoever, NXP Semiconductors' aggregate and cumulative liability towards customer for the products described herein shall be limited in accordance with the Terms and conditions of commercial sale of NXP Semiconductors.

Right to make changes — NXP Semiconductors reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

Applications — Applications that are described herein for any of these products are for illustrative purposes only. NXP Semiconductors makes no representation or warranty that such applications will be suitable for the specified use without further testing or modification.

Customers are responsible for the design and operation of their applications and products using NXP Semiconductors products, and NXP Semiconductors accepts no liability for any assistance with applications or customer product design. It is customer's sole responsibility to determine whether the NXP Semiconductors product is suitable and fit for the customer's applications and products planned, as well as for the planned application and use of customer's third party customer(s). Customers should provide appropriate design and operating safeguards to minimize the risks associated with their applications and products.

NXP Semiconductors does not accept any liability related to any default, damage, costs or problem which is based on any weakness or default in the customer's applications or products, or the application or use by customer's third party customer(s). Customer is responsible for doing all necessary testing for the customer's applications and products using NXP Semiconductors products in order to avoid a default of the applications and the products or of the application or use by customer's third party customer(s). NXP does not accept any liability in this respect.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at http://www.nxp.com/profile/terms, unless otherwise agreed in a valid written individual agreement. In case an individual agreement is concluded only the terms and conditions of the respective agreement shall apply. NXP Semiconductors hereby expressly objects to applying the customer's general terms and conditions with regard to the purchase of NXP Semiconductors products by customer.

Suitability for use in automotive applications — This NXP product has been qualified for use in automotive applications. If this product is used by customer in the development of, or for incorporation into, products or services (a) used in safety critical applications or (b) in which failure could lead to death, personal injury, or severe physical or environmental damage (such products and services hereinafter referred to as "Critical Applications"), then customer makes the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, safety, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP. As such, customer assumes all risk related to use of any products in Critical Applications and NXP and its suppliers shall not be liable for any such use by customer. Accordingly, customer will indemnify and hold NXP harmless from any claims, liabilities, damages and associated costs and expenses (including attorneys' fees) that NXP may incur related to customer's incorporation of any product in a Critical Application.

Export control — This document as well as the item(s) described herein may be subject to export control regulations. Export might require a prior authorization from competent authorities.

Translations — A non-English (translated) version of a document, including the legal information in that document, is for reference only. The English version shall prevail in case of any discrepancy between the translated and English versions.

Security — Customer understands that all NXP products may be subject to unidentified vulnerabilities or may support established security standards or specifications with known limitations. Customer is responsible for the design and operation of its applications and products throughout their lifecycles to reduce the effect of these vulnerabilities on customer's applications and products. Customer's responsibility also extends to other open and/or proprietary technologies supported by NXP products for use in customer's applications. NXP accepts no liability for any vulnerability. Customer should regularly check security updates from NXP and follow up appropriately.

Customer shall select products with security features that best meet rules, regulations, and standards of the intended application and make the ultimate design decisions regarding its products and is solely responsible for compliance with all legal, regulatory, and security related requirements concerning its products, regardless of any information or support that may be provided by NXP.

NXP has a Product Security Incident Response Team (PSIRT) (reachable at PSIRT@nxp.com) that manages the investigation, reporting, and solution release to security vulnerabilities of NXP products.

14.3 Trademarks

Notice: All referenced brands, product names, service names, and trademarks are the property of their respective owners.

NXP — wordmark and logo are trademarks of NXP B.V.

Tables

NXP Semiconductors

Release Notes

for S32K3XX HSE Firmware 0.2.6.0

Contents

For more information, please visit: http://www.nxp.com

Date of release: 9 December 2022
Document identifier: HSE_FW_S32K3XX_0_2_6_0_ReleaseNotes