Release Notes

for S32G2 HSE Firmware 0.1.0.5

Rev. 1.0 — 15 April 2022 Release notes

COMPANY CONFIDENTIAL

1 Getting Started

IMPORTANT NOTES:

This is the Standard Package variant of the HSE Firmware for S32G2.

This is an **Update** to Release and has **Ready for Production** quality level in terms of features, documentation and testing.

1.1 Package content

This package contains the NXP S32G2 HSE Firmware 0.1.0.5:

- HSE Firmware: encrypted binary
- HSE Firmware interface files
- HSE Service API RM
- `HSE_FW_S32G2_0.1.0.5_ReleaseNotes.pdf` – this file
- The license.txt EULA file and the `uninstall.exe` utility for removing the HSE FW binary

Note:

Demo Application is provided separately and contains details on how to provision HSE FW on virgin devices and demonstrates common use cases of its security features.

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

- *HSE Firmware Reference Manual*

1.2 Installation

Follow the install steps in the demo application.

If targeting the usage of AUTOSAR software stack in the application, it is recommended to install also the RTD crypto driver from the S32G2XX AUTOSAR RTD package by following its installer steps.

2 Release Details

This is the HSE Firmware 0.1.0.5 release for the S32G2 platform.

The provided example code shows how to set up and use the HSE FW and to perform basic crypto operations (refer to the documentation that comes with the demo application). The examples show how to:

- Boot the demo application (secure mode)
- Load the firmware
- Load the key(s)
- Perform crypto operations

This release was developed and tested using:

- Chip: PS32G274ABVUC-0P77B (Rev 2.0)
- Design Board: S32G-VNP-RDB2 (700-47440 REV X2)

Standard HSE Firmware package contains the following configuration:

- 20 RAM keys, 40 NVM symmetric keys, 12 NVM asymmetric keys
- 4 SMR entries, 4 CR entries
- Support only for ECC-256bits and CURVE25519 curve (Montgomery and Twisted)
- Maximum key size limitations: HMAC - 512bits, ECC - max 256bits, RSA- max 2048bits
- SHA3 and IPSec services are not supported

For the Premium Package variant, the customers would need to purchase "premium S32G2 security parts" (to run Premium Package variant in production).

Implemented Errata:

- ERR051257 - BootROM: The boot sequence can hang if the QSPI interrupt pin transitions low during boot.

2.1 Supported Derivatives

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

- S32G274A
- S32G254A
- S32G233A
- S32G234M

2.2 Device Bricking scenario for HSE Firmware

- **N/A**

2.3 Security Aspects

The current release of HSE Firmware implements countermeasures providing protection against remote and local software attacks.

3 Change Logs in 1.0.5

Fixed

- HSE FW does not support a different length of the iteration counter for SP800-108 and SP800-56C-TwoStep KDF schemes besides 32 bits. *(ASHF-4420)*
  - SP800-108 service now allows specifying 1 or 2 bytes counter length.
  - Note that the default value of the iteration counter is still 4 bytes and any value except 1 byte (`HSE_KDF_SP800_108_COUNTER_LEN_1`) or 2 bytes (`HSE_KDF_SP800_108_COUNTER_LEN_2`) will be interpreted as the default length (4 bytes).
  - It is recommended that the field is initialized explicitly, but if not possible, any existing application using the service with its previous interface should make sure the reserved fields of the service descriptor are initialized to 0 to avoid unexpected errors.

4 Change Logs in 1.0.4

Fixed

- HSE FW does not handle ECC errors in program images (i.e. SYS_IMG, SMR, AppBL in basic secure boot) when loading from external flash via the QSPI if the QSPI interrupt pin is connected to the external flash and this pin transitions low *(ASHF-4751)*
  - HSE clears the ECC error bits in QSPI.FR until HSE_STATUS_INIT_OK status bit is set
  - This is in the context of *ERR051257*. The recommendation is to apply one of the proposed solutions that will also cover the above cases.
- HSE is non-operational when loading a valid SYS_IMG partially (BOOT_SEQ=0) *(ASHF-4756)*
- HSE status and error bits are not updated on the application side (MU.FSR and MU.GSR) until HSE_STATUS_INIT_OK is set *(ASHF-4782)*
- ST-DCD cannot be signed/verified using the HSE FW boot data sign/verify services *(ASHF-4828)*

5 Change Logs in 1.0.1

Added

- Service `HSE_SRV_ID_CMAC_WITH_COUNTER` (see `hseCmacWithCounterSrv_t`)
- Service `HSE_SRV_ID_VERIFY_SYS_IMAGE` to verify SYS-IMG integrity after it is written in the external flash (see `hseVerifySysImageSrv_t`)
- Service `HSE_SRV_ID_SELF_TEST` (see `hseSelfTestSrv_t`)
- NVM Attribute `HSE_RAM_PUB_KEY_IMPORT_POLICY_ATTR_ID`. New key management policy regarding import of the RAM public keys. (see `hseAttrRamPubKeyImportPolicy_t`)
- Secure ADKP Provisioning: the ADKP can be provisioned in an encrypted format by securely importing a key (via import key service) in a key slot and then using that key slot to initialize ADKP in fuse memory (see `hseAttrSecureApplDebugKey_t`)
- Support for “Extended Master Secret” option in TLS 1.2 PRF scheme.
- Generation of the pre-master secret for TLS 1.2 RSA key exchange. (see `hseKeyGenTls12RsaPreMaster_t`)
- Option `HSE_ERASE_KEYGROUP_ON_MU_IF` in erase key service to erase the entire key group (see `hseEraseKeySrv_t`)
- Optional version offset in SMR where the image version can be stored. It may be used to protect against anti-rollback attacks during the update. Ignored if set to `HSE_SMR_VERSION_NOT_USED` (see `hseSmrEntry_t`)
- HSE FW automatic handling of VDD_EFUSE pin during start-up. Configuration resides in IVT and is used during the start-up with an updated HSE FW/SYS-IMG to connect VDD_EFUSE pin to 1.8V temporarily

Updated

- Filter Duration (from *hseAttrPhysicalTamper_t*) is a must requirement for Active Tamper and optional for Passive Tamper.
- Key Import:
  - RAM provision keys can now be imported only authenticated and can be used only to import 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.
- Monotonic counters:
  - SuperUser rights are needed to configure/enable the monotonic counters.
- `HSE_STREAM_COUNT` increase from `2` to `4`.
- Fixed the initialization sequence when the SYS-IMG loading fails.
- Improved firmware vulnerability and interface.

6 Change Logs in 0.9.2 (hotfix)

Fixed

- HSE reports a fatal error when multiple requests of different priority levels are issued concurrently. This impacts the parallel execution of a subset of the high priority services (service ID: *0xXXA5XXXX*) that are processed synchronously by HSE with a subset of the low priority services that are using the symmetric crypto accelerator. *(ASHF-3492)*

API updates

- *HSE_SRV_ID_GET_RANDOM_NUM* macro value updated.

7 Change Logs in 0.9.1 (hotfix)

Removed

- 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)*

Fixed

- Encrypted SMRs not linked with CR table that have the periodic checks enabled are not decrypted when loaded in RAM during start-up. SMRs that are loaded at run-time (linked with CR on-demand entries or not linked at all) can be used for periodic checks only without encryption. *(ASHF-3306)*
- OTFAD installation/update does not trigger a correct update of the SYS_IMG and publishing it, in this case, outputs corrupted content. *(ASHF-3434)*
- OTFAD module will not be enabled if ALL installed regions have the *HSE_OTFAD_CTX_INACTIVE_ON_BOOT* flag set. *(ASHF-3322)*
- HSE goes to shutdown mode, becoming non-operational if RNG initialization fails at start-up. *(ASHF-3435)*
- The key catalogs referenced in the Format Key Catalogs service request cannot be in the address range above the first 3.5 GB. *(ASHF-3148)*
- The key generation service for RSA and ECC is not providing the correct public key. *(ASHF-3049)*
- Loading a SHE RAM Key using a key that has the DEBUG PROT flag set fails (returns “key not available”). *(ASHF-3309)*
- Export a SHE RAM Key using the Master ECU key that has the DEBUG PROT flag set fails (returns key not available). *(ASHF-3310)*
- SMR verify request using RSA authentication scheme returns INVALID_PARAM instead of VERIFY_FAILED when the signature is not flashed. *(ASHF-2957)*

8 Change Logs in 0.9.0

Added

- Handling of tamper violations: clock monitoring (CMU), temperature sensor (TMU), and physical tamper.
- Service *HSE_SRV_ID_SIPHASH* (see *hseSipHashSrv_t*)
- Service *HSE_SRV_ID_XTS_AES_CIPHER* (see *hseXtsAesCipherSrv_t*)
- Service *HSE_SRV_ID_PREPARE_FOR_STANDBY*. This service must be called by the host before entering standby mode.
- 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).
- 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 access to the 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.

Updated

- Interface comments
- SHE keys catalog formatting must be configured for the *HSE_KEY_OWNER_ANY* group owner.
- Secure Memory Regions (SMR):
  - 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 400MHz frequency)
- Core Reset:
  - Updated Core Reset entries to include *PRE-BOOT*, *ALT_PRE_BOOT,* and *POST-BOOT* SMR bitfields.
  - 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)
  - Added *HSE_CORE_RESET_RELEASE_ATTR_ID* attribute to configure the release-from-reset strategy:
    - all-at-once (cores are released all at once after all boot SMRs are verified);
    - one-by-one (cores are released one by one as soon as the boot SMR(s) verification passed for that core)
- 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
- If VDD_EFUSE is connected to GROUND and a fuse needs to be written, the HSE FW returns an error.

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.

9 Change Logs in 0.8.5

Added

- *HSE_HOST_PERIPH_CONFIG_DONE* event sent from host to HSE (writing the MUB_GCR register) to signal when the system and QSPI/SD/eMMC clock configuration were updated by application (see *hseHostEvent_t*)
- CRC32 service (see *hseCrc32Srv_t* service)
- On-the-fly AES decryption support (see *hseInstallOtfadContextSrv_t*, *hseActivateOtfadContextSrv_t*, *hseGetOtfadContextSrv_t*)
- Scatter-Gather support for RSA and ECDSA signature (refer to *hseSignSrv_t)*
- New HSE attributes (see *hseAttrId_t*):
- *HSE_AVAIL_ANTI_ROLLBACK_COUNTER_ATTR_ID* – The anti-rollback counter updates left
- *HSE_FW_PARTITION_ATTR_ID* – specifies the partition (primary or backup) used by BootROM to load the HSE Firmware (only for Rev2.0)
- *HSE_OTFAD_CTX_STATUS_ATTR_ID* – returns the OTFAD context status

Updated

- Interface comments
- 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 is supporting 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*)
- Publish SYS-IMG service: publish SYS-IMG in chunks was removed (see *hsePublishSysImageSrv_t*)
- TLS1.2 KDF to support KEY-EXCHANGE-PSK and KEY-EXCHANGE-ECDHE-PSK (see *hseKdfTLS12PrfScheme_t*)
- HMAC to support key sizes greater than hash block size (updated *hseMacSrv_t* service)
- Firmware Update service to return the total length of published HSE FW (see *hseFirmwareUpdateSrv_t*)
- Encrypt-then-MAC operation (see *hseAuthEncSrv_t* service) to support addition combination AES_CFB/OFB-THEN-HMAC.
- Erase service to delete the SHE keys only if system authorization was performed beforehand using the MASTER_ECU key. Other keys (non-SHE keys) can be erased if the authorization operation was performed using any key type, including the 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 SuperUser 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.

- Core Reset (CR) / Secure Memory Regions (SMR) (see *hseSmrEntry_t*, *hseCrEntry_t*):
  - Added support for SMR periodic check
  - Updated CR to support an Alternative SMR(s) verification (called PRE_BOOT_ALT) if the PRE_BOOT SMR(s) verification fails.
  - Defined *HSE_SMR_VERIF_RUN_TIME_MASK* verification method used only for on-demand SMR verification
  - For non-secure boot (BOOT_SEQ=0), the SMRs are not loaded at boot time. The application can use the *hseSmrVerifySrv_t* service to load and verify the SMR (for validation purposes)
  - Updated the SHE Secure Boot used with SMR entry#0 (see *hseSmrEntryInstallSrv_t* comments)
  - Updated *hseSmrVerifySrv_t* service to:
    - loads and verifies the RUN_TIME SMR (if loaded before, HSE will perform only the verification)
    - PRE-BOOT, PRE-BOOT-ALT, or POST-BOOT SMR can be verified on-demand only if:
      - it was loaded at boot-time (only verification in SRAM is performed)
      - or the *BOOT_SEQ = 0*: the first call will trigger the load and verification; the next call will perform only the verification in SRAM.

Removed

- *HSE_FLASH_PAGE_SIZE_ATTR_ID* attribute

10 List of Limitations Existing in This Release

- VDD_EFUSE must be connected to *1.8V* to write the HSE fuse area. If VDD_EFUSE is connected to *GND*, the HSE fuse area can only be read (cannot be written).
  The fuses are written:
  - By the application, through the Set Attribute service (e.g. life cycle, ADKP key, debug authorization method, etc.). In this case, the application must supply power (1.8V) to the VDD_EFUSE pin.
  - By HSE FW, at start-up with an updated HSE FW/SYS-IMG. To connect VDD_EFUSE to *1.8V* during start-up, the configuration words within IVT shall be used.
- Limited tests were performed on services using 40 bits addresses.
- During SD card booting, the last 4KB (*start_address = 0x347FF000, length = 0x1000*) and first 32KB (*start_address = 0x34000000, length = 0x8000*) from SRAM are used. These memory regions can be used by the application after a successful HSE initialization (HSE status shall be *HSE_STATUS_INIT_OK* for *BOOT_SEQ = 0* and *HSE_STATUS_BOOT_OK* for *BOOT_SEQ = 1*).
- Defining SMR entries that are checked periodically may impact the overall HSE FW performance.
- The quality of random number generation (RNG) is guaranteed between 200MHz and 400MHz *XBAR_CLK*. If the *XBAR_CLK* is below 200Mhz, the required source of entropy is not ensured for the services that use the RNG module (e.g. asymmetric cryptographic services, random number generation service).
- SipHash variant *HSE_SIPHASH_VARIANT_32* is not supported.

11 List of Services Available

***Note:** **All available HSE features/services** are also listed in the `hse_h_config.h` file (from HSE Interface). All other features not listed in the table below (or enabled in `hse_h_config.h` file) **are NOT supported**.*

Table 1.

Service Class	HSE Service ID	Description/Notes
Administrative	HSE_SRV_ID_SET_ATTR	**Set an HSE attribute**. Attributes related to FUSE 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 canceled if it is in the processing queue and NOT passed to the hardware to be executed.
	HSE_SRV_ID_FIRMWARE_UPDATE	**HSE firmware update** (generates the HSE FW blue image)
	HSE_SRV_ID_SYS_AUTH_REQ	**SYS Authorization request** used to be granted with CUST/OEM SuperUser rights
	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 IVT, DCD & SELF TEST images**. Also, signs the APP image for Basic Secure Boot (BSB).
	HSE_SRV_ID_BOOT_DATA_IMAGE_VERIFY	**Verify the signature on IVT, DCD & SELF TEST images.** Also, verifies the APP image for Basic Secure Boot (BSB).
	HSE_SRV_ID_IMPORT_EXPORT_STREAM_CTX	**Import and Export service for the crypto streaming context.**
	HSE_SRV_ID_PUBLISH_SYS_IMAGE	**Publish SYS-IMAGE file in System RAM.**
	HSE_SRV_ID_GET_SYS_IMAGE_SIZE	**Get SYS-IMAGE size.**
	HSE_SRV_ID_VERIFY_SYS_IMAGE	**Verify SYS-IMAGE integrity after it is written in the external flash.**
	HSE_SRV_ID_PUBLISH_LOAD_CNT_TBL	**Request to publish/load the NVM container for the Monotonic Counter table**
	HSE_SRV_ID_INSTALL_OTFAD_CTX	Install an On-The-Fly AES Decryption (OTFAD) context.
	HSE_SRV_ID_ACTIVATE_OTFAD_CTX	Activate on-demand OTFAD context
	HSE_SRV_ID_GET_OTFAD_CTX	Get OTFAD context information
	HSE_SRV_ID_PREPARE_FOR_STANDBY	Prepare HSE before the system goes to Stand-by mode
	HSE_SRV_ID_SELF_TEST	Performs a self-test on a specific security block or a full self-test. (HSE FW integrity, RNG, AES, HASH, MAC, CRC, RSA, ECC)

Table 1. *...continued*

Service Class	HSE Service ID	Description/Notes
	HSE_SRV_ID_CONFIG_ COUNTER	Configures the monotonic counters
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 (which are 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).**
	HSE_SRV_ID_ERASE_KEY	**Erase NVM/RAM key(s).** Erase key service depends on authorization rights. One or multiple keys can 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 depend 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 depend 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 * Brainpool curves: BRAINPOOLP256R1 * Montgomery curve: CURVE25519 * 3 user-defined ECC curves (see Load ECC curve service)
	HSE_SRV_ID_KEY_DERIVE	**Perform a key derivation function:** * NXP Generic KDF, Extract KDF, SP800_56C One Step, SP800_56C Two Step, SP800_108 (Only Counter Mode), ANS_X963, ISO/IEC 18033 KDF2, ISO/IEC 18033 KDF1, PBKDF2HMAC, HKDF, IKEV2, TLS12PRF
	HSE_SRV_ID_KEY_DERIVE_ COPY	**Extract a key from the derived key material to a key slot.**
	HSE_SRV_ID_SHE_LOAD_ KEY	**Load a SHE key** using the SHE memory update protocol.
	HSE_SRV_ID_SHE_LOAD_ PLAIN_KEY	**Load the SHE RAM key** as plain text.

Table 1. *...continued*

Service Class	HSE Service ID	Description/Notes
	HSE_SRV_ID_SHE_EXPORT_RAM_KEY	**Export the SHE RAM key.**
	HSE_SRV_ID_SHE_GET_ID	**Get UID 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).**
Crypto	HSE_SRV_ID_HASH	**Hash service (one-pass and streaming):** * MD5 * 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, AES-XCBC-MAC * HMAC_(MD5, SHA1, all SHA2)
	HSE_SRV_ID_FAST_CMAC	**Low latency, high-performance CMAC generate/verify the request**
	HSE_SRV_ID_CMAC_WITH_COUNTER	Generates/verifies the CMAC of a given input message concatenated with a selected secure 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) * RSASAA_PKCS1-v1_5(1024, 2048) * ECDSA (all supported ECC curves) * EDDSA (for ED25519 curve)
	HSE_SRV_ID_RSA_CIPHER	**RSA encryption/decryption**: * RSAES-PKCS1-v1_5 (1024, 2048) * RSAES-OEAP (1024, 2048)
	HSE_SRV_ID_AUTHENC	**Combined Authenticated Encryption service:** ***AES_(ECB, CBC, CTR, CFB, OFB) -THEN- HMAC_ (MD5, SHA1, SHA2_224, SHA2_256, SHA2_384, SHA2_512) for “Encrypt-then-MAC” *NULL cipher with all MAC algorithms (CMAC, GMAC, XCBC_MAC, HMAC(MD5, SHA1, SHA2))
	HSE_SRV_ID_CRC32	**Computes CRC32 checksum.**
	HSE_SRV_ID_SIPHASH	**SipHash** is optimized for fast processing speeds when used to authenticate small messages. (MACs)

Table 1. *...continued*

Service Class	HSE Service ID	Description/Notes
	HSE_SRV_ID_XTS_AES_ CIPHER	**XTS AES encryption/decryption**
RNG	HSE_SRV_ID_GET_RANDOM_ NUM	**Get a random number.** AIS31 and FIPS 140-2 compliant
Counters	HSE_SRV_ID_INCREMENT_ COUNTER	**Incrementing volatile counters.** The Counter table can be published and load as an encrypted and authenticated blob using the HSE_SRV_ID_PUBLISH_LOAD_CNT_ TBL service.
	HSE_SRV_ID_READ_ COUNTER	**Read volatile counters.**
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**

12 Legal information

12.1 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.

12.2 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.

Suitability for use — NXP Semiconductors products are not designed, authorized or warranted to be suitable for use in life support, life-critical or safety-critical systems or equipment, nor in applications where failure or malfunction of an NXP Semiconductors product can reasonably be expected to result in personal injury, death or severe property or environmental damage. NXP Semiconductors and its suppliers accept no liability for inclusion and/or use of NXP Semiconductors products in such equipment or applications and therefore such inclusion and/or use is at the customer's own risk.

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.

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.

Evaluation products — This product is provided on an "as is" and "with all faults" basis for evaluation purposes only. NXP Semiconductors, its affiliates and their suppliers expressly disclaim all warranties, whether express, implied or statutory, including but not limited to the implied warranties of non-infringement, merchantability and fitness for a particular purpose. The entire risk as to the quality, or arising out of the use or performance, of this product remains with customer. In no event shall NXP Semiconductors, its affiliates or their suppliers be liable to customer for any special, indirect, consequential, punitive or incidental damages (including without limitation damages for loss of business, business interruption, loss of use, loss of data or information, and the like) arising out the use of or inability to use the product, whether or not based on tort (including negligence), strict liability, breach of contract, breach of warranty or any other theory, even if advised of the possibility of such damages. Notwithstanding any damages that customer might incur for any reason whatsoever (including without limitation, all damages referenced above and all direct or general damages), the entire liability of NXP Semiconductors, its affiliates and their suppliers and customer's exclusive remedy for all of the foregoing shall be limited to actual damages incurred by customer based on reasonable reliance up to the greater of the amount actually paid by customer for the product or five dollars (US$5.00). The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails of its essential purpose.

Translations — A non-English (translated) version of a 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 or documented vulnerabilities. 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.

12.3 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.

NXP Semiconductors

Release Notes

for S32G2 HSE Firmware 0.1.0.5

Contents

For more information, please visit: http://www.nxp.com
For sales office addresses, please send an email to: salesaddresses@nxp.com

Date of release: 15 April 2022
Document identifier: HSE_FW_S32G2_0.1.0.5_ReleaseNotes.pdf