Release Notes

for S32G3 HSE Firmware 0.2.51.0

Rev. 1.0 — 23 April 2024

Release notes
CONFIDENTIAL

1 Getting Started

IMPORTANT NOTES:

This is the Standard Package variant of the HSE Firmware for S32G3.

This release is a Service Release and has RFP (Release For Production) quality in terms of testing and quality documentation. Service Release contains all features and is fully tested on Customer Engineering Samples or Qual Intend Samples. The RFP release is software release that can be used in cars production. RFP release is delivered with complete software documentation and quality package.

1.1 Package content

This package contains the NXP S32G3 HSE Firmware 0.2.51.0:

- HSE Firmware (encrypted binary)
  - HW
  - Rev 1.1 (latest version of the SoC)
- HSE Firmware interface files
- HSE Service API RM
- HSE Security Installation Guide
- `HSE_FW_S32G3_0.2.51.0_ReleaseNotes.pdf` – this file
- The `license.txt` EULA file and `ApacheLicense2.0.txt`
- 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.

The following associated documentation can be obtained from the NXP website (https://www.nxp.com), Sign In / Register > My NXP Account > Secure Files:

- HSE Firmware Reference Manual – Rev 2.2

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 AUTOSAR RTD package for the targeted platform by following its installer steps.

2 Release Details

This is the HSE Firmware 0.2.51.0 release for the S32G3 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:
  - P32G399AAK1CVUC (rev 1.1)
- Design Board: S32G-VNP-EVB

Standard HSE Firmware package contains the following configuration:

- 20 RAM keys, 40 NVM symmetric keys, 12 NVM asymmetric keys
- 8 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, IPSec, Classic DH and Burmester-Desmedt services are not supported
- CURVE448 is not supported (Montgomery and Twisted)

Note:

- The release package provides the firmware image for rev 1.1 of the S32G3XX chip.
- For the Premium Package variant, the customers would need to purchase “premium S32G3 security parts” (to run Premium Package variant in production).

Ensure that the proper SoC revision and the latest HSE Firmware version are used.

Implemented Errata:

- ***ERR051655*** erratum - OCOTP: Incorrect data may be read from fuses after software power down and up of the fusebox.

2.1 Supported Derivatives

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

- S32G399A

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 Known issues

- Do not enable the temperature sensor violation in HSE firmware using the hseTempSensVioConfig_t attribute. At random points in time, a false measurement can be reported by the Temperature Monitoring Unit (TMU) and HSE goes into shutdown mode.

4 Change Logs in 0.2.51.0

Added

- Extended the disableOtpRollbackProtect parameter of hseOtpRollback ProtectionPolicy_t attribute to include the HSE_ON_DEMAND_ANTI_RBC_UPDATE option: the rollback protection mechanism is enabled, and the anti-rollback counter can be updated in fuses only on-demand by calling the hseOnDemandAntiRbcUpdateSrv_t service.
- Added the hseOnDemandAntiRbcUpdateSrv_t service that can be used to update on demand the anti-rollback counter in fuse (of SYS-IMF or/and FW IMG). This service can be used only if disableOtpRollbackProtect == HSE_ON_DEMAND_ANTI_RBC_UPDATE (refer to hseOtpRollbackProtectionPolicy_t attribute).
- Added hseFirmwareVerifySrv_t service to verify on demand the blue or pink firmware image (in external flash or SRAM)
- Added the hseAttrOtpBootSeq_t attribute (OTP_BOOT_SEQ) to enforce the BOOT_SEQ flag in IVT not to be changed to 0 in secure boot mode. If IVT_BOOT_SEQ == 1 (secure boot), this attribute can be used to set the in OTP_BOOT_SEQ in fuses. At start-up, HSE verifies the value of OTP_BOOT_SEQ (from fuses) against the value of IVT_BOOT_SEQ as follows: if(LC == OEM_PROD or IN_FIELD) and (OTP_BOOT_SEQ == 1) and (OTP_BOOT_SEQ != IVT_BOOT_SEQ), apply a functional reset; otherwise, continue the boot sequence.
- Added the read-only hseRbCounterInfo_t attribute to provide:
  - the OTP counter for SYS-IMG
  - the OTP counter for FW-IMG
  - the counter from SYS-IMG header (returns 0xff if the SYS-IMG was not loaded)
  - the counter from blue FW header (returns 0xff if the firmware was loaded from the pink FW image).
- Updated `hseKeyVerifySrv_t` service: added support to verify the asymmetric keys inside HSE key store (public key, key pair, or _PUB_EXT keys) providing a SHA256 or CMAC tag. Removed the SHA384 or SHA2_512 options.
- Added `HSE_SRV_RSP_RNG_INIT_IN_PROGRESS` service response: this response status can be received when the Get Random Number service is called and the RNG initialization is in progress. The application can try again later.
- Added the `hseDisablePairWiseConsistencyTest_t` attribute (SET-ONLY-ONCE-ATTR attribute) to disable the pair-wise consistency check when importing an ECC/RSA key pair to increase the key import performance. By default, HSE checks the pair-wise consistency.

Updated

- Enhanced security countermeasures (code hardening).
- For the `hseSignSrv_t` service, if the `bInputIsHashed` parameter is set to TRUE and the `hashAlgo` for the `signScheme` scheme is provided, HSE checks that the `inputLength` is equal to the hash output length.
- NXP ROM provision keys cannot be used to export keys.
- When rollback protection is enabled and status bit `HSE_WA_OTP_FUSE_WRITE_FAILURE_ ON_BOOT` is set, the application should trigger a destructive reset or POR such that the HSE firmware retries programming the fuse.
- Reduced `HSE_MAX_NUM_OF_SGT_ENTRIES` to 16 entries (instead of 32).
- Reduced `MAX_STREAMING_CONTEXT_SIZE` to 372 bytes (instead of 616 bytes).
- Default `HSE_DEFAULT_MIN_FAST_CMAC_TAG_BITLEN` is 32 bits (instead of 64).
- Super User (SU) rights are no longer mandatory for storing the application specific data in persistent memory via `HSE_APP_SPECIFIC_DATA_ATTR_ID` attribute (refer to `hseAppSpecificData_t` structure).
- Improved the HSE Service API Reference Manual.

Fixes

- HSE entered shutdown mode with fatal error GSR= 0x73080001: when the RNG re-initialization is triggered due to a reseed failure (RNG reseeding can fail), it shall not be interrupted by high-priority crypto operation such as AES encryption.
- HSE entered shutdown mode with fatal error GSR=0x33AA0001: Fix the race condition when the watchdog idle/running state changes.
- The host cannot access the shared memory when HSE is in shutdown mode; make HSE-host shared memory accessible by host (even if HSE went to shutdown mode).
- The input length cannot zero for ECDSA
- The second public key of the Burmester-Desmedt HSE service cannot be exported
- Fix the boot sequence when the VDD_EFUSE is grounded and the FW or SYS_IMG are not updated.
- Do not allow monotonic counter read/increment if the counter table loading fails

5 Change Logs in 0.2.22.0

Added

- Added the firmware build information attribute (see `HSE_FW_BUILD_INFO_ATTR_ID`). This is a read-only attribute that provides a 8-byte unique ID, the date and time of the build.
- Added `HSE_DISABLE_APP_SPECIFIC_DATA_WRITE_ATTR_ID` attribute (see `hseDisableAppSpecificDataWrite_t` structure) which disables writing of application-specific data in SYS-IMG (disable writing of the `HSE_APP_SPECIFIC_DATA_ATTR_ID` attribute).
- An ECC private key can be imported without providing the public key. The public is computed internally from the private key.
- Indirect SYS-IMG access: the SYS-IMG pointer from IVT can point to a list of 16 addresses/entries (instead of pointing directly to the SYS-IMG location). An non-empty entry has the address value different from 0xFFFFFFFF. At reset, HSE firmware parse the entry-list (from 0 to 15) to find the lasted non-entry entry, and uses the address found to read-out the SYS-IMG. In this way, the SYS-IMG can be written at multiple flash locations. To enable this indirect access of the SYS-IMG, the IVT must be configured to include a marker at a specific offset in IVT (refer the HSE Firmware reference manual).

Updated

- Updated the fuse read/write handlers to cover ***ERR051655*** erratum. Additional code hardening was included. **Ensure that the latest HSE Firmware is used.**
- Enhanced security countermeasures (code hardening).
- Update the register address for `HSE_GPR_STATUS_ADDRESS`
- Updated the `HSE_APP_SPECIFIC_DATA_ATTR_ID` attribute that allow to store application-specific data in SYS-IMG (persistent memory); refer to `hseAppSpecificData_t` structure.
- Updated the Publish SYS-IMG service (`hsePublishSysImageSrv_t`): the `HSE_PUBLISH_UPDATED_DATA_SET` option was removed.
- Allow Lifecycle advancement without Super User Rights.
- Increased the performance for EdDSA signature verification for big data
- Enhanced the Firmware Update service: code hardening and added additional checks
- Improved the HSE Service API Reference Manual (HSE header files comments).
- Increased the plaintext FW image size by 32KB. The size of the image as provided by NXP (pink image) is 389KB.

Fixed

- The first RSA signature verify costs 6x times than the same service requested after that
- Incorrect AES-GCM tag is computed when IV counter wraps
- An encrypted SMR install request from flash with a large SMR size cause HSE to go to shutdown mode
- A self-test firmware integrity request without a prior publish sys-image request cause HSE to go to shutdown mode
- Anti-rollback counter for the HSE FW blue image is incremented twice at first installation. Note that the rollback protection for HSE FW blue image can be disabled using an SYS-IMG attribute.
- Set the `HSE_FW_ROLLBACK_MARKER` marker in `BOOT_POR_CTRL_REG` register if at least one host core is booted
- Removed the QSPI reads done by HSE at start-up after booting the application core(s).
- If the length of the shared secret slot is >= 256 bytes, the TLS 1.2 KDF pre-master computation using DHE-PSK schemes failed.

6 Change Logs in 2.16.1

Added

- Support for boot data images (IVT/DCD/ST-DCD/AppBL for BSB) MAC generation/verification for the new HW revision – `hseBootDataImageSignSrv_t` and `hseBootDataImageVerifySrv_t` updated:
  - On previous revision (1.0), these services are using a static IV, HSE FW giving as output at signature generation only the GMAC
  - On latest revision (1.1), when generating the signature, a random IV is generated by the HSE FW and returned to the application (along with the GMAC). This IV needs to be incorporated into the image at the fixed offset (as per SoC RM). When verifying the GMAC using the HSE FW service, the IV has to be already part of the image.
  - HSE FW supports these services for both revisions, however the generated artifacts are not interchangeable – i.e. an IVT authenticated for the previous revision cannot be used on the newer revision and vice versa.
  - Revision can be read from `SIUL2_0.MIDR1` register
- Support for HSE FW released image for the new HW revision
  - The two encrypted binaries cannot be interchanged – i.e. the image for the previous revision (1.0) cannot be used on the newer revision and vice versa
- Support for Extend Key Catalog service - `hseExtendKeyCatalogSrv_t`
- Support for ROM public keys - `HSE_ROM_KEY_ECC256_PUB_KEY0`
- Support for a new attribute by which application specific data can be stored in the SYS_IMG - `hseAppSpecificData_t`
- Support for SGT input in CMAC with counter service - `hseCmacWithCounterSrv_t`
- Support for SMR verification options when performing on-demand, run-time verification - `hseSmrVerificationOptions_t`
- Support for SMR/CR entry erase - `hseSmrEntryEraseSrv_t hseCrEntryEraseSrv_t`
- Support for handling data provided in the DDR0 (1.5G-2G) range for HSE descriptor, input for SipHash and input for Pure-EDDSA

Updated

- Increased maximum number of regions configurable via the attribute `HSE_MEM_REGIONS_PROTECT_ATTR_ID` – from 6 to 12 regions per MU
- Increased representation of the key counter for the NVM non-SHE keys - `hseKeyInfo_t` – from 28 bits to 32 bits
- Minimum number of iterations for PBKDF2 – 100
- Minimum length of IV used with the GMAC scheme for key import/export in an authenticated container – 12 bytes
- Internal scheduler by increasing 5 times the time slot allocated for the fast jobs' execution
- SMR periodic checks are disabled until the next reset if the associated SMR is updated
- Enhanced HSE FW update service
- Enhanced reactions to tamper violations
- Enhanced security countermeasures

Fixed

- Anti-rollback counter for the HSE FW blue image is incremented twice at first installation
- TLS 1.2 KDF pre-master computation using DHE-PSK schemes and shared secret with length >= 256 bytes fails
- When HSE FW is running from the backup location, after eight consecutive functional resets HES does not respond

- When BOOT_SEQ=1 and HSE FW is running from primary location but fails before complete initialization (e.g. not application boots), the device will go in serial boot mode before attempting to run HSE FW from the backup location

7 Change Logs in 0.21.0

Added

- NVM attribute for configuring the policy on HSE FW rollback protection - `hseOtpRollbackProtectionPolicy_t`. Can be used to enforce HSE FW to boot only from device-specific (blue image) and/or to disable the rollback protection altogether
- NVM attribute to configure HSE reaction to a tamper violation – it can either go to shutdown or directly issue a reset - `hseResetSocOnTamper_t`
- AAD support for encrypted SMR - `hseSmrDecrypt_t`
- Support for compressed ECC keys - `hseEccKeyFormat_t`
- Key verify service - `hseKeyVerifySrv_t` – verifies a hash/MAC (provided by the application) over a symmetric key from HSE key store
- `HSE_KF_USAGE_XTS_TWEAK` usage flag that must be set for AES-XTS tweak keys
- SGT support for AES-XTS service
- `HSE_KF_USAGE_OTFAD_DECRYPT` usage flag that must be set for keys used for OTFAD decryption
- 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
- The key derive copy restrictions on starting offset and number of bytes extracted - `hseKeyDeriveCopyKeySrv_t`
- Support for different lengths of the iteration counter for SP800-108 and SP800-56C-TwoStep KDF schemes besides 32 bits; refer to `hseKdfSP800_108Scheme_t`

Updated

- Increased HSE raw FW (plaintext FW) size by 32KB. The size of the image as provided by NXP (pink image) is 357KB.
- Policy on encrypted keys import/export. If encrypted, it must also be authenticated
- TLS 1.2 pre-master secret generation and KDF - `hseKeyGenTls12RsaPreMaster_t` and `hseKdfTLS12PrfScheme_t`
- OTFAD services by adding the instance number
- Minimum MAC length to 16 bytes for plain SMR initial authentication proof, authenticated key import/export and system authorization services
- Minimum MAC length to 8 bytes for MAC service

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
  - HSE clears the ECC error bits in QSPI.FR until HSE_STATUS_INIT_OK status bit is set
- HSE is non-operational when loading a valid SYS_IMG partially (BOOT_SEQ=0)
- HSE status and error bits are not updated on the application side (MU.FSR and MU.GSR) until HSE_STATUS_INIT_OK is set
- ST-DCD cannot be signed/verified using the HSE FW boot data sign/verify services
- The quality of random number generation not being ensured if XBAR_CLK is below 200MHz

Removed

- MD5 support
- SHA1 support for key derivation services
- HMAC and CMAC support as PRF for NXP Generic KDF scheme
- SipHash variant `HSE_SIPHASH_VARIANT_32` and the support of 64-bits SipHash keys

- Specific fatal error events for tamper violations - `hseError_t`

8 List of Limitations Existing in This Release

- The RNG re-initialization is triggered at the first call of the following services: `HSE_SRV_ID_GET_RANDOM_NUM`, `HSE_SRV_ID_KEY_GENERATE` or `HSE_SRV_ID_SYS_AUTH_REQ`.
- 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 when the blue FW-ING/SYS-IMG is updated and disableOtpRollbackProtect parameter is set to “NO” (refer to hseOtpRollbackProtectionPolicy_t attribute)
- During SD card booting, the first 36KB (`start_address = 0x34000000, length = 0x9000`) from SRAM are used. This memory region 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.

9 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_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)
	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_FIRMWARE_VERIFY	Verifies the blue or pink FW images (in SRAM or external flash)
	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/IEE) context.

Table 1. *...continued*

Service Class	HSE Service ID	Description/Notes
	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_CONFIG_COUNTER	Configures the monotonic counters
	HSE_SRV_ON_DEMAND_ANTI_RBC_UPDATE	Update on demand the anti-rollback counter(s) in fuses for SYS-IMG and/or FW-IMG
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

Table 1. *...continued*

Service Class	HSE Service ID	Description/Notes
		* 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_KEY_VERIFY	**Verifies a provided hash/MAC over a symmetric/asymmetric key inside HSE key store.**
	HSE_SRV_ID_EXTEND_KEY_CATALOG	**Update the NVM or RAM key catalogs by appending new key groups.**
	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.
	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 (without RSA)**
Crypto	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, AES-XCBC-MAC * HMAC_(SHA1, all SHA2)
	HSE_SRV_ID_FAST_CMAC	**Low latency, high-performance CMAC generate/verify the request**
	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**)

Table 1. *...continued*

Service Class	HSE Service ID	Description/Notes
		* AES-GCM-128/-192/-256 (one-pass and streaming)
	HSE_SRV_ID_XTS_AES_CIPHER	**XTS AES encryption/decryption**
	HSE_SRV_ID_SIGN	**Request a Digital Signature Generation/Verification (one-pass and streaming):** * RSASAA_PSS (from 1024 up to 2048 bits key) * RSASAA_PKCS1-v1_5 (from 1024 up to 2048 bits key) * ECDSA (all supported ECC curves) * EDDSA (for ED25519 curve)
	HSE_SRV_ID_RSA_CIPHER	**RSA encryption/decryption**: * RSAES-PKCS1-v1_5 (from 1024 up to 2048 bits key) * RSAES-OEAP (from 1024 up to 2048 bits key)
	HSE_SRV_ID_AUTHENC	**Combined Authenticated Encryption service:** *****AES_(ECB, CBC, CTR, CFB, OFB) -THEN- HMAC_ (SHA1, SHA2_224, SHA2_256, SHA2_384, SHA2_512) for “Encrypt-then-MAC” *NULL cipher with all MAC algorithms (CMAC, GMAC, XCBC_MAC, HMAC(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)
	HSE_SRV_ID_CMAC_WITH_COUNTER	Generates/verifies the CMAC of a given input message concatenated with a selected secure counter.
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**

Table 1. *...continued*

Service Class	HSE Service ID	Description/Notes
	HSE_SRV_ID_SMR_ENTRY_ERASE	**Erase an SMR entry**
	HSE_SRV_ID_CORE_RESET_ENTRY_ERASE	**Erase a CR entry**

Legal information

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.

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.

Terms and conditions of commercial sale — NXP Semiconductors products are sold subject to the general terms and conditions of commercial sale, as published at https://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.

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.

Suitability for use in non-automotive qualified products — Unless this document expressly states that this specific NXP Semiconductors product is automotive qualified, the product is not suitable for automotive use. It is neither qualified nor tested in accordance with automotive testing or application requirements. NXP Semiconductors accepts no liability for inclusion and/or use of non-automotive qualified products in automotive equipment or applications.

In the event that customer uses the product for design-in and use in automotive applications to automotive specifications and standards, customer (a) shall use the product without NXP Semiconductors' warranty of the product for such automotive applications, use and specifications, and (b) whenever customer uses the product for automotive applications beyond NXP Semiconductors' specifications such use shall be solely at customer's own risk, and (c) customer fully indemnifies NXP Semiconductors for any liability, damages or failed product claims resulting from customer design and use of the product for automotive applications beyond NXP Semiconductors' standard warranty and NXP Semiconductors' product specifications.

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.

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 S32G3 HSE Firmware 0.2.51.0

Contents

1 Getting Started 1
1.1 Package content 1
1.2 Installation 1
2 Release Details 2
2.1 Supported Derivatives 2
2.2 Device Bricking scenario for HSE Firmware 2
2.3 Security Aspects 2
3 Known issues 3
4 Change Logs in 0.2.51.0 4
5 Change Logs in 0.2.22.0 6
6 Change Logs in 2.16.1 7
7 Change Logs in 0.21.0 9
8 List of Limitations Existing in This Release 11
9 List of Services Available 12
Legal information 17

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

Date of release: 23 April 2024
Document identifier: HSE_FW_S32G3_0.2.51.0_ReleaseNotes