Release Notes

for S32G3 HSE Firmware 0.2.16.1

Rev. 1.0 — 7 October 2022 Release notes

COMPANY CONFIDENTIAL

1 Getting Started

IMPORTANT NOTES:

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

This release has **RTM** quality level in terms of features, documentation, and testing.

1.1 Package content

This package contains the NXP S32G3 HSE Firmware 0.2.16.1:

- HSE Firmware: encrypted binaries
  - Rev 1.0 for previous version of the SoC
  - Rev 1.1 for latest version of the SoC
- HSE Firmware interface files
- HSE Service API RM
- HSE Security Installation Guide
- `HSE_FW_S32G3_0.2.16.1_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.

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

- HSE Firmware Reference Manual – Rev 1.5, 10/22

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 0.2.16.1 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:
  - P32G399AACK0VUC (rev 1.0)
  - P32G399AACVUC (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

For the Premium Package variant, the customers would need to purchase "premium S32G3 security parts" (to run Premium Package variant in production).

Implemented Errata:

- ERR051257 (for rev 1.0) - 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:

- 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 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

4 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`

5 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.
- 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.

6 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_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.
	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

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_KEY_VERIFY	**Computes a hash/MAC over a symmetric 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.

Table 1. *...continued*

Service Class	HSE Service ID	Description/Notes
	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**) * 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))

Table 1. *...continued*

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

7 Legal information

7.1 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.

7.2 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.

7.3 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 S32G3 HSE Firmware 0.2.16.1

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: 7 October 2022
Document identifier: HSE_FW_S32G3_0.2.16.1_ReleaseNotes.pdf