NXP Semiconductors
Product Brief

Document Number: 1.3
Rev. 1.3, 01/2022

HSE Firmware Product Brief

Contents

1. Software Product Overview

The Hardware Security Engine (HSE) is a security subsystem, which aims at running relevant security functions for applications having stringent confidentiality and/or authenticity requirements, with the following foremost objectives:

- Isolating security-sensitive information (e.g., secret keys) from the application (the host);
- Offloading the application from processing cryptographic operations;
- Accelerating cryptographic operations with dedicated coprocessors;
- Enforcing security measures on the application, during run-time and system startup.

The HSE firmware is a software product specifically designed to run in the HSE subsystem. It essentially serves the host (application cores) with a set of native security services:

- **Administration services** are provided to install, configure and test the HSE firmware;

- **Key management services** are available for the application to manage different set of keys that are handled by the HSE firmware via e.g., the cryptographic services;
- **Cryptographic services** provide the application with cryptographic primitives that are used by high-level security stacks in the application;
- **Random number services** generate random streams that can be used in various security protocols;
- **Memory verification services** allow the application to verify different memory areas at start-up (after reset) and during run-time;
- **Monotonic counter services** provide the application with a set of monotonic counters that can be read and only incremented;
- **Secure time services** allow the configuration of a secure tick to be signaled to the application;
- **Network services** provide support for acceleration the network security protocols (IPsec, SSL/TLS).

An overview of NXP's native services supported by HSE firmware are highlighted in Figure1. It contains also services and interfaces for SHE+ specification emulation.

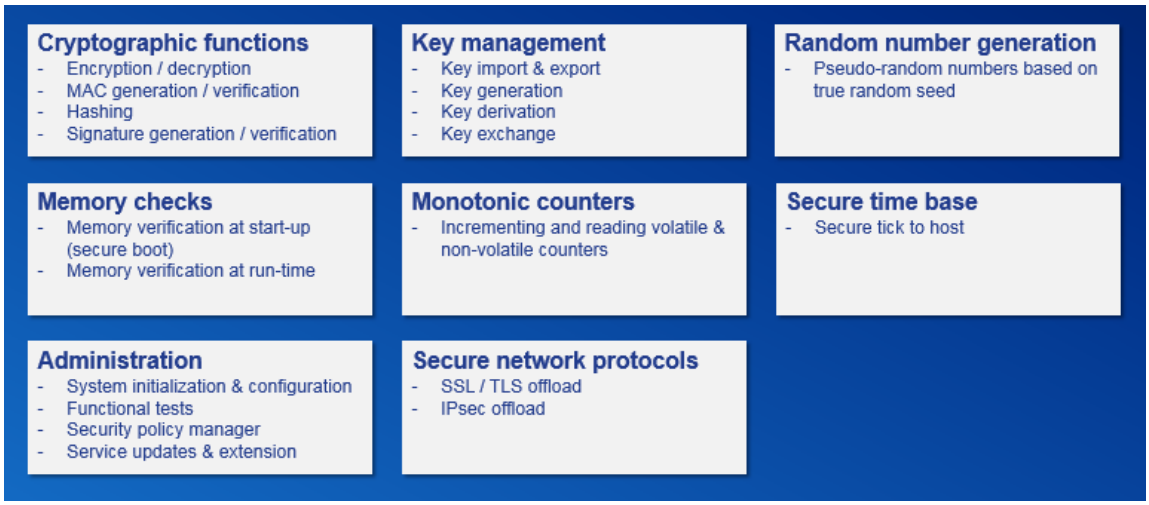

Figure 1**. NXP's Native Services**

Upgradable in the field, the HSE firmware comprises all the required security functions to fulfill a broad set of automotive security requirements and use cases (AUTOSAR® SecOC, SSL/TLS, IPsec, etc.). The services are accessed over a flexible and configurable communication interface which allows simultaneously asynchronous requests, ensuring at the same time Freedom from Interference between applications/cores.
The basic enablement (Common Security API) allows the customers integrating the HSE subsystem into different security stacks.

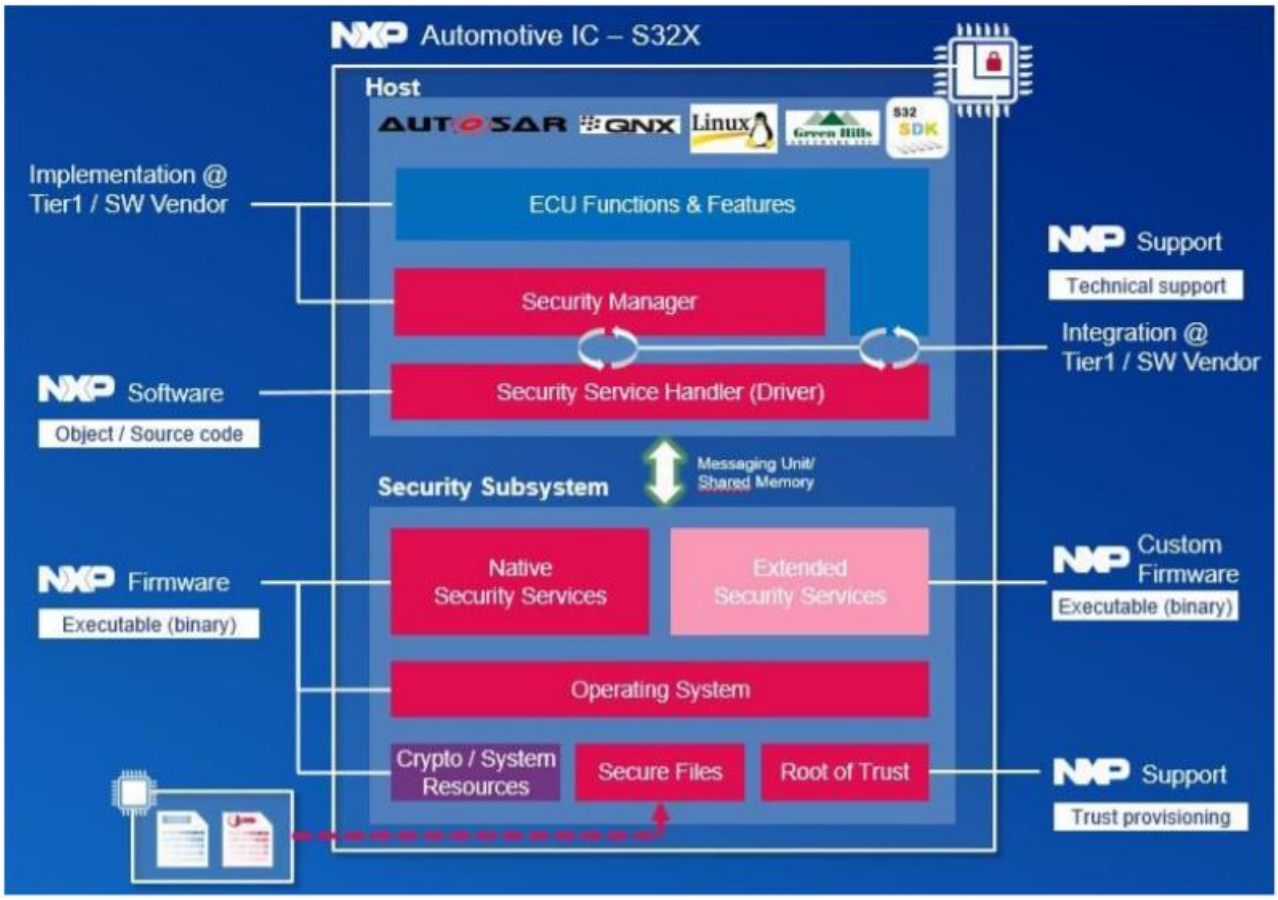

Figure 2**. NXP's Security Components in Play**

2. Software Content

The HSE Security Firmware is delivered in executable form, encrypted and signed by NXP.

The below table provides an overview of services/features supported by the HSE Firmware

Table 1**. HSE Firmware Services and Features**

Service	Category	Feature
Cryptography	Ciphers	AES: ECB, CBC, CFB, CTR, XTS 3DES: CBC, ECB, CFB, OFB RSAES: PKCS1-v1_5, OAEP
	Message Authentication Code (MAC)	AES: CMAC, GMAC, XCBC-MAC HMAC
	Hashing	SHA1 SHA224, SHA256, SHA384, SHA512 SHA3_224, SHA3_256, SHA3_384, SHA3_512 MD5 Miyaguchi-Preneel Compression
	Authenticated ciphers	AES: CCM, GCM
	Digital signature generation and verification	RSASSA_PSS RSASSA_PKCS1-v1_5 ECDSA – ECC over GF(p) with all prime standard curve supported EdDSA - Ed25519 pre-hashed curve
Key Management	Max key sizes	AES: 256 bits RSA: 4096 bits ECC: 521 bits
	Key generation	Permanent and ephemeral RSA and ECC key pair generation
	Key import	Plain or encrypted form, with optional authentication tag SHE key update protocol
	Key derivation	NIST 800-108, PBKDF2
	Key exchange	ECDH and Classic DH
	Certificate handling	Key Installation for x.509 and CVC certificates Certificate installation for Root of Trust establishment.
Boot and Memory Verification	Supported authentication	AES CMAC XCBC-MAC HMAC GMAC RSA & ECC signatures
	Verification flow	Before application startup (strict secure boot) In parallel of the application startup On demand by the application
	Sanctions	No startup (strict secure boot) Device reset Key usage restrictions
Monotonic Counter	Counter management	Incrementing & reading volatile & non-volatilel counters
Network Offloading Services	Dual purpose ciphers	Combined cipher and hash services for IPSec and TLS throughput enhancement
Random Number	Pseudo random generation	Based on a True Rdanom Number AIS31 Class P2 high and FIPS 140-2 compliant
Secure Time	Secure Tick	Application interrupts at configurable frequency
Administration Services	HSE administration	Firmware installation / update Subsystem configuration and testing

The HSE Firmware Reference Manual and HSE Firmware Service Description Reference Manual, available on NXP DocStore, provide more information about HSE Firmware. The HSE Firmware will be available in two variants: Standard package and Premium package.

HSE firmware variant	Standard	Premium
Key types (max key size)	AES (256 bits) RSA (2048 bits) ECC (256 bits) HMAC (512 bits) DH (2048 bits)	AES (256 bits) RSA (4096 bits) ECC (521 bits) HMAC (1152 bits) DH (4096 bits)
Number of keys	RAM keys: 20 NVM keys: 12(asym) + 40(sym)	RAM keys: user configurable NVM keys: user configurable
Key import	SHE key update protocol + Plain form or AES / RSA encrypted / CMAC authenticated or RSA / ECC signed	
Key export	RAM key export according to SHE protocol / AES / RSA encrypted + CMAC authenticated or RSA / ECC signed	
Key generation	RSA and ECC key pair generation	
Key derivation	Standard KDF and TLS PRF	
Key exchange	Classic DH and ECDH(E)	
Public key certificates	Extraction of key values & properties supported	
AES encryption & decryption	ECB CBC CTR OFB CFB XTS	
AES authenticated encryption & decryption	CCM GCM	
Hashing	SHA-1, SHA-2 (all digest sizes) Miyaguchi-Preneel	+ SHA-3[3] (all digest sizes)
MAC generation & verification	CMAC HMAC GMAC	+ XCBC-MAC
Signature generation & verification	RSA PKCS-1.5 and PSS, ECDSA[1], EdDSA[2]	
RSA encryption & decryption	PKCS-1.5 and OAEP	
ECC encryption & decryption	ECIES[4]	
Random number generation	AIS31 and FIPS 140-2 compliant	
Number of memory regions verified	4	Max. 32
Protocol Offloads		IPsec

[1] Standard and user configurable Weierstrass curves
[2] Curve Ed25519
[3] Not hardware accelerated
[4] Supported via combined services

Figure 3. **HSE Firmware Offering**

3. Supported Targets

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

- S32G2

4. Quality, Standards Compliance and Testing Approach

The HSE Firmware product is developed according to NXP Software Development Processes that is Automotive-SPICE, IATF16949 and ISO9001 compliant.

5. Document Information

Table 1. **Sample revision history**

Revision number	Date	Substantive changes
1	10/2021	Initial release

How to Reach Us:

Home Page:
nxp.com

Web Support:
nxp.com/support

Document Number: 1.3
Rev. 1.3
01/2022