硬件安全引擎（HSE）固件产品简介

目录

1. 软件产品概述

硬件安全引擎（HSE）是安全子系统，可为有严格保密和/或可靠性要求的应用程序运行相关的安全功能，其首要目标如下：

- 将安全敏感信息（例如密钥）与应用程序（主机）隔离；
- 从处理加密操作中分流应用程序；
- 使用专用协处理器加速加密操作；
- 在运行时和系统启动期间对应用程序加强安全措施。

HSE固件是专门设计在HSE子系统中运行的软件产品。它本质上为主机（应用程序核心）提供了一组本地安全服务：

- **管理服务**，安装、配置和测试HSE固件；

- **密钥管理服务**，可供应用程序管理由HSE固件（例如通过加密服务）处理的不同密钥集；
- **加密服务**，为应用程序提供加密原语，供应用程序中的高级安全栈使用；
- **随机数服务**，生成可用于各种安全协议的随机流；
- **内存验证服务**，允许应用程序在启动时（重启后）和运行时验证不同的内存区域；
- **单频计数器服务**，为应用程序提供一组可读且只能递增的单频计数器；
- **安全时间服务**，允许将安全嘀嗒（tick）的配置发信号给应用程序；
- **网络服务**，提供支持网络安全协议（IPsec、SSL/TLS）的加速。

图1重点介绍了HSE固件支持的恩智浦本地服务，也包含用于SHE+规范模拟的服务和接口。

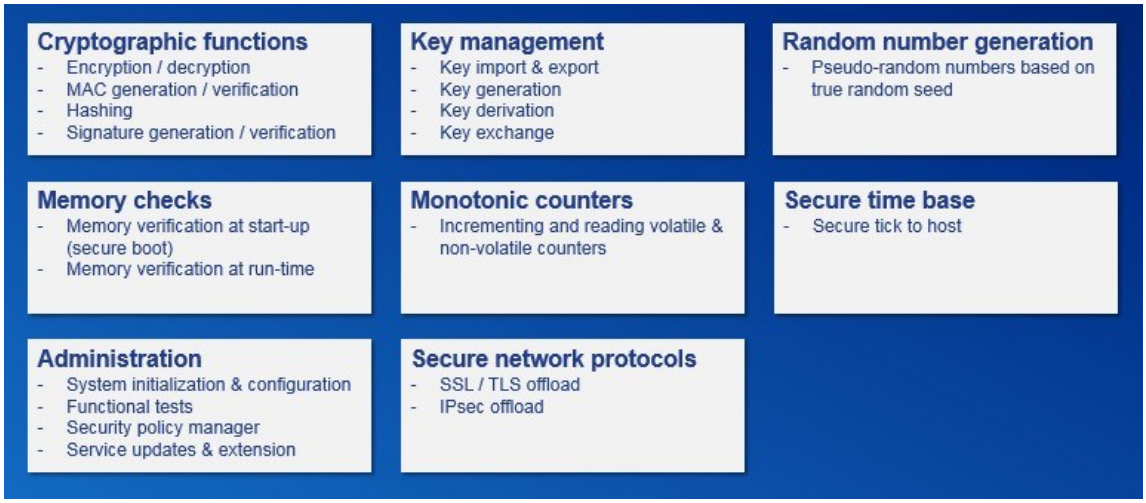

图1. 恩智浦本地服务

HSE固件可现场升级，它包括所有必需的安全功能，以满足广泛的汽车安全需求和用例（AUTOSAR® SecOC、SSL/TLS、IPsec等）。这些服务通过灵活且可配置的通信接口接入，该接口支持同时地异步请求，确保在同一时间应用程序/内核之间不受干扰。
基本功能（通用安全API）允许客户将HSE子系统集成到不同的安全栈中。

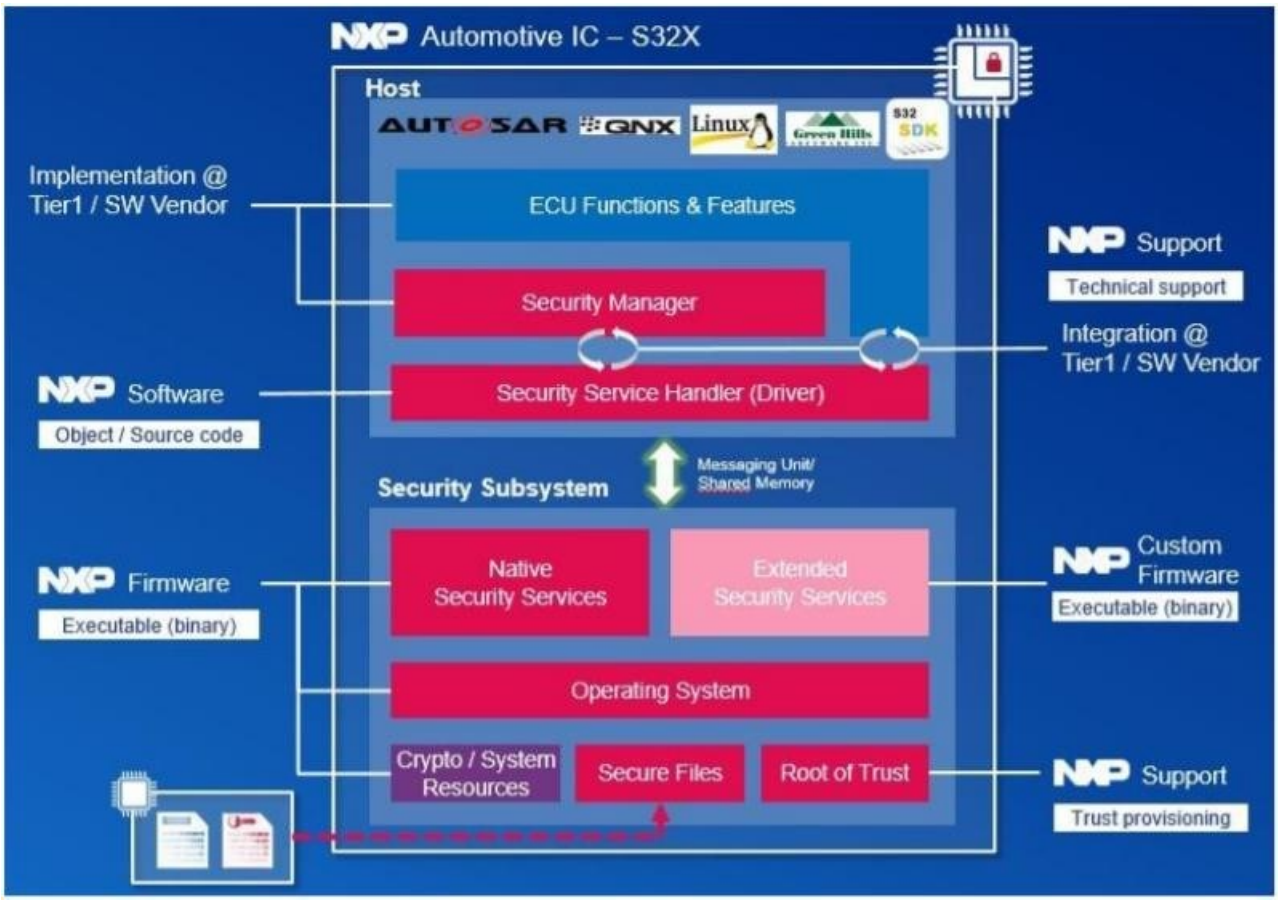

图2. 恩智浦使用中的安全组件

2. 软件内容

HSE安全固件以可执行的形式交付，由恩智浦加密并签署。

下表概述了HSE固件支持的服务/功能

表1. HSE固件服务和特性

服务	种类	特性
加密	密码	AES：ECB、CBC、CFB、CTR、XTS 3DES：CBC、ECB、CFB、OFB RSAES：PKCS1-v1_5、OAEP
	信息验证码（MAC）	AES：CMAC、GMAC、XCBC-MAC HMAC
	使用散列表	SHA1 SHA224、SHA256、SHA384、SHA512 SHA3_224、SHA3_256、SHA3_384、SHA3_512 MD5 Miyaguchi-Preneel压缩
	已验证的密码	AES：CCM、GCM
	数字签名生成与验证	RSASSA_PSS RSASSA_PKCS1-v1_5 ECDSA - ECC over GF(p)，支持所有prime标准曲线 EdDSA - Ed25519 pre-hashed曲线
密钥管理	最大密钥长度	AES：256位 RSA：4096位 ECC：521位
	密钥生成	永久和临时的RSA和ECC密钥对生成
	密钥导入	普通的或加密的表单，带有可选的验证标签 SHE密钥更新协议
	密钥衍生	NIST 800-108, PBKDF2
	密钥交换	ECDH和Classic DH
	证书处理	用于x.509和CVC证书的密钥安装 用于建立信任根的证书安装。
启动和内存验证	支持的认证	AES CMAC XCBC-MAC HMAC GMAC RSA和ECC签名
	验证流程	在应用程序启动之前（严格的安全启动） 在应用程序启动的同时 根据应用程序的需求
	处罚	不启动（严格的安全启动） 设备重启 密钥使用限制
单频计数器	计数器管理	增加和读取易失性和非易失性计数器
网络分流服务	两用密码	IPSec和TLS的组合密码和哈希服务 提高吞吐量
随机数	伪随机生成	基于真实的随机数 符合AIS31的P2高级标准和FIPS140-2标准
安全时间	安全嘀嗒	应用程序以可配置的频率中断
管理服务	HSE管理	固件安装/更新 子系统配置和测试

《HSE固件参考手册》和《HSE固件服务描述参考手册》提供了关于HSE固件的更多信息，可以从恩智浦文档商店（NXP DocStore）获取。HSE固件有两种版本：标准包和高级包。

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

图3. HSE固件产品

3. 支持的目标

本文档中描述的软件用于恩智浦半导体的下列器件：

- S32G2

4. 质量、符合的标准和测试方法

HSE固件产品是根据“恩智浦软件开发流程”开发的，符合Automotive-SPICE、IATF16949和ISO9001标准。

5. 文档信息

表1. 测试样本修订记录

版本号	日期	实质性变更
1	2021年10月	初版发布

How to Reach Us:

Home Page:
nxp.com

Web Support:
nxp.com/support

Document Number: 1.3
Rev. 1.3
01/2022