NXP S32K3xx之HSE使用方法（二）

原创 于 2025-12-04 10:07:14 发布 · 1.2k 阅读 · 16 · 21 · CC 4.0 BY-SA版权

文章标签： #网络安全

目录

声明：本文部分内容源自NXP官网的HSE使用手册，在原手册基础上，经过个人的翻译，理解和总结，如读者想了解更详细的内容，可自行至官网下<RM758226-RM00286 HSE-B Firmware Reference Manual - V2.6(2.6).pdf>

1. HSE Configuration and Attributes

1.1 HSE configuration

HSE配置包括以下内容：

- 影响设备启动行为的HSE系统属性
- 格式化 Application Key Catalog，即NVM & RAM Key Catalogs
- 初始NVM密钥的配置或请求密钥生成（如RSA/ECC密钥对）
- UTEST系统配置
- 主核Debug保护认证模式
- 安全启动的安全内存区域
- 设置monotonic计数器

以上配置必须在生命周期LC为**CUST_DEL或OEM_PROD配置完成。**配置完成后，LC必须演进至IN_FIELD状态。

1.2 HSE system attributes

HSE的系统属性类型定义了主机访问这些属性的权限，如下表所示：

属性	说明
RO-ATTR	Read-Only（只读）
OTP-ATTR	One Time Programmable 一次编程，只能在OTP区域写入一次，可读
OTP-ADVANCE-ATTR	One Time Programmable One Time Programmable attribute

NVM-RW-ATTR	System NVM attribute 系统NVM属性，可读可写
SET-ONCE	Once the attribute is set; it can only be changed after a reset 一旦该属性设置，只能在复位后修改，如在初始化时设置
RAM-RW	RAM attribute which can be set/reset as many times as possible RAM属性可以在设置/重置任意次数

以下是常用系统的配置ID及属性类型：

Attribute ID	Type
HSE_FW_VERSION_ATTR_ID	RO-ATTR
HSE_CAPABILITIES_ATTR_ID	RO-ATTR
HSE_SMR_CORE_BOOT_STATUS_ATTR_ID	RO-ATTR
HSE_DEBUG_AUTH_MODE_ATTR_ID	OTP-ATTR
HSE_APP_DEBUG_KEY_ATTR_ID	OTP-ATTR
HSE_SECURE_LIFE_CYCLE_ATTR_ID	OTP-ADVANCE-ATTR
HSE_ENABLE_BOOT_AUTH_ATTR_ID	OTP-ATTR
HSE_MU_CONFIG_ATTR_ID	NVM-RW-ATTR
HSE_EXTEND_CUST_SECURITY_POLICY_ATTR_ID	OTP-ATTR & NVM-RW-ATTR
HSE_EXTEND_OEM_SECURITY_POLICY_ATTR_ID	NVM-RW-ATTR
HSE_FAST_CAMC_MIN_TAG_BIT_LEN_ATTR_ID	NVM-RW-ATTR
HSE_SECURE_RECOVERY_CONFIG_ATTR_ID	OTP-ATTR
HSE_FIRC_DIVIDER_CONFIG_ATTR_ID	RAM-RW
HSE_CORE_RESET_RELEASE_ATTR_ID	NVM-RW-ATTR
HSE_PHYSICAL_TAMPER_ATTR_ID	SET-ONCE-ATTR
HSE_MEM_REGIONS_PROTECT_ATTR_ID	SET-ONCE-ATTR
HSE_RAM_PUB_KEY_IMPORT_POLICY_ATTR_ID	NVM-RW-ATTR
HSE_ENABLE_PUBLISH_KEY_STORE_RAM_TO_FLASH_ATTR_ID	RAM-RW

系统属性的设置和读取需要配置hse的服务结构体，定义读取的属性ID，HSE服务类型等内容，通过MU方式发送至Hse，查看hse的响应即可确认读取成功。

设置系统属性的示例代码如下所示：

objectivec AI写代码 复制

```objectivec
/* configure the HSE/host interface RAM */
hseSrvDescriptor_t* pHseSrvDesc;
hseSetAttrSrv_t* pSetSysAttr;
hseAttrMUConfig_t config;
hseSrvResponse_t srvResp;

/* allocate the memory for the service descriptor in HSE/host interface
RAM (not described here)*/
```

展开

1.3 HSE Secure NvM

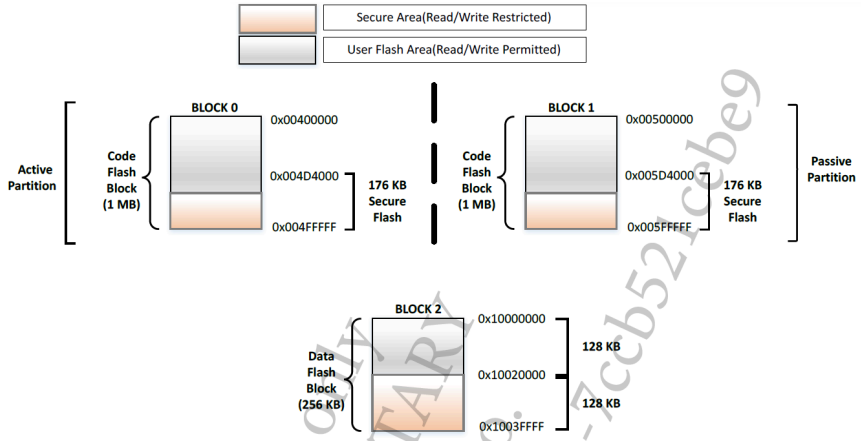
安全NVM是只能由HSE子系统访问的非易失性存储的内存区域，包括代码(Code Flash)，数据(Data Flash) 和配置(UTEST)，具体的内存地址示：

Table 134. Secure NVM mapping (AB_SWAP)

Device	Flash area	Start address	Size
Common	HSE data flash	0x10020000	128KB
	HSE configuration (UTEST)	0x1B000000	8KB
S32K311, S32K310,	HSE code flash (passive area)	0x004D4000	176KB
	HSE code flash (active area)	0x00454000	176KB
S32K312, S32K342, S32K322, S32K341	HSE code flash (passive area)	0x005D4000	176KB
	HSE code flash (active area)	0x004D4000	176KB

1. HSE Code Flash

存储HSE的固件，如果为AB SWAP类型，Active和Pa



2. HSE Data Flash

存储各种类型的密钥Key：密钥属性，密钥值和密钥大小等信息，具体请参考第2章节。

3. UTEST

具有OTP属性的HSE系统配置如下表所示：

参数	大小	说明
IVT_AUTH	8 bits	**选择IVT的认证模式:** 0（default）：无需认证 1：在运行HSE固件之前强制进行IVT认证
AUTH_MODE	8 bits	**选择打开Debug保护的方式:** 0（default）：静态认证方式，即密码 1：动态认证方式，即challenge/response
ADKP	128 bits	**打开Debug的密钥或者密码:** 如果AUTH_MODE为0，ADKP是密码 如果AUTH_MODE为0，ADKP是密钥
ADKP_MASTER	1 bit	**选择在安全NVM提供ADKP的方式:** 0（default）：输入值为ADKP，并在安全中原样写入安全NVM 1: 输入值被视为master debug key，且在写入安全NVM前，与设备的UID进行了多样化
LC	8 bits	**选择生命周期**：OEM_PROD or IN_FIELD

2. HSE Cryptographic Key

2.1 Key group and Key type

Key group是具有相同类型密钥的集合，需要定义每个key group组索引，按照在key catalog中的顺序，如第一个group的索引为0，第二个group

此类推。

支持的Key type如下表所示：

Key type	Description	Key catalog
HSE_KEY_TYPE_AES	AES key	NVM and RAM
HSE_KEY_TYPE_SHE	AES key used with SHE specific services	NVM and RAM
HSE_KEY_TYPE_HMAC	HMAC key	NVM and RAM
HSE_KEY_TYPE_RSA_PAIR	RSA key pair (public and private)	NVM only
HSE_KEY_TYPE_RSA_PUB	RSA public key	NVM and RAM
HSE_KEY_TYPE_RSA_PUB_EXT	RSA public key, stored in application NVM	NVM and RAM
HSE_KEY_TYPE_ECC_PAIR	ECC key pair (public and private)	NVM and RAM
HSE_KEY_TYPE_ECC_PUB	ECC public key	NVM and RAM
HSE_KEY_TYPE_ECC_PUB_EXT	ECC public key, stored in application NVM	NVM and RAM
HSE_KEY_TYPE_DH_PAIR	DH key pair (public & private)	NVM and RAM
HSE_KEY_TYPE_DH_PUB	DH public key	NVM and RAM
HSE_KEY_TYPE_SHARED_SECRET	Shared secret - can be used to derive a secret key	RAM only
HSE_KEY_TYPE_OSCCA_SM4		

2.2 Key slot

Key slot是存储一个key的内存，包括key的值和属性。每个slot也需定义索引，按照在key group中的顺序，如第一个slot的索引为0，第二个slot索此类推。

1. **Key values**: 由一个或若干字节的无符号整数组成，大小取决于key的类型

2. **Key attributes**：包含大小，访问方式和使用标志，以下介绍常用的几个属性：

- Bit size: key的大小，以bit计数
- Key access restriction flags：以下枚举可以通过or进行组合

枚举	说明
HSE_KF_ACCESS_WRITE_PROT	key被写保护
HSE_KF_ACCESS_DEBUG_PROT	如果LC为OEM_PROD或IN_FIELD，当debugger连接时，该key无法访问；如果LC为CUST_DEL，此标志无影响
HSE_KF_ACCESS_ EXPORTABLE	如果设置该标志位，该key可以导出 注：RSA/ECC的私钥不可以被导出

- Key usage flags：以下枚举可以通过or进行组合

枚举	说明
HSE_KF_USAGE_ENCRYPT	该key用于加密操作
HSE_KF_USAGE_DECRYPT	该key用于解密操作
HSE_KF_USAGE_SIGN	对于RSA/ECC keys: 用于签名生成（只适用于私钥） 对于AES/HMAC keys: 用于MAC生成
HSE_KF_USAGE_VERIFY	对于RSA/ECC keys: 用于签名验证（只适用于公钥） 对于AES/HMAC keys: 用于MAC验证
HSE_KF_USAGE_EXCHANGE	对于DH/ECC keys: 用于密钥协议（DH/ECDH）
HSE_KF_USAGE_DERIVE	该密钥可用于派生其他密钥（无法设置为RSA、ECC，或者DH key）
HSE_KF_USAGE_KEY_PROVISION	当设置该标志位时，只有key import/export操作，即该key只能用于解密在import时被加密的key，或者加密需要export的key值
HSE_KF_USAGE_AUTHORIZATION	当设置该标志时，该密钥可用于验证主核请求超级用户权限(SU)，该标志位只能与HSE_KF_USAGE_VERIFY一起设置(HSE_KF_USAGE_SIGN不能被设置)
HSE_KF_USAGE_SMR_DECRYPT	当设置该标志时，该密钥可用于SMR解密

例如，一个AES key可以用于CMAC验证和key的派生，则可以设置usage flags为：HSE_KF_USAGE_VERIFY | HSE_KF_USAGE_DERIVE

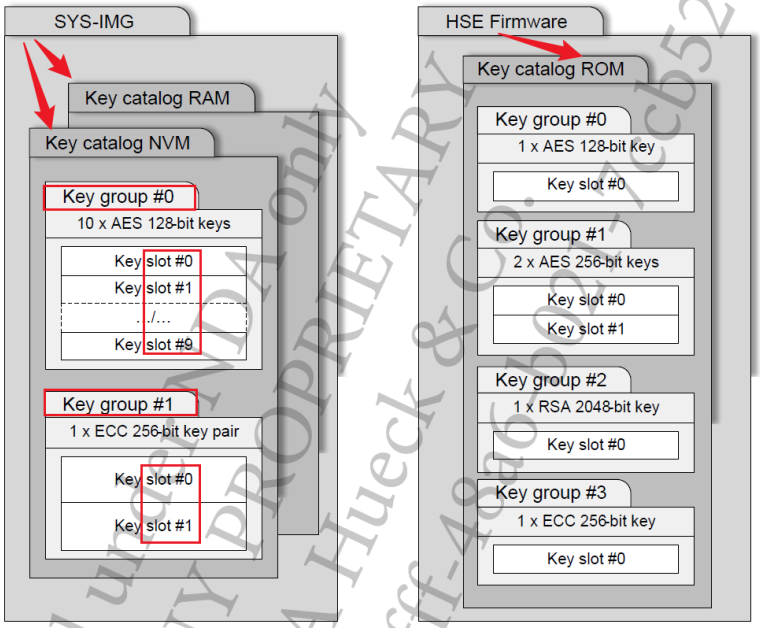
- SMR verification map：定义在使用该key之前，必须验证的secure memory regions（SMR）

枚举	说明
HSE_KF_SMR_0	只有secure memory region #0成功验证后，该key才可以使用
HSE_KF_SMR_1	只有secure memory region #1成功验证后，该key才可以使用
. . .	. . .
HSE_KF_SMR_7	只有secure memory region #7成功验证后，该key才可以使用

例如，一个key只有secure memory region #2和#5验证成功后才可以使用，则可以设置为：HSE_KF_SMR_2 | HSE_KF_SMR_5

2.3 Key Catalog

Keys被3种key catalogs进行管理，分别为key catalog NVM和key catalog RAM ，存放在SYS-IMG，key catalog ROM存放在HSE的固件，如



2.3.1 Key catalog ID

每个key catalog具有标识符，如下表所示：

Key catalog ID	值	配置	说明
HSE_KEY_CATALOG_ID_ROM	0	否	ROM key catalog，存储在安全的NVM中，由NXP配置
HSE_KEY_CATALOG_ID_NVM	1	是	NVM key catalog，key的值可以存储在SYS-IMG或者应用的NVM中（对于RSA和ECC的公钥） key的属性存储在SYS-IMG
HSE_KEY_CATALOG_ID_RAM	2	是	RAM key catalog，key的属性和值存储在安全RAM中

2.3.2 ROM key catalog

ROM key catalog包括以下4种key的类型可供使用：

key group index	key slot index	key type	usage restrictions	Key size
0	0	HSE_KEY_TYPE_AES	HSE_KF_USAGE_ENCRYPT | HSE_KF_USAGE_DECRYPT	256bit
	1	HSE_KEY_TYPE_AES	HSE_KF_USAGE_DERIVE | HSE_KF_USAGE_VERIFY | HSE_KF_USAGE_ENCRYPT | HSE_KF_USAGE_DECRYPT | HSE_KF_USAGE_KEY_PROVISION	256bit (owned by NXP)
1	0	HSE_KEY_TYPE_RSA_PUB	HSE_KF_USAGE_ENCRYPT | HSE_KF_USAGE_VERIFY | HSE_KF_USAGE_KEY_PROVISION	3072bit (owned by NXP)
2	0	HSE_KEY_TYPE_ECC_PUB	HSE_KF_USAGE_VERIFY | HSE_KF_USAGE_KEY_PROVISION	256bit (owned by NXP)

以上的ROM key可以通过任意的MU进行访问。

ROM key设置了以下的访问权限：**HSE_KF_ACCESS**

2.3.3 NVM and RAM key catalog

NVM和RAM key catalog由用户通过配置表进行配置，其中每个key group定义了以下5个属性：

- **MU instance map**：即可以访问key group的MU instance

Table 41. MU instance map for key usage

Enumerate	Influence on the key when set
HSE_MU0_MASK	The key group can be used through services triggered via the MU instance 0
HSE_MU1_MASK	The key group can be used through services triggered via the MU instance 1

- **key group owner:** 根据以下表格进行配置

Table 42. Key group owners

Key group owner	Applies to	Description
HSE_KEY_OWNER_CUST	NVM key catalog	Keys can be managed without restrictions if the host is granted with Super User (SU) rights and if the HID is CUST (system integrator). With User rights, the host can provision keys only based on the knowledge of a key owned by CUST (system integrator).
HSE_KEY_OWNER_OEM	NVM key catalog	Keys can be managed without restrictions if the host is granted with Super User (SU) rights and if the HID is OEM. With User rights, the host can provision keys only based on the knowledge of a key owned by the OEM.
HSE_KEY_OWNER_ANY	NVM[1] and RAM key catalog	Keys can be managed without restrictions if the host is granted with Super User (SU) rights. With User rights, restrictions apply on the key management services.

- **key type**: key的类型，参考2.1节
- **Number of keys**: key slots的数量
- **Maximum key size in bits**: key的最大长度，以下表格为常用的key类型及最大长度:

Key type	Maximum key sizes allowed
HSE_KEY_TYPE_AES	128, 192 or 256
HSE_KEY_TYPE_SHE	128
HSE_KEY_TYPE_HMAC	大于128 且小于 1152
HSE_KEY_TYPE_ECC_PUB	大于192 且小于 640
HSE_KEY_TYPE_RSA_PUB	大于1024 且小于 4096

2.3.4 Key catalog formatting

NVM和RAM key catalogs的key在使用之前，必须进行key catalog格式化。通过key catalog formatting的服务进行，且该服务只能在**LC 为CUST**时可用，所以必须在HSE的第一阶段完成配置。

完成NVM and RAM key catalog formatting之后，在这些catalogs中声明的key为**empty key**, empty key是无法使用的。

2.4 Key Handle

Key handle是一个32位整数，具有唯一的索引值来引用key catalog中的密钥。当hse服务中使用密钥时，都会通过Key handle来引用。其格式如

Bit number	31 ~ 24	23 ~ 16	15 ~ 8	7 ~ 0
Description	0	Key catalog ID	Key group index	Key slot index

举例，以下为NVM cata log配置为例：

objectivec AI写代码 复制

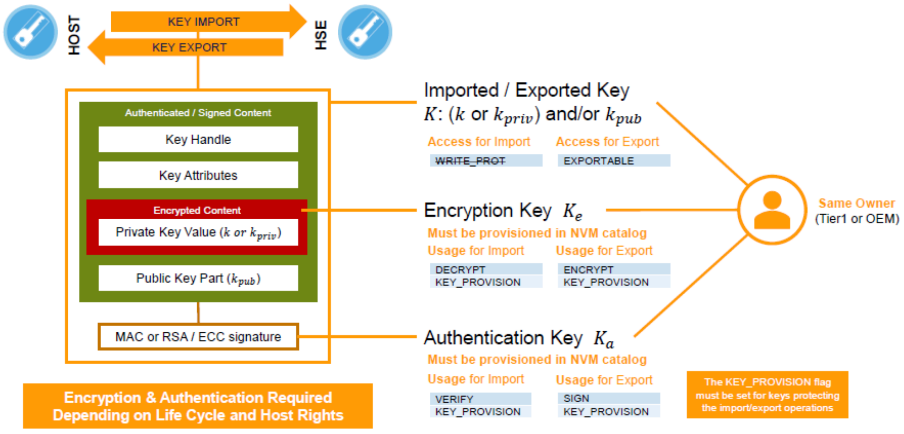
```
hseKeyGroupCfgEntry_t my_NVM_key_catalog[] = {
/* AES keys */
    {HSE_MU0_MASK, HSE_KEY_OWNER_CUST, HSE_KEY_TYPE_AES, 10, 128},
    {HSE_MU0_MASK, HSE_KEY_OWNER_CUST, HSE_KEY_TYPE_AES, 10, 256},
/* ECC keys */
    {HSE_MU0_MASK, HSE_KEY_OWNER_CUST, HSE_KEY_TYPE_ECC_PAIR, 2, 256},
    {HSE_MU0_MASK, HSE_KEY_OWNER_CUST, HSE_KEY_TYPE_ECC_PUB, 5, 256},
/* RSA keys */
```

key handle value的使用如下表所示：

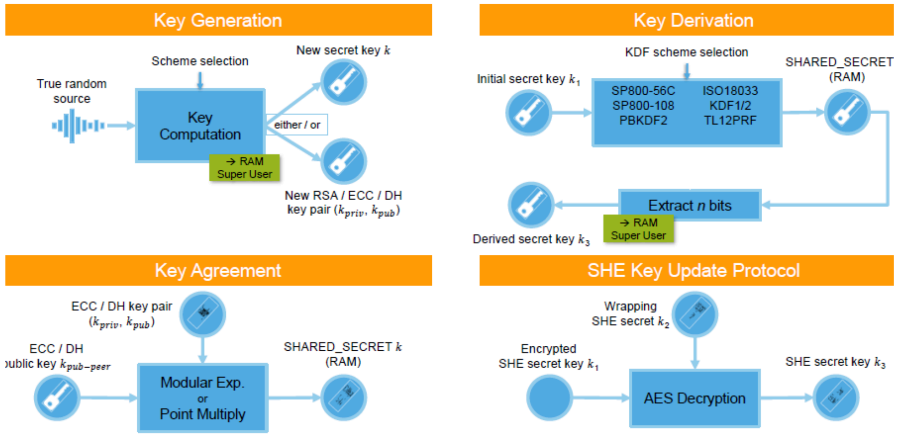
Key handle 值	说明
0x00010000	在NVM key catalog的第1个group的第1个key为128-bit AES key
0x0001000**A**	该handle是**无效**的，因为128-bit AES keys数量只有10个 (index从0 to 9)，index为10(即A)无效
0x00010101	在NVM key catalog的第2个group的第2个key为256-bit AES key
0x00010300	在NVM key catalog的第3个group的第1个key为256-bit ECC public key
0x000103**06**	该handle是**无效，因为第4个group只支持5个**256-bit ECC public keys (index从0 to 4)，index为6无效
0x00010509	在NVM key catalog的第6个group，最后一个为4096-bit RSA public key（index为9）
0x0001**06**00	该handle是**无效**，读者可自行分析

2.5 Key Services

Key Import/Export: Key的导入/导出。在进行key catalog formatting之后，其中的key为empty key，并不能直接使用，需要通过key import将真正到HSE中，用于之后的加密/解密等操作。不同类型key在导入/导出的说明如下图所示：



另外还有其他的key操作服务，如下图所示：



以上关于key相关服务的使用方法，其更详细的描述请参考RM758226-RM00286 HSE-B Firmware Reference Manual - V2.6(2.6)手册。

3. Super User Rights

主核可以获取两种类型的权限，即：

- 用户权限(User rights)：某些服务不可使用
- 超级用户权限(Super User rights)：所有的操作和配置可使用(取决于属性和设备的生命周期)

以下为用户权限和超级用户权限可以使用的服务列表：

Service	SU Rights	User Rights
Import a new NVM key (i.e., in an empty key slot)	Optional encryption and optional authentication	Mandatory encryption and mandatory authentication
NVM key generation (i.e., in an empty key slot)	Possible	Not possible
NVM key deletion	Possible	Not possible
Copy part of a RAM key to an NVM key slot	Possible	Not Possible
Load a uer defined ECC curve	Possible	Not Possible

Service	SU Rights	Us
Set HSE system attributes	Possible	No (e SE ATT
Authenticate the host system images (IVT, CFG)	Possible	No
Complete SMR entry update (including key handle)	Possible	No
Update a Core Reset Entry	Possible	No
Monotonic counter configuration	Possible	No

3.1 Execution rights after reset

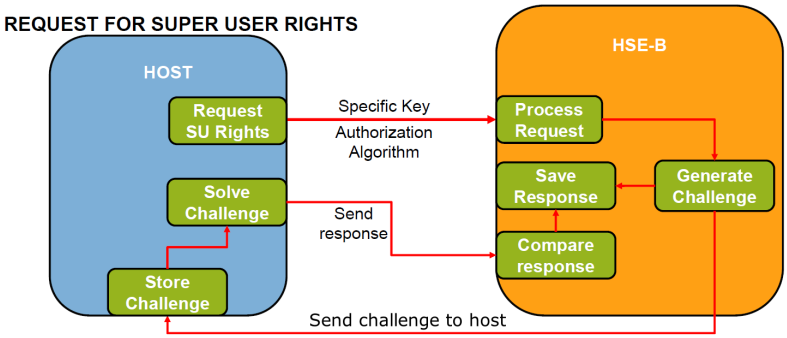
在LC为CUST_DEL和OEM_PROD时，复位后主核获取超级用户权限(SU)，拥有较高的执行权限和服务请求，在其他的LC状态，在复位之后主核用户权限，部分执行权限和服务被限制。

如果在LC为CUST_DEL和OEM_PROD时，需要在复位后强制设定为普通用户权限，则可以通过系统属性hseAttrExtendedCustSecurityPolicy_t hseAttrExtendedOemSecurityPolicy_t 配置 “Start As User”。不同LC和系统属性下的复位后执行权限如下表所示：

LC state	HSE system attribute	Host rights after reset	Host identity (HID)
CUST_DEL	CUST_START_AS_USER = 0	Super User (SU)	System integrator (CUST)
CUST_DEL	CUST_START_AS_USER = 1	User	System integrator (CUST)
OEM_PROD	OEM_START_AS_USER = 0	Super User (SU)	OEM
OEM_PROD	OEM_START_AS_USER = 1	User	OEM
IN_FIELD	N/A	User	Not identified (ANY)

3.2 Request Super User Rights

主核可以通过请求HSE服务来短暂的获取超级用户权限。请求权限时的认证过程如下图所示：



超级用户权限获取后，直至下一次复位或者主核请求获取普通用户权限后失效。

1. 认证算法选择

- 16-bytes CMAC TAG
- RSA Signature
- ECC Signature

2. Key选择

- **MASTER_ECU_KEY**：只有声明在**SHE的key group #0 slot#0的key**可以使用，其他声明为HSE_KEY_TYPE_SHE的SHE key无法用于认证
- **NVM Key**：该key的usage flags需要设置为 **HSE_KF_USAGE_VERIFY | HSE_KF_USAGE_AUTHORIZATION**

3. Challenge格式

- **request with MASTER_ECU_KEY**

Table 102. Challenge format when requesting SU rights with MASTER_ECU_KEY

Bytes 30~15	Bytes 14~7	Bytes 7~0	
16-byte random	7-bytes to 0	8-bytes UID	**31 bytes** in total

- **request with NVM Key**

Table 103. Challenge format when requesting SU rights with a key different from MASTER_ECU_KEY

Bytes 31~8		Bytes 7~0	
24-byte random	8-byte UID		**32 bytes** in total

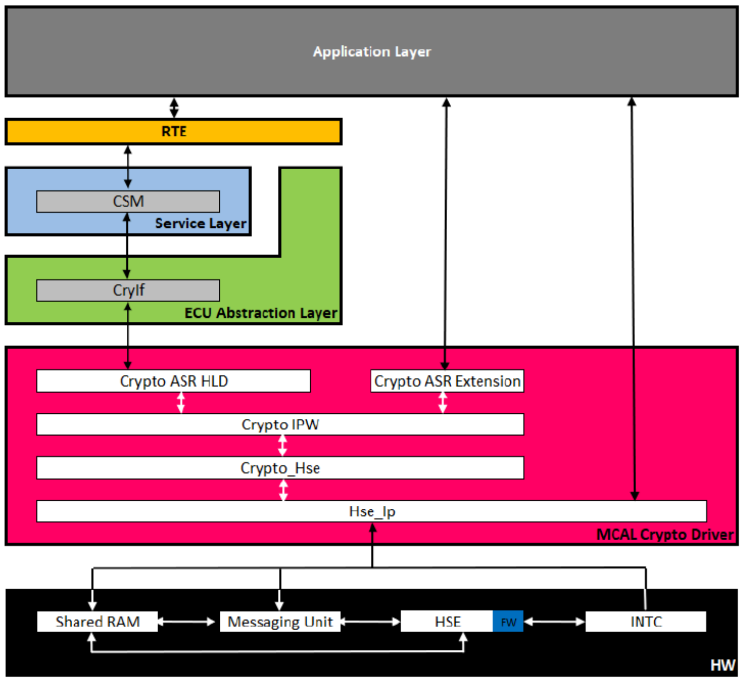
4. 示例代码

```objectivec
void RequestSURights(void)
{
    hseSrvDescriptor_t* pHseSrvDesc;
    hseSysAuthorizationReqSrv_t* pInitiateSysAuth;
    hseSysAuthorizationRespSrv_t* pFinalizeSysAuth;
    uint8_t challenge[32];
    uint8_t response[256];
    // initialize the service descriptor to initiate a request for SU rights
```

展开

4. AUTOSAR Crypto Stack

按照AUTOSAR架构，MCAL提供加密的底层驱动模块，用于向上层提供加密服务，同时通过MU的方式调用hse实现加密功能。在NXP的MCAL **Crypto ASR HLD, Crypto IPW，Crypto_Hse和Hse_Ip**等模块，如下图所示：



使用MCAL工具对Crypto Driver进行配置，主要包括如下内容：

1. Crypto Driver Object

表示一种独立的加密算法实例，支持2种Crypto Driver Objects，一个是Symmetric对称操作，另一个为Asymmetric非对称操作。

2. Job

配置的一种工作对象，引用相关的key和primitive的配置内容。

3. Primitive

需要在Crypto Driver Object上实现的一个加密算法实例。

4. Key

配置需要使用的key的相关属性。

详细的配置及内容此处不再展开介绍。

参考文档及Demo

REF01: <TP-TD-NANJING-HARDWARE-ZERO-HERO.pd

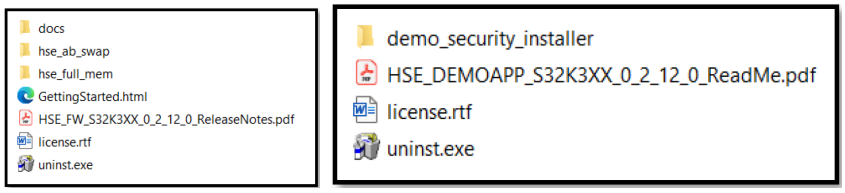
REF02: <RM758226-RM00286 HSE-B Firmware Referenc

REF03: NXP standard HSE FW package:

- Pink file and interface (.h文件)
- HSE Service API RM

REF04: HSE FW Demo App package

- 样例工程(脚本, readme)
- HSE FW FAQ
- HSE Demo App



系统启动流程及安全boot等内容在NXP S32K3xx之HSE使用方法（三）进行介绍~