S32K3XX SECURITY OVERVIEW AND BRING UP

Automotive Systems & Applications Engineering Team
GPIS-BL, Automotive Processing

SECURE CONNECTIONS
FOR A SMARTER WORLD

PUBLIC

AGENDA

1. S32K3 HSE (Hardware Security Engine) Overview
2. HSE Installation and Bring up
3. Software Enablement

S32K3 HSE Overview

SECURE CONNECTIONS
FOR A SMARTER WORLD

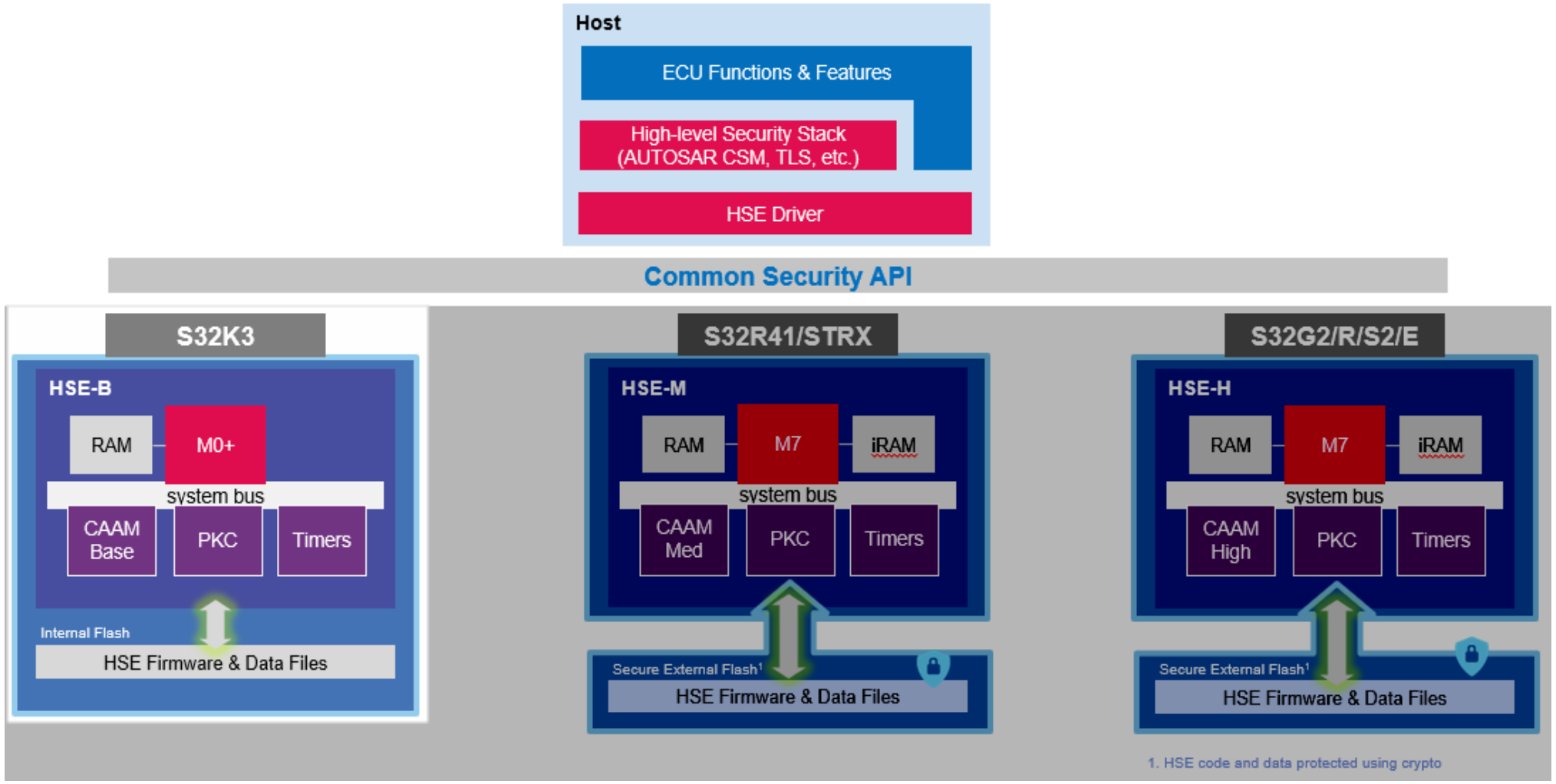
PUBLIC

ABOUT HARDWARE SECURITY ENGINE (HSE)

In a nutshell….

- HSE = **H**ardware **S**ecurity **E**ngine
- High-performance Security sub system with dedicated core, firmware, memory.
- Advanced Security HW accelerators: AES 256, RSA 4096, ECC 521, SHA-2 256…
- Firmware upgradable
- Exceed leading OEM security requirements in S32K3 target applications.

S32X HSE PORTFOLIO:
THREE VARIANTS, OPTIMIZED FOR DIFFERENT APPLICATIONS



S32K1 CSEC VS S32K3 HSE

		S32K1	S32K3
Security System		**CSEc**	**HSE-B**
Location in SoC architecture		Embedded within Flash Controller module	Independent Subsystem
Firmware Upgradable		no	yes
Firmware installed from factory		yes	no
Security Ciphers	**Symmetric**	AES-128 (20 keys max)	AES-128 / 192 / 256 (100+ keys, configurable)
	Cipher modes	ECB (CBC, CMAC)	ECB, CBC, CMAC, CTR, OFB, CCM, GCM
	Asymmetric	no	RSA (up to 4096b) & ECC (up to 521b)
	Hash	Miyaguchi-Preneel	Miyaguchi-Preneel SHA-2/SHA3 (up to 512b)
Secure Boot		As specified by SHE. Single memory área for verification using AES CMAC	Up to 32 flexible memory regions. Authentication tag can be AES CMAC/GMAC or RSA/ECC signature
Random Number Generator		TRNG & PRNG	TRNG & PRNG (AIS & NIST compliant)
Attack Resistance		-	Side Channel Resistance / Environment Monitoring

S32 SECURITY SUBSYSTEM: NATIVE SECURITY SERVICES

Cryptographic functions
- Encryption / decryption
- MAC generation / verification
- Hashing
- Signature generation / verification

Key management
- Key import & export
- Key generation
- Key derivation
- Key exchange

Random number generation
- Pseudo-random numbers based on true random seed

Memory checks
- Memory verification at start-up (secure boot)
- Memory verification at run-time

Monotonic counters
- Incrementing and reading volatile & non-volatile counters

Secure time base
- Secure tick to host

Administration
- System initialization & configuration
- Functional tests
- Security policy manager
- Service updates & extension

S32K3 – KEY MANAGEMENT

HSE firmware variant	HSE-B
Key types (max key size)	AES (256 bits) RSA (4096 bits) ECC (521 bits) HMAC (1152 bits with SHA-2 256/224) GMAC DH (4096 bits)
Number of keys	ROM keys: 1 device dependent Key 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 per 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

S32K3 – CRYPTOGRAPHIC FUNCTIONS

HSE firmware variant	HSE-B
AES encryption & decryption	ECB CBC CTR OFB CFB
AES authenticated encryption & decryption	CCM / GCM
Hashing	Miyaguchi-Preneel SHA-1 SHA-2 (all digest sizes) SHA-3 (all digest sizes)
MAC generation & verification	CMAC / HMAC / GMAC
HSE Firmware update	Supported
Customer code update	Supported
Signature generation & verification	RSASSA-PSS (PKCS#1 v2.2) ECDSA EdDSA
RSA encryption & decryption	PKCS-1.5 and OAEP
ECC encryption & decryption	ECIES
Random number generation	AIS31 and FIPS 140-2 compliant

S32K3 – TRUSTED EXECUTION

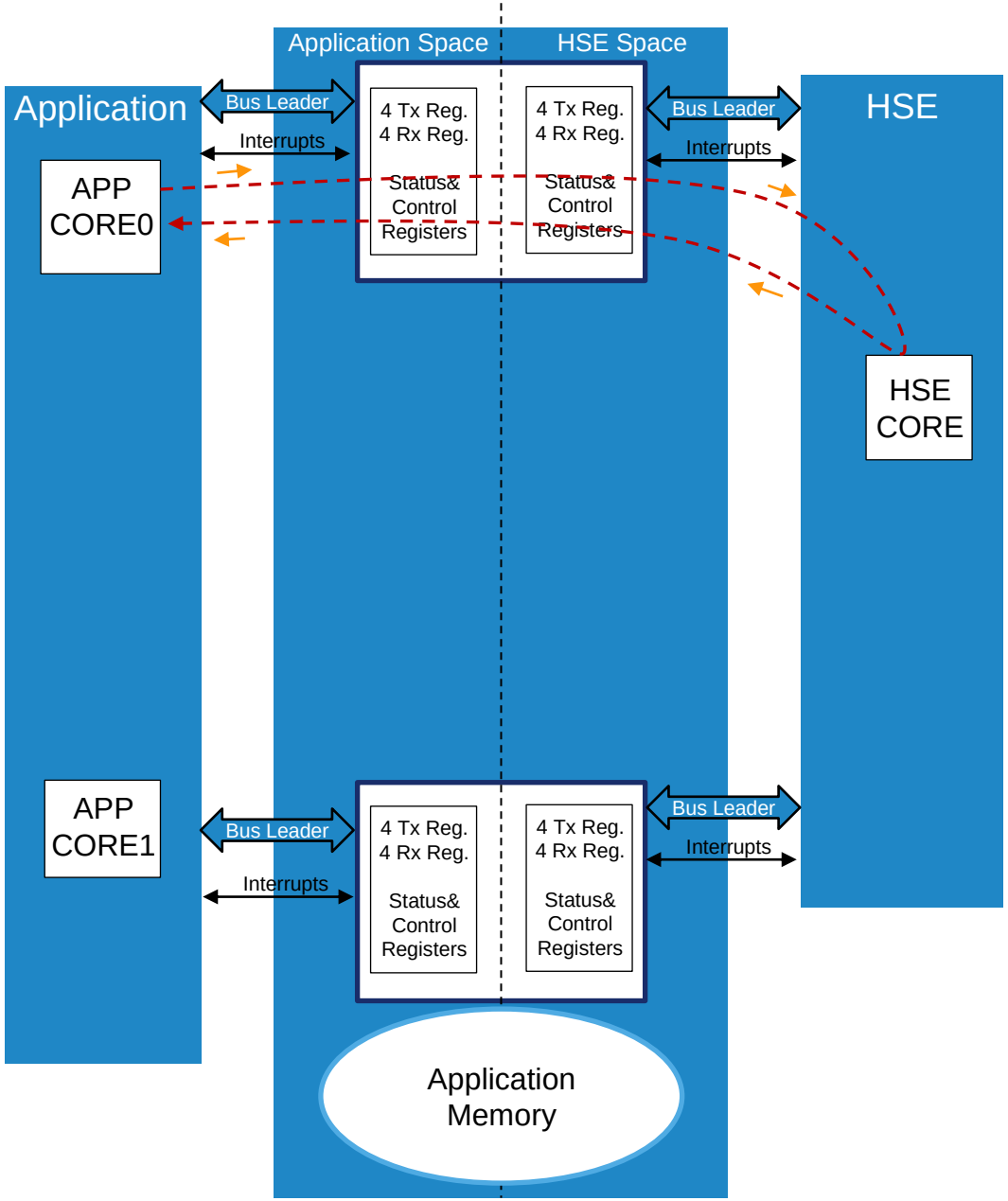
HSE firmware variant	HSE-B
Number of memory regions verified	Max. 32
Size of the memory region(s) verified	Flexible
Authentication methods supported	CMAC / HMAC / GMAC RSA signature ECDSA signature
Image authentication on-demand	Supported
Image authentication before application startup	Supported (strict secure boot)
Image authentication after application startup	Supported (parallel secure boot)
Image authentication at regular interval of times	Supported
Sanctions on failed verification (configurable)	Key usage System reset System stop (strict secure boot) All keys disabled
Application core release upon successful verification (before application startup)	Selectable among the available cores

HSE INTERFACE

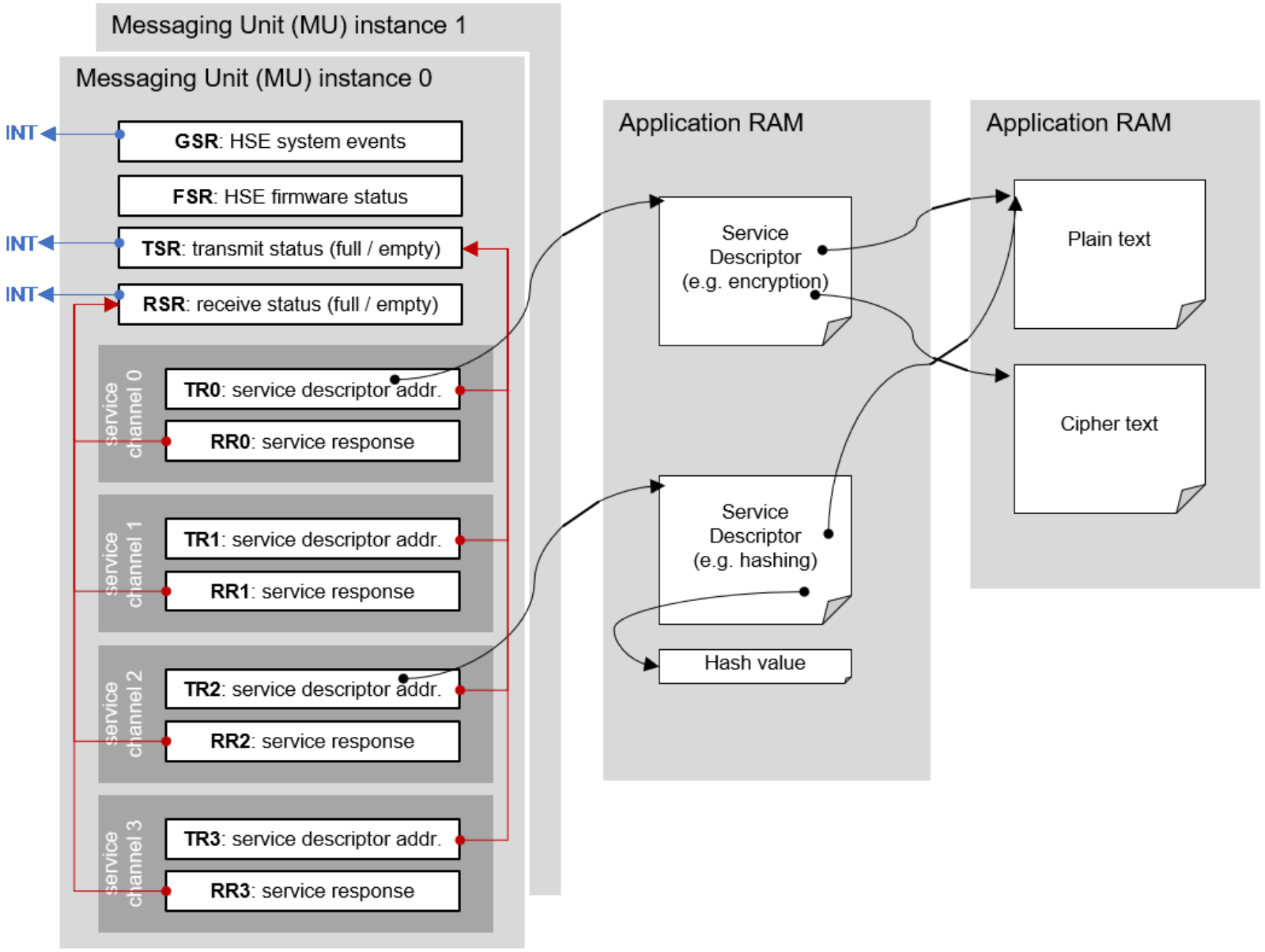
– **Messaging Unit (MU):** communication interface between the host and the HSE subsystem

- It is used by the host to trigger service requests and receive service responses
- It is used by the HSE firmware to receive service requests, return service responses and provide several HSE firmware status information relevant to the host.

MU instances	Tx / Rx registers per MU instance	Total Tx / Rx registers
2	4	8



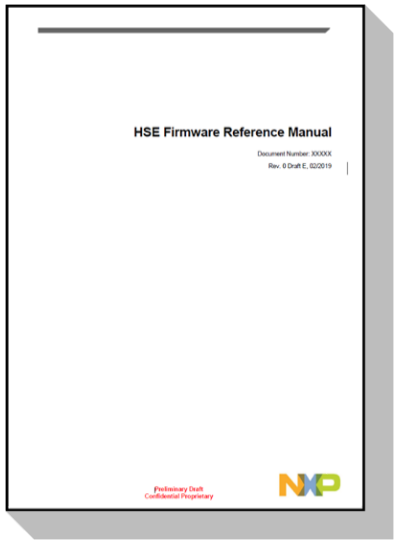
MESSAGING UNIT EXAMPLE – ILLUSTRATIONS



HSE FIRMWARE – DELIVERABLES

DocStore repository
www.docstore.nxp.com

HSE FW Reference Manual (detailing the HSE configuration & usage)



NXP online tool: Flexera

NXP HSE FW package:
- Binary and interface (.h files)
- HSE Service API RM

- docs
  - S32K3XX_HSE_Service_API_Reference_Manual.pdf
- hse_ab_swap
  - hse
    - bin
  - interface
- hse_full_mem
  - hse
    - bin
  - interface
- GettingStarted.htm
- HSE_FW_S32K3XX_EAR_0_0_8_3_ReleaseNotes.pdf

NXP online tool: Flexera

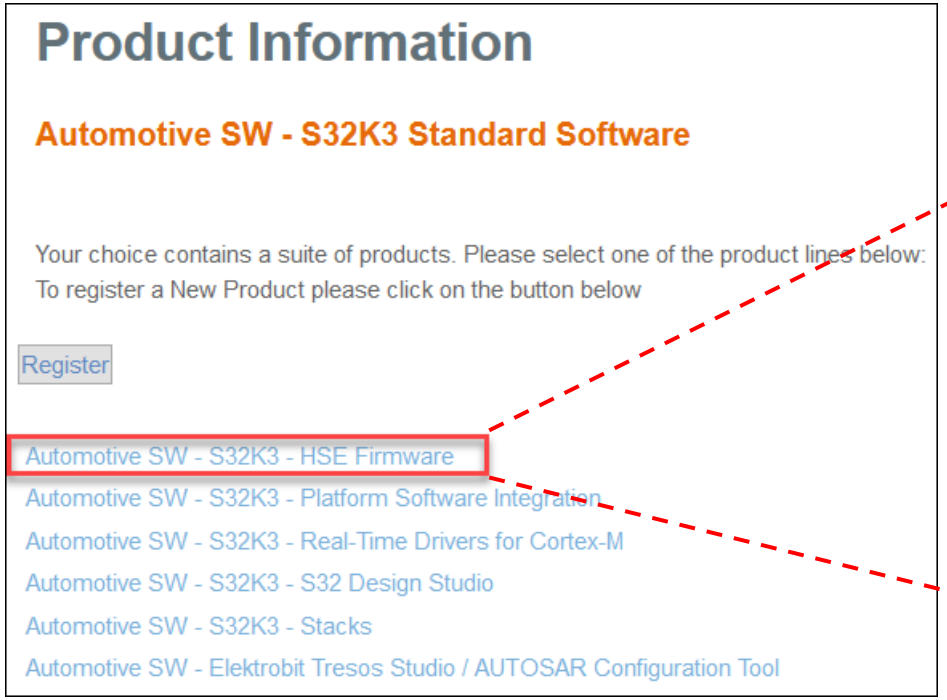
HSE FW Demo App package:
- Sample code (scripts, readme):
  S32DS IDE demo project
  GHS MULTI IDE demo project
- HSE FW FAQ,
- HSE Demo App installer.

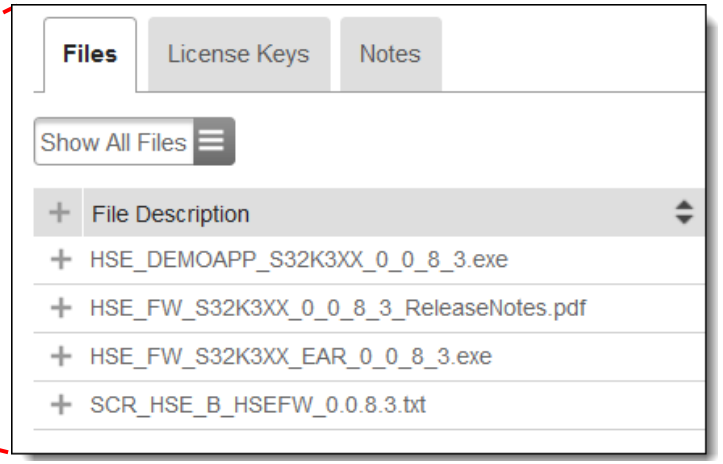
- doc
  - NXP HSE BASIC FW FAQ.pdf
  - NXP_HSE_FW_Key_Storage_Calculator.xlsx
- images
- scripts
- src
- HSE_DEMOAPP_S32K3XX_0_0_8_3_ReadMe.pdf

ACCESSING NXP HSE FIRMWARE STANDARD PACKAGE AND DEMO APP PACKAGE

- The standard HSE FW and Demo App packages can be downloaded from the S32K3 Standard Software collection in Flexera:

  https://nxp.flexnetoperations.com/control/frse/product?plneID=830607





*SW License Agreement must be accepted

ACCESSING S32K3 SECURITY DOCUMENTATION

Create docstore account

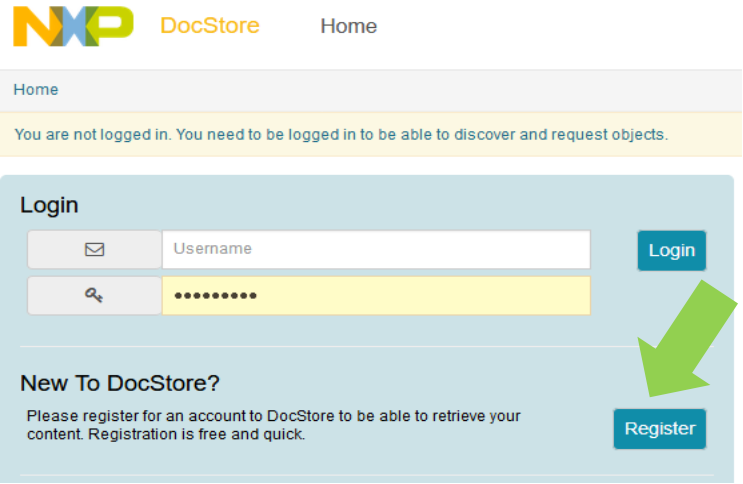
- www.docstore.nxp.com

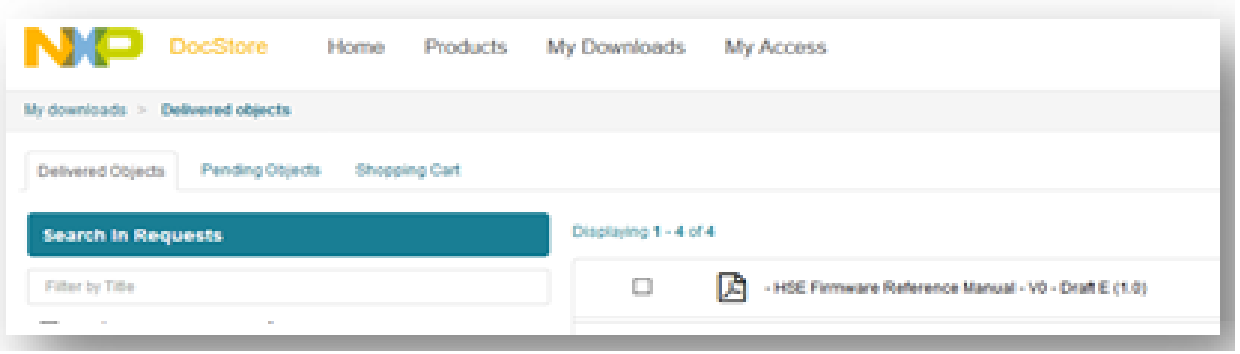
Request documents to be pushed to account (email)

- Internal (Sales/FAE) → Applications / Product management
- Customers → Sales/FAE → Applications / Product management

Documents will be pushed to requestors

- Security certificate needs to be received and installed (if not done already).
- Document needs to be downloaded from docstore.





HSE
Installation and Bring up

SECURE CONNECTIONS
FOR A SMARTER WORLD

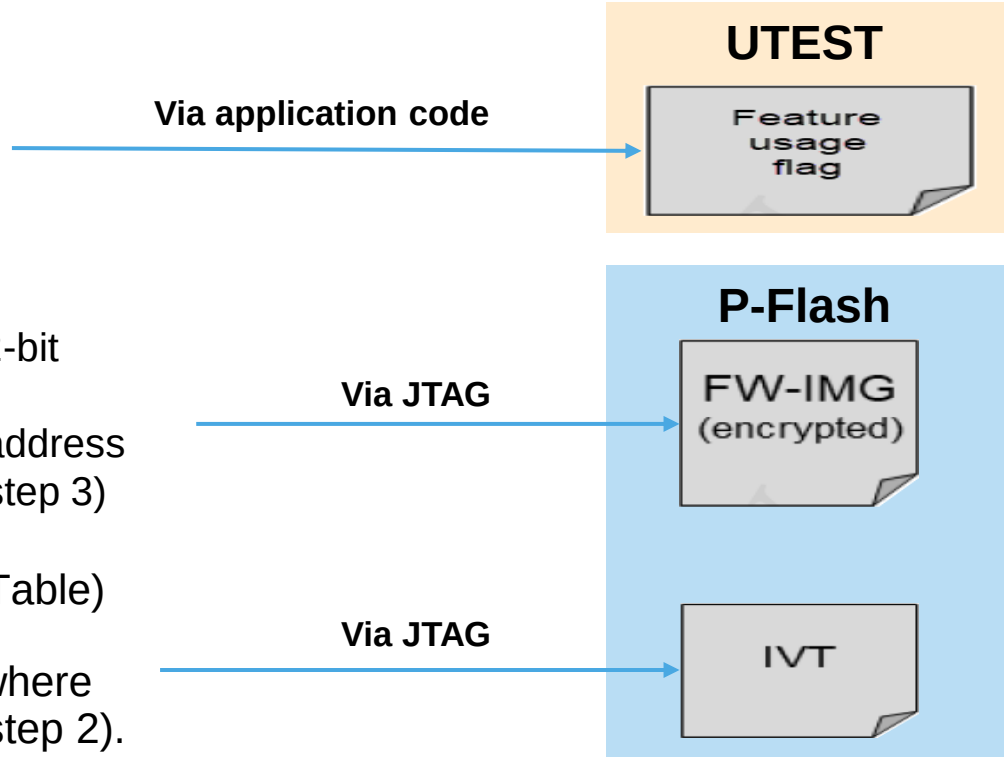
HSE FIRMWARE INSTALLATION

1. Program UTEST HSE FW feature usage flag value 0xAABBCCDDDDCCBBAA to address 0x1B000000. 8 bytes total.

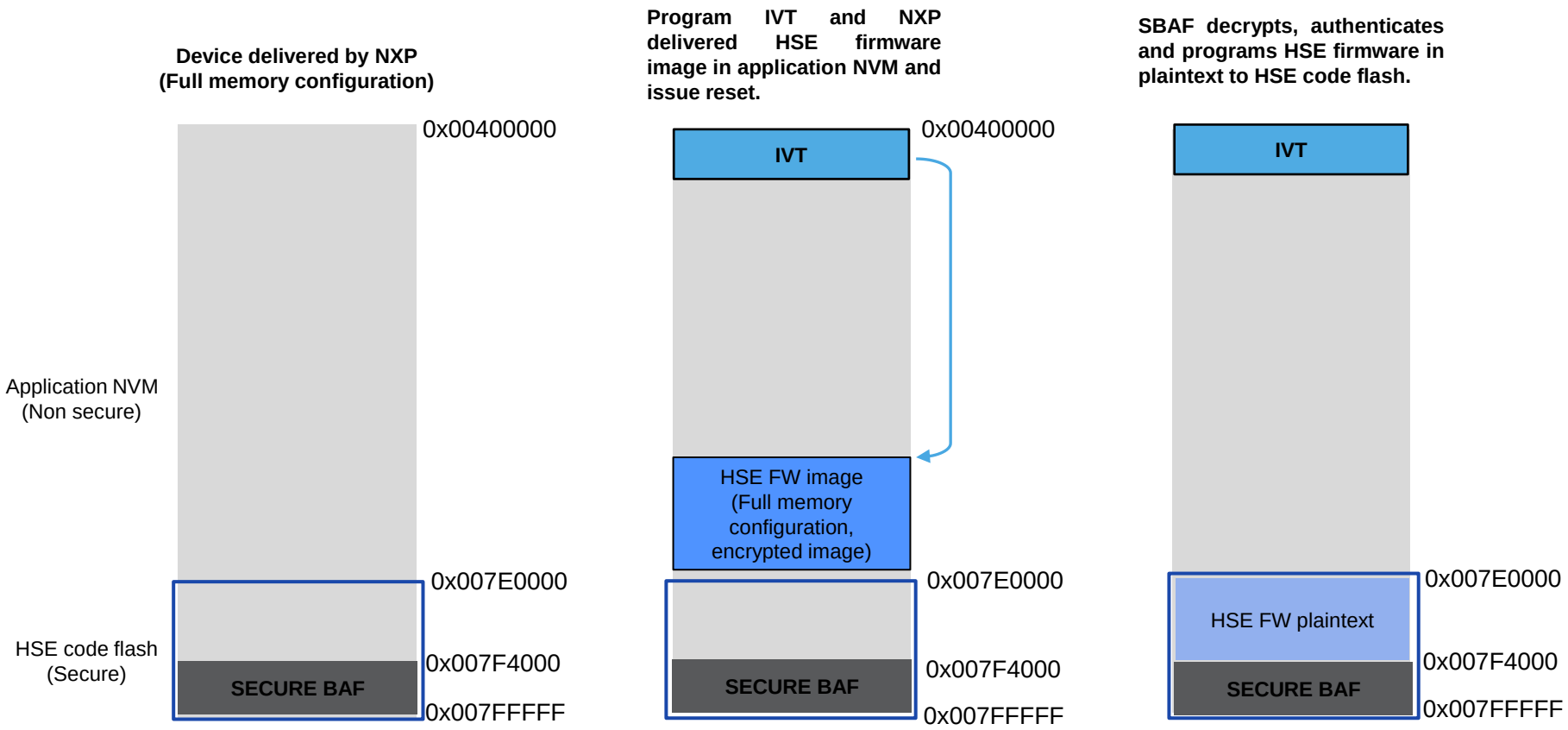
2. Program HSE encrypted binary to a 32-bit aligned address in P-Flash.
<u>Optional:</u> Load HSE binary directly at address 0x400000 so that IVT is not required (step 3)

3. Program a valid IVT (Image Vector Table) in one of the possible addresses, containing a pointer to the location where HSE encrypted binary was loaded (step 2).

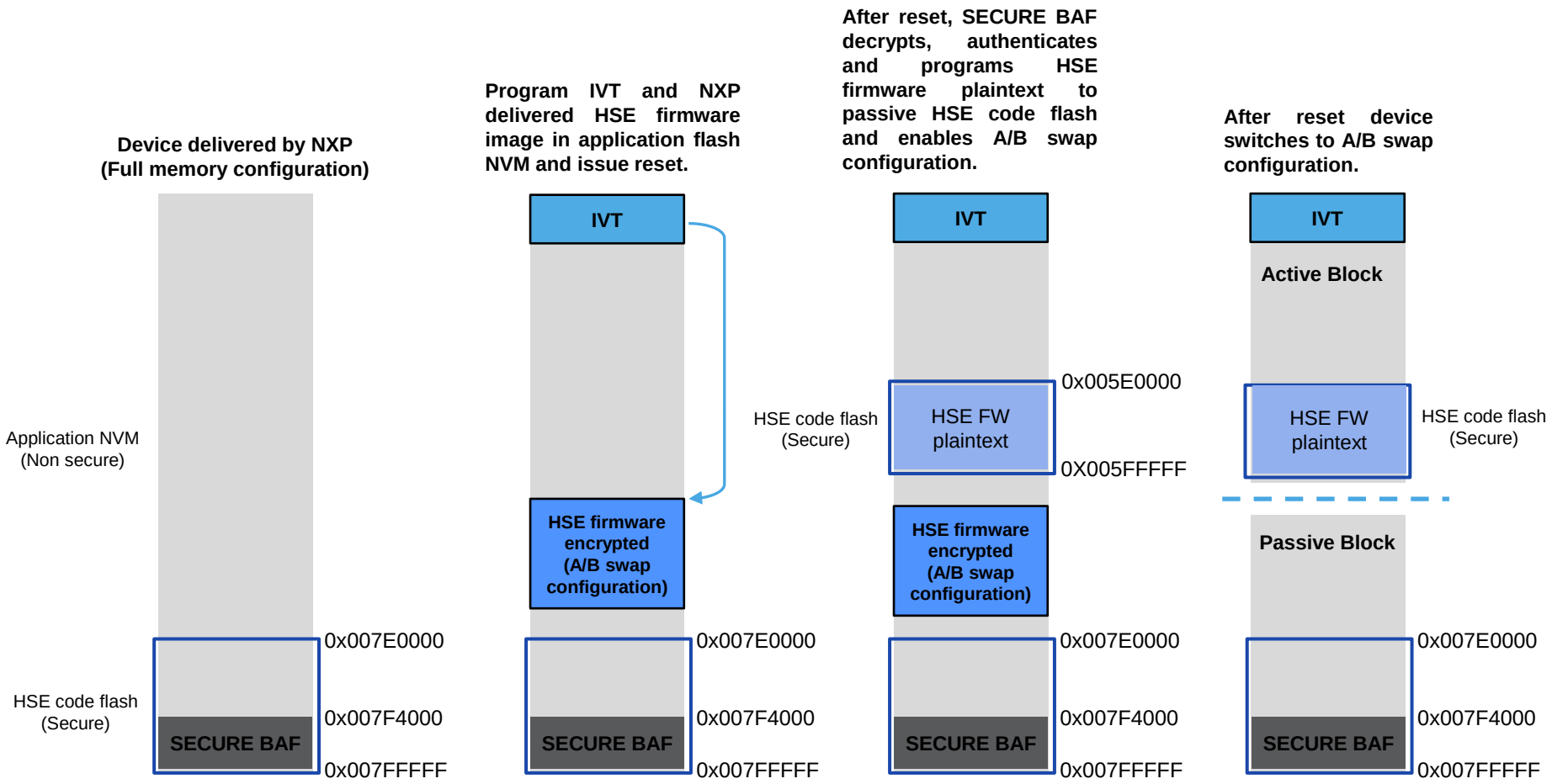
4. During next reset, the sBAF boot firmware runs the HSE installation process.
The encrypted binary in P-Flash can then be erased.



FLASH MEMORY LAYOUT DURING HSE FW INSTALLATION (FULL_MEM)



FLASH MEMORY LAYOUT DURING HSE FW INSTALLATION (AB_SWAP)

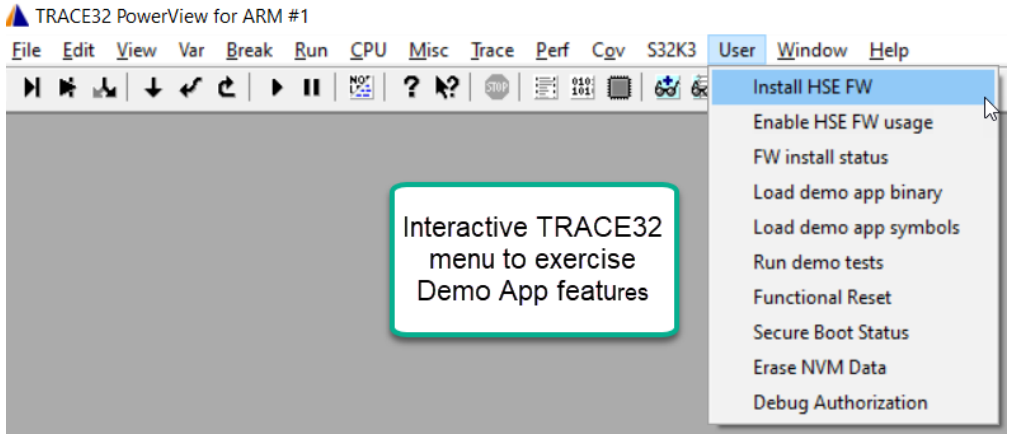


Note: A/B swap activation is definitive

HSE FW INSTALLATION AND BRING UP USING DEMO APP

The Demo App shows how to provision HSE FW on the S32K344 devices first time delivered to customer, while also running several examples of HSE services usage, such as:

- Initial configuration
- Cryptographic services
- FW Updates
- Secure boot
- UTEST programming for application debug process and life cycle advancement



For a detailed step by step guide on how to run the Demo App refer to the readme file in the Demo App package.

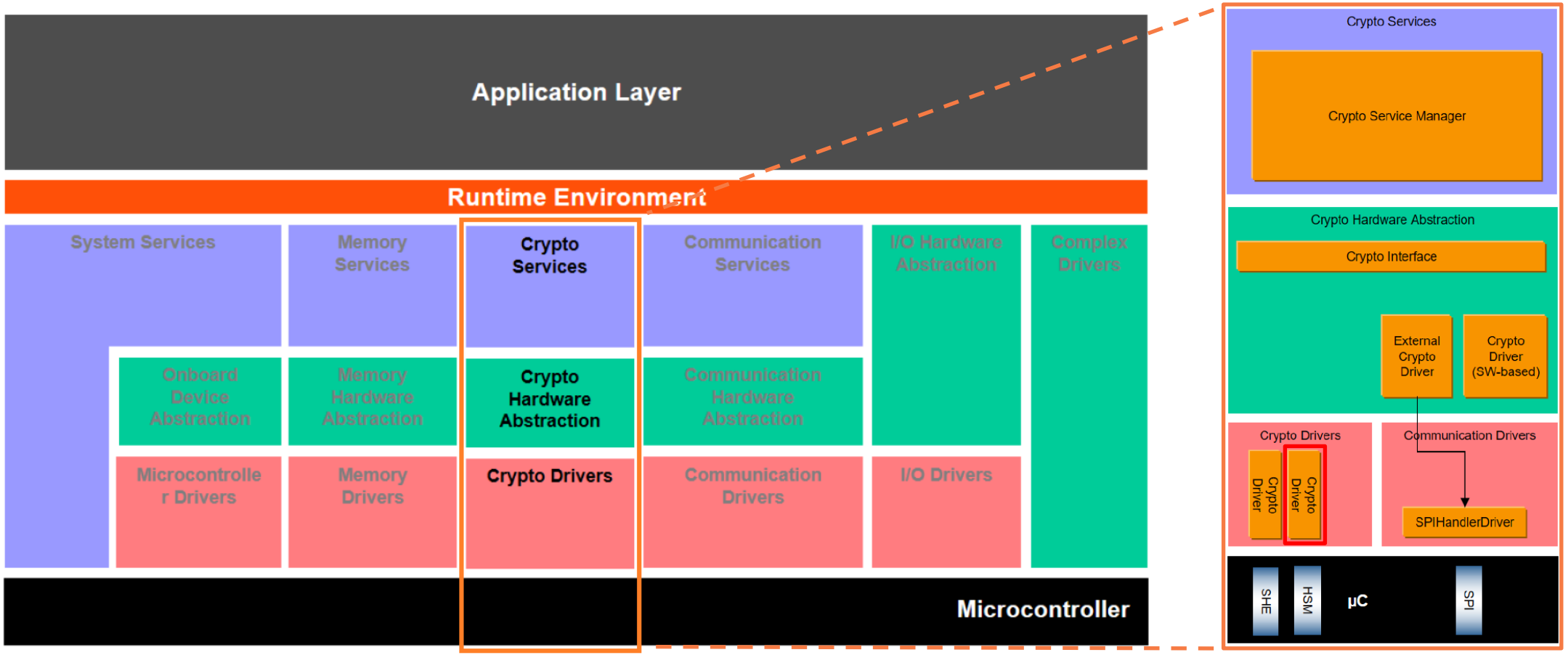
HSE_DEMOAPP_S32K3XX_0_0_8_3_ReadMe.pdf

Software Enablement

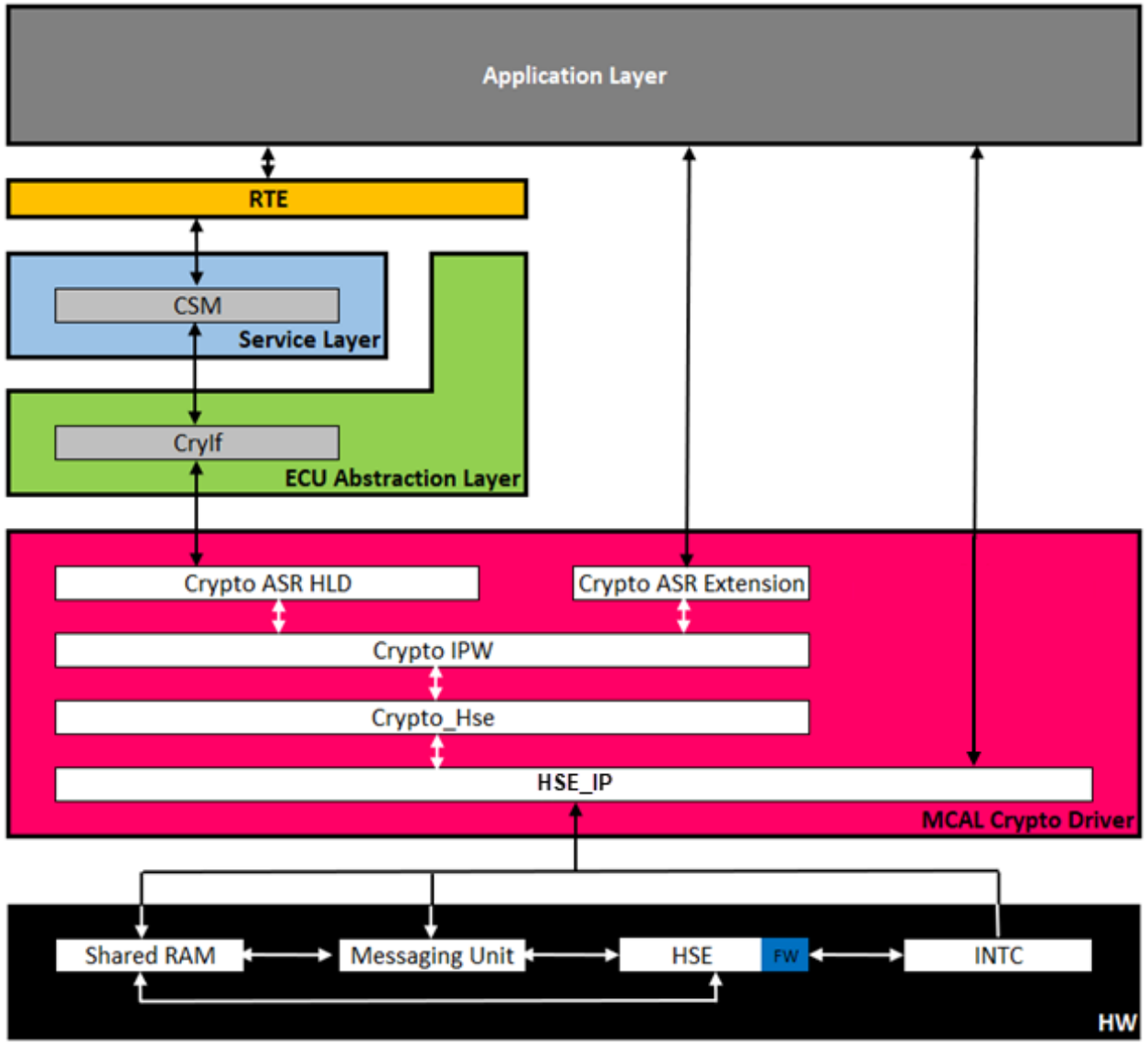
SECURE CONNECTIONS
FOR A SMARTER WORLD

CRYPTO DRIVER AS PART OF THE AUTOSAR STACK

- The Crypto Stack offers a standardized access to cryptographic services for applications and system functions.
- The Crypto Driver is a driver for a specific device, that is only abstracting the features supported by the hardware.



HSE ENABLED NXP CRYPTO STACK STRUCTURE
REAL-TIME DRIVERS (RTD)



S32K3 MICROCONTROLLERS FOR AUTOMOTIVE AND INDUSTRIAL

Tackling cost and complexity of automotive software development

S32K MCU family page

S32K3 MCU page

Online engineering support:

- S32K MCUs community

SECURE CONNECTIONS
FOR A SMARTER WORLD

SHOWROOM.NXP.COM