Automotive MCU Security and OTA Solution with Cost Optimized S32K1xx and S32K3xx Automotive MCUs

Osvaldo Romero and Guillaume Perret
GPIS Automotive System Engineering

OCTOBER 2020

SECURE CONNECTIONS
FOR A SMARTER WORLD

EXTERNAL

AGENDA

- Introduction on OTA and Security
- Use Cases
- Automotive Requirements
- S32K Solution
- Summary

THE S32K3 PRODUCT FAMILY ALSO FEATURED IN THIS PRESENTATION WILL ENTER PRODUCTION BEGINNING IN THE FOURTH QUARTER OF 2021. PRODUCT SPECIFICATIONS ARE SUBJECT TO CHANGE.

KEY DRIVERS FOR OVER THE AIR UPDATES

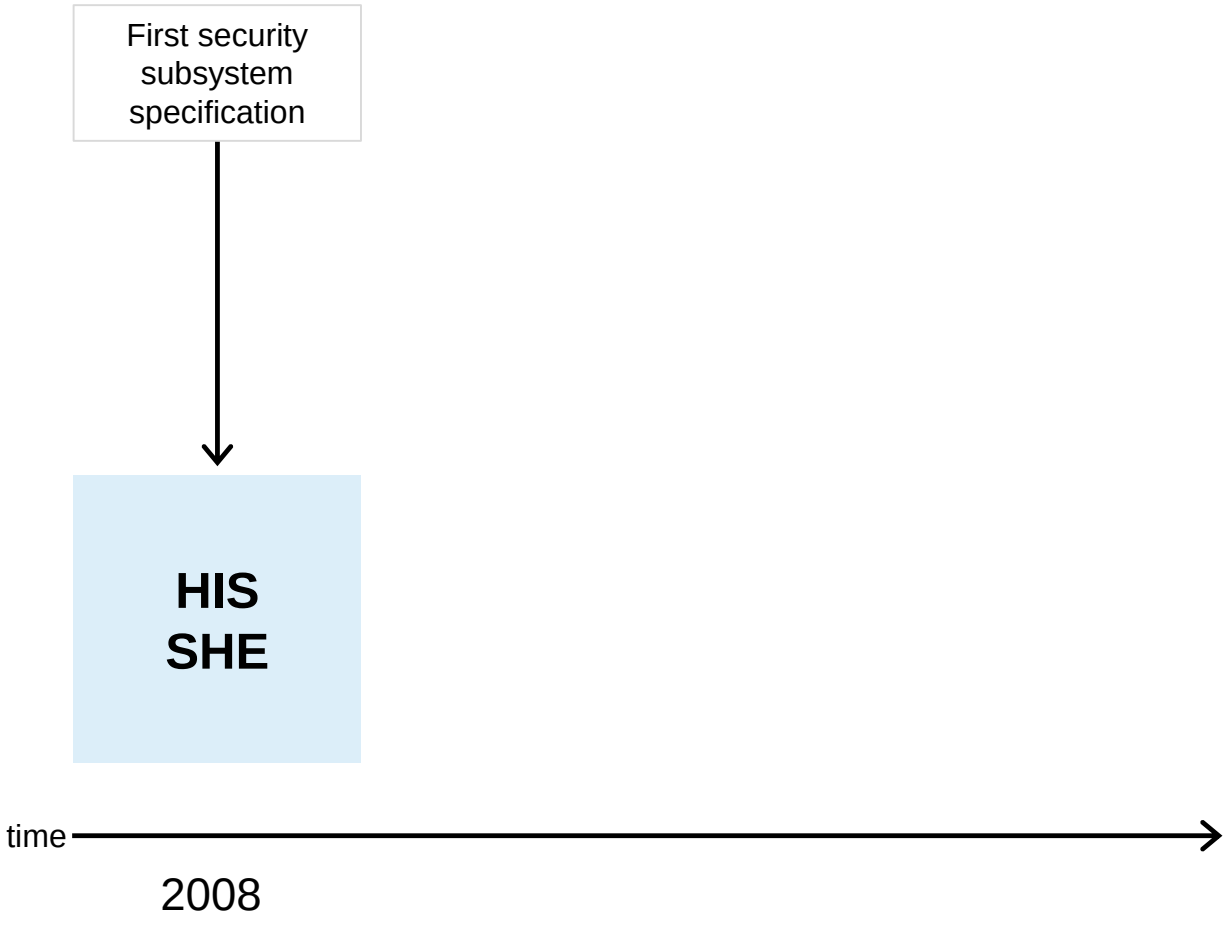
- Premium vehicles have over 100M lines of code! (Windows 10 has 50M)
- 15% of vehicle recalls and 60% of warranty costs are firmware related

- Firmware updates require vehicle to be returned to the garage
  - Time-consuming and costly
- No guarantee customer will return it for recall

- Difficult to deliver new features to vehicle owners
- OEMs are missing post-purchase, revenue-generation opportunities

AUTOMOTIVE SECURITY SPECIFICATIONS

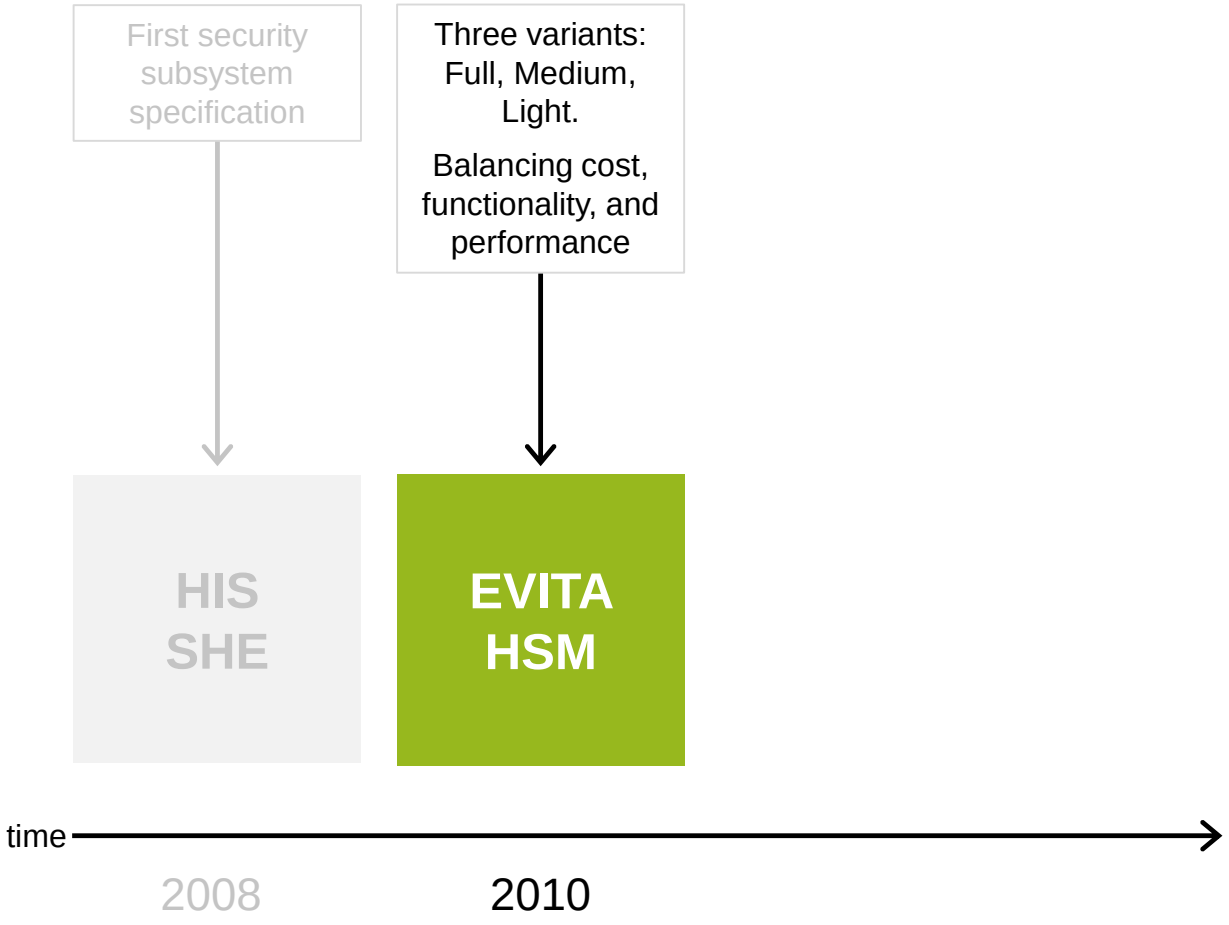
The SHE specification set the foundation, introducing the concept of a configurable (automotive) security subsystem



AUTOMOTIVE SECURITY SPECIFICATIONS

The SHE specification set the foundation, introducing the concept of a configurable (automotive) security subsystem

EVITA's HSM specification extended this concept into a programmable subsystem, in three flavors (Full, Medium, and Light), addressing a broader range of use cases

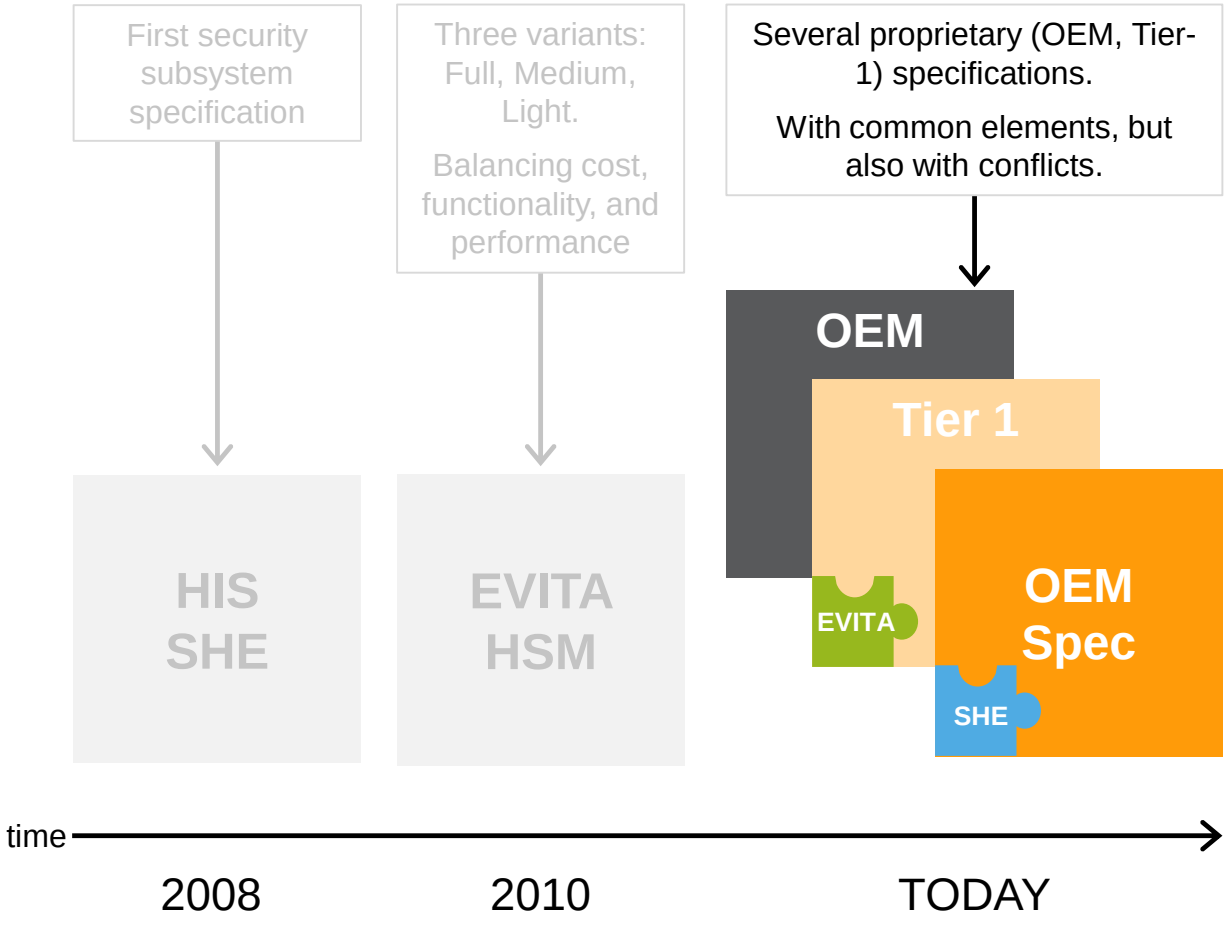


AUTOMOTIVE SECURITY SPECIFICATIONS

The SHE specification set the foundation, introducing the concept of a configurable (automotive) security subsystem

EVITA's HSM specification extended this concept into a programmable subsystem, in three flavors (Full, Medium, and Light), addressing a broader range of use cases

Nowadays, OEMs are creating their own technical specifications, including select aspects of SHE, EVITA, and FIPS 140-2



NO OTA WITHOUT SECURITY

- **Allowing Over The Air updates on a Automotive ECU opens new ways of hacking the device**

  → Protect communications and authenticate new data

- **Each step of the process must be secured and verified**

  → Establish a Chain of Trust

- **To keep up against malicious attacks, Security must remain up to date**

  → Security sub system must be updatable

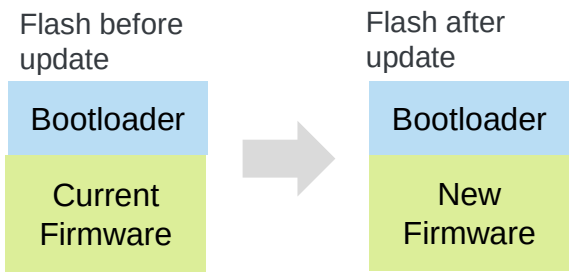
OTA and Security Use Cases in Automotive

OVER THE AIR (OTA) UPDATE METHODS

In general, there are 2 methods for performing updates to an end node

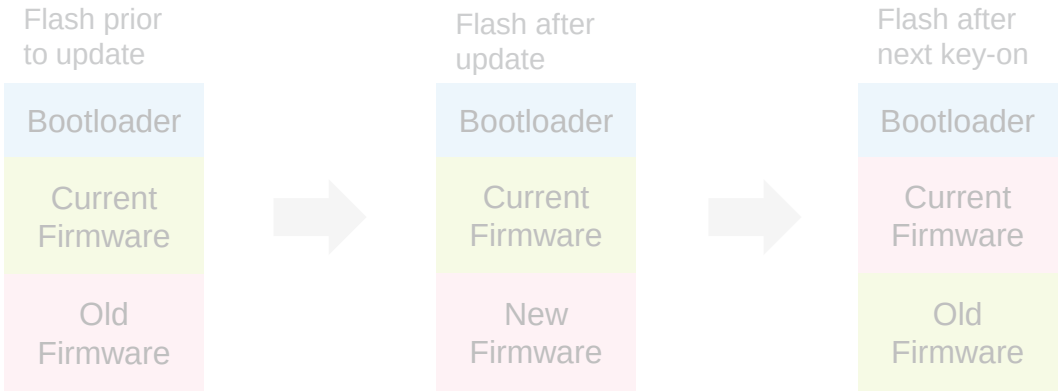
In Place

Update is performed on top of existing version



A/B

2 versions of firmware exist in internal flash.

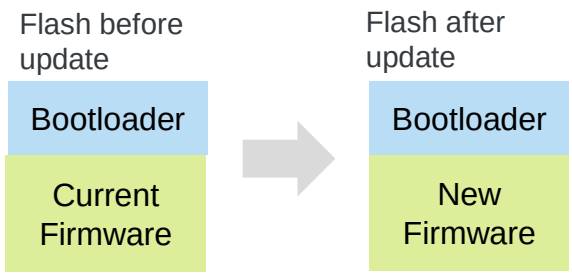


OVER THE AIR (OTA) UPDATE METHODS

In general, there are 2 methods for performing updates to an end node

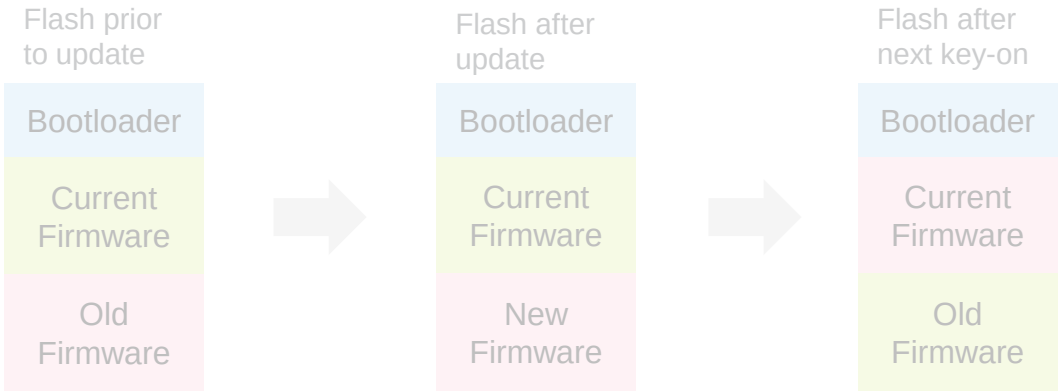
In Place

Update is performed on top of existing version



A/B

2 versions of firmware exist in internal flash.



Advantages

- No need for additional flash

Cost

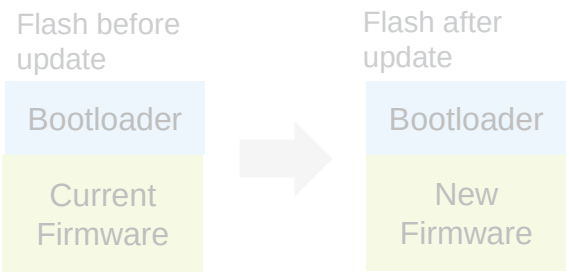
- Requires vehicle downtime during update process
- Not possible to instantly “roll-back” if an issue occurs
- Higher risk to have an ECU inoperable

OVER THE AIR (OTA) UPDATE METHODS

In general, there are 2 methods for performing updates to an end node

In Place

Update is performed on top of existing version



Advantages

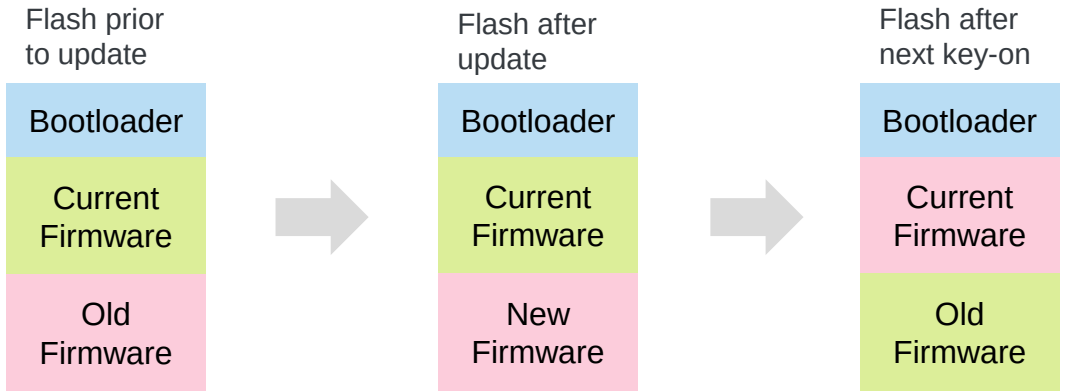
- No need for additional flash

Cost

- Requires vehicle downtime during update process
- Not possible to instantly “roll-back” if an issue occurs
- Higher risk to have an ECU inoperable

A/B

2 versions of firmware exist in internal flash.



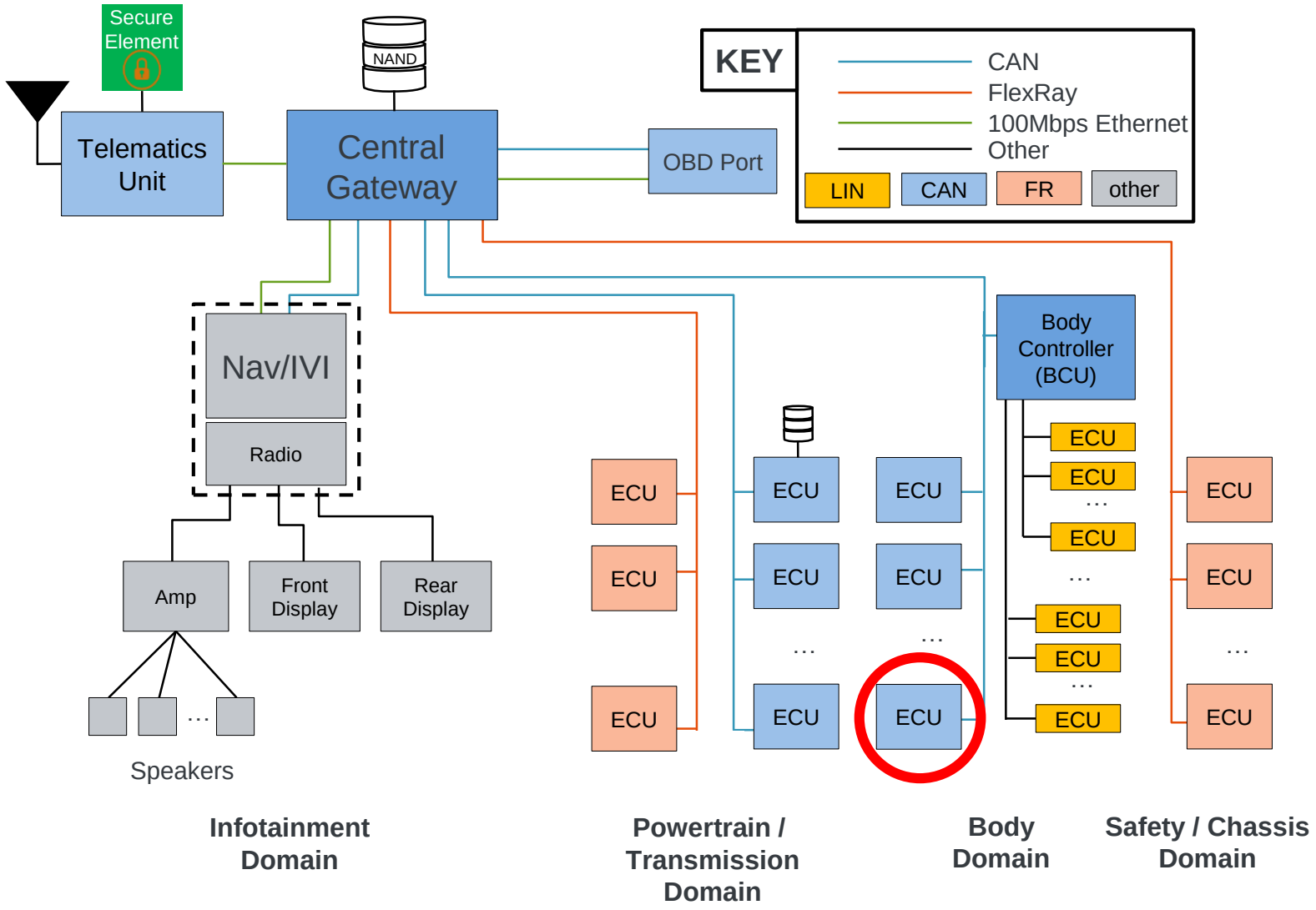
Advantages

- Update can be carried out whilst application is actively running from flash
- Always have original firmware to roll back to in case of issue
- Vehicle always available – guaranteed no vehicle downtime regardless of update errors

Cost

- Requires 2x flash application storage
- Higher max current (run current in block A + erase/program current in block B)

OTA USE CASE: 2 FW VERSIONS IN INTERNAL MEMORY



Example ECU A

Flash: 2x internal flash available

Security: Supports CMAC authentication and AES-128 decryption

Connection to Gateway: Ethernet

Vehicle Downtime: **none**

Security: **high**

Steps:

- Encrypted binary trickle downloaded and stored onto empty “B” flash on ECU.
- Firmware is decrypted and integrity checked as it is downloaded. Allows end-to-end security
- Once download complete, GW switches ECU to use new firmware from next boot

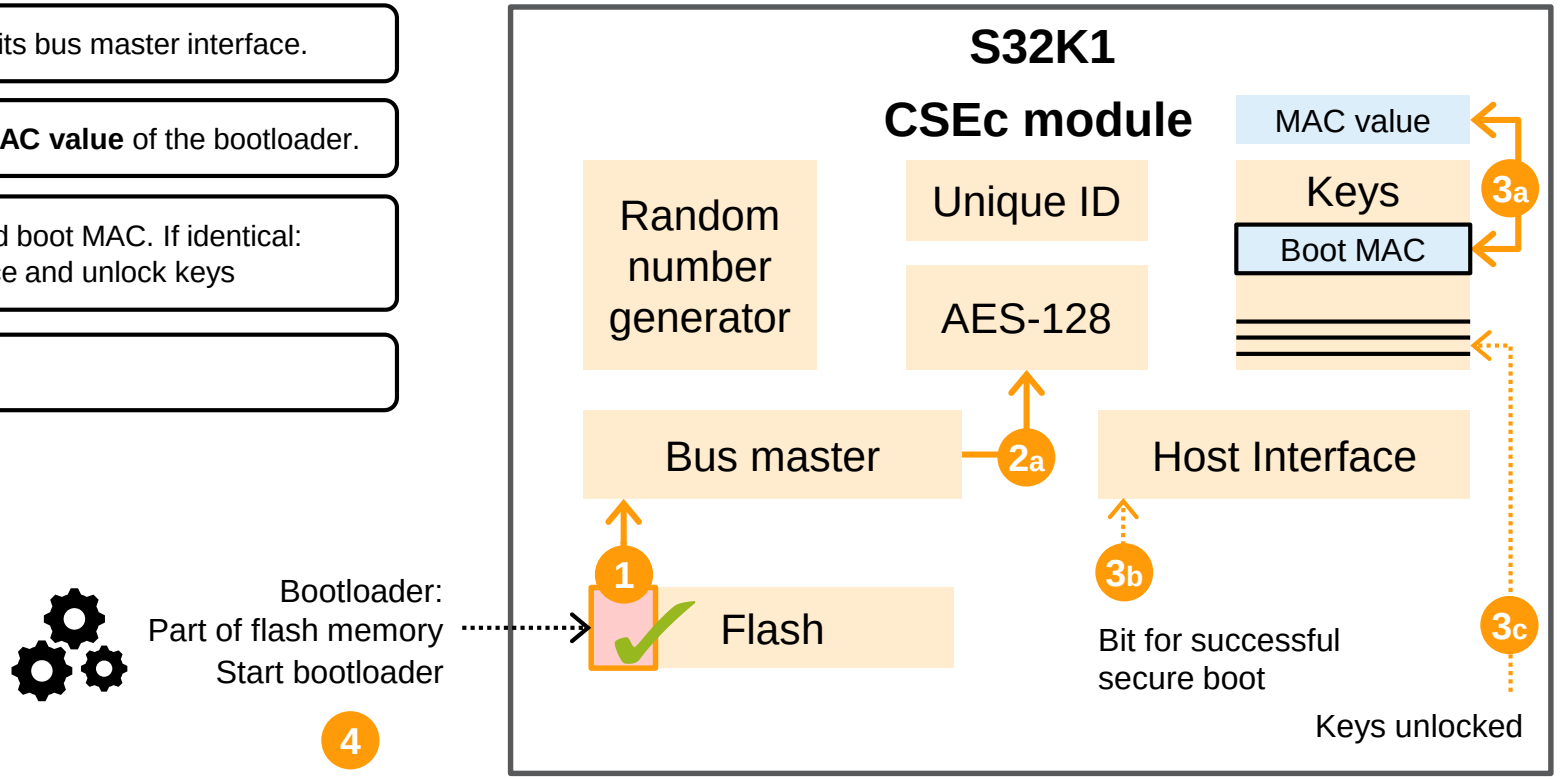
SECURE BOOT - CHECK BOOT LOADER FOR INTEGRITY AND AUTHENTICITY ON S32K1

Step 1: After power on: CSE module reads bootloader via its bus master interface.

Step 2: CSE module uses the boot key to calculates the **MAC value** of the bootloader.

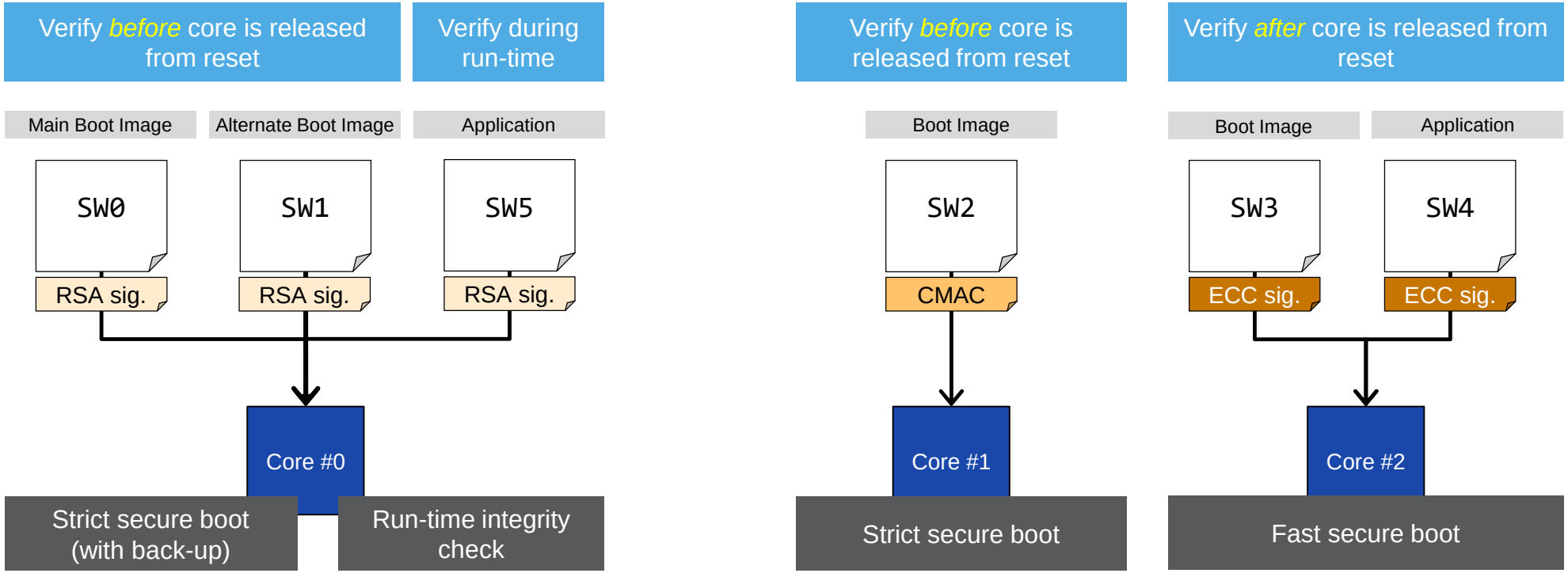
Step 3: CSE module compares calculated MAC with stored boot MAC. If identical: successful secure boot → set respective bit in host interface and unlock keys

Step 4: MCU always starts bootloader.

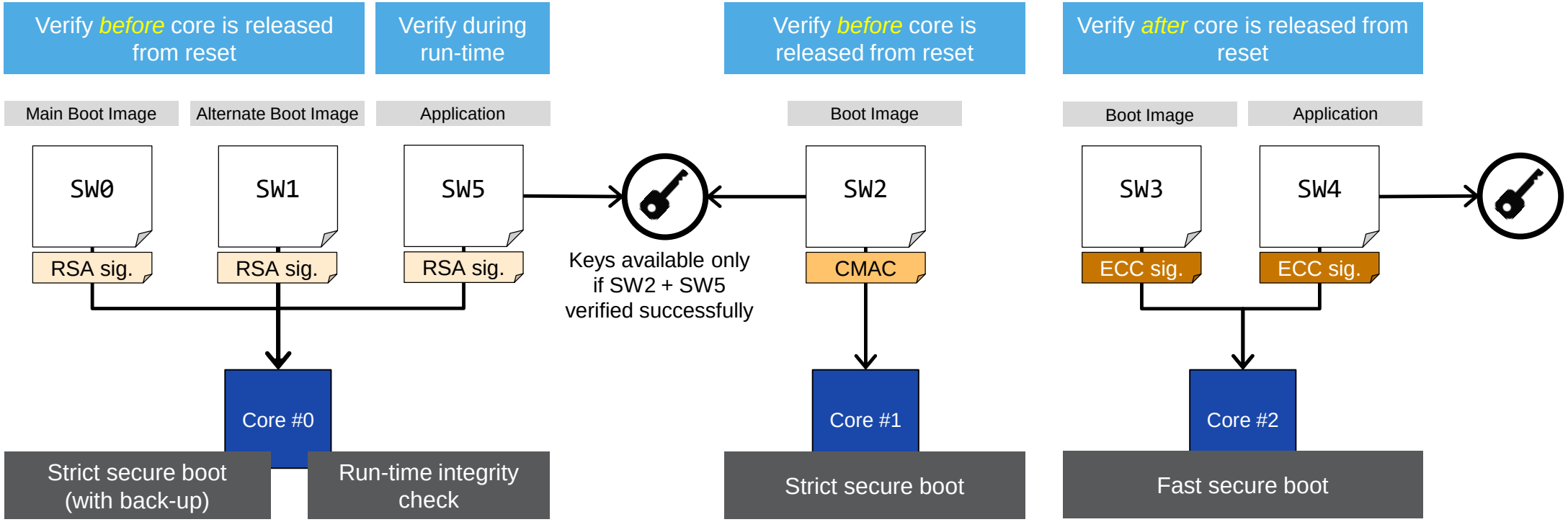


- **MAC** protects against modification of bootloader and depends on the (secret) boot key → integrity and authenticity of bootloader.
- Only if calculated MAC value matches stored boot MAC value: successful secure boot → set respective bit in host interface and unlock keys for further usage

SECURE BOOT CONFIGURATION EXAMPLE WITH S32K3



SECURE BOOT CONFIGURATION EXAMPLE WITH S32K3



→ Allows Versatile Verification Methods, Multiple Startup Orders and Sanctions ←

OTA and Security Automotive Requirements

OVER THE AIR UPDATES REQUIREMENTS

ECU reprogramming outside garage
Seamless update for driver (zero down time)

Seamless update
- Download while application running
- Zero down time
- Zero installation time

Memory features
- Read while write between flash banks
- Automatic firmware address translation
- Backup firmware

Always guarantee a working firmware in ECU as backup

Reliable and robust update
- Power and communication loss detection
- Multiple version of firmware available

System features
- Rollback functionality
- Version control
- Back up Firmware

Opens a door for security vulnerability

Attack protection
- Against firmware stealing
- Against malicious firmware installation

Security hardware
- Encryption/ decryption of data
- Firmware authentication check

SECURITY REQUIREMENTS – TODAY'S LANDSCAPE

	SHE	EVITA (Light / Medium / Full)	More recent needs
ARCHITECTURE	• Configurable, fixed function	• Programmable (except EVITA Light)	• Acceleration close to the interfaces (CAN and ETH MAC/PHYs) • Support for Flash-less technologies
FUNCTIONALITY	• Secure boot • Memory update protocol • AES-128 (ECB, CBC) • CMAC, AES-MP • TRNG, PRNG • Key derivation (fixed algorithm) • 10+4 keys, key-usage flags	Same as SHE, plus: • AES-PRNG • monotonic counters (16x, 64-bit) Plus, for EVITA Medium and Full: • WHIRLPOOL, HMAC-SHA1, ECDH and ECDSA (P256)	• Further crypto algorithms (e.g. RSA, SHA1-3, Curve25519, …) • Rollback protection • Key negotiation protocols • Communication protocol offloading (e.g. TLS, IPsec, MACsec, …) • Context separation / multi-application scenarios
OTHER			• Increased attack resistance (e.g. SCA, Fault Injection, …)
Covered by:	NXP CSE family (since 2010)		
	NXP HSM family (since 2015)		
	NXP HSE family (since 2019)		

S32K Solution

S32K OTA SOLUTION

S32K offers the most complete OTA portfolio

- A/B Swap support
- In place support

Seamless update

- Zero downtime - download while application running with **Read while write** between flash banks

No compiler/linker restrictions

- Automatic firmware **address translation**

Reliable and Robust update

- **Rollback functionality** to backup firmware controlled
- Secure firmware version control in hw
- Brownout and communication monitor in hw by **Firmware indicator validation**

Attack protection

- Encryption/ decryption of data
- Firmware authentication check

S32K3XX OVER-THE-AIR UPDATE – A/B SWAP SUPPORT

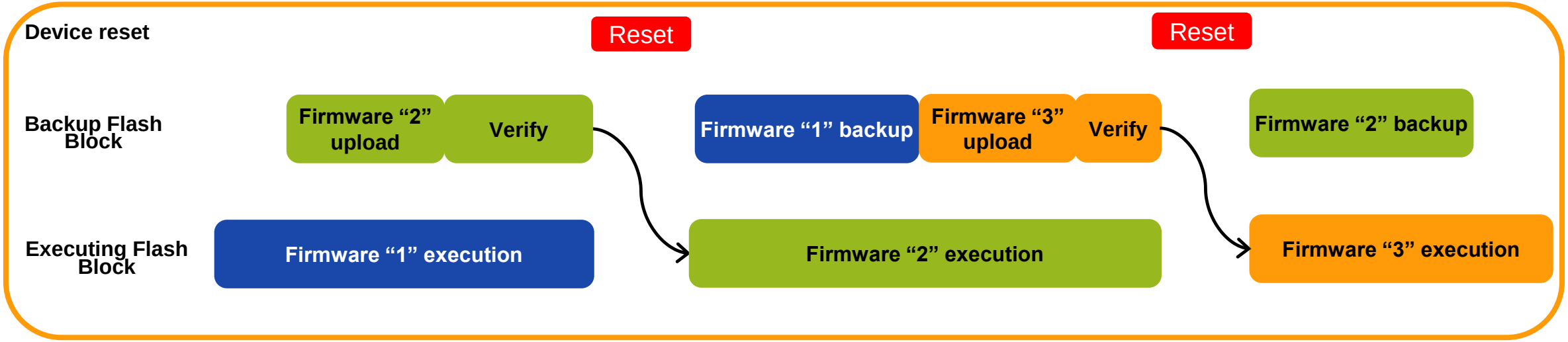
Use case: A/B swap in internal flash

- Current firmware executes and simultaneously uploads new firmware image into backup flash block
- After new firmware upload and verification. On the next reset new firmware will be executed

S32K3 Value

- Zero downtime, instant A/B swap after reset
- Download while application running
- Automatic address translation
- Backup firmware available

S32K3xx Firmware Update



S32K1 AND S32K3 FEATURE SET

S32K1	Basic set of cryptographic functions for SHE support	20 keys SHE update key protocol	SHE memory authenticity checks during start-up (CMAC)	
S32K3	Comprehensive cipher suite SHA-2, SHA-3, RSA and ECC support	Configurable set of keys Extensive key management (import, export, derive)	Extended memory authenticity checks during boot & run-time	Monotonic counters Secure tick

Proven Extensive Security Experience

- High security industry:
  - Leadership in banking card, e-passport, mobile payment

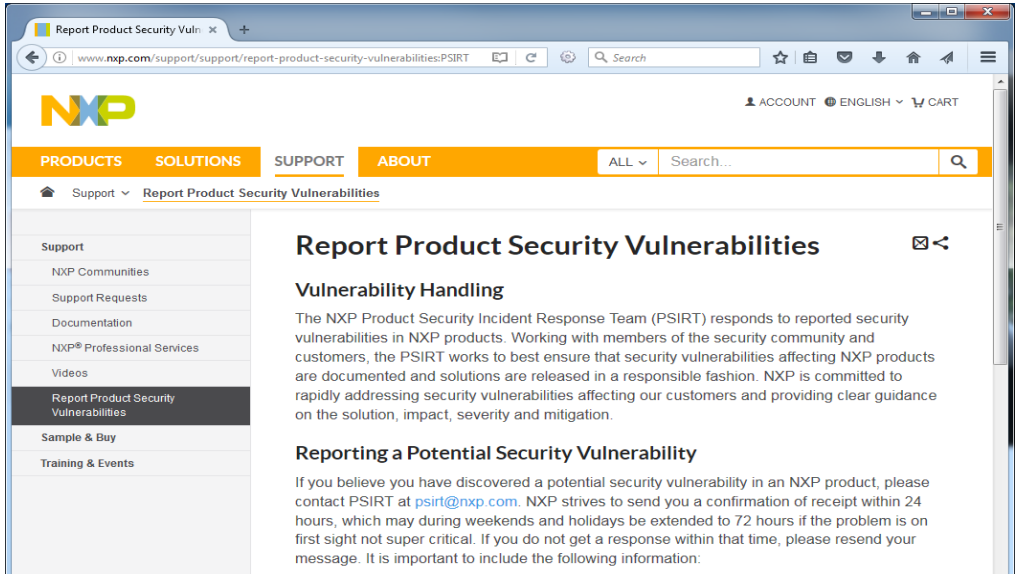
- Auto:
  - First to implement SHE security on silicon (2010)
  - All MPU/MCUs 2017 onward include crypto hardware

Root of Trust & Trusted Process

- Secure Trust Provisioning in non-secure production environment
- BootROM used to establish the Root of Trust during manufacturing

Product Security Incident Response Team

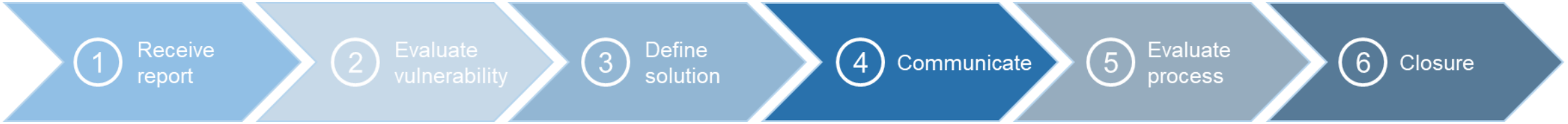
- Established in 2008
- Confirmation of receipt within 24 hours



Contact: www.nxp.com/psirt, psirt@nxp.com

Product Security Incident Response Team

- Established in 2008
- Confirmation of receipt within 24 hours
- Committed to Responsible Disclosure



Incident response process

Product Security Incident Response Team

- Established in 2008
- Confirmation of receipt within 24 hours
- Committed to Responsible Disclosure
- Security intelligence sharing with Auto ISAC

S32K3 SECURITY OFFER IS SIMPLER

Comprehensive service offer

- FAE support
- FQE analysis
- PSIRT
- Standard crypto-driver: MCAL

One-stop-shop (HW + FW)
Cost-optimized solution

S32x

ECU Functions & Features

High-level Security Stack
(AUTOSAR CSM, TLS, etc.)

VS

Two suppliers (HW / FW)
Higher solution cost & complexity

Competition

ECU Functions & Features

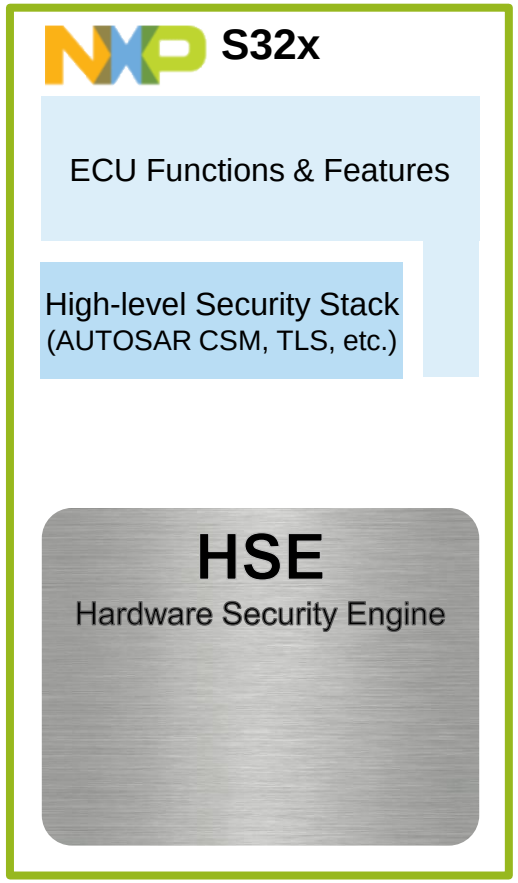
High-level Security Stack
(AUTOSAR CSM, TLS, etc.)

S32K3 SECURITY OFFER IS SIMPLER

Comprehensive service offer

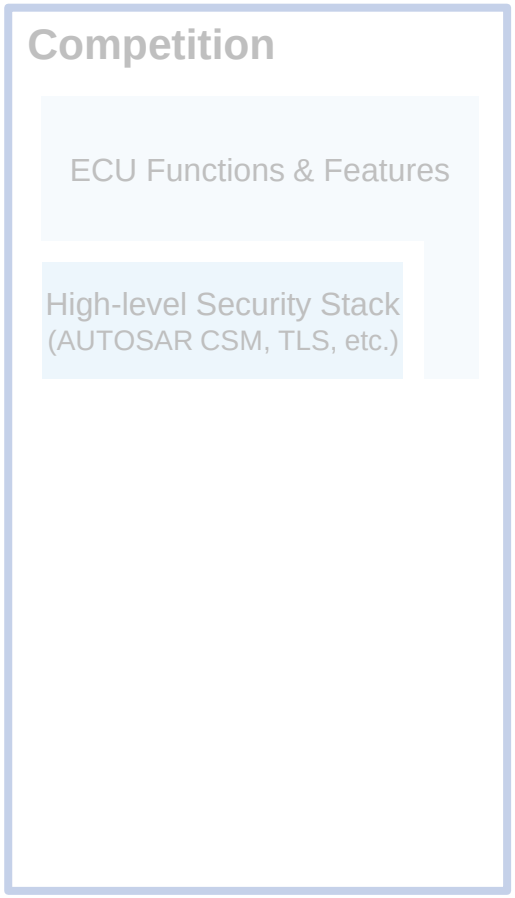
- FAE support
- FQE analysis
- PSIRT
- Standard crypto-driver: MCAL

One-stop-shop (HW + FW)
Cost-optimized solution



VS

Two suppliers (HW / FW)
Higher solution cost & complexity

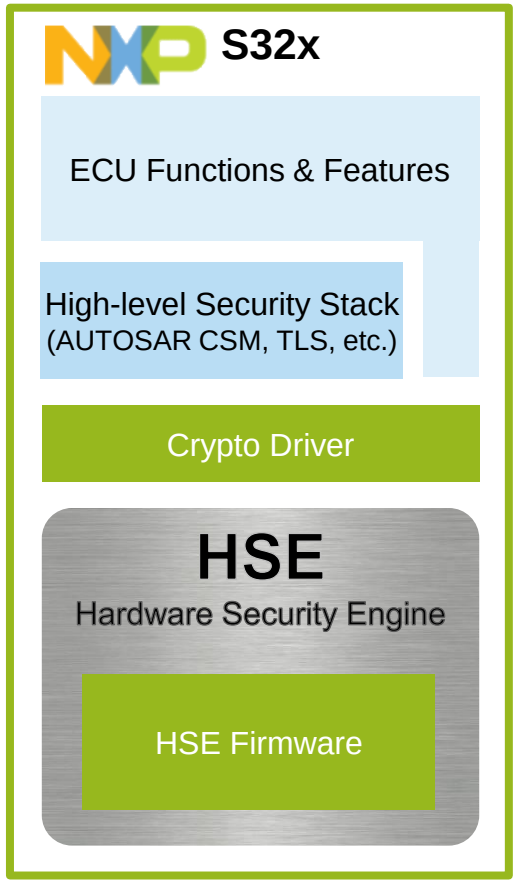


S32K3 SECURITY OFFER IS SIMPLER

Comprehensive service offer

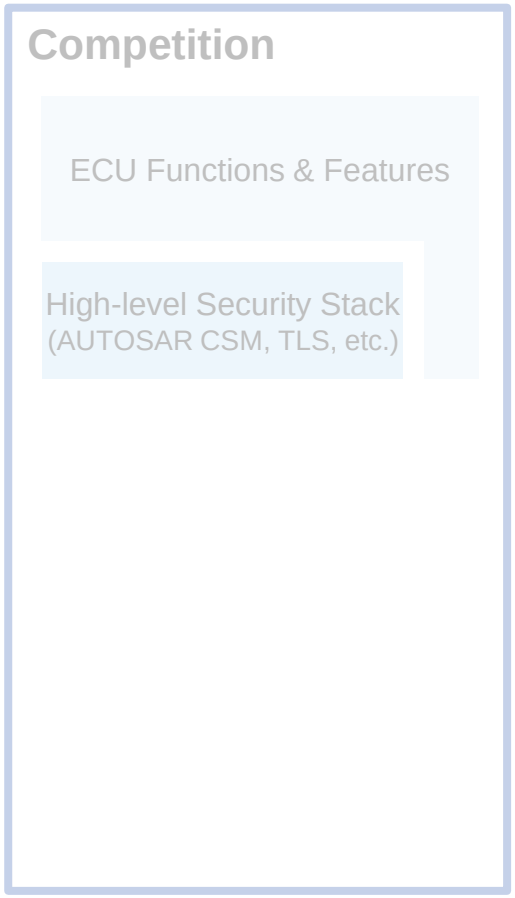
- FAE support
- FQE analysis
- PSIRT
- Standard crypto-driver: MCAL

One-stop-shop (HW + FW)
Cost-optimized solution



VS

Two suppliers (HW / FW)
Higher solution cost & complexity



S32K3 SECURITY OFFER IS SIMPLER

Comprehensive service offer

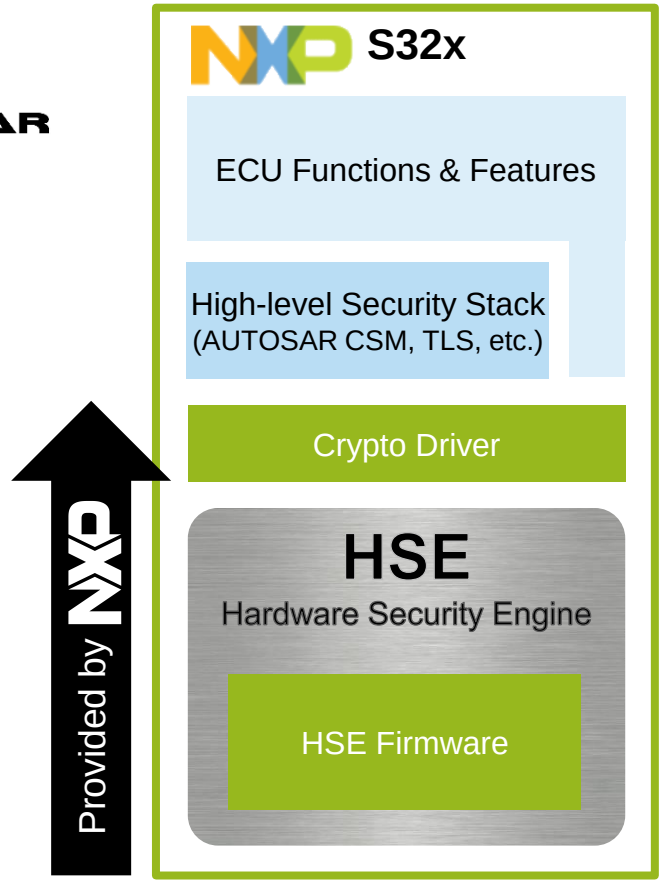
- FAE support
- FQE analysis
- PSIRT
- Standard crypto-driver: MCAL

AUTOSAR

No extra costs

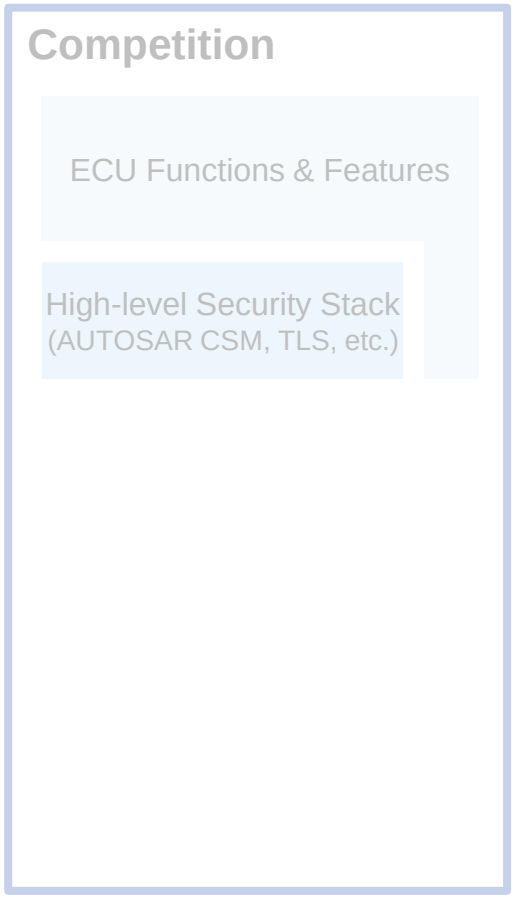
- No license fees
- No maintenance fees
- Solution cost covered by device price

One-stop-shop (HW + FW)
Cost-optimized solution



VS

Two suppliers (HW / FW)
Higher solution cost & complexity



S32K3 SECURITY OFFER IS SIMPLER

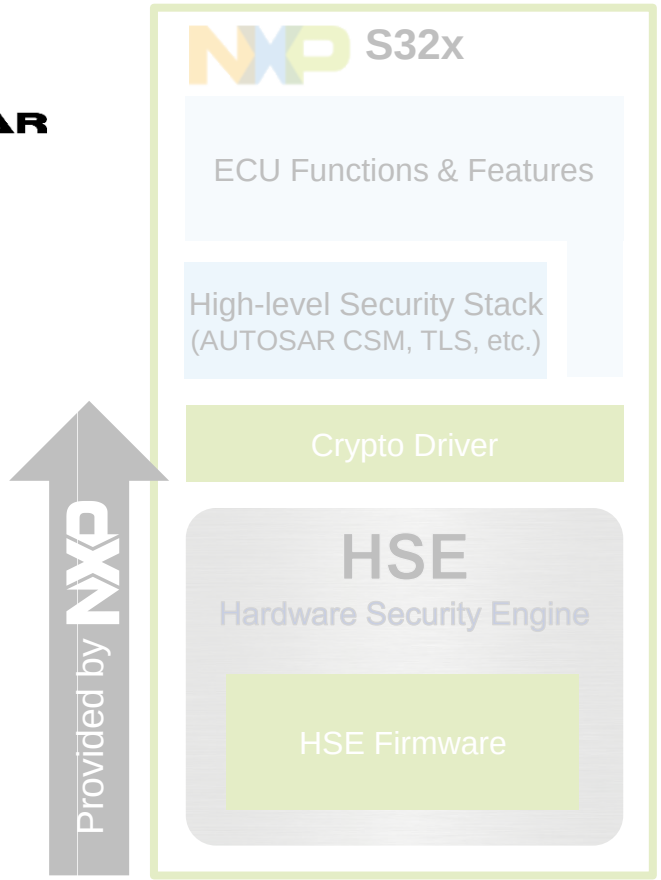
Comprehensive service offer

- FAE support
- FQE analysis
- PSIRT
- Standard crypto-driver: MCAL

No extra costs

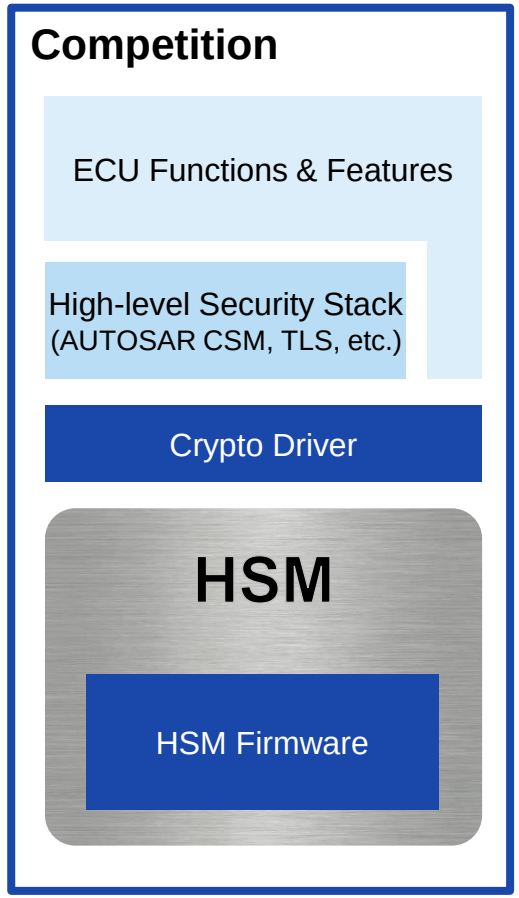
- No license fees
- No maintenance fees
- Solution cost covered by device price

One-stop-shop (HW + FW)
Cost-optimized solution



VS

Two suppliers (HW / FW)
Higher solution cost & complexity



S32K3 SECURITY OFFER IS SIMPLER

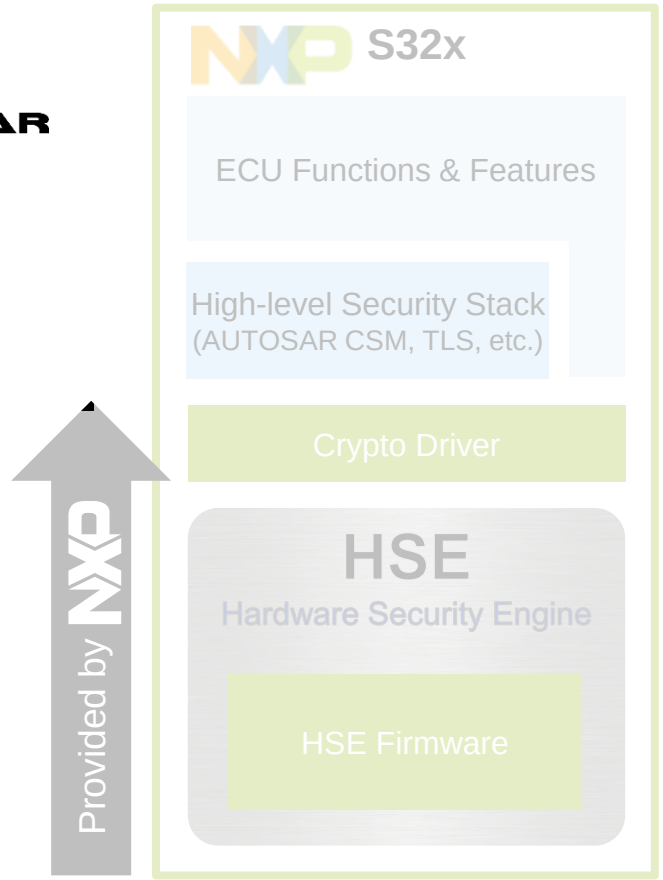
Comprehensive service offer

- FAE support
- FQE analysis
- PSIRT
- Standard crypto-driver: MCAL

No extra costs

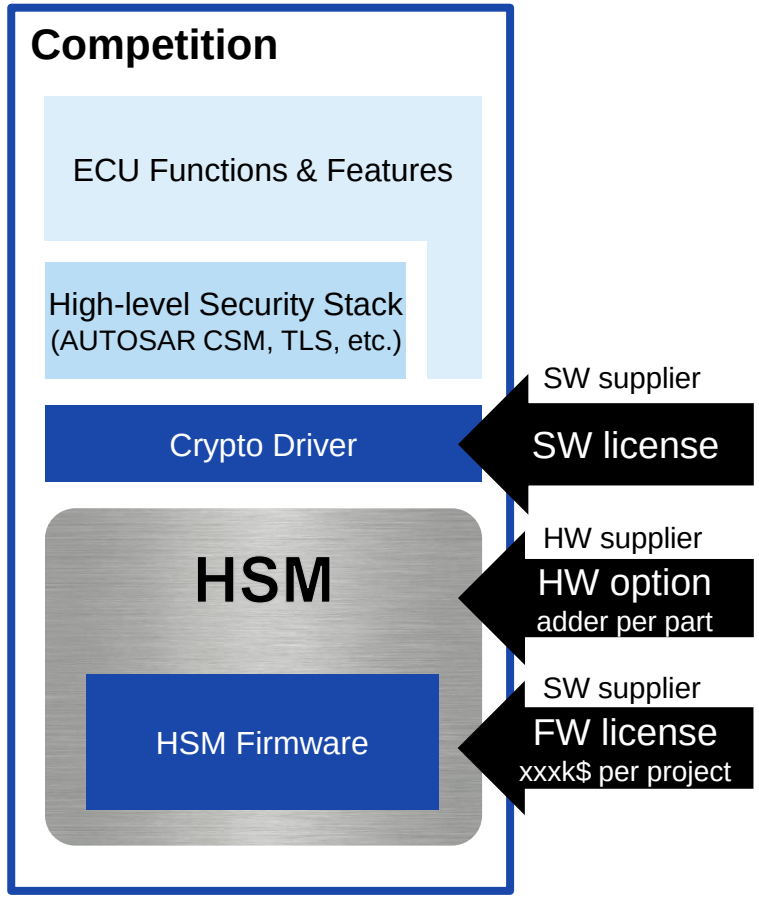
- No license fees
- No maintenance fees
- Solution cost covered by device price

One-stop-shop (HW + FW)
Cost-optimized solution

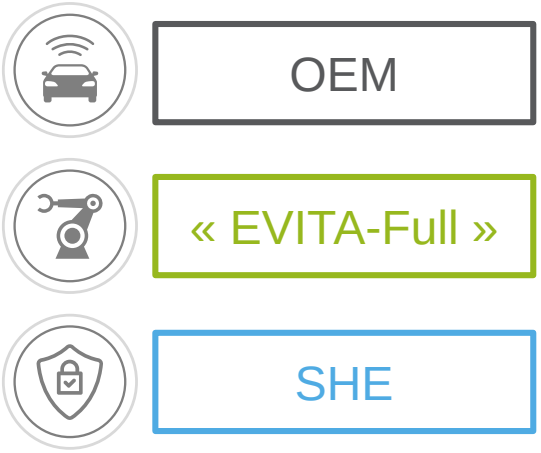


VS

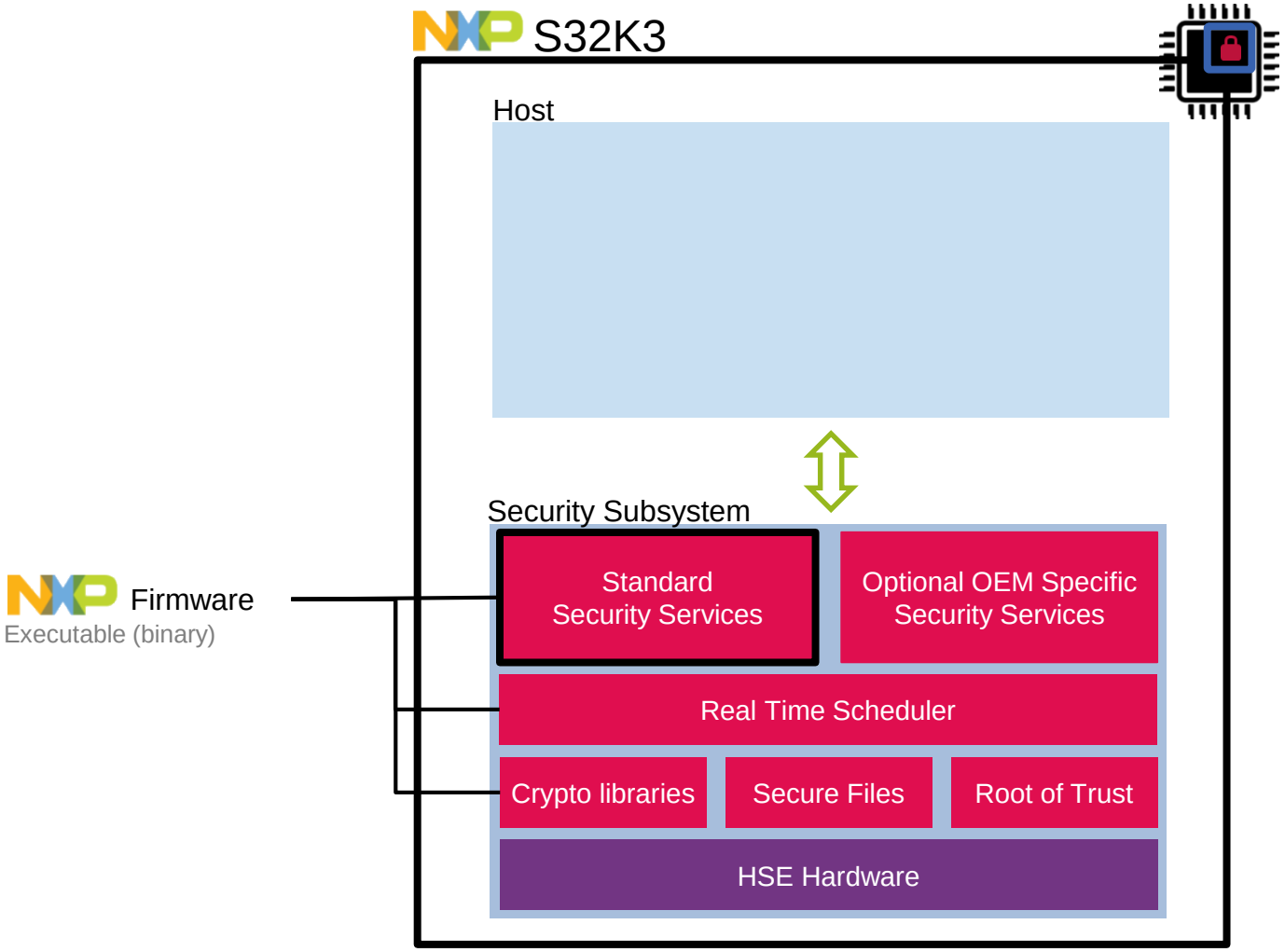
Two suppliers (HW / FW)
Higher solution cost & complexity



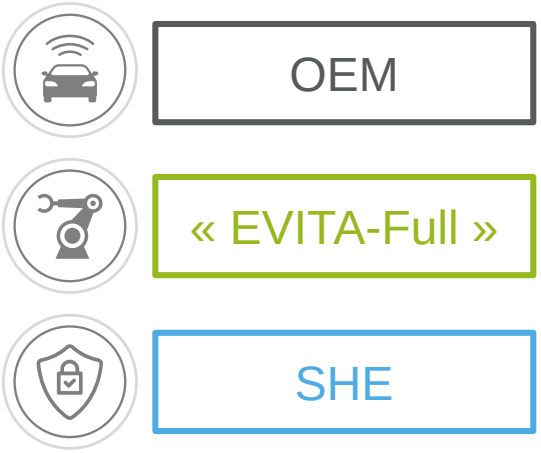
HOW S32K3 SUPPORTS AUTOMOTIVE REQUIREMENTS



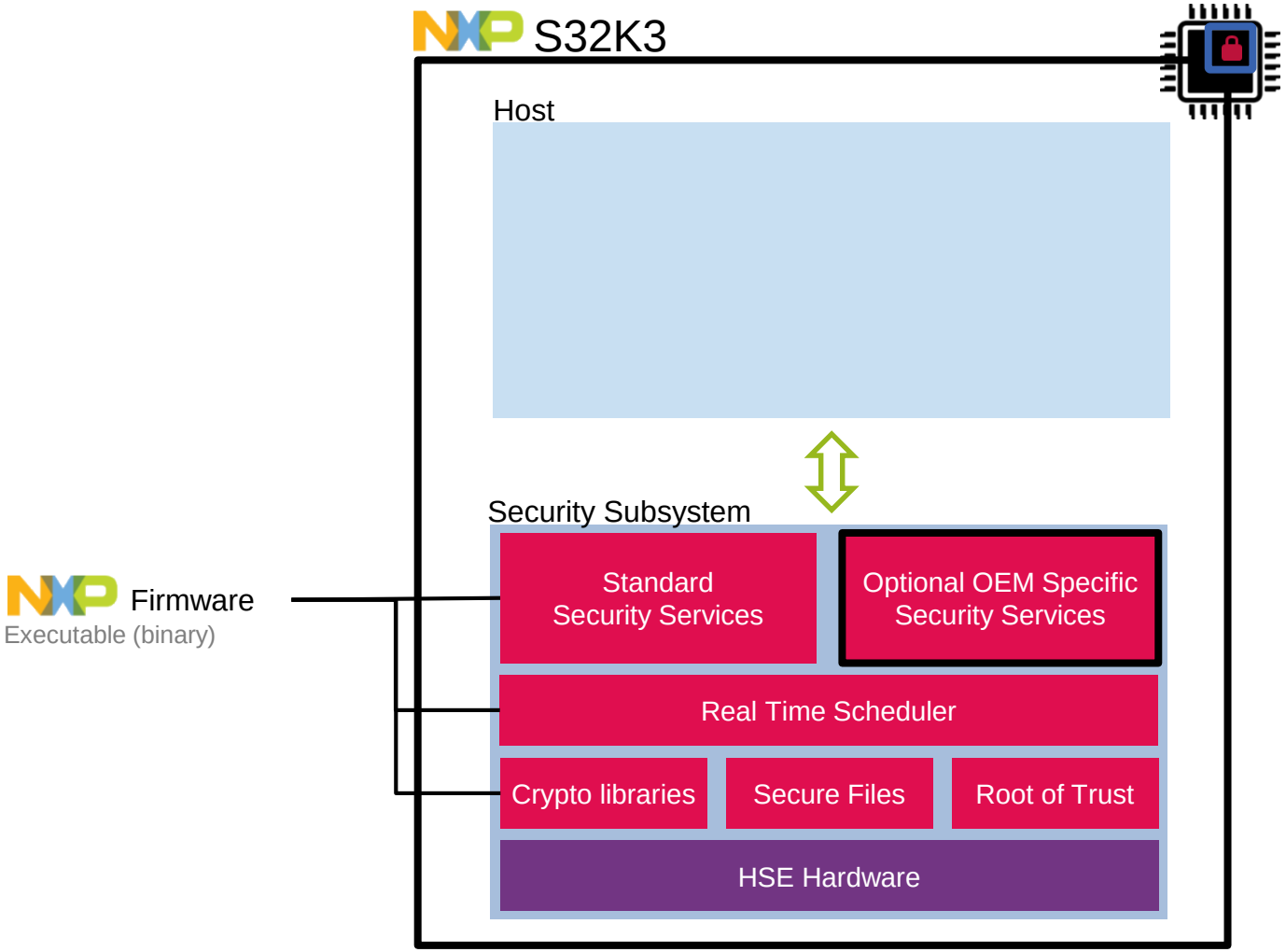
Requirements



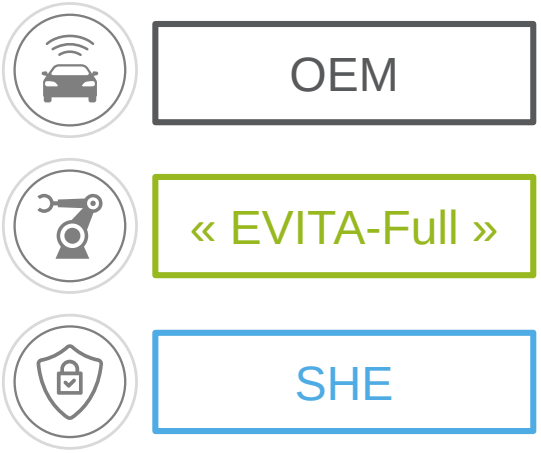
HOW S32K3 SUPPORTS AUTOMOTIVE REQUIREMENTS



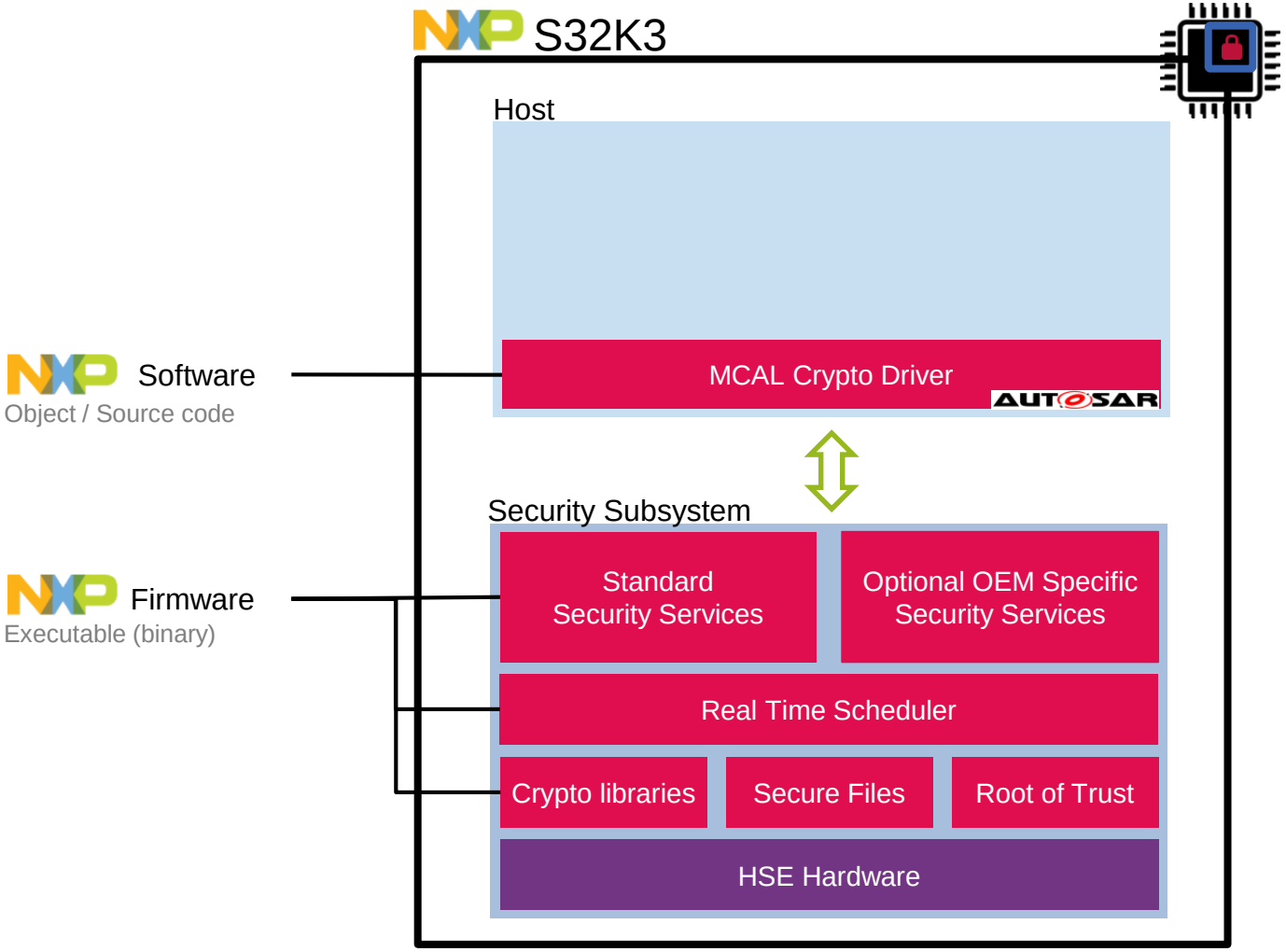
Requirements



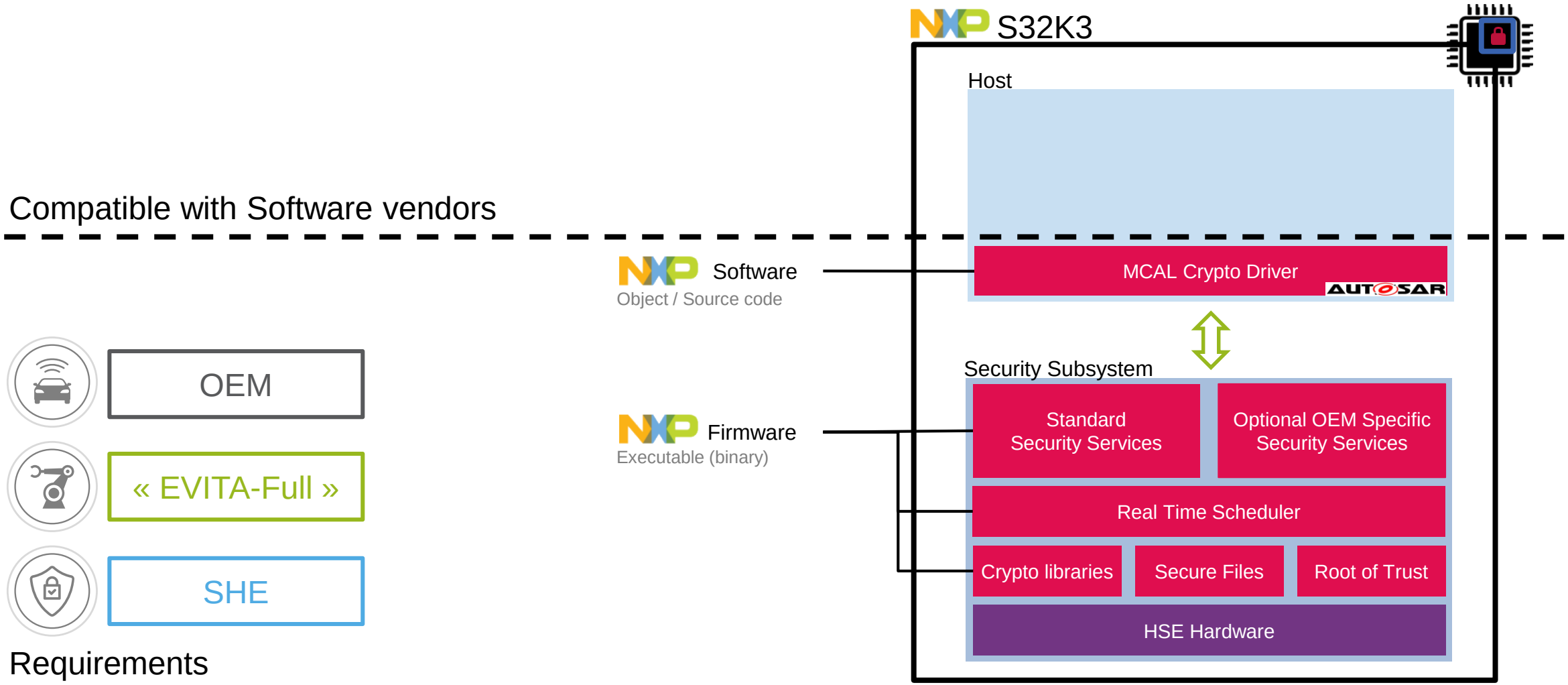
HOW S32K3 SUPPORTS AUTOMOTIVE REQUIREMENTS



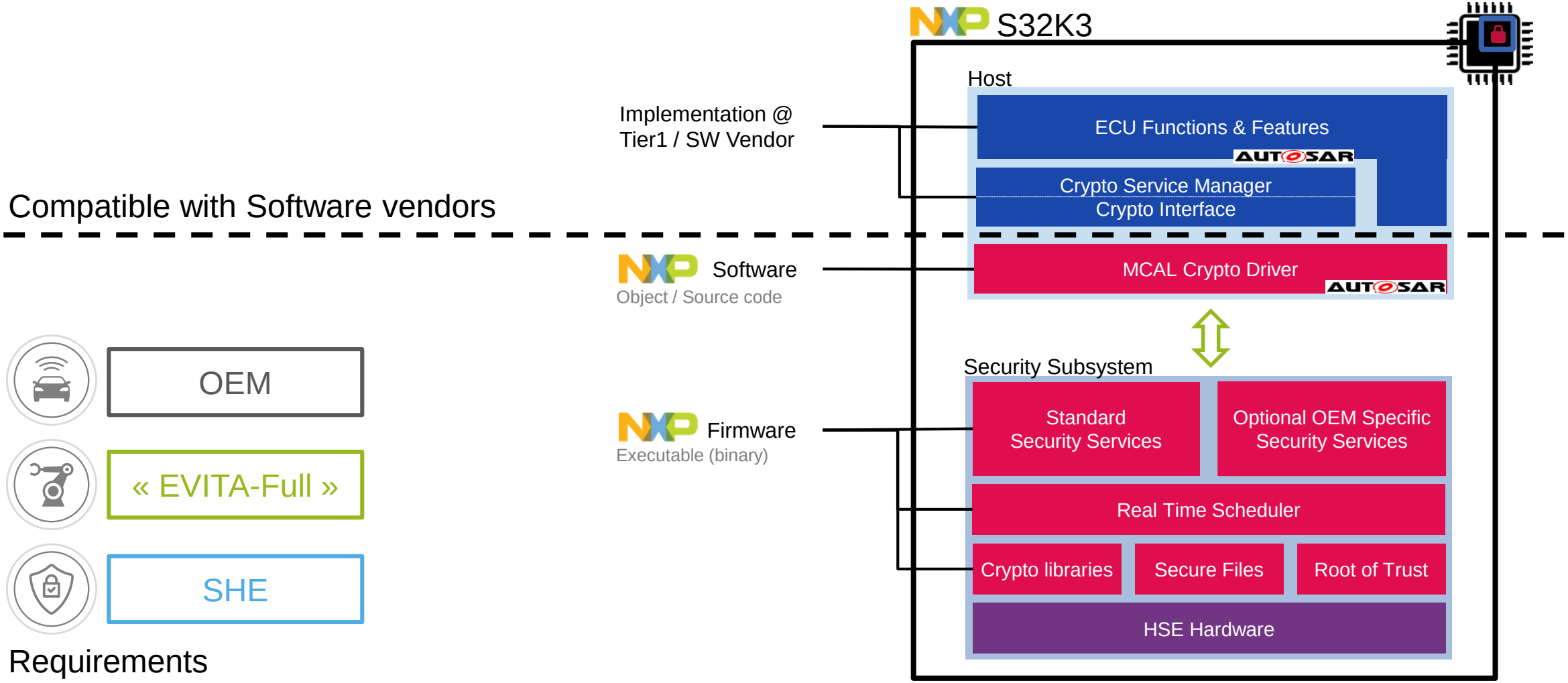
Requirements



HOW S32K3 SUPPORTS AUTOMOTIVE REQUIREMENTS



HOW S32K3 SUPPORTS AUTOMOTIVE REQUIREMENTS



ON-CHIP SECURE SUBSYSTEM: HSE SERVICE EXAMPLES

KEY MANAGEMENT

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

AES key up to 256 bits
RSA key up to 4096 bits

CRYPTO OPERATIONS

- AES
  Encryption & decryption
- CMAC / HMAC
  Generation & verification
- Hashing (SHA)
- RSA / ECC signature
  Generation & verification
- RSA OAEP / ECIES
  Encryption & decryption
- Random generation
  TRNG & PRNG

All operations hardware accelerated

PLATFORM SECURITY

- Strict secure boot
  Verify-then-start
- Parallel secure boot
  Verify-and-start
- On-demand verification
  Secure boot control in app.
- Configurable sanctions
  E.g. key usage restrictions

Secure boot optimized for latency

NXP: SECURITY 1 STOP-SHOP

- HW, FW and SW co developed and co verified by NXP:
  - **Total quality**
  - NXP is able to fix HW, FW or SW by applying change to any of those items
- FAE team support: a single point of contact with experienced engineers both in HW and SW that already know your application
- Enablement for development:
  - Reference manuals, application notes, demos…
  - AUTOSAR support: one supplier for Security and all other functions
- Logistics, ECU and Car Manufacturing, In-Field support:
  - Dealing with 1 supplier only, that will manage HW **and** SW issues
  - Cost efficient and streamline solution (no license fee or maintenance for third party FW)

S32K3 offers a complete secure OTA Solution

- Seamless and robust solution for A/B Swap and In place updates
- Security 1 stop-shop: Hardware + Software
- Meeting latest security and OTA market requirements
- Future proof with updatable secure software

SECURE CONNECTIONS
FOR A SMARTER WORLD