S32K3安全和无线更新(OTA)

曾福 & 唐林
系统应用工程师

2021年12月

SECURE CONNECTIONS
FOR A SMARTER WORLD

PUBLIC

AGENDA

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

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

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

KEY DRIVERS FOR OVER THE AIR UPDATES

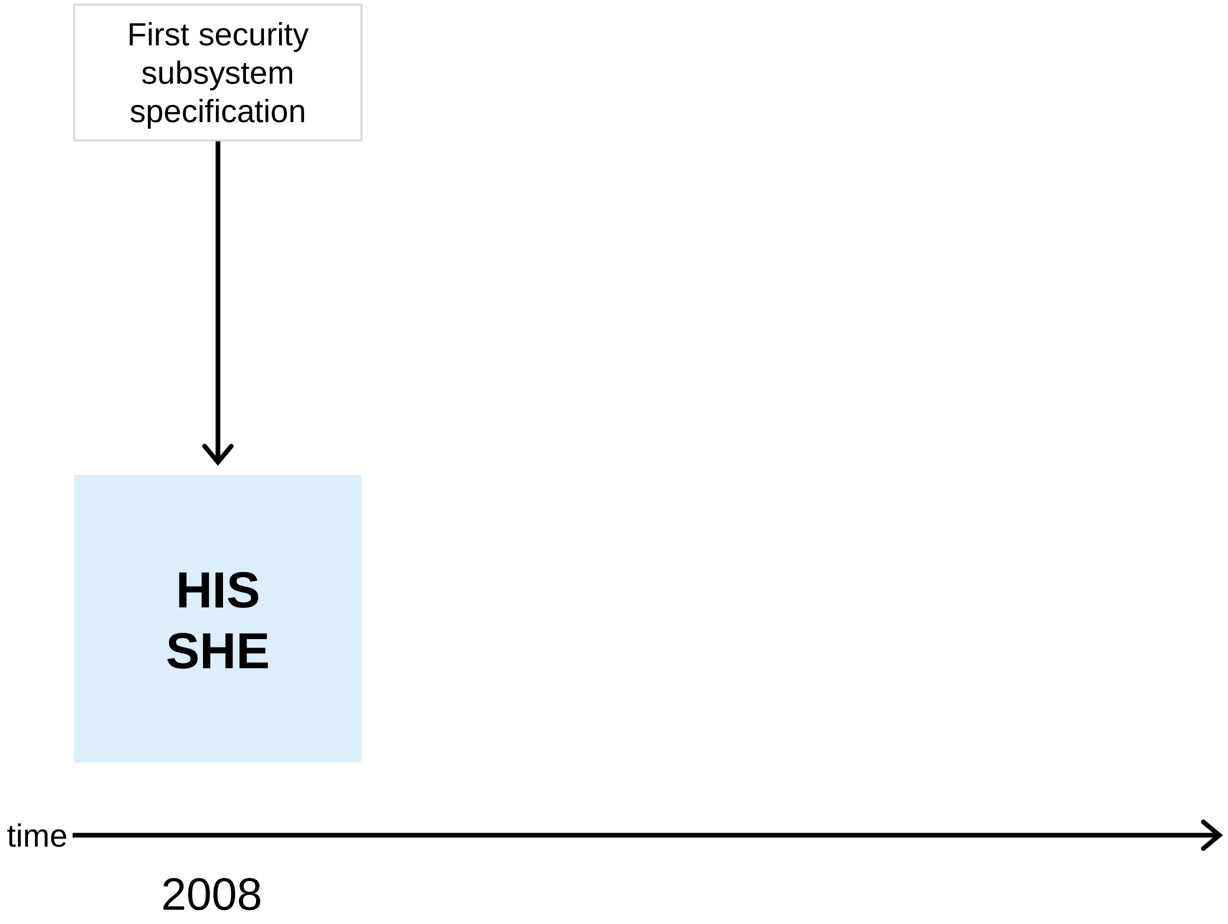
- Premium vehicles have over 100M lines of code! (Windows 10 has 50M)
- 15% of vehicle recalls and 60% of warranty costs are firmware related

- 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

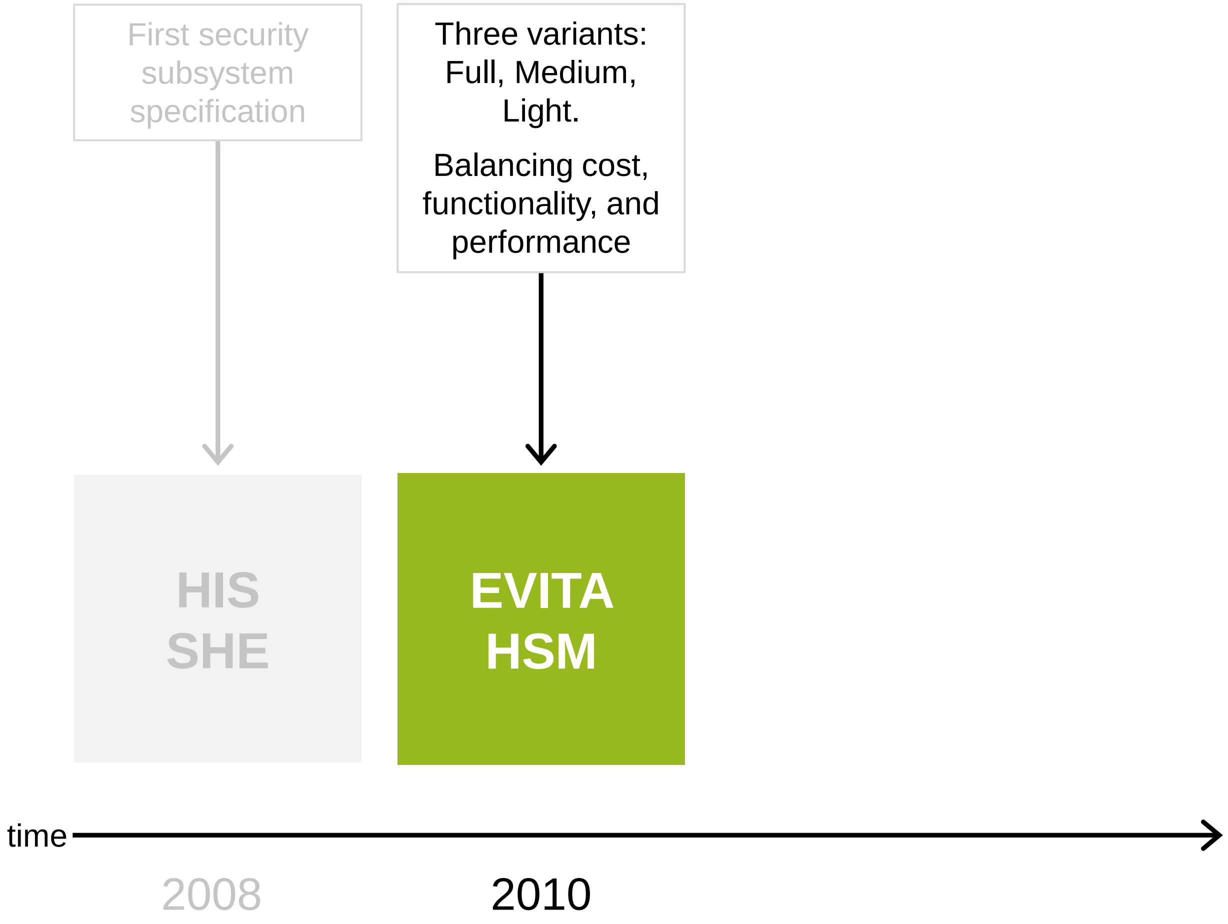
The SHE specification set the foundation, introducing the concept of a configurable (automotive) security subsystem



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



First security subsystem specification

Three variants: Full, Medium, Light.

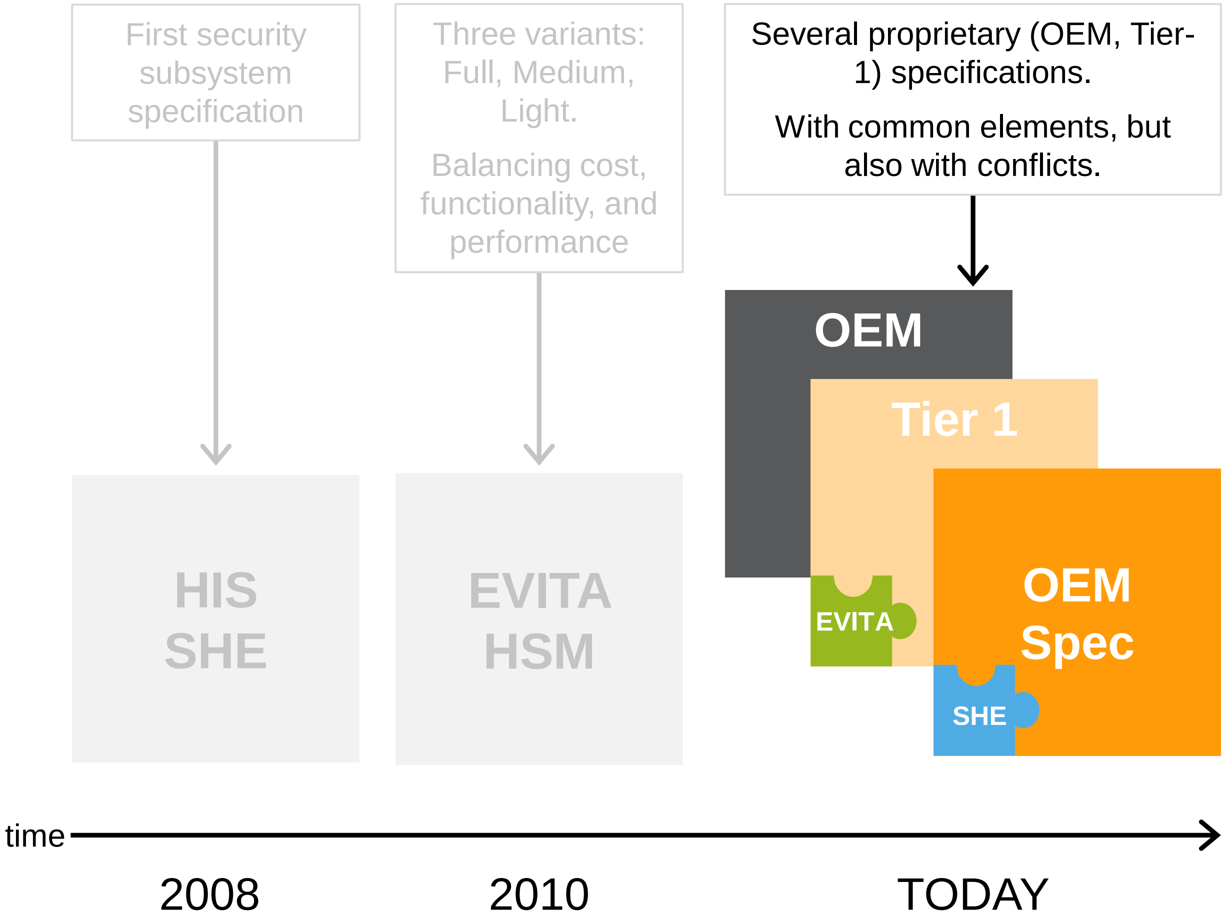
Balancing cost, functionality, and performance

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 selected aspects of SHE, EVITA, and FIPS 140-2


First security subsystem specification
Three variants: Full, Medium, Light.
Balancing cost, functionality, and performance
Several proprietary (OEM, Tier-1) specifications.
With common elements, but also with conflicts.
HIS
SHE
EVITA
HSM
OEM
Tier 1
EVITA
OEM
Spec
SHE
time
2008
2010
TODAY

JULY 2021 UPDATE – UN R155 AND ISO 21434

From July 2022 onward, vehicle manufacturers must comply with the R155 automotive cybersecurity regulation for new vehicle type launches in Europe, Japan and Korea.

The standard **ISO/SAE 21434** is deemed very supportive in implementing the requirements on the Cyber Security Management System (CSMS), as specified in UN R155, in organizations along the supply chain.

NXP therefore aims at supporting the OEMs, as well as its direct (Tier-1) customers, by ensuring organizational compliance with the standard and by ensuring that new (future) products are developed in compliance with the standard. Additionally, existing products will be supported by the associated processes of our CSMS (PSIRT etc.).

NO OTA WITHOUT SECURITY

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

  → Protect communications and authenticate new data

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

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

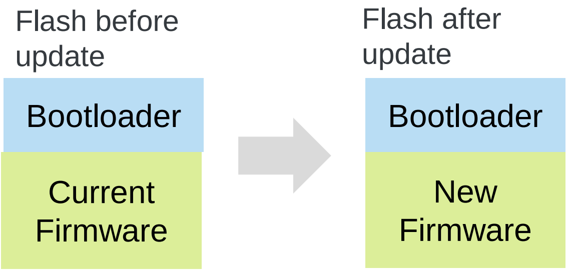
In general, there are 2 methods for performing updates to an end node

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



Flash before update

Bootloader

Current Firmware

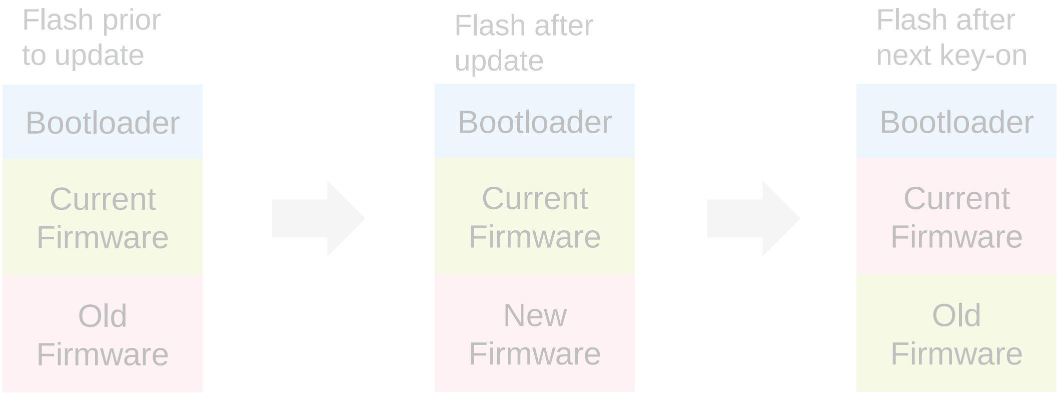
Flash after update

Bootloader

New Firmware

A/B

2 versions of firmware exist in internal flash.



Flash prior to update

Bootloader

Current Firmware

Old Firmware

Flash after update

Bootloader

Current Firmware

New Firmware

Flash after next key-on

Bootloader

Current Firmware

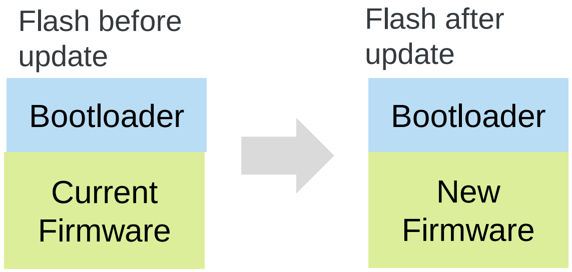
Old Firmware

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



Flash before update

Bootloader

Current Firmware

Flash after update

Bootloader

New Firmware

Advantages

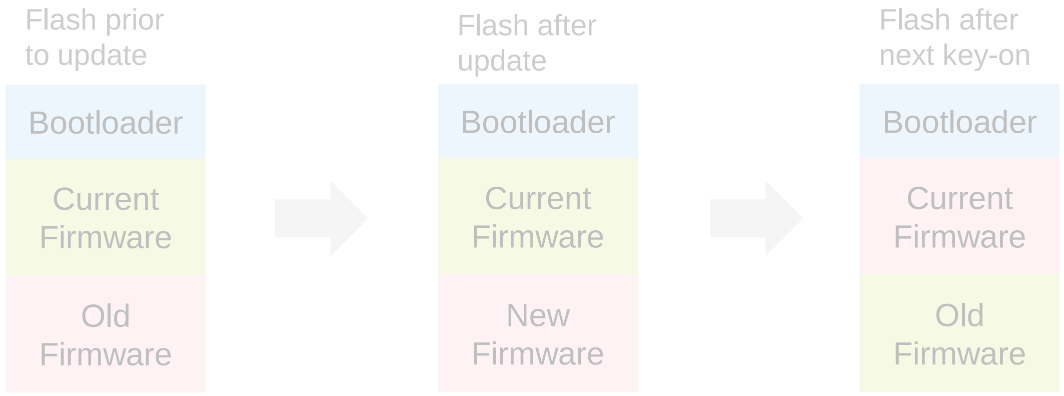
- No need for additional flash

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.



Flash prior to update

Bootloader

Current Firmware

Old Firmware

Flash after update

Bootloader

Current Firmware

New Firmware

Flash after next key-on

Bootloader

Current Firmware

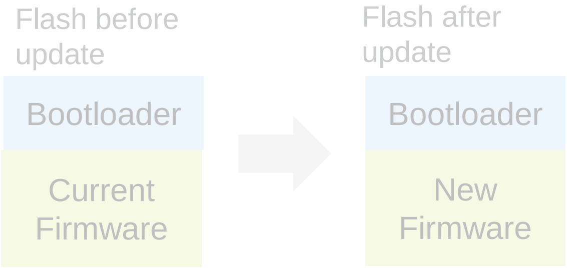
Old Firmware

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



Flash before update

Bootloader

Current Firmware

Flash after update

Bootloader

New Firmware

Advantages

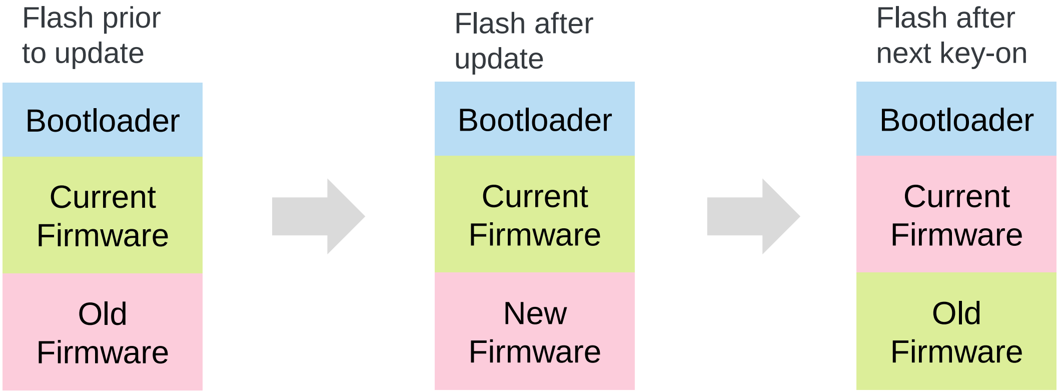
- No need for additional flash

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.



Flash prior to update

Bootloader

Current Firmware

Old Firmware

Flash after update

Bootloader

Current Firmware

New Firmware

Flash after next key-on

Bootloader

Current Firmware

Old Firmware

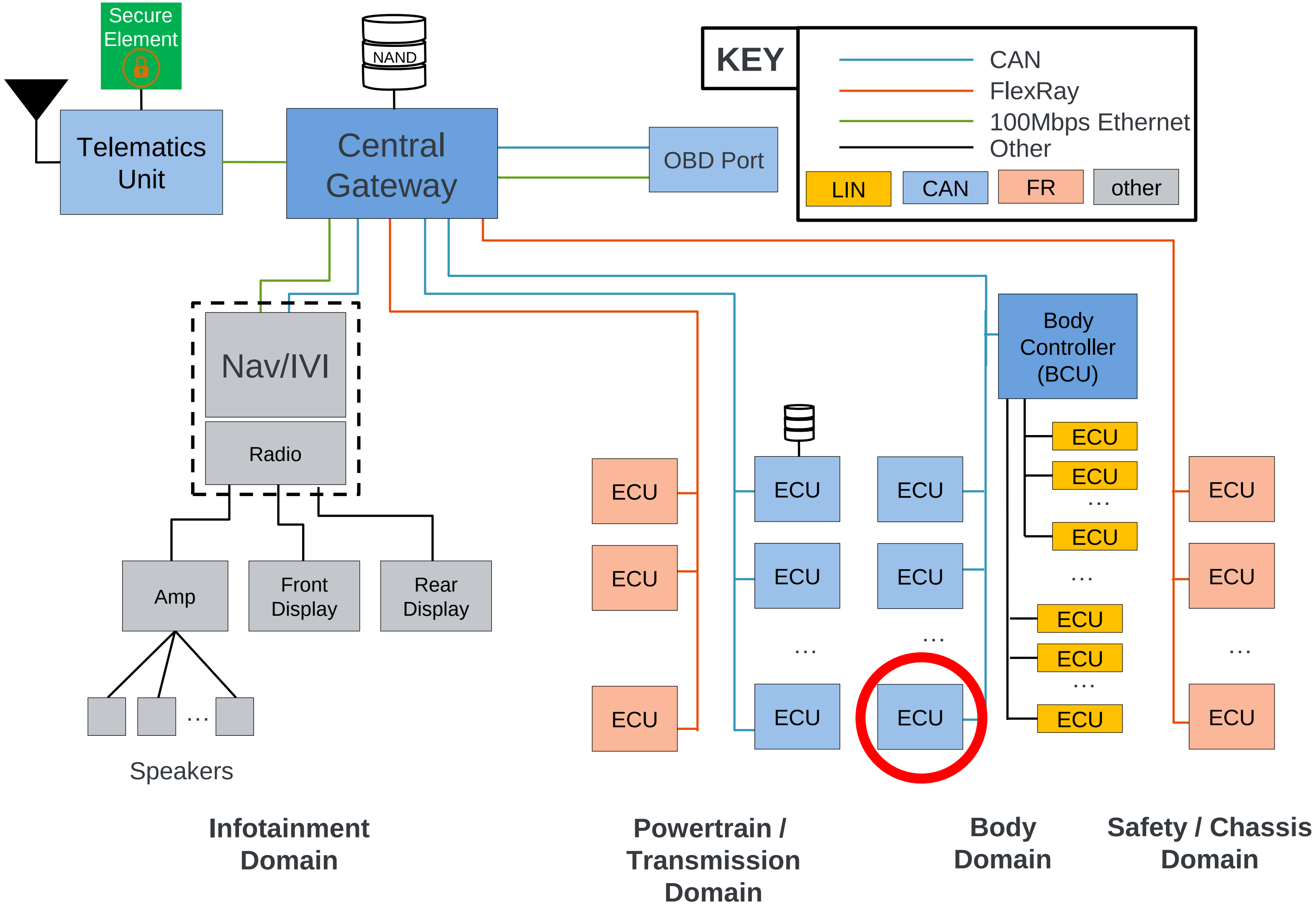
Advantages

- 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

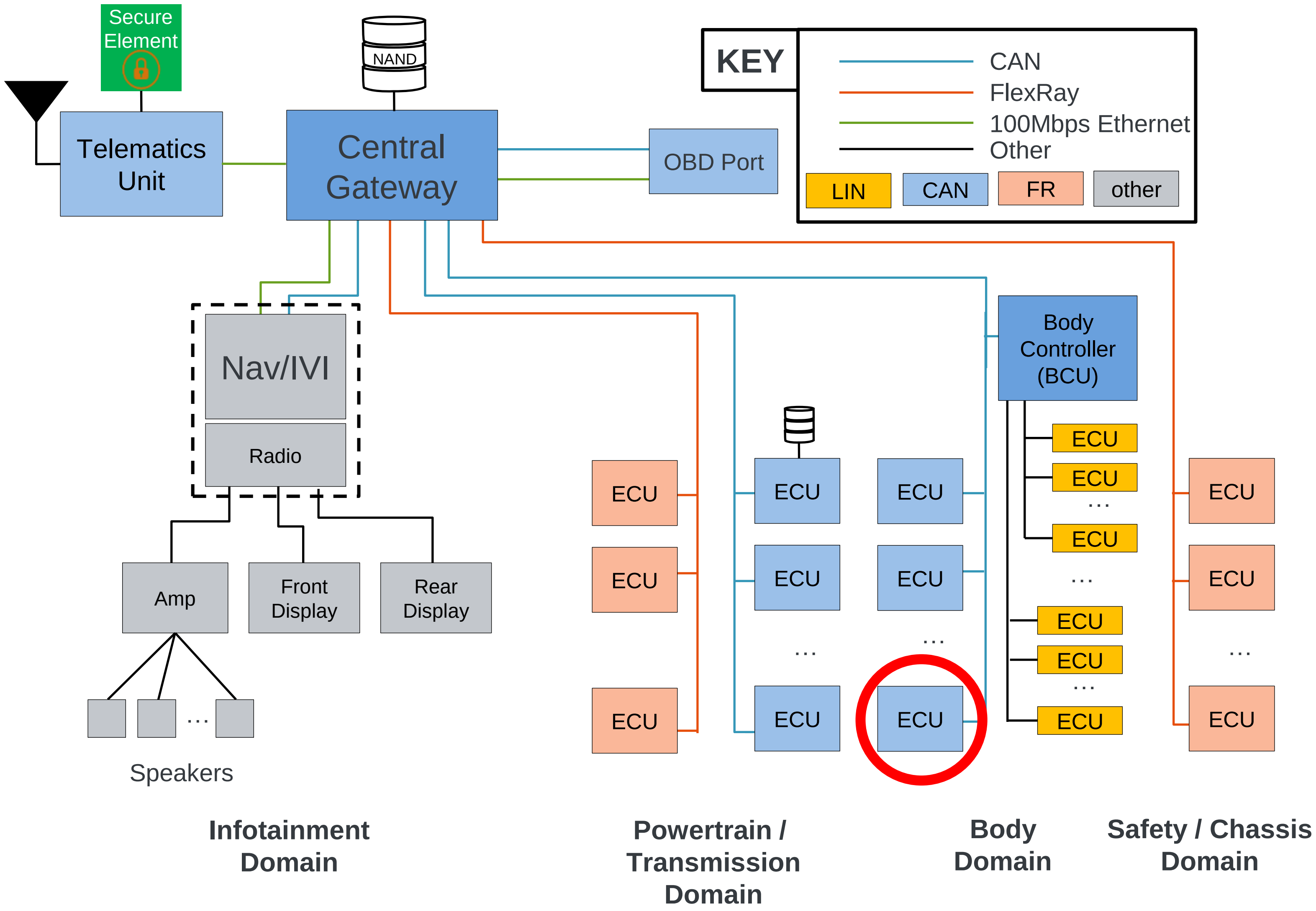
Security: Supports CMAC authentication and AES-128 decryption

Connection to Gateway: Ethernet

Vehicle Downtime: **none**

Security: **high**

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**

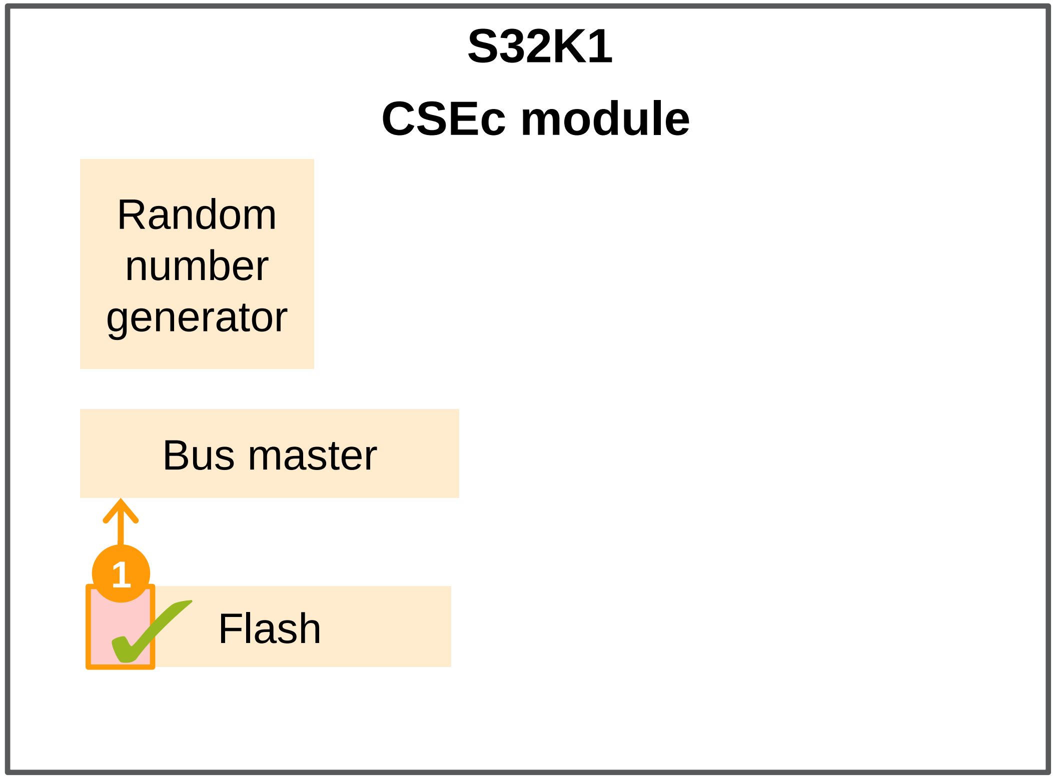
Security: **high**

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

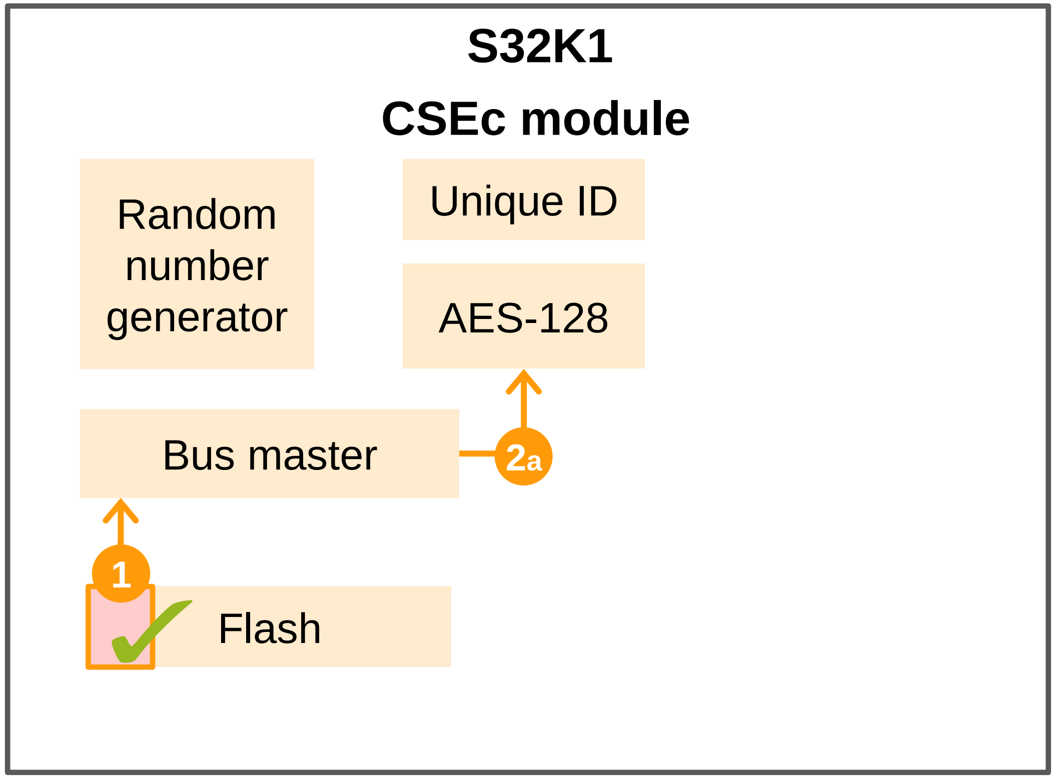
Step 1: After power on: CSE module reads bootloader via its bus master interface.



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.

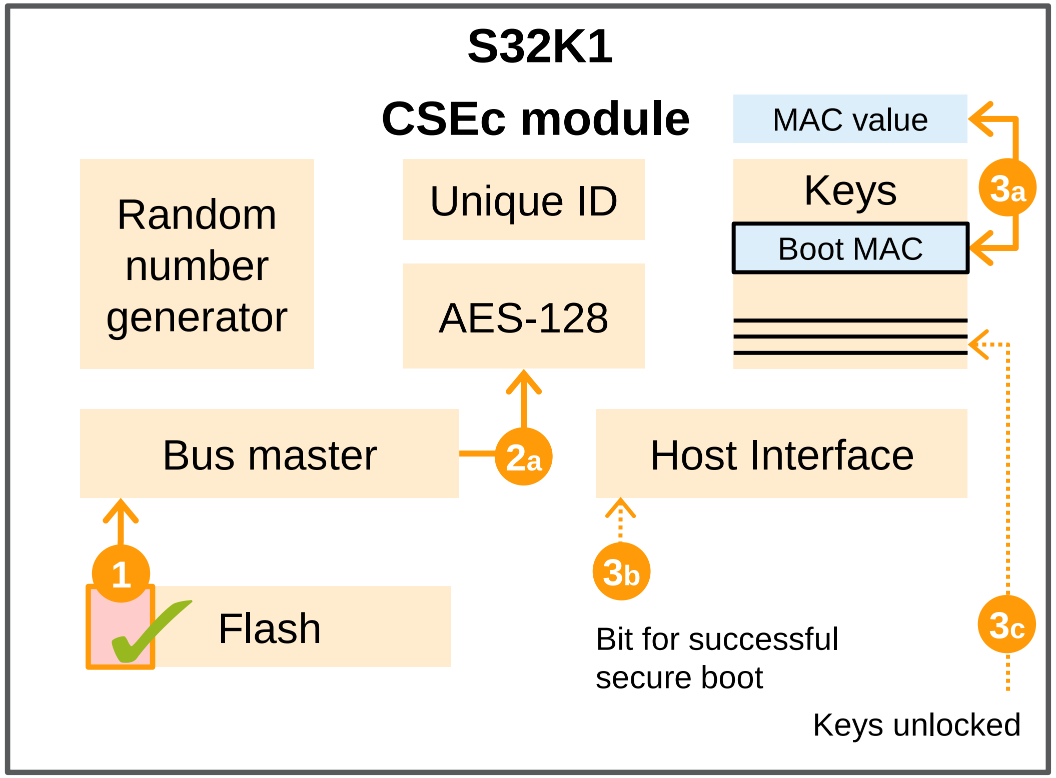


SECURE BOOT - CHECK BOOT LOADER FOR INTEGRITY AND AUTHENTICITY ON S32K1

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



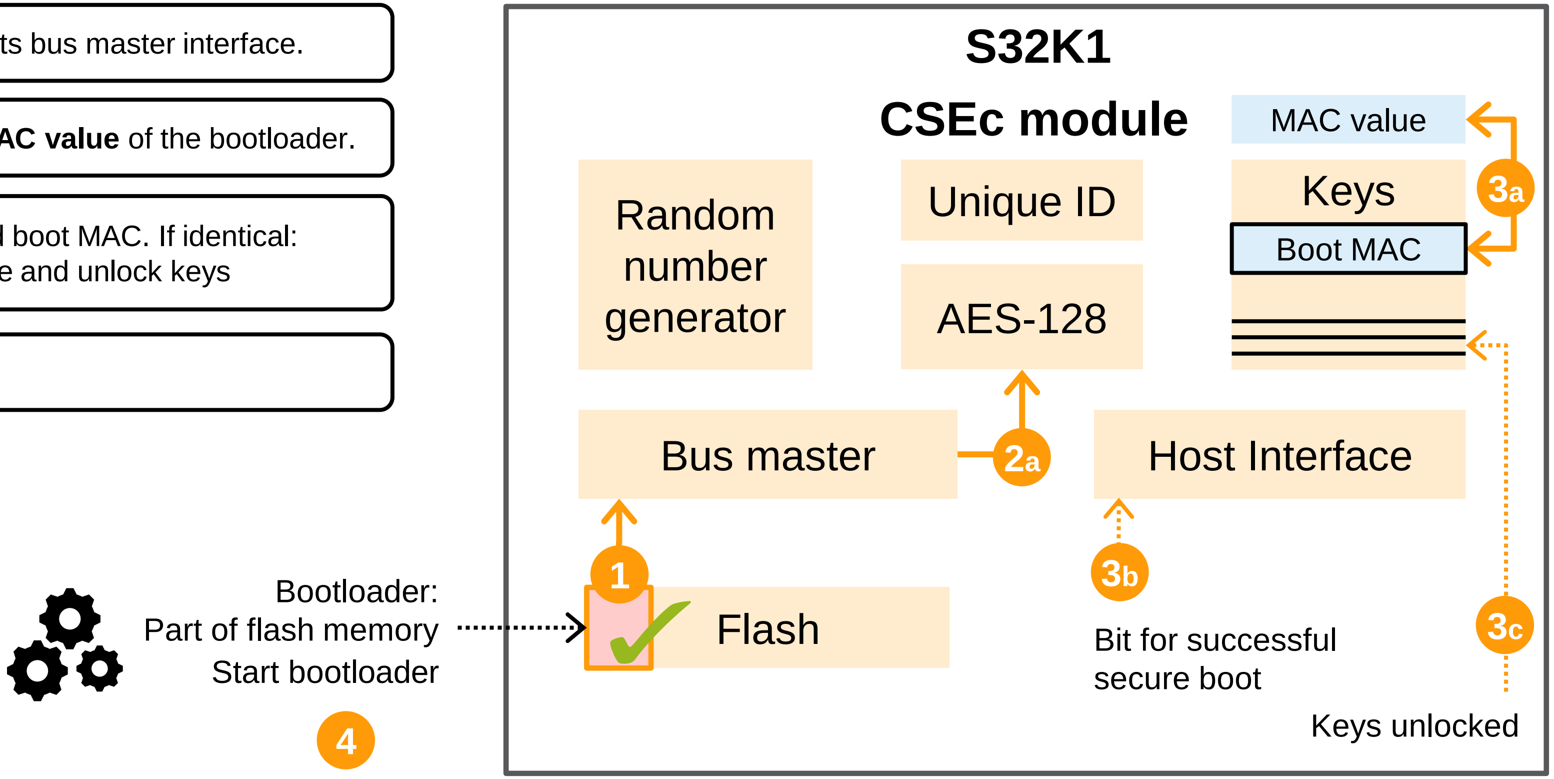
SECURE BOOT - CHECK BOOT LOADER FOR INTEGRITY AND AUTHENTICITY ON S32K1

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.



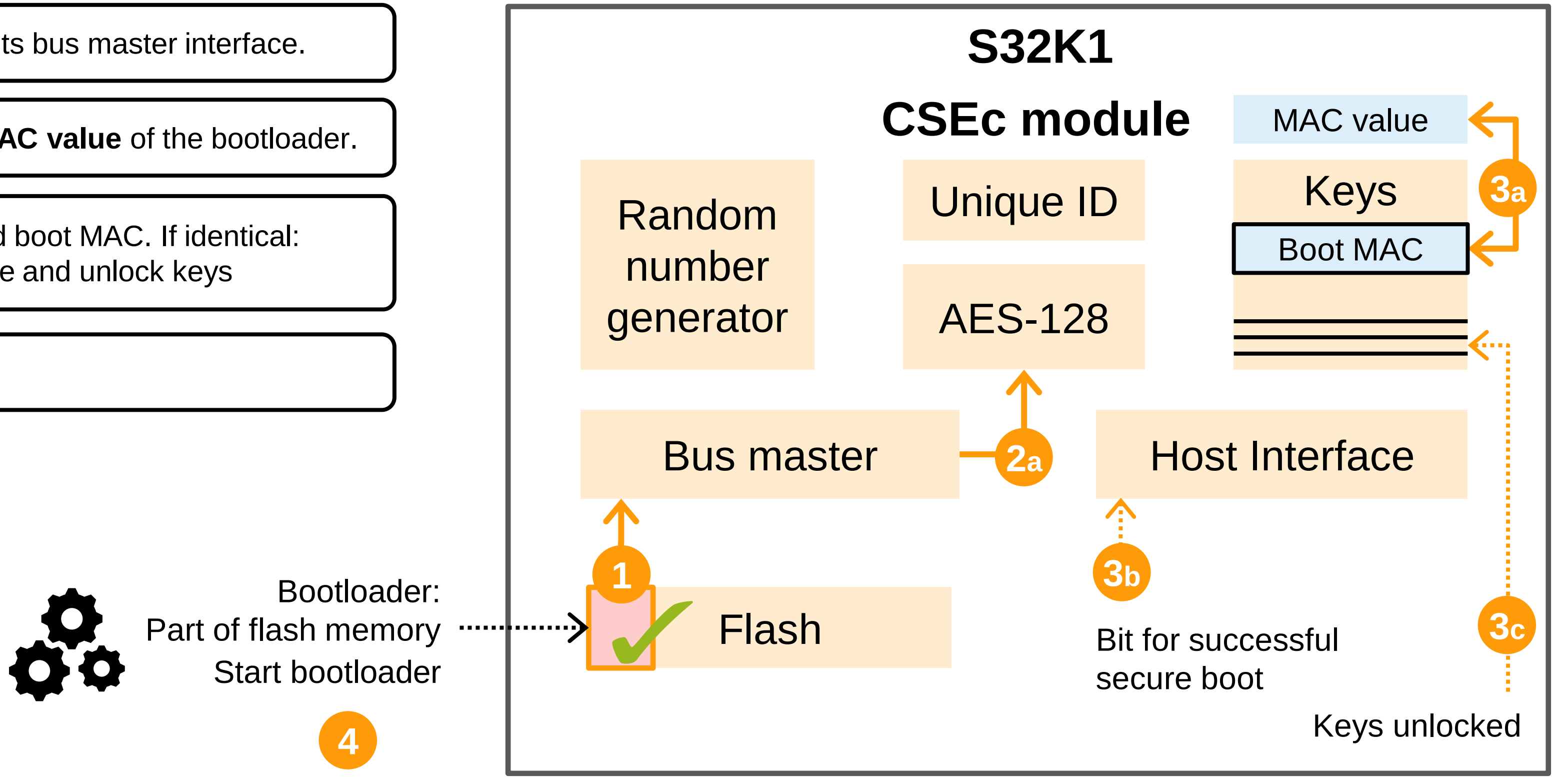
SECURE BOOT - CHECK BOOT LOADER FOR INTEGRITY AND AUTHENTICITY ON S32K1

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.

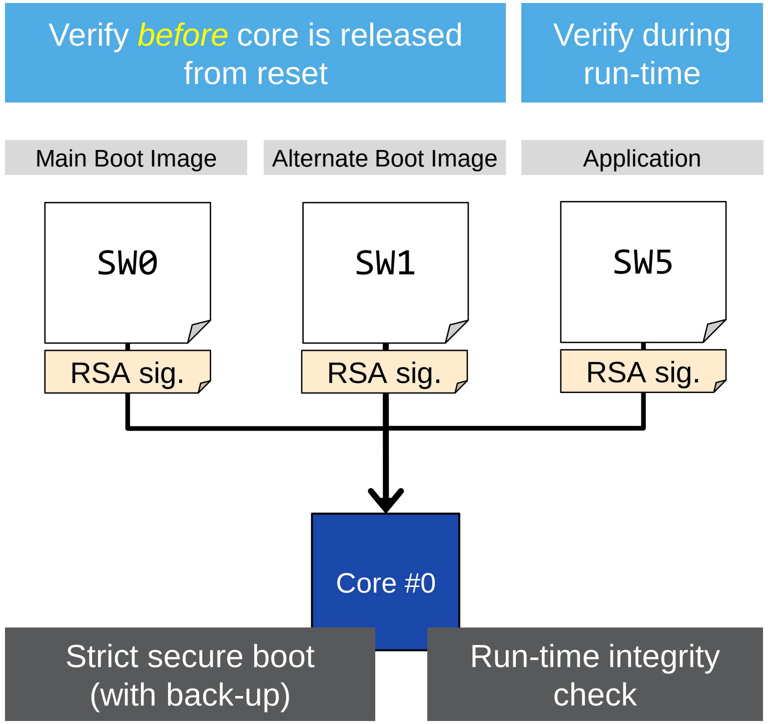
Step 3: CSE module compares calculated MAC with stored boot MAC. If identical: successful secure boot → set respective bit in host interface and unlock keys

Step 4: MCU always starts bootloader.

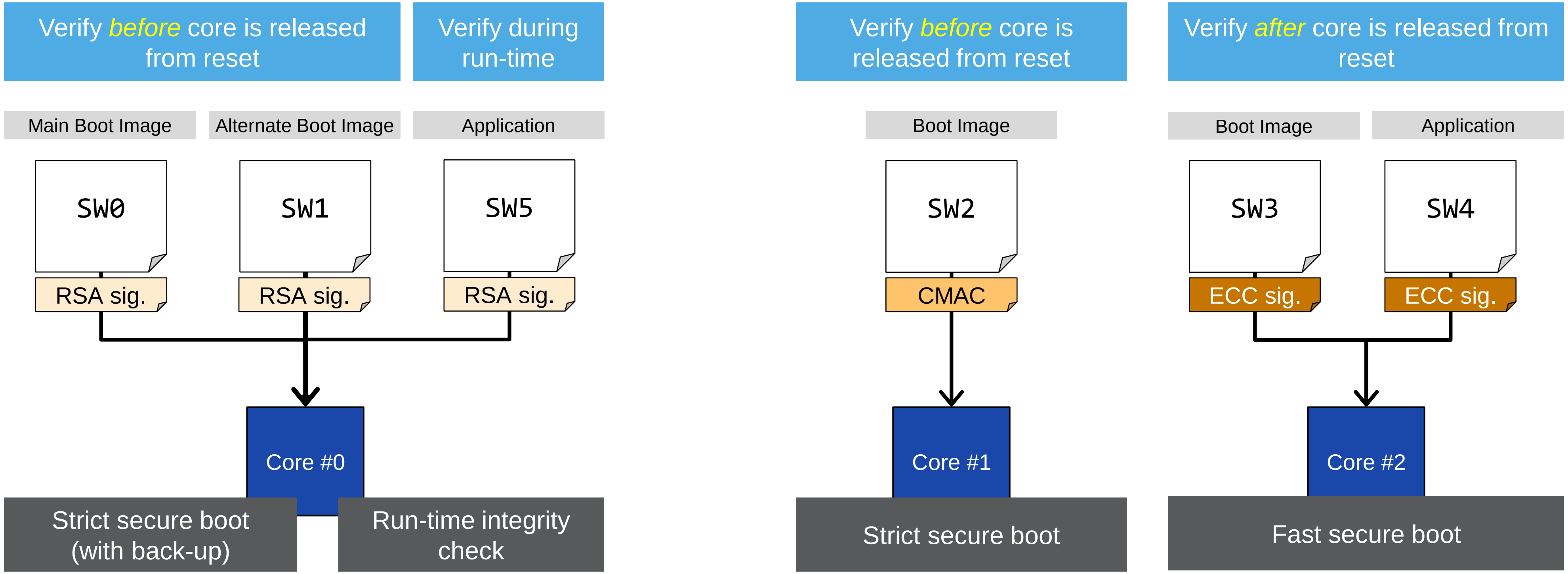


- **MAC** protects against modification of bootloader and depends on the (secret) boot key → integrity and authenticity of bootloader.
- Only if calculated MAC value matches stored boot MAC value: successful secure boot → set respective bit in host interface and unlock keys for further usage (see next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

SECURE BOOT CONFIGURATION EXAMPLE WITH S32K3



SECURE BOOT CONFIGURATION EXAMPLE WITH S32K3



Verify *before* core is released from reset

Verify during run-time

Main Boot Image

Alternate Boot Image

Application

SW0

SW1

SW5

RSA sig.

RSA sig.

RSA sig.

Core #0

Strict secure boot (with back-up)

Run-time integrity check

Verify *before* core is released from reset

Boot Image

SW2

CMAC

Core #1

Strict secure boot

Verify *after* core is released from reset

Boot Image

Application

SW3

SW4

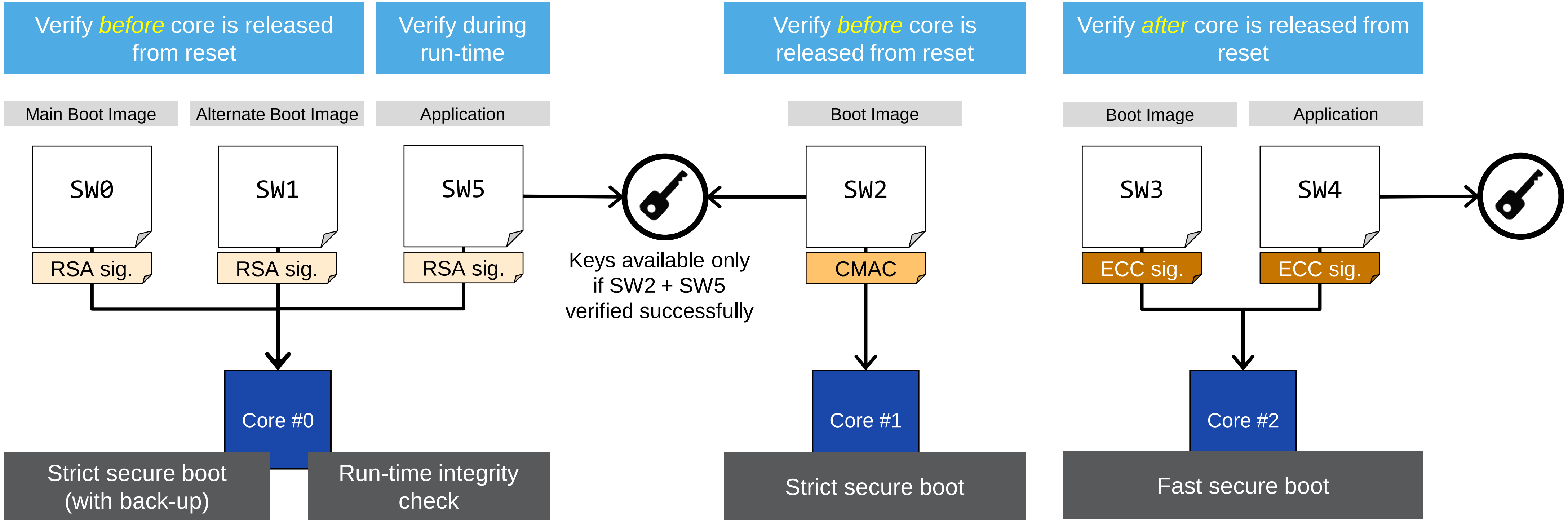
ECC sig.

ECC sig.

Core #2

Fast secure boot

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.

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

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, 64bit) 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

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

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**

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**

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

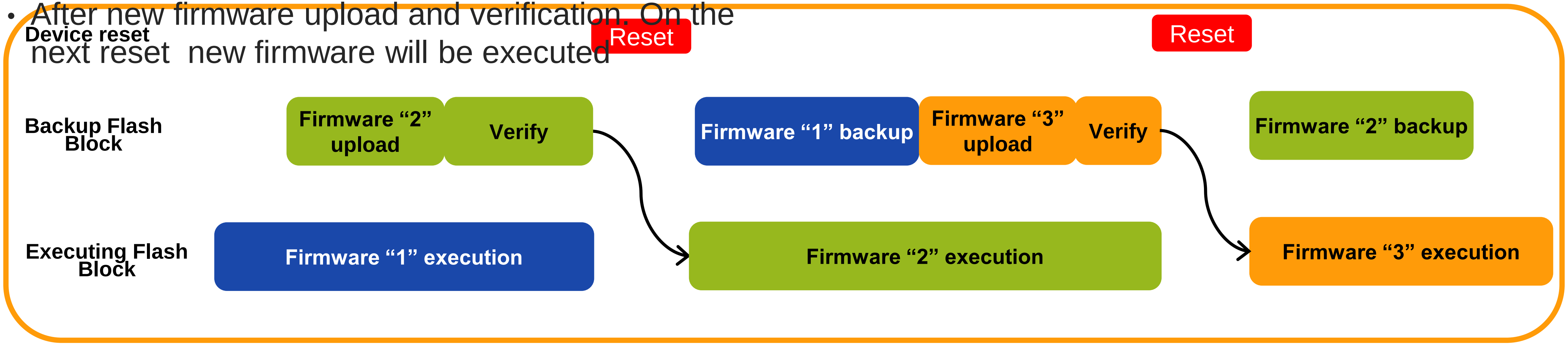
- Encryption/ decryption of data
- Firmware authentication check

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

S32K3xx Firmware Update



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

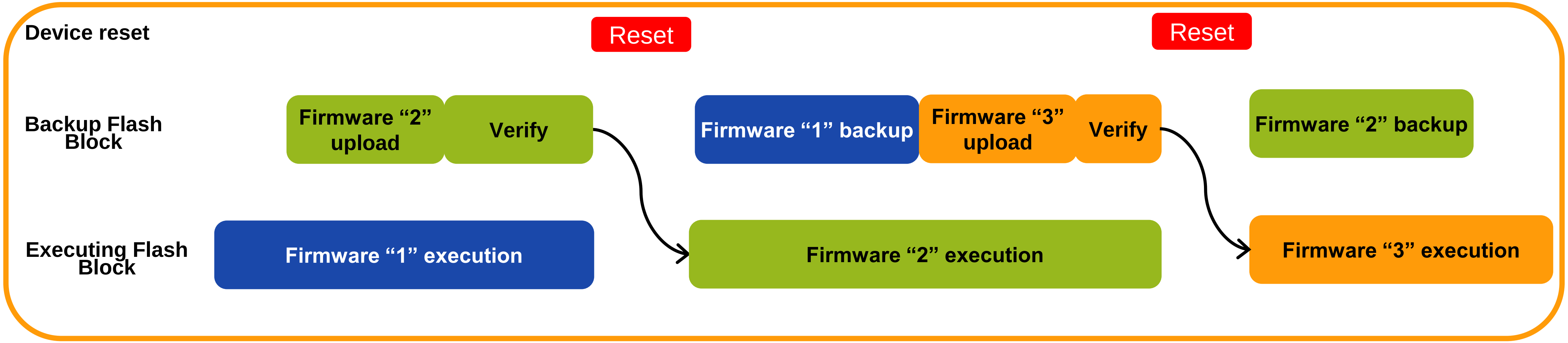
Use case: A/B swap in internal flash

- 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)

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

SECURITY LEADERSHIP – PROVEN EXTENSIVE SECURITY EXPERIENCE

Proven Extensive Security Experience

Proven Extensive Security Experience

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

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
  - **ISO 21434**: NXP cybersecurity engineering processes are now certified as compliant with the new automotive cybersecurity standard ISO/SAE 21434. (Certified by TÜV SÜD)

Root of Trust & Trusted Process

SECURITY LEADERSHIP – ROOT OF TRUST & TRUSTED PROCESS

Root of Trust & Trusted Process

- Secure Trust Provisioning in non-secure production environment

SECURITY LEADERSHIP – ROOT OF TRUST & TRUSTED PROCESS

Root of Trust & Trusted Process

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

SECURITY LEADERSHIP – PRODUCT SECURITY INCIDENT RESPONSE TEAM

Product Security Incident Response Team

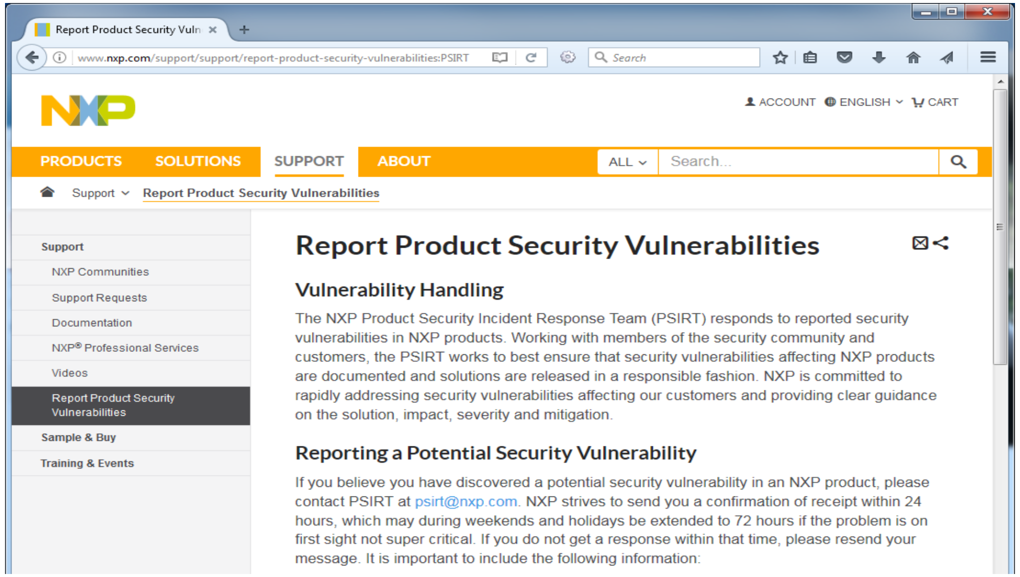
Product Security Incident Response Team

- Established in 2008

SECURITY LEADERSHIP – PRODUCT SECURITY INCIDENT RESPONSE TEAM

Product Security Incident Response Team

- Established in 2008
- Confirmation of receipt within 24 hours


Report Product Security Vuln
www.nxp.com/support/support/report-product-security-vulnerabilities:PSIRT
Search
ACCOUNT
ENGLISH
CART
PRODUCTS
SOLUTIONS
SUPPORT
ABOUT
ALL
Search...
Support
Report Product Security Vulnerabilities
Support
NXP Communities
Support Requests
Documentation
NXP® Professional Services
Videos
Report Product Security Vulnerabilities
Sample & Buy
Training & Events

Report Product Security Vulnerabilities

Vulnerability Handling

The NXP Product Security Incident Response Team (PSIRT) responds to reported security vulnerabilities in NXP products. Working with members of the security community and customers, the PSIRT works to best ensure that security vulnerabilities affecting NXP products are documented and solutions are released in a responsible fashion. NXP is committed to rapidly addressing security vulnerabilities affecting our customers and providing clear guidance on the solution, impact, severity and mitigation.

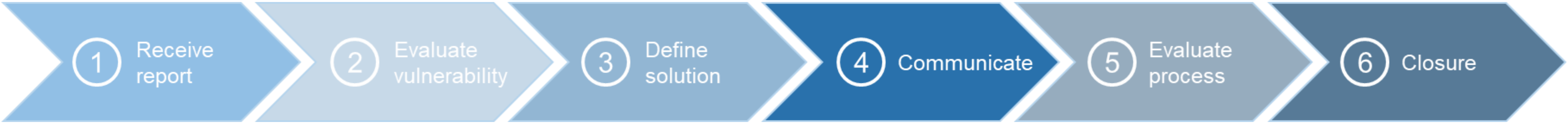
Reporting a Potential Security Vulnerability

If you believe you have discovered a potential security vulnerability in an NXP product, please contact PSIRT at psirt@nxp.com. NXP strives to send you a confirmation of receipt within 24 hours, which may during weekends and holidays be extended to 72 hours if the problem is on first sight not super critical. If you do not get a response within that time, please resend your message. It is important to include the following information:

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

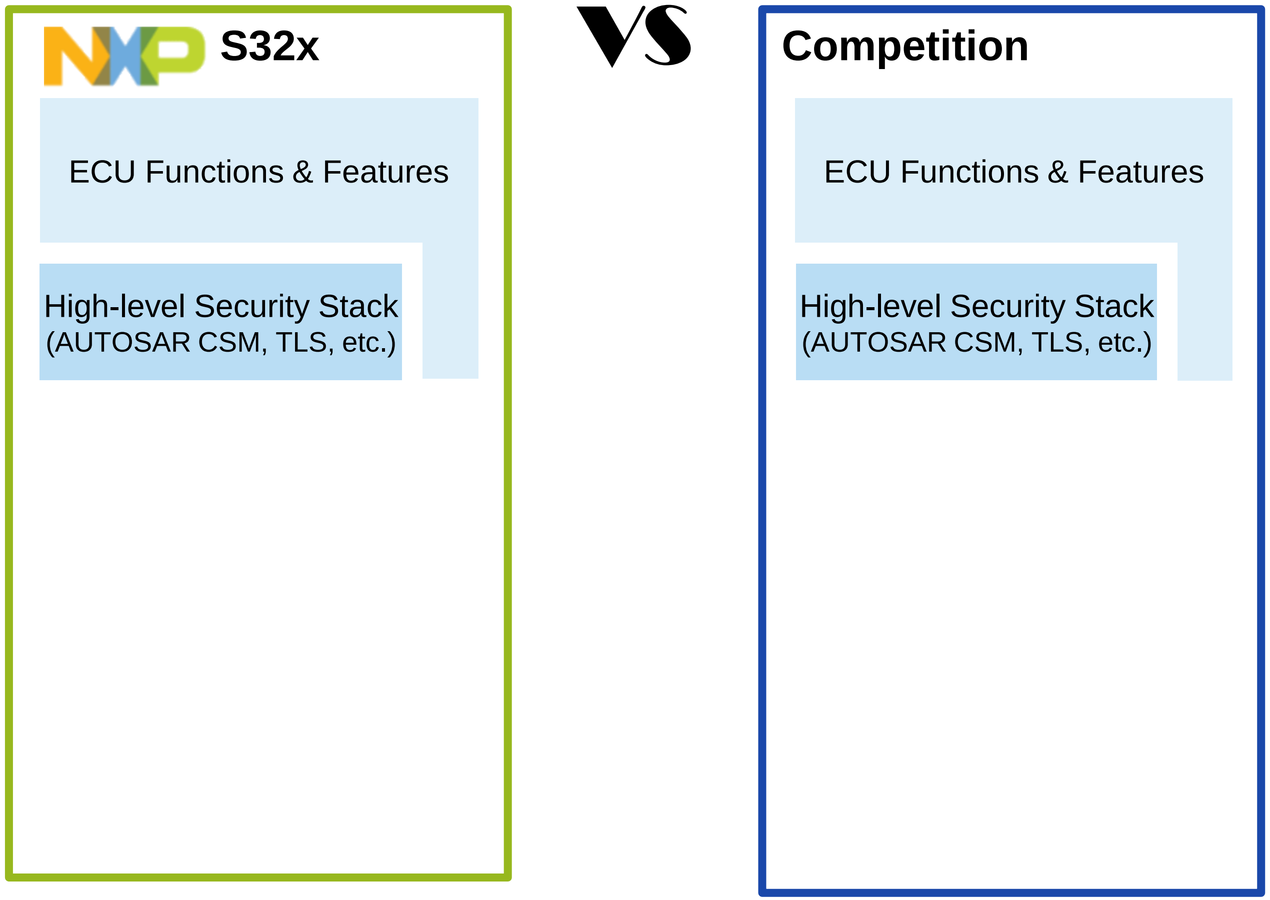
S32K3 SECURITY OFFER IS SIMPLER

Comprehensive service offer

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

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

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


NXP S32x
ECU Functions & Features
High-level Security Stack (AUTOSAR CSM, TLS, etc.)
VS
Competition
ECU Functions & Features
High-level Security Stack (AUTOSAR CSM, TLS, etc.)

S32K3 SECURITY OFFER IS SIMPLER

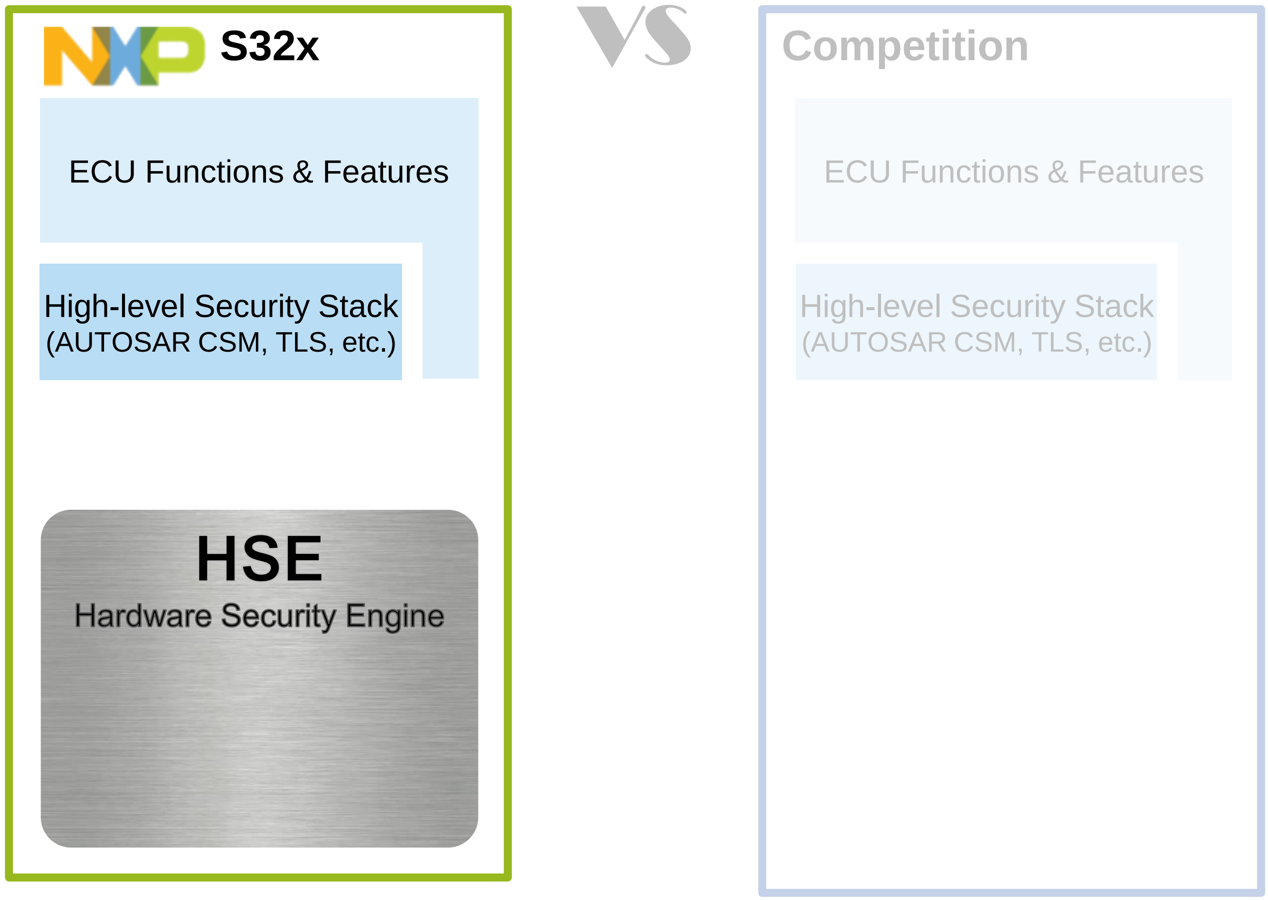
Comprehensive service offer

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

AUTOSAR

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

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



S32x

ECU Functions & Features

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

HSE
Hardware Security Engine

VS

Competition

ECU Functions & Features

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

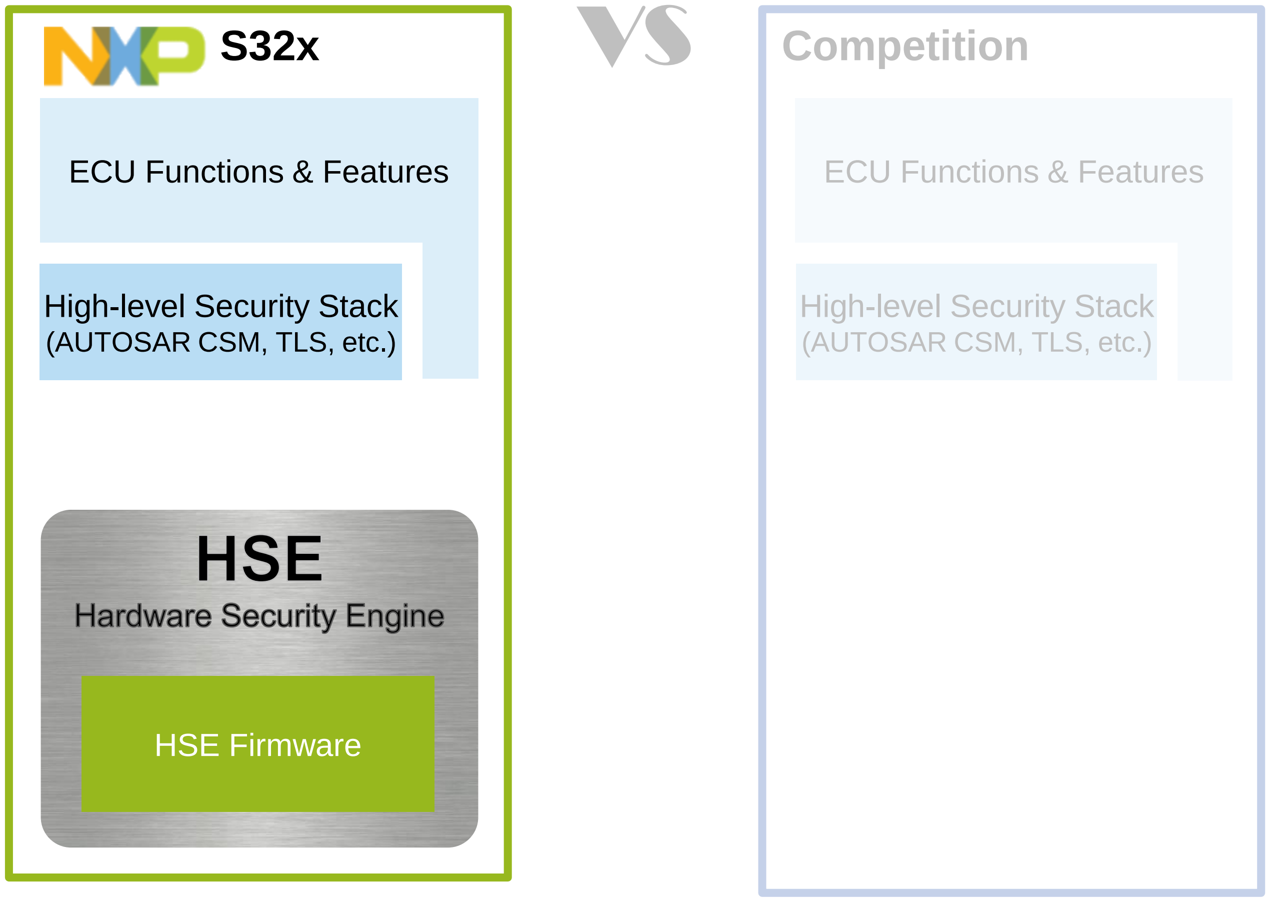
S32K3 SECURITY OFFER IS SIMPLER

Comprehensive service offer

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

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

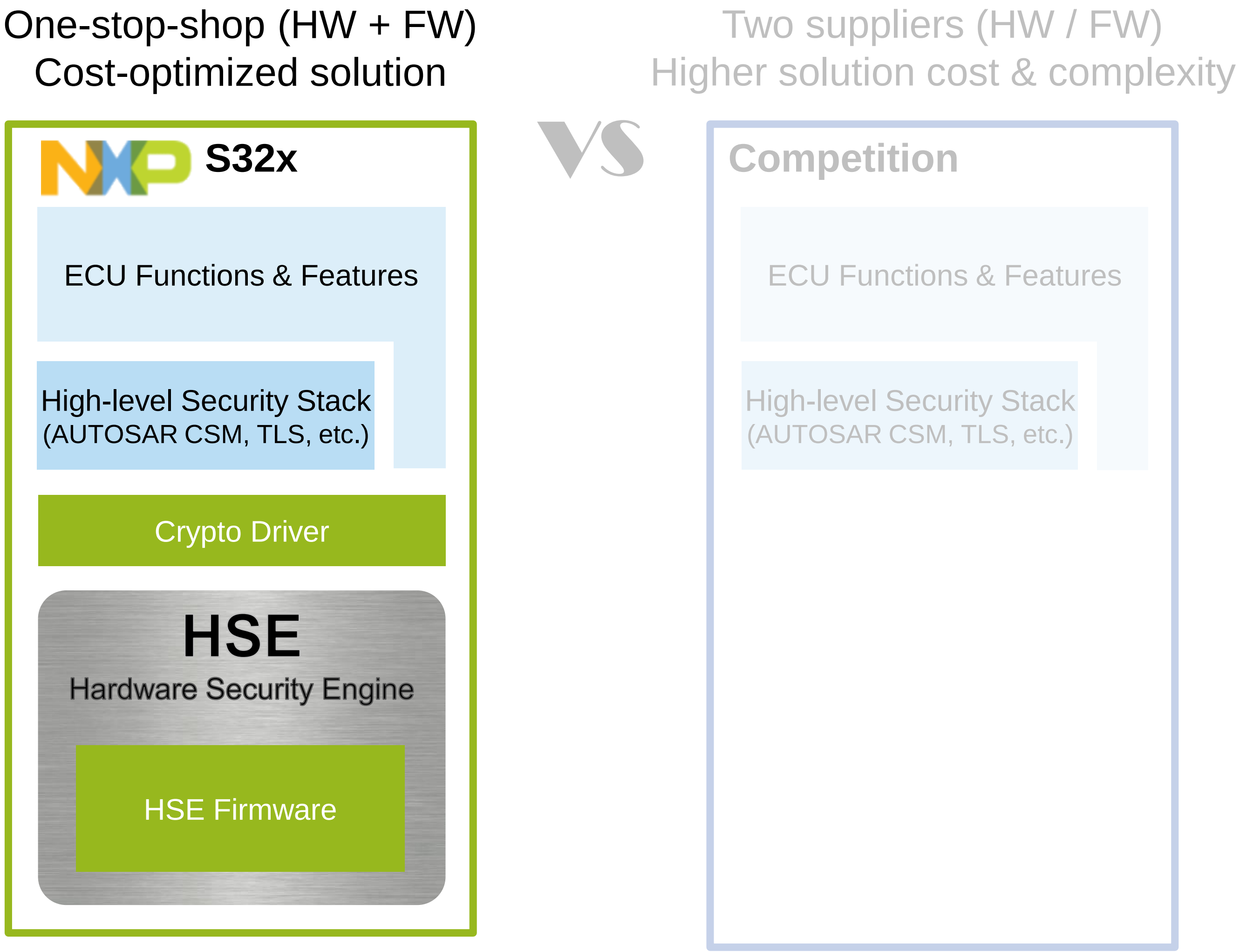
Two suppliers (HW / FW)
Higher solution cost & complexity



S32K3 SECURITY OFFER IS SIMPLER

Comprehensive service offer

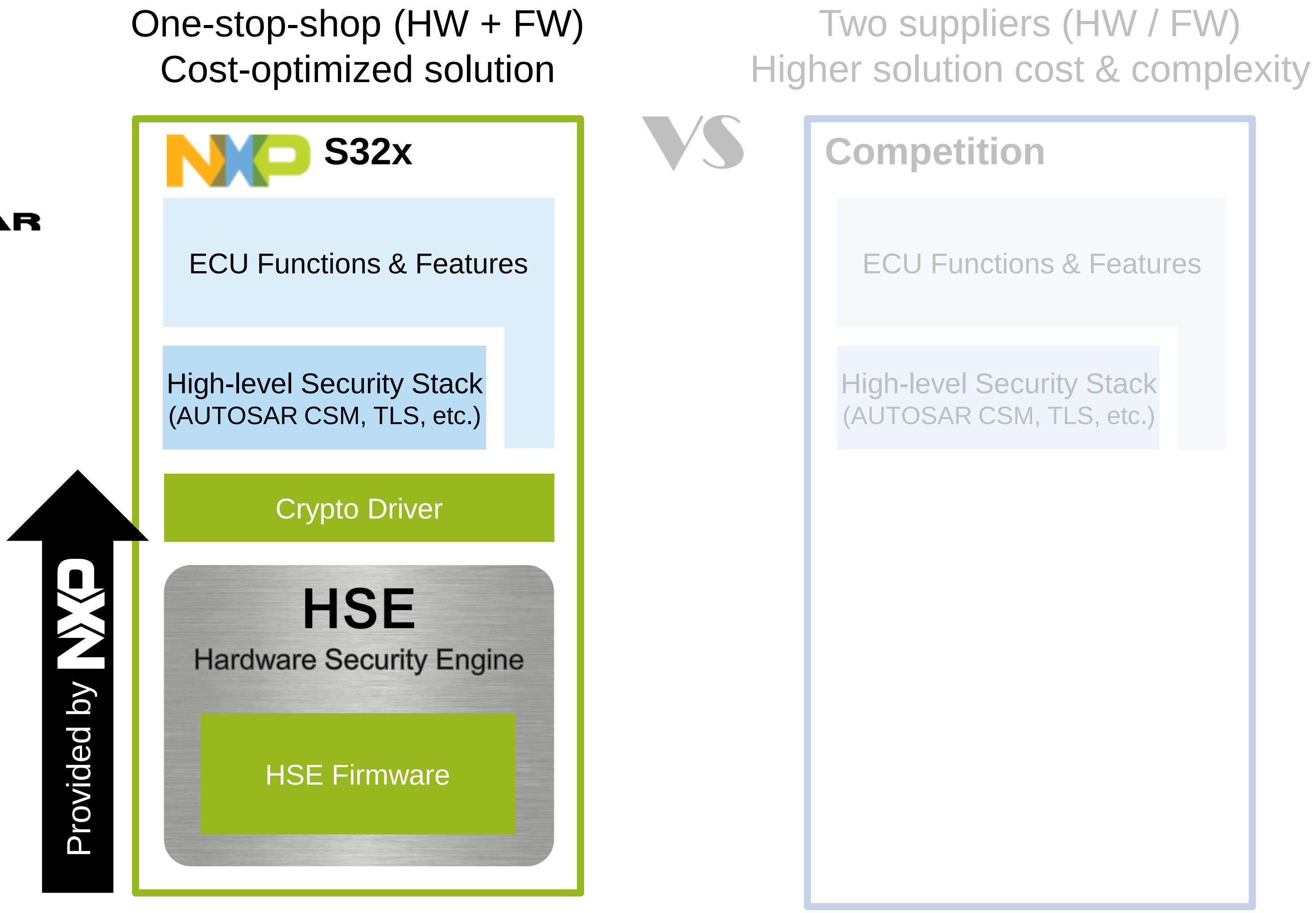
- FAE support
- FQE analysis
- PSIRT
- Standard crypto-driver: MCAL AUTOSAR



S32K3 SECURITY OFFER IS SIMPLER

Comprehensive service offer

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



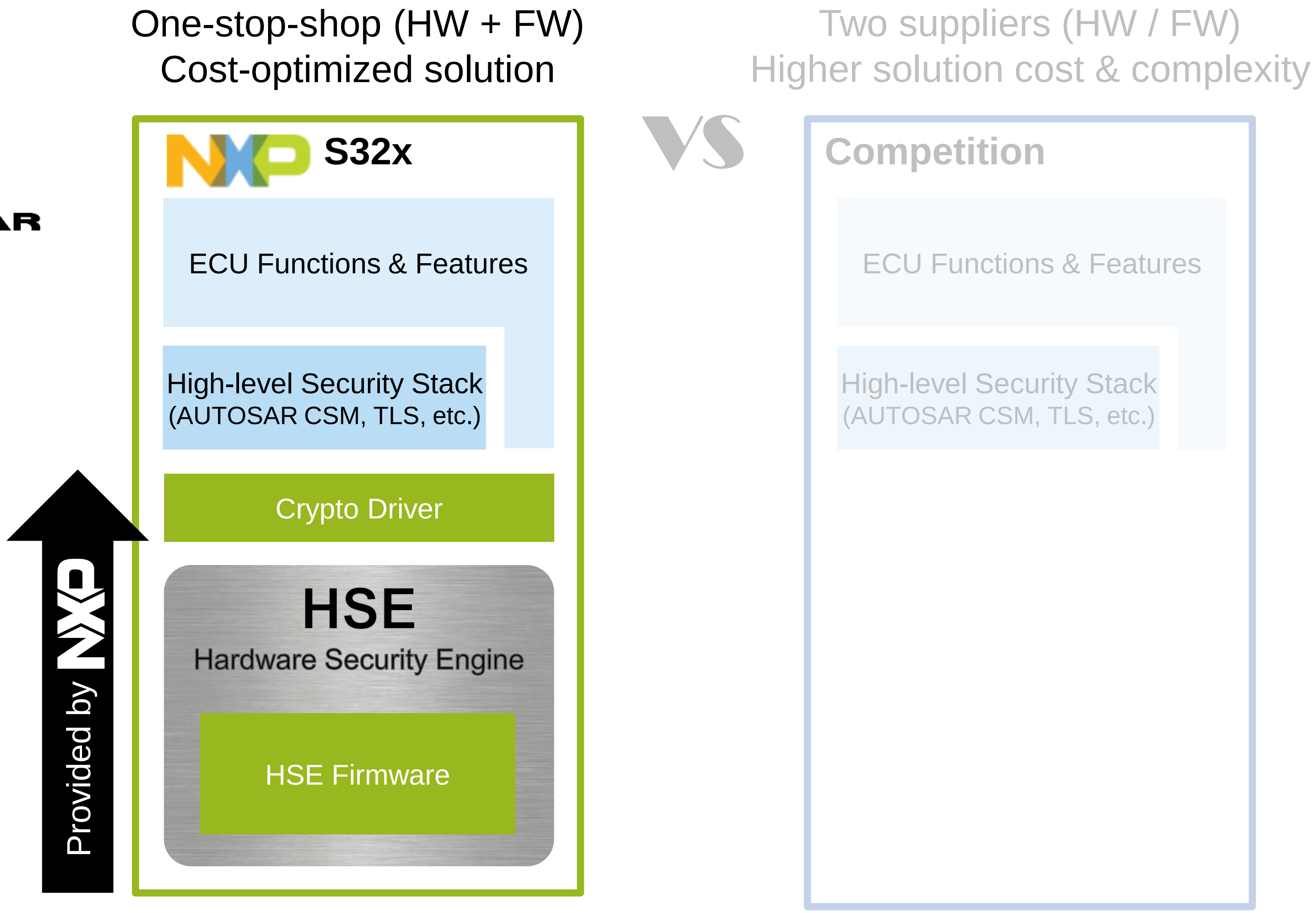
S32K3 SECURITY OFFER IS SIMPLER

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



S32K3 SECURITY OFFER IS SIMPLER

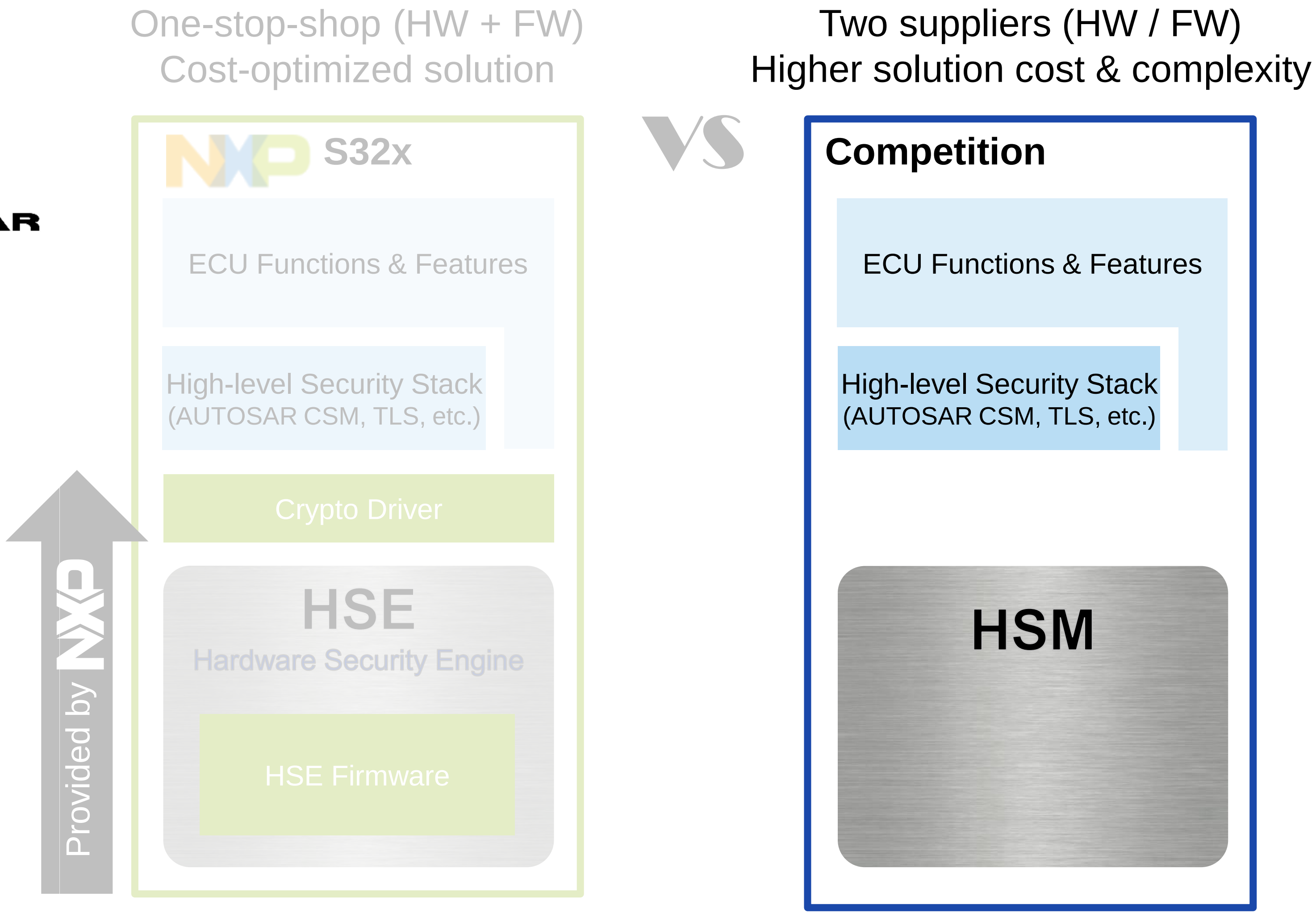
Comprehensive service offer

- 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

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

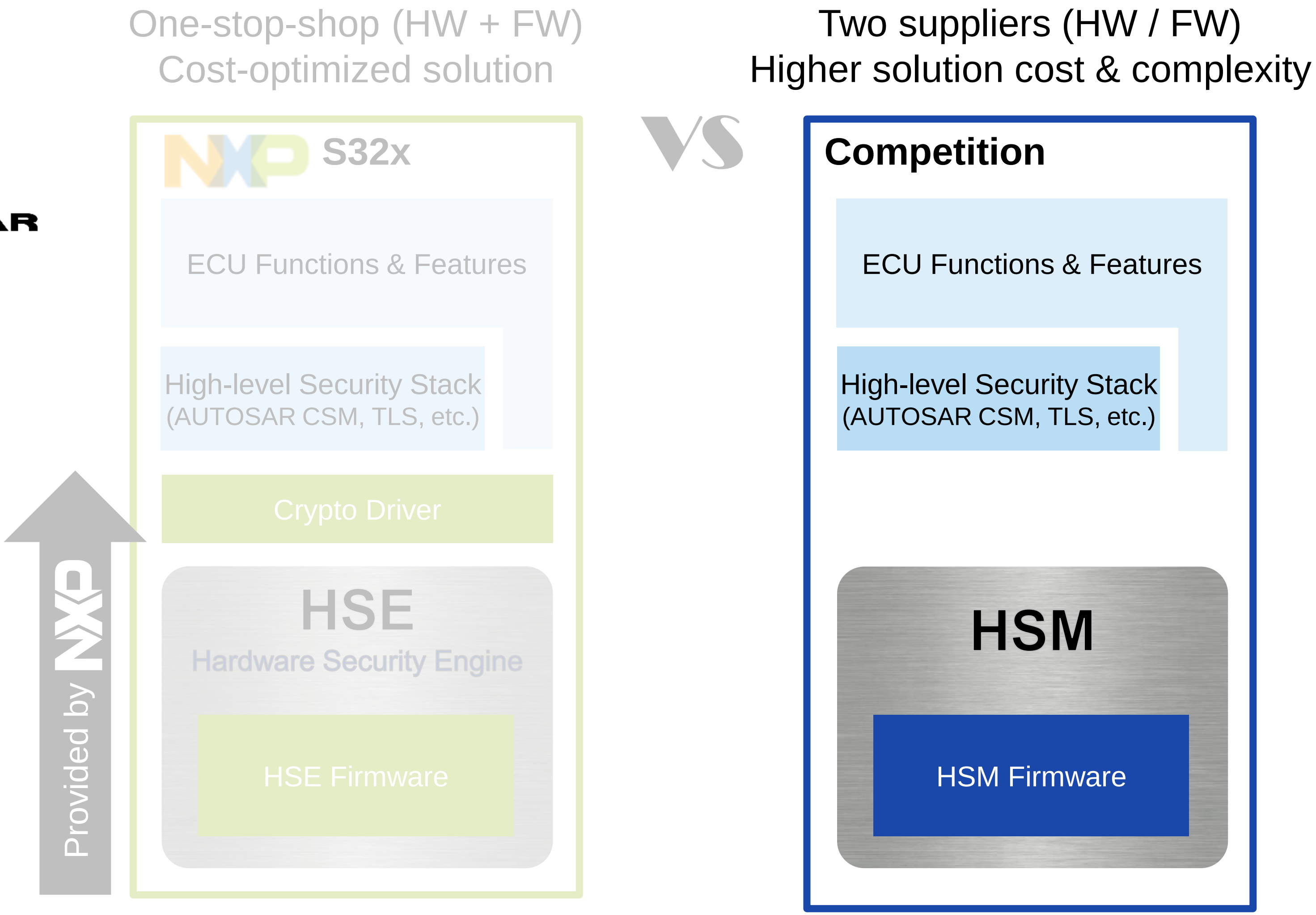
S32K3 SECURITY OFFER IS SIMPLER

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



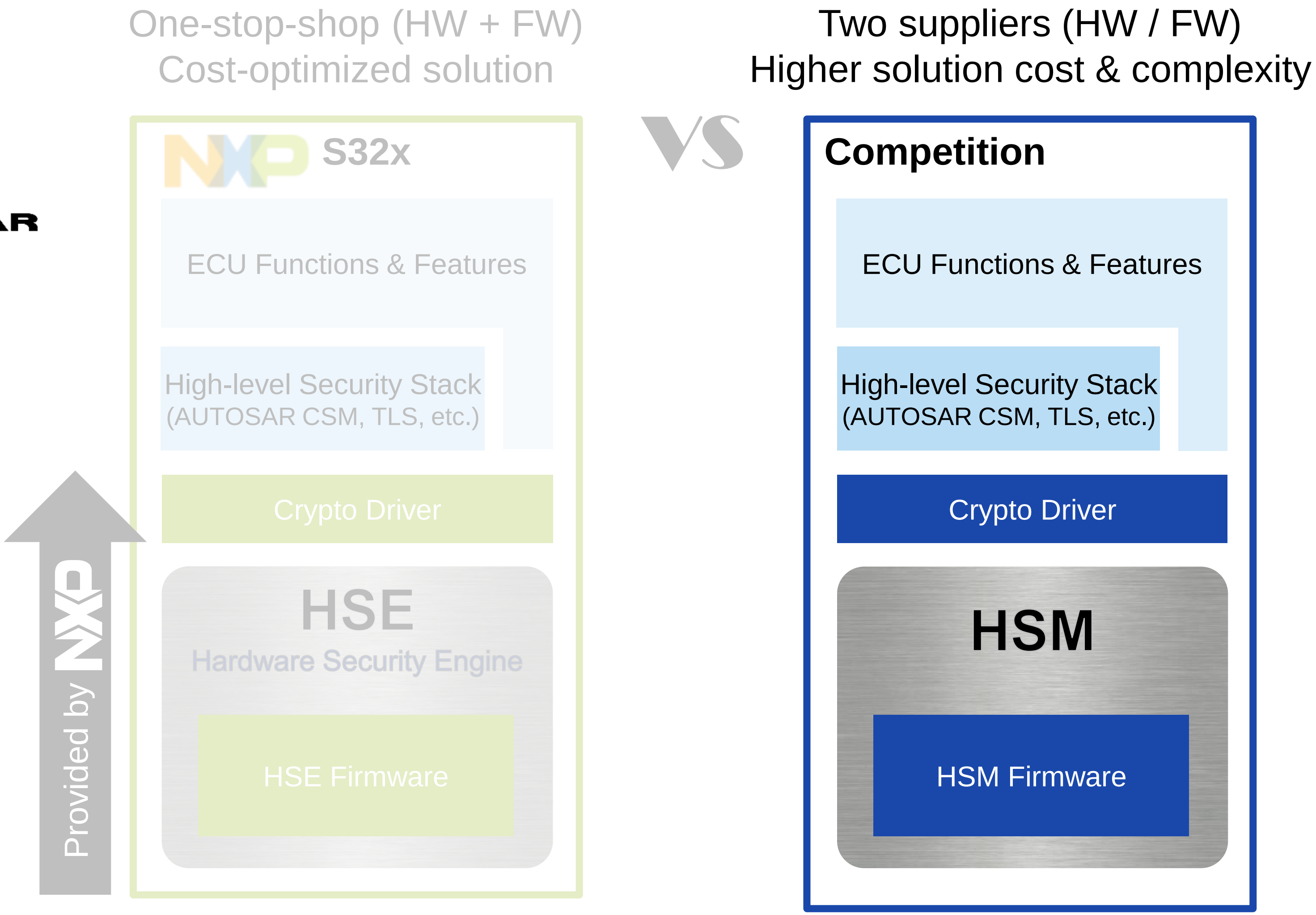
S32K3 SECURITY OFFER IS SIMPLER

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



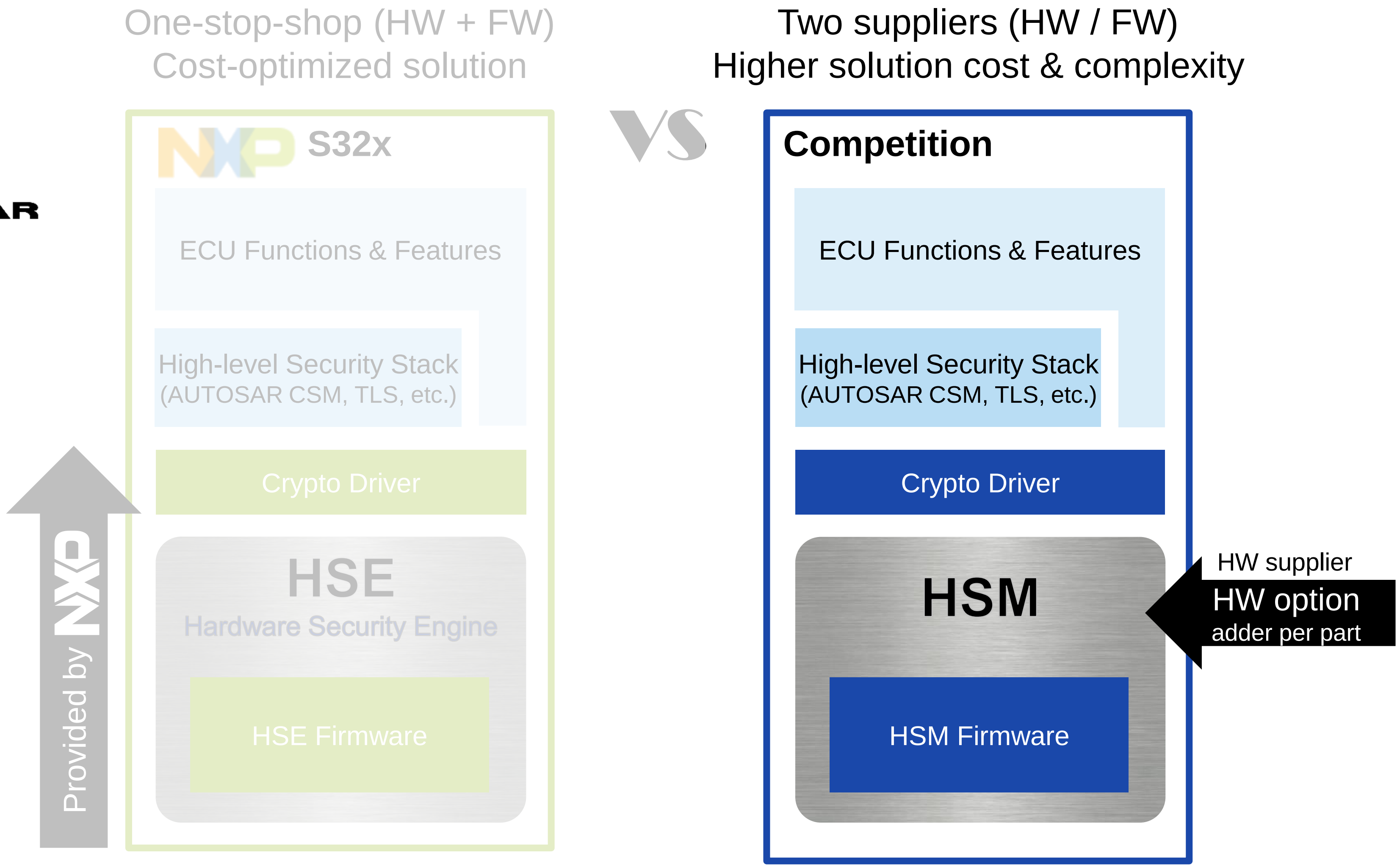
S32K3 SECURITY OFFER IS SIMPLER

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



S32K3 SECURITY OFFER IS SIMPLER

Comprehensive service offer

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

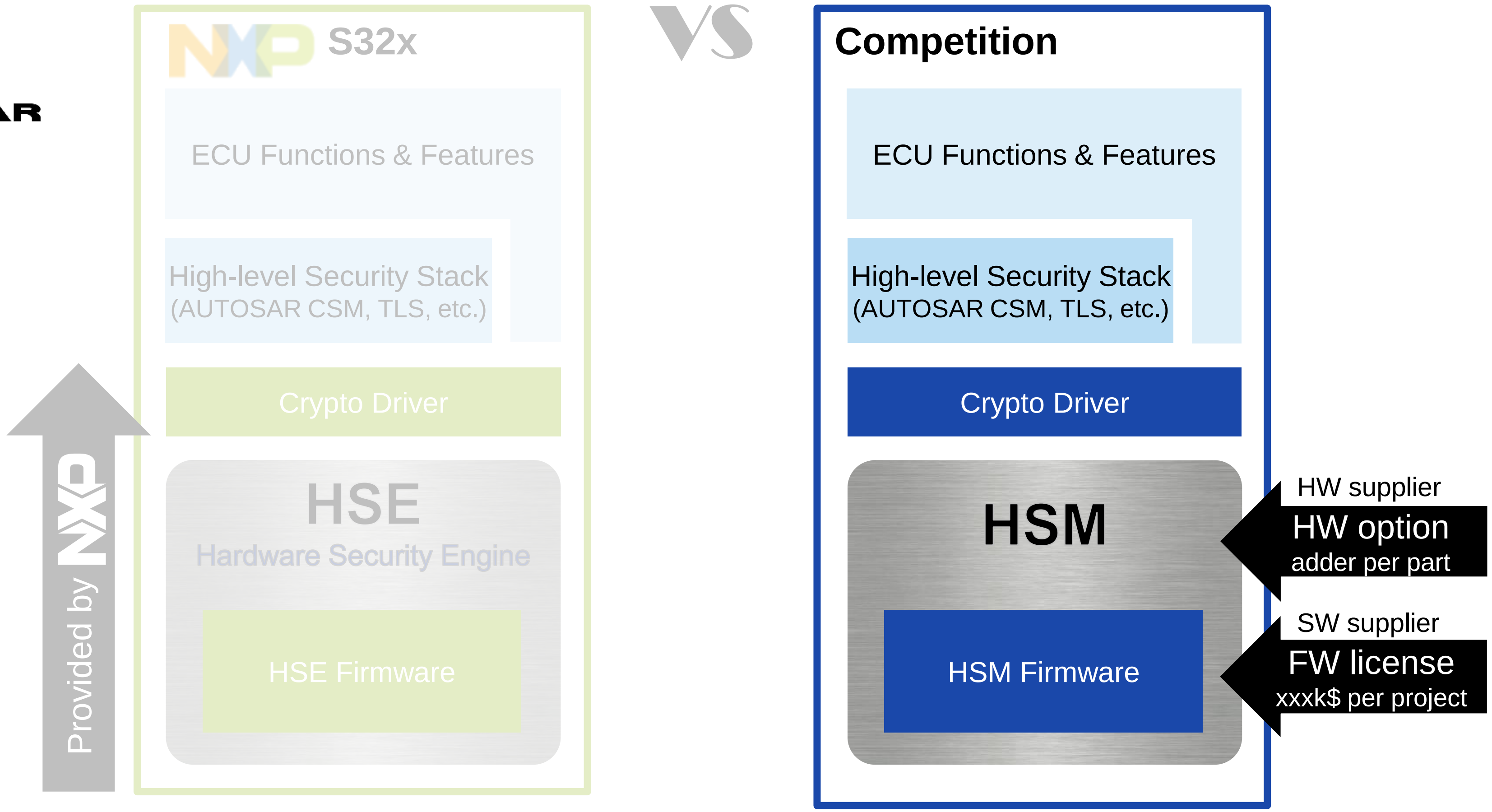
No extra costs

- 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



Provided by NXP

NXP S32x

ECU Functions & Features

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

Crypto Driver

HSE
Hardware Security Engine

HSE Firmware

Competition

ECU Functions & Features

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

Crypto Driver

HSM

HSM Firmware

HW supplier
HW option
adder per part

SW supplier
FW license
xxxk$ per project

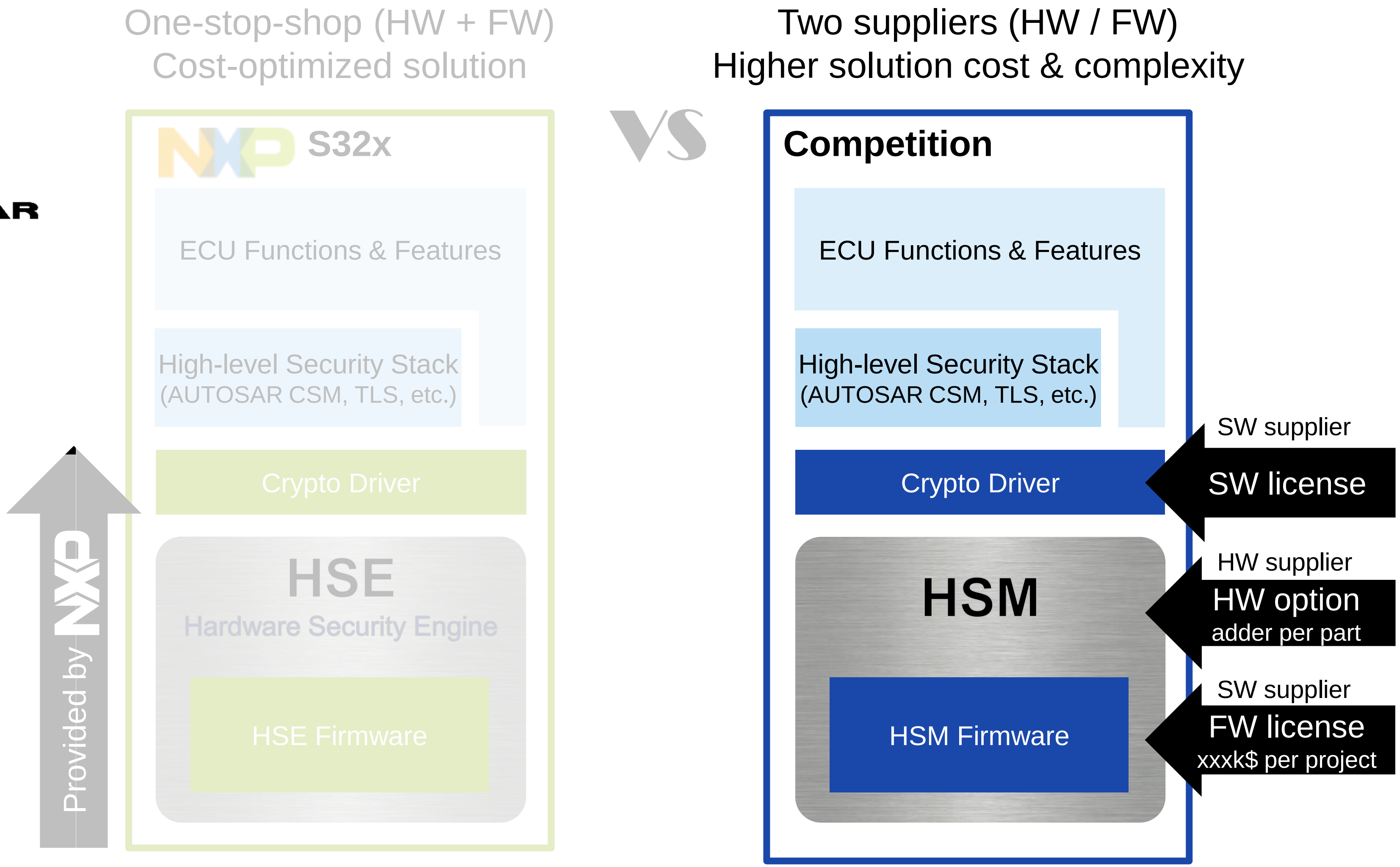
S32K3 SECURITY OFFER IS SIMPLER

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

NXP S32x

ECU Functions & Features

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

Crypto Driver

HSE
Hardware Security Engine

HSE Firmware

Provided by NXP

VS

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

Competition

ECU Functions & Features

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

Crypto Driver

HSM

HSM Firmware

SW supplier
SW license

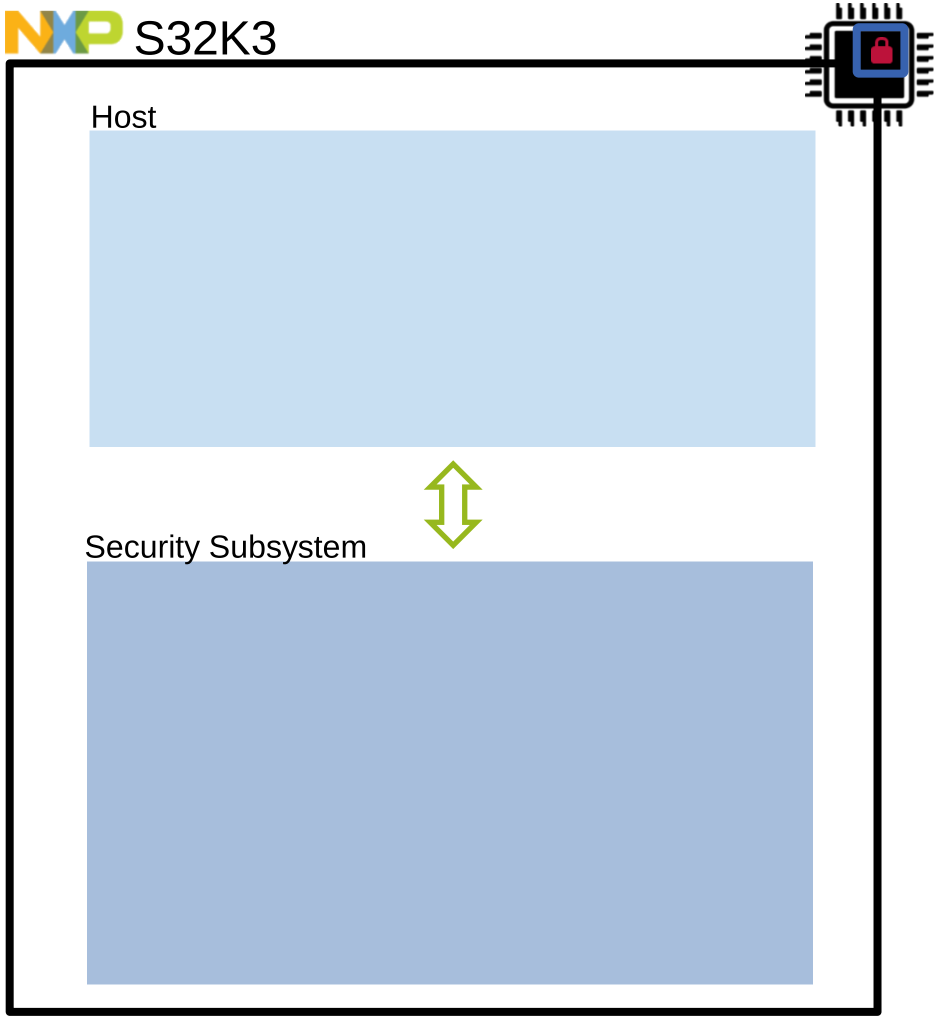
HW supplier
HW option
adder per part

SW supplier
FW license
xxxk$ per project

HOW S32K3 SUPPORTS AUTOMOTIVE REQUIREMENTS

SHE

Requirements

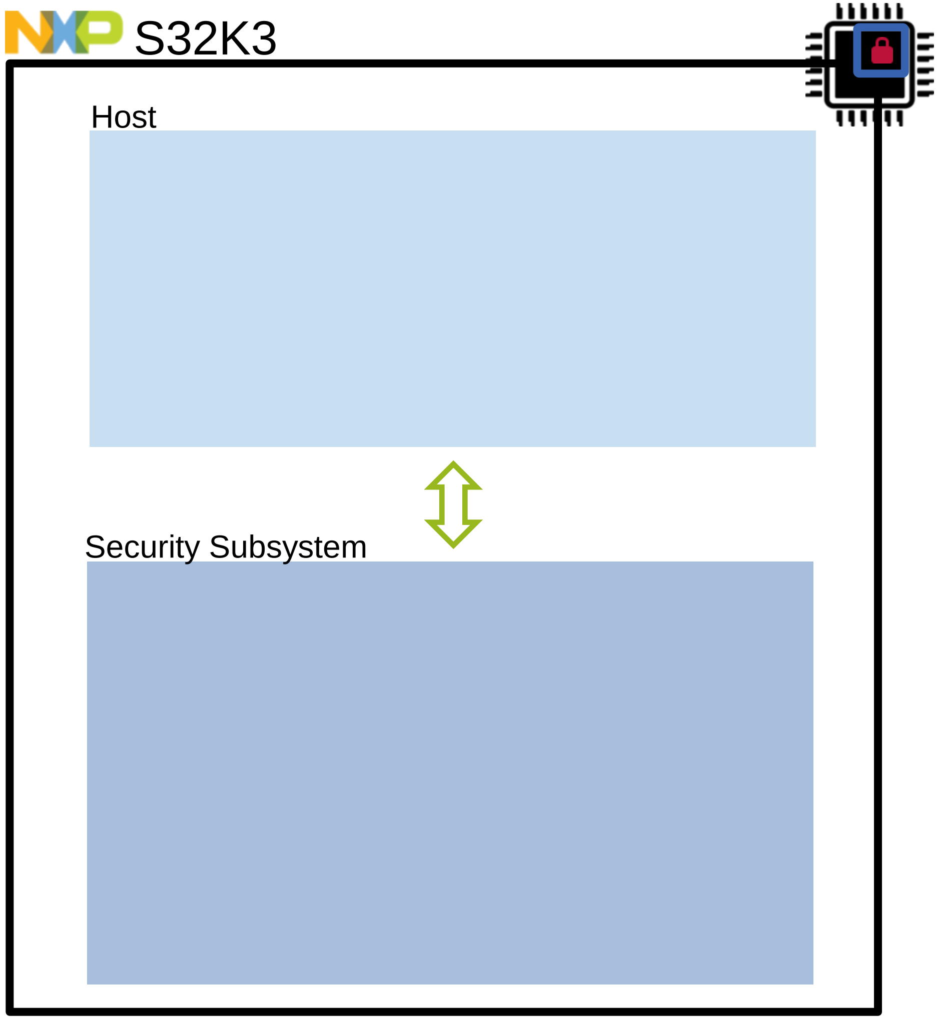


HOW S32K3 SUPPORTS AUTOMOTIVE REQUIREMENTS

« EVITA-Full »

SHE

Requirements



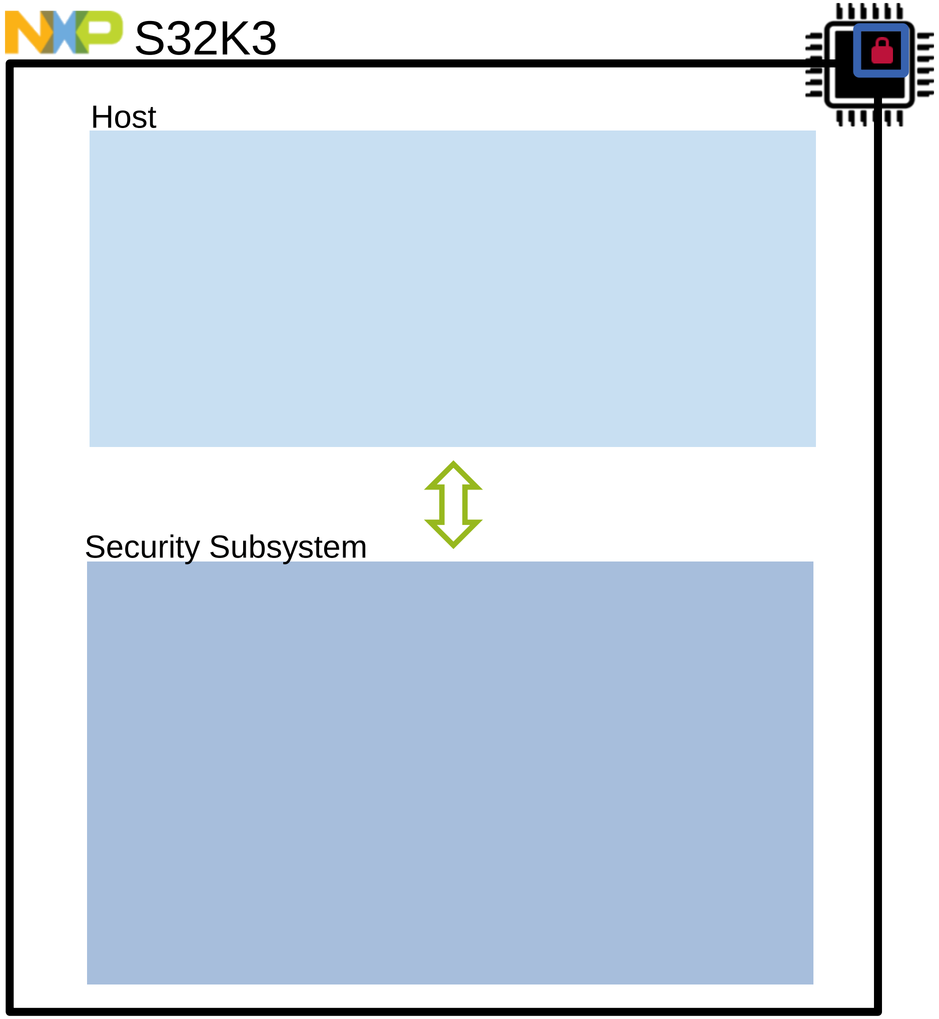
HOW S32K3 SUPPORTS AUTOMOTIVE REQUIREMENTS

OEM

« EVITA-Full »

SHE

Requirements



S32K3

Host

Security Subsystem

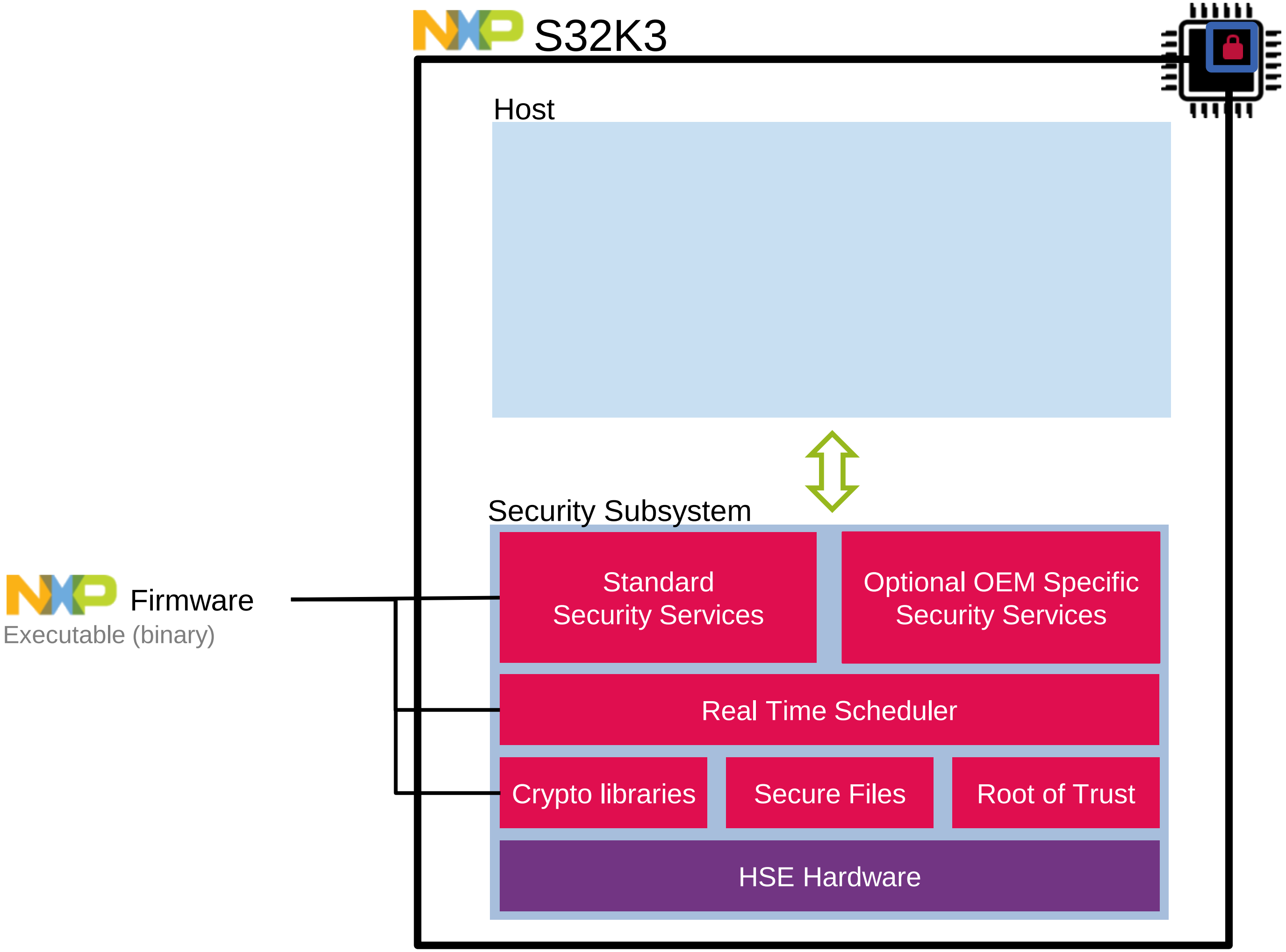
HOW S32K3 SUPPORTS AUTOMOTIVE REQUIREMENTS

OEM

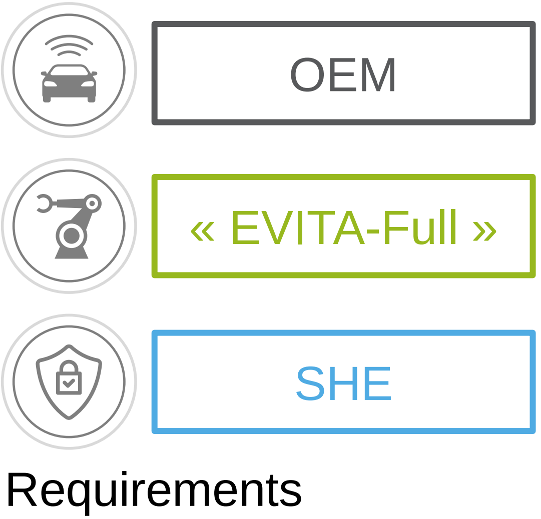
« EVITA-Full »

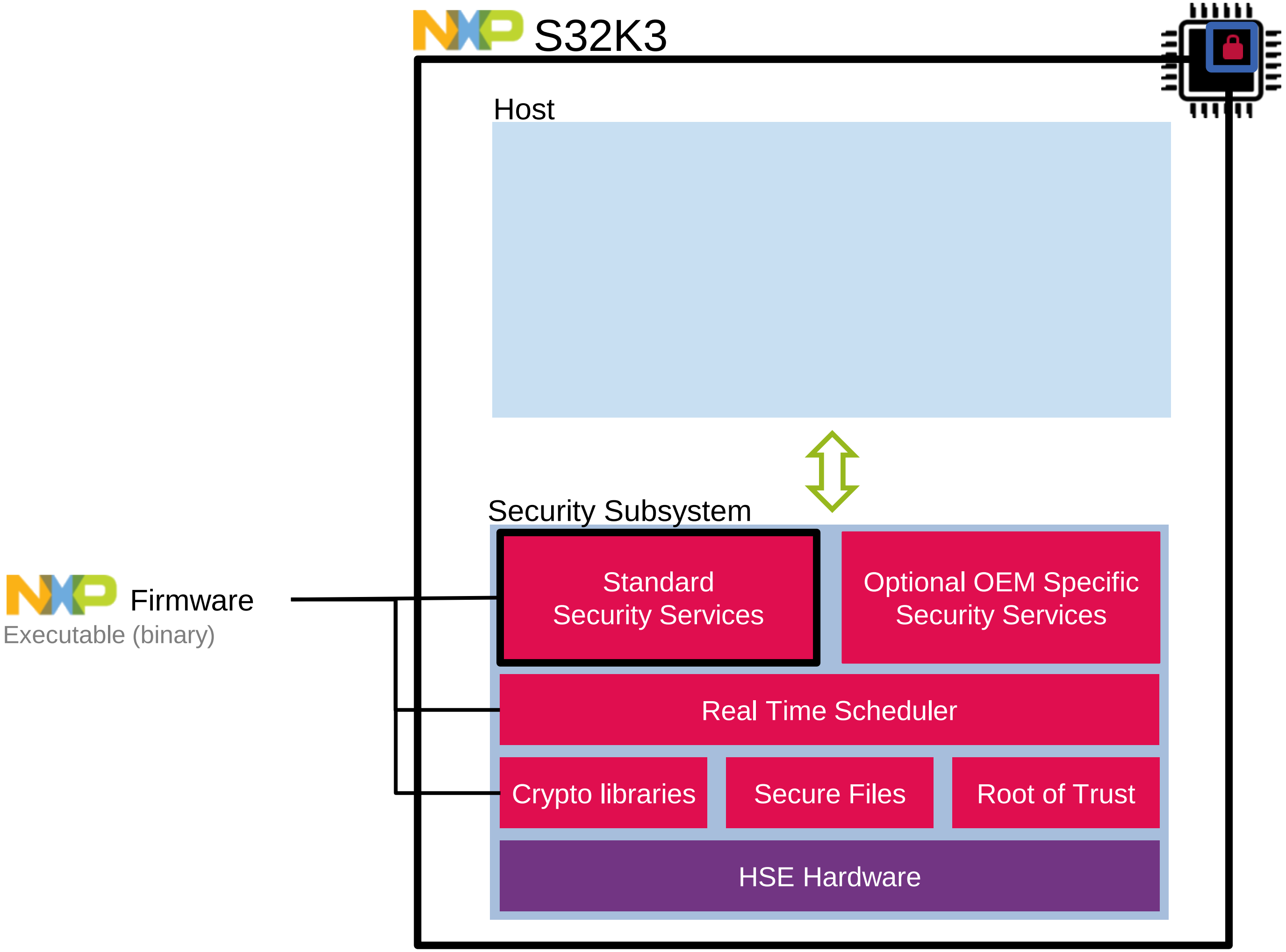
SHE

Requirements



HOW S32K3 SUPPORTS AUTOMOTIVE REQUIREMENTS





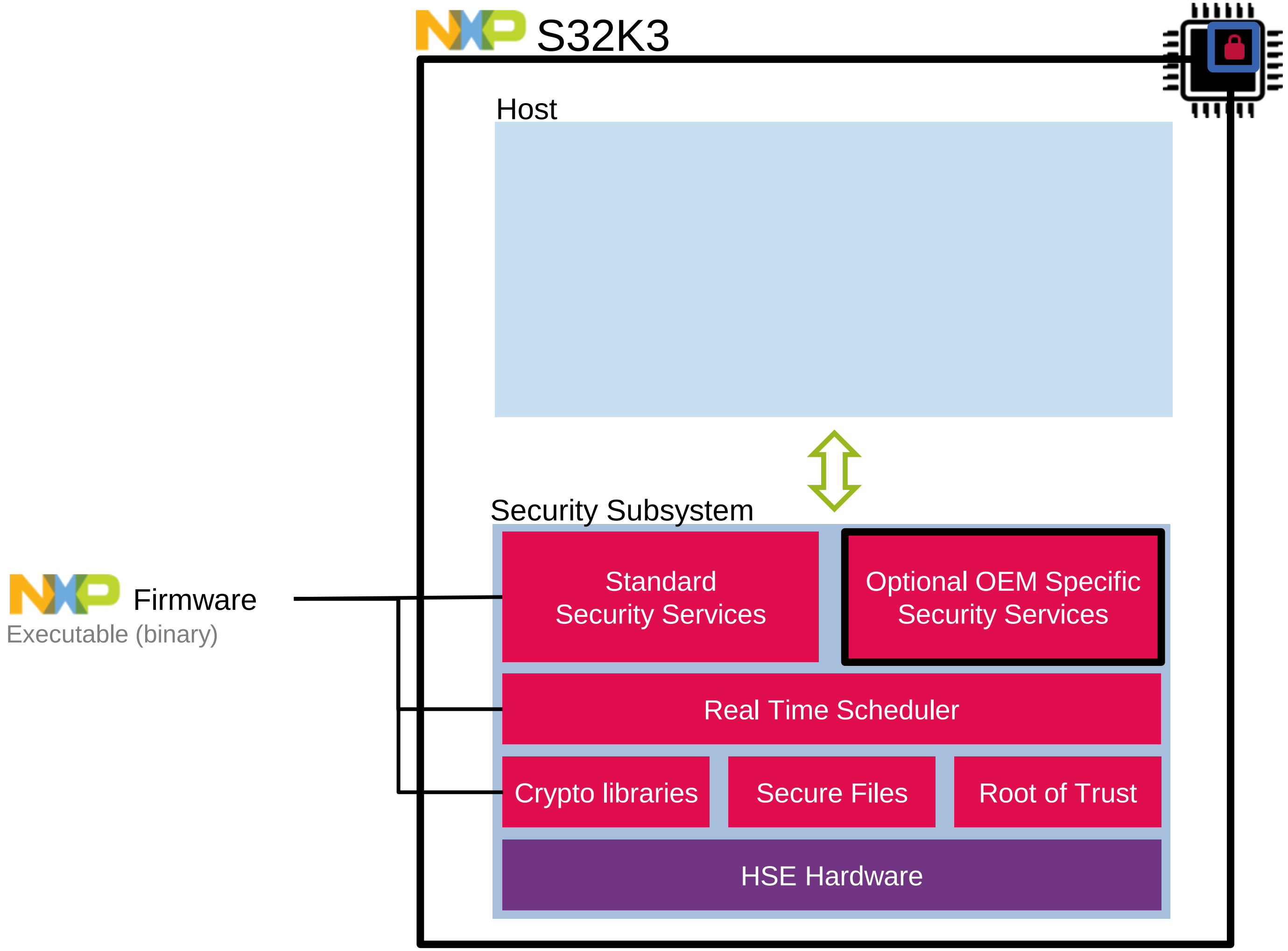
HOW S32K3 SUPPORTS AUTOMOTIVE REQUIREMENTS

OEM

« EVITA-Full »

SHE

Requirements



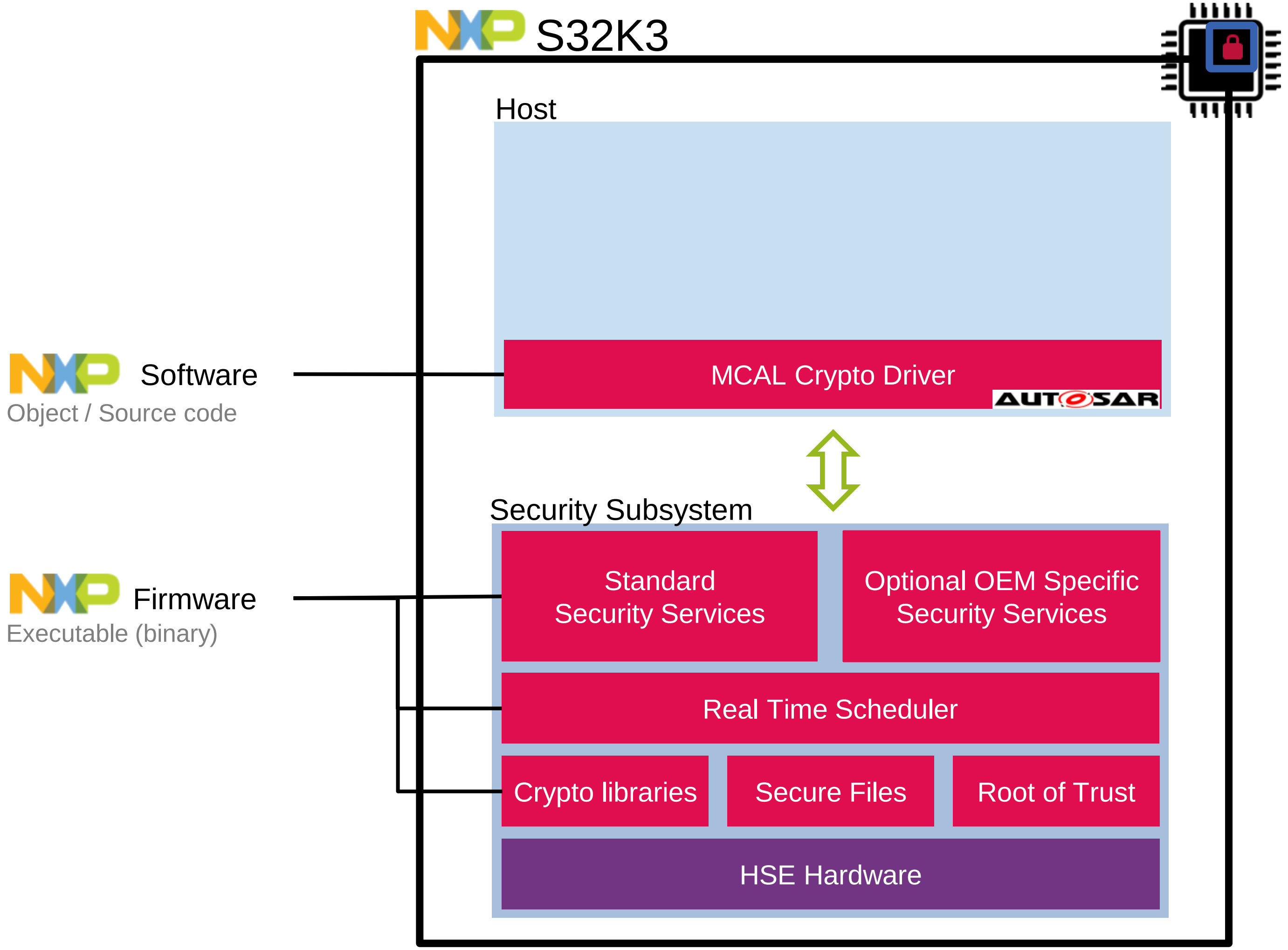
HOW S32K3 SUPPORTS AUTOMOTIVE REQUIREMENTS

OEM

« EVITA-Full »

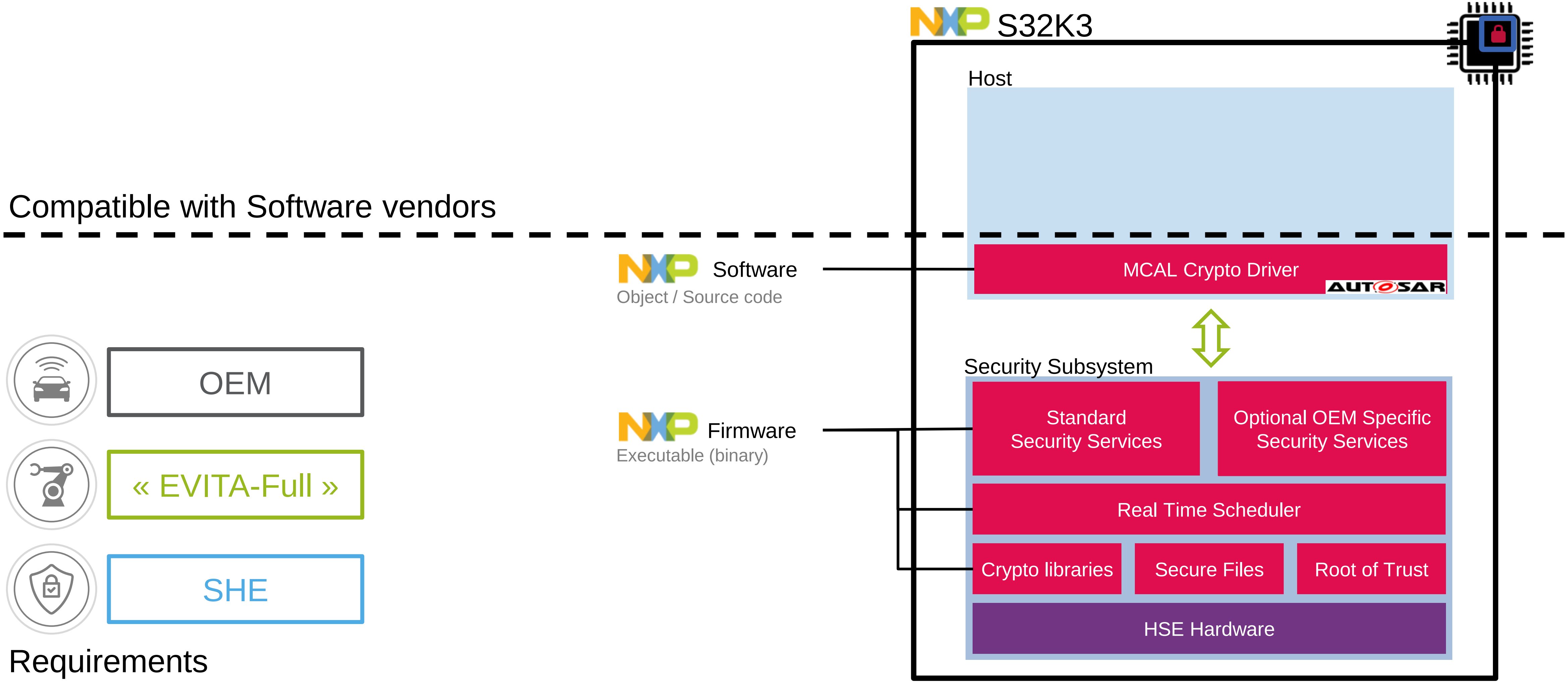
SHE

Requirements



HOW S32K3 SUPPORTS AUTOMOTIVE REQUIREMENTS

Compatible with Software vendors



Requirements

HOW S32K3 SUPPORTS AUTOMOTIVE REQUIREMENTS

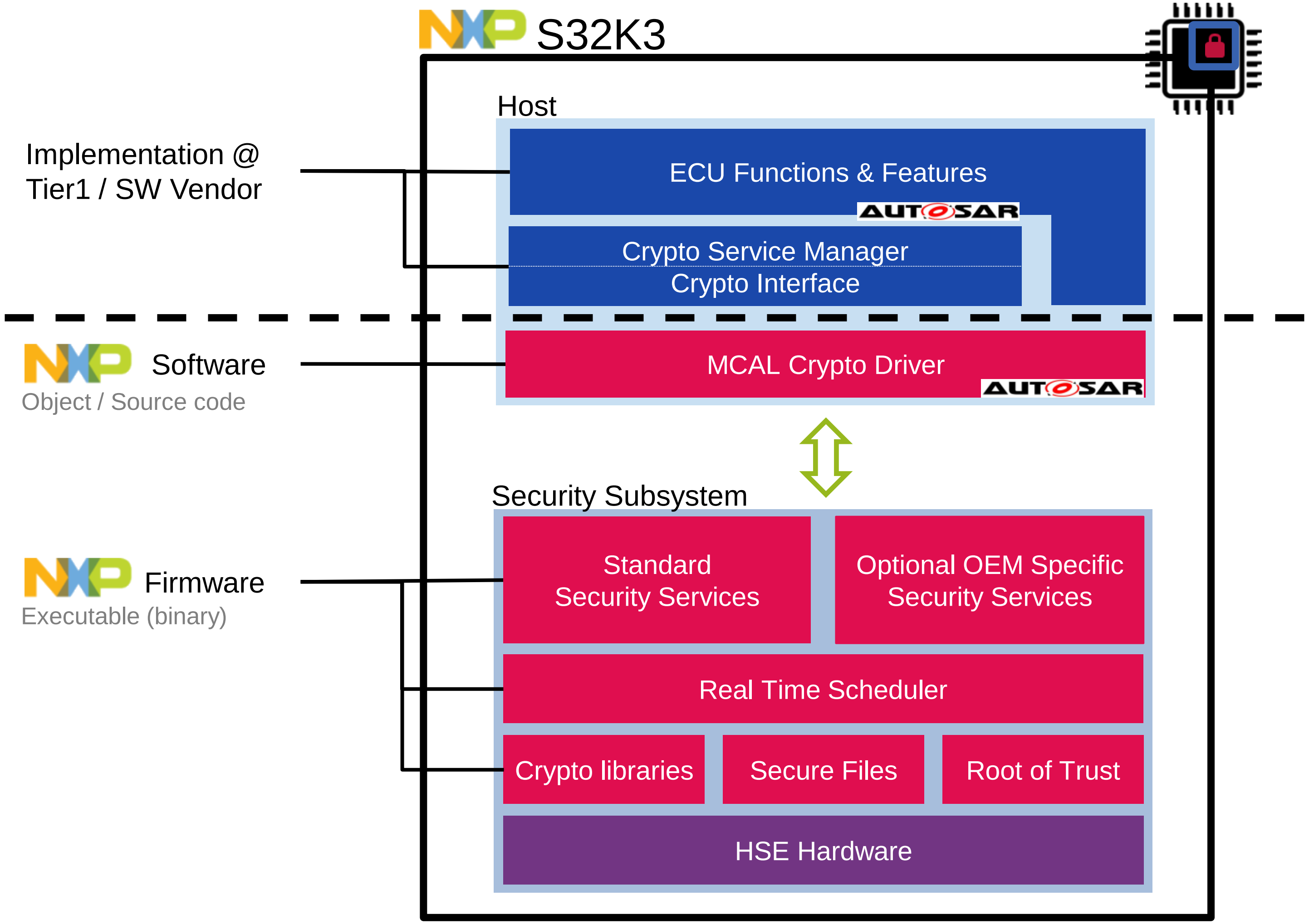
Compatible with Software vendors

OEM

« EVITA-Full »

SHE

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

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

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

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

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

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)

EDGELOCK™ ASSURANCE by NXP

THE S32K3 MICROCONTROLLER WILL BE PART OF THE EDGELOCK™ ASSURANCE PROGRAM

- Provides root-of-trust and implements secure boot, secure debug, lifecycle management, run-time integrity protection
- Features a security enclave (subsystem) that provides security services to the application(s)
- Provides logical and physical isolation of critical assets including crypto keys
- Provides resistance against software attacks and basic hardware attacks such as glitching and basic SCA.
- Security verified and validated under NXP’s secure development process (Security Maturity Process)
- Protection against basic hardware attacks has been assessed and confirmed by NXP’s vulnerability analysis (VA) lab.
- Experienced product support incident response team (PSIRT), and proven process, to professionally handle incidents, if they happen.
- Designed to comply with the ISO/SAE 21434 standard (cybersecurity engineering for road vehicles)

SUMMARY

S32K3 offers a complete secure OTA Solution

SUMMARY

S32K3 offers a complete secure OTA Solution

- Seamless and robust solution for A/B Swap and In place updates

SUMMARY

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

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

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
- For more information visit nxp.com/S32K3

Q&A

SECURE CONNECTIONS
FOR A SMARTER WORLD

SHOWROOM.NXP.COM