# eSE AUTOMOTIVE standardization

# GlobalPlatform Automotive Task Force

GlobalPlatform / STMicroelectronics
Munich, October the 21th 2026

Laurent TABARIES (STMicroelectronics)

Global Platform™

# You already trust a Secure Element every day

Apple Pay, Google Pay and mobile wallets rely on the eSE inside your phone.

## Trusted in your phone

Securely provisioned in factory

Continuously updated to maintain state-of-the-art security

Designed to stay resilient as threats evolve in the field

## Why not in your car?

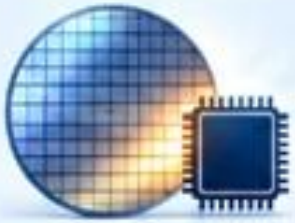
If you already trust the eSE in your smartphone for payments and sensitive credentials, the same trust model can inspire a more secure vehicle architecture.

**Same trust anchor. Same lifecycle mindset. New opportunity for automotive.**

# Automotive security starts in the supply chain

Multiple actors, multiple steps, multiple risks before the ECU reaches the vehicle

### Silicon / MCU supplier



Manufacture and deliver chips

### Tier-1 manufacturing

Assemble ECU (hardware)

### Identity & key provisioning

Generate and inject ECU identity, certificates and keys

### OEM assembly

Integrate ECU in vehicle

### In the field (operation)

Vehicle on the road (ADAS, connected services, updates)

### After-sales & maintenance

Workshops, diagnostics, software updates (OTA / service)

### Identity substitution / cloning

- Counterfeit or unauthorized components
- Duplicate ECU identity
- Fake or reused certificates

### Key exposure or injection

- Keys generated outside secure environment
- Leakage at supplier or subcontractor
- Wrong keys injected
- Insider threats

### Unauthorized programming / tampering

- Malicious or untrusted software
- Insecure manufacturing tools
- Debug interfaces left enabled
- Modification of security parameters
- Unauthorized access to ECU

### Lifecycle fragmentation

- Multiple Tier-1 and suppliers
- Different provisioning processes
- Multiple certification authorities
- Inconsistent security policies across manufacturing, aftermarket and OTA updates

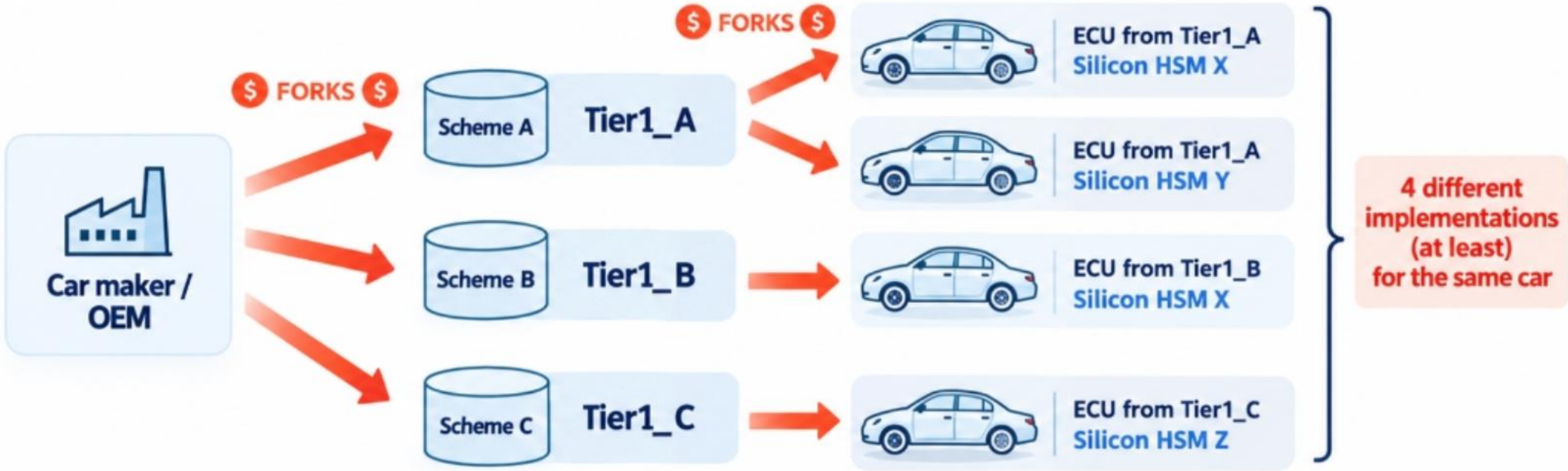
KEY MESSAGE

**The automotive supply chain introduces multiple security risks that must be addressed from chip to end of life.**

Global Platform™

# Today's fragmented landscape

**Today's situation: multiplication of FORKS, with different schemes (sometimes proprietary) and associated costs**




**EVITA-HSM does not define a standardized scheme, despite the AUTOSAR framework, increasing final car-maker OEM integration cost**

Global Platform™

# A Proven Path from Telecom to Automotive

Leveraging the GSMA/GlobalPlatform heritage to standardize and scale Secure Element provisioning in the automotive industry

Same trusted foundation.
New opportunities
**for the automotive world.**

Standardized, large-scale Secure Element provisioning driven by TSMs for billions of devices

Apply the proven model with OEM and sub-CA servers to provision Secure Elements in vehicles

### Proven Trust

GSMA/GlobalPlatform heritage with years of real-world deployment and operational experience.

### Standardized Flow

End-to-end provisioning model already defined and interoperable across the ecosystem.

### Greater Efficiency

Uniform approach reduces complexity, accelerates time to market and lowers overall costs.

### A Scalable Future

A common foundation to support diverse automotive use cases and a growing ecosystem.

GSMA™ | GlobalPlatform®

TRUSTED STANDARDS. GREATER POSSIBILITIES.

# From GSMA / GlobalPlatform track record to scalable automotive SE provisioning

Leverage the proven mobile ecosystem model to inspire a standardized and efficient provisioning approach for automotive

## PROVEN MOBILE / TELECOM MODEL

Standardized and widely deployed for many years

GSMA + GlobalPlatform ecosystem

| Service provider (MNO / MVNO) | GSMA standardized servers (e.g. SM-DP, SM-SR, SM-DP+) | Device host (smartphone & OS) | eUICC / Secure Element in device |
|---|---|---|---|
| • Subscription management<br>• Profile ordering<br>• Business rules | • Secure profile preparation<br>• Profile delivery<br>• Life-cycle management (install, enable, disable, delete) | • Secure channel to SE<br>• Profile download and management<br>• GSMA / GlobalPlatform interfaces | • Secure storage and execution<br>• Multiple profiles and applications<br>• Tamper resistant |

**Standardized end-to-end provisioning flow (GSMA + GlobalPlatform)**

Proven at large scale with multi-vendor interoperability

**REUSE PRINCIPLES, ROLES & OPERATIONAL KNOW-HOW**

NOT A DROP-IN GSMA STANDARD, BUT A PROVEN MODEL TO ADAPT

## PROPOSED AUTOMOTIVE ADAPTATION

Apply the same provisioning aprodel to automotive use cases

Inspired by GSMA / GlobalPlatform track record

| OEM backend / authorized suppliers | Provisioning orchestration & SE vendor backends | In-vehicle host (gateway / ECU) | Automotive Secure Element (eSE) |
|---|---|---|---|
| • Vehicle and user management<br>• Application ordering<br>• Authorization policies<br>• Integration with manufacturing and after-sales | • Prepare and manage secure applications<br>• Secure delivery to vehicles<br>• Life-cycle management (install, update, enable, disable, revoke)<br>• Multi-vendor support | • Secure channel to SE (GlobalPlatform)<br>• Application download and installation<br>• Interface with vehicle systems (e.g. OTA) | • Secure storage and execution<br>• Automotive-grade (AEC-Q100 etc.)<br>• Multiple applications (e.g. identities, keys, certificates) |

**Standardized provisioning architecture for automotive (inspired by GSMA)**

Same principles, adapted to automotive actors, constraints and use cases

## Key benefits for automotive

### Established deployment track record

- Proven model in the mobile industry
- Operational experience at global scale

### Multi-vendor interoperability potential

- Standardized roles and interfaces
- Leverage GlobalPlatform ecosystem
- Reduced fragmentation across suppliers

### Reduce ECU-specific integration & provisioning effort

- Reuse proven architecture and operational model
- More uniform and scalable deployment
- Lower complexity and time-to-market (architecture dependent)

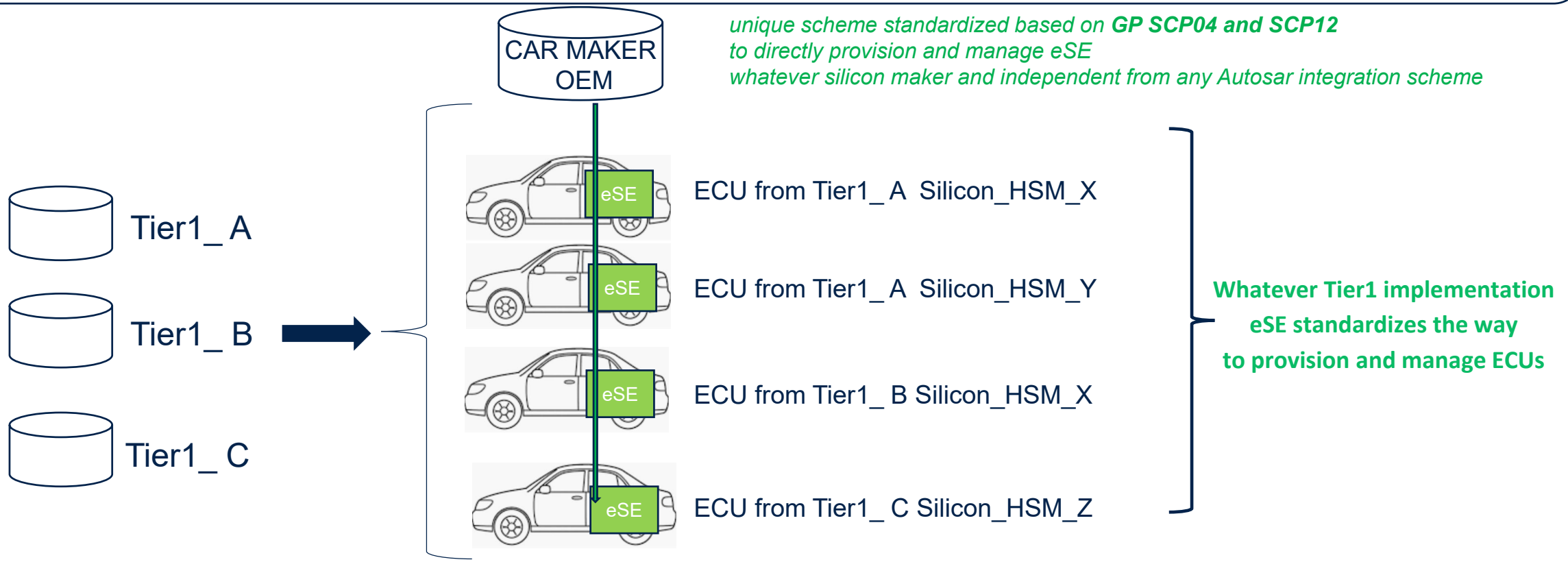
Global Platform™

**GlobalPlatform Secure Channel Protocols** (e.g. SCP03/SCP04/SCP11/SCP12) are transport and device-side management enablers.
Provisioning, orchestration, APIs, business processes and trust governance must be standardized and defined by the automotive ecosystem (OEMs, suppliers, SE vendors).

# eSE automotive framework for provisioning and supply chain cost saving

**Today identified ECU automotive points that can be improved thanks to an eSE**

➡ **eSE is a secure vault, enabling central and secure provisioning (whatever sub-contractors with any custom scheme) can help to save a lot of money from overall cost point of view**




Global Platform™

**Adding an eSE is the way to rely on a standard (GP) independant from any implementation**

**Once inside the eSE data are LOCKED … OEMs can rely on it without risk whatever the supply chain (without integrity check)**

# ONE framework. MANY programs. LOWER costs.

Standardize security lifecycle services across Tier-1 and silicon variants — under OEM control.

## TODAY | N CUSTOM FLOWS

- Tier-1 A — Custom provisioning A
- Tier-1 B — Custom provisioning B
- Tier-1 C — Custom provisioning C

Repeated tools • repeated validation

→

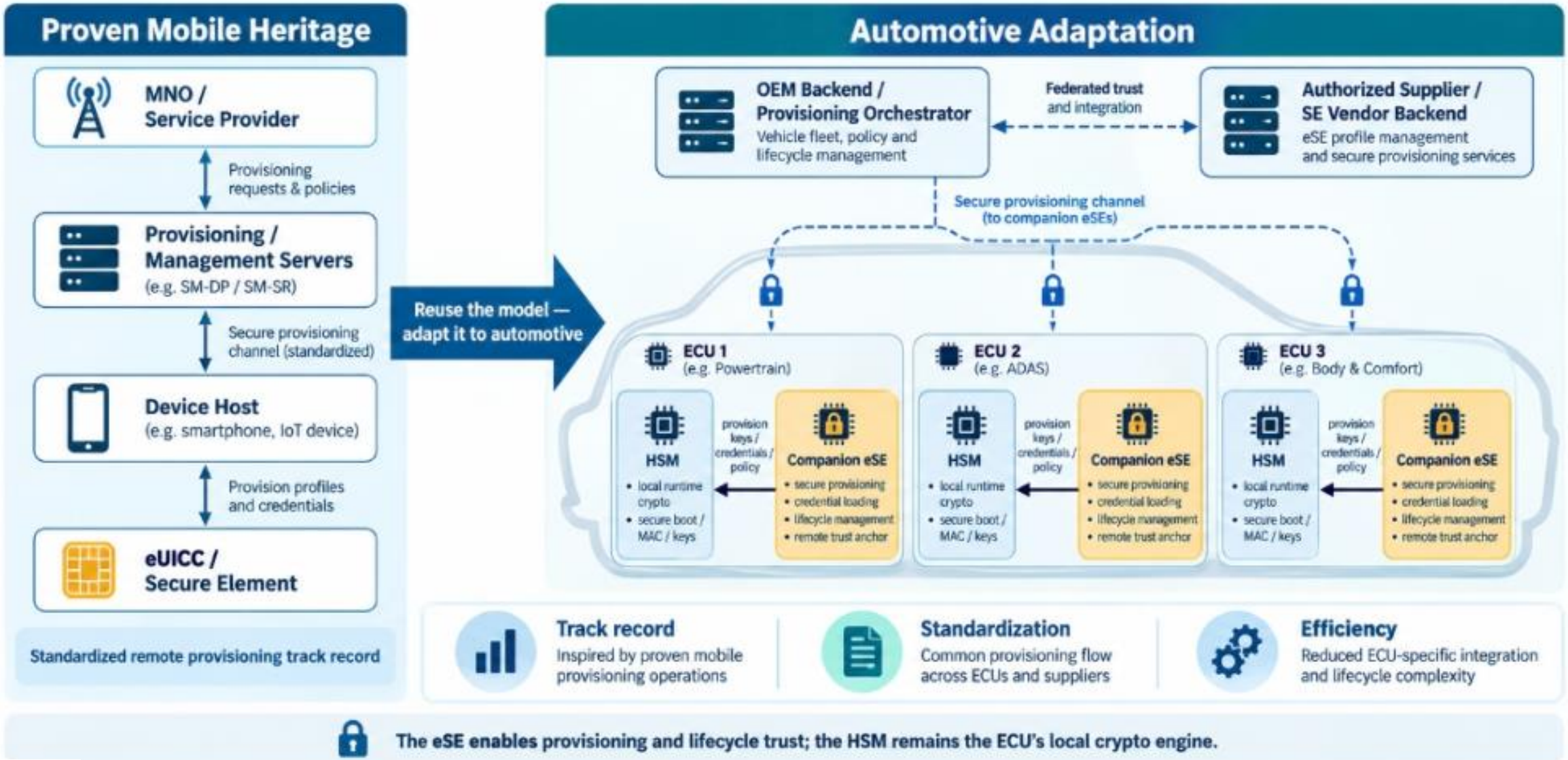
## WITH eSE | ONE REUSABLE FRAMEWORK

## COST REDUCTION

Fewer custom integrations • Shared tooling • Less repeated qualification

# GSMA-Inspired Provisioning for Automotive ECUs

Use the proven mobile remote-provisioning model to manage companion eSEs across vehicle ECUs

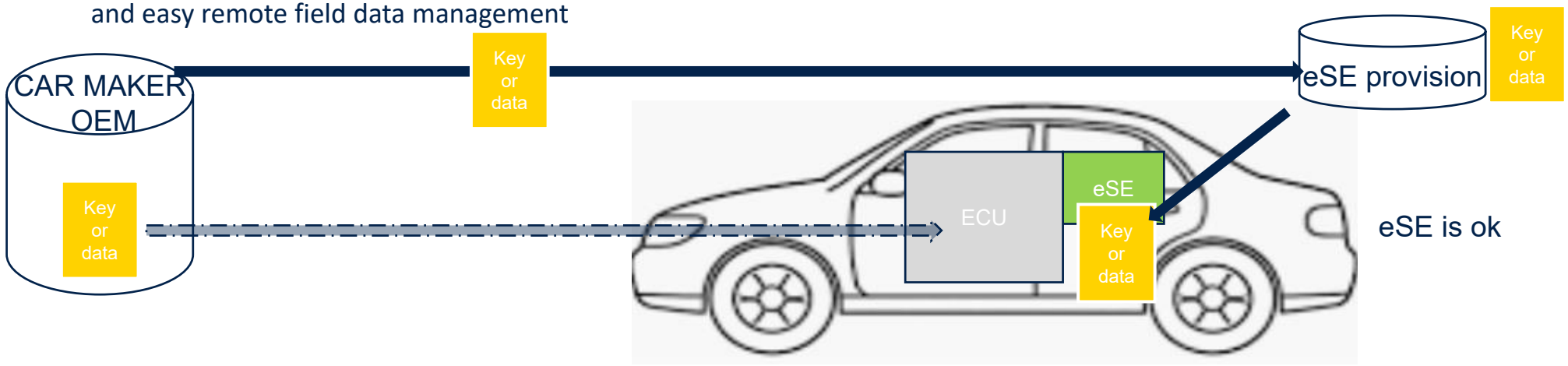



Global Platform™

# eSE automotive for easy provisioning and easy field maintenance

**eSE automotive using SCP** (Secure Channel Protocol) **is offering AGNOSTIC, UNIFORMIZED, and EASIER provisioning and data management**

- eSE has a secure life cycle and secure production flow to make robust provisioning whatever next steps production and easy remote field data management



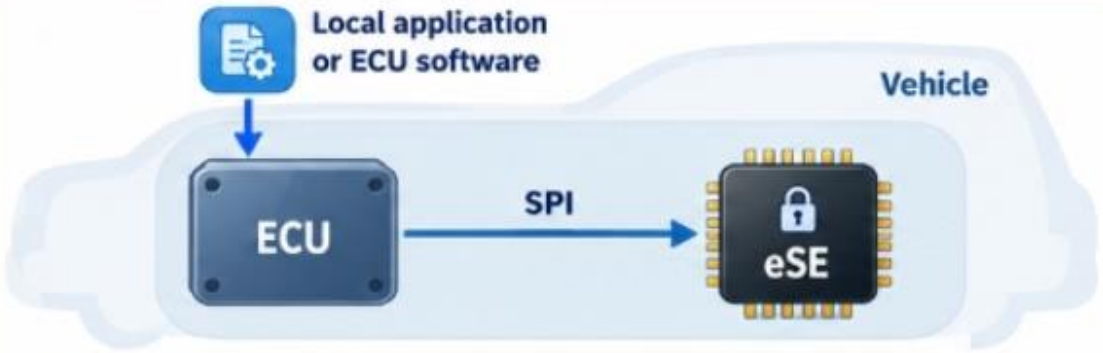

- eSE to require ECU to behave as a rooter, just to encapsulate relevant commands and data coming from OEM server

Global Platform™

# eSE administration paths in the vehicle

Local administration and remote administration use the same eSE, but the command origin and ECU role differ.

## 1. Local administration



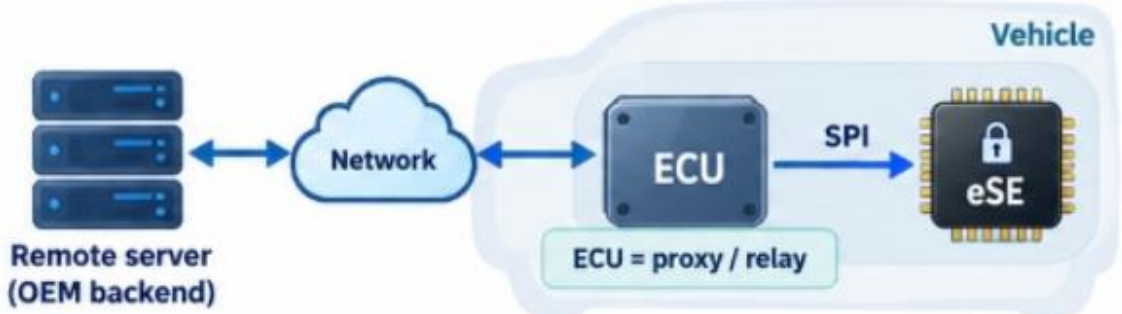

1. Local application or ECU software triggers an admin command
2. ECU sends the command to the eSE over SPI
3. eSE executes the admin function
4. Response returns locally to the ECU

### Typical admin functions

- Applet / application management
- Key or credential update
- Configuration / lifecycle action

**ECU acts as the local administrator**

## 2. Remote administration




1. Remote management server creates an admin command
2. Command is sent securely to the vehicle
3. ECU receives the command and forwards it
4. eSE executes the command
5. Response is returned through the ECU back to the server

### Key point

- Command origin is remote
- ECU transports the command
- eSE remains the trusted execution endpoint

**ECU acts as a proxy; the admin intent comes from the backend**

## Main difference

**Local admin:**
command starts in the ECU

**Remote admin:**
command starts in a backend server, ECU forwards it to the eSE

In both cases, the eSE is the secure execution endpoint; SPI is the local transport between ECU and eSE.

Global Platform™

# GlobalPlatform Secure Channels: SCP03 / SCP11 → SCP04 / SCP12

Same objectives, stronger cryptography and more flexibility for future needs

GlobalPlatform

## Current generation

### SCP03 – Symmetric Secure Channel — GP 2.2 / 2.3

| | |
|---|---|
| Trust model | Pre-shared symmetric keys (e.g. ENC, MAC, DEK) |
| Authentication | Mutual authentication using card and host cryptograms (challenge–response) |
| Session keys | Derived from static keys (GP key derivation) |
| Message protection | Confidentiality and integrity (AES-CBC + CMAC) |

### SCP11 – Asymmetric Secure Channel — GP 2.3.1

| | |
|---|---|
| Trust model | Pre-provisioned ECC key pair and certificates (PKI) |
| Authentication | Mutual authentication using ECC and certificates (EAC-like) |
| Session keys | Derived via ECDH key agreement (then AES session keys) |
| Message protection | Confidentiality and integrity (AES-CBC + CMAC) |

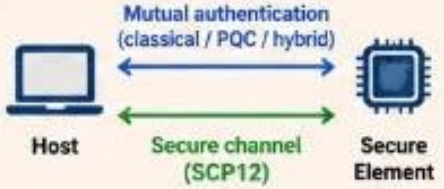
## Next generation

### SCP04 – Symmetric Secure Channel — GP 2.4 (published)

| | |
|---|---|
| Trust model | Pre-shared symmetric keys (more flexible profiles) |
| Authentication | Mutual authentication (improved mechanisms and options) |
| Session keys | Enhanced key derivation and algorithm agility |
| Message protection | AES-GCM (and other options, e.g. SM4), configurable security levels |

### SCP12 – Asymmetric Secure Channel — GP 2.4+ (in development)

| | |
|---|---|
| Trust model | Public key infrastructure (classical and post-quantum options) |
| Authentication | Mutual authentication (classical, PQC or hybrid) |
| Session keys | Key agreement using traditional ECC and/or post-quantum algorithms (e.g. ML-KEM) |
| Message protection | AES-GCM (and other options), agility for post-quantum transition |




## Key evolution highlights

**Stronger cryptography**
From AES-CBC + CMAC (SCP03/SCP11) to AES-GCM and additional algorithms (SCP04/SCP12).

**Algorithm agility**
Multiple cryptographic options (e.g. AES, SM4, future algorithms).

**Post-quantum readiness**
SCP12 introduces PQC and hybrid modes to address future threats.

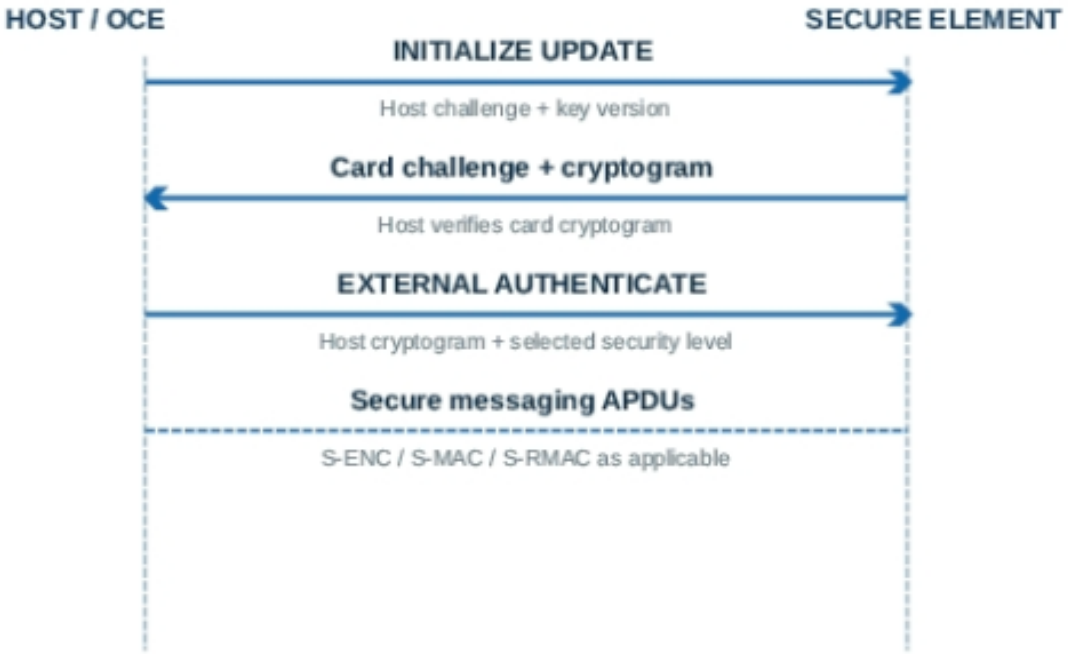
**Same security objectives**
Mutual authentication, session key establishment, confidentiality and integrity for secure management of the Secure Element.

Global Platform™

# GlobalPlatform Secure Channels | Host–Secure Element sequence

Two complementary trust models: symmetric pre-shared keys versus ECC certificate-based key establishment

## SCP03 | symmetric authentication




Both sides derive session keys from pre-shared AES keys and challenges.

## SCP11a | ECC + certificates

SCP11a: mutual authentication. SCP11b authenticates the card only.

**EVOLUTION • SCP04: configurable symmetric cryptography and AEAD profiles | SCP12: post-quantum / hybrid asymmetric direction (details subject to final specification)**

Global Platform™

# PQC and security evolution can drive HSM cost inflation

Long vehicle lifecycles and evolving cryptography raise memory, compute and security demands.

**eSE opportunity: isolate eligible crypto and credentials to limit future MCU/HSM resource growth**

# eSE: contain HSM inflation and unlock BOM opportunities

Two value horizons: avoid future HSM upgrades and reduce today's BOM where the ECU architecture allows.

## MCU / HSM-ONLY PATH

**New crypto + new security services**

↓

**Potential larger / costlier HSM or MCU**

More memory, compute, integration and qualification

## MCU / HSM + eSE PATH

**Assign selected security functions to the eSE**

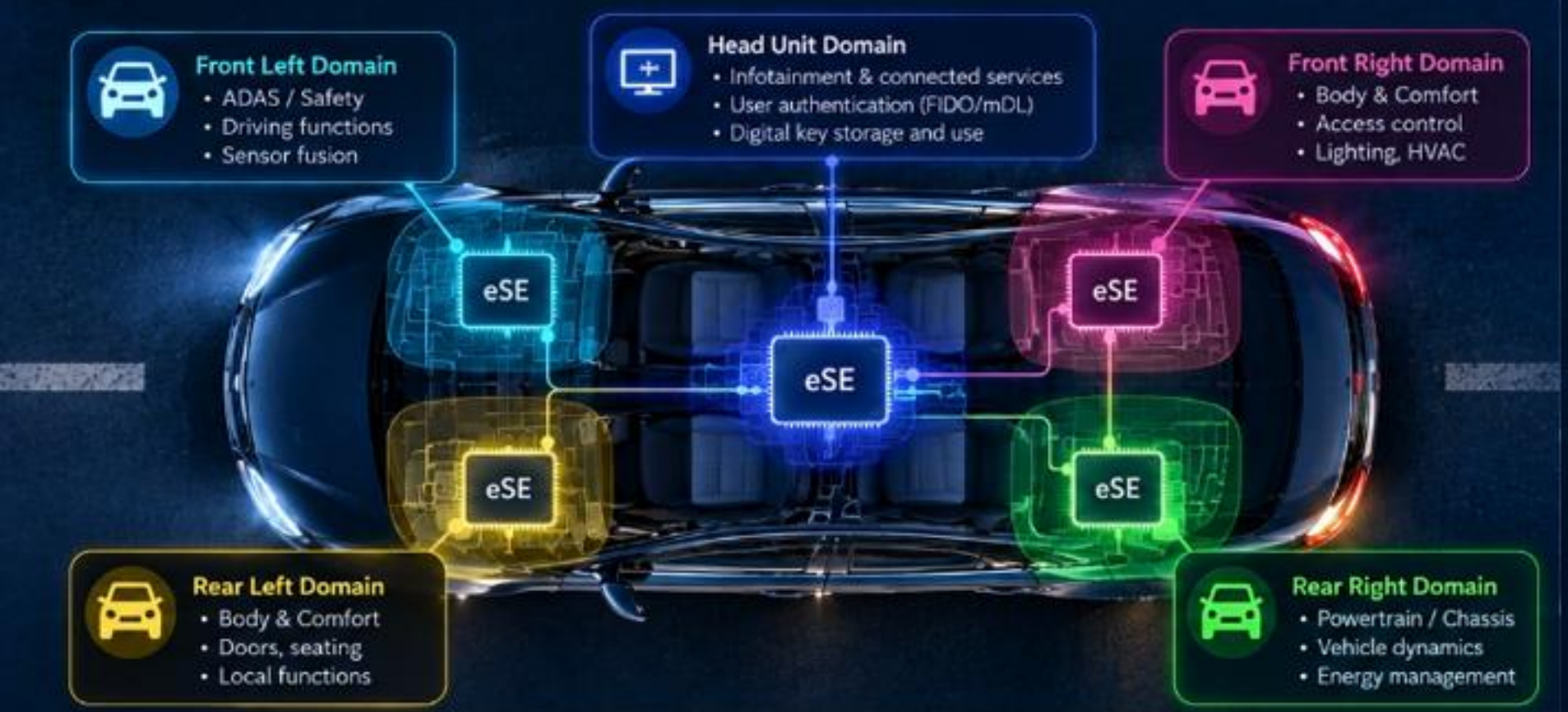
**Right-sized MCU / HSM** → **eSE**
Protected identity
Eligible crypto

In eligible ECU designs, an eSE can also avoid a separate HSM — validate boot, latency and safety constraints

**FUTURE: avoid HSM upsizing | TODAY: possible HSM removal / MCU downsize | NET BOM: design-dependent**

# Zonal architecture – multiple eSEs across domains

A scalable architecture with dedicated eSEs per domain and use case




## 5 security domains

**1 Head Unit (Infotainment)**
- User authentication (FIDO/mDL)
- Digital key storage and use
- Connected services

**2 Front Left (ADAS / Safety)**
- Secure identity and certificates
- Sensor data protection
- Functional safety alignment

**3 Front Right (Body & Comfort)**
- Vehicle access (UWB/NFC/BLE)
- Key management and permissions
- Lighting, HVAC

**4 Rear Left (Body & Comfort)**
- Doors, seating, climate
- Local functions and peripherals
- Tamper-resistant key storage

**5 Rear Right (Powertrain / Chassis)**
- Secure boot and software integrity
- ECU authentication and control
- Protection of critical parameters

**Domain isolation**
Dedicated eSE per domain and use case

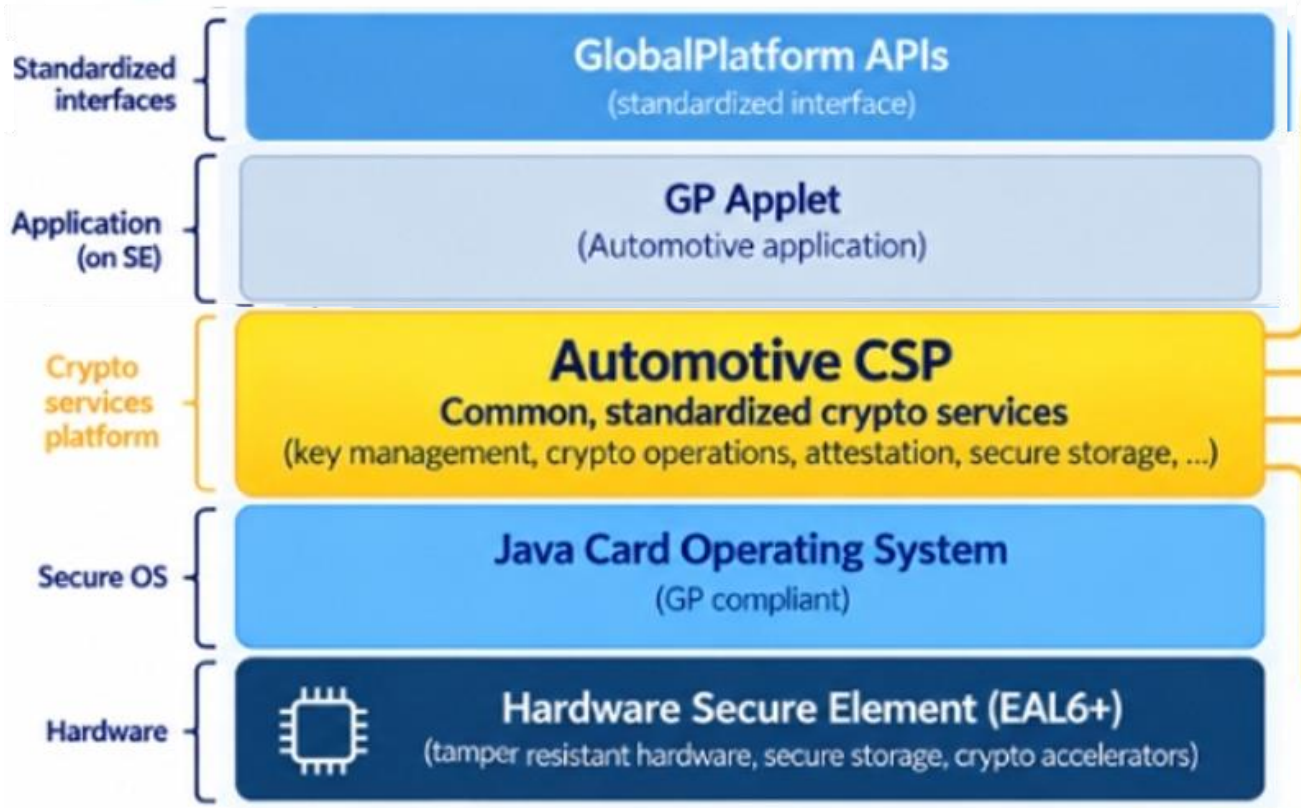
**Scalable architecture**
From 1 to n eSEs depending on platform

**Common platform**
Same secure foundation across all domains

**Ready for evolution**
Supports new services and future algorithms (PQC)

# Automotive CSP is the game changer

From multiple proprietary implementations to a common, standardized crypto services platform




## 100% compliant with SAE J3101

The CSP provides all required automotive crypto services according to SAE J3101.

## No composite certification

The CSP is certified as a complete crypto services platform, removing the need for composite certification (application + OS + hardware).

## Secure Element as a commodity

Without composite certification, the Secure Element can be used as a standard, off-the-shelf component (multiple vendors), reducing cost and supply risks.

## Standardized and interoperable

Based on GlobalPlatform, ensuring a common, open and interoperable implementation across OEMs, Tier-1 and suppliers.

**Lower development cost**
Reuse common, certified building blocks

**Faster time to market**
Standardized implementation

**Higher security and maintainability**
Common platform, consistent security policies

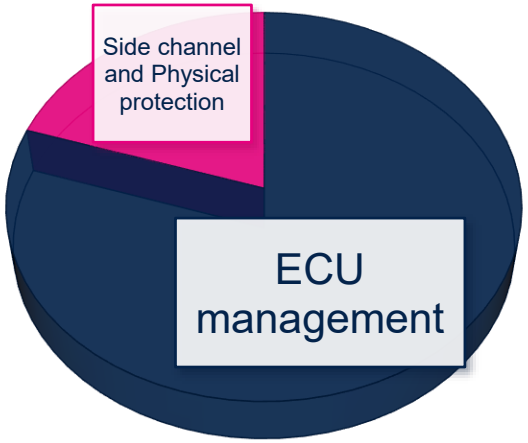
Global Platform™

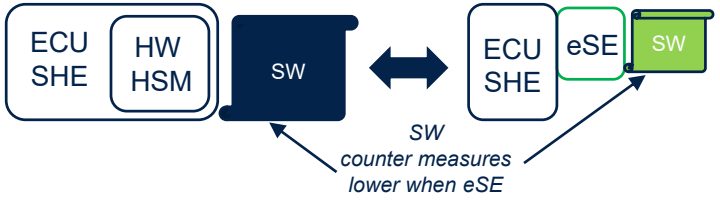
# CONCLUSION :eSE automotive for immediate benefit and cost saving

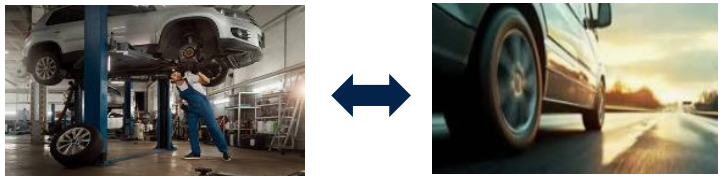
## Today identified ECU automotive points that can be improved thanks to an eSE

**➡ eSE is offering, on top of intrinsic side channel and physical attack protection, a valuable solution for ECU management (provisioning, traceability, maintenance, data storage and data management), and security services calls**

### eSE RATIONAL



**eSE automotive to be understood as a standardized and pragmatic solution for OEMs addressing risk mitigation**

- eSE is offering
  - *Tamper resistance against physical attacks (AVA_VAN 5)*
  - *Well-defined certification scheme with high assurance (EAL4+)*
  - *Crypto agility, Patchability and Upgradability*
  - *Advanced crypto algorithms AND PQC readiness*
  - *Key Management life cycle*
  - *Secure execution environment for hosting business logic (GP Auto Applet)*

**➡ eSE BOM cheaper to replace proprietary Secure BOOT and Root of Trust provisioning today HSM + eSE cost saving regarding SW countermeasures simplification**
**There are about 80 ECUs per car …. up to 150 for premium**

**➡ eSE cost saving and insurance for field robustness and field maintenance**
**100$/€ is a row fee per car in case of recall (outside time of change ECU, ECU price themselves), and in case no recall is possible, immobilizer weakness will impact the car insurance**

# CONCLUSION :eSE automotive for immediate benefit and cost saving