Global Platform®

GlobalPlatform ATF

GP eSE automotive framework

26th of May 2026 - TOKYO meeting

Laurent TABARIES (STMicroelectronics)

CONTEXT and GOALS to achieve

- **TO GIVE A STATUS ABOUT AUTOMOTIVE CYBERSECURITY CHALLENGES TODAY AND TOMORROW**
  => SW countermeasures effort, flexibility, provisioning, field maintenance
  => Standardization, OEM low integration effort and lower field maintenance are game changer KPI
  => PQC is a disruptive point …. Particularly with HW crypto support, side channel resistant, and with good Keys management

- **TO EXPLAIN HOW eSE WILL BECOME A STANDARDIZED SOLUTION EASY TO USE WITH MINIMUM OEM EFFORT**
  => eSE is expected to be used on top of (HSM extension or TELEMATICS services), and in a flexible way
  => CSP is the way to use an eSE without drawback (no CC or composite certification)
  => eCALL could be reused a generic eSE and even more robust with SAM
  => eSE as convergence points of many cybersecurity use cases (today and tomorrow)

- **TO EXPLAIN eSE concrete benefits**
  => Standardized, to lower today SW countermeasure management, provisioning and maintenance effort
  => Long term state of the art robust solution
  => Concrete OTA use case on-going to give eSE benefits metrics

… GP to promote eSE automotive as an efficient and easy to use solution for automotive OEMs

1. Synopsis

Automotive security landscape is first a fragmented landscape…

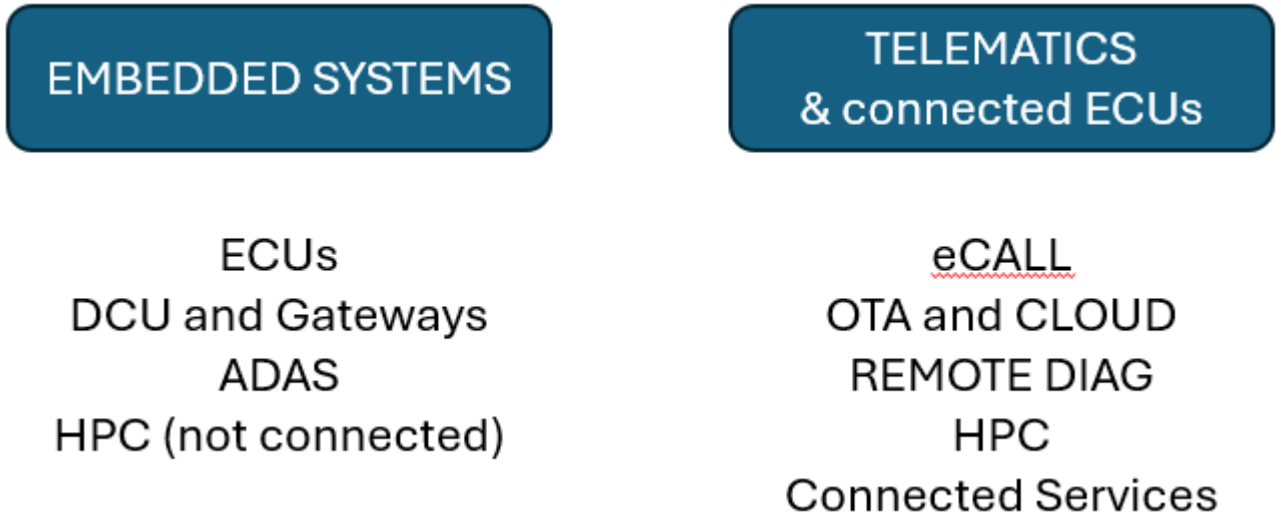
Building a car today combines many challenges, to ensure safety and security for what happens inside the car but also outside the connected car; so many things with different ecosystems, different integrations, and different security challenges.

eSE automotive framework initiative is paving the road to improve today situation,
by proposing guide and recommendation about how to use eSE automotive,
to make eSE usage standardized,
to help solving most of automotive security challenges

2. Automotive security landscape is a complex environment

Car integration be split into 2 main groups: “Telematics” and “Embedded systems”
“Telematics” in the car is managing mainly connected services, OTA (over the air) updates, Remote diagnostics …
“Embedded Systems” is mainly dealing with ECUs, HPC not connected, DCU, Gateways, ADAS

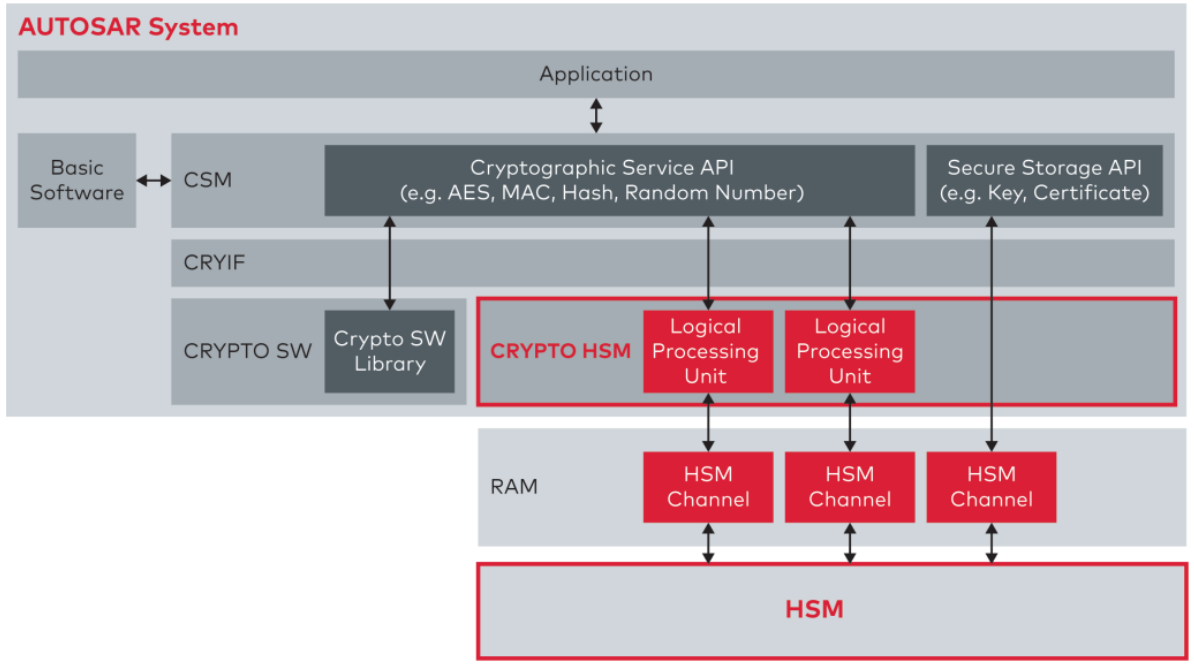
Most of AUTOSAR security functions, for embedded systems are using some CSM APIs (Cryptography Service APIs)



2. AUTOSAR CLASSIC integration challenges

When executing these AUTOSAR CSM APIs, It can be executed either by an HW HSM, but also by a SW crypto lib, (by a CPU without any memory protection) …. but there is no standard for HSM

Many integrations are possible, leading to forks and impacting the cost of SW maintenance

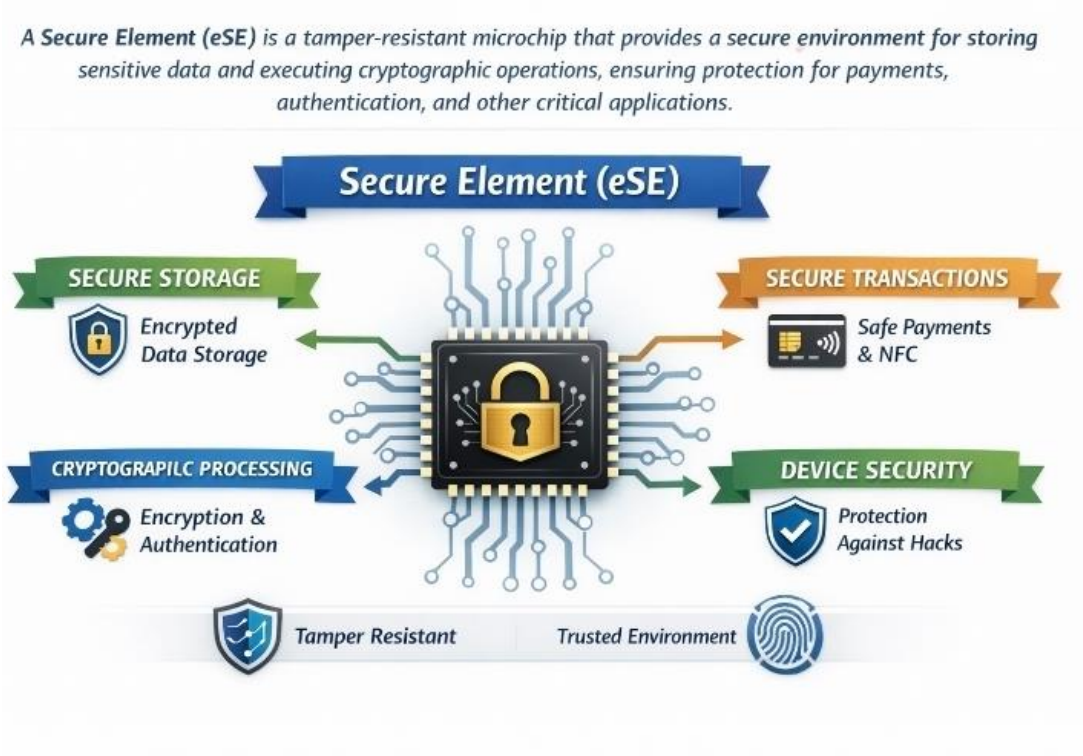


2. eSE definition

A Secure Element (eSE) is a tamper-resistant hardware component designed to provide a trusted execution environment for storing sensitive data and performing cryptographic operations, and to guarantee integrity asset.

In automotive systems, It acts as a hardware root of trust, enabling secure authentication, key management, and protection against physical and logical attacks.

The eSE is a critical building block for securing connected vehicles, supporting use cases such as secure communications, OTA updates, digital keys, in-vehicle payments and many other robust cryptographic services to reinforce local ECU challenges.



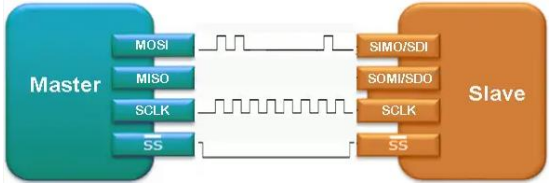
- **eSE is used as an extension of EVITA (HSM, SHE) to improve security features**
- **eSE is also used on top TEE and Micro-TEE to guarantee NVM availability and integrity (in case the REE used to call TEE or Micro-TEE is corrupted)**

3. eSE integration and car communications interfaces

Today car architecture is using different communications interfaces for embedded systems based on Ethernet, CAN, LIN, FlexRay etc, and for Telematics 5G, GNSS, V2X, Wi-Fi, BT, UWB…. to define the whole car connectivity topology

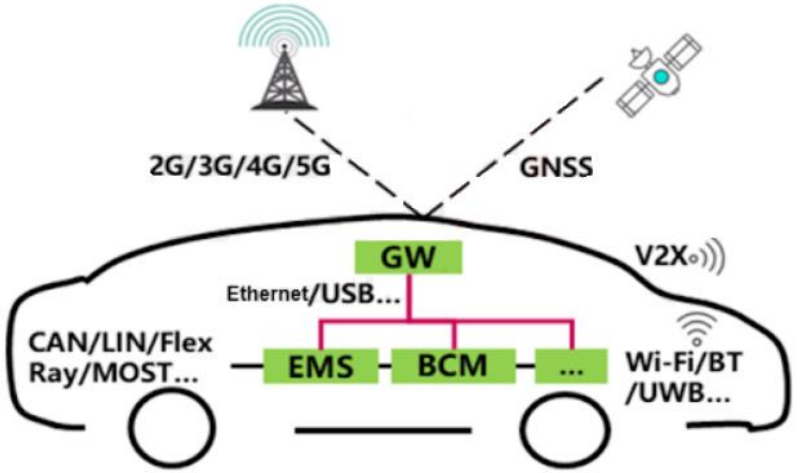
In this context, eSE is mainly used as an ECU companion chip (HSM extension), to enhance the security features capability, and is suitable anywhere in the car

eSE can be used mainly with **SPI** (GP T=1 with secure channel protocol (SCP))

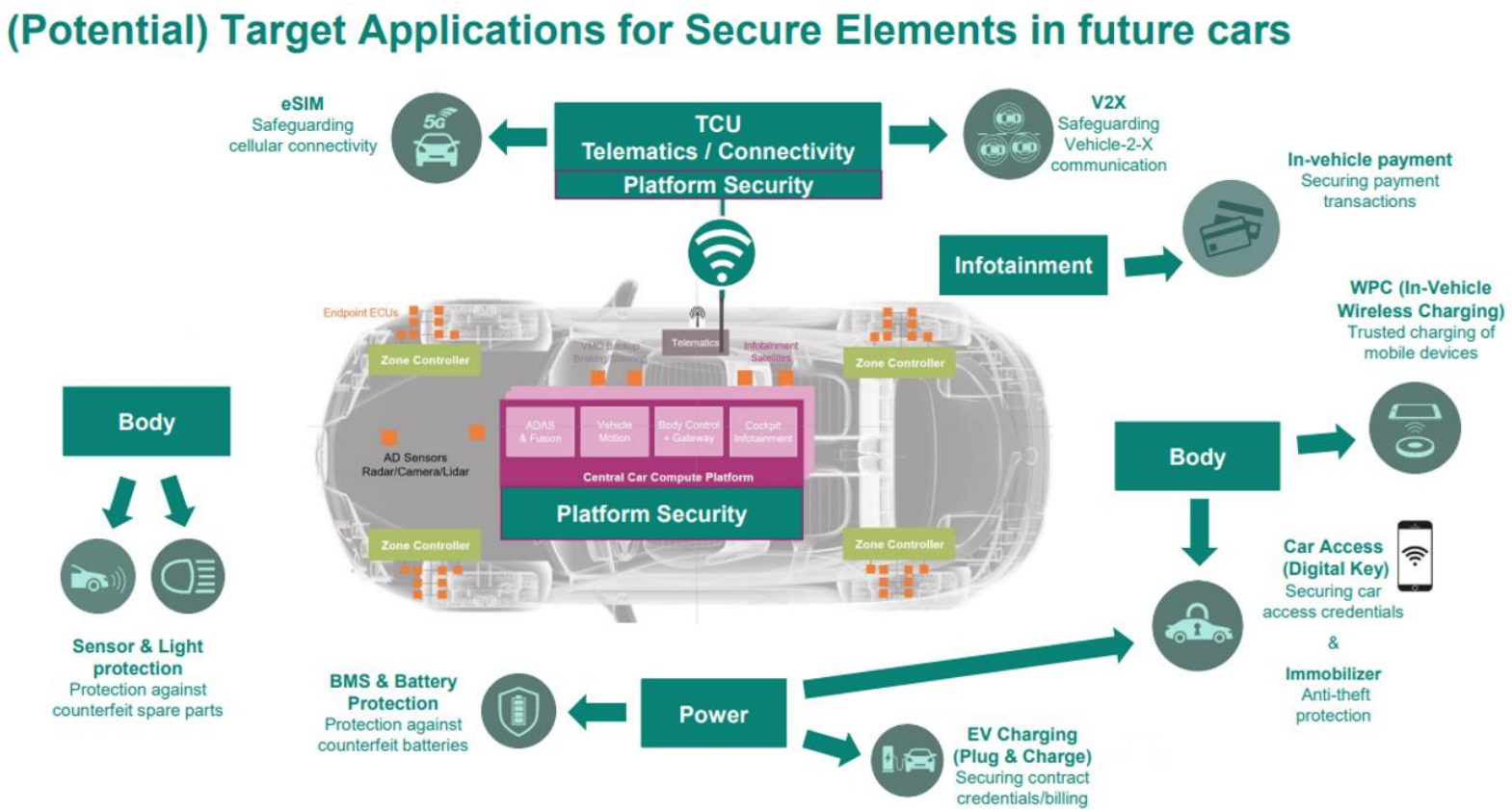


(I2C also, and I3C in the coming soon future)

For long term perspective eSE with **ethernet 10MHz to 10GHz** will open new use cases and eSE could become a central secure vault in the car architecture



3. eSE mapping use cases



IFX courtesy slide

4. Generic eSE Features and Services for Automotive

HSMs and eSE have a number of features in common: monotonic counters, entropy sources, (own) isolated memory, a dedicated MCU (this is typical for an HSM), secure storage;

What eSE offer on top of that:

- Standard features and interfaces (every newly integrated HSM mean a new development project, a clean slate start);
- Crypto-accelerators are generally the norm;
- Side-channel protections;
- Well defined and standard security assurance metrics (in this regard, HSMs tend to be black boxes);

What are the eSE features and services:

- ✓ Security Key Management
- ✓ Attestation
- ✓ Secure Boot and Root of Trust
- ✓ Cryptographic algo
- ✓ Cryptofraphic services with scalable security target for best performance/security trade-off
- ✓ PQC
- ✓ Firmware update
- ✓ Autosar classic integration

5. Java Card and Cryptographic Service Provider (CSP)

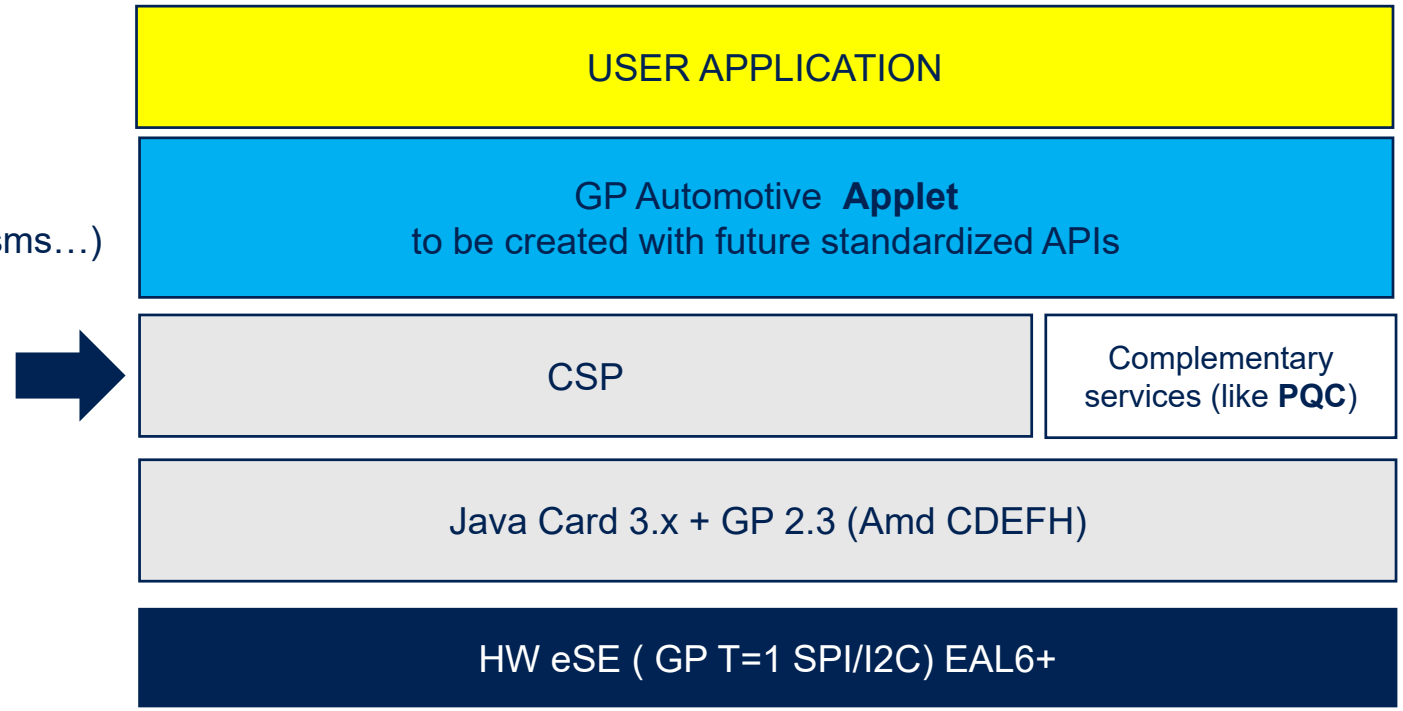
Jaca Card is the well-known solution for eSE applications can take advantage of CSP
CSP is the way to expose CSP-API that will offer some default services
Applet on top of will be Business Logic only point of view : most of security guidances are included inside CSP API

CSP advantages :

- Mostly static, few code-changes
- Requires EAL4+/VAN.5
- Ensure critical operation are secure
- Reuse existing mechanism (crypto-lib, GP mechanisms…)

CSP is offering services like :

- Securely store Keys
- Provide Cryptographic operations
- Key Management
- Full crypto Protocols (Authent, signing, etc…)
- Key-Provisioning for Protocols

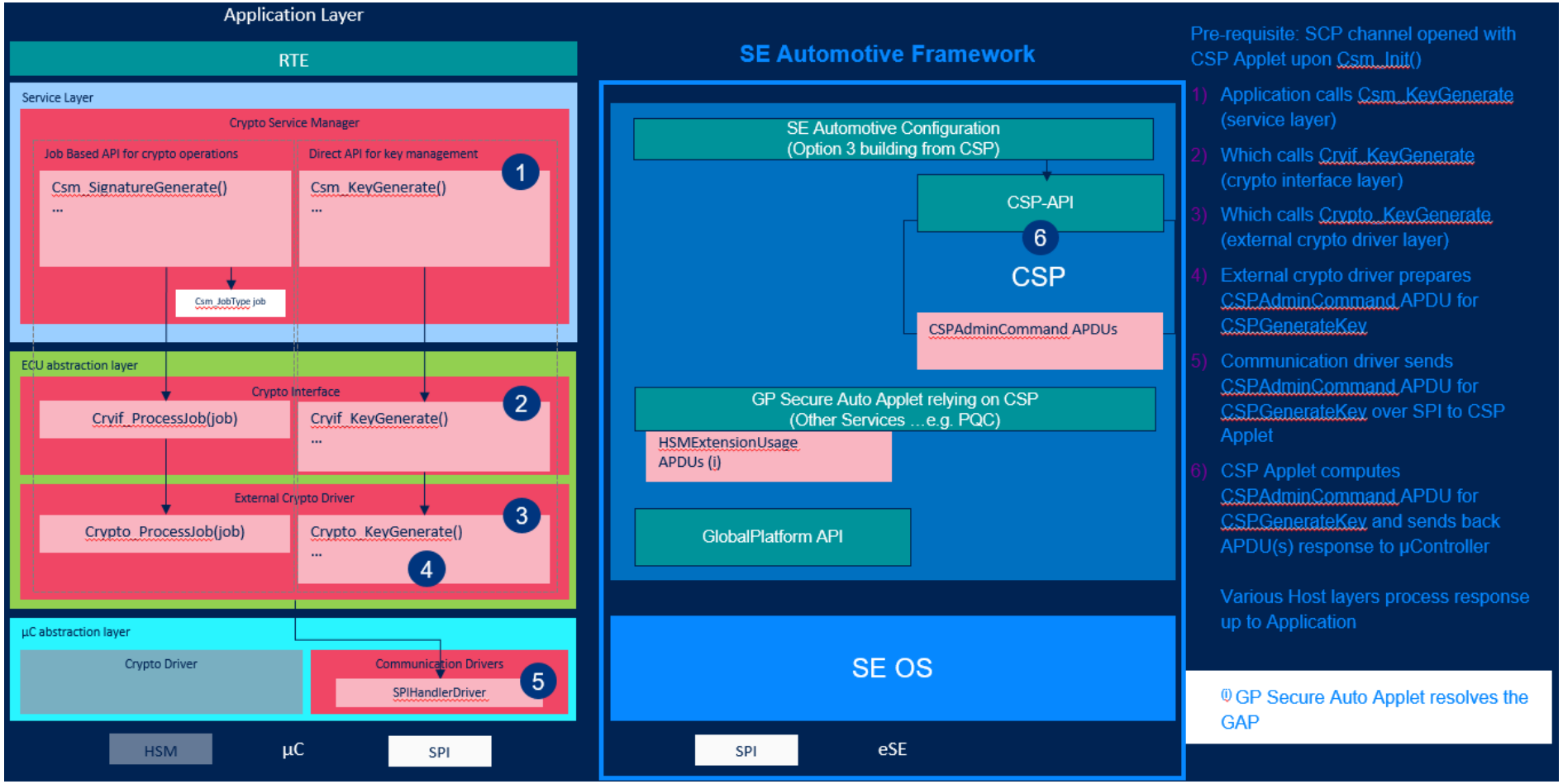


6. eUICC and Secure Application Mobile SAM for Automotive

If a car maker embeds an eCALL (emergency call), then there is something available to run CSP
By default, eUICC can enable complementary services like CSP (previously described) with GP Automotive applet on top of this CSP

In case MNO could require certified isolation, GP to consider complementary approach by using SAM (Secure Application Mobile) to improve isolation robustness

6. eSE framework with AUTOSAR stack and APDU flow



THALES courtesy slide

6. In-Vehicule eSE application (Platform Security) driven by other KPI

- **In-Vehicle eSE application driven by cryptography efficiency**
  - SW countermeasure management
  - Security point2point with symmetric approach
  - Security guidance, security maintenance, and field update

- **In-Vehicle eSE application driven by PQC**
  - Private key management
  - Execution time constraint

- **In-Vehicle eSE application driven by security new functions**
  - New security API creation
  - Security customization capability

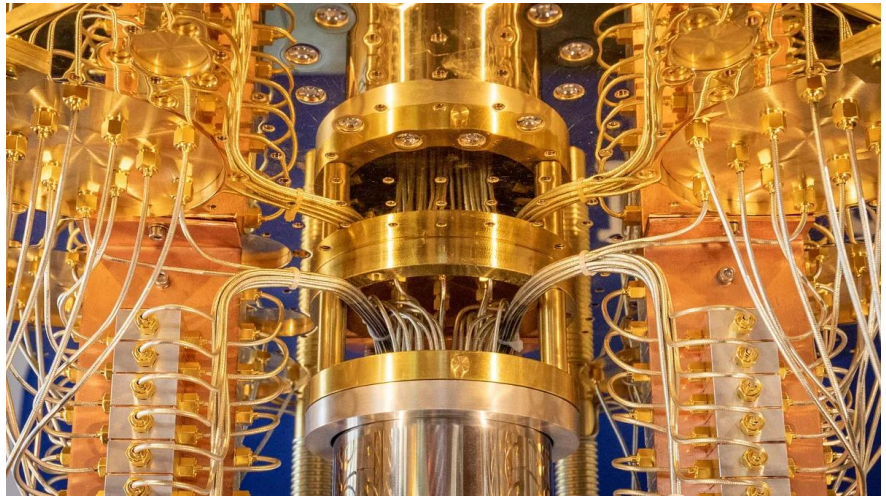
- **In-Vehicle eSE application driven by power efficiency**
  - Efficient very low power mode

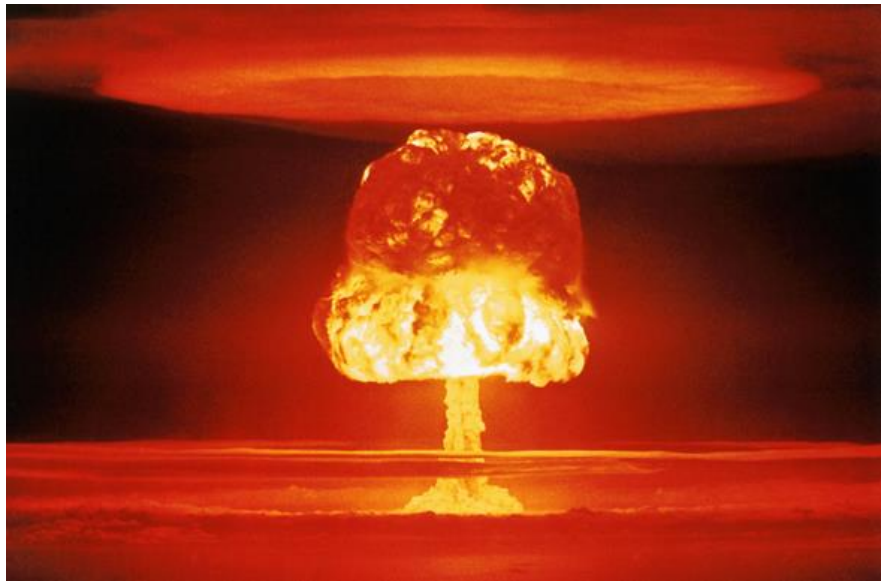
- **In-Vehicle eSE application driven by communication interface**
  - SPI/I²C and I3C to come
  - Next steps : Ethernet 10MHZ-100MHz (Zonal) and 1GHz-10GHz (Head Unit)

Open questions

Global Platform™

PQC BKP SLIDES





- Asymmetric Cryptography: **will be broken** (Shor's algorithm)
  - Signature: RSA, ECC
  - Key Exchange: DH, ECDH, ECDHE..
- Symmetric Cryptography: (Grover's algorithm)
  - Key strength divided by 2
  - AES128/192 will be weakened
  - AES-256 ok (256 →128 bits key strength)
- SHA2-256/384/512 & SHA3 not impacted

- Crypto Armaggedon planned for …2035-2050
  - Quantum Computer feasibility is difficult to predict
  - Worst case scenario: Quantum World in 10-15 years
  - $10^4/10^7$ logical/physical qubits required to break RSA2048
  - Google Willow (9/Dec/24): 105 logical qubits
- Migration must be anticipated for assets vulnerable to attacks **«store now, decrypt later »**
- NIST launched a contest for Post Quantum Crypto
  - Call for papers Dec/16 + Submission deadlines: Nov/17
  - Jul/22: 4 candidates for standardization after 4 rounds
  - Aug/24: 3 standard released

Use cases and threat answer

PQC algorithm	Replacing	Use Case	Threat
LMS	RSA, ECC	SW/FW signature	Firmware authenticity
ML-KEM	ECDH, ECDHE	Key encryption	Store now, decrypt later
ML-DSA	RSA, ECC	Signature	Long term PKI certificate

Quantum resistant authentication protocols can also be achieved with AES keys (with longer key lengths) and pre-shared secrets.

Hybrid protocols can be implemented with classical and/or PQ cryptography

- AND: both classical & PQ cryptography are combined to anticipate any future vulnerability that would affect only one
- OR: ML-KEM could be used for key encryption in combination with RSA or ECC for (short-term) authentication

- **eSE attached to HSM to manage PQC challenges** :
  - Symmetric crypto – PQC resistant AES-256
  - LMS support (based on SHA-256)
  - Key Encryption – ML-KEM
    - All key sizes to be supported (ML-KEM 512/768/1024)
    - Limited memory footprint
    - Performances aligned with good user experience
  - Signature – ML-DSA
    - All key sizes to be supported(ML-DSA 44/65/87)
    - Significant memory footprint
    - Major key storage dedicated footprint
    - Signature generation timing is by design “variable” (average performance is ok)

Status

- There is a global analysis that HSM landscape is too fragmented …

- When using Autosar CSM APIs, the service executed can be done among very different setup (HSM, CPU, HW accelerator, Hybrid implementation….);
(To help regression, sometimes SW usage is used despite HW accelerator)
In this case how to evaluate the associated robustness
when do not know how it is executed from low level point of view ?
And side effect, what could be the associated SESIP level that is achieved ?

- As a conclusion, CSM API is a host frozen API; from implementation point of view, different flavor are possible (with different associated robustness…..)

Global Platform®

Securing the digital future

Membership

membership@globalplatform.org

PR Contact

pressoffice@globalplatform.org

Questions

secretariat@globalplatform.org

→ globalplatform.org