life.augmented

Global Platform
GP Automotive JVC Applet

Laurent TABARIES

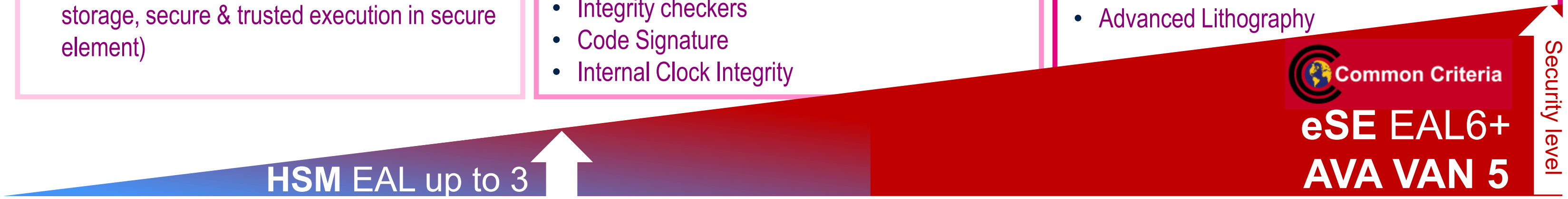
STMicroelectronics

December 2024

How to classify security robustness?

A complete set of Hardware & Software countermeasures + certification

	Software attack	Board-level attack	Silicon-level attack
Major attacks	• Network protocols weakness (weak ciphers, short keys,…) • Flaws in software design / implementation, buffer overflows • Debug interfaces, gaining admin rights	• SPA / DPA Power analysis, emission analysis, timing analysis • Fault injection: glitches, laser, light, UV, X-rays, Electro-Magnetic • Memory probing	• Device delayering, circuit reverse engineering, micro-probing • Fault injection: Focused Ion Beam • Advanced microscopy
Countermeasures *Hardware & Software*	• No external debug interface • Hardware secure crypto fast computing • Enhanced security of MCU with physical isolation of security toolbox (secure key storage, secure & trusted execution in secure element)	• Randomization • Secured crypto-engines • Design Flow • Power regulation • Environment Sensors • Integrity checkers • Code Signature • Internal Clock Integrity • OS features (MPU) • Jittered Clocks • Data whitening	• Physical Shield • Lock-step EDC • Glue Logic Layout • Bus & Memory Scrambling • Bus & Memory Encryption • Anti-reverse • Advanced Lithography



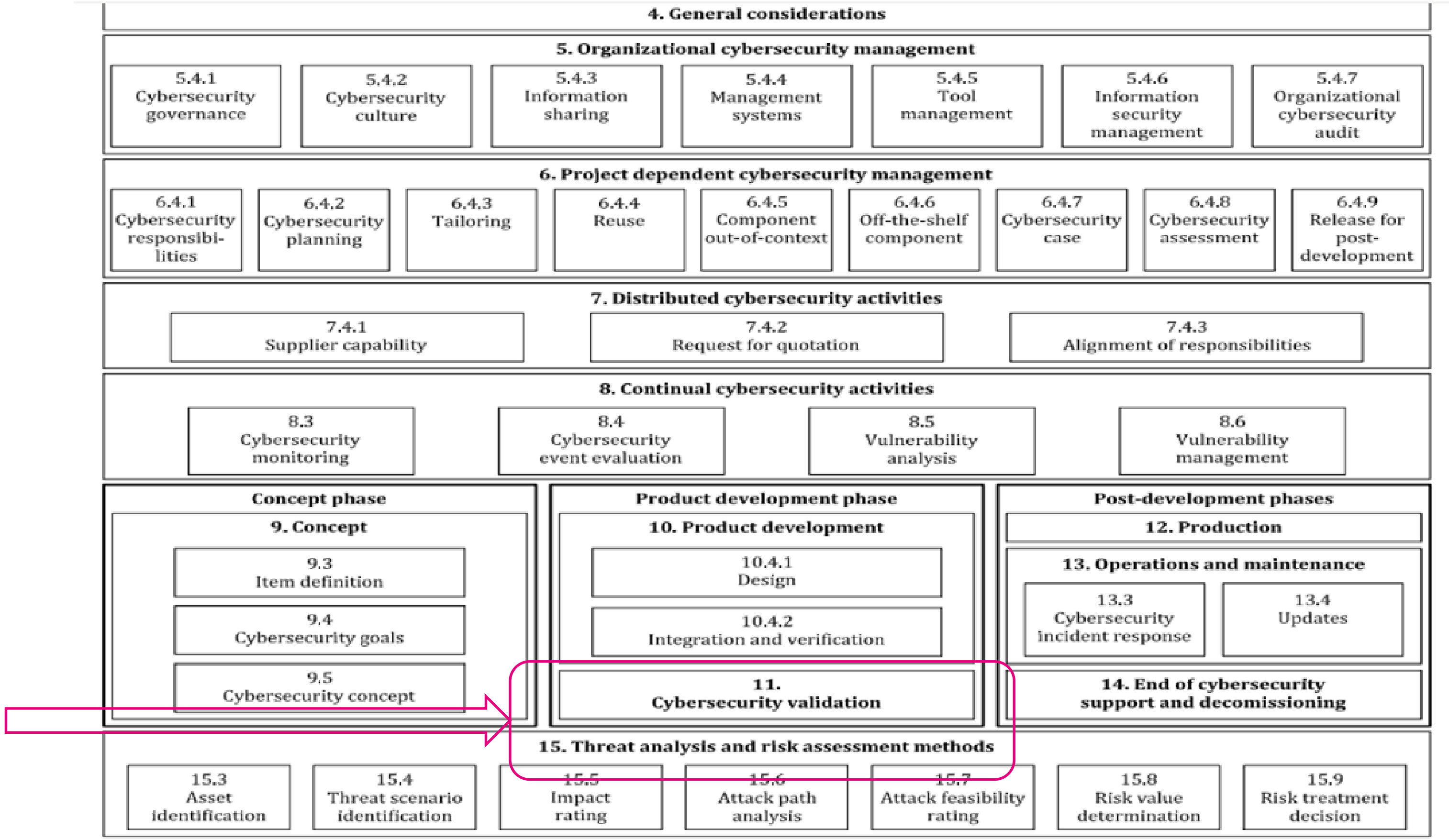
~SESIP 2 or 3

Ex: Side channel 60 to 5k curves robustness
=> hacker in a garage

~SESIP 4 or 5

Ex: Side channel >1M curves robustness
=> BSI or expert lab

ISO21434 and TARA analysis : where is executed my function?



4. General considerations

5. Organizational cybersecurity management
- 5.4.1 Cybersecurity governance
- 5.4.2 Cybersecurity culture
- 5.4.3 Information sharing
- 5.4.4 Management systems
- 5.4.5 Tool management
- 5.4.6 Information security management
- 5.4.7 Organizational cybersecurity audit

6. Project dependent cybersecurity management
- 6.4.1 Cybersecurity responsibilities
- 6.4.2 Cybersecurity planning
- 6.4.3 Tailoring
- 6.4.4 Reuse
- 6.4.5 Component out-of-context
- 6.4.6 Off-the-shelf component
- 6.4.7 Cybersecurity case
- 6.4.8 Cybersecurity assessment
- 6.4.9 Release for post-development

7. Distributed cybersecurity activities
- 7.4.1 Supplier capability
- 7.4.2 Request for quotation
- 7.4.3 Alignment of responsibilities

8. Continual cybersecurity activities
- 8.3 Cybersecurity monitoring
- 8.4 Cybersecurity event evaluation
- 8.5 Vulnerability analysis
- 8.6 Vulnerability management

Concept phase
- 9. Concept
  - 9.3 Item definition
  - 9.4 Cybersecurity goals
  - 9.5 Cybersecurity concept

Product development phase
- 10. Product development
  - 10.4.1 Design
  - 10.4.2 Integration and verification
- 11. Cybersecurity validation

Post-development phases
- 12. Production
- 13. Operations and maintenance
  - 13.3 Cybersecurity incident response
  - 13.4 Updates
- 14. End of cybersecurity support and decomissioning

15. Threat analysis and risk assessment methods
- 15.3 Asset identification
- 15.4 Threat scenario identification
- 15.5 Impact rating
- 15.6 Attack path analysis
- 15.7 Attack feasibility rating
- 15.8 Risk value determination
- 15.9 Risk treatment decision

How is it possible to cope with security functions execution place uncertainty: HSM HW or CPU ?

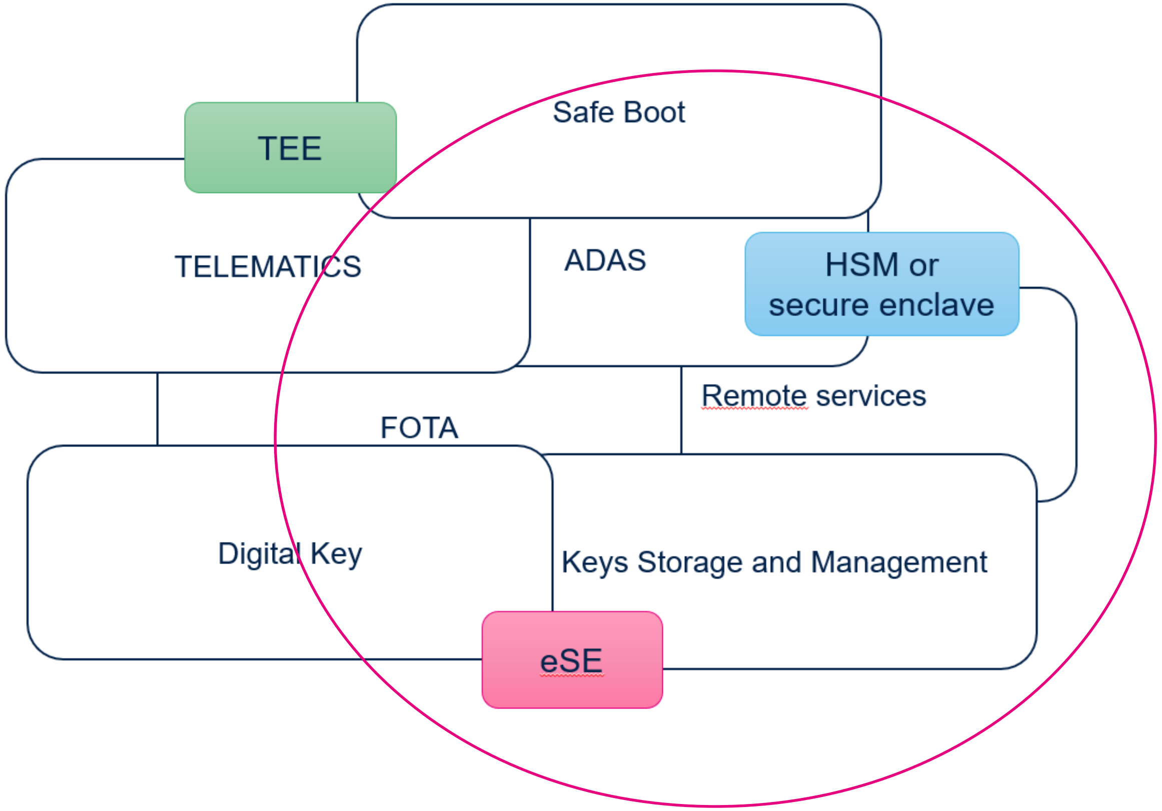
There is a fundamental need to identify the real level of security robustness needed to be reach

Which functions have to be **bake or harden** from security point of view ?

For exemple, could you accept an ECDSA-256 signature generation perfomed on a standard CPU (without demonstrated robustness) ?

life.augmented

“Automotive security” : a galaxy of different use cases



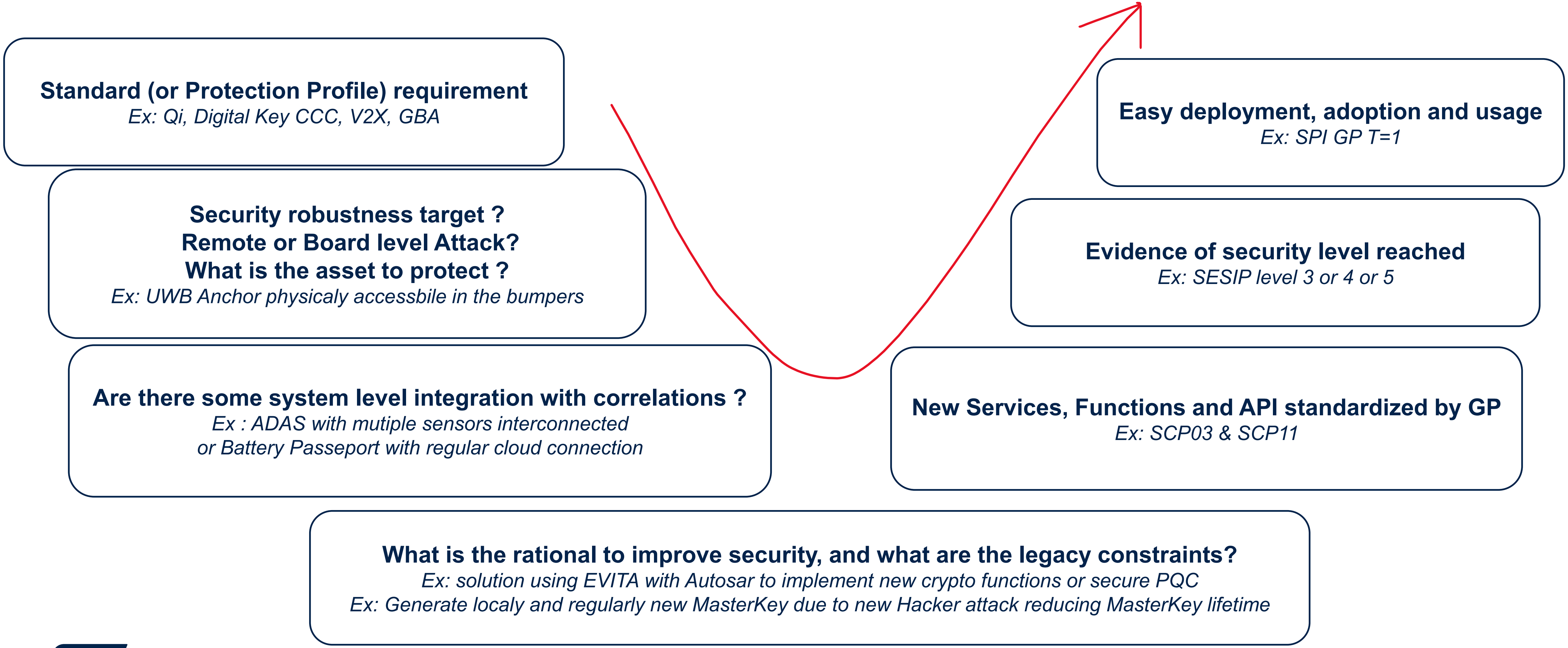
Many use cases with different expectations…… **BUT**
SW vehicle must become a reality without security tradeoff

Focusing on MCU, there are regular complains about how to improve today solution to manage all the security cases because of:

- *lack of crypto field solution to be enhanced, updated for the next decade*
- *lack of customization/personalization capabilities*
- *difficulty to match supported features with targeted security goals*

For MCU point of view, HSM inside Autosar using CSM APIs is the security backbone, and there is a demand to fill the gap, to enhance it, but not to replace it.

Use Case "security needs" driven by



Standard (or Protection Profile) requirement
Ex: Qi, Digital Key CCC, V2X, GBA

Security robustness target ?
Remote or Board level Attack?
What is the asset to protect ?
Ex: UWB Anchor physicaly accessbile in the bumpers

Are there some system level integration with correlations ?
Ex : ADAS with mutiple sensors interconnected
or Battery Passeport with regular cloud connection

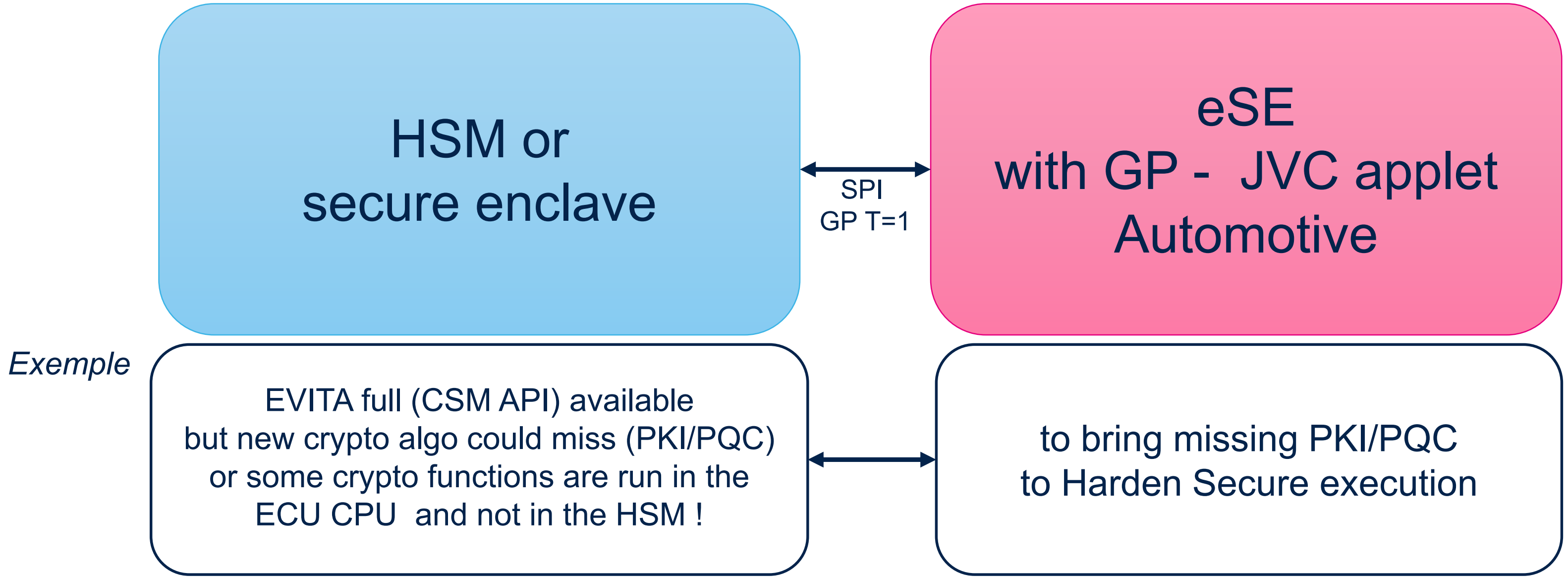
What is the rational to improve security, and what are the legacy constraints?
Ex: solution using EVITA with Autosar to implement new crypto functions or secure PQC
Ex: Generate localy and regularly new MasterKey due to new Hacker attack reducing MasterKey lifetime

New Services, Functions and API standardized by GP
Ex: SCP03 & SCP11

Evidence of security level reached
Ex: SESIP level 3 or 4 or 5

Easy deployment, adoption and usage
Ex: SPI GP T=1

eSE on top of HSM (and not to replace HSM) !



HSM or secure enclave

SPI
GP T=1

eSE
with GP - JVC applet
Automotive

Exemple

EVITA full (CSM API) available
but new crypto algo could miss (PKI/PQC)
or some crypto functions are run in the
ECU CPU and not in the HSM !

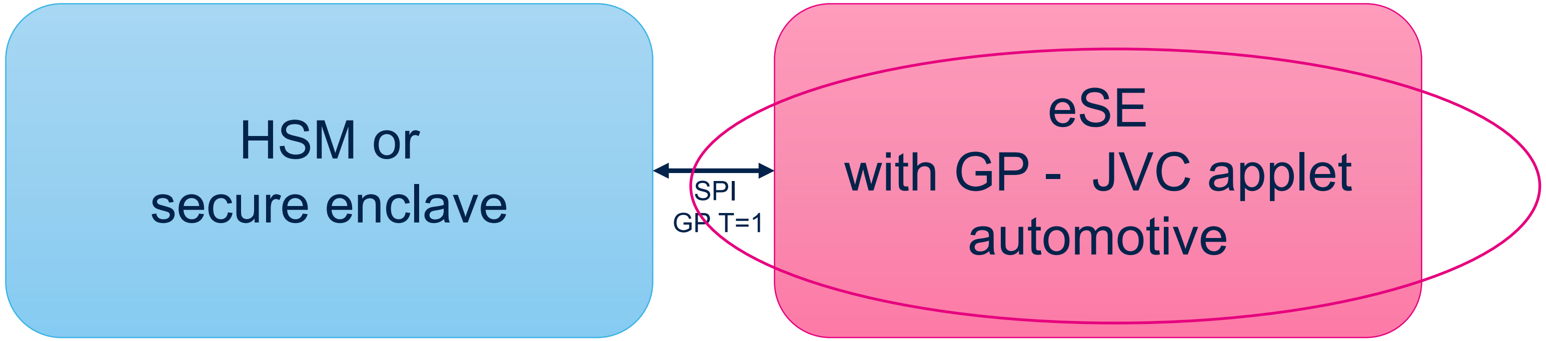
to bring missing PKI/PQC
to Harden Secure execution

Because today mainstream Automotive MCU is HSM based with Autosar,
Proposal is to have an « HSM augmented by an eSE with services based on standardized GP-APIs »
Such services will be based on GP-JVC applet to be run inside an eSE connected on top of legacy HSM

This proposal could enhance today solution with complementary APIs:

- Standardized
- Flexible
- Level of security robustness guaranteed

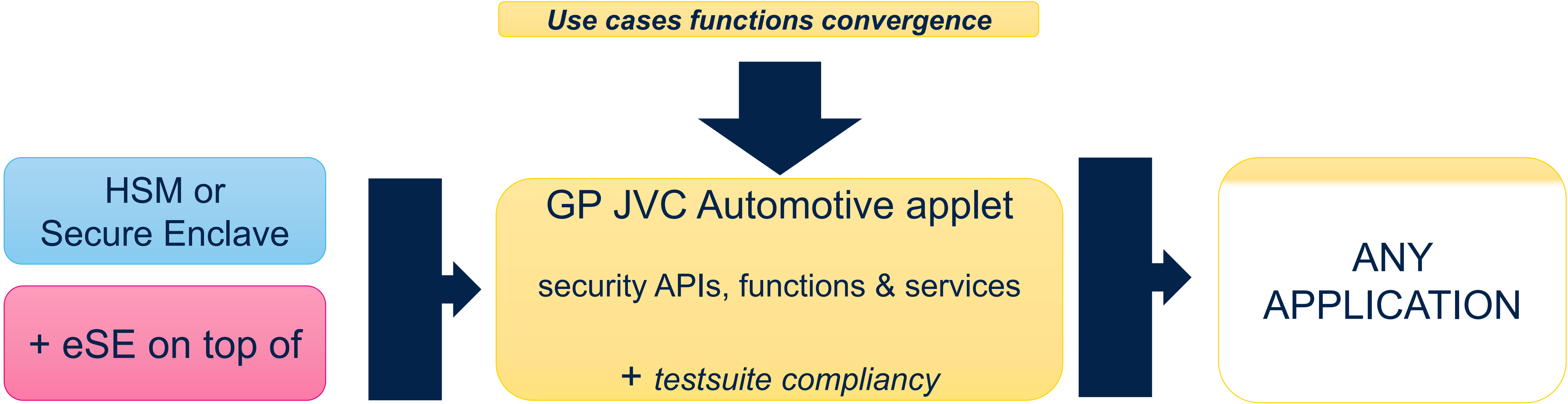
Why JVC Applet Automotive ?



Because already adopted everywhere, ruling most of everyday life use cases (Banking, ID, Telecom, Wallets, …)

- Agnotsic from any silicon vendor; just rely on top of JVC 3.x with standardized APIs
- Flexible, easy to patch or to personalize
- Customization remains possible
- Global solution (HW+SW) can be certified (composite certification, and protection profile reference is also possible)
- Code of the GP JVC Applet Automotive to be given as a reference code
- Testsuite for compliancy can be managed to guarantee good intgeration (free JVC simulator is available like JCARDSIM)

GP Automotive security convergence for MCU



Use cases functions convergence

HSM or
Secure Enclave

+ eSE on top of

GP JVC Automotive applet

security APIs, functions & services

+ *testsuite compliancy*

ANY
APPLICATION

HSM to remain the solution when priority is given to performances
eSE on top of HSM (with GP JVC Automotive Applet)
as a proxy to extend HSM capabilities

GP JVC Applet Automotive in 3 steps

To identify and list expected APIs, functions and services :

- RoT
- Key Generation, Derivation and Key Management
- Crypto, MAC, Hash, PQC ….
- Remote services
- Data personalization
- Etc ….

To formalize a GP specification

setup early JVC Applet (to rely on top of default JVC 3.x)
with incremental approach based on regular field feedbacks

To implement a GP Automotive JVC Applet POC

provide integration guide and metrics for performances and security robustness assesment