life.augmented

Global Platform ATF
GP JVC Applet for Automotive

STMicroelectronics

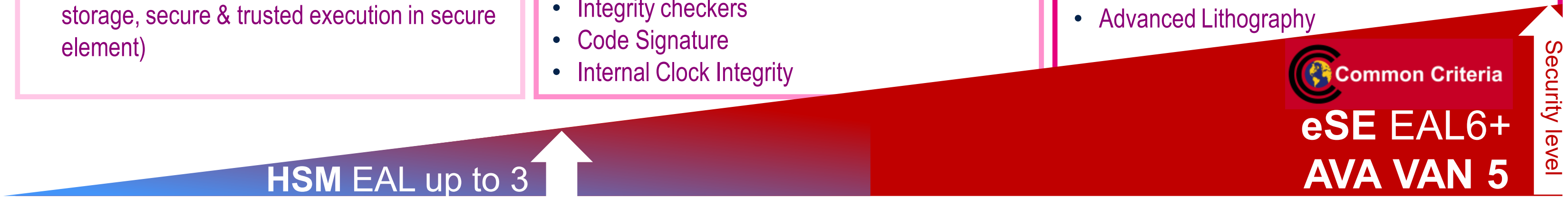
3rd of April 2025

ST Restricted

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



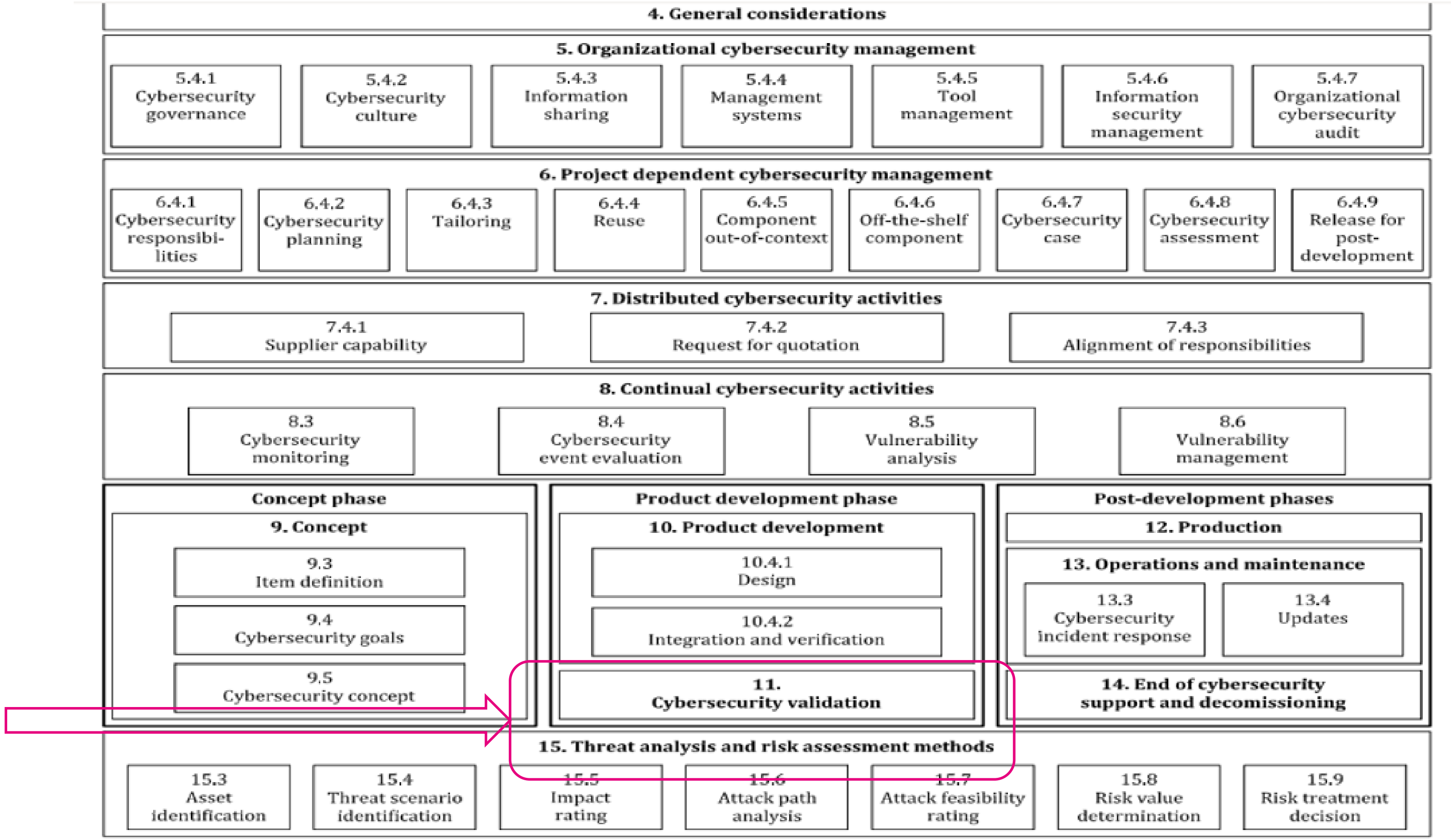
~SESIP 2 or 3

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

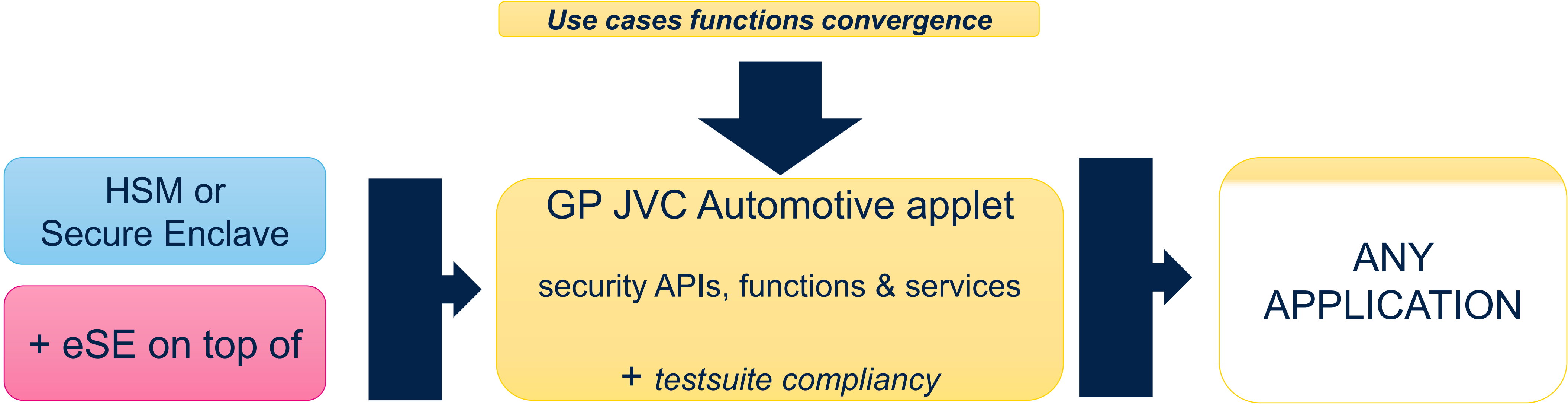
How is it possible to cope with security functions execution place uncertainty: HSM HW or CPU ?

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) ?

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 Automotive JVC Applet

Automotive ECUs are more and more challenged to address risks with higher level of security robustness
with sometimes unclear visibility about strategy to setup and how to maintain it “state of the art” over a decade

ECUs can rely on AUTOSAR CSM APIs to answer most of cybersecurity challenges
BUT higher level of security (>SESIP 3 or EAL4+/5+) is sometimes required

eSE must be understood as a **complementary solution on top of ECU HSM used in AUTOSAR with CSM APIs**
Any customer who wants to keep going using AUTOSAR for practical and legacy reason
and just delegate specific tasks to eSE as a companion chip.

eSE standardized APIs is likely to address generic services :

- Key management
- Secure Storage
- Certificates management
- Complementary crypto services (if some could miss, or if some could require higher security)
- Remote provisioning
- Possible ROT improvement scheme
- Capability to maintain state of the art security robustness on the field

GP Automotive JVC Applet

Many cars are already equipped at least with on eSE for DigitalKey,
and most the eSE used for DK could propose additional room for complementary use cases:

- Qi
- Car BlackBox
- Specific parts serial number check
- Specifics car settings check
- Driver Biometrics credentials management
- Car driver preference settings record
- User applicative and dynamic rights management

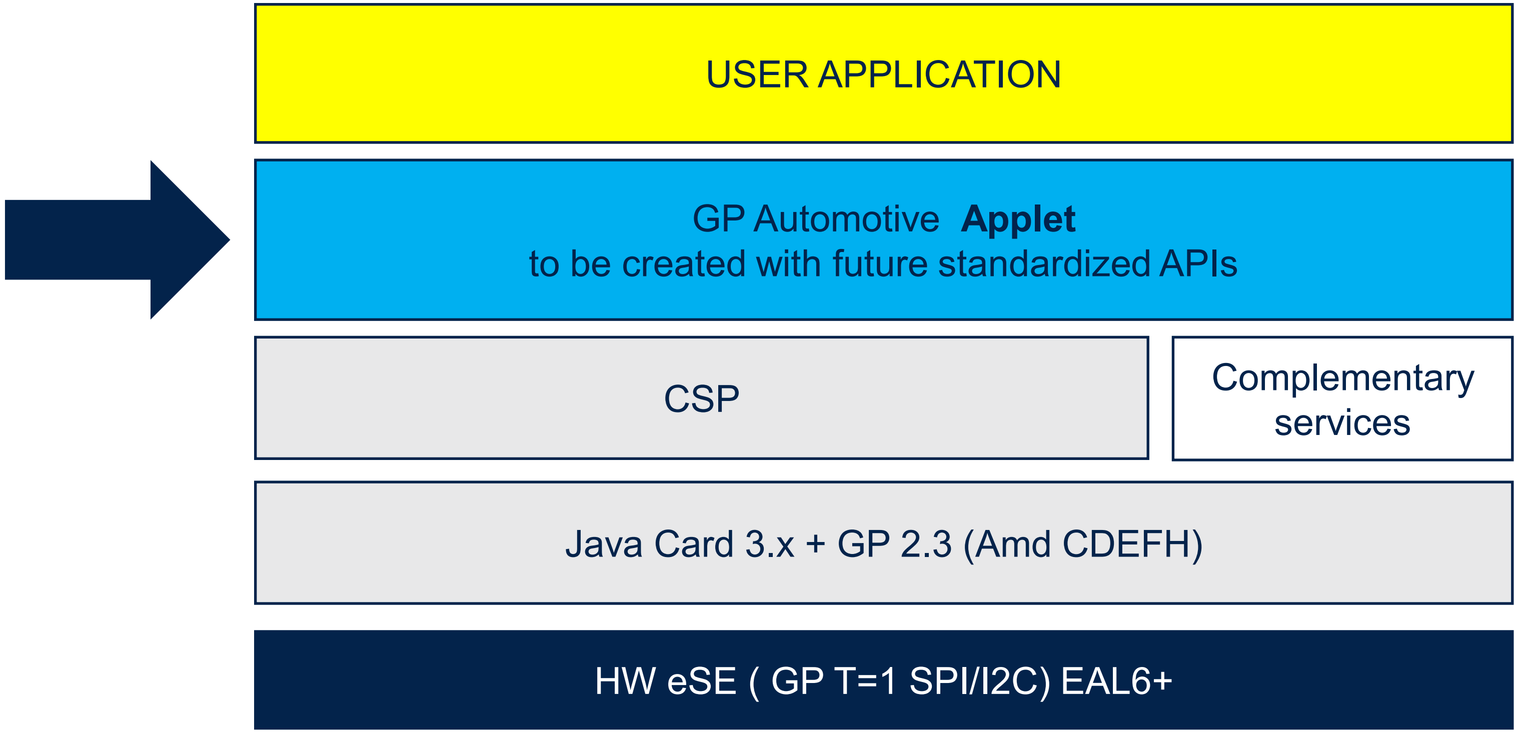
=> All these use cases can be addressed by classic HSM integration approach ….
But could take benefit of eSE with GP JVC applet to reinforce it

GP Automotive JVC Applet

Why does not already exist today ?

Today eSE are mainly used with **proprietary solutions** that is a **mainstream adoption drawback**

So even if some eSE are used for a specific use cases (Digital Key, Qi …) It is not easy to extend it for generic services, especially for AUTOSAR
GP could be the way to develop such “Applet” offering a generic a set of standardized APIs to be run on top of an “eSE with JVC OS”


USER APPLICATION

GP Automotive **Applet**
to be created with future standardized APIs

CSP

Complementary services

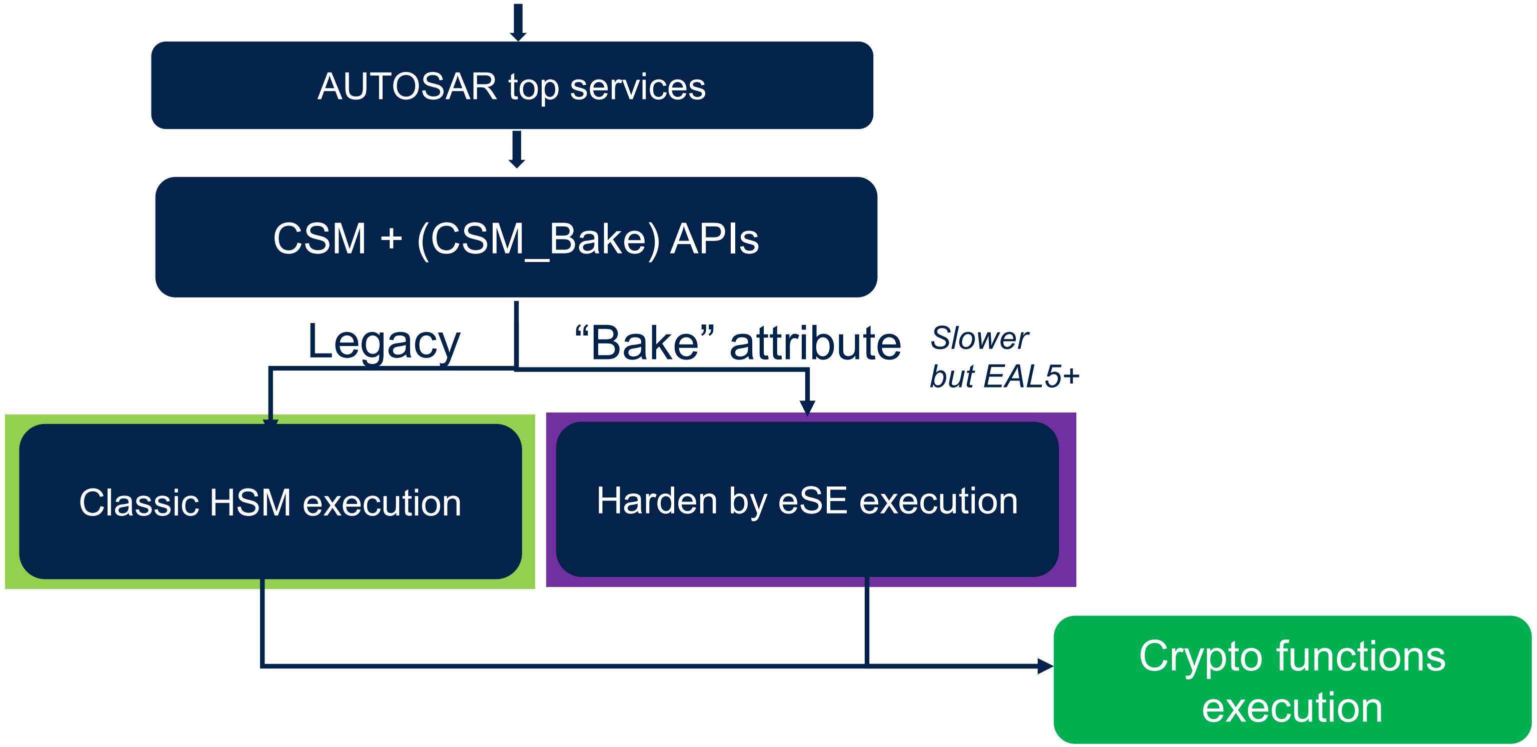
Java Card 3.x + GP 2.3 (Amd CDEFH)

HW eSE (GP T=1 SPI/I2C) EAL6+

Next possible step ?

Valuable solution having CSM APIs + CSM APIs “bake” ?

Mainstream APIs to keep on going with today CMS APIs executed by HSM
BUT…sometimes TARA could identify some potential opportunities to reinforce the security (or to use eSE)
eSE could propose on top of HSM same APIs but more “robust” from security point of view.
Having inside AUTOSAR “CSM APIs ” (executed by HSM) and “CSM_bake APIs” (executed by eSE) could be valuable



Autosar CSM-extended HSM + eSE

**Improve AUTOSAR CSM APIs “used today” using HSM
with extended and harden capability (from security robustness point of view)
to address all the use cases and security robustness challenges**

BACKUP SLIDES

life.augmented

GP Automotive JVC Applet

Why JavaCard (JVC) and Cryptographic Service Provider (CSP) ?

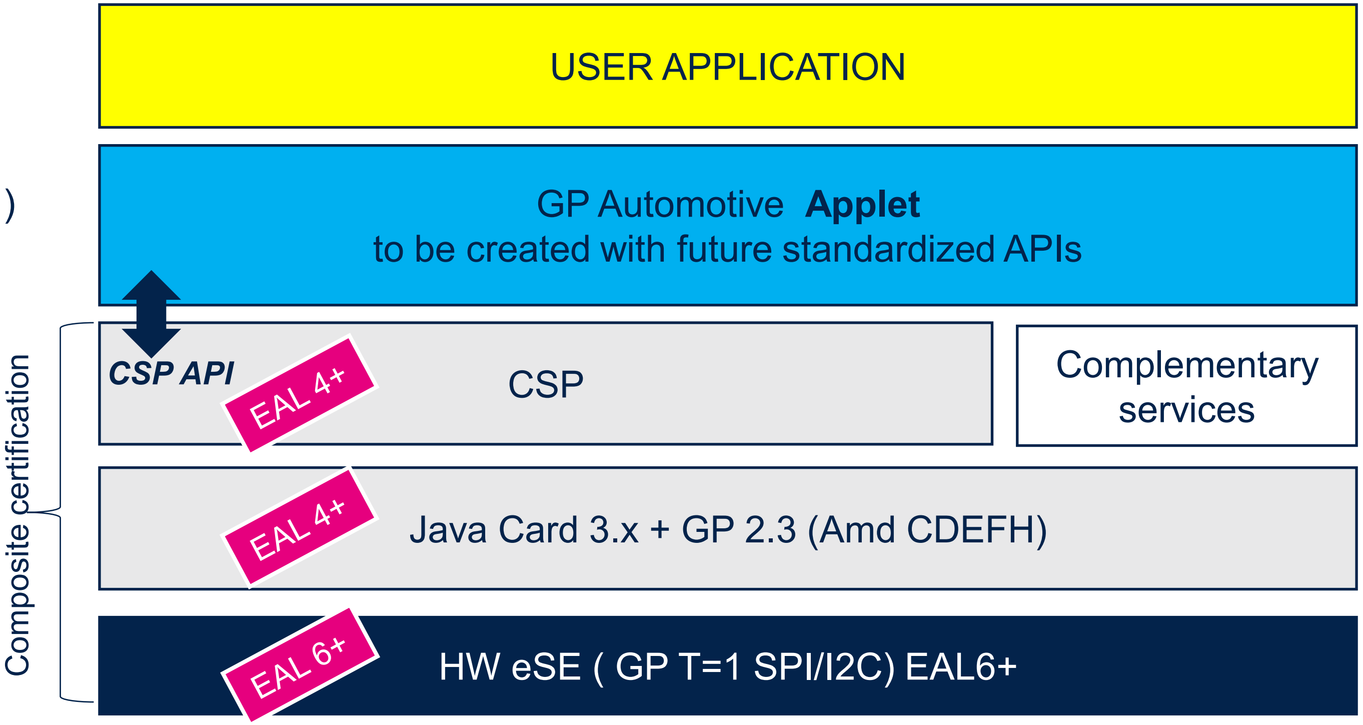
JVC is the well-known solution for eSE applications, and It can take also advantage of CSP
CSP (defined by the BSI) is the way to expose CSP-API that will offer some default useful services
“Applet on top of” will be “Business Logic only” : most of security guidance are included inside CSP API
CSP prevents applet to be certified for each specific platform type and version they will be used on

CSP advantages :

- Mostly static, few code-changes
- Requires EAL4+/VAN.5
- Ensure critical operation are secure
- Reuse existing mechanism (crypto-lib, GP mechanisms…)
- Manage applications having different roles and access rules

CSP is offering services like :

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



Our technology starts with You

life.augmented