

Extension of HSM capabilities with Secure Elements

Laurence Bringer
Yves Le Bobinnec
Cybersecurity Vehicle Forum
Berlin - December 4, 2024

www.thalesgroup.com





Laurence Bringer

Technical Director, Smart Mobility

**Standardization Expert and
Director at Car Connectivity Consortium**



Yves Le Bobinnec

Cyber Solution Architect, Smart Mobility

Thales Digital Identity & Security in Automotive Market

Connectivity

Car makers and automotive suppliers trust Thales to manage worldwide cellular connectivity

Cybersecurity

Thales designs, builds and operates cybersecurity solutions and services to protect sensitive assets of the automotive industry players

Vehicles Connected Services



Software Updates



Vehicle Management



Mobility



Electrification

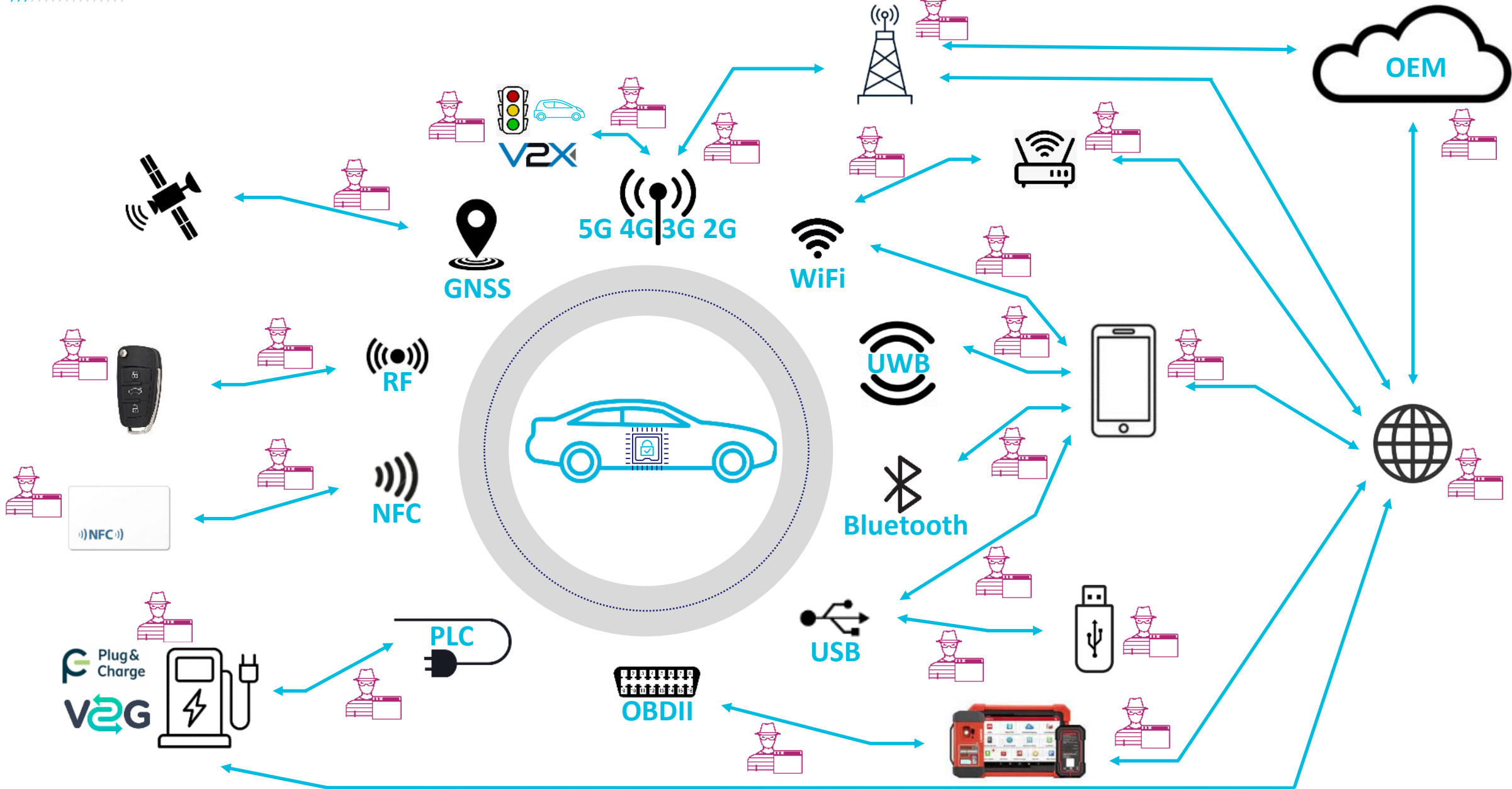


Maintenance



ADAS

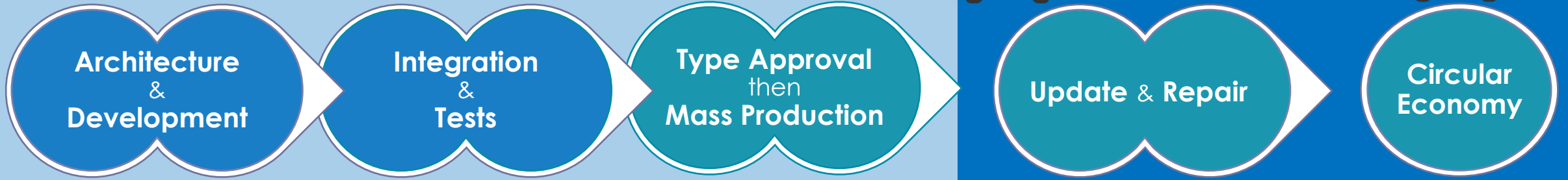




Many cyber challenges throughout the vehicle life cycle



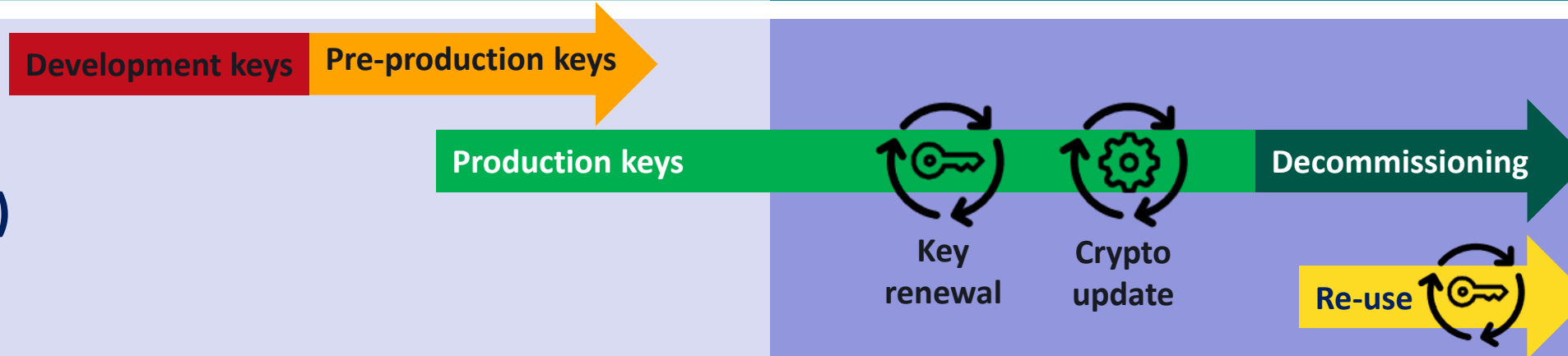
Secured by design in the automotive life cycle



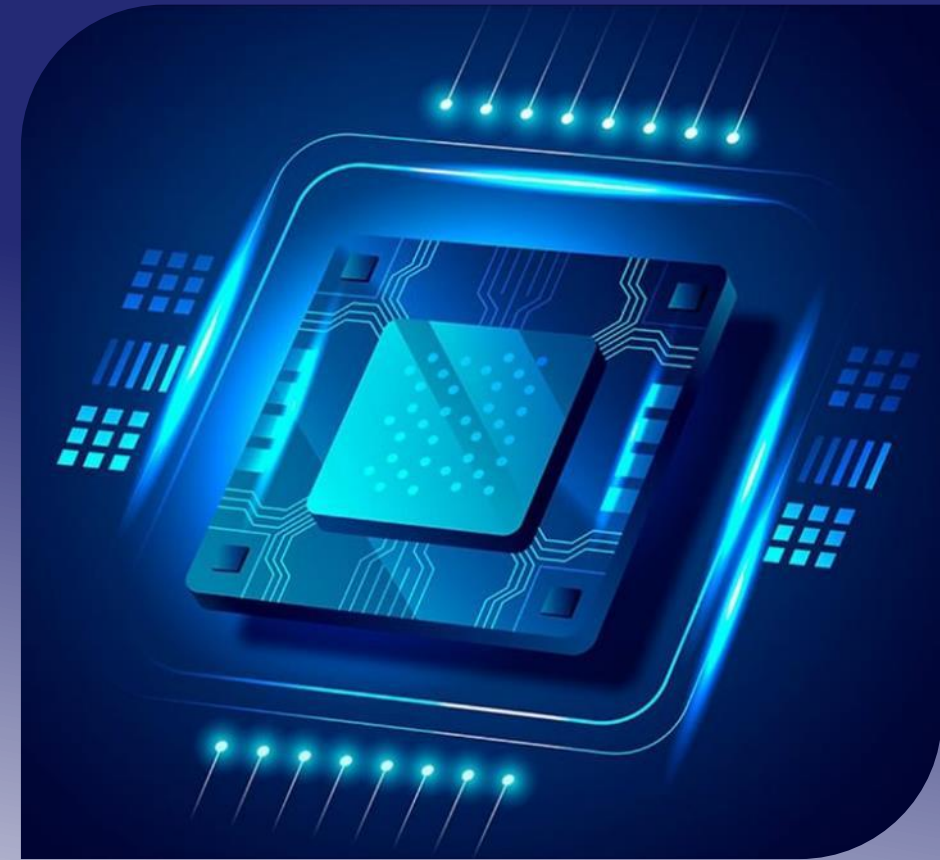
Progressive Activation of Cyber mechanisms



Impacts to Key Management (Crypto)



Secure Element is ideal to support and answer these challenges



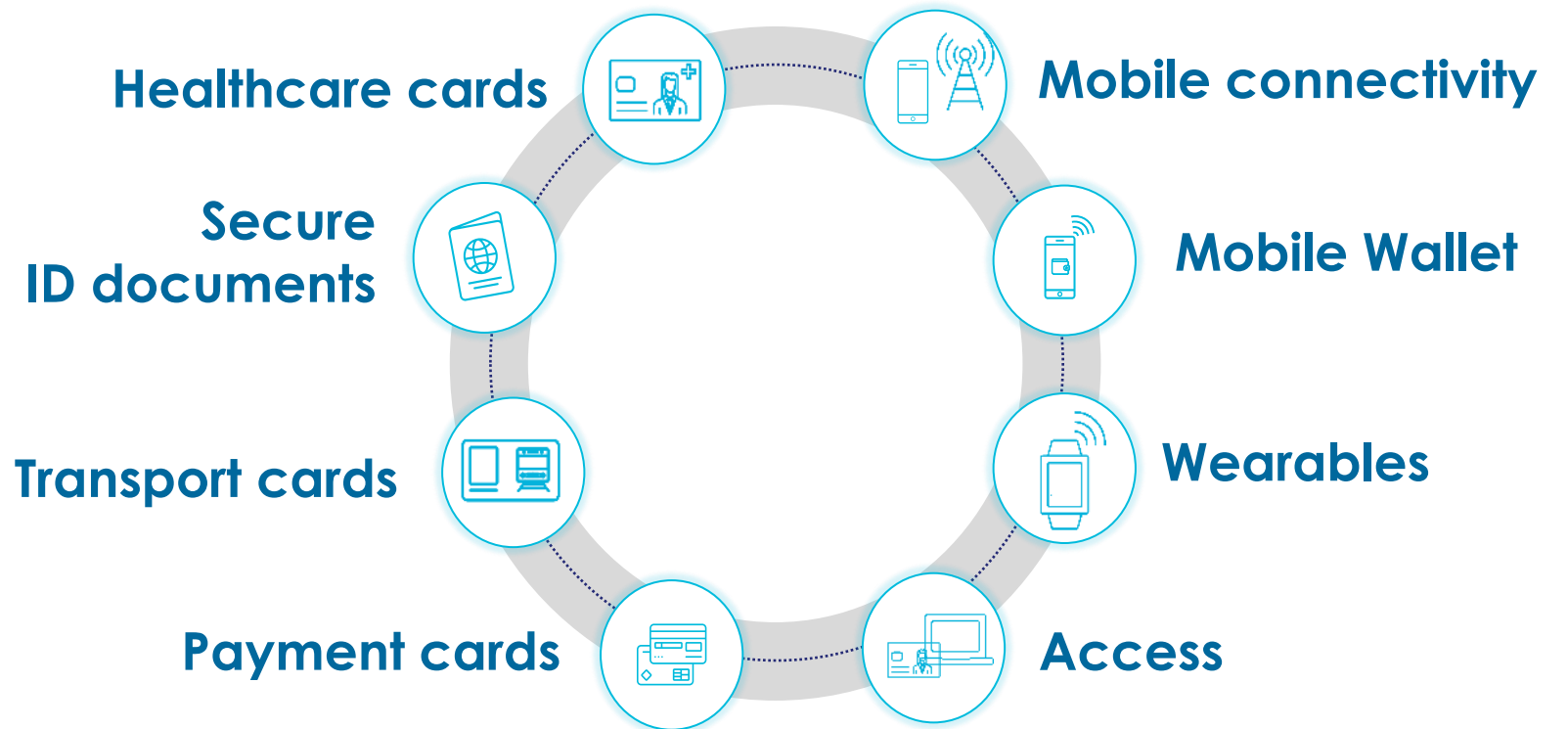
What is a Secure Element?



Present in your daily life for decades



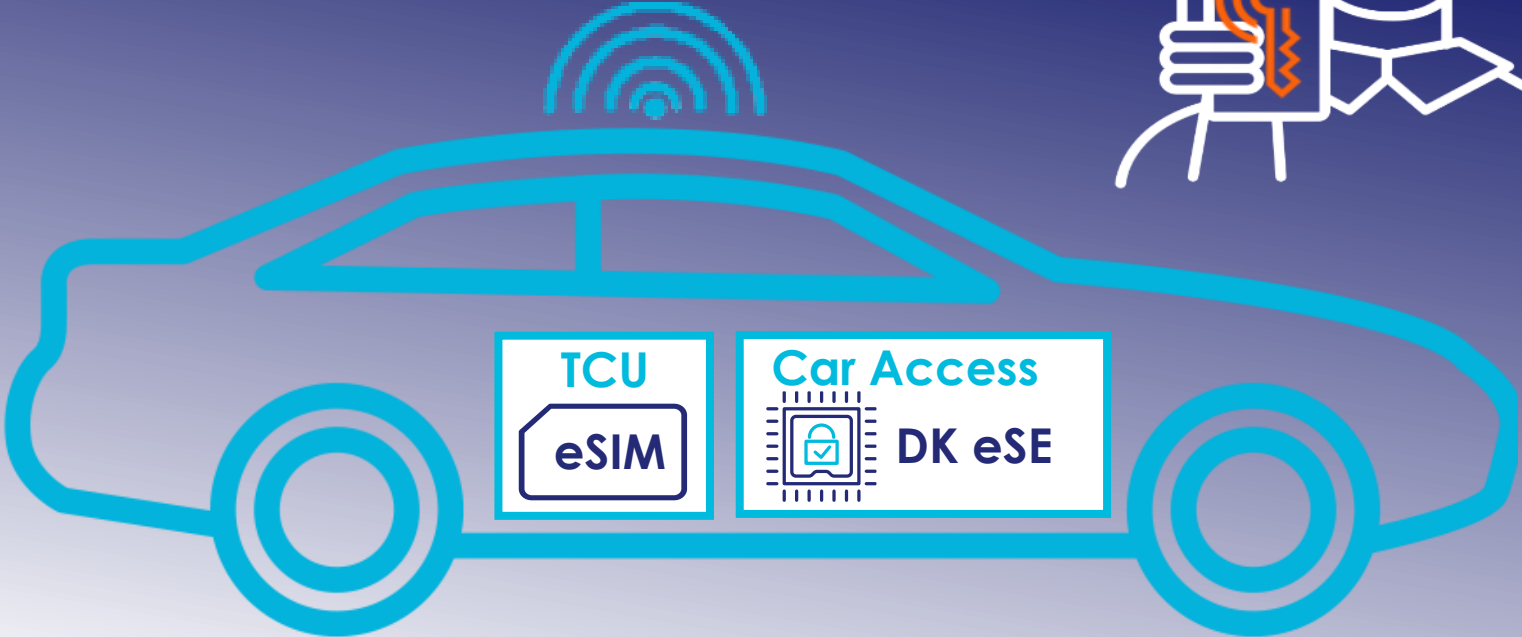
Source GlobalPlatform



Deployed in all connected vehicles



Car
Connectivity
Consortium
Digital Key



Going deeper into the usage of Secure Elements



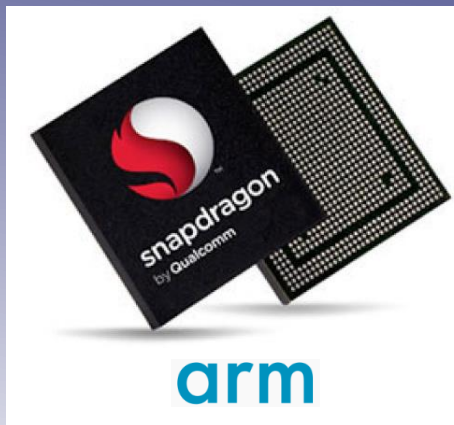


μProcessor A-Class (TEE, TZ)



Examples:

- ▶ Telematic
- ▶ Central HPC
- ▶ Infotainment
- ▶ ADAS Supervisor
- ▶ ...



μController (HSM)



Examples:

- ▶ VHL Access
- ▶ VHL Health
- ▶ EV Charging
- ▶ Anti Chip Tuning
- ▶ Zonal Controller
- ▶ ...

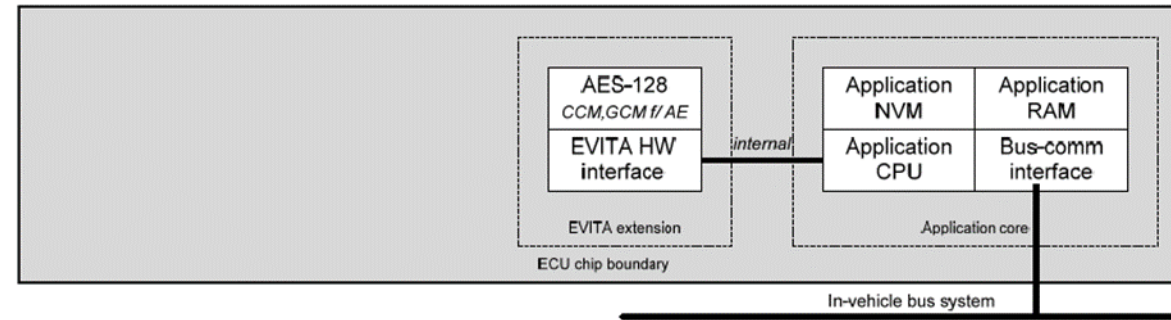


EVITA project – HSM Version



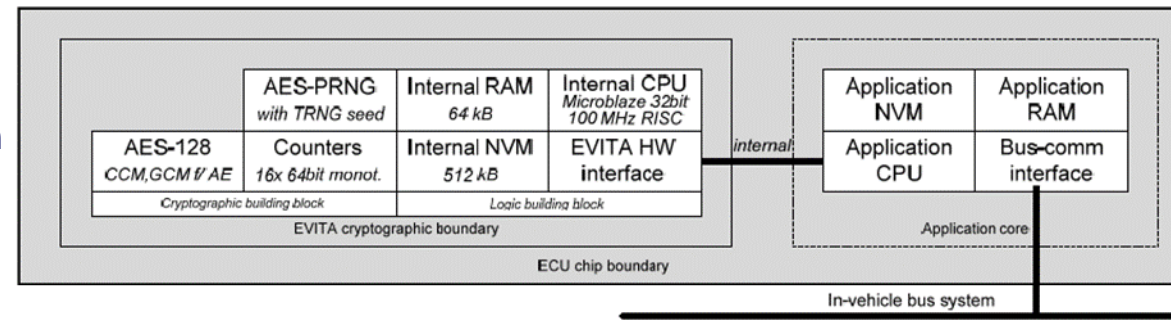
> HSM Light

- For security-critical sensors and actuators



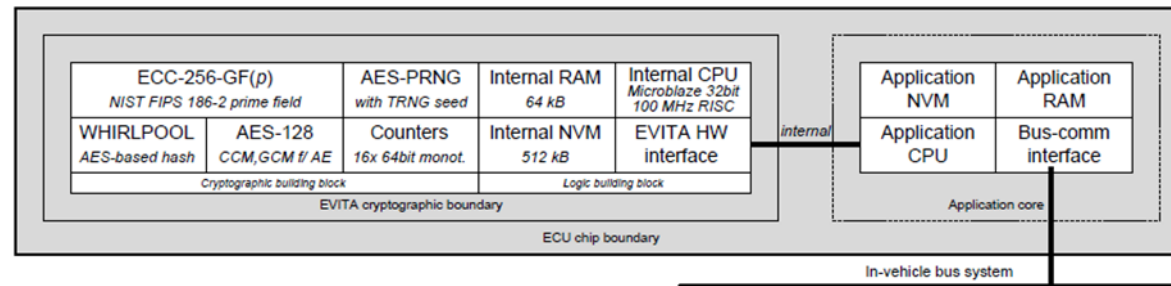
> HSM Medium

- As hardware extension to the ECU connected to the in-vehicle domain controls



> HSM Full

- As hardware extension to the ECU specifically responsible for V2X applications



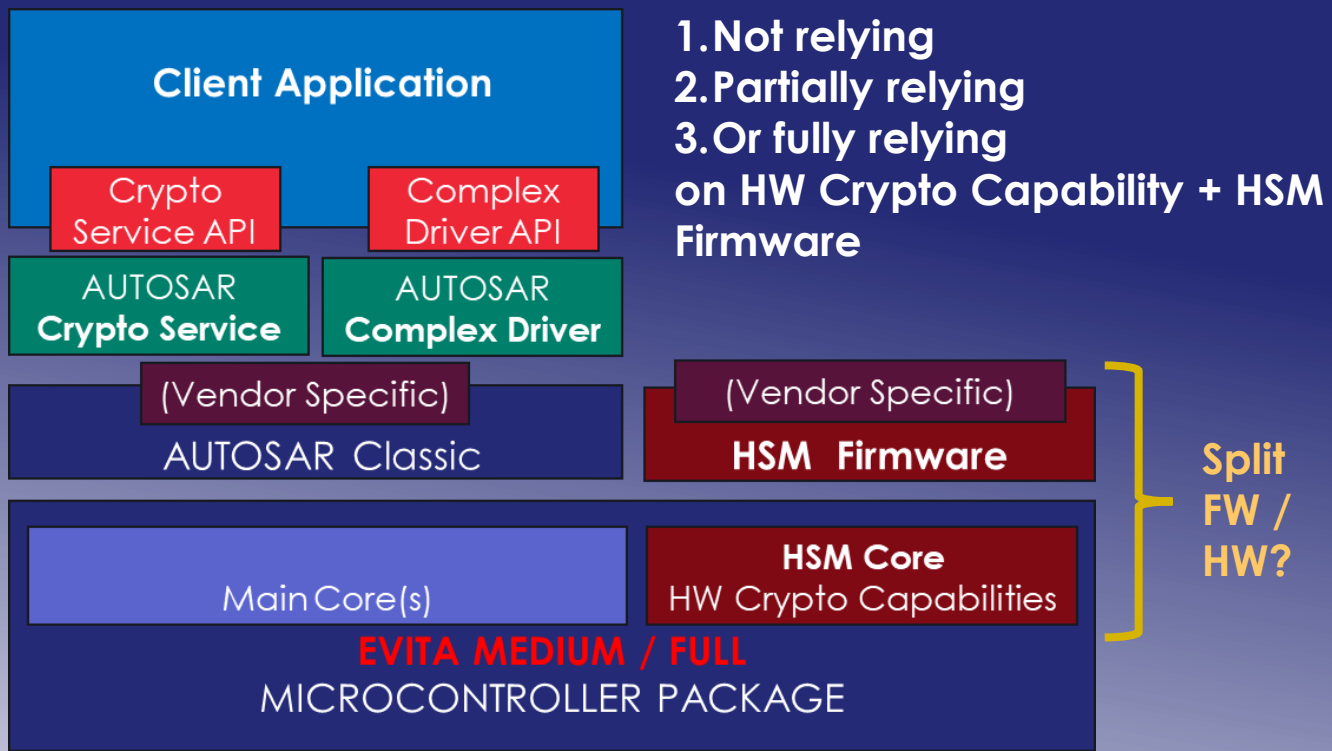
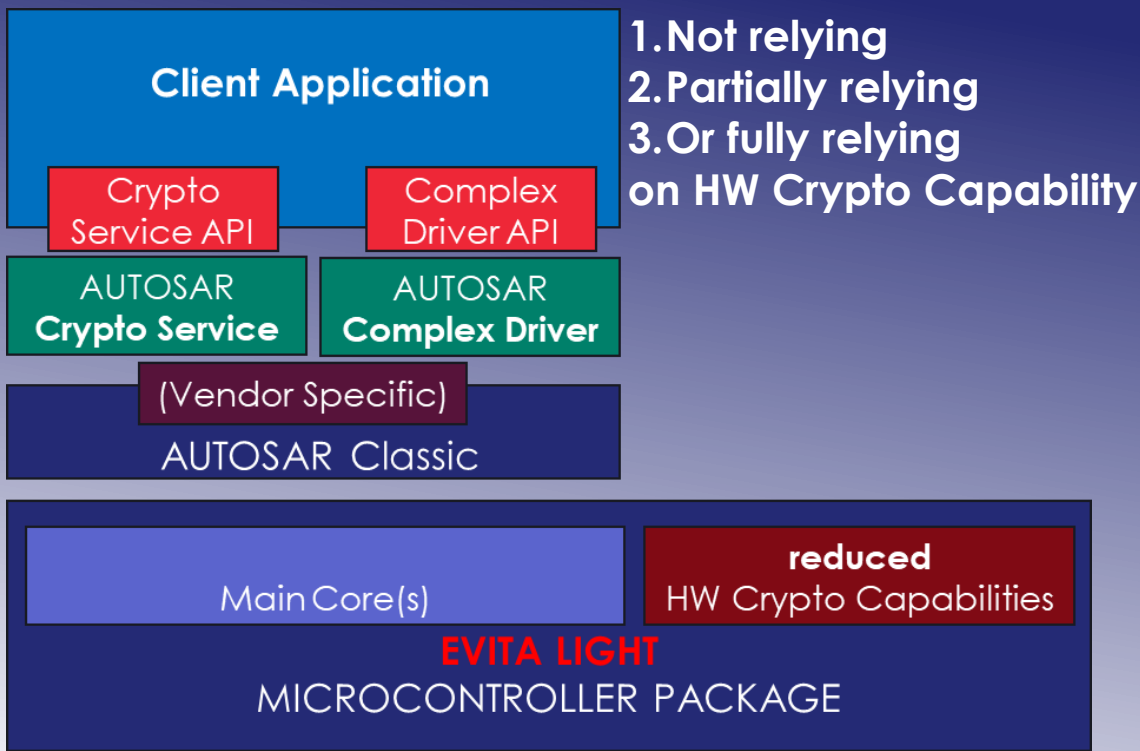
▶ Symmetric crypto engines

▶ + CPU to execute HSM Firmware with privileged access to Flash / RAM area

▶ + Asymmetric crypto engines

Implementation variants with AUTOSAR + Evita HSM

AUTOSAR Crypto Service/ Complex Driver



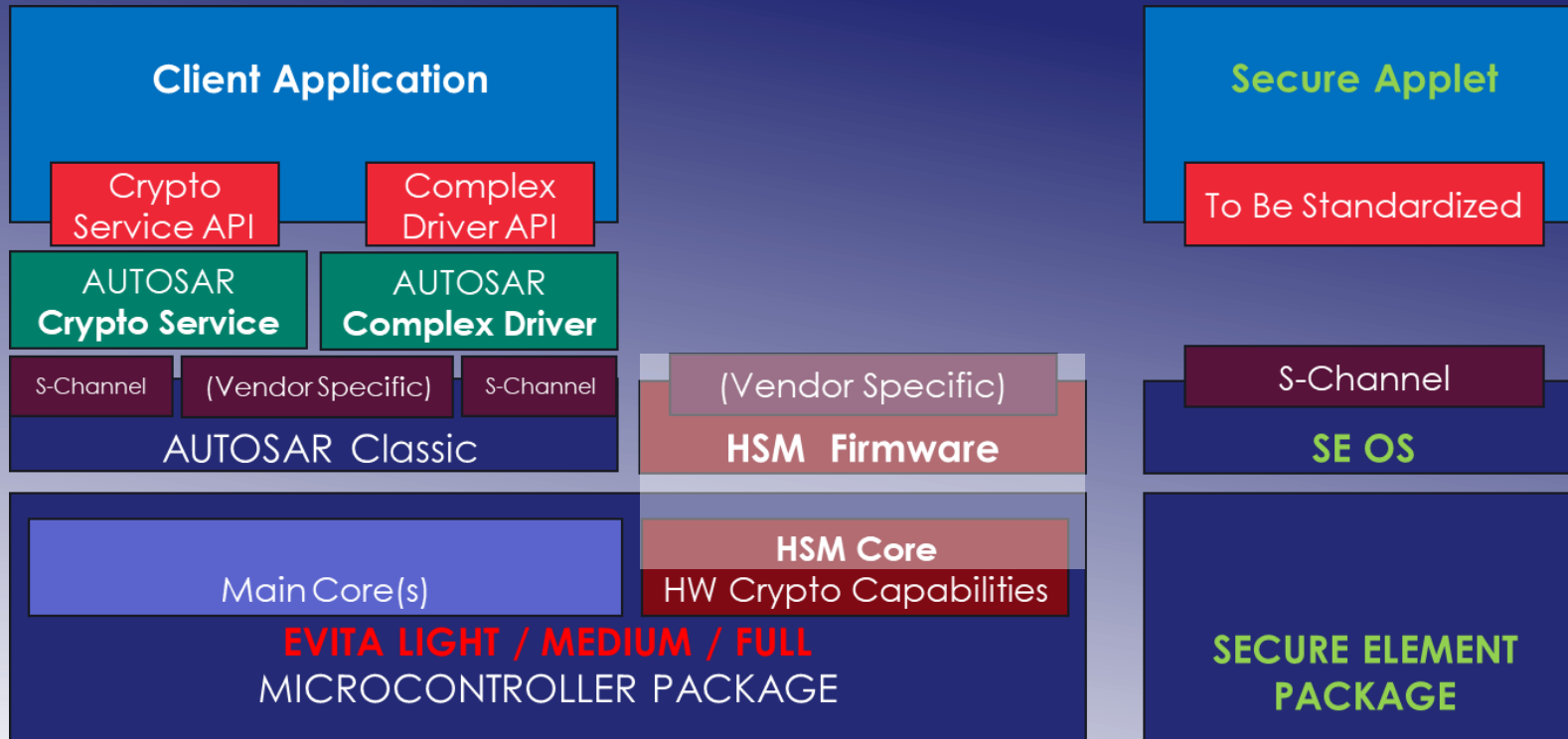
A nightmare to understand how things are really working
 Difficult to demonstrate security objectives are met and evaluate resistance level



Obscure by design

- > Lack of clarity on how/where crypto services are implemented
- > As many implementations as actors to fit given security goal.
- > Supported features are vendor (HW and FW) specific
- > No resistance to hardware attacks
- > Maturity is difficult to evaluate
- > Frozen capabilities, no agility
- > Huge costs and planning impacts each time a change is required
- > Limited cryptographic algorithms
- > No or low capability to fix vulnerability after deployment

Extension of HSM capabilities with Secure Elements



HSM

- Legacy implementation
- Access to internal resources

eSE

- Tamper resistance
- Certification
- Advanced crypto algorithms
Diffie Hellman, miscellaneous
ECC curves, etc.
- Crypto agility.
Upgradable, PQC readiness
- Key Management Life Cycle
- Business logic

Take benefit of the both HSM and Secure Element.
Crypto services always running in secure environment (HSM or SE)

Benefits of embedded Secure Elements in Automotive



a secure execution environment

Tamper resistant⁽¹⁾

Execution of crypto service and business logic

Separated resources




standardized, proven, mass-produced

Standardized protocols & mechanisms

interoperable⁽²⁾ & upgradable applications

Well-defined certification schemes with high assurance (EAL4+)



with interesting complementary properties

Agile

Low consumption

More than 1Mbytes available

Good performances boot time / crypto operations

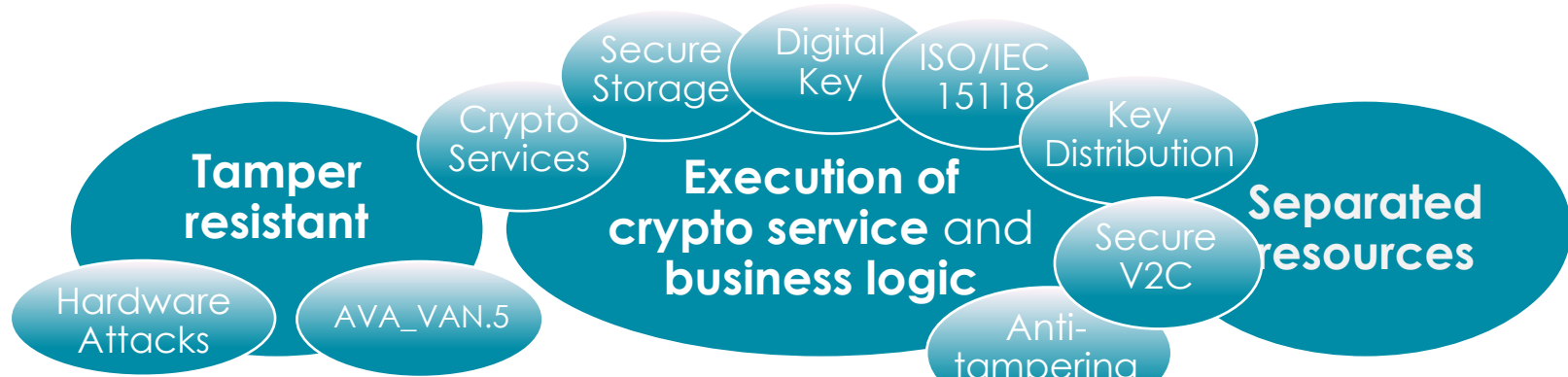
(1) Resistant to physical attacks, AVA.VAN.5

(2) Interoperability of the binary level

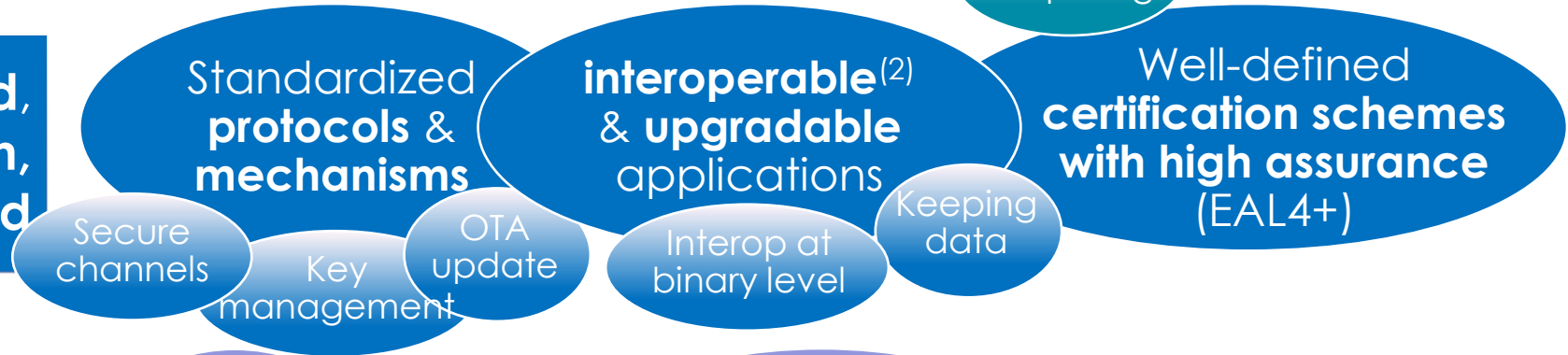

Benefits of embedded Secure Elements in Automotive



a secure execution environment




standardized, proven, mass-produced

with interesting complementary properties



USECASE

HSM ROLE

eSE ROLE

Secure binding between MCU and eSE

- Secure storage of SCP¹ Key / MCU side
- ¹ Secure Channel Protocol (e.g. SCP03)

- Secure storage of SCP¹ Key / eSE side
- Secure Channel Protocol implementation

Secure Boot of MCU

- Before releasing from reset, CMAC signature verification of immutable boot area
- Hash computation

- Asymmetric signature verification of updatable area(s) against pre-defined Root Of Trust

MACSec between 2 ECUs

- GMAC computation/verification using Secure Association Key

- CAK¹ provisioning/learning
 - MACSec key agreement and SAK² creation
- ¹ Connectivity Association Key ² Secure Association Key

Vehicle to Cloud mTLS

- Not supported

- Manage critical steps during mTLS handshake

Digital Key (DK)

- Not relevant in DK protocol
- Secure transfer of UWB keys to UWB sub-system

- Digital Key storage
- Implementation of the CCC protocol between vehicle and device

Use cases with embedded Secure Elements in Automotive



> Key management life cycle

- ▶ Personalize eSE during its production
- ▶ Ease transition phases from development to production
- ▶ Allow secure key provisioning at Tier1 manufacturing and OEM assembly line

> Business logic control

- ▶ Business logic implemented eSE
- ▶ Enforce control of key and crypto engine usage

> Crypto agility

- ▶ Provide secure key provisioning on-field, at repair
- ▶ Tackle circular economy
- ▶ Support OS and Applet upgrade
- ▶ Ensure PQC readiness

Thales Automotive eSE



A trust enabler for the new generation of **car applications**

Get in touch

Laurence Bringer

Technical Director - Smart Mobility Segment
Digital Identity and Security

 **+33 6 62 85 17 33**

 **laurence.bringer@thalesgroup.com**

Yves Le Bobinnec

Cybersecurity Solution Architect – Smart Mobility
Digital Identity and Security

 **+33 6 64 15 52 96**

 **yves-emmanuel.le-bobinnec@thalesgroup.com**

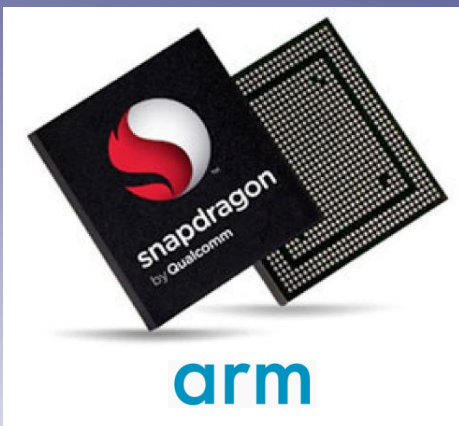


μProcessor A-Class platform (TEE, TZ)



Examples:

- ▶ Telematic
- ▶ Central HPC
- ▶ Infotainment
- ▶ ADAS Supervisor
- ▶ ...



μController (HSM)

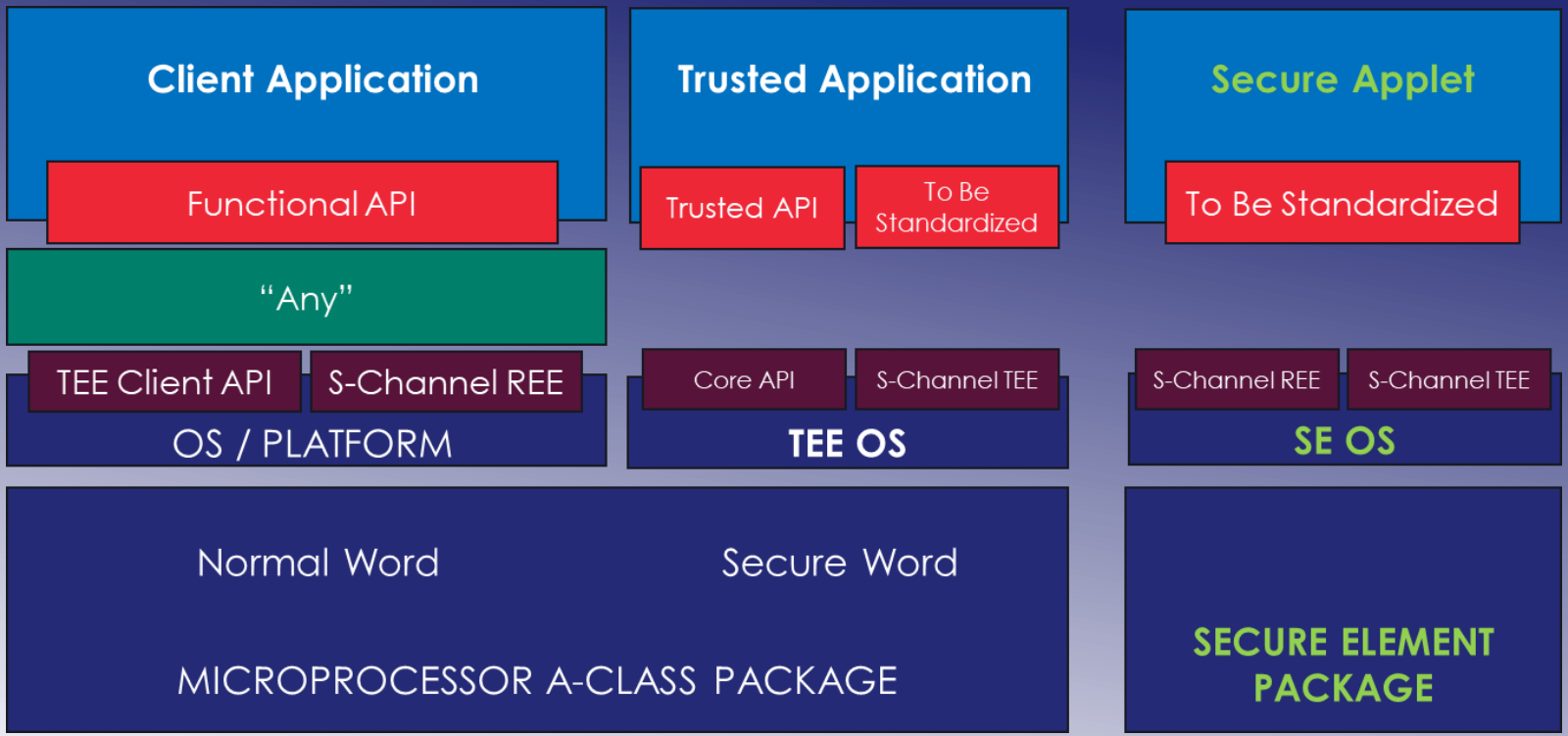


Examples:

- ▶ VHL Access
- ▶ VHL Health
- ▶ EV Charging
- ▶ Anti Chip Tuning
- ▶ Zonal Controller
- ▶ ...



Extension of TEE capabilities with Secure Elements



TEE

- Standardization
- Access to internal resources
- CPU performance

eSE

- Tamper resistance
- Certification
- Key Management Life Cycle
- Available for REE at very early boot phase
- Independent resources (CPU, Non-volatile storage)

Take benefit of the both TEE and Secure Element.
 Crypto services always running in secure environment (TEE or SE)



Next generation μController R-Class platform (μTEE, TZ)

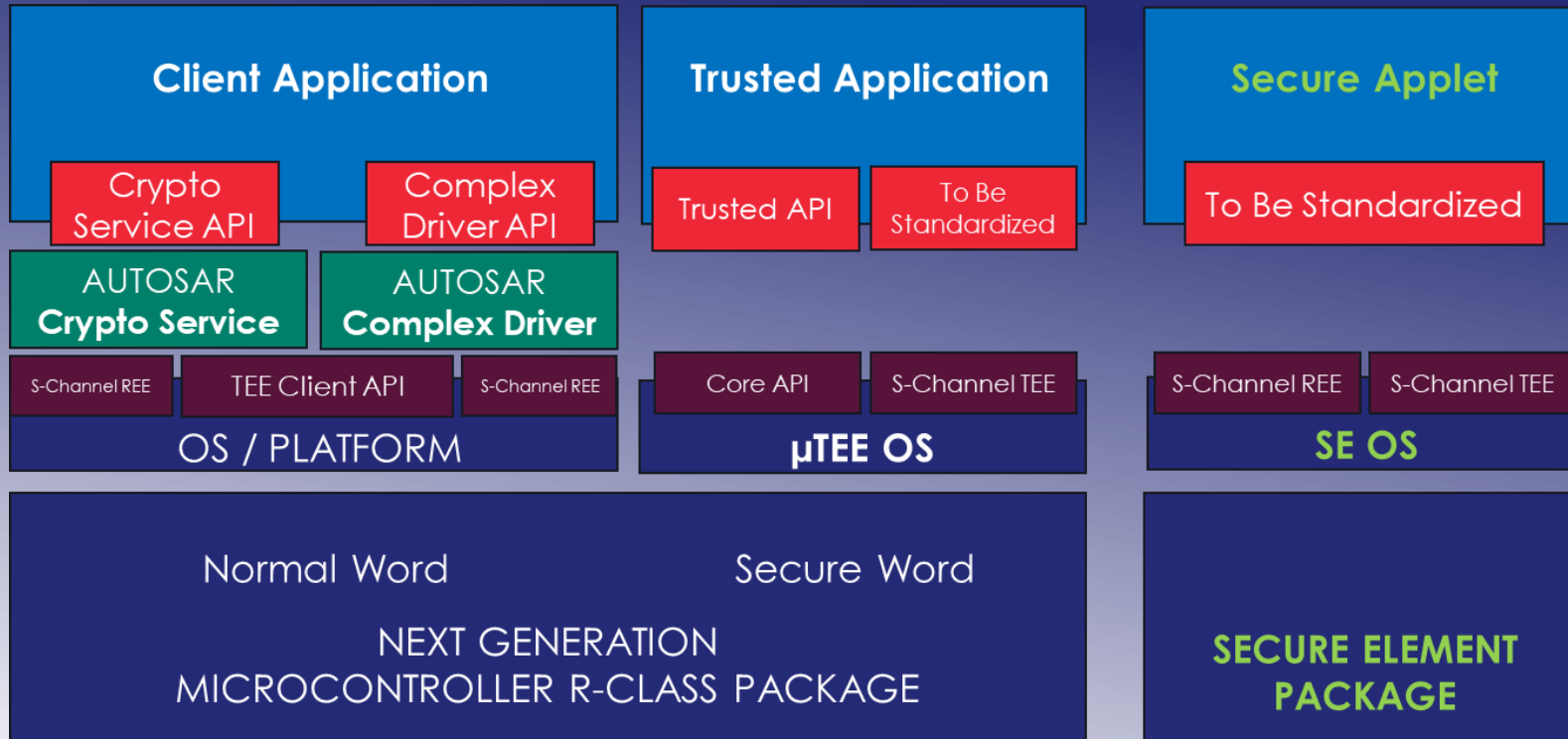


Examples:

- ▶ To be defined
- ▶ ...



Extension of μ TEE capabilities with Secure Elements



μ TEE

- Standardization
- Access to internal resources

eSE

- Tamper resistance
- Certification
- Advanced crypto algorithms
Diffie Hellman, miscellaneous ECC curves, etc.
- Crypto agility
Upgradable, PQC readiness
- Key Management Life Cycle
- Independent resources (CPU, Non-volatile storage)

Take benefit of the both μ TEE and Secure Element.
Crypto services always running in secure environment (μ TEE or SE)