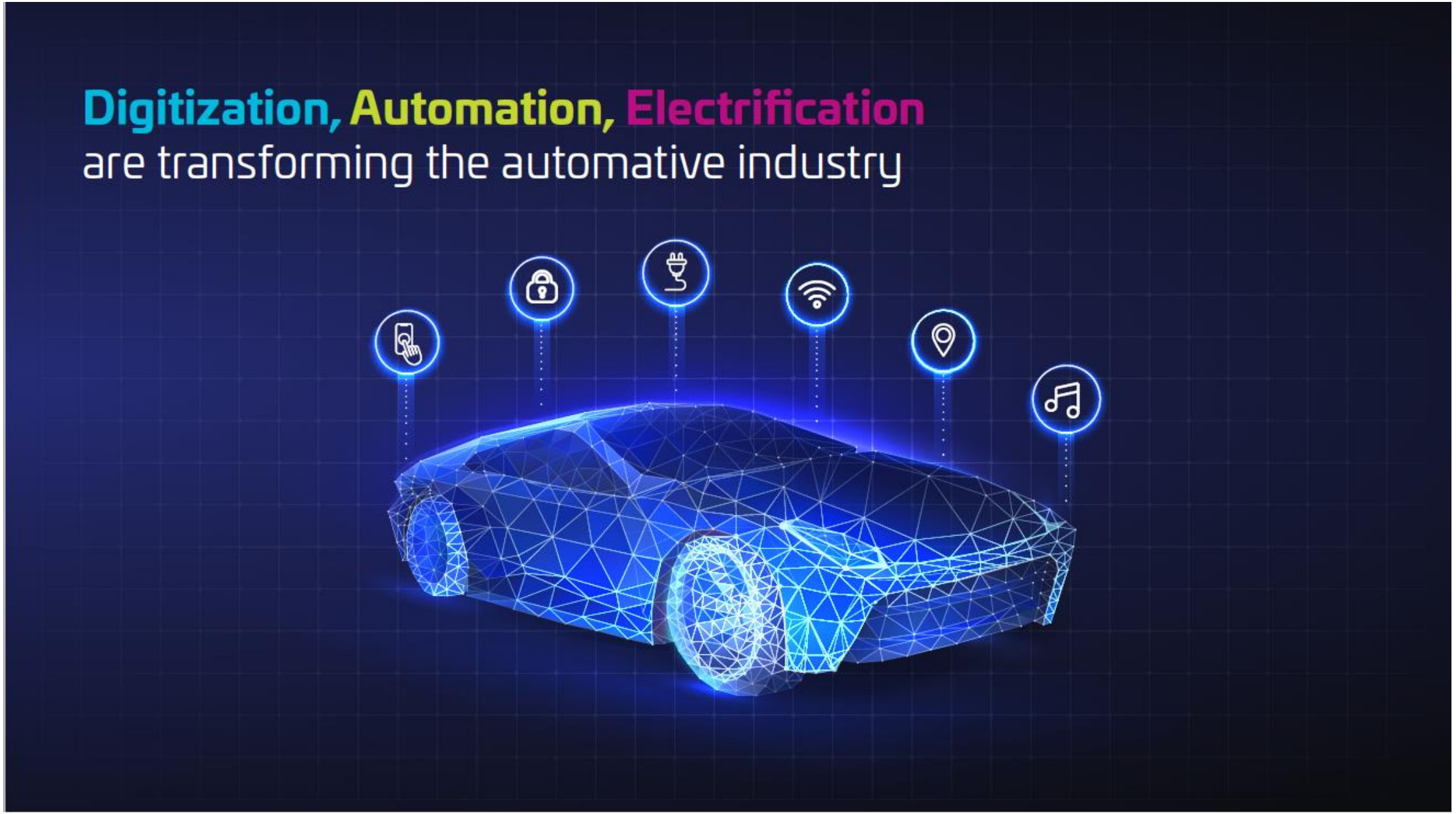
THALES
Building a future we can all trust

eSE in Automotive

GlobalPlatform
CYBER VEHICLE FORUM
Sept. 2023 - Tokyo

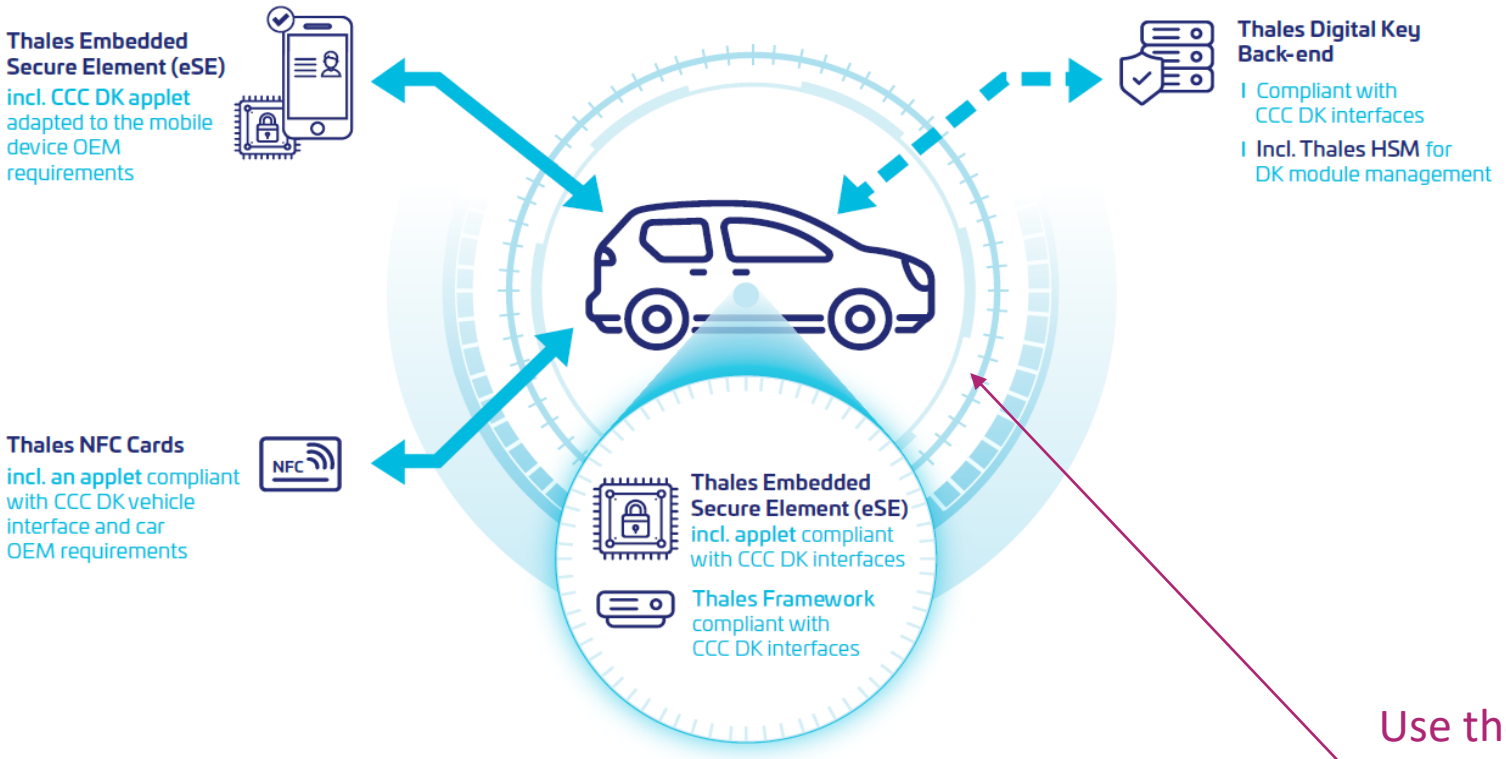
www.thalesgroup.com



New technologies and services are being deployed

- **Vehicle softwarization**
- **Cellular connectivity**
  Emergency Call
  Infotainment
  Smart Traffic
- **Electrification**
  Plug N Charge
  Vehicle to Grid
- **Smart Mobility**
  Digital Car Key

Enabling the Car Connectivity Consortium® (CCC) Digital Key



- CCC Digital Key Applet in the embedded SE of the end user device
- CCC protocol implemented in SE of Vehicle
- Contactless cards based on CCC specification and using SE

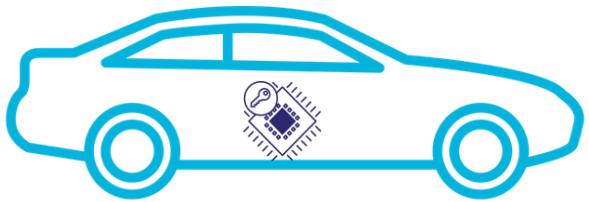
➢ **The highest level of end-to-end security**

Use the end user device (e.g., mobile) to
- Open/Close the vehicle
- Start the engine

Handling the Cellular Connectivity

Cellular connectivity

Mobile Network Operators



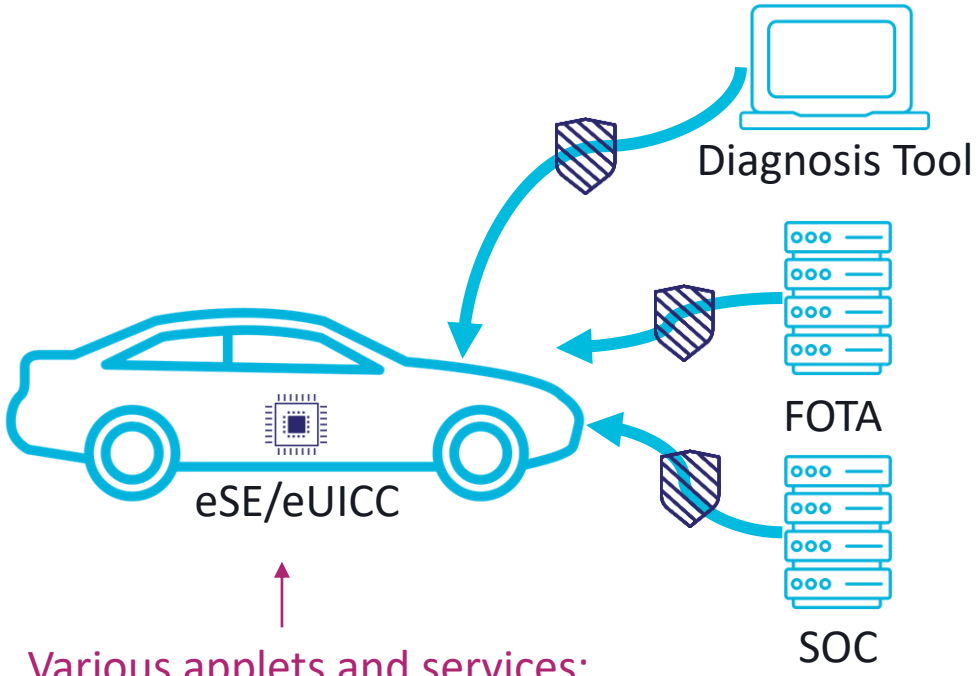
eUICC

Use cases:

- Emergency call
- Infotainment
- Telematics, Maintenance, Monitoring

- Network Authentication Application (NAA)
- Remote SIM Provisioning (RSP)

Addressing the cybersecurity requirements

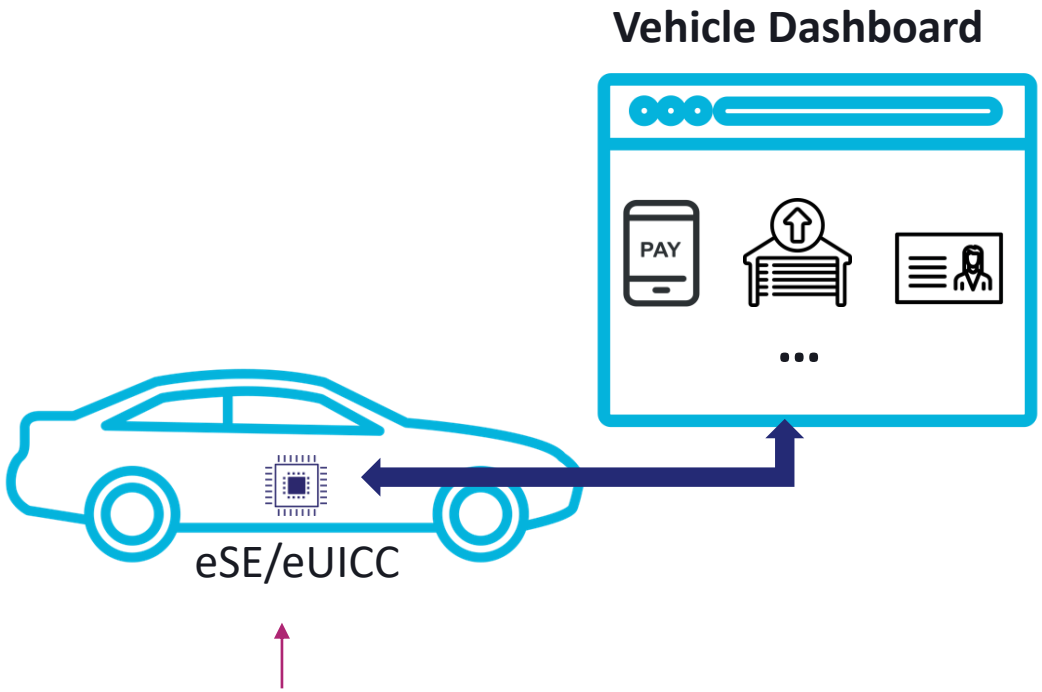


Use cases: support to

- Secure Software / Firmware Update
- Secure Diagnosis (with a local or remote diag. tool)
- Secure Probe and remote Security Operation Center - SOC
- Secure Data Management (end-user privacy)

- Various applets and services:
  - Secure Storage: certificates, sensitive data
  - Secure TLS establishment
  - Crypto toolbox: signature verification, signature generation, data encryption, data decryption

Enabling sensitive consumer applications in connected vehicle

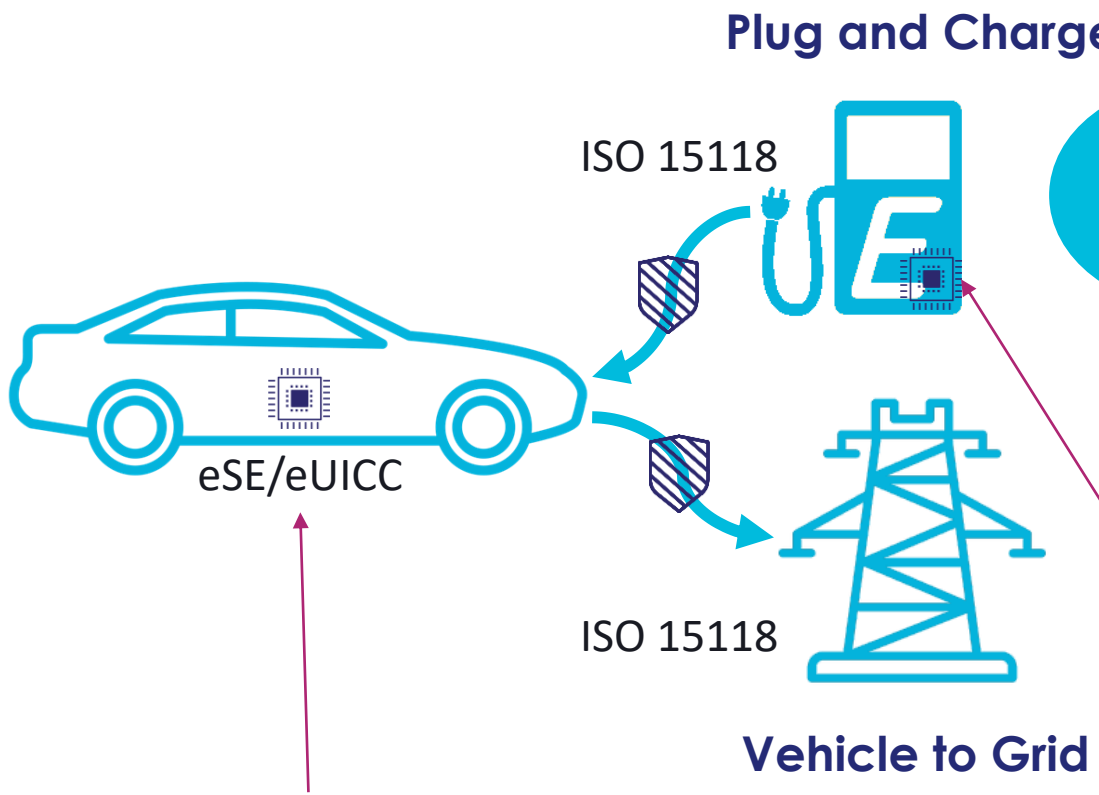


Use cases: Consumer applications running on the head unit of the vehicle

- Payment applications
- Access control applications
- ID applications
- Etc.

- Some of these applications need a Secure Element (e.g., EMVCo applications).
  - These applications are already integrated in consumer end-user device environments (like Android or iOS).
  - Migration to the new vehicle dashboard environments (e.g., Android automotive) could be straight forward thanks to the GlobalPlatform technologies.
- Other applications may benefit from Secure Storage area or Crypto Services available in the Secure Element.

Securing the Electrical Vehicle Infrastructure



eMobility roaming hub

e-Mobility Service Provider

Charge Point Provider

Use cases:

- Plug and charge
- Vehicle to Grid

- Strong charging station authentication
- Secure firmware update
- Secure remote administration

Strong vehicle and user authentication

Ready for the Software Defined Vehicle (SDV)

> All previous use cases remain valid

- Host applications requesting high security level.
- Manage secure storage or crypto services required to enable vehicle features requesting high security (Firmware update, etc.) to answer to the – increasing - cybersecurity challenges.

> Secure Elements and GlobalPlatform features fits the following requirements for SDV

- Perfect candidate to manage keys in vehicles: tamper resistant key storage with standardized key management protocols.
- Standardized interfaces and mechanisms: secure channels, confidential key loading, key update, etc.
- Host applications implementing end-to-end protocols or part of it with hardware isolation, tamper resistance(1) and isolation between applications
- Support interoperable (2) and upgradable applications
- Compliant with in-cloud development architecture: standardized OTA deployment or update mechanisms

(1) physical attacks, AVA.VAN.5 (2) Interoperability of the binary level

THALES
Building a future we can all trust

Contact

Name

Job title

Phone number

email

Laurence BRINGER

Technical Director
Automotive Business Line

+33 662 851 733

Laurence.bringer@thalesgroup.com

THALES
Building a future we can all trust

Thank you

www.thalesgroup.com