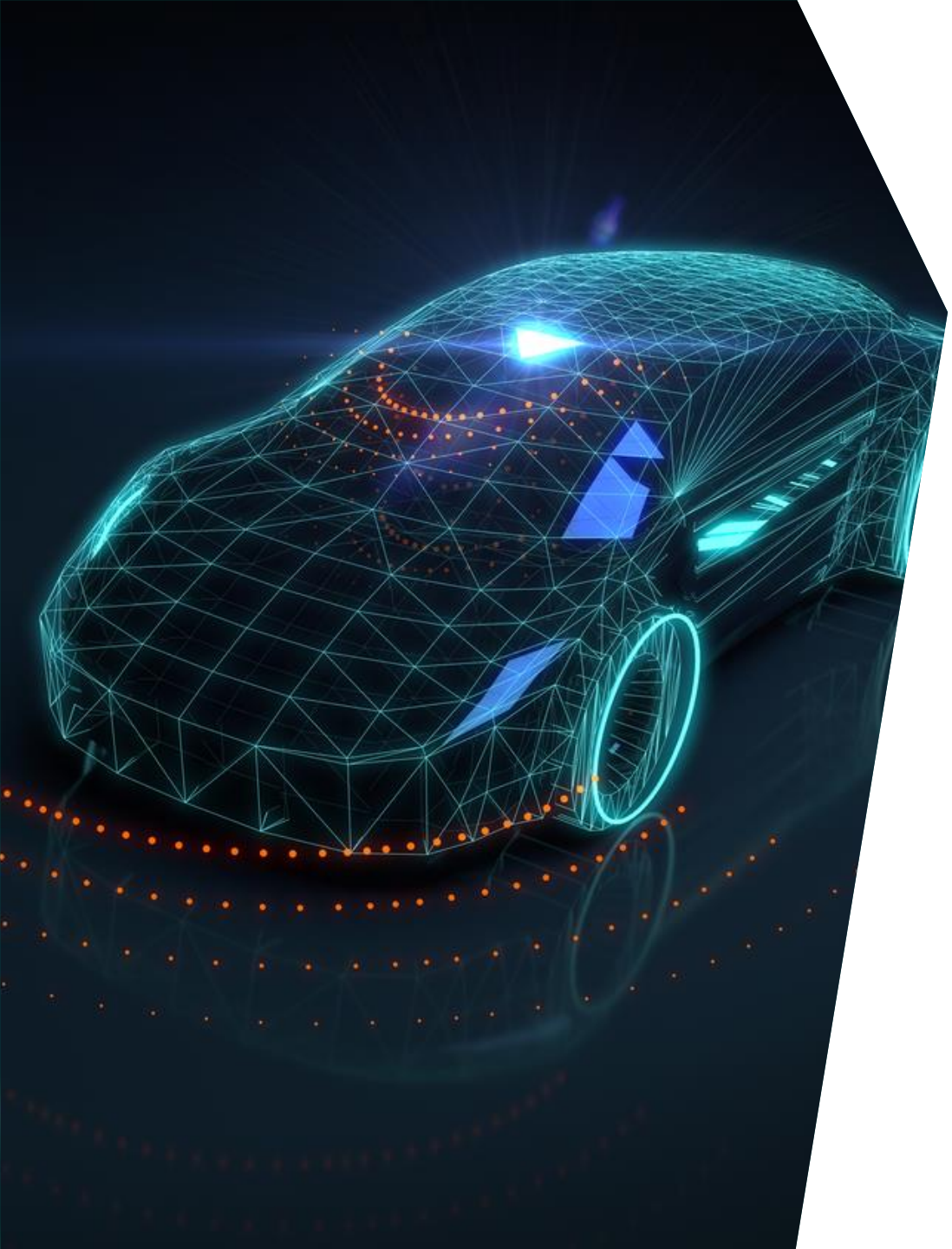


Target Applications for Secure Elements in Future Cars

Antoaneta Kondeva
Security Architect for Dedicated Security Modules for Automotive Applications

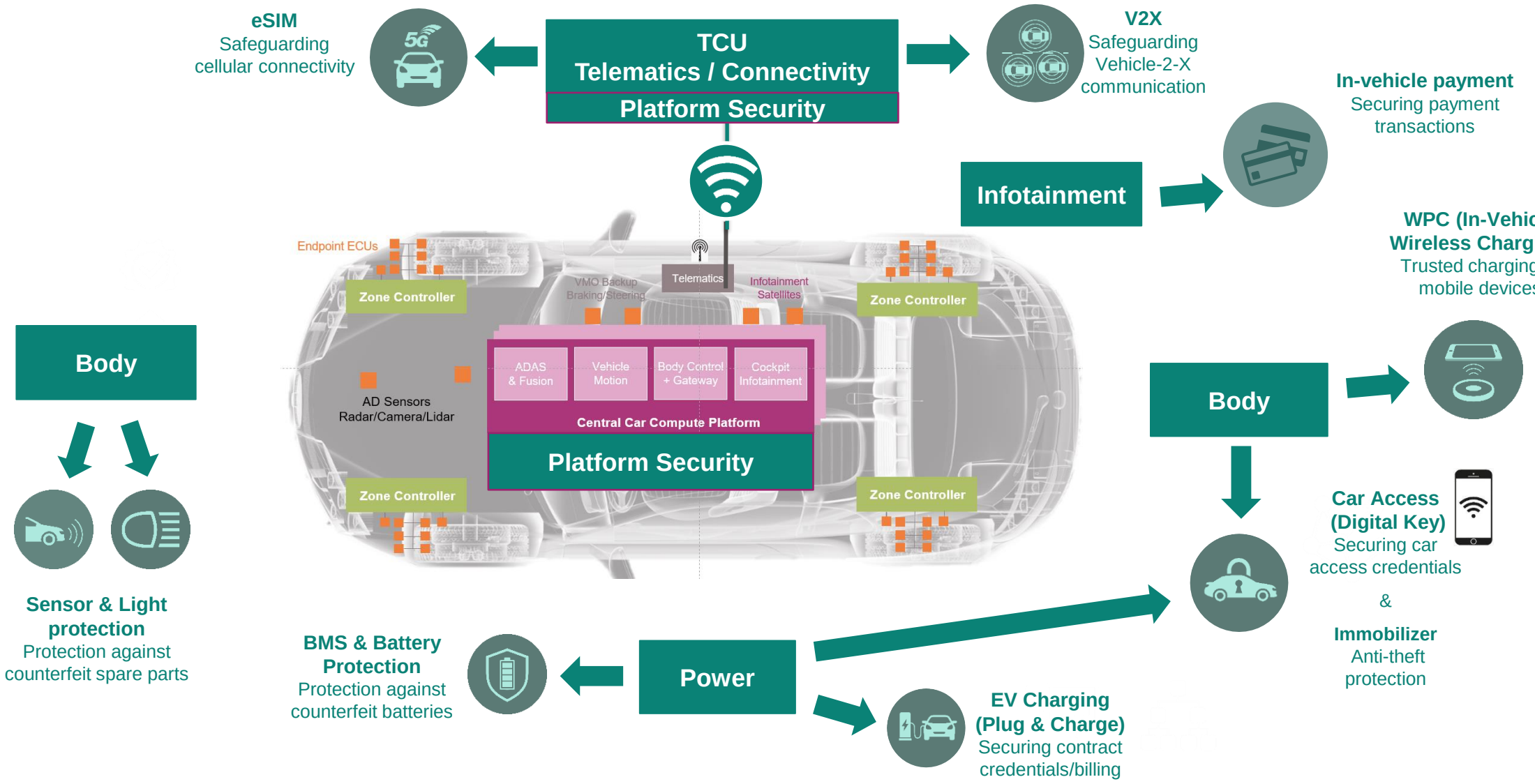
GlobalPlatform Cybersecurity Forum, Hamburg, Germany
2023-11-14

Table of contents

Cybersecurity is defining the next level of quality for the automotive industry

The Automotive Market is currently shaped by three Megatrends.
They are all linked to Automotive Cybersecurity

(Potential) Target Applications for Secure Elements in future cars

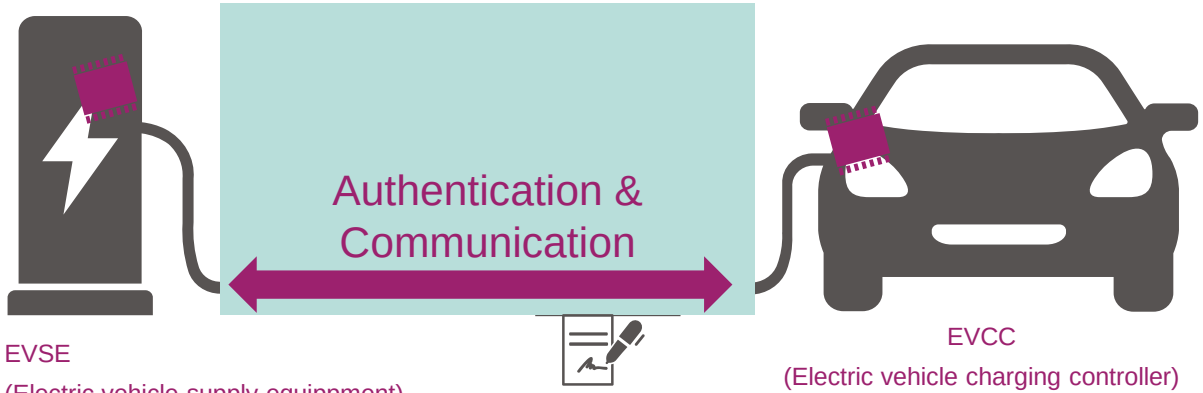


EV-Charging – Secured charging communication & billing

- Smart EV-Charging (Plug & Charge) according to ISO 15118
  - Automatic authentica[illegible]and charging stations for public and private charging
  - Charging Card as a[illegible]authentication is integrated into the vehicle
  - Payment process i[illegible]hicle and OEM via contracts that are selected by the user dependent on the station

- Security in charging communication according to ISO 15118
  - Authorization of the charging and billing process (Plug & Charge)
  - Non-repudiation of the billing process
  - Confidentiality in charging communication

- Security measures: message encryption, authentication, and authorization based on digital signatures and certificates
  - The role of SE: temper-resistant security protection for the contract credentials, private keys, and billing

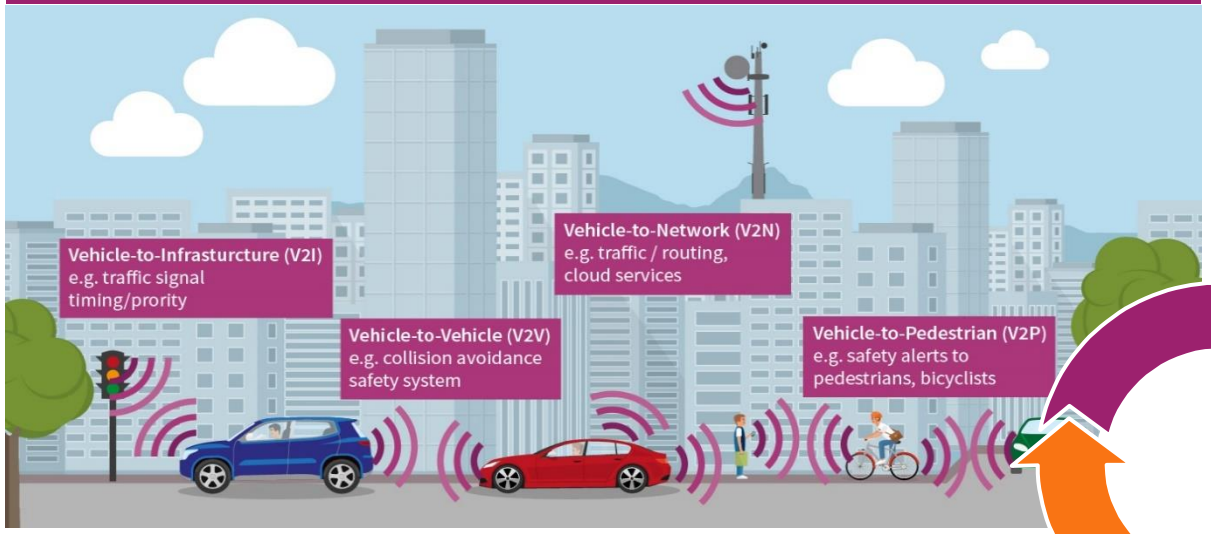


CCC Digital Key

- Purpose:
  - Digitalize the vehicle key to enable a better user experience
    - Share access
    - Control the usage of the vehicle
- Security requirements:
  - Secure distance bounding
  - Secure authentication
  - Confidentiality of the messages for key pairing
  - Freshness of the messages
- Security measures: message encryption, authentication, and authorization based on digital signatures and certificates
- The role of the SE:
  - Offers tamper-resistant storage of cryptographic credentials and authentication processing

Vehicle-to-Everything communication (V2X) for improved road safety and traffic efficiency

What is V2X?



V2X is driven by Standards

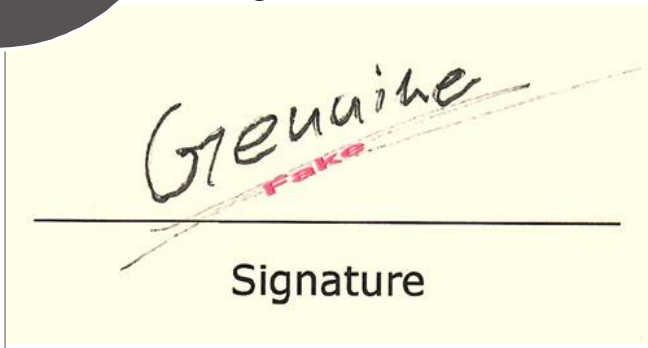
- Mandate high security for signing and private keys
- Security certifications provide assurance – leveraging region-specific certification schemes
- **Secure Elements** based on a highly secured tamper resistant microcontroller to safeguard secured V2X communication

From standards to product

Why V2X?

- Improve road safety
- Increase traffic efficiency
- Support automated driving
- Services for travelers, OEMs, mobility providers, road operators
- Regulatory requirements
- Better NCAP safety scoring

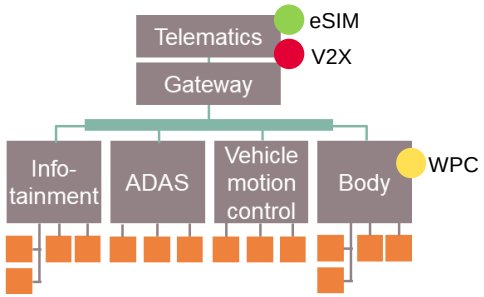
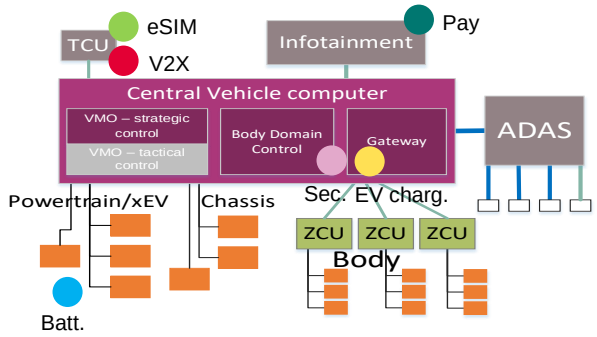
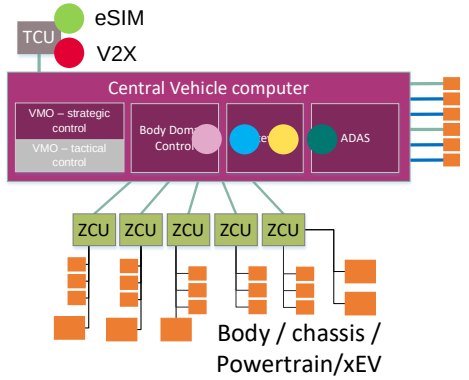
- **V2X has high requirements towards integrity, authenticity and privacy**
- Message authentication via digital signatures required against threats such as:



- Message manipulation (change/delete content)
- Unauthorized sender, fake alerts
- Privacy abuse (profiling driver data)

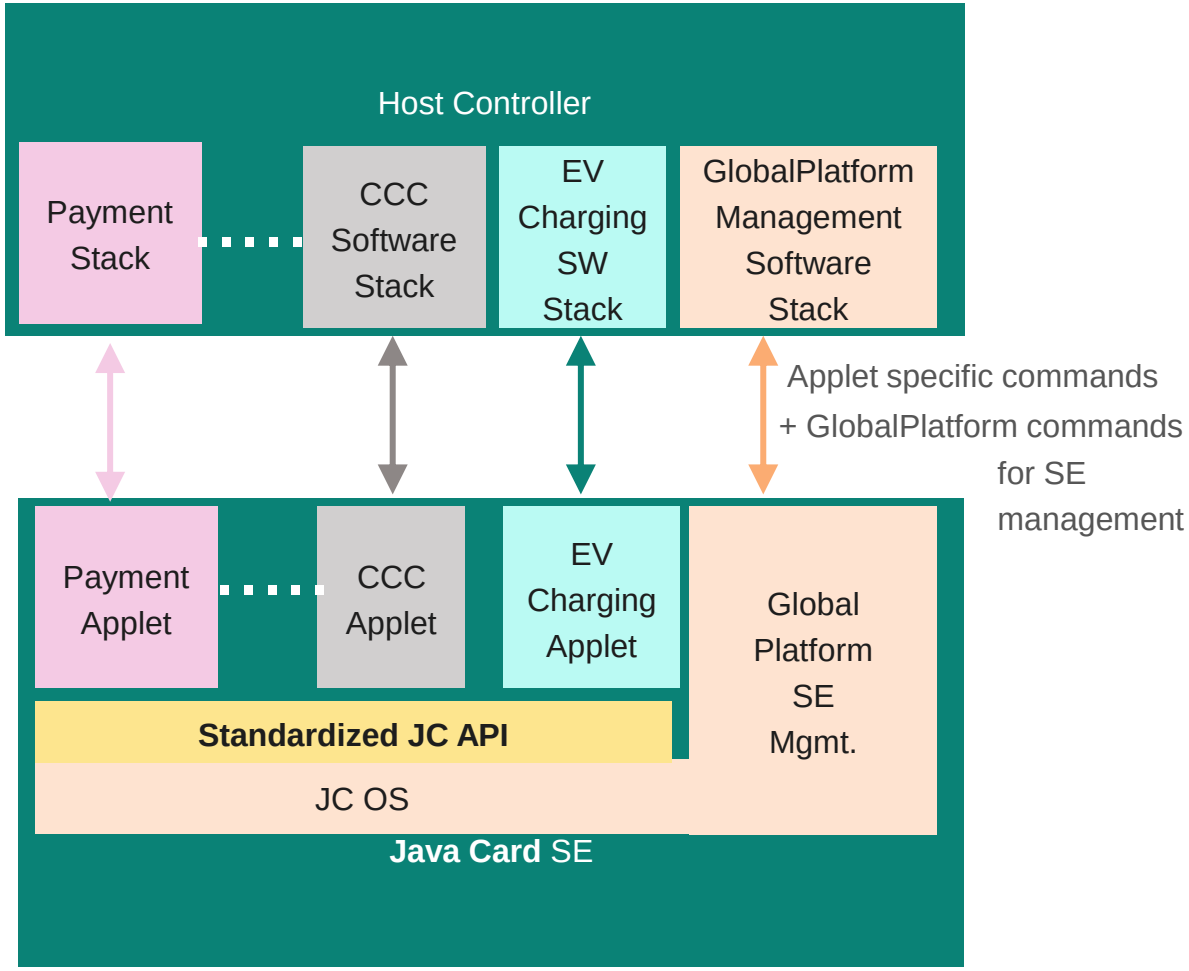
Security and privacy

Automotive E/E Architecture transformation and the role of SE? – Trends & Outlook

	Today	Tomorrow (2025-2030)	Tomorrow + 1 (2030+)
	Domain Architectures	Mixed domain / zone architectures	Highly integrated zone architectures
1 Architecture Evolution			
2 # of applications	› 4: eSIM, Car Access, V2X, WPC	› Number of applications will grow (e.g. payment, EV charging, Battery protection, brand/ECU protection, platform security)	› Harmonization of SE usage: – Secure elements will address not only multiple applications but will be deeper integrated into the vehicle platforms – SE will be part of platform security concept
3 # of applications per SE	› SE usage for dedicated applications: 1 application per SE	› 2-3 applications per Secured Element	› n applications per Secured Element

eSE as a platform for several automotive applications

- GlobalPlatform specifications
  - GP Card Spec (v2.4 coming soon)
  - Configurations
    - SE, IoT, UICC, SAM, Automotive (in work)
  - Secure Channel Protocols SCP02/03/11/81
    - Crypto Agile Variants SCP04/12 (in work)
  - SE content Management
    - Confidential Key setup (Amd A)
    - Applet update (Amd H)
  - Crypto Service Provider (in work)
  - Protocol Specification
    - APDU over SPI/I²C (T=1‘)
  - Protection Profiles
    - SE + SAM Protection Profile




Infineon