TRUSTONIC

TEE Automotive Use Cases – September 2023

Kenji Takahashi
Japan Business Development
kenji.takahashi@trustonic.com
Trustonic

Talk overview at 100,000ft

Who am I?

Kenji Takahashi
Business Development, Japan
Trustonic Ltd.

Who is Trustonic?

Leading Vendor for solutions based on Trusted Execution Environments

Why should you care?

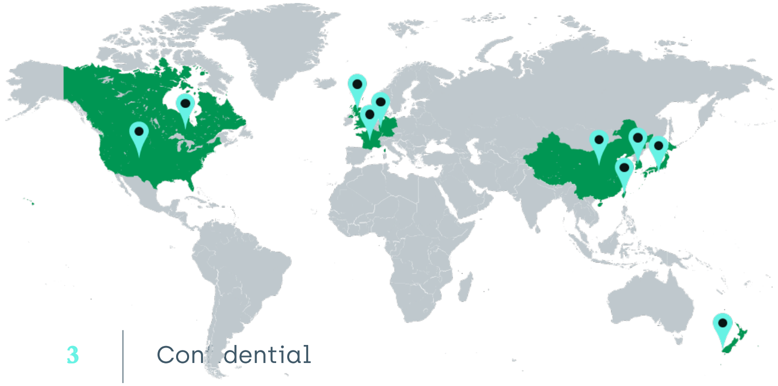
What are TEEs and which challenges do they help address

TRUSTONIC

Who Are We

- Founded by ARM, Gemalto & G&D in 2010
- Independent since 2020
- Deployments in 23m+vehicles
- Additional 60m+additional vehicles under contract
- Zero reported breeches

- Global operations and support



2 BN+ Devices

120+ Patents

80M+ Vehicles

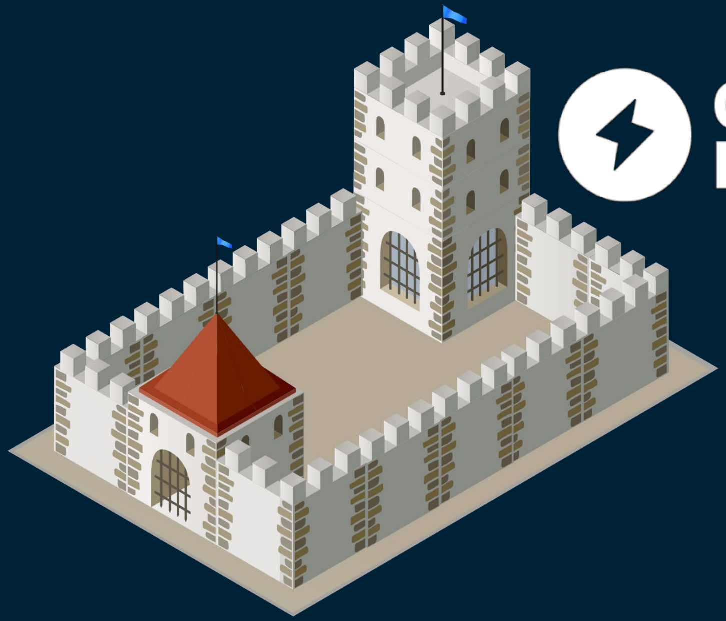
GLOBAL SILICON PARTNERS

Work with the leading SOC vendors to integrate at the BSP level

HARDWARE BACKED SECURITY: TRUSTED EXECUTION ENVIRONMENT

EMVCo Common Criteria FIPS VALIDATED 140-2 SECURITY VISA GLOBALPLATFORM

Trusted Execution Environments

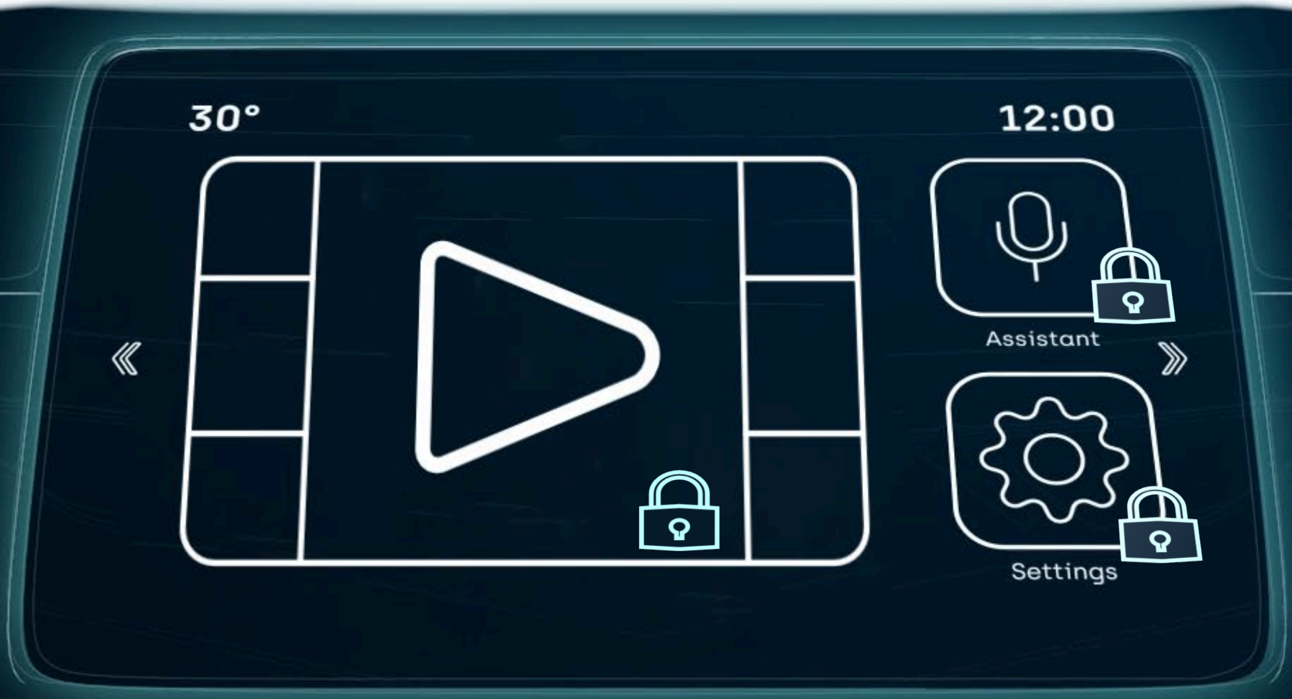


TEEs are an "environment" to run security related software in embedded devices.

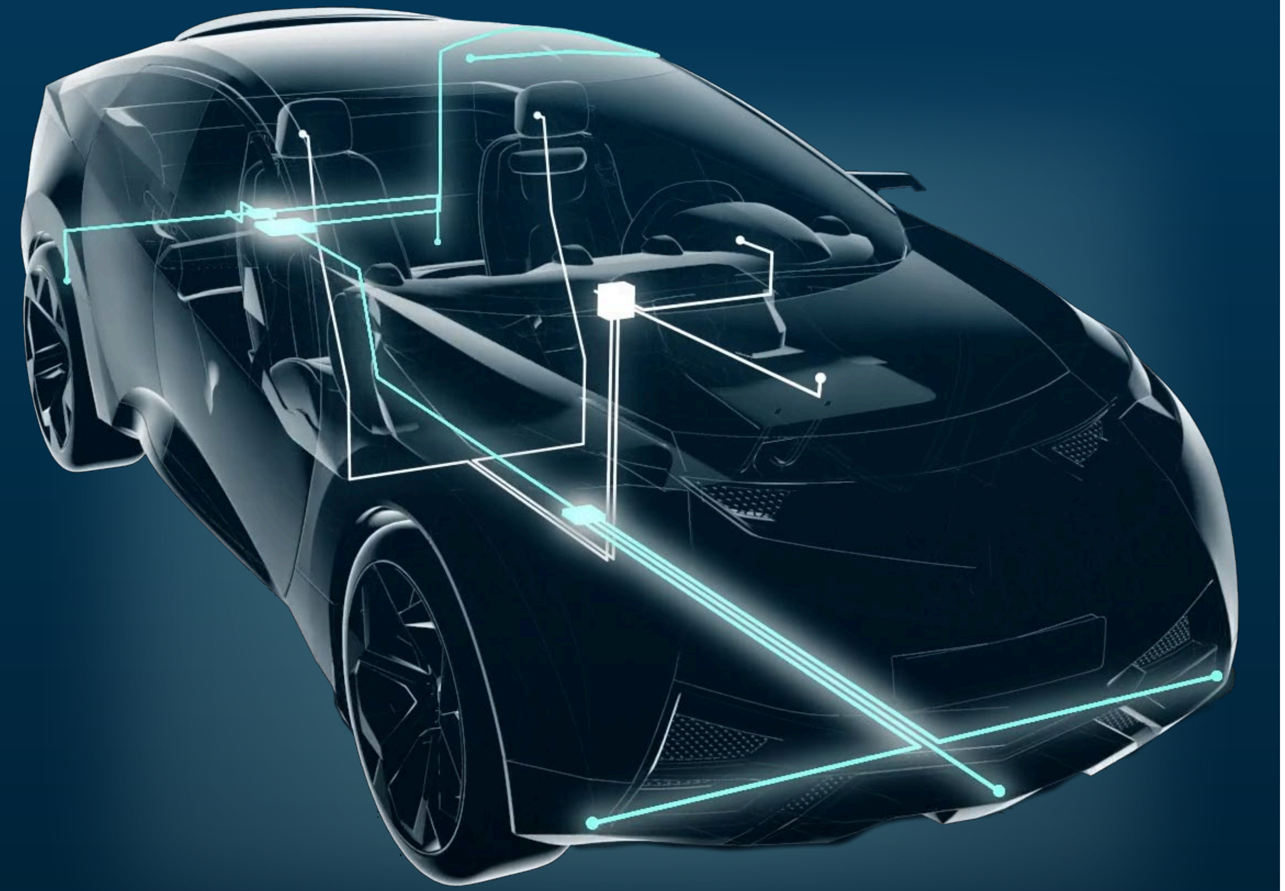
Initial focus was on phones, but broadly applicable to IoT and Automotive.

- Common automotive applications for TEE
- Future trends

Common Automotive IVI Use Cases



- IVI systems are often based on Android (which mandates use of a TEE) making a TEE a common choice
- DRM systems typically require that video decode and secure video path is managed by TEE for HD video
- Virtual Assistants and 'Profiles' increasingly rely on TEE to ensure privacy & security of user data



Broader Automotive Use Cases

- TEEs can be used anywhere within a vehicle
  - Increasingly common in Telematics and Cluster
- Key role is to establish and maintain trust
  - ...between components within vehicle
  - …between vehicle and OEM cloud services
- TEEs run on the main application processor so gain many software advantages
  - Ability to update software (Post-Quantum Crypto)
  - Ability to store and protect large amounts of data (Privacy + Data Integrity)
- TEEs can leverage privileged hardware access
  - Protected peripheral access (e.g. DRM or Biometrics)
  - Per-SOC secret keys
  - Increasingly used to mediate access to HSMs / Secure Elements

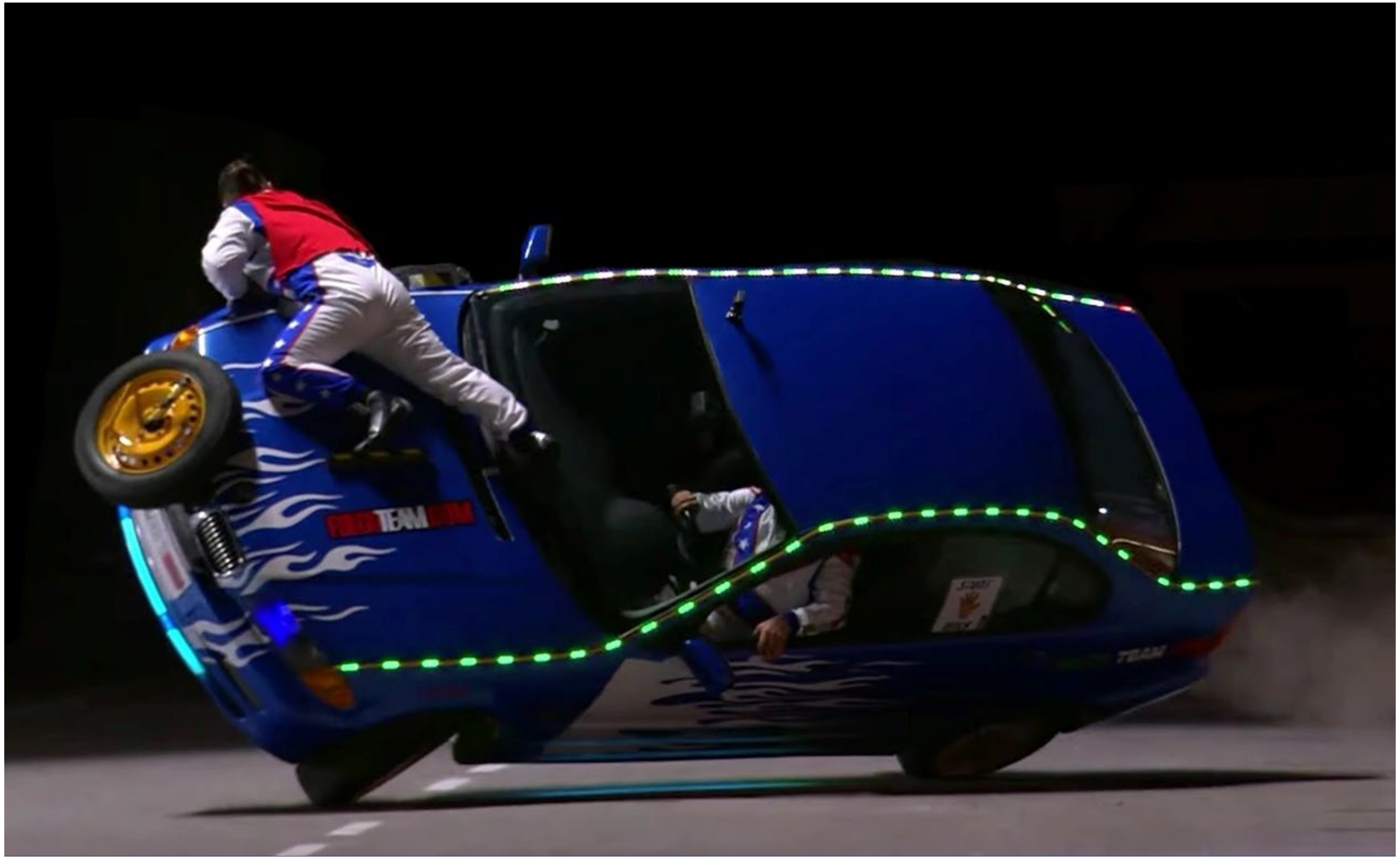
TRUSTONIC

Protecting vehicles of the future

now → 2030

Post Quantum Crypto

- PQC may still be a few years away – but today's cars will be around for 15 years
  - Need ability to update software and keys OTA
- But PQC will drive deeper change
  - New certificates / CAs
  - Global TLS Changes
  - New Open SSL Providers
  - Challenges with boot ROMs
  - Regional variation

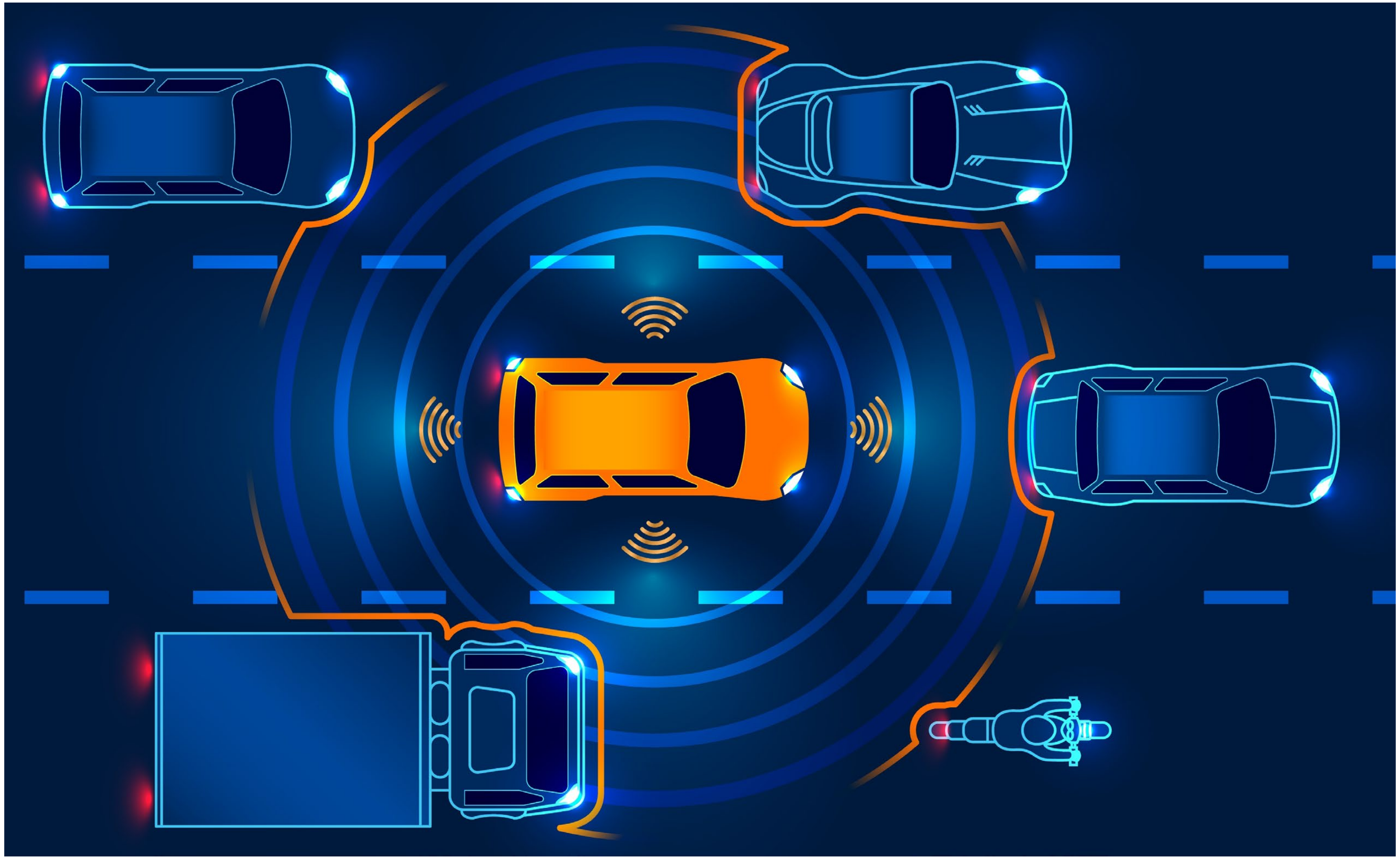


Protecting vehicles of the future

now → 2030

Attestation and Trust

- ADAS/ Autonomous systems need to trust the data on which they rely
- Both legal and illegal modifications to a vehicle can lead to the introduction of fake parts, or untrustworthy data.
- TEEs in core ECUs or Endpoints can sign messages and provide a basis for vehicle wide trust



Protecting vehicles of the future

now → 2030

Data Privacy

- Automakers are increasingly aware of GDPR and similar global legislation.
- A framework for managing user data is needed, which respects privacy whilst providing a seamless experience across devices
- TEEs have long been used in Mobile devices for user privacy, and there are natural synergies in Automotive

Protecting vehicles of the future

now → 2030

IP Protection

- Software within devices can cost millions of dollars, and needs protection against theft.
- AI algorithms in particular are high value and susceptible to theft
- The TEE can be used to securely execute code without exposing it to prying eyes

Protecting vehicles of the future

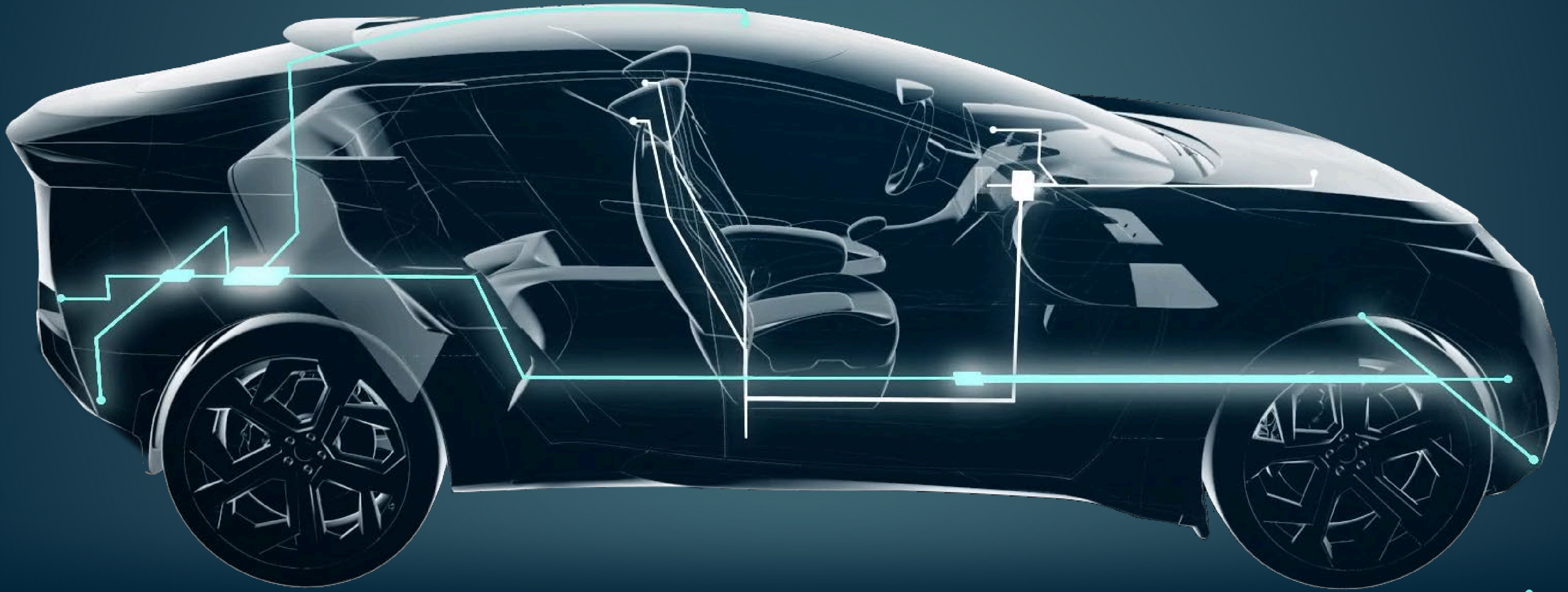
now → 2030

Data Monetization

- Data generated by users and by vehicles has high potential value
- Controlling the monetize pathways, and not gift to Silicon Valley partners.
- The TEE can be used to generate and store data at the highest levels of security.

Summary

- Global legislation and data opportunities means a renewed focus on software security.
- TEEs provide a robust platform
- Complementary to SEs and HSMs
- In the future TEEs will be present in increasing numbers of components, enabling new use cases and vehicle wide trust.



TRUSTONIC

Thank You - Questions