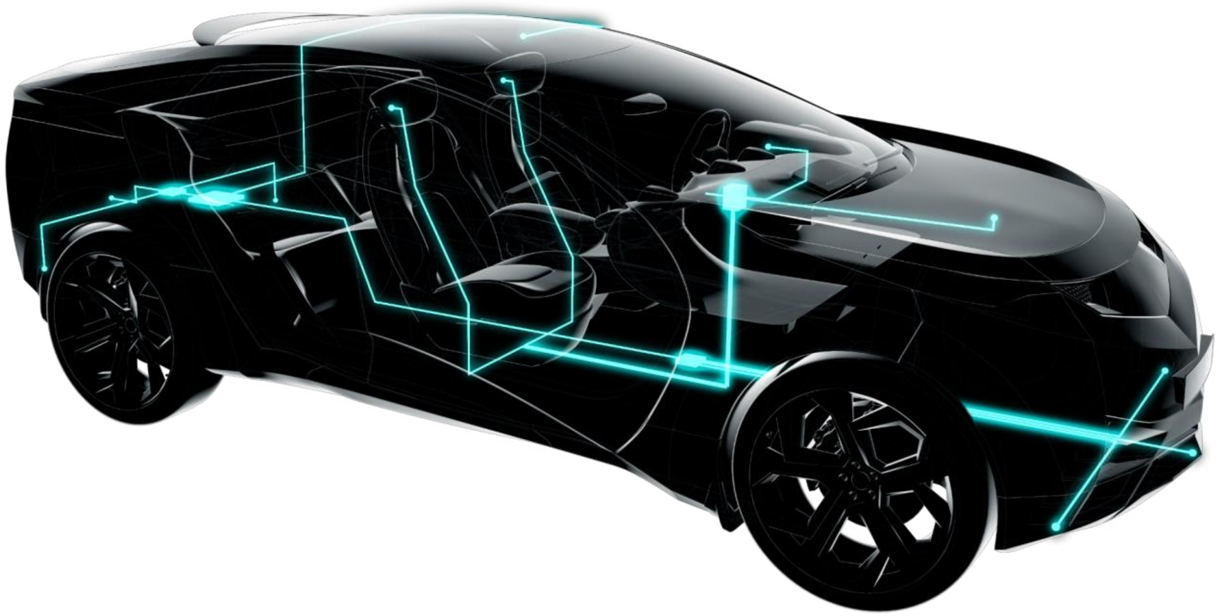
How does TEE Protect Security of Connected Vehicles

Trustonic China

Jason Lin

Software Defined Vehicles ➔ Opportunities & Threats

- Autonomous and ADAS *mean* more sensors, actuators and compute power
- Customers expect voice, gestures, and latest apps
- New opportunities for revenue by entering “internet speed” innovation
- But – more software means more attack vectors
- And enhanced connectivity makes attacks scalable



Regulation and Compliance – Relevant Everywhere

UNECE WP.29

- Legal Requirement for Type approval in 60 countries around the world
- R155/156 requires SOFA updates and proactive resolution of Vehicle Cyber Security

ISO 21434

- Set of recommendations for managing Vehicle Cyber Security Risks.
- Complements WP.29 but is not a legal requirement

China Specific Laws

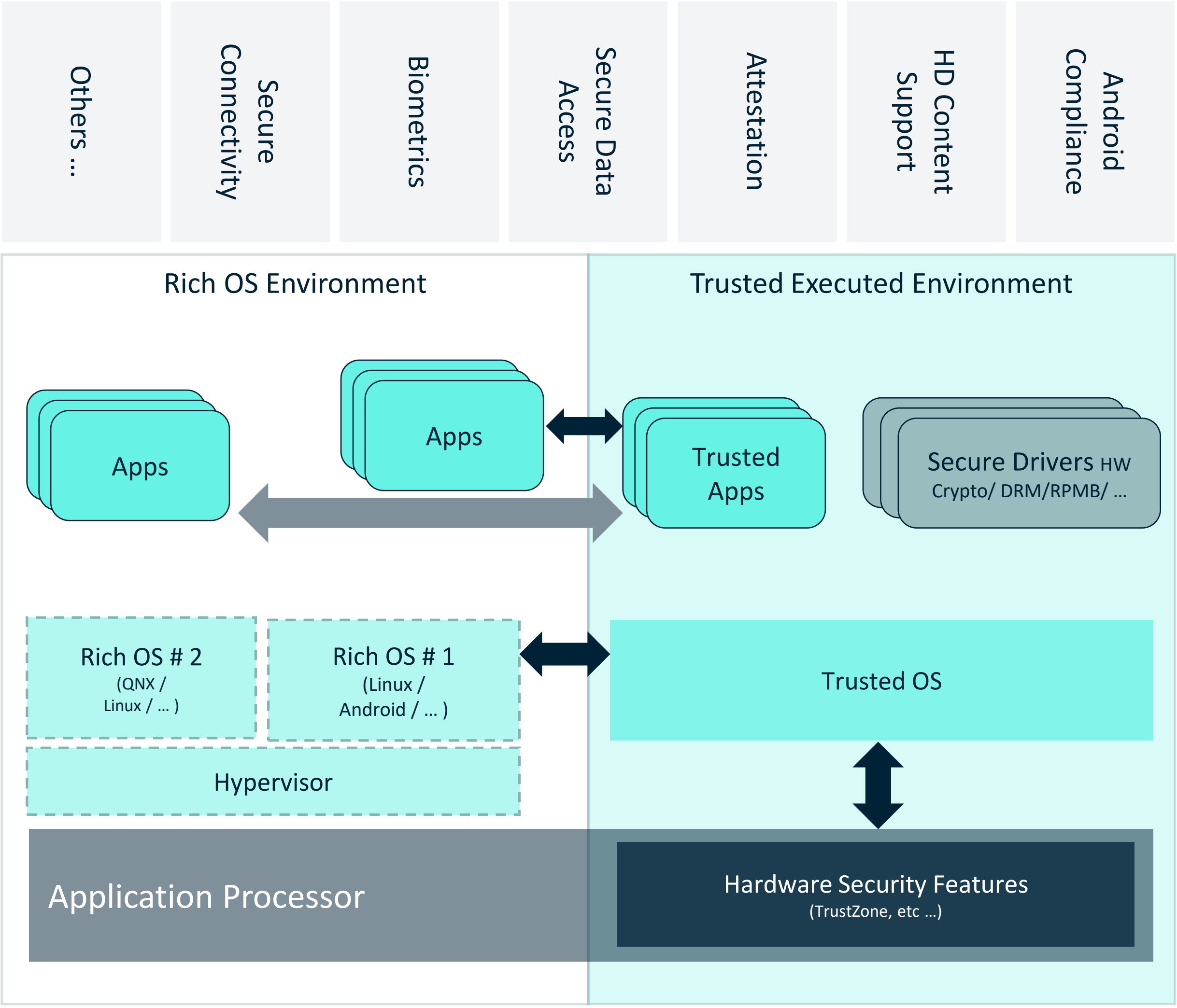
- Multiple laws including
  - Technical requirements for vehicle cybersecurity （2024）
  - The Data Security Law (DSL) (2021)
  - The Personal Information Protection Law (PIPL) (2012)

A Trusted Execution Environment (TEE) Overview

A Trusted Execution Environment (TEE) provides a secure enclave to isolate and protect custom code and data

Benefits include:

- Hardware security with zero additional hardware cost
- Hardware root of trust
- High performance with very large memory
- Ability to run secured Trusted Applications (TAs)
- Privileged access to ECU peripherals



Others ...

Secure Connectivity

Biometrics

Secure Data Access

Attestation

HD Content Support

Android Compliance

Rich OS Environment

Trusted Executed Environment

Apps

Apps

Trusted Apps

Secure Drivers HW
Crypto/ DRM/RPMB/ ...

Rich OS # 2
(QNX /
Linux / ...)

Rich OS # 1
(Linux /
Android / ...)

Trusted OS

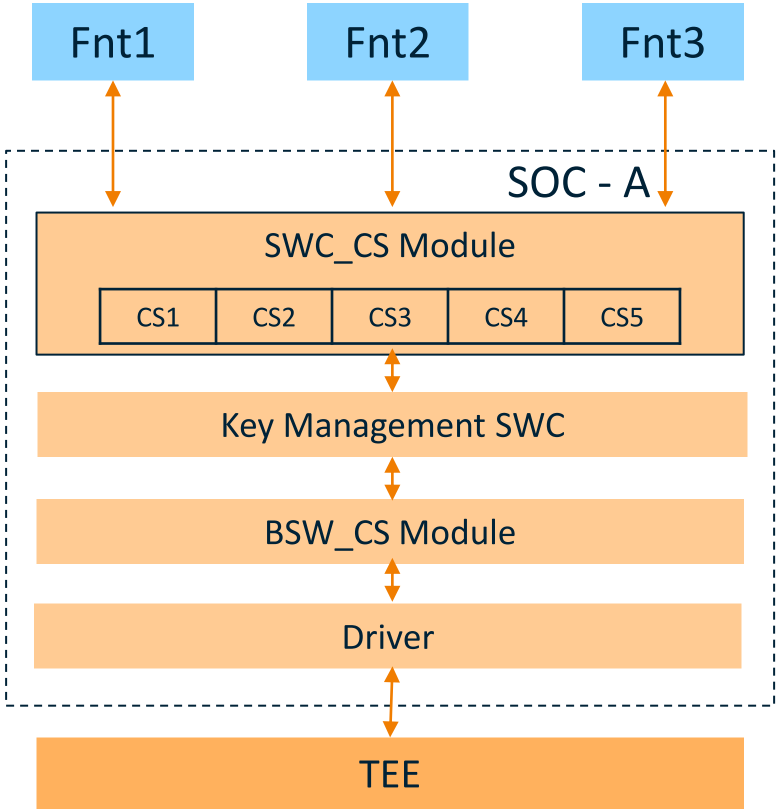
Hypervisor

Application Processor

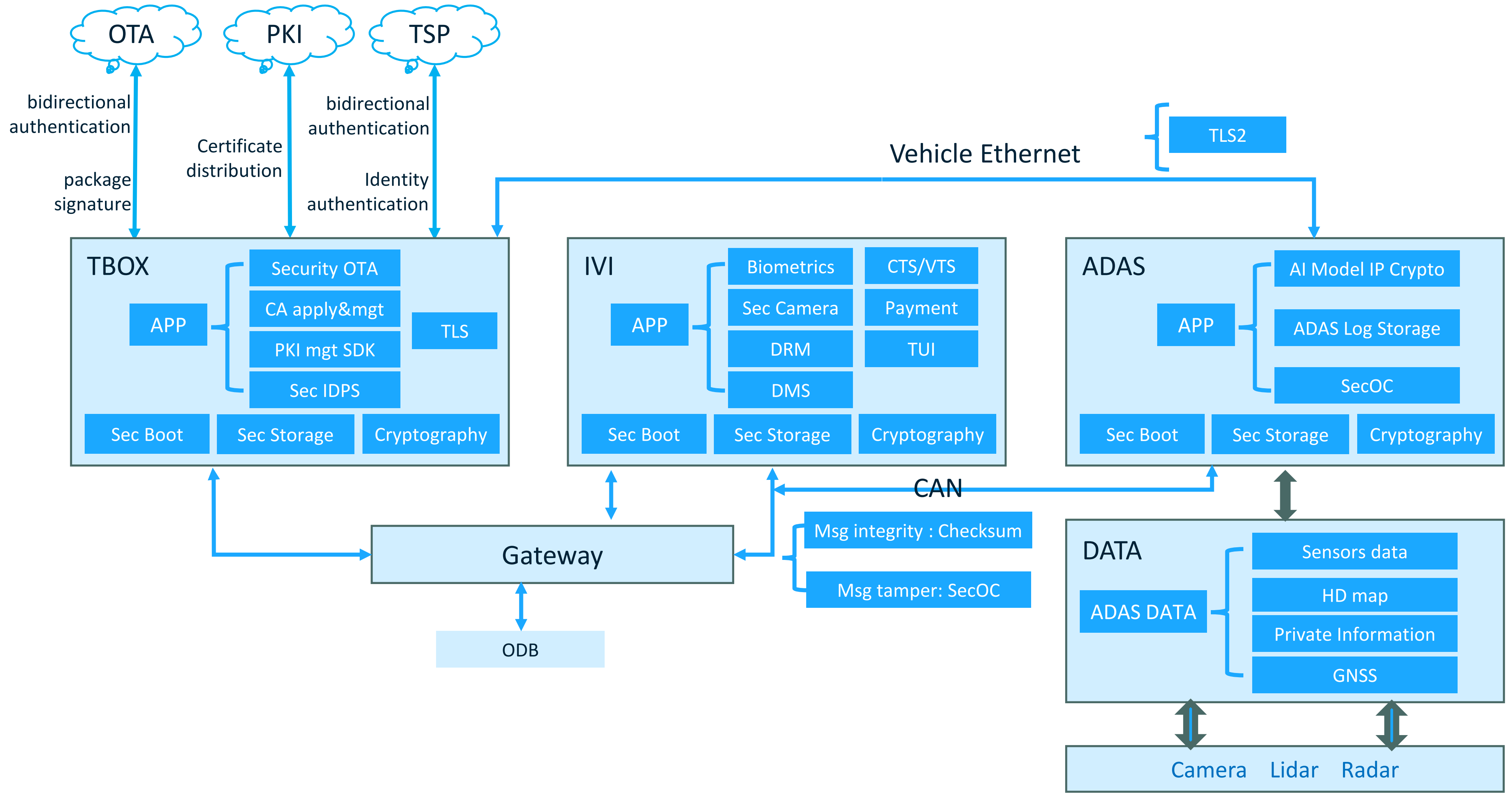
Hardware Security Features
(TrustZone, etc ...)

TEE Meets Next-generation Hardware and Software Integration

- TEE is the fundamental component and solution to meet the next generation of connected vehicles
- The benefits of TEE solution:
  - TEE focus on SOC Security
  - Simplifying Architecture, more flexible system solutions
  - Standard solution to cross multiple SOC, by-pass the HW compatibility
  - Trusted Application（TA）to protect the code/IP
  - Lowering cost
  - Improved performance
  - Possibility of extended use-cases
  - Crypto agility and updateability
  - Reducing risk on supply chain

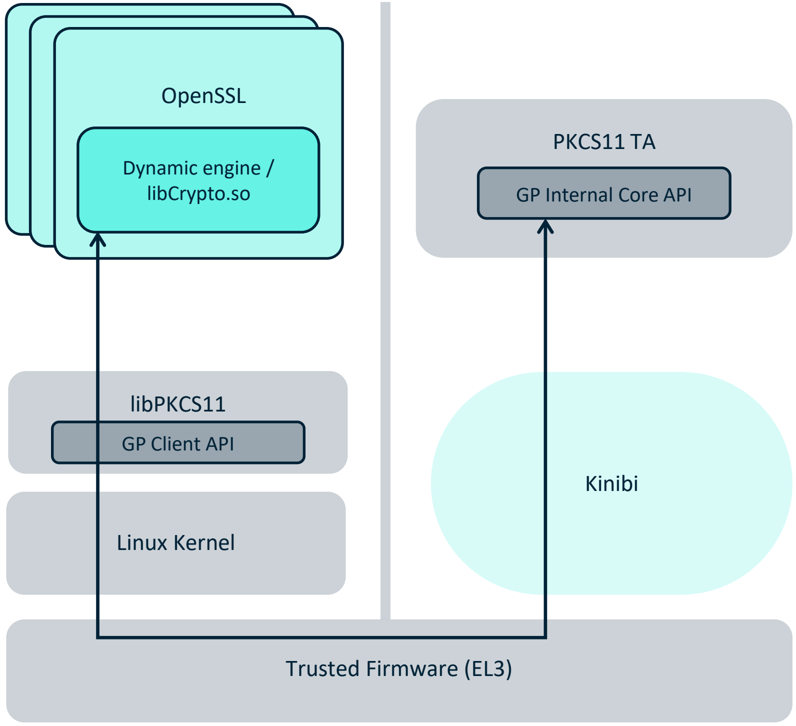


Vehicle Security Architecture Design



TEE HSM / Crypto Provider

- Isolate core crypto stacks and keys inside the TEE.
- Can be used to protect communication, storage etc
- Wide range of crypto support
  - Random number generation
  - SHA224, SHA256, SHA384, SHA512
  - RSA (1024-4096)(keygen, key import & export, persistent or transient)
  - PKCS1 v1.5
  - PSS
  - OAEP
  - ECC (P192, P256, P384, P512)
  - ECDSA
  - ECDH
- Can be presented to application via standard APIs
  - PKCS#11 APIs (for OpenSSL etc.)
  - EVITA / 3rd party HSM APIs
  - AutoSAR Crypto APIs
  - Custom APIs suited to application needs



(PKCS#11 Example)

Enhanced Secure OTA :
Authenticating peers and defeating the disassembly attack

- Main OS remains in control of major functions
- Security-critical functions delegated to TA executing in TrustZone

- TA acts as gateway, transparently providing fully secured channel with mutual authentication
- Binding between APU and UICC / SHE established in factory using vehicle-unique keys

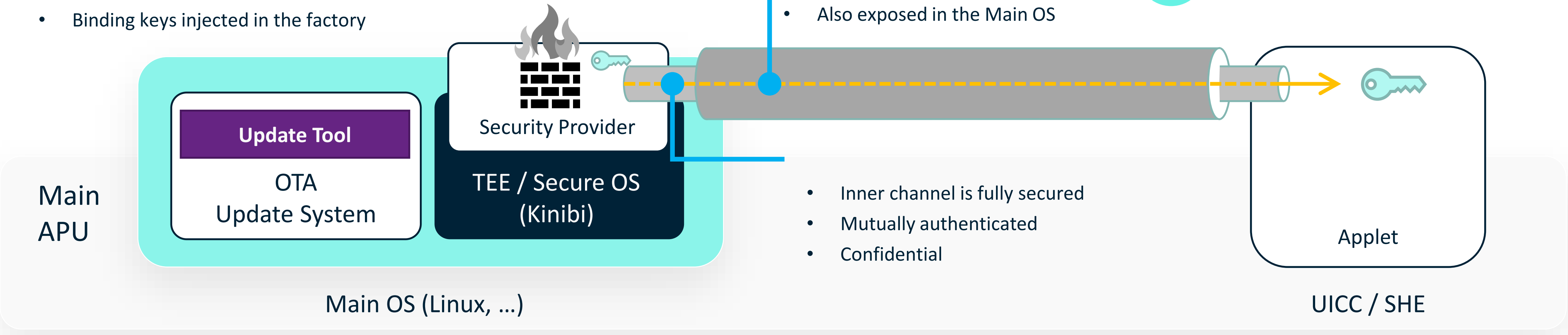
- TrustZone-protection means secure channel keys cannot be extracted
- Secure code execution in TrustZone ensures ‘unwrapped’ secure channel cannot be observed
- Renders disassembled peripherals worthless

Regardless of peripheral connectivity

- Supports on-board peripherals, typically SPI or I^{2}C-connected
- Supports off-board peripherals, i.e. via Ethernet or CAN
- Binding keys injected in the factory

- Physical channel is exposed on the PCB
- Also exposed in the Main OS

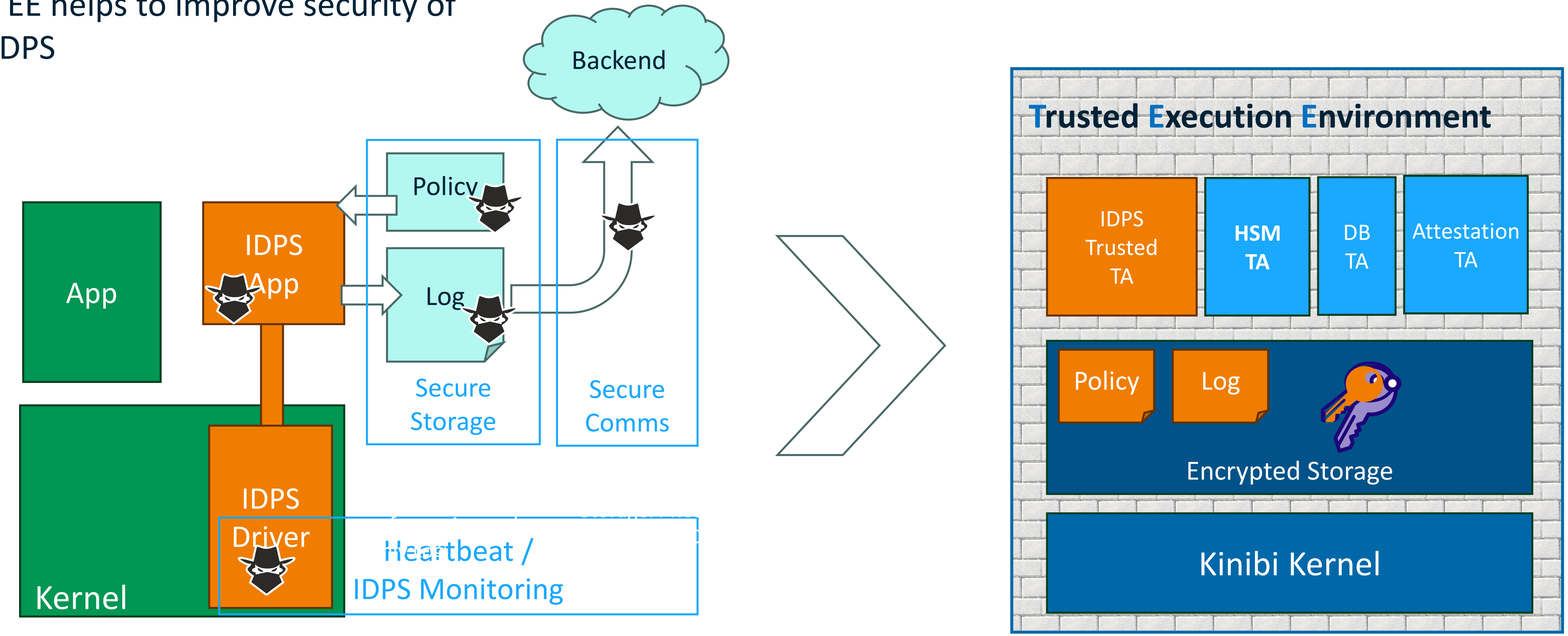
→ This exposure creates the need for security



- Inner channel is fully secured
- Mutually authenticated
- Confidential

TEE Based IDPS Architecture

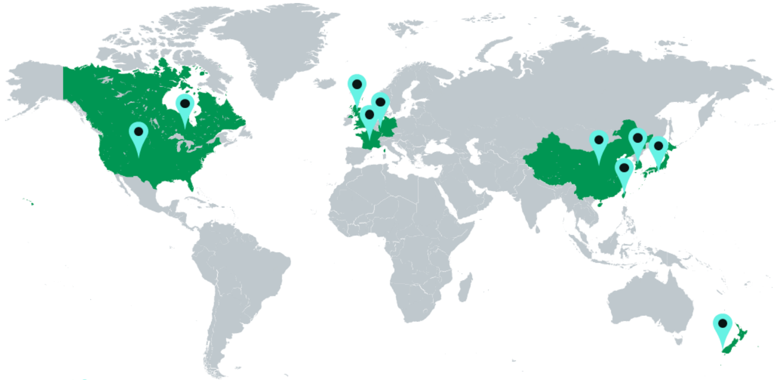
- TEE helps to improve security of IDPS



TRUSTONIC

Fast Facts

- Founded by ARM & Gemalto in 2012, **leading TEE technology development**
  - Focused on accelerating Trustonic's growth
  - The GP TEE Committee is chaired by Richard Hayton from Trustonic
- Deployments in 20m+ vehicles on-road
  - Additional 60m+ additional vehicles under contract
  - 2bn deployments across all device types
  - Zero reported breeches
  - Support options for 10 & 15 years
- Global operations and support



2 BN+

Devices

120+

Patents

80M+

Vehicles

GLOBAL SILICON PARTNERS

SAMSUNG RENESAS siengine 芯擎科技 NXP

MEDIATEK TEXAS INSTRUMENTS MICROCHIP NVIDIA

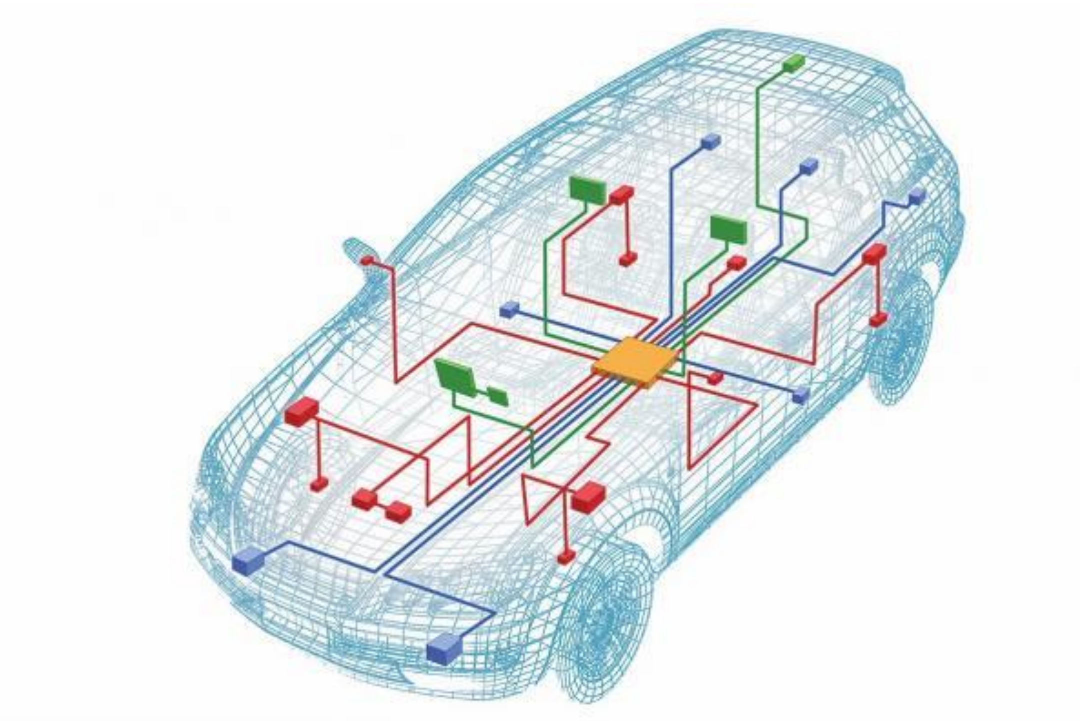
HARDWARE BACKED SECURITY: TRUSTED EXECUTION ENVIRONMENT

EMVCo Common Criteria FIPS VALIDATED 140-2 SECURITY VISA GLOBALPLATFORM

Trustonic wide Application Scenarios and TAs

Trustonic provides a leading portfolio to the global market

- The TOP TEE vendor to support you and your customers around the world
- Trustonic TEE OS has the best technical capabilities, performance, security, reliabi and a variety ecological partners in the market
- Trustonic TEE is generally integrated into mainstream international vehicle-mount chips, including TI, NXP, Renesas, MTK, SAMSUNG, SiEngine, NVIDIA.



Application Scenarios

- The following OEMs and Tier 1s use our solutions for multiple use cases
    - IVI Systems, Security OTA, TEE-Based HSM, T-BOX, Gateway, Digital Car Key
    - Used by BMW, Honda, Aptiv, Panasonic, Nissan, Toyota, Vinfast, Suzuki, Daihatsu, DensoTen, Harman, Audi, VW, Porches, JetOpto, Bentley, FIH, Stellantis, Megatronix, GAC-NIO
- Trustonic already supports the following TAs
    - Biometrics TA, Widevine DRM, WeChat, TEE Provisioning, Secure Storage, TUI, GP eSE TEE API, TEE HSM for PKCS11, KeyMaster/KeyMint, GateKeeper

Thank You

Jason Lin

jason.lin@trustonic.com

TRUSTONIC