



DEC 9 2025

# Automotive Key management

Over the last Decade  
R. Lambert ETAS

# Outline

- What did EVITA-light (SHE) get right? How did it evolve? SHE+
- How has the situation changed?
- What can GlobalPlatform key do to emulate EVITA-light's success?

**A look back at  
Automotive  
Key  
Management**

# What did EVITA-light (SHE) get right?

## How did it evolve? SHE+

- 2008-2011: EVITA (E-safety Vehicle Intrusion Protected Applications) was an EU FP7 project: HSM-L, HSM-M, HSM-F
- 2007-2010: SHE (German OEMs, Semis) standardized an HSM-L
- 2010-2015: SHE+ more OEMs notably GM.
- 2015+: SHE+ Dominance.

SHE gave just enough functionality:

- Symmetric key slots, CMAC-AES-128, secure key update, RNG
- Targetted: Secure Messaging and Secure FW & Boot.

SHE+ allowed more keys, plus limitation of what keys could be used for:

- e.g. MAC generation vs MAC verification

# How has the situation changed? (1)

Much more need for asymmetric (public-private key) cryptography, with all its complications

- Fragmented usage
- Each OEM's security architecture uses public key in different ways
- Some standard SW update frameworks, Uptane
- Internet connection requirements: TLS, IPsec
- Automotive Ethernet:
  - favours pre-shared symmetric keys just for ECU startup timing

# How has the situation changed? (2)

- Newer standards such as ISO 15118-2,-20 have explicit key management components
  - Explicit private key injection
- Asymmetric crypto has more complexity to manage: secure clocks, certs chains and PKIs, cross signing
  - Certificates and Key Usages can emulate the restrictions that SHE+ allowed
  - CSRs include proof of possession and support non-repudiation
  - Root rollover and Crypto agility (PQC relates here too)

# How has the situation changed? (3)

- Automotive use cases are more architecturally diverse than mobile:
  - Some datapath keys need loaded: MACSEC or SecOC keys: getting keys to switches
  - Multiple ECUs need to be keyed which come from possibly different Tier1s
  - Need to plan for repair/update and replacement
  - Centralized ECUs
- AUTOSAR has subsumed the SHE+ standardization, along with its Key Manager (KeyM)
  - Need to more than that to be successful
  - AUTOSAR classic targets more legacy platforms, but can still be inspirational

# What can GlobalPlatform key do to emulate SHE's success? (1)

- Give just enough for the new situation
- Fast usage of symmetric keys
  - Fast datapath or connection to another datapath (e.g. auto ethernet switch or phi)
  - Proof of update
  - Usage restrictions (e.g. MAC generate vs verify)

# What can GlobalPlatform key do to emulate SHE's success? (2)

- Similar Public Key facilities:
  - If tied to a Certificate key-usage can restrict usage
  - CSR generation to ensure non-repudiation and proof of possession
  - PKI Certificate Chaining and Management, Understanding Cross-Signatures
  - Revocation and Online Status Checking
  - Secure clock capabilities
  - Basic security protocols such as TLS or IPSec, tunnel extends right in
  - Root changeover
  - Algorithm migration capabilities
  - Secure Key Server capabilities to setup keying across different ECU or domains. E.g. Automotive ethernet keying



**Global  
Platform<sup>®</sup>**

Securing the digital future

→ [globalplatform.org](https://globalplatform.org)