



Lessons from deploying Secure Services Across Multiple Mobiles

Gil Bernabeu, CTO, GlobalPlatform



Reach: all smartphones shipped in Europe feature at least one eSE, SIM or eSIM. The momentum for eSIM shows a tremendous penetration rate in the short term, as summarized in the table below:

Close to half a billion eSIM-capable devices were shipped worldwide in 2023 ¹²	Over 9 billion eSIM-capable devices to be shipped worldwide by 2030 ¹³	Nearly 70% Proportion of eSIM-capable cellular devices by 2030 ¹⁰	474.2 million Projected eSIM smartphone shipments in Europe by 2028 ¹⁴ for an EU population of 448.4 million ¹⁵
---	---	--	--

What's the market trend ?

Key drivers

- Mobile Payments:**

eSEs are crucial for securing mobile wallets and financial transactions.

- Identity and Data Protection:**

They are used to protect sensitive data and perform secure identity verification.

- Emergence of eSIM:**

The increasing adoption of eSIM technology fuels demand for integrated secure elements for remote provisioning and subscriber authentication.

- Connected Services:**

Smartphones are becoming central to other connected services, such as unlocking cars, which requires a high level of hardware-based security.

**Secure
Elements are
embedded in
smartphones
and provide
more and
more secure
services
going
forward**

Member State

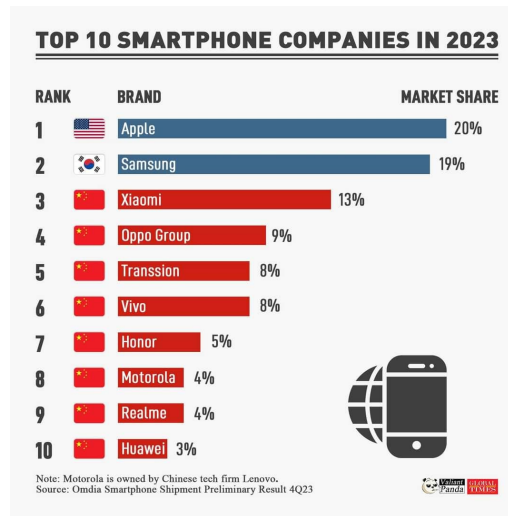


Smartphone



Citizen

27

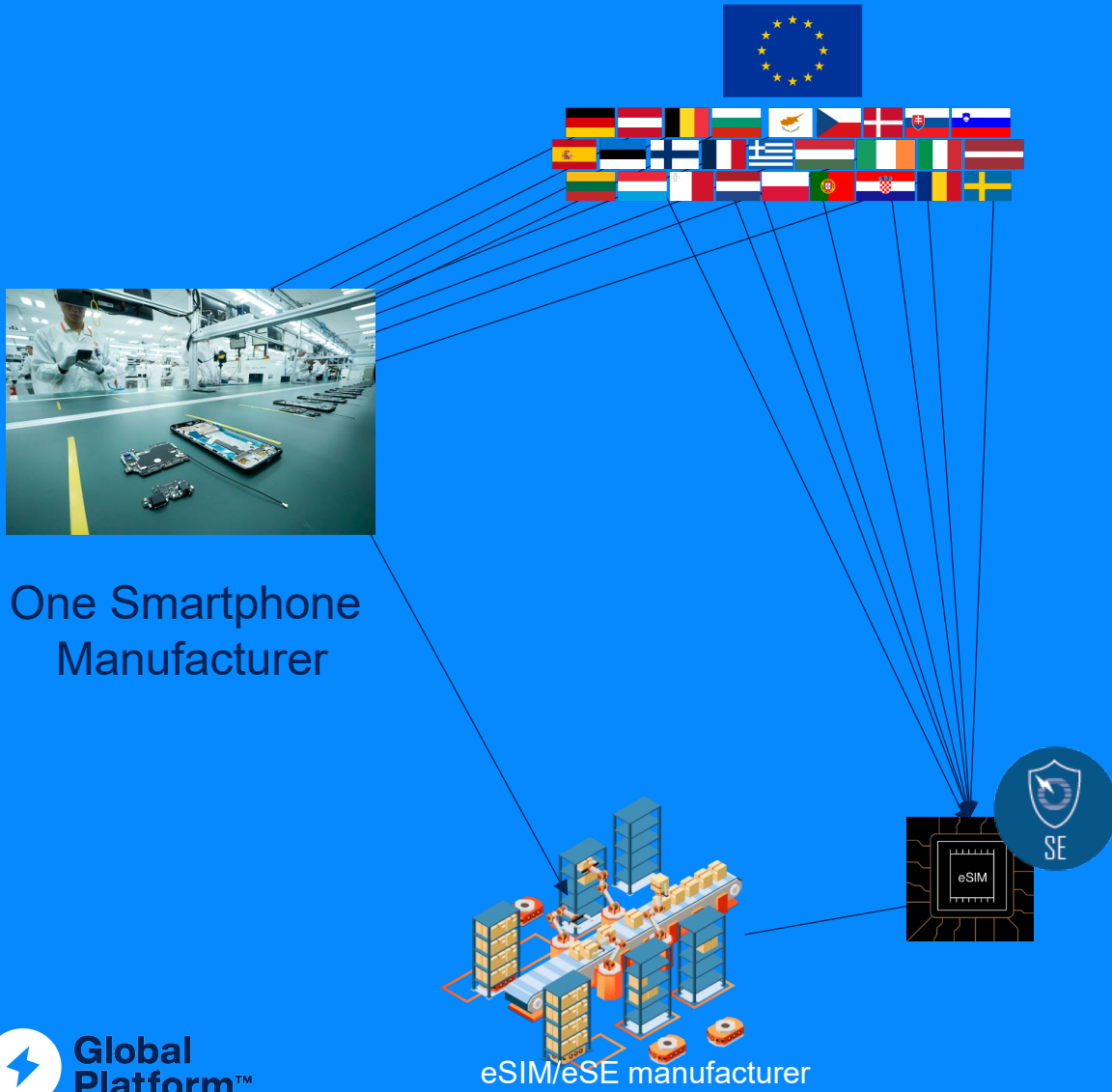


A smartphone stays in the field around 7 years

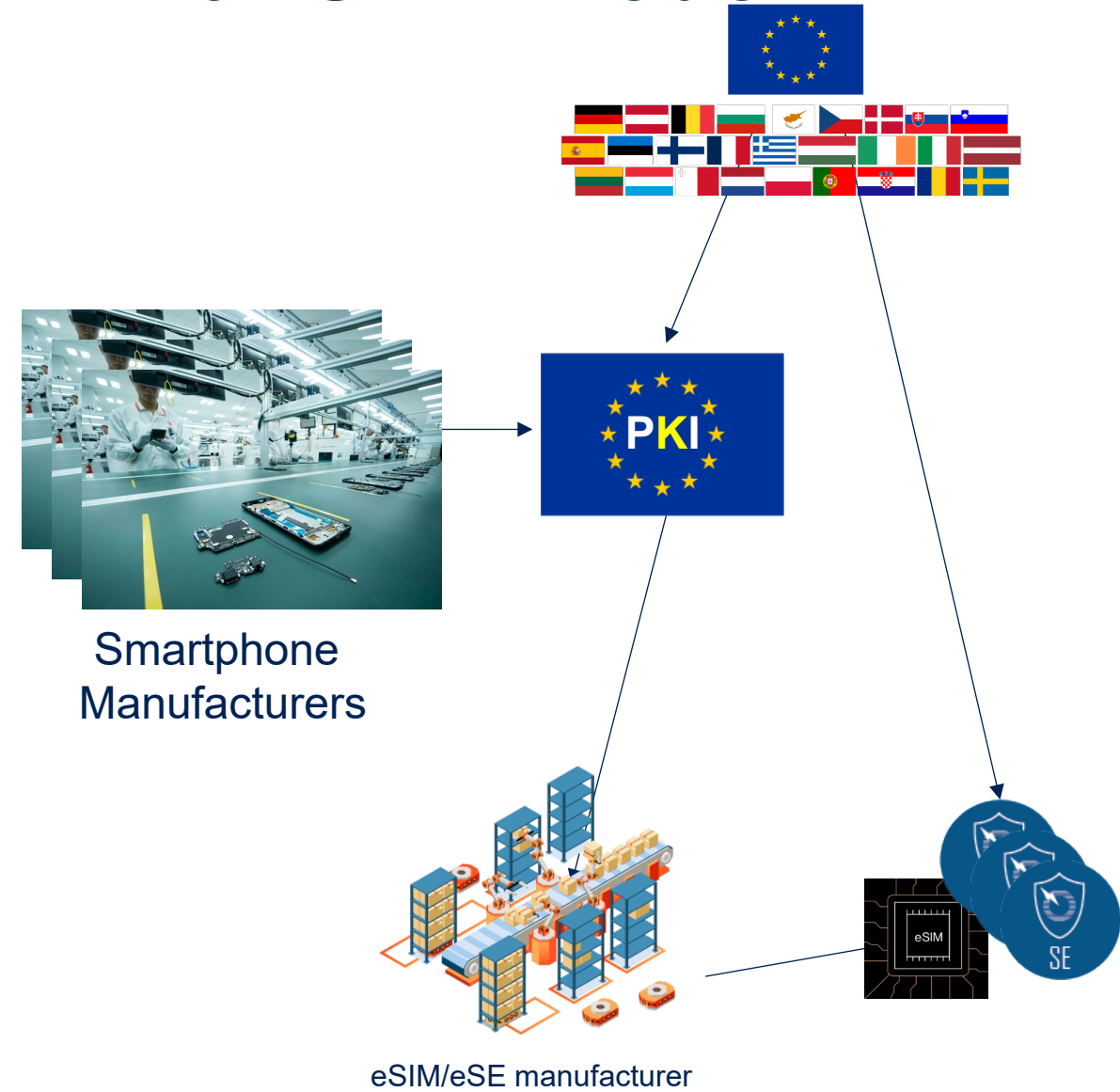


Current eIDAS2 regulation requires high level of robustness (AVA_VAN.5)
Secure Element must be CC certified at least EAL 4 or 5+

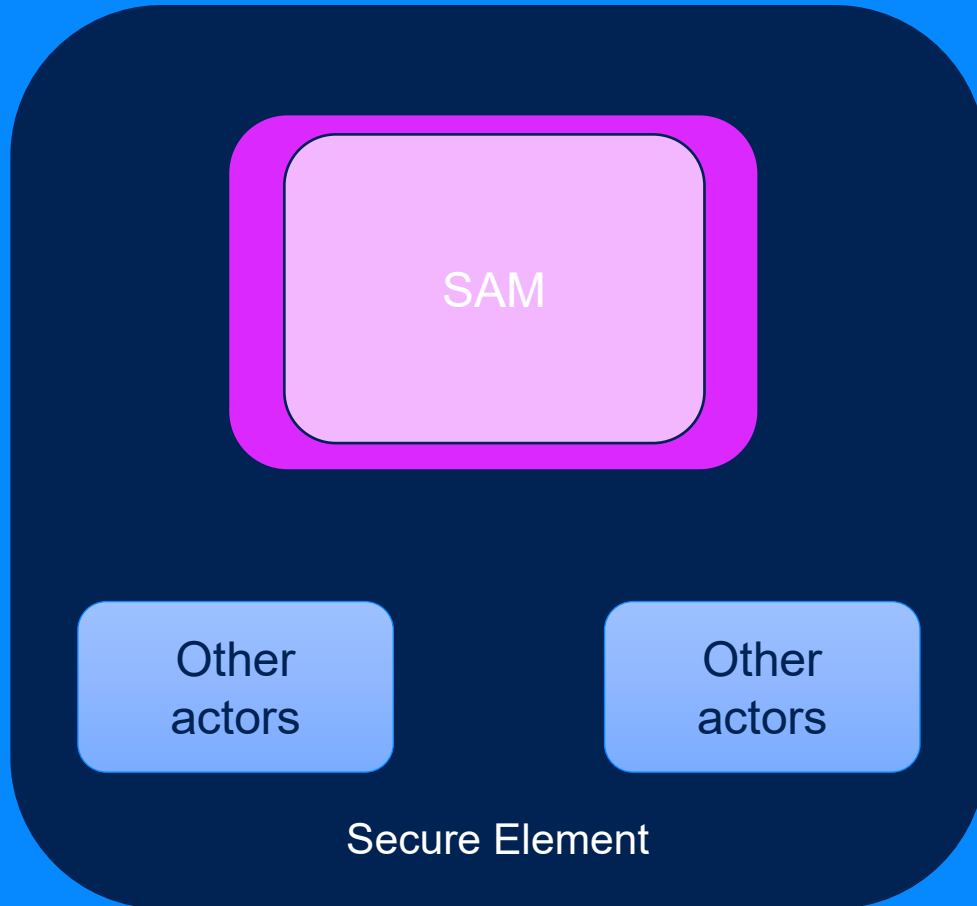
Key management



With SAM Model



SAM

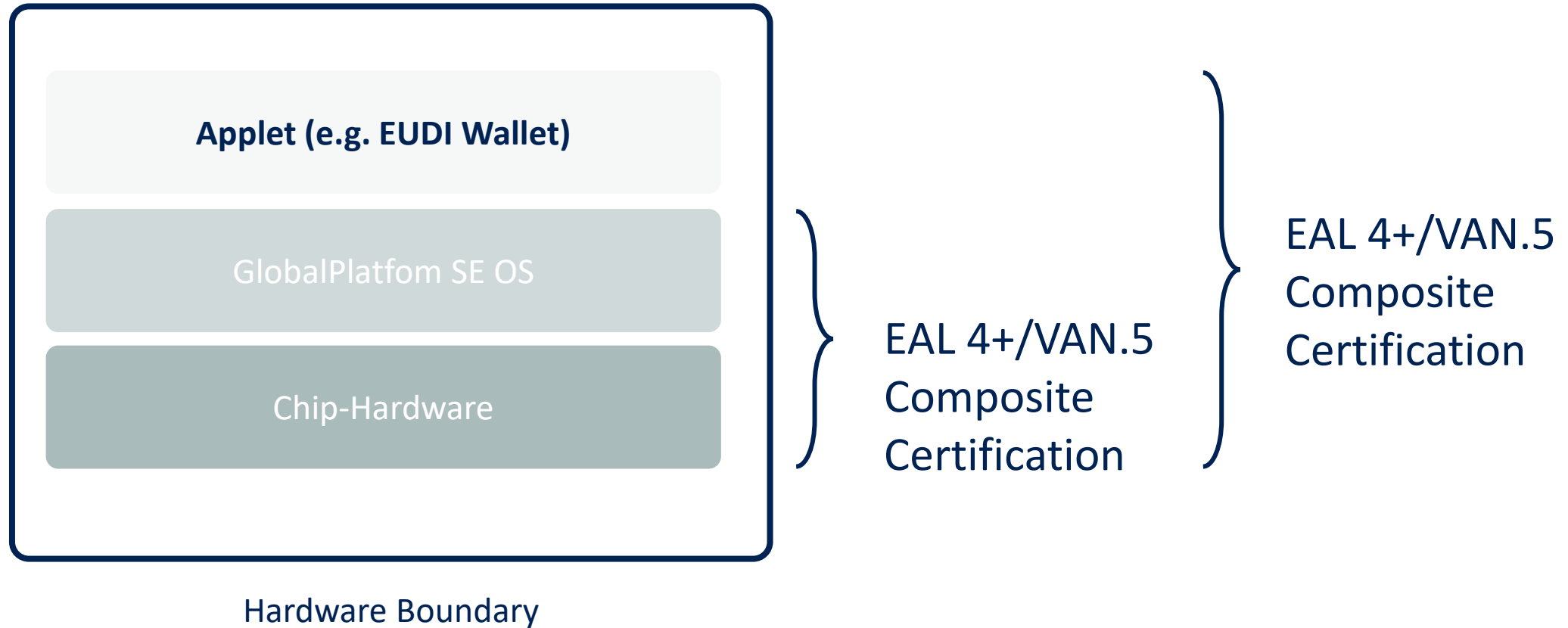


is

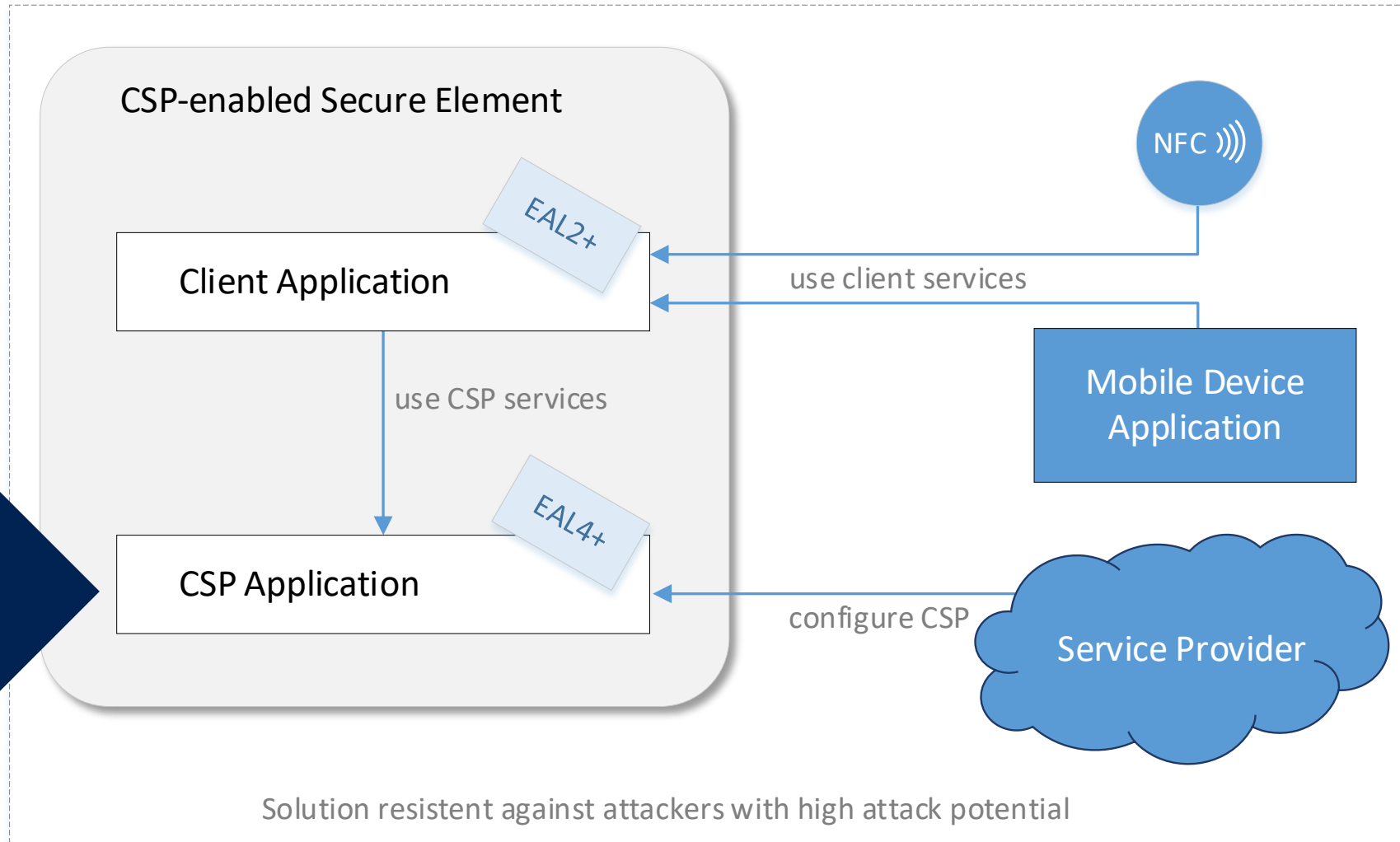
An isolated environment within a eSE or eSIM

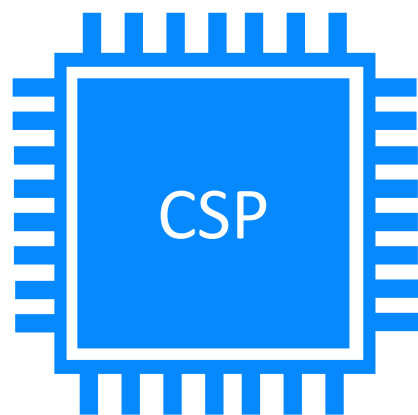
- **Independent Administration based on certificate**
 - All actors (Service providers, platform, SE manufacturers) are checked
 - Host 3rd party on card services
 - CASD
 - Additional security protection
 - Multiscope Protection profile
- SAM PKI confirm that all rules are applied by the actors by generating the certificate that are shared inside the eco system

Current approach to smart card certification



Simplify Client Application to a trivial TOE.



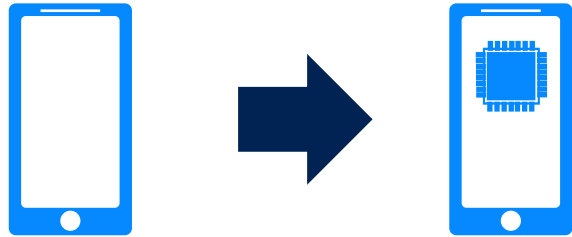


- secure key storage & use
- high level crypto protocols (PACE, EAC etc.)
- secure storage
- PIN/PUK management
- secure messaging
- configurability
- easier CC-certification

The CSP operates similarly to an HSM for mobile platforms.

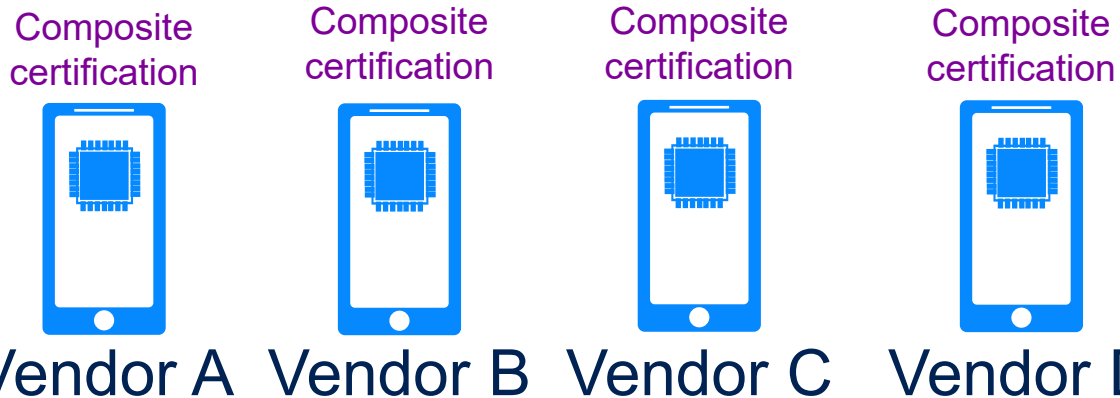
- CSP-internal Key Management:
 - Client Application does not handle keys. It uses cryptographic CSP services (e.g. signing, encryption) without providing keys.
- CSP Provides high-level cryptographic services:
 - E.g., complete authentication protocols (mDL-ECDH, EAC, PACE-CAM),
 - Attestation, Key Derivation, Key Agreement, Secure Storage, etc.
- CSP handles security-related work-flows inside the CSP
 - Password Retry-Counters, PUK check for unblocking a PIN, Attestation signatures for associated keys, etc.

Composite certification (Applet with platform) is required for applet when targeting EAL_VAN.5 level of robustness.

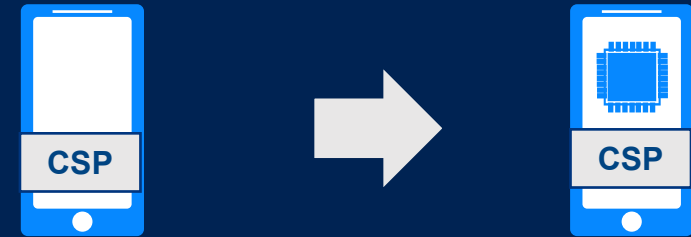


Platform certification Composite certification

Composite certifications do not scale in a multiple vendor deployment



The Cryptographic Service Provider (CSP) is a self-contained component that includes software, firmware, and hardware of a CSP-enabled Secure Element.



Platform certification 1 unique "composite" certification

Only one "EAL+++>" allows to be deployed in any CSP-enabled platform



SAM

SAM (Secured Applications for Mobile)

- Enables hosting 3rd party applications, such as the WSCA, on (e)SIMs independently of the GSMA or Mobile Network Operator

All actors are part of the same PKI that allows to verify certification requirements and administration rights

SAM Configuration, v1.0 (March 2024)

CSP

CSP (Crypto Service Provider)

Enables post-issuance installation of an EUDI Applet (WSCA) without the need for composite certification, **while the combined security of the applet and the CSP still achieves an overall security level comparable to EAL4+ VAN.5**

GP Card Specification – Amendment N (Late 2025)

Two EUDI Wallet enablers

- Designed for future use with EUDI, but **equally relevant for broader digital wallet and identity ecosystems.**



A certified Secure Element, provide with a standardized and certified execution environment in all smartphone

SAM provide a central model of certificate that simplify the Key management across smartphone and additional independence for administration and security

CSP allows to reach high level of security without the complexity of the multi-platform management