May 2026

Cost Benefits in Reusability of Standardized Hardware Protected Security Environments

Bill Mazzara, Craig Rawlings

Stellantis
GlobalPlatform Board Member
Automotive Task Force Chair

v5

Agenda

Focus on Differentiation

Standardized Solutions enables OEM to focus on Product Differentiating Functions

Certification

Yes certification will cost more for the first product
Certification is performed once for a product and may be performed incrementally for next gen products vs. pen testing for each ECU development cycle saving ECU development costs and time.

Certainty

Certification provides program certainty
Shift Left uncertainty of development
Transferability of certification
Achieve Higher orders of Complexity with certainty of a foundation built on GlobalPlatform

Reuse

Industry shift to leverage cybersecurity expertise
Objectives of Software Defined Vehicle : Separation of Software and Hardware
Supply Chain Agility

Achievablity

Builds on 15 years of Auto Industry evolution of Cybersecuirty
Leveraging 25 years of GlobalPlatform Experience

Standardized Solutions enables companies to focus on Product Differentiating Functions

Cost : NRE and Unit Cost Reduction through reuse of commodity

Solutions certified to universal metrics.

– Also Mitigates surprises of novel cybersecurity Laws and Regulations that prompt product changes. Transferability of certification across jurisdictions

Quality : Certainty of supply and interchangeability of source

Enables Software Ownership and maturation of solutions over time

Platform of compatibility for improved interoperability of solutions.

GlobalPlatform is Key to Total Customer Experience

Timing : Enables innovation of higher orders of

complexity reduction of development time for new high-tech features.

Platform for integration of multiple solution sources

Standardized Solutions enables companies to focus on Product Differentiating Functions

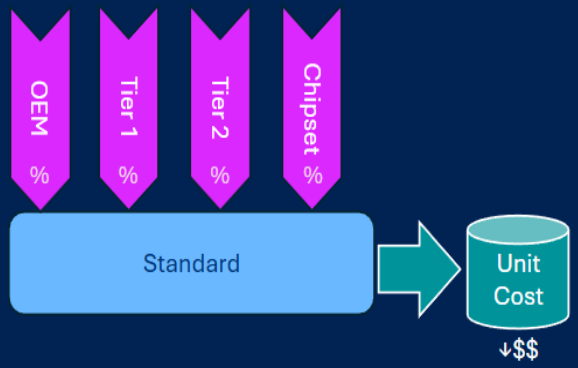
Reduction of Effort for Cybersecurity

Certainty of Supply

Transferability of Certification

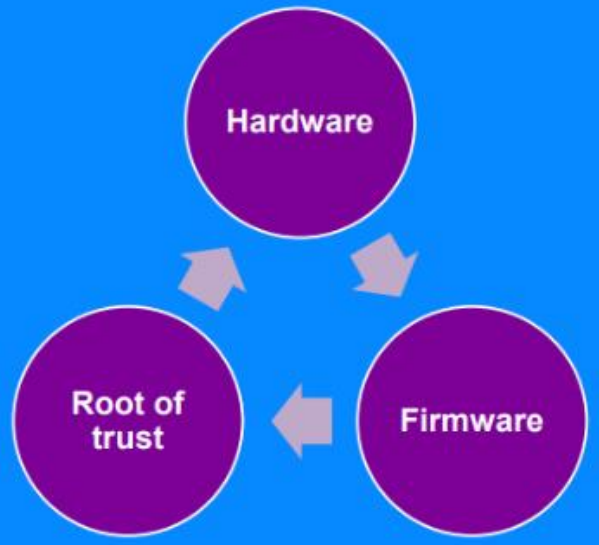
Enable systems with higher orders of complexity

Product Identity and Access Management



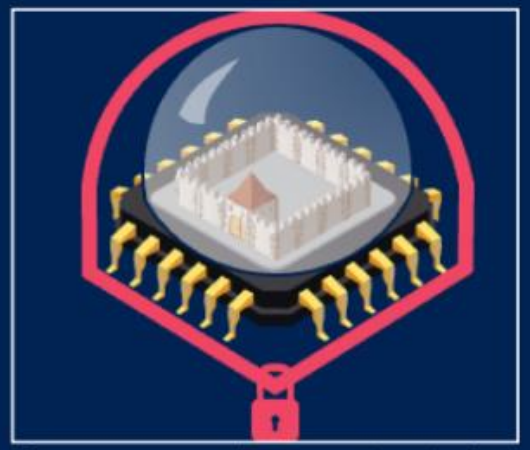
- Unit Cost Reduction through reuse of solutions industry wide

GlobalPlatform Foundation Technologies



Protect Keys, Applications, AI
Remote update

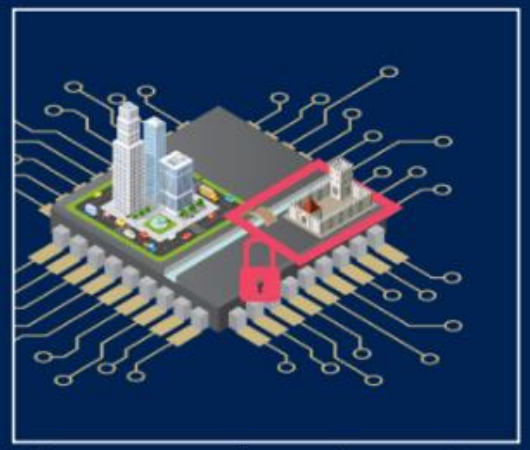
Secure Element



A secure enclave protected against physical and software attack

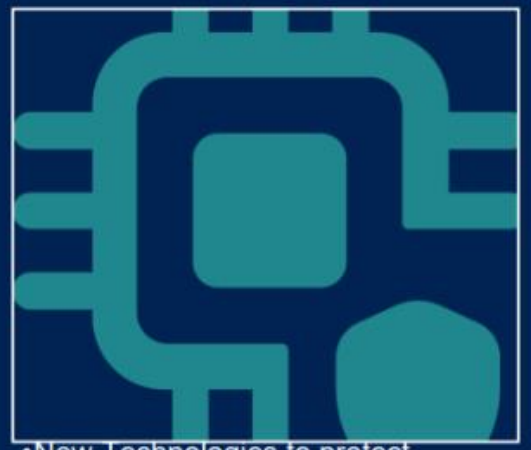
- Tamper resistant hardware
- Example Existing Use cases:
  - Digital Car Key
  - Electrical Vehicle Charging
  - All eUICCs (embedded Sims)
  - Key Management

Trusted Execution Environment



- A secure operating system running on a standard CPU alongside regular OS/Applications
- Protected against attack by hardware chip features + software mechanisms
- Example of Existing Use Cases:
  - Digital Rights Management / Media for Advanced Infotainment
  - Protecting High Value Assets such as ADAS
  - Key and Certificate management
  - Personal Data and Biometric

Isolated Technologies



- New Technologies to protect isolated execution environments
- Chipsets offer new security services and isolation mechanisms
- GlobalPlatform focus on simplifying access to security services and security evaluation
- Extending the range of SE and TEE offering to address different implementation market needs

- Runs a full operating system providing standardized APIs and functions
- 3rd party Security Certification
- Full support for App and OS update over-the-air

Global Platform®

Extending GlobalPlatform SESIP Ecosystem

Certification Bodies

TRUSTCB

SGS brightsight

2 potential new certification bodies under review

SESIP Industry Adoption

CARCONNECTIVITY consortium

DTSec

csa connectivity standards alliance

GSMA

cen

ETSI

qi

SESIP Labs

Applus

BCTC 国家金融科技测评中心 National FinTech Evaluation Center 银行卡检测中心 Bank Card Test Center

brightsight By SGS

DEKRA

OPLS Lab

ESEC LABORATORY

INSTITUTE FOR INFORMATION INDUSTRY

KEYSIGHT

SERMA SAFETY & SECURITY

THALES

SESIP Regulatory Alignments

Cyber Resilience Act,
US Cyber Trust Mark

Existing Industry Profiles

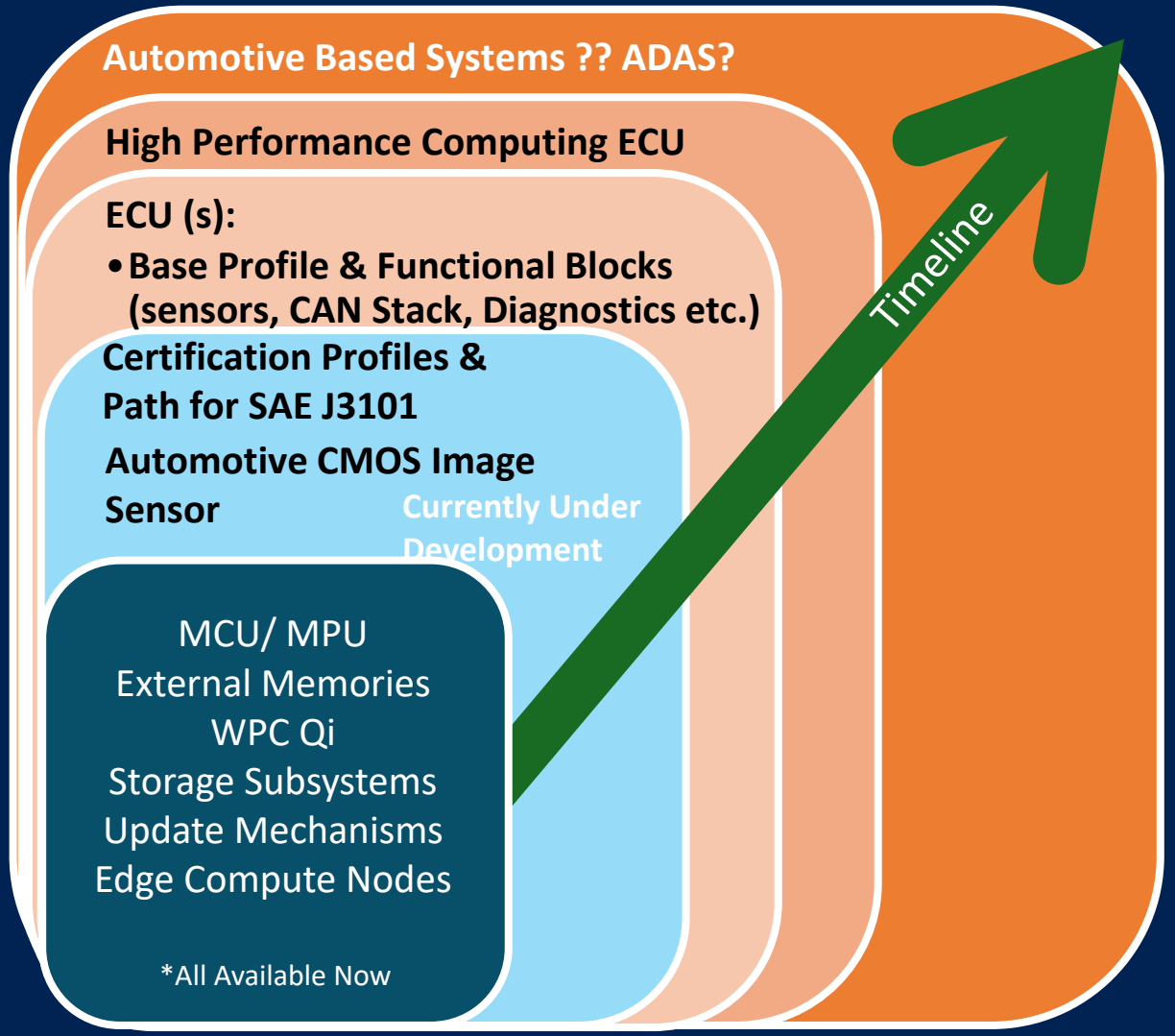
- Secure MCU/MPU
- Secure External Memories
- WPC Qi Secure Storage Subsystem
- Edge Compute Node
- Code Update Mechanism

psacertified™

GlobalPlatform assumed governance of PSA Certified

SESIP Automotive Profiles Roadmap (illustrative)

Useful Next Profiles?



Certainty of Program Development

Shift Left Development Timing Risk

- Pre-qualify solutions
- Certification before System Pen Testing

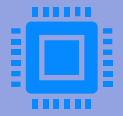
Transferability of Certification

- SESIP Certification instead of market specific testing
- Audit of prior results

Achieve Higher orders of Complexity

- Certainty of a foundation built on GlobalPlatform Technologies
- Composite Certification Built on past

Certainty of Supply



Device Identities

Creation of a "birth certificate" for every part

- By serial number

A Device becomes enabled to act on its own security

Attestation of parts

Ability to authenticate the source and history of any part

- Before installation
- Before service delivery
- Before Upgrade

In person and Over the Air

Authentication of data

The Individual data collected by a specific part can be authenticated to that part

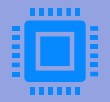
Also Enables confidentiality of customer private data from its source

may be relevant to data integrity and traceability for AI applications.

Global Platform®

STELLANTIS

Industry Wide Reuse



Leverage Expertise

Cybersecurity expertise not automotive expertise learned cyber

Cross industry proven solutions

Software Defined Vehicle Portfolio

Separation of software from hardware

Reuse of trusted application across portfolio

Refinement

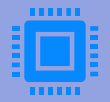
Reuse of trusted applications across generations

Improved Quality assurance

Global Platform®

STELLANTIS

Supply Chain Agility



Supply Chain Robustness

Pivot to other certified sources after disruption

Redundancy of supply to address shortages

Diversity of Source

Localized supply to address supply chain regulation

Agility in response

Pivot to other sources in response to Cybersecurity Incidents

Availability of compatible response mechanisms

Evolution of Hardware Security To GlobalPlatform

Automotive Security Standardization has been in progress for 15 years

SHE (2009)

- Full Crypto System
- Proprietary Solutions

HSM (2013)

- Proprietary Implementations
- AutoSAR Compatibility

HTA (2015)

- CS.00098
- Make Common use of tech (SHE & HSM)
- Unique to FCA (Most OEMs had their own)

SAE J3101 (2020)

- Recommended Best Practices of Industry Common Requirements

J3101-1 (2024)

- AutOSAr Mapping
- Implementable specification of Hardware Security

J3101-5 (2025)

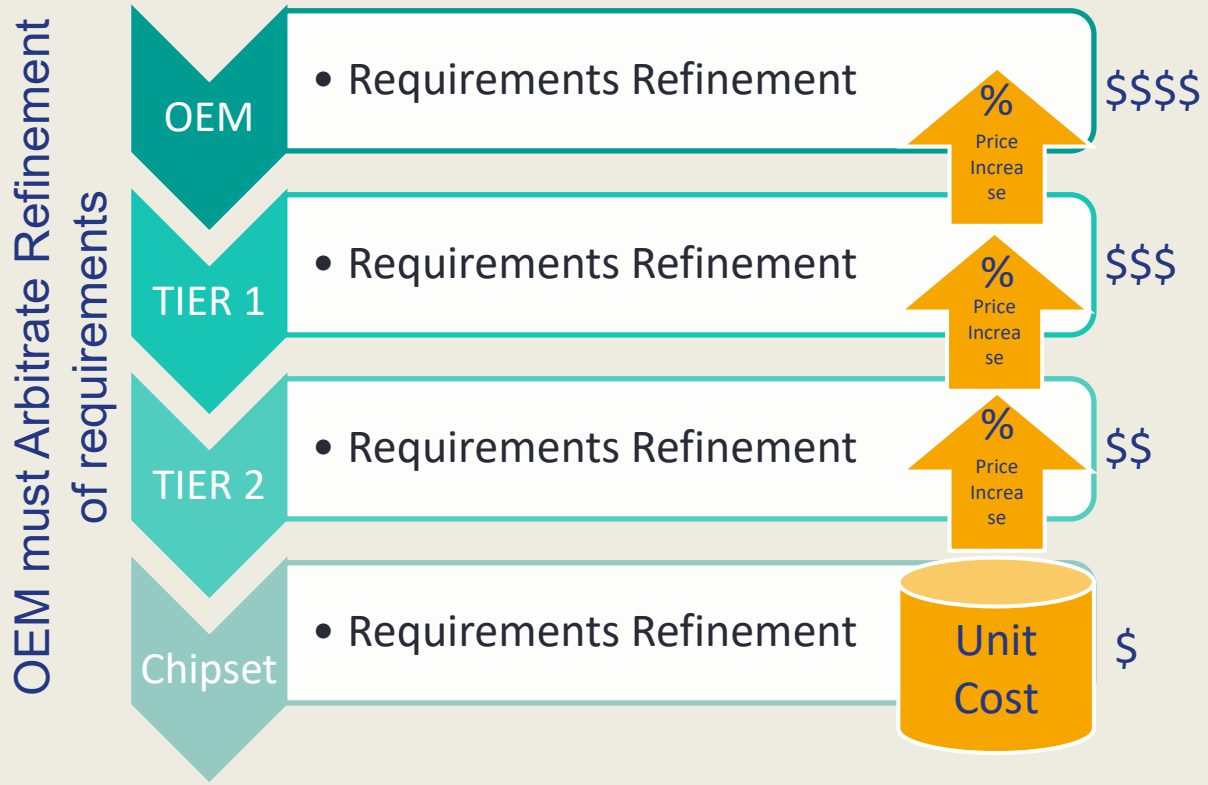
- GlobalPlatform Mapping
- 99% coverage
- Achieve traceability of GlobalPlatform Requirements to AutOSAr implementations

SESIP Certification (Future)

- Automotive Profile based on current industry common requirements
- Industry universal measurements of solutions
- commodity markets (NOT unique to STLA)

Standardization Leverages Common Requirements: Reduction in Efforts

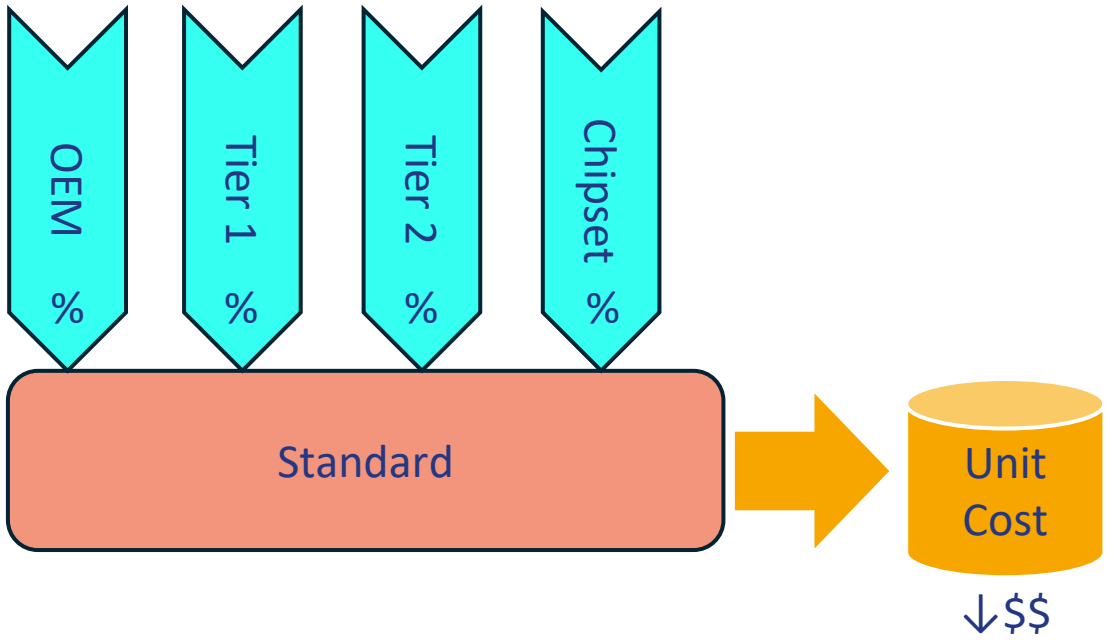
Proprietary HSM



Price Increase : Customer Specific Requirements & Time for Interpretation of Requirements

(HSM = x) * (Chipmaker +30%) * (T2 +30%) * (T1 +30%)
= 2.2 * x

GlobalPlatform HPSE



Standardized Specific Requirements from each contributor (OEM, Tiers) :
No Redundancy of Efforts

(GP HPSE = $x) ➔ **$x**

Per Chip Cost Comparison (illustrative)

Automotive HSM = $6 ~ $10 / chip

The integration of a Hardware Security Module (HSM) into an automotive System-on-Chip (SoC) typically increases the hardware cost of that component by approximately **15%**. In practical terms, this means that for a high-performance microcontroller, adding an HSM can increase the unit cost by **roughly $6 to $10** (e.g., from $41 to $47, based on Infineon Aurix examples).

- No standards for cybersecurity metrics, assurance, workflows, Secure OS, or Trusted Applications development – often firmware and RoT keys are locked to the Tier-2 chip maker
- No certification, costly one-off blackbox penetration testing is required for each ECU development cycle
- Issues are possible at the end of each ECU dev cycle

IoT Secure Element (SE) = $0.70 ~ $1.25 / chip

Typical secure element (SE) chips for devices like IoT or authentication tokens generally cost between **$0.50 and $2.00 per unit** in high-volume production, with prices sometimes falling below $1 for specific models. Popular, readily available models like the Microchip ATECC608B often cost around $0.70 to $1.25, depending on quantity.

- Standardized HPSE platform with standardized cybersecurity assurance and international lab support
- Multiple vendors for SecureOS interoperable across all chip makers products
- Commodity per chip pricing
- 3rd party and in-house development of Trusted Applications
- SESIP certification – no issues possibility
- BONUS : Protections against fault injection & side channels