Standardisation of Hardware Protected Security Environments

GlobalPlatform Alignment with SAE's J3101: An Opportunity for Japanese Standardisation Alignment

Francesca Forestieri [1] Gil Bernabeu [2]

1) GlobalPlatform, USA

E-mail: francesca.forestieri@globalplatform.org

2) GlobalPlatform, USA

E-mail: gil.bernabeu@globalplatform.org

ABSTRACT:

Standardisation alignment on hardware protected security environments provide an important opportunity to improve automotive cybersecurity, through transparent compliance with global regulations (such as UNECE 155/156) and improved flexibility for common security requirements that meet market demands. GlobalPlatform, an international member-driven standards organization, which has more than 25 years of experience in enabling secure-by-design digital services and devices globally, with Secure Elements (SEs) and Trusted Execution Environments (TEEs). This presentation will discuss how GlobalPlatform has been working together with the Society of Automotive Engineers (SAE) on supporting the specifications and detailed implementation requirements in compliance with the requirements for SAE's J3101 (Hardware Protected Security Environments). This market alignment has the potential to provide the automotive industry, JSAE, and Japanese members a foundation for further alignment on common security standards. This alignment supports vendors and OEMs in focusing their engineering efforts on core differentiators (instead of common security requirements), streamlines requirements for RFPs, and transparently demonstrates alignment with security requirements associated to SAE.

KEY WORDS: Cybersecurity, UNECE 155/156, SAE/ISO 21434, Software defined vehicles,

1. The Evolution of Connected Vehicles

The evolution of connected cars has taken an exponential leap with the move to autonomous driving features, engagement with extended value chains for in-vehicle services, Mobility As A Service (MaaS), and Software Defined Vehicles. This move explicitly requires a robust solution for trusted services that allows for agility in deploying services, flexibility in developing services post-production, evolving cryptography requirements, and the increase in capabilities for security solutions. These needs have the added complexity of not only being relevant for automotive OEM's (and their suppliers) but also for the full value chain.

These developments are leading to more complex automotive use cases with increased and articulated security requirements. Examples include:

- Personal data, privacy and biometrics
- Securing Over-the-Air software updates
- Electrical vehicle charging
- Digital car keys
- Media protection (DRM) and license-based feature activation
- Protecting high value assets such as ADAS software IP
- Securing communications within vehicle and V2X
- Securing the software defined vehicle
- Maintaining trust with Right-to-Repair, controlling diagnostic/configuration access
- Secure analytics for predictive maintenance, fleet management and insurance
- Vehicle and history

As the above list demonstrates, the increase in security requirements around automotive services is growing and therefore, the relevance of standardized technologies is increasing. In fact, Microsoft asserts that the SDV is the largest threat surface in the world:

Figure 1: Software Developed Vehicle Threat Surface as Presented by Microsoft (Source: https://www.microsoft.com/en-us/industry/blog/manufacturing-and-mobility/automotive/2023/10/31/the-security-cultural-transformation-of-the-automotive-industry/)

In particular, some of the overriding requirements associated to these use cases include: Enablement of Chains of Trust Across Software Modules; Secure update exchanges that are INDEPENDENT of the infrastructure and protocol used, allowing both updates to a single device (e.g. car keys) and/or to a group of devices (e.g. update of software); Deployment of new services with standardized APIs in hardware protected environments; Comprehensive and agile lifecycle management: from the production process, during operations, all the way through decommissioning; Portability of services in different trusted operating systems; Management of Multiple Trusted Service Providers: Managing the control of ownership across the value chain and hosting the trusted services of third parties in isolation. ***GlobalPlatform's technologies satisfy these requirements directly and this is demonstrated by the current deployment of Secure Components in vehicles around the world.***

2. Traditional Automotive HSMs

Traditional Automotive HSMs (e.g. SHE, EVITA, etc.) have historically managed a series of security related functions including Cybersecurity, Secure Boot, Secure Logging, Key Negotiation, Etc. The fact that these solutions have been proprietary has meant:

- vendor lock-in (especially critical during the chip shortage)
- a new unique development path specific for each ECU (without the ability to incrementally develop security services)
- lack of Common Hardware APIs
- lack of a common platform administration with multiple Over the Air updates (one to many, many to many, etc.) for OS and firmware
- Lack of neutral, multi-actor security platform services

This approach does not meet the emerging needs of the software defined vehicles.

3. Cybersecurity Regulation & Standardisation

Moreover, the current global focus on automotive cybersecurity (regulations, standards) and other regulatory changes (such as postquantum cryptography) combined with the evolution towards software defined vehicles provides a new context for security solutions.

Regulators are demanding that OEMs prove their solutions meet today's needs and will be updated appropriately and securely to meet tomorrow's requirements. These requirements go beyond SAE/ISO standards supporting UNECE 155/156 (relevant for 64 countries in the world) and extend to Right to Repair Regulations; Privacy – Regulations - e.g. GDPR; National & EU Cybersecurity Acts; Post Quantum Cryptography requirements; Radio Equipment Directive (RED) 2014/53/EU; etc.

The UNECE work of WP29 in defining UNECE regulation 155 & 156[1] has resulted in a series of standards for cybersecurity process management ISO/SAE 21434[2] and 24089[3]. The complementary standards on product level cybersecurity have been defined by SAE J3101 as the best practice recommendations for Hardware Protected Security Environments. This SAE work defines a common glossary of required Hardware Protected Secure Environment Characteristics, based upon primary use and application use cases currently present in the market.

Under MoU with SAE International, and through direct engagement with the Vehicle Electrical Hardware Security Task Force TEVEES18B, GlobalPlatform conducted a mapping of our specifications for secure components to SAE's J3101 Hardware Protected Security Environment Recommend Practices. This work details how our certified components directly comply with the identified automotive requirements while leveraging best-in-class security standards.

4. Robust Security Needs

The need for security in Software Defined Vehicles is not only the result of global regulations but also a dramatic change in the software assets of the vehicles. In fact, the Boston Consulting Group indicates: *The emergence of software-defined vehicles will create over $650 billion in value for the auto industry by 2030, making up 15% to 20% of automotive value.*[4]

Furthermore, the OEMs desire to ensure that only paid features are enabled in vehicles and to prevent warranty fraud provide a strong financial motivation to ensure robust security in SDVs.

[1] https://unece.org/sustainable-development/press/three-landmark-un-vehicle-regulations-enter-force
[2] https://www.iso.org/standard/70918.html
[3] https://www.iso.org/standard/87522.html
[4] https://www.bcg.com/publications/2023/rewriting-rules-of-software-defined-vehicles

5. GlobalPlatform Technologies

Secure component is a platform combining hardware, firmware, and root of trust to distribute and manage trusted applications. In order to answer to different requirements of protection, GlobalPlatform continuously works toward the evolution of Secure Elements (SE), Trusted Execution Environments (TEE) and interfaces to access secure services from secure components and innovative isolation technologies. The secure component specifications, encompassing secure elements and trusted execution environments, developed by GlobalPlatform, are already implemented in most connected vehicles.

Secure Elements are a secure enclave protected against physical and software attack, hosted in a tamper resistant hardware, which installs and updates OTA applications (not just keys). In 2023, OVER 192 Million secure elements[5] were in Connected Cars in 2023 (Juniper Research). Tamper resistance for secure element is defined by a specific set of attacks[6] regularly updated and defined by the J-HAS group that a product must be able to mitigate.

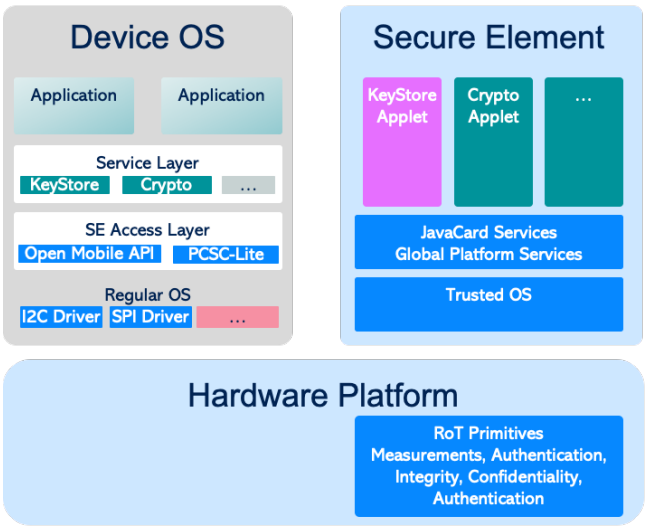


Figure 2: Secure Element Architecture

Trusted Execution Environments provide a secure operating system running on a standard CPU alongside regular OS/Applications. It is protected against attack by hardware chip features and software mechanisms. In 2023, Over 100 million Vehicles were in production with TEEs. (Confidential Source), and this technology is widely used in the transition to SDV.

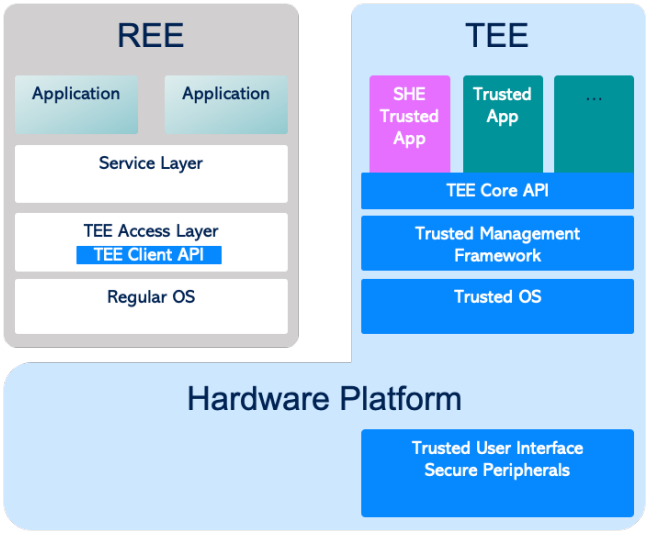


Figure 3: GlobalPlatform Trusted Execution Environment Architecture

The adoption of GlobalPlatform technologies for Banking, Government, Mobile, and other connected devices, has been driven by the desire to establish a mass market of multi-tenant products based upon defined security requirements, providing portability and interoperability for trusted applications/applets. A key part of the success in ensuring interoperability of services on a global scale has been the development of functional and security certification programs (our organization's certification body is ISO 17065 certified). Today, over 76 Billion Secure Components issued globally follow GlobalPlatform standards: https://globalplatform.org/specs-library/.

The GlobalPlatform community gathers security experts from multiple markets to ensure that cybersecurity requirements are always evolving. GlobalPlatform continues to advance its specifications to answer the needs of existing and new markets such as the automotive industry.

6. Key management of the Root of Trust

The success of the GlobalPlatform technology is not just related to the standardisation of the API to develop and deploy services with the associated command to remotely manage the platform and additional services. In a mass market with multiple suppliers, consistency of the Root of Trust (RoT) key injection is a key element. The initialization of Root of Trust is key for cybersecurity as all secure services that will be provided by the platform are related to this initial RoT. RoT consists of a computing engine,

[5] https://www.juniperresearch.com/press/connected-vehicles-to-surpass-367-million-globally#:~:text=Hampshire%2C%20UK%20-%209th%20January%202023,from%20192%20million%20in%202023

[6] attack methodology for tamper resistance : https://sogis.eu/documents/cc/domains/sc/JIL-Application-of-Attack-Potential-to-Smartcards-v3.2.1.pdf

code and data and/or key(s), all co-located on the same platform and provides at least one security service. RoT shall be as small as possible to limit the attack surface. During the production of GlobalPlatform secure components, the process, the location and the key source are defined depending on the level of security expected and checked during the certification of the development and production location.

This is very important for the car manufacturer. As an example, the deployment of MACsec Automotive Profile-from Open Alliance requires to have a key life cycle (injection, renewal) across multiple vendors standardized. GlobalPlatform has implemented a similar key life cycle that is being used by 44,000 banks, deployed on banking cards all over the world.

7. Market Utility of Security Certification

Security standardisation (over developing proprietary solutions) supports the automotive ecosystem by enabling effective cybersecurity best practices such as, transparency on security approaches, evidence of compliance through certification, and timely and effective cybersecurity responses. Additionally, standardisation offers opportunities for product optimization by lowering the cost of mass market produced solutions, providing more vendor options, simplified ECU development, and enabling a robust ecosystem.

Certification is a key step to ensuring that specifications are functionally and security-wise compliant with standardized specifications. The importance of certification in securing devices and services provides a means to ensure functional interoperability and product assurances and credibility. Certification also provides the following:

1. Demonstrates quality and robustness (UNECE-155)
2. Makes it easier to write and respond to requests for comment (RFCs)
3. Ensures a level of security is achieved in products (vs. claimed)
4. Provides a basis for legal defence if there is ever a breach

GlobalPlatform believes that this certification provides an invaluable support to the automotive market in generating evidence of due diligence on the security for products adhering to UNECE 155/6 but also requirements for data protection such as GDPR.

8. Mapping Alignment Between GlobalPlatform Specifications and SAE's J3101

The cooperation between SAE and GlobalPlatform began in 2023 with a series of meetings to discuss context around SAE requirements and details around GlobalPlatform technologies. The mapping activity was then conducted over the course of a year:

- GlobalPlatform's elaboration of the full SAE J3101[7] requirements (mandatory and optional)
- Analysis of how GlobalPlatform specifications covered the SAE requirements
- Defined coverage levels (i.e. Full, Trusted Application, and Not Covered).
- Areas highlighted by GlobalPlatform for further discussion with SAE on possible compliance paths for selected requirements
- Internal GlobalPlatform discussions on future automotive developments. GlobalPlatform is assessing the utility of creating a standardised trusted application (for trusted execution environments) or applet (for secure elements) for a "J3101 key store" in order to have a plug and play solution for J3101.

GlobalPlatform issued a Liaison Statement in February 2024 with the result of this mapping to SAE's Vehicle Electrical Hardware Security Task Force TEVEES18B.

In December 2024, SAE's Vehicle Electrical System Security Committee approved the ballot for the J3101-5 Information Report[8], which provides an analysis and summary of the coverage of SAE's J3101 requirements by existing GlobalPlatform technologies – Secure Elements (SE) and Trusted Execution Environment (TEE).

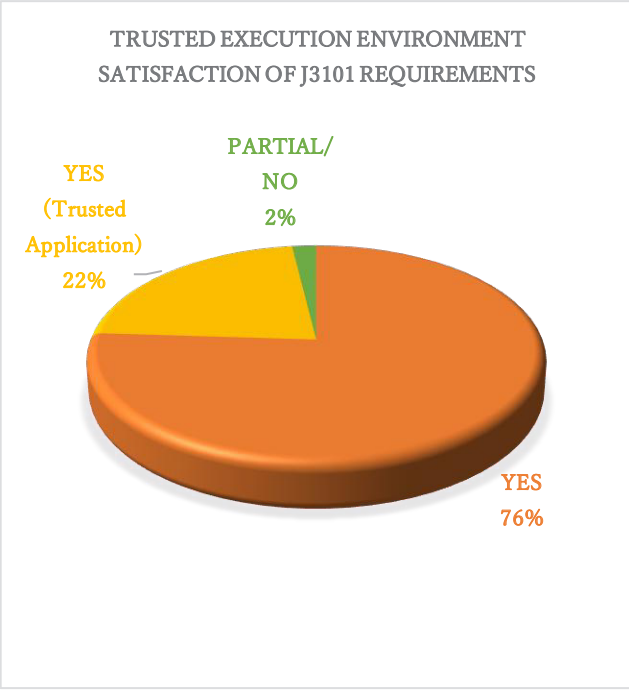
9. Cooperation on Standards to Simplify Compliance

The alignment between GlobalPlatform's specifications in satisfying SAE's J3101 requirements is very strong. GlobalPlatform technologies:

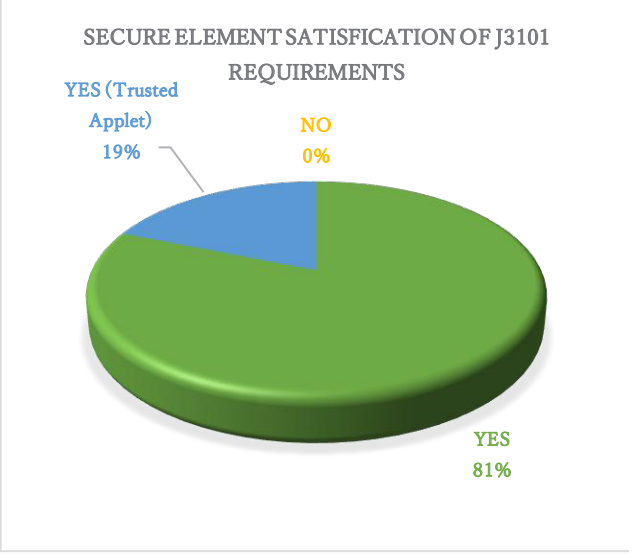
- Fully Support SAE's J3101 Hardware Protected Security Environments Best Practices:
    - 98% of GlobalPlatform Trusted Execution Environment specifications fully meet the J3101 requirements

[7] https://www.sae.org/standards/content/j3101_202002/

[8] https://www.sae.org/standards/content/j3101-5/



- 100% of GlobalPlatform Secure Element specifications fully meet the J3101 requirements



SAE J3101 Requirement Fulfillment Level	Description of GlobalPlatform categorization for the mapping
Yes	This J3101 requirement is Fully covered by GlobalPlatform's compliant platform for Secure Elements or Trusted Execution Environments as indicated. These requirements are also supported by existing Common Criteria (CC) protection profiles.
Yes (TA)	Full alignment is achieved through the development of Trusted Applet/ Application (TA) running on a GlobalPlatform compliant platform. Development of TA are an Innate Characteristic Supported by GlobalPlatform GlobalPlatform is assessing whether to develop application-level protection profiles for these applications in order to more explicitly correspond to these requirements of J3101, fostering standardized testing and certification of complete solutions.
No/Partially	There are three J3101 requirements which are not fully met by GlobalPlatform TEE specifications. • Hardware Tamper resistance is not a basic requirement of the TEE Protection Profile (although implementations may address this aspect). • Firmware update of the TEE itself is outside the scope of the TEE protection profile but Trusted Application (TA) update is covered by TMF protection profile.

- Extend the implementation guidelines for solutions that are compliant with SAE's J3101's requirements.
  - GlobalPlatform provides (free of charge also to non-members https://globalplatform.org/specs-library/) our specifications and implementation guidelines
  - GlobalPlatform continues to develop and maintain the security platform and tools

GlobalPlatform specifications and certification of Secure Components ensure:

- Standard hardware APIs across implementation
- Trusted application re-use (not redesigned for each ECU generation)
- Demonstratable security robustness (in terms of protection against attack) for products on the market through certification

10. Key Flexibility Features from Standards Alignment

The benefits of this standardisation are disruptive and strongly correspond to the type of flexibility required for software defined vehicles:

- Portability of trusted services across vendors (second sourcing options vs. vendor lock-in)
- Opportunity to develop and evolve post-production security services, including those bringing in new service providers (while still maintaining complete isolation for security services)
- Possibility to execute incremental design of services across different ECUs (not starting from scratch)
- Define an evolution path for future requirements and updates in standards or specifications to address mutually advantageous areas for more close correspondence
- Opportunity to independently certify solutions

11. Market Relevance of this Standard Alignment

GlobalPlatform certified solutions, in line with SAE's J3101, offer a automotive security baseline, which:

- Allows vendors and OEMs to focus their engineering efforts on core differentiators
- Streamlines requirements for RFPs
- Demonstrates faster alignment with J3101 requirements, using existing GlobalPlatform implementation guidelines

12. Conclusion: Further International Alignment for Hardware Protected Security Environments?

GlobalPlatform's remit for digitalized interoperable security services positions the standards alignment on Hardware Protected Security Environments as a potential area for multiple automotive geographies.

Moreover, the cooperation between SAE and GlobalPlatform provides a foundation upon which further international alignment could be possible. GlobalPlatform is interested in understanding if there is alignment with Japanese requirements for hardware protected security environments. This alignment could begin by assessing the alignment with SAE's J3101's requirements and then add/modify any additional requirements or use cases to fit emerging needs.

Our vision is that this standardized configuration could be then validated for other markets. We are currently in discussions with multiple standards bodies in Asia.

Appendix: References

GlobalPlatform Technologies Included in the Analysis for J3101-5

GlobalPlatform Secure Element	DOCUMENT REFERENCE	TITLE	VERSION	REFERENCE LINK
SE	GPC_SPE_034	Card Specification [GPCS]	2.3.1	https://globalplatform.org/specs-library/card-specification-v2-3-1/
	GPC_SPE_174	Secure Element Protection Profile [SE PP]	1.0	https://globalplatform.org/specs-library/secure-element-protection-profile/
		GlobalPlatform Card API	1.7.1	https://globalplatform.org/specs-library/globalplatform-card-api-org-globalplatform/
TEE	GPD_SPE_009	TEE System Architecture [TEE Sys Arch]	1.3	https://globalplatform.org/specs-library/tee-system-architecture/
	GPD_SPE_010	GPD TEE Internal Core API [TEE Core]	1.3.1 / 1.4	https://globalplatform.org/specs-library/tee-internal-core-api-specification/
	GPD_SPE_021	TEE Protection Profile [TEE PP]	1.3	https://globalplatform.org/specs-library/tee-protection-profile-v1-3/
	GPD_SPE_025	TEE TA Debug Specification [TEE Debug]	1.0.1	https://globalplatform.org/specs-library/tee-ta-debug-specification-v1-0-1/
	GPD_SPE_120	TEE Management Framework (TMF) including ASN.1 Profile [TMF]	1.1.2	https://globalplatform.org/specs-library/tee-management-framework-including-asn1-profile-1-1-2/
	GPD_GUI_069	TEE Initial Configuration [TEE Config]	1.1	https://globalplatform.org/specs-library/tee-initial-configuration-v1-1/
	GPD_GUI_089	TMF Initial Configuration [TMF Config]	1.0	https://globalplatform.org/specs-library/tmf-initial-configuration-v1-0/
SE and TEE	GP_TEN_053	Cryptographic Algorithm Recommendations [Crypto Rec]	2.0	https://globalplatform.org/specs-library/globalplatform-technology-cryptographic-algorithm-recommendations/
	GP_REQ_025	Root of Trust Definitions and Requirements [RoT]	1.1.1	https://globalplatform.org/specs-library/root-of-trust-definitions-and-requirements-v1-1-gp-req_025/