| 講演番号 | 156 |
|---|---|

# A Standardized Security Platform for Software-Defined Vehicles: GlobalPlatform Technologies, SAE J3101-5, and the SESIP Certification Framework

**Francesca Forestieri** [1)] **Gil Bernabeu** [1)]

*1) GlobalPlatform, Inc., Redwood City, CA, USA (secretariat@globalplatform.org)*

**KEY WORDS:** software-defined vehicle, hardware-protected security environment, SAE J3101, GlobalPlatform, trusted execution environment, secure element, root of trust, SESIP, compositional certification, automotive cybersecurity

The software-defined vehicle demands hardware-protected security environments that are standardized, independently certifiable, and maintainable across vehicle lifetimes of 10 to 15 years. UNECE R155 and R156 establish regulatory obligations for cybersecurity management. ISO/SAE 21434 provides the engineering process standard. SAE J3101 addresses the product level, defining what hardware-protected security environments must provide at the component level. GlobalPlatform provides the HOW: detailed, implementable specifications for Secure Elements (SEs) and Trusted Execution Environments (TEEs) backed by independent certification. SESIP provides the MEASURE: a defined metric for assessing the security level of final component products and comparing them consistently across the supply chain.

Current solutions, principally Secure Hardware Extensions (SHEs) and proprietary Hardware Security Modules (HSMs), share three structural limitations. First, neither SHEs nor proprietary HSMs offer guaranteed updateability through a standardized, authenticated mechanism across all implementations. Second, no current proprietary solution provides a standardized and independently verifiable multi-tenant isolation model. Third, OEMs have no defined metric for comparing security assurance across vendors: the evidence available is whatever the supplier provides, interpreted against criteria the OEM itself defines.

The GlobalPlatform platform-centric model was developed to enable mass-market deployment of trusted digital services across a diverse ecosystem of manufacturers, silicon vendors, and service providers. A certified execution environment provides guaranteed security properties for every trusted application that runs on it, regardless of developer or purpose, while applications remain mutually isolated. This guarantee is a property of the platform, not of individual applications, enabling OEMs to host trusted applications from multiple parties on a single SE or TEE. GlobalPlatform SEs provide tamper-resistant protection for vehicle access credentials, V2X certificates, and EV charging contracts per ISO 15118. TEEs support gateway and domain controllers for network security and OTA update management. SEs and TEEs are frequently combined, with credentials in the SE and higher-performance processing in the TEE, connected by a GlobalPlatform Secure Channel Protocol inaccessible to the regular operating system. SESIP provides three missing engineering capabilities: a defined assurance metric grounded in ISO/IEC 15408 vulnerability assessment levels; a repeatable, methodology-driven evaluation ensuring certificates from different laboratories are comparable; and compositional chaining enabling early V-model component certification.

Table 1 maps J3101 requirement areas to GlobalPlatform platform and trusted application capabilities. Platform-level requirements, including root of trust, key management, secure boot, cryptographic services, OTA lifecycle management, and multi-stakeholder isolation, are satisfied by the certified platform before any application development. An OEM procuring a GlobalPlatform-certified SE or TEE can rely on J3101 coverage for these areas without independent assessment. Vehicle-specific functions are implemented as trusted applications.

Supplier substitution at the platform level does not require re-evaluation of J3101 coverage, directly addressing the supply chain resilience concerns raised during the 2021 to 2022 global chip shortage.

Table 2 shows the SESIP automotive profile roadmap. Two profiles are published; the Automotive CMOS Image Sensor profile is near publication. The J3101-aligned profile for non-GlobalPlatform technologies allows SHE and HSM implementations to be evaluated against the same J3101-aligned security functional requirements, enabling comparable, independently certified evidence regardless of underlying technology.

GlobalPlatform and SAE International have recently agreed to demonstrate formally how SESIP supports ISO/SAE 21434 cybersecurity assurance objectives, with work commencing in summer 2026.

| J3101 Requirement | Level | GP Mechanism |
|---|---|---|
| Root of Trust | Plat. | Immutable RoT; certified |
| Key store | Plat. | HW-isolated; GP Key API |
| Secure boot / attest. | Plat. | Verified chain; SE/TEE |
| Cryptographic svcs. | Plat. | Certified; algorithm-agile |
| Secure comms. | Plat. | TLS via TA; SE PKI mgmt |
| OTA lifecycle | Plat. | GP Trusted App Manager |
| Multi-party isolation | Plat. | Security domain model |
| Diagnostics ctrl. | TA | OEM-configurable TA |
| Vehicle attestation | TA | Entity Attestation Token |
| HSM/SHE functions | TA | Dedicated TA on SE/TEE |

*Table 1. J3101 requirements mapped to GlobalPlatform (J3101-5, Sep. 2025).*

| SESIP Profile | Status (H2 2025) |
|---|---|
| Secure MCUs & MPUs v1.1 | Published Jun 2025 |
| Secure External Memories v1.1 | Published Jan 2025 |
| Automotive CMOS Image Sensor | Near publication |
| J3101-aligned for GP tech. | In development |
| J3101-aligned for non-GP tech. | In development |
| ECU-level profile | In development |
| Micro-TEE requirements | Scoping |

*Table 2. GlobalPlatform SESIP automotive profile roadmap.*

**References:** (1) GlobalPlatform Annual Report 2025. (2) SAE J3101-5, Sep. 2025. (3) SESIP Profile for Secure MCUs/MPUs v1.1, GPT_SPE_150, Jun. 2025. (4) SESIP Methodology v1.2, GP_FST_070, Dec. 2024. (5) ISO/SAE 21434:2021. All GP specs: https://globalplatform.org/specs-library/