SAE J3101: Opportunity for Synergies in Japan?

22nd May 2025

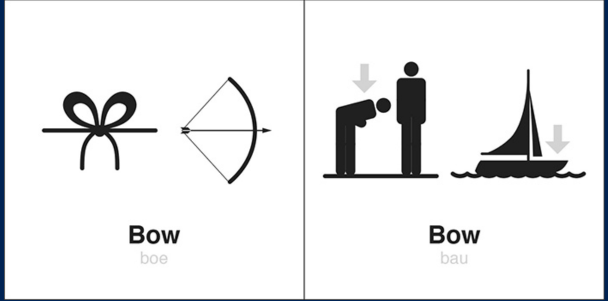
Francesca Forestieri, GlobalPlatform

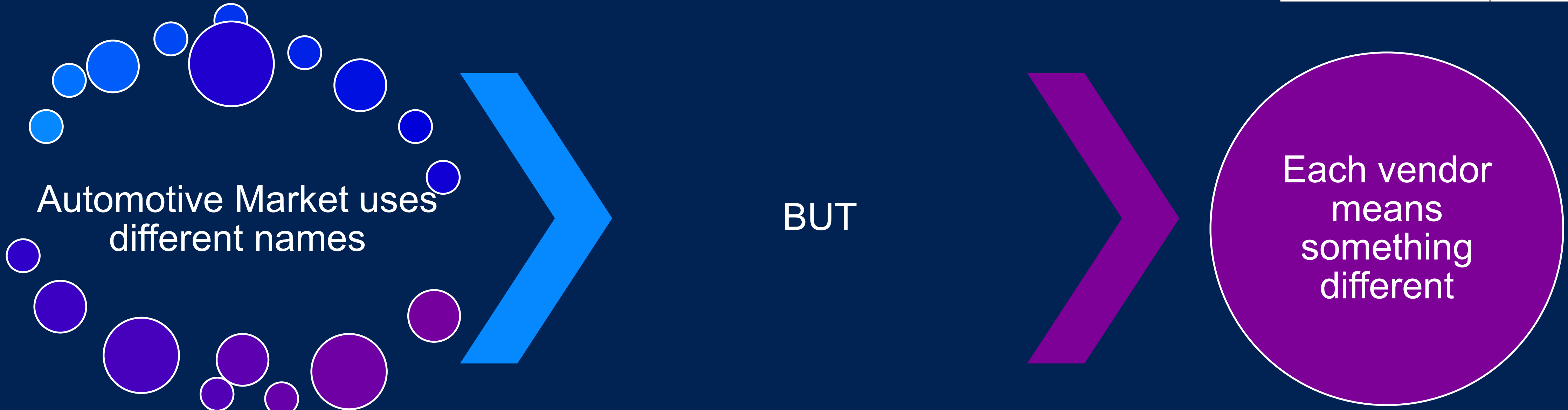
Global Platform™

Hardware Protected Security Environments

SAE J3101-5

Same Words Meaning Different Things: Reason Why SAE's J3101 Was Created





Automotive Market uses different names

BUT

Each vendor means something different

HSM

- General term used for dedicated security hardware in vehicles

SHE/SHE++

- Developed 2004-2005 / Maintained by the AUTOSAR consortium

EVITA

- EVITA Project (2008-2011):

- Same name has different characteristics
- No framework to compare across products

GlobalPlatform™

SAE J3101: A Common Reference for Hardware Protected Security Environments

Basic characteristics

Requirements

Establish trustworthiness

- device identity
- sealing
- attestation
- data integrity
- availability

Resilience to a wide range of attacks

- beyond software-only security mechanisms.

A hardware root of trust

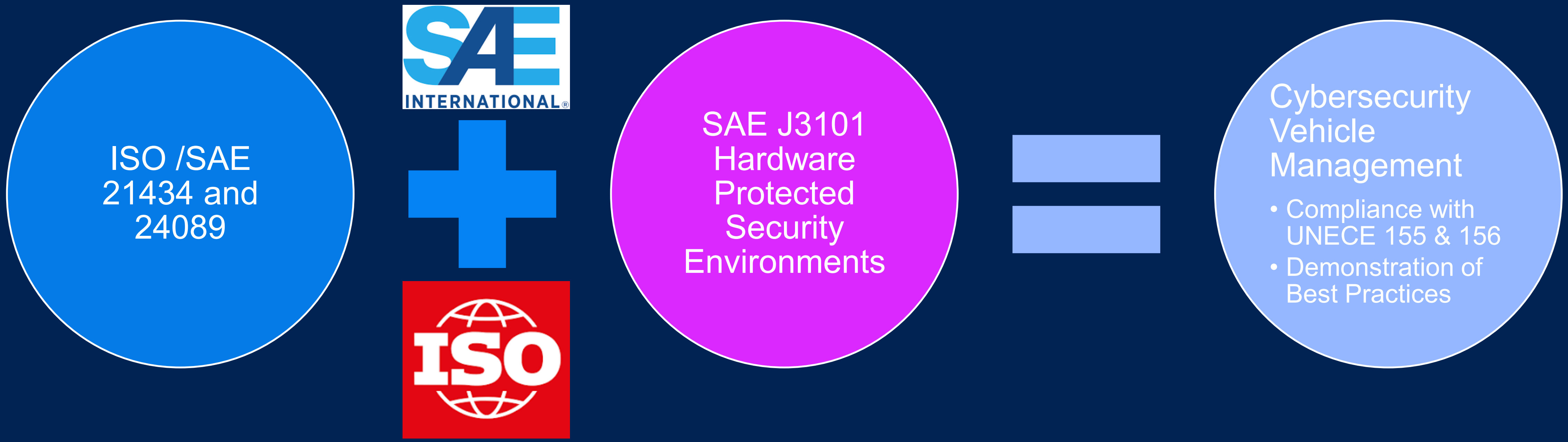
- hardware-based security primitives
- for connected and highly or fully automated vehicles.

Source: SAE, Surface Vehicle Recommended Practice, *Hardware Protected Security for Ground Vehicles* J3101 ™ FEB2020, Issued 2020-02

Role of J3101 in Cybersecurity Compliance: Framework for Product Security

Relevant for 64 Countries

Process *Product* *Compliance*



ISO /SAE 21434 and 24089

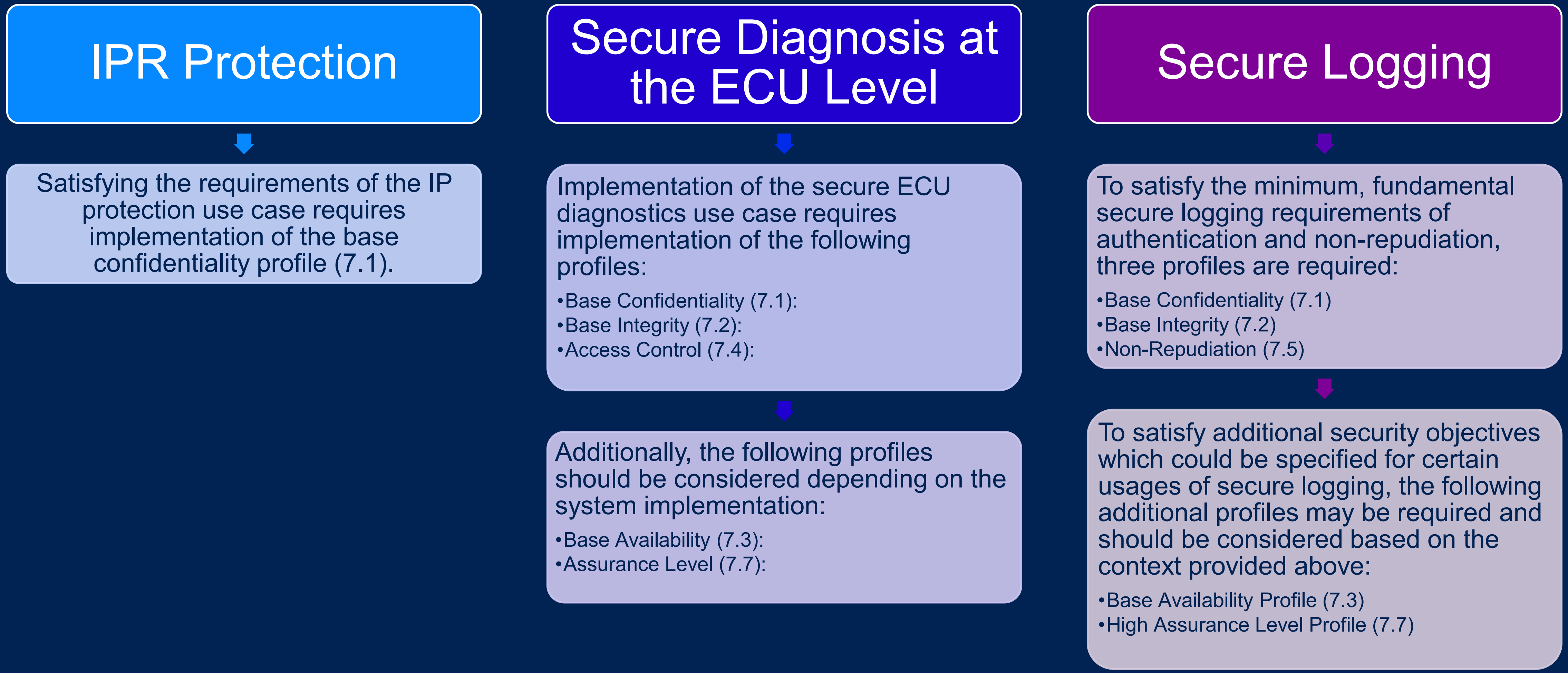
SAE J3101 Hardware Protected Security Environments

Cybersecurity Vehicle Management

- Compliance with UNECE 155 & 156
- Demonstration of Best Practices

- ISO/PAS 5112:2022 - Road vehicles — Guidelines for auditing cybersecurity engineering. Security, safety & risk
- ISO/SAE PAS 8475 Road vehicles - Cybersecurity Assurance Levels (CAL) and Targeted Attack Feasibility (TAF) (under development)
- ISO/SAE PWI 8477 Road Vehicles Cybersecurity Validation and Verification (under development)

Hardware Protected Security Environments (J3101): Application Use Cases



IPR Protection

Satisfying the requirements of the IP protection use case requires implementation of the base confidentiality profile (7.1).

Secure Diagnosis at the ECU Level

Implementation of the secure ECU diagnostics use case requires implementation of the following profiles:

- Base Confidentiality (7.1):
- Base Integrity (7.2):
- Access Control (7.4):

Additionally, the following profiles should be considered depending on the system implementation:

- Base Availability (7.3):
- Assurance Level (7.7):

Secure Logging

To satisfy the minimum, fundamental secure logging requirements of authentication and non-repudiation, three profiles are required:

- Base Confidentiality (7.1)
- Base Integrity (7.2)
- Non-Repudiation (7.5)

To satisfy additional security objectives which could be specified for certain usages of secure logging, the following additional profiles may be required and should be considered based on the context provided above:

- Base Availability Profile (7.3)
- High Assurance Level Profile (7.7)

SAE J3101
Hardware Protected Security Environments

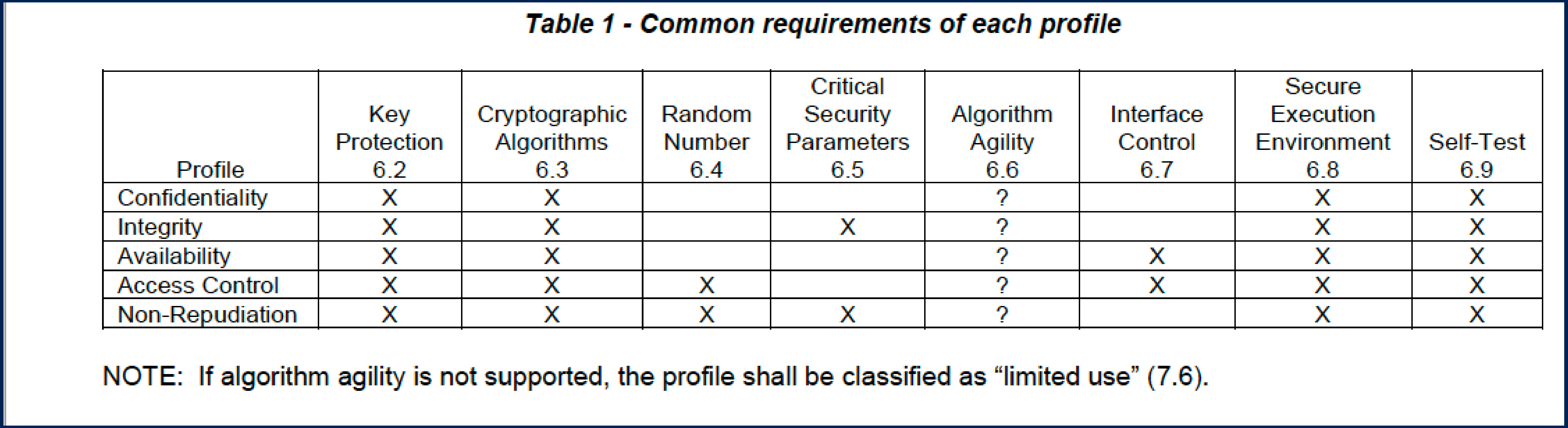


Table 1 - Common requirements of each profile

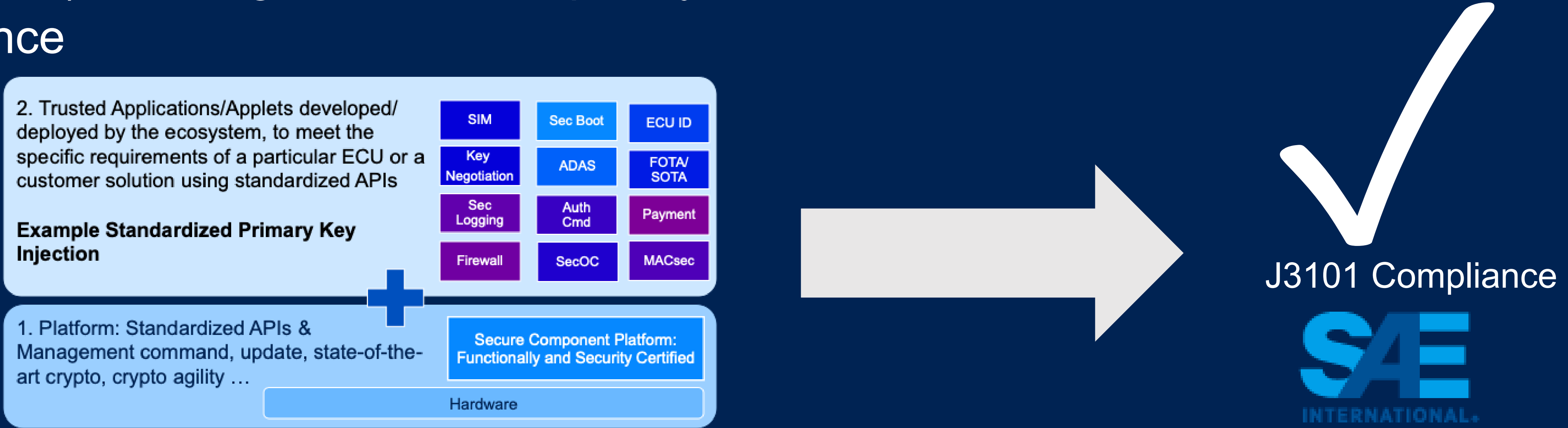
Profile	Key Protection 6.2	Cryptographic Algorithms 6.3	Random Number 6.4	Critical Security Parameters 6.5	Algorithm Agility 6.6	Interface Control 6.7	Secure Execution Environment 6.8	Self-Test 6.9
Confidentiality	X	X			?		X	X
Integrity	X	X		X	?		X	X
Availability	X	X			?	X	X	X
Access Control	X	X	X		?	X	X	X
Non-Repudiation	X	X	X	X	?		X	X

NOTE: If algorithm agility is not supported, the profile shall be classified as “limited use” (7.6).

Source: SAE, Surface Vehicle Recommended Practice, *Hardware Protected Security for Ground Vehicles* J3101™ FEB2020, Issued 2020-02

Collaboration

By leveraging GlobalPlatform technologies, a large proportion of the requirements can be met by the platform (TEE or SE) reducing cost and complexity of J3101 compliance



2. Trusted Applications/Applets developed/ deployed by the ecosystem, to meet the specific requirements of a particular ECU or a customer solution using standardized APIs

Example Standardized Primary Key Injection

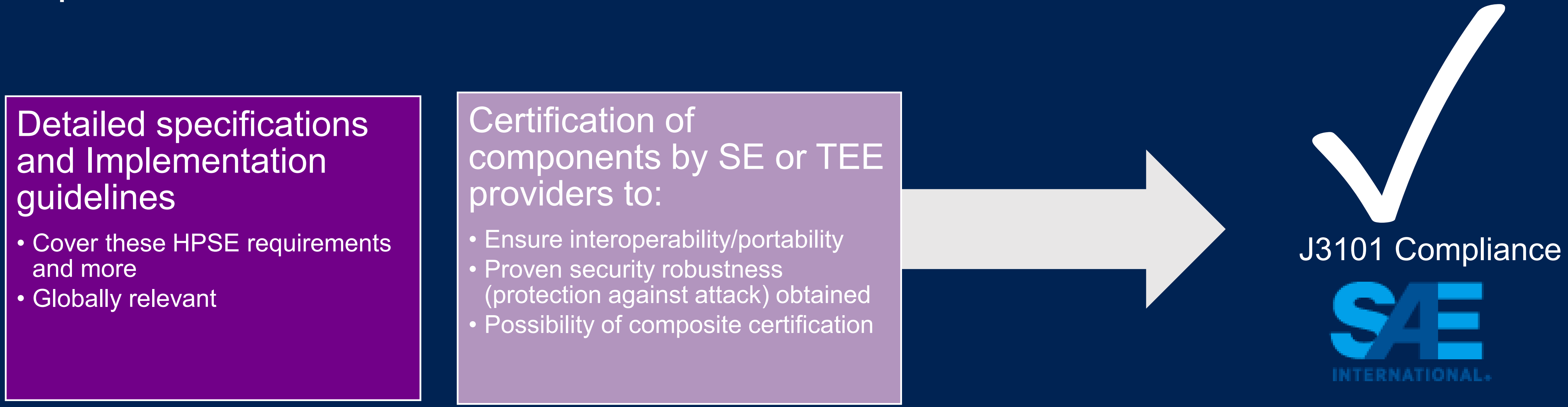
1. Platform: Standardized APIs & Management command, update, state-of-the-art crypto, crypto agility …

Secure Component Platform: Functionally and Security Certified
Hardware

J3101 Compliance

Collaboration

By leveraging GlobalPlatform technologies, additional benefits of standardised specifications support SDV requirements



Detailed specifications and Implementation guidelines

- Cover these HPSE requirements and more
- Globally relevant

Certification of components by SE or TEE providers to:

- Ensure interoperability/portability
- Proven security robustness (protection against attack) obtained
- Possibility of composite certification

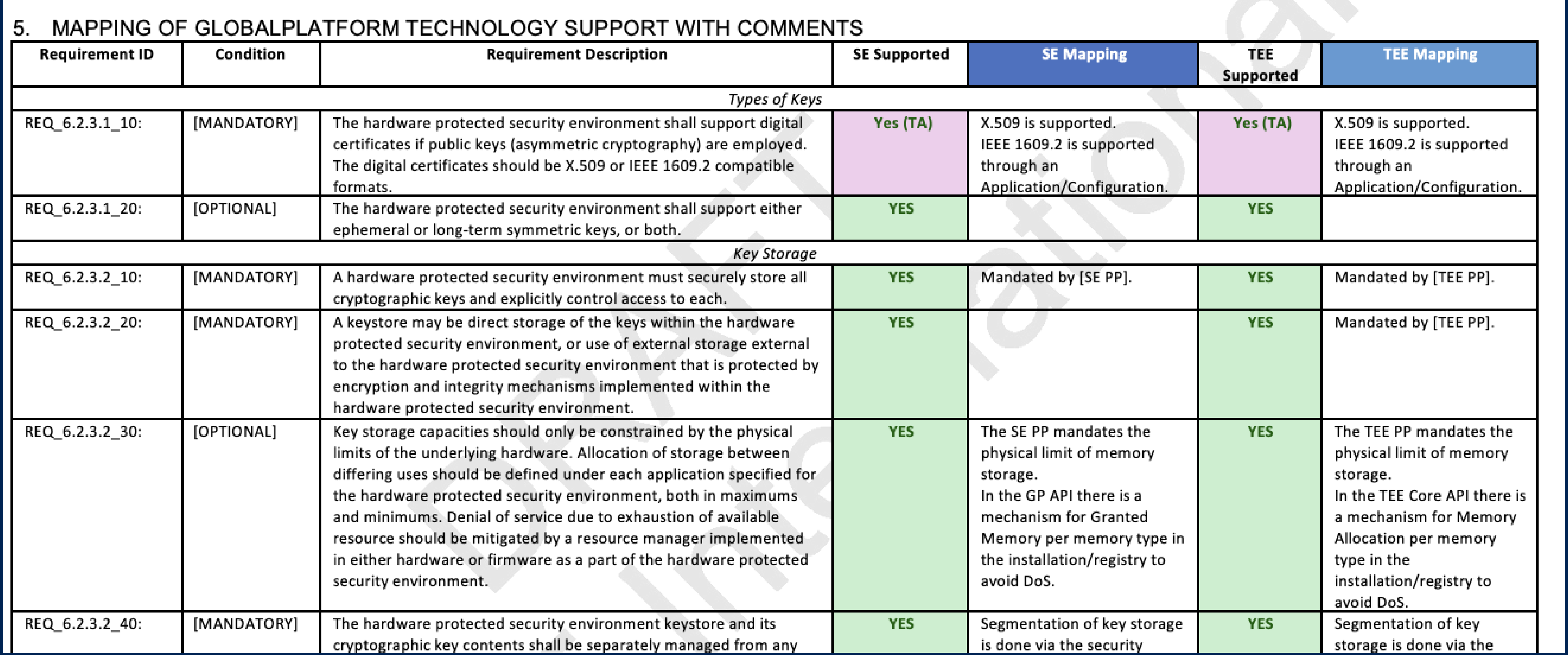
J3101 Compliance

SAE INTERNATIONAL

Methodology – GlobalPlatform Specifications Assessed

GP TECHNOLOGY	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/

Mapping Conducted for Secure Elements and Trusted Execution Environments



5. MAPPING OF GLOBALPLATFORM TECHNOLOGY SUPPORT WITH COMMENTS

Requirement ID	Condition	Requirement Description	SE Supported	SE Mapping	TEE Supported	TEE Mapping
		Types of Keys				
REQ_6.2.3.1_10:	[MANDATORY]	The hardware protected security environment shall support digital certificates if public keys (asymmetric cryptography) are employed. The digital certificates should be X.509 or IEEE 1609.2 compatible formats.	Yes (TA)	X.509 is supported. IEEE 1609.2 is supported through an Application/Configuration.	Yes (TA)	X.509 is supported. IEEE 1609.2 is supported through an Application/Configuration.
REQ_6.2.3.1_20:	[OPTIONAL]	The hardware protected security environment shall support either ephemeral or long-term symmetric keys, or both.	YES		YES	
		Key Storage				
REQ_6.2.3.2_10:	[MANDATORY]	A hardware protected security environment must securely store all cryptographic keys and explicitly control access to each.	YES	Mandated by [SE PP].	YES	Mandated by [TEE PP].
REQ_6.2.3.2_20:	[MANDATORY]	A keystore may be direct storage of the keys within the hardware protected security environment, or use of external storage external to the hardware protected security environment that is protected by encryption and integrity mechanisms implemented within the hardware protected security environment.	YES		YES	Mandated by [TEE PP].
REQ_6.2.3.2_30:	[OPTIONAL]	Key storage capacities should only be constrained by the physical limits of the underlying hardware. Allocation of storage between differing uses should be defined under each application specified for the hardware protected security environment, both in maximums and minimums. Denial of service due to exhaustion of available resource should be mitigated by a resource manager implemented in either hardware or firmware as a part of the hardware protected security environment.	YES	The SE PP mandates the physical limit of memory storage. In the GP API there is a mechanism for Granted Memory per memory type in the installation/registry to avoid DoS.	YES	The TEE PP mandates the physical limit of memory storage. In the TEE Core API there is a mechanism for Memory Allocation per memory type in the installation/registry to avoid DoS.
REQ_6.2.3.2_40:	[MANDATORY]	The hardware protected security environment keystore and its cryptographic key contents shall be separately managed from any	YES	Segmentation of key storage is done via the security	YES	Segmentation of key storage is done via the

Coverage Definitions

Yes:

- Satisfied by Existing GlobalPlatform Specifications
- This J3101 requirement is Fully covered by GP compliant platform for Secure Elements or Trusted Execution Environments.
- Detailed Implementation Guidelines Exist

Yes by Trusted Application:

- Innate Characteristic Supported by GlobalPlatform
- Full alignment is achieved through development of Trusted Applet/ Application running on a GlobalPlatform compliant platform.

Not Covered

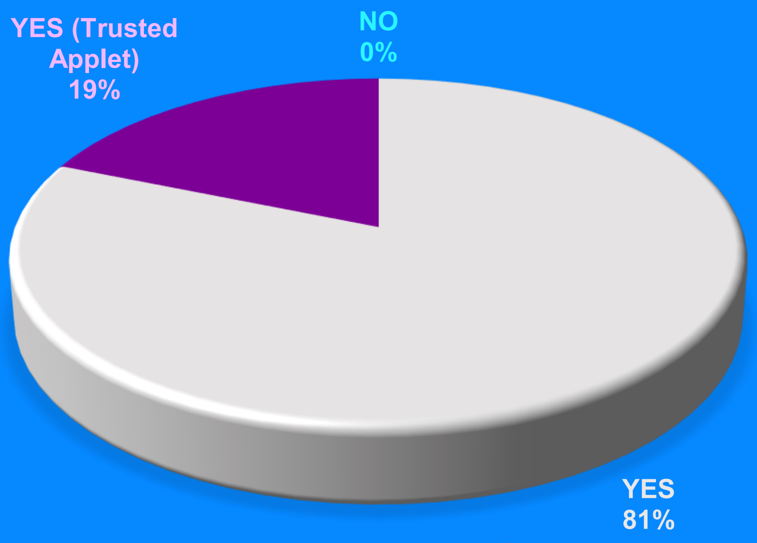
Only 3 J3101 requirements are not fully met by GlobalPlatform (TEE) specifications.

Hardware Tamper resistance is not a basic requirement of the TEE Protection Profile (although implementations may address this aspect).

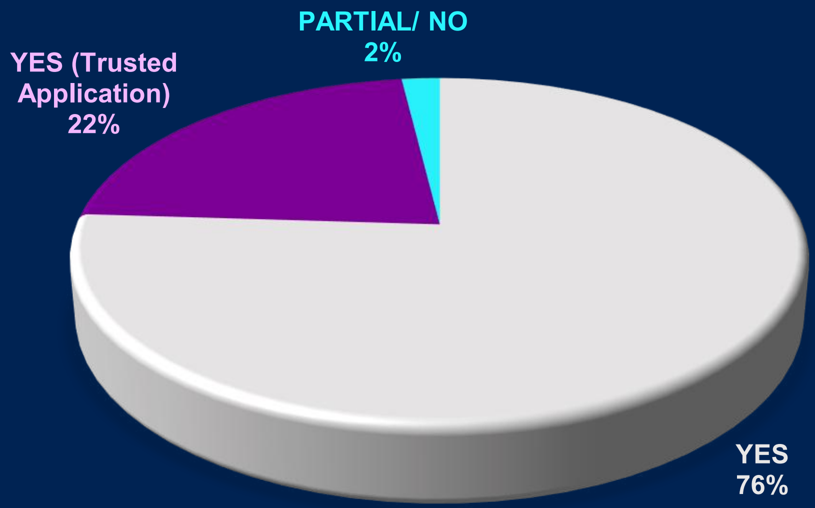
Furthermore, firmware update of the TEE itself is outside the scope of the TEE protection profile but Trusted Application (TA) update is covered by TMF protection profile.

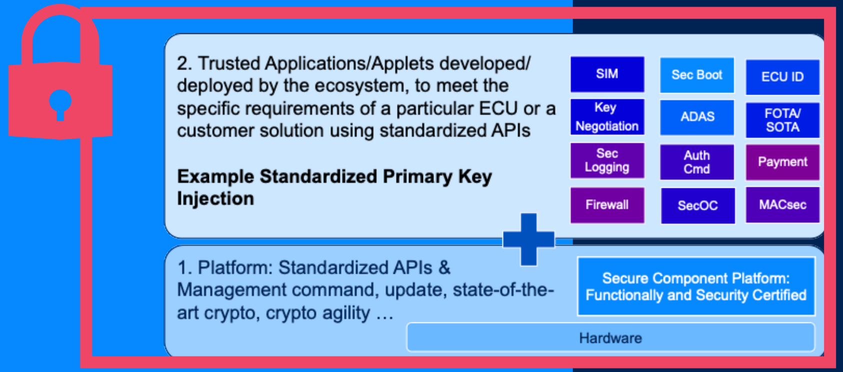
Analysis Results: GlobalPlatform Specifications

Secure Element Satisfaction Of 100% OF J3101 Requirements



Trusted Execution Environment Satisfaction Of 98% Of J3101 Requirements





2. Trusted Applications/Applets developed/ deployed by the ecosystem, to meet the specific requirements of a particular ECU or a customer solution using standardized APIs

Example Standardized Primary Key Injection

1. Platform: Standardized APIs & Management command, update, state-of-the-art crypto, crypto agility …

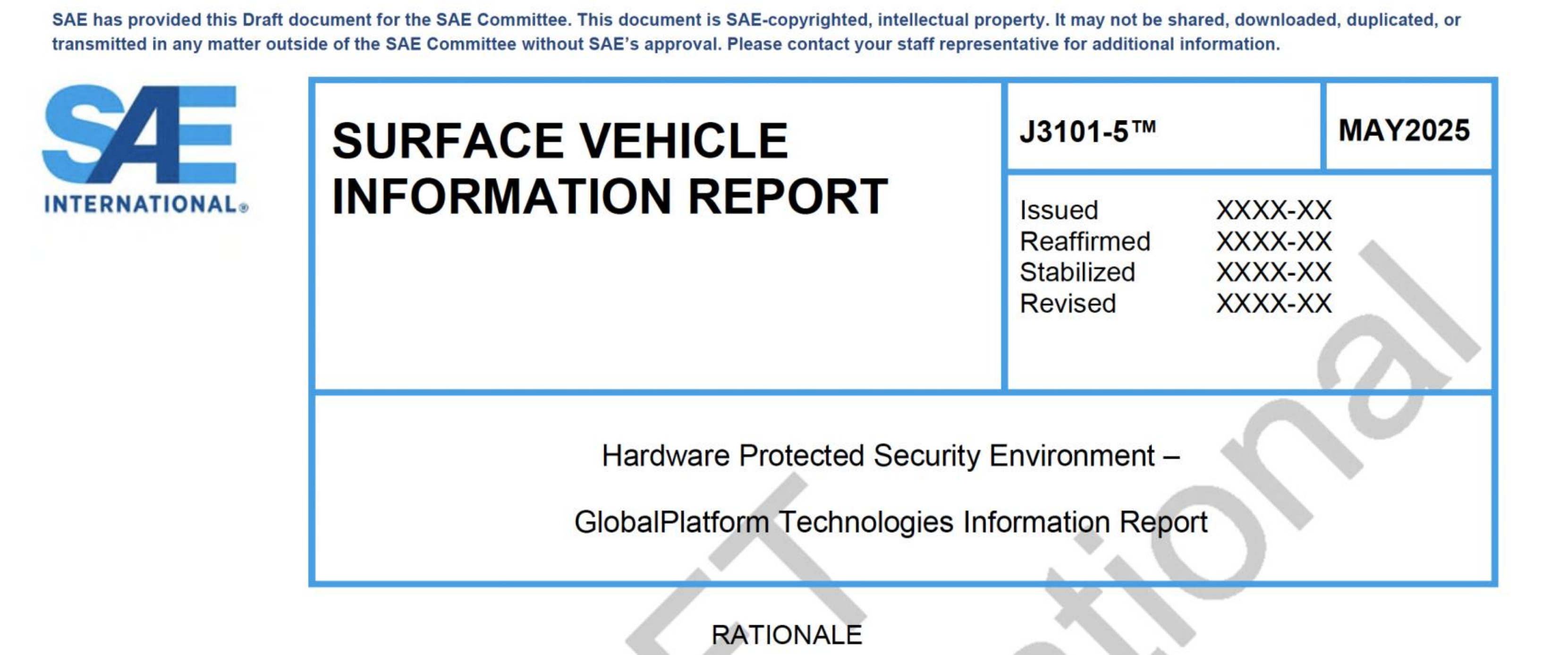
YES-TA

YES - Platform

SAE’s Vehicle Electrical System Security Committee – Final Ballot J3101-5

COMING SOON!

- Final confirmation Ballot Concluded
- Awaiting SAE Technical Writer Edits and Publication



SAE has provided this Draft document for the SAE Committee. This document is SAE-copyrighted, intellectual property. It may not be shared, downloaded, duplicated, or transmitted in any matter outside of the SAE Committee without SAE’s approval. Please contact your staff representative for additional information.

SAE INTERNATIONAL

SURFACE VEHICLE INFORMATION REPORT	J3101-5™	MAY2025
	Issued XXXX-XX Reaffirmed XXXX-XX Stabilized XXXX-XX Revised XXXX-XX	

Hardware Protected Security Environment –

GlobalPlatform Technologies Information Report

RATIONALE

What is the importance of J3101-5?

A way to demonstrate "compliance" with SAE J3101 for

- RFPs
- ISO/SAE 21434

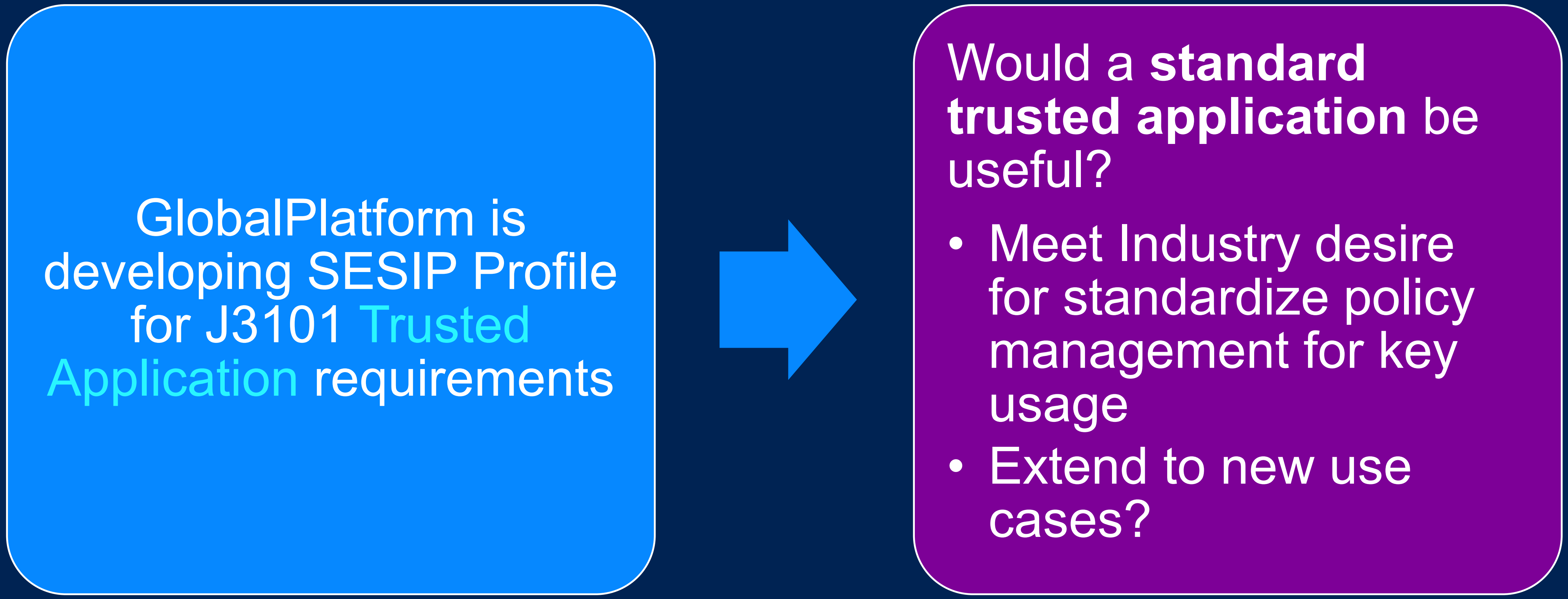
AND

GP provides

- certified security assurance levels
- functional interoperability
- flexibility in developing secure services

Global Platform™

What do We Have?

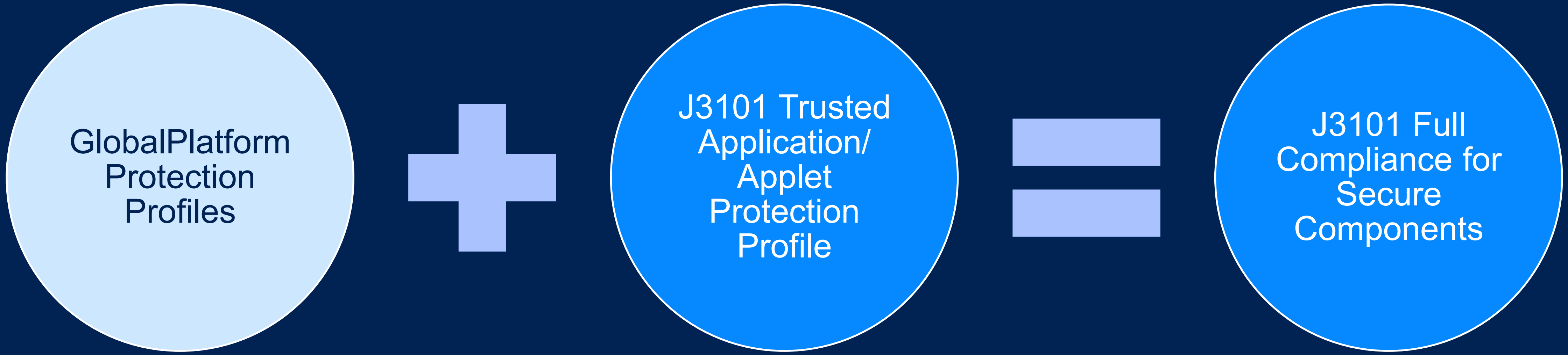


GlobalPlatform is developing SESIP Profile for J3101 Trusted Application requirements

Would a **standard trusted application** be useful?

- Meet Industry desire for standardize policy management for key usage
- Extend to new use cases?

Next Steps: How SESIP Profiles Support Demonstrating Compliance for J3101



GlobalPlatform Protection Profiles

J3101 Trusted Application/ Applet Protection Profile

J3101 Full Compliance for Secure Components

- Detailed Implementation Guidelines have been Defined by GlobalPlatform
- Existing Protection Profiles

- GlobalPlatform is developing SESIP profiles with interpretations on implementation
- Example of Potential Acceptance Criteria

Next Steps: Open Questions

Is SAE's work on J3101 a departure point for discussing Japanese requirements?

- Through JasPar
- Through JSAE

PQC: How does GlobalPlatform Help?

22nd May 2025

Beatrice Peirani, Thales
Yves-Emmanuel Le Bobinnec, Thales