Housekeeping

Zoom Link:
https://zoom.us/j/2660561185?pwd=ovMgDmwbaayZuw3yjl4IFEJPo2UZew.1&omn=91777893524
Meeting ID: 266 056 1185
Passcode: CSVF2025

In the room

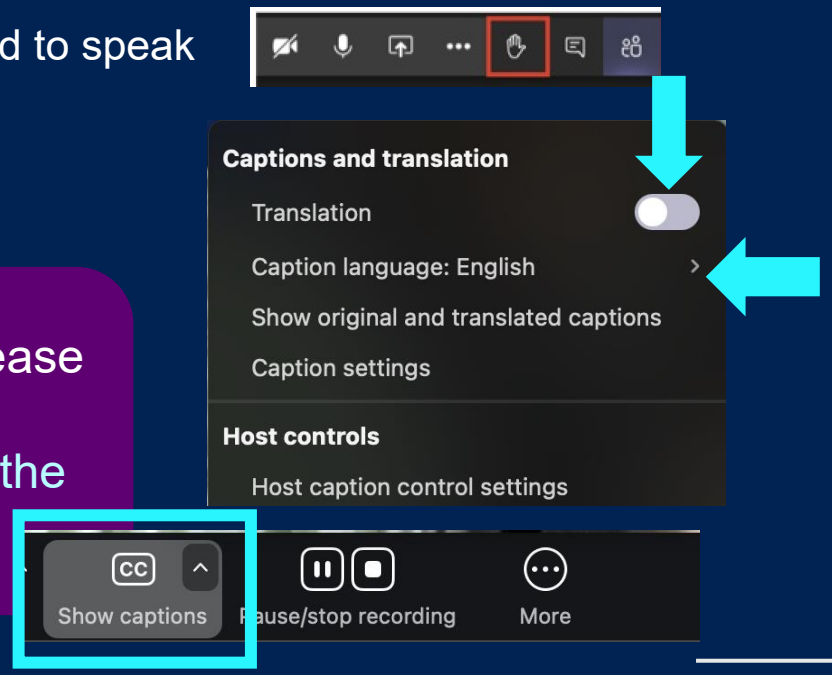
- **Please download Zoom on your device**
- Please join Zoom so you can take part in polls and interactive sessions

Please DO NOT join Zoom audio(!)

- Muting is not enough, you also have to have your speaker turned off

Online

- Please respond to polls
- Please use chat if there are audio/video problems
- Please mute when not speaking.
- Please raise hand to speak



Everyone:

- Please put your name + company in Zoom (if you prefer not to share, please put ‘OEM’ or ‘SIP’ or ‘…’)
- Please activate the Closed Caption (subtitles) to the speeches selecting the relevant languages of interest

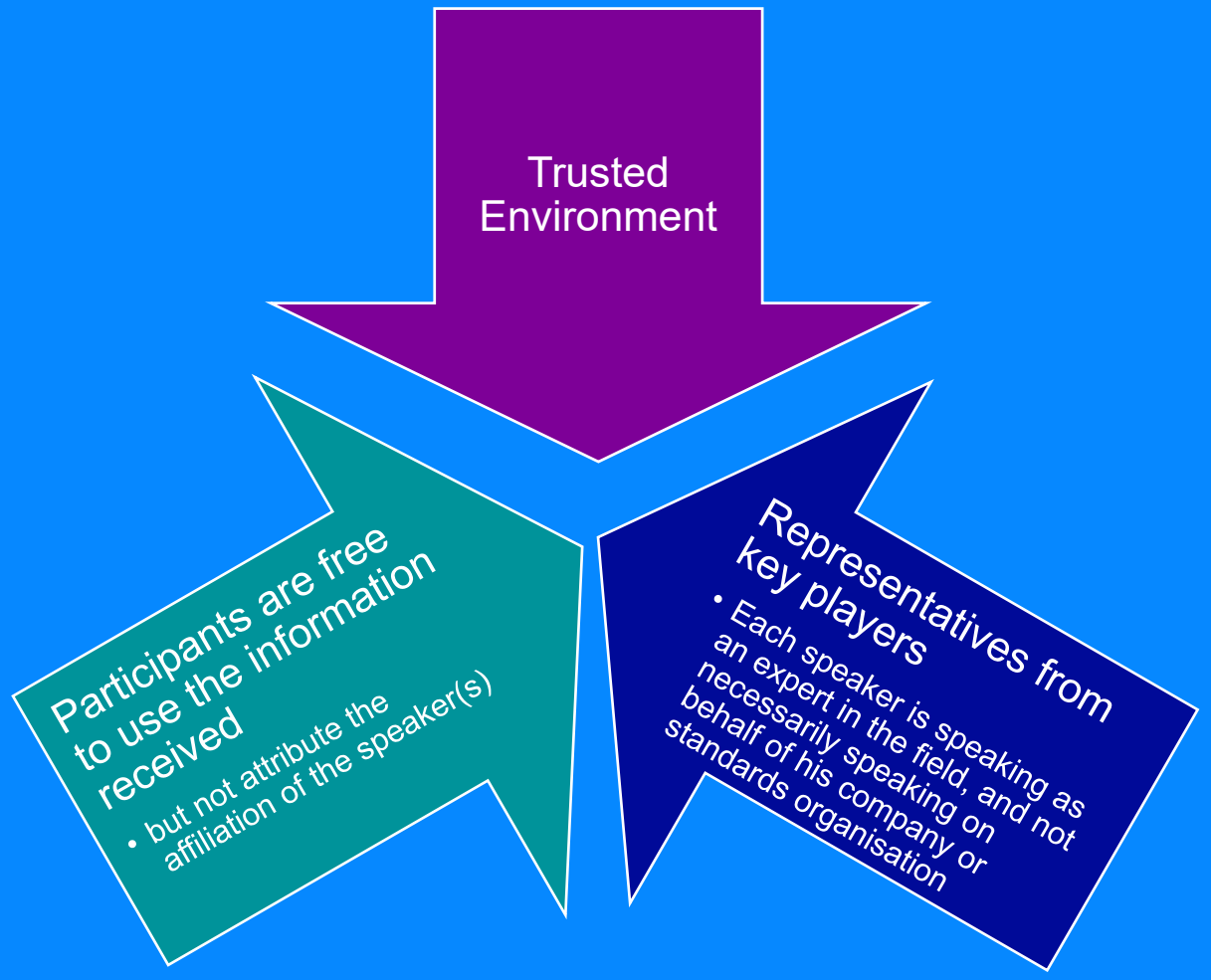
Global Platform™

Cybersecurity Vehicle Forum – Shanghai

15th May 2025

Ana Lattibeaudiere, CEO GlobalPlatform
Gil Bernabeu, CTO GlobalPlatform
Francesca Forestieri, Automotive Lead

Ground Rules CSVF

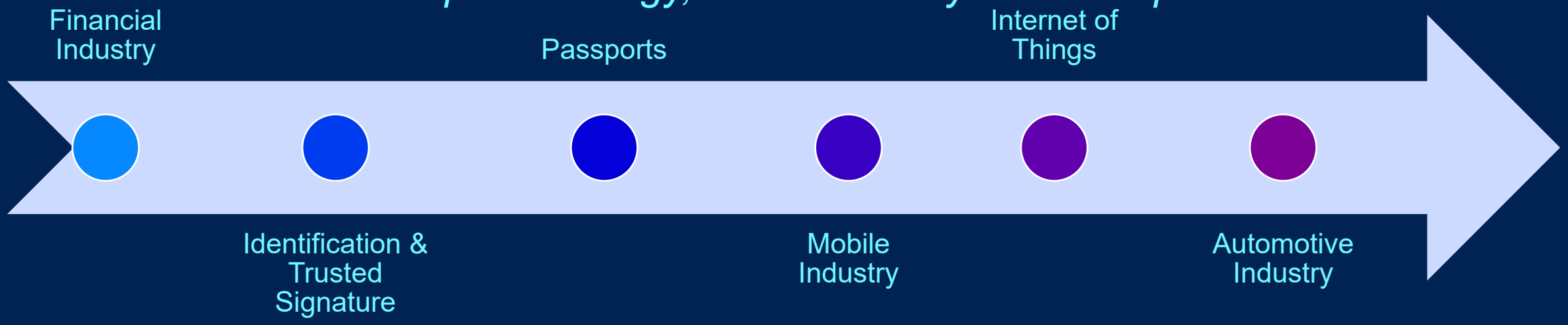


GlobalPlatform will post the recording on our website, as well as

- the relevant slides (as made available by speakers) for your reference.
- https://globalplatform.org/blog-overview/

GlobalPlatform

THE standard for managing applications on secure chip technology, with over 25 years of experience



Mass Market deployment of industries has required: agreed functionality for transactions and transparent robust security to create trust among competitors and in the overall ecosystem

CSVF Agenda: May 15th

10:00:00	Welcome		Ana Tavares Lattibeaudiere, CEO of GlobalPlatform
10:10:00	Keynote: Standards and Test Technologies for the Application of Commercial Cryptography in the Automotive Field		Bao Yue, CATARC
10:30:00	GlobalPlatform Technologies		Gil Bernabeu, CTO of GlobalPlatform
10:50:00	Risks & Threats; International Regulatory Developments, including PQC		Dennis Kengo Oka, IAV Gmbh
11:20:00	Automotive Security Use Cases		
11:20:00		Platform-Based Full-Vehicle Cybersecurity Framework for Next-Gen Connected Vehicles	David Wei Wang, Head of Digital Security Development of NIO
11:40:00	Lunch		
12:40:00		HSM evolutions: opportunities for standardisation?	Raymond Li, Co-founder, Uni-Sentry
13:00:00		Automotive Security: Trends and Standardisation Opportunities	Xiaochao Xie, UAES
13:20:00		Automotive iHSM Security Solution	Kevin Zhang, RAMBUS Senior Principal Field Application Engineer for Security IP
13:40:00	Introduction to Automotive in GlobalPlatform		Francesca Forestieri, Head of Automotive, GlobalPlatform
14:00:00	Hardware Protected Security Environments: Ground for Synergies on J3101 Requirements		Francesca Forestieri, Head of Automotive, GlobalPlatform
14:15:00	SESIP Certification: How it works and its use in Automotive		Francesca Forestieri, Head of Automotive and Gil Bernabeu, CTO GlobalPlatform
14:45:00	Assessing Security Levels & Functional Interoperability		Wei Yuan Mao, APPlus
15:15:00		Attack Methodology	
15:15:00		Protection Profiles	
15:15:00	Coffee Break		
15:45:00	The Coordination between Chip and Component Security Testing under the CC System and the Information Security Compliance of the Entire Vehicle		Bai ZhiChao, Vice General Manager, DPLS Labss
16:15:00		SE, Building the Digital Security Foundation for Automobiles	Song Weifeng, Senior Product Manager, G&D
16:35:00		Secure Elements: Topics of Interest in Automotive	Gil Bernabeau, CTO of GlobalPlatform
16:55:00	Trusted Execution Environments: Evolution in Automotive		Richard Hayton, Chair of Automotive Task Force
17:25:00	Wrap-up and Goodbye		Francesca Forestieri, Head of Automotive, GlobalPlatform

Lunch is on the 37th Floor

Coffee Break is Outside the Meeting Room

Global Platform™

Why GlobalPlatform: Market Presence in Automotive

Secure Element

OVER 192 Million Connected Cars in 2023

- Digital Car Key
- Electrical Vehicle Charging
- All eUICCs (embedded Sims)
- Key Management

Trusted Execution Environment

In Over 100 Million Vehicles as of 2023*

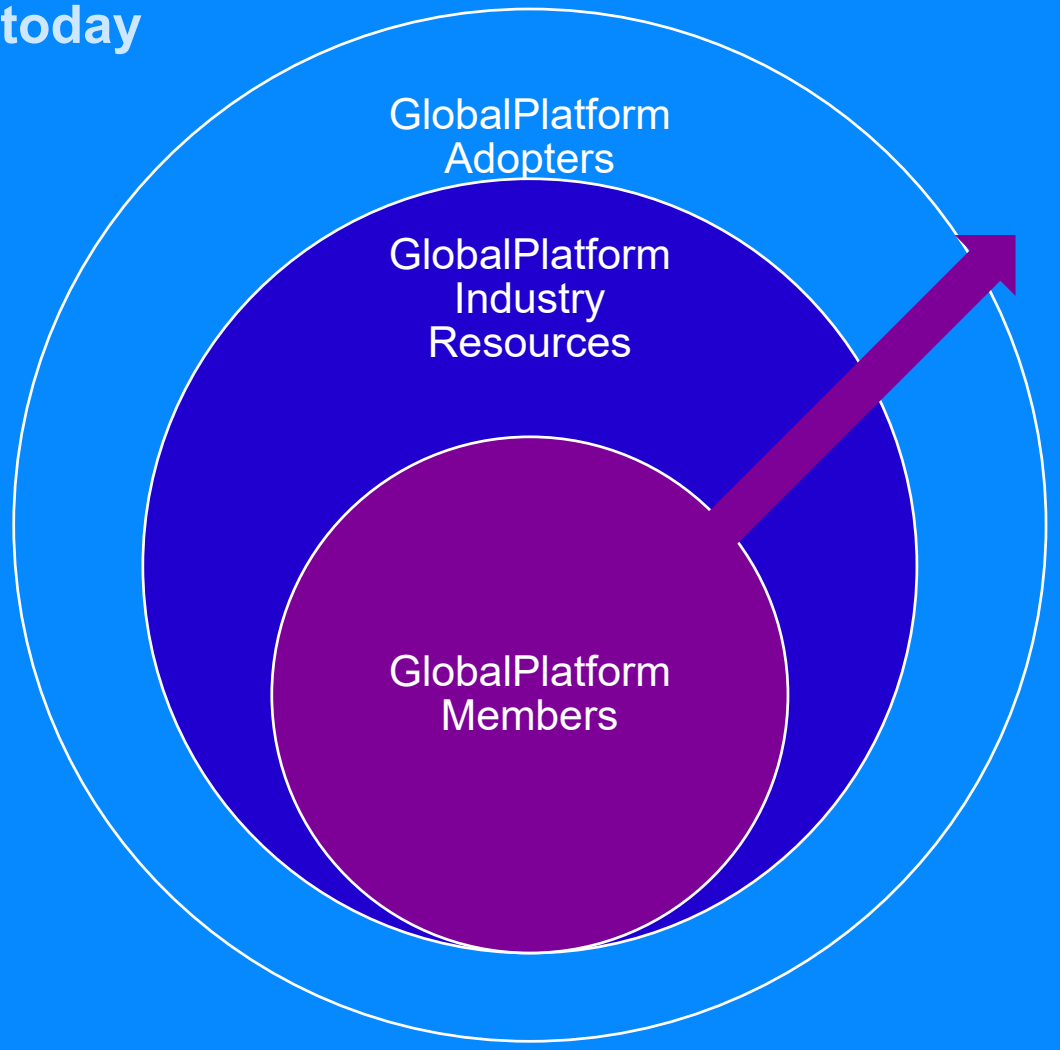
- Digital Rights Management / Media for Advanced Infotainment
- Protecting High Value Assets such as ADAS
- Key and Certificate management
- Personal Data and Biometric

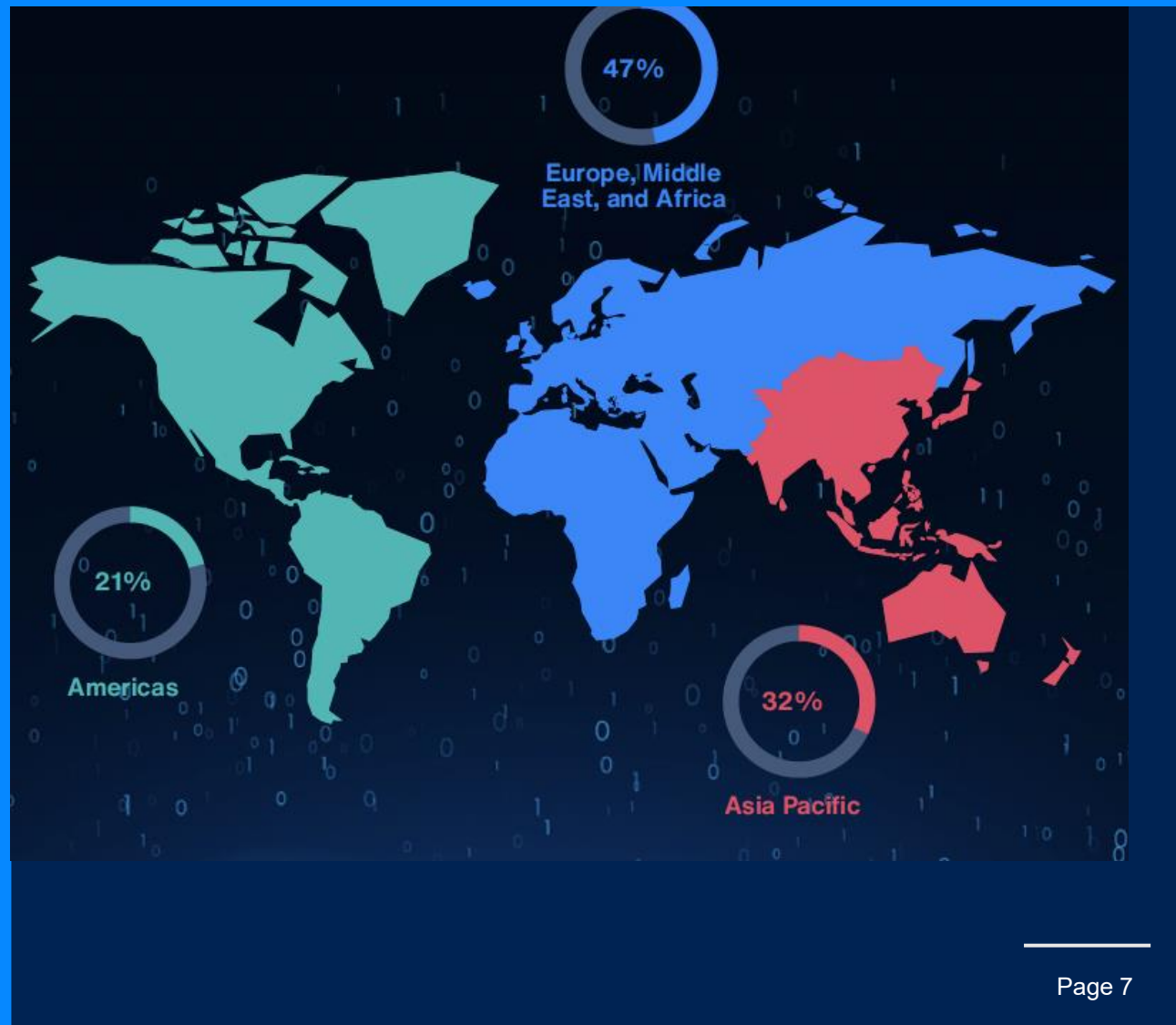
192 Million Connected Cars in 2023 by Juniper Research
https://www.juniperresearch.com/press/connected-vehicles-to-surpass-367-million-globally#:~:text=Hampshire%2C%20UK%20–%209th%20January%202023,from%20192%20million%20in%202023.

*Confidential Source on Market Presence

GlobalPlatform's Market Adoption

- 70 billion+ Secure Elements shipped worldwide are based on GlobalPlatform specifications
- Over 10's of billions GlobalPlatform-compliant Trusted Execution Environment in the market today





Global Platform™

GlobalPlatform Members 1/2

Payment Services

American Express
Cartes Bancaires
Discover Financial Services
FeliCa Networks, Inc.
JCB Co. Ltd.
Licel Cooperation
Mastercard
Visa Inc.

Mobile Device Manufacturers

Apple Inc.
Huawei Device Co., Ltd.
Xiaomi

Mobile Network Operators (MNOs)

AT&T, Deutsche Telekom
KONA International,Orange
SK Telink, Synapse Mobile Networks, T-Mobile

Automotive Tech Providers

CARIAD SE
ETAS GmbH
Woven

Semiconductor & Hardware Vendors

Analog Devices Inc. (ADI)
Arm Limited
Austriacard
Bundesdruckerei GmbH
Dai Nippon Printing
Eastcompeace Technology Co., Ltd
Feitian Technologies Co., Ltd
Giesecke+Devrient
HID Global
Infineon Technologies AG
Kigen Lda
MaskTech Intl GmbH
MK Smart JSC
NXP Semiconductors
Qualcomm Technologies Inc.
PQShield
Renesas
Samsung Electronics
Shanghai Fudan Microelectronics Group
Spreadtrum Communications
STMicroelectronics
Toshiba
Thales
Ubivelox
Xard Pay
XCure
Valid
Watchdata System
Winbond Technology Ltd.
WiseSecurity Technology
Zwipe Germany

GlobalPlatform Members 2/2

OS & Software Platform Providers

CISCO

Google

Oracle

Rambus

Trustonic

Linaro

Public Sector & Government Entities

BSI - Bundesamt für Sicherheit in der Informationstechnik

Department of Defense (USA)

Institute for Information Industry

Wuhan University

Consulting & Integration Firms

Digital Cubes

Galitt

Internet of Trust SAS

Monetech

Nextendis

NthPermutation Security LLC

Safepay Systems

Security, Certification & Testing Labs

Applus+

BacTech

Beijing Unionpay Card Technology

Beijing ZhiHuiYunCe (DPLS Lab)

Brightsight BV

CEA - Leti

COMPRION GmbH

DEKRA

FIME

Kaspersky Lab

Keysight

SERMA

TrustCB

Quarkslab

UL (Underwriters Laboratories)

Your Partner for Security Standards

Collaboration is KEY

Our strong collaborative relationships across the world, from international standards organizations to regional industry bodies, are key to realizing our vision of:

- Fully open ecosystems that focus on interoperability
- Efficiently delivers innovative digital services
- Across vertical markets
- Supporting different levels of security, while
- Providing privacy, simplicity, and convenience for the user.

GlobalPlatform has 34 Industry partners from around the world, integrating our specifications and services in their work.

GlobalPlatform's Success in International Digital Security Transformation

- Interoperable APIs
- Publicly available on a royalty free basis

Test Suites

Protection Profiles

- Test Suites
- Common set of security needs
- "I want" this level of security

3rd Party Certification

- Functional / security
- A mechanism to provide Vendors the ability to make claims regarding their security products

As a security foundation for service / device innovation in mass market deployments for different industries, e.g. mobile market and services

Common Criteria definitions source: https://commoncriteriaportal.org/files/ccfiles/CC2022PART1R1.pdf

GlobalPlatform Brings Lessons to Automotive:

How to Create the Security Foundation for a Healthy, Innovative Ecosystem Services

GlobalPlatform standards create a fertile environment for mass market growth and innovation of services and hardware

Services are key dynamic of industry BUT hardware remains a critical base for trust

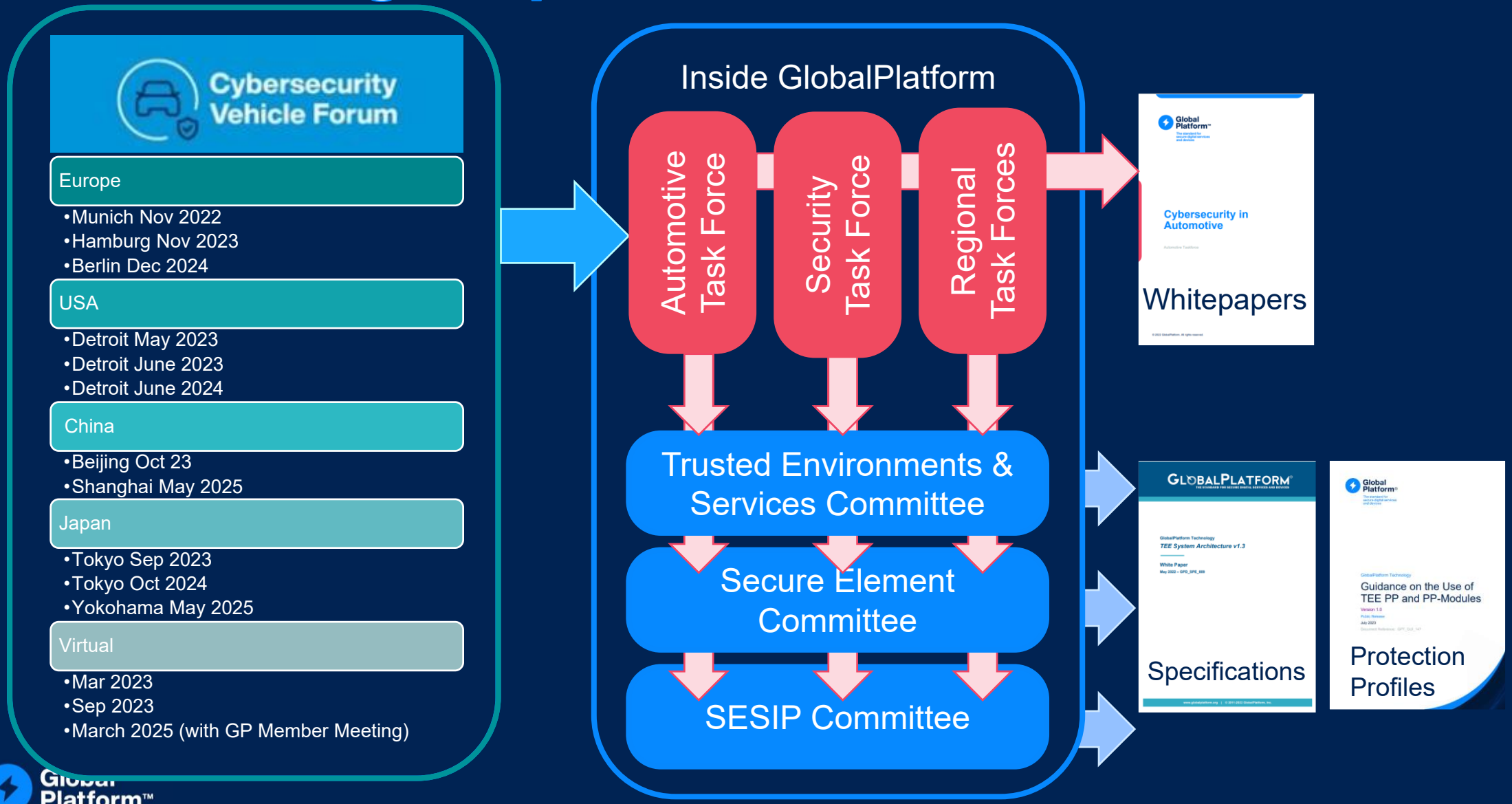
High Evolution in Markets over time, with issuance of new services on very short timelines (3-6 months).

With standardised portability and updatability, device product life is extended since it can adapt to requirements of new services.

Synergistic opportunities (also across “Frenemies”) for the development of new services (not everything has to be developed from scratch by a provider)

Based upon GlobalPlatform’s Experience in Over 25 Years with Smart Cards, Mobile, IoT

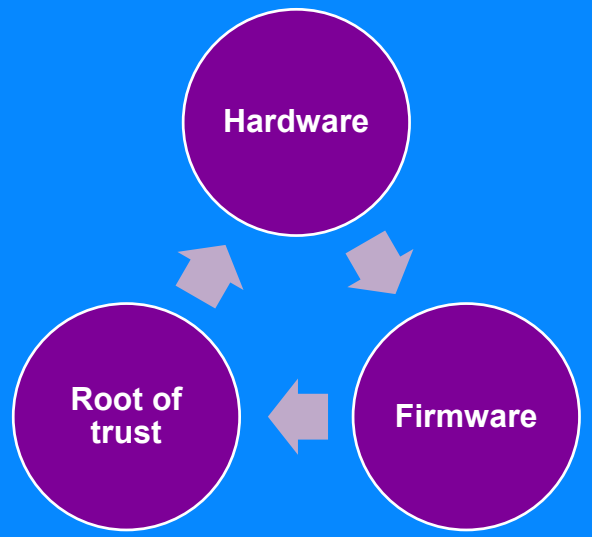
Driving Requirements into GlobalPlatform



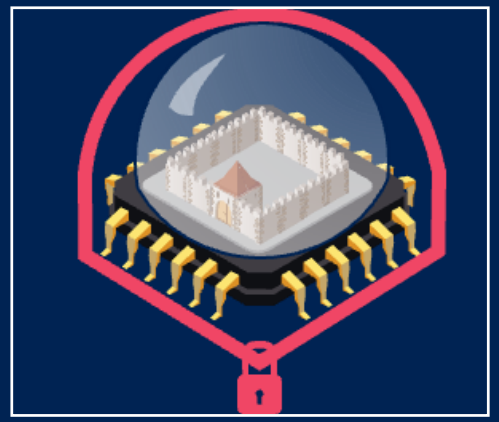
Global Platform™

GlobalPlatform Technology

GlobalPlatform Foundation Technologies



Secure Element

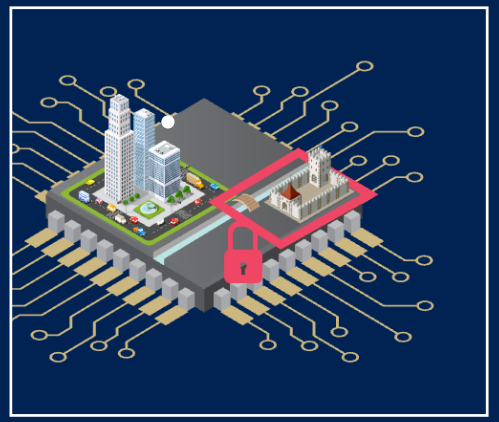


A secure enclave protected against physical and software attack

- Tamper resistant hardware
- Install, update OTA applications (not just keys)
- In OVER 192 Million Connected Cars in 2023 (Juniper Research)

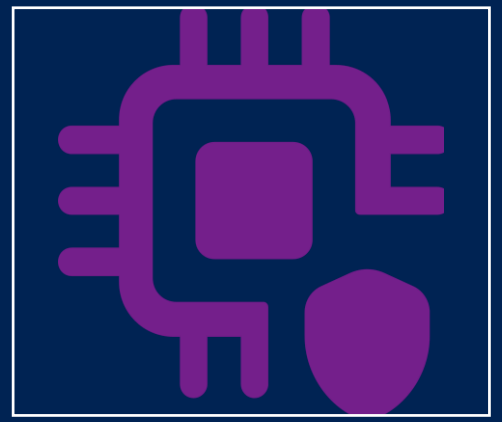
https://www.juniperresearch.com/press/connected-vehicles-to-surpass-367-million-globally#:~:text=Hampshire%2C%20UK%20–%209th%20January%202023,from%20192%20million%20in%202023

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
- In Over 100 Million Vehicles as of 2023 (Confidential Source)

Isolated Technologies



- New Technologies that create 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™

Roots of Trust for Secure Software: Providing OEMs Standardised Management Capabilities

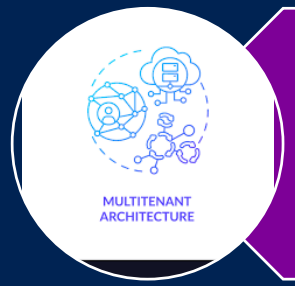
Plenty of hardware, root of trusts, each with secure crypto

- OEM Manage Objects across different producers
- Key management + crypto between hardware and service layers

GlobalPlatform provides a bridge between hardware and software security – as well as supporting across multi-tenant service providers. Standardisation of the common security requirements, augments hardware and software with interoperable functionality and transparent security robustness levels.

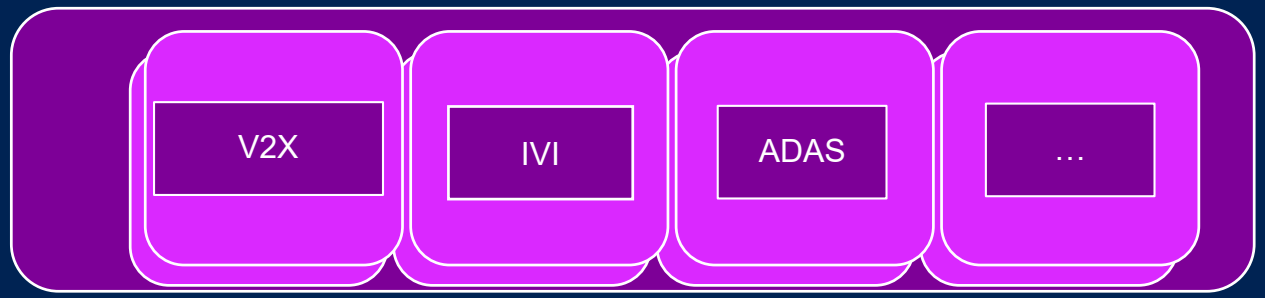
Global Platform™

GlobalPlatform Setting the Standards for Common Security Specifications



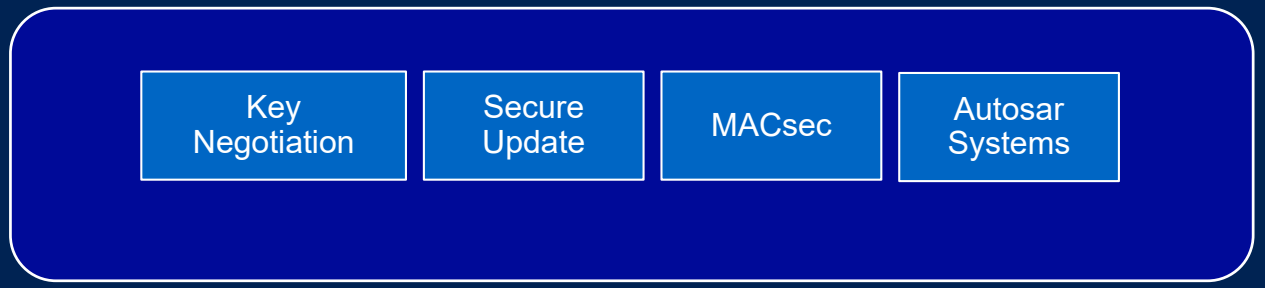
Vehicle Services

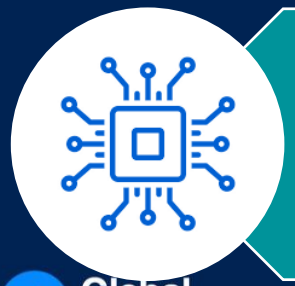
- Broader Vehicle Services (building upon Trusted Applications)



Automakers & Standardised Auto Solutions

- OEM Controlled Trusted Applications (using GP standardized APIs)





Silicon and Hardware & GlobalPlatform Platform:

- Standardized APIs & Management
- Update
- State-of-the-art Crypto
- Crypto Agility

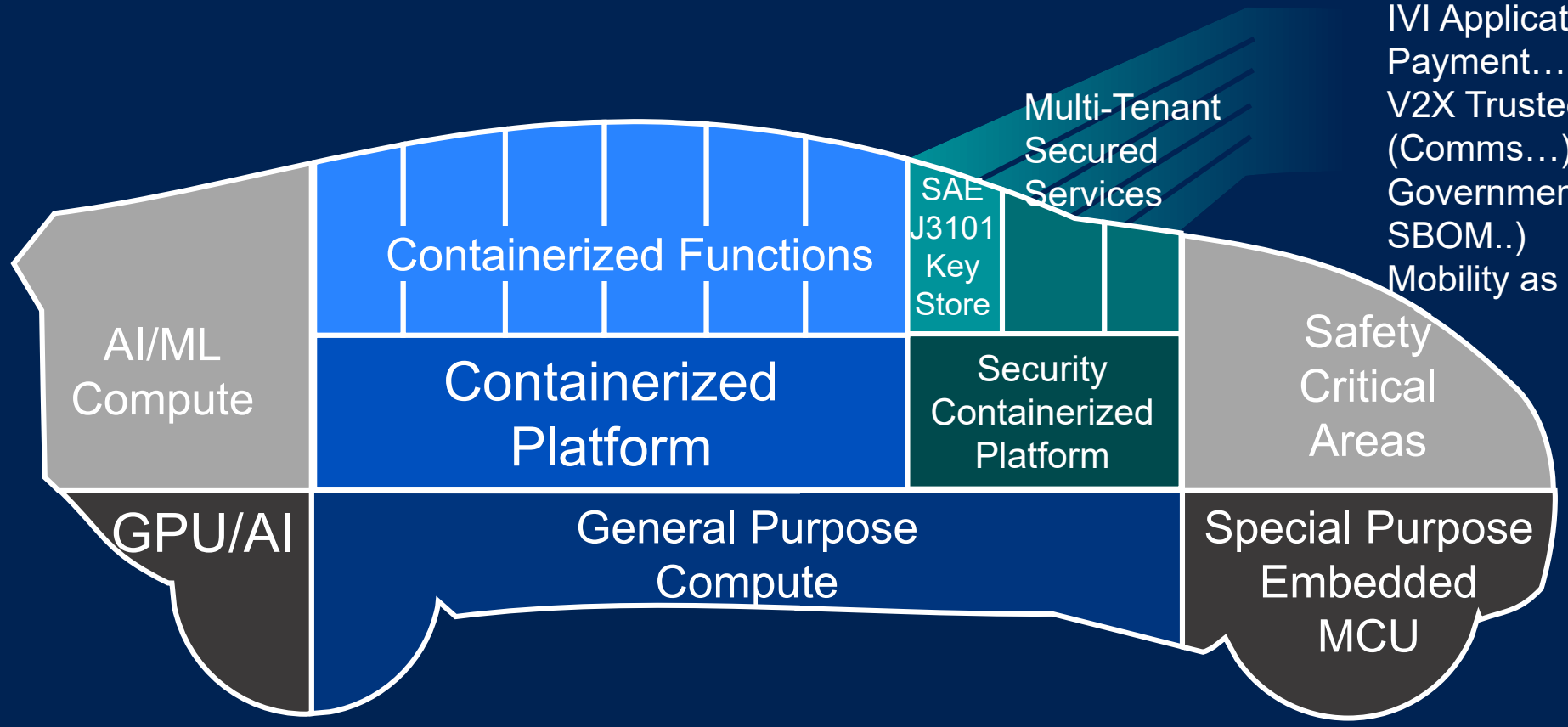
Global Platform™

Supporting Software Defined Vehicle Use Cases: Examples of Functional Security Primitives

Device Attestation	Secure Updates	Secure Onboarding and Offboarding	Secure Provisioning and Decommissioning	Secure Communication (Protocols)	Secure Debug and Test
Secure Backup and Recovery	Account Authentication and Management	(Attested) Secure State and Life Cycle Management	Genuine Identification	Secure Initialization	Anomaly Detection and Reaction
Cryptographic Key Generation and Injection	Cryptographic Key and Certificate Store	Secure (Encrypted) Storage	Cryptographic Operation	Cryptographic Random Number Generation	System Event Logging
Silicon Root of Trust	Residual Information Purging	Software Isolation	Monotonic Time	Reliable Control Transfer	Cyber Resilience

https://www.nxp.com/docs/en/white-paper/SEC_PRIMITIVES_WP.pdf

GlobalPlatform & In-Vehicle Multi-Tenant Services



Digital Car Key
General Purpose Security (KeyStore…)
IVI Applications (DRM, Payment…)
V2X Trusted Applications (Comms…)
Government Regulation (Audit, SBOM..)
Mobility as a Service (….)

GlobalPlatform Approach

OEMs and Tier 1s can manage key rotation

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

SIM	Sec Boot	ECU ID	DRM
Key Negotiation	ADAS	FOTA/ SOTA	IDS
Sec Logging	Auth Cmd	Payment	Digital Car Keys
Firewall	SecOC	MACsec	IVI

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

Secure Component Platform: Functionally and Security Certified

Hardware

This approach fits well with Software Defined Vehicles with upper layer security certification

Securing Any SDV Service with GlobalPlatform

Multi-Tenant Security Services

Security Assurance of Products Demonstrated by Certification

Agility in Deployment of Common Security Requirements while supporting innovation

Multiple, Comprehensive Update Features

Designed To Support Future Cryptographic Requirements & Evolving Regulations

Leverages combined expertise of community in deploying security specifications & in addressing emerging threats

Global Platform™

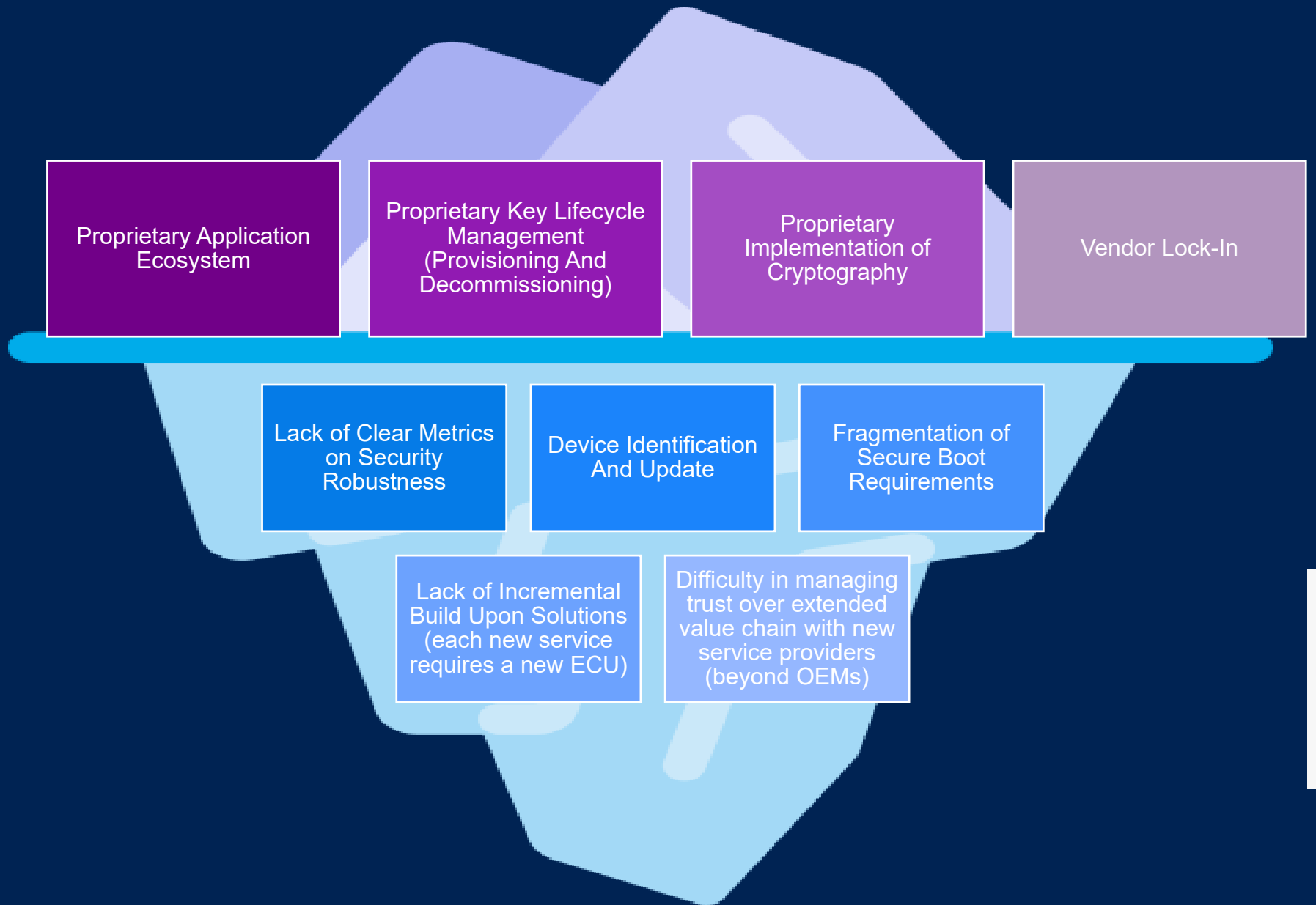
Global Platform™

Automotive GlobalPlatform

Need for New Tools in Automotive to Meet SDV Promises:

Standards, Certification, APIs, Guidelines

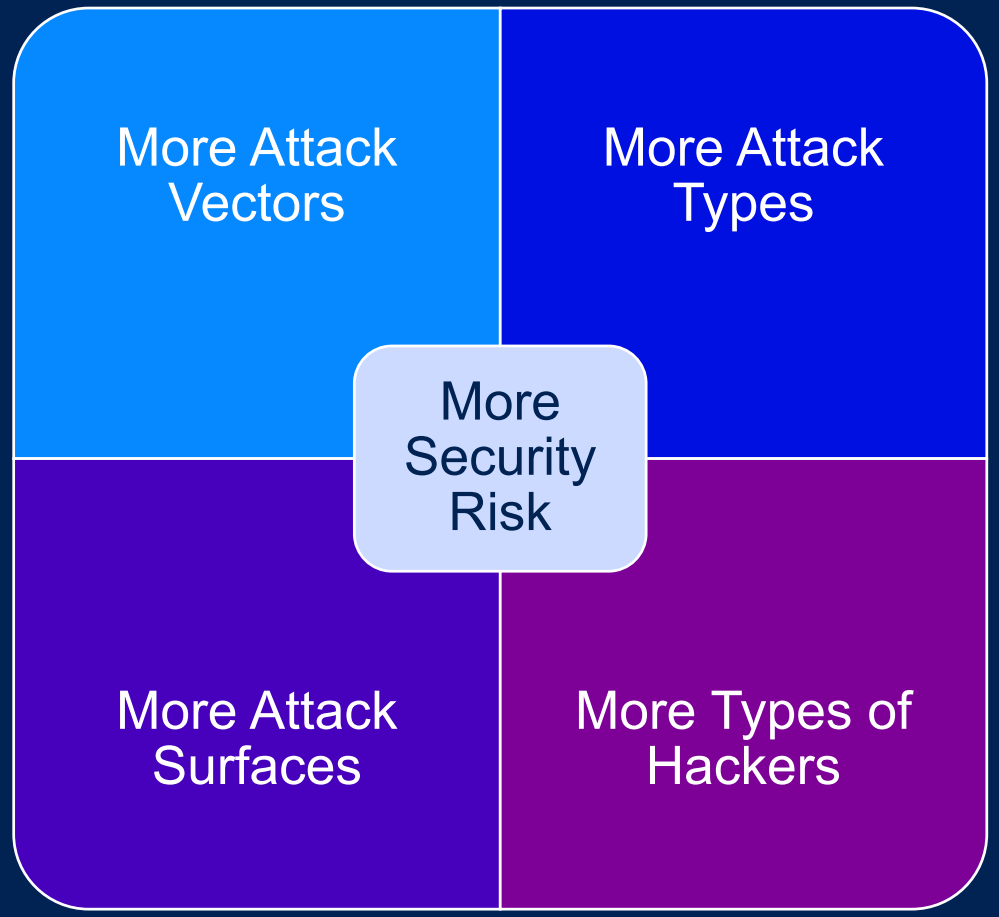
Challenges of Automotive Security Market Today



Big Changes are Coming with Software Defined Vehicles

New Architectures, New Services, New Players

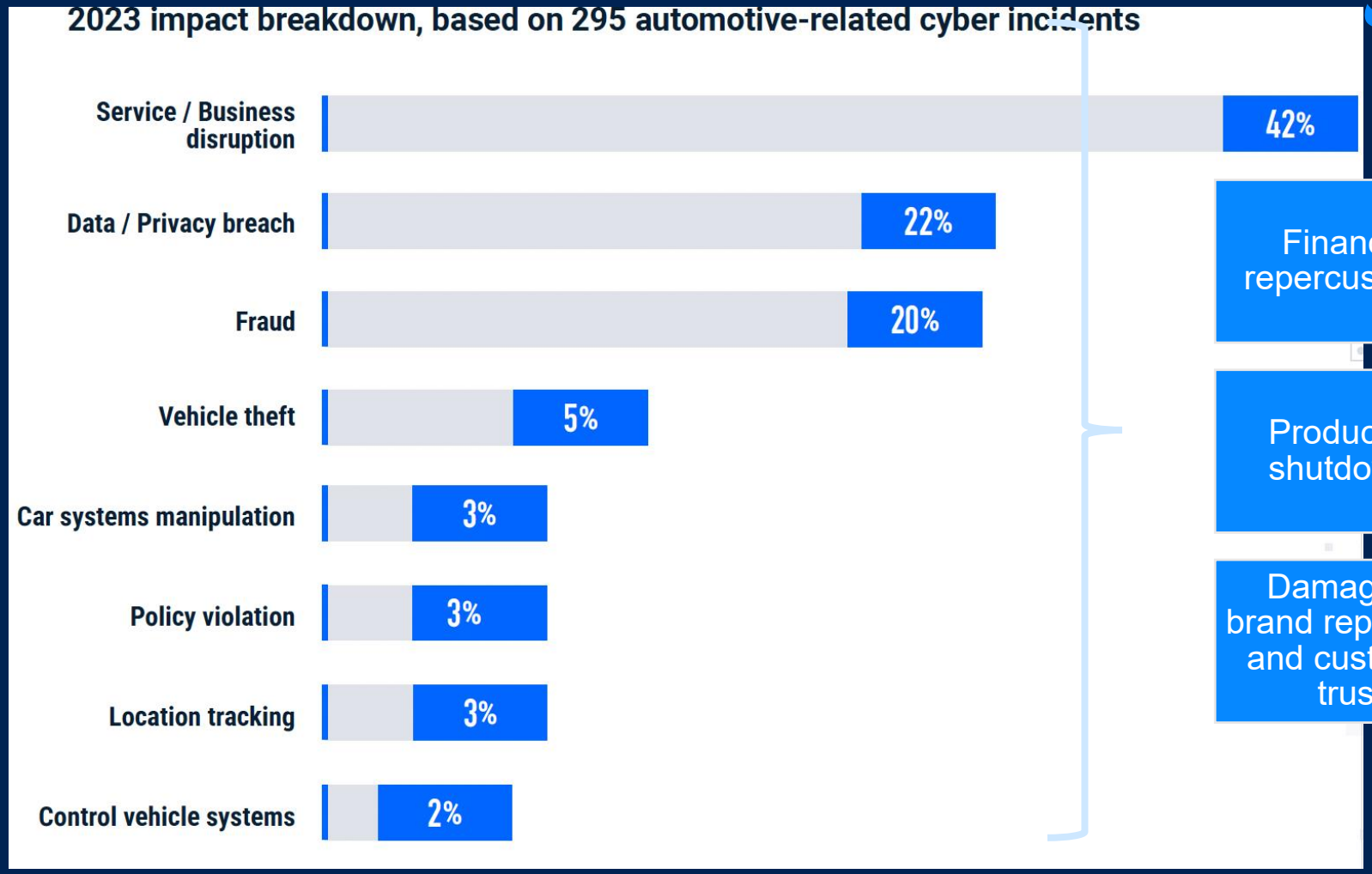
https://semiengineering.com/software-defined-cars/



Global Platform™

https://www.microsoft.com/en-us/industry/blog/manufacturing-and-mobility/automotive/2023/10/31/the-security-cultural-transformation-of-the-automotive-industry/

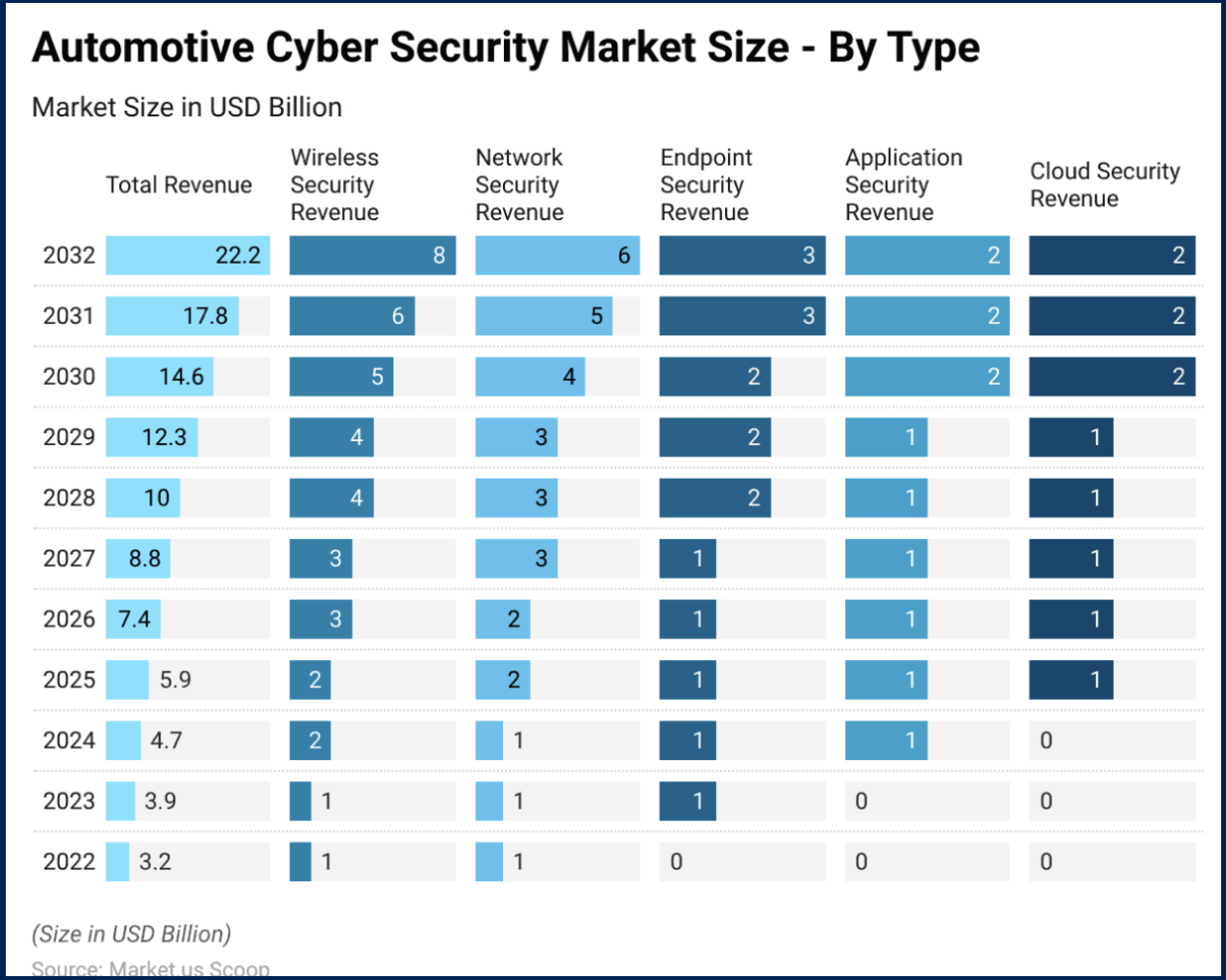
Cyber Incidents Are Expensive



- Financial repercussions
- Recalls or OTAs
- Production shutdowns
- Ransomware payments
- Damage to brand reputation and customer trust
- Large regulatory fines

Source:(Upstream 2024). https://upstream.auto

Forecasted Revenue in Cybersecurity by Security Type



Who Pays?

https://scoop.market.us/automotive-cyber-security-statistics/

No one wants to pay for “Security” BUT ….
OEMs have Increased Skin in the game to warrant Cybersecurity Spend

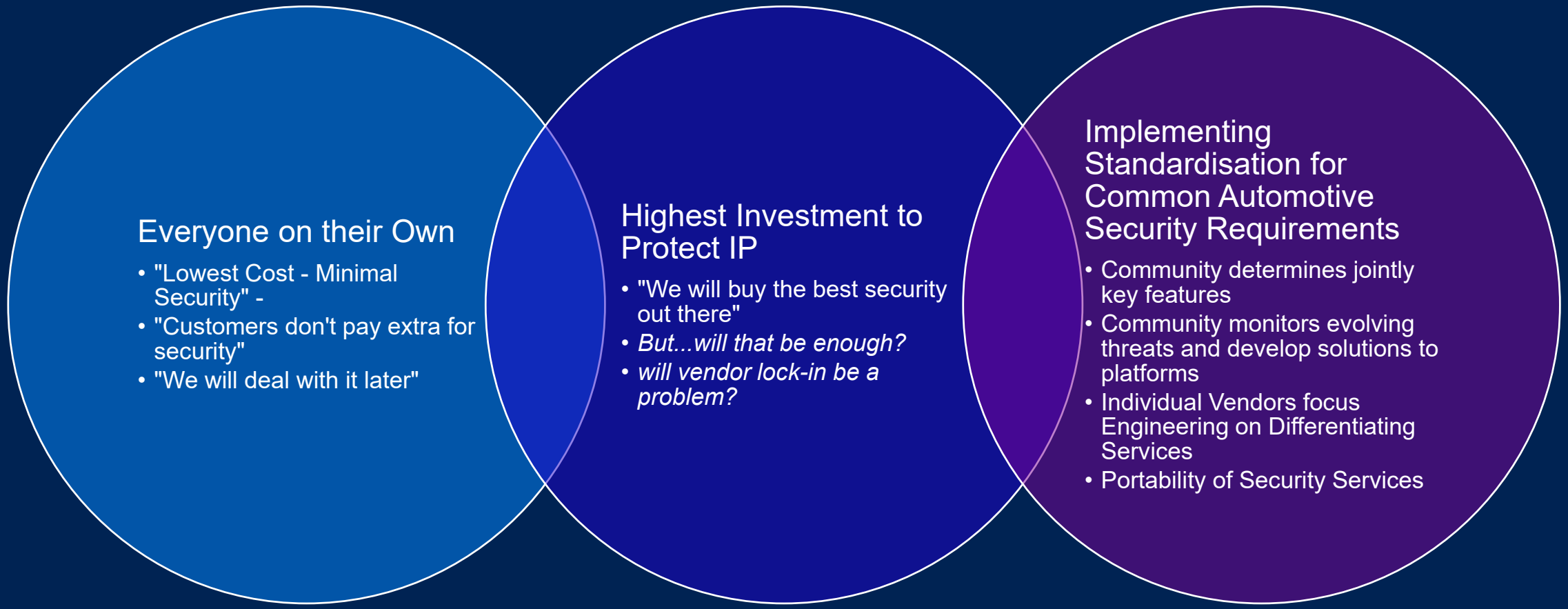
Regulatory Compliance & Reducing Liability

- Compliance with Cybersecurity Management Processes for type approval (UNECE 155 64 countries)
- Evidence of implementation of best practices

Protecting Investments

- Protecting High Value of Software Assets of Vehicle
- **Protecting Against Unpaid Feature Enablement**
- **Reduction of Warranty Fraud**

Different Security Paths by Automotive OEMs



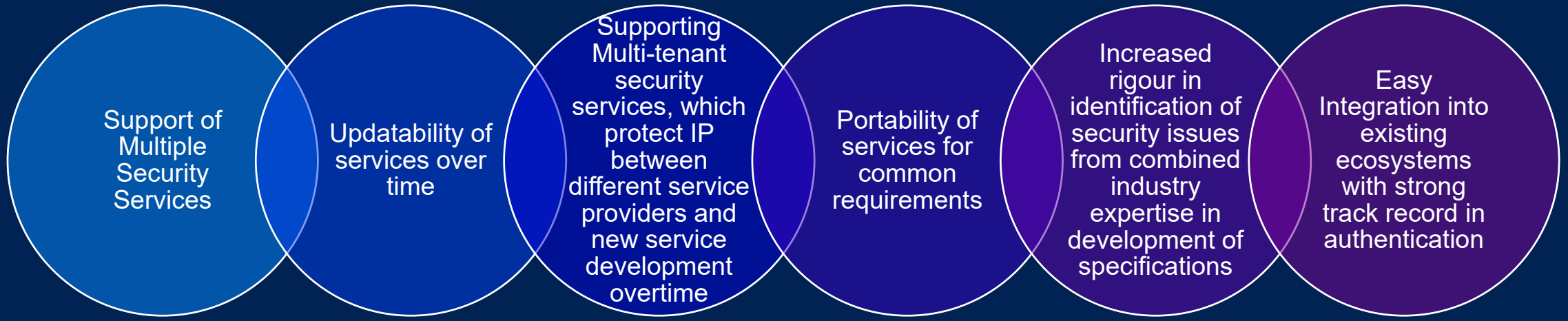
Low Cost,
High Risk
Potentially Untenable Future

Higher Cost,
Lower Risk Today
Unclear Future

Shared Cost (split between participants)
Lower Risk Today & Future
Provides Needed Future Flexibility

GlobalPlatform Provides Future Proofing of Security Services & Adds Flexibility

Unlike traditional automotive HSMs/SHEs, GlobalPlatform offers standard requirements, common APIs, testing suites, and certification of compliance with specifications on security robustness and interoperability



Possibility of reuse, incremental developments across ECU evolution (without having to start over from scratch each time for every new ECU project)

Example of SDV Security Standardisation Benefits

- Open Portable Application Ecosystem
- Standardised Key Lifecycle Management (in-house or SaS solutions)
- Standardised State of the Art Cryptography
- Standardised Levels for Security
- Innovation for non-common security services

…Resulting in Flexibility & Transparency on Robustness

- Certification of Functional and Security Robustness
- Device Attestation (secure state and lifecycle) inherited from root of trust
- Standardised Secure Boot Requirements
- Ability to Incrementally Build Upon Security Applications
- More Plug and Play in the Supply Chain, while maintaining High Levels of Trust

Global Platform™

Hardware Protected Security Environments

SAE J3101-5

Why was J3101 created?

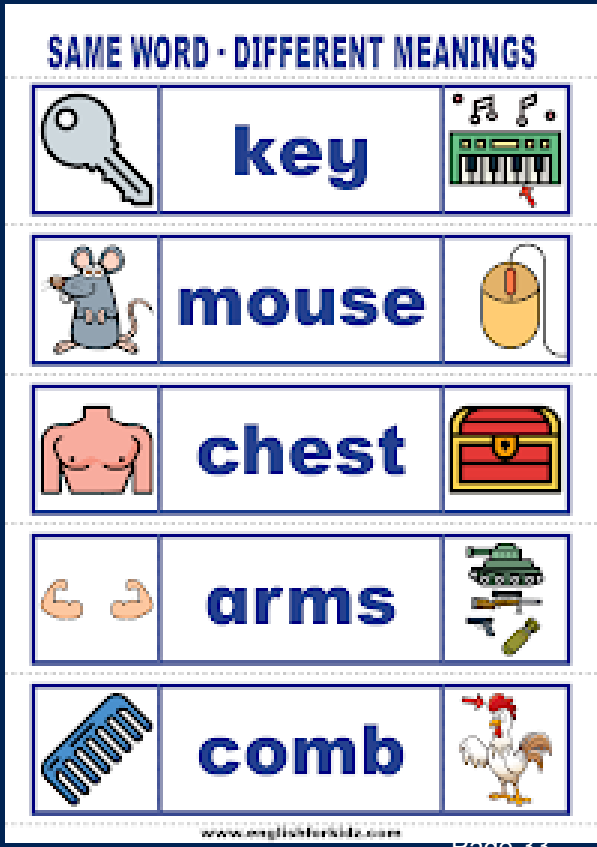
Global Automotive Market uses different references to for hardware protected security environments.

Some names include:

- HSM
- SHE/SHE++
- EVITA

BUT

- Each vendor means something different
- Has different characteristics
- No framework to compare across products



SAE J3101: A Common Reference for Hardware Protected Security Environments

Basic characteristics

Establish trustworthiness through device identity, sealing, attestation, data integrity, and availability.

Must be resilient to a wide range of attacks that cannot be thwarted through software-only security mechanisms.

Requirements for a hardware protected security environment

A hardware root of trust and the hardware-based security primitives are fundamentally necessary to satisfy demands of 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

Why Cooperation with SAE on Hardware Protected Security Environments Is Optimal

SAE USA J3101

Defines Common Glossary of Required Hardware Protected Secure Environment Characteristics

GlobalPlatform

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 and
- Proven security robustness (protection against attack) obtained
- Possibility of composite certification

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].

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

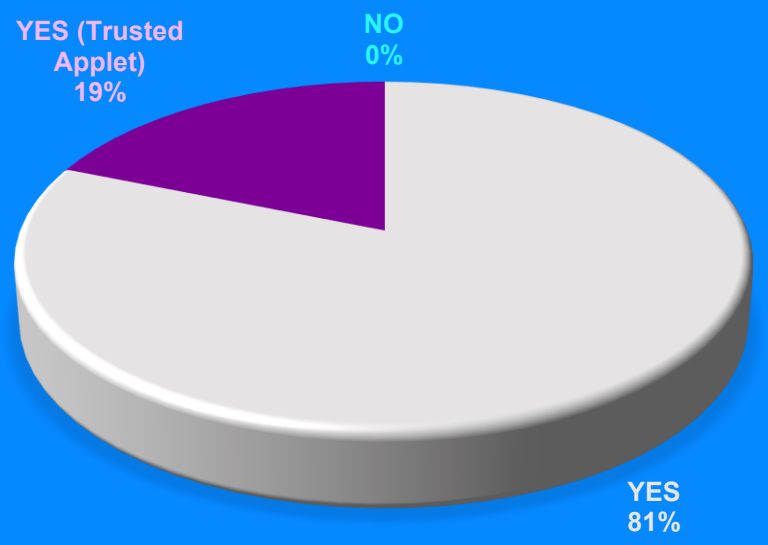
Only 3 J3101 requirements are not fully met by GlobalPlatform (TEE) specifications.

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

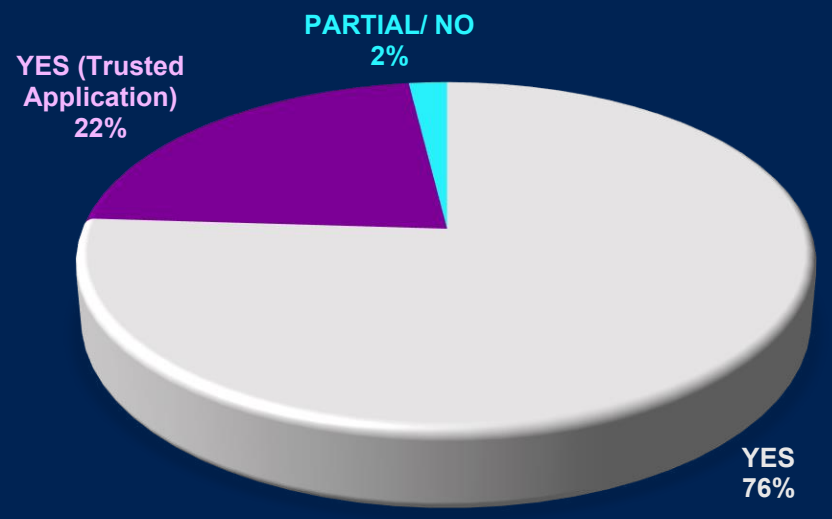
Furthermore, firmware update of the TEE itself is outside the scope of the TEE protection profile but Trusted Application (TA) update is covered by TMF protection profile.

Analysis Results: GlobalPlatform Specifications

Secure Element Satisfaction Of 100% OF J3101 Requirements

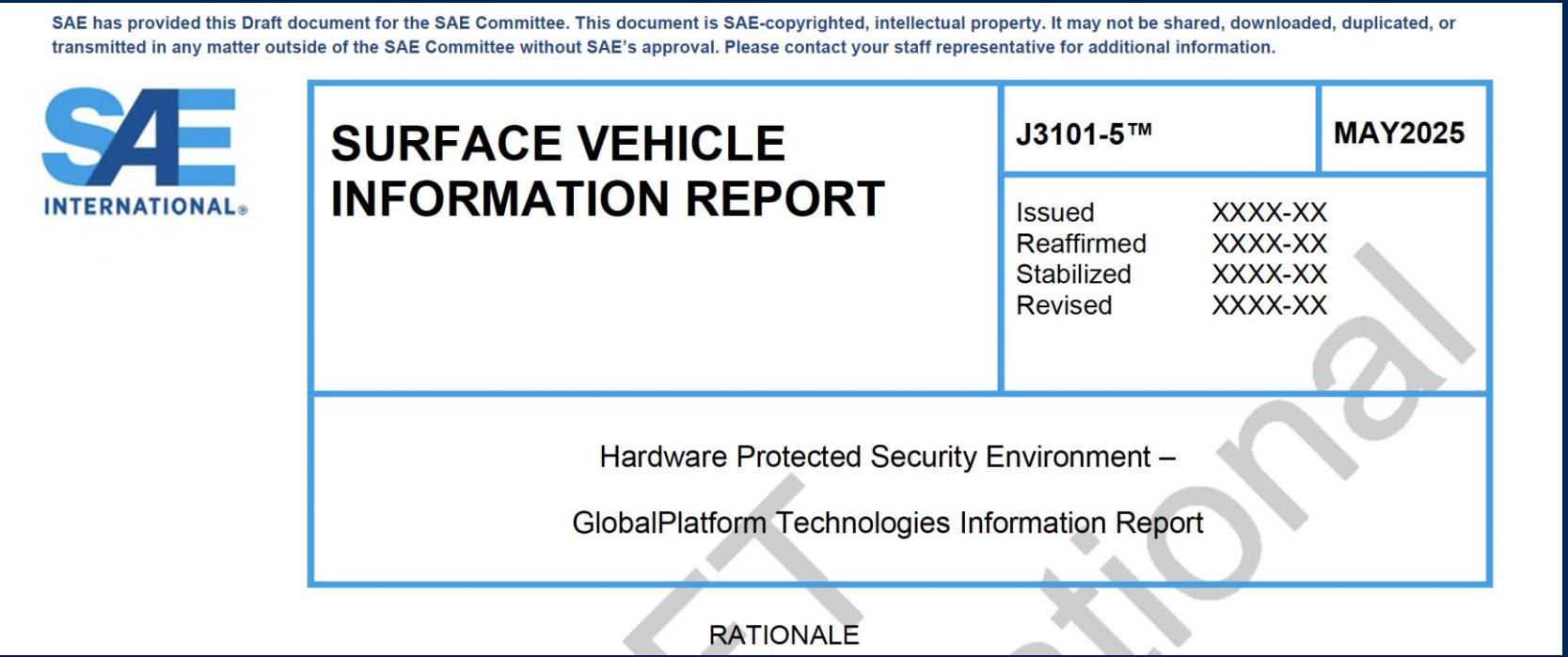


Trusted Execution Environment Satisfaction Of 98% Of J3101 Requirements



Evaluated using Common Criteria (CC) existing Protection Profile

Global 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

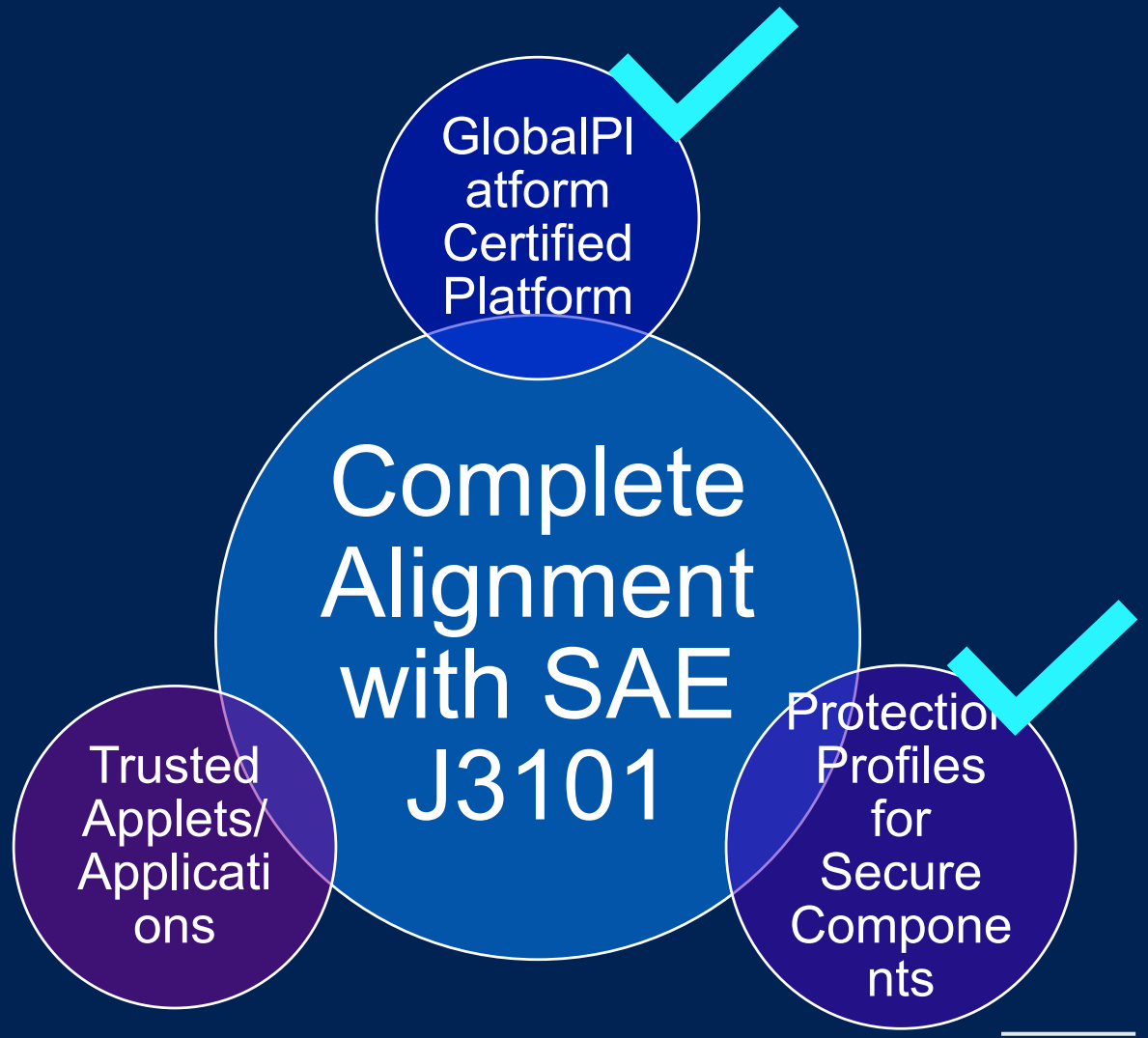
What is the importance of J3101-5?

GlobalPlatform Solutions Comply "Automatically" to J3101 for the Platform

AND

GP Technology leverages proven rigorous security while ensuring functional interoperability

GP Technology provides Flexibility in development of the Trusted Applications



SAE J3101 Demonstrating Compliance with SESIP Profiles for GlobalPlatform Secure Components

GlobalPlatform Protection Profiles (~76/81% of requirements)

+

J3101 Trusted Application/ Applet Protection Profile (~19/22% of requirements)

- TBD

=

J3101 Full Compliance for Secure Components

Detailed Implementation Guidelines have been Defined by GlobalPlatform as well as How to Test

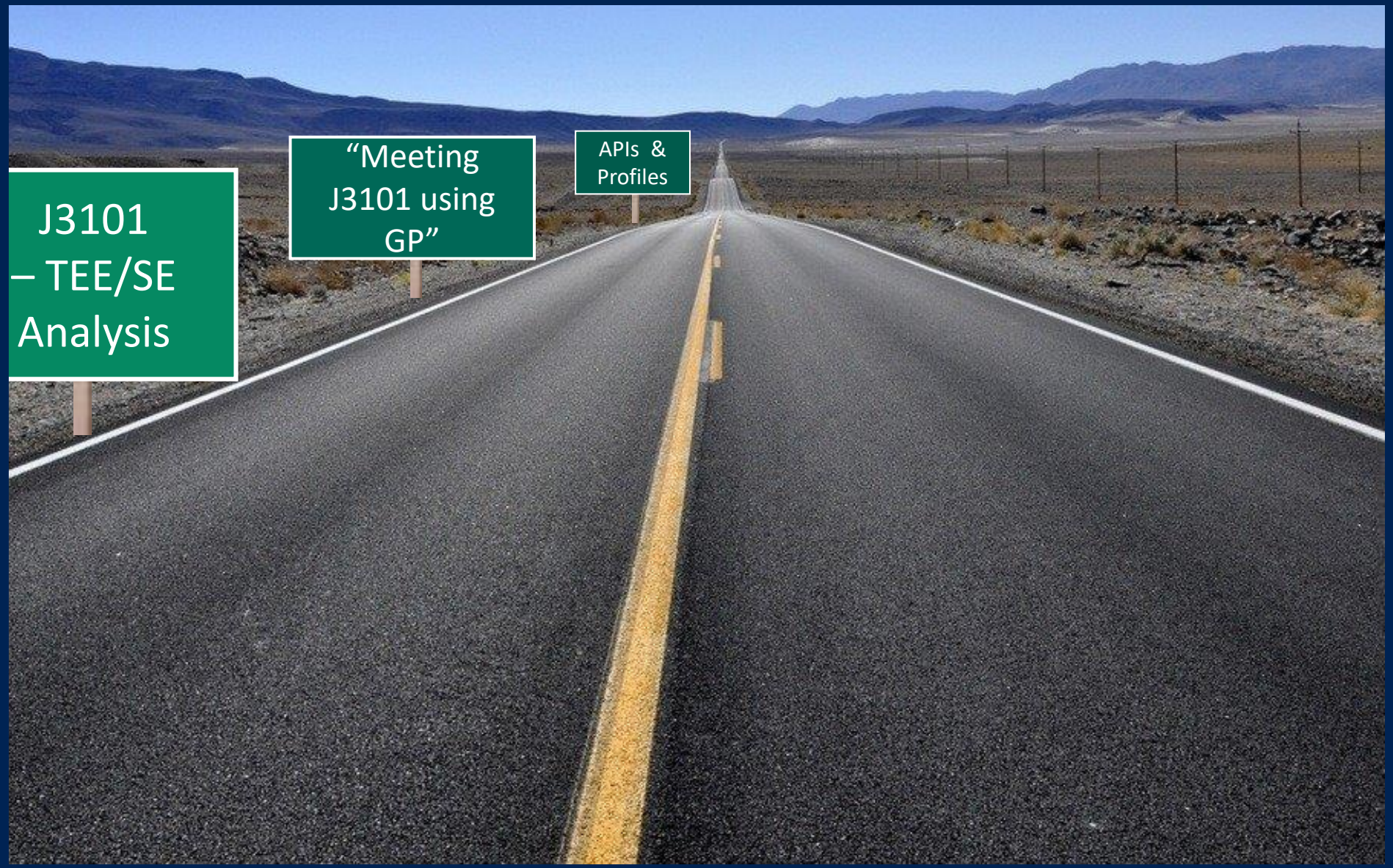
No Implementation Guidelines have been Defined by GlobalPlatform nor How to Test

Going Forward

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?



Hardware Protected Security Environments in China: Open Questions

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

Is there interest in standardising a Chinese version?

Would it be useful to cooperate with GlobalPlatform to explore how GlobalPlatform technologies meet eventual Chinese specific requirements?

Would it be useful to provide some educational opportunities on GlobalPlatform technologies?

Global Platform™

SESIP Certification:

How it works and its use in Automotive

Francesca Forestieri, Head of Automotive
Gil Bernabeu, CTO

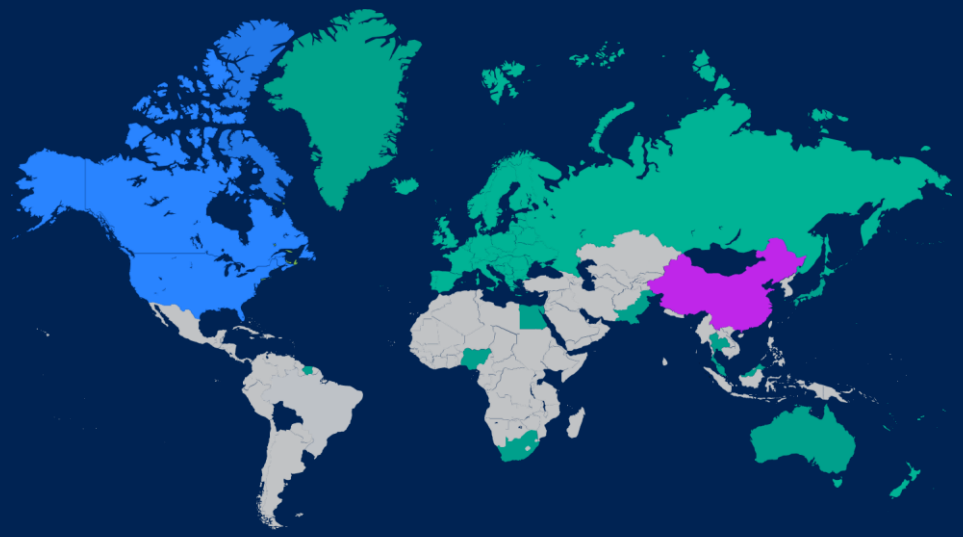
Why does security certification matter?

1. World is a scary place?

Cybercrime and cyber insecurity are new entrants into the Top 10 rankings of the most severe global risks over the next decade, according to the World Economic Forum.

Now taking the 8th spot, cybercrime now stands side-by-side with threats including climate change and involuntary migration.

2. Emergence of Regulations and Standards on CyberSecurity?



CN CS Law GB

UN R155 / 156 AND ISO/SAE 21434 and 24089

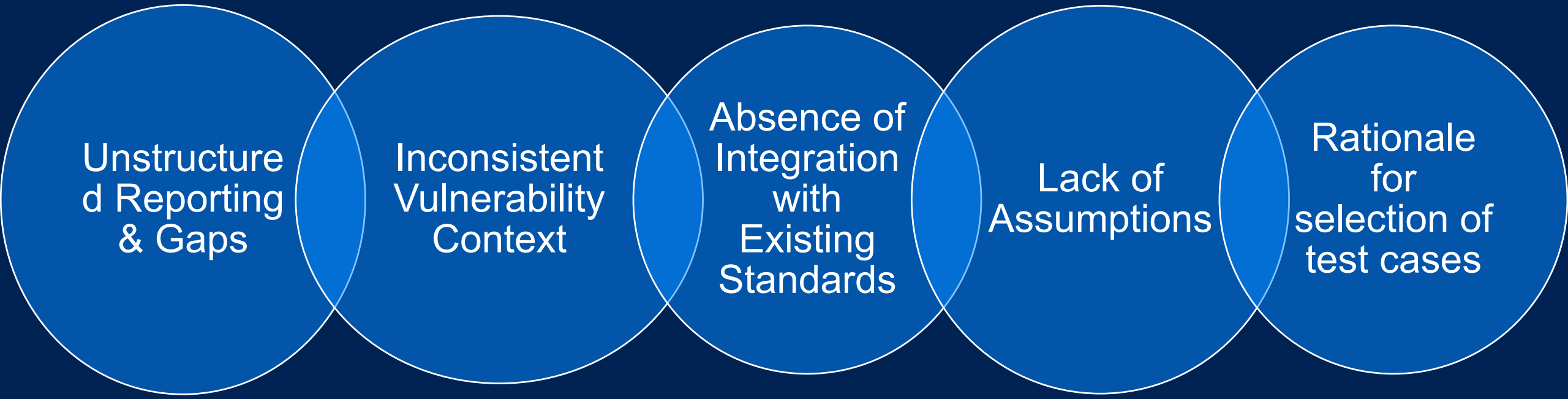
64 Countries

SAE/ISO 21434 and 24089

https://cybersecurityventures.com/cybersecurity-almanac-2023/

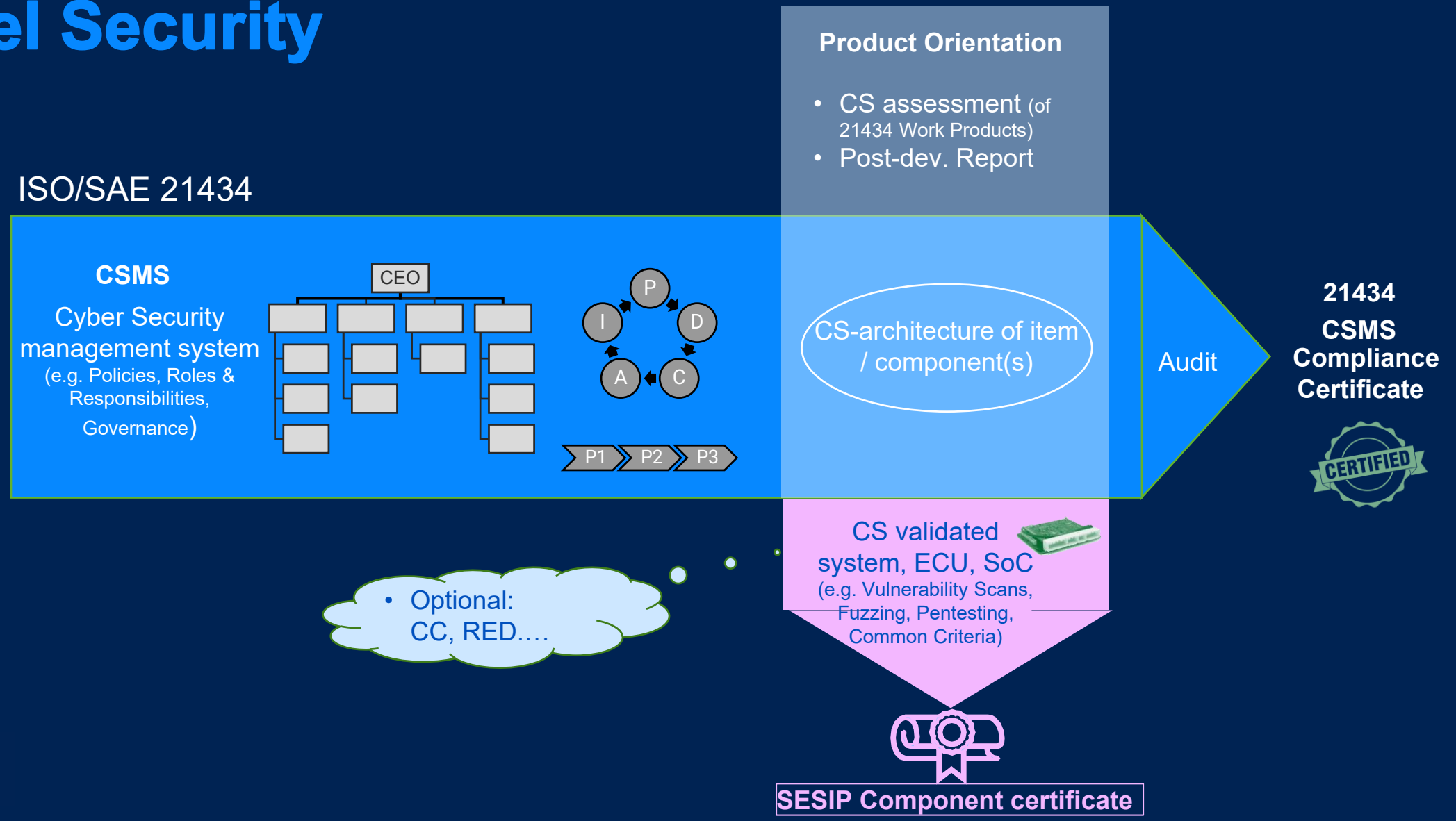
Implementation of UNECE 155 & 156 ….. Complicated

Frequent Rejection of Reports at Type Approval

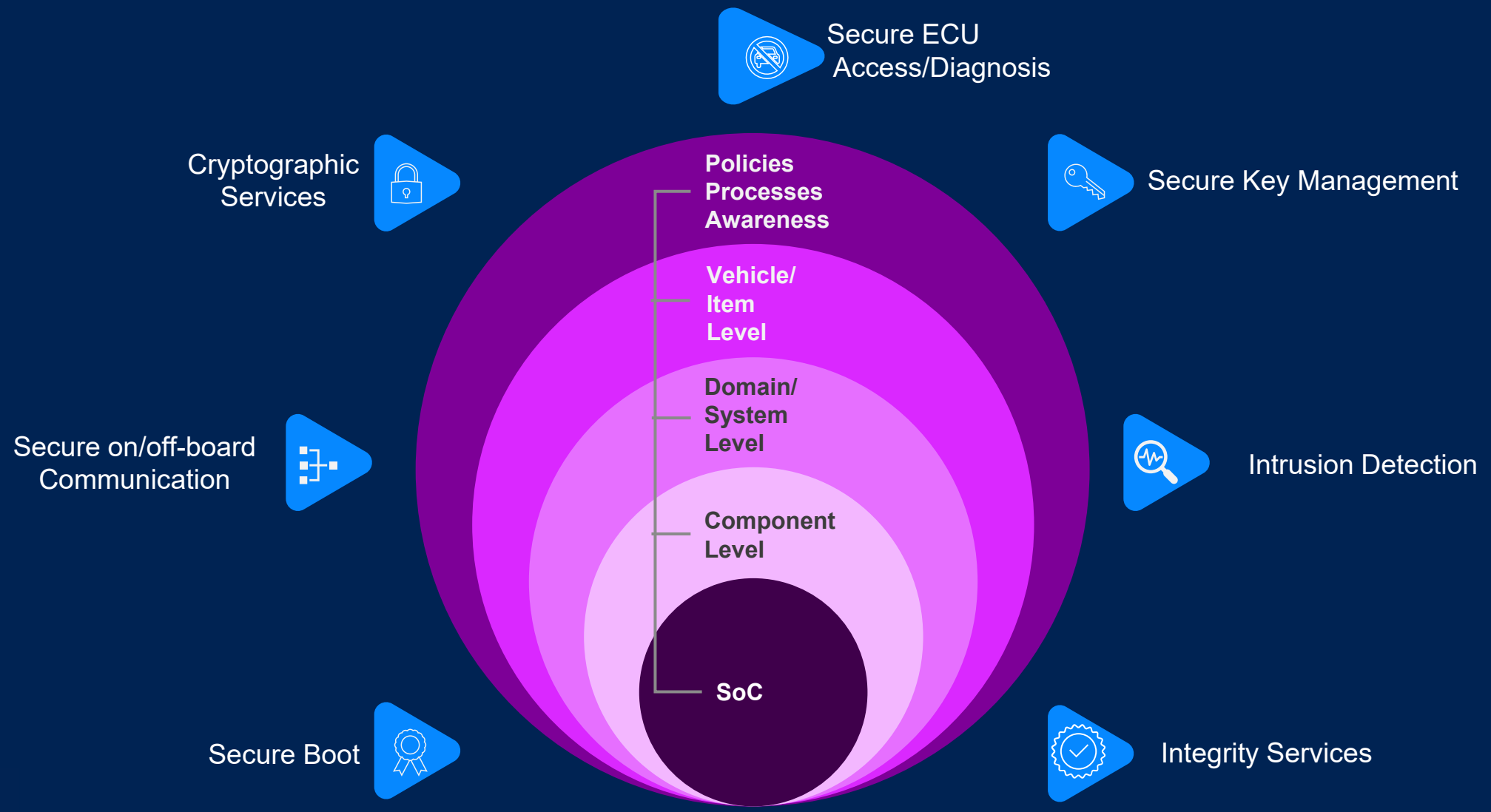


Examples of Common Reasons

Certification Framework for UNECE Countries, Using SESIP to Address Component Product Level Security



SESIP Opportunity: Beyond SoCs



Global Platform™

SESIP Evaluation: Goal Oriented

Focuses on whether security outcomes are achieved not just whether processes are followed.

Less emphasis on extensive formal documentation

More on evidence that requirements are met (as compared to Common. Criteria)

Certifying to Desired Security Robustness Levels

A complete set of Hardware & Software countermeasures + certification

	Software attack	Board-level attack	Silicon-level attack
Major attacks	• Network protocols weakness (weak ciphers, short keys,…) • Flaws in software design / implementation, buffer overflows • Debug interfaces, gaining admin rights	• SPA / DPA Power analysis, emission analysis, timing analysis • Fault injection: glitches, laser, light, UV, X-rays, Electro-Magnetic • Memory probing	• Device delayering, circuit reverse engineering, micro-probing • Fault injection: Focused Ion Beam • Advanced microscopy
Countermeasures *Hardware & Software*	• No external debug interface • Hardware secure crypto fast computing • Enhanced security of MCU with physical isolation of security toolbox (secure key storage, secure & trusted execution in secure element)	• Randomization • Secured crypto-engines • Design Flow • Power regulation • Environment Sensors • Integrity checkers • Code Signature • Internal Clock Integrity • OS features (MPU) • Jittered Clocks • Data whitening	• Physical Shield • Lock-step EDC • Glue Logic Layout • Bus & Memory Scrambling • Bus & Memory Encryption • Anti-reverse • Advanced Lithography

Security level

HSM EAL up to 3

Common Criteria
eSE EAL6+
AVA VAN 5

~SESIP 2 or 3

Ex: Side channel 60 to 5k curves robustness
=> hacker in a garage

~SESIP 4 or 5

Ex: Side channel >1M curves robustness
=> BSI or expert lab

Global Platform™

SESIP Process for Certification: Based on Vendor Positioning Market

Select applicable Protection Profiles for product

→

Detail Security Target

- Developed by Vendor
- Definition of Standardised protection profile for product
- Definition of the Target of Evaluation (scope of system to be tested)

→

Select a SESIP Certified Lab & Certification Body

- provide product and documentation
- sign contract with lab

↓

Lab Testing

- development of test plan for product
  - according to
    - Protection profile,
    - security targets,
    - target of evaluation, and
    - latest rules of implementation of the SESIP methodology, including:
      - attack, functional tests, process/document verifications, audit etc.
- Validation of testing plan by certification body

→

Issuance of SESIP Certificate with Level for Product X

- Validation of testing results by certification body
- Certificate indicates which PPs are satisfied

Benefits of Scale

Common Hardware System Requirements for Platform As a basis for SDV

Security Target Definition: Key Decisions

Define TOE Boundaries:

- Clearly identify what's in/out of evaluation scope

Select Assurance Level:

- Choose appropriate SESIP level (1-5) based on risk

Document Assets & Threats:

- Identify what needs protection and potential attacks

Set Security Objectives:

- Define security goals addressing all threats

Select Requirements:

- Choose appropriate Security Functional Requirements (SFRs):

•Authentication
•Secure Boot
•Communication Security
•Cryptographic Support
•Secure Storage
•Self-Protection

Role of Protection Profiles in SESIP

Setting Standardized Requirements

- Establish **baseline security requirements** for product categories
- Represent **industry consensus** on necessary security features
- Create **common security language across manufacturers**
- Define appropriate security level **based on product risk**

Streamlining Security Target Development

- Provide ready-made **template for Security Target creation**
- **Reduce effort** for product developers and evaluators
- Ensure **consistent security approach** across similar products
- **Simplify conformance demonstration** through structured requirements

Enabling Consistent Evaluation

- Create **uniform evaluation criteria** for certification laboratories
- Establish **standard test methodologies for specific product types**
- **Reduce** subjective **interpretation** of security requirements

Facilitating Market Comparability

- Enables "apples-to-apples" **security comparison** between products
- Create **recognizable security profiles for procurement**
- Establish **clear security expectations for specific product categories**
- Support **security differentiation** while ensuring baseline protection

Standardised SESIP Profiles Exist can be point of Departure for Product Specific Profiles

Lowest level building block of platforms with immutable root of trust

Secure MCU/MPU

Secure External Memories

Code Update Mechanism

WPC Qi Secure Storage Subsystem

Edge Compute Node

Please Download @ https://globalplatform.org/specs-library/?filter-committee=sesip

Why Certify?

Regulatory Requirements

Regulatory Compliance

- Structured evidence demonstrates real product achievements

Supply Chain Management

- Simplifies procurement with transparency on security characteristics and interoperability functionality
- Streamlines collaboration through reusable 3rd party certifications

Supports Risk Management

Structured approach to evaluating supplier security capabilities

Brand Protection:

Prevents costly and damaging security incidents

Checks & Balances in SESIP Certification using Standard SESIP Profiles

Vendor

- Definition of Security Target & Target of Evaluation
- Selection of Protection Profiles (with pre-defined Assurance Level or identification of desired assurance level)

SESIP Lab

- Confirmation of Appropriateness of Scope and Protection Profile (based upon context (i.e. implementation in product))
- Develop Test Plan
- Run Tests

SESIP Certification Body

- Confirmation of Appropriateness of Test Plan (based upon recent developments in threats and for objective)
- Confirmation of Test Results
- Issuing Certificate

Attack Working Groups

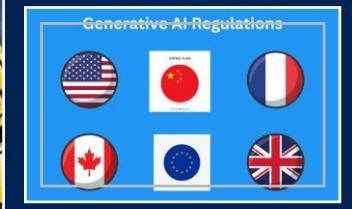
- Up-to-Date Attack Knowledge Working for all protection profiles
- International Working Groups
  - Attack Subgroup from the EU Senior Officials Group Information Systems Security (JHAS SOG-IS)
- GlobalPlatform
  - Working for all protection profiles

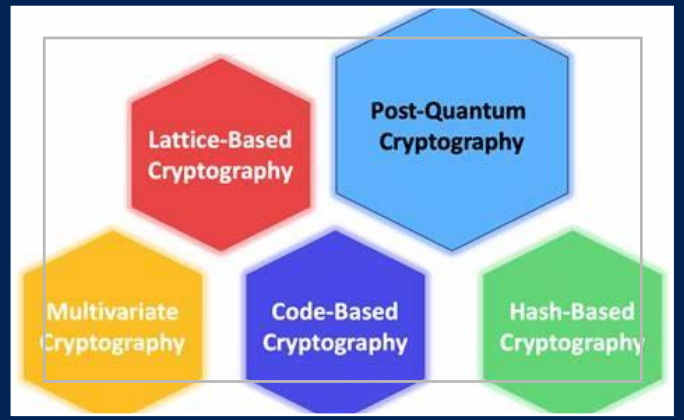
Global Platform™

Secure Elements: Topics of Interest in Automotive

Gil Bernabeu, CTO

Context of the high security uses cases





Benefits of embedded Secure Elements in Automotive

a **secure execution environment**

- **Tamper resistant**(1)
- **Execution of State of the art crypto service** and **business logic**
- **Separated resources**
- **Primary Root Of Trust**

standardized, proven, mass-produced

- Standardized **protocols & mechanisms**
- **interoperable**(2) **& upgradable** applications
- Well-defined **certification schemes with high assurance** (EAL4+)

with interesting **complementary properties**

- **Agile**
- **Remotely updatable**
- **Low consumption**
- **More than 1Mbytes available**
- **Good performances** boot time / crypto operations

Use cases with embedded Secure Elements in Automotive

Key management life cycle

- Personalize eSE during its production
- Ease transition phases from development to production
- Allow secure key provisioning at Tier1 manufacturing and OEM assembly line

Business logic control

- Business logic implemented eSE
- Enforce control of key and crypto engine usage

Crypto agility

- Provide secure key provisioning on-field, at repair
- Tackle circular economy
- Support OS and Applet upgrade
- Ensure PQC readiness

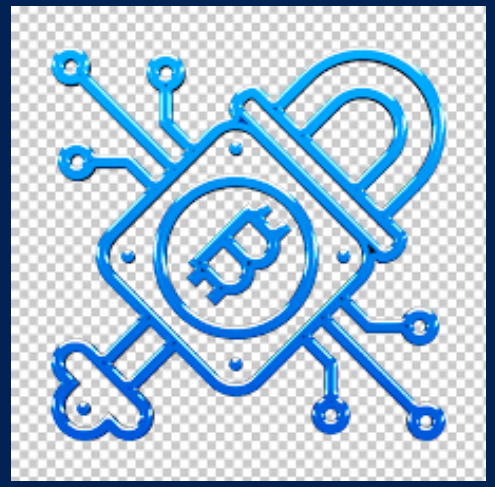
Leverage Digital Car Key SE and eSIM deployment to support new use cases

Many cars are already equipped at least with on eSE for DigitalKey, or eSIM for connectivity and most the SE could propose additional room for complementary use cases:

Qi	Car BlackBox	Specific parts serial number check
Specifics car settings check	Driver Biometrics credentials management • Privacy regulation	Car driver preference settings record • User applicative and dynamic rights management

Leveraging investments to deliver higher cybersecurity robustness for identified use cases

USECASE	HSM ROLE	eSE ROLE
Secure binding between MCU and eSE	• Secure storage of SCP[1] Key / MCU side [1] Secure Channel Protocol (e.g. SCP03)	• Secure storage of SCP[1] Key / eSE side • Secure Channel Protocol implementation
Secure Boot of MCU	• Before releasing from reset, CMAC signature verification of immutable boot area • Hash computation	• Asymmetric signature verification of updatable area(s) against pre-defined Root Of Trust
MACSec between 2 ECUs	• GMAC computation/verification using Secure Association Key	• CAK[1] provisioning/learning • MACSec key agreement and SAK[2] creation [1] Connectivity Association Key [2] Secure Association Key
Vehicle to Cloud mTLS	• Not supported	• Manage critical steps during mTLS handshake
Digital Key (DK)	• Not relevant in DK protocol • Secure transfer of UWB keys to UWB sub-system	• Digital Key storage • Implementation of the CCC protocol between vehicle and device



Today's Autosar Crypto Service Manager Implementations

- Lack of clarity on how/where crypto services are implemented
- HW Crypto Capabilities and associated interfaces are chipset specific
- HSM FirmWare (when relevant) capabilities and API are vendor specific.
- Unknown resistance to hardware attacks
- Lack of agility for extending capabilities post deployment
- High impact on resources (incl. non-recurring engineering) to address needed changes
- Fixed and limited cryptographic algorithms
- Capability to address post-deployment vulnerabilities is not foreseen

Use cases with embedded Secure Elements in Automotive

Automotive ECUs are more and more challenged to address risks with higher level of security robustness sometimes with

- unclear visibility about the strategy to setup and
- how to maintain it “state of the art” over more than a decade

ECUs can rely on AUTOSAR CSM APIs to answer many cybersecurity challenges

- Higher level of security (>SESIP 3 or EAL4+/5+) is sometimes required

- eSE must be understood as a **complementary solution on top of ECU HSM used in AUTOSAR with CSM APIs**
- Any customer who wants to keep going using AUTOSAR for practical and legacy reason and just delegate specific tasks to eSE as a companion chip.
- eSE standardized APIs is likely to address generic services :

Key management

Secure Storage

Certificates management

Complementary crypto services (if some could miss, or if some could require higher security)

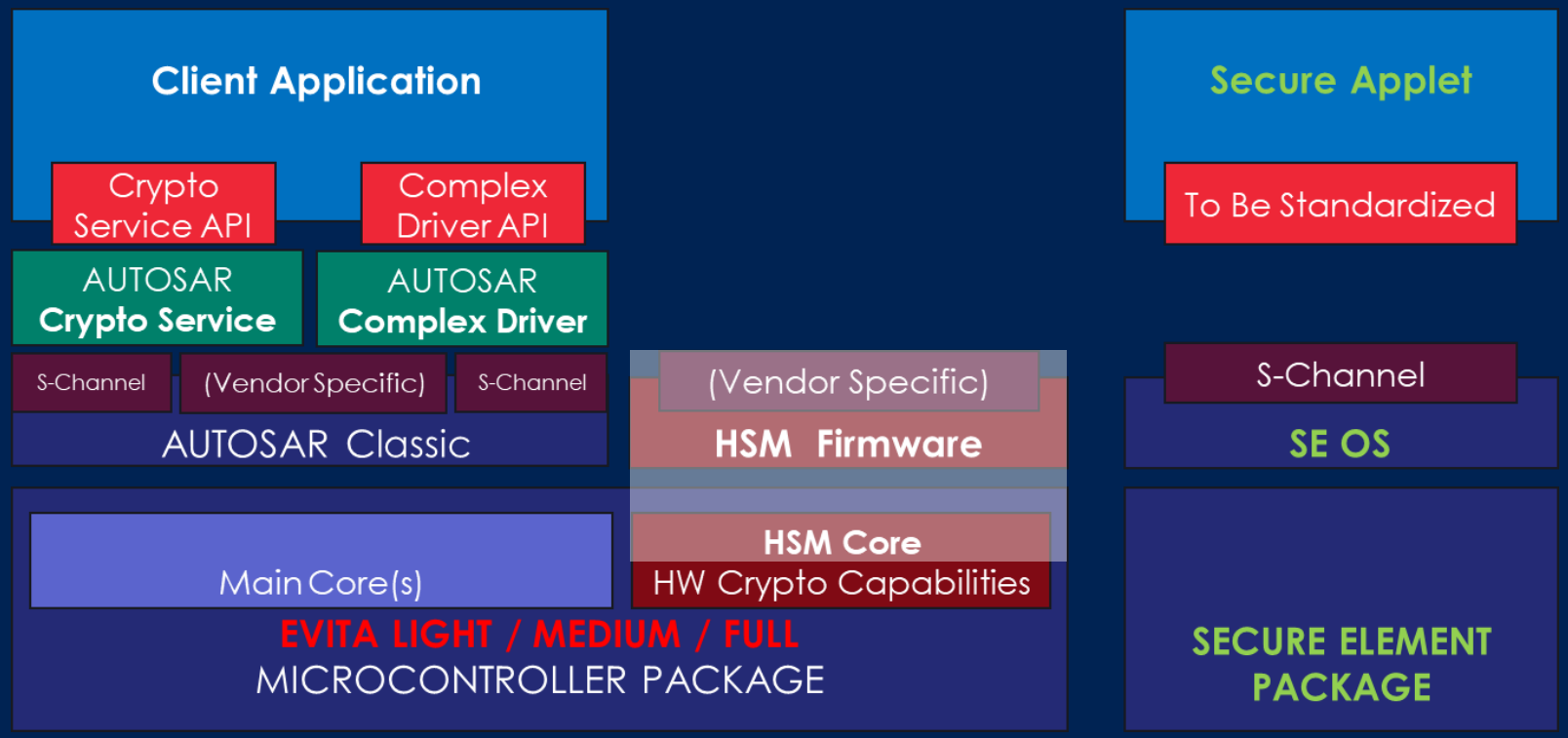
Remote provisioning

Possible ROT improvement scheme

Capability to maintain state of the art security robustness on the field

Migration towards SDV

GlobalPlatform is working on leveraging Secure Elements to extend proprietary HSM within the AUTOSAR framework



HSM

- Legacy implementation
- Access to internal resources

eSE

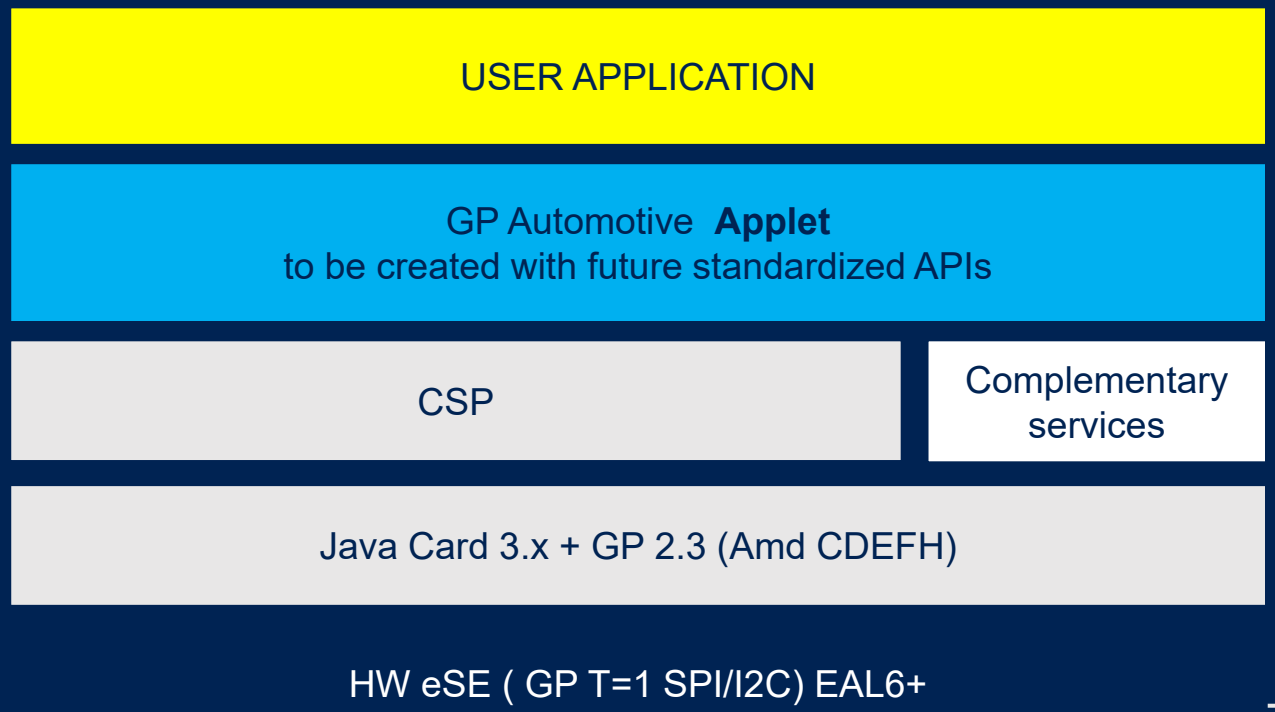
- Tamper resistance
- Certification
- Advanced crypto algorithms
  Diffie Hellman, miscellaneous ECC curves, etc.
- Crypto agility.
  Upgradable, PQC readiness
- Key Management Life Cycle
- Business logic

Leverage Capabilities of both HSM and Secure Element.

Crypto services always running in secure environment (HSM or SE)

USECASE	HSM ROLE	eSE ROLE
Secure binding between MCU and eSE	• Secure storage of SCP[1] Key / MCU side [1] Secure Channel Protocol (e.g. SCP03)	• Secure storage of SCP[1] Key / eSE side • Secure Channel Protocol implementation
Secure Boot of MCU	• Before releasing from reset, CMAC signature verification of immutable boot area • Hash computation	• Asymmetric signature verification of updatable area(s) against pre-defined Root Of Trust
MACSec between 2 ECUs	• GMAC computation/verification using Secure Association Key	• CAK[1] provisioning/learning • MACSec key agreement and SAK[2] creation [1] Connectivity Association Key [2] Secure Association Key
Vehicle to Cloud mTLS	• Not supported	• Manage critical steps during mTLS handshake
Digital Key (DK)	• Not relevant in DK protocol • Secure transfer of UWB keys to UWB sub-system	• Digital Key storage • Implementation of the CCC protocol between vehicle and device

Opportunity for Standardized APIs, interoperability testing and security certification?



Global Platform™

Wrap-Up

Francesca Forestieri

Topics Discussed in GlobalPlatform

Automotive & Cybersecurity Vehicle Forums

Join Us: Cooperation for Security Specifications

Standardise minimum common interoperable security services that allow service providers to develop applications for SDVs

Determine how product certification can provide evidence for the CSMS (UNECE 155/156) process

Global Platform™

If you are interested in joining in on the fun…

https://www.cartoonstock.com/cartoon?searchID=EC326385

Automotive Lead

Francesca Forestieri,
Based in Italy

GlobalPlatform China

Harry Wang,
Based in Shanghai

Global Platform™

The standard for secure digital services and devices

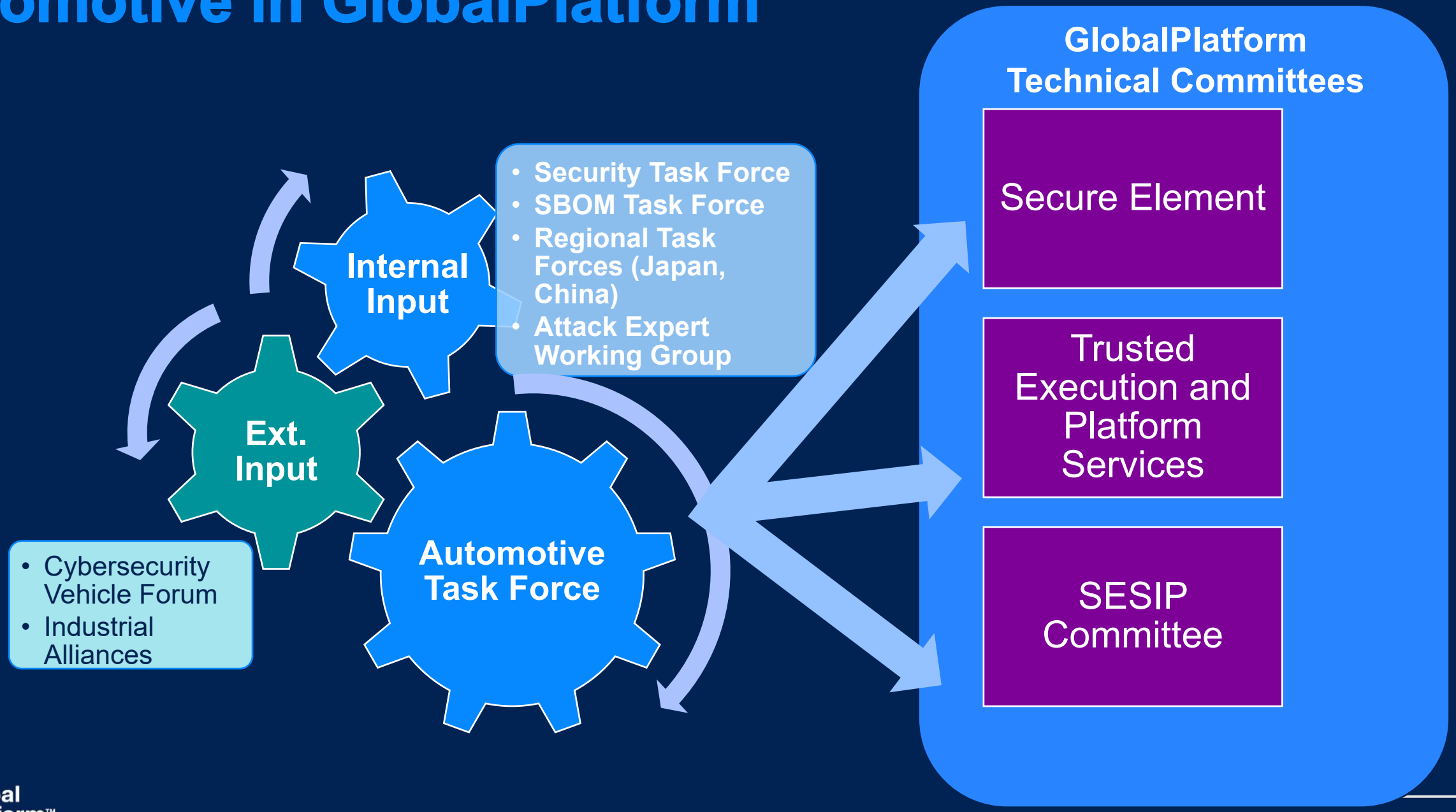
→globalplatform.org

Global Platform™

The standard for secure digital services and devices

→globalplatform.org

Automotive in GlobalPlatform



J3101-1: Hardware Protected Security Environments (HPSEs) for Ground Vehicles

Goal:

Provide a common glossary for describing security mechanisms (i.e. hardware root of trust and the hardware-based security primitives) supported in hardware for automotive use cases, along with best practices for using such mechanisms.

Additional Complementary Standardization Around Hardware Protected

Latest WIPs *4 WIPs*

J3101-5
Hardware Protected Security Environment - GlobalPlatform Technologies Information Report

J3101-2
In this report we aim to complete HPSE trusted applications threat analysis to determine effectiveness of isolation security models and recommend HPSE Isolation building blocks.

J3101-4
An information report on side channel attacks

J3101-3_202407
Hardware Protected Security Environment Management of Confidential Data
Issued

J3101-1_202407
Hardware Protected Security Environment - Application Programming Interface Analysis - Information Report
Issued

13

Global Platform™

You are in the right place for the:

Cybersecurity Vehicle Forum – Shanghai

We are on Break and will return @

SESIP Certification Benefits: OEMs

Enhances trust in vehicle cybersecurity for customers and regulators.

Transparency on security targets achieved

Simplifies Verification and Validation Phase

- given composite certification for chips? ECUs? components? etc.

Consistency Across Security Claims

SESIP: Business Benefits

Faster Development:

- Pre-certified components speed time-to-market
- Avoid redundant security evaluations across vehicle models

Cost Efficiency:

- Test once, use across multiple vehicle platforms

Competitive Edge:

- Demonstrates security commitment to customers

Future-Proof:

- Structured approach to managing security updates

SESIP: Implementation Path for OEMs

Security Target Definitions: Best Practices

Be Specific:

- Include implementation details for each security feature

Ensure Traceability:

- Clear links between threats, objectives, and requirements

Balance Detail:

- Technical enough for evaluators, clear enough for stakeholders

Address Standards:

- Include relevant Protection Profile conformance

The Security Target is your security blueprint—comprehensive enough to guide evaluation while precisely defining what security claims you're making about your product."

Protection Profiles in SESIP: Industry-Standard Security Templates

Protection Profiles (PPs) define **consensus-based security expectations** for **specific product categories**, creating:

- a common foundation for security evaluation.

Protection Profiles transform SESIP certification:

- from a custom evaluation process into a **standardized framework** that balances security rigor with evaluation efficiency, creating:
  - recognizable security benchmarks for IoT and embedded systems across industries.

SAE J3101: Application-Level Protection Profile

Scope

Clearly define :

- scope of the protection profile to cover application-specific requirements

Ensure the profile addresses both:

- mandatory and
- optional application-layer requirements

Challenges

- Application nature (boundaries, granularity, …)
- Lifecycle management
- Composition
- Self test vs Crypto validation

Reference Parameters

- Intent and range of variables (minutes vs. years)
- Utility of defining specific testability requirements for key elements
- Industry Expectations / Annex of Current Best Practice

GlobalPlatform Automotive Topics Under Exploration

Guidelines

- SESIP to Generate Artefacts for UNECE 155
- Secure Boot
- Supporting HPC ADAS functionality
- Virtualisation of multiple TEEs
- Isolation: Work Items in RISCV
- Applicability of SAE's Hardware Protected Security Environments to Other Regions
- PQC migration across regions

Technical Requirements

- Embedded Se as an Extension to HSM
- Managing Mixed Criticalities for Safety
- Standardisation of TEE Non-Security Attributes (e.g. performance, profile, memory usage, start up time, etc.)