Global Platform™

Cybersecurity Vehicle Forum Berlin

4 December 2024

Richard Hayton, Chair of Automotive Task Force, Trustonic
Francesca Forestieri, Automotive Lead

Ground Rules for Cybersecurity Vehicle Forum

We aim to create a trusted environment to understand and resolve complex problems and identify future potential synergies.

We have representatives from key players and from key standardisation organisations.

Each speaker is speaking as an expert in the field, and not necessarily speaking on behalf of his company or standards organisation.

Therefore, participants are free to use the information received, but not attribute the affiliation of the speaker(s).

After the Cybersecurity Vehicle Forum, we will post the recording on our website, as well as the relevant slides (as made available by speakers) for your reference.

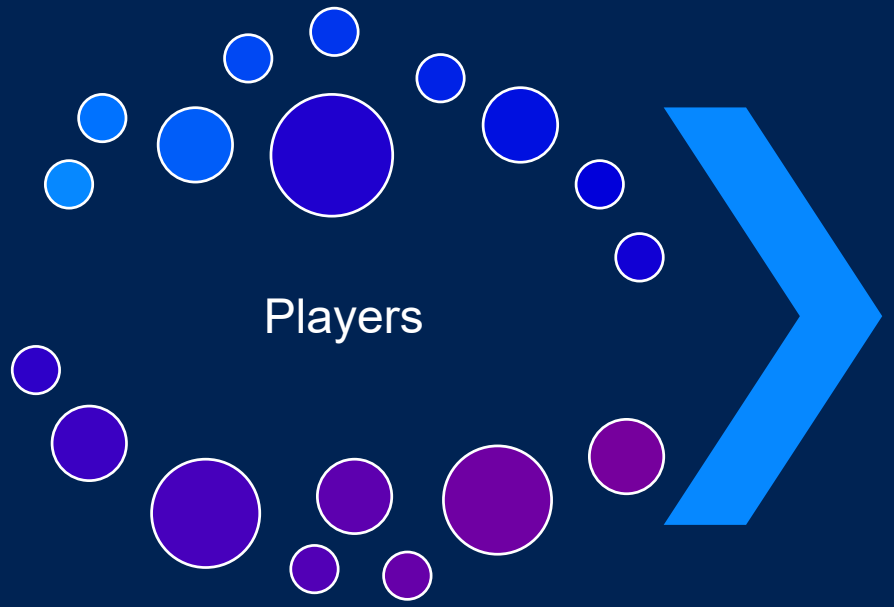
https://globalplatform.org/blog-overview/

Global Platform™

Welcome to GlobalPlatform's Cybersecurity Vehicle Forum in Berlin

Cybersecurity Vehicle Forum

What is the Cybersecurity Vehicle Forum?



Relevant Security Technologies

GlobalPlatform's Cybersecurity Vehicle Forum

- Trusted Service Experts
- Automotive Value Chain
- Governments
- Development Partnerships
- Trade Associations

- Hardware Protected Secure Environments
- Security APIs
- Security Lifecycle Management
- SESIP Security Evaluation Methodology

Objective: To Identify Outstanding Automotive Requirements and Use Cases where cross-industry work on security standardisation would aid deployment

Driving Requirements into GlobalPlatform

Cybersecurity Vehicle Forum

Nov 2022 Munich
June 2023 Detroit
Sept 2023 Tokyo
Oct 2023 Beijing
Nov 2023 Hamburg
June 2024 Detroit
Oct 2024 Tokyo
Nov 2024 Berlin

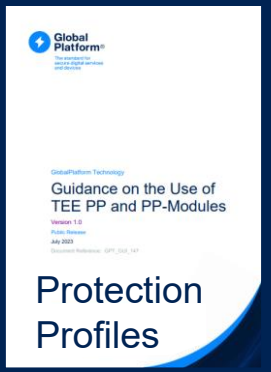
Inside GlobalPlatform

- Automotive Task Force
- Security Task Force
- Regional Task Forces

- Trusted Environments & Services Committee
- Secure Element Committee
- SESIP Committee

Whitepapers

Specifications



Protection Profiles

CSVF Berlin Dec 4th Registered Participants

Automakers and Automotive Technology

- Jaguar Land Rover
- Mercedes-Benz AG
- Toyota Motor Europe
- Stellantis
- KTM AG
- Panasonic Automotive
- ZF Automotive UK Limited
- DENSO
- MHP Management- und IT-Beratung GmbH *(Subsidiary of Porsche)*
- AMPERE
- ETAS (Bosch)
- Woven

Semiconductor and Electronics

- ARM
- Infineon
- NXP Semiconductors
- Oracle
- Renesas Electronics
- STMicroelectronics
- Giesecke & Devrient
- Thales

Trusted Execution Environment (TEE) Suppliers

- Trustonic
- ProvenRun

Cybersecurity Solutions and Consulting

- Auxilium Pentest Labs
- PQShield
- Intrinsic ID
- Kali Security Partners
- **Technology Consulting and Innovation**
- Capgemini
- Technology Innovation Institute
- High North Inc
- Mimer Information Technology AB
- Entrust
- HERE Technologies
- Eaton

Certification and Standards

- Dekra
- DEKRA Certification GmbH
- VDA
- GlobalPlatform

In-person	**17**
Virtual	**39**
TOTAL	**56**

Agenda

09:30	**Meet and Greet**		
10:00	Welcome, GlobalPlatform & Automotive		Francesca Forestieri, GlobalPlatform
	SESIP For Automotive		
10:30	SESIP Evaluation Methodology: a Tool for Automotive?		Jorge Ruiz Wallace, Dekra
10:50	Fireside Chat (Moderated by Francesca Forestieri)	What are the curent challenges of ISO 21434 without product security targets & certification?	Jorge Ruiz Wallace, Dekra
		Can Composite Certification support Type Approval Process?	Bill Mazarra,Stellantis
11:30	**Developments with Regulations and Standards**		
11:30	Update on PQC for Secure Elements		Sebastian Hans, Oracle
11:50	**Lunch**		
13:00	PQC: practical issues that will impact the future of hardware protected security environments		Mike Ounsworth, Entrust
13:20	Evolution of ISO/SAE 21434 and progress on CAL/TAF		John Krzeszewski, Eaton
13:40	Updates on Evolution of Functional Safety of ISO 26262		David Ward, Horiba-Mira
13:40	**SDV: The Intersection of Safety with Security Isolation**		
14:00	OEM Use Case on fusion & Managing Mixed Criticalities		Redouane SOUM, AMPERE
14:30	Different Strategies for Managing Mixed Criticalities: Standardisation Useful?		Richard Hayton, Trustonic
14:50	Panel Topics	What is the role of standards for security isolation within a SDV?	David Ward, Horiba-Mira
		Mixed Criticality in software? Is it practical to run safety critical or real time services that share CPUs with other guests.	Andrew Jones, AVCC
			Richard Hayton, Trustonic
			SOUM Redouane, AMPERE
15:20	**Evolution of Secure Silicon**		
15:20	**Secure Boot**		Philip Lapczynski, Renesas
15:40	**Coffee Break**		
16:00	Extension of HSM Capabilities with Secure Elements		Yves Le Bobinnec, Thales
16:20	Potential Roadmap Moving Forward		Laurent Tabaries, STM
16:40	Evolving Industry Requirements for Security		Craig Rawlings, Stellantis
17:00	Panel Topics	Opportunity for Secure Elements for HSM 2.0?	Craig Rawlings, Stellantis
			Riemenschneider Lukas (ETAS-SEC/XPC-Bo2)
		Does safety critical mean silicon?	Laurence Bringer, Thales
			Laurent Tabaries, STM
17:30	**Closing**		Richard Hayton, Trustonic

Global Platform™

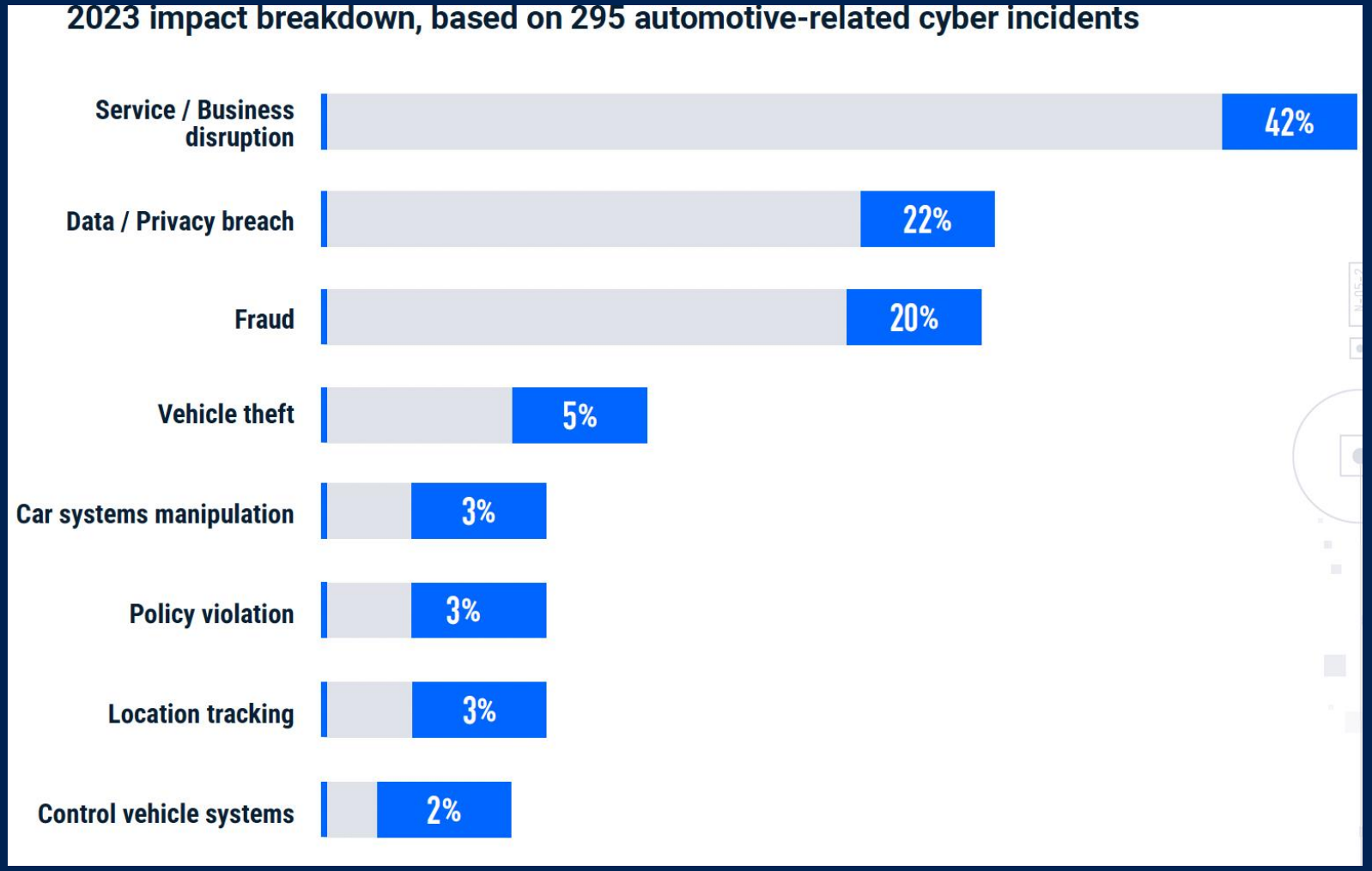
Cybersecurity 2024

Cybersecurity Vehicle Forum

Cybersecurity: The Perfect Storm

- International Cybersecurity Regulations for Automotive
- National Cybersecurity Regulations
- Evolution of Connected Cars
- Increase in Attack Surfaces
- Increase in Attacker Types

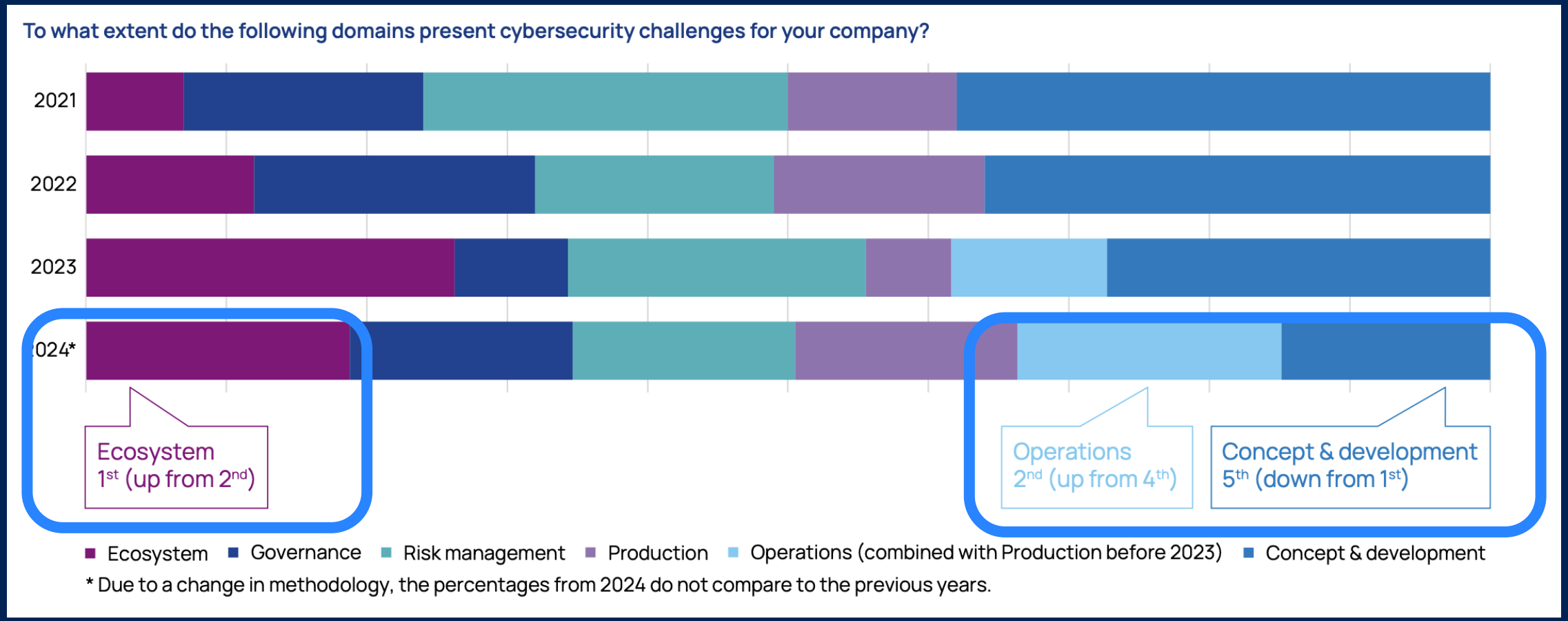
What Are the Consequences of Cyber Incidents?



- 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

Today's Cybersecurity Challenges

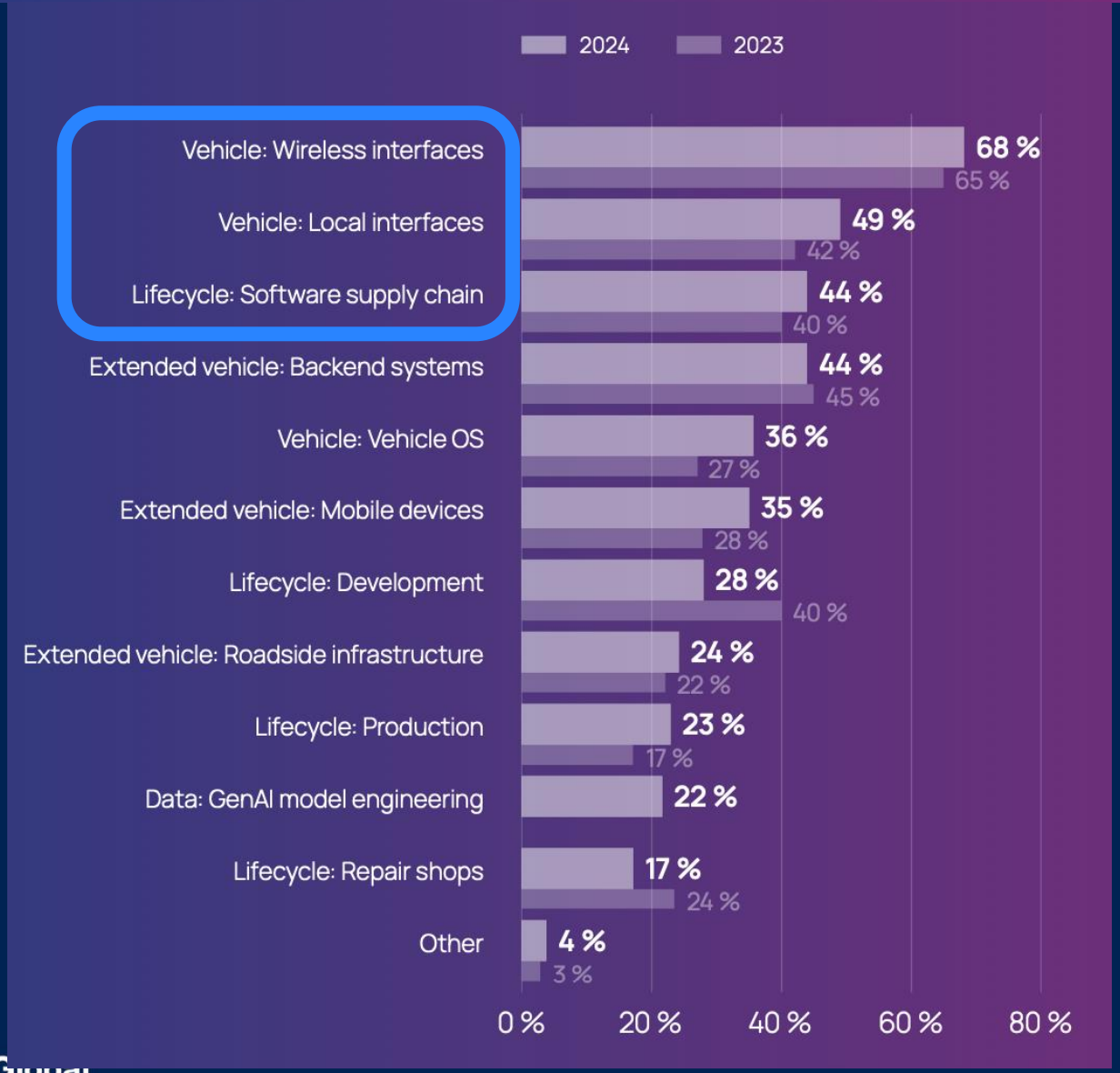


https://www.etas.com/download-center-files/DLC_products_ESCRYPT/etas-automotive-cyber-maturity-report-2024-en-20240719.pdf

Cybersecurity Challenges 2024

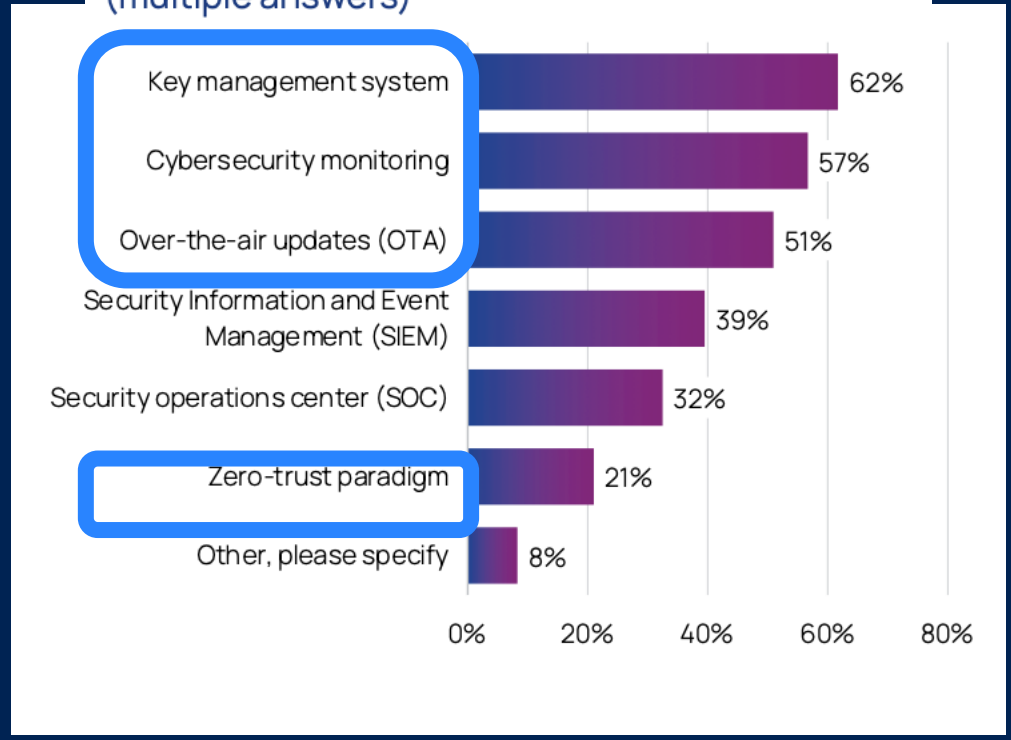
14. What attack vectors on vehicles are you most concerned about?

(multiple answers)



15. What measures does your company take to secure its product's ecosystem?

(multiple answers)



https://www.etas.com/download-center-files/DLC_products_ESCRYPT/etas-automotive-cyber-maturity-report-2024-en-20240719.pdf

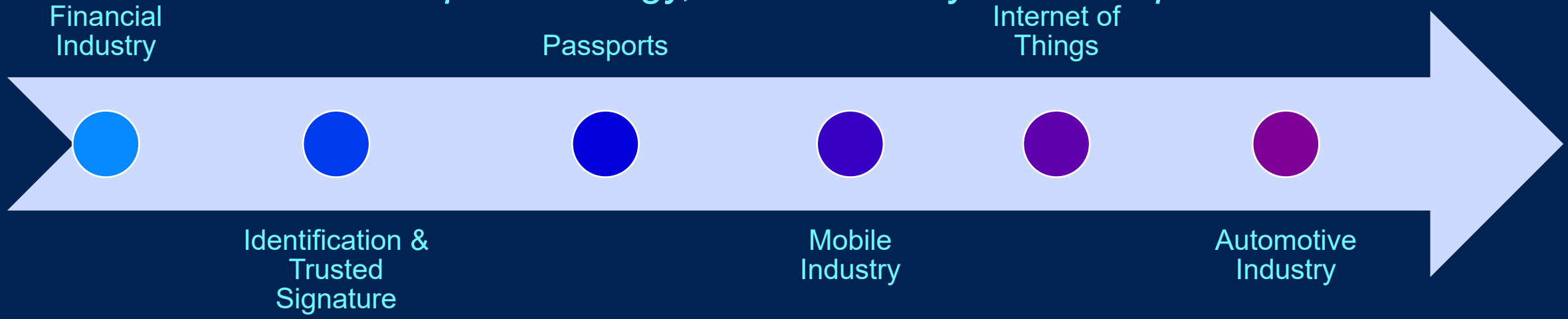
Global Platform™

https://www.darkreading.com/endpoint-security/cartoon-connected-car-security

Relevance of GlobalPlatform

GlobalPlatform

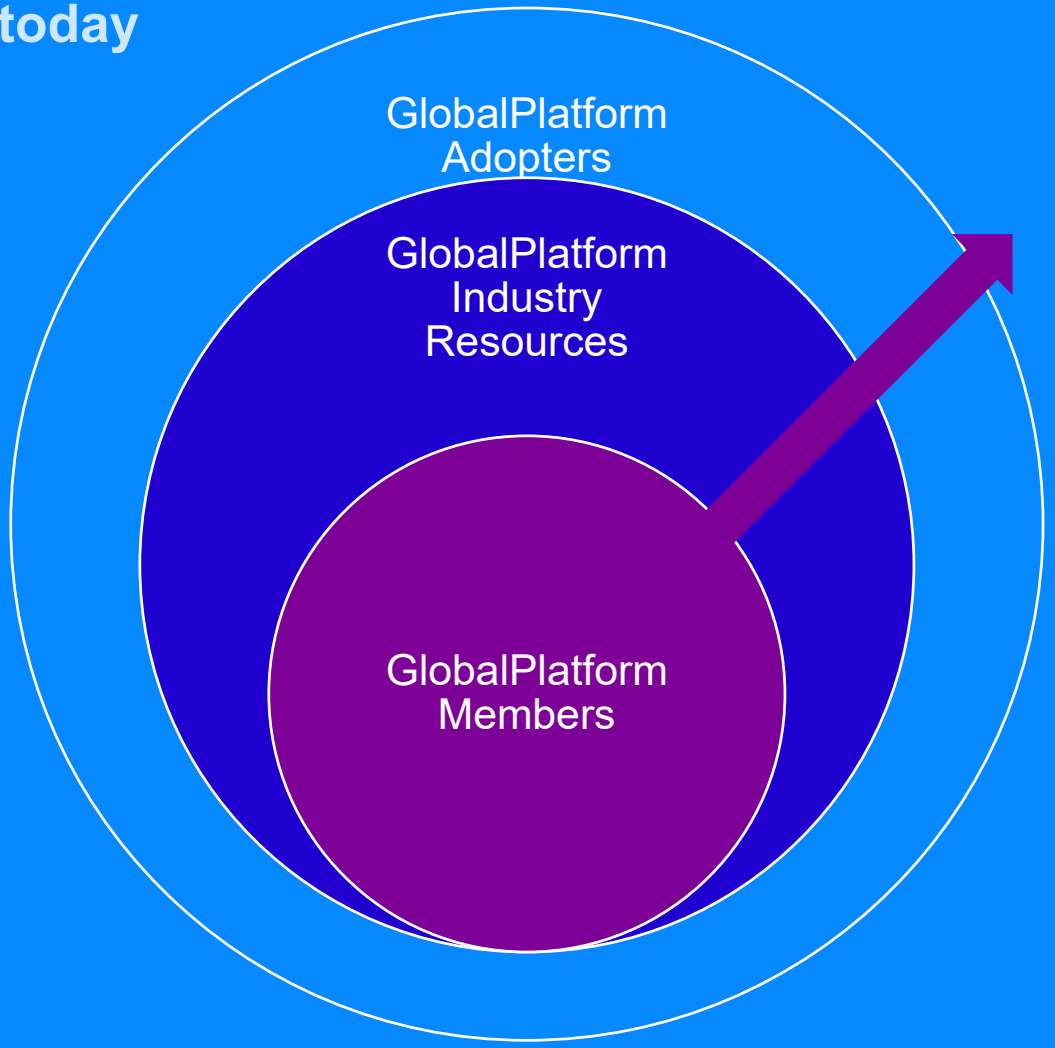
THE standard for managing applications on secure chip technology, with over 20 years of experience

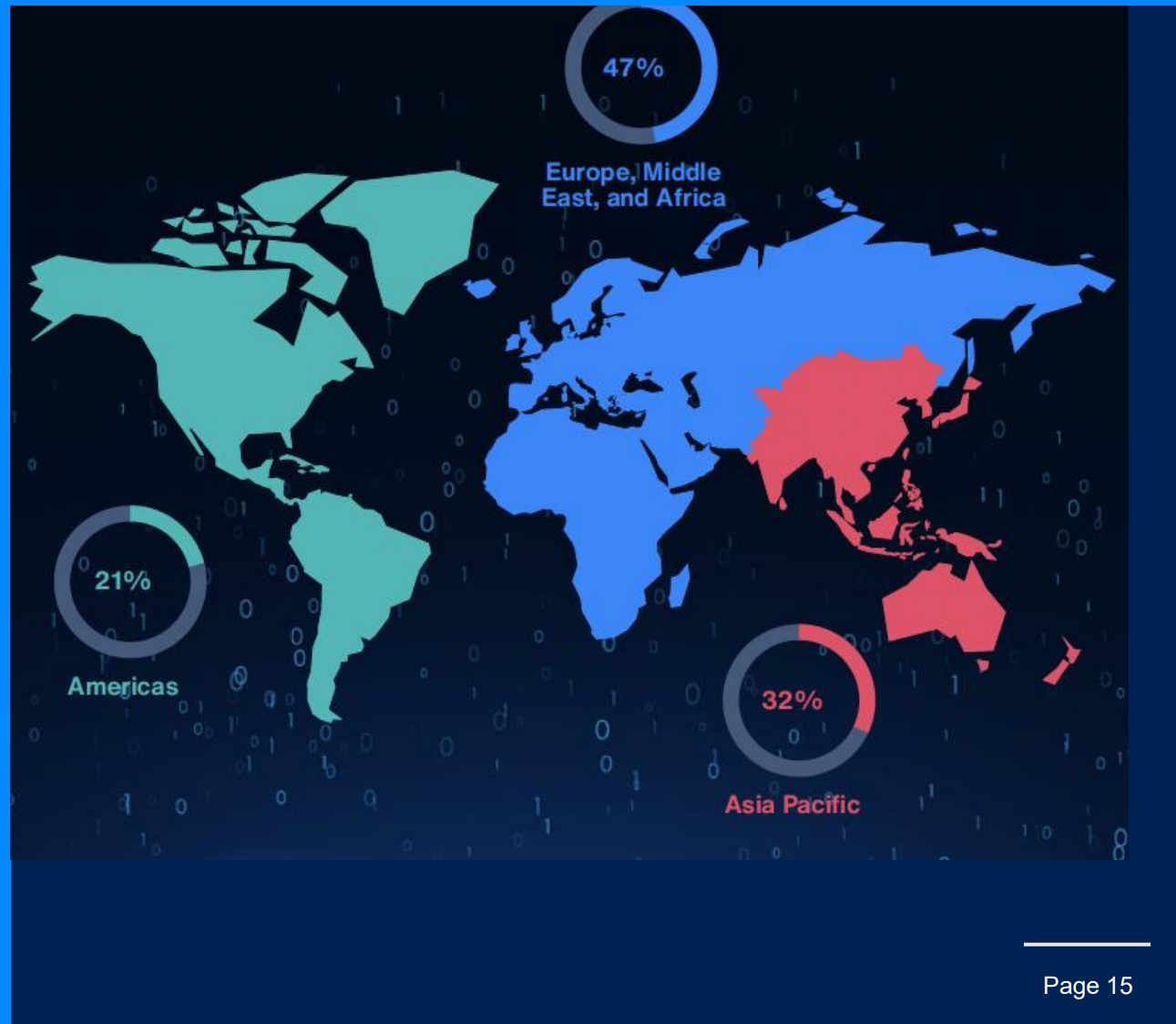


Mass Market deployment of industries has required: agreed functionality for transactions and transparent robust security to create trust among competitors and in the overall ecosystem

GlobalPlatform's Market Adoption

- 62 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's Success in International Digital Security Services

Publicly available on a royalty free basis

Protection Profiles

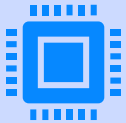
- Common set of security needs
- "I want" this level of security

3rd Party Certification

- A mechanism to provide Vendors the ability to make claims regarding their security products
- I "Provide"

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

GlobalPlatform Members



Solution Providers

Semiconductors and System on Chip (SoC) Providers
Identity Solutions and Smart Cards
Security Firmware
IP Providers for Silicon
Security Software

Labs/ Research Institutes

Industries

Software and Services
Government and Defence
Payments and Financial Services
Consumer Electronics and Devices
Automotive
Telecommunications

Our Members

Full

ANALOG DEVICES — AHEAD OF WHAT'S POSSIBLE™
arm
Bundesamt für Sicherheit in der Informationstechnik
BCTC 银行卡检测中心 BANK CARD TEST CENTER
T··
ERICSSON
fime
Google
galitt — a Sopra Steria company
G+D Mobile Security
HID
HUAWEI
IDEMIA — augmented identity
infineon
mastercard
NTT
NXP
ORACLE
Qualcomm
SAMSUNG
life.augmented
T-Mobile
THALES
TRUSTONIC
verizon
VISA
winbond

Participant

Applus+
COMPRION — Test it. Prove it. Move it.
DEKRA
DNP
OPUS Lab
HONOR
財團法人資訊工業策進會 INSTITUTE FOR INFORMATION INDUSTRY
orange
riscure — Challenge your security
SERMA — SAFETY & SECURITY
SGS brightsight
Quarkslab
TRUSTCB — TRUST AND VERIFY
UL Valid
woven by TOYOTA

Observer, Public Entity and Consultants

AMEX
AT&T
bdr BUNDESDRUCKEREI
CARIAD
cea leti
CB
cisco
楚天龙 CHUTIAN DRAGON 龙行天下 品赢未来
DEPARTMENT OF DEFENSE
DISCOVER
eTAS
东信和平 EASTCOMPEACE
FEITIAN — WE BUILD SECURITY
intel
JCB
kaspersky
Kigen
kona i
MASKTECH
MK smart — Smart Digital Security
PQSHIELD
Rambus
SAMSUNG
SAMSUNG SDS
上海复旦微电子集团股份有限公司 Shanghai Fudan Microelectronics Group Company Limited
SK
SPREADTRUM
synapse mobile networks
TELUS
TOSHIBA
UBIVELOX
UNISOC
xardpay
XCURE CORP.
mi
RENESAS — BIG IDEAS FOR EVERY SPACE
BACTECH
Digital Cubes
INTERNET OF TRUST
MoneTECH
NEXTENDIS — INNOVATION CONSULTANCY
SAFEPAY
zwipe

Collaborative Partnerships: Underpinning Deployment

Standards Bodies

International Standards and Certification Bodies:

- ISO, ETSI, SAE International, GCF, PTCRB, TAF, FIRA, W3C, EMVCo

National Standards and Certification Bodies:

- NIST (USA), ANSSI (France), NICSS (Japan)

Associations for Solution Adoption

Smart Cards:

- Java Card Forum, APSCA, Smart Ticketing Alliance

Identity:

- Secure Identity Alliance, OSIA, NFC Forum

Security:

- FIDO Alliance, CCDS, ioXt, Trusted Computing Group, Trusted Connectivity Alliance, RISC-V

Technology and Computing Platforms:

- RISC-V, Trusted Platform

Vertical Industry Associations

Financial and Payment Services:

- IFAA, Mobey Forum, EMVCo, IFAM

Telecommunications:

- GSMA, PTCRB, GCF

IoT:

- IoT Connectivity Alliance, Industrial Internet Consortium, oneM2M, OMA SpecWorks, Wireless Power Consortium

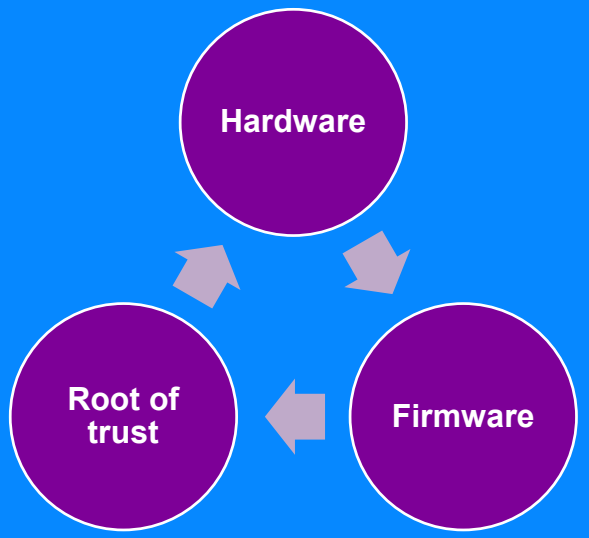
Automotive and Transportation:

- Auto-ISAC, AUTOSAR, Car Connectivity Consortium, SAE International

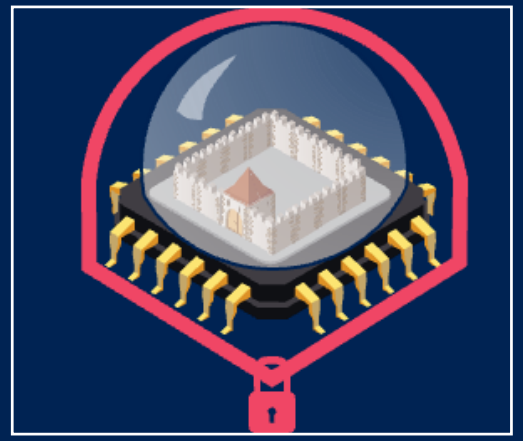
Industry-Specific Alliances and Forums:

- Eurosmart, ACN, Secure Technology Alliance

GlobalPlatform Foundation Technologies



Secure Element

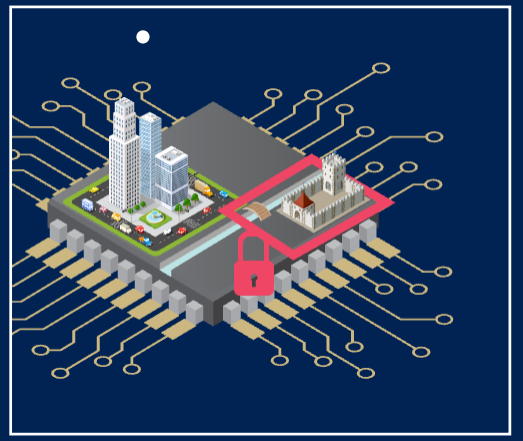


A secure enclave protected against physical and software attack

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

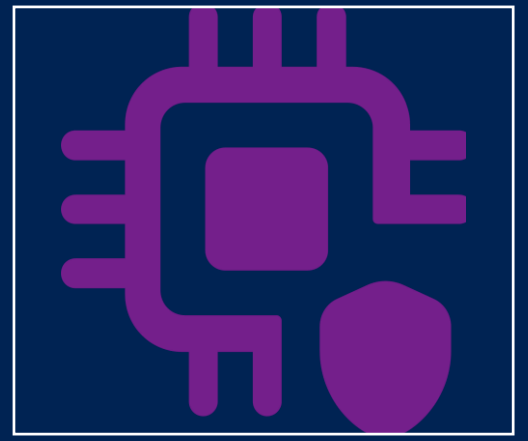
https://www.juniperresearch.com/press/connected-vehicles-to-surpass-367-million-globally#:~:text=Hampshire%2C%20UK%20–%209th%20January%202023,from%20192%20million%20in%202023

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

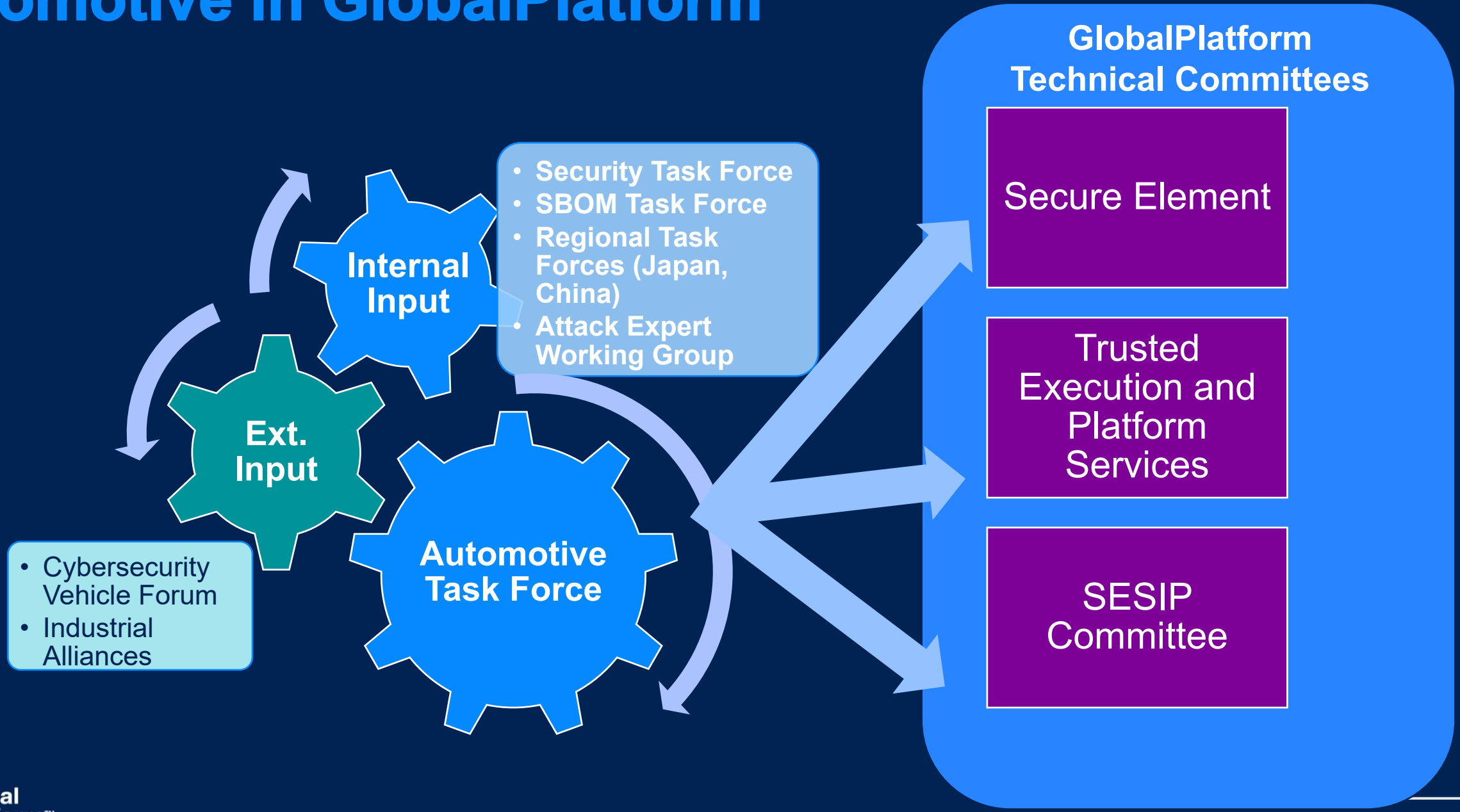


New Technologies that create isolated execution environments

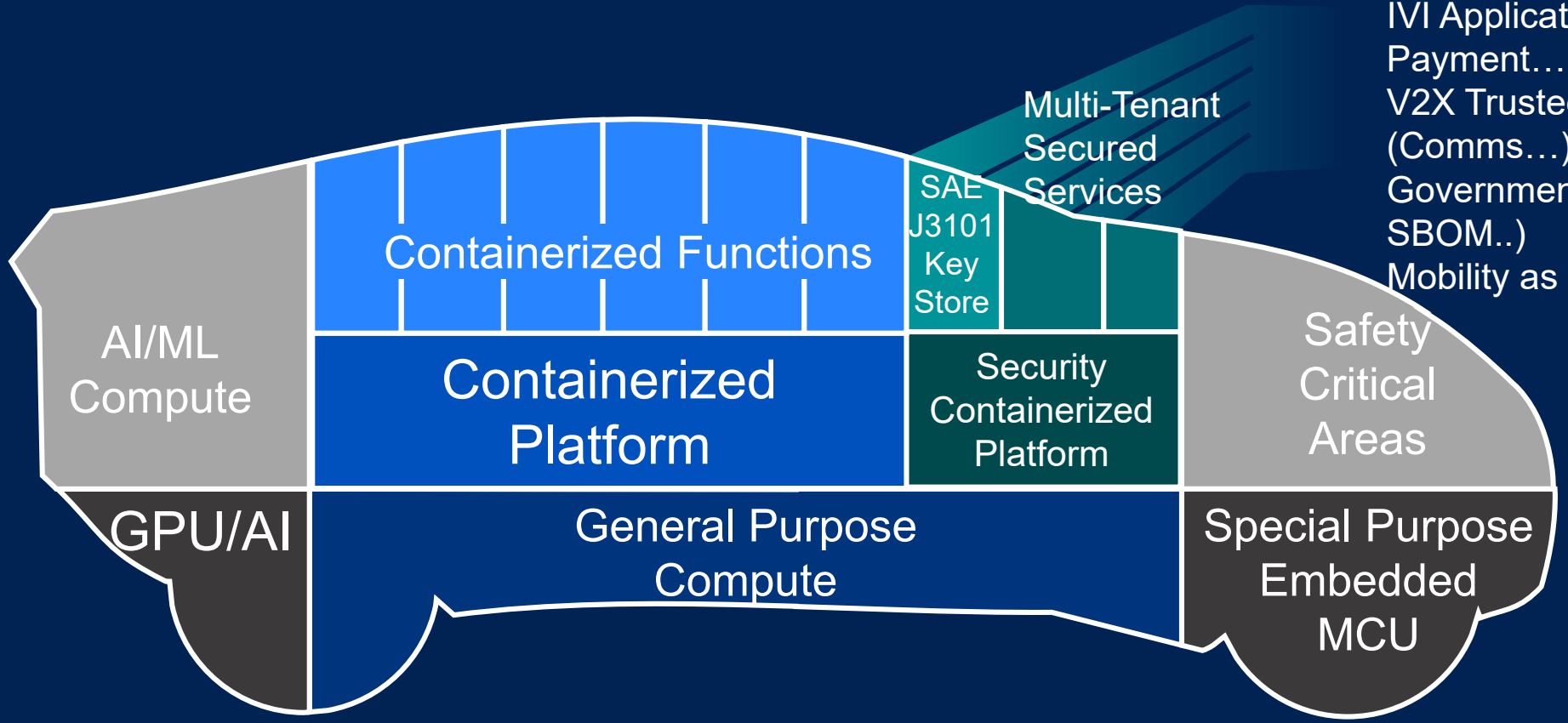
- Runs a full operating system providing standardized APIs and functions
- 3rd party Security Certification
- Full support for App and OS update over-the-air

Global Platform™

Automotive in GlobalPlatform



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

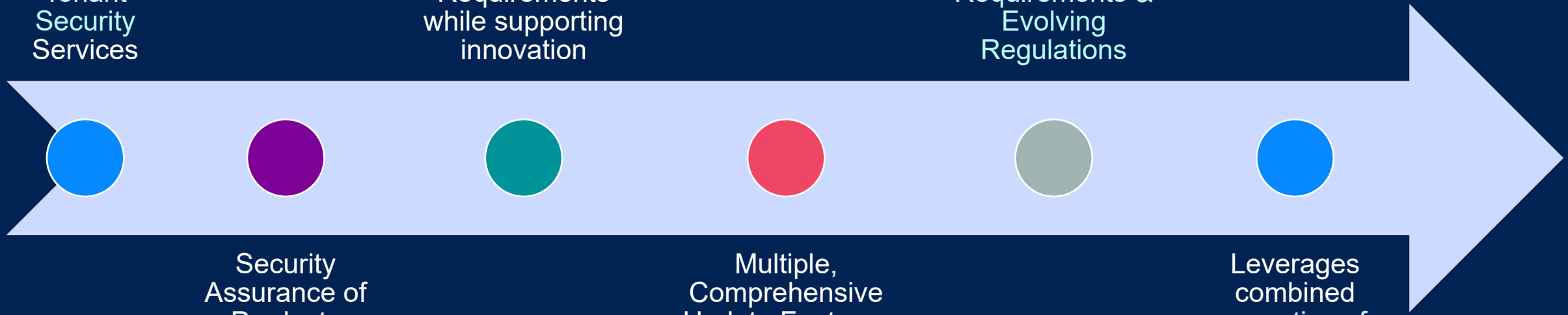
1. Platform: Standardized APIs & Management command, update, state-of-the-art crypto, crypto agility …

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



Global Platform™

Standards Alignment in Automotive

How UNECE 155 Compliance Possible with Process and Product Security

Relevant for 64 Countries

Process

ISO /SAE 21434 and 24089

+

Product

SAE J3101 Hardware Protected Security Environments

=

Compliance

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)

SAE J3101
Hardware Protected Security Environments

Automotive computer systems are required to establish trustworthiness through device identity, sealing, attestation, data integrity, and availability.

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

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.

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).

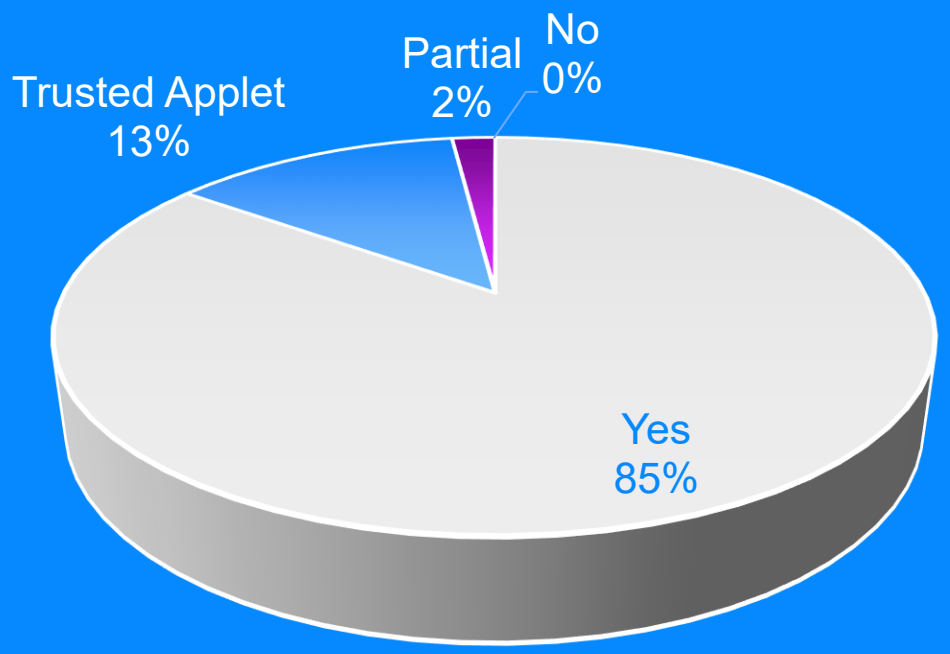
Source: SAE, Surface Vehicle Recommended Practice, *Hardware Protected Security for Ground Vehicles* J3101™ FEB2020, Issued 2020-02

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/

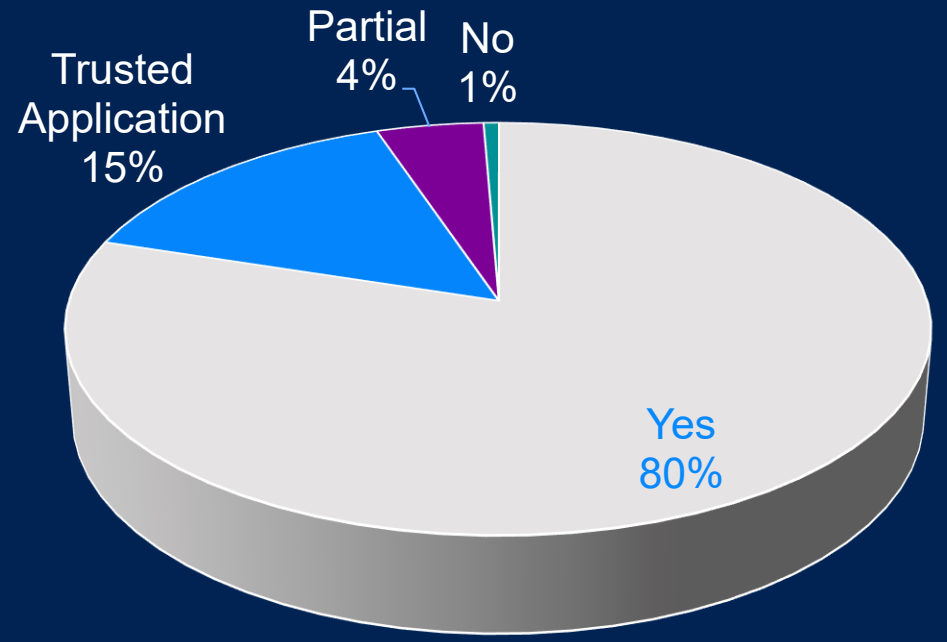
Analysis Results: GlobalPlatform Specifications

Secure Elements Fully Meet 98% J3101 Requirements

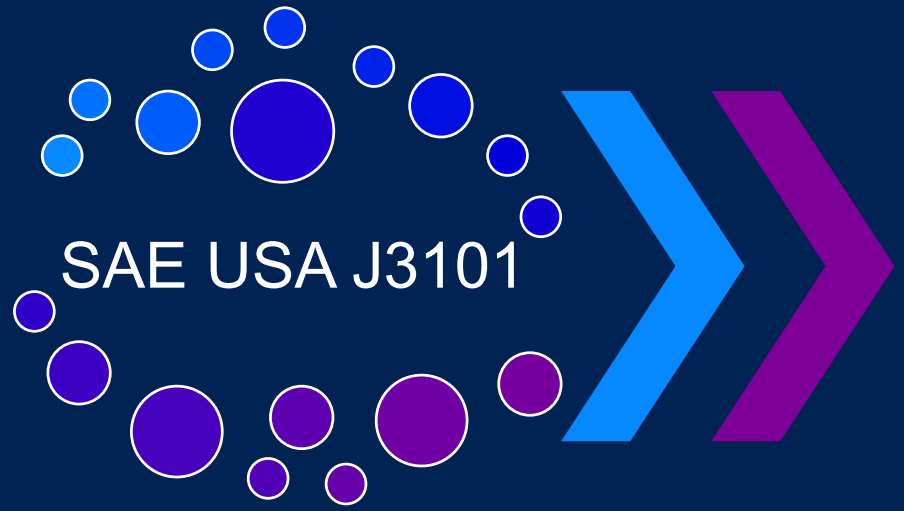


Evaluated using Common Criteria (CC) existing Protection Profile

Trusted Execution Environments Fully Meet 95% J3101 Requirements



Why Cooperation with SAE on Hardware Protected Security Environments Is Optimal



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

Global Platform™

Panel 1: SESIP

(CEN/CENLAC 17927)

SESIP

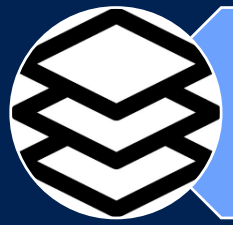
Overview SESIP

SESIP is methodology that reduces the cost, complexity and effort of security evaluation and certification.

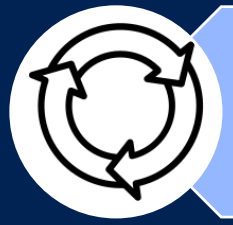
Allows to designate specific security requirements

Defines common security vulnerability assessment and testing approach.

Technology agnostic approach



Built around the security services provided by all layers of a system from sub-component to final product



Re-uses security testing

- Resulting in cost/time effective

What is SESIP?

Key Features

Protection Profiles:
- Provide predefined sets of security requirements tailored to specific use cases.

Composition and Reuse:
- Certified components can be integrated into devices with built-in security assurances.

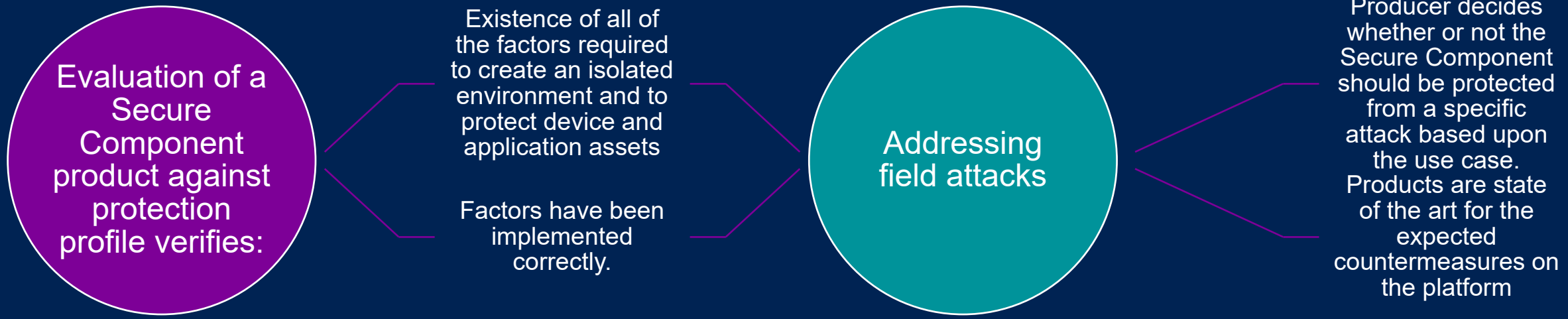
Broad Applicability:
- Primarily targets SoC (System on Chip) security but can also be used for devices, systems or components.

Automotive Focus

Aligns with key standards and regulations:
- ISO/SAE 21434 for cybersecurity engineering.
- UNECE WP.29 R155/R156 for cybersecurity management and software updates.

Promotes reusability of security evidence across the automotive supply chain.

Why are Protection Profiles so Important?



Secure Component products certified by GlobalPlatform offer

- a clearly-defined level of security
- are protected against vulnerabilities that are subject to widespread, software-based exploitation.

GlobalPlatform evaluation methodology has been created from the ISO standard.

Used by multiple security communities.

SESIP Adoption

				
Adopted by CENELEC as EN 17927	**Methodology for** • PSA Certified for PSA L2 and PSA L3 • Qi chargers • CCC UWB modules • Evidence of conformance for the CSA PSWG v1.0 • Composition methodology for the GSMA MDSCert and ETSI EN 103 732 (mobile consumer devices)	Today labs are seeing an increasing request for SESIP certification in many markets • Automotive is also starting to request pre-certification on SESIP to understand security risks-	Ongoing Discussions on Adoption in Additional Countries in Asia	Ongoing Discussion on Adoption with Major IOT Associations

Panel 1:
SESIP Certification (CEN/CENLAC 17927) :
Value Proposition for Automotive ?

Jorge Ruiz Wallace, Dekra

Bill Mazarra,Stellantis

https://images.app.goo.gl/UkcDfyHUbDNeWF1s7

Global Platform™

Segment 2: Evolution of Regulations and Standards

Global Platform™

You are in the right Place for the Cybersecurity Vehicle Forum Berlin

We are in a break until 16:05 CET!

Segment 2: Developments of Regulations and Standards

Sebastian Hans, Oracle

- PQC Secure Elements

Mike Ounsworth, Entrust

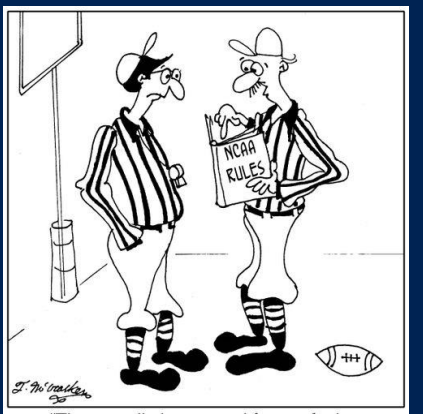
- PQC: practical issues impacting the future

John Krzeszewski, Eaton

- Evolution of ISO/SAE 21434 and progress on CAL/TAF

David Ward, Horiba-Mira

- Updates on Evolution of Functional Safety of ISO 26262



"There really is no need for confusion. Rule 10, section 5, article a, subsection 3, exception 4 quite clearly states ... "

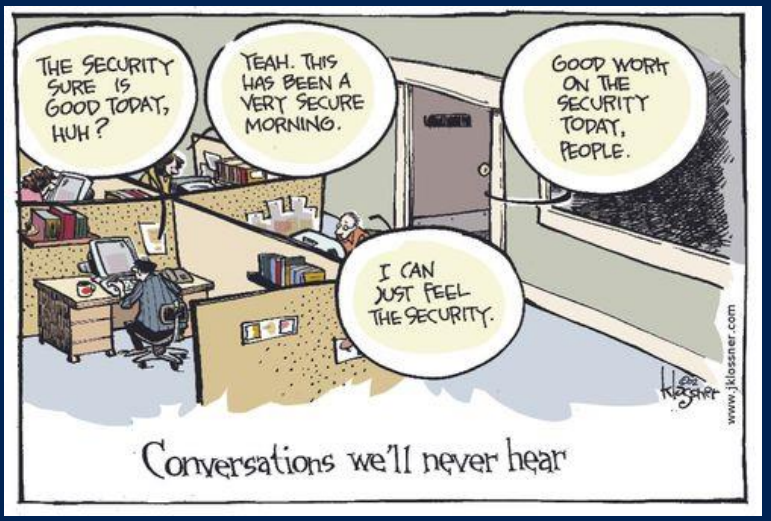
https://www.cartoonstock.com/directory/m/motor_vehicle_regulations.asp

Global Platform™

Panel 3:
Intersection of Safety with Security Isolation

Panel 3: Intersection of Safety with Security Isolation

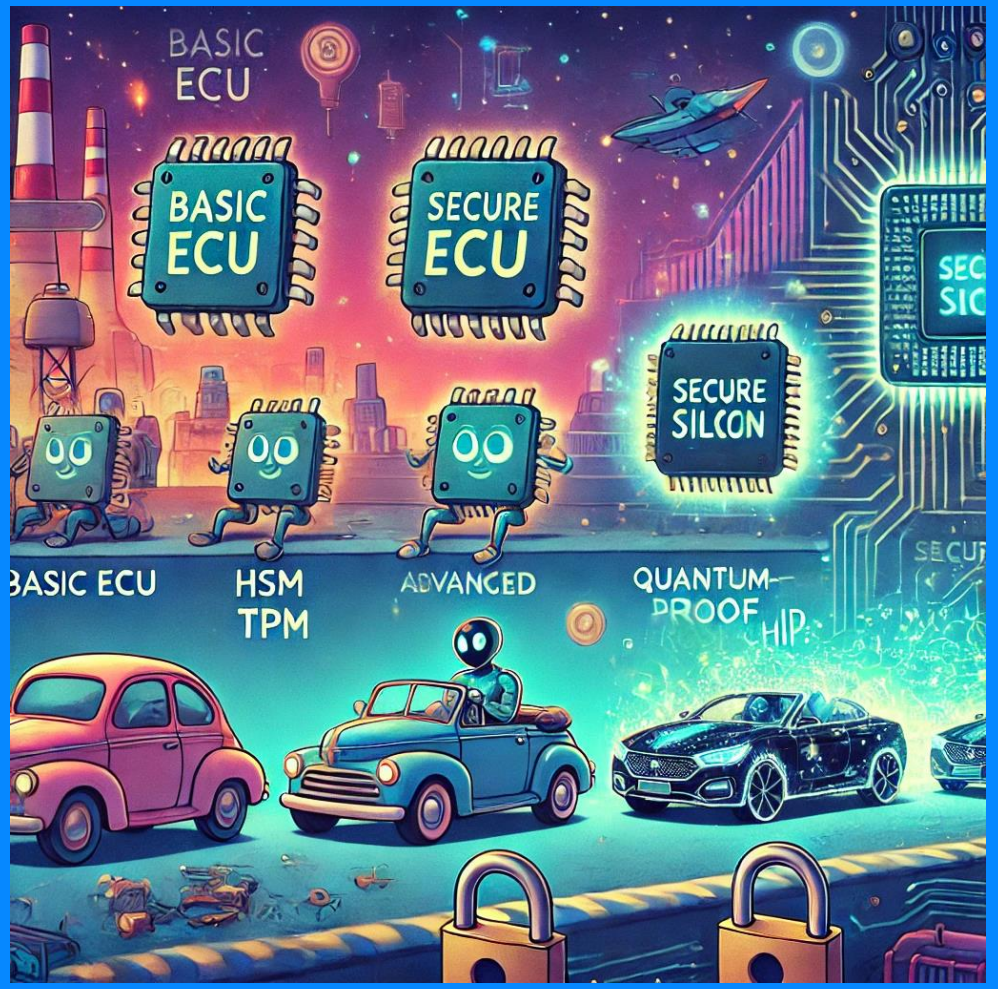
David Ward, Horiba-Mira	Redouane SOUM, AMPERE	Richard Hayton, Trustonic
David Ward, Horiba-Mira	Andrew Jones, AVCC	Richard Hayton, Trustonic
	SOUM Redouane, AMPERE	



https://www.cartoonstock.com/cartoon?searchID=CX916324

Global Platform™

Panel 4: Evolution of Secure Silicon



HSM:

- Hardware Security Modules

SHE:

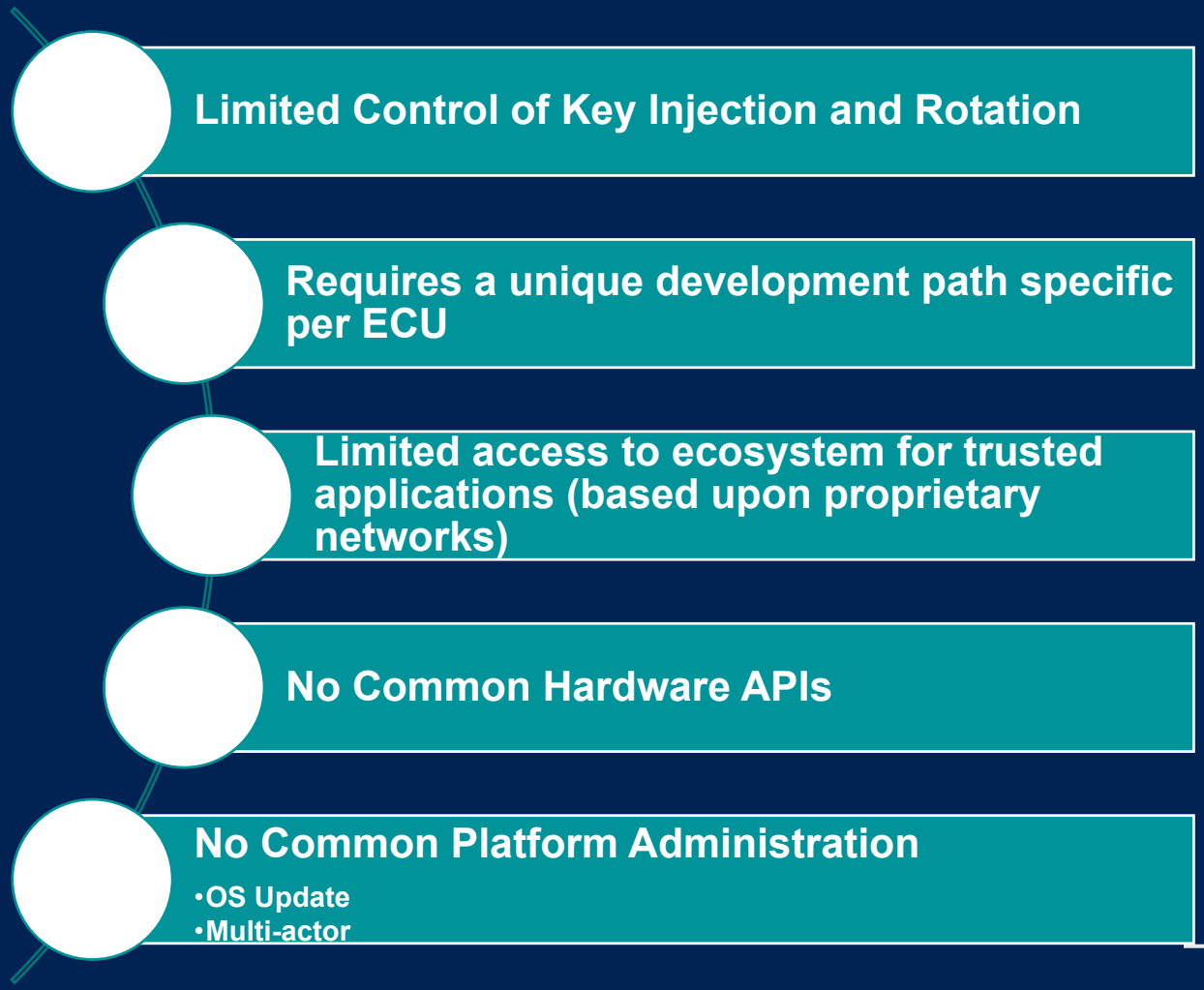
- automotive Microcontroller Unit (MCU) by HSI

Evita

- Fragmented proprietary HW APIs

SHE+

Traditional Automotive HSMs Have Important Gaps



Different Compliance Scenarios Possible

Panel 4: Evolution of Secure Silicon

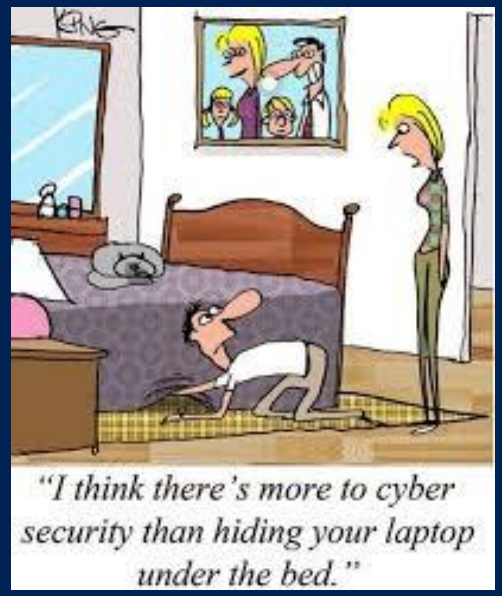
Philip Lapczynski, Renesas

Laurence Bringer, Thales
Yves Le Bobinnec, Thales

Laurent Tabaries, STM

Craig Rawlings, Stellantis

Riemenschneider Lukas (ETAS-SEC/XPC-Bo2)



https://www.cartoonstock.com/cartoon?searchID=CS162634

Global Platform™

If you are interested in joining in on the fun…

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

Global Platform™

The standard for secure digital services and devices

→globalplatform.org

Global Platform™

Panel Questions

Panel 1: SESIP Certification: Value Proposition for Automotive?

- Based upon the different development models (including V-model), where could SESIP certification contribute the most?
- Could SESIP reduce the efforts during the verification and validation phases?
- Would SESIP certification @ different levels contribute to the TARA development process?
- What would likely be the motivation for Tier 1's to adopt SESIP?
- How important is mutual recognition by different regulatory bodies be for adoption of SESIP in Automotive?
- What standardized protection profiles are needed most by the automotive industry to drive the market?
- How can SESIP help sort the good, better, and best of Hardware Protected Security for autos?

Segment 2: Developments of Regulations and Standards

PQC

Impact on Automotive? How can we plan?

ISO 21434

Potential New Developments

Panel 3: Intersection of Safety with Security Isolation

Is there a role for Safety and Security to be compatibly managed in sharing & isolation technologies in Automotive?

David

Are there standardisation opportunities?

David
Andrew

How are artificial intelligence and machine learning transforming the landscape of automotive security, and what opportunities do they present for predictive threat detection and response?

Can these be used in Asil B ?

Asil D?

David

In what way does the emerging role of Cloud computing in automotive change the requirements for hardware security use cases (both functional safety & non-safety critical use cases)?

David
Andrew

How do you manage mixed criticalities in isolation? priority inversion', shared services ? What may be the use case differences that decide between the implementation choices?

Is there a desire to increase sharing across isolation domains to reduce costs/improve efficiency?

If so, is this compatible for safety critical areas? Or can it only happen with general purpose compute in Automotive?

Andrew

How do you manage trust relationships in future open architectures across vendors?

Panel 4: Evolution of Secure Silicon

What role will standardisation play in the evolution of HPSEs?

Can incremental development of ECUs foster more efficient and effective SDV realisation?

How do you ensure key provision & management effective over the whole life of the vehicle?

Is there a business case to extend HSM capabilities with Secure Elements for specific use cases?

How business logic in SE can improve the overall security of the solution?

Should the multi-tenant characteristics of the automotive value chain drive the ownership for the provisioning of keys?

How important is portability for trusted applications across ECUs?

Is there an opportunity for standardization to foster the evolving need for flexibility ?

How do we migrate from proprietary hardware and basic software environments to a platform-oriented architecture for

Do we expect future requirements for safety rated HPSEs?

What are the real time and start up requirements of HSM that could drive future evolutions?

Would guidelines on minimum requirements for secure boot be beneficial for the ecosystem?

Global Platform™

The standard for secure digital services and devices

→globalplatform.org