Global Platform™

Standardisation Supporting Software Defined Vehicles

20 November 2023

Francesca Forestieri, Automotive Lead

JAVA CARD Forum

Building the Foundation of Security for 20+ years

GlobalPlatform is *THE* standard for managing applications on secure chip technology:

- **60 billion+ Secure Elements shipped worldwide are based on GlobalPlatform specifications**
- **Over 15 billion GlobalPlatform-compliant Trusted Execution Environment in the market today**

Financial Industry	Identification & Trusted Signature	Passports	Mobile Industry	Internet of Things	Automotive Industry
Majority of bank cards based on GP specs	Health cards	Many ePassports based on GP specs	All SIMs are based on GP Technology	Connected TVs	Digital Car Key
Majority of credit cards based on GP specs	Social security cards		GSMA eSIM is based on GP technology	Meter Gateways	Infotainment systems
PoS	Government Identification Cards		Most Android phones use GP TEE	Smart Meter	Digital Rights Management
	Enterprise Identifications			Smart Home Devices	Telematics
				Wearables	IPR Protection of ADAS
					Migration to Software Defined Vehicles

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

ERICSSON

HUAWEI

fime

galitt — a Sopra Steria company

G+D Mobile Security

HID

IDEMIA — augmented identity

infineon

mastercard

NTT

NXP

ORACLE

Qualcomm

SAMSUNG

life.augmented

T-Mobile

THALES

TRUSTONIC

verizon

VISA

winbond

Participant

Applus+

OPLS Lab

COMPRION — Test it. Prove it. Move it.

HONOR

riscure — Challenge your security

SERMA — SAFETY & SECURITY

SGS brightsight

orange

Quarkslab

TRUSTCB — TRUST AND VERIFY

UL

VALID

Observer, Public Entity and Consultants

AMEX

AT&T

CARIAD

cea

leti

CB

cisco

楚天龙 CHUTIAN DRAGON 龙行天下 品质未来

DNP

DISCOVER

东信和平 EASTCOMPEACE

FEITIAN — WE BUILD SECURITY

財團法人資訊工業策進會 INSTITUTE FOR INFORMATION INDUSTRY

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

天喻信息

xardpay

XCURE CORP.

mi

BACTECH

Digital Cubes

INTERNET OF TRUST

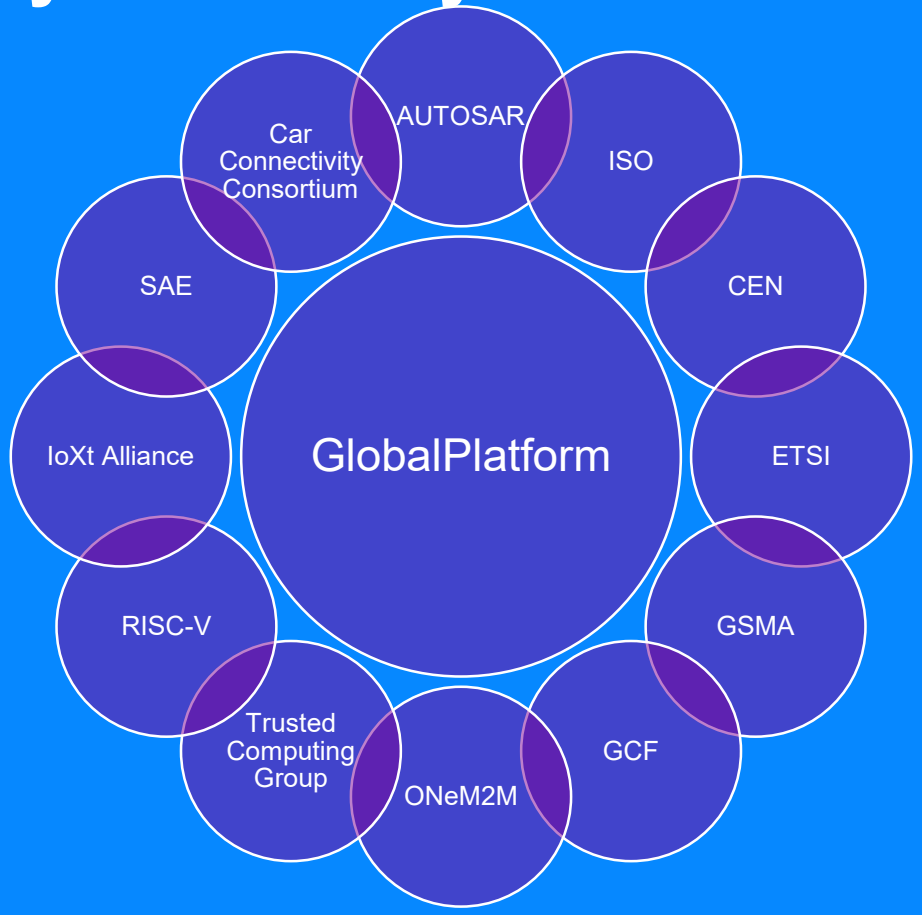
MoneTECH

NEXTENDIS

SAFEPAY

zwipe

Your Partner for CyberSecurity 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 Collaborative Partners

Agence nationale de la sécurité des systèmes d'information
ACN Alliance pour la confiance numérique
APSCA Asia Pacific Smart Card Association
EMVCo
European Payments Council
EUROSMART The Voice of the Digital Security Industry
Asia IC Card Forum
fido alliance
NICSS
IFAA 互联网金融身份认证联盟 Internet Finance Authentication Alliance
PTCRB
industrial internet CONSORTIUM
oma SpecWorks For a Connected World
SECURE TECHNOLOGY ALLIANCE
SMART TICKETING Alliance
TAF
TRUSTED PLATFORM
TRUSTED COMPUTING GROUP
mobey forum
W3C

Automotive & Mobility Related

AUTO-ISAC Automotive Information Sharing and Analysis Center
AUTOSAR
CARCONNECTIVITY consortium
cen
ETSI
GSMA
GCF Global Certification Forum
ISO International Organization for Standardization
JAVA CARD Forum
IoT Connectivity Alliance
ioXt internet of secure things
NFC FORUM
NIST National Institute of Standards and Technology U.S. Department of Commerce
oneM2M The IoT Standard
RISC-V
SAE INTERNATIONAL
TCA TRUSTED CONNECTIVITY ALLIANCE

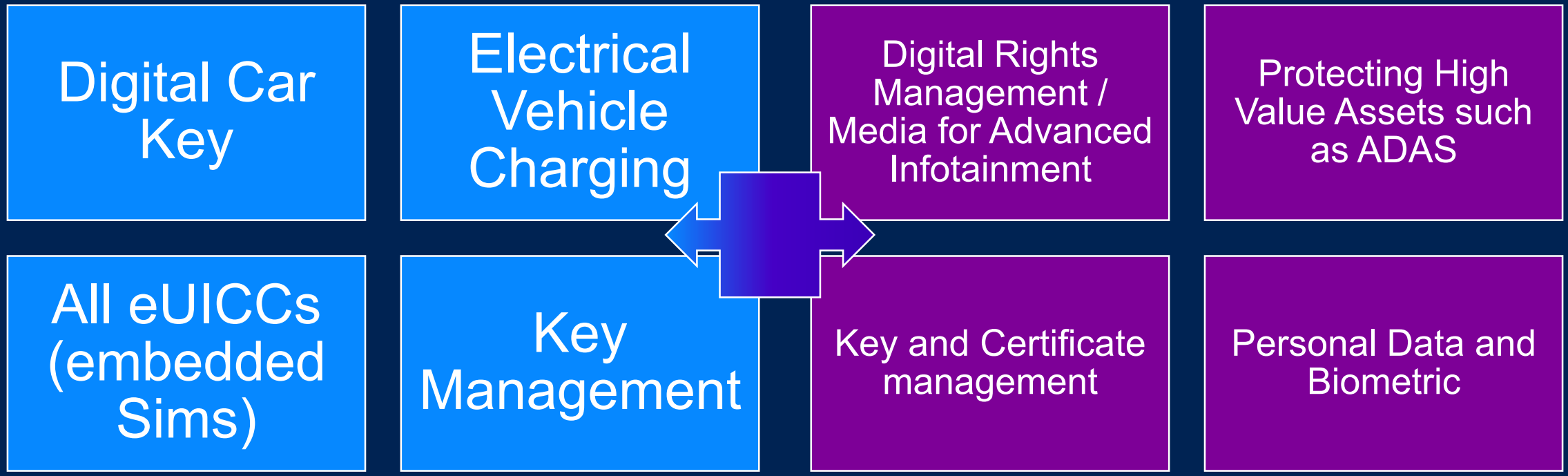
Why GlobalPlatform: Market Presence in Automotive

Secure Element

OVER 192 Million Connected Cars in 2023

Trusted Execution Environment

In Over 100 Million Vehicles as of 2023*



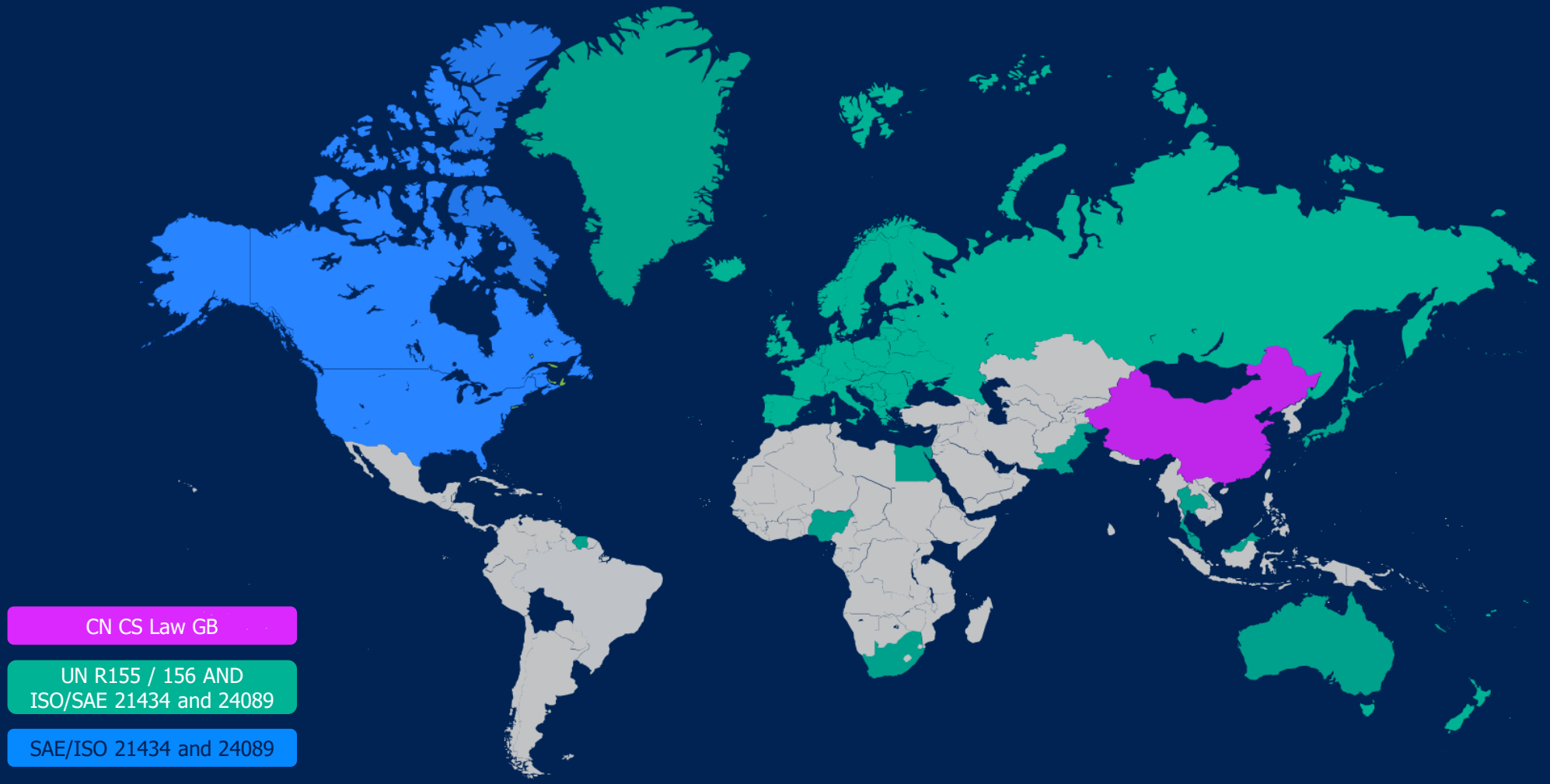
192 Million Connected Cars in 2023 by Juniper Research
https://www.juniperresearch.com/press/connected-vehicles-to-surpass-367-million-globally#:~:text=Hampshire%2C%20UK%20–%209th%20January%202023,from%20192%20million%20in%202023.

*Confidential Source on Market Presence

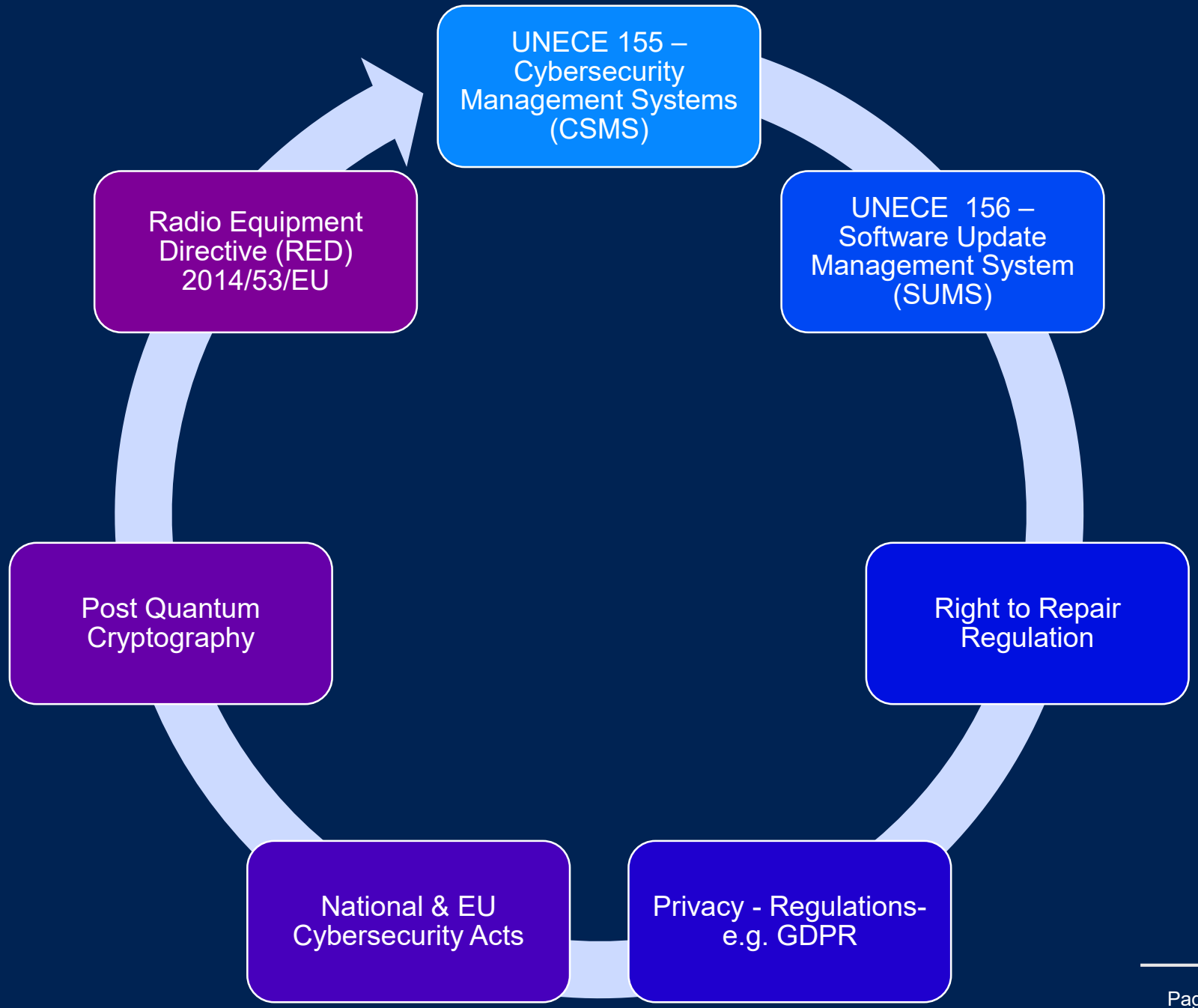
New Requirements

How will they manifest themselves?

Automotive needs the “how” of security standards



Increased Cybersecurity Regulations in Automotive: Global Trend



UNECE Regulations for Cybersecurity

UNECE 155 – Cybersecurity Management Systems (CSMS)

- **Puts the onus of the cybersecurity certification process on the OEM.**
  - Demand that best practices are incorporated into the design of vehicles
  - Demand vehicle manufacturers provide **a reasoned argument as to the cybersecurity of their vehicles**
  - **Require ongoing cybersecurity for vehicles throughout all stages of the vehicle's lifecycle including post-production**
  - Risk assessments for each type of vehicle
  - **Cyber security audits for every type of vehicle**
  - Analysis of weak points during the entire development and production process
  - Cyber security monitoring and incident response to existing vehicle types
  - **Documentation of a cyber security management**

UNECE 156 – Software Update Management System (SUMS)

- Systematic control and compliance with government guidelines
- Establish Software identification management
- Documentation of the **hardware and software versions relevant for a vehicle type**
- Identification of the software relevance for type approval **including the dependencies from software updates**
- Assessment whether a **software update (SU) affects type approval and security of vehicle**
- **Transparent information for vehicle owner about software updates**

https://unece.org/sites/default/files/2021-03/R156e.pdf
https://unece.org/sites/default/files/2021-10/GRE-85-36e.pdf
https://unece.org/sites/default/files/2021-06/GRPE-83-27.pdf

Automotive Standards for Cybersecurity are impacted also from…

Standarisation Bodies from Different Ecosystems

Global Standards on ICT-enabled systems, applications and services deployed across all sectors of industry and society

- 900+ member organizations are drawn from over 60 countries and five continents.
- **ETSI EN 303 645:**
  - Standard '**Cyber Security for Consumer Internet of Things: Baseline Requirements**' is intended to prepare consumer IoT devices to withstand common cybersecurity threats
- **ETSI TS 103 701**
  - '**Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements**

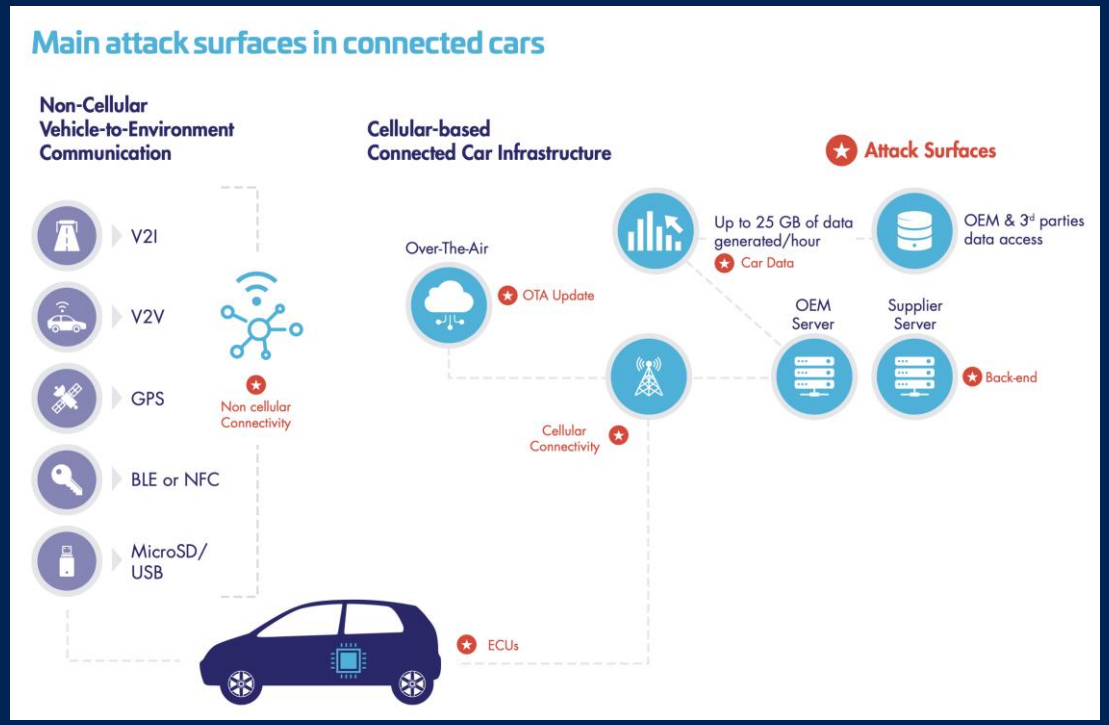
Independent, non-governmental international organization specialised in Technology and Manufacturing (two top sectors in 2021 were ICT, Transport)

- Membership of 167 national standards bodies.
- **ISO PAS 5112:2022**
  - **Guidelines for auditing cybersecurity engineering**
  - managing an audit programme for a cybersecurity management system (CSMS);
  - conducting organizational CSMS audits;
  - competencies of CSMS auditors; and
  - providing evidence during CSMS audits.

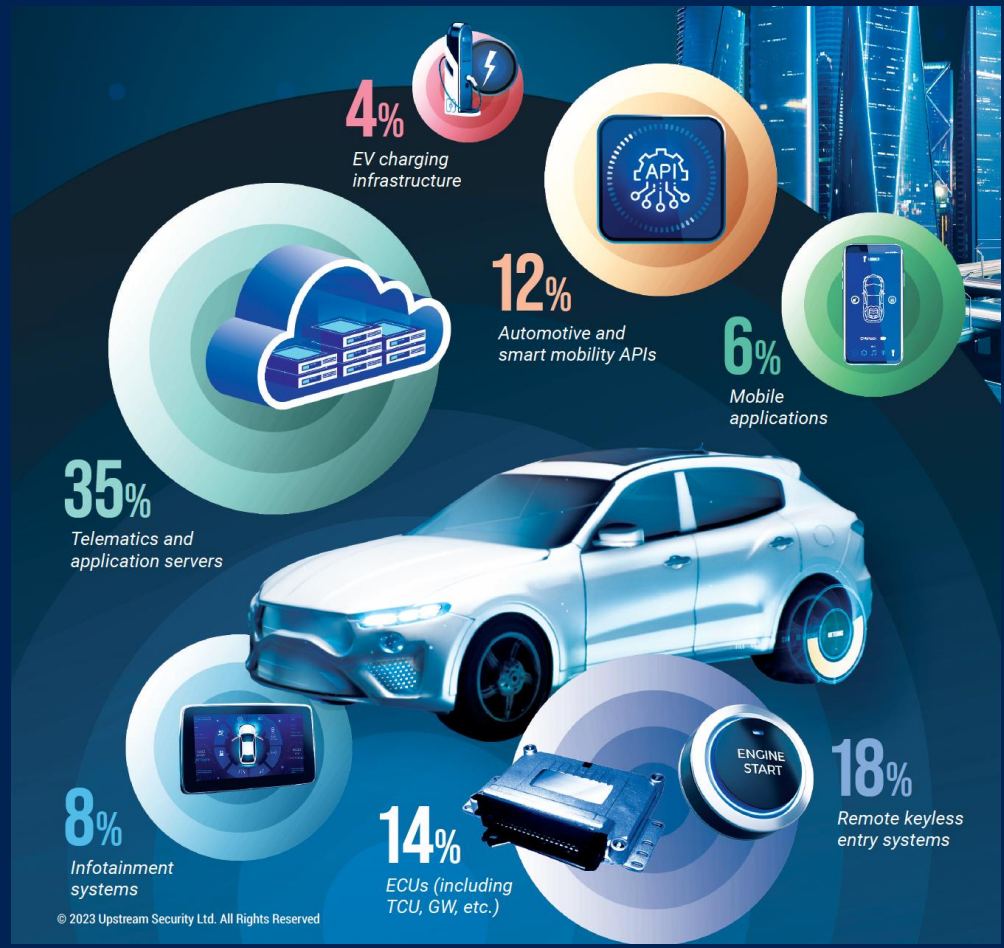
Association of International Society for Automotive Engineers which develops cconsensus standards.

- a global association of more than 200,000 engineers and related technical experts in the aerospace, automotive and commercial-vehicle industries. Present in 86 countries as well as all 50 U.S. states.
- **SAE J3101**
  - **Standardises Protected Security for Ground Vehicles**
    - hardware root of trust and the hardware-based security primitives are fundamentally necessary to satisfy demands of connected and highly or fully automated vehicles.
    - Provides a view of security mechanisms supported in hardware for automotive use cases, along with best practices for using such mechanism

Security Challenges

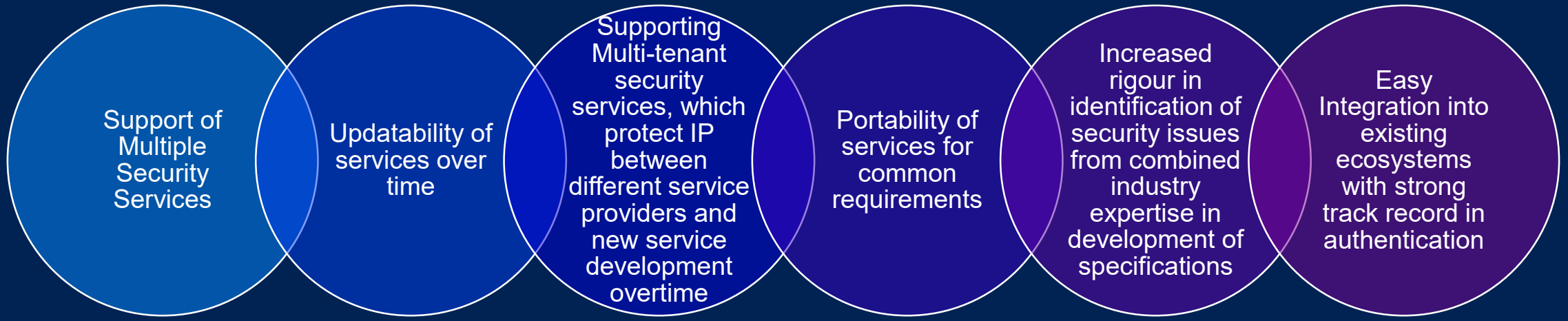


https://sc.pages05.net/lp/22466/800491/iot-automotive-cybersecurity-challenges_0.pdf



https://upstream.auto/reports/h1-2023-automotive-cyber-trend-report/

Future Proofing Security: Adding Flexibility

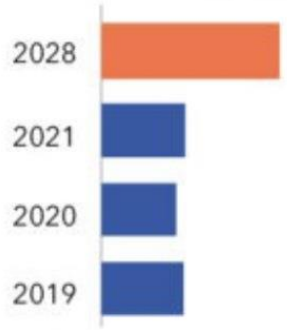


Market Forecasts E/E in Automotive

Automotive E-E Architecture Market by Type, Product Type, End User, Sales Channel and by Region, Global Trends and Forecast from 2019 to 2028

EXACTITUDE CONSULTANCY

Market Size



Market is expected to grow faster in next decade with more than double digit growth.

11.44%

The continuing and innovative advancements in airbag technology, the effectiveness of Automotive airbags in reducing the impact of collisions has improved.

Electrification of vehicles and connected cars are the major drivers of the Automotive E-E Architectures market.

Autonomous driving has the potential to boost the production of Automotive E-E Architecture.

37% APAC

Key Players

HELLA, Continental, APTIV, MAGNA, MAHLE, Visteon

https://exactitudeconsultancy.com/reports/987/automotive-e-e-architecture-market/

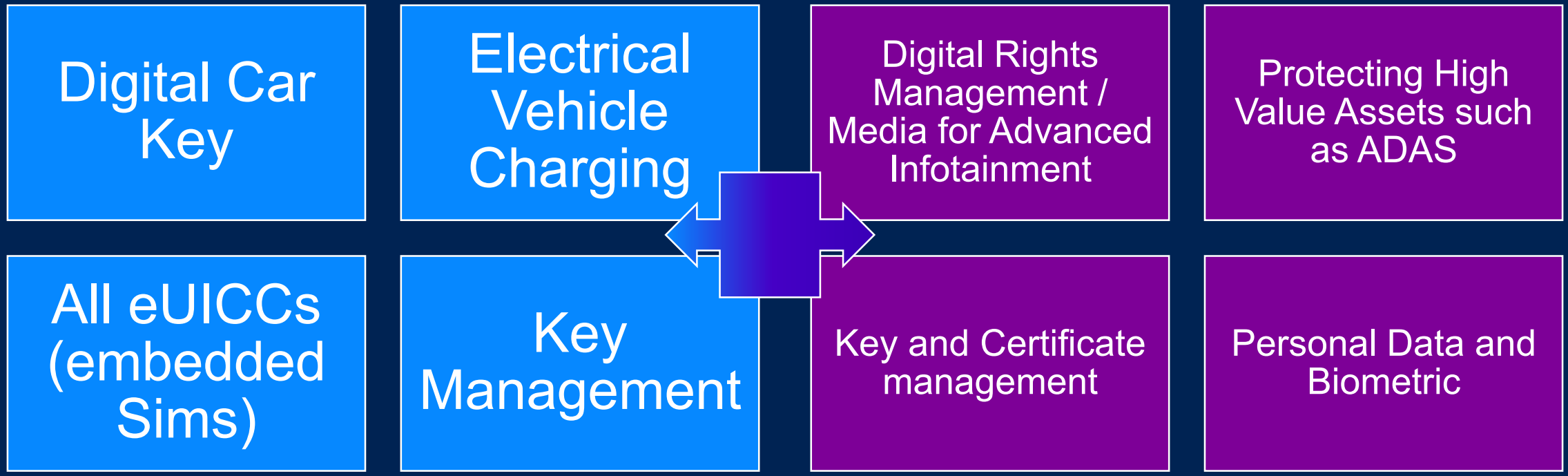
Why GlobalPlatform: Market Presence in Automotive

Secure Element

OVER 192 Million Connected Cars in 2023

Trusted Execution Environment

In Over 100 Million Vehicles as of 2023*

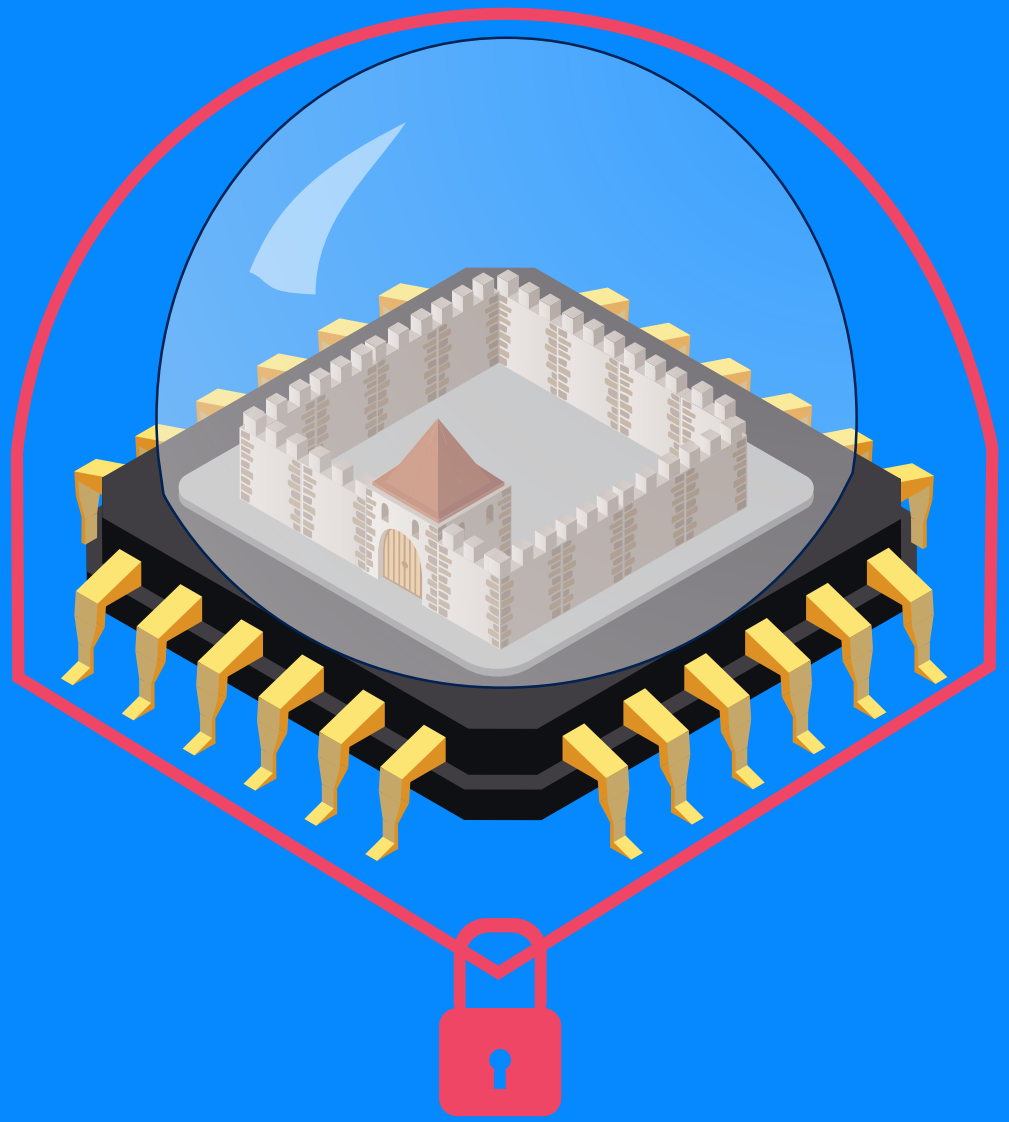


192 Million Connected Cars in 2023 by Juniper Research
https://www.juniperresearch.com/press/connected-vehicles-to-surpass-367-million-globally#:~:text=Hampshire%2C%20UK%20–%209th%20January%202023,from%20192%20million%20in%202023.

*Confidential Source on Market Presence

GlobalPlatform Technologies

GlobalPlatform Secure Element



- A secure enclave protected against physical and software attack
- Runs an embedded JavaCard OS providing standard APIs and functions
- Commonly used in SIM cards, Passports, Bank Card and embedded applications
- Supports multiple independent applications (containers)

GP Protection Profiles

GP Sets Security Objectives

Set of security objectives and requirements for a category of products

- Independent from any specific implementation
- Reusable
- Enables the development of functional standards
- Helps in defining the security specification of a product

GP Defines Implementation Requirements

A set of security requirements which are useful and efficient to satisfy identified objectives

Products will be tested to ensure they meet these requirements

Accredited Lab Evaluates Profile

Evaluated by an accredited Common Criteria (CC) lab

- The lab checks that the Protection Profile is consistent, i.e. requirements match the objectives, objectives are consistent with products and usage

Protection Profile is Published

GlobalPlatform Protection profile accessible from http://www.globalplatform.org/specificationsdevice.asp

The protection profile can then be used by 3rd party labs to validate a product meets the agreed security level

Common Criteria

SESIP

GlobalPlatform's Secure Element Leverages Java Card Protection Profile

support any type of SE deployment from ID card to embedded Se

Secure Element Protection Profile (PP): Modular

By extending the Java Card PP [PP0099], the core SE PP defines the:

- Security problem
- Objectives and
- Requirements for SEs.

SE PP is a standardized description for the evaluation:

- The assets
- The threats
- The security objectives
- The security requirements) of all the Card Content Management.

Additionally, four PP Modules are defined to cover:

- Confidential Card Content Management [Amd A]
- Contactless Services [Amd C]
- Executable Load File Upgrade [Amd H]
- Secure Element Management Service [Amd I]

Global Platform™

GlobalPlatform Work Items in Automotive

Driving Requirements into GlobalPlatform

Cybersecurity Vehicle Forum

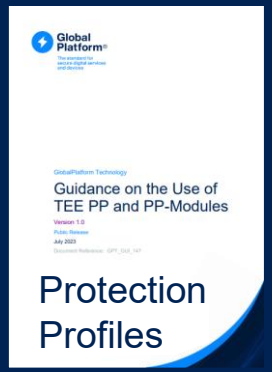
Nov 2022 Munich
June 2023 Detroit
Sept 2023 Tokyo
Oct 2023 Beijing
Nov 2023 Hamburg

Inside GlobalPlatform

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

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

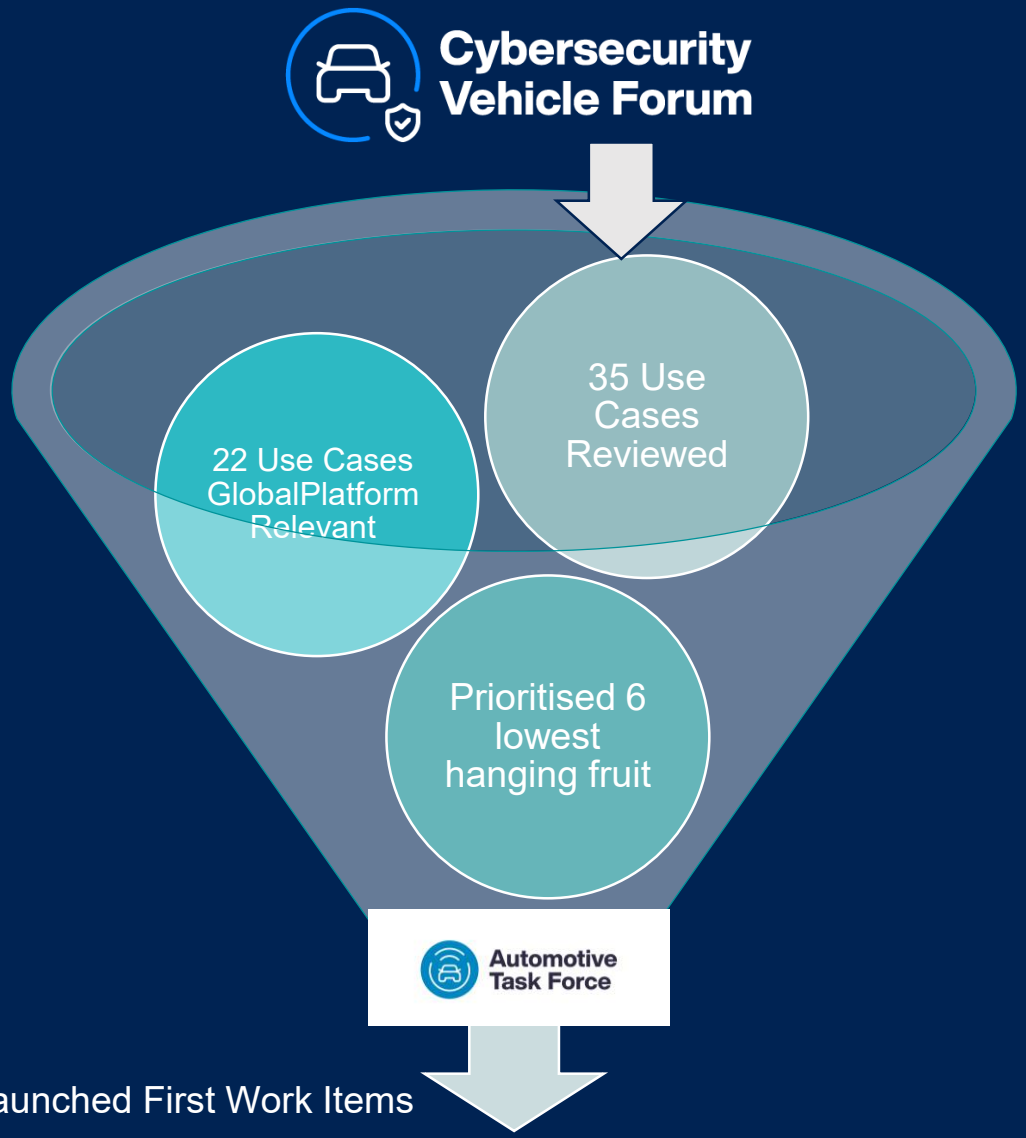
Whitepapers



Specifications

Protection Profiles

GlobalPlatform Automotive Activities: First Year



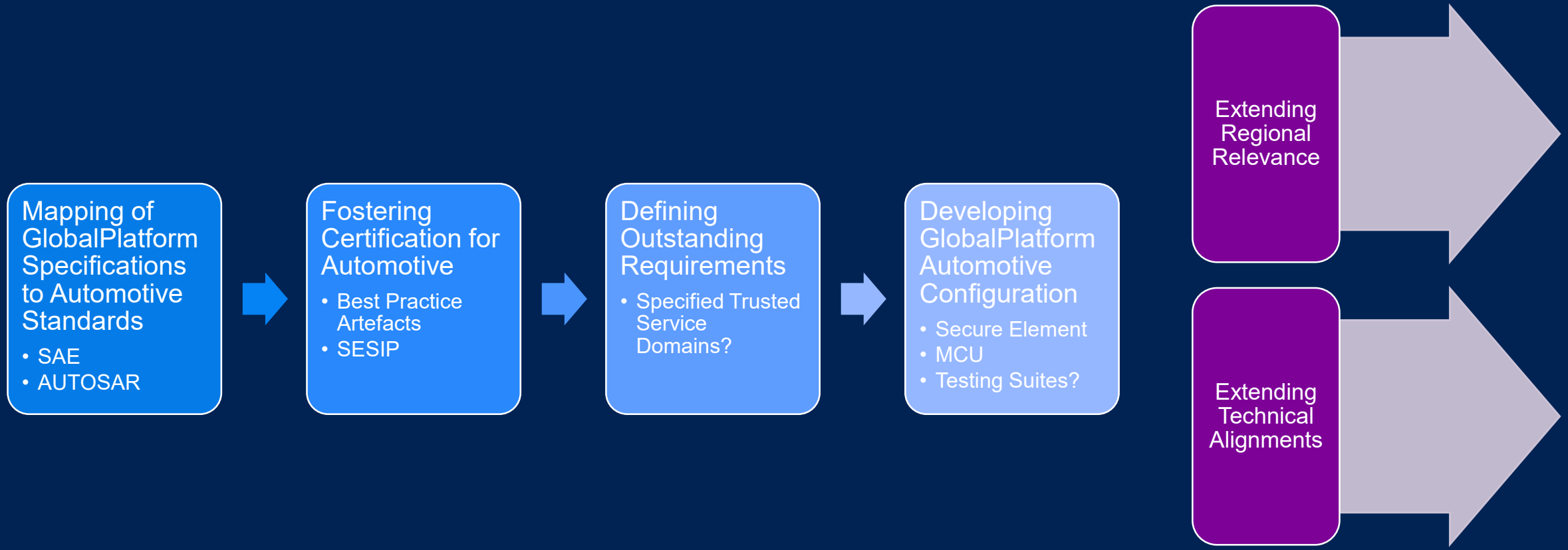
Launched First Work Items

- Standards Alignment:
  - SAE International Hardware Protected Security Mapping J3101
    - Autosar Coordination
- Guidelines on Trust Anchors
  - Security and Trust in Automotive Systems

GlobalPlatform Security White Papers

https://globalplatform.org/resource-publication/cybersecurity-in-automotive-v1-0/

Automotive Vision:
"Securing Software Defined Vehicles"



Relevant Automotive Industry Organisations

....

Global Platform™

Work with SAE on J3101: Hardware Protected Security Environments

Relevance of GlobalPlatform's Alignment with SAE on Hardware Protected Security Environments

Process

ISO /SAE 21434

+

Product

SAE J3101 Hardware Protected Security Environments

=

Compliance

Cybersecurity Vehicle Management

- Compliance with UNECE 155
- Demonstration of Best Practices

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)

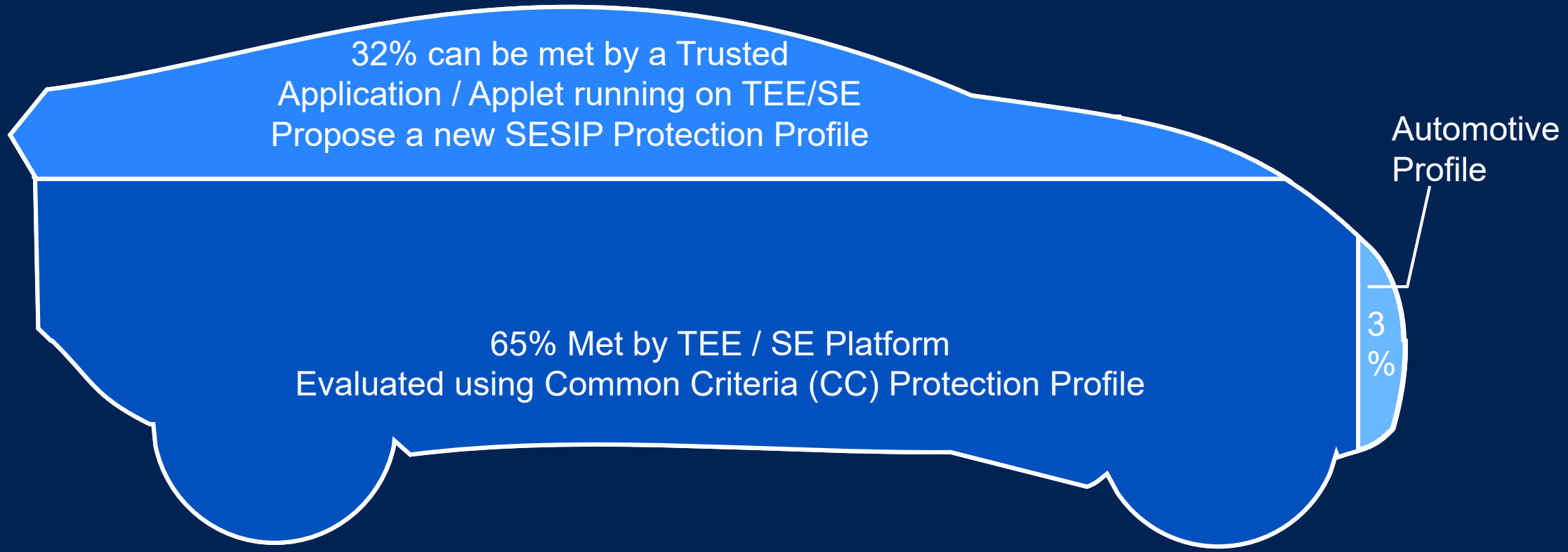
To satisfy additional security objectives which could be specified for certain usages of secure logging, the following additional profiles may be required and should be considered based on the context provided above:

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

SAE INTERNATIONAL

Global Platform™

Meeting J3101 Requirements



Mapping J3101 requirements to standard technology, makes it easier for automaker to meet requirements, and ultimately pass type approval

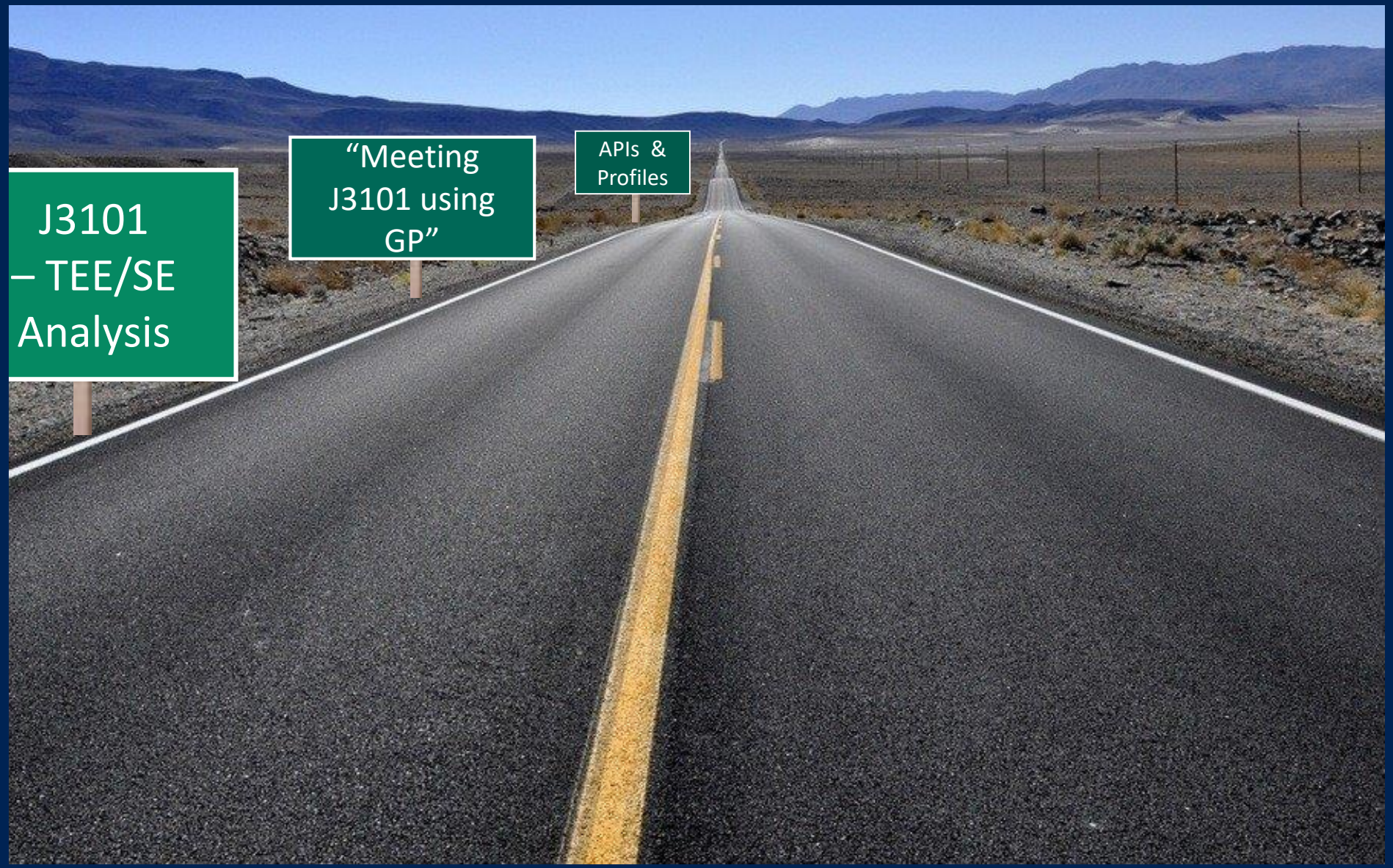
Route

First few steps are clear

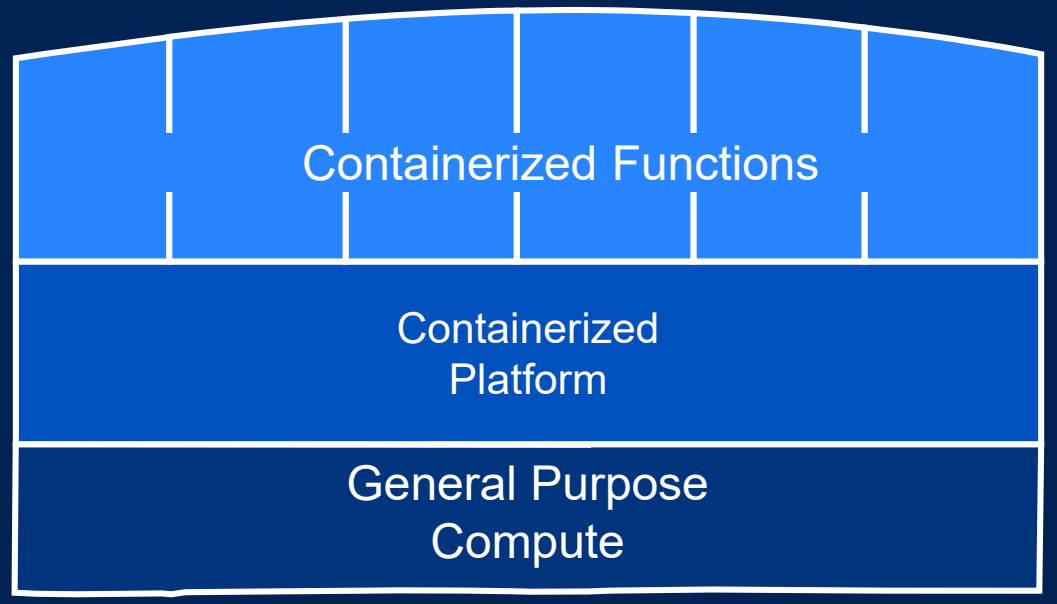
Will enable vendors to build J3101 compliant solutions

Eventually [we] may define a successor to SHE++/HSM/EVITA?

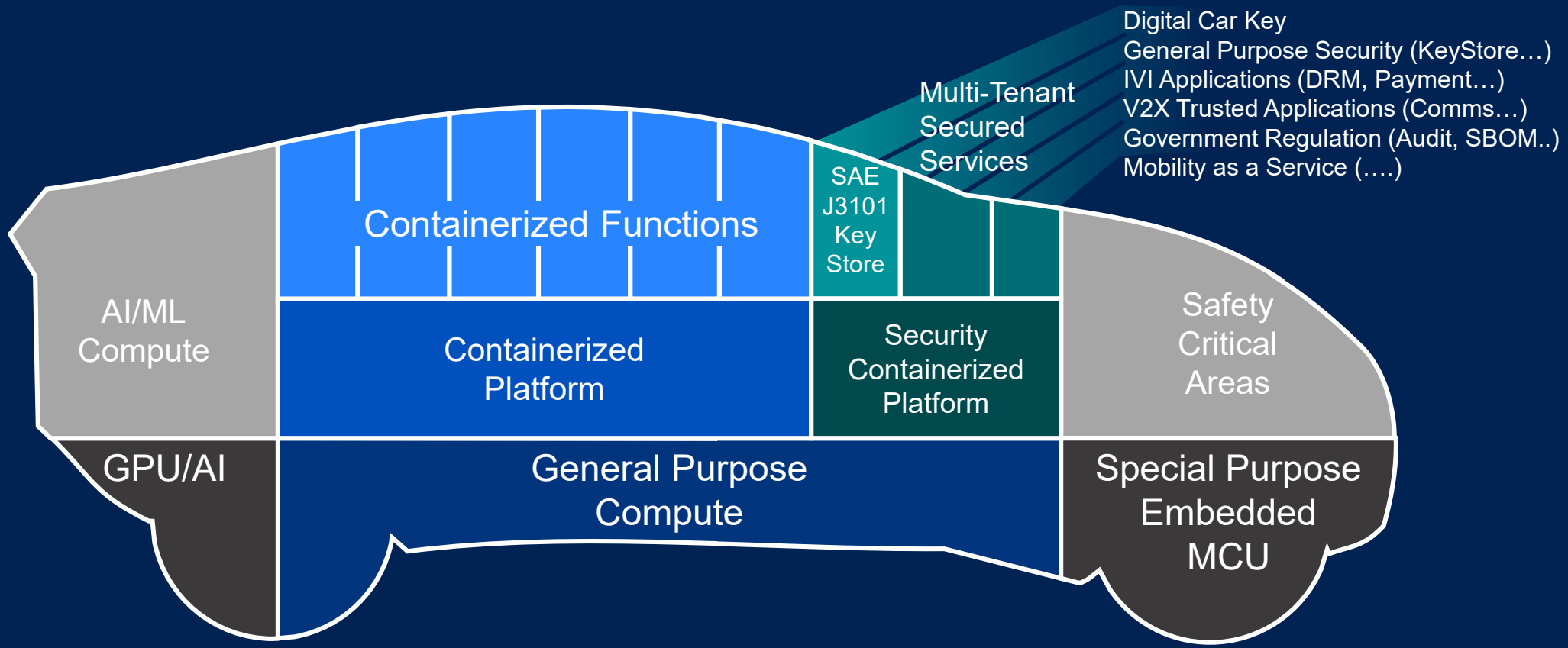
Meet Industry desire for standardize policy management for key usage



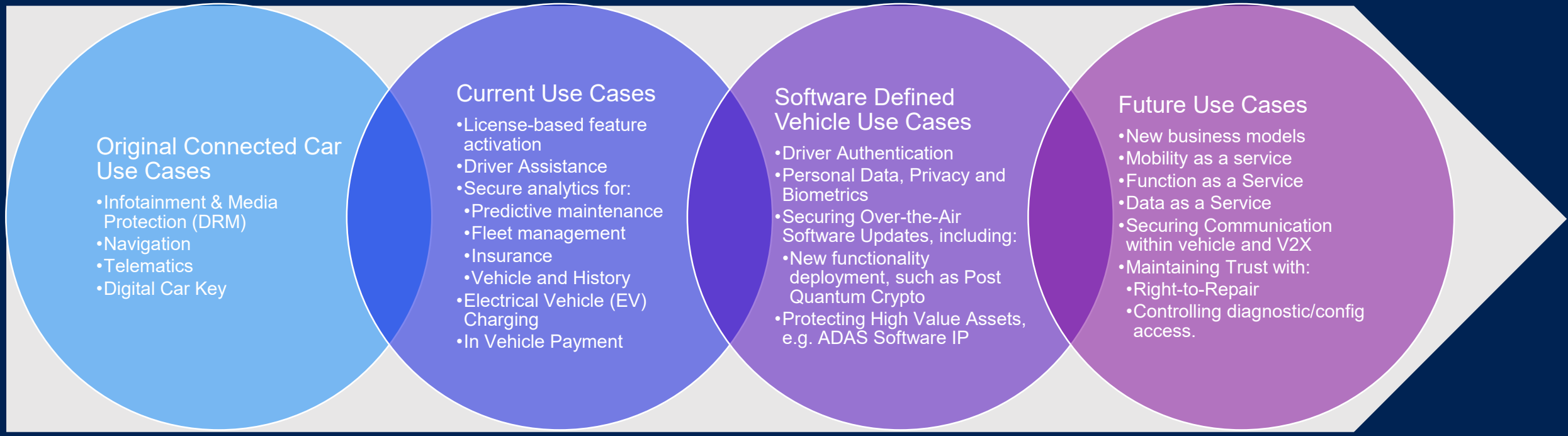
GlobalPlatform & Software Defined Vehicles



GlobalPlatform & Software Defined Vehicles



GlobalPlatform Supports the Evolution Path for Security Critical Use Case



Get Involved!

Why Engage in Security Standardisation (vs a solely Proprietary Solution): Benefits on Effective Cybersecurity Practices

Transparency on Security Approaches

Standards discussed, debated (vs. security by obscurity)

Regional requirements are addressed

Evidence of Compliance

Security Certification

- Measured and proven compliance to security target level
- Comparability of services across vendors in terms of target of evaluation and vulnerability analysis

Functional Compliance

- Demonstratable compliance for portability of common services
- For Exact Scope of Evaluation and for specific parameters

Evidence for due diligence and best practice adoption

Timely, Effective Cybersecurity Responses

Community Analysis of Threats and Responses

Transparency of coordinated responses for solutions required for multiple OEM clients

Evolution in platform protection in response to trends in attacks and threats

Why Engage in Security Standardisation (vs a solely Proprietary Solution): Optimised Products

Lower cost of mass market produced solutions

- Better value for money as organization can focus engineering on differentiators and less on aspects that do not provide competitive advantage
- The "costs" of common features is depreciated across the community
- Leveraging common set of requirements WHILE incorporating greater sophistication on cybersecurity solutions than in the past

More Vendor Options

- Reducing vendor lock-in given portability of services
- Increased second source options

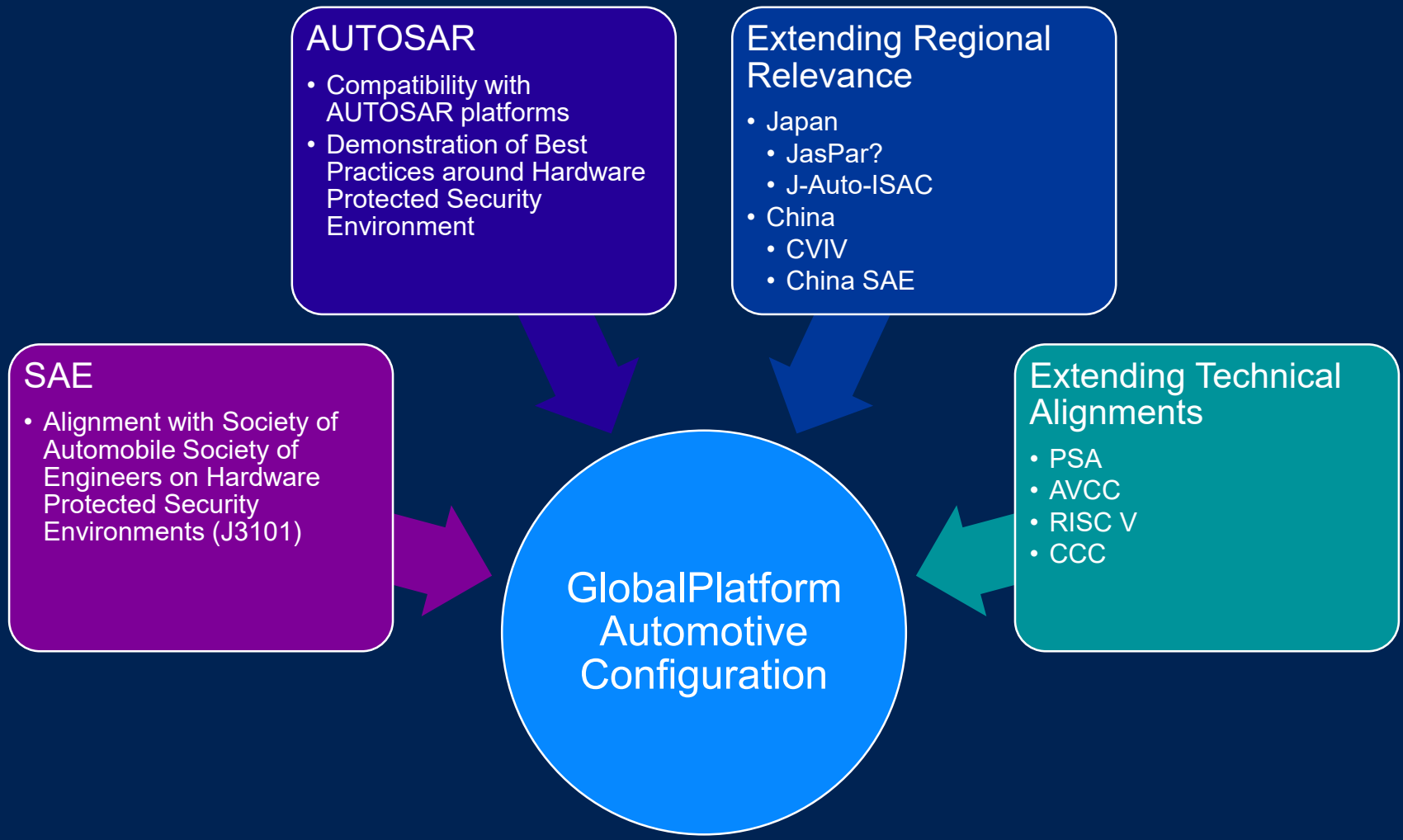
Simplified ECU development

- Reduction of Integration Costs
- Faster development of new ECU generations, given the increase in portability of common services (i.e. for non-differentiator services)

Robust Ecosystem

- Multiple Skilled Stakeholders to support service developments
- International Coverage of Multiple markets

Alignment on Automotive



How GlobalPlatform Works for Automotive

Participation in GlobalPlatform Automotive Activities

Cybersecurity Vehicle Forum

- 70-100 average participants
- Majority of non-GlobalPlatform participants

Members of Automotive Task Force

- 121 Individuals
- 49 Companies
- 63 documents submitted

Join Us!

Follow GlobalPlatform Specifications

Become a GlobalPlatform Member: Optimise your roadmap

Contribute on Development of Automotive Specifications within GP

- Working on Identified Topics
- Identifying New Topics

automotive@globalplatform.org

Global Platform™

The standard for secure digital services and devices

→globalplatform.org