Global
Platform™

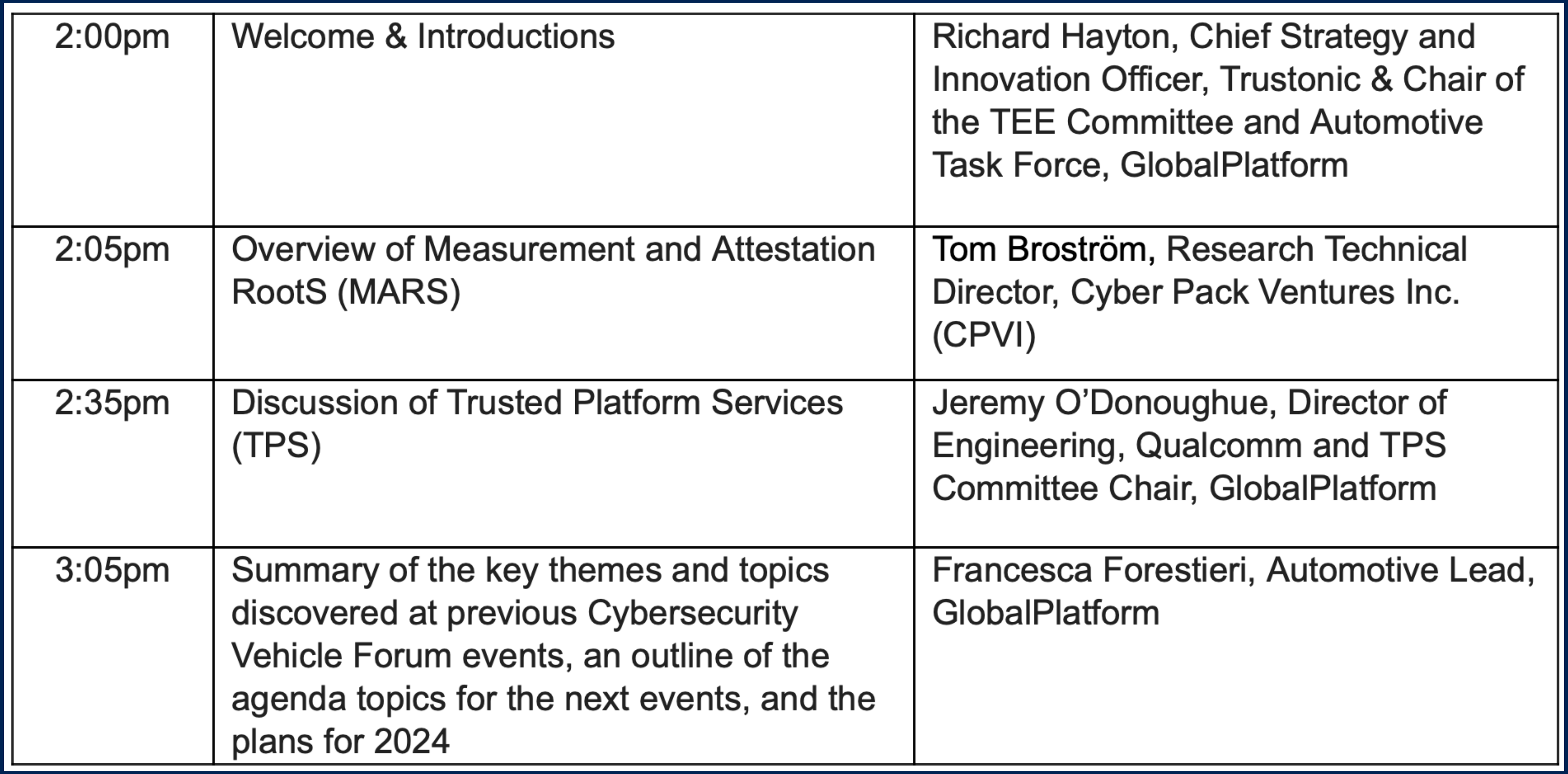
Cybersecurity Vehicle Forum - Virtual

25th September 2023

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

Cybersecurity
Vehicle Forum

Agenda

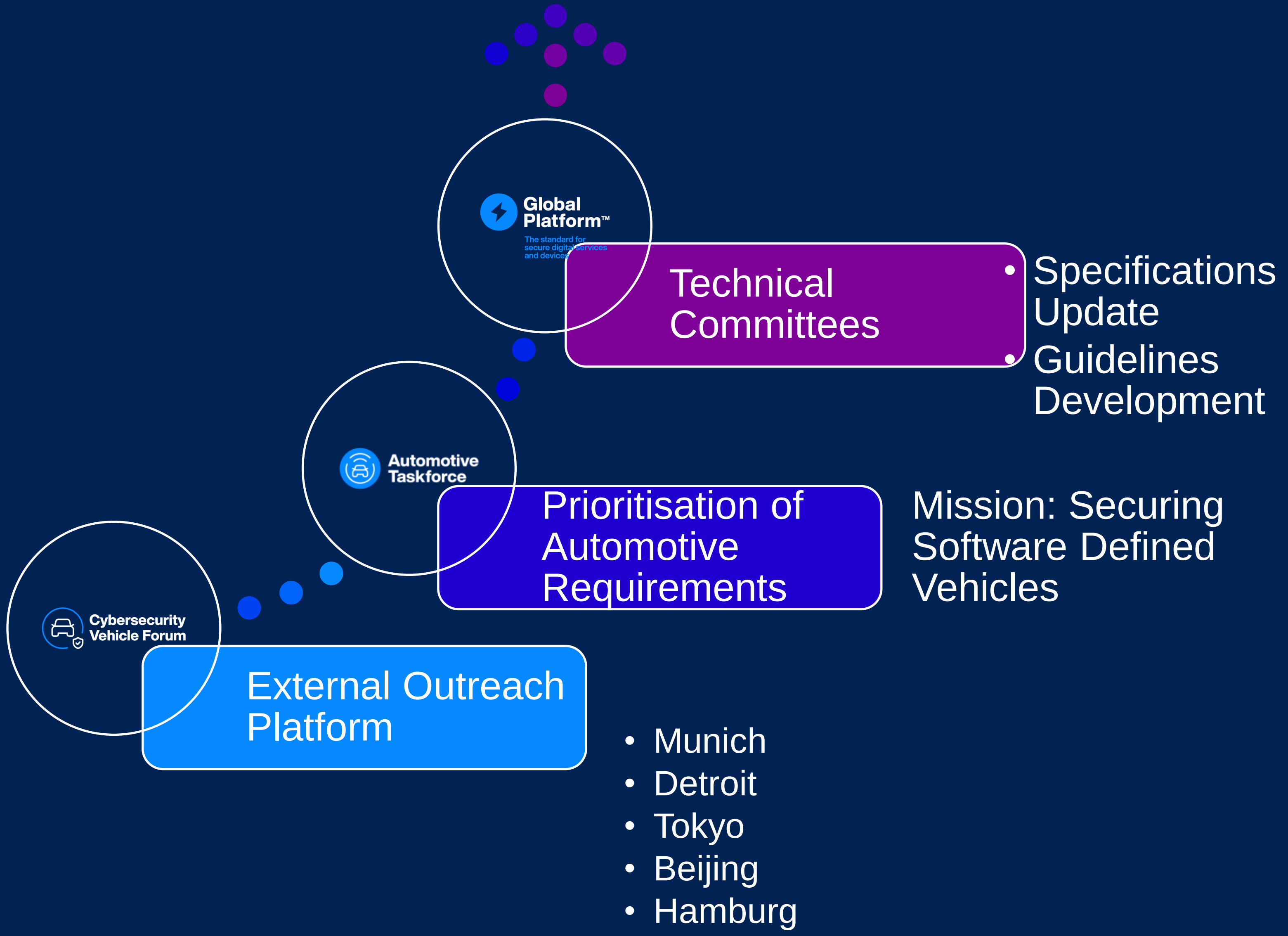


2:00pm	Welcome & Introductions	Richard Hayton, Chief Strategy and Innovation Officer, Trustonic & Chair of the TEE Committee and Automotive Task Force, GlobalPlatform
2:05pm	Overview of Measurement and Attestation RootS (MARS)	Tom Broström, Research Technical Director, Cyber Pack Ventures Inc. (CPVI)
2:35pm	Discussion of Trusted Platform Services (TPS)	Jeremy O'Donoughue, Director of Engineering, Qualcomm and TPS Committee Chair, GlobalPlatform
3:05pm	Summary of the key themes and topics discovered at previous Cybersecurity Vehicle Forum events, an outline of the agenda topics for the next events, and the plans for 2024	Francesca Forestieri, Automotive Lead, GlobalPlatform

How CSVF Input Drives Changes

SAE INTERNATIONAL
AUTOSAR
CAR CONNECTIVITY consortium
ETSI
AUTO-ISAC
Automotive Information Sharing and Analysis Center

Working with broader industry


Global Platform™
The standard for secure digital services and devices
Automotive Taskforce
Cybersecurity Vehicle Forum

Technical Committees

- Specifications Update
- Guidelines Development

Prioritisation of Automotive Requirements

Mission: Securing Software Defined Vehicles

External Outreach Platform

- Munich
- Detroit
- Tokyo
- Beijing
- Hamburg

CSVF Detroit 06 23

103 Participants

Cybersecurity Vehicle Forum

OEMS

CARIAD
A VOLKSWAGEN GROUP COMPANY

mazda

Ford

NISSAN
MOTOR CORPORATION

GM

STELLANTIS

HONDA

VOLVO

VIA

Tier 1s

APTIV

Motional

BOSCH

MITSUBISHI ELECTRIC
Changes for the Better

Continental
The Future in Motion

Panasonic
AUTOMOTIVE

DENSO
Crafting the Core

SUMITOMO ELECTRIC
Connect with Innovation

ETAS

Quon Technology

GARMIN

SwRI
SOUTHWEST RESEARCH INSTITUTE

HARMAN
A SAMSUNG COMPANY

ZF INDIA
Steering Success with Safety
ZF STEERING GEAR (INDIA) LIMITED

LUMINAR

Silicon & Solution Vendors

ANALOG DEVICES
AHEAD OF WHAT'S P

ST
life.augmented

Infineon

RENESAS
BIG IDEAS FOR EVERY SPACE

SAMSUNG
ELECTRONICS

Giesecke+Devrient

GP Solutions

NXP

PROVENRUN

Qualcomm

THALES
Building a future we can all trust

TRUSTONIC

Test Labs

riscure
Driving your security forward

財團法人電信技術中心
TELECOM TECHNOLOGY CENTER

UBIVELOX

Industry Organizations

AUTOSAR

SAE INTERNATIONAL

Global Platform™

Government

NIST

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

Universities

EASTERN MICHIGAN UNIVERSITY

Middlesex University

Broader Ecosystem

Applus+ laboratories

P3

CYBEATS

CYBER PACK VENTURES
Cyber Security Consulting for a Secure World

Rambus

CYMOTIVE TECHNOLOGIES

PQSHIELD

C2A security

Red Balloon Security

DEVICE AUTHORITY
Automating Zero Trust for IoT

INTEGRATING SECURE MOBILITY SOLUTIONS

EATON

SBD

flex

SONY

IOActive

High North Inc

TII Technology Innovation Institute

kaspersky

HORIBA MIRA

unify

Mimer

utimaco

Global Platform™

CSVF Tokyo 14 09 23

Cybersecurity Vehicle Forum

62 Participants

Automotive Value Chain

mazda

Automotive Suppliers

ALPSALPINE

eSoL

Crevavi

here

DENSO
Crafting the Core

MITSUBISHI ELECTRIC
Changes for the Better

Silicon & Solution Vendors

Giesecke+Devrient

infineon

REALTEK

socionext

ST
life.augmented

SYNOPSYS

TOSHIBA

GP Solutions

NXP

Qualcomm

TRUSTONIC

THALES
Building a future we can all trust

winbond
We Deliver

Test Labs

SGS

Industry Organizations

AUTOSAR

Global Platform™

Government

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

Universities

सी-डैक
CDAC
CENTER FOR DEVELOPMENT OF ADVANCED COMPUTING

Broader Ecosystem

BACTECH

MineSec

DNP

NEC

FeliCa Networks

NTT

NTT

fime

NTT Data
NTT DATA INTELLILINK Corporation

Rambus

Innovation Japan

SECOM

Inventec
Inventec Appliances

SoftBank

SONY

Intralink

Linaro

TOMOWEL | Kyodo Printing Co., Ltd.

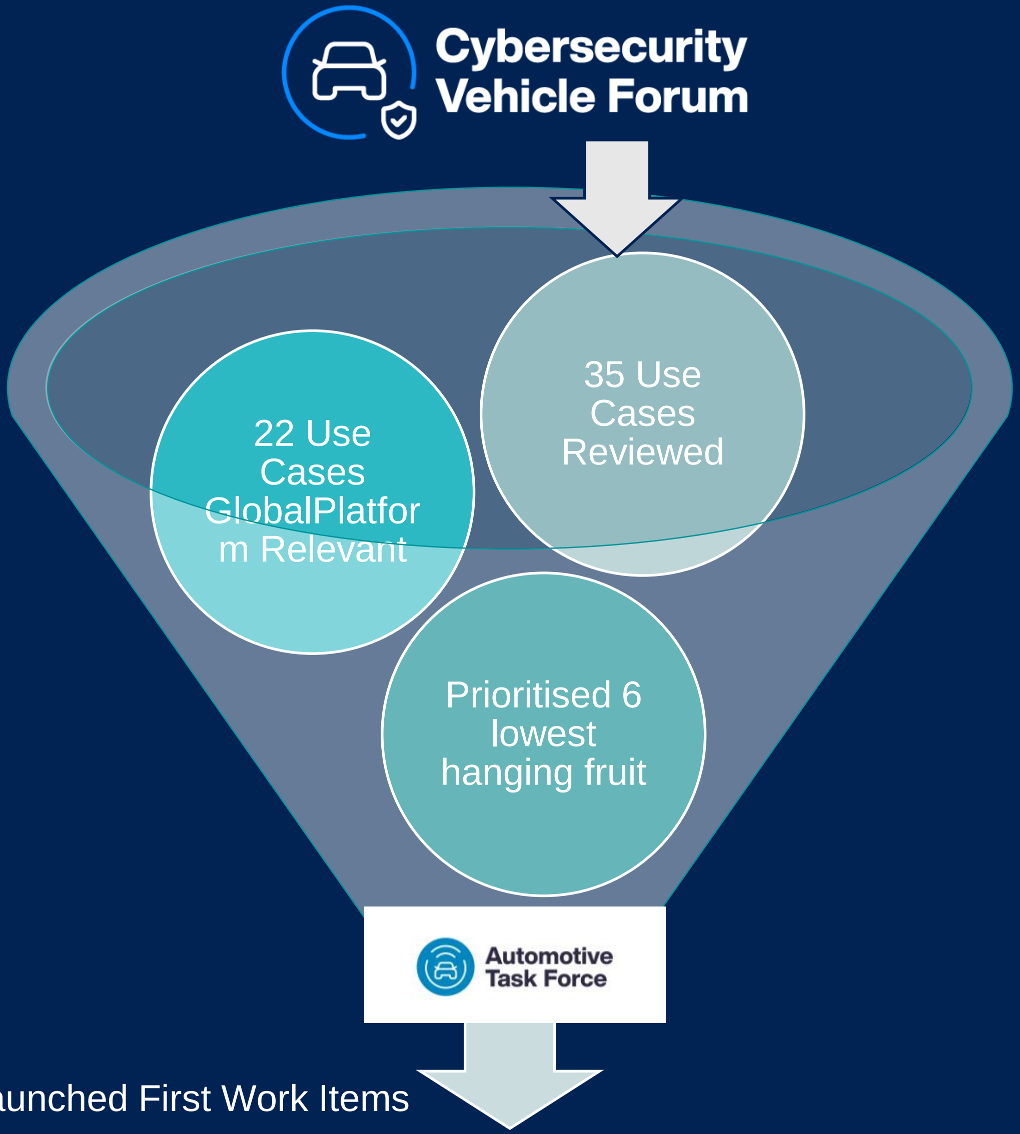
Ubiquitous AI

mastercard

VECTOR

Global Platform™

GlobalPlatform Automotive Activities: First Year


Cybersecurity Vehicle Forum
35 Use Cases Reviewed
22 Use Cases GlobalPlatform Relevant
Prioritised 6 lowest hanging fruit
Automotive Task Force

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 Whitepapers

Global Platform™
The standard for secure digital services and devices

2022

Cybersecurity in Automotive

GLOBALPLATFORM'S AUTOMOTIVE TASK FORCE

Global Platform®

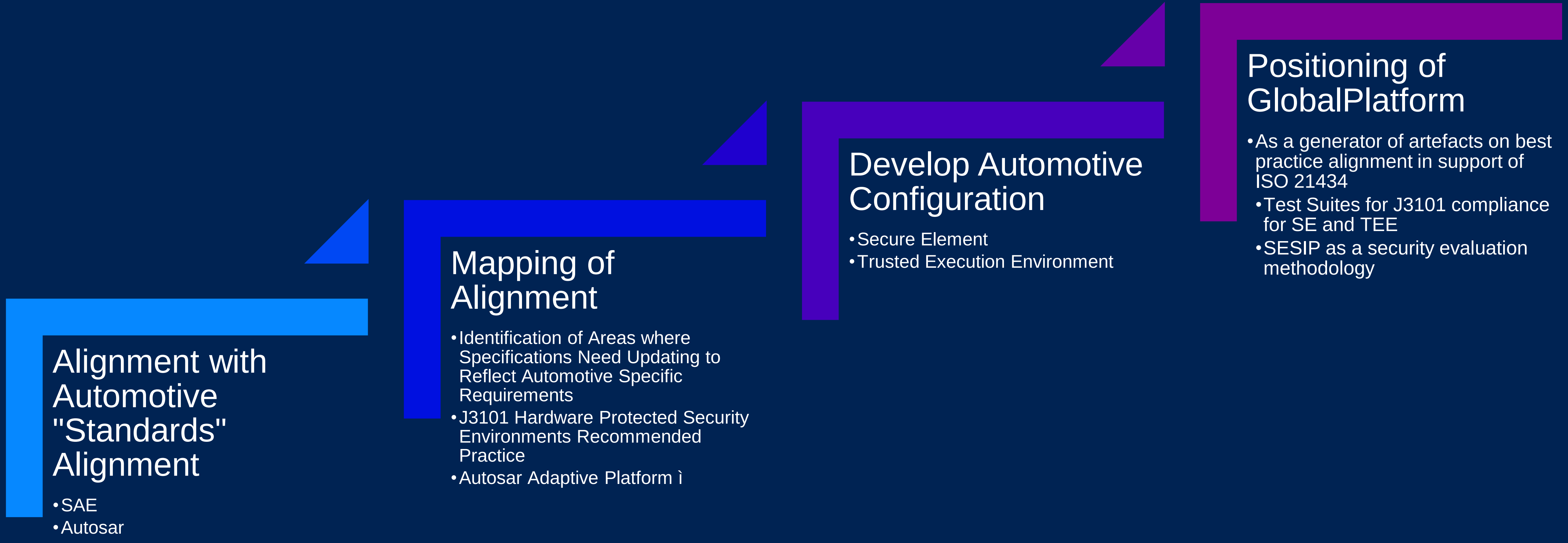
Autom
Task F

GlobalPlatform Technology

Trust & Security in Automotive Systems

COMING SOON!

Ongoing Strategy…



Alignment with Automotive "Standards" Alignment

- SAE
- Autosar

Mapping of Alignment

- Identification of Areas where Specifications Need Updating to Reflect Automotive Specific Requirements
- J3101 Hardware Protected Security Environments Recommended Practice
- Autosar Adaptive Platform ì

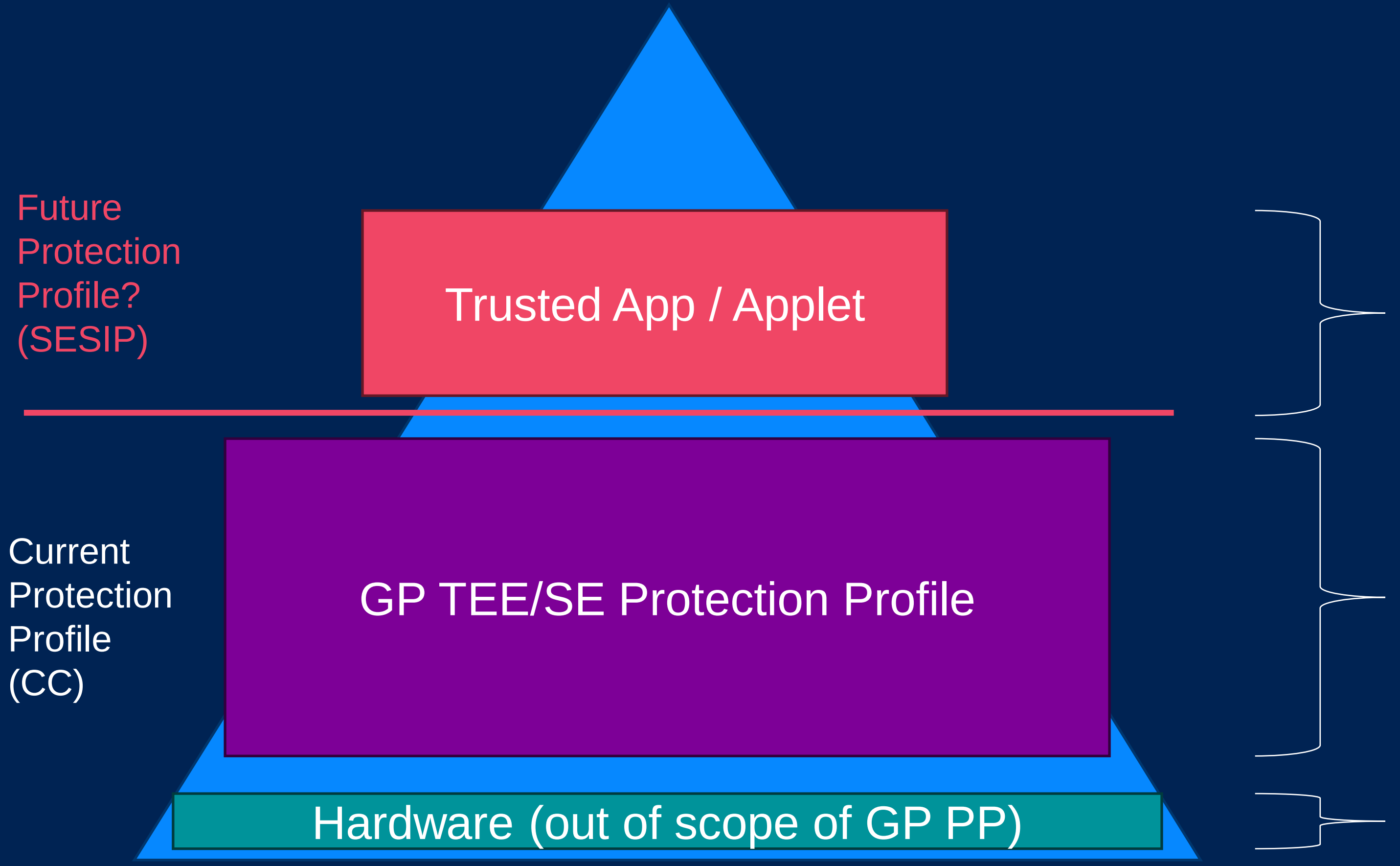
Develop Automotive Configuration

- Secure Element
- Trusted Execution Environment

Positioning of GlobalPlatform

- As a generator of artefacts on best practice alignment in support of ISO 21434
  - Test Suites for J3101 compliance for SE and TEE
  - SESIP as a security evaluation methodology

SAE J3101 Mapping

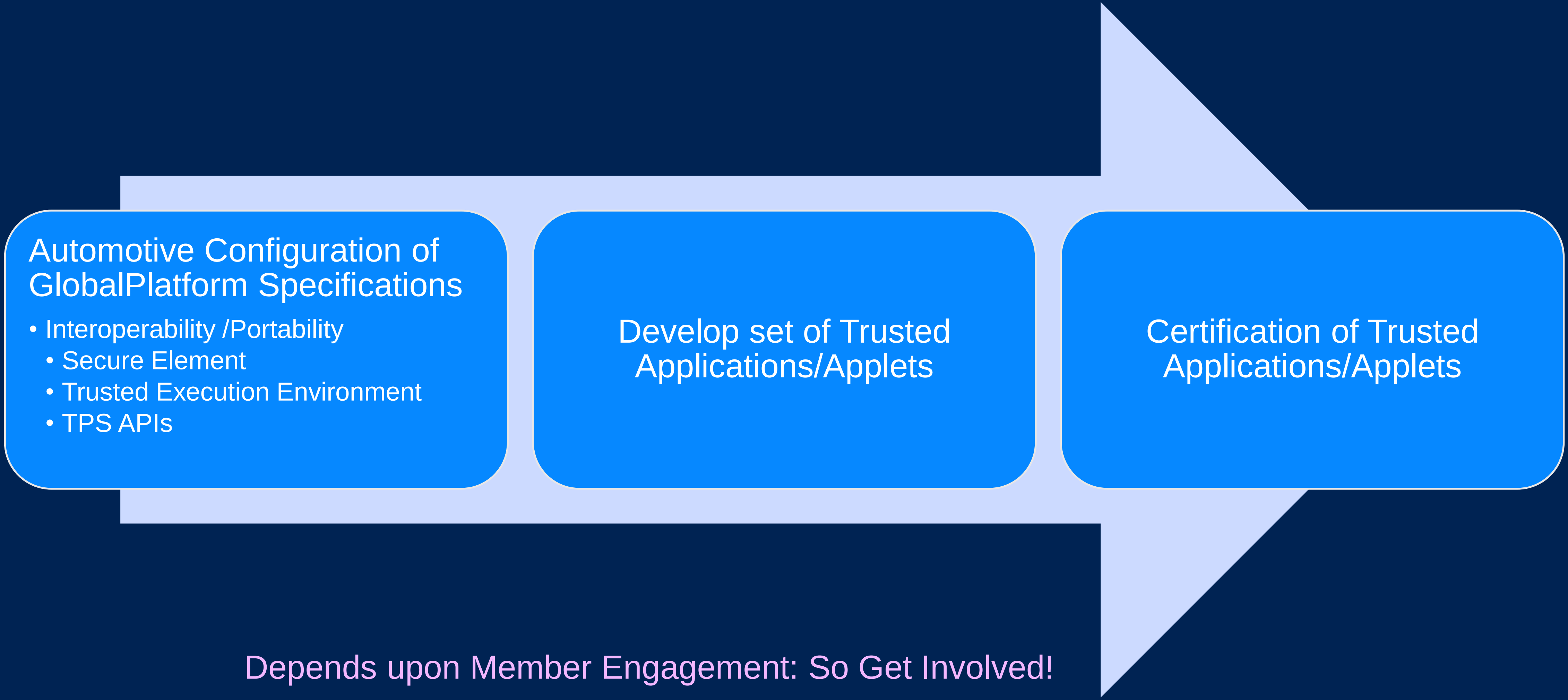

Future Protection Profile? (SESIP)
Trusted App / Applet
Current Protection Profile (CC)
GP TEE/SE Protection Profile
Hardware (out of scope of GP PP)

~32% of recommend requirements could be met by a TA/Applet

~65% of recommended requirements are met by use of GP technology

~3% of recommended requirements not covered by GP PPs

Automotive in GlobalPlatform: Outlook



Automotive Configuration of GlobalPlatform Specifications

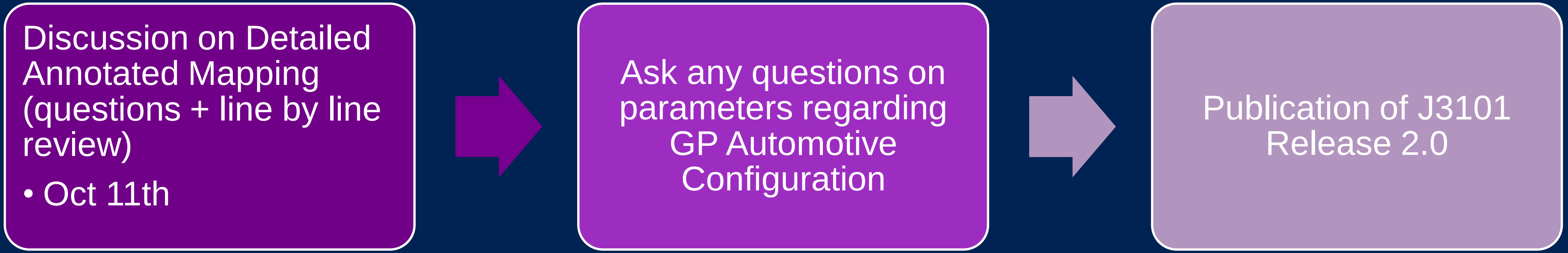
- Interoperability /Portability
  - Secure Element
  - Trusted Execution Environment
  - TPS APIs

Develop set of Trusted Applications/Applets

Certification of Trusted Applications/Applets

Depends upon Member Engagement: So Get Involved!

Next Dates for Technical Alignment

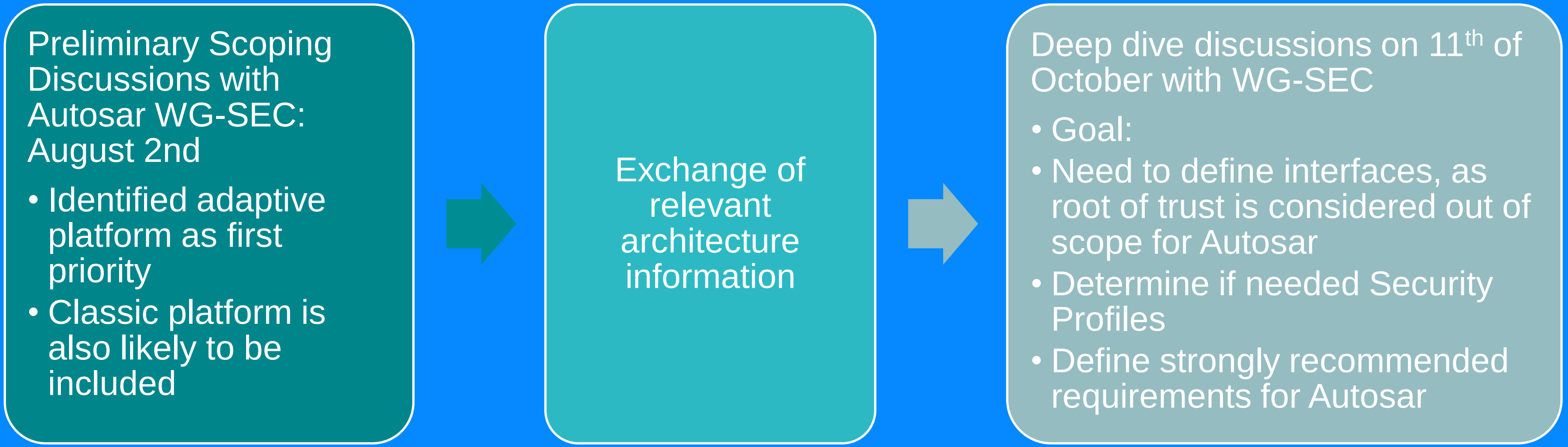


Discussion on Detailed Annotated Mapping (questions + line by line review)

- Oct 11th

Ask any questions on parameters regarding GP Automotive Configuration

Publication of J3101 Release 2.0



Preliminary Scoping Discussions with Autosar WG-SEC: August 2nd

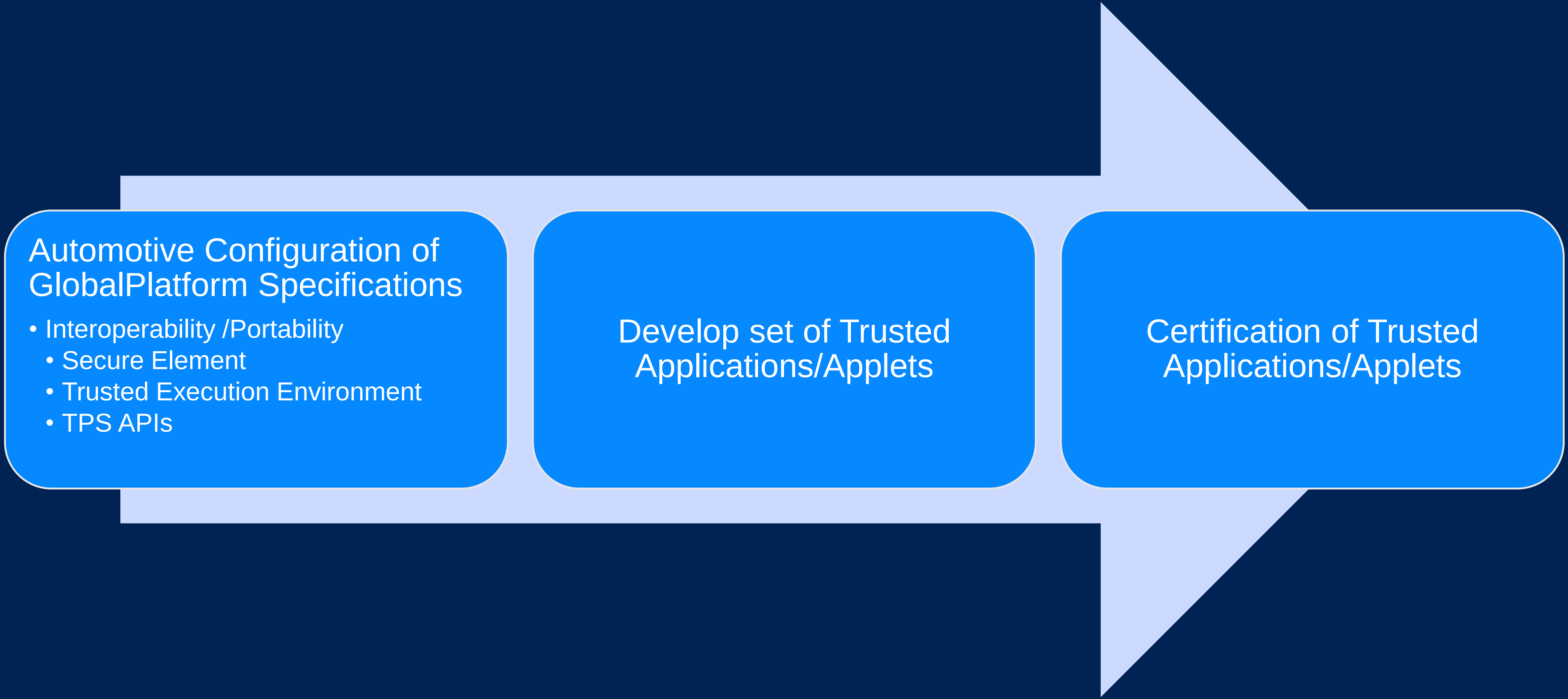
- Identified adaptive platform as first priority
- Classic platform is also likely to be included

Exchange of relevant architecture information

Deep dive discussions on 11th of October with WG-SEC

- Goal:
- Need to define interfaces, as root of trust is considered out of scope for Autosar
- Determine if needed Security Profiles
- Define strongly recommended requirements for Autosar

Automotive in GlobalPlatform: Phase 2



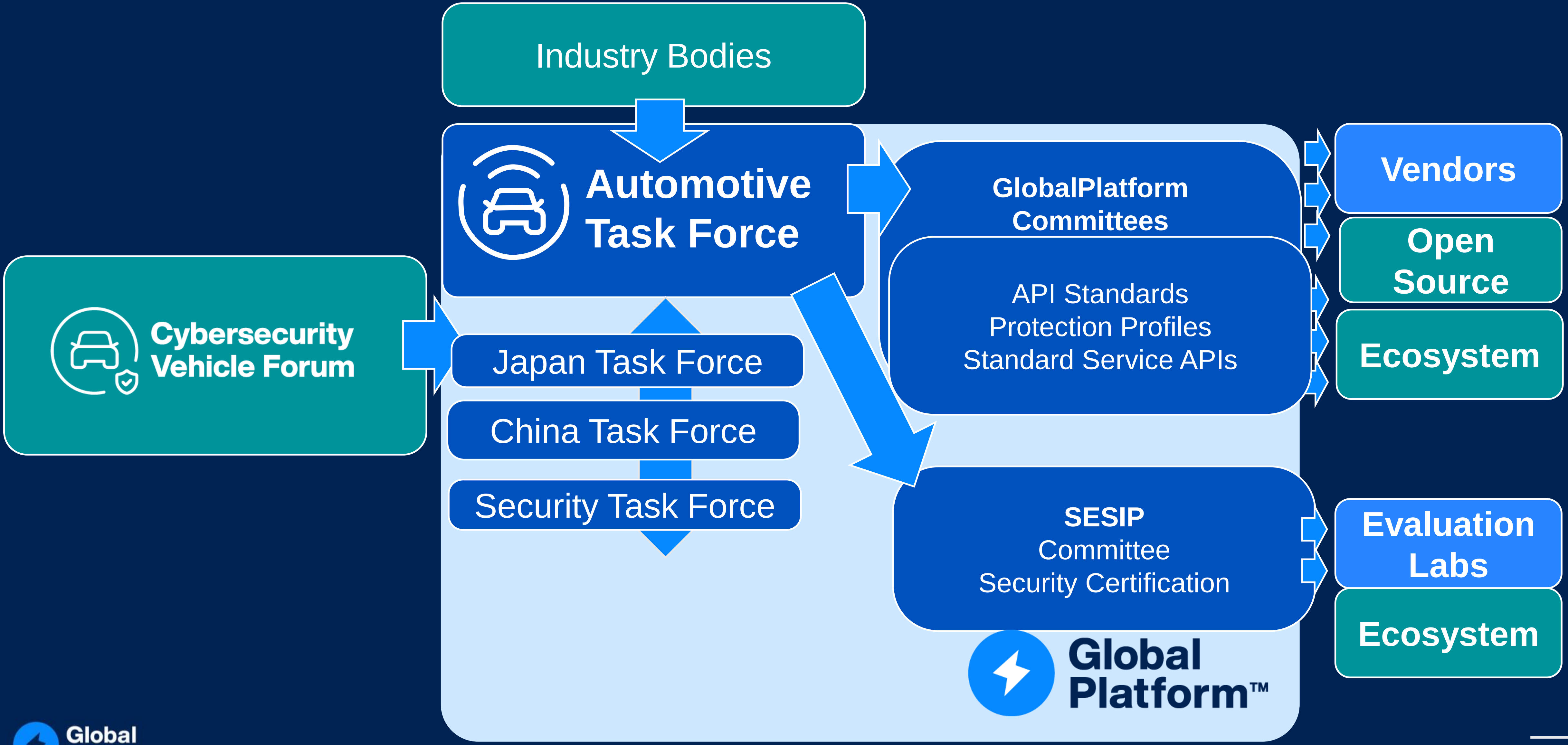
Automotive Configuration of GlobalPlatform Specifications

- Interoperability /Portability
  - Secure Element
  - Trusted Execution Environment
  - TPS APIs

Develop set of Trusted Applications/Applets

Certification of Trusted Applications/Applets

How GlobalPlatform Works for Automotive



Industry Bodies

Automotive Task Force

Cybersecurity Vehicle Forum

Japan Task Force

China Task Force

Security Task Force

GlobalPlatform Committees

API Standards
Protection Profiles
Standard Service APIs

SESIP
Committee
Security Certification

Vendors

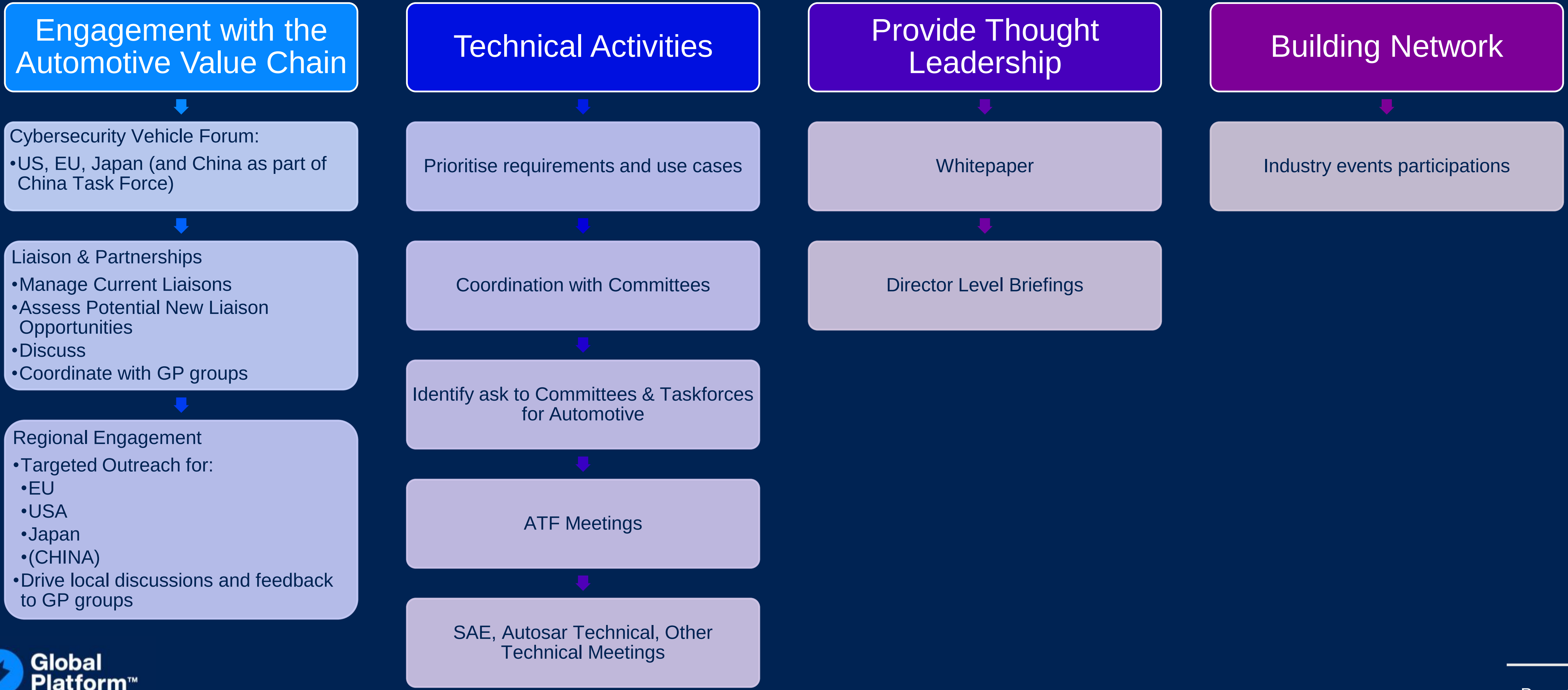
Open Source

Ecosystem

Evaluation Labs

Ecosystem

High Level View of Activities Planned for 2023/2024: Following the Pilasters of This Year



Engagement with the Automotive Value Chain

Cybersecurity Vehicle Forum:

- US, EU, Japan (and China as part of China Task Force)

Liaison & Partnerships

- Manage Current Liaisons
- Assess Potential New Liaison Opportunities
- Discuss
- Coordinate with GP groups

Regional Engagement

- Targeted Outreach for:
  - EU
  - USA
  - Japan
  - (CHINA)
- Drive local discussions and feedback to GP groups

Technical Activities

Prioritise requirements and use cases

Coordination with Committees

Identify ask to Committees & Taskforces for Automotive

ATF Meetings

SAE, Autosar Technical, Other Technical Meetings

Provide Thought Leadership

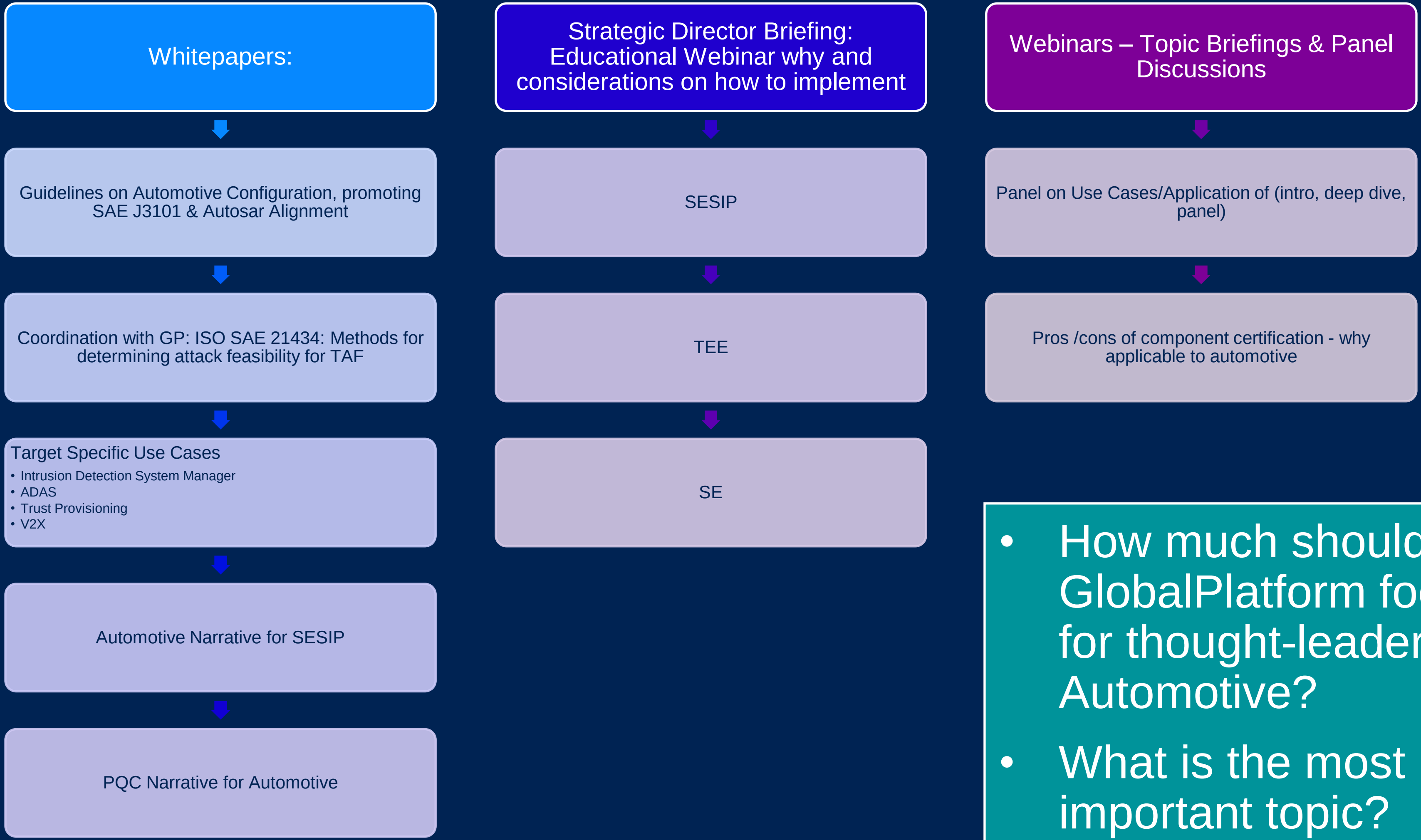
Whitepaper

Director Level Briefings

Building Network

Industry events participations

Potential Thought Leadership Themes



Whitepapers:

Guidelines on Automotive Configuration, promoting SAE J3101 & Autosar Alignment

Coordination with GP: ISO SAE 21434: Methods for determining attack feasibility for TAF

Target Specific Use Cases

- Intrusion Detection System Manager
- ADAS
- Trust Provisioning
- V2X

Automotive Narrative for SESIP

PQC Narrative for Automotive

Strategic Director Briefing: Educational Webinar why and considerations on how to implement

SESIP

TEE

SE

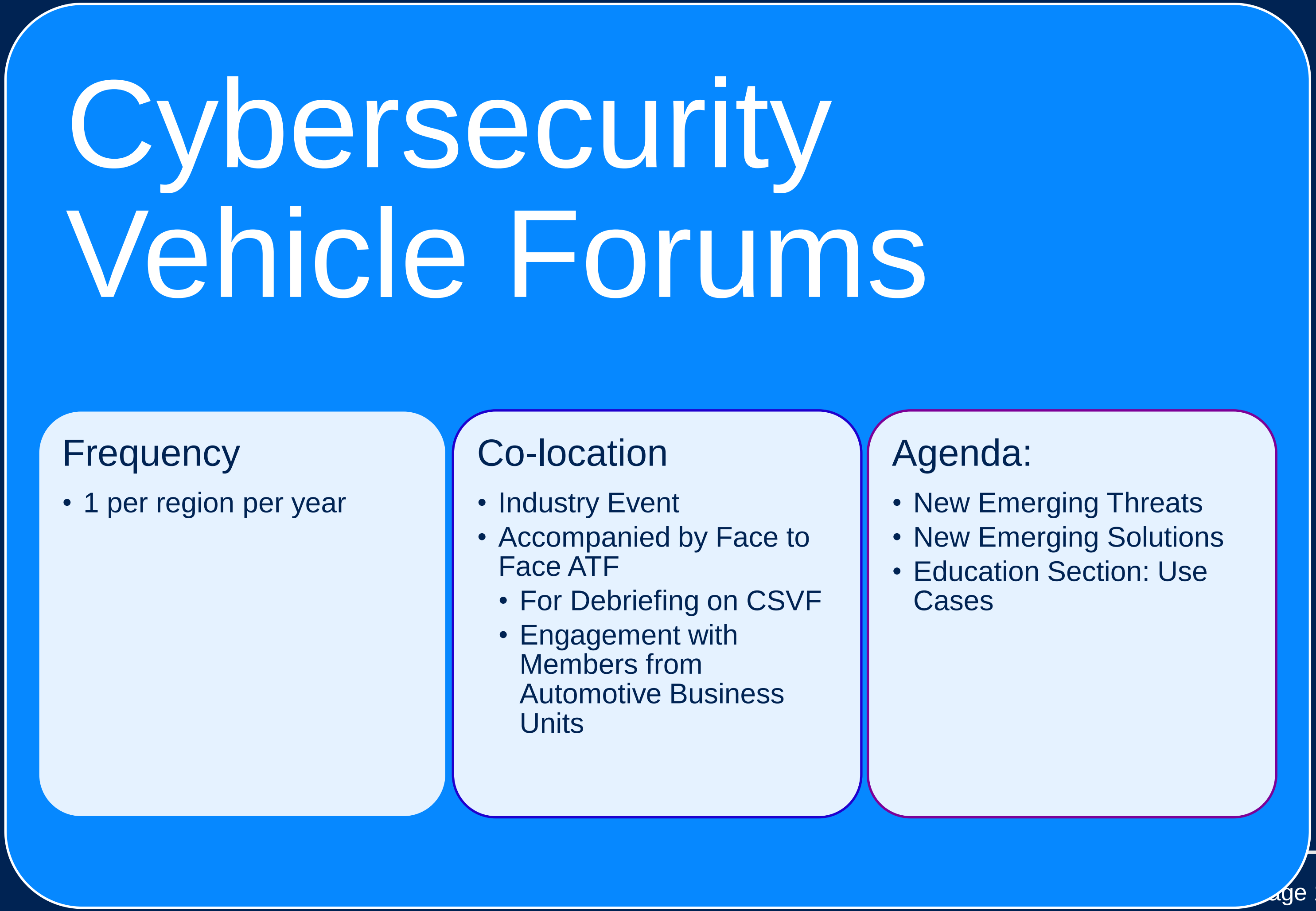
Webinars – Topic Briefings & Panel Discussions

Panel on Use Cases/Application of (intro, deep dive, panel)

Pros /cons of component certification - why applicable to automotive

- How much should GlobalPlatform focus on for thought-leadership in Automotive?
- What is the most important topic?

Cybersecurity Vehicle Forum 2.0



Cybersecurity Vehicle Forums

Frequency

- 1 per region per year

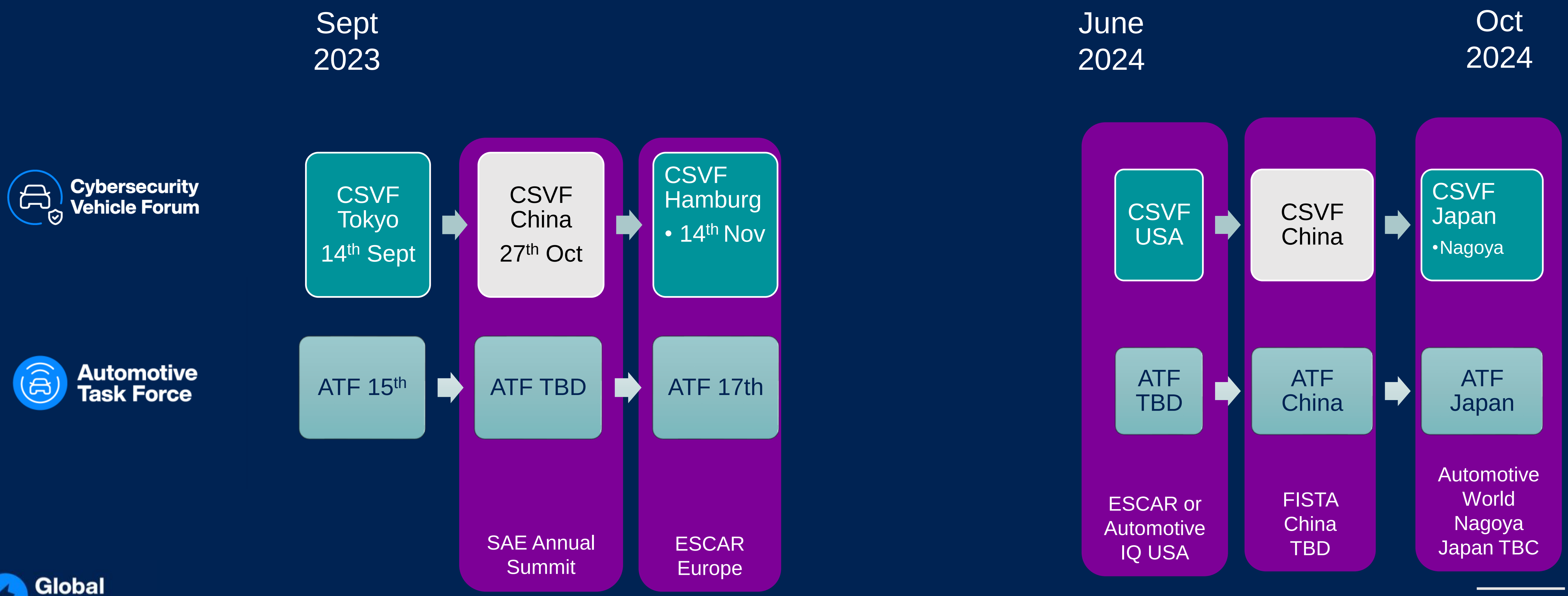
Co-location

- Industry Event
- Accompanied by Face to Face ATF
  - For Debriefing on CSVF
  - Engagement with Members from Automotive Business Units

Agenda:

- New Emerging Threats
- New Emerging Solutions
- Education Section: Use Cases

CSVF Face-to-Face Events



Sept 2023

June 2024

Oct 2024

Cybersecurity Vehicle Forum

Automotive Task Force

CSVF Tokyo 14th Sept → CSVF China 27th Oct → CSVF Hamburg
- 14th Nov

ATF 15th → ATF TBD → ATF 17th

SAE Annual Summit

ESCAR Europe

CSVF USA → CSVF China → CSVF Japan
- Nagoya

ATF TBD → ATF China → ATF Japan

ESCAR or Automotive IQ USA

FISTA China TBD

Automotive World Nagoya Japan TBC

Global Platform™

China Cybersecurity Vehicle Forum

24th of October (the day before the SAE China Summit)

In partnership with SAE China

CHINA SAE 中国汽车工程学会 China Society of Automotive Engineers

Beijing, China

13:30-17:30

Please register on the www.globalplatform.org/news/globalplatformevents

GlobalPlatform Overview

Automotive Security Use Cases

SESIP

New policies on cybersecurity in China and how that is impacting standardization

Cybersecurity Threats

Autosar China

EU Cybersecurity Vehicle Forum

November 14th (the day before ESCAR EU)

Hamburg, DE

10:00-17:00

Please register on the www.globalplatform.org/news/globalplatformevents

Fault Injection:

- Threats
- Trends

Updates on Post Quantum Crypto

New Emerging Security Solutions: Use Cases

GlobalPlatform Technology Focus:

- SESIP: Generating Artefacts for ISO 21434
- Trusted Platform Services
- Update on Automotive Configuration SAE J3101 & Autosar Compatibility

US Cybersecurity Vehicle Forum

TBC June 2024 (the day before ESCAR USA) OR May 22nd 2024 (the day after Automotive IQ)

Detroit, Michigan

10:00-17:00

Please register on the www.globalplatform.org/news/globalplatformevents

Fault Injection:

- Threats
- Trends

Updates on Post Quantum Crypto

New Emerging Security Solutions: Use Cases

GlobalPlatform Technology Focus:

- SESIP: Generating Artefacts for ISO 21434
- Trusted Platform Services
- Update on Automotive Configuration SAE J3101 & Autosar Compatibility

Japan Cybersecurity Vehicle Forum

TBD

Current Idea is

October 2024 (in conjunction with Automotive World Nagoya)

Nagoya, Japan

10:00-17:00

Automotive Security Use Cases

SESIP

Post Quantum Crypto Update

Cybersecurity Threats Landscape in Japan

Certification Lab Reports

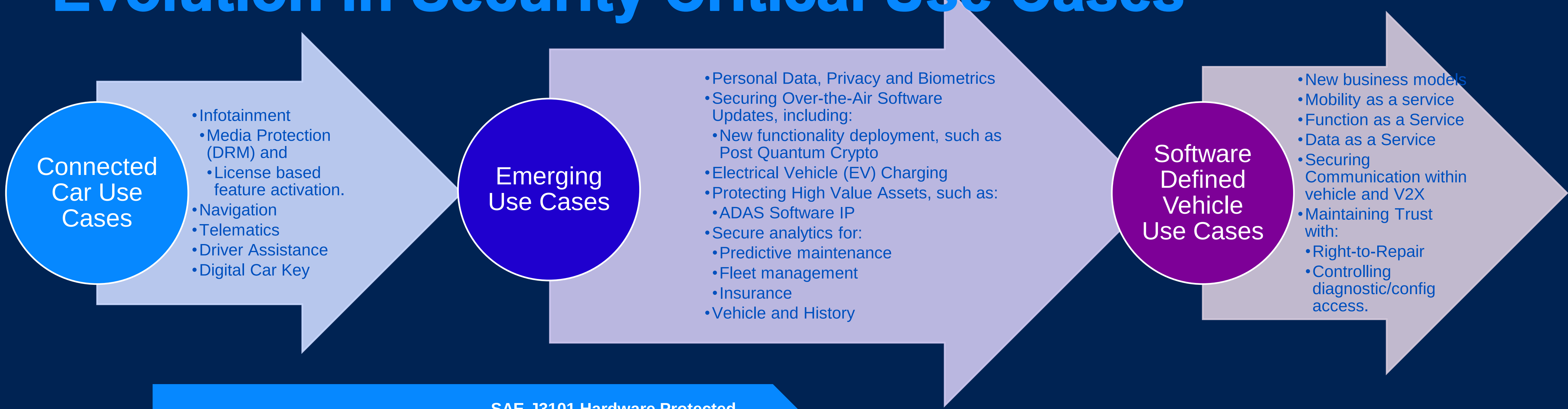
Synergies with Japanese Standardisation

Requirements for GlobalPlatform Automotive Configuration to foster compatibility in Japan

Global Platform™

Use Case Evolution: Towards SDV

Evolution in Security Critical Use Cases



Connected Car Use Cases

- Infotainment
  - Media Protection (DRM) and
    - License based feature activation.
- Navigation
- Telematics
- Driver Assistance
- Digital Car Key

Emerging Use Cases

- Personal Data, Privacy and Biometrics
- Securing Over-the-Air Software Updates, including:
  - New functionality deployment, such as Post Quantum Crypto
- Electrical Vehicle (EV) Charging
- Protecting High Value Assets, such as:
  - ADAS Software IP
- Secure analytics for:
  - Predictive maintenance
  - Fleet management
  - Insurance
- Vehicle and History

Software Defined Vehicle Use Cases

- New business models
- Mobility as a service
- Function as a Service
- Data as a Service
- Securing Communication within vehicle and V2X
- Maintaining Trust with:
  - Right-to-Repair
  - Controlling diagnostic/config access.

SAE INTERNATIONAL

SAE J3101 Hardware Protected Security Environments for Ground Vehicles

IPR Protection

Secure Diagnosis at the ECU level

Secure Logging

AUTOSAR

Classic Platform

- Crypto API, Key Management, Identity and Access Management, Trusted Platform

Adaptive Platform

- Key management, Cryptographic transformations, Dedicated certificate support

What are the use cases that pose the greatest interest for future needs in support of Software Defined Vehicles?

Join Us!

Follow GlobalPlatform Specifications

Become a GlobalPlatform Member and Optimise your roadmap

Contribute on Development of automotive Specifications within GP for:

- Ensure agility in deployment of common services
- Future proofing solutions
- Leverage mature and interoperable specifications for secure components as the foundation for cybersecurity
- Rely on externally validated certification program to ensure compliance with robustness and with desired security level

- Migration roadmaps for new requirements (Post Quantum Crypto, Security Regulation)
- Learn In advance about new regulations and technologies to ascertain how they can improve your business (e.g. SBOM, vulnerability disclosure)
- Obtain early visibility of standards development as the evolve
- Help shape the development of standards directly (ensuring that they answer your requirements)
- Leverage security evaluation methodologies

- Secure Element
- Trusted Execution Environments
- Trusted Platform Service APIs
- SESIP Evaluation Methodologies

Global Platform™

Detroit Polling Results

Polling Results Detroit CSVF 1/3

Are there any areas that you believe would be useful to address in greater detail in future GlobalPlatform guidelines?

1. Use Cases for different GlobalPlatform solutions
2. Security Evaluation Decisions
3. Protection Profiles

When will you require certification (SESIP, CC, FIPS, etc) in your specifications, RFQs, Proposals, etc:

1. Less than 5 years 7/15
2. Less than 10 years 3/15
3. Now 4/15
4. Never 1/15

Is solving the right keystore the right question to ask?

1. No 9/11
2. Yes 3/11

Do you think SESIP is a useful tool for automotive?

1. Yes, to generate evidence for 21434 (8/11)
2. Yes, to certify new solutions (2/11)
3. No, we will only be generating process information on cybersecurity for 21434 (1/11)

Polling Results Detroit CSVF 2/3

Do you think it is important for GlobalPlatform to have seamless alignment between SAE J3101 and AUTOSAR?

100%: Yes - clarity on compliance will benefit the entire industry

Do you think that hardware protected security environments (SAE J3101) will be useful in demonstrating compliance with ISO/SAE 21434?

100% Yes

Have you begun citing SAE J3101 in your specifications, RFQs, Proposals, etc.

1. No 16/22
2. Yes 5/22

J3101 mapping - Do you think implementation guidelines for hardware protected security environments will be useful for the industry?

- Yes comparability between products will help sourcing10/12
- Yes- other 1/12
- No 1/12

Do you think test suits to demonstrate compliance to J3101 will be useful for:

1. Yes for both SE and TEEs (16/19)
2. For Secure Elements (3/19)

Guidelines on Trust Management in Automotive - Do you believe security certification will become mandatory?

1. Yes - 3rd party lab (13/19)
2. Yes - Self certification (3/19)
3. No (3/19)

Polling Results Detroit CSVF 3/3

When will SDV approaches (software on standard compute) replace specialist parts for safety critical embedded MCUs:

1. 10 Years 15/27
2. 5 Years 7/27
3. Never 4/27
4. Now 1/27

How are you planning for regional differences in post quantum today?

1. I don’t know yet but need to decide 6/11
2. One solution with multiple configurations for different regions 3/11
3. Different solutions for different regions 1/11
4. Post quantum is not on my agenda at all 1/11

Do you believe that GlobalPlatform solutions would be beneficial in supporting the V2X Certificate lifecycle?

1. Yes (8/9)

Global Platform™

The standard for secure digital services and devices

→globalplatform.org

Potential Regional Synergies

China Automotive Technology and Research Center (CATARC) is a science research institute established in 1985 to meet China's need of managing the automotive industry and now belongs to SASAC (State-owned Assets Supervision and Administration Commission of the State Council).

- CATARC is the centralized technical organization of the auto industry and the technical supporting body to the relevant national government departments. With the independent and neutral role, we firmly take the development road of "guided by science and technology, focusing on service to the industry and supported by commercialization"
- Also responsible for the C-Auto-ISAC: China Automotive Information Security Sharing Analysis Center
- CATARC Europe Testing & Certification GmbH supporting automotive industry in Europe in its dealings with Chinese Market and Entry Regulations
- CPG is a Subsidiary providing test tracks and facilities both for passenger cars and commercial vehicles, our core services are road test and laboratory service, including regulation tests of whole vehicles and auto parts, R&D and export certification test.

Japan's Automotive Cybersecurity Information Sharing Center

- 1.Deterrence of the occurrence of security incidents and the spread of damage
- 2. Planning, planning and support of cyber security measures
- 3. Planning, planning and support of measures for the development of cyber security human resources
- 4. Support for system development
- 5. External cooperation

Japanese Engineering Standardisation for Automotive (under FISTA Organisation)

Proposed Meeting Schedule

	GP Meetings	ATF			CSVF				
		ATF F2F	ATF Working Mtg	ATF Update Virtual	Europe	USA	Japan	China	CSVF Virtual update
Sep-23			TBD	26th			14th		25th
Oct-23								SAE China 27th	
Nov-23	6th Athens	17th Hamburg			ESCAR 14th Hamburg				
Dec-23									
Jan-24				16th					23rd
Feb-24									
Mar-24	GP Spring TBD								
Apr-24				16th					?
May-24									
Jun-24	Technical Roadmap TBD EU	x				ESCAR Detroit TBD			
Jul-24				16th					
Aug-24									
Sep-24	Board Strategy Meeting TBD								TBD
Oct-24		x					JSAE Nagoya TBD		
Nov-24									

Global Platform™

Promotion & Synergies

	Speaking Opportunities				Other Relevant Events TBD				
	Europe	USA	Japan	China	Europe	USA	Japan	China	New Regions
Sep-23	14-16 2024 FISTA World Mobility Summit				26-28th AVCC Cambridge				
Oct-23						17-18 AutoIsac California	25-27 Automotive World Nagoya		
Nov-23	27th-30th AutoTech Munich				27-30 Munich Automotive IQ		EdgeTech+ in Yokohama		
Dec-23									
Jan-24									
Feb-24					26-29th Mobile World Congress, Barcelona				
Mar-24									
Apr-24					Embedded World Europe 9-11th	18-20 SAE WCX Detroit			
May-24						19-21 Detroit Automotive IQ	EVTeC Japan JSAE		
Jun-24					AutoIsac Europe Summit	19-21 Autotech Detroit	Autosar AOC Tokyo 11/12		
Jul-24							J-autoisac Japan Cybersecurity Forum	FISTA China	
Aug-24									
Sep-24									?
Oct-24									
Nov-24									

Global Platform™

Next Steps: Regional Engagement

Potential Regional Synergies

JasPar

J-Auto-ISAC
Japan Automotive Information Sharing and Analysis Center

JSAE

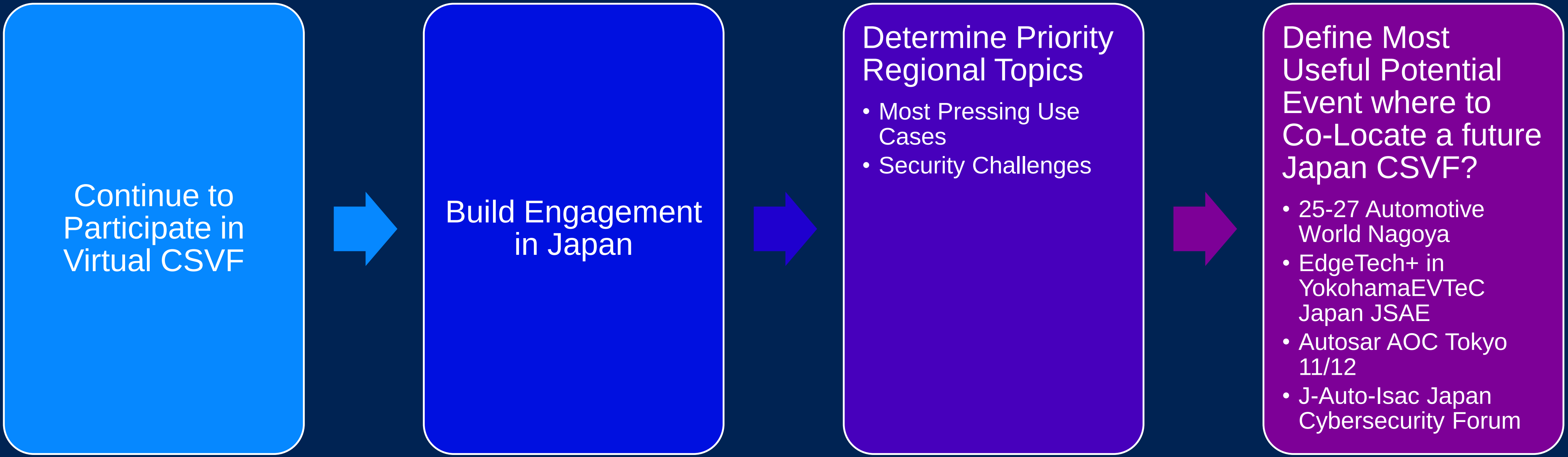
Jaspar Information Exchange

- 2nd Round of Meetings: 15/09/23

Japan's Automotive Cybersecurity Information Sharing Center

Japanese Engineering Standardisation for Automotive

Future Cybersecurity Vehicle Forums



Continue to Participate in Virtual CSVF

Build Engagement in Japan

Determine Priority Regional Topics

- Most Pressing Use Cases
- Security Challenges

Define Most Useful Potential Event where to Co-Locate a future Japan CSVF?

- 25-27 Automotive World Nagoya
- EdgeTech+ in YokohamaEVTeC Japan JSAE
- Autosar AOC Tokyo 11/12
- J-Auto-Isac Japan Cybersecurity Forum

Topics for Discussion

GlobalPlatform Automotive Use Cases

- Secure Components and eSE
- Trusted Execution Environments
- In-car payments
- Biggest Opportunities to Support Secure Component Evolution to Fit Automotive Use Cases

Secure Evaluation Methodology:

- SESIP Certification in Support of UNECE Cybersecurity Regulations?

ISO 21434:

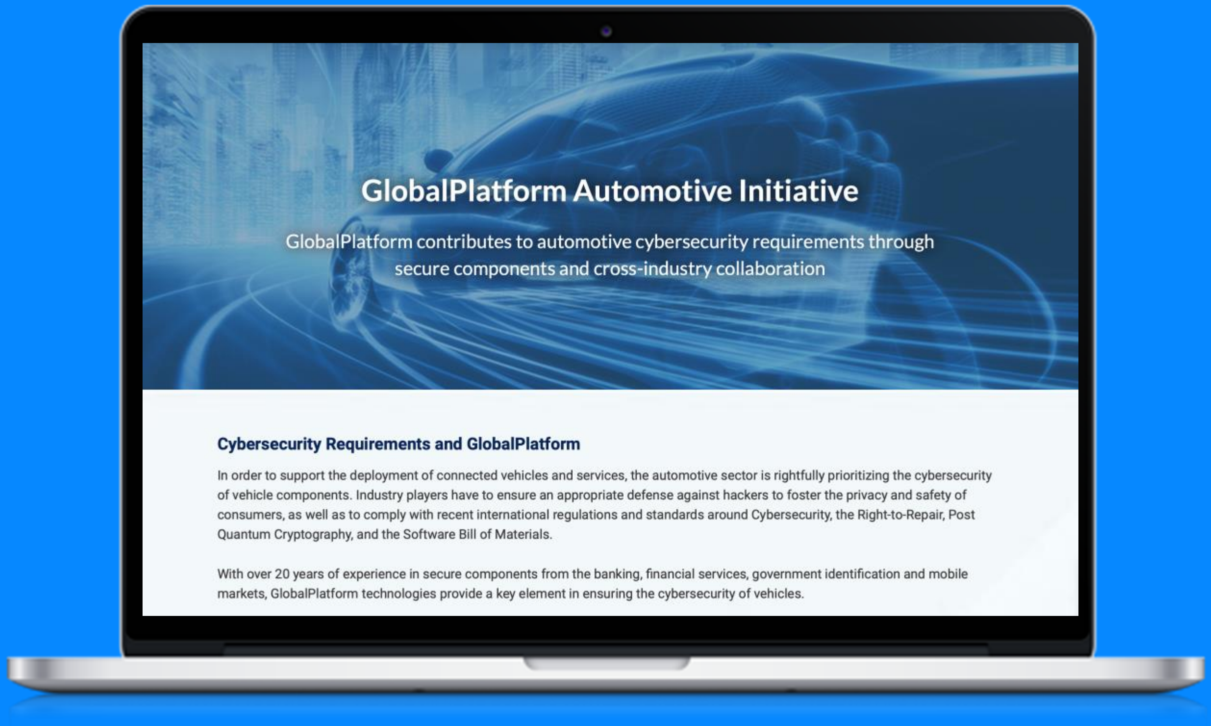
- How to Drive Security Best Practices for Products?

Autosar

- How to best facilitate security robustness and compatibility of hardware trust anchors?

Specific Japanese Market Requirements and Use Cases

Get Involved



GlobalPlatform Automotive Initiative

GlobalPlatform contributes to automotive cybersecurity requirements through secure components and cross-industry collaboration

Cybersecurity Requirements and GlobalPlatform

In order to support the deployment of connected vehicles and services, the automotive sector is rightfully prioritizing the cybersecurity of vehicle components. Industry players have to ensure an appropriate defense against hackers to foster the privacy and safety of consumers, as well as to comply with recent international regulations and standards around Cybersecurity, the Right-to-Repair, Post Quantum Cryptography, and the Software Bill of Materials.

With over 20 years of experience in secure components from the banking, financial services, government identification and mobile markets, GlobalPlatform technologies provide a key element in ensuring the cybersecurity of vehicles.

www.globalplatform.org

Contact Us

Membership:
membership@globalplatform.org

PR Contact:
pressoffice@globalplatform.org
Tel: +44 (0) 113 350 1922

Questions:
automotive@globalplatform.org

Twitter
@GlobalPlatform_

YouTube
GlobalPlatformTV

LinkedIn
GlobalPlatform

WeChat
GlobalPlatform China

YouKu
GlobalPlatform

GitHub
GlobalPlatform.GitHub.com

GlobalPlatform™

Global Platform™

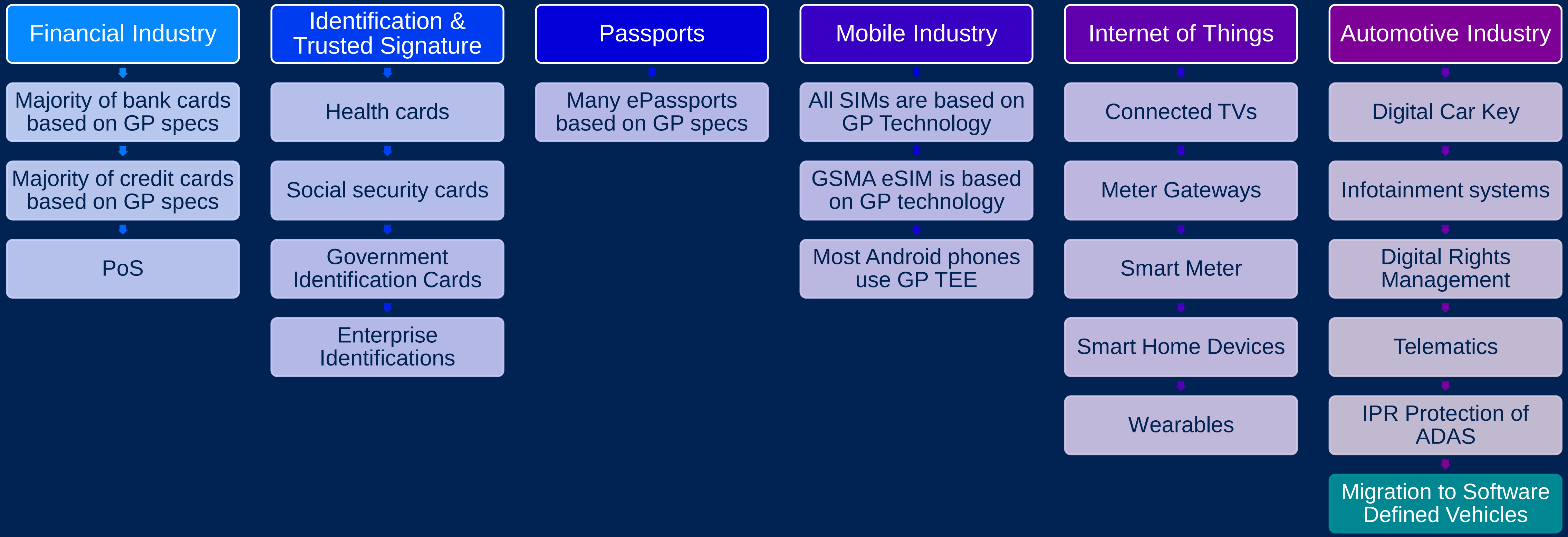
GlobalPlatform: Overview

Francesca Forestieri,
Automotive Lead for GlobalPlatform

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
- Majority of bank cards based on GP specs
- Majority of credit cards based on GP specs
- PoS

Identification & Trusted Signature
- Health cards
- Social security cards
- Government Identification Cards
- Enterprise Identifications

Passports
- Many ePassports based on GP specs

Mobile Industry
- All SIMs are based on GP Technology
- GSMA eSIM is based on GP technology
- Most Android phones use GP TEE

Internet of Things
- Connected TVs
- Meter Gateways
- Smart Meter
- Smart Home Devices
- Wearables

Automotive Industry
- Digital Car Key
- Infotainment systems
- Digital Rights Management
- Telematics
- IPR Protection of ADAS
- Migration to Software Defined Vehicles

GlobalPlatform specifications are publicly available for use on a royalty-free basis.

Global Platform®

GlobalPlatform Members

AMERICAN EXPRESS
ANALOG DEVICES AHEAD OF WHAT'S POSSIBLE™
Applus⊕
arm
AT&T
Bundesamt für Sicherheit in der Informationstechnik
BCTC 银行卡检测中心 BANK CARD TEST CENTER
cisco
T · ·

ERICSSON
FeliCa Networks
fime
Galitt
G+D Mobile Security
HID

HUAWEI
IDEMIA augmented identity
infineon
NTT
NXP

ORACLE
orange
QUALCOMM
SAMSUNG
ST life.augmented

THALES
T Mobile
TRUSTONIC
verizon✓
VISA
winbond

ANSECURITY
COMPRION
OPL Lab
riscure
SGS brightsight
SERMA SAFETY & SECURITY
TRUSTCB TRUST AND VERIFY
FINGERPRINTS
HONOR
TOSHIBA
財團法人資訊工業策進會 INSTITUTE FOR INFORMATION INDUSTRY
kaspersky
UL
VALID

BACTECH
CARIAD A VOLKSWAGEN GROUP COMPANY
CB
DISCOVER
DNP
楚天龙 CHUTIAN DRAGON
cea leti
DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA
东信和平 EASTCOMPEACE
FEITIAN WE BUILD SECURITY

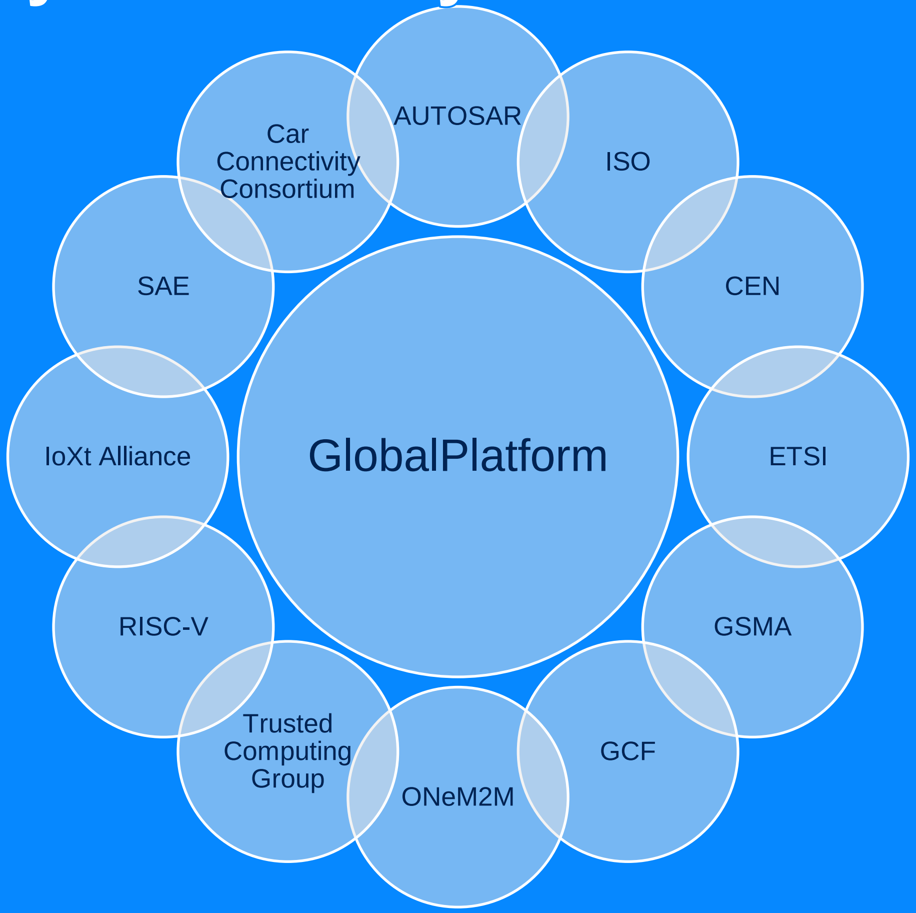
FORTRESS
Goldpac
GOODIX 汇顶科技
intel
INTERNET OF TRUST
JCB
Kigen
Kona i
MASKTECH
MK smart Smart Digital Security
MoneTECH
NEXTENDIS

PQSHIELD THALES
Rambus
SAFEPAY
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
TELUS

TTL
TOPPAN
truphone
UBIVELOX
Watchdata
xardpay
XCURE CORP.
mi
zwipe

□ Recent Members
Specifically for Automotive

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
One Card, One Asia on the Silk Road

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

mobey forum

TRUSTED® COMPUTING GROUP

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

RISC-V®

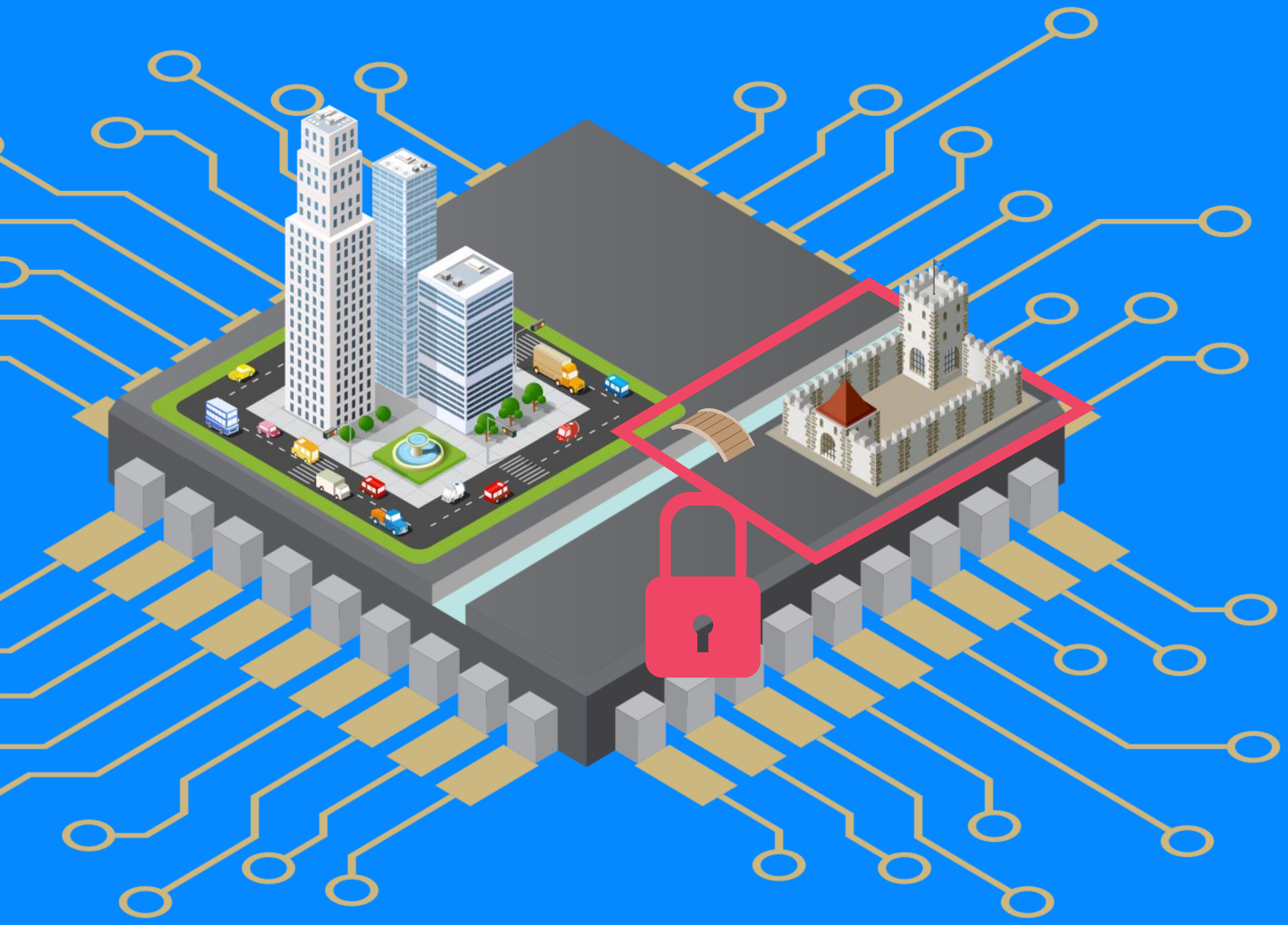
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

oneM2M
The IoT Standard

SAE INTERNATIONAL

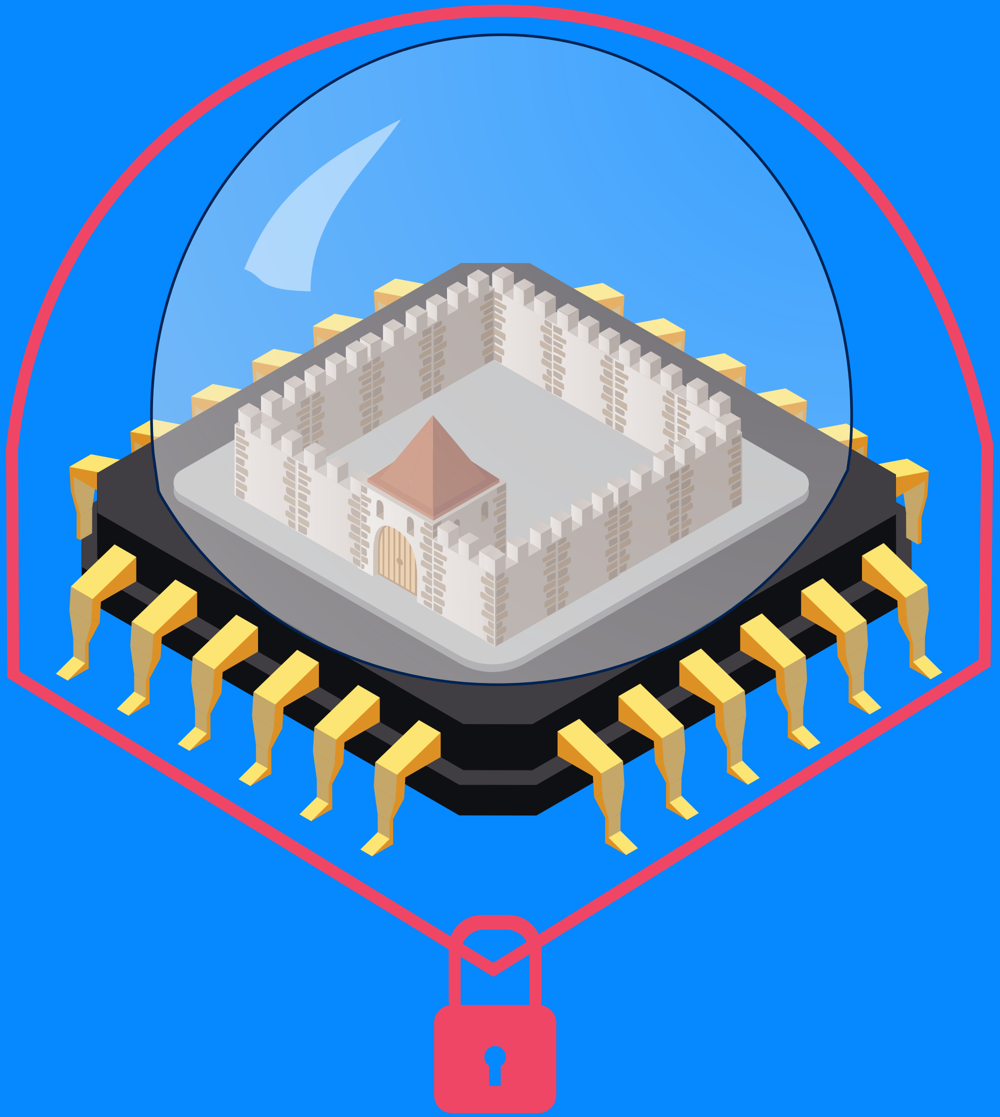
TCA
TRUSTED CONNECTIVITY ALLIANCE

GlobalPlatform
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
- Runs a full operating system providing standardized APIs and functions
- Commonly used in Mobile Devices, Automotive and IoT
- 3rd party Security Certification
- Full support for App and OS update over the air

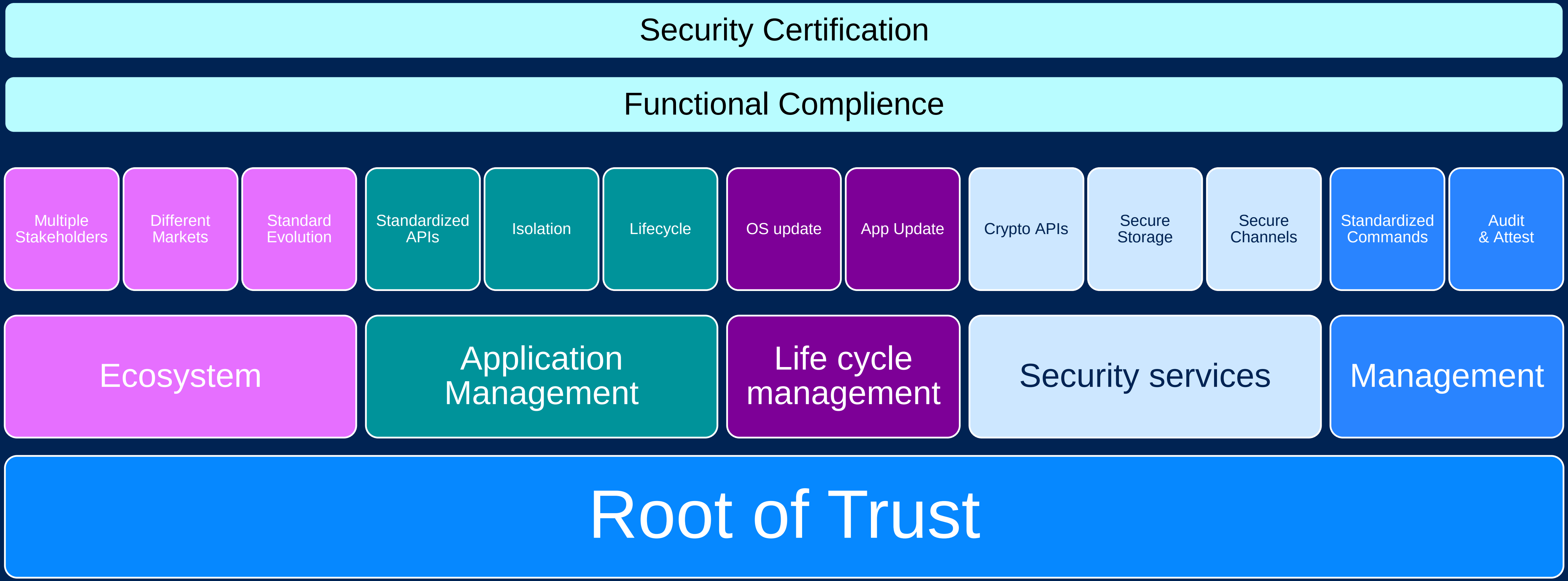
GlobalPlatform Secure Element



- 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
- 3rd party Security Certification
- Full support for App and OS update over the air

Why GlobalPlatform Platform is More than Traditional HSMs or SHE+?

Much like AUTOSAR or POSIX there is much more than just “running code” to providing a platform



Security Certification

Functional Complience

Multiple Stakeholders | Different Markets | Standard Evolution | Standardized APIs | Isolation | Lifecycle | OS update | App Update | Crypto APIs | Secure Storage | Secure Channels | Standardized Commands | Audit & Attest

Ecosystem | Application Management | Life cycle management | Security services | Management

Root of Trust

GP Protection Profiles

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

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

Certification

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

Publication

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

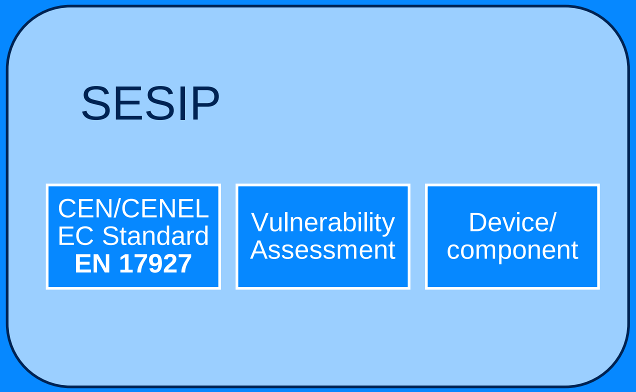
Common Criteria

SESIP

Global Platform™

Evaluation Methodology

SESIP



Structured Security Methodology

Designed to not require security expertise for use

Functional Requirements	Assurance Requirements

Global Platform™

GlobalPlatform specifications are freely available

GlobalPlatform Specifications: https://globalplatform.org/specs-library/

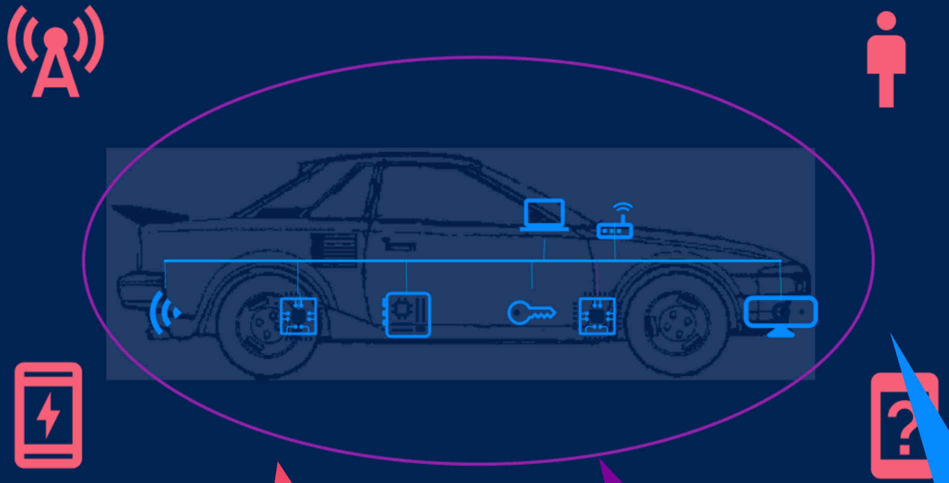
Secure Element	•https://globalplatform.org/specs-library/?filter-committee=se
Trusted Execution Environments	•https://globalplatform.org/specs-library/?filter-committee=tee
Root of Trust Definitions	•https://globalplatform.org/specs-library/root-of-trust-definitions-and-requirements-v1-1-gp-req_025/
Trusted Platform Services	•https://globalplatform.org/specs-library/?filter-committee=tps
Trusted Platform Services APIs	•Open Source Implementation Available Now: •https://github.com/GlobalPlatform/TPS-API-Reference-Implementations
Security Evaluation Methodology SESIP	•https://globalplatform.org/specs-library/#collapse-17

GlobalPlatform™

Trust Management with Secure Components

Jeremy O'Donoghue,
GlobalPlatform Chair Trusted Platform Services Committee

Walled Garden

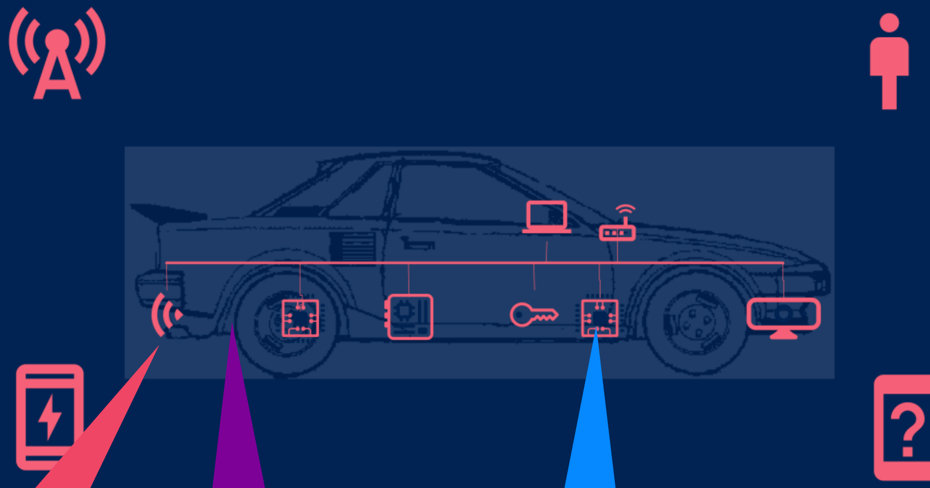


Everything outside the perimeter is untrusted

Physical protection or firewall

Everything inside the firewall is trusted

Zero Trust



Everything is untrusted

Each component verifies that others are trustworthy

Interaction operates on “least privilege” basis

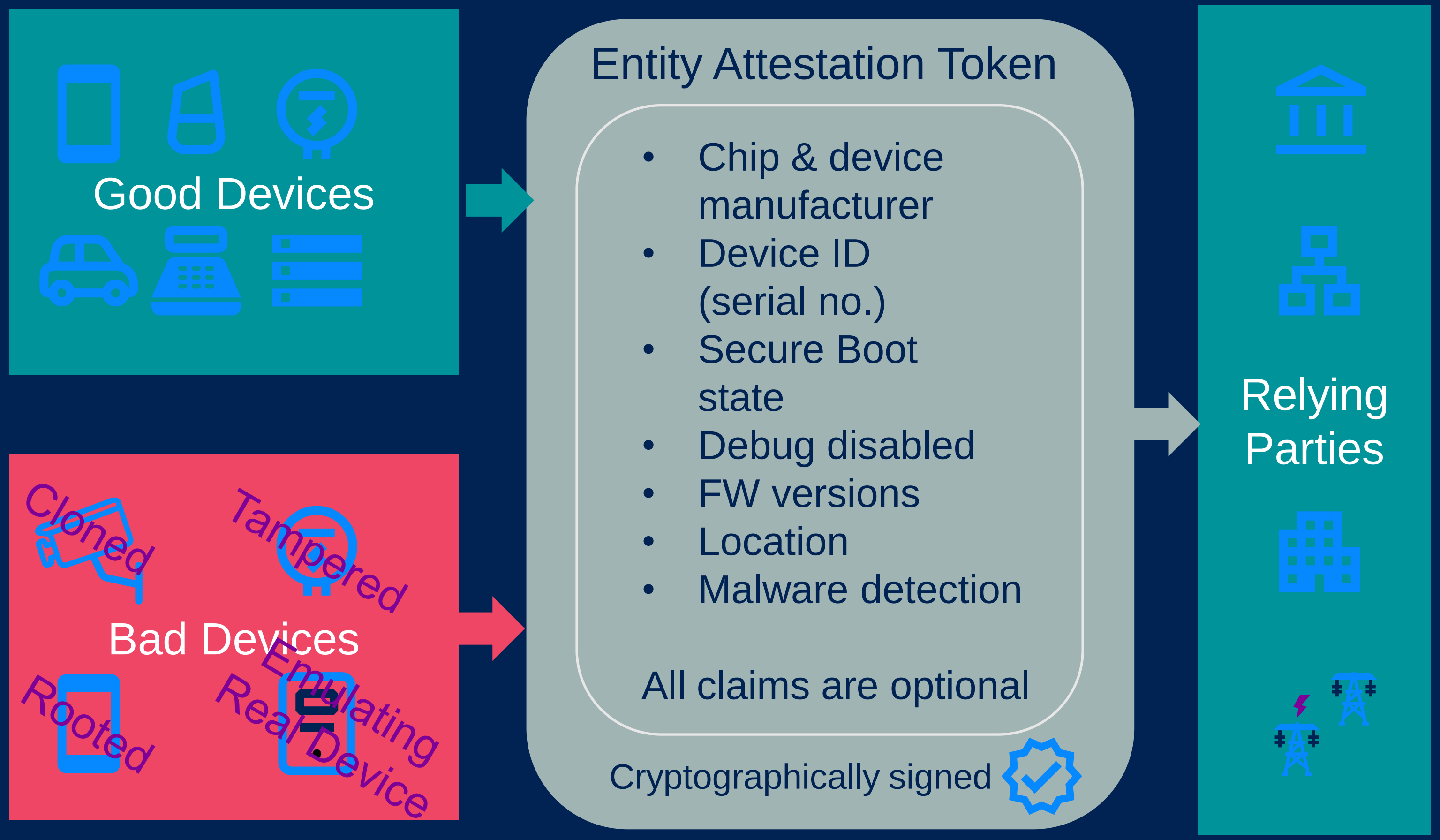
Global Platform™

What is trust?

Requirements

- Strong (cryptographic) identity for each entity.
- Mechanisms to control device state
  - Secure boot (only load authentic FW)
  - Anti-rollback (prevent vulnerable code from running)
  - Measurement of device state
  - Only allow authentic components to work in the system
  - Reporting mechanisms

Entity Attestation Token



Good Devices

Cloned

Tampered

Bad Devices

Emulating Real Device

Rooted

Entity Attestation Token

- Chip & device manufacturer
- Device ID (serial no.)
- Secure Boot state
- Debug disabled
- FW versions
- Location
- Malware detection

All claims are optional

Cryptographically signed

Relying Parties

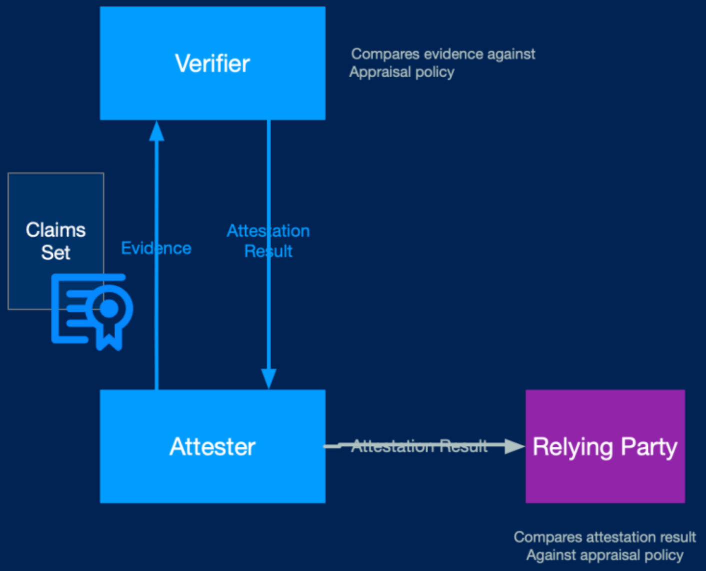
- **Shortly to be published RFC**
- **Highly flexible**
- **Based on CBOR, CWT, COSE (or JSON, JWT, JOSE)**
- **Suitable for constrained, MCU-based devices**
- **Already in use:**
  - PSA token
  - FIDO device onboarding

Attestation Models

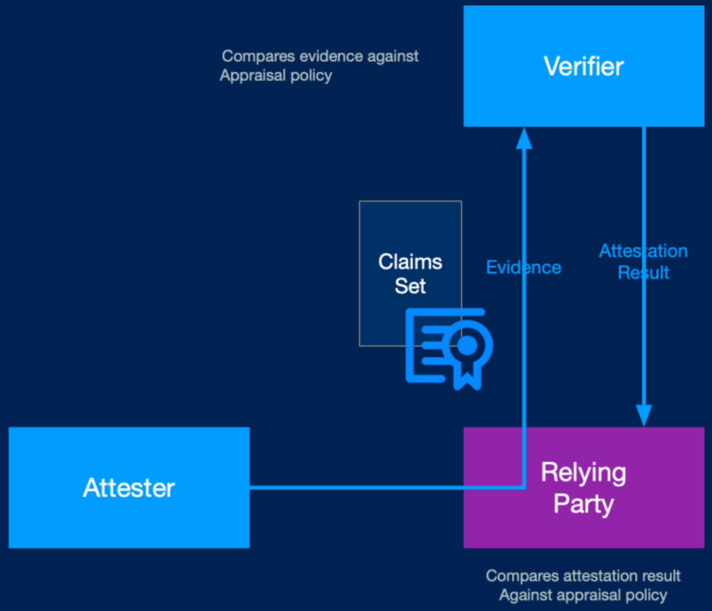
Roles in the system:

- Attester
  - A role performed by an entity (typically a device) whose Evidence must be appraised in order to infer the extent to which the Attester is considered trustworthy, such as when deciding whether it is authorized to perform some operation.
- Verifier
  - A role performed by an entity that appraises the validity of Evidence about an Attester and produces Attestation Results to be used by a Relying Party.
- Relying Party
  - A role performed by an entity that depends on the validity of information about an Attester for purposes of reliably applying application-specific actions.

Passport Model

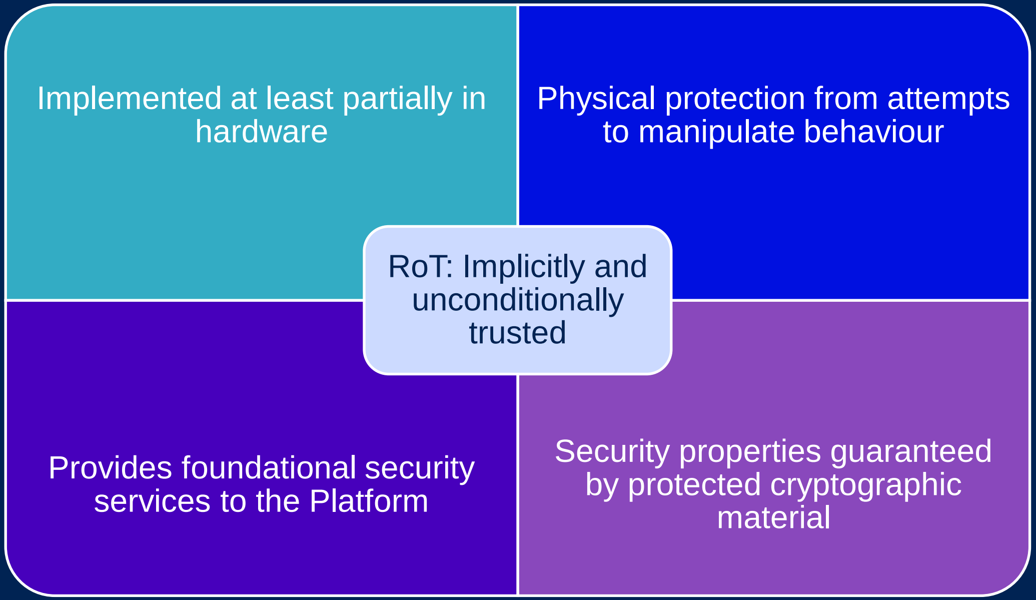


Background Check Model



What is a Root of Trust

*“A set of **unconditionally** trusted functional blocks on a Platform, whose misbehaviour cannot be detected”*


Implemented at least partially in hardware

Physical protection from attempts to manipulate behaviour

RoT: Implicitly and unconditionally trusted

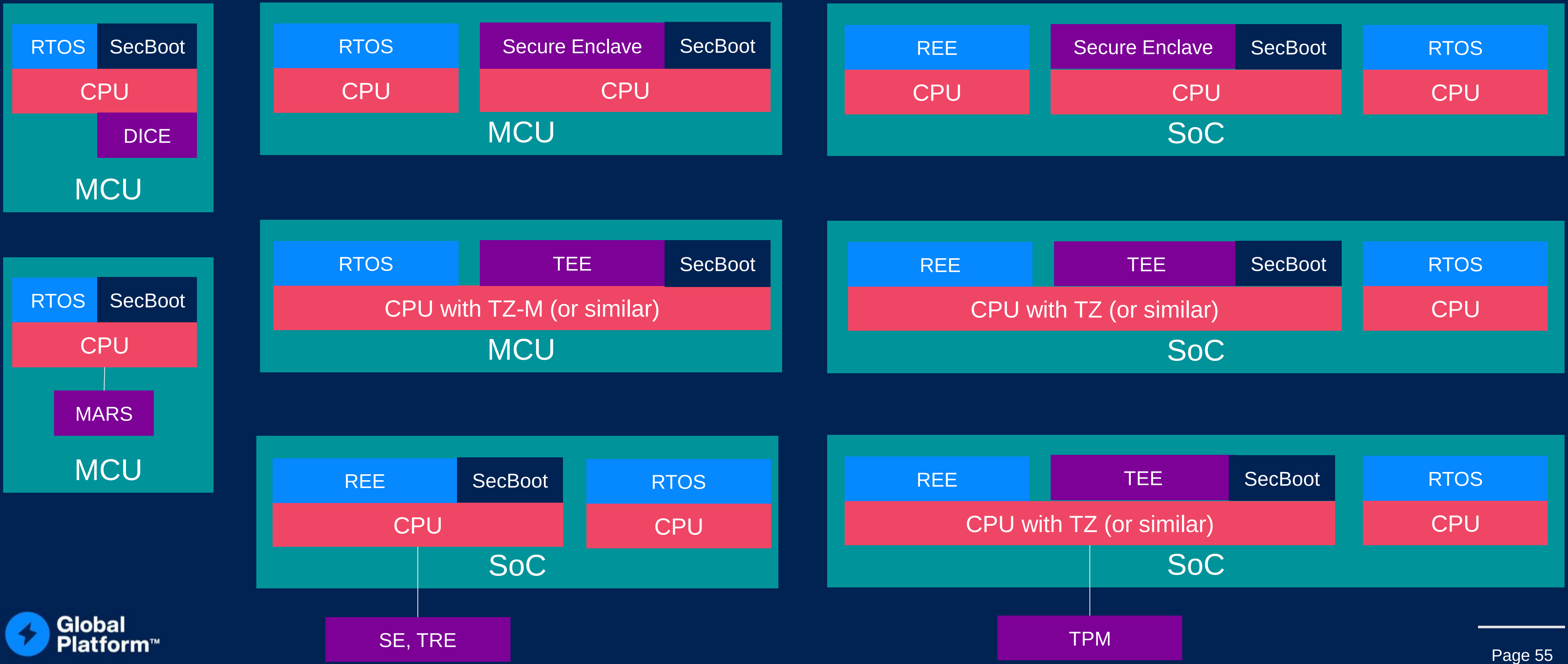
Provides foundational security services to the Platform

Security properties guaranteed by protected cryptographic material

Characteristics

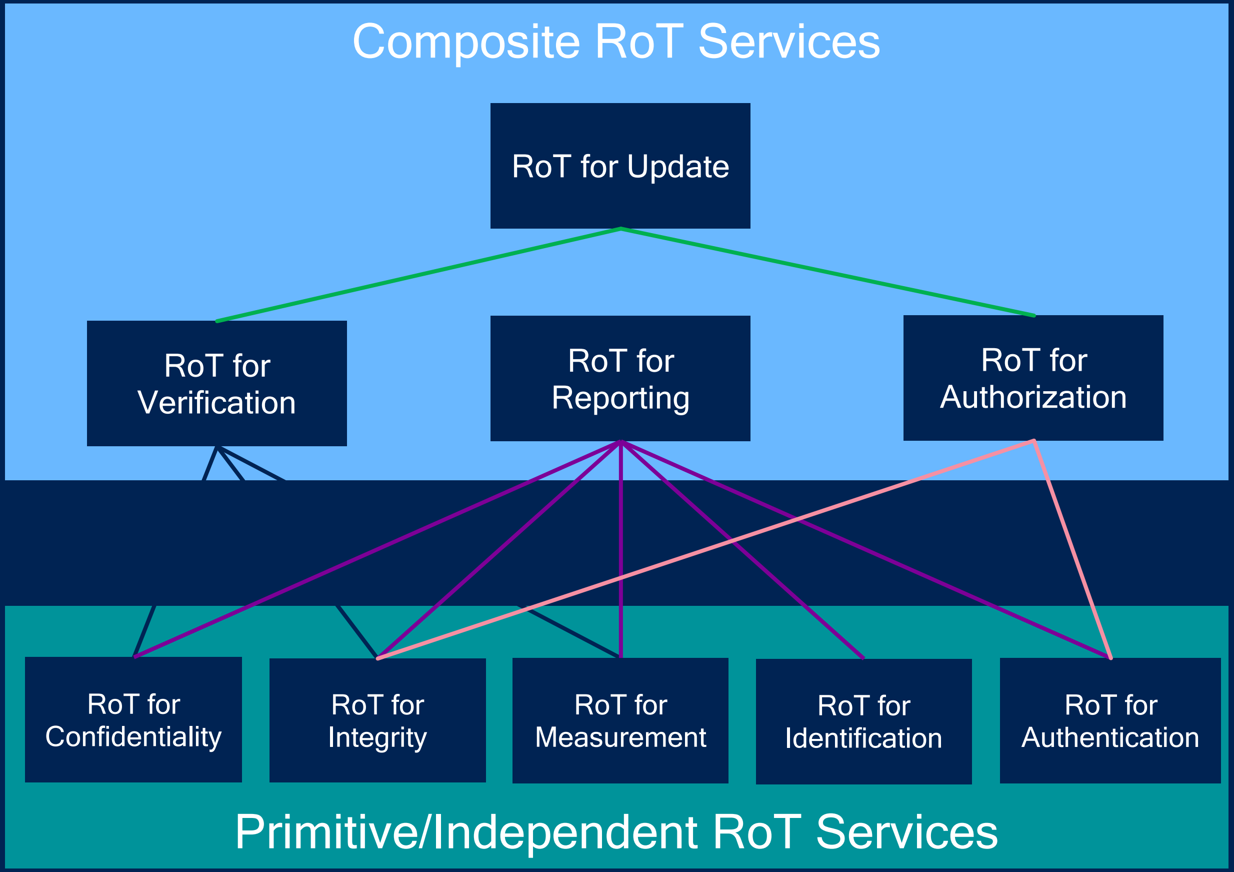
- Implemented at least partially in hardware to ensure that it cannot be manipulated to misbehave.
- Physically protected from attempts to manipulate its behaviour.
- Performs actions (functions) which are foundational to the security of a Platform. This means that it **must** include a computing engine.
- Usually contains cryptographic keys which must not be compromised if the Root of Trust is to be useful in guaranteeing security properties.

Approaches to Root of Trust on Devices



Global Platform™

Root of Trust Services



RoT for Update

- Verify updates and initiate update process

RoT for Authorisation

- Verify that auth token satisfies auth policy

RoT for Verification

- Verifiy authenticity and integrity of digitally signed objects

RoT for Reporting

- Reliably report Platform characteristics

RoT for Integrity

- Protect integrity of non-secret Platform params

RoT for Measurement

- Reliably report Platform characteristics

RoT for Authentication

- Provides shielded credential storage

RoT for Confidentiality

- Provides shielded locations to store sensitive information

RoT for Identification

- Provides a verifiable and non-repudiable Platform identity

Secure Components

MARS (TCG)

- Very small (~8kB)
- Limited client API
- Loosely bound to system
- Single tenant
- Probably not certified

TPM (TCG)

- Small implementation (~150kB)
- Rich client API
- Loosely bound to system
- Limited multi-tenant capability
- Usually high assurance (EAL4+)

SE / TRE (GlobalPlatform)

- Mid-size implementation (~350kB)
- Rich internal application APIs
- Loosely bound to the system
- Rich multi-tenant capability
- Always high assurance (EAL4+)

DICE (TCG)

- Very small (~20kB)
- Client API not standardized
- Closely bound to system
- Single tenant
- Probably not certified

TEE (GlobalPlatform)

- Large implementation (>1MB)
- Rich client and internal application APIs
- Closely bound to system
- Rich multi-tenant capability
- Often medium assurance (EAL2+)

Secure Enclave (Proprietary)

- Mid-size implementation (~250kB)
  Proprietary APIs
- Tightly bound to the system
- Single tenant
- Probably not certified

Secure Component Architecture

Initial Root of Trust

- Provides basic security services

Trusted OS layer

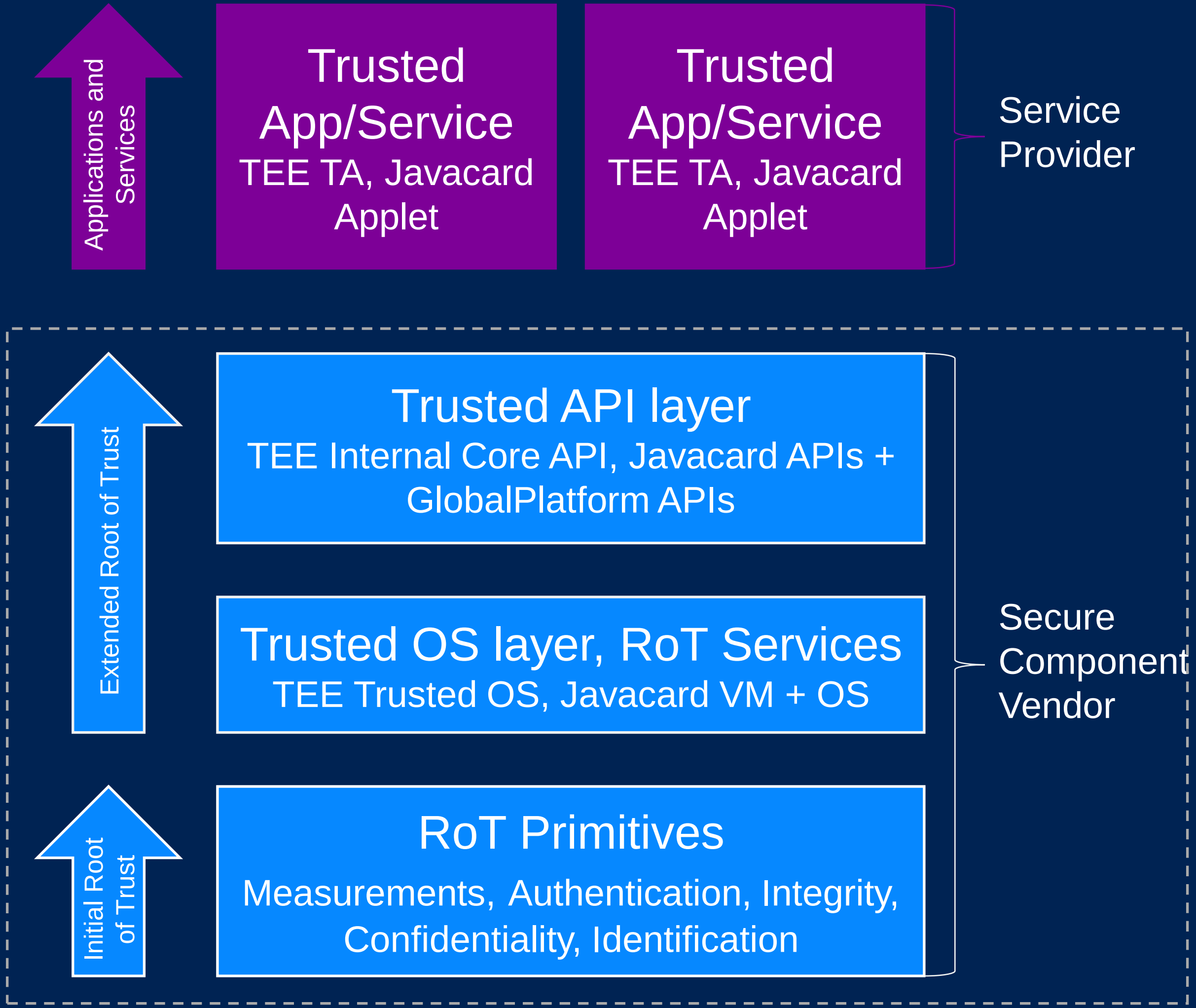
- Kernel, extended services (update, reporting, time, memory management, peripherals and interfaces)
  - TRE provides a Javacard VM and associated services

Trusted API layer

- APIs allowing security services to be constructed by Service Providers

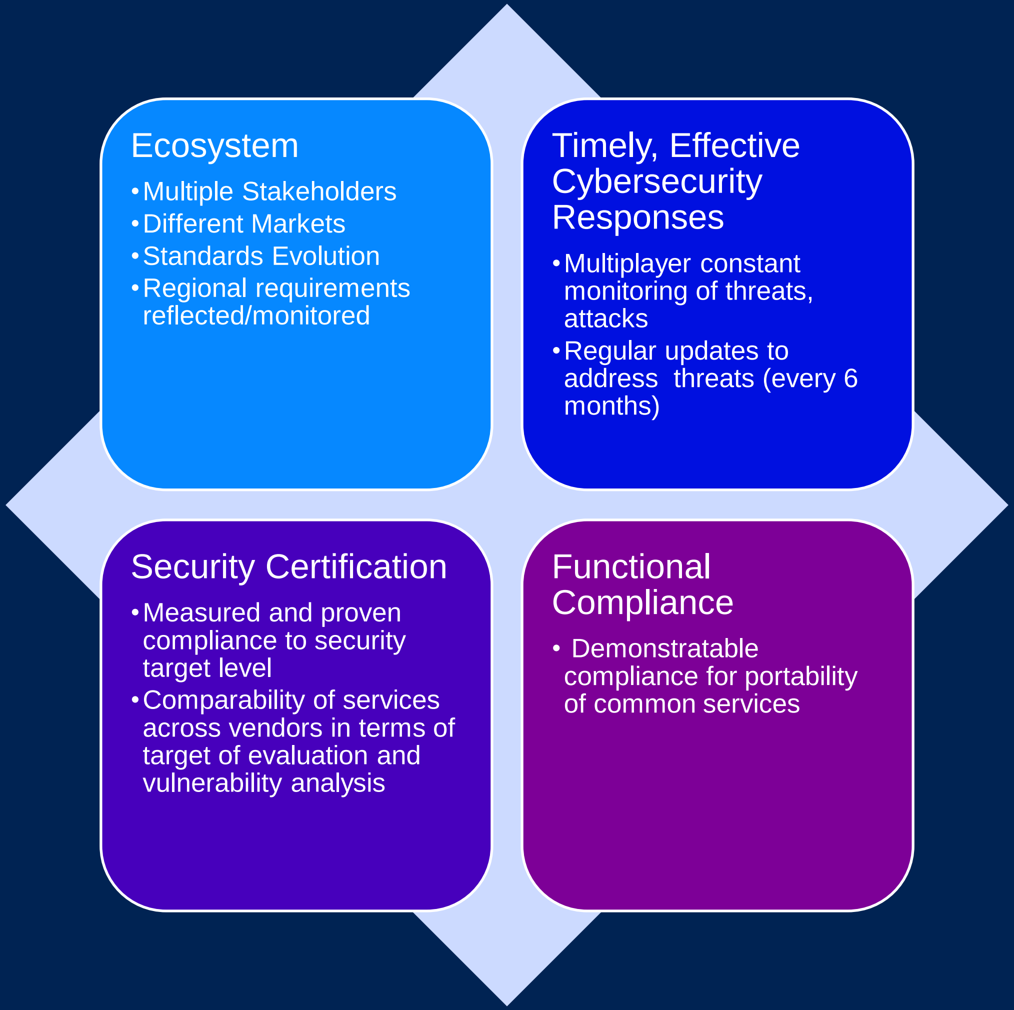
Trusted Applications & Services

- Implemented as TAs on TEE (native code: usually C, increasingly Rust)
- Implemented as Applets on TRE (Virtual Machine: in Java)



Applications and Services
Trusted App/Service
TEE TA, Javacard Applet
Trusted App/Service
TEE TA, Javacard Applet
Service Provider
Extended Root of Trust
Trusted API layer
TEE Internal Core API, Javacard APIs + GlobalPlatform APIs
Trusted OS layer, RoT Services
TEE Trusted OS, Javacard VM + OS
Initial Root of Trust
RoT Primitives
Measurements, Authentication, Integrity, Confidentiality, Identification
Secure Component Vendor

Why a Standardised Platform vs Proprietary Solution?



Ecosystem

- Multiple Stakeholders
- Different Markets
- Standards Evolution
- Regional requirements reflected/monitored

Timely, Effective Cybersecurity Responses

- Multiplayer constant monitoring of threats, attacks
- Regular updates to address threats (every 6 months)

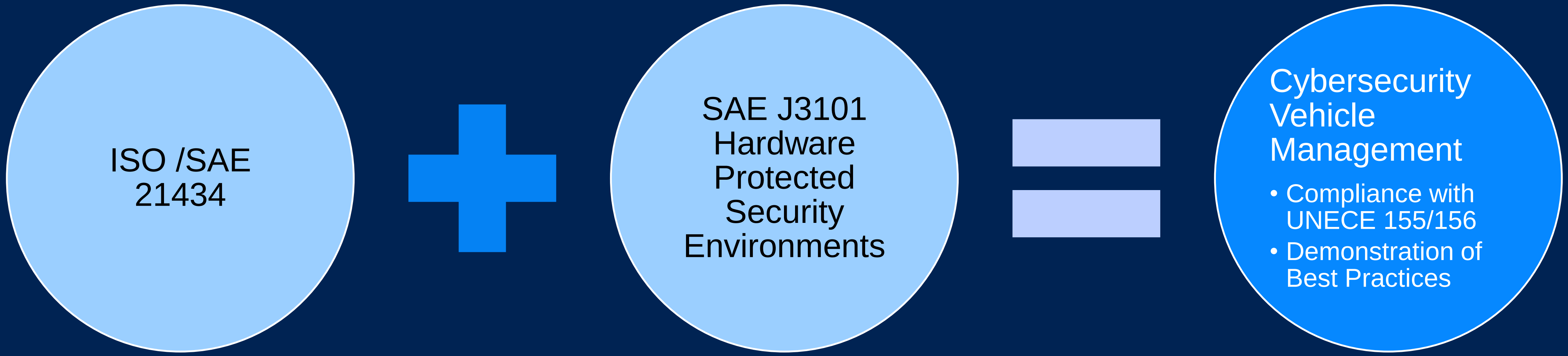
Security Certification

- 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

Cybersecurity: Compliance with UNECE 155 & 156



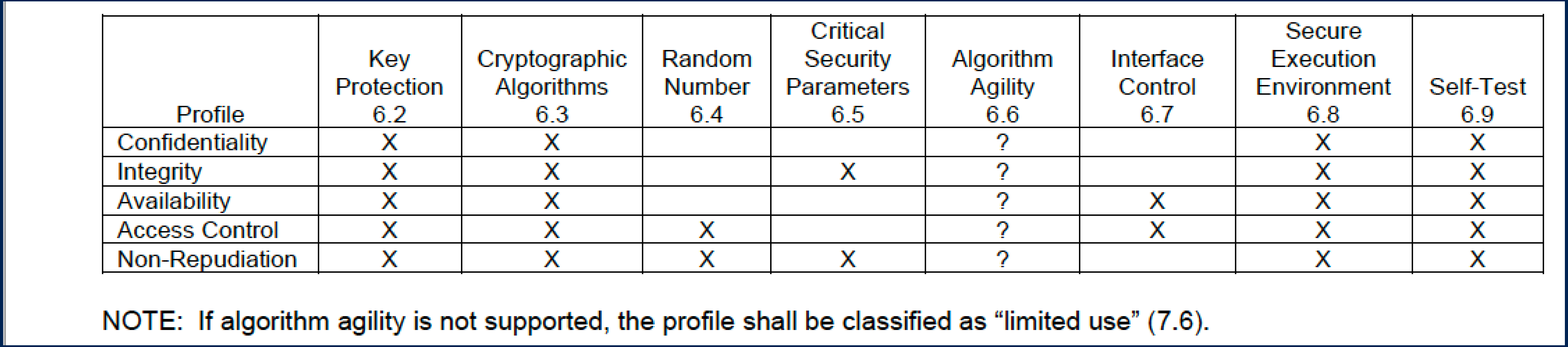
ISO /SAE 21434

SAE J3101 Hardware Protected Security Environments

Cybersecurity Vehicle Management

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

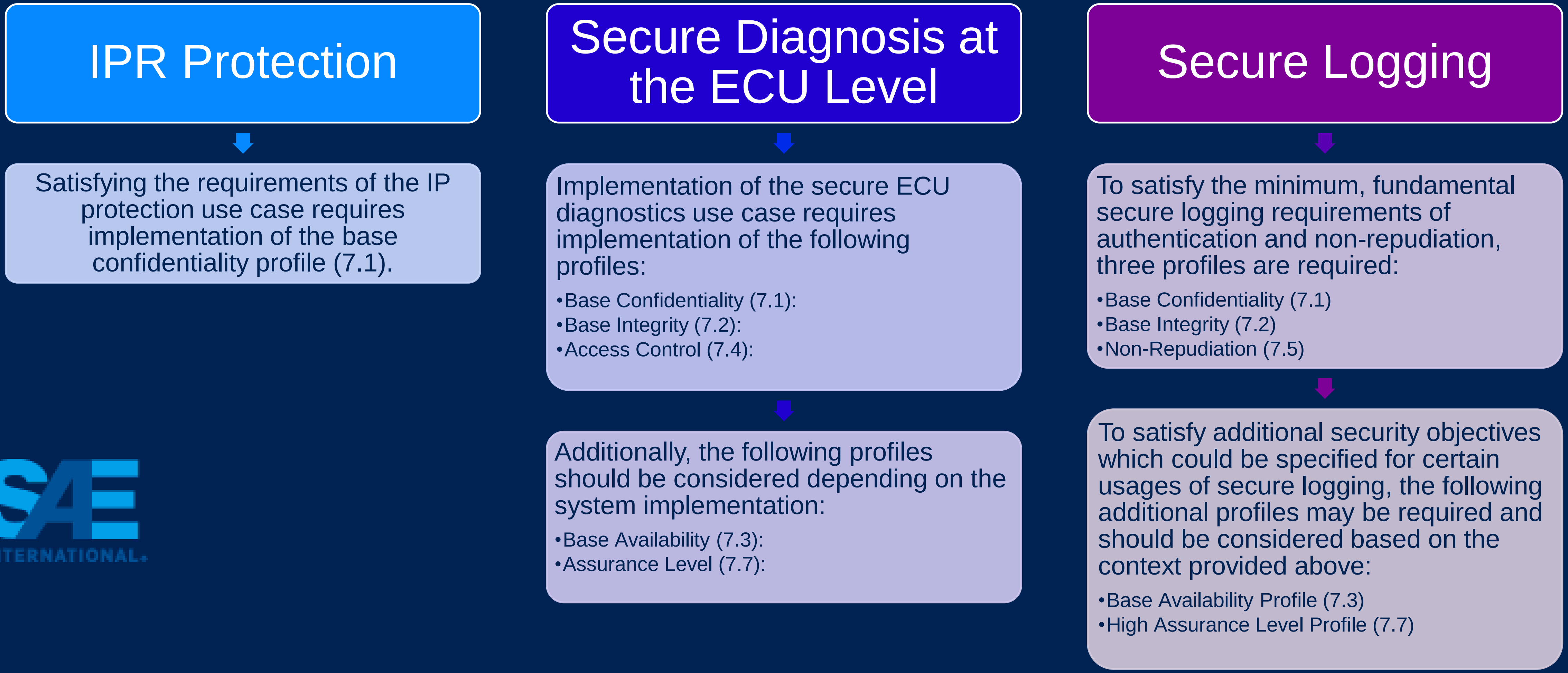
SAE Hardware Protected Security Environments J3101: Common Security Use Case Requirements



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).

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

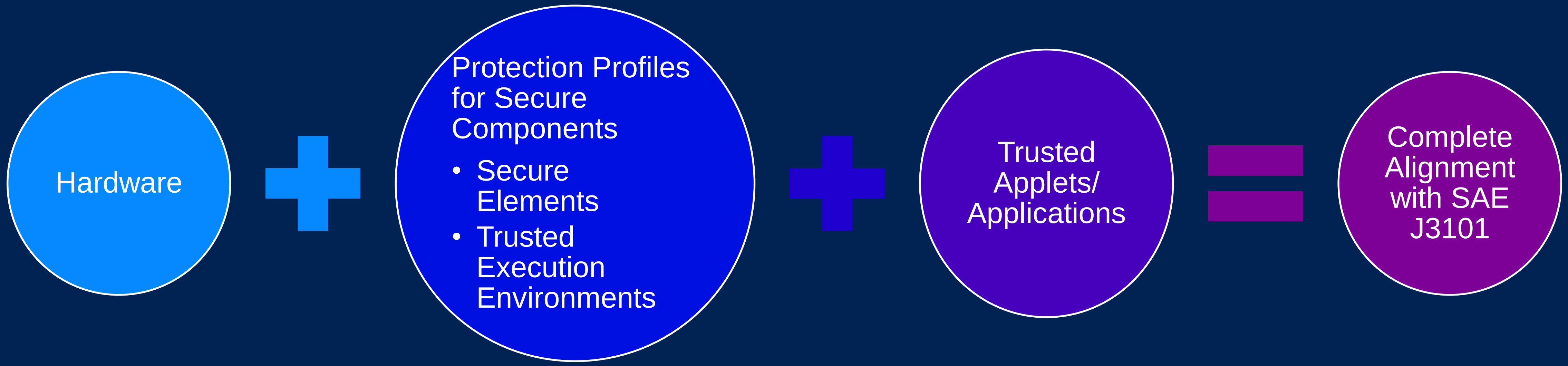
To satisfy the minimum, fundamental secure logging requirements of authentication and non-repudiation, three profiles are required:

- 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)

GlobalPlatform Alignment with Hardware Protected Security Environments J3101



Hardware

+

Protection Profiles for Secure Components

- Secure Elements
- Trusted Execution Environments

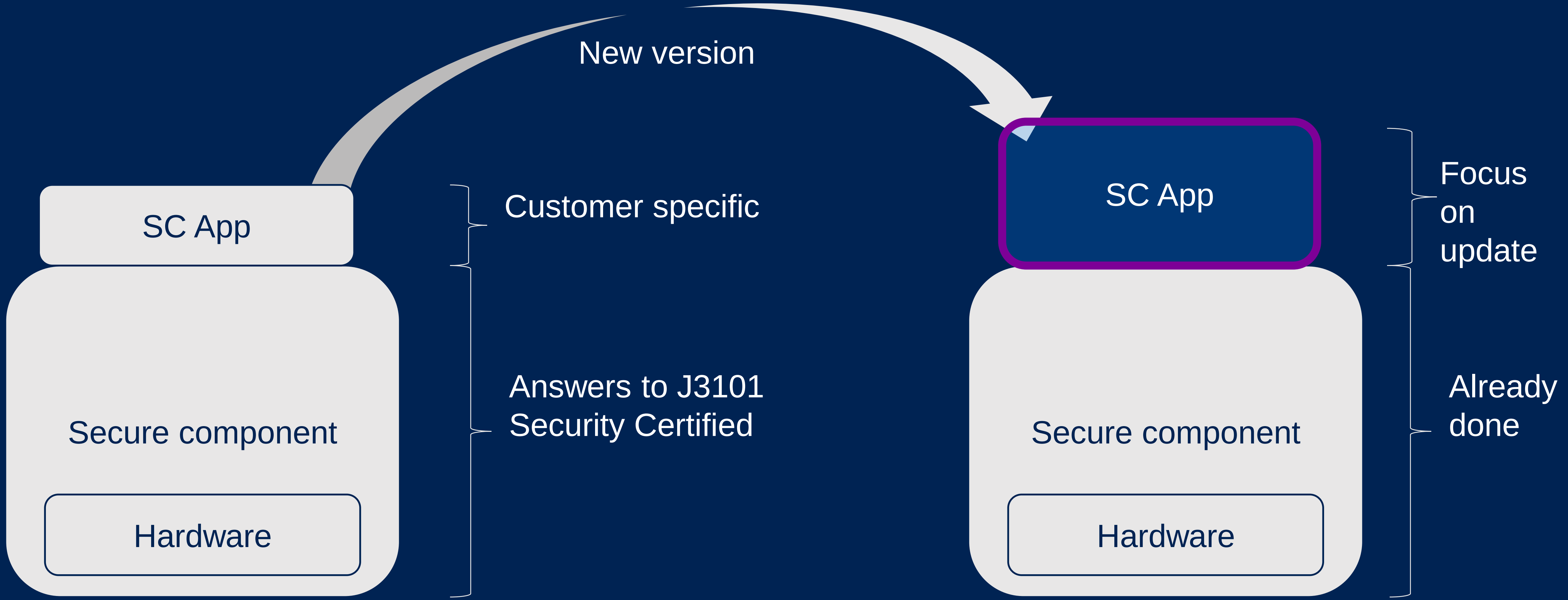
+

Trusted Applets/ Applications

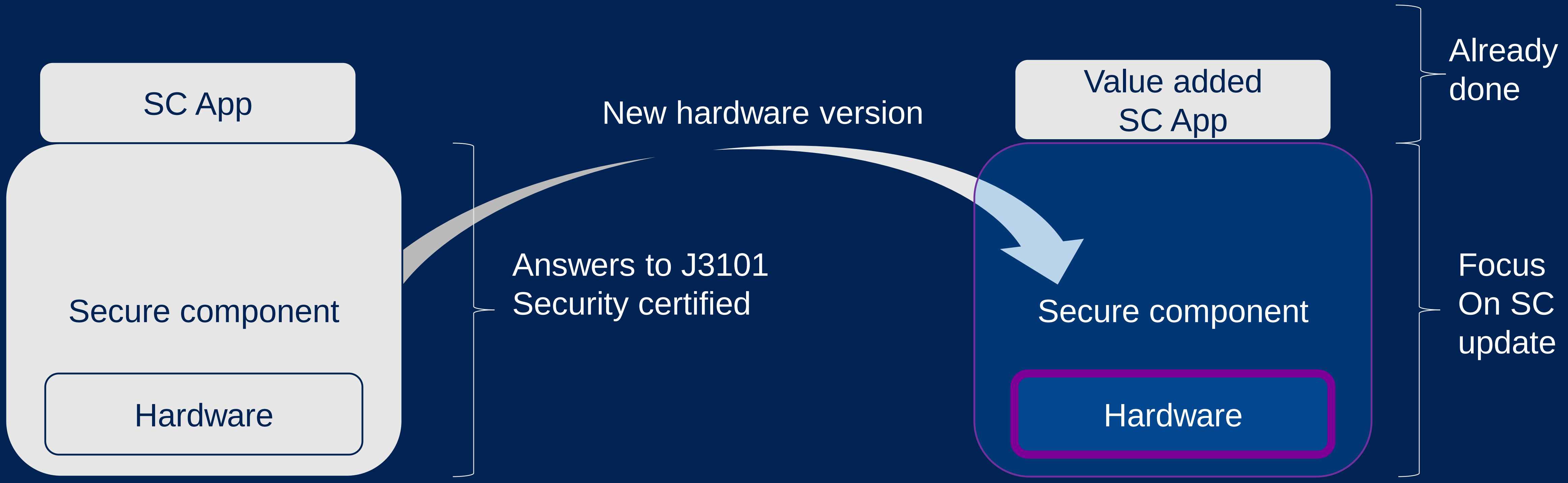
=

Complete Alignment with SAE J3101

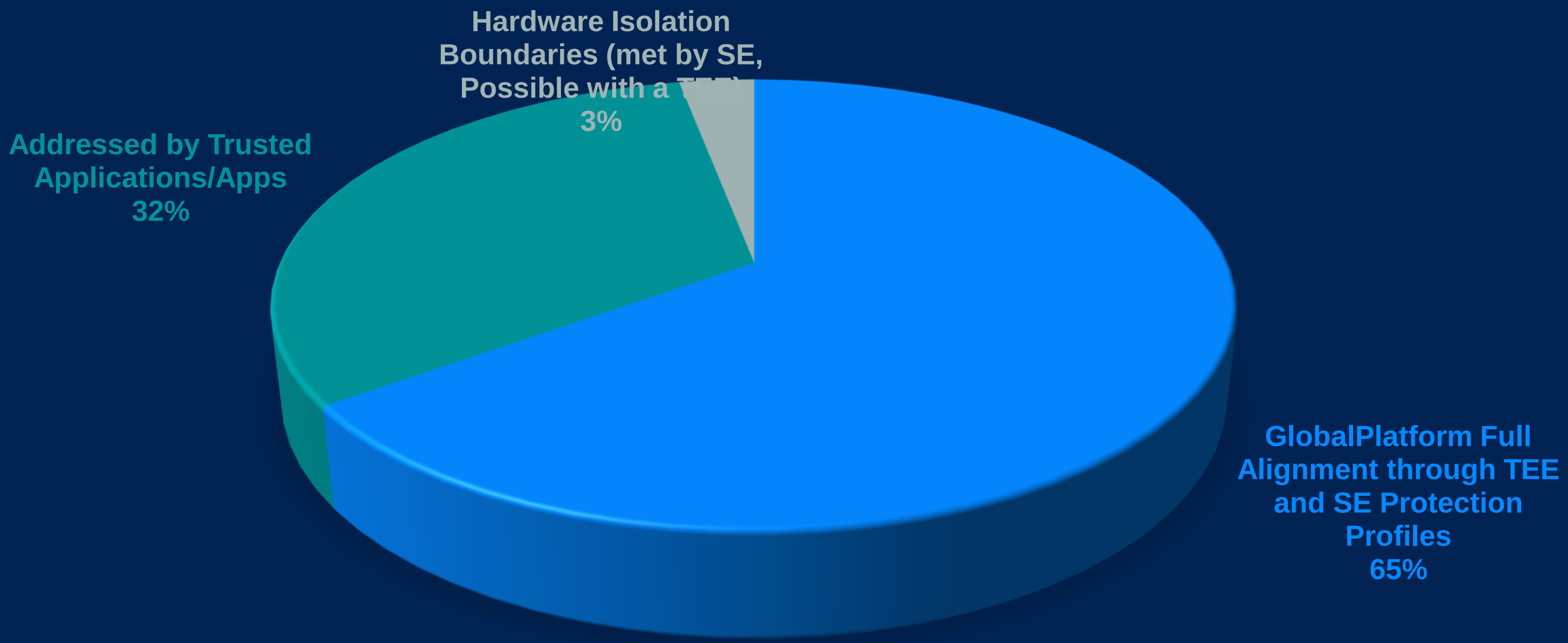
What does this mean for Tier 1s? #1/2



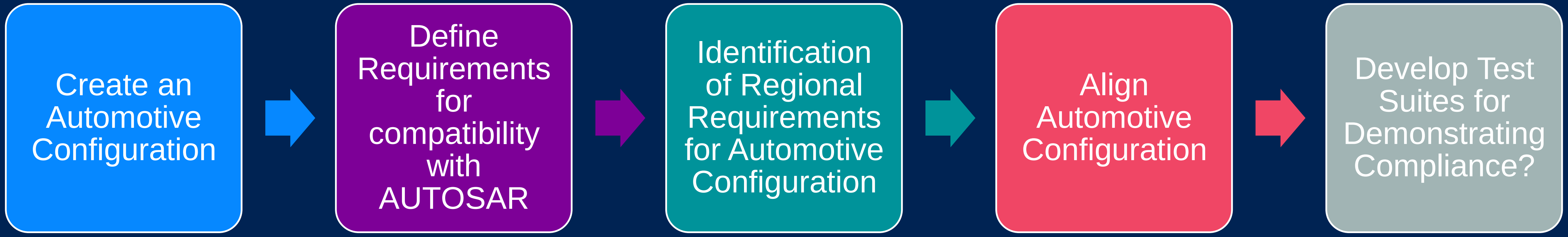
What does this mean for Tier 1s? #2/2



Analysis of J3101 Alignment with GP Specifications



Building Alignment with Standards



Create an Automotive Configuration

Define Requirements for compatibility with AUTOSAR

Identification of Regional Requirements for Automotive Configuration

Align Automotive Configuration

Develop Test Suites for Demonstrating Compliance?

Global Platform™

Cybersecurity Vehicle Forum Update - Tokyo

CSVF 14 09 23

62 Participants

Cybersecurity Vehicle Forum

Automotive Value Chain

- mazda
- Toyota

Automotive Suppliers

- ALPSALPINE
- eSOL
- Crevavi
- here
- DENSO Crafting the Core
- MITSUBISHI ELECTRIC Changes for the Better

Silicon & Solution Vendors

- Giesecke+Devrient
- Infineon
- REALTEK
- socionext
- ST life.augmented
- SYNOPSYS®
- TOSHIBA

GP Solutions

- NXP
- Qualcomm
- TRUSTONIC
- THALES Building a future we can all trust
- winbond We Deliver

Test Labs

- SGS

Industry Organizations

- AUTOSAR
- Global Platform™

Government

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

Universities

- सी-डैक CDAC CENTER FOR DEVELOPMENT OF ADVANCED COMPUTING

Broader Ecosystem

- BACTECH
- MineSec
- DNP
- NEC
- FeliCa Networks
- NTT
- fime
- NTT DATA NTT DATA INTELLILINK Corporation
- Rambus
- Innovation Japan
- SECOM
- Inventec Inventec Appliances
- SoftBank
- SONY
- Intralink
- Linaro
- TOMOWEL | Kyodo Printing Co., Ltd.
- Ubiquitous AI
- mastercard
- VECTOR

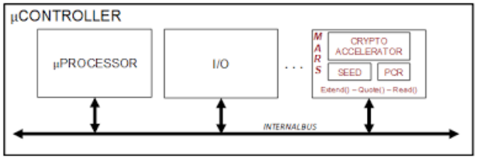
Global Platform™

Global Platform™

Potential Synergies

Considerations on Synergistic Opportunities

MARs



- MARS has a role as a small HW-backed crypto engine (so well aligned with a small profile of TPS Keystore), and for attestation by measurement (so EAT).
- MARS also has a very interesting protocol for change of ownership and key rotation, which has many potential automotive use-cases.

CCC

CARCONNECTIVITY consortium®

GlobalPlatform Opportunity:

- Providing input on:
  - Physical Attack Surfaces
  - **Security Updates via patch (OTA) during vehicle lifetime**

RISCV

RISC-V

GlobalPlatform Opportunity:

- Detailed mapping of TEE specifications and RISCV compatibility
- Identification of ways to foster viability of TEE for RISCV deployments

Other Potential Synergies

SOAFEE	Uptane		SDV Eclipse Software Defined Vehicle	AVC CONSORTIUM	COVESA	OP-TEE .org	CONFIDENTIAL COMPUTING CONSORTIUM
Foster cloud-native development paradigm and its ubiquitous ecosystem to the highly diverse, heterogeneous compute platforms that will power the next generation of automotive and safety critical system •GlobalPlatform could contribute to Security Group •Identified Partitioning Recipes as Future Work	Linux Foundation Joint Development Foundation project Open and secure software update framework design which protects software delivered over-the-air to automobile electronic control units (ECUs). •GP could use Uptane use cases for alignment with the automotive configuration for the TEE: •Orchestrator in the vehicle of	Trusted Firmware Organisation •Reference implementation of secure software for Armv8-A, Armv9-A and Armv8-M. It provides SoC developers and OEMs with a reference trusted code base complying with the relevant Arm specifications •GlobalPlatform could assess the compatibility with the Automotive Configuration	Eclipse Foundation's **Community for Open Innovation and Collaboration:** **Dedicated to Software Defined Vehicles** •**focused on accelerating innovation of automotive-grade in-car software stacks using open source and open specifications developed by a vibrant community.**	Autonomous Vehicle Computing Consortium (AVCC®) *Driving Industry Consensus on Automated & Assisted Driving Compute Solutions* Specifies and benchmarks solutions for Autonomous Vehicles computing, cybersecurity, functional safety, and building block interconnects. *GlobalPlatform Opportunity: on*	Connected Vehicle Systems Alliance 3 Working Groups EV Charging Expert Group In-Vehicle Payment SIG Security Team	OPTEE •Open source project, which contains a full implementation to make up a complete Trusted Execution Environment using the ARM® TrustZone®	Confidential Computing Group Linux Foundation Project Open source licensed projects securing data in use & accelerating the adoption of confidential computing through open collaboration. Future in ADAS?

Strategic Questions : Phase 2

Should GlobalPlatform develop Trusted Application Areas for common required applications?

- Compliance with SAE J3101
  - Keystore
  - Attestation
- For Uptane Use Cases
- Would TPS be the right Starting Place?
- if so, How would it be best to develop the Protection Profiles?

Should GlobalPlatform have a formal position on mCUs for Automotive?

Should GlobalPlatform ramp up work with organisations for which there are existing MoUs -i.e. exploring a more in-depth coordinated working method:

- Connected Car Consortium
- RISC-V