Global Platform™

CyberSecurity Vehicle Forum

Gil Bernabeu, CTO
Richard Hayton, Chair Automotive Task Force
Francesca Forestieri, Automotive Lead

Global Platform™

Everyone Get Connected!

Meeting ID: 233 444 112 381 Passcode t7Yb94

EVERYONE

- Please join Teams so you can take part in polls and interactive sessions
- Please DO NOT join audio if you are in the room(!)
- Muting is not enough, you also have to have your speaker turned off

GDPR

- We will record the sessions and make the recording available
- We will also give participants a list of attendees. If you do not want your contact details to be shared, please let Francesca know during the meeting or within 24 hours at francesca.forestieri@globalplatform.org

Tips

- Please put your name + company in Teams
  (if you prefer not to share, please put 'OEM' or 'SIP' or '…')
  The meeting will be recorded.
- Please mute when not speaking.
- Please use chat if there are audio/video problems
- Please use Q&A for questions to the general audience
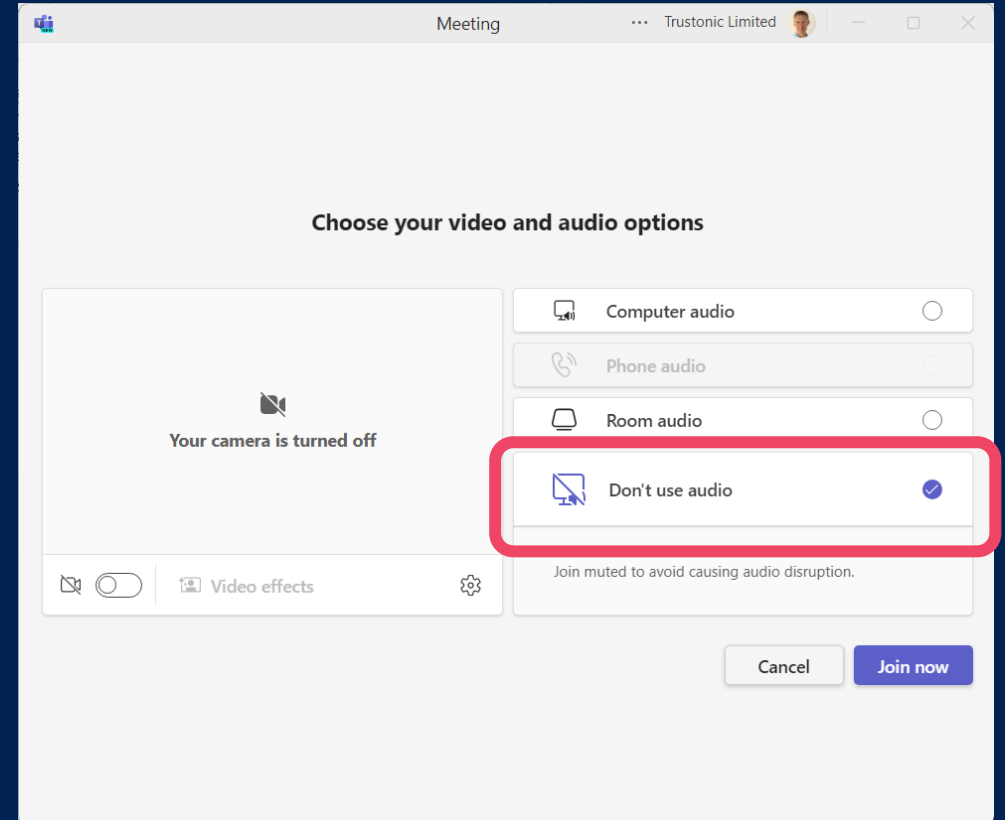
Speakers

Dr. Julian Brough
BSI

Axel Poschmann
PQ Shield

Martin Emele
Auto ISAC

Antoaneta Kondeva
Infineon

Pascal van Gimst
Riscure

Dr. Michael Leitner
Car Connectivity
Consortium

Andrew Jones
AVCC and ARM

Shreyas Derashri
Imagination
Technology

Karl (Kalli) Schlauch
VicOne

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

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

Our Members

Full

Participant
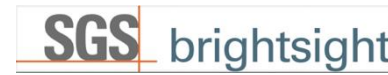
Observer, Public Entity and Consultants

# 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 <u>our vision</u> 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

Automotive & Mobility Related
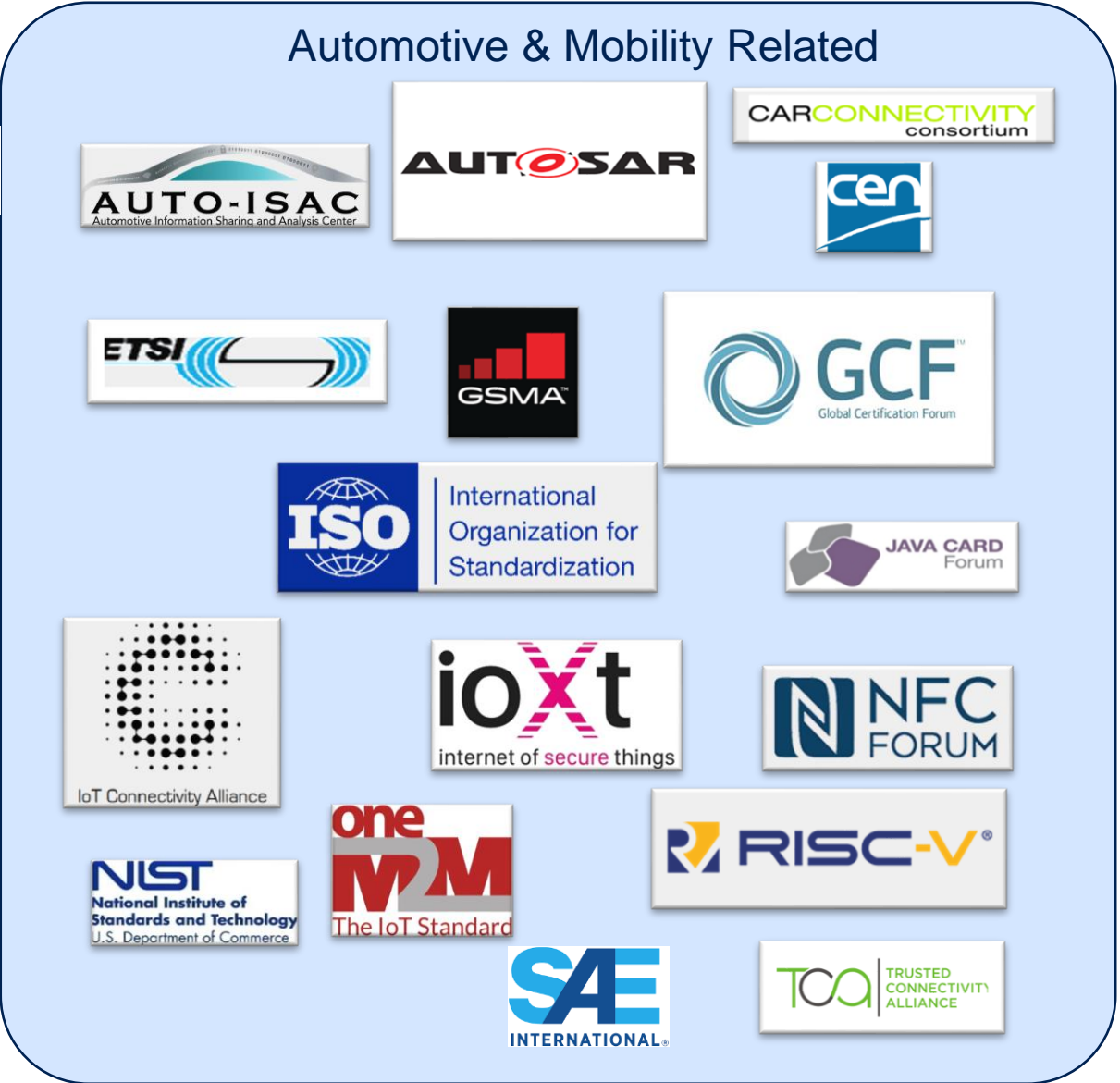
GlobalPlatform specifications are freely available

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

Global Platform™

GlobalPlatform: Technology

Richard Hayton,
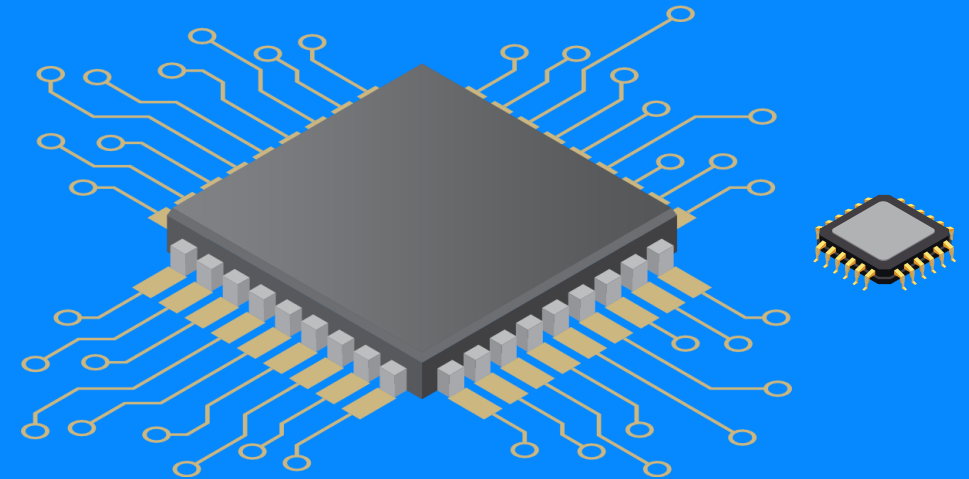Chair of Automotive, GlobalPlatform

Hardware Security Approaches

Higher Performance
More Memory
Peripheral Access
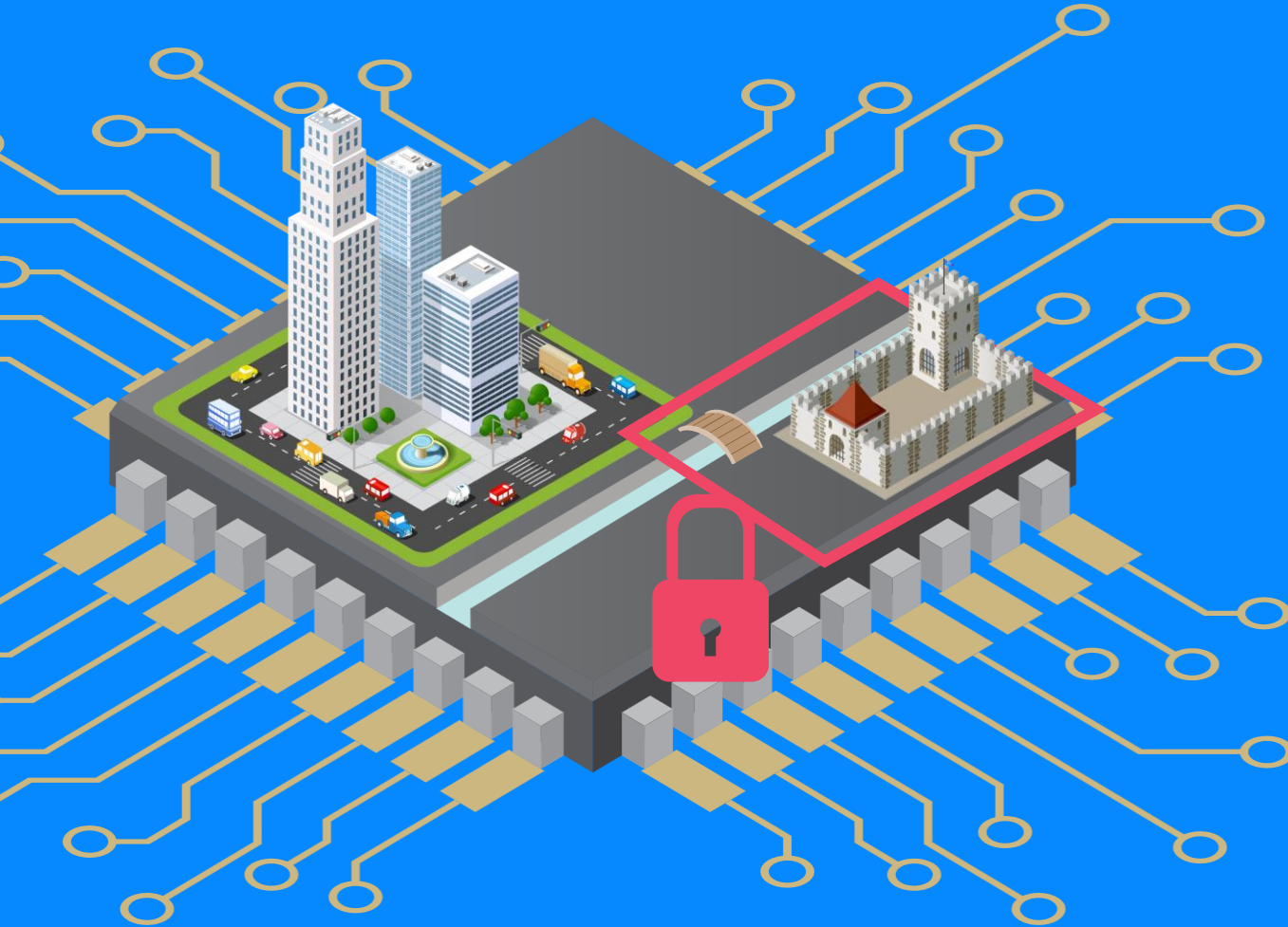
.V.

Better Physical Security
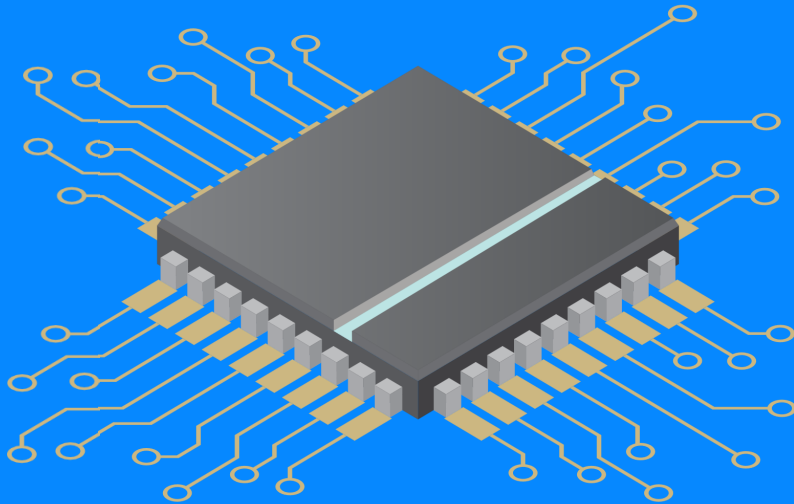
Isolate part of a traditional
CPU to focus on security
(E.g. Arm TrustZone™)

Add a separate security CPU
(E.g. Secure Element/TPM/…)

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

- Supports multiple independent applications (containers)

- Commonly used in Mobile Devices, Automotive and IoT

Diagram © Trustonic Ltd

GlobalPlatform Secure Element
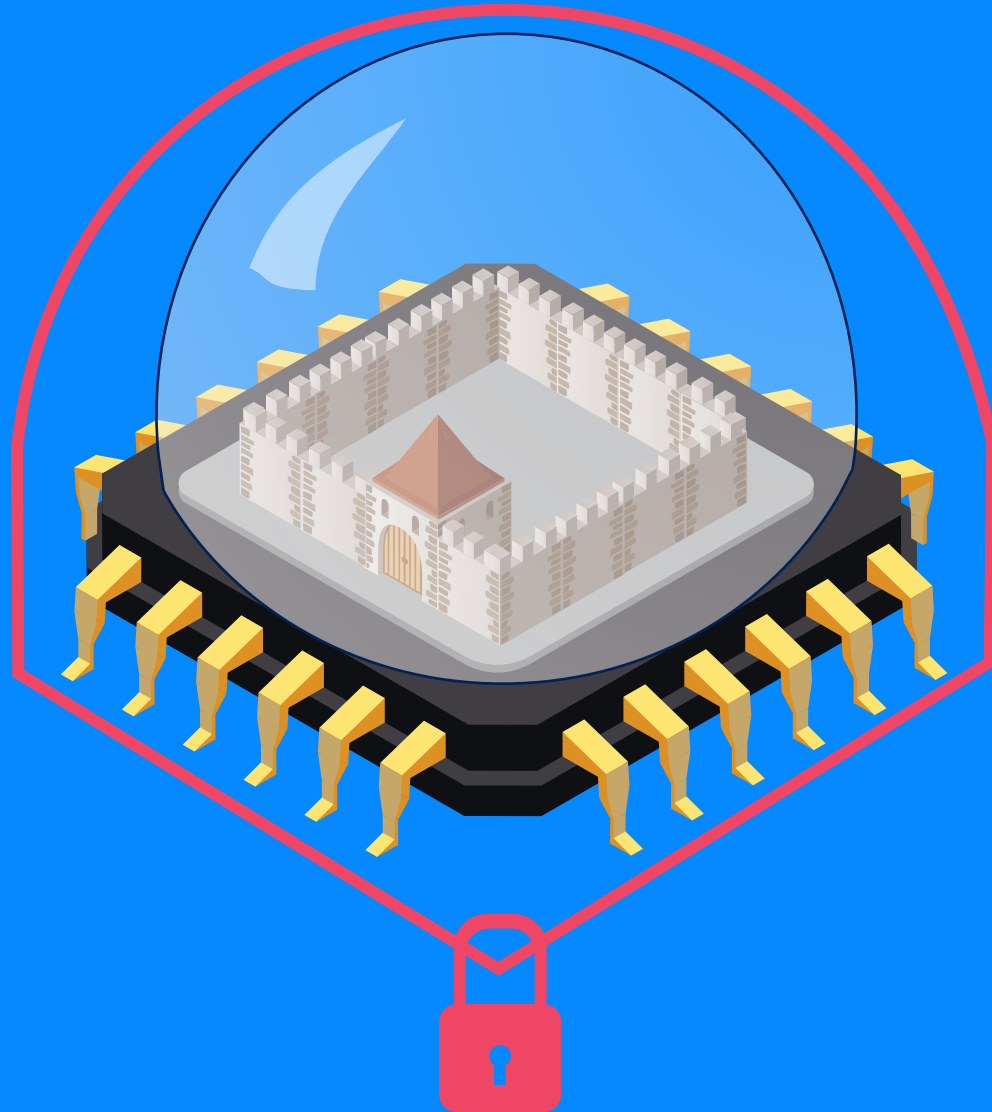
- A secure enclave protected against physical and software attack

- 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

Protection Profile is Published

Accredited Lab Evaluates Profile

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

GP Defines Implementation Requirements

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

GP Sets Security Objectives

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

Products will be tested to ensure they meet these requirements

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

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

Common Criteria

SESIP

Certification because….

Global Platform™

01
Demonstrates quality and robustness (UNECE-155)

02
Makes it easier to write and respond to RFCs

03
Provides a basis for legal defence if there ever is a breach

04
V-Model ensures good security process.

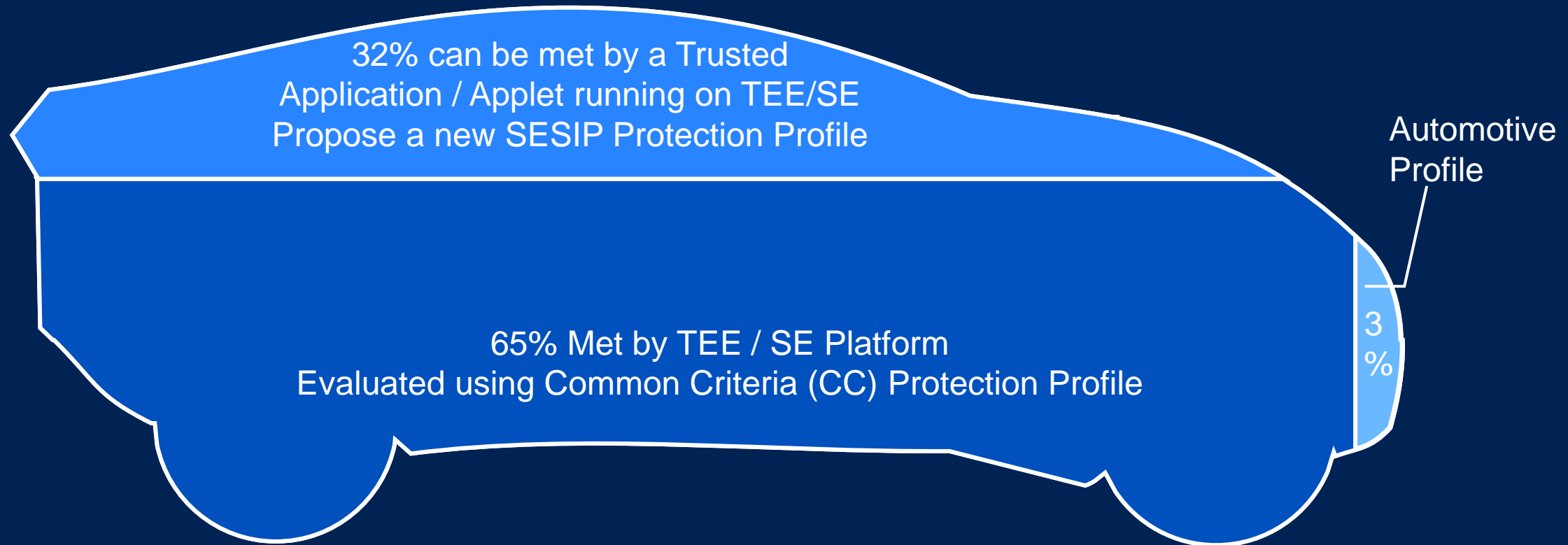Certification ensures a level of security is achieved in practice.

Automotive Activities

Richard Hayton,
Chair of Automotive, GlobalPlatform

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

Global Platform™

Meeting J3101 Requirements

32% can be met by a Trusted
Application / Applet running on TEE/SE
Propose a new SESIP Protection Profile

Automotive
Profile

65% Met by TEE / SE Platform
Evaluated using Common Criteria (CC) Protection Profile

3%

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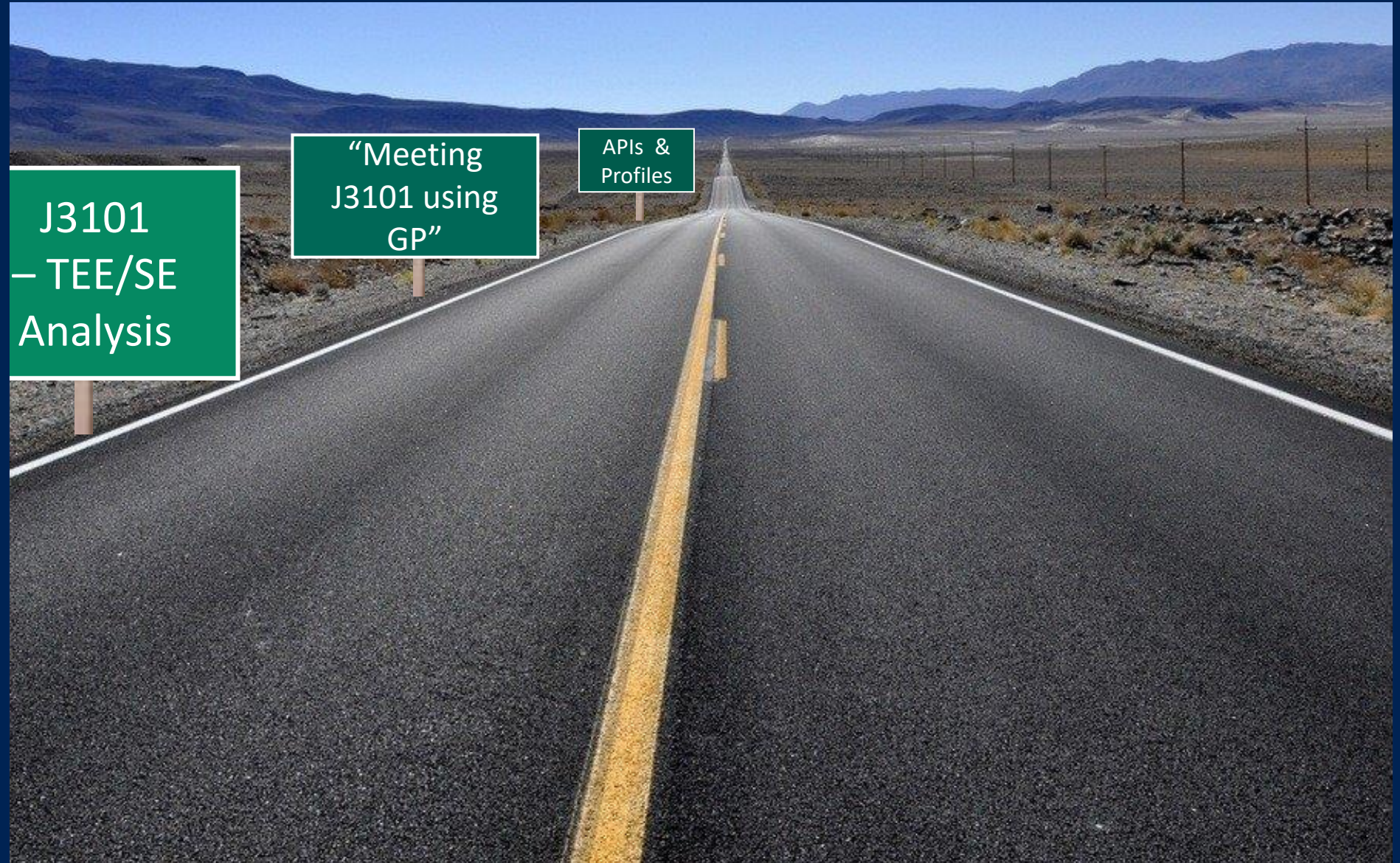
Global Platform™
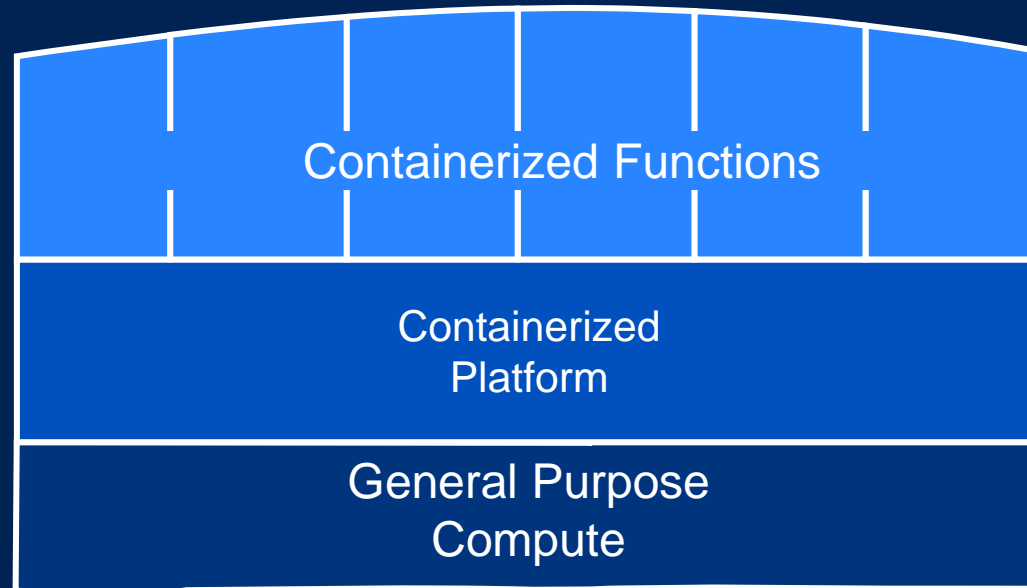
Route

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

J3101 – TEE/SE Analysis

"Meeting J3101 using GP"

APIs & Profiles

Global Platform™

GlobalPlatform &
Software Defined Vehicles

Containerized Functions

Containerized Platform

General Purpose Compute

GlobalPlatform & Software Defined Vehicles

Multi-Tenant Secured Services

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

Containerized Functions

SAE J3101 Key Store

AI/ML Compute

Containerized Platform

Security Containerized Platform

Safety Critical Areas

GPU/AI

General Purpose Compute

Special Purpose Embedded MCU

Global Platform™

Cybersecurity Vehicle Forum

Francesca Forestieri, Automotive Lead

What is the Cybersecurity Vehicle Forum?

Players

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

Relevant Security Technologies

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

GlobalPlatform's Cybersecurity Vehicle Forum

Global Platform™

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

Cybersecurity in Automotive

Whitepapers

Specifications

Protection Profiles

GlobalPlatform Automotive Activities: First Year

Cybersecurity Vehicle Forum

22 Use Cases GlobalPlatform Relevant

35 Use Cases Reviewed

Prioritised 6 lowest hanging fruit

Automotive Task Force
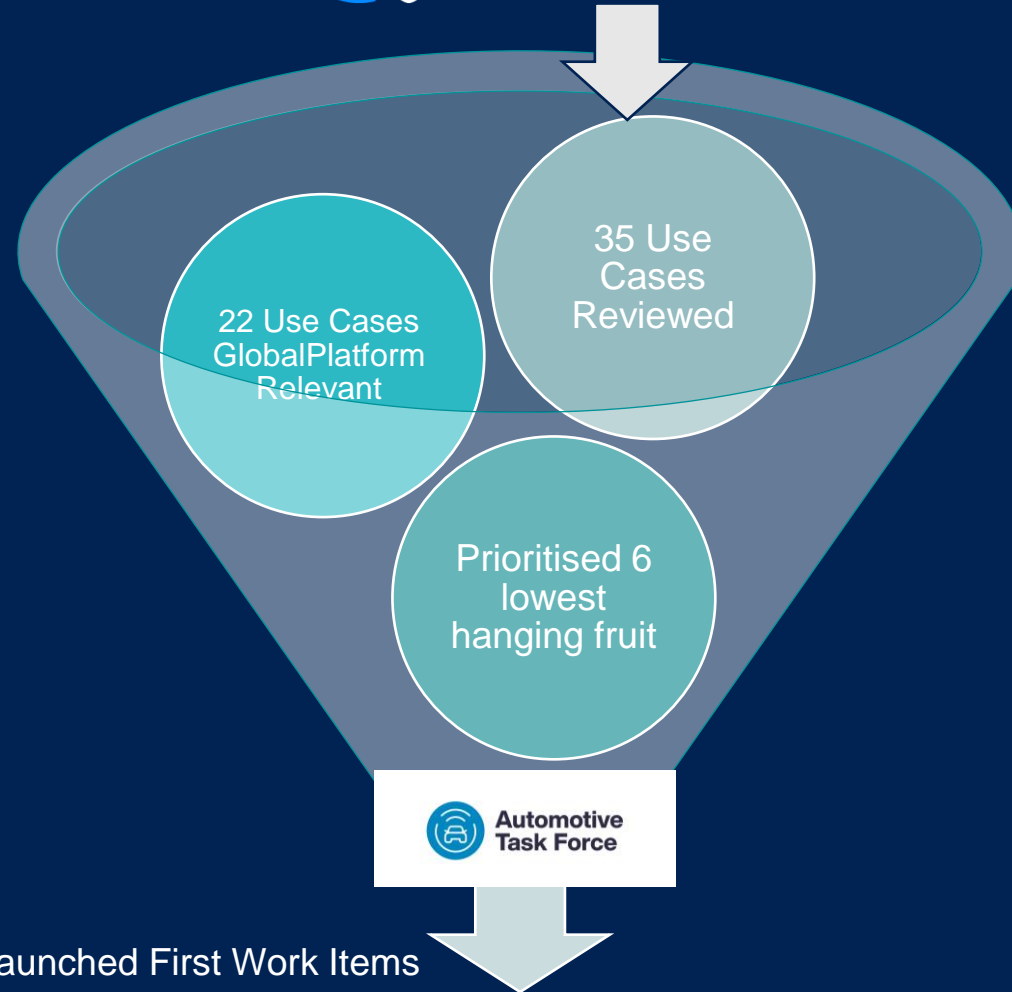
Launched First Work Items

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

Global Platform™

GlobalPlatform Security White Papers

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

→globalplatform.org