Global Platform®

Securing the digital future

Cybersecurity Vehicle Forum – Munich

21 October, 2026

Ana Lattibeaudiere, CEO of GlobalPlatform
Gil Bernabeu, CTO of GlobalPlatform
Richard Hayton, Co-Chair of Automotive Task Force, Qualcomm
Francesca Forestieri, GlobalPlatform Automotive Lead

© GlobalPlatform 2026 |

Cybersecurity Vehicle Forum: WELCOME!

44 organisations from across the vehicle security value chain, from silicon to the road

Vehicle makers

4 organisations

Stellantis · CARIAD · Renault Group · Toyota Motor North America

Tier 1s and automotive software

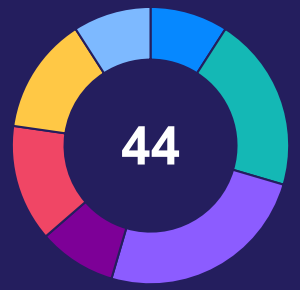
9 organisations

Hitachi Solutions Technology · DENSO · Minerva Systems · Bosch · Vector Informatik · Green Hills Software · Xen Project · HERE Technologies · Huawei Device

Semiconductors and security IP

11 organisations

Infineon · Renesas · Rambus · STMicroelectronics · NXP · Qualcomm · Arm · Ampere · Arteris · PQShield · Xiphera



75 registrations

44 organisations

Security and trust solutions

4 organisations

Giesecke+Devrient · Thales CDI · Futurex · Autocrypt

Testing, evaluation and labs

6 organisations

Keysight · COMPRION · DEKRA · DPLS Lab · HORIBA MIRA · Quarkslab

Engineering services and consulting

6 organisations

EPAM · Digital Universe · Alten · Intexus · High North · PxConsult

Public bodies, research and associations

4 organisations

BSI · Universität der Bundeswehr München · Catena-X · ITU IDA

Registrations excluding GlobalPlatform hosts. Colours in the ring match the group icons

Agenda

01 PQC, specifications, traceability & AI risks

09:30 **Welcome & Introduction**
Francesca Forestieri, GlobalPlatform; Richard Hayton, Co-Chair of Automotive Task Force, GlobalPlatform

09:45 **PQC: Beyond Algorithms**
Morgane Guerreau, PQShield

10:05 **Planning for Global Specifications: Agility**
Yves Le-Bobinnec, Thales

10:25 **Traceability**
Digital Product Passports: Battery Case Study
Mathias Moser, Catena-X

10:45 **Agentic AI Risks**
Artur Hecker, ITU TIDA

11:05-11:20 Coffee Break

02 Safety, Security & Software Isolation Evolution

11:20 **TEE 2.0 Specification Development**
Richard Hayton, GlobalPlatform Chair of Trusted Environments and Services Committee

11:50 **XEN Safety Certification**
Artem Mygaiev, Xen Project

12:10 **Managing Mixed Criticalities**
Redouane Soum, Ampere

12:30 **Assurance from freedom of interference**
Frederic Ameye, Renesas

12:50 **Co-Existing of Safety and Security Mechanisms in Hard Real Time Systems**
Hans-Leo Ross, CARIAD

13:10-14:10 Lunch

PANEL 1 I 14:10-14:40
SAFETY, SECURITY & SOFTWARE ISOLATION EVOLUTION
Richard Hayton, Qualcomm; Redouane Soum, Ampere; Frederic Ameye, Renesas; Jorge Wallace Ruiz, DEKRA
Hans-Leo Ross, CARIAD

03 Security in Zonal Architecture

14:40 **Secure Element: Evolution**
Laurent Tabaries, STMicroelectronics

15:00 **GP Micro-TEE: Evolving Firmware Framework for M and PSA APIs**
Richard Hayton, GlobalPlatform Chair of Trusted Environments and Services Committee

15:20 **Future Security Strategies in Isolation**
Guillaume Perret, NXP

PANEL 2 I 15:40-16:10
SECURITY IN ZONAL ARCHITECTURE
Laurent Tabaries, STMicroelectronics; Andrew Thoelke, Arm; Richard Hayton, Qualcomm; Gil Bernabeu, GlobalPlatform; Guillaume Perret, NXP

16:10-16:25 Coffee Break

04 Automotive Cybersecurity Assurance

16:25 **ISO/SAE PAS 8475 & TR 8477 Update**
Paul Wooderson, HORIBA MIRA

16:45 **Automotive SESIP: Automotive SESIP Domain, SAE J3600, ECU Profile**
Jorge Wallace Ruiz, DEKRA

17:20 **Automotive High Performance Computing Requirements in China**
Junning Yao, Huawei

17:40 **Research Results: Hardware Trojan detection by using Formal Verification**
Christian Appold, DENSO

PANEL 3 I 18:00-18:20
AUTOMOTIVE CYBERSECURITY ASSURANCE
Paul Wooderson, HORIBA MIRA; Jorge Wallace Ruiz, DEKRA; Christian Appold, DENSO; Junning Yao, Huawei

18:20-18:30 **Closing & Wrap Up** Ana Lattibeaudiere, GlobalPlatform

CSVF Ground Rules

A trusted space to share expert views openly

A trusted environment

Speak openly: this room is for sharing views and learning from each other

Experts speak for themselves

Each speaker shares their own expert view, not necessarily that of their company or standards organisation

Use what you hear, don't attribute it

You are free to use the information you receive, but not to attribute it to a speaker's affiliation

After the forum: GlobalPlatform will post the recording and the speakers' slides (as made available) at globalplatform.org/blog-overview

Cybersecurity Vehicle Forum Objectives

Driving security standardisation priorities and requirements into GlobalPlatform

1 LISTEN TO THE MARKET

Cybersecurity Vehicle Forum

17 editions since 2022, four regions plus online

Europe	Munich Nov 2022	Hamburg Nov 2023	Berlin Dec 2024	Munich Oct 2026
USA	Detroit May 2023	Detroit Jun 2023	Detroit Jun 2024	Detroit April 2026
China	Beijing Oct 2023	Shanghai May 2025	Shanghai Dec 2026	
Japan	Tokyo Sep 2023	Tokyo Oct 2024	Yokohama May 2025	Tokyo May 2026
Online	Virtual Mar 2023	Virtual Sep 2023	Virtual Mar 2025*	Virtual Dec 2025

2026 editions * *with the GP Member Meeting*

2 SHAPE PRIORITIES AND STANDARDS

TASK FORCES · set priorities

- **Automotive** Task Force
- **Market** Task Forces
- **Regional** Task Forces

COMMITTEES · write the standards

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

3 PUBLISH

FROM TASK FORCES

- **Whitepapers**
- **Functional requirements**
- **Guidelines**

FROM COMMITTEES

- **Specifications**
- **Protection profiles**

e.g. Cybersecurity in Automotive white paper, TEE System Architecture, SESIP methodology

Housekeeping

Join on Zoom: **zoom.us/j/93778495815**

Meeting ID: 937 7849 5815

Passcode: 802637

DURING THE SESSION

Download Zoom
on your device before you join

Use the chat
if you have audio or video problems

Mute yourself
when you are not speaking

Raise your hand
to speak

Raise hand is in the meeting toolbar:

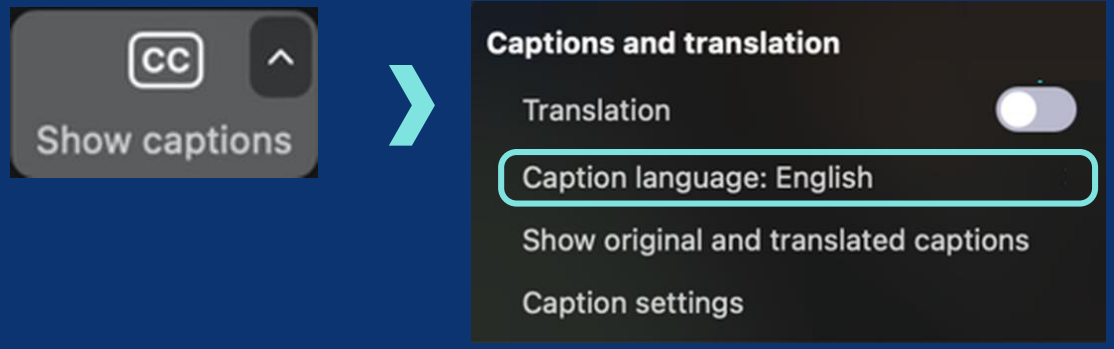
EVERYONE, PLEASE

Show your name + company in Zoom
Prefer not to share? Use 'OEM', 'SIP' or '…' instead

Turn on captions in your language
Closed captions (subtitles) for every speech

1 Click **Show captions**

2 Open **Caption language** and pick yours



GlobalPlatform

The Missing Standard

Why GlobalPlatform is talking to automotive **about security standardization**

1 EVERYONE BUILDS THEIR OWN

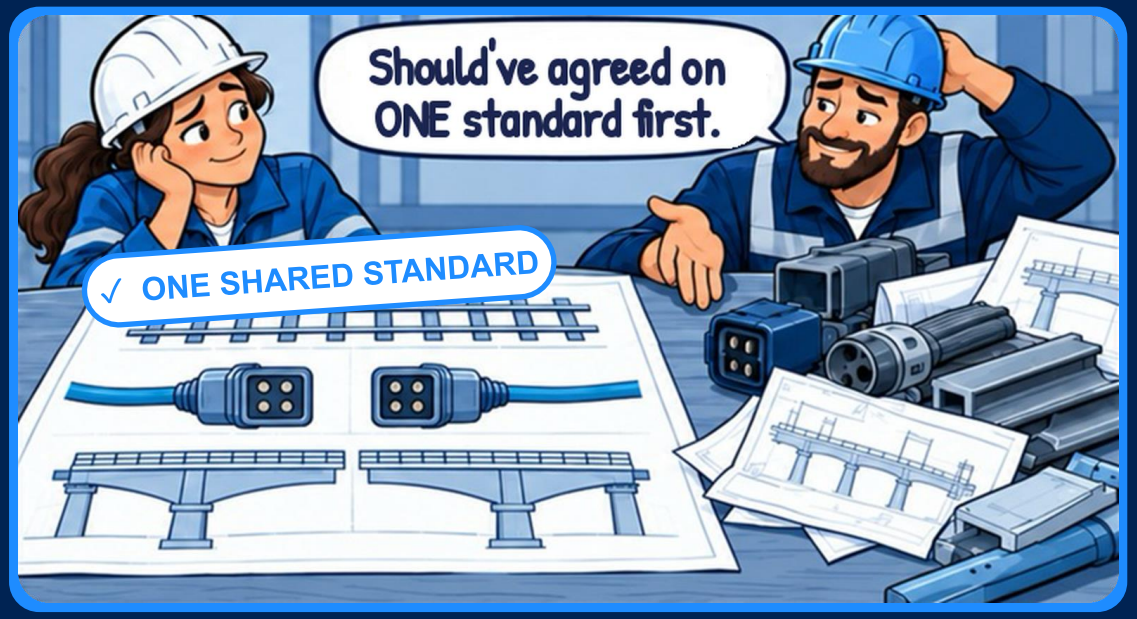
IN AUTOMOTIVE

Proprietary interfaces to secure hardware

IN AUTOMOTIVE

Security requirements rewritten for every program

2 THE LESSON



Agree on one standard up front, and every part fits. **That's what GlobalPlatform engagement builds.**

Engaging on standards scaled SIM, payment and identity. **Can automotive security afford to wait and see?**

Standardization Unlocks Scale

Every industry broke its inertia the same way: **not by inventing more technology, but by agreeing on a standard.**

	Fragmentation	Common standard	Scale	Ecosystem blossoms
Identity	Paper identity documents reach their limit	Governments choose GP technology	FIPS 201 PIV cards deployed across the US	**Multi-service cards: one credential, many uses**
Telecom	Services locked to each operator and handset	ETSI adopts GP for SIM; GSMA for eSIM	MNOs deploy services across any handset	**Phones now embed eSIM**
Payment	Local, incompatible payment schemes	EMVCo transactions + GP deployment infrastructure	One infrastructure for card and mobile	**Visa and Mastercard become the de facto means**
Automotive *today*	Closed, OEM-specific software stacks	Tesla patents, Android Automotive: open, but not a foundation	**The inflection point is visible.** Not yet crossed: scale and an ecosystem are waiting on a common standard.	

GlobalPlatform

Global Support For Industries Moving To Mass-market Security For Digital Services

100B+ technology deployments · **89B** Secure Elements shipped · **16B** devices with GlobalPlatform TEEs

Financial Services

14.7B

bank cards in circulation

96% of all card-present transactions

Mobile

5B+

smartphones with GlobalPlatform TEEs

9B active SIMs authenticating users and devices

Identity

1B+

ePassports issued by 140+ governments

Current Focus: Digital Wallets, SAM and CSP on SEs and eSIMs

IoT

SESIP

European Standard EN 17927

CRA-ready evaluation, aligned with PSA Certified

Automotive

335M+

vehicles with GlobalPlatform SEs and TEEs

IVI · digital car key · telematics secure channel

How GlobalPlatform takes industries to mass market

Standardize

Royalty-free SE, TEE and SESIP specifications,

Referenced by EMVCo, GSMA, ETSI, ISO and SAE

Certify

ISO/IEC 17065 accredited Certification Body; GlobalPlatform SESIP (EN 17927), PSA Certified schemes

Convene

Nearly 100 members and 40+ industry partners

across EMEA (46%), Asia Pacific (34%) and the Americas (20%)

Specifications: globalplatform.org/specs-library

Nearly 100 members, 40+ partners including OEMs

Silicon, software, banks, carriers, certification labs and governments and Automotive

Regional reach: EMEA 46% · Asia Pacific 34% · Americas 20%

Automotive voices at the table:
Stellantis, Toyota, CARIAD, Woven by Toyota, ETAS, Renesas, NXP, Infineon, ST, Qualcomm

SAE, AUTOSAR, COVESA, CCC and Auto-ISAC as partners

Partners set scope and requirements

GlobalPlatform writes the detailed specifications, profiles and certification

GlobalPlatform And Its Industry Alliances

Industry Alliances Set Scope & Requirements → **GlobalPlatform Develops Detailed Implementation Guidelines, Specifications, Test Suites, Common Profiles**

GSMA · ETSI · TCA · GCF
Scope: eSIM, RSP, UICC, SAM requirements; handset compliance
GP: SE spec, secure channels, eUICC certification

NFC Forum · FiRa · WPC
Scope: NFC, UWB, wireless power
GP: SEAC, OMAPI, SE as trust anchor

EMVCo · EPC
Scope: Payment application and security evaluation
GP: SE platform, composition model, certification

TCG · FIDO Alliance
Scope: TPM services, authenticator levels
GP: TPM services in TEE, SE PP for FIDO L3+

Global Platform®

The standard for secure digital services and devices

GlobalPlatform

SE · TEE · SESIP

Detailed specifications
Configurations
Protection profiles
Certification schemes
SESIP Mapping
Cryptographic Recommendations
Attack Working Group

SAE International
Scope: J3101 · J3101-5: hardware protected security environment
J3600: ISO/SAE 21434 assurance levels (CALs)
GP: Coverage report, automotive config, SESIP PP
SESIP as evidence for CALs & TAFs

AUTOSAR · CCC · Auto-ISAC · COVESA
Scope: Software stack, digital key, threat intel
GP: Crypto API mapping, MoU, coordination

CEN/CENELEC · ISO
Scope: Standards development: certification schemes, security frameworks
GP: SESIP (EN 17927), requirement mappings

NIST
Scope: Standards development, PQC, Traceability, security frameworks, Cyber Trust Mark Scheme SP8001319A Cryptographic Recommendations,
GP: Security Task Force, SESP Mapping, PQC algorithm recommendations

Formal joint deliverable or GP certification recognised by partner
Alignment mapping, MoU, liaison or joint working group
Work in progress, not yet published

Three Things For Secure Vehicles, Standardised Once

Two levels of protection for trusted code, and a common way to prove it is secure

INSIDE THE VEHICLE · TWO LEVELS OF TRUSTED EXECUTION

1 HARDENED

Dedicated tamper-resistant chip

Secure Element

Built to resist physical tampering

Holds keys and small trusted applications. GlobalPlatform defines how they are loaded, isolated, updated and managed remotely, for the life of the vehicle.

IN VEHICLES TODAY

- eSIM / eUICC
- Digital car keys
- EV charging
- Vehicle history
- Secure OTA updates

2 ISOLATED

Secure area of the main processor

Trusted Execution Environment

Shielded from the rest of the processor

Runs sensitive code with standard APIs for keys, storage and attestation.

Micro-TEE (planned) brings the same model to small ECUs.

IN VEHICLES TODAY

- Digital Rights Management
- IVI
- Biometrics
- ADAS model protection
- Secure OTA updates
- Vehicle history
- Telematics

certifies

INDEPENDENT

3 ASSURANCE

Optimised security assessment

SESIP

Certification with a common yardstick

- Supports functional security interoperability
- Profiles make product classes comparable
- Reusable certified components (ECUs,, SEs, TEEs, MCUs)

AUTOMOTIVE STANDARDS TODAY

ISO/SAE 21434	CAL/TAF objectives for components
ISO/SAE 8477	Addresses V&V methods
SAE J3322	Addresses testing methods

Make New Services Easier to Source, Add and Prove

GP gives OEMs a common foundation for protected services and component assurance.

OEM BENEFITS

Add Protected Services

Reuse an isolation and API baseline.

PROOF GP SE / TEE APIs; 5B+ phones

Buy with Defined Proof

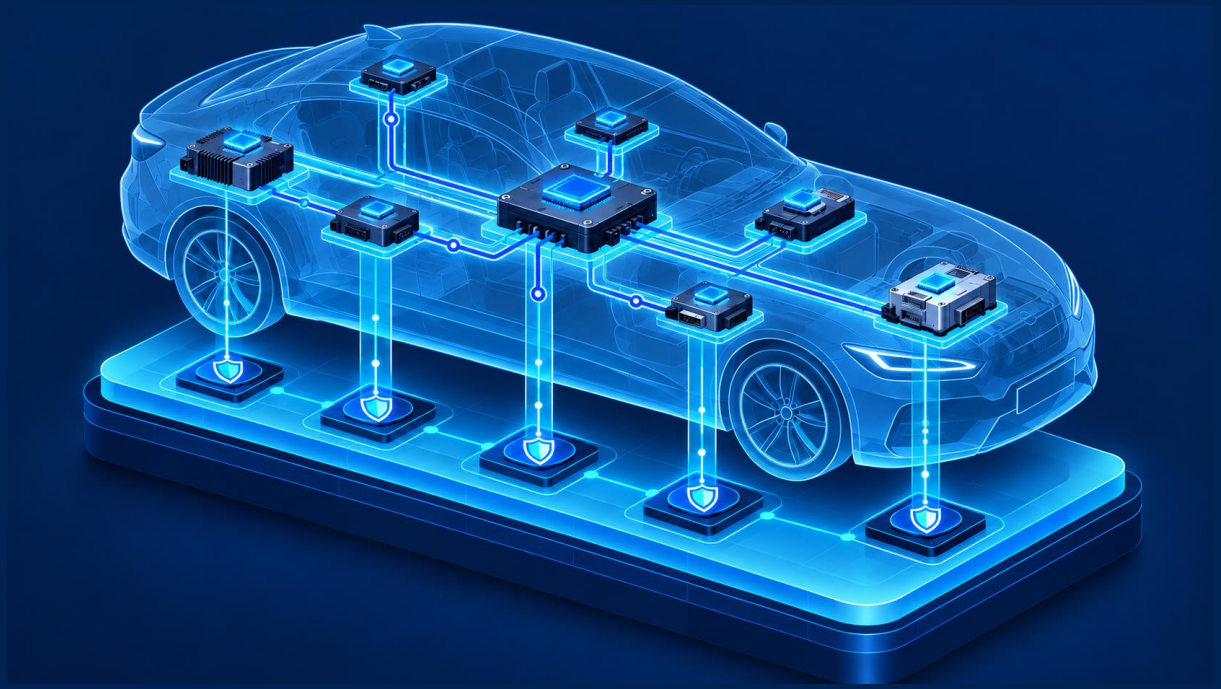
Compare component evidence before award.

PROOF SESIP EN 17927; 28+ certified products

Keep the Baseline Current

Refresh RFQ criteria as threats change.

PROOF GP crypto guidance; Automotive Task Force



GP Annual Report 2026: 100B+ deployments

COMPLEMENTARY ROLES

TCG	FIDO	GP
Device trust and attestation	User authentication	Protected apps, APIs and assurance

Global Platform™

The standard for secure digital services and devices

→globalplatform.org