Global Platform™

Cybersecurity Vehicle Forum - Beijing

24th September 2023

Ana Lattibeaudiere, CEO
Gil Bernabeu, CTO
Francesca Forestieri, Automotive Lead

Cybersecurity Vehicle Forum

Global Platform™

Welcome

Ana Lattibeaudiere, CEO 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**

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

Our Members

Full

ANALOG DEVICES — AHEAD OF WHAT'S POSSIBLE™
Apple
arm
Bundesamt für Sicherheit in der Informationstechnik
BCTC 银行卡检测中心 BANK CARD TEST CENTER
T..
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 品赢未来
DNP
DEPARTMENT OF DEFENSE — UNITED STATES OF AMERICA
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
TTL
TELUS
TOSHIBA
UBIVELOX
UNISOC
天喻信息
xardpay
XCURE CORP.
mi
BACTECH
Digital Cubes
INTERNET OF TRUST
MoneTECH
NEXTENDIS — INNOVATION CONSULTANCY
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

Everyone Get Connected!

EVERYONE

- Please join Zoom so you can take part in polls and interactive sessions
- Muting is not enough, you also have to have your speaker turned off

Tips

- Please put your name + company in Zoom
  (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

Global Platform™

Cybersecurity Vehicle Forum

Francesca Forestieri, Automotive Lead

Welcome China!

87 Participants
60 In Person

Cybersecurity Vehicle Forum

Automotive Value Chain

China EV100 中国电动汽车百人会

GWM

HOZON

Automotive Suppliers

ANN 安领

BOSCH

国科础石 KERNELSOFT

ZF

Global Platform™

Silicon & Solution Vendors

北京华弘 用芯识别数字世界

CEC 中国电子 | 华大智宝 HuaDa ZhiBao

交通 China T-Union 联合

东信和平 EASTCOMPEACE

CPK 信长城

FUDAN MICRO

Giesecke+Devrient

Powertime 时代新威

GOODiX

PQSHIELD

SAMSUNG ELECTRONICS

紫光同芯 TONGXIN MICRO

STi life.augmented

Watchdata

W.UNITED 万协通

GP Solutions

HUAWEI

NXP

天喻信息 用科技构建安全智慧的数字

TRUSTONIC

THALES Building a future we can all trust

UNISOC

winbond

Industry Organizations

AUTOSAR

Global Platform™

Universities

北京理工大学 BEIJING INSTITUTE OF TECHNOLOGY

CICV 创新中心 组织者

Test Labs

BACTECH

SGS brightsigl

国家金融科技测评中心 National FinTech Evaluation Center
银行卡检测中心 Bank Card Test Center

TÜV NORD

OPLS Lab

VALID

riscure

Broader Ecosystem

AFW

Digital Cubes

FEITIAN WE BUILD SECURITY

GEETEST

NAGA·IN

accenture

protiviti Global Business Consulting 甫瀚

中海庭 HEADING DATA INTELLIGENCE

Why GlobalPlatform: Market Presence in Automotive

Secure Element

OVER 192 Million Connected Cars in 2023

- Digital Car Key
- Electrical Vehicle Charging
- All eUICCs (embedded Sims)
- Key Management

Trusted Execution Environment

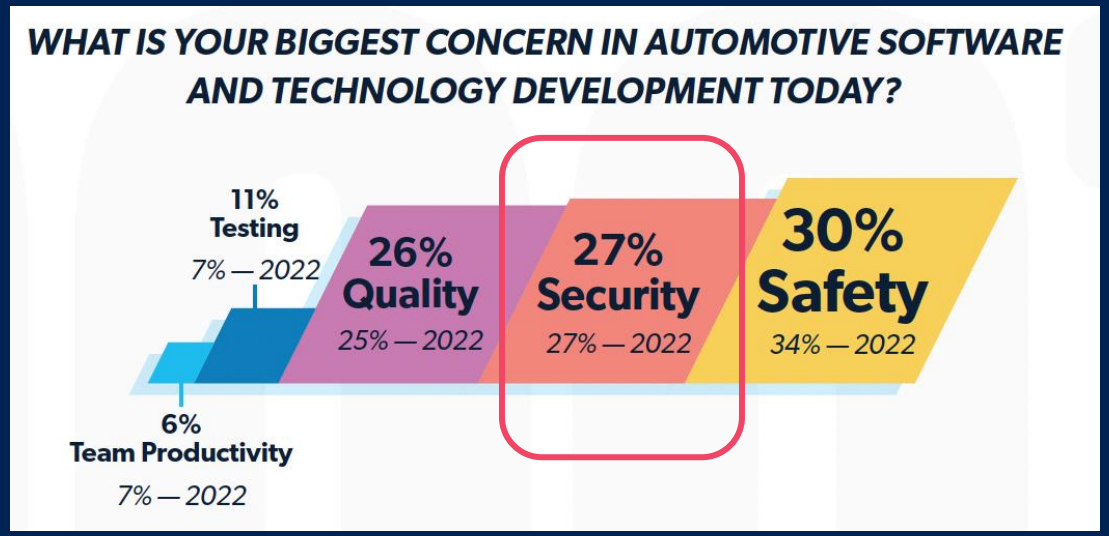
In Over 100 Million Vehicles as of 2023*

- Digital Rights Management / Media for Advanced Infotainment
- Protecting High Value Assets such as ADAS
- Key and Certificate management
- Personal Data and Biometric

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

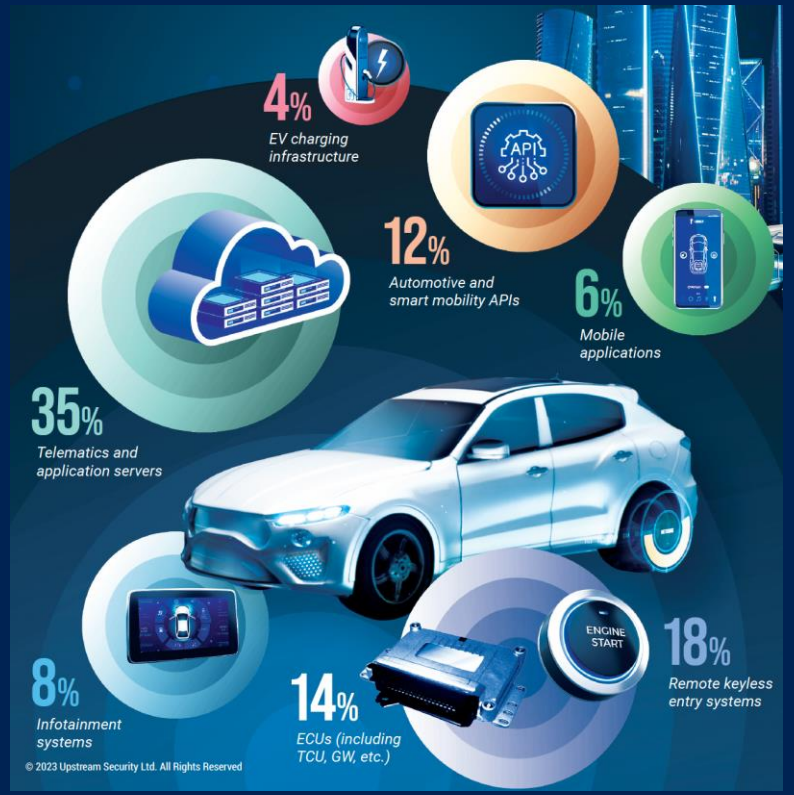
Security Remains a Leading Challenge in Automotive Software Development 2023



Source: Automotive IQ, *2023 State of Automotive Software Development Report*
https://www.automotive-iq.com/autonomous-drive/reports/2023-state-of-automotive-software-development-report?ty-ur

Based on: *an anonymous survey conducted between January 9 and February 20, 2023. It targeted automotive professionals from across the globe and received 400 responses*

Wide-spread Automotive Attack Vectors

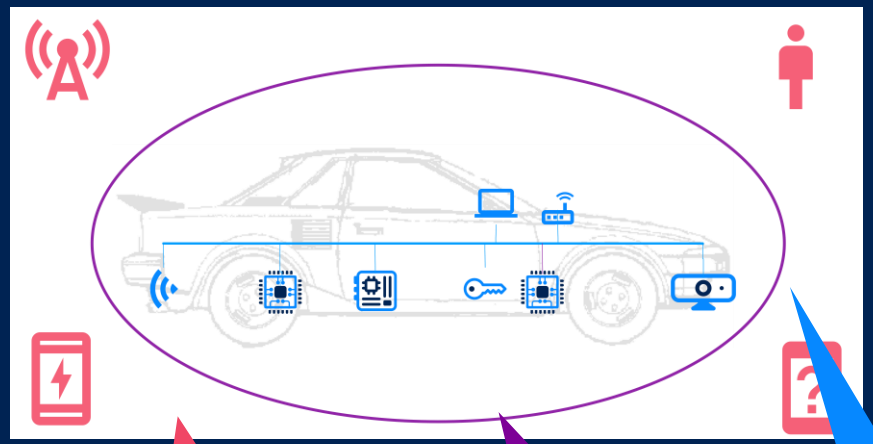


https://upstream.auto/reports/h1-2023-automotive-cyber-trend-report/

Global Platform™

Automotive Security Paradigm Has Shifted Towards Zero Trust

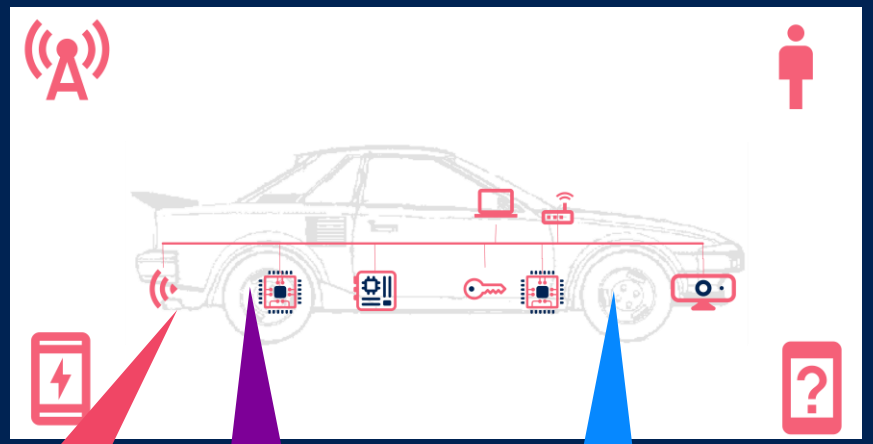
Walled Garden



- Everything outside the perimeter is untrusted
- Physical protection or firewall
- Everything inside the firewall is trusted

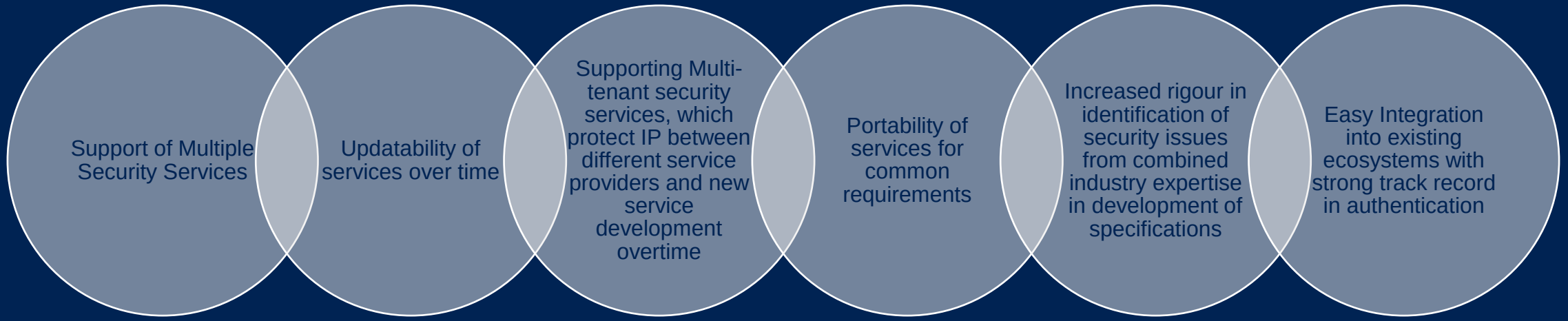
Versus

Zero Trust

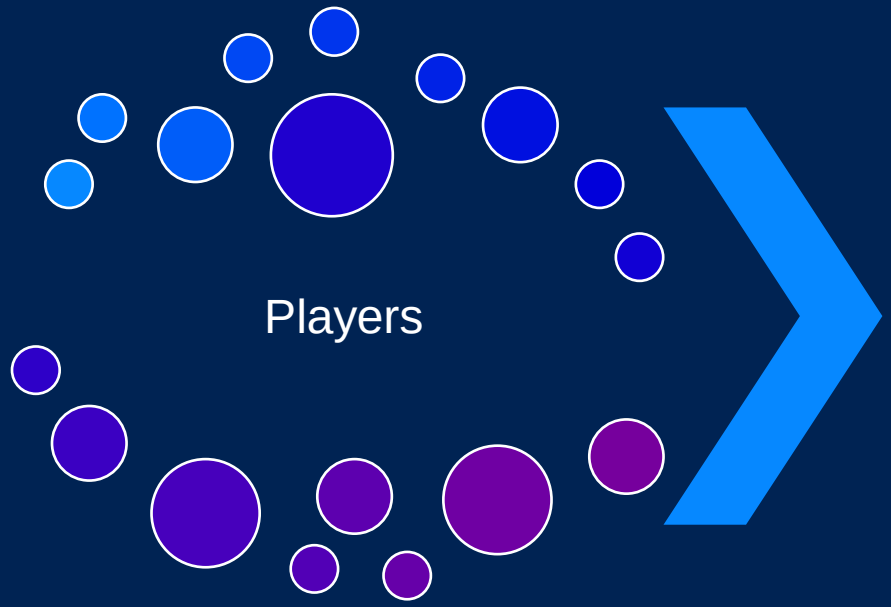


- Everything is untrusted
- Each component verifies that others are trustworthy
- Interaction operates on “least privilege” basis

Future Proofing Security: Adding Flexibility



What is the Cybersecurity Vehicle Forum?



- 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

Agenda

13:30	Welcome	Ana Lattibeaudiere, CEO GlobalPlatform
13:40	Presentation of Automotive Objectives of GlobalPlatform & the Cybersecurity Vehicle Forum	Francesca Forestieri, Automotive Lead GlobalPlatform
14:10	Security Across the Wider Value Chain	Zhe Jing, Bosch & Autosar
14:40	Break	
15:10	GlobalPlatform Technology Overview Standards Alignment Benefits for Secure Components in Automotive	Gil Bernabeu, CTO GlobalPlatform
15:50	SESIP Certification & ISO/SAE 21434 Guidelines for Automotive Chip Standardization Systems	Junjiang Zhang, NXP
16:20	GlobalPlatform Automotive Use Cases • Secure Components and eSE • Trusted Execution Environments	SUNG Kiseung ,Thales Jason Lin, Trustonic
17:20	Priorities for automotive activities in China FY24 Discussion	Harry Wang, Head of Strategic Engagement APAC and Francesca Forestieri, Automotive Lead
17:30	End of Meeting	

Objectives

Exchange

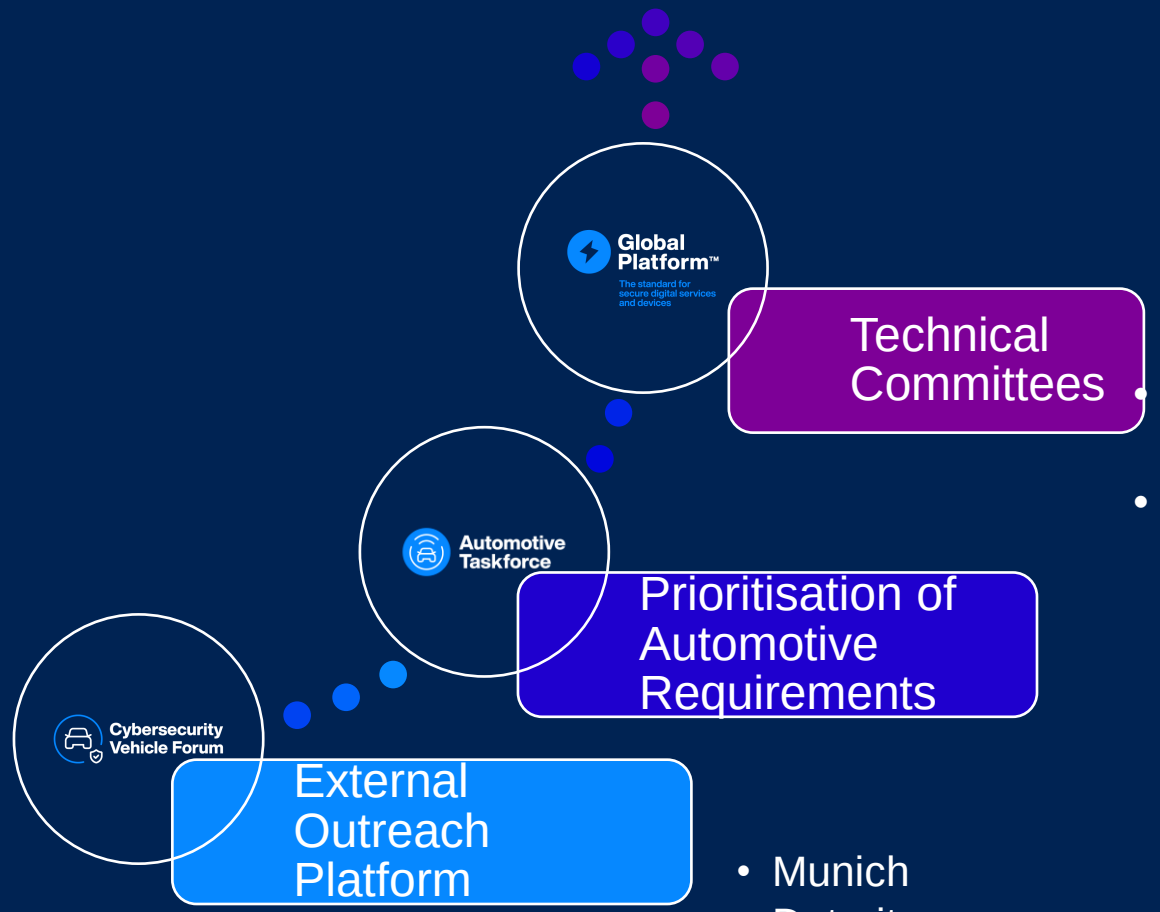
Increasing Understanding

Contribute to Supporting Needs

Opportunities for Cross-Industry Engagement

Determine Regional Needs

How CSVF Input Drives Changes



- Specifications Update
- Guidelines Development

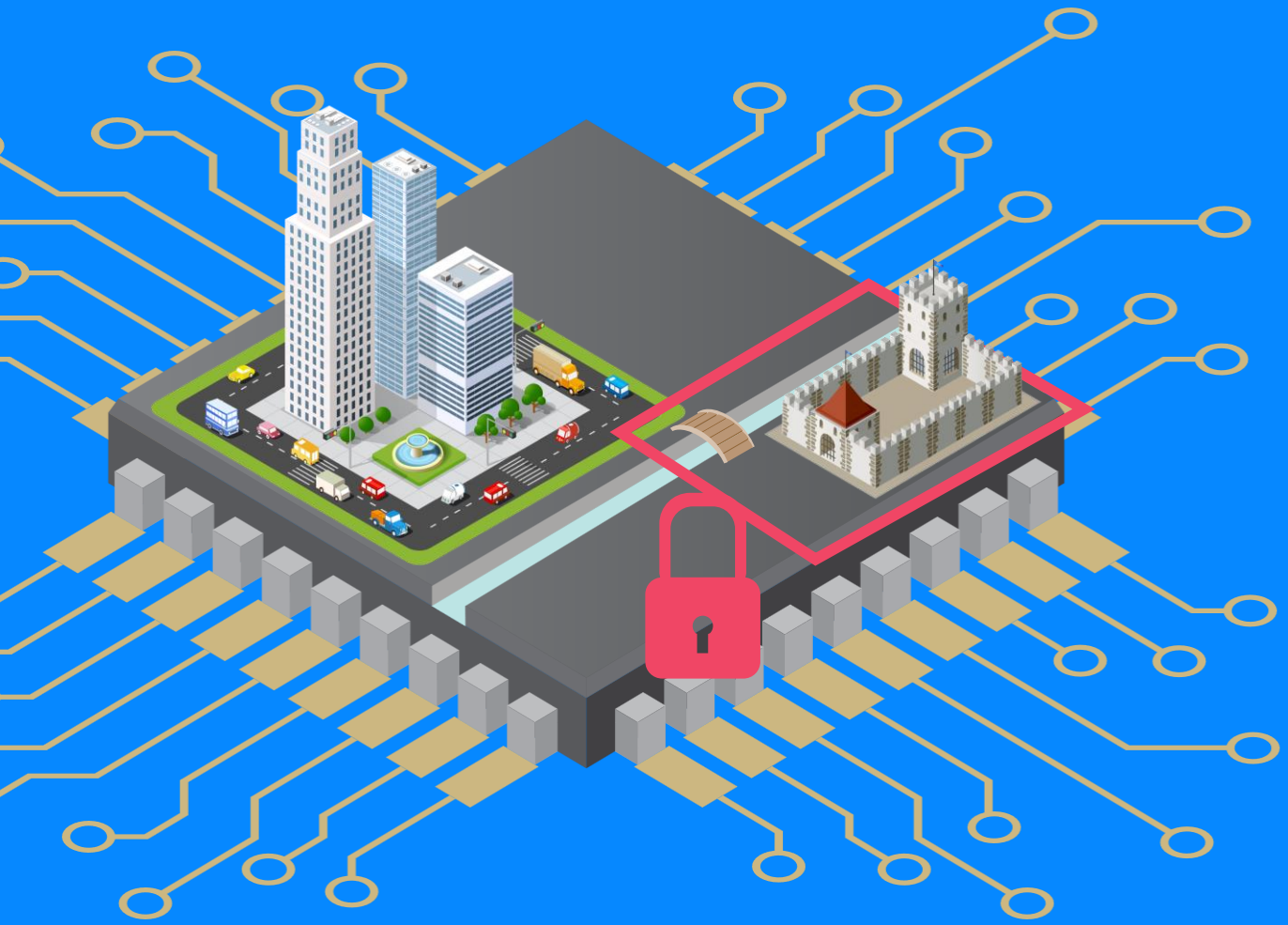
- Munich
- Detroit
- Tokyo
- Beijing
- Hamburg

Global Platform™

GlobalPlatform Technology

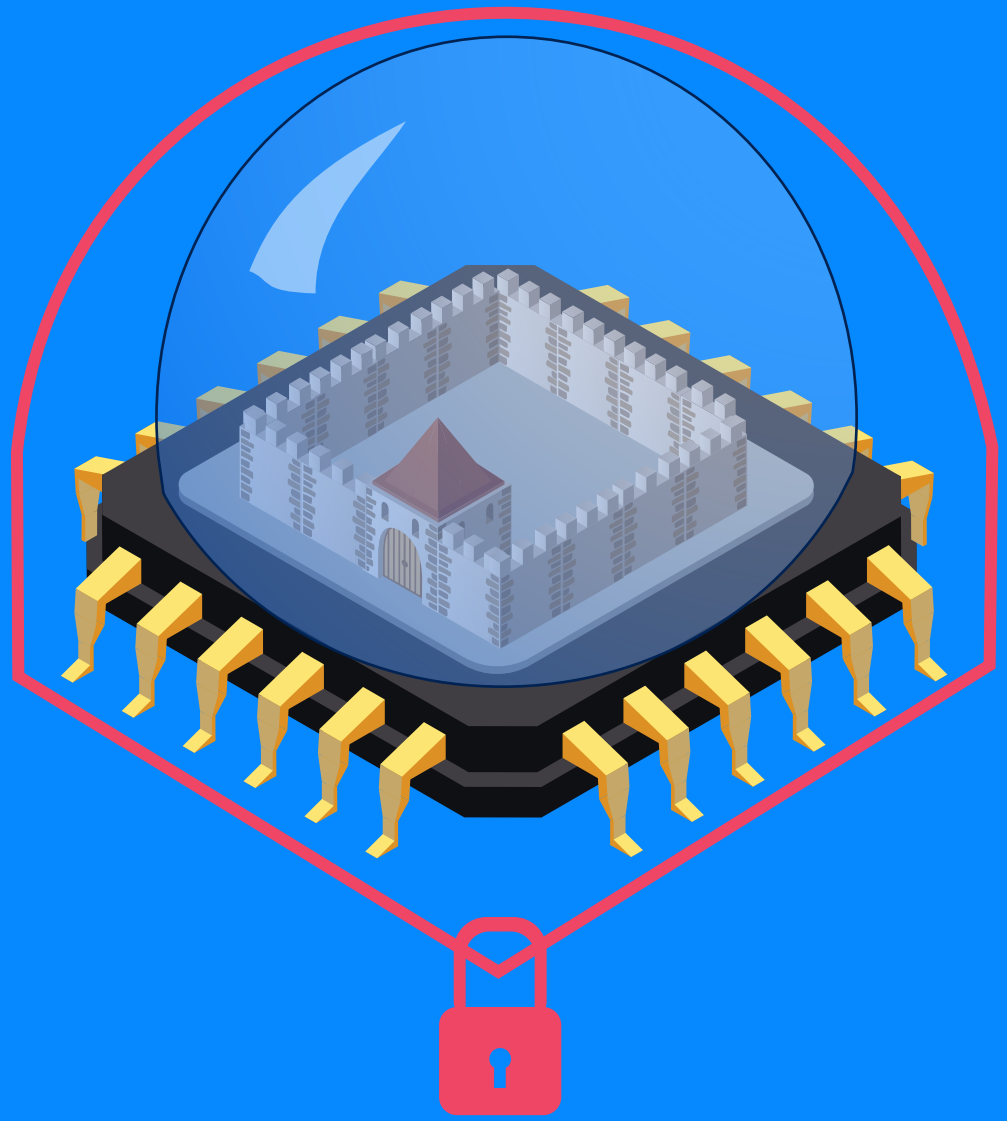
Gil Bernabeu, CTO

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

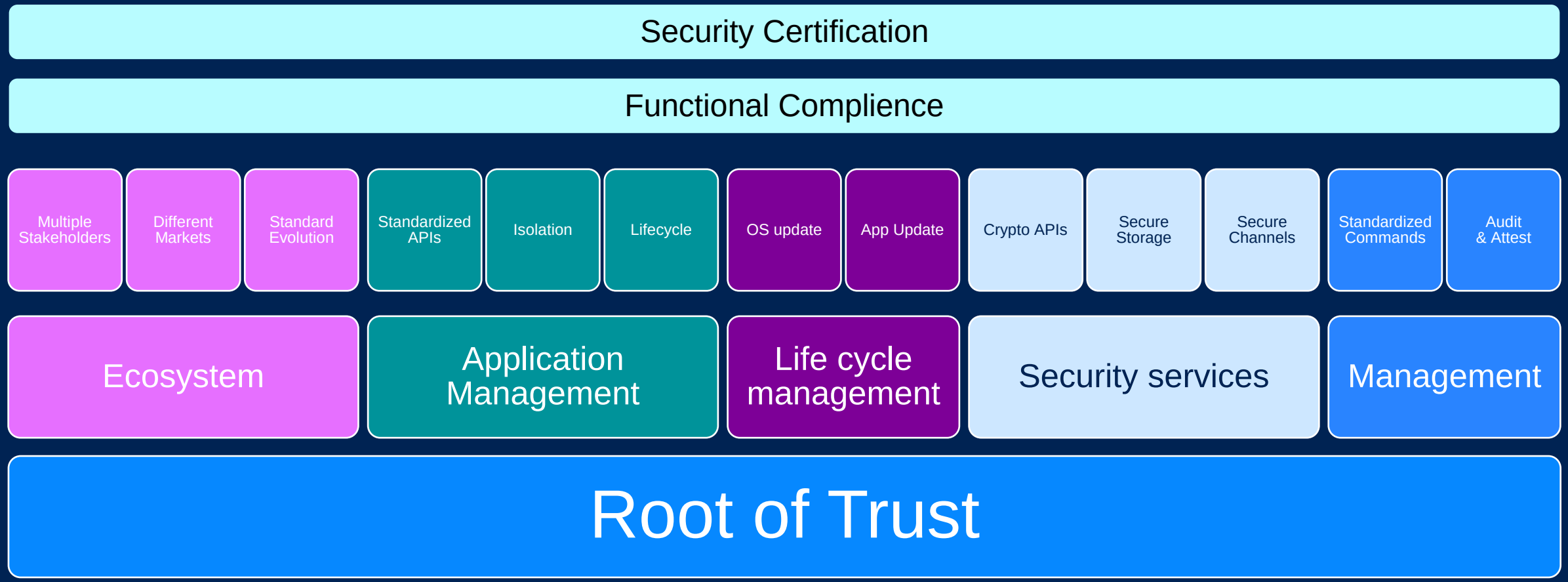
GlobalPlatform Secure Element



- 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



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

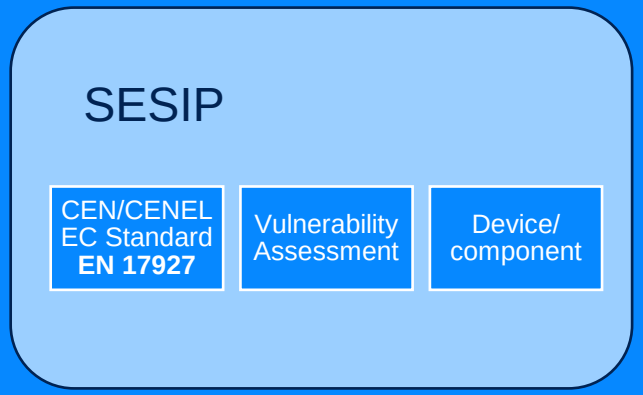
The protection profile can then be used by 3rd party labs to validate a product meets the agreed security level

Common Criteria

SESIP

Evaluation Methodology

SESIP



Structured Security Methodology

Designed to not require security expertise for use

Functional Requirements	Assurance Requirements

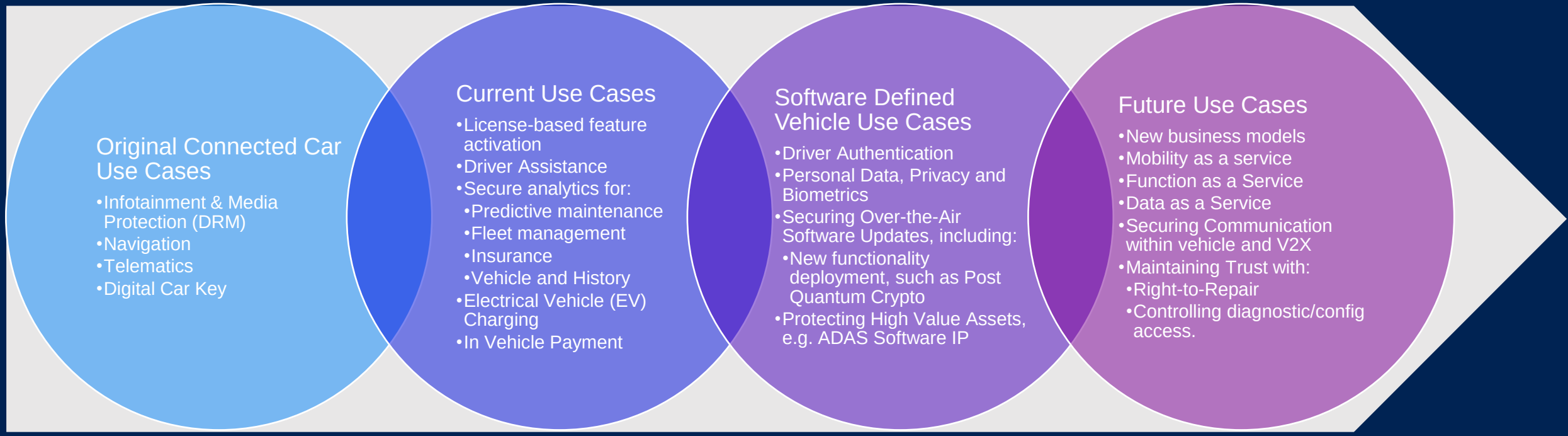
Global Platform™

GlobalPlatform specifications are freely available

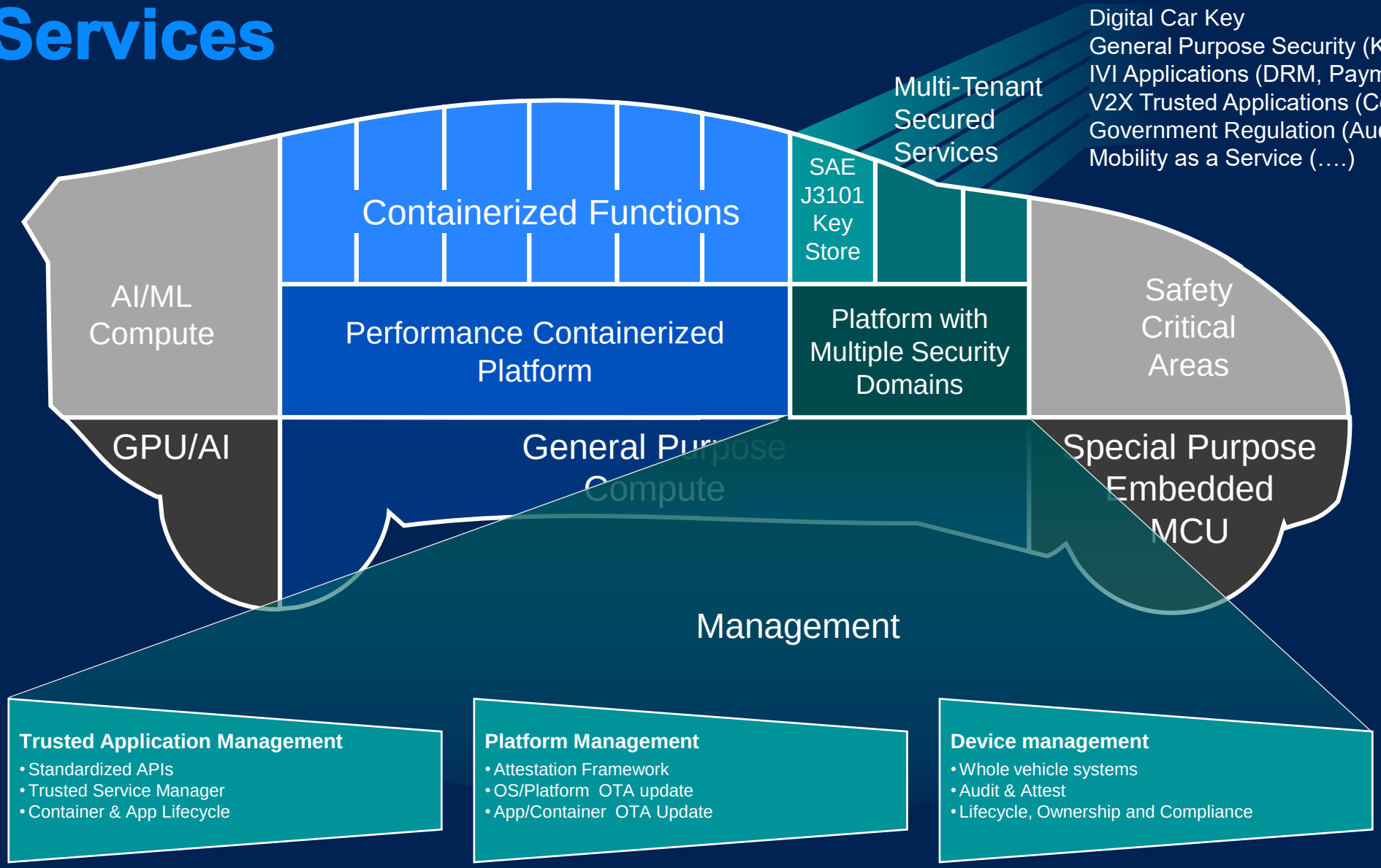
GlobalPlatform Specifications: https://globalplatform.org/specs-library/

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 Supports the Evolution Path for Security Critical Use Case



GlobalPlatform Technologies Supporting Value-Added Services



Global Platform™

GlobalPlatform Automotive Initiative

Francesca Forestieri, Automotive Lead

How GlobalPlatform Works for Automotive

Participation in GlobalPlatform Automotive Activities

Cybersecurity Vehicle Forum

- 103 participants in Detroit June 20th Forum
- An average around 70 persons participating
- Majority of non-GlobalPlatform participants

Members of Automotive Task Force

- 121 Individuals
- 49 Companies
- 63 documents submitted

Automotive Goals: Standardising Roots of Trust in Software Defined Vehicles

Alignment with Automotive "Standards" Alignment

Mapping of Alignment with Specifications for Secure Elements and Trusted Execution Environments

- J3101 Hardware Protected Security Environments Recommended Practice
- Autosar Adaptive Platform

Develop Automotive Configuration

- Secure Element
- Trusted Execution Environment

Decision on development of trusted applications, e.g.

- Key Store for J3101

Support ISO/SAE Compliance

- 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

Automotive Organizations

Society of Automotive Engineers (SAE Intl: USA + Small Chinese Office) is standardizing Security for Hardware Protected Security Environments (J3101). The current recommended best practices does not provide lacks implementation guidelines and insufficient details to foster comparability of products.

Opportunity for GlobalPlatform to demonstrate implementation and to generate compliance documentation to standard.

AUTomotive Open System Architecture (AUTOSAR) is the standardized software framework and open E/E system architecture for intelligent mobility.

The platform is supported internationally by 10 OEMs and is deployed widelye internationally

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

Process

ISO /SAE 21434

+

Product

SAE J3101 Hardware Protected Security Environments

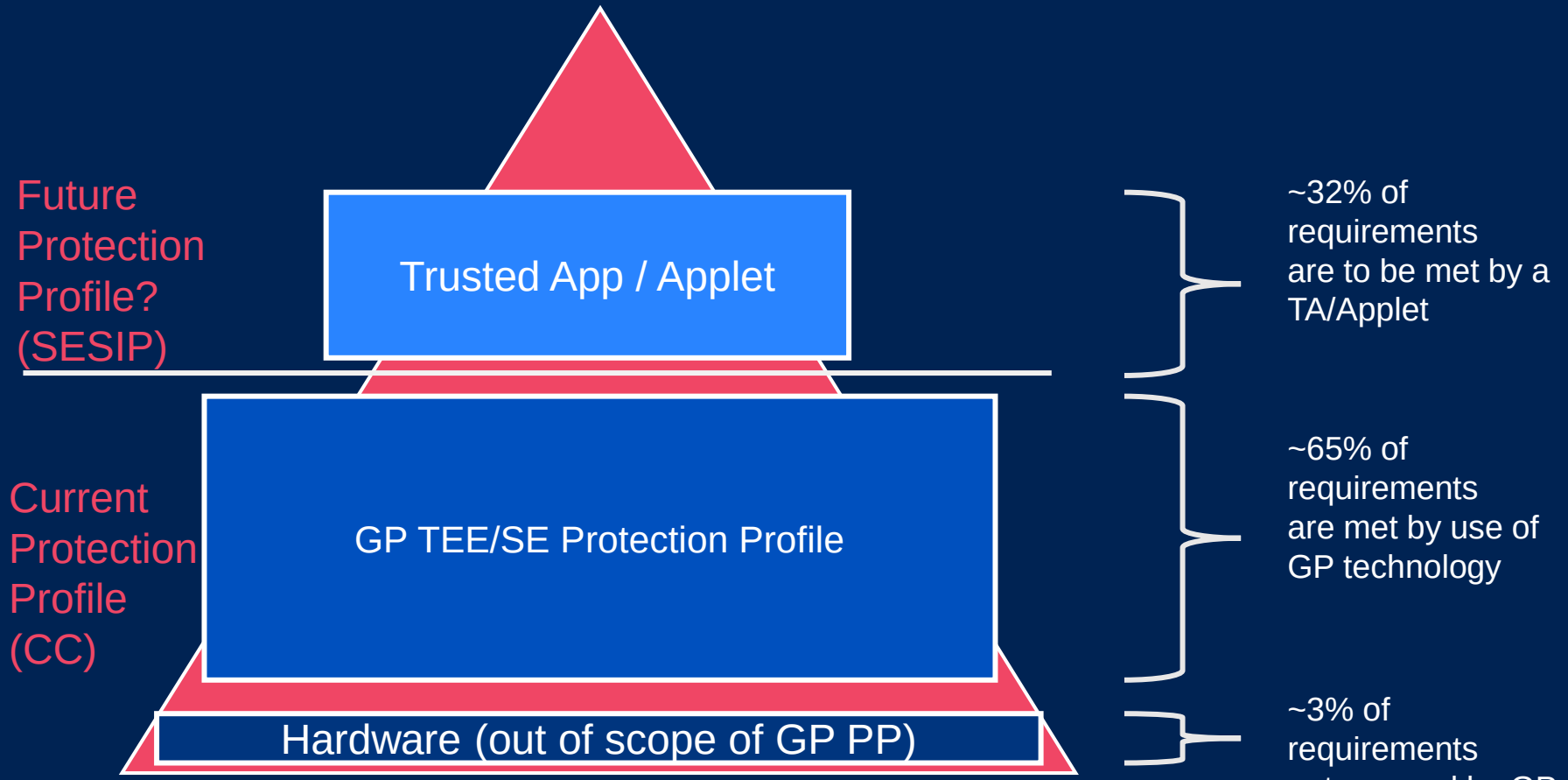
=

Compliance

Cybersecurity Vehicle Management

- Compliance with UNECE 155
- Demonstration of Best Practices

Security “How”: GlobalPlatform to J3101



GlobalPlatform is planning to develop an automotive configuration for our technology applied to the J3101 requirements. We are also assessing the utility of developing the trusted applet/applications defined in J3101, e.g. the keystore.

In this way, GlobalPlatform technology can be one way to “guarantee” full compliance with J3101’s requirements.

Next Dates for Technical Alignment

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

- Sept 27th

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 10/11 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

Global Platform™

Next Steps: Engagement on Automotive in China

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

Decisions to be Made

Potential Regional Synergies

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:

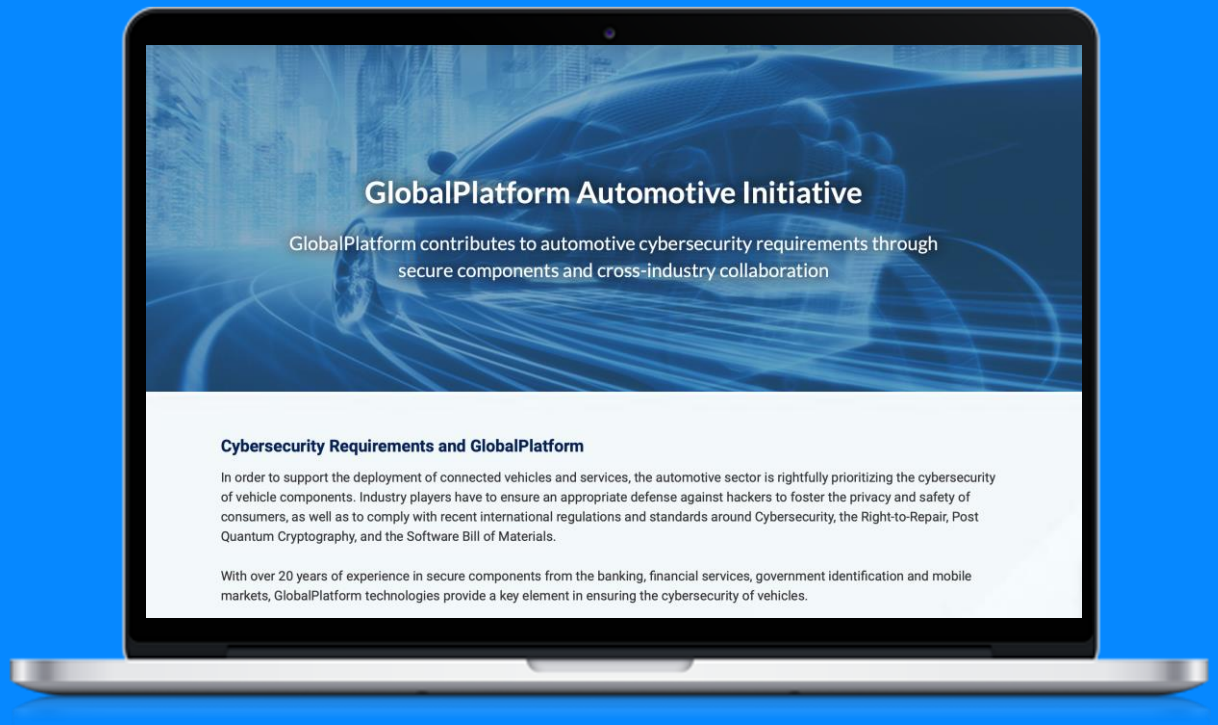
- How to Drive Security Best Practices for Products?

Autosar

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

Specific Chinese Market Requirements and Use Cases

Get Involved



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

Global Platform™

The standard for secure digital services and devices

→globalplatform.org

Approaches to Root of Trust on Devices

Comparing Different Trust Anchors: "Generalizations"

	Trusted Computing Group			GlobalPlatform		Automotive HSM/ Secure Enclave (Proprietary)
	DICE	MARS	TPM	Secure Element	Trusted Execution Environment	
Size	Very small (~20kB+)	Very small (~8kB)	Small implementation (~150kB+)	Mid-size implementation (~350kB)	Large implementation (>1MB)	Mid-size implementation (generally ~250kB)
APIs	Client API not standardized	Simple client API	Rich client API	Rich internal application APIs	Rich client and internal application APIs	Proprietary APIs
System Binding	Closely bound to system	Loosely bound to system	Loosely bound to system	Loosely bound to the system	Closely bound to system	Tightly bound to the system
Tenant Capability	Single tenant	Single tenant	Limited multi-tenant capability	Rich multi-tenant capability	Rich multi-tenant capability	Single tenant (generally)
Certification	Probably not certified	Probably not certified	Usually high assurance (EAL4+)	Always high assurance (EAL4+)	Often medium assurance (EAL2+)	Probably not certified
Breadth of Security Services, including: -OTA Updates	Partially standardized	Limited set of services	Designed to do a fixed set of services very well (e.g., measured boot)	Any type of secure services can be added with Trusted Applets	Any type of secure services can be added with Trusted Applications	HSM implementations embrace many different versions depending upon supplier
-Security Use Case	N/A	N/A	Proprietary	OTA Updatable in a Standardised Manner	OTA Updatable in a Standardised Manner	
		Less expensive		Designed to support flexibility in high security use cases with more limited performance requirements	Designed to support flexibility in supporting security use cases for multiple service types with higher performance requirements (e.g. 20-50 X faster)	
Examples of Implementation Hardware	Usually MCU class	Usually MCU class runs at native clock rates	Usually dedicated 32 bit MCU running at 10-24 MHZ	Ex. CPU Class 32 bit MCU running at 50MHZ	Ex. CPU Class Cortex A8 64 bit at 2GHZ or more	Could be any variation – tends toward MCU class