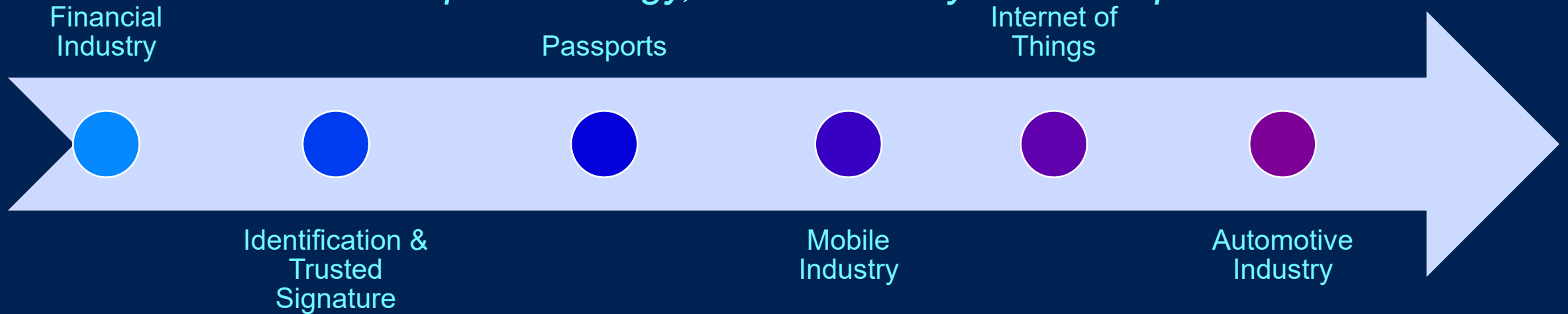# GlobalPlatform Overview

22nd May 2025

Richard Hayton,
GlobalPlatform Board Member, Chair of TES Committee and Automotive Task Force
Francesca Forestieri,
GlobalPlatform Automotive Lead

GlobalPlatform

*THE standard for managing applications on
secure chip technology, with over 25 years of experience*

Financial
Industry

Passports

Internet of
Things

Identification &
Trusted
Signature
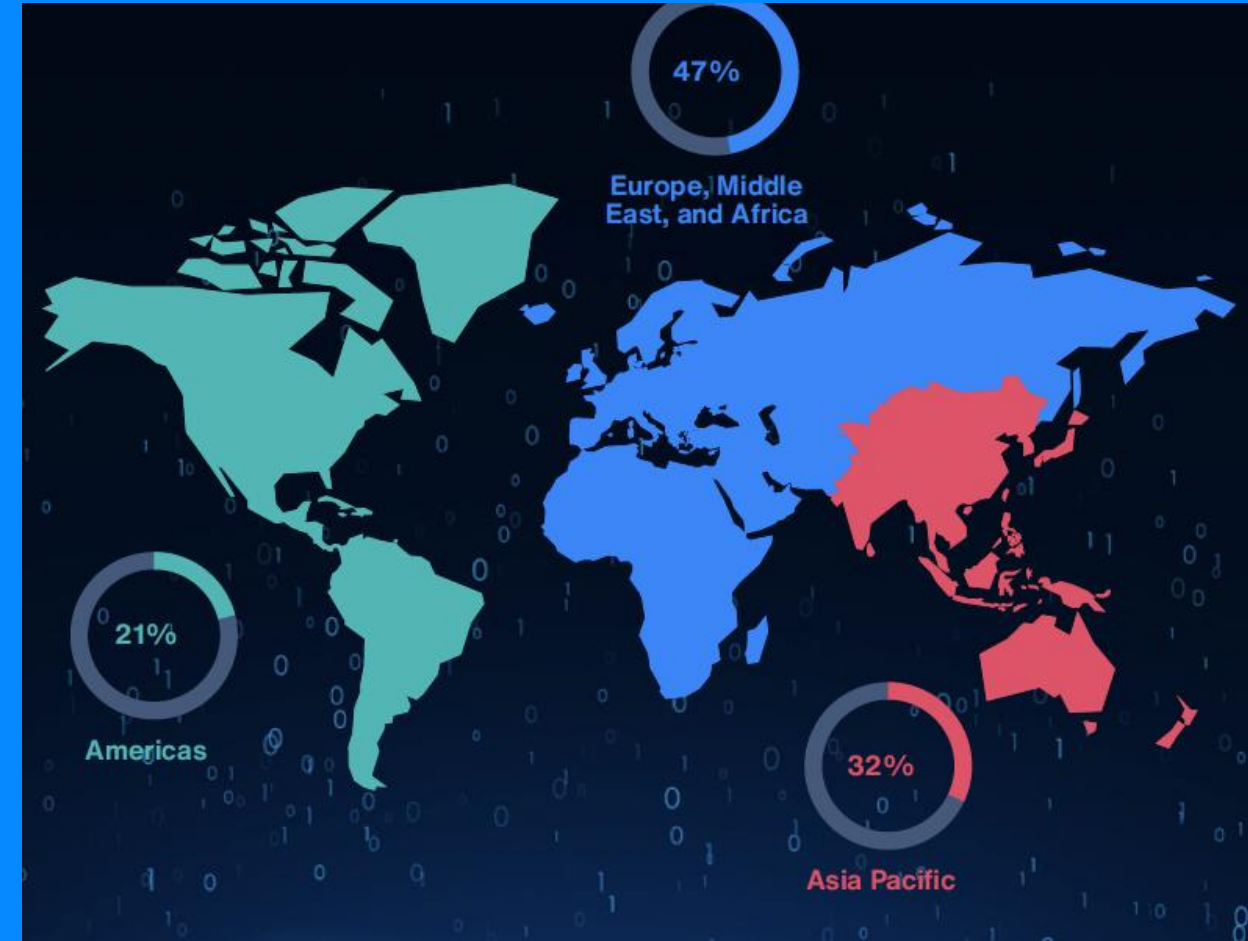
Mobile
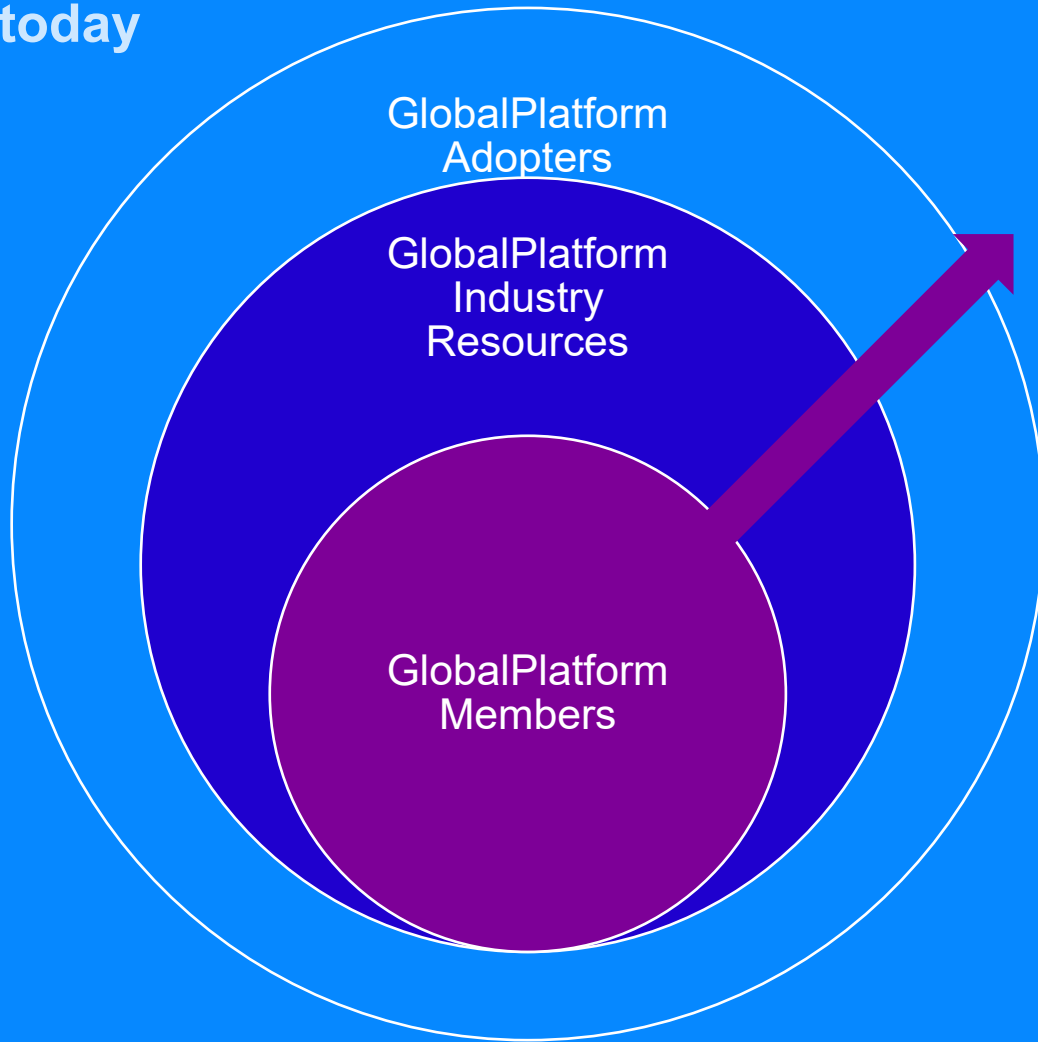Industry

Automotive
Industry

Mass Market deployment of industries has required: agreed functionality for transactions and transparent robust security to create trust among competitors and in the overall ecosystem

GlobalPlatform Specifications: Royalty Free Use: https://globalplatform.org/specs-library/

GlobalPlatform's Market Adoption

- **70 billion+ Secure Elements shipped worldwide are based on GlobalPlatform specifications**
- **Over 10's of billions GlobalPlatform-compliant Trusted Execution Environment in the market today**

GlobalPlatform
Adopters

GlobalPlatform
Industry
Resources

GlobalPlatform
Members

47%
Europe, Middle East, and Africa

21%
Americas

32%
Asia Pacific

Global Platform™

Our Members

Full
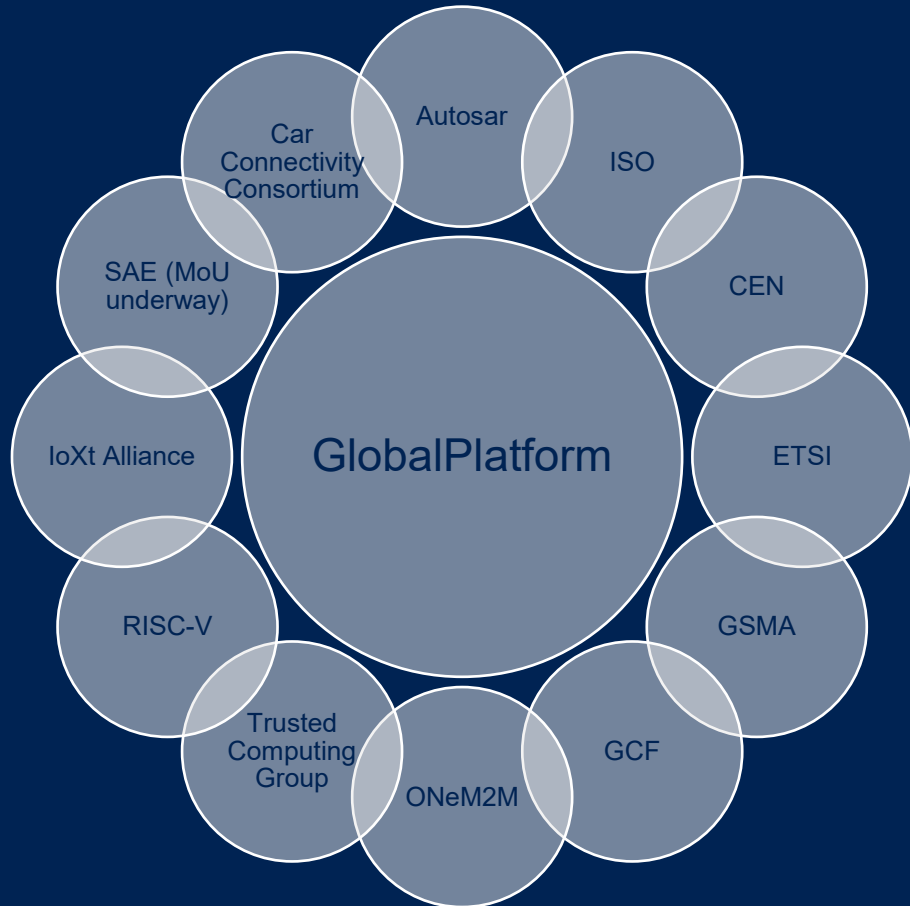
Participant

Observer

Public Entity

Consultants

Your Partner for Security 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 Brings Lessons to Automotive:
How to Create the Security Foundation for a Healthy, Innovative Ecosystem Services

GlobalPlatform standards create a fertile environment for mass market growth and innovation of services and hardware

Services are key dynamic of industry BUT hardware remains a critical base for trust

High Evolution in Markets over time, with issuance of new services on very short timelines (3-6 months).

With standardised portability and updatability, device product life is extended since it can adapt to requirements of new services.

Synergistic opportunities (also across "Frenemies") for the development of new services (not everything has to be developed from scratch by a provider)

Based upon GlobalPlatform's Experience in Over 25 Years with Smart Cards, Mobile, IoT

Global Platform™

What GlobalPlatform in Automotive?

Challenges of Automotive Security Market Today

Proprietary Application Ecosystem

Proprietary Key Lifecycle Management (Provisioning And Decommissioning)

Proprietary Implementation of Cryptography

Vendor Lock-In

Lack of Clear Metrics on Security Robustness

Device Identification And Update

Fragmentation of Secure Boot Requirements

Lack of Incremental Build Upon Solutions (each new service requires a new ECU)

Difficulty in managing trust over extended value chain with new service providers (beyond OEMs)

WHAT NEXT?

Global Platform™

Largest Threat Surface In The World

Attack Surfaces

Attack on OBD2

Compromised Actuator

Remote Attack on Vehicle Bus

Malware Delivery thru Data Storage Device

Attack on Key/ Certificate Stores

Telematic/ Cellular

V2X

In Car Network

Sensors

Key Fob

IVI system

Supply Chain - HW

Supply Chain - SW

Exploiting SW Vulnerabilities

Sniffing of User Data

Attack from Mobile Device

Attack from Download Apps

Man-in-the-Middle Attack

Malicious Firmware Update

150+ Million Lines of Codes

1000s file systems

ECUs · Domain Controllers · Access to buses thru exposed wires · Telematics Units · Onboard Diagnostics · Smart Phone connection · IVI Systems · In-Vehicle network · Software Update Process · Open debug ports · Toll comms · Vehicle data servers · Other wireless Comm · Object detection sensors · Cloud based Network · On-board Diagnostics ports · OODBII port · Vehicle sensors and cameras · Remote keys, Fobs

Different Security Paths by Automotive OEMs

Everyone on their Own

- "Lowest Cost - Minimal Security" -
- "Customers don't pay extra for security"
- "We will deal with it later"

Highest Investment to Protect IP

- "We will buy the best security out there"
- *But...will that be enough?*
- *will vendor lock-in be a problem?*

Implementing Standardisation for Common Automotive Security Requirements

- Community determines jointly key features
- Community monitors evolving threats and develop solutions to platforms
- Individual Vendors focus Engineering on Differentiating Services
- Portability of Security Services

Low Cost,
High Risk
Potentially Untenable Future

Higher Cost,
Lower Risk Today
Unclear Future

Shared Cost (split between participants)
Lower Risk Today & Future
Provides Needed Future Flexibility

Global Platform™

No one wants to pay for "Security" BUT ….
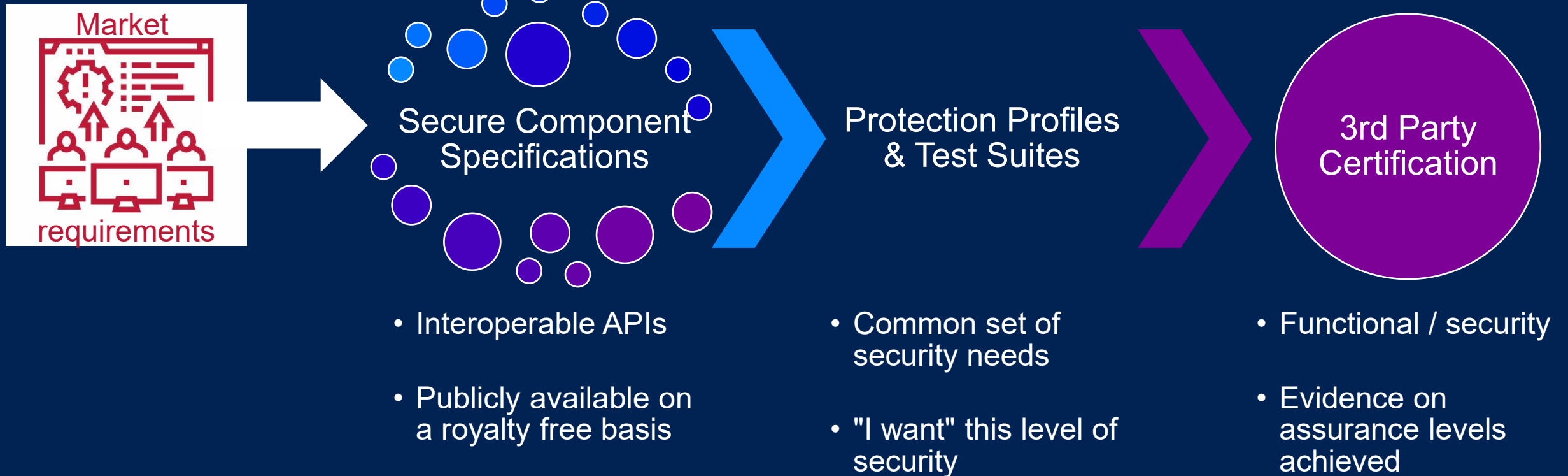# OEMs have Increased Skin in the game to warrant Cybersecurity Spend

Regulatory Compliance & Reducing Liability

- Compliance with Cybersecurity Management Processes for type approval (UNECE 155 64 countries)
- Evidence of implementation of best practices

Protecting Investments

- Protecting High Value of Software Assets of Vehicle
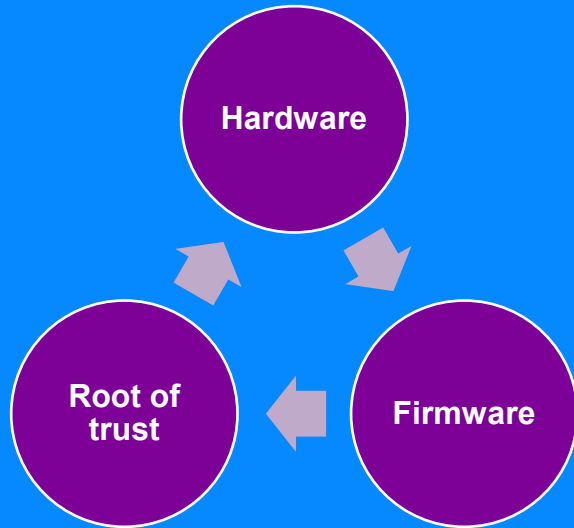- **Protecting Against Unpaid Feature Enablement**
- **Reduction of Warranty Fraud**

Global Platform™

International Digital Security Transformation: GlobalPlatform's Recipe for Success

Market requirements

Secure Component Specifications

- Interoperable APIs
- Publicly available on a royalty free basis

Protection Profiles & Test Suites

- Common set of security needs
- "I want" this level of security

3rd Party Certification

- Functional / security
- Evidence on assurance levels achieved

GlobalPlatform Specifications: Royalty Free Use: https://globalplatform.org/specs-library/

GlobalPlatform Technology

GlobalPlatform Foundation Technologies

Hardware

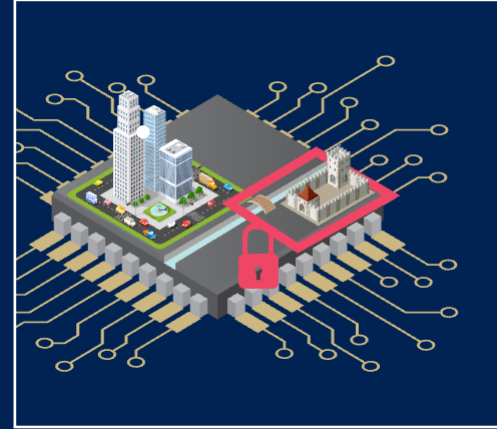**Root of trust**

Firmware

Secure Element
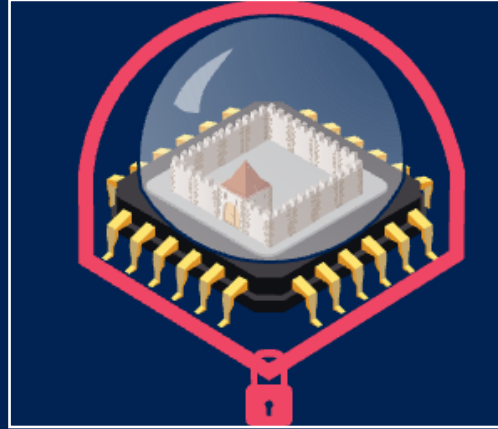
A secure enclave protected against physical and software attack
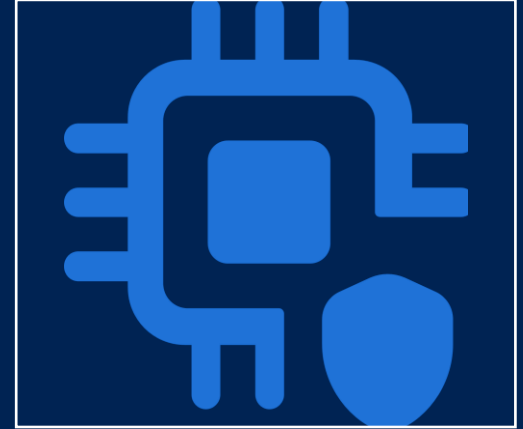
- In OVER 192 Million Connected Cars in 2023

Trusted Execution Environment

A secure operating system running on a standard CPU alongside regular OS/Applications

- In Over 100 Million Vehicles as of 2023
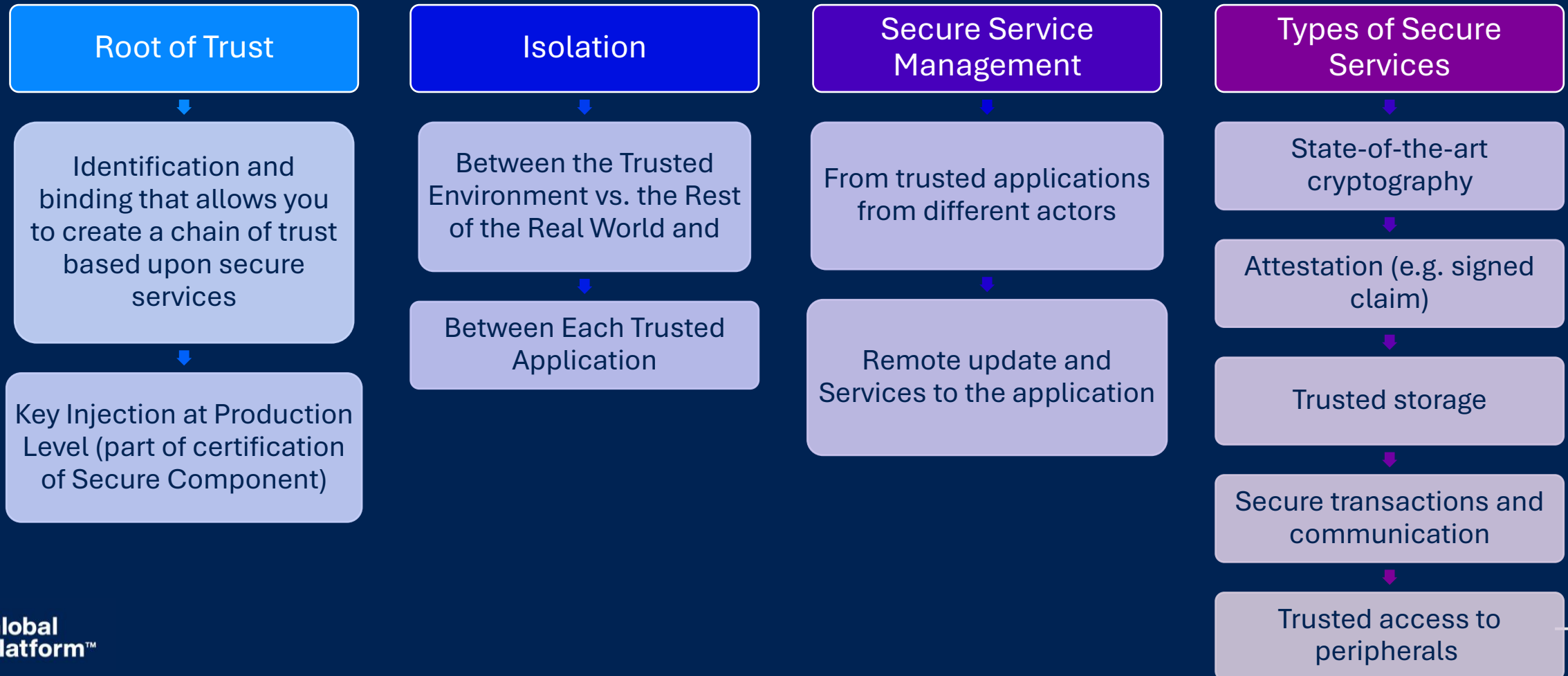
Isolation Technologies

Higher level services and broad capabilities to support specific use cases

For example, APIs and capabilities of keystores that might be implemented in SEs, TEEs or other technologies.
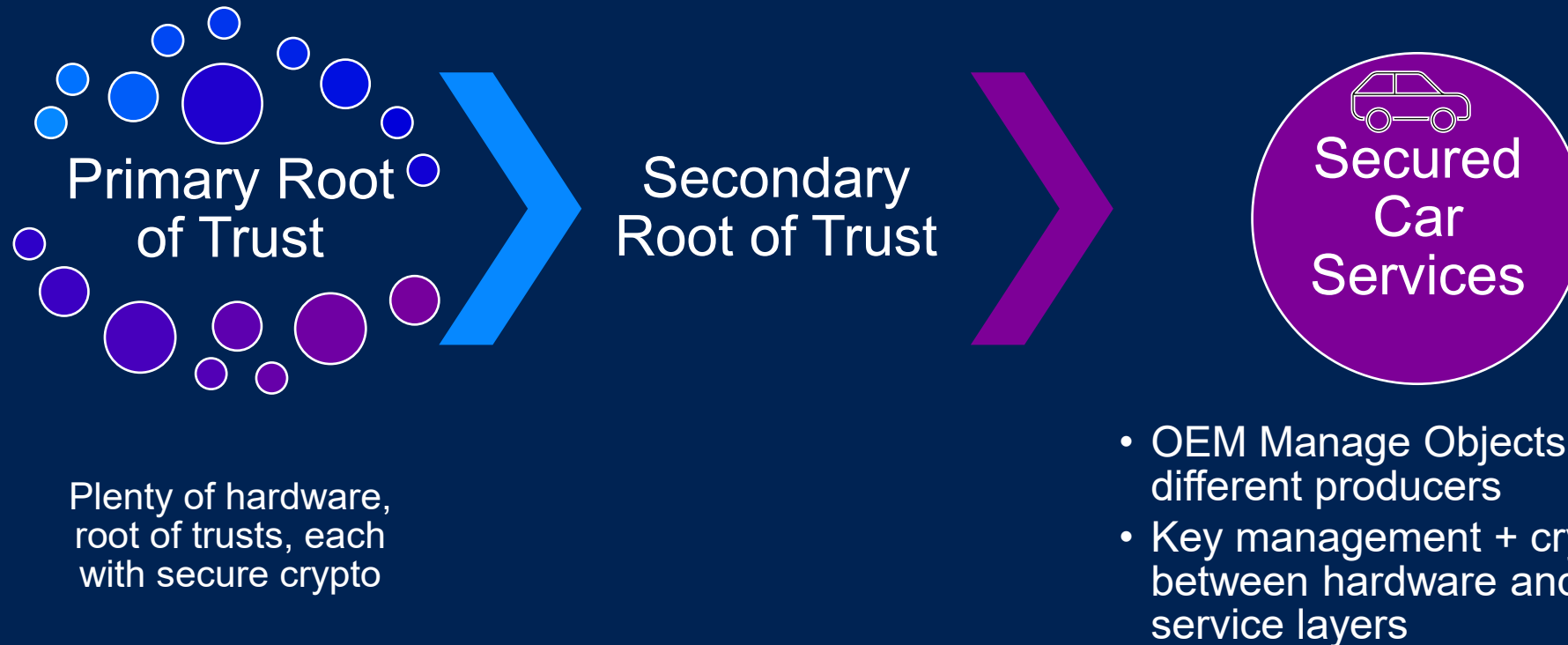
- Runs a full operating system providing standardized APIs and functions
- 3rd party Security Certification
- Full support for App and OS update over-the-air

Secure Components

offer a standardised controlled and protected execution environment with the following characteristics:
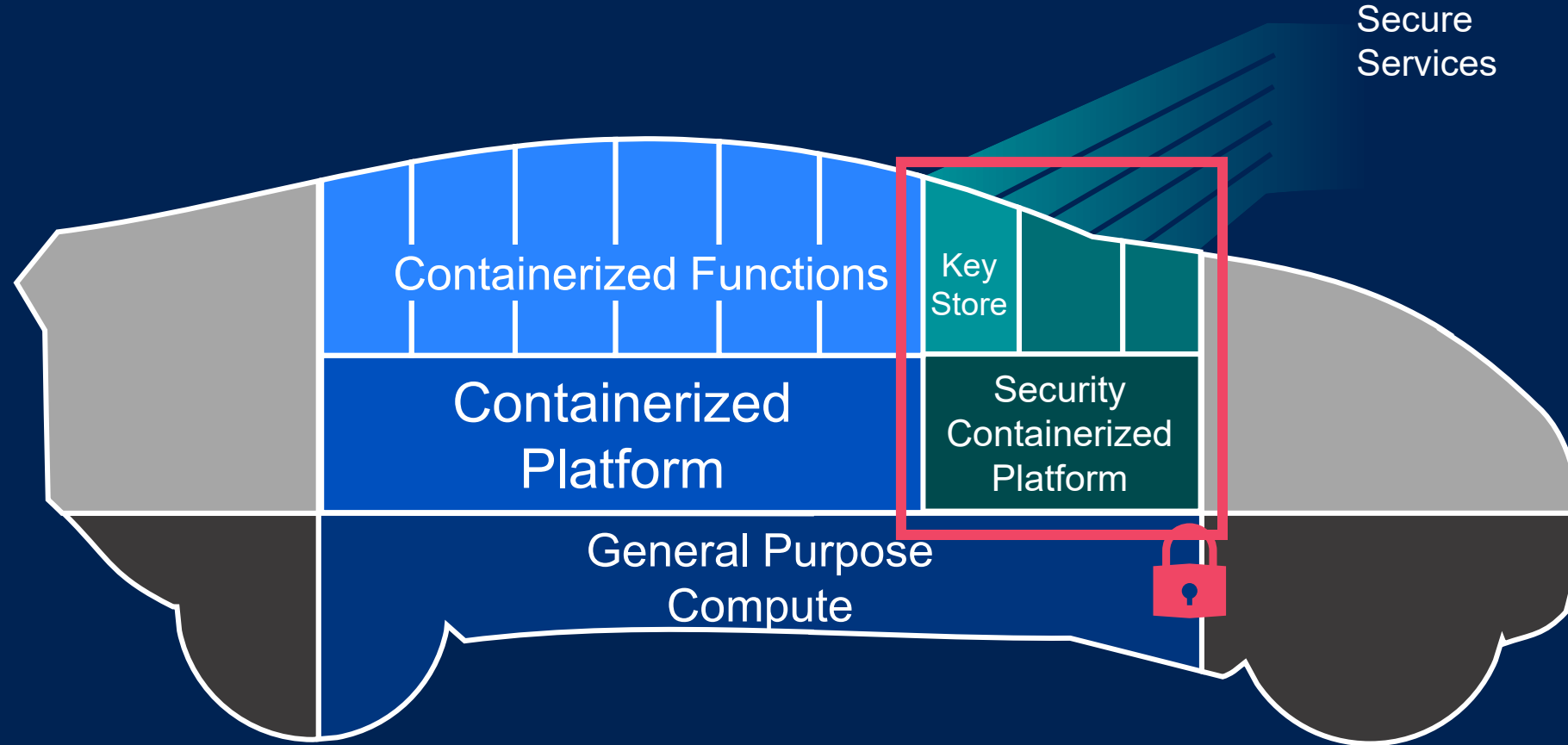
Root of Trust	Isolation	Secure Service Management	Types of Secure Services
↓	↓	↓	↓
Identification and binding that allows you to create a chain of trust based upon secure services	Between the Trusted Environment vs. the Rest of the Real World and	From trusted applications from different actors	State-of-the-art cryptography
↓	↓	↓	↓
Key Injection at Production Level (part of certification of Secure Component)	Between Each Trusted Application	Remote update and Services to the application	Attestation (e.g. signed claim)
			↓
			Trusted storage
			↓
			Secure transactions and communication
			↓
			Trusted access to peripherals

Global Platform™

Roots of Trust for Secure Software: Providing OEMs Standardised Management Capabilities

Primary Root of Trust

Plenty of hardware, root of trusts, each with secure crypto

Secondary Root of Trust

Secured Car Services

- OEM Manage Objects across different producers
- Key management + crypto between hardware and service layers

GlobalPlatform provides a bridge between hardware and software security – as well as supporting across multi-tenant service providers. Standardisation of the common security requirements, augments hardware and software with interoperable functionality and transparent security robustness levels.

Global Platform™

GlobalPlatform & In-Vehicle Multi-Tenant Services

Secure Services

Containerized Functions

Key Store

Containerized Platform

Security Containerized Platform

General Purpose Compute

Global Platform™

GlobalPlatform Approch

2. Trusted Applications/Applets developed/ deployed by the ecosystem, to meet the specific requirements of a particular ECU or a customer solution using standardized APIs

Example Standardized Primary Key Injection

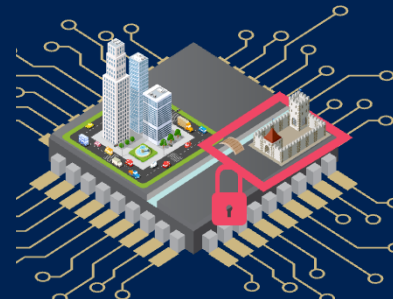|		
SIM	Sec Boot	ECU ID
Key Negotiation	ADAS	FOTA/ SOTA
Sec Logging	Auth Cmd	Payment
Firewall	SecOC	MACsec

+

1. Platform: Standardized APIs & Management command, update, state-of-the-art crypto, crypto agility …

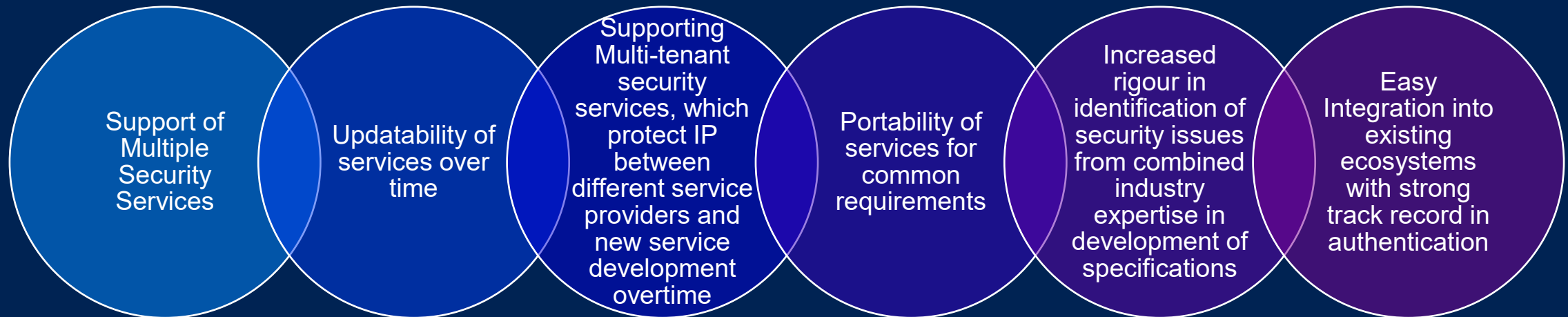Secure Component Platform: Functionally and Security Certified

Hardware

Secure Element

Trusted Execution Environment

Global Platform™

GlobalPlatform Provides Future Proofing of Security Services & Adds Flexibility

Unlike traditional automotive HSMs/SHEs, GlobalPlatform offers standard requirements, common APIs, testing suites, and certification of compliance with specifications on security robustness and interoperability

Support of Multiple Security Services

Updatability of services over time

Supporting Multi-tenant security services, which protect IP between different service providers and new service development overtime

Portability of services for common requirements

Increased rigour in identification of security issues from combined industry expertise in development of specifications

Easy Integration into existing ecosystems with strong track record in authentication

Possibility of reuse, incremental developments across ECU evolution (without having to start over from scratch each time for every new ECU project)

Trends of Automotive Threats/Attacks

22nd May 2025

Dennis Kengo OKA, IAV Co. Ltd.