Global Platform™

The standard for secure digital services and devices

Cybersecurity in Automotive

Automotive Taskforce

Table of contents

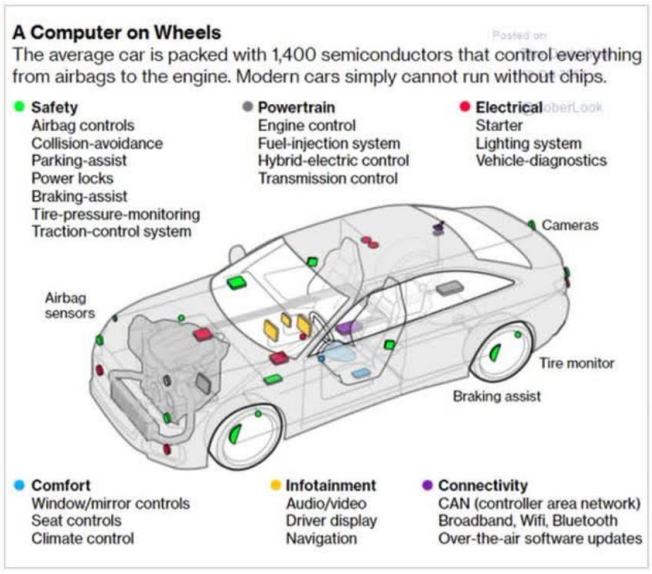
Cybersecurity in Automotive

Disruptive Context

The emphasis on automotive cybersecurity is the result of a perfect storm between the ever-increasing hyperconnectivity of vehicles and the new international regulations on cybersecurity management and over-the-air updates. All of which results in a tremendous growth in the market for cybersecurity.

Evolution in Connectivity

Today's vehicles offer hyper-connectivity with services ranging from safety, comfort, powertrain, electrical, to infotainment. The role of computing is only growing in vehicles, delivering more and more sophisticated connected services – in fact 45% of the cost of new cars will be due to electronics. Innovations such as electric vehicles and Advanced Driver Assistance Systems (ADAS) are leading to a significant focus on computing and dramatically increasing the focus on cybersecurity.



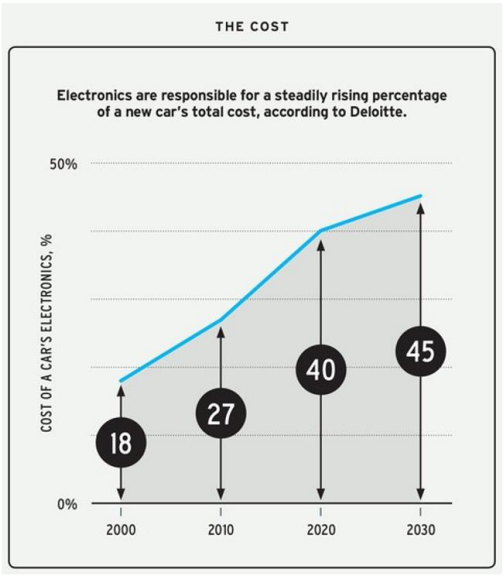


Figure 1: https://economistwritingeveryday.com/2022/01/04/how-many-semiconductor-chips-are-there-in-a-car/

Regulatory Changes

Historically, cybersecurity has been managed in an ad hoc manner, relying on a compilation of standards and different national regulations, until 2022 with the entry in force of the UNECE 155 and 156 which regulate the approval process of new types of vehicles regarding the type of cybersecurity management systems and the management of software updates. These regulations have corresponding SAE and ISO standards defining the compliance with the UNECE's regulations which are then transposed nationally (currently with 64 countries adhering to the regulation 155).

United Nations Economic Commission for Europe (UNECE)

- UNECE Transport Division has been providing secretariat services to the World Forum for Harmonization of Vehicle Regulations (WP.29)
- UNECE 155 -Cybersecurity Management Systems (CSMS)
- UNECE 156 – Software Update Management System (SUMS)

Standard ISO/SAE21434, “Road Vehicle Cyber Security Engineering”

- Industry standard to meet the UNECE regulatory requirements
- Threat analysis and Risk Assessment (TARA)

National Type Approval

- Deployment effective as of June 2022 for 64 countries
  - compliance with the UN regulation for:
    - new type approval vehicles for cyber security, cyber security management systems, OTA updates as of July 2022 and
    - all new vehicles produced from July 2024.

In addition, other relevant regulations and standards are being issued. For instance, in the US in 2021, the executive order on Software-Bill-Of-Materials (SBOM), defined the Minimum Elements for a Software Bill of Materials. This order has clear pertinence to the automotive sector, as well as requiring a future proofing approach regarding software updates.

Although many pillars have been defined with regards to cybersecurity, many questions have not been resolved regarding how best to ensure effective cybersecurity within the automotive sector.

GlobalPlatform

What Is GlobalPlatform?

GlobalPlatform is a member-driven technical community focused on developing, deploying and managing trusted digital services and devices.

We promote a framework to create trustworthy devices based on secure components and to allow service providers to build a Chain of Trust that protects both devices and digital services.

We publish functional and security specifications regarding core technology and maintain certification programs. While our original focus was on technologies found in mobile devices, we have expanded to IoT, and many of our technologies have already been adopted into automotive. We are now building on this existing relationship with the creation of a GlobalPlatform automotive task force to focus our future activities.

Membership

GlobalPlatform is a member-driven technical community

Common Goal
Our members have a common goal to develop GlobalPlatform's specifications

Established Standards
Over 200 specifications and technical documents available

Successful Collaboration
20 years of implementations

2,600
Representatives from
90+ Member companies

6 Task Forces
34 Industry Partners

GlobalPlatform Technology is developed by
3 Technical Committees with
14 Working groups

Certification Program

The GlobalPlatform Certification confirms product adherence to functional requirements and market defined security thresholds.

Device Manufacturers can:

- Market products as meeting digital service providers needs
- Prove that their digital service management capabilities met security requirements

ISO 17065:2012

ACCREDITED number 5486.01

Service Providers have:

- Reassurance that certified products meet their needs

11
Accredited Labs
68 Test Suites

175 Qualified Products

- Dedicated Certification Secretariats
- Independent Program
- Internationally Recognized

Global Platform™

Members

Full members

Participating members

Observer, Public and Consultant Members

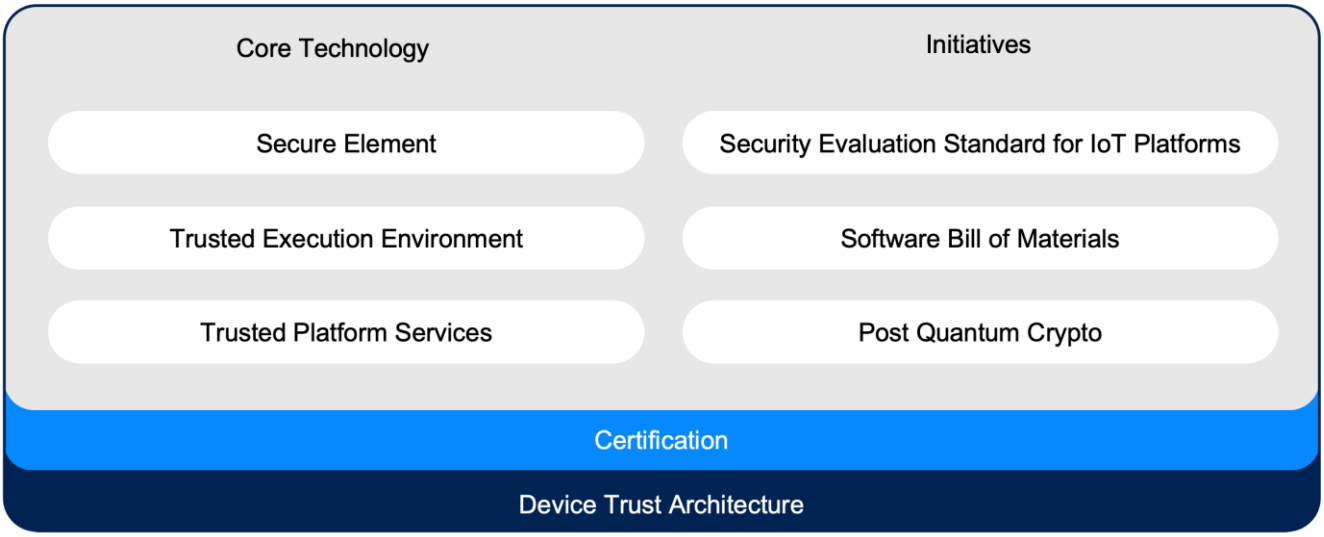
Collaborative Partners

GlobalPlatform's Proposal in Automotive

GlobalPlatform's core assets provide a base for addressing many automotive security requirements solutions based on our standards are already used in automotive - both in-vehicle and on connected devices.

GlobalPlatform Specifications, which are regarded as the industry standard for trusted end-to-end secure deployment and management solutions, offer several features that can address the privacy and security concerns of multiple connected markets (e.g., banking, governments, mobile, automotive).

The GlobalPlatform process is based on secure components, an architecture for device trust, and a certification scheme - all backed by services to support a secure lifecycle.



Device Trust Architecture

The GlobalPlatform Device Trust Architecture provides a way for manufacturers to ensure that their devices are trustworthy through the use of Secure Components to provide Roots of Trust (RoT).

A Root of Trust contains a set of unconditionally trusted functions that are sufficient to enable a description of the characteristics of a platform that affect its trustworthiness. A Root of Trust must operate as expected, as failures within it are undetectable, and it is therefore desirable that it should be as small as possible and designed with security in mind.

A Root of Trust is the foundation that allows the trustworthiness of code and data loaded into a system at run-time to be established, so that eventually a larger system can be considered trustworthy.

The Root of Trust provides a small number of security services, of which the minimum subset is:

- *Identification*: A Root of Trust has a unique and unforgeable identity that can be independently verified. This is assured through the manufacturing process of the Root of Trust.
- *Integrity*: A Root of Trust can verify the *provenance* of an asset (i.e. who created it) and whether that asset has been changed by an unauthorized actor. It does this by verifying digital signatures over those assets.
- *Authentication*: A Root of Trust can securely store credentials to be used in authentication protocols.

- *Confidentiality*: A Root of Trust provides mechanisms to ensure the confidentiality of sensitive data, generally through the use of strong encryption.
- *Measurement*: A Root of Trust is able to generate reliable measurements of platform characteristics and unforgeably convey these to other parties, generally by creating a digital signature over the set of characteristics.

The Device Trust Architecture supported by GlobalPlatform Secure Components provides a platform for Service Providers to host their own trusted security components within a purpose-built execution environment. The two GlobalPlatform standardized Secure Components, the *Trusted Execution Environment* and the *Secure Element*, while they differ significantly in detail, are constructed from trustworthy OS and API layers whose integrity and provenance are verified by the Root of Trust.

GlobalPlatform Certification

Moreover, GlobalPlatform supports certification in several ways. The organization operates functional and security certification programs, enabling stakeholders to verify product adherence to the association's technical specifications, market-specific configurations and security levels.

Certification validates that a product meets a set of relevant national, global and/or industry requirements. It is essential to facilitate trust, confidence and collaboration between stakeholders, as well as foster market stability and growth:

- Demonstrates conformance, interoperability and robustness;
- Enables stakeholders to maximize the potential of existing opportunities and break into new markets;
- Confirms alignment with business, security, regulatory and data protection requirements;
- Differentiates products from competing solutions;
- Reduces costs and time to market; and
- Protects brands and end users.

Moreover, GlobalPlatform supports the industry by developing generic security protection profiles per type of product and based on industry needs.

The protection profiles include:

- Security Functional Requirements (which security features are required)
- Security Assurance Requirements (which evaluation activities need to be performed)

GlobalPlatform has developed several protection profiles for Common Criteria and SESIP certification programs; for Secure Element, Trusted Execution Environment, microcontroller units and Secure External Memories.

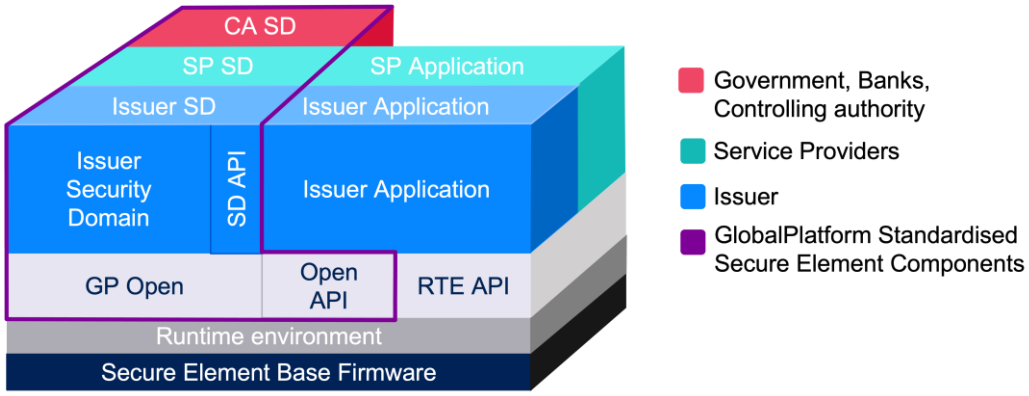
Core Technologies

Secure Element

GlobalPlatform's Secure Element is a tamper-resistant platform (typically a one-chip secure microcontroller) capable of securely hosting applications and their confidential and cryptographic data (for example cryptographic keys) in accordance with the rules and security requirements set by well-identified trusted authorities.

There are different form factors of SE: embedded and integrated SEs, SIM, eSIM /eUICC, iSIM as well as smart cards to address the requirements of different business implementations and market needs. GlobalPlatform publications specify several protocols to communicate securely with the SE, as well as manage SE applications and data.

Secure Elements are used extensively across many industries, and we are seeing increased use in automotive for storage and management of strong identities, together with traditional SIM related applications.



GlobalPlatform's Objectives on Secure Element:

1) Develop, maintain and evolve the SE and related supporting documents and tools (based on GlobalPlatform Card Specification [aka Secure Element Specification] v2.3.1 | GPC_SPE_034).
2) Recommend security evaluation processes and features to ensure that GlobalPlatform technology offers the highest levels of security.
3) Advance the GlobalPlatform Certification Program to facilitate and assure interoperability within the marketplace.
4) Engage with other relevant industry and standardization groups and identify new technical requirements and opportunities for progressing joint working initiatives.

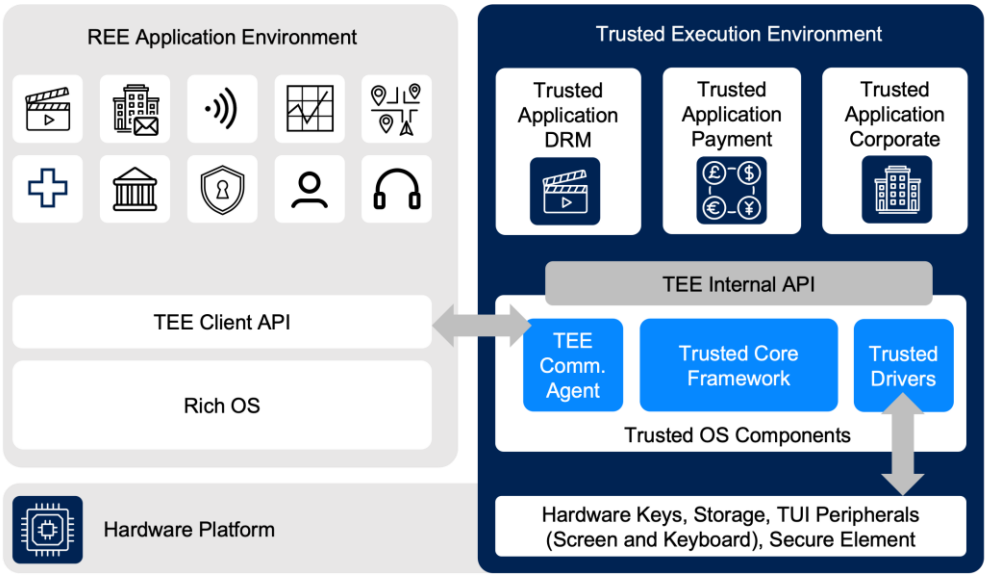
Why Is Secure Element Relevant for Automotive?

The SE provides the highest value per investment in security and is used in multiple markets (e.g. banking, governments, mobile) that require robust protection against cyberattacks on assets and data and in compliance with cybersecurity regulations. In fact, some connected vehicles already embed GlobalPlatform compliant SEs. Furthermore, the automotive market can extend this usage to protect other services given the inherent flexibility of the technology.

Trusted Execution Environment

GlobalPlatform defines a TEE as a secure area of the main processor in any connected device to enable a minimal trusted computing base (TCB). It ensures that sensitive data is stored, processed and protected in an isolated, trusted environment. The TEE's ability to offer isolated safe execution of authorized security software, known as 'trusted applications', enable it to provide end-to-end security by enforcing protected execution of authenticated code, confidentiality, authenticity, privacy, system integrity and data access rights. The TEE protects sensitive data in transit, while processed and when stored. The TEE offers a level of protection against attacks that originate from the Regular OS environment or remotely. It also assists in the control of access rights and houses sensitive applications, which need to be isolated from the Regular OS.

Trusted Execution Environments are near universal in mobile phones, and very common in any device that requires an isolated secure processing environment – for example a secure video device (one that supports DRM). Initial automotive applications were focused on in-vehicle infotainment (IVI) systems, but increasingly TEEs are used for broader applications including trust establishment – often in combination with a SE or Hardware Security Module (HSM), secure data processing and biometrics.



GlobalPlatform Objectives on Trusted Execution Environment:

1) Manage, prioritize, develop, maintain and evolve specifications for the TEE, including specifications relating to:
   a) APIs to communicate to a TEE
   b) APIs to develop Trusted Applications (TAs) running within the TEE and enabling interactions with secure peripherals such as the trusted user interface, biometric peripherals and Secure Elements (SEs)
   c) The TEE Management Framework (TMF)
   d) Configurations to serve a specific class of devices
2) Advance and maintain the GlobalPlatform TEE Functional and Security Certification Programs to facilitate portability and interoperability of TA deployments on different TEE implementations, and to enable standardized security evaluations.

3) Liaise, collaborate, and/or coordinate activities with relevant external organizations, that perform similar/complementary activities, and support interest in Root of Trust in secure microcontroller units (MCUs) and associated secure services.

Why is Trusted Execution Environment Relevant for Automotive?

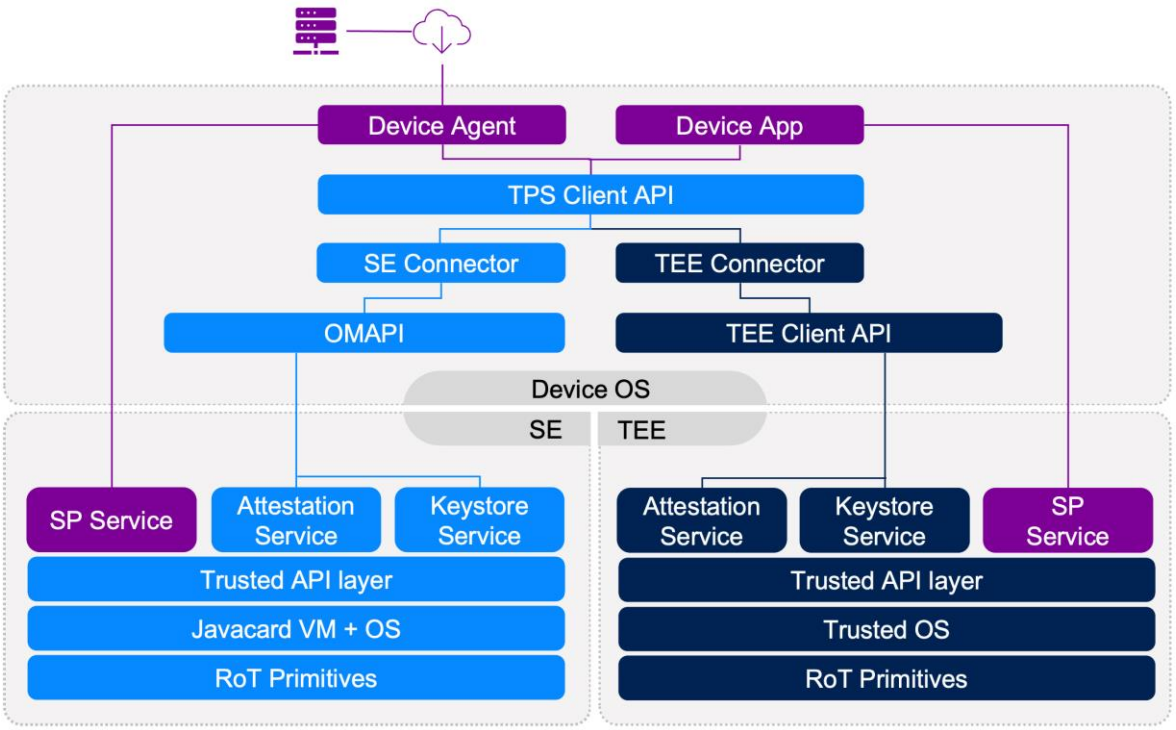
Compared to other security environments on the device, the TEE offers high processing speeds and a large amount of accessible memory. The TEE is able to manage interaction with the end user, thanks to a trusted user interface. Many connected vehicles already embed GlobalPlatform compliant TEEs to protect media and the entertainment system. Furthermore, the automotive market can extend this usage to protect other services given the inherent flexibility of the technology.

Trusted Platform Services

Trusted Platform Services

GlobalPlatform's Trusted Platform Services strategy simplifies the access to the Secure Component Services from the boot to application and provides:

- *Open specifications provide mechanisms enabling access to platform services offered by standardized secure components (such as the SE and TEE), both from within a device and from platforms external to it.*
- *These mechanisms assure the trustworthiness of a secure component within a device enabling a secure service, thanks to an attestable Chain of Trust (from the Root of Trust (RoT) to the application or the cloud).*
- *The aim is to make it easier for service providers and application developers in different market sectors to link together the strong security technology offered by secure components in their products. This is achieved through GlobalPlatform's Device Trust Architecture (DTA).*



GlobalPlatform's Objectives for Trusted Platform Services:

- Develop and maintain the existing GlobalPlatform Specifications that define high-level platform services.
- Define new specifications or open-source deliverables for devices hosting secure applications relying on a chain of trust anchored on Root of Trust and secure boot.
- Collaborate with existing technologies already available in the marketplace.

Why Is Trusted Platform Services (TPS) Relevant for Automotive?

TPS provides interoperable middleware for secure services that simplifies the access to secure components. The attestation mechanism allows the users of the services to know the exact security level of the provider. TPS supports open-source TPS APIs, which simplifies the integration into any kind of device.

GlobalPlatform Initiatives

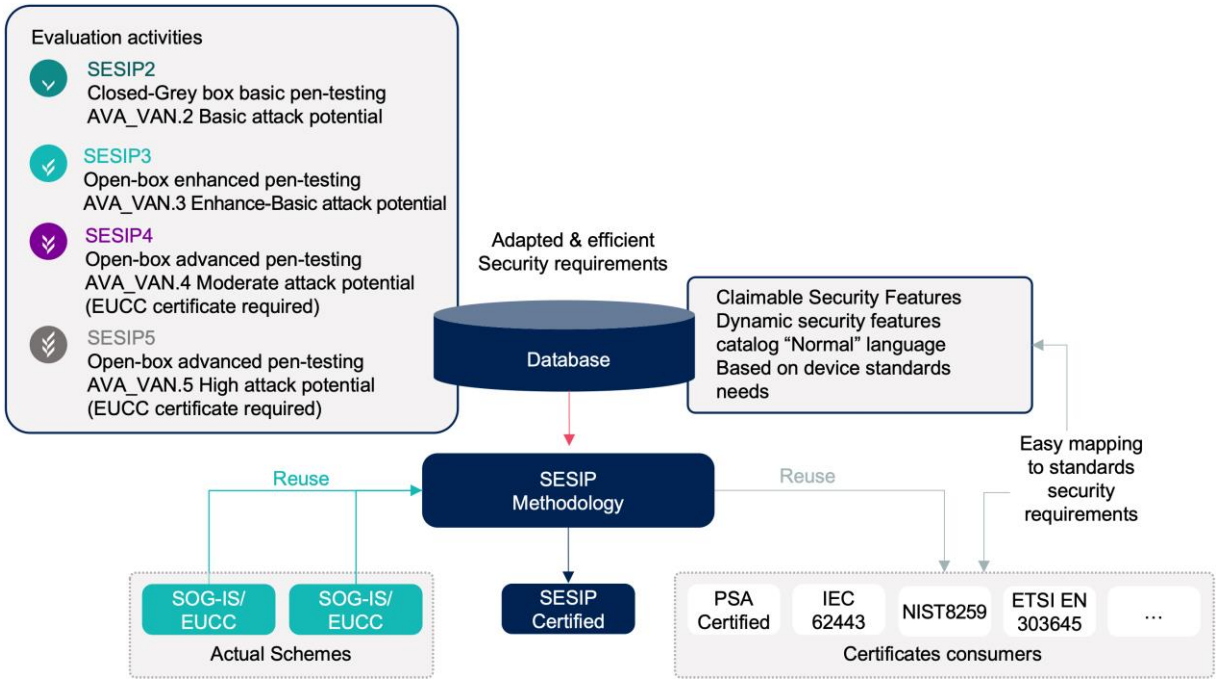
GlobalPlatform also has some transversal work ongoing to future proof solutions that are relevant for automotive, including:

SESIP

Security Evaluation Standard for IOT Platforms (SESIP)

The Security Evaluation Standard for IoT Platforms (SESIP) addresses the scale and complexity of security certification for the IoT ecosystem. It provides an optimized approach to security evaluation designed specifically for IoT platforms and their parts. In addition, it enables the composite evaluation of IoT products: Components that have been certified for one particular use case can be reused to answer the requirements of other markets. This reuse optimizes the process, reducing the cost and time of security evaluations for device makers.

By mapping to other security requirements, such as NIST 8259, ISA/IEC 62443, and ETSI/EN 303 645, SESIP defines assurance levels that are mutually recognizable and can be reused across multiple market-specific schemes, therefore achieving scale.



SESIP provides assurance on foundational security provided by third-party providers. It defines a catalogue of six Security Functional Requirement Categories (SFRs), which allows for a consistent definition of platforms and their part and supports a comparison between them. **The SESIP SFRs define generic and intuitive security requirements with flexibility to address different use cases and the cybersecurity threats specific to them, by focusing on**:

- Identification and Attestation: to demonstrate that the platform is the expected one and is in the expected state.
- Product Life Cycle: to secure all life cycle steps - installation, initialization, flaw remediation, secure update, decommission, field return, etc.
- Secure Communication: to confirm support for secure communications with external entities.
- Cryptographic functionality: to assess cryptographic features.
- Compliance functionality: to assess some additional useful security features - secure storage, residual information purging, auditing, debugging, etc.
- Extra attacker resistance: to cover the different environment context of various IoT products.

With clear and simple definitions, SFRs enable all stakeholders to understand the security functions provided by hardware components and software within IoT devices.

GlobalPlatform Objectives for SESIP:

1. Develop and maintain GlobalPlatform's SESIP methodology, expand applicability to a global audience and grow awareness of GlobalPlatform's role in IoT security certification.
2. Collaborate with Government agencies including ENISA and NIST, SOG-IS Certification Bodies, and global Standardization groups such as ISO and ETSI, to increase recognition of SESIP certificates, and create SESIP Profiles that map SESIP to other standards requirements.
3. Establish SESIP governance within GlobalPlatform.

Why Is SESIP Relevant for Automotive?

Automotive cybersecurity regulatory requirements can be mapped to concept software requirements using the SESIP methodology.

GlobalPlatform has developed a mapping between SESIP and ISO/SAE 21434 and is developing the mapping for UNECE regulation No. 155 – Cyber security and cyber security management system.

SESIP's focus on reuse enables component certifications to be reused both within automotive, and potentially between non-automotive and automotive markets.

Software Bill of Materials (SBOM)

The US Executive Order for Software Bill of Materials requires a *"formal record containing the details and supply chain relationships of various components used in building software… similar to food ingredient labels on packaging. SBOMs hold the potential to provide increased transparency, provenance, and speed at which vulnerabilities can be identified and remediated by federal departments and agencies"*[1].

[1] https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1

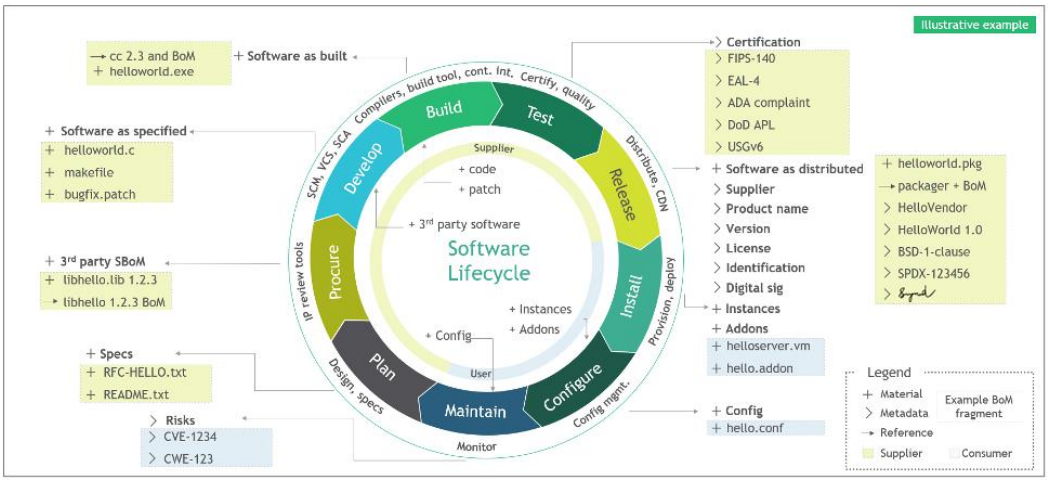


Figure 2: Software Bill of Materials NTIA (https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity/software-security-supply-chains-software-1)

GlobalPlatform's Objectives for Software Bill of Materials:

Given the relevance of SBOM to cybersecurity solutions, GlobalPlatform has current work to:

1. Assess the impact of the deployment of SBOM.
2. Clarify the concepts of software transparency and assurance and provide guidance, such as:
    a. A consistent means to produce, consume and exchange software transparency and assurance information.
    b. A guide to improve interoperability of software transparency and assurance data exchange.
    c. Dialogue and collaborate with impacted markets such as telecoms, healthcare and automotive.
    d. Collaboration within GlobalPlatform and with external organizations on SBOM and other key initiatives.
    e. Definition of any necessary requirements for technology development in relation to SBOM.

Why Is SBOM Relevant for Automotive?

As part of the management of security, OEMs need to have a precise specification of all the devices used in a vehicle and SBOM is the relevant tool to manage the software components. Because of the need to update vehicles during their lifetime, GlobalPlatform's work on SBOM seeks to provide a means for managing the software updates and the specific case of security certified components.

Post Quantum Cryptography Migration

By 2030, all security evaluated components should deploy post quantum cryptography (i.e., *cryptographic systems that are secure against both quantum and classical computers, and can interoperate with existing communications protocols and networks*[2]*).* NIST has announced the list of future post quantum cryptographic algorithms for signature and key exchange; nonetheless, the field

[2] https://csrc.nist.gov/projects/post-quantum-cryptography

is not sufficiently mature and hybrid crypto would be a good means for transitioning to full Post Quantum Crypto in 2030.

GlobalPlatform's Objectives on Post Quantum Crypto Migration:

GlobalPlatform sees the following as key to successful PQC migration:

- A secure channel based upon the AES256 crypto (resistant to quantum computers) as an update channel;
- The ability to update the OS of the certified components; and
- Selection of the right post quantum crypto or hybrid approach to be deployed between today and 2030. We will continue to evaluate and provide recommendations on the cryptographic mechanisms used in GlobalPlatform technology, to ensure high levels of security, as cryptography trends and technologies evolve.

Why Is GlobalPlatform's PQC Work Relevant for Automotive?

Given that the automotive market faces the same 2030 mandate as other markets, combined with its planning cycle (3-5 years), it is urgent to make decisions on the appropriate hybrid approach to be deployed. Due to the lifecycle of the car (10-15 years), timely solutions must be defined to protect data stored in the vehicle today that may be susceptible to being decrypted after 2030 by quantum computers.

GlobalPlatform's DNA

…answers both the opportunity and urgency facing the automotive market: GlobalPlatform has characteristics and assets that clearly correspond to the pressures facing the automotive market. Firstly, GlobalPlatform's specifications offer a long-term approach that fosters:

- Interoperability
- Flexibility
- Multi-application management
- Privacy
- Multi-actor collaboration
- Different security solutions for different markets

Importantly, GlobalPlatform is not an all-or-nothing proposition. GlobalPlatform APIs and protocols

- Can be used independently or in combination;
- Work together with proprietary models; and
- Support both single and multiple application devices.

To complement and complete the solution, GlobalPlatform offers a Compliance Program and Certification Scheme (see GlobalPlatform Certification).

Furthermore, GlobalPlatform has a long history of collaborative relationships with relevant industry partners across the world, from international standards organizations to regional industry bodies. This collaboration is key to realizing our vision of fully open ecosystems that efficiently deliver innovative, digital, interoperable services across all vertical markets, while providing greater security, privacy, simplicity, and convenience for the user. (See Collaborative Partners).

Current and Future Use Cases

GlobalPlatform TEE and SE technologies are used in hundreds of millions of vehicles today. With the increased focus on regulation, there is an increased focus on further extending these uses.

Video and Streaming Services

High-definition video playback, whether in IVI units or seat back entertainment systems, requires digital media rights (DRM) protection, and most schemes mandate the use of a TEE.

Android Security

Android is increasingly common in IVI units and requires the use of a TEE to pass Android CTS compliance. Increasingly customers are looking to blend Android and non-Android systems within Electronic Control Units (ECUs), adding new requirements for sharing of crypto assets.

Attestation

Attestation is the process of asserting and validating the identity or status of a device. Attestation has been a key part of GlobalPlatform's DNA for many years – but only recently has the automotive industry started to appreciate the possibilities of validating that an ECU is genuine from the cloud. New forms of attestation, based on emerging standards such as EAT (Entity Attestation Tokens), are being championed by GlobalPlatform, and the rich information they provide is a basis for reasoning about trust in components where 'right to repair' has been exercised.

Biometrics

Biometrics in mobile devices are extremely mature, and the biometric ecosystem has a long experience of GlobalPlatform APIs. Increasingly biometrics are now being used in automotive applications – in particular for driver alertness monitoring. There are many hot topics around both the capture and storage of biometric data, and how automakers should respond to varying privacy legislations from around the world.

Infotainment 'Apps'

Applications within IVI systems, each have their own security requirements, particularly as relates to user data, and must meet the ever-increasing security requirements of 3rd party platforms, such as 'Alexa'.

Cryptography, Agility and Post Quantum

Security libraries, such as OpenSSL are often configured to call out to security enclaves such as HSMs, TEEs or SEs to manage private keys. As crypto-agility and post quantum cryptography are gaining in importance, there is renewed discussion on the systems, APIs, and processes used to deliver high-level features, such as secure communication.

Protecting access to hardware security (HSMs and SEs)

HSMs and SEs provide tamper-proof storage and processing of cryptographic assets, but that does not mean that other parts of the system have no security role. The increased use of multi-purpose or multi-guest ECUs increases the risk of abuse of security subsystems. We are seeing opportunities for a TEE to be used to mediate such access, as it has greater visibility on the client application and privileged access to the HSM/SE.

Secure Data Storage

Secure data storage is a key requirement in many systems.

TEEs can be used to store and process other security or privacy sensitive data, such as that protected by privacy legislation. An interesting new area is using the TEE to capture and anonymize data prior to exporting to cloud services.

The SESIP Protection Profile for Secure External Memories addresses security functions and requirements specific to the functionality of external memory components and, more specifically, to the non-volatile external storage in embedded systems.

Digital Car Key

Digital Car Keys offer car owners a means to lock/unlock/start their car using their smartphone. Digital Car Keys rely on Secure Elements in both the car and the mobile device to ensure high security requirements. Embedded Secure Elements provide a tamper resistant environment to store the car-key and protect them from hardware and software attacks. Future possibilities include secure car key sharing via the cloud.

Secure Root of Trust for ECUs

Electronic Control Units (ECUs) perform many critical functions, and the number of ECUs is growing. The abundance of connectivity increases the potential for threats and cyberattacks. GlobalPlatform's Secure Elements provide a certified, tamper resistant Root-of-Trust for ECUs, enabling use cases such as secure boot, software image verification, end-to-end secure connectivity, secure firmware update, and secure storage of credentials and sensitive data.

Securing Vehicle to Cloud Services

Secure Components provide the services required to provide secure vehicle to cloud services. They support secure update by ensuring that connections occur only to authorized servers; that firmware updates have not been modified and that there is no attempt to roll back to older firmware versions. They can support secure billing and licensing mechanisms for service monetization.

Protection of ADAS Models

The AI models and associated training data used in Advanced Driver Assistance Systems (ADAS) are created at huge cost and represent highly valuable IP. Secure Components can protect the ADAS model from reverse engineering or license violation.

Participate Now in the Work in Automotive

GlobalPlatform has established an Automotive Task Force for its members, which pilots the priority use cases to be supported by GlobalPlatform technical work. Furthermore, GlobalPlatform hosts three Cybersecurity Vehicle Forums a year, where GlobalPlatform members and the automotive value chain work together on defining the automotive requirements and use cases for which cybersecurity specifications and guidelines are needed. **Come join us now!**