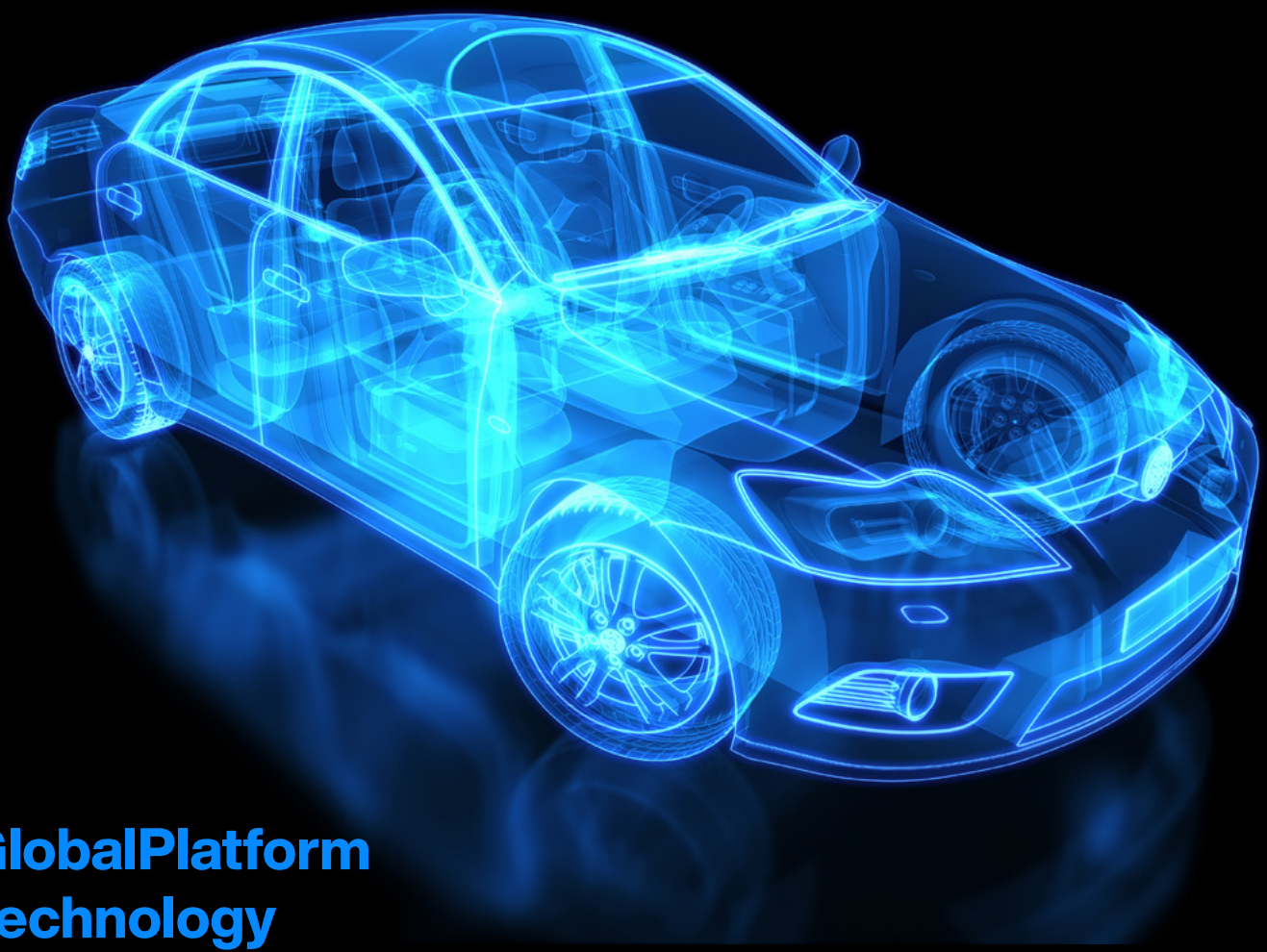
Global Platform™

Automotive Task Force



GlobalPlatform Technology

Trust & Security in Automotive Systems

White Paper - October 2023

Contents

1	**Executive Summary**	**3**
2	**Evolving Needs**	**5**
2.1	New Automotive Market Demands	6
2.2	Evolution in ECU Architecture	7
2.3	Stringent Cybersecurity Regulations	9
2.4	Standards for Cybersecurity Compliance	10
2.5	GlobalPlatform's Answer for Automotive	10
3	**Security as a Platform**	**13**
3.1	Security Definitions	14
3.2	Common Platform	18
3.3	Platform Certification	19
4	**GlobalPlatform Secure Components**	**21**
4.1	Common Characteristics	21
4.2	Secure Elements	22
4.3	Trusted Execution Environment (TEE)	24
5	**Selecting The Right Secure Component**	**27**
5.1	Functional Requirements	28
5.2	Implementation Requirements	30
5.3	Security Evaluation	31
5.4	GlobalPlatform Security Certification Scheme	35
5.5	Comparing Secure Components	36
6	**Additional GlobalPlatform Security Resources**	**39**
6.1	Device-Level Access to Secure Services	39
6.2	Security Evaluation Standard for IoT Platforms: SESIP	41
7	**Conclusions**	**45**
Annex A	Get Involved	46
Annex B	Traditional Automotive Trust Anchors	47
Annex C	SESIP Assurance Levels	50
Annex D	Abbreviations	51
Annex E	List of Figures	55

Global Platform™
Automotive Task Force

01. Executive Summary

The evolution of connected cars has taken an exponential leap with the move to:

- Autonomous driving features,
- Engagement with extended value chains for in-vehicle services,
- Mobility As A Service (MaaS), and
- Software Defined Vehicles.

This move explicitly requires a robust solution for trusted services that allows for agility in deploying services, flexibility in developing services post-production, evolving cryptography requirements, and the increase in capabilities for security solutions.

GlobalPlatform provides a *platform centric* approach to security with the necessary flexibility to allow vendors to differentiate their solutions while meeting the demand for agility and security compliance. We offer a choice of solutions that can be used together or independently and are working with automotive bodies to show how our technologies can be used to meet current and emerging requirements.

This white paper provides an overview of GlobalPlatform security technologies, which leverage best-in-class security solutions demonstrated over 20 years in the development of digital services for the mass market, in particular:

- how GlobalPlatform technologies support the specific security requirements in Automotive;
- the different distinctions regarding Roots of Trust, Chains of Trust and Trust Anchors as the hardware-based security anchor for software solutions in the vehicle;
- benefits of a platform-centric approach to security for developing trusted services across multiple parties and of the platform certification to facilitate portability of solutions;
- considerations on selecting secure components on the basis of the specific implementation context technology; and
- additional GlobalPlatform resources with the security evaluation methodology (SESIP) and application-level APIs to leverage secure solutions by abstracting the underlying technology so the normal world application does not need to know implementation details.

Target Audience

This white paper targets both:

- Automotive Value Chain decision-makers on cybersecurity for hardware protected security environments: to foster understanding of how GlobalPlatform resources support the emerging requirements of Automotive; and
- Producers of secure digital services and devices: to outline the key requirements driving the adoption of GlobalPlatform specifications in support of Automotive use cases.

Global Platform™
Automotive Task Force

02. Evolving Needs

Automotive cybersecurity has become a very important and demanding security topic for Automotive OEMs and for the extended value chain, requiring a change in the way cybersecurity is conceived and managed. The drivers behind this change include:

Figure 1:
Trends Driving Changes in Security Management in Automotive

These drivers change the depth, breadth, and urgency regarding security for Automotive. In fact, Synopsys emphasizes the intricate relationship between cybersecurity and functional safety, which has resulted in OEMs demanding both data protection and safety in the chip level:

> *To avoid weaknesses in security, OEMs are demanding both data protection and safety in the chip level. Automotive systems must address high-grade security and also must meet functional safety standards, which means implementing security functions to ensure that functional safety cannot be tampered with. Without security, there is no safety, and vice versa. Secure systems must be able to handle unpredictable inputs that would create unacceptable behaviors. Designing the security into automotive SoCs from the hardware level will help ensure that connected cars behave as expected, are able to protect against malicious security attacks, and are capable of preventing random and systematic safety faults.*[1]

1 https://www.synopsys.com/designware-ip/technical-bulletin/automotive-cybersecurity-starts-with-chips.html

2.1 New Automotive Market Demands

The evolution of connected cars has taken an exponential leap with the move to:

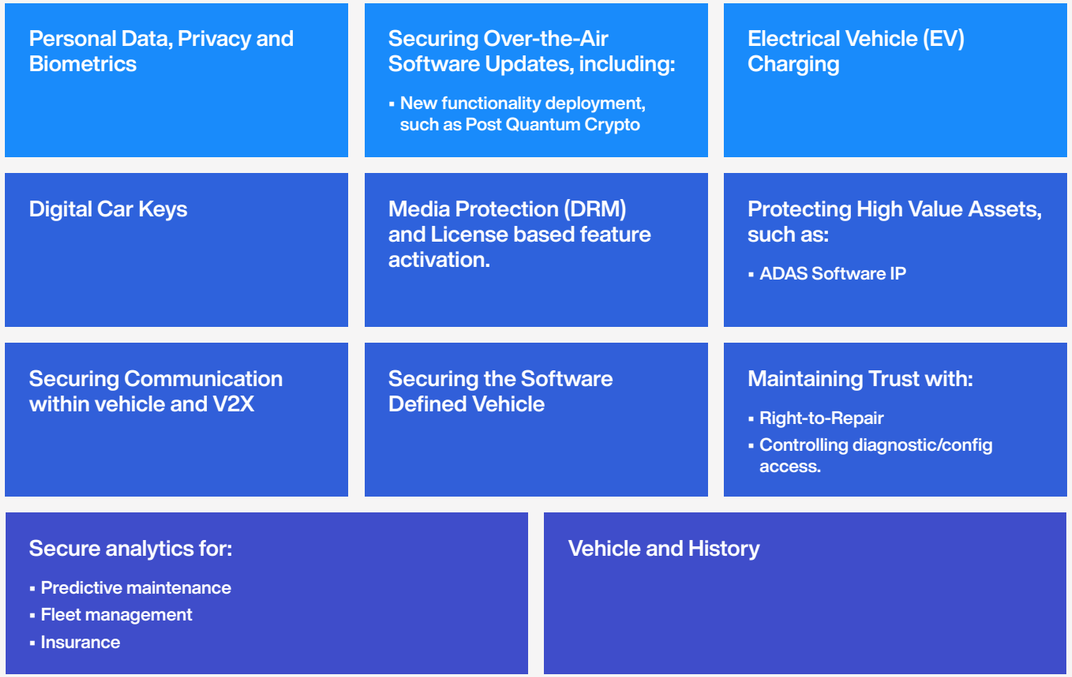
- Autonomous driving features,
- Engagement with extended value chains for in-vehicle services,
- Mobility As A Service (MaaS), and
- Software Defined Vehicles.

This move explicitly requires a robust solution for trusted services that allows for agility in deploying services, flexibility in developing services post-production, evolving cryptography requirements, and the increase in capabilities for security solutions. These needs have the added complexity of not only being relevant for the OEM (and their suppliers) but also for as greater and differentiated value chain for related services.

2.1.1 New Use Cases for Secure Services in Automotive

As Automotive has undergone tremendous changes in the types of services offered inside and outside the vehicle, these services have resulted in use cases with more increased and articulated security requirements. Some examples of these use cases are highlighted in the following figure.

Figure 2:
Examples of Automotive Use Cases with Enhanced Security Requirements



As the security requirements around automotive services have grown, the relevance of GlobalPlatform technologies has increased. In particular, some of the overriding requirements associated to these use cases include:

- Enablement of Chains of Trust Across Software Modules;
- Secure update exchanges that are INDEPENDENT of the infrastructure and protocol used, allowing both updates to a single device (e.g. car keys) and/or to a group of devices (e.g. update of software);
- Deployment of new services with standardised APIs in hardware protected environments;
- Comprehensive and agile lifecycle management: from the production process, during operations, all the way through decommissioning;
- Portability of services in different trusted operating systems;
- Management of Multiple Trusted Service Providers:
  - Managing the control of ownership across the value chain
  - Hosting the trusted services of third parties in isolation.

GlobalPlatform's technologies satisfy these requirements directly and this alignment is demonstrated by the current deployment of Secure Components in vehicles around the world.

2.2 Evolution in ECU Architecture

Historically, the automotive industry has had independent ECUs with isolated functions and each function has had one ECU for each connection. This has been in part due to the primary role of functional safety requirements in Automotive.[2] This differentiation has created an important change also in the security required within the vehicle.

2.2.1 Security as a Guarantee for Safety

Security and safety are intricately related but have important distinctions. While an individual embedded ECU may be able to behave correctly (i.e., safely) when under attack, it is hard to argue that a vehicle as-a-whole will be safe if its broader systems are insecure. Simple security – such as ensuring communications integrity and preventing illicit software update – is needed throughout the vehicle. Nonetheless, many of the most security critical domains are not themselves considered safety critical.

GlobalPlatform technologies are relevant throughout the vehicle, but much of the early commercial focus has been on ECUs that were considered security critical, while not being (as) safety critical (for example, Infotainment, Cluster, Gateway, Telematics, etc.). With an increase in the number of attack surfaces[3] and the increased amount of data exchange, the importance of security in the vehicle continues to grow.

2 https://www.iso.org/standard/68383.html

3 NIST definition of Attack Surface: The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment. https://csrc.nist.gov/glossary/term/attack_surface#:~:text=Definitions%3A,%2C%20system%20element%2C%20or%20environment.

2.2.2 Move to General Purpose Computing Units

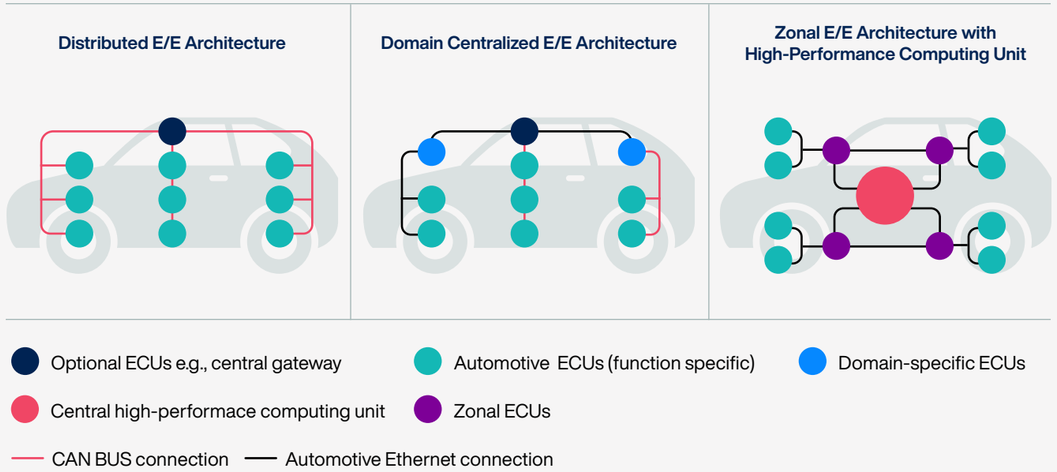
Often heralded as "software defined vehicles", there is a significant trend toward using more general-purpose computing, rather than specialized components, as core elements of vehicles. This approach provides the advantage of flexibility – for example, in terms of ability to tackle supply chain issues, or to upgrade functionality over the life of a vehicle.

There are clear advantages of this approach, but also challenges – in particular, in ensuring safety and security levels. GlobalPlatform TEEs and SEs are both general purpose *security* environments, which answer to the automotive needs. Furthermore, both GlobalPlatform TEEs and SEs are standardized to allow flexibility of hardware and software supply (with the portability of services), and to support malleable yet secure software applications.

2.2.3 Differentiation of ECUs

Combined with the general move to general purpose computing units, the automotive industry has been undergoing many evolutions with the creation of collaboration across ECUs within one domain and cross-functional connections with a central gateway. These evolutions are forecasted to continue with the implementation of domain controllers, consolidation functions, and the inclusion of high-performance computing in many areas.[4] The differentiation between ECUs has become necessary to support the sophisticated services emerging in the automotive industry. In the move towards zonal E/E architecture, the control of access and authentication requires robust security in each component. With these changes, the enhanced security features of GlobalPlatform Secure Elements and Trusted Execution Environments becomes more relevant to automotive.

Figure 3:
Forecasted Evolution in E/E



Source: Askaripoor, H.; Hashemi Farzaneh, M.; Knoll, A. E/E, Architecture Synthesis: Challenges and Technologies. Electronics 2022, 11, 518. https://doi.org/10.3390/electronics11040518

4 https://www.mckinsey.com/automotive-software-and-electronics-2030-full-report.pdf

2.2.4 In Vehicle and Off-Vehicle Communications

Increasingly ECUs need to *securely* communicate with other ECUs and with cloud services or roadside infrastructure. This will require the use of cryptographic keys, and these keys must be protected. While early systems focused on fixed symmetric keys and fixed algorithms, often in hardware, increasingly there is a need to be more dynamic. Public Key Cryptography is the norm, and Post-Quantum Cryptography is anticipated within relatively few years. Maturing security practices mean that keys need to be dynamically upgraded, and deployment and use audited. Increasingly standard protocols are used – such as X.509 certificates and TLS – and these bring with them larger software stacks and a greater chance of vulnerabilities that need to be patched. All of this means that a much more flexible, more powerful approach is needed. GlobalPlatform SE and TEE technologies can both provide appropriate solutions.

2.3 Stringent Cybersecurity Regulations

The way cybersecurity is regulated in Automotive has seen a dramatic change with UNECE 155[5] for *Cyber Security and Cyber Security Management System* and UNECE 156[6] for *Software Update and Software Updates Management System*. These regulations are applicable in over 60 countries around the world and provide a framework to ensure that cybersecurity is appropriately addressed along the entire value chain and that the OEM is responsible for ensuring this compliance. These regulations have proved to be a gamechanger for cybersecurity, as cybersecurity was primarily dealt with by OEM suppliers and without a common agreement on what was the baseline for the bar of achievement.

Furthermore, regulations on Post-Quantum Cryptography[7] are evolving around the world. The approaches are regionalized and unlikely to be harmonized. In the USA, the NSA has set 2035 as the deadline for the adoption of Post-Quantum Cryptography across national security systems; traditional networking equipment is expected to comply with the new standards by 2030.[8]

In addition, other relatively new automotive-relevant cybersecurity regulations exist in different regions, such as:

- Europe: Cybersecurity Act in Europe, General Data Protection Regulation in Europe, and the NIS2 Directive on common level cybersecurity
- China: Cybersecurity Law, Encryption Law, Information Security (SAC/TC 260), and SAC/TC 114/SC 34/WG Cyber
- USA: NHTSA Cybersecurity Guidelines

The ramp-up on cybersecurity regulations has resulted in the need for OEMs to be engaged directly in the cybersecurity compliance process and to determine how to best ensure cybersecurity approaches in products as well. GlobalPlatform technologies are best in class for trusted digital services and devices and provide a relevant piece of the puzzle in ensuring cybersecurity best practices are adopted.

5 https://unece.org/sites/default/files/2023-02/R155e%20%282%29.pdf
6 https://unece.org/sites/default/files/2021-03/R156e.pdf
7 https://csrc.nist.gov/projects/post-quantum-cryptography
8 https://fedscoop.com/nsa-sets-2035-deadline-for-adoption-of-post-quantum-cryptography-across-natsec-systems/

2.4 Standards for Cybersecurity Compliance

With the wave of changes in regulations, relevant standards have also been issued by different organizations including British Standards Institution (BSI), the International Electrotechnical Commission (IEC), the International Standards Organization (ISO), and the Society of American Engineers (SAE).

Two reference standards for demonstrating compliance with the UNECE 155/156 Cybersecurity Regulations exist:

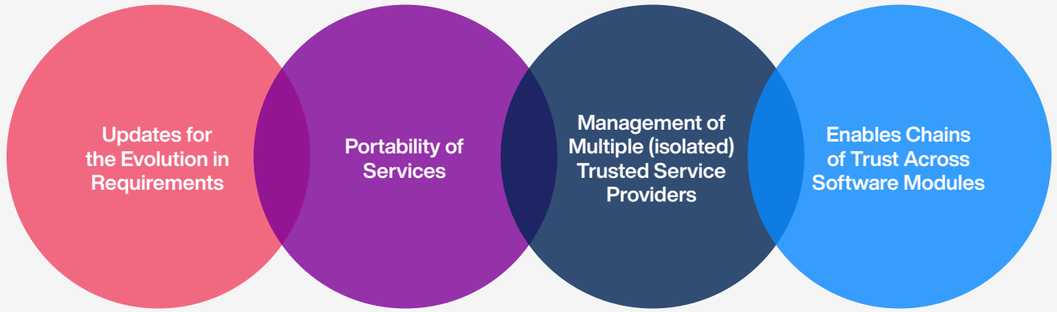
- SAE/ISO 21434[9] *Road Vehicles — Cybersecurity Engineering*, which is the de facto guidelines on how to demonstrate compliance for UNECE 155 with regards to processes and threat analysis and risk assessment.
- ISO 24089 *Software Update Engineering*[10], which is the guidelines for addressing compliance to the UNECE 156 regulation.

SAE has also issued the Hardware Protected Security for Ground Vehicles (J3101) standard[11] which provides guidelines on different practices for access mechanisms to system data and/or control. The standard provides a generalization of the common requirements for this use case, focusing on authentication, authorization, and access enforcement. Although this standard is not explicitly referenced in ISO/SAE 21434, it provides indications on requirements for product-level security.

2.5 GlobalPlatform's Answer for Automotive

GlobalPlatform's technologies explicitly answer the security requirements of the previously presented trends impacting the automotive sector by providing a secure environment, which engages with a host of different trusted applications. This security and hardware protected environment is based upon a Platform, i.e., a common software environment where different applications run. This platform approach answers today's requirements from Automotive, while allowing to future-proof now:

Figure 4:
Key GlobalPlatform Features for Automotive Security



9 https://www.iso.org/standard/70918.html
10 https://www.iso.org/standard/77796.html
11 https://www.sae.org/standards/content/j3101_202002/

Moreover, the implementation of GlobalPlatform technologies is fostered by: existing compliant applications, tools to create new ones, as well as a vibrant existing eco-system which also supports customised development.

2.5.1 GlobalPlatform Alignment with Automotive Sector

GlobalPlatform is cooperating with Society of Automobile Engineers (SAE International) to ensure alignment. In 2023, GlobalPlatform conducted a mapping of GlobalPlatform specifications for Secure Components to the SAE J3101 Hardware Protected Security Environment Recommendations. This work details how GlobalPlatform certified components directly comply with these automotive requirements while leveraging best-in-class security standards. Some areas regarding trusted applications/applets are being reviewed to be included in dedicated GlobalPlatform Automotive Configurations.

Furthermore, GlobalPlatform is cooperating with AUTOSAR to ensure alignment as well.

To this end, the GlobalPlatform automotive configurations will be a tool to verify direct compliance of products with SAE's J3101 Hardware Protected Security Environment and integration capabilities with AUTOSAR Platforms. Furthermore, this configuration will also have associated test suites to demonstrate traceability of compliance with J3101 requirements (and others as relevant).

2.5.2 GlobalPlatform Market Presence

GlobalPlatform technologies are based upon more than 20 years of experience in supporting trusted digital services and devices in different industries and represent *the* global standard for managing applications on secure chip technologies. In fact, there are over:

- 70 Billion Secure Elements (SEs)[12] shipped worldwide that comply with GlobalPlatform specifications.
- 15 Billion GlobalPlatform compliant Trusted Execution Environments (TEEs)[13] in the market today.

GlobalPlatform specifications are publicly available for use on a royalty-free basis (https://globalplatform.org/specs-library/).

12 GlobalPlatform Secure Elements are tamper-resistant platforms used to host applications as well as confidential and cryptographic data.
13 A Trusted Execution Environment (TEE) is a combination of hardware and software: a secure operating system and the hardware on which it runs and which has sufficient security features to isolate the secure operating system from selected external software threats. TEEs are most commonly found on Arm application processors, where Arm hardware features (TrustZone™) provide the necessary security isolation and a TEE Operating System runs isolated from a Regular Execution Environment (REE), consisting of one or more Regular Operating Systems, possibly on a hypervisor. Whilst this is the most prevalent deployment today, the TEE architecture is *not* limited to Arm-based solutions.

03. Security as a Platform

For GlobalPlatform, security is based upon a common security and hardware protected environment platform, which engages with a host of different trusted applications. This platform approach is based upon three main principles of Secure by Design:

Figure 5:
GlobalPlatform's Principles for Common Security and Hardware Protected Environment Platform

Secure Design

Overall Device Trust Architecture

- provides a framework for ensuring trustworthiness with Roots of Trust using Secure Components.
- APIs support interoperability and reuse across secure components

Trust chains

- use the established trustworthiness of code and data at boot time to extend it to other code and data throughout the runtime of the device.
- A chain of trust can be extended beyond the device to the management system.

Platform & Application-Centric Approach

- Trusted applications within the secure component (TEE or SE) have access to a set of secure services that are certified (e.g. state of the art crypto services)
- offers services to other components within the secure component, or elsewhere in the system.
- Based upon a common security and hardware protected environment platform
- Multi-tenant with isolation

Design for Certification

- The design of the secure component is structured to simplify the certification.
- Device manufacturers get value from this design from the beginning in optimising of the functional and security certification.
- Specific evaluation technology has been created to optimise the certification (e.g. SESIP)

3.1 Security Definitions

In order to navigate the different nuances in security, this paper also provides some key security definitions for roots of trust, chains of trust and trust anchors, as well as an overview of the specific meanings for GlobalPlatform.

3.1.1 Roots of Trust

Computing systems can use technologies such as cryptography to demonstrate the trustworthiness of code or data – for example a message may be signed – but in all computing systems there must be a base system that is *unconditionally trusted* – as there is nothing that can 'prove' its trustworthiness that would not itself need to be unconditionally trusted to do so. We call these systems 'Roots of Trust'.

Many standards bodies have developed formal definitions of roots of trust, but all are similar in concept. Relevant standard bodies with definitions include:

- GlobalPlatform
- Trusted Computing Group (TCG)
- Open Compute Project (OCP)
- National Institute of Standards and Technology (NIST), US Department of Commerce

GlobalPlatform defines Roots of Trust as:

Figure 6:
GlobalPlatform Root of Trust Definition

A computing engine, code, and possibly data, all co-located on the same platform; providing security services; as small as possible to limit the attack surface.	***No ancestor entity is able to provide a trustable attestation (in digest or other form) for the initial code and data state of the Root of Trust.***	***Depending on the implementation, the Root of Trust is either Bootstrapped or Non-Bootstrapped.***

GlobalPlatform further specifies that the Root of Trust must have the following properties and characteristics.

Figure 7:
Root of Trust Requirements

Properties:	Immutability	
	Or mutability under authorization	Unique identifiable ownership
		Ownership optionally transferable
	Suitable for certification	
Characteristics:	Manufacturing process SHALL be protected and certified.	
	When a platform is starting, it SHALL verify the integrity and presence of key and data sets.	If the verification fails the RoT SHALL forbid any interaction with any (communication) interface.
	All service providers using the security services of an actor SHALL be identified.	
	Each RoT SHALL have a unique RoT Identification number.	

3.1.2 Chains of Trust

The Chain of Trust leverages the root of trust to verify trust across software modules.

When service providers want to enable and update digital services, they need to create an end-to-end secure communication with the end-point platform or device. The reliability of this secure communication is based on the secure services and the RoT available in the endpoints. With consumer devices, the endpoint will be used to authenticate the end user and store private data. IoT devices generate data that needs to be authenticated by the device and protected before management in the IoT network's cloud server. Both use cases require security in the endpoint to enable this secure link and perform authentication.[14]

Formal GlobalPlatform Definition: *A transitive trust relationship starting from a Root of Trust that is propagated to the Validated/Measured Modules, when a software module verifies/measures the next software module and keeps a reportable record of this verification.* [15]

The strength of the Chain of Trust is based upon the strength of Root of Trust. Chains of Trust allow device manufacturers and service providers to offer secure digital services while ensuring device integrity and security, alongside end-user privacy. [16]

3.1.3 Trust Anchors

Formally, Trust Anchors are defined in terms of public key cryptography representing a trusted entity. A trust anchor usually appears in the form of a root certificate. Trust anchors have different definitions in many different systems. Two relevant definitions for trust anchors include:

- The Internet Engineering Task Force (IETF) defined standards for trust anchor in 2010 as: *An authoritative entity represented by a public key and associated data. The public key is used to verify digital signatures and the associated data is used to constrain the types of information or actions for which the Trust Anchor is authoritative. [RFC5914, Abstract* https://www.rfc-editor.org/rfc/rfc5914 *]. Trust anchor is a core concept within PKI denoting the digital certificate of an entity for which trust is assumed. Trust anchor is required for the validation of the digital certificate trust path between parties.* [17]
- More recently, and focusing specifically on Automotive, the Society of Automotive Engineers (SAE) defined Trust Anchors mapped to root certificates in J3101: *Trusted Root Certificate (aka Trust Anchor): The top-level certificate in a certificate chain hierarchy, kept in a trust store to verify a certificate's trustworthiness* [18]

Using the formal definition, a root of trust could be used to store a Trust Anchor (certificate and private key).

14 GlobalPlatform, Deploying and Protecting Digital Services with Chains of Trust, May 2018, pg. 8 https://globalplatform.wpengine.com/wp-content/uploads/2018/05/GlobalPlatform-Chains-of-Trust-16May2018.pdf

15 GlobalPlatform Root of Trust Definitions and Requirements v1.1, June 2018 – GP_REQ_025 – https://globalplatform.org/specs-library/root-of-trust-definitions-and-requirements-v1-1-gp-req_025/

16 GlobalPlatform, Deploying and Protecting Digital Services with Chains of Trust, May 2018, pg. 7 https://globalplatform.wpengine.com/wp-content/uploads/2018/05/GlobalPlatform-Chains-of-Trust-16May2018.pdf

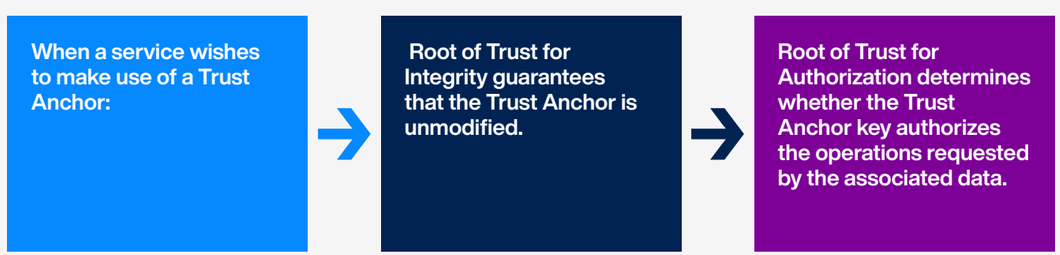
17 https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Trust+Models+Guidance

18 SAE International, J3101 Hardware Protected Security for Ground Vehicles, 02/2020, page 70.

3.1.4 GlobalPlatform Trust Anchors

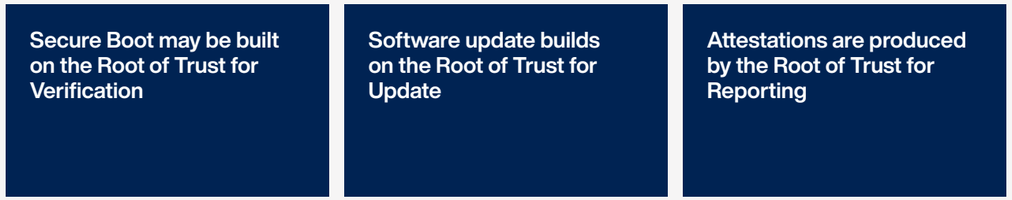
As a basis for PKI security, trust anchors must be securely stored to ensure their integrity – and in the case of private keys – to limit access appropriately.

Figure 8:
Using a Trust Anchor



The Root of Trust, therefore, enables proper management of the trust anchor.[19]

Figure 9:
Service Examples Built Upon the Trust Foundation

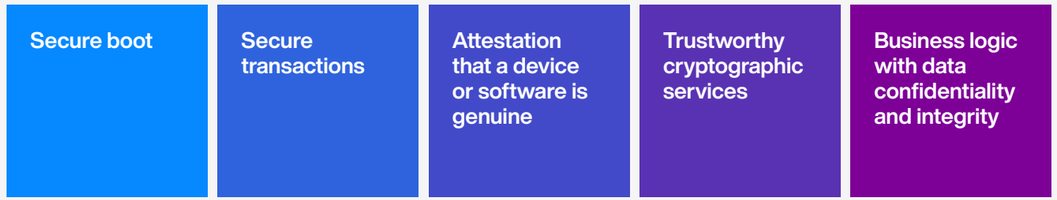


19 https://globalplatform.org/specs-library/root-of-trust-definitions-and-requirements-v1-1-gp-req_025/

3.1.5 Higher Level Services

While “Root of Trust” and “Trust anchors” have emerged separately, both provide the trust foundations on which more complex services can be developed. Examples include:

Figure 10:
Trust Foundation Examples



These functions are important in many different applications, and standards bodies often discuss the need for trust anchors and define minimal or expected characteristics for their industries or use cases. SAE, ISO, TCG, and GlobalPlatform are examples of organizations that define specific forms of Roots of Trust and Trust Anchors. While some definitions are focused on specific implementations, SAE defines a general abstract characterization of a trust anchor in J3101 Hardware Protected Security Environments. These characterizations provide the key elements upon which many different technical solutions demonstrate compliance. GlobalPlatform technologies, upon analysis by the Automotive Task Force, demonstrate compliance with these characterizations either through the platform or as a combination with the trusted applications.

3.2 Common Platform

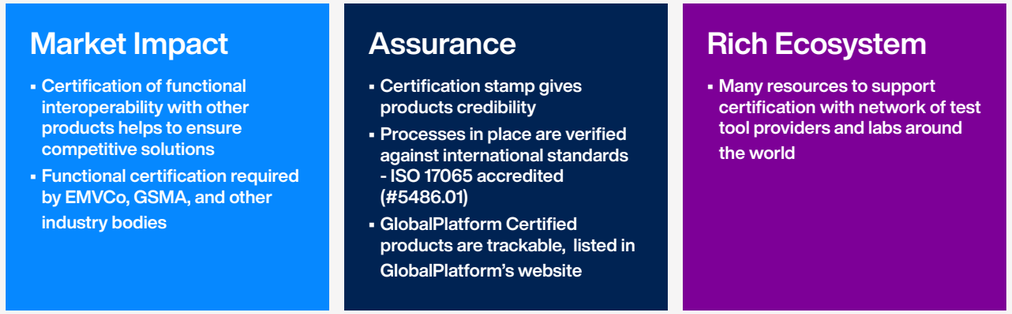
GlobalPlatform’s SE and TEE technologies are built upon a secure platform upon which multiple trusted applications can be created and executed. The platform itself provides a set of secure services and is certified for functional compliance and security. Trusted applications are then written to meet the specific requirements of a particular ECU or a customer solution. Key Stores, Digital Car Keys, and DRM solutions are examples of applications that can be written to run on these platforms.

The distinction between the platform services and the applications provides significant flexibility. TEE and SE vendors can focus on providing state-of-the-art platforms, and evolve them over time with horizontal features, such as new cryptographic algorithms. OEMs and Tier 1s are then able to focus on project or vehicle specific applications, which benefit from the common platform security. Both platform and trusted applications can be updated independently as needed.

3.3 Platform Certification

GlobalPlatform designs solutions on the principle that certifications are a key step to ensuring that specifications are functionally and security-wise compliant with GlobalPlatform Specifications. Moreover, the importance of certification in securing devices and services provides a means to ensure key benefits:

Figure 11:
Benefits of Certification



To achieve this, GlobalPlatform solutions:

- Structure the design of secure components in a manner that enables ease in certification (given that the specifications are designed from the beginning to be validated in certification).
- Ensure the design value to device makers from the beginning in optimizing the functional and security certification.

Certification to ensure security should entail the following characteristics:

- Testing by a 3rd Party so that there is an “independent” inspection of results;
- Publicly available results on the certification levels and the protection profiles used;
- Transparent definition of the scope being certified (i.e., Target of Evaluation) in terms of components vs. systems.

Furthermore, a specific evaluation methodology has been created to support certifications: the Security Evaluation Standard for IoT Platforms (SESIP), described in section 6.2.

04. GlobalPlatform Secure Components

GlobalPlatform Secure Components (SCs)[20] protect keys, trusted applications, data, and devices across a wide range of use cases. GlobalPlatform Secure Components include:

- Secure Elements (SEs)[21]
- Trusted Execution Environments (TEEs)[22]

These solutions can be used singularly or together, as most appropriate.

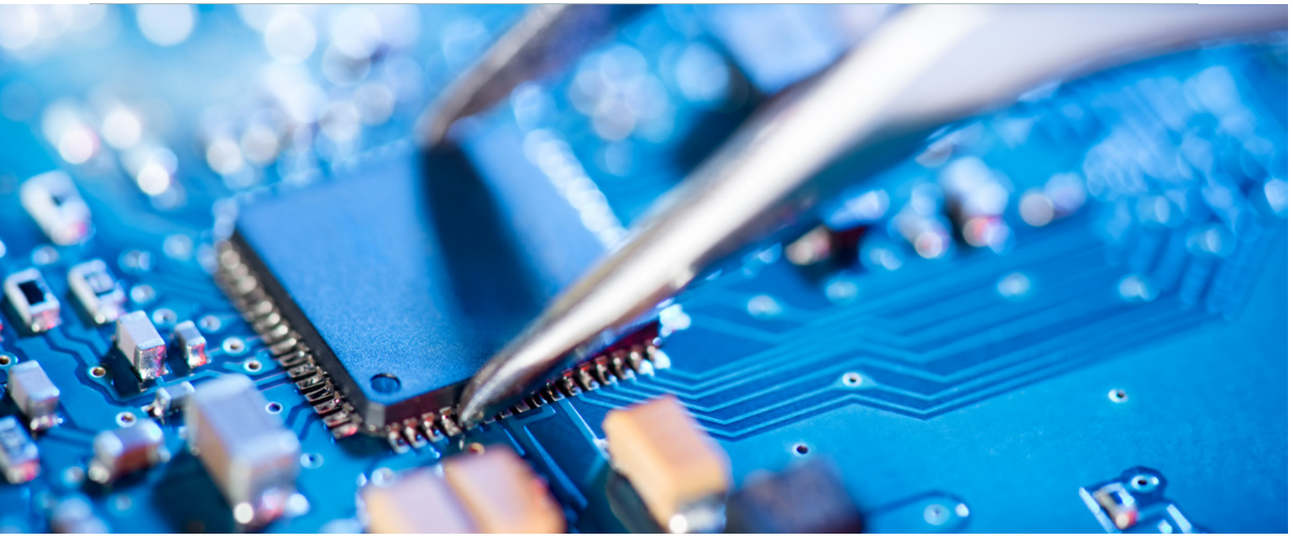
4.1 Common Characteristics

GlobalPlatform supports the vision that flexibility and reuse are critical for the automotive market. Because GlobalPlatform specifications accommodate different hardware, operating systems, and firmware, they support innovation and portability, as well as fostering creative solutions available in the market. To this end, an application written for one SE or TEE can be easily moved to another. Common APIs and approaches across vendors mean that engineers learn transferable skills.

Figure 12:
GlobalPlatform Technologies: Providing Flexibility While Supporting Innovation and Portability

Provides Clear Security Foundation for Service Providers	Accommodates Different Implementations	Supportes Differentiation of:	Enables Externally Verifiable Compliance with Specifications for both:
▪ No need for Service Providers to understand all the details of the implementation ▪ Supports service development across value chain	▪ Innovation is not stifled by single OS, firmware, hardware ▪ Not an all-or-nothing proposition ▪ Existing multiple competitive solutions available in the market	▪ Secure functions required ▪ Security level desired	▪ Robustness and security level declared ▪ Functional behavior and interoperability

20 https://globalplatform.org/insight-series-the-evolution-of-secure-components/
21 GlobalPlatform Secure Elements are tamper-resistant platforms used to host applications as well as confidential and cryptographic data.
22 A Trusted Execution Environment (TEE) is a combination of hardware and software: a secure operating system and the hardware on which it runs and which has sufficient security features to isolate the secure operating system from selected external software threats. TEEs are most commonly found on Arm application processors, where Arm hardware features (TrustZone™) provide the necessary security isolation and a TEE Operating System runs isolated from a Regular Execution Environment (REE), consisting of one or more Regular Operating Systems, possibly on a hypervisor. Whilst this is the most prevalent deployment today, the TEE architecture is *not* limited to Arm-based solutions.



GlobalPlatform also specifies a means for updating secure components that is independent of the details of the infrastructure and protocols used by a particular commercial implementation. The approach allows for online or offline update and supports both single device and group updates. This enables the ecosystem to ensure a consistently high degree of security while enabling innovation in other aspects of commercial software update solutions. This approach supports automotive requirements regarding the ability to ensure brand differentiation as well as comparable security solutions.

4.2 Secure Elements

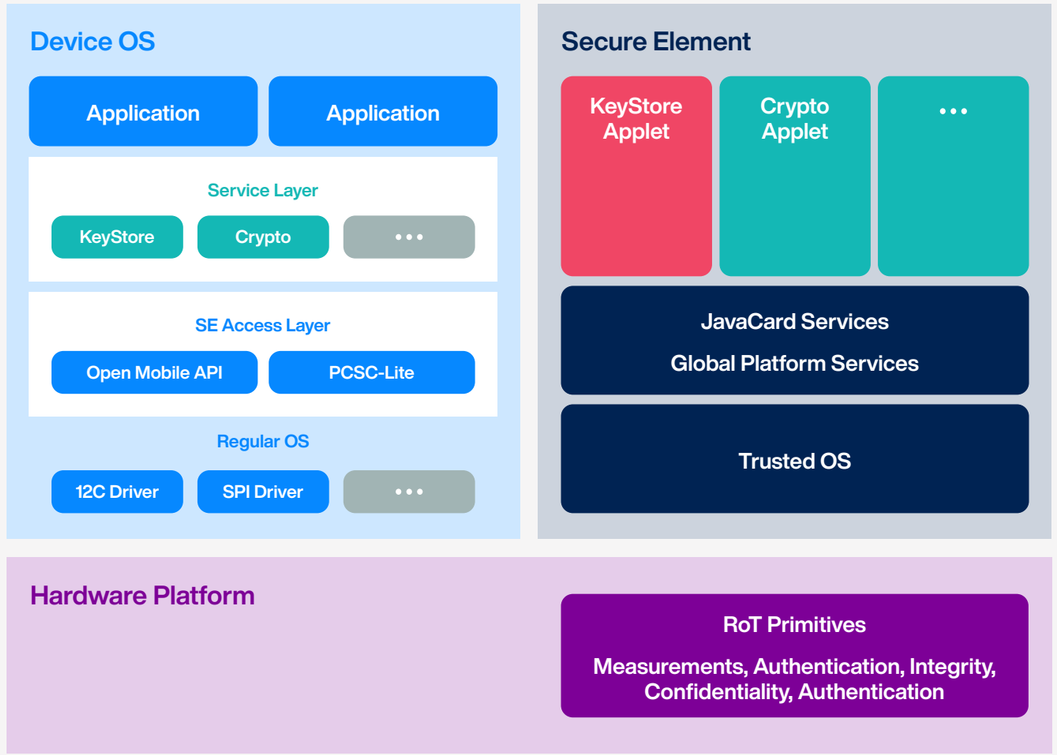
GlobalPlatform Secure Elements are tamper-resistant platforms used to host applications and confidential and cryptographic data.

Figure 13:
Features of GlobalPlatform Secure Element

See GlobalPlatform's Secure Element specifications (https://globalplatform.org/specs-library/?filter-committee=se) which are free for public use.

4.2.1 Secure Element Architecture

Figure 14:
Secure Element Architecture



4.2.2 Secure Element Form Factors

Secure Elements are widely deployed in different form factors, including:

- Removable SIM cards (UICC),
- Embedded Secure Elements (eSE),
- Token (USB / Contactless NFC), and
- Embedded SIM (eUICC).

All these Secure Elements are implemented and certified according to GlobalPlatform specifications, thus providing interoperability on a wide range of form factors.

4.2.3 Embedded Secure Elements

Embedded Secure Elements can be used in a vehicle for different use cases, and as such can be integrated in different components, generally thru an SPI (Serial Peripheral Interface) or I2C (Inter-Integrated Circuit) interface.

UICCs, also known as SIM (Subscriber Identity Module), are typically connected to the vehicle's telematics unit, which is responsible for managing the vehicle's communications and networking capabilities. While in some cars the UICC is a removable Secure Element inserted in a UICC slot, this has increasingly been replaced by embedded UICCs (eUICC) that are directly connected to the telematics unit. UICC or eUICC provide and secure the connectivity of the car. They can be updated with operator profiles over-the-air (OTA) using remote SIM provisioning to securely download the operator profile and activate the new mobile network operator and allow the car to access its services.

In the case of the Digital Key, which is a specification of the Car Connectivity Consortium[23] for controlling the car from a mobile phone (e.g., for opening the doors or starting the engine), the eSE is integrated into the Vehicle Gateway ECU. As another example, for Electrical Vehicle (EV) charging, following the ISO 15118 standard specifying the communication protocol for EVs, the eSE is typically connected to the vehicle's charging system or powertrain system.

4.3 Trusted Execution Environment (TEE)

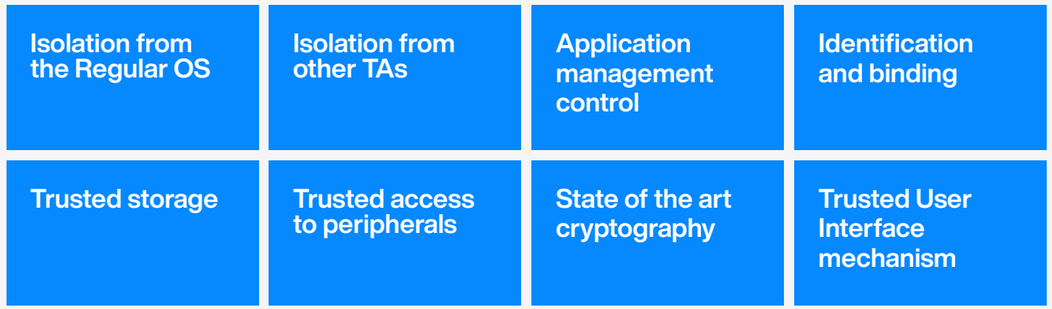
A Trusted Execution Environment (TEE) is a combination of hardware and software: a secure operating system and the hardware on which it runs and which has sufficient security features to isolate the secure operating system from selected external software threats. TEEs are most commonly found on Arm[24] application processors, where:

- Arm hardware features (TrustZone™) provide the necessary security isolation and
- a TEE Operating System runs isolated from the Regular Execution Environment (REE), consisting of one or more Regular Operating Systems, possibly on a hypervisor.

While this is the most prevalent deployment today, the TEE architecture is *not* limited to Arm-based solutions.

A TEE provides a set of features for Trusted Applications (TAs) running within it:

Figure 15:
GlobalPlatform TEE Security Features



23 https://carconnectivity.org
24 https://www.arm.com/markets/automotive

As a TEE typically runs on an application-class processor, it generally offers high processing speeds and a large amount of accessible memory. TEEs often have privileged access to hardware peripherals, enabling them to be used to mediate access to a protected peripheral, for example to provide a Trusted User Interface (privileged access to display) or to provide secure connectivity (privileged access to keys stored in a Secure Element, HSM, or SHE[25]).

See the GlobalPlatform Trusted Execution Environment specifications: https://globalplatform.org/specs-library/?filter-committee=tee, which are free for public use.

4.3.1 Trusted Execution Environment Architecture

Figure 16:
GlobalPlatform Trusted Execution Environment Architecture

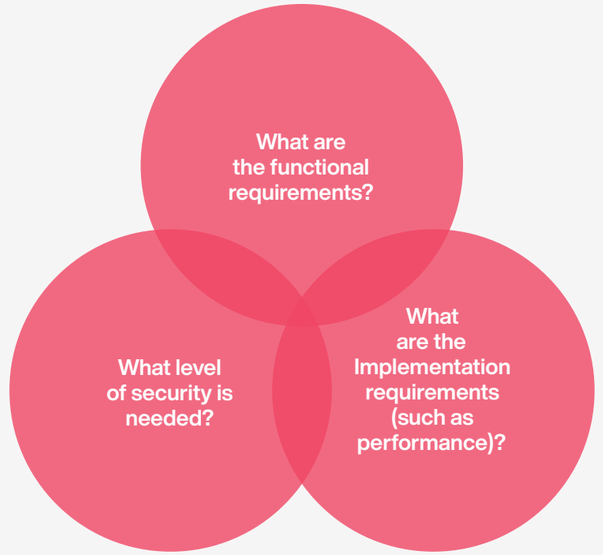
25 See Annex B for more information on traditional automotive trust anchors.

Global Platform™
Automotive Task Force

05. Selecting The Right Secure Component

Choosing the most secure component to support security management is based upon the specific implementation context, regarding:

Figure 17:
Key Questions Driving the Selection Between Secure Components



GlobalPlatform solutions provide a variety of alternatives to meet varying product requirements. A particularly important aspect is that GlobalPlatform's Technical Community and Secure Component Attack Working Groups are regularly analyzing the different known attacks and new attack methodologies. GlobalPlatform solutions are updated to maintain the attack list, consistent with the different industrial markets.

5.1 Functional Requirements

The first and most important question when selecting a root of trust or trust anchor is:

What is Its Purpose?

GlobalPlatform technologies provide a secure environment for more than one trusted application and include multi-tenant services (versus more traditional automotive implementations with a single fixed purpose).

This type of security solution, which benefits from a range of secure trusted applications, provides flexibility to support a variety of new services, e.g., Post-Quantum Cryptography migration, Over-The-Air (OTA) updates, as well as others. For example, while a Trusted Platform Module (TPM) is traditionally a separate hardware device, it can also be created as a trusted application running inside a GlobalPlatform Secure Component.

5.1.1 Secure Services Supported

GlobalPlatform TEEs and SEs can both support multiple trusted applications/applets. This makes them particularly relevant for the parts of the vehicle services subject to change. For example, many OEMs have plans to introduce additional in-vehicle services that need protection. Furthermore, GlobalPlatform specifications support Secure In-Vehicle Communications (with secure channels) and Secure Updates of the Device.

5.1.1.1 Secure Boot

Secure boot is a critical part of any secure system; however, the technical steps to ensure secure boot vary depending on the hardware used.

5.1.1.1.1 Secure Element

As the SE contains all code that it will execute within a physically secure boundary, there is no opportunity for an attacker to modify the code once it is in place. Boot time validation is therefore (at best) a secondary consideration. Of much more import is the validation of software when it is first loaded into the SE, either in factory or as part of an Over The Air update.

5.1.1.1.2 MCUs

Embedded MCUs often run entirely from firmware images. If there is any possibility that the firmware could have been modified, then it is important to validate that the image is as expected. SHEs are commonly used to calculate a message digest of a firmware image either before, or in parallel with, booting an MCU. If the hash is found to have the wrong value, the boot is aborted.

5.1.1.1.3 Application Class Processors

Larger application class processors have a more complex boot flow. They initially boot from ROM, which is immutable. The ROM code then loads a first level boot loader, which loads subsequent software images. Unlike MCU/SHE[26] combinations, validation of images is usually done by the CPU itself as part of the boot process, and also unlike the SHE, typically asymmetric cryptography is used to validate the images. This simplifies update, as there is no need to recalculate a message digest and there is a means to validate a previously unseen image. As validation is asymmetric, no secrets are involved in the validation step, so there is no need for a secure enclave of any sort during boot.

26 See Annex B for more information on traditional automotive trust anchors.

While TEEs are part of the secure boot flow on a modern processor, the majority of the boot security relates to the low-level ROM code and dynamically loaded bootloader code. There is really no opportunity (or need) for a SHE-like parallel validation of the image.

However, it is interesting to note that as concerns over Post-Quantum Cryptography grow, the dominant approach for application processors is not without its issues. One possible future approach is to simply change the signature scheme to one considered PQC-safe. Another is to move away from signatures for boot validation and adopt a message digest-based approach.

5.1.1.2 Boot Attestation

Boot is increasingly complex, especially for application processors running hypervisors and multiple operating systems. An increasing trend for the boot machinery is to be designed so that it can record and later attest the state of the system it booted – either directly (as a set of properties) or by deriving a key from the hash of 'the entire system' (DICE[27]). Attestation is a common feature of Trusted Platform Modules (TPMs[28]) and also GlobalPlatform SEs and TEEs.

5.1.2 Over-the-Air (OTA) Updates

Given that most vehicle OEMs are considering a 10- to 15-year lifecycle for new vehicles, it is essential that the *security applications, keys, and cryptographic algorithms* can be updated. This is particularly important given the expected changes related to Post-Quantum Cryptography.

GlobalPlatform has defined protocols for OS update and Trusted Application updates for both Trusted Execution Environments[29] and Secure Elements[30] (ref SAM[31]).

Generally speaking, the more complex the application is, the greater the need is for the ability to update. Given current expectations regarding post-quantum algorithms, even the simplest system using cryptography is likely to need updates during its lifetime. If OTA updates are not supported, the only alternative is an expensive recall.

5.1.3 Functional Certification

Functional certification verifies the behaviour and completeness of products (including compliance with GlobalPlatform requirements and configurations for SEs and TEEs). This certification confirms that a digital service will perform as intended in the field on any certified product, regardless of the product provider.

Furthermore, this certification enables fast deployment of secure components across products. Moreover, functional certification drives market interoperability.

5.1.3.1 Ensuring Flexibility with Interoperability

OEMs need the flexibility to switch suppliers during the lifetime of a vehicle model. Choosing a technology with a strong functional certification ensures that changes in suppliers do not lead to a need to reimplement critical software applications.

27 https://trustedcomputinggroup.org/work-groups/dice-architectures/
28 https://trustedcomputinggroup.org/work-groups/trusted-platform-module/
29 https://globalplatform.org/specs-library/tee-management-framework-including-asn1-profile-1-1-2/
30 https://globalplatform.org/specs-library/globalplatform-technology-secure-element-management-service-amendment-i/
31 https://globalplatform.org/resource-publication/secure-application-for-mobile-sam-for-mobile-operators/

5.2 Implementation Requirements

Once the functional requirements have been locked down, various other criteria should be considered.

5.2.1. Performance

When identifying the required performance characteristics of the secure component (whether SE or TEE), the focus should not be on absolute performance characteristics, but on whether there is *sufficient* performance for the given task, especially given other tasks assigned to the system at the same time.

There is often a misconception that customized hardware is always faster than general purpose hardware. Although this is true in some limited cases, generally speaking, a software implementation on a modern application-class CPU will far exceed the performance of a special purpose hardware element such as a SHE or HSM. There are several reasons for this, including:

- Modern CPUs have acceleration for atomic operations that crypto algorithms are based on, negating the advantage of custom hardware.
- The connection between a specialized SHE or HSM and the main application process can also be a bottleneck.

5.2.2 Memory Cost

Another consideration is the amount of memory that must be allocated for a given task.

- Secure Elements are isolated systems so they do not share memory with other parts of the system – however a sufficiently large memory size should be specified both to meet current application needs and to ensure sufficient head room for any future additions or upgrades.
- Some systems may support dynamic allocation – for example to support a short-lived but memory-intensive task, such as face recognition. Nonetheless, there generally is also a need to permanently allocate memory to a Trusted Execution Environment, meaning the system designer must ensure there is enough memory to support both the TEE and REE.

5.2.3 Use of Standard Technology

Many system designers prefer to use standard APIs rather than rely on proprietary designs. The advantage of a standard API set is three-fold:

- The APIs have undergone significant industry review and refinement.
- There is an existing ecosystem of experienced developers.
- The use of standard APIs provide flexibility in vendor selection and change.

GlobalPlatform provides standard API sets available to the designers of trusted applications/applets.

5.2.4 Resistance to Attack

It is important to understand what types of threats are important, and how to balance the need to protect subsystems sufficiently, without overly increasing cost or limiting implementation choices.

- Some applications may need to protect against physical attack: for example, during a vehicle service; and
- For others, the focus may be on software attacks: for example, based on malicious software applications.

Based upon the differences in target security, GlobalPlatform components provide different options.

5.3 Security Evaluation

GlobalPlatform certifies products in line with Common Criteria-recognized protection profiles, thus ensuring that secure components meet the required levels of security defined for a particular service. Such certification enables service providers to manage security risks confidently and effectively, while also demonstrating irrefutable proof of compliance to industry requirements.

GlobalPlatform has a strong focus on security certification for Secure Element and Trusted Execution Environments, based on Common Criteria protection profiles which it publishes.

GlobalPlatform has also begun publishing SESIP profiles, beginning with secure external memories, followed by secure MCUs and MPUs. Additional SESIP profiles are under development.

Regardless of whether the profile is written using the Common Criteria or SESIP methodology, the concepts of scope definition through *Security Targets* and common baseline definition through *Protection Profiles* remain the same.

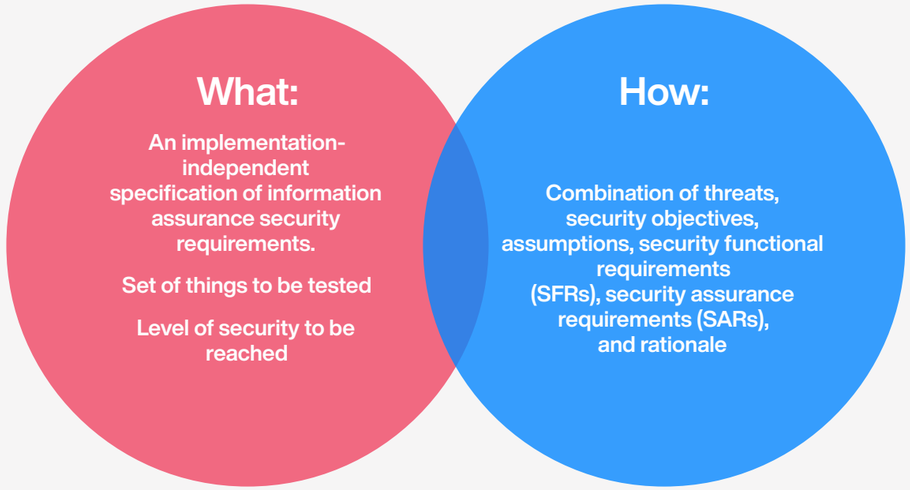
5.3.1 Scope

The scope of the security assessment is a strategically critical choice. A narrower definition of scope for evaluation (e.g., components vs. full solution) requires fewer resources but also provides less evidence.

5.3.2 Protection Profiles: Ensuring Compliance on Standardized Security Features

Protection profiles are definitions of common or, minimum required, security features that are tested to a specific security level. Protection profiles are typically defined for types or classes of products. Protection profiles provide transparency on the features tested across different solutions. GlobalPlatform has standardized different protection profiles and SESIP profiles for different solutions (SE, TEE, iSE, MCU) to foster comparable product robustness. Standardized protection profiles facilitate comparison of security features and robustness across products.

Figure 18:
Protection Profiles & Comparing Equivalency of Products



5.3.2.1 AVA_VAN Level

VAN Level is the part of the Common Criteria and SESIP that focuses on the assessment of vulnerability. This is an assessment to determine whether potential vulnerabilities could allow attackers to violate the Security Functional Requirements.

> *Vulnerability analysis... deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the Trusted Security Foundation (TSF), or interfere with the authorised capabilities of other users.*[32]

- AVA_VAN.2 (Unstructured) Vulnerability Analysis or Target of Evaluation (TOE) resistance against Basic Attack Potential
- AVA_VAN.3 Focused (Unstructured) Vulnerability Analysis or TOE resistance against Enhanced-Basic AP
- AVA_VAN.4 Methodical Vulnerability Analysis or TOE resistance against Moderate AP

32 Common Criteria definition of Vulnerability Assessment (https://www.commoncriteriaportal.org/files/ccfiles/CommonCriteriaDevelopersGuide_1_0.pdf) page 78

- AVA_VAN.5 Advanced Methodical Vulnerability Analysis

For Secure Elements, the TOE comprises the:

- hardware
- firmware
- software components and
- mechanisms that provide the security features as defined in the applicable PPs and PP-Modules.

Technically, the TOE is the part of the Product that is in the scope of the vulnerability analysis and testing but, informally, the TOE and Product are the same thing for Secure Elements.33

For Trusted Execution Environments, the TOE is the execution environment that provides secure initialization, isolation from the Regular Execution Environment (REE), isolation between Trusted Applications (TAs), Trusted Storage, Random Number Generation (RNG), cryptographic operations, etc.[34]

5.3.3 Security Target

The definition of the Security Target (ST) is the functional security level and the assurance level claimed for a particular product. The security target defines the exact threat model that the product declares resistance to. In the case of Common Criteria, the Security Target is an Evaluation Assurance Level (EAL)[35]. In the case of SESIP, the Security Target defines the assurance claim in the form of a SESIP Assurance Level between SESIP1 and SESIP5 (see Annex C for additional information).

A Security Target may comply with one or several Protection Profiles (PPs), meeting all the requirements defined in the PPs, and it can add and/or increase the evaluation items beyond the minimum requirements defined in the PP.

Informally the protection profile defines the 'test/exam' on security and functional behaviour. The EAL level or SESIP Assurance Level that is achieved by a product indicates how well it did in passing the test/exam. The relevance of either is meaningless without the other.

5.3.4 Assessing Attack Potential

A key decision for trust management is the scale of resistance to attack, both in terms of ability to generate the attack, as well as, to exploit access from attack. Attack potentials according to Common Criteria are defined as being: Basic, Enhanced-Basic, Moderate, and High. The attack potential corresponds to the effort required to apply an attack to a product in terms of:

- Expertise Needed for Attack (Layman to Multiple Experts)
- Time Needed for Attack
- Investment (Equipment) Needed for Attack
- Window of Opportunity: Is it widely available (easy to access)? #Products on Market

33 https://globalplatform.org/wp-content/uploads/2021/02/GP_SE_CertificationProcess_v2.0_PublicRelease.pdf
34 https://globalplatform.org/wp-content/uploads/2021/01/GP_TEECertificationProcess_v2.0_PublicRelease.pdf
35 **EAL Levels for Common Criteria**
EAL1: Functionally Tested
EAL2: Structurally Tested
EAL3: Methodically Tested and Checked
EAL4: Methodically Designed, Tested and Reviewed
EAL5: Semi formally Designed and Tested
EAL6: Semi formally Verified Design and Tested
EAL7: Formally Verified Design and Tested

Security evaluation is an effective means to understanding resilience for easily exploitable logical vulnerability (as well as "zero-day" and resource intensive attacks). Security evaluation evolves to reflect process and security requirements. This evaluation facilitates staying ahead of widespread attacks and verifies state-of-the-art countermeasures.

5.3.5 Robustness Testing

Security testing verifies the robustness of a clearly defined security baseline established, e.g., SE and TEE products, through their related protection profiles. Robustness is the ability of the evaluation target to resist attacks.

Robustness testing is done according to many major attack classes, such as physical attacks, perturbation attacks, logical attacks, ...

Assurance ratings on robustness are provided by different certification schemes.

For illustrative purposes, we include a discussion on side-channel attacks.

5.3.5.1 Side-Channel Attack: An Example of Attack Classes

Side Channel Attack is a leakage of information from the system under test. Hardware characteristics that could be exploited in a side-channel attack include timing, power consumption, electromagnetic and acoustic emissions. Software side channel attacks can relate to cache or memory manipulation attacks or timing and performance measurement performed in software.

One consideration for security levels needed regards the importance of hardware side-channel attacks for a product, given the distinction in GlobalPlatform specifications for Secure Components:

- Secure Elements have high resistance to hardware side-channel attacks (i.e. tamper proof) while
- Trusted Execution Environments do not directly address Hardware Side Channel Resistance (as it is not in scope of the protection profile).

Global Platform™
Automotive Task Force

5.4 GlobalPlatform Security Certification Scheme

Security certification allows a customer to validate that the solution they have selected is an appropriate base upon which to build their applications. While a full solution for an automotive certification may need to adhere to process standards (such as ASPICE)[36] or coding standards (such as MISRA)[37], these solutions will not alone ensure security: The base security environment must be secure. GlobalPlatform provides the base security environment, which guarantee enhanced and high security:

- High (Attack Resistance Potential equivalent to VAN 4 and VAN 5)
- Enhanced (Attack Resistance Potential equivalent to VAN 3)

GlobalPlatform Secure Elements provide High resistance to attack potential while GlobalPlatform Trusted Execution Environments provide Enhanced resistance to attack potential. For instance, a GlobalPlatform TEE will be resistant to attacks that may come from proficient hackers.

5.4.1 GlobalPlatform Product Assessment Process

The laboratory evaluates the Product against the requirements covered by the scope of certification in compliance, i.e., the evaluation consists of a vulnerability analysis phase (documentation review, source code inspection, and possibly some manual and/or automated testing) which gives rise to a Penetration Test Plan (PTP) submitted to GlobalPlatform Certification Body (CB), and a functional and penetration testing phase that addresses the behaviour of the security functionality and covers the attack methods.

GlobalPlatform CB reviews the PTP and confirms that it is adapted to the Security Target and fully answers to the targeted security for the scheme.

The typical duration of a GlobalPlatform evaluation is less than three (3) months for either a Secure Element or a Trusted Execution Environment, provided:

- Secure Element: The Product complies with GlobalPlatform and/or GSMA specifications, and all the necessary evaluation inputs are available as required in GlobalPlatform SE/eUICC Evaluation Methodology (GPC_GUI_163), e.g., Security Target, source code, samples. Such a duration applies for one product version.[38]
- Trusted Execution Environment: The Product complies with GlobalPlatform APIs, and the Vendor grants access to the source code of the TEE firmware and software and to a sufficient number of boards and/or devices. The developer must provide API and architecture descriptions, development boards and devices to the evaluator.[39]

The applicable Protection Profile(s) and PP-Modules are available on the public website: www.globalplatform.org.

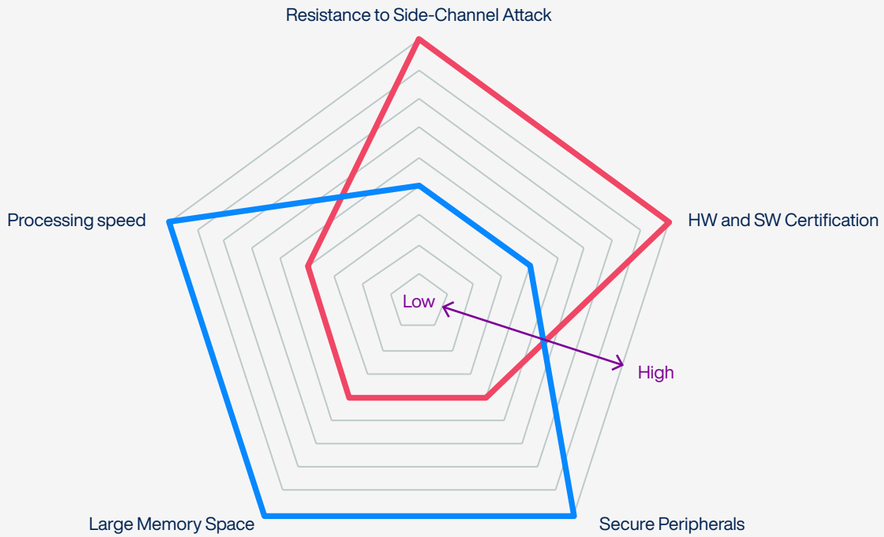
36 https://www.automotivespice.com
37 https://www.misra.org.uk
38 https://globalplatform.org/wp-content/uploads/2021/02/GP_SE_CertificationProcess_v2.0_PublicRelease.pdf
39 https://globalplatform.org/wp-content/uploads/2021/01/GP_TEECertificationProcess_v2.0_PublicRelease.pdf

5.5 Comparing Secure Components

The choice between secure components is the result of consideration of many different parameters, as evidenced by the previous chapters, specifically related to the product's characteristics and the desired security management approach. The following figure includes a comparison between Secure Elements and Trusted Execution Environments according to five differentiating parameters:

- Resistance to Side-Channel Attack
- Hardware and Software Certification
- Secure Peripherals
- Large Memory Space
- Processing Speed.

Figure 19:
Comparing Secure Elements and Trusted Execution Environments



The importance of the different parameters depends upon the relevant use case and the implementation context. For instance, if the most important parameter for a set use case is the resistance to side channel attack, then the most appropriate solution would be the Secure Element. One the other hand, if the processing speed is the most important parameter for a use case, then the most appropriate solution would be the Trusted Execution Environment.

The details between Secure Elements and Trusted Execution Environments is presented in the following table.

Figure 20:
GlobalPlatform Technology Considerations

			SE		TEE	
			OS	**Trusted Applet**	**OS**	**Trusted App**
Functional Requirements	General Purpose or Special Purpose		General	Special Purpose	General	Special Purpose
	Root of Trust		Yes	Yes	Yes	Yes
	Key Management		Yes	Yes	Yes	Yes
	Application Management		Yes		Yes	
	Life Cycle and Ownership Management		Yes		Yes	
	Communication Services		Yes		Yes	
	Over the Air Updates		Yes		Yes	
	Additional Secure Services Supported		Yes		Yes	
	Standardized APIs		Yes	Yes	Yes	Yes
	Functional Certification		Yes (GP)	Multiple	Yes (GP)	Some
Implementation Requirements	Performance	Security	HW protection + Tamper resistant		Hardware protection	
		How many cores	Mono core		CPU/Multi Core	
		How much memory	Small		Large	
		How much power	Small		Flexible	
Level of Security	Protection Profile	Scope	SE PP (OS) based on HW PP		TEE PP & MCURoT PP (SW and HW boundary)	
		Security Target template	Yes		Yes	
		Attack (incl. side channel)	Catalogue is managed by SOGIS – JHAS		Catalogue is managed by GlobalPlatform	
	Robustness	VAN level	Minimum EAL4+ with AVA_VAN.5 (High attack resistance for HW and SW)		Minimum EAL2+ with AVA_VAN_AP.3 (Enhanced-basic attack resistance for HW and SW)	
	Certification		Yes (GP simplified and CC)		Yes (GP simplified and CC)	

The selection of the most appropriate solution fundamentally depends upon the context for implementation.

GlobalPlatform technologies can be used singularly or together, as most appropriate for the use cases and implementation context: for example, Secure Elements together with TEEs are more powerful than individually. In addition, automotive HSM or SHE functions can be supported as a dedicated applet for the SE or a trusted application for the TEE.

Global Platform™
Automotive Task Force

06. Additional GlobalPlatform Security Resources

In addition to supporting security management with Secure Elements and Trusted Execution Environments, GlobalPlatform has two other relevant security resources:

- Device Level Access to Secure Services with Trusted Platform Service APIs, which provides universal access to secure services to Regular Execution Environment and device applications; and
- Security Evaluation Standard for IoT Platforms: SESIP.

6.1 Device-Level Access to Secure Services

Many applications that make use of trusted services run outside the secure environment within the Regular Operating System. GlobalPlatform has developed application-level APIs to enable customers to leverage secure solutions in a way that abstracts the underlying technology (SE, TEE or non-GlobalPlatform technologies) so the normal world application (in the REE) does not need to know implementation details.

6.1.1 Trusted Platform Service APIs (Device Level)

The TPS APIs provide a single-entry point for high-level system security services, which are ***agnostic*** to the environment hosting the services. With a single API, common services can be developed for different service providers, ensuring appropriate data confidentiality, integrity, and privacy.

The TPS APIs support multiple environments, including GlobalPlatform TEE, GlobalPlatform SE, TCG TPM/ DICE (collaboration with TCG), as well as others. This flexibility fosters an easy interface point for remote service providers.

These APIs are designed to be easy to implement and to deploy. They enable trust between a device and IoT Service Provider and allow a Service Provider to:

- Determine what a device is and how it is configured;
- Provision key material to a device;
- Establish how a device should behave.

Furthermore, TPS APIs are scalable to be used from embedded Microcontrollers running an RTOS to Server Class Devices. In addition, the TPS APIs are restful, message based, discovery mechanisms.

In most implementations the TPS Service is running in a separate operating system, i.e., within a Secure Component, which exists in parallel to the Platform that runs the TPS Clients. It is important that the integration of the TPS Service alongside the Platform cannot be used to weaken the security of the Platform itself. The implementation of the TPS Service must ensure that TPS Clients cannot use the features they expose to bypass the security sandbox used by the Platform to isolate processes. In fact, TPS Services do not trust the client device inherently, but treat all devices as potentially malicious.[40]

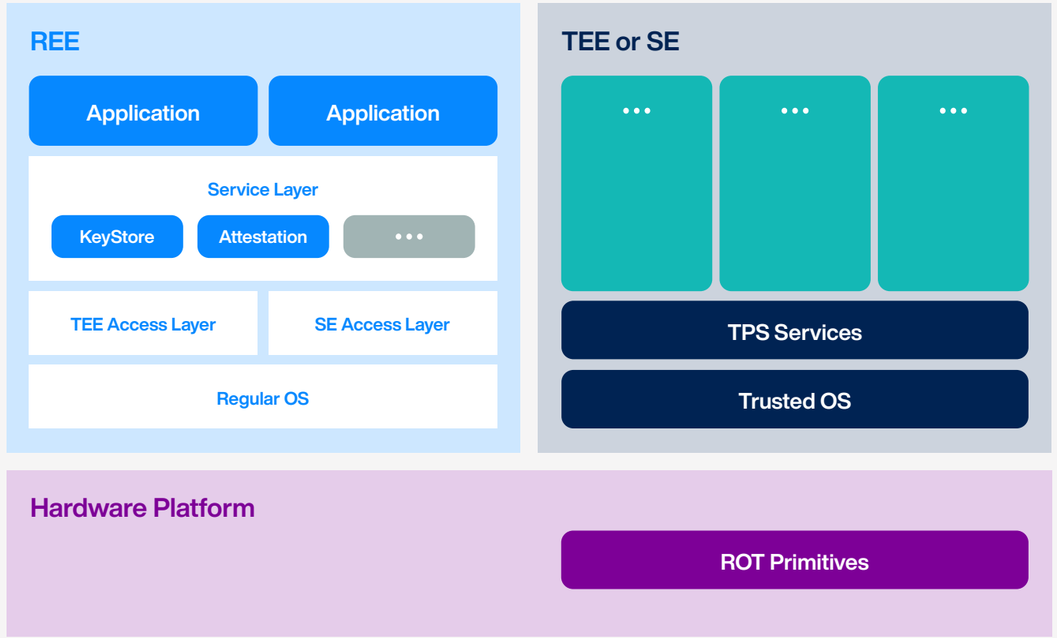
TPS APIs are certified for functional compliance (functional certification for interoperability) and for the security properties of implementation (security certification).

40 https://globalplatform.org/insight-series-trusted-platform-services-establishing-trust-between-devices-and-service-providers-2/

Figure 21:
Trusted Platform Service APIs: Easy to Implement and Easy to Deploy

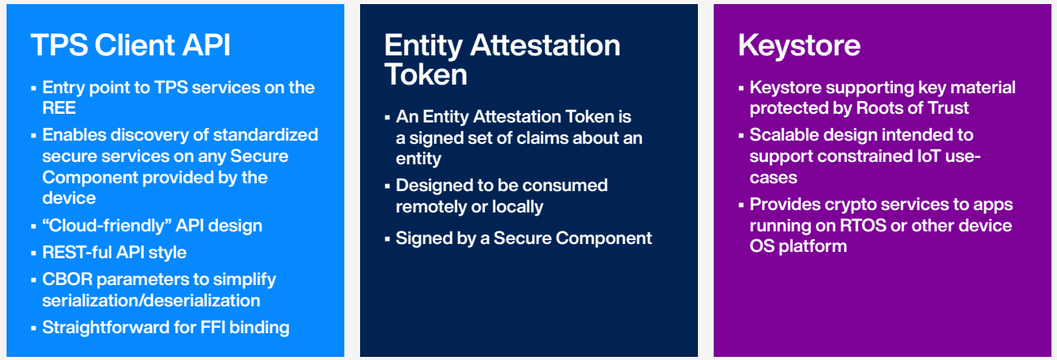
The TPS API implementation is highlighted in the following figure:

Figure 22:
Trusted Platform Service API Implementations



Currently, three APIs are to be published with additional ones planned:

Figure 23:
First TPS APIs



The specifications will be soon available on our website, as well as the Reference Implementation on GitHub:
https://github.com/GlobalPlatform/TPS-API-Reference-Implementations

6.2 Security Evaluation Standard for IoT Platforms: SESIP

6.2.1 Why SESIP?

Connected products are complex, often much more than most of the products that have had their security formally certified until today. SESIP recognizes this by providing a dedicated methodology for the Connected Platforms on which these products are based. Connected Platforms are often built by assembling several pre-existing hardware and software components; some of them include security components that protect critical assets and need to be evaluated at a high assurance level. Such components are often integrated in several Connected Platforms targeting different use cases.[41]

SESIP methodology defines ways to independently evaluate subsets of components, which may then be called platform parts, and reuse the evaluation results in any Connected Platform. SESIP importantly has been designed specifically to not require security expertise for use, to address device security, and to provide vulnerability assessment.

41 https://globalplatform.org/specs-library/security-evaluation-standard-for-iot-platforms-sesip-v1-1-gp_fst_070/

Figure 24:
SESIP Security Evaluation Methodology

6.2.2 New CEN/CENELEC Standard EN 17927

The SESIP Methodology (CEN/CENELEC Standard EN 17927), which has become a European CEN/CENELEC standard, can be used to certify a broader scope of components for connected devices; e.g., ECUs. SESIP is also useful when composing a device with already certified parts since these do not need to be reevaluated. That means that the evaluation results can simply be re-used. In the certification domain, this reuse is called composition.

SESIP is a three-party security evaluation and certification scheme.

Figure 25:
SESIP Security Evaluation and Certification Process

6.2.3 An Opportunity to Generate Artefacts for ISO/SAE 21434?

SESIP is a tool to express which security services of a product have undergone independent cybersecurity testing. Hence, it is useful for product vendors to demonstrate adherence to secure development process requirements (e.g., ISO/SAE 21434) while providing independent evidence of Cybersecurity Validation to stakeholders (e.g., customers).

Secure development process requirements (e.g., ISO/SAE 21434) apply to the entire stack of components, including the:

- MCU/MPU hardware,
- firmware,
- OS,
- application software, and
- ECU

to the entire vehicle.

For this reason, it is important that the customer receives tangible evidence, as well as the list of claims (i.e., the Security Target) and the summary verdict (i.e., the security certificate).

SESIP has already demonstrated that such tangible evidence can be easily provided in the form of a customer-shareable summary report (i.e., similar to an Evaluation Technical Report for composition), issued by the evaluating ISO 17025 accredited security laboratory. This report serves as proof of testing of the security features, in line with a defined threat model for a specific product.

6.2.4 SESIP Generated Mapping Tools for UNECE 155

SESIP also provides mapping tools to generate evidence for specific regulatory requirements. A draft mapping of SESIP for UNECE R-155 and compliance to ISO/SAE 21434 has been completed, and other schemes are ongoing.

6.2.5 SESIP Relationship to Common Criteria

SESIP is based on the Common Criteria methodology ISO/IEC 15408-3, specialized for the evaluation of Connected Platforms in the context of IoT. The Common Criteria foundation provides the formalism, while specialization for a specific set of security products allows optimization of the evaluation process.

SESIP can then be seen as a variant of the Common Criteria framework, from which it adopts many guiding principles:

- SESIP follows the main Common Criteria principles as defined in Common Criteria Part 1.
- SESIP does not use the SFR catalogue defined in Common Criteria Part 2 but keeps the concept of a catalogue of SFRs, specialized for the IoT ecosystem. Also, each SFR targets a full security purpose rather than being split into low level mechanisms to maximize genericity.
- SESIP uses the SAR catalogue as defined in Common Criteria Part 3, with some refinements of the SARs defined in Part 3 and the addition of new ones. SESIP does not use EAL packages defined in Part 3 but defines its own assurance packages adapted to the IoT ecosystem: the SESIP levels (see Annex C for additional information on SESIP levels).[42]

42 https://globalplatform.org/specs-library/security-evaluation-standard-for-iot-platforms-sesip-v1-1-gp_fst_070/

6.2.5.1 SESIP Profiles

The SESIP methodology allows the definition of security profiles generic to a type of platform (part); e.g.:

- MCU/MPU,
- cryptographic library,
- communication library, etc.

These are called SESIP Profiles and are equivalent to Common Criteria Protection Profiles: A SESIP Profile document is a generic SESIP Security Target defining the SESIP requirements in terms of security features and evaluation activities that need to be addressed during the evaluation of a platform (part) of the type targeted by the profile.[43]

6.2.5.1.1 Secure MCUs and MPUs

The MCU/MPU is the lowest level building block of an IoT Platform and therefore is intended to provide the fundamental security service layers of the platform; this includes the immutable Root of Trust (RoT). In particular, these security services enable the higher layers to:

- trust, manage, and update the state, software, and configuration of the MCU/MPU;
- control access to the device on the lowest layer;
- store assets and perform secure and cryptographic operations with them;
- attest the secure state of the device at start-up and during runtime; and
- provide different levels of isolation and protection, such that it is possible to shield different types of operations and computation.

MCUs/MPUs may also require extended security features (e.g., strong cryptography or secure communications) and/or could be operating in different environments (e.g., publicly accessible or in a private environment; open or closed to untrusted software downloads). These different use cases involve specific security features.

To allow the evaluation of these use cases, a SESIP Profile is made of a Base SESIP Profile plus Packages that can be added depending on the functionality and/or the product environment context.[44]

6.2.5.1.2 SESIP Profile for Secure External Memories: Secure Flash

A secure flash is a cost sensitive solution for creating a Root of Trust. A secure flash handles protection of:

- firmware,
- secure storage of data,
- secure authenticated firmware update,
- secure measurement and platform attestation,
- key management.

The secure storage handles the more complicated cryptographic services and APIs, to allow the combined solution to provide all the required services of a Trust Anchor. Usage of secure flash allows the firmware to be protected from unauthorized modifications and roll-back for the life of the system and is suitable for designs ranging from high-end SoC to very simple, yet critical microcontrollers (MCUs) in the car environment.[45]

43 https://globalplatform.org/specs-library/security-evaluation-standard-for-iot-platforms-sesip-v1-1-gp_fst_070/
44 https://globalplatform.org/specs-library/globalplatform-technology-sesip-profile-for-secure-mcus-and-mpus-gpt_spe_150/
45 https://globalplatform.org/specs-library/globalplatform-technology-sesip-profile-for-secure-mcus-and-mpus-gpt_spe_150/

Global Platform™
Automotive Task Force

07. Conclusions

Automotive is moving toward an increasingly software-defined approach. OEMs need flexibility with choice of suppliers – as was seen during the recent global chip shortages – and need the ability to upgrade vehicles to meet “internet speed” consumer demand for new features. Security is not immune from these needs – new applications mean new security needs, and new threats and increased connectivity mean that software solutions will themselves need to be updated. Regulators are demanding that OEMs prove their solutions meet today’s needs and will be updated to meet tomorrow’s requirements.

GlobalPlatform provides a *platform centric* approach to security that provides the necessary flexibility to allow vendors to differentiate their solutions while meeting standards for APIs and security compliance. We offer a choice of solutions that can be used together or independently and are working with automotive bodies to show how our technologies can be used to meet current and emerging standards.

Annex A: Get Involved

GlobalPlatform believes that appropriate trust management for Automotive requires cooperation across the automotive industry in order to validate use cases and identify areas where additional guidelines or specification updates could be useful to most seamlessly leverage solutions. In order to best accomplish these goals, GlobalPlatform has created official relationships, with:

- Car Connectivity Consortium
- SAE
- AUTOSAR
- Auto-ISAC

GlobalPlatform seeks to leverage these cooperations to foster a stronger alignment between automotive requirements and GlobalPlatform specifications.

A.1 Follow GlobalPlatform Specifications

GlobalPlatform specifications support interoperability and the ability to update over the air over the full life cycle of the vehicle. All GlobalPlatform specifications are free (see All GlobalPlatform Specifications: https://globalplatform.org/specs-library/). They:

- Leverage mature and interoperable specifications for secure components as the foundation for cybersecurity; and
- Rely on an externally validated certification program to ensure compliance with robustness and with desired security level.

A.2 Become a GlobalPlatform Member

GlobalPlatform is a member-driven standards organization for trusted digital services and devices. Consider becoming a member, if you are interested in:

- Obtaining early visibility of standards development as they evolve
- Shaping the development of standards directly (ensuring that they answer your requirements)
- Planning your roadmap to optimize:
  - Future proofing solutions
  - Migration roadmaps for new requirements (Post-Quantum Cryptography, security regulation)
- Learning In advance about new regulations and technologies to ascertain how they can improve your business (e.g., SBOM, vulnerability disclosure)
- Leveraging security evaluation methodologies

Annex B: Traditional Automotive Trust Anchors

Traditional automotive trust anchors are not developed by GlobalPlatform. The information in this annex has been included for disambiguation purposes only and should not be considered exhaustive in any way.

In the article by Plappert, Fuchs, and Heddergott, *Analysis and Evaluation of Hardware Trust Anchors in the Automotive Domain*, The 17th International Conference on Availability, Reliability and Security, Vienna, Austria, August 2022 (https://dl.acm.org/doi/fullHtml/10.1145/3538969.3538995), the authors address the current Automotive application of Hardware Trust Anchors:

> [Paraphrased]... Hardware Trust Anchors (HTAs) [are used] to mitigate against ... cyberattacks. The HTAs use hardware isolation mechanisms to shield security-sensitive data, e.g., cryptographic keys, and operations, e.g., signature generation, from the possibly compromised host and thus mitigate against both software and also even hardware attacks. In the automotive domain HTAs are ... increasingly used in ECUs across the whole vehicle.
>
> *Different hardware manufacturers use different names for their HTAs. For example, Infineon offers SHE+ for their first and EVITA drivers for their second generation Aurix, Renesas provides SHE/EVITA drivers for their Intelligent Cryptographic Unit (ICU) HSM, and NXP Semiconductors has with the Hardware Security Engine (HSE) an HSM compliant with SHE and EVITA .*
>
> *From this short overview, it is already clear that there is a huge variety of HTA technologies to secure automotive applications. Each of these technologies have their corresponding advantages and disadvantages with respect to different evaluation criteria. While EVITA and SHE are still the predominant HTAs used in the automotive domain, they are quite dated and may not be appropriate to secure upcoming vehicle trends.*

Figure 26:
Typical Automotive Trust Anchors[46]

Proprietary Automotive "Hardware Security Modules"

- ETAS provides an overview of HSMs in Automotive Security From The Inside Out:
  - HSMs are a form of hardware that physically encapsulates security functions. Specifically designed for IT security applications, these integrated chips typically have their own processor core, various types of memory (e. g., RAM, ROM, flash), and hardware crypto accelerators. HSMs must also meet specific standards for use in vehicles, and highly efficient integration is essential to keep costs down. Key requirements include secure interfaces between the ECU application and the HSM as well as debugging and testing interfaces for analysing malfunctions. HSMs must be able to process cryptographic information with minimal latency and exhibit adequate resistance to the typical temperatures found in automotive environments. Essentially, the HSM uses its own processor core to provide all the IT security functions required for automotive use cases. These include a 128-bit AES hardware accelerator, a true random number generator (TRNG) to generate key material, hardware-protected storage of cryptographic keys, flash and debugging functions, and the HSM's own RAM that is separate from system memory.
  - https://www.etas.com/download-center-files/DLC_realtimes/rt_2018_1_58_en.pdf

"Secure Hardware Extensions" (SHEs) specification for an on-chip extension to an automotive Microcontroller Unit (MCU)

- SHE is a specification for an on-chip extension to an automotive Microcontroller Unit (MCU) by the Hersteller Initiative Software consortium founded in 2004 by Audi, BMW, Daimler, Porsche, and Volkswagen
- Engineering Insights provides an overview of secure hardware extension (SHE):
  - is an actual on-chip extension to microcontrollers and is intended to enhance the security of the cryptographic keys in order to protect them from cyber-attacks. SHE is an alternative to highly-secure solutions like smart cards or TMP chips. SHE is a simple standard that allows for easy integration of short-and-simple authentication and encryption functions for any messages, based on 128-bit AES (Advanced Encryption Standard). If your focus is on encryption strength over ease of integration, choose an HSM (Hardware Security Module) instead of SHE. There is no standard to define an HSM, each hardware implementation is free to implement and expose any cryptographic operations they see fit.
- Engineering Insights also provides a description of how the keys are protected in SHE or HSMs:
  - In simple terms, what SHE or HSM actually does is protect the encryption keys in a cryptographic memory, while still allowing on-demand cryptographic operations using the keys. This way, the owner of the SHE or HSM hardware can operate as if they know the secret keys, while in reality keys are locked inside the security hardware and are never accessible. It is no longer possible to give the keys to someone else, except by giving them physical access to the secure hardware.

KEYFACTOR in *Automotive IoT Security for Next Gen Connected Vehicles* (2023) highlights critical challenges facing OEMs and Tier 1s regarding Trust Management:

46 https://tremend.com/blog/engineering-insights/how-to-easily-integrate-authentication-and-encryption-using-she-and-hsm/

Figure 27:
KEYFACTOR Highlights Critical Challenges Facing OEMs and Tier 1s Regarding Trust Management in Automotive

Hardware Constraints:

- Certificates and asymmetric keys are ideal, but they won't fit everywhere, so PKI strategies for connected vehicles need to include a combination of symmetric and asymmetric encryption. Part of this involves making sure manufacturers have systems that can couple asymmetric and certificate-based cryptography with more traditional symmetric cryptographic algorithms.

Massive Scalability:

- Manufacturers will need to manage hundreds of millions (if not billions) of keys, certificates, and identities across their fleets to account for everything in and around each vehicle. As a result, massive scalability is critical to ensure keys and certificates get carefully issued, managed and renewed throughout their lifespan.

Sporadic Connectivity:

- Protocols and approaches for issuing updates and communicating with vehicles must be able to handle unreliable connections and vehicles that are offline for extended periods of time. For instance, imagine being in the middle of an update as a vehicle goes through a tunnel — the system needs a way to easily recover from that situation. Or consider cases where people don't drive their cars for months at a time and therefore no communication can happen during that time period.

Key Sharing and Supply Chains:

- A big challenge in vehicle supply chains is that most Tier 1 suppliers manage cryptographic keys for several vehicle manufacturers. So a manufacturer like GM needs to be able to distribute cryptographic keys to the numerous Tier 1 suppliers that make the components for GM vehicles. But those suppliers have cryptographic keys from a variety of manufacturers because they make components not just for GM, but also manufacturers like Honda and Toyota. This means those suppliers have a very large number of keys that they need to keep separate from one another while also keeping them readily available to install on specific ECUs and firmware for each manufacturer. This situation creates significant and highly unique key management challenges for suppliers.

Source: "IoT Security for Next Gen Connected Vehicles" (2023) (https://www.keyfactor.com/education-center/automotive-iot-security/?utm_content=dsa&gad=1&gclid=Cj0KCQjw5f2lBhCkARIsAHeTvlhmZO-P6rlPB-bJrDFFv5ydtKuY0pap-nbNn43J_LkPlGg_XoZtmrAaAnyMEALw_wcB)

Annex C: SESIP Assurance Levels

SESIP has five Assurance Levels to address the wide variety of product security requirements:

- SESIP Assurance Level 1 (SESIP1) is a self-assessment-based level:
  - The developer provides a simplified Security Target, describing the security claims of his product, together with a compliance rationale why he believes these claims are met.
    - Only minimal evaluator effort is needed: The compliance rationales are checked for consistency and clarity.
    - There is no independent check by the evaluators that the platform implements the SFRs. SESIP1 provides a basic level of assurance.
- SESIP Assurance Level 2 (SESIP2) is a black-box penetration testing level:
  - The evaluation is structured around a time-limited penetration testing effort.
  - No design or source code is required to be available besides a full functional specification.
  - This is the highest level that can be applied to a closed-source platform without cooperation by the developer.
  - SESIP2 provides a moderate level of assurance.
- SESIP Assurance Level 3 (SESIP3) is a traditional white-box vulnerability analysis:
  - The evaluation is structured around a time-limited source code analysis combined with a time-limited penetration testing effort.
  - Other assurance components have only been included to support this approach to save as much effort as possible.
  - SESIP3 provides a substantial level of assurance.
- SESIP Assurance Level 4 (SESIP4) is exclusively for re-use of SOG-IS certified platforms or platform parts by licensed evaluation laboratories, allowing those platforms to utilize the mappings from SESIP to specific commercial product domains.
  - A SESIP4 evaluation must be performed as a complement to a SOG-IS certification that includes at least all the standard Common Criteria assurance components, and in particular AVA_VAN.4.
  - The current methodology simply provides guidance on how to obtain a SESIP4 certificate in addition to such a SOG-IS certificate.
- SESIP Assurance Level 5 (SESIP5) is exclusively for re-use of SOG-IS certified platforms or platform parts by licensed evaluation laboratories, allowing those platforms to utilize the mappings from SESIP to specific commercial product domains.
  - A SESIP5 evaluation must be performed as a complement to a SOG-IS certification that includes at least all the standard Common Criteria assurance components, and in particular AVA_VAN.5.
  - The current methodology simply provides guidance on how to obtain a SESIP5 certificate in addition to such a SOG-IS certificate.[47]

47 https://globalplatform.org/specs-library/security-evaluation-standard-for-iot-platforms-sesip-v1-1-gp_fst_070/

Annex D: Abbreviations

Abbreviation	Meaning
ADAS	Advanced Driver Assistance Systems
AES	Advanced Encryption Standard
AP	Attack Potential
API	Application Programming Interface
ASPICE	Automotive Software Process Improvement Capability dEtermination
Auto-ISAC	Automotive Information Sharing and Analysis Center
AUTOSAR	AUTomotive Open System ARchitecture
BSI	British Standards Institution
CB	Certification Body
CBOR	Concise Binary Object Representation (RFC 8949)
CC	Common Criteria
CCC	Car Connectivity Consortium
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
DICE	Device Identifier Composition Engine
DRM	Digital Rights Management
EAL	Evaluation Assurance Level
ECU	Electronic Control Unit
EN	European Standard
eSE	embedded Secure Element

Abbreviation	Meaning
eUICC	embedded SIM (i.e., embedded UICC)
EV	Electrical Vehicle
EVITA	E-safety Vehicle Intrusion Protected Applications
GSMA	Global System for Mobile Communications (originally Groupe Spécial Mobile)
HSM	Hardware Security Module
HTA	Hardware Trust Anchor
HW	Hardware
I2C	Inter-Integrated Circuit
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IoT	Internet of Things
IPR	Intellectual Property Rights
iSE	Integrated Secure Element
ISO	International Standards Organization
IVI	In Vehicle Infotainment
JHAS	JIL Hardware-related Attacks Subgroup
MaaS	Mobility As A Service
MCU	Microcontroller Unit
MISRA	Motor Industry Software Reliability Association
MPU	Memory Protection Unit
NHTSA	National Highway Traffic Safety Administration
NIS	Network and Information Security

Global Platform™ Automotive Task Force

Abbreviation	Meaning
NIST	National Institute of Standards and Technology, US Department of Commerce
NSA	National Security Agency
OCP	Open Compute Project
OEM	Original Equipment Manufacturer
OS	Operating System
OTA	Over-the-air
PKI	Public Key Infrastructure
PLC	Power Line Communication
PP	Protection Profile
PQC	Post-Quantum Cryptography
PTP	Penetration Test Plan
REE	Regular Execution Environment
RFC	Request for Comments
RNG	Random Number Generation
ROM	Read Only Memory
RoT	Root of Trust
RTOS	Real-Time Operating System
SAC/TC	Standardization Administration of China / Technical Committee
SAE	Society of American Engineers
SAM	Secure Application for Mobile
SAR	Security Assurance Requirements
SBOM	Software Bill of Materials

Abbreviation	Meaning
SC	Secure Components
SE	Secure Element
SESIP	Security Evaluation Standard for IoT Platforms
SFR	Security Functional Requirements
SHE	Secure Hardware Extension
SIM	Subscriber Identity Module
SoC	System On Chip
SOG-IS JHAS	Senior Officials Group - Information Systems Security
SPI	Serial Peripheral Interface
ST	Security Target
SW	Software
TA	Trusted Application
TCG	Trusted Computing Group
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TOE	Target of Evaluation
TPM	Trusted Platform Module
TPS	Trusted Platform Service
TSF	Trusted Security Foundation
UICC	Universal Integrated Circuit Card
UNECE	United Nations Economic Commission for Europe
VAC	Vehicle Access Certificate
VAN	Vulnerability Analysis

Global Platform™ Automotive Task Force

Annex E: List of Figures

Figure 1: Trends Driving Changes in Security Management in Automotive 5
Figure 2: Examples of Automotive Use Cases with Enhanced Security Requirements 6
Figure 3: Forecasted Evolution in E/E 8
Figure 4: Key GlobalPlatform Features for Automotive Security 10
Figure 5: GlobalPlatform's Principles for Common Security and Hardware Protected Environment Platform 13
Figure 6: GlobalPlatform Root of Trust Definition 14
Figure 7: Root of Trust Requirements 15
Figure 8: Using a Trust Anchor 17
Figure 9: Service Examples Built Upon the Trust Foundation 17
Figure 10: Trust Foundation Examples 18
Figure 11: Benefits of Certification 19
Figure 12: GlobalPlatform Technologies: Providing Flexibility While Supporting Innovation and Portability 21
Figure 13: Features of GlobalPlatform Secure Element 23
Figure 14: Secure Element Architecture 23
Figure 15: GlobalPlatform TEE Security Features 24
Figure 16: GlobalPlatform Trusted Execution Environment Architecture 25
Figure 17: Key Questions Driving the Selection Between Secure Components 27
Figure 18: Protection Profiles & Comparing Equivalency of Products 32
Figure 19: Comparing Secure Elements and Trusted Execution Environments 36
Figure 20: GlobalPlatform Technology Considerations 37
Figure 21: Trusted Platform Service APIs: Easy to Implement and Easy to Deploy 40
Figure 22: Trusted Platform Service API Implementations 40
Figure 23: First TPS APIs 41
Figure 24: SESIP Security Evaluation Methodology 42
Figure 25: SESIP Security Evaluation and Certification Process 42
Figure 26: Typical Automotive Trust Anchors 48
Figure 27: KEYFACTOR Highlights Critical Challenges Facing OEMs and Tier 1s Regarding Trust Management in Automotive 49

Trust for Secure Automotive Services

Global Platform™

The standard for secure digital services and devices

globalplatform.org