GLOBALPLATFORM®
THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Introduction to Secure Elements

May 2018

SECURE ELEMENTS (SE)

An introduction to SE functionality and how GlobalPlatform supports it.

THE TECHNOLOGY

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

There are different form factors of SE: embedded and integrated SEs, SIM/UICC, smart microSD as well as smart cards. SEs exist in different form factors to address the requirements of different business implementations and market needs.

THE BACKGROUND

SEs are an evolution of the traditional chip that resides in smart cards, which have been adapted to suit the needs of an increasingly digitalized world, such as smartphones, tablets, set top boxes, wearables, connected cars, and other internet of things (IoT) devices.

With multiple applications being stored and their processes executed within a single device, it is essential to be able to host trusted applications and their associated credentials in a secure environment. Examples of this include authentication, identification, signatures and PIN management, all of which are needed for different consumer services and require a protected environment to operate securely.

Digital Car Key Protection and Use Example

Users are getting accustomed to all their services being accessible from a smartphone. The tamper resistant security of the SE enables the mobile device to securely store car keys, which is essential given the very high value nature of the item. The SE uses NFC touch to securely send the key data. The smartphone application, through authentication, directs the SE to use the key to open car doors, start the car, or even temporarily share the key with another SE (used by a valet or service technician).

THE ROLE OF GLOBALPLATFORM

GlobalPlatform is a non-profit industry association driven by over 100-member companies. Members share a common goal to develop GlobalPlatform's specifications, which are today highly regarded as the international standard for enabling digital services and devices to be trusted and securely managed throughout their lifecycle.

One element of its work is the standardization and interoperability of application management within an SE. GlobalPlatform is form factor agnostic and is working to standardize all available SE technologies.

This work benefits the market as:

- Service providers and application developers can have confidence in SE application management services when developing their products.
- Manufacturers can develop once and deploy across multiple markets, reducing time to market, as well as development costs.

41% of SEs globally

GlobalPlatform conservatively estimates that 22 billion or 41% of all Secure Elements deployed globally between 2010 and 2016 were based on GlobalPlatform Specifications.[1]

[1] GlobalPlatform's estimations are based on Eurosmart's SE shipment figures for 2010-2016, published in May 2017.

FUNCTIONAL CERTIFICATION

GlobalPlatform's SE Certification Program evaluates the functional behavior of a product against the requirements outlined by GlobalPlatform SE configurations and associated specifications to achieve market interoperability. Independent testing of this nature provides confirmation that a digital service will perform as intended in the field.

- **Device manufacturers** that use GlobalPlatform certified secure components can proactively market their products as meeting the needs of digital service providers. They can effectively illustrate that their digital service management capabilities are interoperable and meet industry defined security requirements.

- **Service providers** recognize this level of assurances, which enables them to select a product which matches their security and privacy needs.

GlobalPlatform SE standards have been implemented across a wide range of markets globally, including payments, telecoms, transportation, automotive, smart cities, smart home, utilities, healthcare, premium content, government and enterprise ID.

GLOBALPLATFORM SE TECHNOLOGY

GlobalPlatform Card Specification v2.2 is a proven foundation on which many GlobalPlatform SE technical documents are developed. It defines card components, command sets, transaction sequences and interfaces. The technology also supports dynamic post-issuance card management, which facilitates the addition and modification of applications. This specification is hardware, operating system, vendor and application neutral, enabling it to be applicable to any type of deployment and industry.

In addition to this core specification, GlobalPlatform has developed a number of documents to meet the specific needs of the SE community. Highlighted below is a summary of just some of the key documents available to download.

End-to-End (E2E) Frameworks	
What	The E2E frameworks are developed for different markets from the service provider perspective. Currently available for the contactless payments market and transport community, the guidelines address simplified business models for particular ecosystems and outline exactly what is required on the SE, device, system to deploy secure mobile services that align with GlobalPlatform Specifications and Configurations.
How	The guidelines incorporate SE, mobile application and mobile messaging specifications applicable to a specific market to reduce the deployment time of secure NFC services.
Why	Document creation was driven in response to demand from markets for the development of a secure E2E infrastructure that clearly defines each actor's role within the ecosystem and specifies the exact technology specifications to be used. This means new service providers or issuers can deploy implementations faster, by using a simple and pre-customized model.

Confidential Card Content Management (Amendment A)	
What	The standardized framework enables the service provider to confidentially and independently manage their application on a GlobalPlatform compliant SE remotely, while using a third party's infrastructure.
How	The technical document explains how a SE issuer can create 'space' in the SE and then control this area. This document was created in close collaboration with GSMA and the European Telecommunications Standardisation Institute (ETSI).
Why	As more and more secure applications are loaded, personalized and managed on mobile devices to deliver convenient services to end-users, it is important that a service provider can securely manage and take responsibility for its application. This ensures that the service provider retains accountability for the sensitive information and the responsibility for managing the application.

NFC Managing Entity Specification	
What	This specification completes a 'stack' of complementary software standards from ETSI and the NFC Forum that ensures multiple mobile contactless services can successfully coexist within a device and operate as intended, regardless of the hosting environment selected by the service provider
How	The specification is backward compatible to all SEs already in the field. It supports the activation of multiple NFC services at the same time within a single device independent of the hosting environment and has the ability to detect any potential conflicts. It also details how to simplify the end-user experience when selecting NFC services for entities such as mobile wallet providers.
Why	The behavior of NFC services can be unpredictable due to a lack of implementation clarity, impacted by factors such as the model and configuration of a device. This standardized approach provides much needed clarity to service providers delivering NFC services in devices such as smartphones, and benefits OEMs developing devices that support NFC services. It ensures service delivery is not compromised by the external device environment.

Privacy Framework and Privacy-Enhanced ID Configuration	
What	These two documents combine to allow governments and identity issuers to enable state of the art privacy and security for SE based digital identity programs, like ePassports, driving licenses and eID documents. The framework and configuration bring together a range of widely deployed standards, allowing program managers to comprehensively answer to the latest global and regional privacy requirements.
How	The GlobalPlatform Privacy Framework gives implementers the tools and knowledge of 'how' regulatory privacy guidelines can be applied using GlobalPlatform's Card Specifications. It integrates a range of protocols that can be combined or applied individually. This enables ID providers to answer the new regional demand to enhance the privacy of digital identity services on ID documents while supporting current applications to aid the migration. The GlobalPlatform Privacy Enhanced ID Configuration explains how to configure SEs to implement the additional features and protocols defined in the GlobalPlatform Privacy Framework. The documents ensure digital identity services can be effectively managed, irrespective of the protocols used, and allow the addition or removal of protocols over time as requirements change.
Why	Governments, enterprises and individuals are demanding greater privacy. ID providers need to migrate from their current ID documents to align with new personal data management regulations. The combination of these documents offers a simple universal tool to enable the swift and efficient deployment of privacy-enhanced technologies, which align with the latest geographic and market sector requirements.

Open Firmware Loader for Tamper Resistant Elements (OFL)	
What	The specification standardizes how SE firmware – combining the secure operating system (OS), applications and data – can be remotely loaded and managed onto a SE after a device has been issued. This ensures that the device's longevity is no longer impacted by the lifecycle of the SE and opens up a range of new use cases like in-field OS and firmware provisioning, device refurbishment, backup / restoration of the SE and the secure transfer of a customer profile to a new device.
How	The OFL protocol enables the industry to: • Distribute generic and blank embedded hardware featuring a standardized loading mechanism. This enables firmware from various developers to be loaded, with policy enforcement, after the issuance of the device. • Distribute new firmware once the device has been issued to address additional use cases. • Mitigate the challenges of loading firmware containing diversified data into embedded hardware during manufacturing. • Use a standardized loader, shared between multiple silicon makers, allowing firmware implementers to produce loadable OSs. • Ensure forward secrecy and confidentiality between firmware makers easing compliancy with the latest data regulations (GDPR).
Why	The growth of embedded SEs is driving the development of new solutions as previously there has not been a standardized way to load the OS to an eUICC after the device has been produced. With the OFL protocol, the selection of an OS can be delayed until the device reaches its destination. This brings greater flexibility as devices are likely to have more than one owner, such as a smartphone or connected car. OFL ensures a new OS can replace an existing one and, importantly, a personalized OS and its services can be securely transferred to a new device.

Consumer Centric Model	
What	This configuration places consumers at the center of the application ecosystem without compromising device security. It achieves this by giving consumers control over which secure applications they want to use from the SE hosted within their devices. While the new model can also work in collaboration with other application management models that have been defined by GlobalPlatform. A single SE can therefore host multiple trusted applications, each of which can be managed in a range of different ways.
How	The technical document defines an end user security domain and opens up this isolated area of the SE for end user-controlled activity. This enables issuers to give end users control over value added services on their device through a PIN-protected interface module that allows them to download and maintain apps. The model focuses on a trusted token onto which applications are downloaded; a secure chip-based object, owned by the consumer, that adopts the role of a personal security container.
Why	This configuration provides a blueprint for a move away from the issuer centric model to putting the consumer in control. It encourages consumers to tailor the applications on their devices to suit their individual requirements, representing a significant change from service providers determining what consumers can have to consumers choosing the digital services they want. This configuration is of particular interest to service providers of applications such as loyalty, couponing and temporary physical access, as well as wearables and device manufacturers.

Web API for Accessing Secure Element	
What	GlobalPlatform has defined a standardized communications interface between web applications and SEs, which will enable developers of web services to build in advanced security features to protect online services against many types of attack and fraud.
How	The technical document details how sensitive data from online applications can be securely stored and processed in a SE. This API extends the highest levels of security available currently to web services, empowering online service providers to take advantage of new use cases to protect their assets and customers in a way that has not previously been possible. The document is complementary to W3C standards, with no overlap of functionality.
Why	Extending the benefits of GlobalPlatform's secure and standardized infrastructure to web services presents web app developers with advanced security options. This will help them to overcome multiple security challenges presented by the increasing connectivity of mobile devices. This is particularly relevant as the Internet of Things (IoT) leads to an unprecedented volume of connected devices and greatly increases the attack surface at risk.

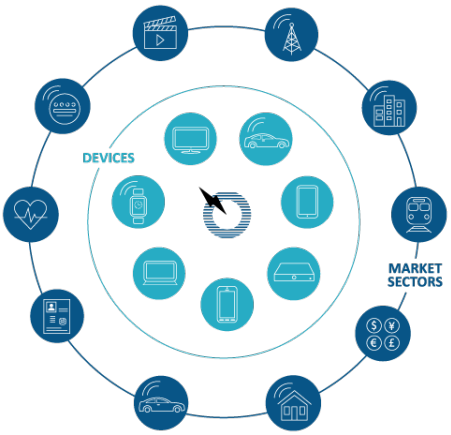
Composition Model	
What	This is a cross industry certification model for SEs with post-issuance capabilities. In essence, it outlines a methodology and streamlines the security evaluation of NFC mobile composite products by specifying how EMVCo and Common Criteria (CC) certificates can be re-used for SE platforms that have previously been certified.
How	The model specifies how: • Existing security evaluation results from EMVCo and CC can be re-used. • Security evaluation work can be limited to only test the impact of a new application and SE combination. • This modular approach streamlines evaluation requirements. Model was created in close collaboration with EMVCo and the GSMA. It is endorsed by the European Payments Council, ETSI, and SIMalliance.
Why	The industry needs ways to reduce product time to market while simultaneously advancing the security of a NFC mobile product. As SEs host multiple applications, it is important that all applications perform as intended and do not interfere with the other services being delivered. Evaluating all applications is therefore vital but this needs to be done in a manner that balances technical, commercial and security requirements. Reusing certification, and isolating certification requirements helps to reduce costs and speed up time to market.

To learn more about GlobalPlatform's Secure Element technology, educational resources and events, please visit www.globalplatform.org.

ABOUT GLOBALPLATFORM

GlobalPlatform is a non-profit industry association driven by over 100 member companies. Members share a common goal to develop GlobalPlatform's specifications, which are today highly regarded as the international standard for enabling digital services and devices to be trusted and securely managed throughout their lifecycle.

GlobalPlatform protects digital services by standardizing and certifying a security hardware/firmware combination, known as a secure component, which acts as an on-device trust anchor. This facilitates collaboration between service providers and device manufacturers, empowering them to ensure the right level of security within all devices to protect against threats.



GlobalPlatform specifications also standardize the secure management of digital services and devices once deployed in the field. Altogether, GlobalPlatform enables convenient and secure digital service delivery to end users, while supporting privacy, regardless of market sector or device type. Devices secured by GlobalPlatform include connected cars, set top boxes, smart cards, smartphones, tablets, wearables, and other Internet-of-Things (IoT) devices.

The technology's widespread global adoption delivers cost and time-to-market efficiencies to all. Market sectors adopting GlobalPlatform technology include automotive, healthcare, government and enterprise ID, payments, premium content, smart cities, smart home, telecoms, transportation, and utilities.

GlobalPlatform's legacy of successful technical specification development is thanks to two decades of energetic and effective industry collaboration. Members influence the organization's output through participation in technical committees, working groups and strategic task forces. GlobalPlatform technology is developed in collaboration with numerous standards bodies and regional organizations across the world, to ensure continual relevance and timeliness.