GLOBALPLATFORM®

THE STANDARD FOR SECURE DIGITAL SERVICES AND DEVICES

Introduction to Trusted Execution Environments

May 2018

TRUSTED EXECUTION ENVIRONMENTS (TEE)

An Introduction to TEE functionality and how GlobalPlatform supports it.

THE TECHNOLOGY

The TEE is a secure area of the main processor of a connected device that ensures sensitive data is stored, processed and protected in an isolated and trusted environment. As such, it offers protection against software attacks generated in the Rich Operating System (Rich OS).

The TEE's ability to offer safe execution of authorized security software, known as 'trusted applications' (TAs), enables it to provide end-to-end security by protecting the execution of authenticated code, confidentiality, authenticity, privacy, system integrity and data access rights. Comparative to other security environments on the device, the TEE also offers high processing speeds and a large amount of accessible memory. The primary purpose of the isolated execution environment, provided by the TEE, is to protect device and TA assets.

GlobalPlatform TEE standards achieve this by defining the below security features:

1. **Isolation from the Rich OS** – all trusted applications and their related data are separated from the rich environment.
2. **Isolation from other TAs** – TAs are isolated within the TEE, and from the TEE itself.
3. **Application management control** – any modification of the TA and the TEE can only be performed by the authenticated entity.
4. **Identification and binding** – where the boot process is bound to the System-on-Chip (SoC), enforcing authenticity and integrity of TEE firmware and TAs.
5. **Trusted storage** – TA and TEE data is stored security to ensure integrity, confidentiality and binding to the TEE (or anti-cloning).
6. **Trusted access to peripherals –** the TEE offers APIs access to trusted peripherals such as the screen, biometric sensors and SEs, under the control of the TEE.
7. **State of the art cryptography** – random number generation, cryptography and monotonic time stamps are key assets for value added services.

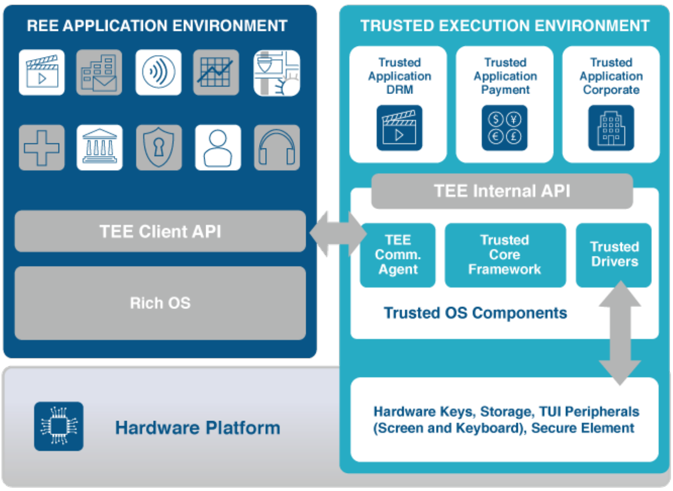
In a consumer device, TEE can also offer a Trusted User Interface mechanism (Trusted UI). This is a specific transient mode in which a mobile device is controlled by the TEE to verify that the information displayed on the device's screen comes from an approved trusted application and that information answered by the user is isolated from other applications in the device.

THE BACKGROUND

Multiple handset and chip manufacturers have already developed and deployed proprietary versions of TEE technology. The resulting lack of standardization presents application developers with a significant challenge to overcome; each proprietary TEE solution requires a different version of the same application to ensure that the application conforms to unique aspects of the technology.

In addition, if the application provider wishes to deploy to multiple TEE solution environments and have assurance that each environment will provide a common level of security, then a security assessment will need to be performed on each TEE solution. This leads to a resource intensive development process.

Architecture of the Trusted Execution Environment


REE APPLICATION ENVIRONMENT
TEE Client API
Rich OS
TRUSTED EXECUTION ENVIRONMENT
Trusted Application DRM
Trusted Application Payment
Trusted Application Corporate
TEE Internal API
TEE Comm. Agent
Trusted Core Framework
Trusted Drivers
Trusted OS Components
Hardware Platform
Hardware Keys, Storage, TUI Peripherals (Screen and Keyboard), Secure Element

Enterprise IT environments, delivery of premium multimedia content, mobile payments, the internet of things, enterprise and government identification programs and more seek to balance the need for a rich experience with security. The TEE isolates trusted applications, keeping them away from any malware in the Rich OS and separate from other apps stored in the TEE. Because of this, the TEE is becoming an essential environment within all devices as the secure services market evolves.

Payment Service Protection & Enhancement Use Case

Payment as a digital service is growing rapidly. Concerns remain, however, about security and mobile payment application vulnerability when relying on the security protections available in Rich OS environments. In addition to security, it is very important that service providers increase the convenience of mobile identity authentication. The security features of the TEE not only enable secure storage of payment credentials on devices, they also facilitate secure biometric authentication and are a platform for delivering additional features and services.

The Role of GlobalPlatform

Defining a secure baseline to protect value added digital services on connected devices.

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 a TEE to deliver flexible security that answers the unique requirements of a range of different markets and use cases.

This work benefits the market as:

- Device manufacturers can embed a standardized and certified TEE that meets the needs of service providers for the protection of digital services from fraud and attack.
- Service providers are free to focus on enhancing their offerings by using a secure component to solve security challenges. They can also develop their service just once and deploy it universally across any device with a certified TEE, with the assurance that security levels will be consistent across devices.
- Digital service users benefit from greater simplicity, convenience, security and privacy for their digital services and personal data.

GlobalPlatform conservatively estimates that there were 5 billion TEE-enabled processors worldwide within devices at the end of 2017.

Functional and Security Certification

GlobalPlatform’s work to develop and maintain a certification program promotes a collaborative and open ecosystem where digital services and devices can be trusted. Certifying secure components within devices is essential in facilitating collaboration between service providers and device manufacturers.

The certification program allows stakeholders to verify product adherence to the association’s specifications and configurations.

- **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 assurance, which enables them to select a product which matches their security and privacy needs.

Security certification confirms conformance of TEE products to the Common Criteria recognized GlobalPlatform Protection Profile, through independent security evaluation. It ensures that secure components meet the required levels of security defined for a particular service, enabling service providers to comply with industry requirements and manage risk effectively.

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

Secure Remote Management of Digital Services

The GlobalPlatform TEE Management Framework (TMF) defines standard methods to manage the life cycle of the TEE once it is active. To support the variety of usage of the TEE in today's digital world, GlobalPlatform technology defined open framework to support the management of TEEs and trusted applications in deployment models which include: one or many actors; connected or unconnected devices; and one-to-one or one-to-many devices, as well as with symmetric and asymmetric cryptography.

GlobalPlatform TEE 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 TEE Technology

GlobalPlatform members recognize the need for standards to be developed in parallel with the evolution of a new ecosystem. With many years of experience in the mobile space and the expertise of a global membership which represents the full ecosystem, GlobalPlatform published its TEE Client API in July 2010. Since then, GlobalPlatform has been responsible for driving TEE standardization on behalf of the industry. Some of the organizations key documents are highlighted below.

TEE System Architecture	
What	This document explains the hardware and software architectures behind the TEE. It introduces TEE management and explains concepts relevant to TEE functional availability in a device.
How	The document outlines different hardware and software architectures to answer to the TEE security and functional requirements.
Why	Devices, from smartphones to servers, offer a Rich Execution Environment (REE), providing a hugely extensible and versatile operating environment. This brings flexibility and capability but leaves the device vulnerable to a wide range of security threats. The TEE System Architecture therefore outlines the high-level functional and security features of a TEE to sit alongside the REE and provide a safe area of the device to protect assets and execute trusted code.

TEE APIs	
What	GlobalPlatform publishes different API specifications to define how the Rich OS can access the TEE and trusted applications. Similarly, the APIs also define how a trusted application hosted in a TEE can access the TEE's secure services.
How	The specifications include the mandatory APIs for supporting all basic tasks, in addition to extended services such as Trusted User Interface, Secure Element access, socket communications, and remote management for trusted applications.
Why	Trusted application developers need standardized APIs to access the secure services offered by a TEE. Rich OS developers also need similar APIs to access trusted applications.

TEE Management Framework	
What	The framework defines standard methods to remotely and dynamically manage TEEs. This includes data and key provisioning, security domain management, trusted application (TA) management, audit, and overall TEE management. It also presents the roles and responsibilities of the different stakeholders involved in the administration of TEEs and TAs, the life cycle of administrated entities, the mechanisms involved in administration operations, and the protocols used to perform these operations.
How	The framework enables this by defining protocols and interfaces accessed either through the GlobalPlatform TEE Client API or via extensions to the TEE Internal Core API. Both on-line and off-line actors can initiate administration operations. An off-line actor may be inside the device itself, such as a component of the Rich Execution Environment (REE), or even inside the TEE.
Why	This framework is a key part of GlobalPlatform's TEE Specification offering. It integrates the lessons learned from trusted application deployments, enabling TEE users to install, update and personalize trusted applications on a TEE, providing clear and practical direction into the management requirements of trusted applications. This standardization brings significant value to those providing trusted services on connected devices.

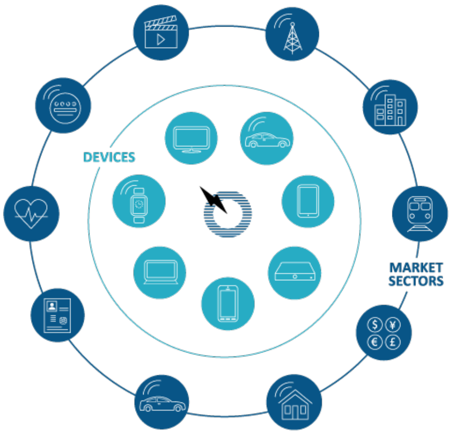
TEE Initial Configuration	
What	The document describes common implementation requirements of core features of the GlobalPlatform Device Specification. It includes refinements to features including the internal core and the client specification. It is intended primarily for the use of TEE vendors and application developers and is the basis for the development of a test suite for use in the compliance program.
How	The configuration brings together the organization's TEE Client API and Internal Core Specifications, which have been updated in response to the latest feedback from the TEE testing and compliance ecosystem's live implementations.
Why	The configuration, and its companion functional and security test suites, will enhance TEE interoperability and security and make it easier for TEE vendors to ensure compliance with GlobalPlatform's Device Specification.

TEE Protection Profile (PP)	
What	The protection profile specifies the typical threats the hardware and software of the TEE needs to withstand. It also details the security objectives that are to be met in order to counter these threats and the security functional requirements that a TEE will have to comply with. A security assurance level of EAL2+ has been selected; the focus is on vulnerabilities that are subject to widespread, software-based exploitation. The document is dedicated to all actors in the TEE value chain: TEE developers, integrators (in particular handset makers), service providers (TA developers), as well as ITSEFs, certification bodies and Common Criteria certificate consumers. In February 2015, GlobalPlatform's TEE Protection Profile was officially certified by Common Criteria.
How	It defines a core configuration with the minimum TEE security requirements and an optional module that implements full rollback protection and persistent monotonic time. With the GlobalPlatform TEE PP officially certified by Common Criteria, product vendors are now able to undertake formal security evaluation of their TEE products using laboratories licensed by supporting certification bodies to evaluate and certify that they meet the security requirements in the document.
Why	The TEE – regardless of manufacturer – must meet the requirements of a range of service providers from a variety of markets. Creating an international baseline for this technology is therefore important to bring clarity and consistency to this secure content environment and enable service providers to effectively manage risk. The protection profile and certification program are part of GlobalPlatform's work to accelerate the deployment of certified TEEs and to create an ecosystem in which GlobalPlatform certification is a prerequisite amongst service providers and handset manufacturers. This is a stepping stone on the way to achieving full market adoption, with the long-term goal of the specifications becoming a de facto standard for the industry.

To learn more about GlobalPlatform's Trusted Execution Environments 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.