# New Standardization Trends at GlobalPlatform—Secure Components for the IoT Era

*Eikazu Niwano*

**Abstract**

GlobalPlatform, which was founded as an international standardization organization targeting smart cards, has expanded its scope of standardization to include a variety of Secure Elements, Trusted Execution Environments, and devices. Furthermore, in the light of current trends surrounding the Internet of Things (IoT) and ecosystems, GlobalPlatform is broadening the functions it provides from application management to device trust management. This article introduces new initiatives toward the IoT and ecosystem era at GlobalPlatform, which has recently restructured its organization.

*Keywords: IoT security, tamper resistant module, secure chip*

## 1. GlobalPlatform

Smart cards have elements similar to those of a computer such as a CPU (central processing unit) and memory and are secure components with hardware characteristics robust to external attacks, making them tamper resistant. They can be used for security processes and safe data management as in user authentication and data encryption.

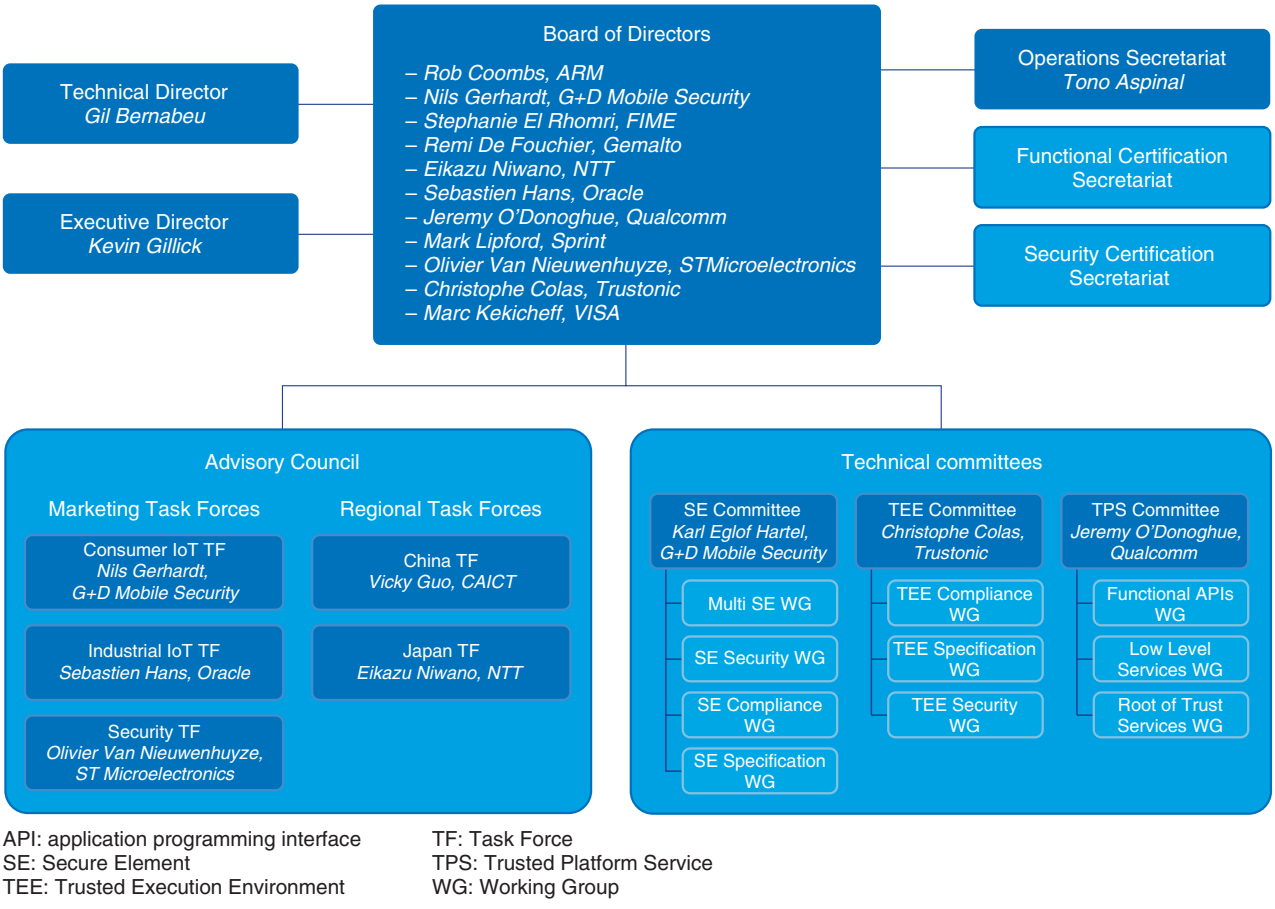
Smart cards are presently being used in many fields including payment systems (smart credit cards etc.), communications (subscriber identity module (SIM) cards), transportation (Suica train/bus cards etc.), workplace/access management (employee identification (ID) cards), and public services (electronic passports, My Number (social security and tax number) cards, etc.).

GlobalPlatform [1] was founded in 1999 as an international standardization organization targeting the management of application programs embedded within smart cards (**Fig. 1**). It is the world's leading industry standardization organization in the field of secure components that enable remote and secure loading/managing of applications in smart cards via collaboration between smart card issuers and service providers after smart card issuance [2].

Since its founding, GlobalPlatform has expanded the range of secure components targeted for standardization from smart cards to various types of Secure Elements (SEs) [3], including embedded SIMs (eSIMs), and to Trusted Execution Environments (TEEs) [4] within a device independent of the device operating system (OS). Of particular importance here is that GlobalPlatform is now extending its target of management as far as the device level. In addition, its scope of standardization continues to expand to include the updating of SE firmware and the creation of an SE/TEE certification program.

Consequently, in addition to contributions from traditional SE-related operators such as chip and card manufacturers for smart card systems as well as telecom operators and others, proactive contributions from mobile-device chip manufacturers such as ARM and mobile-device-related operators such as Apple, Samsung, and Qualcomm in recent years have become an important trend. At present, about 100 companies from around the world are participating in GlobalPlatform as stakeholders.

Meanwhile, a wide variety and massive number of low-to-high-end Internet of Things (IoT) devices are coming to be dynamically added, connected, coordinated, and controlled in ever-expanding IoT environments




API: application programming interface
SE: Secure Element
TEE: Trusted Execution Environment
TF: Task Force
TPS: Trusted Platform Service
WG: Working Group

Fig. 1. GlobalPlatform organizational structure.

that drive the formation of ecosystems.

With the appearance of such complex and dynamic environments, much evidence and many incidents in relation to cyber-attacks are starting to be reported, revealing the vulnerability of IoT devices. These include the hijacking of a connected car and the malicious manipulation of its steering wheel, unauthorized operation of medical equipment, and DDoS (distributed denial of service) attacks using home digital cameras as a springboard.

Consequently, much attention is being focused on how to guarantee device trustworthiness as a critical issue, such as in determining the authenticity of the huge variety of interconnected IoT devices.

Against this background, GlobalPlatform seeks to enable a wide range of device manufacturers and digital service providers to collaborate in performing highly reliable and secure device management, and to this end, it is working to expand the role of secure components from user authentication to device authentication.

Studies have therefore begun on IoT/device authentication at the requirements level, and in conjunction with the first reorganization of technical committees since the founding of GlobalPlatform in 1999, the Trusted Platform Services (TPS) Committee has been established to decide on technical specifications for device authentication.

## 2. Advisory Council

GlobalPlatform has established an Advisory Council as a forum for discussing requirements before formulating technical specifications. At present, the Advisory Council consists of market and regional task forces.

There are three market task forces: Consumer IoT, Industrial IoT, and Security. These task forces hold discussions on issues respectively concerning the consumer IoT field such as wearable devices, the

industrial IoT field such as Industry 4.0, and Root of Trust (RoT), Chain of Trust, and support for the latest encryption schemes (diverse and advanced encryption schemes, lightweight encryption schemes for specific devices, etc.).

The regional task forces, meanwhile, are established considering where GlobalPlatform members are based. The regional task forces share GlobalPlatform information and regional circumstances, study regional conditions and deployment issues, and hold discussions on region-originating technology. At present, there are two regional task forces: China and Japan.

## 3. Technical committees

The GlobalPlatform bodies that decide on technical specifications are the technical committees. Some name changes of these committees have occurred in order to reflect the state of study concerning secure components, which continue to expand from smart cards. The Card Committee is now the SE Committee, and the Device Committee is now the TEE Committee. Additionally, as mentioned above, the most noteworthy change here is the establishment of the TPS Committee to study the trustworthiness of devices. Here, the study theme is the trustworthiness of devices that use secure components.

Through these committees, GlobalPlatform aims to facilitate collaboration between device manufacturers and digital service providers and provide secure digital services regardless of the market sector or device type. To this end, it has technologies for authentication, connectivity, privacy, and security that enable it to provide the following services:

(1) Protection of digital services
(2) Secure remote management of digital services
(3) Certification of secure components

## 4. Protection of digital services

Protection of digital services implements GlobalPlatform's technology designed to protect digital services and assets that use secure components. It provides protection of digital assets (credentials such as fingerprints and authentication/encryption keys) and associated security services (authentication etc.).

This protection is achieved by standardizing two types of secure component technologies—SE and TEE—supporting diverse market needs, as described below.

### 4.1 SE

This is a secure element consisting of tamper-resistant hardware such as a smart card. It includes smart cards and USB (universal serial bus) tokens that link with a terminal from the outside through a reader or writer. Another type of SE includes SIM, smartSD (Secure Digital memory card), and embedded SEs (eSIM, embedded universal integrated circuit cards (eUICCs), etc.) used inside mobile devices, as well as integrated SE (iSE) integrated with a SoC (system on chip).

Standardization of access to multiple SEs within a mobile device is also progressing. Here, an Open Mobile API (OMAPI) is being specified as an application programming interface (API) for accessing an SE from a mobile application. Furthermore, given that mobile devices support proximity communication technology called near-field communication (NFC)[*1], GlobalPlatform is also engaged in joint studies with the NFC Forum and the European Telecommunications Standards Institute (ETSI) on Host Card Emulation as an emulation environment targeting mobile-device cards that use NFC and on Contactless Card Emulation Environments as a mechanism for accessing various types of SEs. Studies are also progressing on the updating of SE firmware and specifically on a mechanism called Virtual Primary Platform as a new study item that separates the iSE OS into upper and lower sections as requested by the GSM Association (GSMA)[*2].

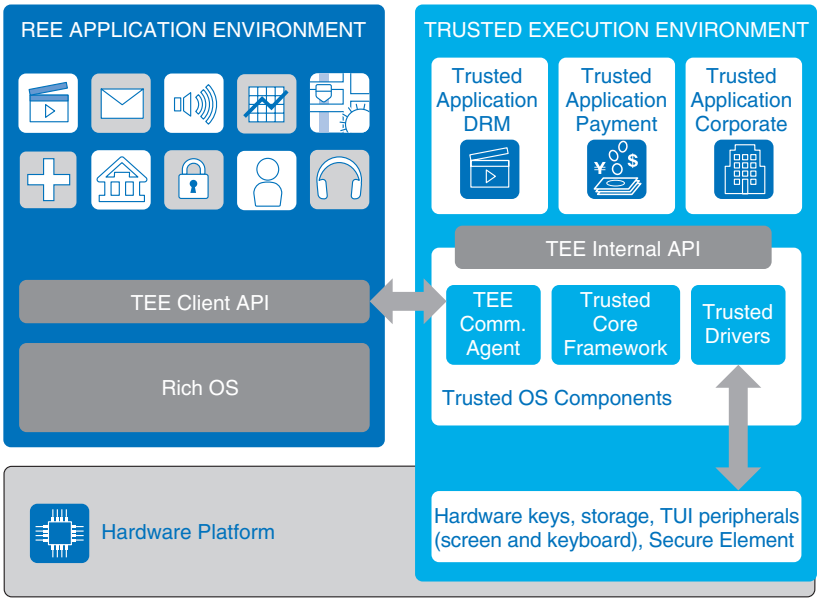
At present, about 22 billion GlobalPlatform-conforming SEs have been deployed (41% of the SE market). It is noteworthy in relation to IoT that GSMA has released remote provisioning specifications for eUICCs that use GlobalPlatform technologies, and that the automobile industry is adopting this mechanism.

### 4.2 TEE

In addition to tamper-resistant hardware such as SEs, GlobalPlatform is also moving forward with the standardization of TEEs (**Fig. 2**) to provide a secure execution environment independent of the existing OS in devices such as mobile phones and to guarantee a level of security higher than that of the device OS.

*1 NFC: A wireless communications standard that includes existing contactless smart card communication standards. It enables the use of a contactless smart card function, reader/writer function, and inter-device (peer-to-peer) communication function.

*2 GSMA: An industry group made up of mobile communications operators and related companies that have adopted the GSM mobile phone system.




Source: GlobalPlatform

DRM: digital rights management
REE: Rich Execution Environment
TUI: trusted user interface

Fig. 2. TEE architecture.

A TEE executes only authorized software known as *trusted applications* and guarantees end-to-end security such as the protection of privacy and data access rights.

A TEE includes interfaces with applications, the device OS, and SEs and provides a trusted user interface (TUI) environment to prevent a man-in-the-browser attack.

At present, TEEs are being used for applications requiring a high level of security such as biometric authentications, digital rights management (DRM) for video content, and payments. The TEE secure component has been mentioned, for example, in IoT Security Guidelines ver. 1.0 [5], specified by the IoT Acceleration Consortium,[*3] which reflects its ongoing deployment.

### 4.3 Four features of digital services protection

The following describes four features provided by the SE and TEE secure components to protect digital services and resources (**Fig. 3**).

The first feature is the provision of a secure execution environment isolated from the device OS by managing the RoT within the secure component.

The second feature is end-to-end secure execution of application management within the secure component through multi-actors (device manufacturers, digital service providers, etc.). Here, SE firmware is also targeted as a managed resource.

The third feature is the ability to add and provide security services common to multiple market sectors on the same secure component in a flexible manner.

Finally, the fourth feature is the ability of multiple digital service providers to respectively manage an isolated and independent area on the same secure component.

## 5. Secure remote management of digital services

Another GlobalPlatform technology is remote management. In an IoT environment, IoT devices including sensors are installed in all sorts of places, so on-site management of these devices over the long term is hardly realistic. A remote management function is extremely important under these circumstances.

*3 IoT Acceleration Consortium: A body established in Japan for the purpose of constructing a system for developing and demonstrating IoT technologies and creating new business models through the participation and collaboration of government, industry, and academia.

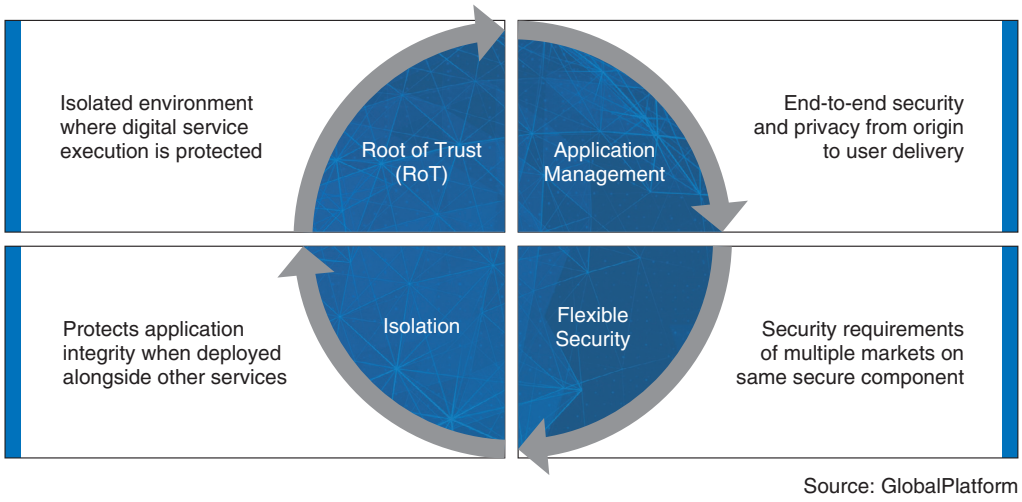



Fig. 3. Four features of digital services protection.

This technology enables secure end-to-end, remote management of SEs such as eSIMs embedded in IoT devices.

## 6. Certification (authentication) of secure components

GlobalPlatform provides a program for performing functional certification of SE/TEE products and security certification of TEE products. In this regard, GlobalPlatform has begun to collaborate with the FIDO Alliance,[*4] an organization that promotes the standardization of multi-factor authentication including biometric authentication. Discussions have begun on how to configure and manage FIDO applications (keys, applications) in an internal device environment including secure components and on the necessity of security certification in relation to this configuration.

Furthermore, in relation to cybersecurity and the problem of supply chains for parts in ever-growing ecosystems, lively discussions are taking place in various organizations around the world on the importance of having a certification mechanism that includes hardware. This certification program is expected to become increasingly important in conjunction with security-by-design principles as the IoT/ecosystem era arrives.

## 7. Device protection—Device Trust Architecture

This section focuses on device protection as the latest initiative taken up by GlobalPlatform. It is an extremely important key to achieving cybersecurity considering the future expansion of IoT and ecosystem environments.

Device protection is a mechanism related to device trustworthiness, including the authentication of device authenticity. Technical specifications for device protection will be specified by the TPS Committee.

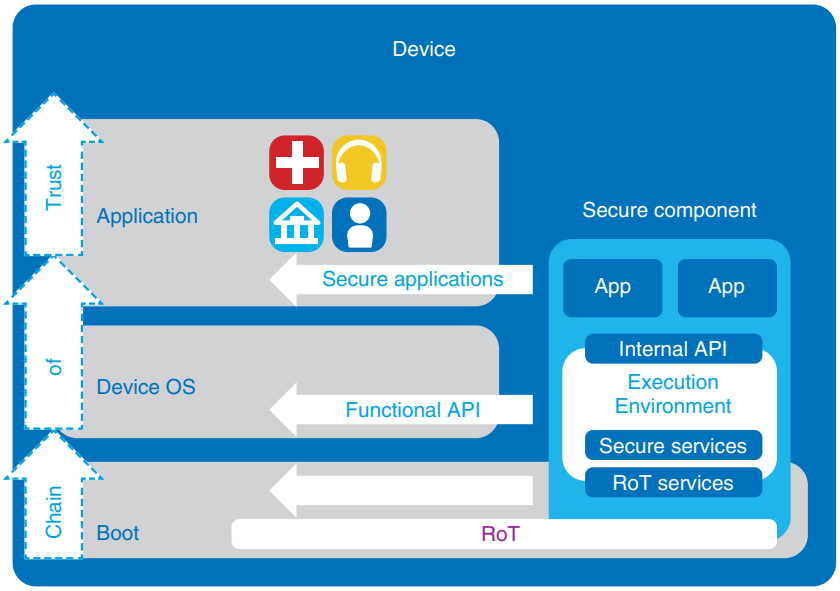
In relation to device protection, the Trusted Computing Group (TCG)[*5] has been standardizing solutions using the Trusted Platform Module (TPM) for some time as part of trusted computing, but GlobalPlatform seeks to develop IoT devices as a general-purpose mechanism using secure components.

As stated above, a key feature of secure components is that they enable device manufacturers and digital service providers to remotely add or update a variety of applications including security functions (and firmware in the case of SEs) regardless of the market sector or device type. Using secure components in this way enables the provision of services such as device RoT, chain of trust, and remote device identification and attestation, which, in turn, enables trustworthy, safe, and flexible device management in a multi-actor environment [6].

This device protection mechanism is called Device Trust Architecture (DTA) [7]. The plan is to promote studies of DTA as architecture integrated with secure

*4 FIDO Alliance: A standardization organization targeting multi-factor authentication including biometric authentication.

*5 TCG: An organization promoting the study of TPM having a secure boot function.




Source: GlobalPlatform

Fig. 4. Device Trust Architecture.

components for protecting digital services (**Fig. 4**).

## 8. Future outlook—Toward the IoT era

A major strength of GlobalPlatform is its collaboration with many standardization organizations. In addition to standardization organizations targeting conventional fields such as smart cards, finance, and communications, it has recently initiated collaboration with GSMA/OneM2M[*6] in the IoT field and the Car Connectivity Consortium (CCC)[*7] in the automotive field. Furthermore, in relation to other types of tamper-resistant hardware, studies are beginning on a mechanism for generalizing secure boots such as RoT and chain of trust in collaboration with TCG to assure device trustworthiness, and work is beginning on defining the relationship of secure components with the Hardware Security Module used for key management and encryption processing in server systems.

With the coming of the IoT/ecosystem era, the trend toward collaboration must be promoted even further. In the IoT security field, however, needs differ according to industry and region due to differences in systems and cultural backgrounds, so it will become increasingly important to analyze the needs and use cases of individual industries and regions and to form tie-ups with standardization organizations in each of those industries and regions. From here on, standardization and certification through cross-sector × cross-region efforts as in the case of smart city initiatives will be essential. Collaboration with other organizations related to tamper-resistant hardware according to such industry/regional characteristics will also be important.

Furthermore, in terms of technology, given an environment that dynamically and dispersedly connects such an array of stakeholders (developers, operators, service providers, users) and various types of devices and systems (and their constituent elements), research and development and standardization will be required for an ID component that manages ID/entity information. Key themes will be how to structure and arrange an ID component using a secure component, how to manage and certify authenticity/trustworthiness of ID components, and what mechanism to use to evaluate and authenticate ID components.

Finally, NTT to date has made contributions to the management of secure components using the public key infrastructure scheme. Going forward, we plan to make further contributions to the IoT security and cybersecurity fields through the application of such

*6 OneM2M: A joint project and standardization organization formed to promote the standardization of IoT platforms.

*7 CCC: An industry group working on the standardization of in-vehicle smartphone connections.

distributed security technologies.

## References


[1] Website of GlobalPlatform, https://globalplatform.org/
[2] E. Niwano and H. Goromaru, "Standardization Trends at GlobalPlatform," NTT Technical Review, Vol. 4, No. 11, pp. 48–52, 2006. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200611048.pdf
[3] GlobalPlatform, "Introduction to Secure Elements," May 2018.
[4] GlobalPlatform, "Introduction to Trusted Execution Environments," May 2018.
[5] IoT Acceleration Consortium, Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry, "IoT Security Guidelines ver. 1.0," 2016.
[6] GlobalPlatform, "Deploying and Protecting Digital Services with Chains of Trust," May 2018.
[7] GlobalPlatform, "Introduction to Device Trust Architecture," July 2018.



**Eikazu Niwano**

NTT Research Professor, NTT Secure Platform Laboratories.

He received a B.S. and M.S. in mathematics from Waseda University, Tokyo, in 1987 and 1989. He joined NTT in 1989 and has studied distributed system architecture including mobile (messaging)/agent/ubiquitous systems, secure chips, and social information platforms with information security. During 2002–2005, he was the general manager of the European office of the NTT laboratories in Paris, and during 2008–2017 he served as producer at the Research and Development Planning Department of NTT. He is currently studying and planning strategies for IoT security, with a focus on secure components.

He received the Information and Communication Technology Award (the Minister of Internal Affairs and Communications Award) from The Telecommunication Committee in Japan in 2018. He is a member of the board of directors and chairman of the Japan Task Force in GlobalPlatform. He is also a Fellow and member of the board of directors of the Next Generation Ic Card System Study group (NICSS) in Japan. He is a member of the Institute of Electrical and Electronics Engineers (IEEE), the Institute of Electronics, Information and Communication Engineers (IEICE), and the Information Processing Society of Japan (IPSJ).