Recent Trends in GlobalPlatform: Digital Trust – Evaluation & Certification, Trusted Execution Environment, and Digital Identity –

Eikazu Niwano, Akira Nagai, and Fumiaki Kudoh

Abstract

In addition to Internet-of-Things security, such as zero trust and supply chain issues, the environment surrounding secure components is rapidly changing due to advances in digital trust technologies such as confidential computing and digital identity. This article introduces the standardization trends in GlobalPlatform in response to these latest changes in the security environment.

Keywords: Secure Element, Trusted Execution Environment, trust

1. What is GlobalPlatform?

A smart card is a type of computer that has strong resistance to external attacks, which is called tamper-resistance. In the late 1990s, in response to the growing need for multipurpose use of smart cards, particularly in the public sector, technology was developed to remotely operate and manage multiple applications after issuance of smart cards. Standardization has since progressed in line with the era of mobile and Internet of Things (IoT).

GlobalPlatform (GP) [1] is a leading standards organization in the operation and management of multi-application smart cards since its establishment in 1999 [2]. GP specifies the following four technical standards (**Figs. 1** and **2**).

Firstly, the most representative technology of GP is Secure Element (SE), which is implemented in smart cards. Embedded subscriber identity modules (eSIMs), which can change the operator after it is issued, and integrated SIMs (iSIMs), which are integrated into system on chips (SoCs), low in cost, and used for secure boot, are emerging and diversifying.

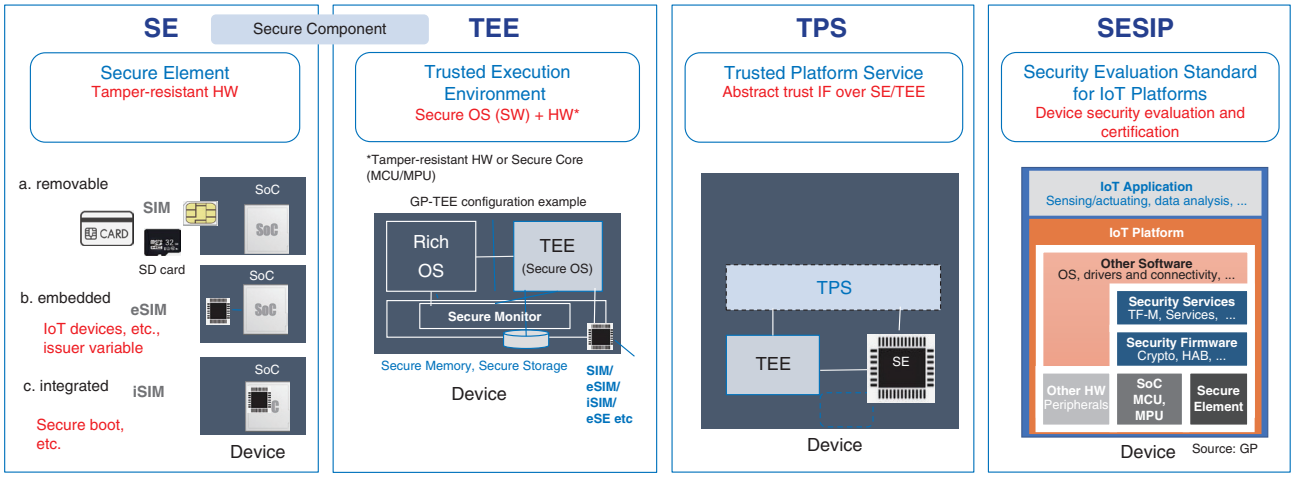
Secondly, GP standardizes a secure operating system (OS) technology called Trusted Execution Environment (TEE), which is installed in a device along with a normal device OS such as Android. This standard is widely used mainly in consumer devices such as mobile phones, Internet protocol televisions, wearable devices, and automotive onboard equipment software. GP has begun studying RISC-V[*1] support and a scheme for installing multiple TEEs on a hypervisor.

Thirdly, GP has started to standardize the Trusted Platform Service (TPS), which is provided with trust-related services such as a remote attestation[*2], as a higher-level interface to the two traditional secure components SE and TEE [3].

Finally, the Security Evaluation Standard for IoT Platforms (SESIP), an evaluation and certification

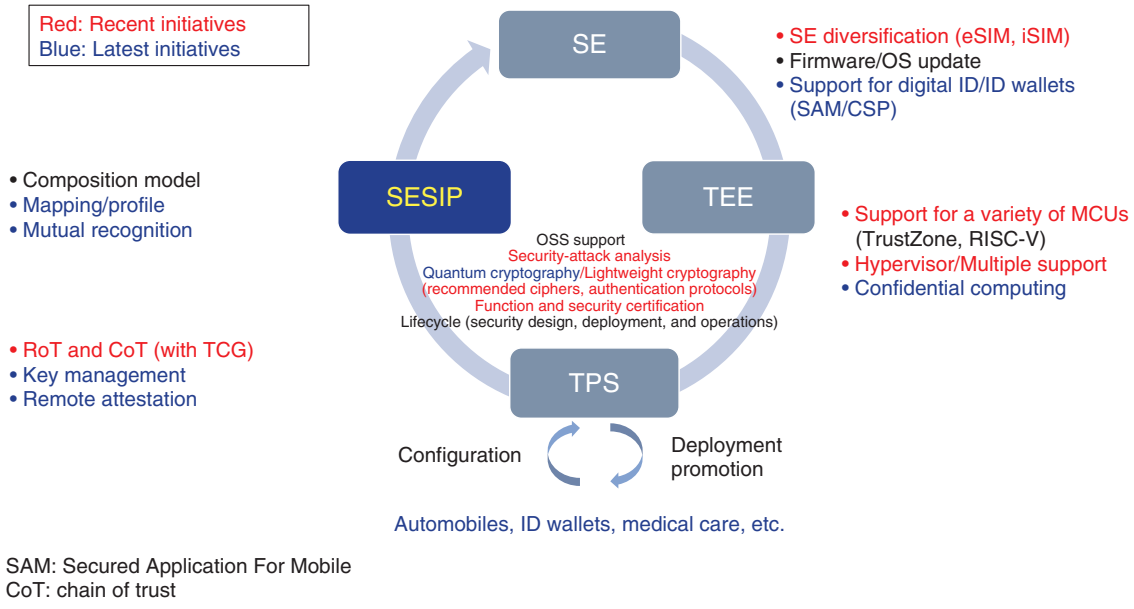
*1 RISC-V: An open-source instruction set architecture based on the reduced instruction set computer (RISC) concept.

*2 Remote attestation: A mechanism for remotely proving and verifying the authenticity of the configuration of device resources. A number of organizations, including the IETF, have made progress in studying the issue.



HAB: high availability boot
HW: hardware
HSM: hardware security module
MCU: microcontroller unit
MPU: memory protection unit
SD card: secure digital card
SW: software
TF-M: TrustedFirmware-M

Fig. 1. GP technologies.



SAM: Secured Application For Mobile
CoT: chain of trust

Fig. 2. Advances in GP technologies.

scheme for device security, is currently being promoted.

As a common approach, open source software (OSS) support and recommended cipher lists have been established, and post-quantum cryptography (PQC) has been studied (Fig. 2). The technology to be standardized by GP continues to expand from the secure component to the device level, and GP is currently developing into a standardization organization for secure devices and services.

2. Changes in GP circumstances and GP technology

The environment surrounding secure components and secure devices has changed greatly along with the expansion of these technologies. Given the increasing number of cybersecurity attacks, especially in the IoT field, there is an urgent need to address device-security issues such as zero trust and supply chain. As data consolidation advances, technologies related to data protection and privacy protection are advancing, and new data-security technologies, such as confidential computing and privacy-enhancing technologies (PETs)[*3], are emerging.

In the user-security field, the need for mutual use of digital identities (IDs) in the public sector is increasing, mainly in Europe, and the examination and standardization of ID wallets that enable the unified management and use of various digital IDs in a wide area are rapidly advancing. Therefore, GP is making progress as discussed in the following sections.

2.1 Zero trust—Root of trust

In response to the complexity of the IoT environment, which is increasingly becoming an ecosystem, zero trust is an approach and architecture that assures security on a per-asset basis, such as devices, software, and IDs, rather than the traditional borderline security that protects against attacks at the border. A key issue for ensuring the trust of a device is how to configure the root of trust (RoT)[*4] [3]. Secure components are becoming an increasingly important technology for this purpose.

To promote RoT study, GP is strengthening cooperation with the Trusted Computing Group (TCG), which promotes the Trusted Platform Module (TPM), an SE that is installed in personal computers for the purpose of secure boot, and is developing an RoT framework. As a mechanism to guarantee the authenticity of devices by using RoT, GP is also urgently standardizing key management and stipulating the aforementioned remote attestation service [3].

In response to this situation, the IoT/machine-to-machine (M2M) standards organization OneM2M specified the application of this secure component in the standards TS0003/TS0016, which were recently officially ratified by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) Study Group 20 (Smart Cities). The application of secure components will progress in various IoT fields.

2.2 Supply-chain issues—Evaluation and certification of device security

As the arrival and distribution of IoT products across national borders is expanding, countermeasures against supply-chain issues to avoid the introduction of vulnerabilities are being rapidly promoted, particularly in Europe and the United States.

In Europe, since the enactment of the NIS Directive on cybersecurity for networks and information systems in 2016, the Cybersecurity Act as a cybersecurity-certification scheme, the Cyber Resilience Act requiring submission of the software bill of materials (SBOM)[*5] for digital products and conformity assessment, and the European Union Cybersecurity Certification Scheme on Common Criteria (EUCC) were drafted. The European Telecommunications Standards Institute (ETSI) has defined TS 103 645, and the National Institute of Standards and Technology (NIST) has defined IR 8259 A in relation to the evaluation and certification for IoT/consumer devices. ETSI also established the TS 103 732 security requirement for mobile devices, and the Global System for Mobile Communications Association (GSMA) has been following suit.

In these circumstances, GP has established SESIP, an evaluation and authentication scheme for device security, and is working with the above organizations to map these guidelines. SESIP has been fully adopted by the European Committee for Standardization (CEN)/European Committee for Electrotechnical Standardization (CENELEC), the official European standardization committees, and was published as the European standard EN17927 in November 2023.

In Japan, ECSEC Laboratory[*6] [4] has been certified as an SESIP evaluation body, and products of Renesas obtained SESIP certifications. GP has concluded a memorandum of understanding (basic agreement) with the Connected Consumer Device Security Council (CCDS)[*7] in relation to secure

*3 Confidential computing and PETs: Both involve data protection. The Confidential Computing Consortium is considering the former on the basis of TEE. The latter uses TEE as a method to enable secure computation.

*4 RoT: Defined by NIST and other organizations to ensure device trust.

*5 SBOM: A mechanism to guarantee the configuration of software components. SBOM has been attracting attention since the issuance of the US Executive Order 14028.

*6 ECSEC Laboratory: A national evaluation organization and accredited as an evaluation body for SESIP in 2023.

*7 CCDS: A review organization of the security of domestic consumer devices and is active in more than 200 companies. It provides IoT security guidelines and IoT device authentication programs.

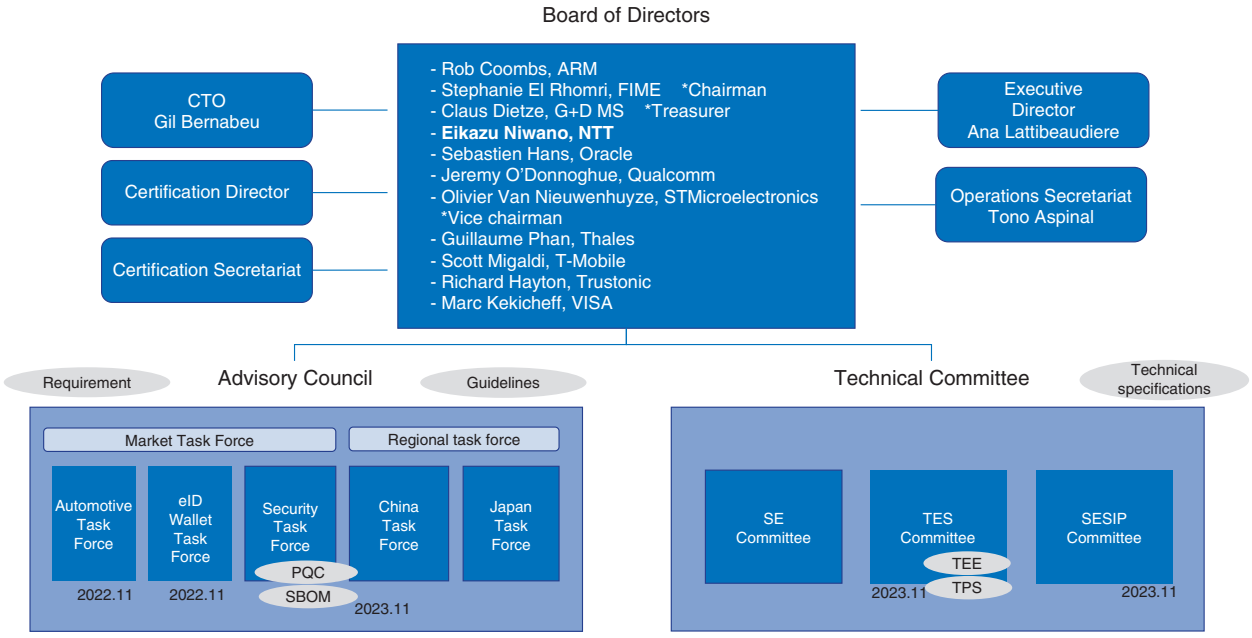


Fig. 3. GP organizations.

components and certification program. Other activities have started in the area of automotive.

To accelerate this standardization work and development, GP established a technical committee dedicated to promoting SESIP study in November 2023 (**Fig. 3**). To promote SBOM, which is important in addition to evaluation and certification, a subordinate organization related to SBOM was established and has moved under the Security Task Force (Fig. 3).

2.3 Confidential computing/PETs—TEE

Confidential computing, which is defined and discussed by the Confidential Computing Consortium, is a technology for data encryption and protection while using TEE as a base technology. There are many discussions on the use of TEE as one of the ways to achieve secure computing (security technology that enables computation while keeping data secret), which is one of the methods of PETs.

To respond to such needs, the TEE Committee and TPS Committee, which were previously independent committees within GP, were integrated and the Trusted Environment and Services (TES) Committee was established in November 2023. We expect to see progress in standardization related to confidential computing.

2.4 ID wallet—Digital ID

The European Digital Identity Wallet (EUDIW) is being aggressively promoted in Europe as a measure to enhance the utilization and sophistication of eIDAS (Electronic Identification, Authentication and Trust Services), a European public ID measure that has been implemented in Europe, and to enhance interoperability across Europe. This enables the presentation and use of various public IDs, credentials, and certificates owned by individuals in Europe.

In response, GP is working to standardize how to configure ID wallets in SE and the cryptographic service provider (CSP) technology that can be used not only for cryptographic services but also for certification of digital ID applications. The Secure Identity Alliance (SIA), an organization that promotes standardization related to the wide-area operation of digital IDs, has also started cooperation related to the technology Open Standard Identity APIs (OSIA), and it is expected that cooperation and standardization with organizations related to ID management will progress as a new area of GP. GP established the eID Wallet Task Force in November 2022 to promote this activity (Fig. 3).

3. Acceleration of market expansion—Automotive

In response to these changes in the security environment, GP is working to identify promising industries and markets and promote the diffusion of its technologies into these markets. The most promising market is the automotive market in which cybersecurity guidelines are currently being standardized by leading standards bodies. There are UN-R155/UN-R156 stipulated by the United Nations Economic Commission for Europe (UNECE), ISO/SAE 21434 stipulated by International Organization for Standardization (ISO) and the Society of Automotive Engineers (SAE) in the United States, and SAE J3101 (Hardware Protected Security for Ground Vehicles), a guideline related to secure components. GP established the Automotive Task Force in November 2022 (Fig. 3), started cooperation with the Automotive Open System Architecture (AUTOSAR), SAE, and Automotive Information Sharing and Analysis Center (AUTO-ISAC), which are global automotive organizations, and started joint work on mapping SESIP with SAE J3101.

4. Future issues and prospects

The standardization of secure components, which started with smart cards, is rapidly expanding. This is in response to recent changes in various information technology environments. It will become more important to pursue mutual use and operation with related standards to promote global interoperability. Therefore, it is necessary to cooperate with TCG for the integrated use of various SEs, standardize inter-TEE connections in a distributed environment, develop a global mutual recognition scheme for evaluation and certification technology, support further digital ID technologies such as decentralized identity (DID)[*8] and self-sovereign identity (SSI)[*8], verifiable credential (VC)[*8] that can be verified online, and blockchain technology, and cooperate with related standardization organizations such as the Internet Engineering Task Force (IETF).

NTT has participated in GP activities since the establishment of GP and has proposed a system for managing SEs based on public key infrastructure, which is now being developed in various fields including eSIM/IoT. In addition to these technical contributions, significant organizational contributions have been made, including serving as a long-time board member, establishing a regional organization scheme in GP, and leading domestic activities as a representative of the Japan Task Force.

In 2023, in recognition of such long-standing efforts, Eikazu Niwano (the first author) became the second person in the world to receive the Kekicheff Award (the first in the world after Marc Kekicheff, from whom the award is derived). This is awarded to a person who creates outstanding long-term and continuous achievements in GP.

NTT is currently promoting the Innovative Optical and Wireless Network (IOWN) initiative, which is based on photonics-electronics convergence technology, and the IOWN Global Forum, an organization that promotes this initiative. On the basis of the results of these activities, NTT hopes to continue to contribute to the development of this field and industry by disseminating and contributing technologies from Japan, promoting cooperation between GP and domestic organizations, and contributing to the creation of a global environment for mutual use through domestic feedback on GP 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] E. Niwano, "New Standardization Trends at GlobalPlatform—Secure Components for the IoT Era," NTT Technical Review, Vol. 17, No. 2, pp. 63–69, 2019. https://doi.org/10.53829/ntr201902gls
[4] ECSEC Laboratory, IoT Evaluation (in Japanese), https://www.ecsec.jp/publics/index/42/

*8 DID/SSI/VC: These are core technologies of digital ID technology, and discussion has been progressing with IETF.

Eikazu Niwano
NTT Research Professor, NTT Social Informatics 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 been engaged in research on distributed system architecture, social information platform, and applied security including secure component. From 2002 to 2005, he worked at an NTT office in Paris, where he was involved in European and International standardization activities. He received the Minister of Internal Affairs and Communications Prize of the Information and Communication Technology Award from The Telecommunication Committee in 2018, the Chairman's Prize of the SCAT Award from the Support Center for Advanced Telecommunications Technology Research in 2021 and the Kekicheff Award from GlobalPlatform in 2023. He has been a board of directors of GlobalPlatform since 2005 and chair of the Japan Task Force of GlobalPlatform. He was a member of the smart card and ICT city-related study group of Ministry of Internal Affairs and Communications of Japan. He is also a member of the Institute of Electronics, Information and Communication Engineers of Japan.

Akira Nagai
Senior Research Engineer, NTT Social Informatics Laboratories.

He received a B.S., M.S., and Ph.D. from Tokyo University of Science in 2006, 2008, and 2017. He is currently involved in applied research on post-quantum cryptography.

Fumiaki Kudoh
Senior Research Engineer, Social Information Sharing Research Project, NTT Social Informatics Laboratories.

He received a B.E. and M.S. in engineering from Waseda University, Tokyo, in 2009 and 2011. Since joining NTT in 2011, he has been studying the field of ID federation and authentication. He is currently involved in applied research on post-quantum cryptography and confidential computing. He was with NTT DOCOMO, INC. from 2017 to 2020, where he was engaged in security enhancement of authentication infrastructure and planning, development, and sales of an electronic Know Your Customer (eKYC) service.