Secure Components in the IoT Ecosystem Era

— Toward a trusted smart society —

Eikazu Niwano
NTT Research Professor
Secure Platform Laboratories
Nippon Telegraph and Telephone Corporation

1. Introduction

The IoT environment has been developing remarkably recently. AI, Big Data and Cloud infrastructure technologies are being used to link and utilize data in many fields, moving toward realization of a smart society.

However, in this environment, reports of incidents due to vulnerabilities in IoT devices are on the rise, and it is becoming increasingly important to study how the authenticity and trustworthiness of data and devices can be ensured.

Secure components are an approach to resolving such issues that is attracting attention and has been applied mainly for conventional strong consumer authentication.

This article discusses the current state and future of secure component technology that is being used to provide a trusted environment for the emerging super smart society, with reference to IoT and the developing IoT ecosystem.

2. Secure Components

So what are secure components? Secure components are secure elements (SE), such as the now-widespread smart cards and smartphone SIM cards, which are very resistant to external attack (tamper-resistant). They have features such as: 1) A secure store that can manage secret and confidential information such as security keys; 2) Security features such as authentication, digital signatures and encryption; and 3) Remote application management.

In recent years, secure components such as embedded SIMs (eSIM) and integrated SIMs (iSIM) have entered the market. eSIMs allow the issuer to be changed remotely, after they are issued, and have started to be used in applications such as connected cars. iSIMs, which are bundled in Systems-on-a-Chip (SoC), strengthening the security of device hardware have appeared. In addition to this expansion in types of SE, secure components are also advancing rapidly, with appearance of new secure execution environments, called Trusted Execution Environments (TEE). These are different from ordinary operating systems and they are much anticipated for use in a wide range of wearable and other IoT devices[1].

In particular, IoT network environments involve a wide range of elements—edge devices, gateways, edges servers and cloud—and discussion has begun regarding how secure components will be integrated, linked and/or isolated with conventional tamper resistant module technologies, such as Trusted Platform Modules (TPMs) Hardware Security Modules (HSMs) used with traditional PCs/servers and secure micro-processing/controller units (MPUs/MCUs).

3. IoT Device Certification and Authentication

The question arises, why are secure components important in the IoT era?

In connected IoT environments a range of edge devices are widely deployed, distributed and connected, and threats and verified results are increasing. These often involve falsification of sensor data, but due to cyber-physical integration, they also include cyber attacks entering via low-end IoT devices to gain illicit control of physical devices that have life-threatening implications (such as medical devices or automobiles). As a cyber-attack countermeasure, the Japanese government has also started a survey of IoT devices through the NOTICE Program in February, 2019.

In the future, as the number of incidents increases and the scope of their effects expand, hopes will increasingly be placed on secure components[1] that support device attestation and secure-boot functions, to provide a basis for trust in strong authentication and device legitimacy, similar to how use of smart cards have spread to provide strong authentication of people.

IoT devices are also often installed over long periods of time in locations where maintenance is difficult so it is important to have flexibly and be able to update and add security functions in tamper resistant chips remotely, as has been pointed out by the GlobalPlatform[1] international standardization organization. Such updates will be used to counter compromises to these functions, for example. It could be argued that the most important feature of secure components is the ability to load, add or modify various functions after installation, using a remote environment in this way.

4. Development of an ecosystem—The importance of secure ID component management

Another important trend in the connectivity environment is development into an ecosystem.

With advances such as 5G and LPWA in the connectivity environment, we are entering an era in which all kinds of objects will be able to connect dynamically.

For people, objects and systems to be able to register and connect dynamically throughout the network in this environment, it is desirable to be able to check their credibility (security) and reliability (safety and trustworthiness).

Within this ecosystem, a connectivity environment will be formed with products deployed from various manufacturers, and spanning national boundaries. Recently, discussion of product supply chain and device life cycle issues is occurring more often, but in the future, our approaches to securing and evaluating the security and trust of overall systems, together with secure components, will also become more important.

As this ecosystem emerges, automobiles, homes, buildings, and other Systems of Systems (SoS) composed of various elements, will increase in complexity and scope. The key to this problem will be in how we assure and authenticate the IDs of each of these systems as well as the components that comprise them (identifiers, but also the legitimacy of various attributes of the actual components).

As such, it will be extremely important how the set of ID components in these extremely complex configurations are composed and structured, in what units and with what interrelations, how they are managed and authenticated using secure components, tamper resistant modules and secure MPUs/MCUs, and how their authenticity and trustworthiness is guaranteed.

In other words, important issues in the future will include organizing the relationships among IDs and other secure components (other tamper resistant modules, secure MPUs/MCUs, etc.), which are the basis for trusting people, objects, systems, SoS and their components; the mechanisms for evaluating and assuring the security and trust in these relations; and the security-by-design.

5. Trusted smart society

In addition to the promising fields of IoT and IoT security, discussion is now also beginning in the promising field of secure component applications and use cases.

Studying in detail, the issue of managing the ID component set and the secure components that we have discussed, including guarantee (attestation) of real object/entity configurations, will ultimately lead to realization of a super smart society and trusted smart cities that support it. This society will be able to safely and securely link data from many fields and types of business.

Another important key in achieving this will be to study social trust in these composition elements at various levels in society[2].

6. Conclusion

Serious study of standardization related to IoT, security and secure components, has just begun.

International organizations including GlobalPlatform, GSMA[3], and OneM2M[4], are collaborating to set these standards.

In February 2019, the ETSI released technical specifications in a consumer IoT oriented cyber security document, including descriptions of managing security services using eUICC/TEE[5]. Similarly, the NIST in the USA, ENISA in Europe, and the IPA and IoT Promotion Consortium in Japan are also referring to tamper resistant modules and secure components in cyber security and IoT related guidelines.

In the future, we look forward to stronger links between GlobalPlatform and other organizations related to tamper resistant chips, such as the Trusted Computing Group (TCG), which is standardizing TPM, and expanding cooperation among organizations involved in tamper resistant chips and IoT. We also anticipate collaboration with and assistance from organizations involved in smart-city technologies, such as ITU-T SG20, in the future.

References
[1] Eikazu NIWANO, “New Standardization Trends at GlobalPlatform—Secure Components for the IoT Era”, NTT Technical review, 2019 Vol. 17 No. 2.
[2] Eikazu NIWANO, “From Secure to Trusted Smart Cities”, Global Forum 2015, 2015.9.29
[3] “GSMA Remote Provisioning Architecture for Embedded UICC”, Technical Specification Version 3.2, June 2017
[4] OneM2M TECHNICAL SPECIFICATION, TS-0003-V2.124.1, Security Solutions, March 2018
[5] “CYBER; Cyber Security for Consumer Internet of Things”, Provision 4.4-1, ETSI TS 103 645 V1.1.1 (2019-02)