Structured ID Components over Secure Environments

Global Forum 2019 @ Angers, France

7th October, 2019

Eikazu NIWANO

Secure Platform Laboratories
NTT Corporation

Background - IoT Security

- Increasing cyber attack risk and needs of authenticity for IoT device
  - Ministry of Internal affairs and Communication in Japan launched "NOTICE*" program in February 2019 to investigate 150M IoT Devices and alert user to change its configuration
    - * National Operation Towards IoT Clean Environment

- Long-term life cycle management in difficult location for rush/onsite operation and huge numbers of distribution– maintenance problem

- Low-end capability of IoT device

- Eco systems - supply chain risk , dynamic configuration

- Digital twin - increasing impact to real through virtual

- Global, but region depended security

- Different requirements by sector according to its cyber security risk

Need strong, flexible, but simple & trustworthy security solution !

On Going Trends of IoT Device Security with Secure Environments

- **Variety of secure environments as Root of Trust (RoT);**
  - TRE(Tamper Resistant Environment) : Secure Element(SE: eSIM, iSIM) , TPM(Trusted Platform Module) and HSM(Hardware Security Module)
  - S-TRE(Semi-TRE): TEE(Trusted Execution Environment), Secure MPU/MCU

- **Secure remote management and update capability**
  - Virtualization (ex. low/high level platform for iSIM(iUICC), TPM function as Application)
  - (Remote) attestation

- **Standardization, policy and deployment effort has started**
  - Especially GlobalPlatform strongly promote this kind of standardization, secure device with some of secure environments and its security certification
  - IoT/Cyber security guideline by public organization has started to touch the usage of secure environments
    – ETSI*1/ENISA(Europe), NIST(US), IoT Acceleration Consortium (by MIC*2 and METI*3 Japan) etc
  - Connected car (GSMA&GlobalPlatform), smart meter etc

*2. Ministry of Internal Affairs and Communication
*3. Ministry of Economy, Trade and Industry

For eco system environments more

Need Trust for Systems-SoS with Secure Environments itself
(I touched this topic at GF2018)

* 1. ETSI TS 103 645 V1.1.1 (2019-02) CYBER; Cyber Security for Consumer Internet of Things

Issue to be addressed – "Structure as Trust"

- Structure management - ID structure of systems and SoS
  - Device components-device–> house/building/car-city-region and so on/etc.
  - Person, things with the role of supplier/consumer/provider etc.

- Assurance of trust for systems and SoS - structured ID components in system/SoS with/over secure environments
  - Security by design
  - Attestation
  - Evaluation
  - Certification

- Normalization of the assurance
  - Trust and its level – criteria
  - (cross) sector * (cross) region – crossover, domain specific