Global Forum
Shaping the future 2017

DIGITALIZATION:
INTELLIGENT PATHWAYS

IoT Security with Trusted Secure Module

Eikazu NIWANO
Secure Platform Laboratories
NTT Corporation

Session2: Safety, Security & Privacy
in an Hyperconnected Society & Ecomony

Beeing Actualized Threats on IoT Devices in Hyperconnected Society

- Actualized incidents and experiments
  - ✓ On automotive, health, home appliance sectors etc
  - ✓ Cyber attacks through/from numerous hacked devices
- Importance of device authenticity and remote IoT device management
  - ✓ Device certification, identification, authentication and authorization
  - ✓ Firmware update
  - ✓ Secure boot/root of trust
  - ✓ Remote attestation and management

Secure Module as the Token of IoT Device

- In Japan, some IoT security related organizations has been established recently and its charter/guidelines touch secure module*
  - ✓ IoT Acceleration Consortium, Oct 2016 – more than 3,000 members
  - ✓ Secure IoT Alliance, Feb 2017
  - ✓ Secure IoT Platform Consortium, April 2017

  * Called tamper resistant module, secure chip, secure element etc

- Intenational standardization effort has been started
  - ✓ GlobalPlatform : general scheme of root of trust, TEE (Trusted Execution Environment) and collaboration with TCG
  - ✓ TCG(Trusted Computing Group) : TPM for IoT
  - ✓ OneM2M and GSMA for remote management of secure module by applying GlobalPlatform scheme etc

- Commercial deployments have already been started by applying eSIM/eUICC, TEE and TPM

Issues to be Considered and Studied – in order secure module be more trusted

- Handle various types of secure module in hyperconnected ecosystem according to required security and trust assurance level
  - ✓ Smart Card, SD, SIM/UICC, eSIM/eUICC, TPM, HSM – HW oriented
  - ✓ Secure Container, TEE etc – SW oriented
- Schema for trust definition, assuarance and evaluation for integrated multi-types of secure modules and devices as system
  - ✓ Security/Trust by Design with secure modules
- Managing not only trust as functional reliability but social trust as safety
  - ✓ Assuarance for chip, device and system profile linked to social aspects in real society and world
- Finally, standardization effort have to be done among existing various types of standardization organizations for integrated trust assuanrace as describe above