NTT

Nippon Telegraph and Telephone Corporation

Diversity-oriented Secure Chip Management towards Network Convergence

Global Forum, 5th November, 2007

Eikazu NIWANO

Service Integration Laboratories

NTT Corporation

Networks and its Environments

- Networks are going to be converged
  - Fixed network/mobile network/Internet (FMC, triple play)
  - Public network/private network/dedicated network
  - Sector-depended networks (education, health, government etc)
- Diversity of terminals
  - STB/fixed phone, mobile phone/smart phone, PC/PDA, ATM
- Diversity of secure services
  - DRM, mobile TV, etc

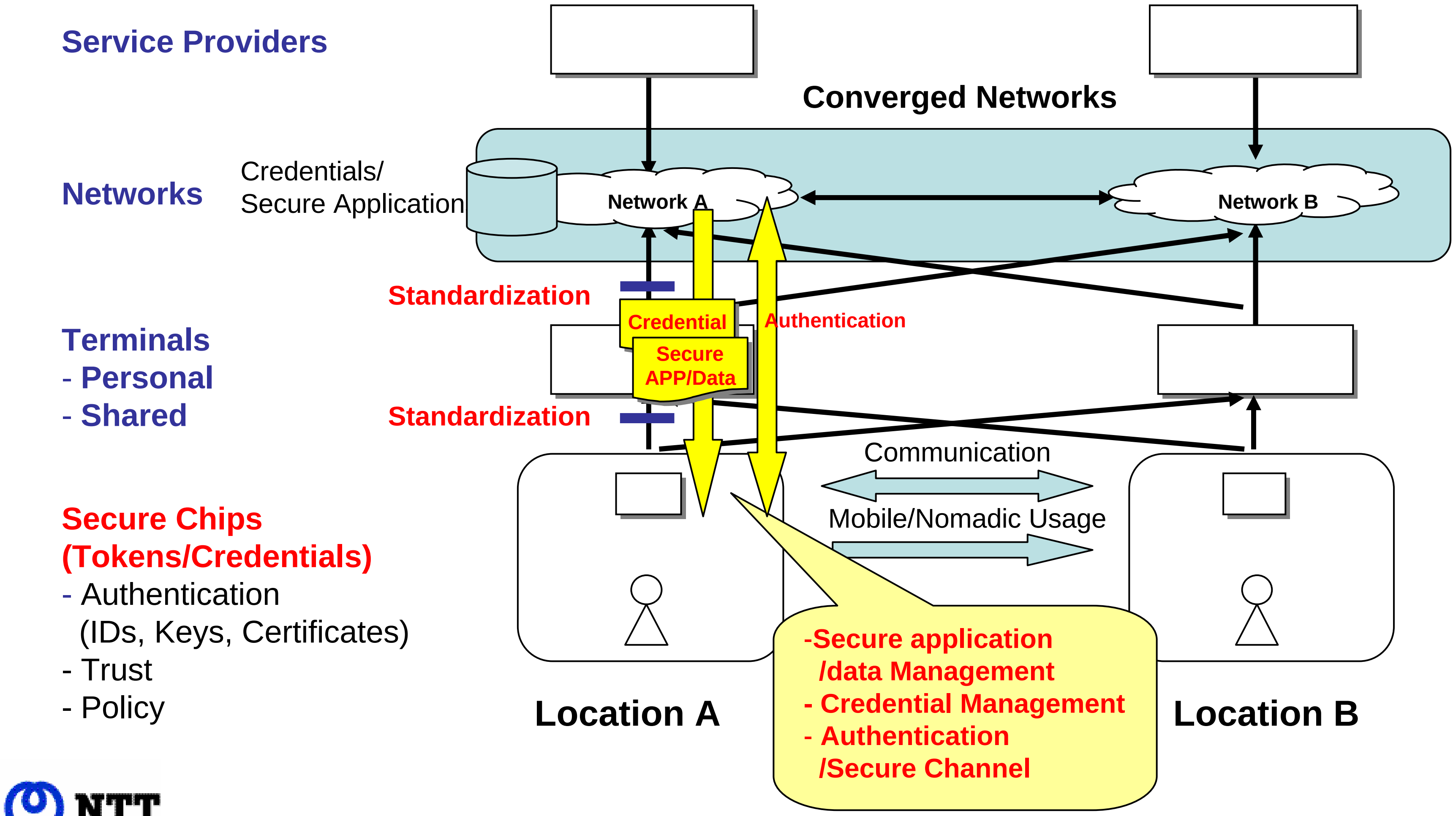
How to manage secure applications/data and credentials
over networks and its environments?

Secure Chip as Key Device

- Smart card is used in various sectors
  - Authentication and value management
  - Financial, Transportation, Telecommunication, Government, ID etc
- SIM (Subscriber Identity Module) is used in mobile network
  - Subscriber authentication
  - Secure services (DRM, mobile TV etc)
- Embedded chip in mobile phone has become to be very popular for secure data management in Japan
  - Mobile payment, transportation ticketing etc
- In fixed network, SIM is defined as an important device for authentication
  - European standardization organization for NGN (Next Generation Network) adopted ISIM for IMS services

Network Convergence by Applying Secure Chip

- Applying secure chip for network convergence
- Open Interface among network, terminal and secure chip



NTT

Existing Convergences

- Secure application/data management
  - Standardization from smart card to SIM
    - ISO, GlobalPlatform -> 3GPP/ETSI SCP
  - For convergence of TPM or software token?
- Credentials management
  - ISO7816-4,8, PKCS#15/ISO7816-15, CEN TS224/WG15 etc
- Authentication/secure channel
  - ISIM for IMS authentication -> ETSI TISPAN
  - EAP protocol -> ETSI SCP
  - CSP (Cryptographic Service Provider) /PKCS#11: the interface between terminal and card is vendor specific
- Middleware between terminal and chip
  - ISO24727
  - OpenSC Project->FINID(Finland), BELPIC(Bergium) etc

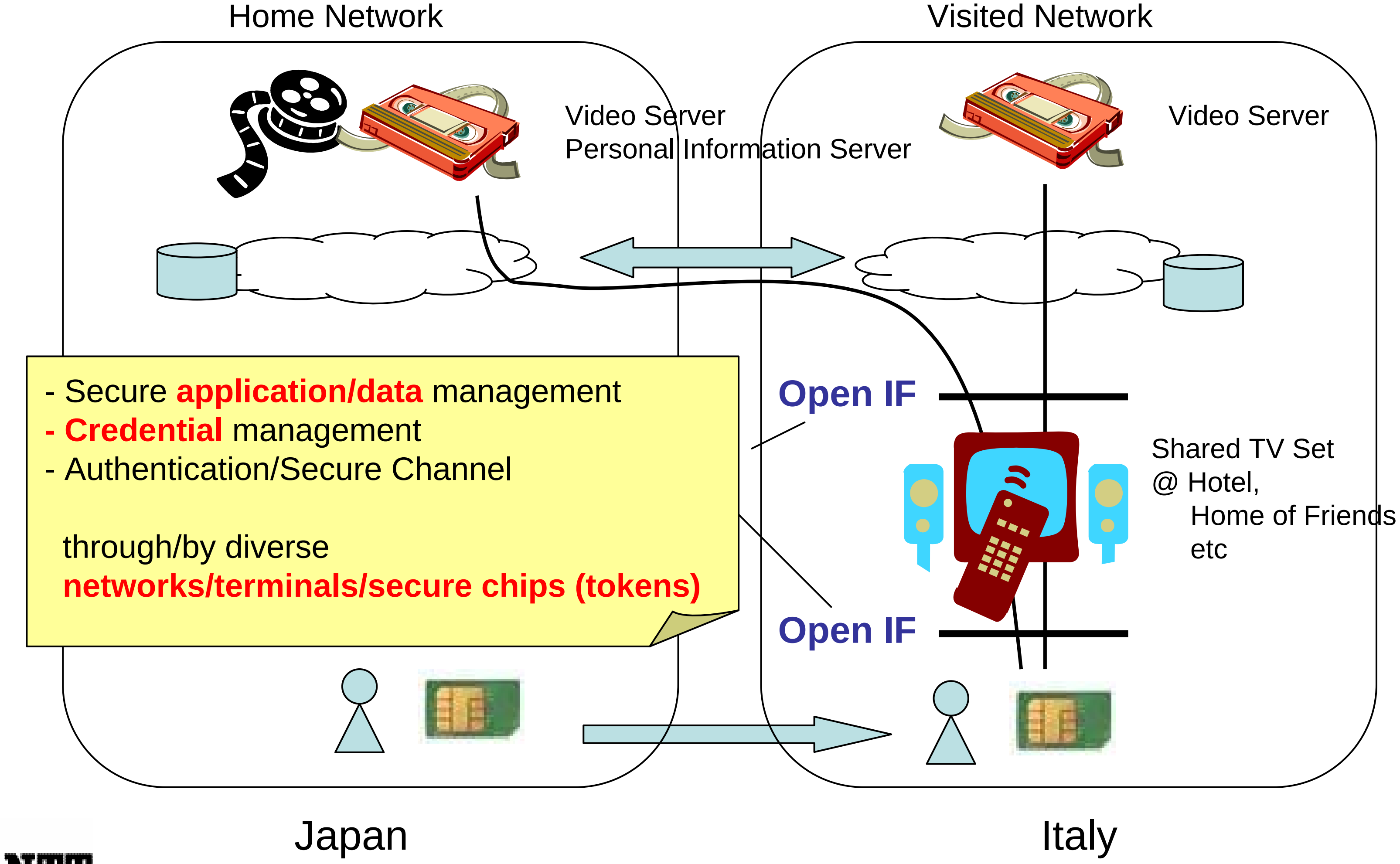
There are standards for each network,
but still has not been converged well especially for fixed network and for diverse chips

Issues to be addressed

- Standardization of interfaces beyond the differences of diverse networks
  - Secure application/data management, credential management and authentication/secure channel
  - Interfaces between servers and terminals
  - Interfaces between servers/terminals and secure chips
- Diversity management of token/credential container for dynamic and easy usage of secure chip on the above environments
  - Many types of chips/tokens
    - Smart card, SIM , USB token/key, SD, TPM, soft SIM, software token
  - Embedded chip/portable chip
  - Newly issued chip/existed chip/white chip (card)
  - Multiple secure elements
    - In one chip holder, in one terminal

An Example

Any network, any terminal, any secure chip in mobile/nomadic environments



- Secure **application/data** management
- **Credential** management
- Authentication/Secure Channel

through/by diverse **networks/terminals/secure chips (tokens)**

Conclusion

- There exist many types of networks and its environments
- Currently network, terminal and token have not been separated completely yet
- Co-existed/federated environments have to be provided with by secure chip (personal token)
- Standardization of secure application/data management , credential management and authentication have to be done over networks
- Diversity of secure chips have to be well managed