ITU-T Study Group 17 Security

An overview of ITU-T SG 17

Identity Management Architecture and Mechanisms

Emerging trends and issues in identity management

Miho Naganuma

On behalf of Q10/17 Rapporteur
Abbie Barbir

ITU-T SG17 mandate established by World Telecommunication Standardization Assembly (WTSA-16)

SG17 Mandate

- Build confidence and security in the use of Information Communication Technologies

SG17 Lead Study Group roles

- Security
- Identity management
- Languages and description techniques

Q10/17

- Responsible for Identity management architecture and mechanisms studies
- Leads Joint Coordination Activity (JCA) on Identity management (JCA-IdM)

JCA-IdM

- SG17 is “Parent” for JCA-IdM
- Coordination and planning of IdM standardization activities

ITU-T JCA-IdM

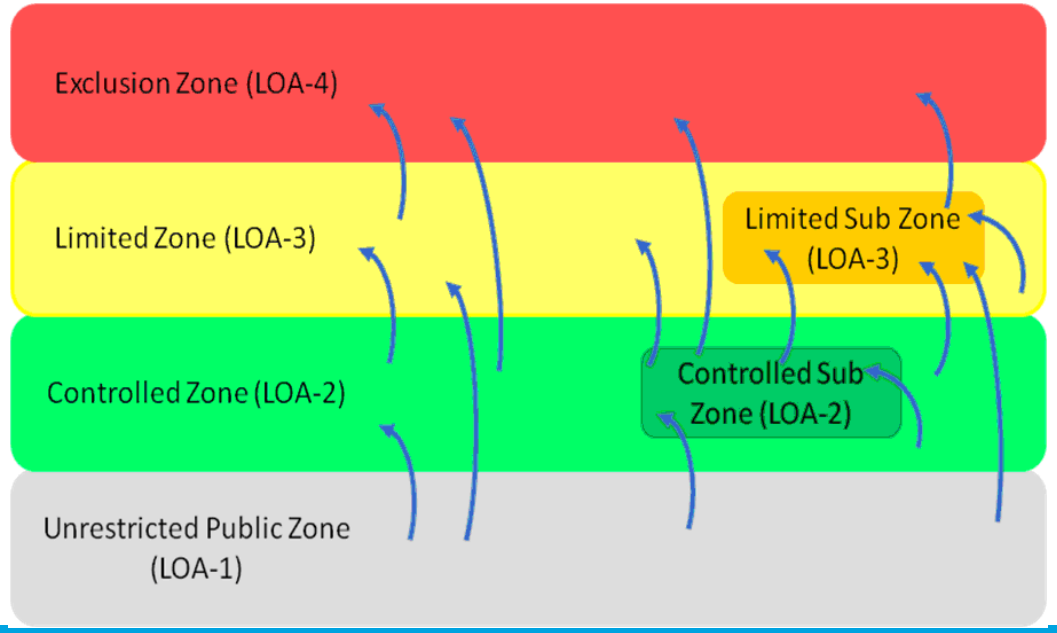
- Coordinates works of ITU-T SGs and other SDO/Fora on IdM
- Analyzes IdM standardization items and coordinates an associated roadmap with ITU-T Q10/17
- Maintains IdM roadmap and landscape document/WIKI
- Led by Mr. Abbie Barbir, Mr. Hiroshi Takechi, Mr. Geundug Park

Q10/17 Activities

- Identity vetting and strong authentication are essential for securing and enabling ICT based services
- Focus is on foundational work on identity management
  - developed basic framework and architecture for identity management (X.1250, X.1251, SAML 2.0 (OASIS) =X.1141)
  - developed the taxonomy and terminology to be used for identity management (X.1252)
    - Definitions adopted globally
  - Expansion of NIST 800-63 series scope and coverage
    - developed X.1254 as a general purpose framework for establishing the foundation of risk based authentication that is not based on binary authentication assumptions that were used by the industry.

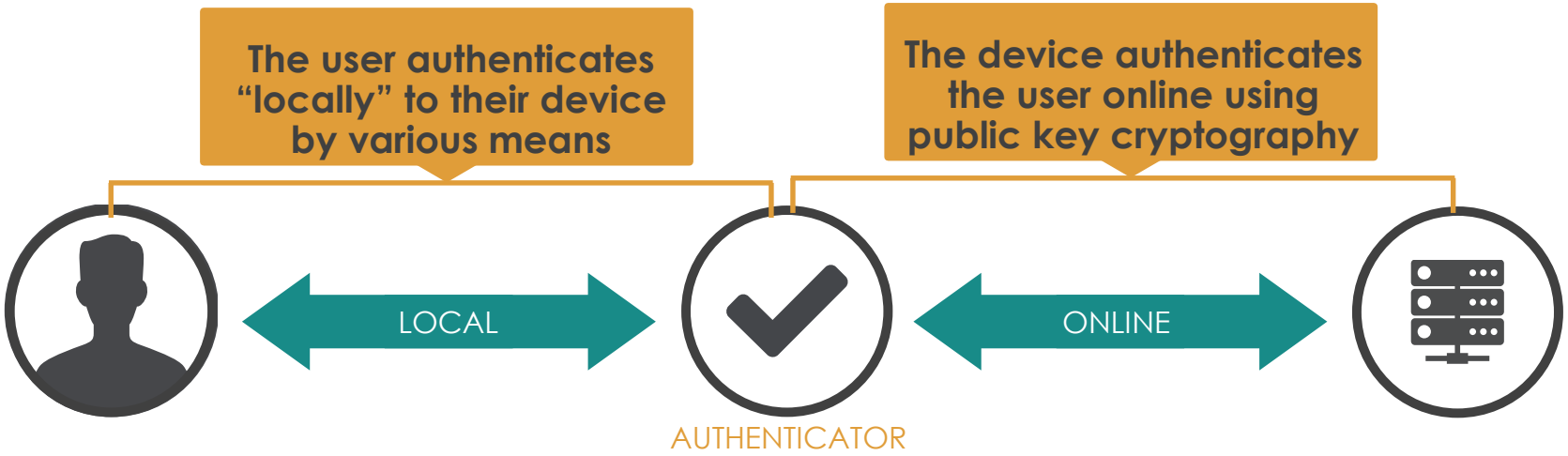
Q10/17 Activities

- Collaboration with SDOs to advance strong authentication standards.
- OASIS
  - Formalized method for step-up or step-down dynamic authentication
  - foundation of risk based authentication.
    - Stronger security and fraud resistance



Q10/17 Activities

- Collaboration with FIDO Alliance to standardize “NO password” solution in ITU-T (X.1277, X.1278)



- No 3rd party in the Protocol
- No secrets on the Server side
- No link-ability Between Services
- No link-ability Between Accounts

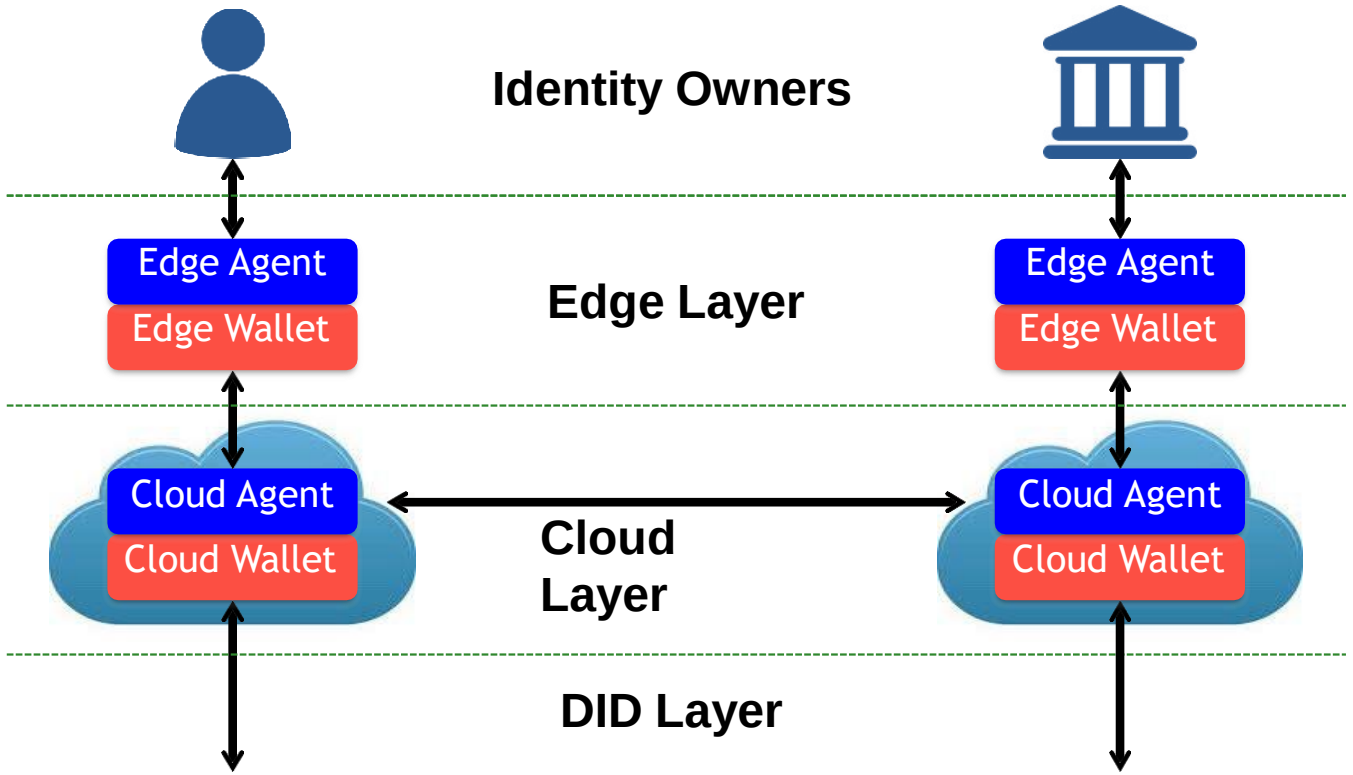
Protection of user login and identity in the era of massive data breaches

Q10/17 Emerging Trends

- Strong authentication in “Trust over IP” decentralized identity based on Distributed Ledgers.
  - Solutions that address issues relating to phishing, mutual authentication and man in the middle attacks
  - Suitable for data minimization when it comes to identity data
  - Mobile wallet technologies combined with strong authentication, and
  - emerging technologies under development (Verifiable Claims, Zero Knowledge Proofs and Decentralized Identifiers)
  - Work requires collaboration with Q11/17 and Q14/17.

Emerging Trust over IP (ToIP) Identity Stack

Decentralized Identifier (DID)



Emerging 5G Identity Trust Frameworks

- 5G represents an opportunity for network providers to re-invent themselves as trusted digital identity providers
  - 5G Identity solutions enhance trust in peer to peer decentralized identity network interactions resulting in more secure identity based services.

With ITU-T Work will require collaboration with Q6/17 and SG 13

Action Plan

- Expand IDM terms and definitions to include emerging technologies
  - Needed for interoperability
- Focus on NO password use cases and implementation
  - Needed in the age of data breaches
- Interoperable Decentralized Identity Management Systems build on new technologies including: Verifiable claims
    - Decentralized Identifiers
    - Secure elements in mobile devices
    - FIDO Alliance and W3C WebAUthN
    - Trusted 5G networks

Conclusions

- It is an exciting time for identity management
- Ability to capitalize on maturing technologies for solving security issues that has plagued traditional identity management systems

Annex

- **ITU-T X.1250 - Baseline capabilities for enhanced global identity management and interoperability**
- **ITU-T - X.1251 - A framework for user control of digital identity**
- **ITU-T - X.1252 - Baseline identity management terms and definitions**
- **ITU-T - X.1254 - Entity authentication assurance framework**
- **ITU-T - X.1277 - Universal authentication framework**
- **ITU-T - X.1278 - Client to authenticator protocol/Universal 2-factor framework**