## The ITU-T SG 17 Q10/17

# IdM standardization activity and Its Relationship to cybersecurity

**Hiroshi Takechi**

**ITU-T SG 17 Q10 Associate Rapporteur**

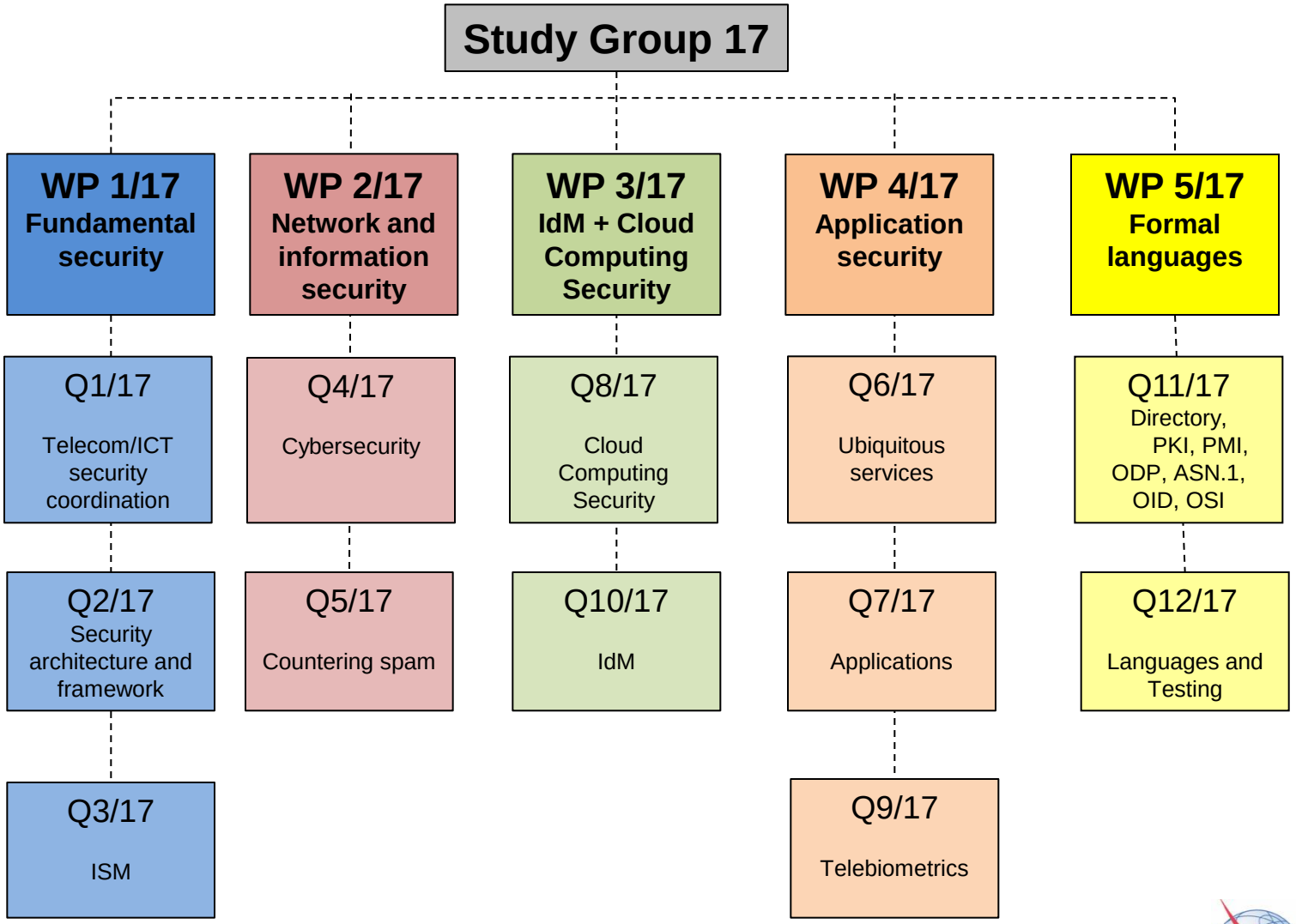
# Contents

- Overview of ITU-T SG 17
- Q 10/17
- JCA-IdM
- Example of Recommendations
- Example of Challenges
- Conclusions

# Overview of ITU-T SG 17

- Primary focus is to build confidence and security in the use of ICTs
- Meets about twice a year
- Lead Study Group on:
  - Security
  - Identity management(IdM)
  - Languages and description techniques
- Work organized into 5 Working Parties with 12 Questions

# Overview of ITU-T SG 17



# ITU-T SG 17 Question 10/17

- Q10/17 Identity management architecture & mechanisms

**Motivation for the Question**

- Dedicated to the vision setting and the coordination and organization of the entire range of IdM activities within ITU-T

**Why Focus on IdM**

- IdM is a critical component in managing network security and enabling the nomadic, on-demand access to networks and e-services that end-users expect
- Along with other defensive mechanisms, IdM helps to prevent fraud and identity theft and thereby increases users' confidence that e-transactions are secure and reliable, e.g. cloud and mobile computing system that are not directly controlled by the user organization
- National/regional specific IdM specifications and solutions will exist and continue to evolve. Harmonization of different national/regional IdM, specifications and solutions is important for global communications

# Q10/17,
# Identity Management architecture and mechanisms

- **Key vision of Q10/17**
  - Security enabler by providing trust in the identity of parties to an e-transaction
  - Providing network operators an opportunity to increase revenues by offering advanced identity-based services
  - Providing global trust and interoperability of diverse IdM capabilities in telecommunication on the base of leveraging and bridging existing solutions
  - The vision setting, and coordination, and organization of the entire range of IdM activities within the ITU-T

- **Key focus of Q10/17**
  - Adoption of interoperable federated identity frameworks that use a variety of authentication methods with well understood security and privacy
  - Encourage the use of authentication methods resistant to known and projected threats
  - Providing a general trust model for making trust-based authentication decisions between two or more parties
  - Ensure security of online transactions with focus on end-to-end identification and authentication of the participants and components involved in conducting the transaction, including people, devices, and services

# JCA-IdM

## SG17 is “Parent” for Joint Coordination Activity (JCA) on Identity Management

JCA is a tool for managing the work programme of ITU-T when there is a need to address a broad subject covering the area of competence of more than one study group. JCA helps to coordinate the planned work effort in terms of subject matter, time-frames for meetings, collocated meetings where necessary and publication goals including, where appropriate, release planning of the resulting Recommendations

# JCA-IdM
# Coordination with other bodies




NSTIC

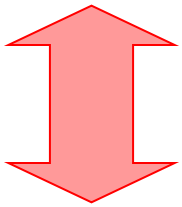

Fido Alliance

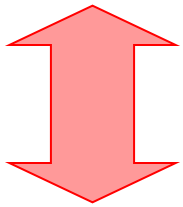


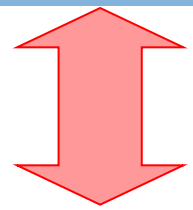





Advancing open standards for the information society



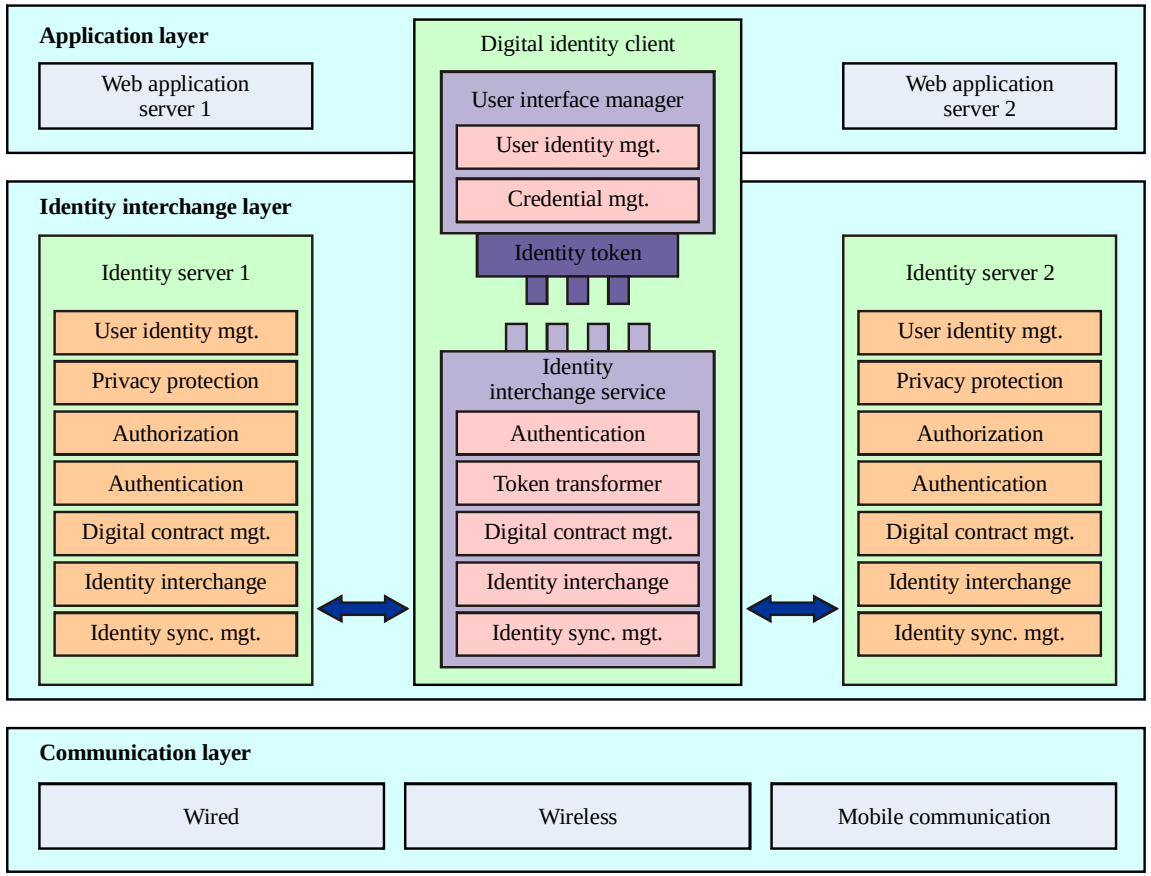


ITU-T Joint coordination activity on IdM (JCA-IdM)

# Examples of Recommendations

## X.1251 - A framework for user control of digital identity

- Defines a framework to enhance user control and exchange of their digital identity related information
- Defines capabilities for the digital identity information exchange
- Provides with the ability to control the release of personally identifiable information




X.1251(09)_F04

# X.1252

## Baseline Identity Management Terms and Definitions

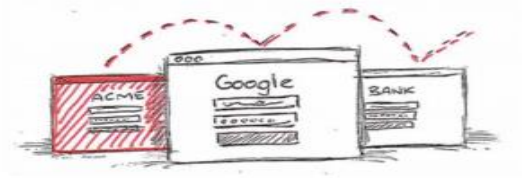
- Provides 70 definitions of key terms used in identity management (IdM)

**6.30 identity**: A representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context. For identity management (IdM) purposes, the term identity is understood as contextual identity (subset of attributes), i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts.
NOTE – Each entity is represented by one holistic identity that comprises all possible information elements characterizing such entity (the attributes). However, this holistic identity is a theoretical issue and eludes any description and practical usage because the number of all possible attributes is indefinite

- Examples of Current Challenges

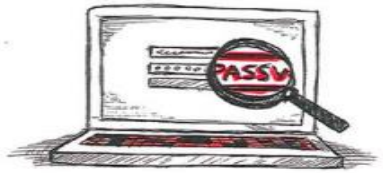
# Authentication Technology has stayed static

- Passwords
  - Users have Too many to passwords to  remember
  - On Mobile devices are difficult to type
  - In general they are not secure




**REUSED**


**PHISHED**




**KEYLOGGED**

- One Time Passcodes :Improve security, but not easy to use

**SMS USABILITY**

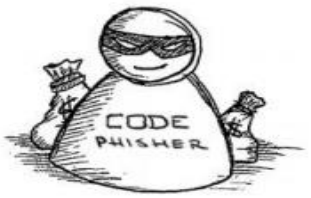
Coverage | Delay | Cost


**DEVICE USABILITY**

One per site | Fragile


**USER EXPERIENCE**

User confusion

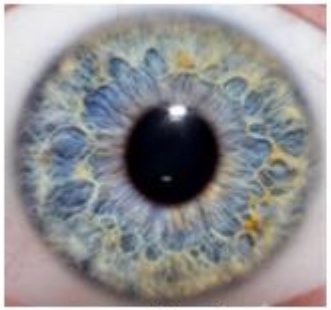



**STILL PHISHABLE**

Social engineering

# Authentication Alternatives

(1) Fingerprint



(2) Iris

(3) DNA

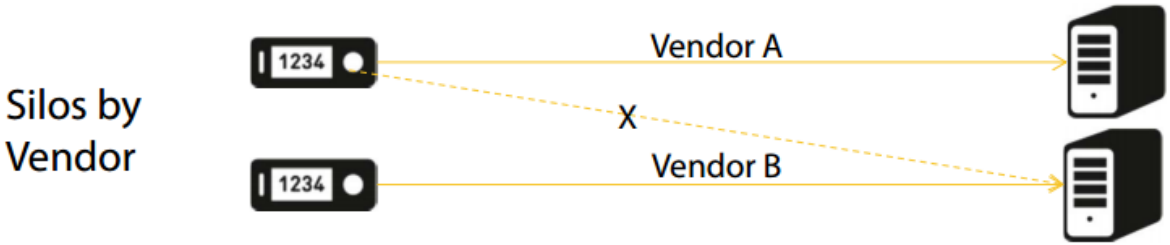
(4) Keystroke pattern

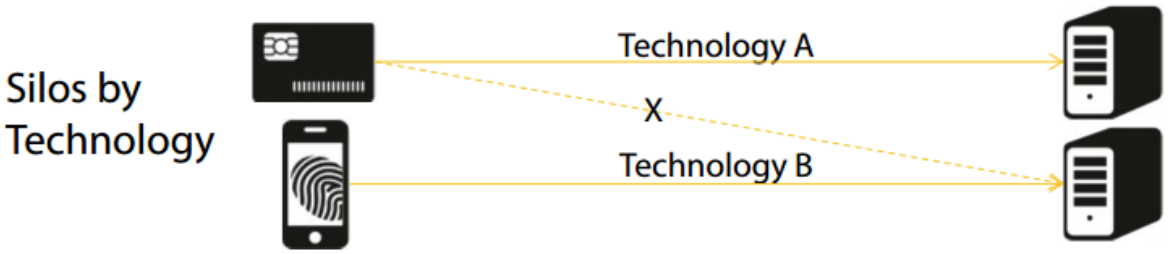
wearables

USB Keys

Facial Recognition

- Implementation is the Challenge
- Each authentication solution requires new HW, SW, and Infrastructure



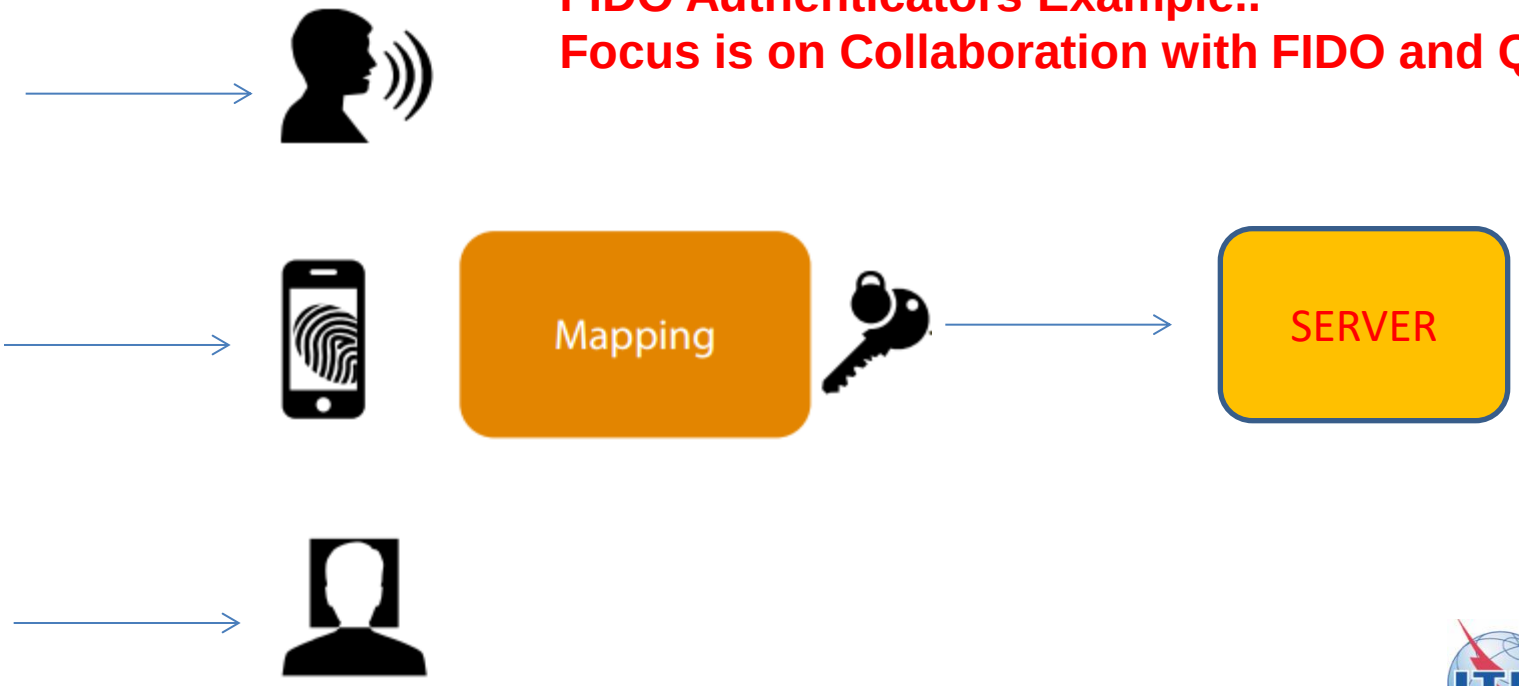



# Scalable Continuous Authentication

Q10/17 Goals is to work with ITU-T SG, FIDO Alliance and OASIS

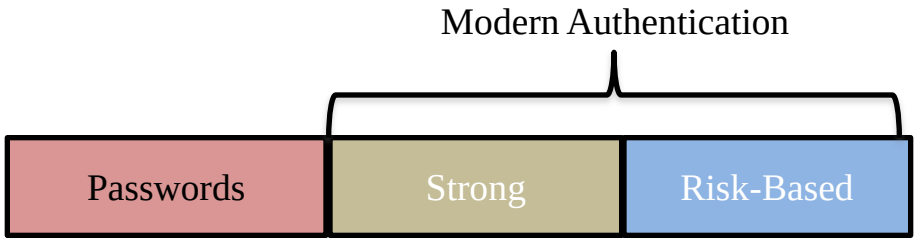
- Support for a broad range of authentication methods, leverage existing hardware capabilities.
- Support for a broad range of assurance levels, let relying party know the authentication method.
- Built-in privacy.

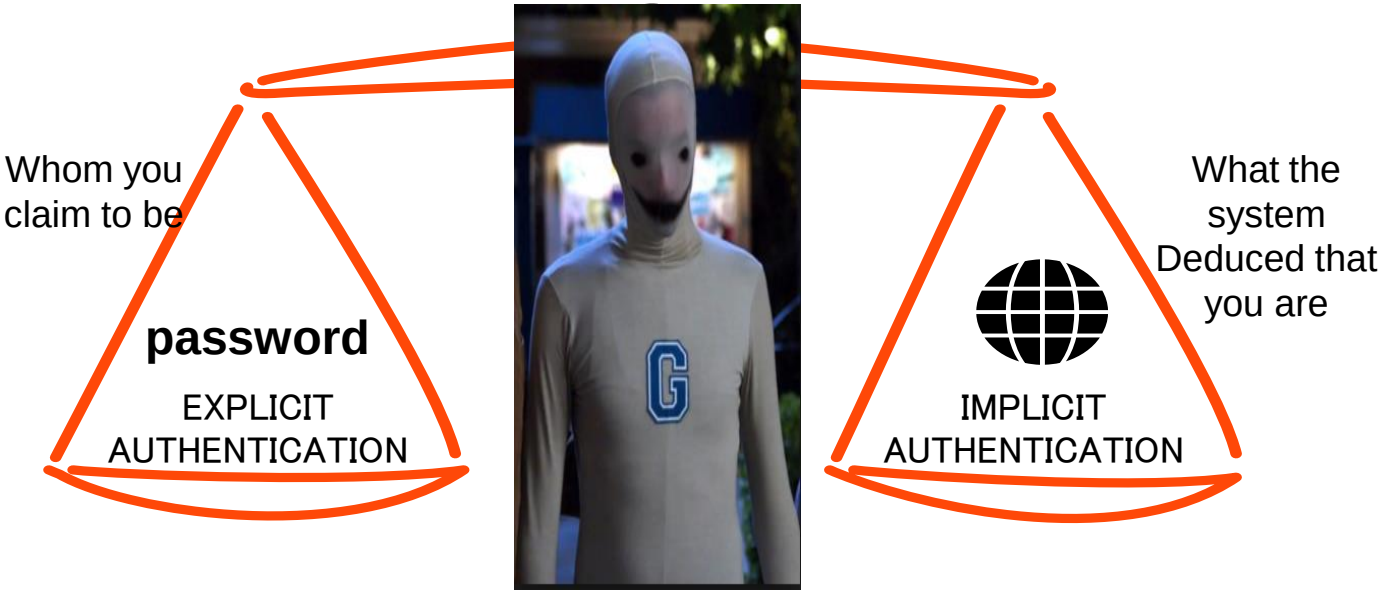
**FIDO Authenticators Example..**
**Focus is on Collaboration with FIDO and Q10/17**



# Core Functionality

- Discover supported authenticators on the client
- Register authenticators to a relying party (and bind it to an existing identity)
- Authenticate (a session)
- Transaction confirmation



# Conclusions

- Identity based services is a key technology for cloud based SaaS
- Online transaction requires means for identification of all parties involved in a transaction
- There need for open interoperable trust frameworks for IdM
- Identity Management continue to be a key security enabler for mobile and wireless interactions
- Protection of Personally Identifiable Identifiers (PII) is a required capability for IdM systems

Enhancing our collaboration between OASIS and ITU

- ITU's advantages

# Thank you!

**Hiroshi Takechi**