ITU-T SG 17 Q10/17

Trust Elevation Frameworks

Abbie Barbir, Ph.D.
ITU-T SG 17 Q10 Rapporteur

Martin Euchner
SG 17 Advisor

ITU Workshop on "Future Trust and Knowledge Infrastructure“
July 1 2016

Contents

- Overview of Q 10/17, JCA-IdM
- What is trust elevation
- Trust elevation protocol and metadata
- FIDO example
- Future work and Conclusions

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

JCA-IdM

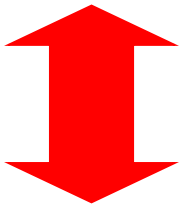
- SG17 is “Parent” for Joint Coordination Activity (JCA) on Identity Management and Q10 manage the JCA
- JCA is a tool for managing the work programme of ITU-T when there is a need to address a broad subject covering the area of competence of more than one study group. JCA helps to coordinate the planned 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

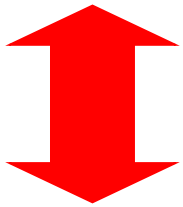
JCA-IdM
Coordination with other bodies

NSTIC

Fido Alliance

Advancing open standards for the information society





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

Rec. ITU-T X.1254
Entity Authentication Assurance Framework

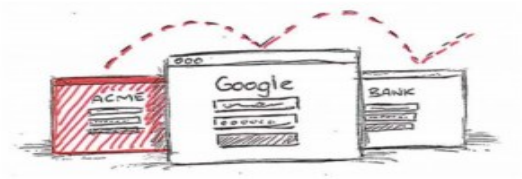
- Example of Q10/17 work
  Rec. ITU-T X.1254 : Entity Authentication Assurance Framework standardizes Levels of Assurance (LoAs) to promote trust, improve interoperability, and facilitate identity federation across organizations.
- Provides a framework for managing entity authentication assurance in a given context.

Level	Description
1	Little confidence the asserted identity
2	Some confidence in the asserted identity
3	High confidence in asserted identity
4	Very High confidence in asserted identity

- specifies four levels of entity authentication assurance;
- specifies criteria and guidelines for each of the four levels of entity authentication assurance
- provides guidance concerning controls that should be used to mitigate authentication threats
- provides guidance for mapping the four levels of assurance to other authentication assurance schemes
- provides guidance for exchanging the results of authentication that are based on the four levels of assurance

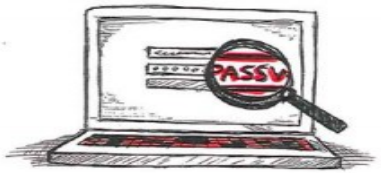
Authentication Technology has stayed static

- 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

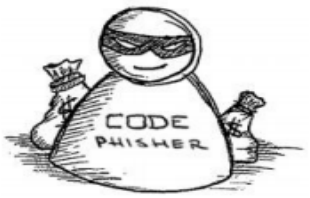
Coverage | Delay | Cost

DEVICE USABILITY

One per site | Fragile

USER EXPERIENCE

User confusion



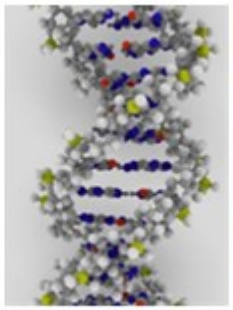
STILL PHISHABLE

Social engineering

Authentication Alternatives

(1) Fingerprint

(2) Iris



(3) DNA

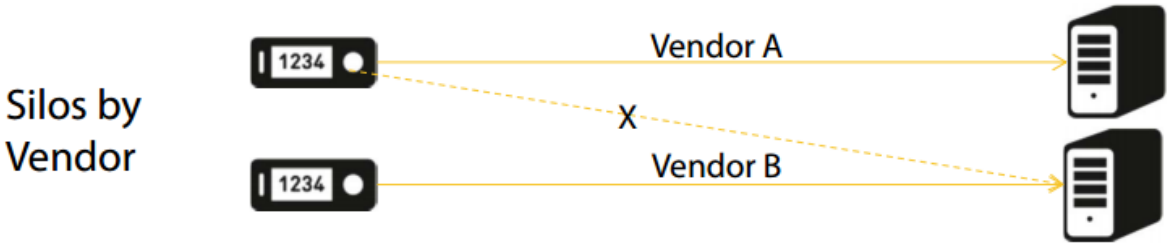
(4) Keystroke pattern

wearables

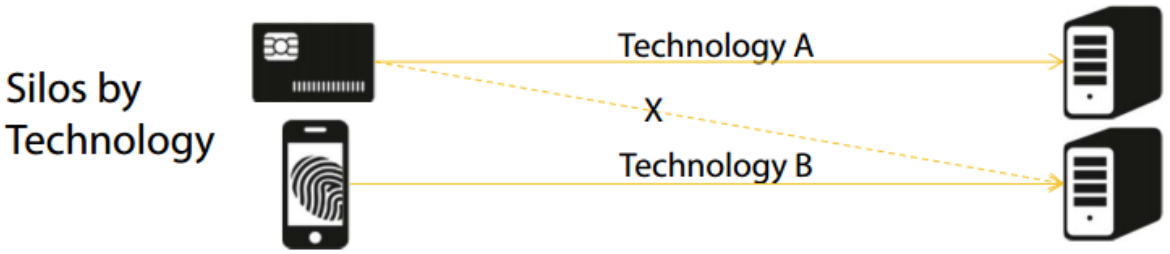
Smart Keys

Facial Recognition

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



Smart Devices

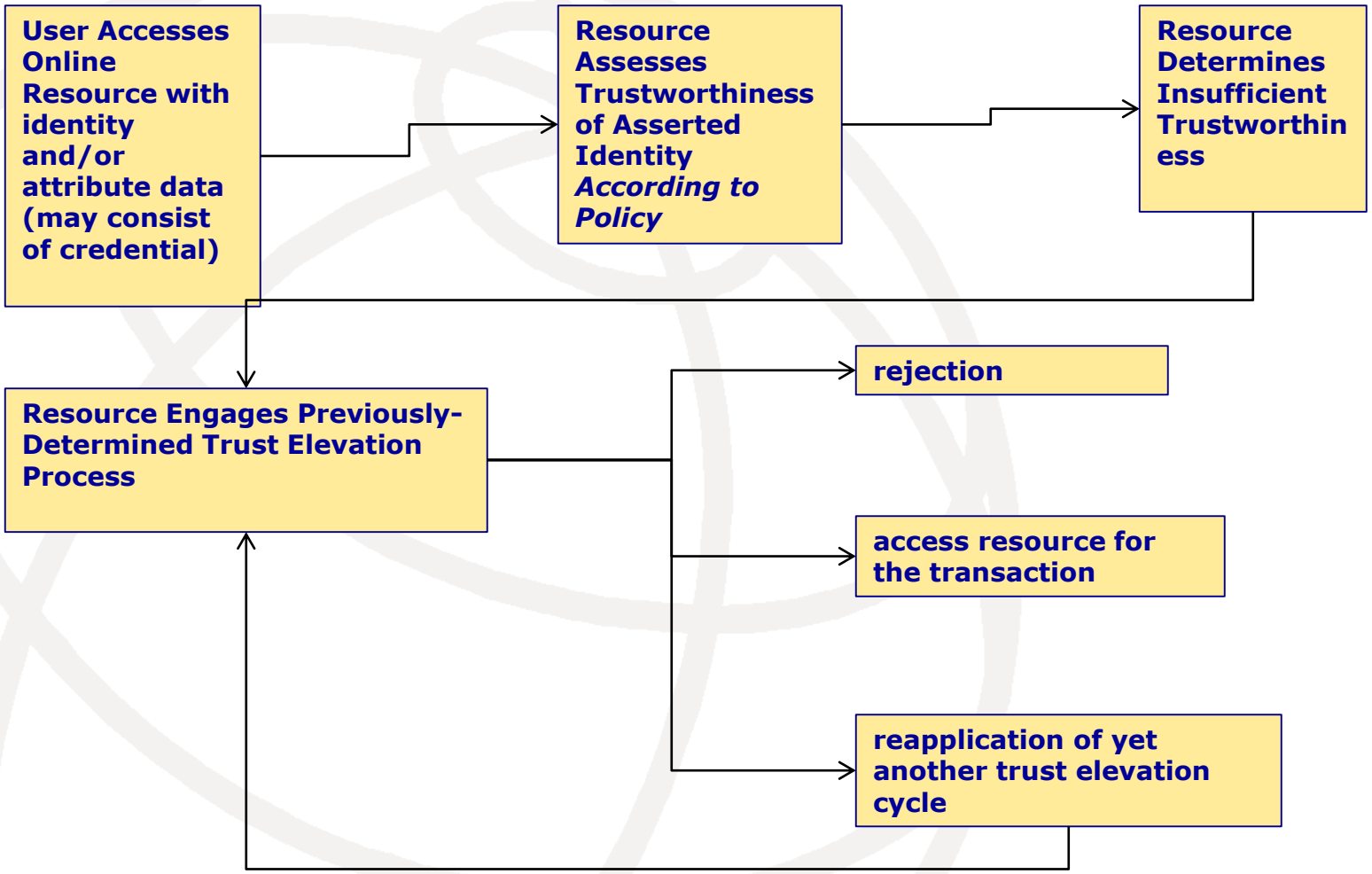


OASIS Trust Elevation (TE)

Trust elevation (step-up Authentication):

- **Increasing the strength of trust (Auth) by adding factors from the same or different categories of trust elevation methods that don't share the same vulnerabilities**
- **There are five categories of trust elevation methods**
  - **who you are (biometrics, behavioral attributes),**
  - **what you know (shared secrets, public and relationship knowledge),**
  - **what you have (devices, tokens - hard, soft, OTP),**
  - **what you typically do (described by ITU-T x1254, behavioral habits that are independent of physical biometric attributes)a nd**
  - **the context (location, time, party, prior relationship, social relationship and source).**
- **Elevation can be within the classic four X.1254 ITU-T LoA**

Trust Elevation Core Model

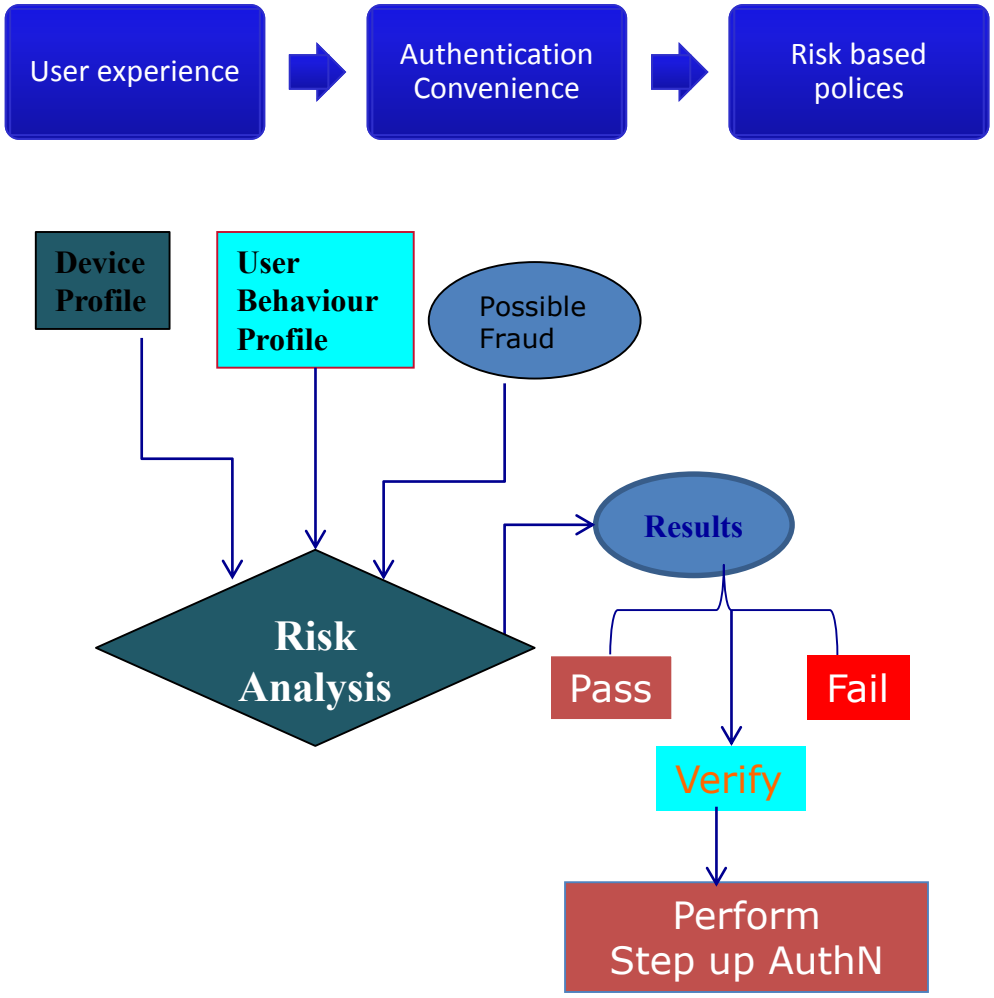


A General Use Case For Trust Elevation

- An authenticated entity attempts access to a protected resource.
- The access control policy engine for that protected resource determines that the authentication assurance or information assurance for the attempt is insufficient.
- The entity is instructed to do an authentication ‘step up’ in order to satisfy the access control policy.
- The cycle repeats.

- One approach to characterize ‘Trustworthiness’ is to determine which authentication threats and threat vectors are mitigated by specific authentication factors based on X.1254

Challenges of Mobile Authentication



Mobile App Considerations

- **Application architecture**
  - Offline vs. online access
  - Storage of information on device
  - Various mobile OS
  - Device ownership: BYOD or Corp Liable
- **Challenges to SSO on Mobile**
  - No standardized SSO
  - Native Mobile apps vs. Web
    - Better user experience
    - Leverage local device capabilities
    - SaaS vendor-provided apps authenticate to SaaS backend systems
  - **Web App**
    - Browsers lack access to native device E.g. Camera,
    - Browsers tend to be underpowered UI for small form factor devices

Mobile app security challenges:

- Broader coverage beyond VPN needed
- Check for malicious behavior and threats at app layer
- Continuous data monitoring and auth

Authentication Step-up and Metadata

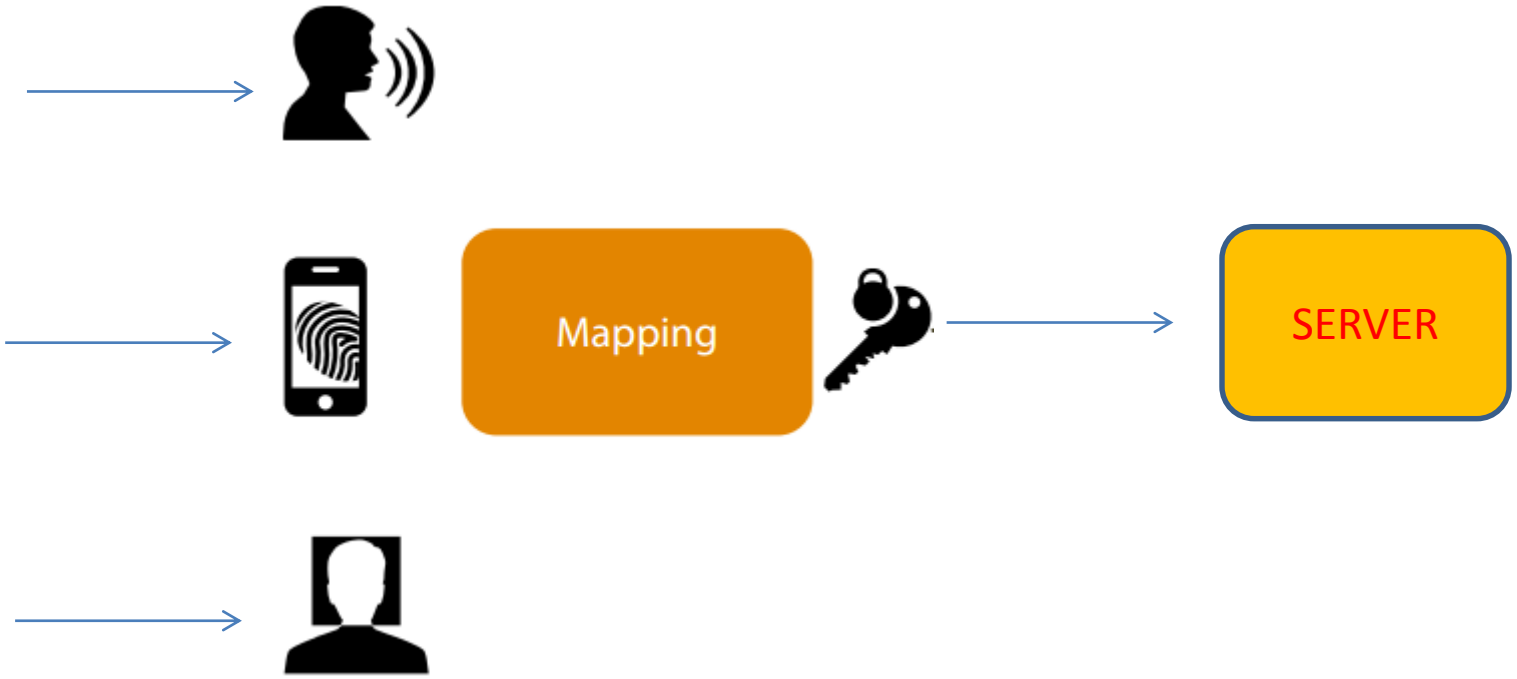
- The goals of this work is :
  - propose Trust Elevation architectural patterns demonstrating the use of Trust Elevation in modern Access Control systems
  - Describe a common metadata set, mechanisms and protocol elements for Trust Elevation information exchanges.
  - Promote the use of Trust Elevation elements to foster standardization among the many technologies and approaches currently in use for credential & authentication risk mitigation
- Focus is in on
- Architecture and implementation considerations
- Relate TE to existing authorization models and patterns
- Provide guidance and examples to enable architects and implementers to use the TE approach in their protocols of choice

Scalable Continuous Authentication

Q10/17 Goals is to also work with FIDO Alliance to eliminate user name/password

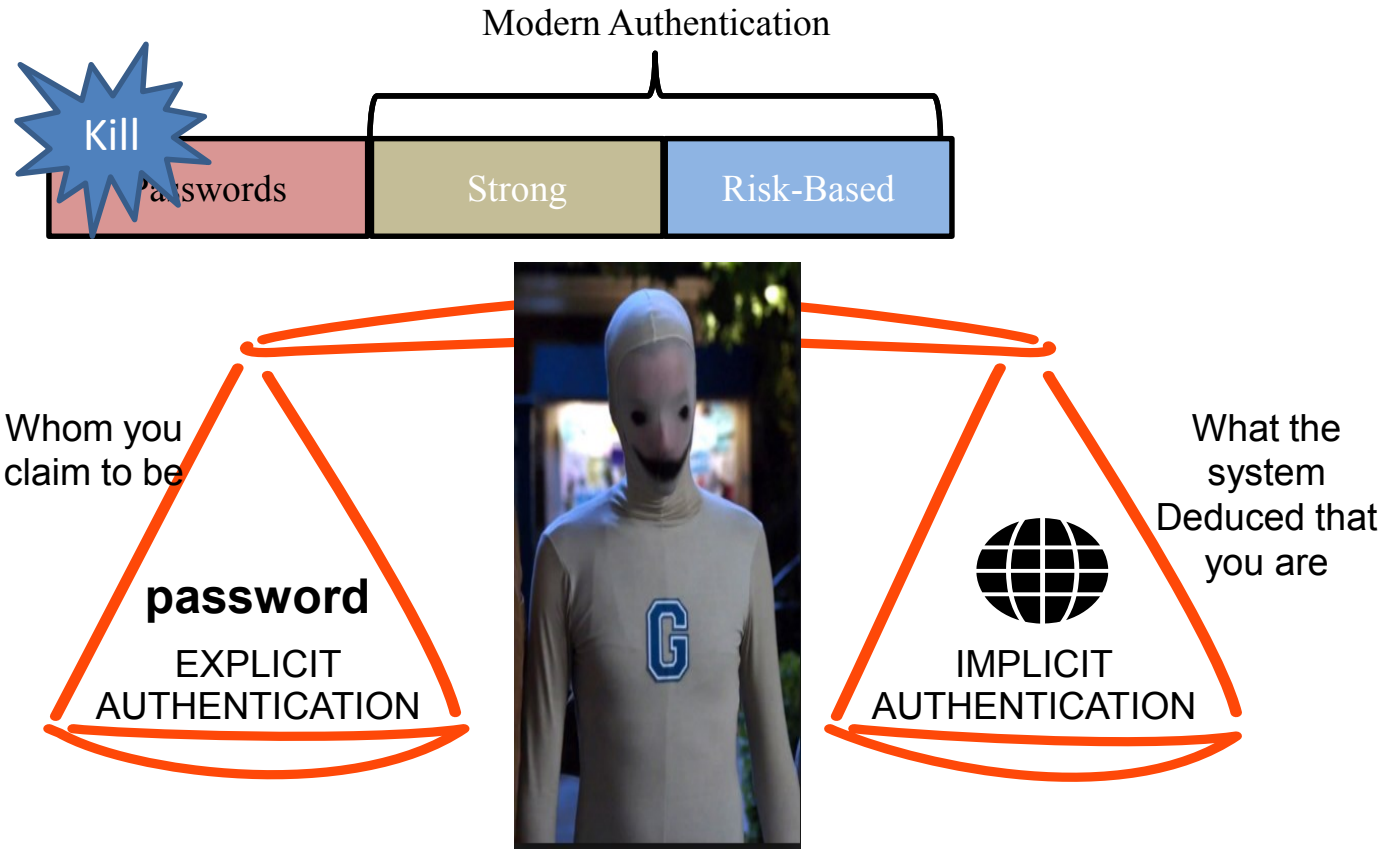
- Support for a broad range of authentication methods, leverage existing hardware capabilities.
- Support for a broad range of assurance levels, let relying party know the authentication method.
- Built-in privacy.

FIDO Authenticators Example



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
- Need to eliminate the reliance on Password

Thank you!

Abbie Barbir

Martin Euchner