Passwordless Authentication
Q10/17 Overview

Abbie Barbir, Ph.D, CISSP

ITU-T SG 17

Question 10/17 Co-rapporteur

ADIA Co-Founder https://adiassociation.org/

Question 10/17
Identity management and Telebiometrics architecture and mechanisms

SG17 Lead Study Group roles

- Security
- Identity management
- Languages and description techniques

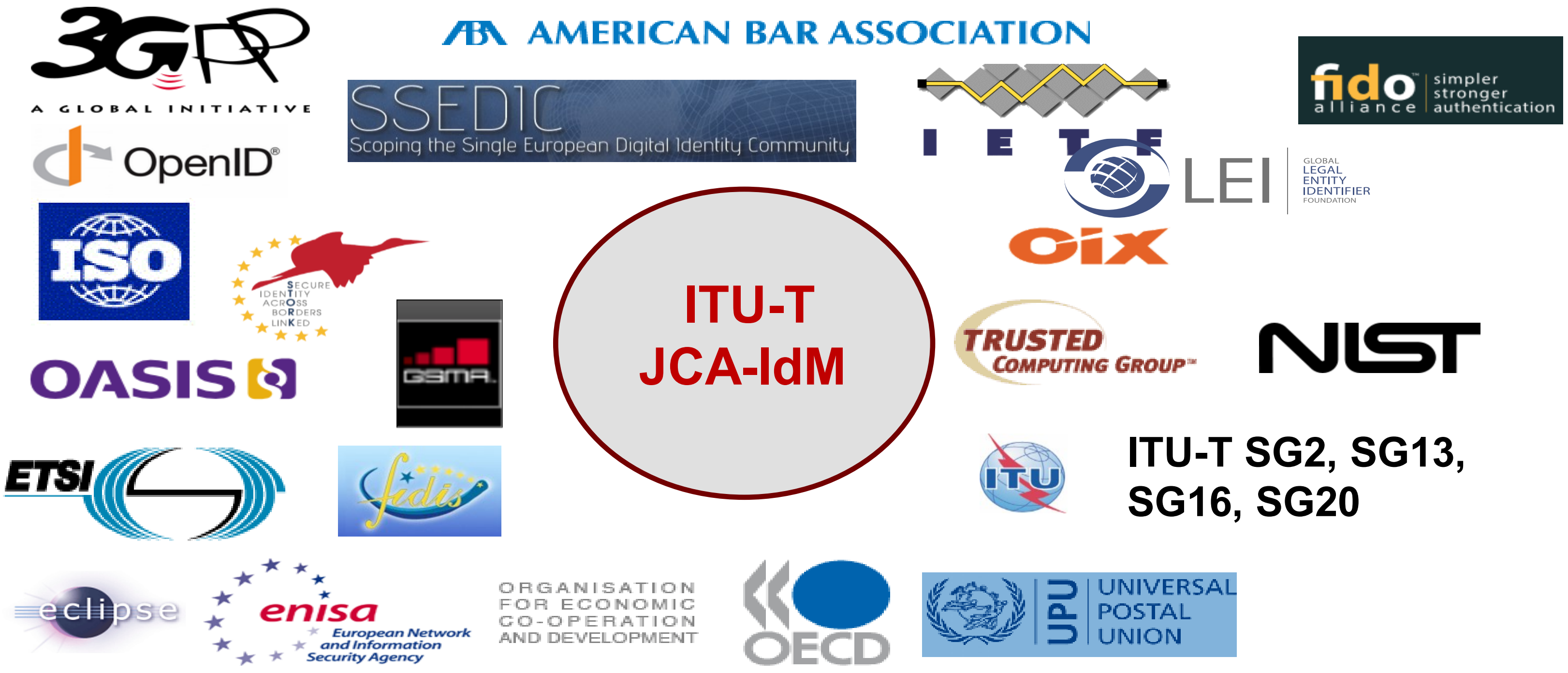
-**Q10/17**

- Responsible for Identity management architecture and mechanisms studies
- Responsible for Telebiomteric authentication, architecture and mechanisms
- 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**

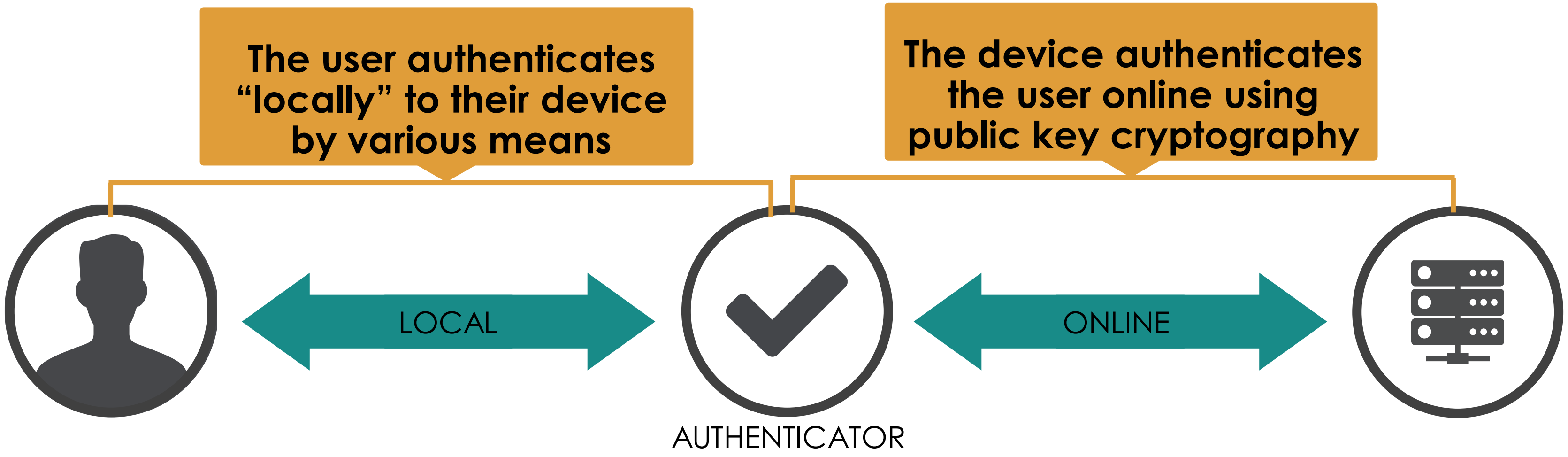

3GPP A GLOBAL INITIATIVE
AMERICAN BAR ASSOCIATION
fido alliance simpler stronger authentication
SSEDIC Scoping the Single European Digital Identity Community
IETF
OpenID
LEI GLOBAL LEGAL ENTITY IDENTIFIER FOUNDATION
ISO
SECURE IDENTITY ACROSS BORDERS LINKED
OIX
ITU-T JCA-IdM
TRUSTED COMPUTING GROUP
NIST
OASIS
GSMA
ETSI
fidis
ITU
ITU-T SG2, SG13, SG16, SG20
eclipse
enisa European Network and Information Security Agency
ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT
OECD
UPU UNIVERSAL POSTAL UNION

Q10/17 Activities

- ITU-T X.509 is an anchor of Trust for many 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.1250rev, X.1251rev)
  - developed the taxonomy and terminology to be used for identity management (X.1252 updated)
    - Definitions adopted globally
  - Expansion of NIST 800-63 series scope and coverage to also include FIDO X.1254(updated)

Q10/17 Activities

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



The user authenticates "locally" to their device by various means

The device authenticates the user online using public key cryptography

- 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

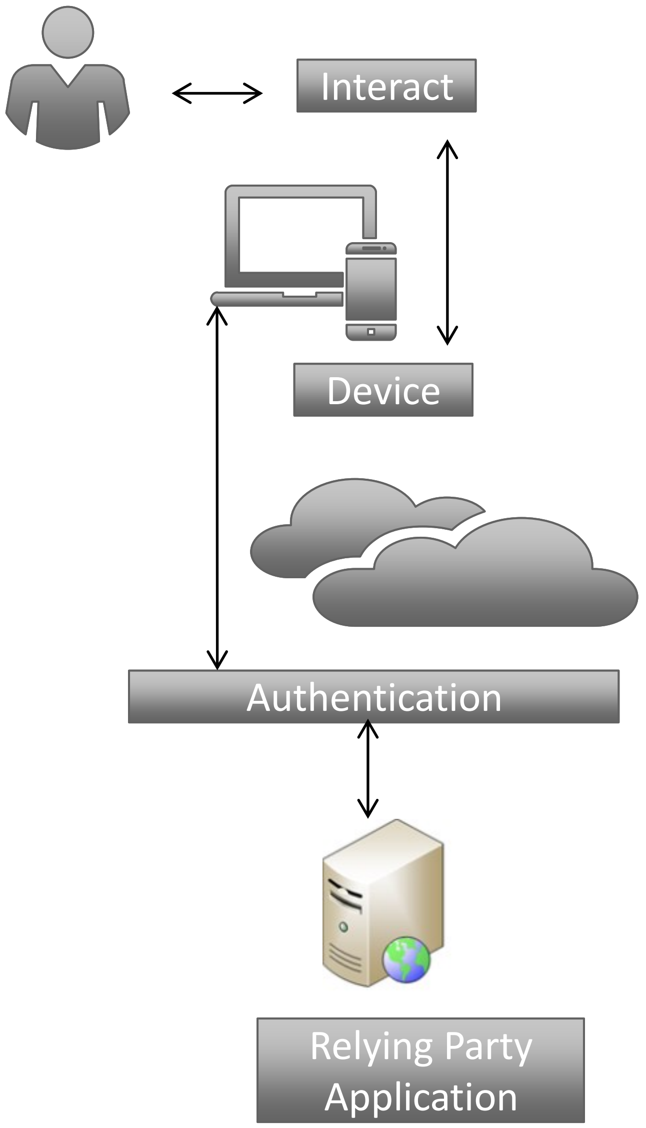
Q10/17 Activities

Work item	Subject/title
X.1250rev	Baseline capabilities for enhanced global identity management and interoperability
X.1251rev	Framework for user control of digital identity
X.gpwd	Threat Analysis and guidelines for securing password and password-less authentication solutions
X.oob-sa	Framework for out-of-band server authentication using mobile devices
X.pet_auth	Entity authentication service for pet animals using telebiometrics
X.srdidm	Security requirements for decentralized identity management systems using distributed ledger technology
X.tec-idms	Management and protection techniques for user data protection in distributed identity systems

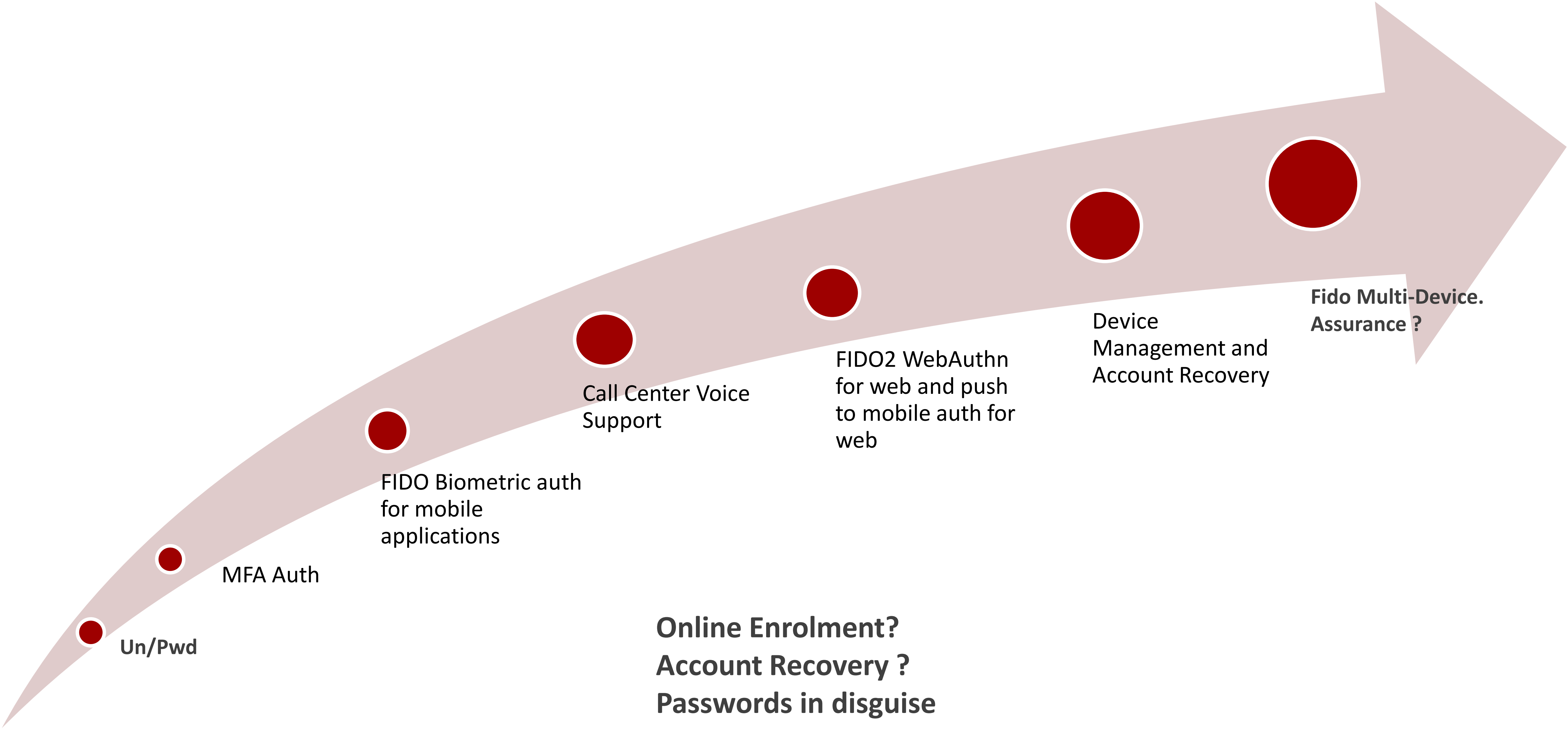
Legacy Authentication has a password problem

Historical Security Landscape

- **Passwords**
  - – Originally thought to secure access to data
  - – Stronger passwords did not solve the issue
- **Short-falls**
  - – Users often reuse passwords
  - – Many people never change passwords
  - – Passwords are often shared
  - – Passwords are easily cracked
  - – Are Easily Phished
- **Entering passwords is time consuming and expensive**
  - – Especially on Mobile Devices



Consumer Authentication is evolving



Un/Pwd

MFA Auth

FIDO Biometric auth for mobile applications

Call Center Voice Support

FIDO2 WebAuthn for web and push to mobile auth for web

Device Management and Account Recovery

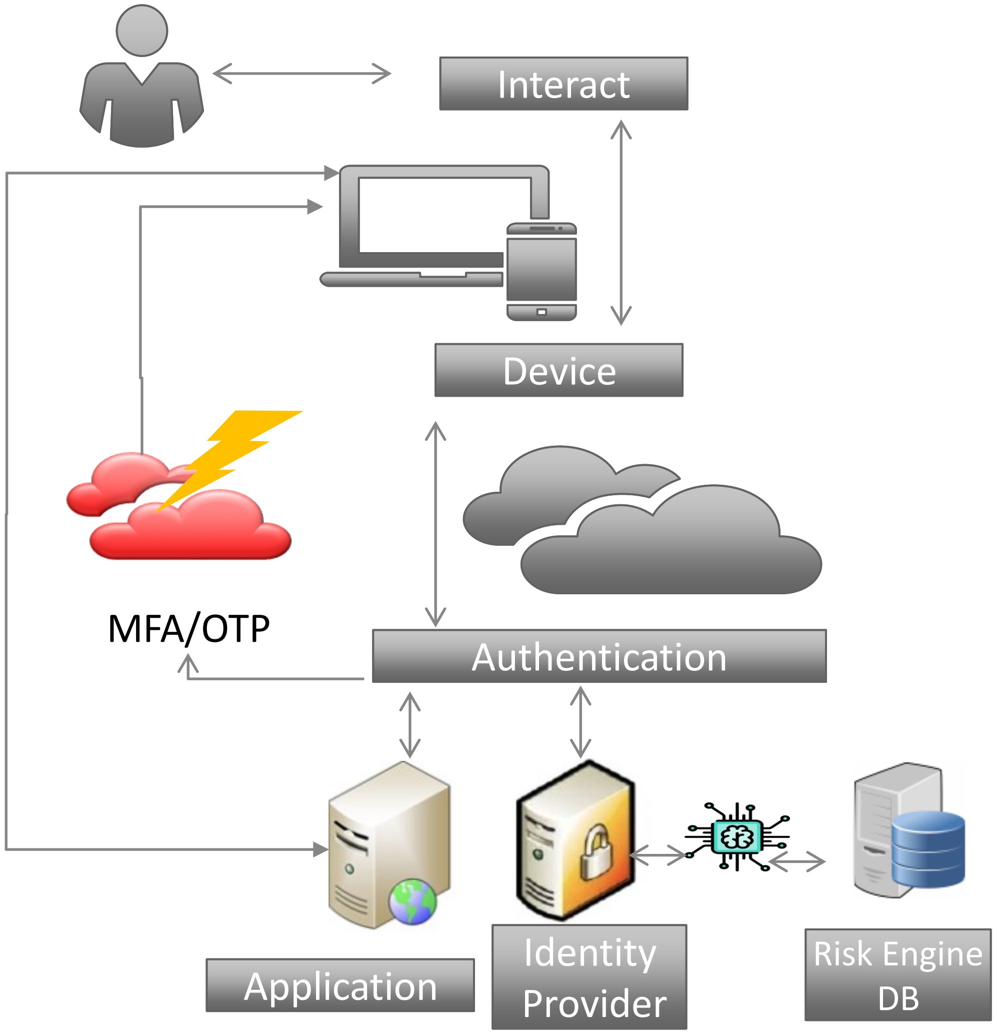
Fido Multi-Device. Assurance ?

Online Enrolment?
Account Recovery ?
Passwords in disguise

Multi Factor authentication with Risk Based Engines

Risk-based authentication for consumers, implemented in a manner that meets applications security risk tolerance

- The objective is to detect fraud and introduce fiction through identity Risk engine for threat adversaries while not impacting legitimate users
- Multi-Factor authentication enabled for high-risk use cases
- The Problem
  - MFA is not very secure and can be bypassed
- Account Recovery is still the weakest Path
- Step Up Authentication

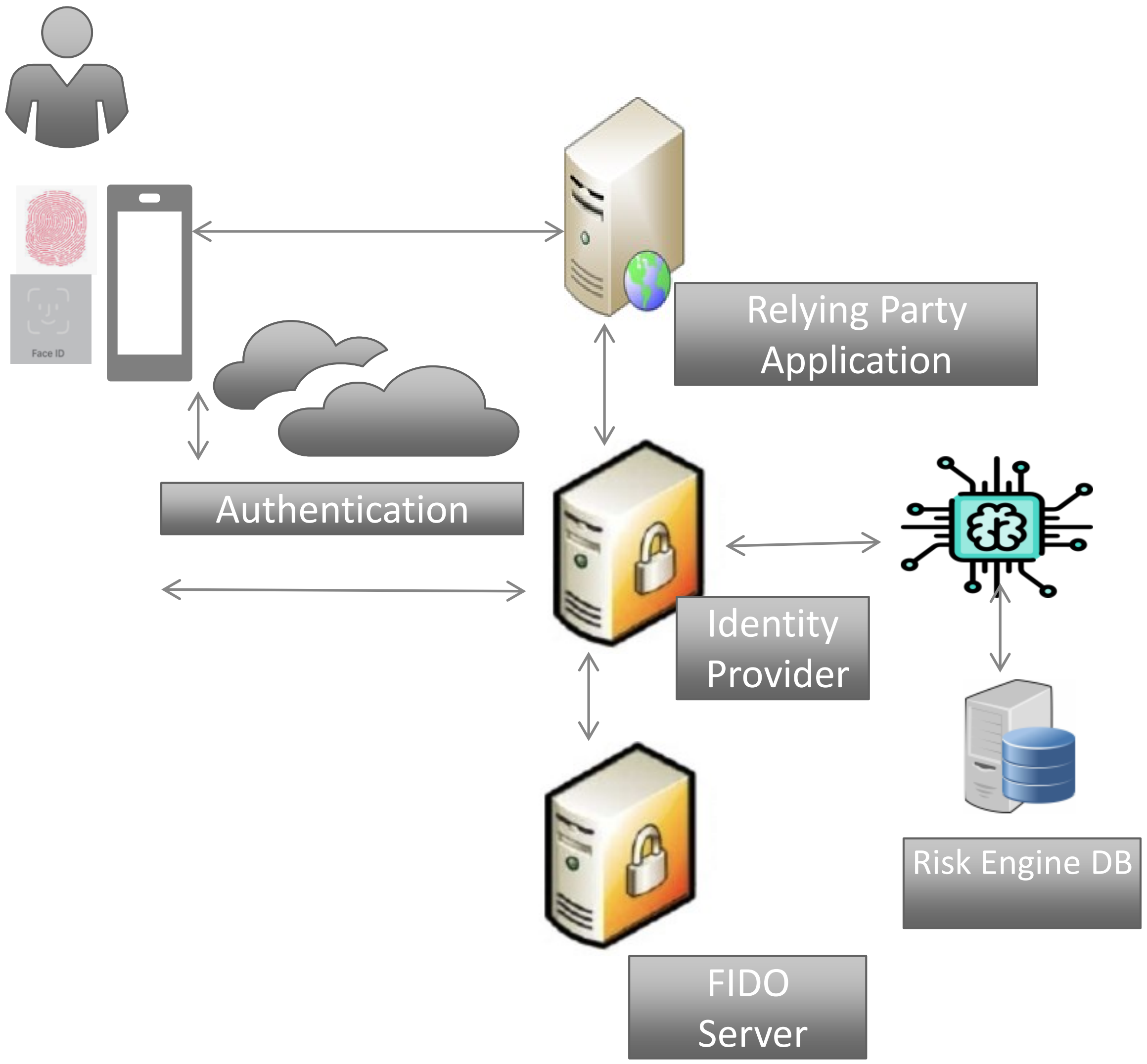


What is Passwordless Authentication

- Passwordless Authentictaion is a desired Goal or an Objective
- A method for verifying an entity without requiring one of the factors to be a password (or any other shared secret)
  - Solutions require application account identifier such as a user ID
  - Complete authentication process using a registered device (phone)
- Best if it relies on public-key cryptography
- Should not be confused with MFA
  - MFA adds a layer of security on top of password authentication
    - passwordless authentication must not include a shared secret
    - Zero Trust methods may be needed
  - Risk Engines help improve security
- Many Solutions are based on QR Codes
  - OASIS ESAT TC “Secure QR Code Authentication Version 1.0” to be published soon, https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=esat

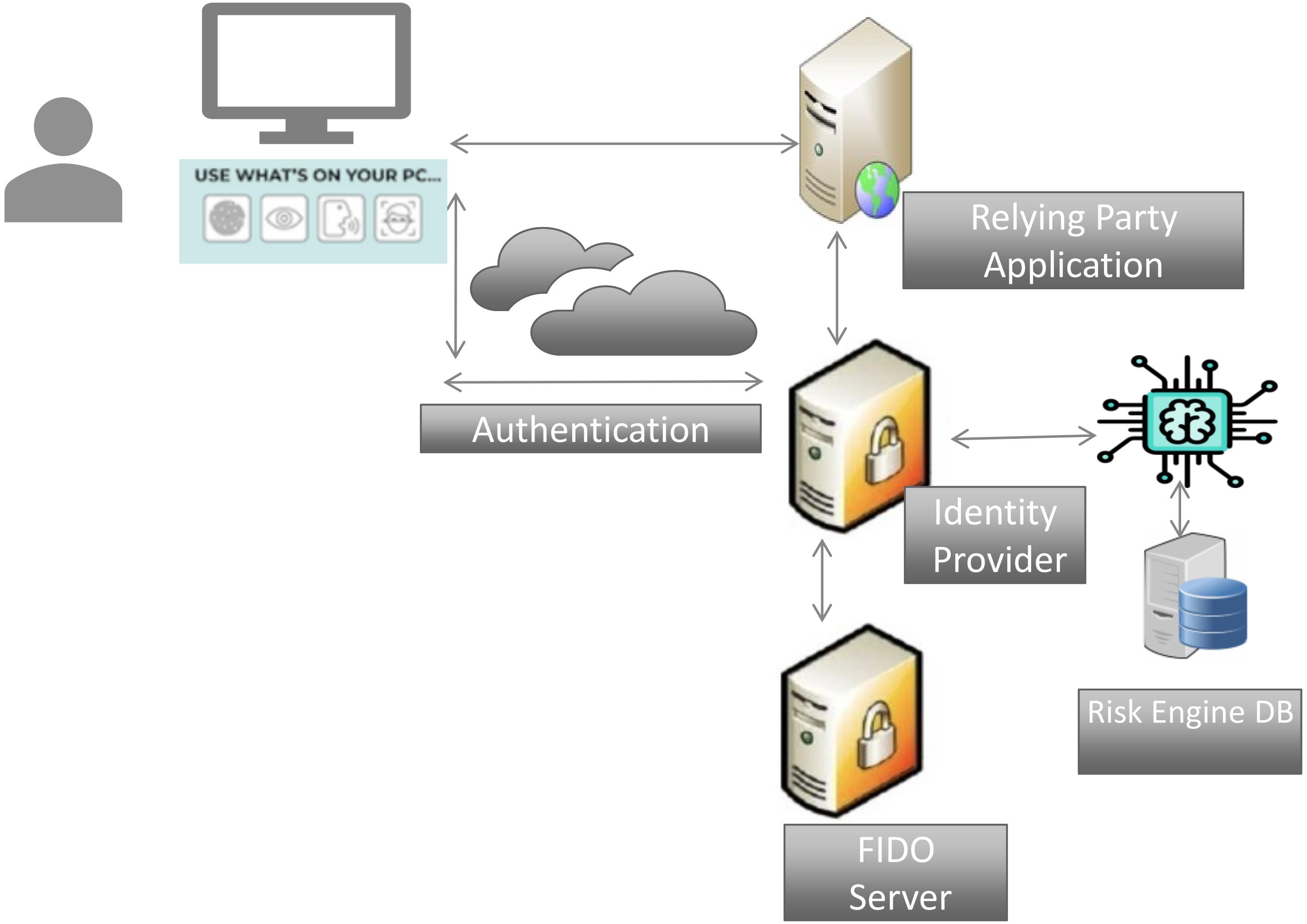
Biometric authentication on mobile based on FIDO standards

- **FIDO allows for**
  - Simpler, stronger authentication using public key cryptography
  - Single Gesture but provides 2 Factor Authentication
  - Phishing-resistant Authentication
  - Keys and biometrics stay on device
  - No server-side secrets
  - No 3rd Party protocol



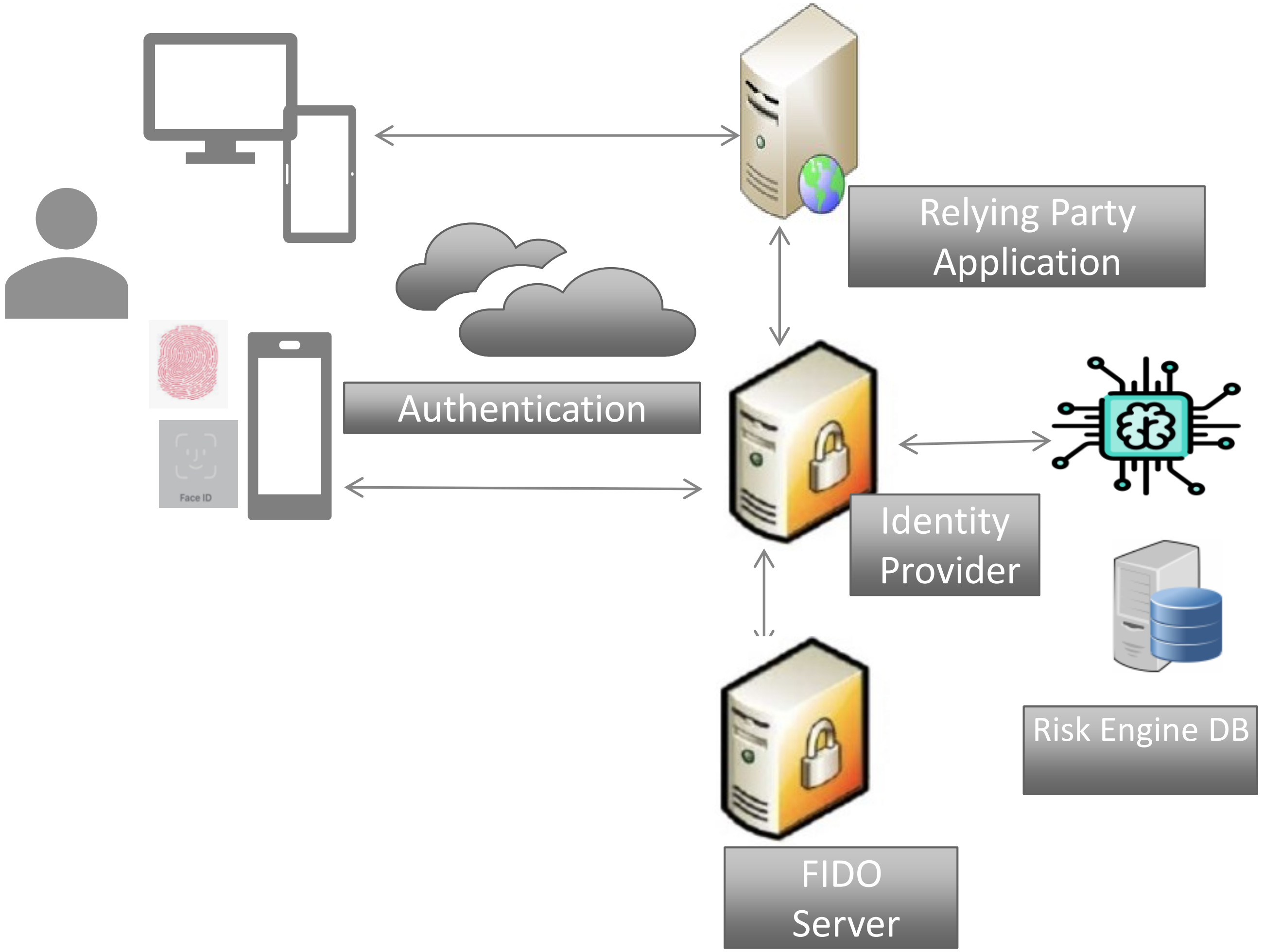
Biometric authentication for web using WebAuthn

- WebAuthn — A browser JS API that describes an interface or specification on how a browser should interact with the Trusted Platform module on the device
- Defines standards for creating and managing public key credentials used for authentication.
- W3C standard
- Sub spec of FIDO2



Push to mobile

- Provides passswordless authentication options
- Enables users to use the FIDO capabilities on mobile devices to authenticate to web
- Allows passwordless authentication to a larger group of users
- Can deploy a Risk Engine to provide resistance to phishing.
- Authentication context is transferred back to risk engine and factored into future interactions



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

Q&A