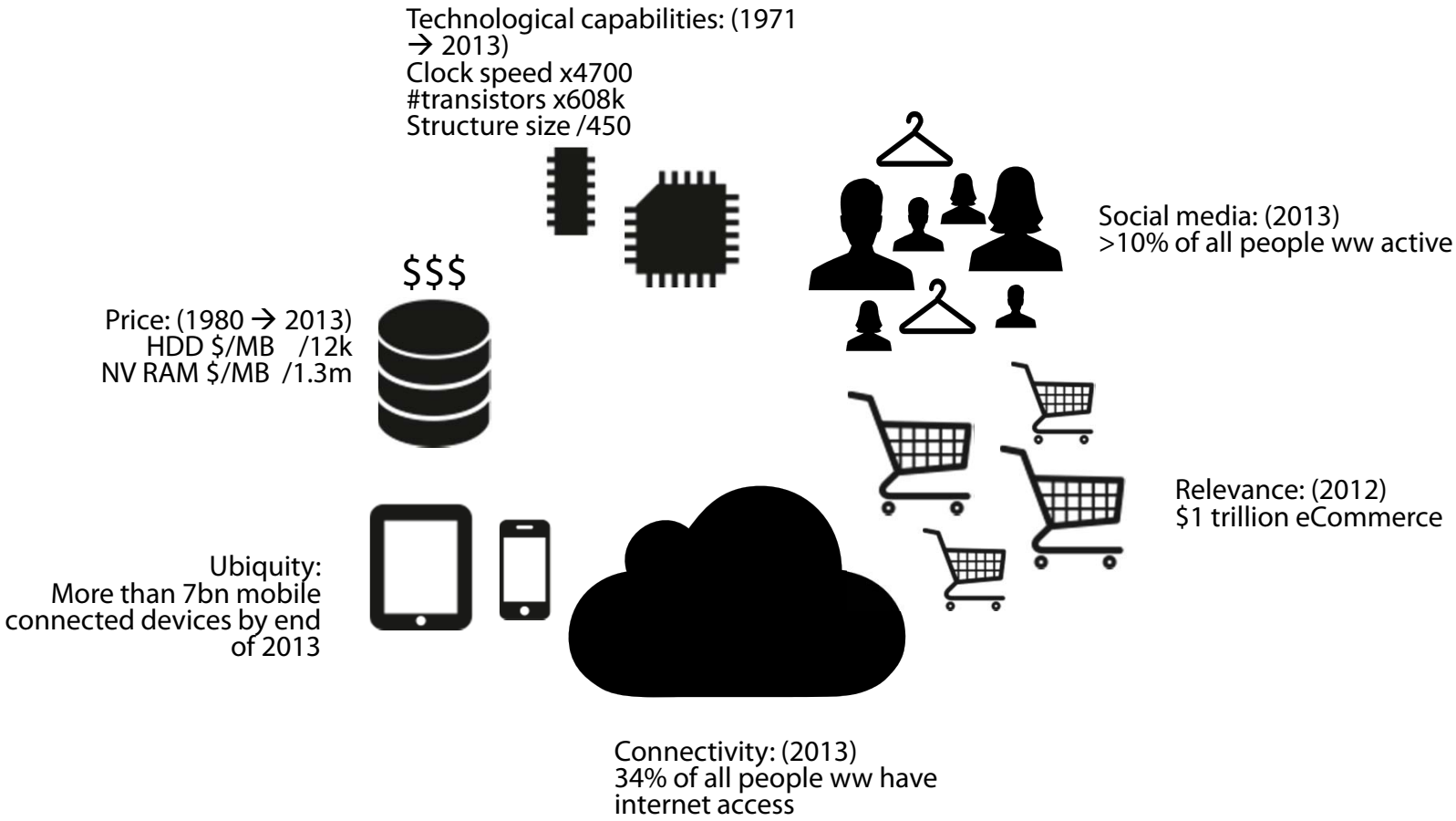
Scalable Authentication

Rolf Lindemann
Nok Nok Labs, Inc.

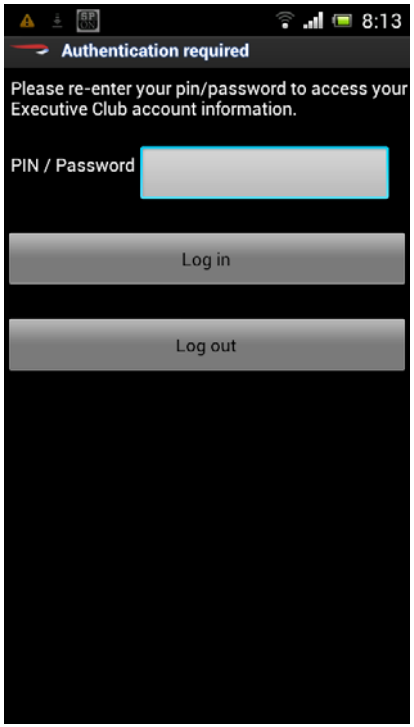
RSA CONFERENCE
EUROPE 2013

Session ID: ARCH-R07
Session Classification: Intermediate

IT Has Scaled

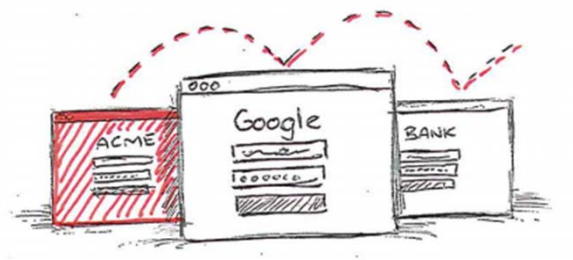


Authentication Hasn't



Passwords

Too many to remember, difficult to type,
and not secure



REUSED

PHISHED

KEYLOGGED

One Time Passcodes

Improve security, but not easy to use

SMS USABILITY

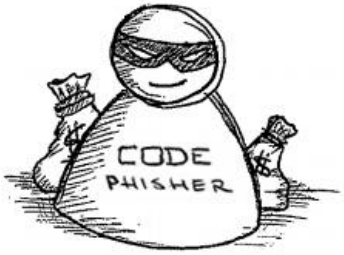
Coverage | Delay | Cost

DEVICE USABILITY

One per site | Fragile

USER EXPERIENCE

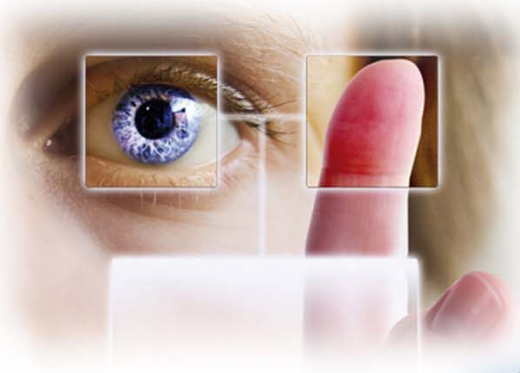
User confusion

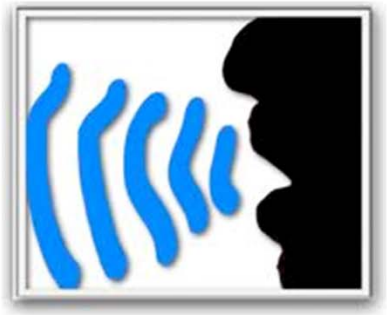


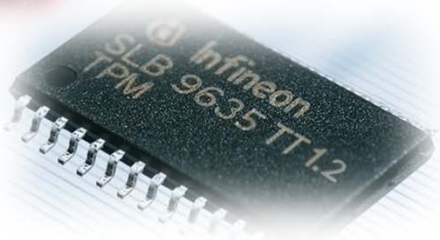
STILL PHISHABLE

Social engineering

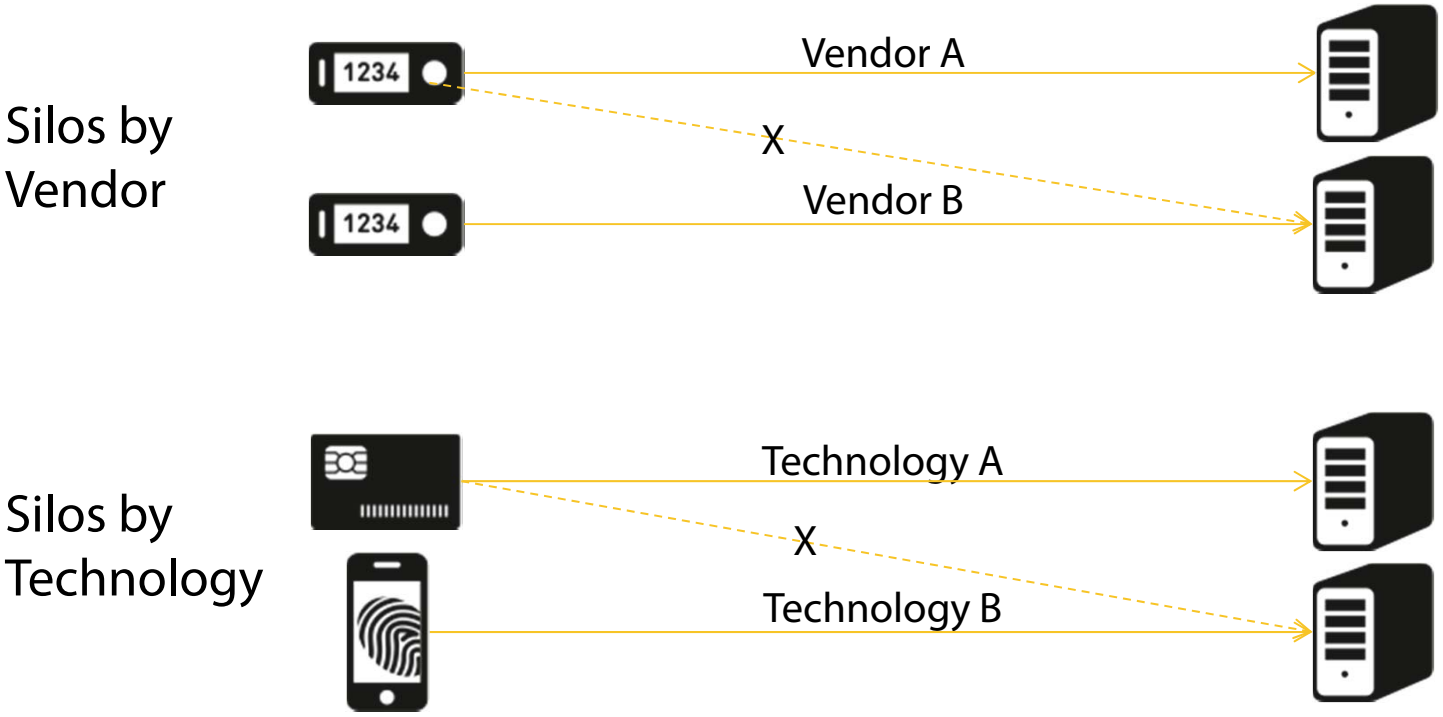
There are alternatives…







Implementation is the Challenge



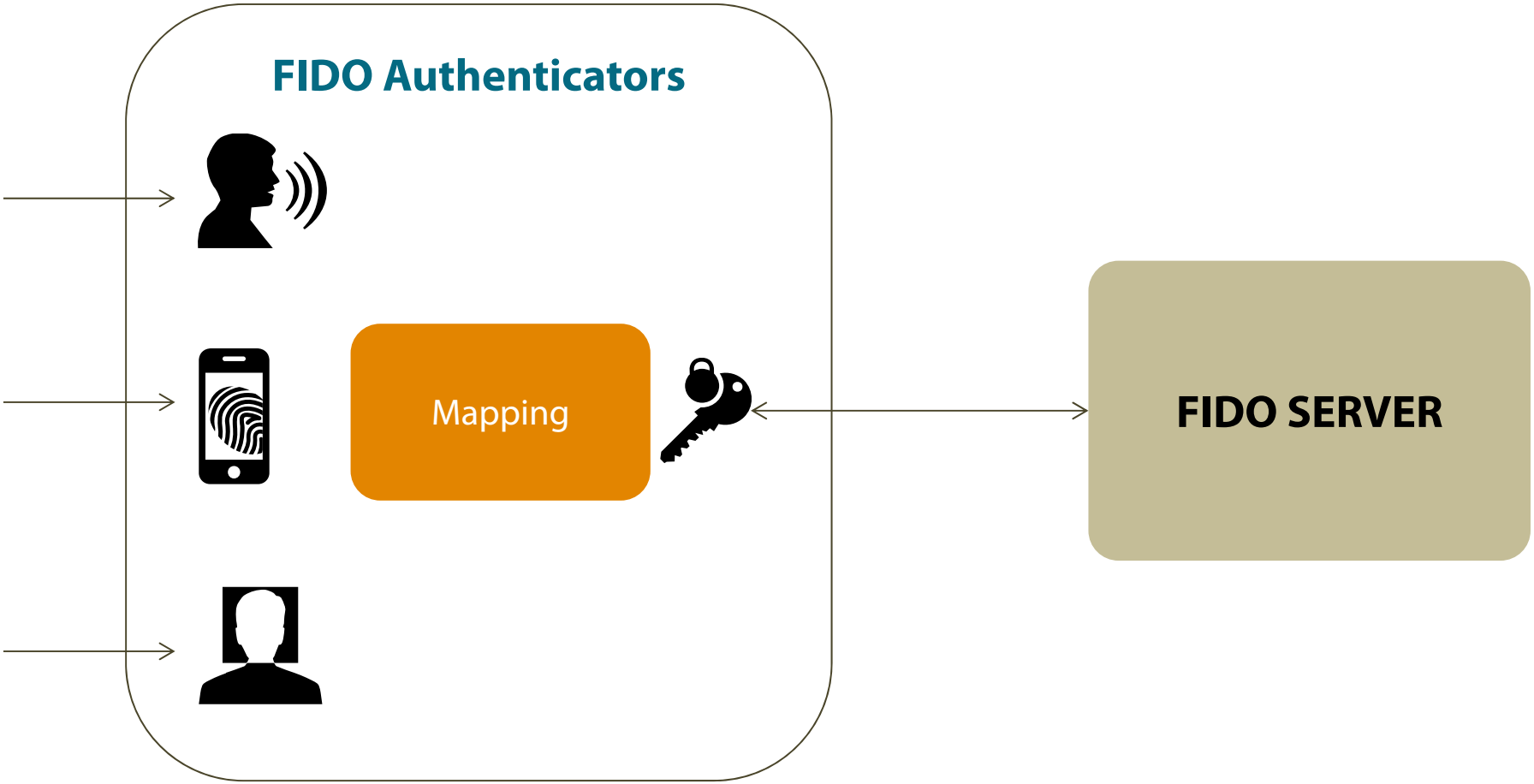
Each new authentication solution requires new HW, SW, and Infrastructure.

➔ We're building 'Silos' of authentication

FIDO Goals

- 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.

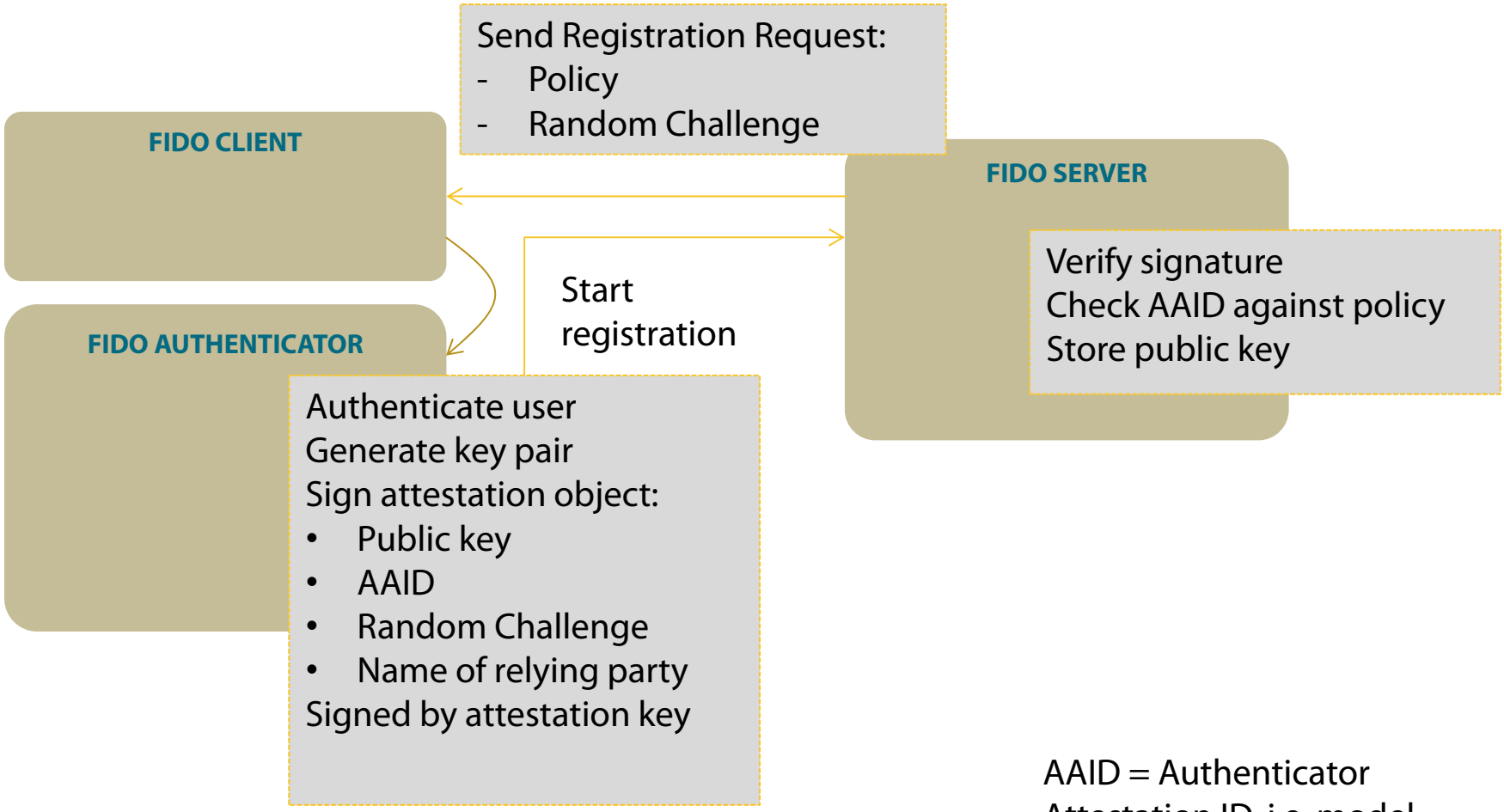
Abstract View



FIDO 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

Registration



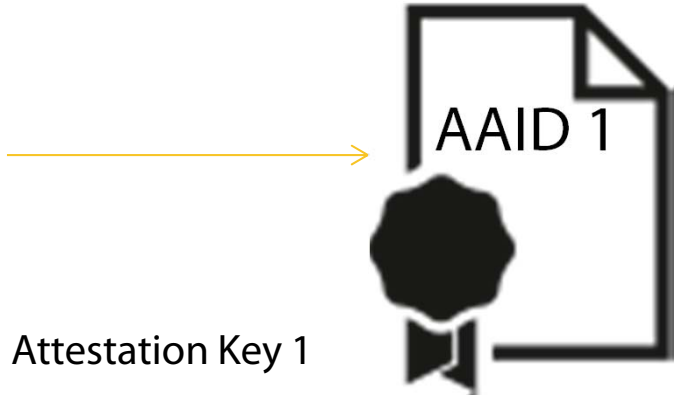
AAID = Authenticator Attestation ID, i.e. model

Regarding AAIDs

FIDO Authenticator

Using HW based crypto

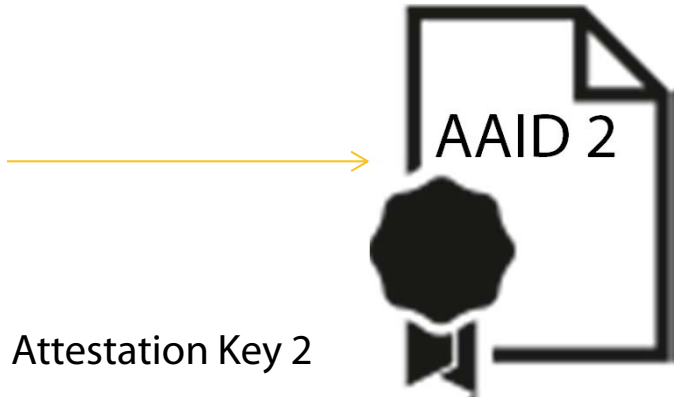
Based on FP Sensor X



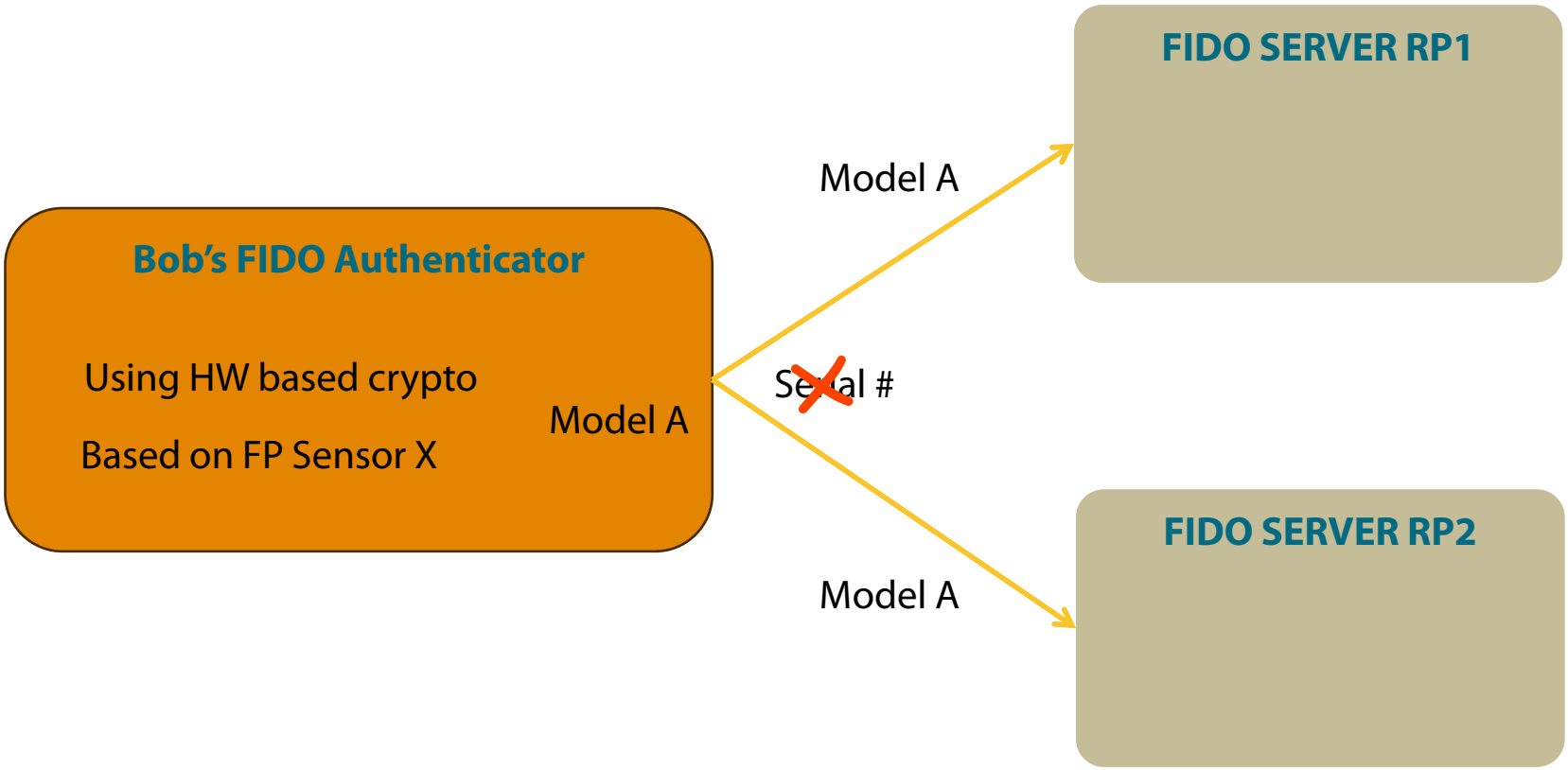
FIDO Authenticator

Pure SW based implementation

Based on Face Recognition alg. Y



Privacy & Attestation



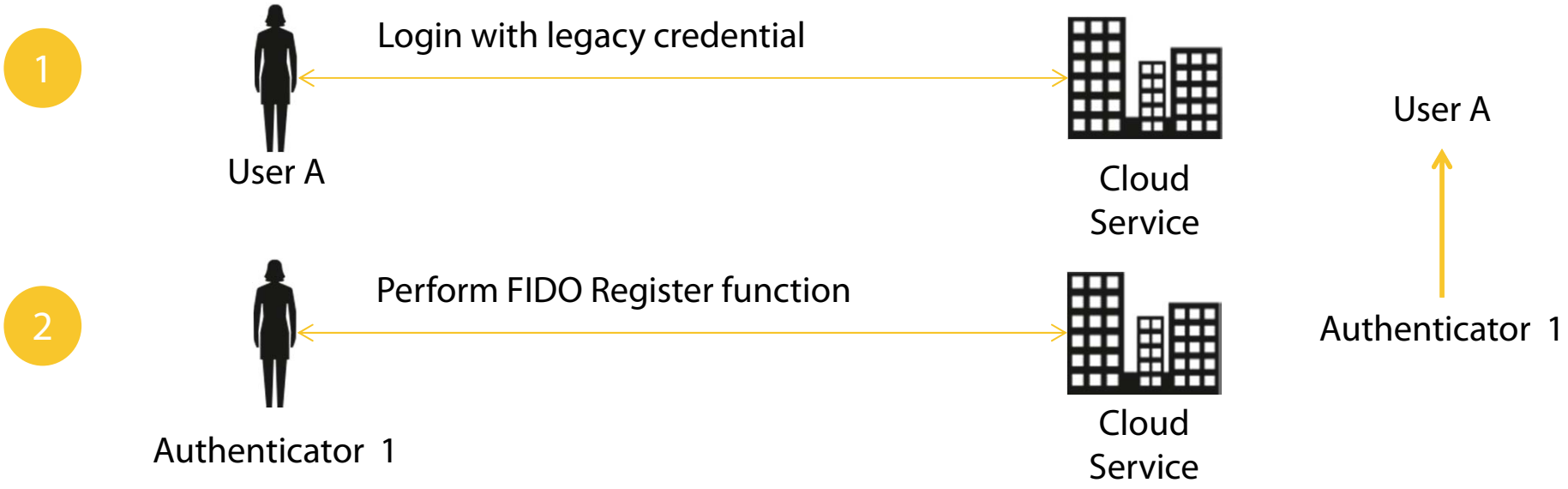
Authenticator Meta-Data

File available to FIDO Server with Authenticator descriptions

- AAID as an index
- Attestation trust anchor
- Implements Secure Display
- Key Protection
- …

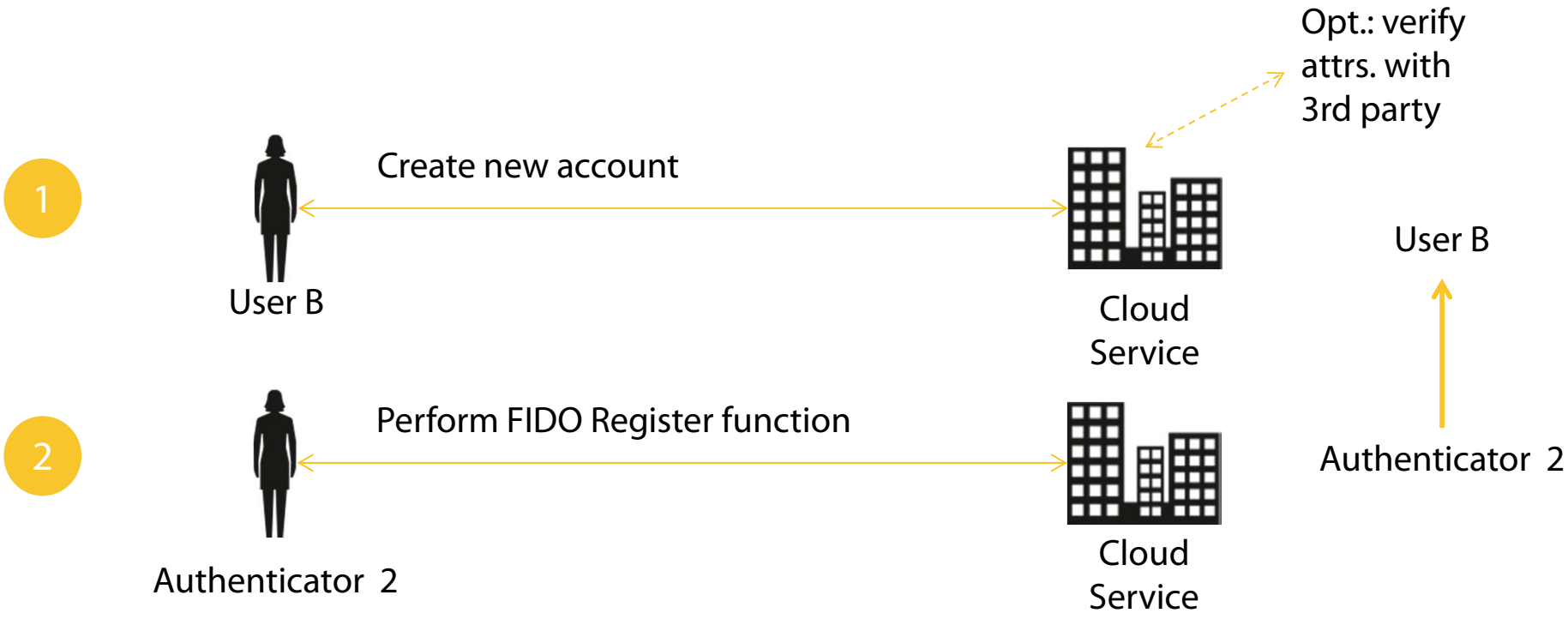
Binding Authenticator to User

Case A: Existing User

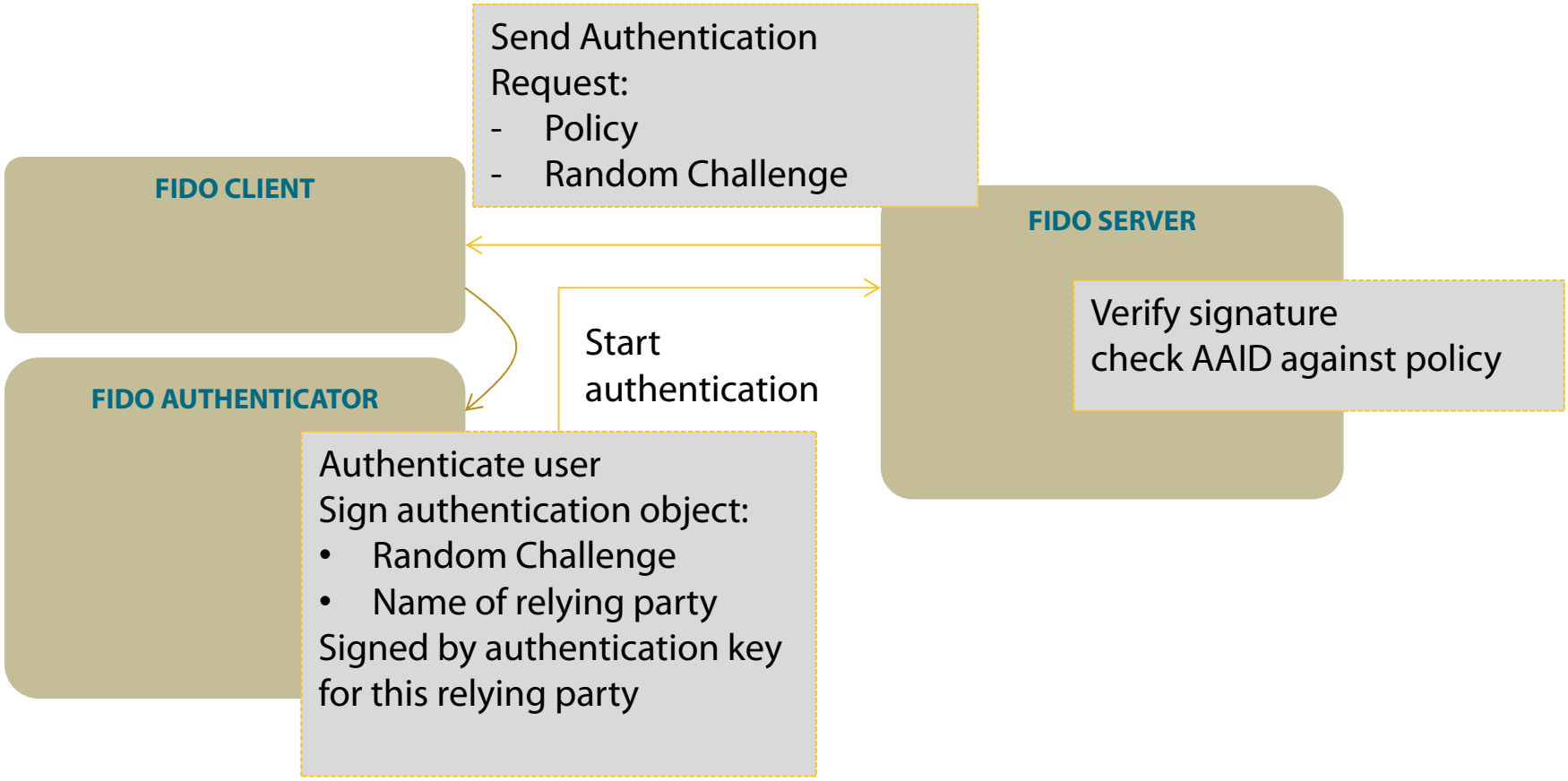


Binding Authenticator to User

Case B: New User

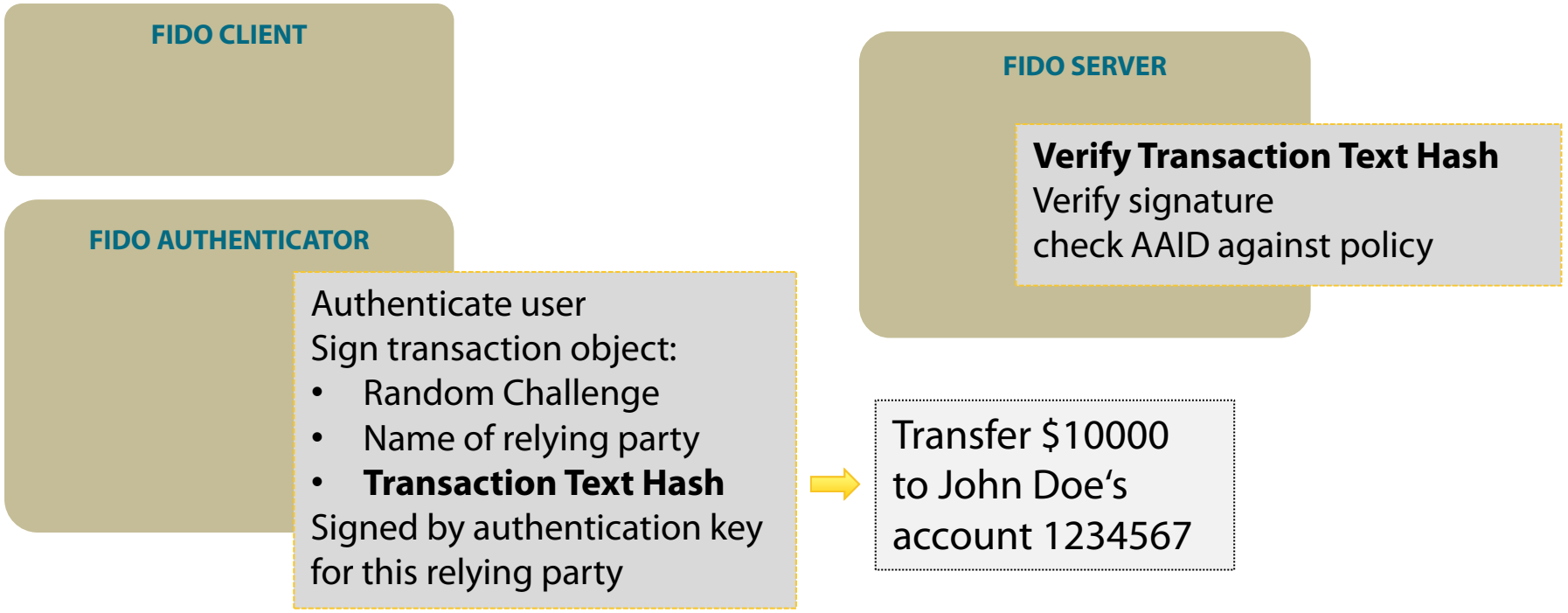


Authentication

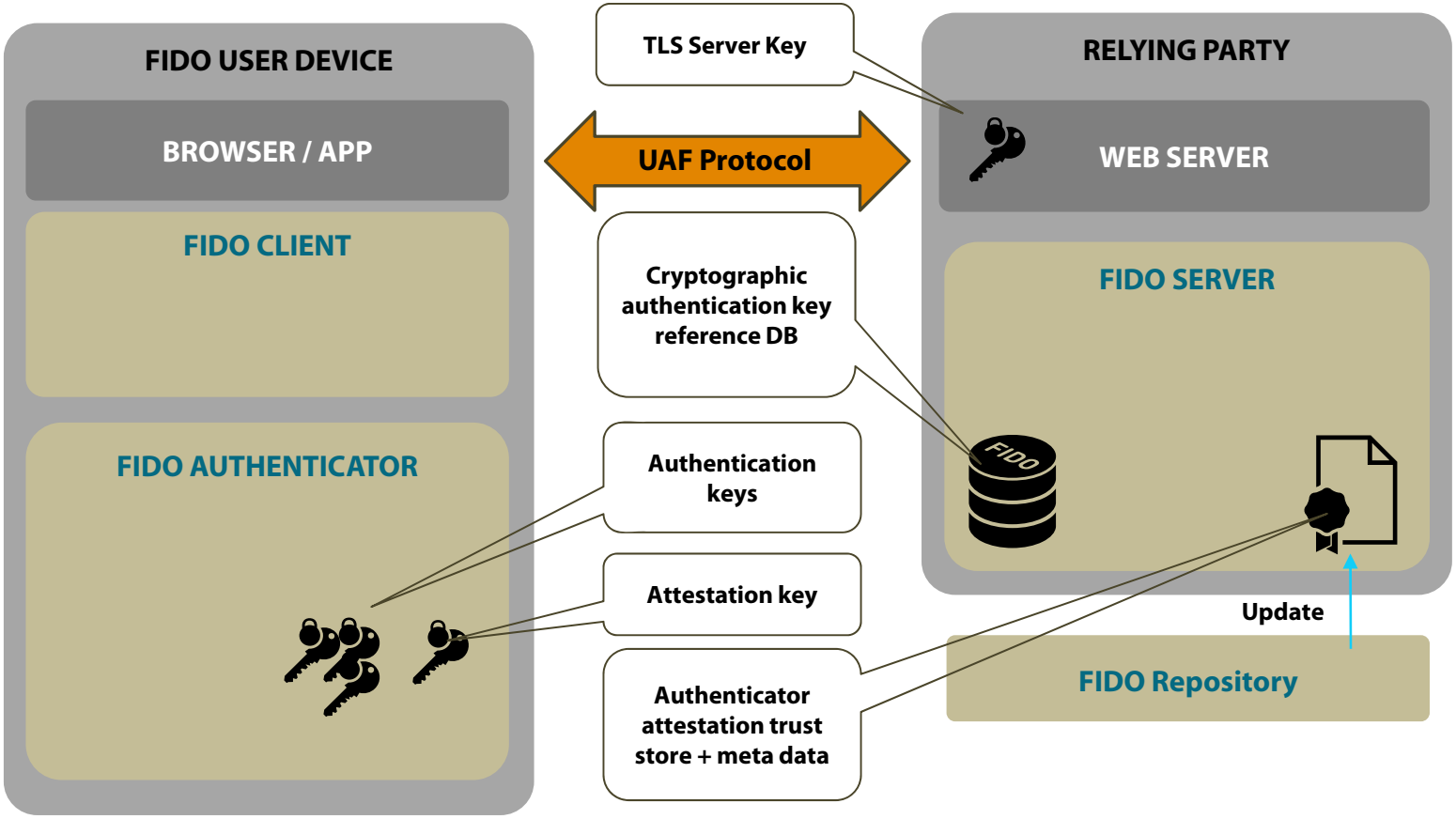


Transaction Confirmation

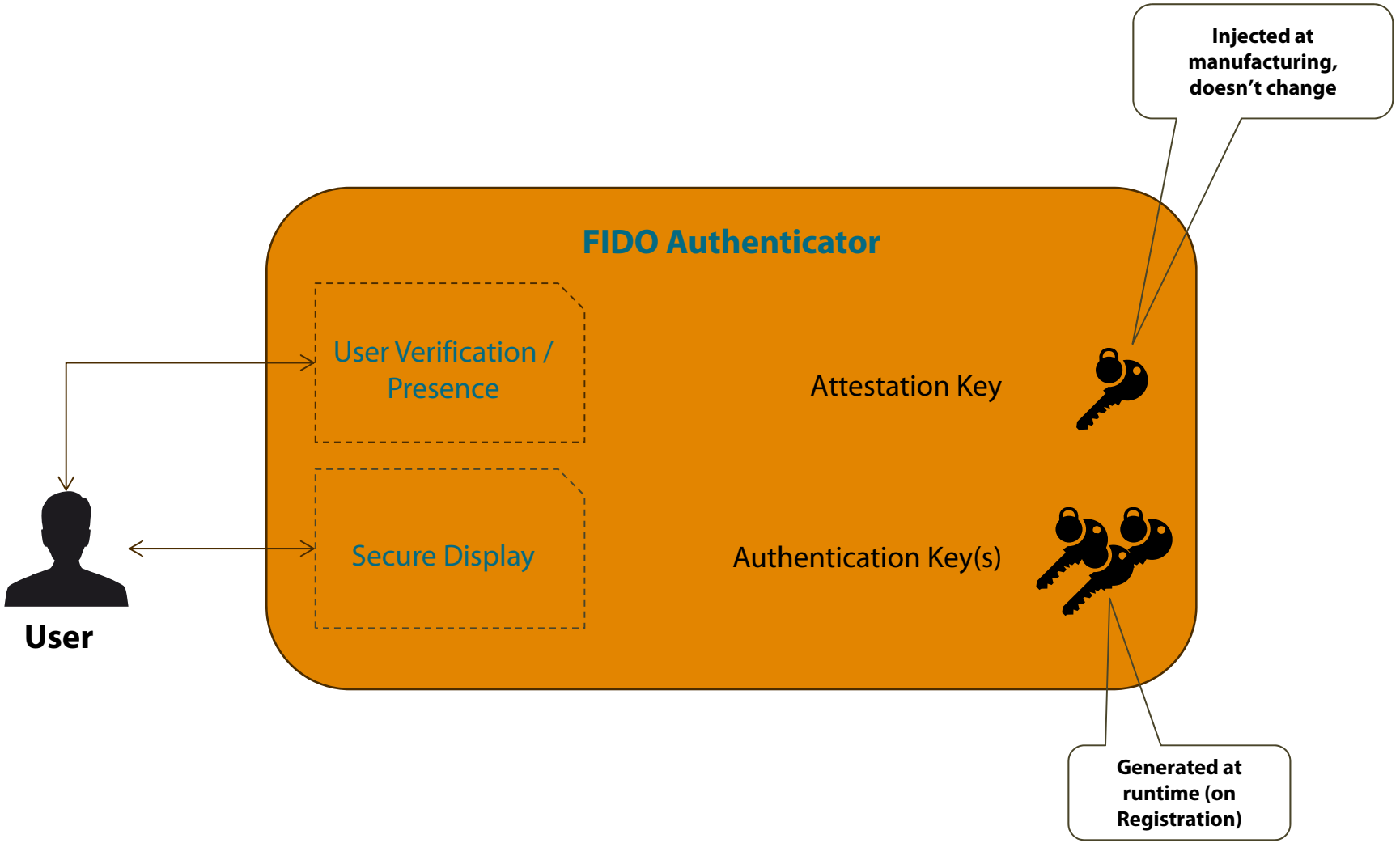
Like Authentication, but Authenticator displays Transaction Text



FIDO Building Blocks

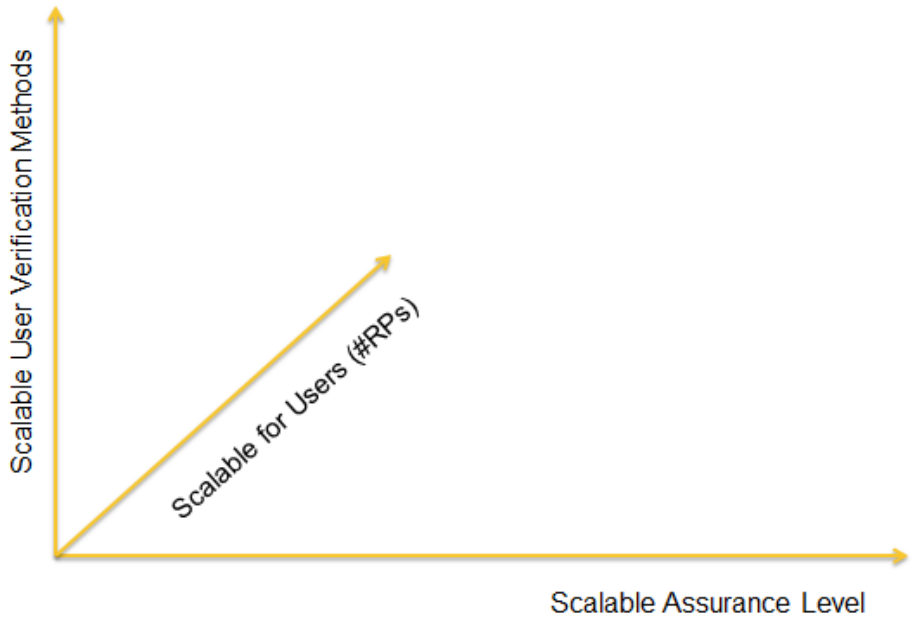


The Authenticator Concept



Scalability of Authentication

- Scalable for Users
- Scalable User Verification Methods
- Scalable Assurance Level



Scalable for Users

Overall complexity doesn't grow with the number of relying parties:

- Choosing & remembering one password per RP is not scalable
- Carrying one (dedicated) OTP token or smart card per RP is not scalable
- In FIDO, the Authenticator maintains one key per RP. This scales & avoid a global correlation handle.

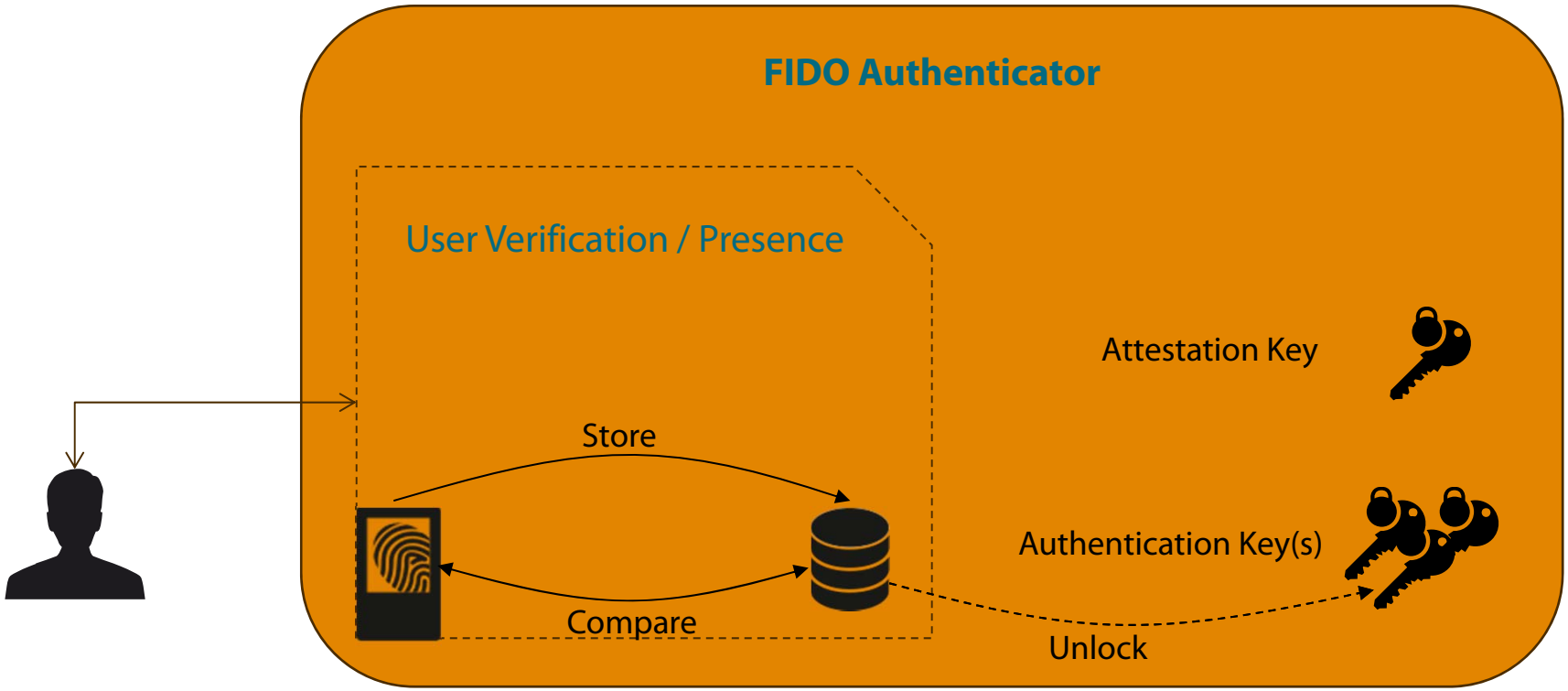
Scalable User Verification Methods

Various User Verification Methods can be implemented without updating server software

- Various cryptographic hardware, e.g. smart cards, USB tokens, …
- All kinds of biometrics
  - Fingerprints
  - Face recognition
  - Typing behavior
  - Gait
  - Cardiac rhythm recognition and more…
- Gadget presence, e.g. smart watch, …

Client Side Biometrics

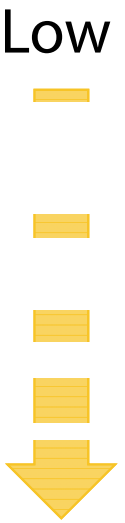
Various User Verification Methods can be implemented without updating server software



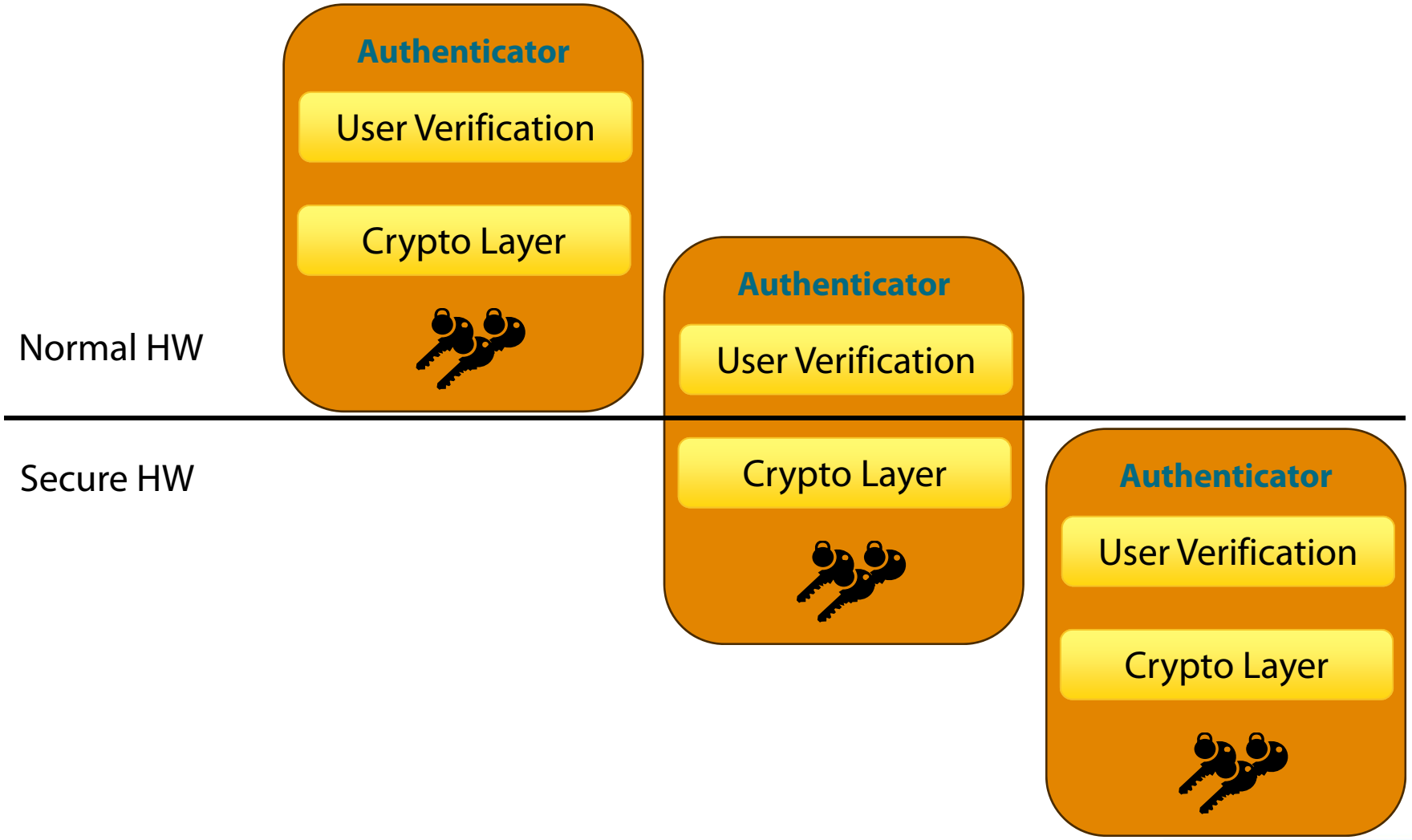
Scalable Security

Broad range of assurance levels

- Login to online account
- Change shipping address
- Transfer $10,000 to Account 1234

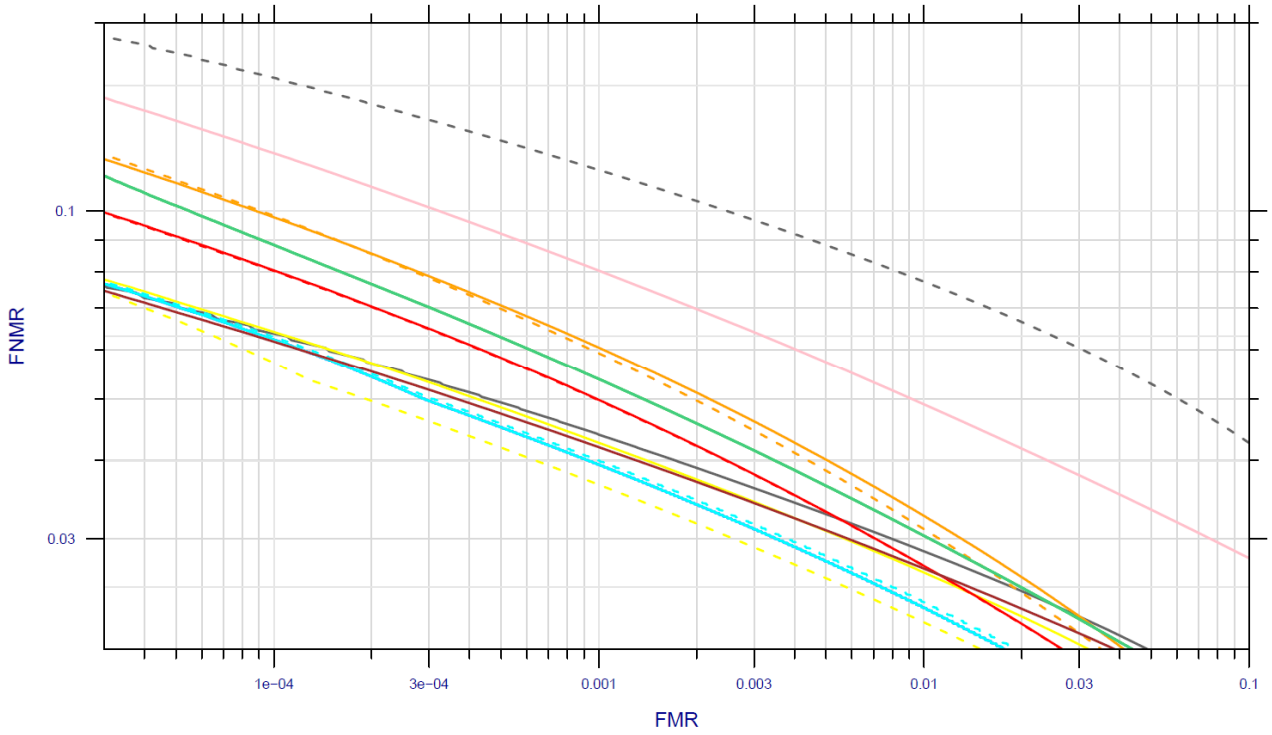


Scalable Security (2)



Scalable Security (3)

Scale the accuracy of the user verification algorithm, e.g. better finger print sensor/algorithm, longer PINs



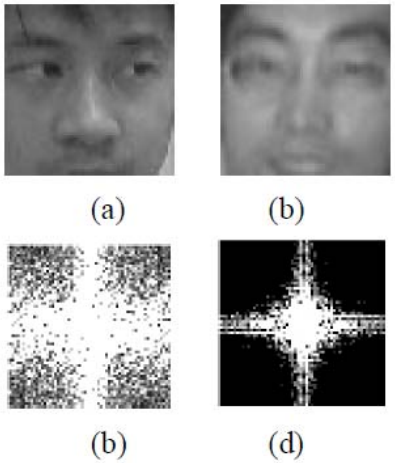
Source: NIST Interagency Report 7477

Scalable Security (4)

Scale security by adding enhanced anti spoofing methods, e.g. enhanced liveness detection for face recognition.

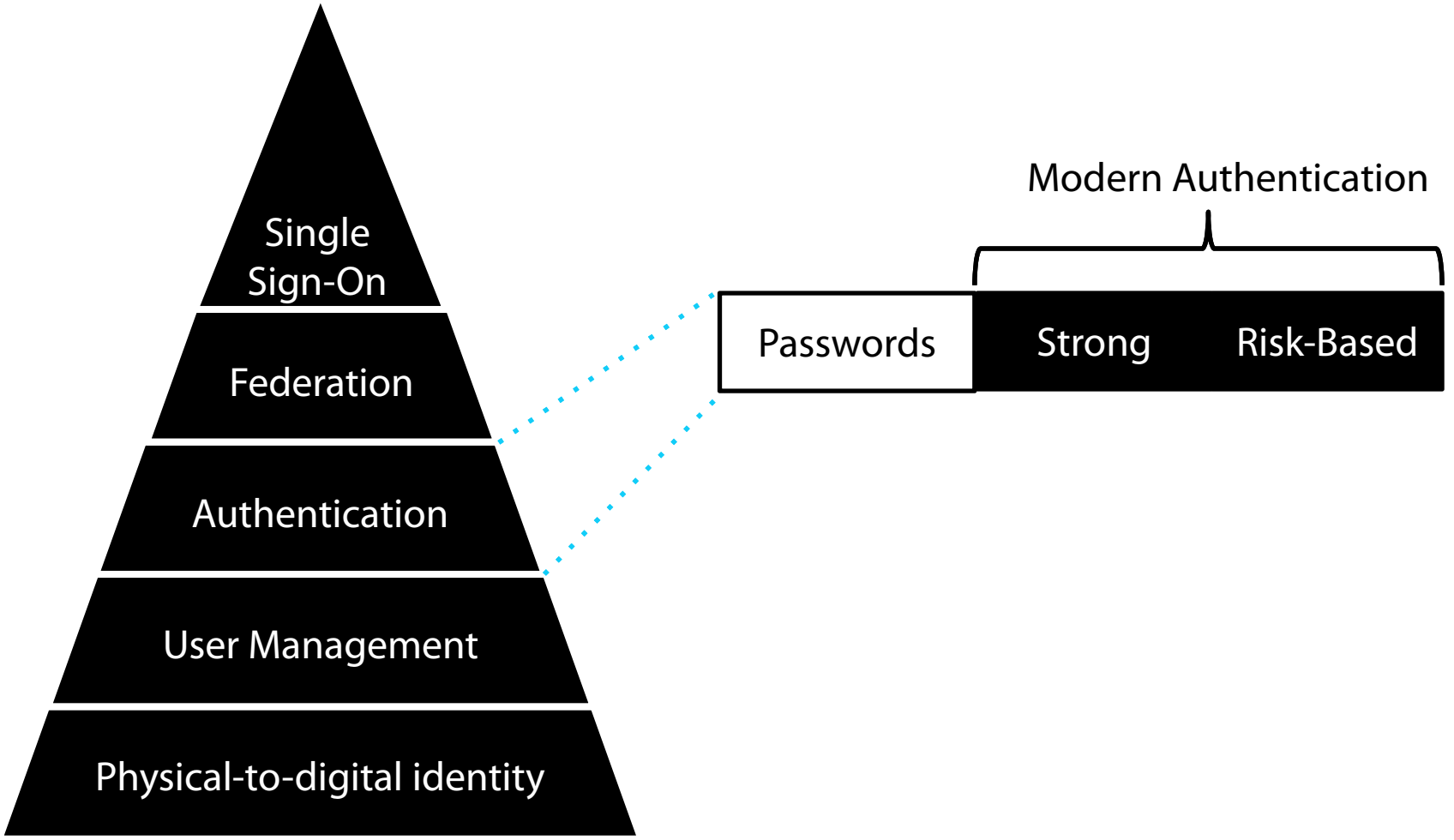
Or by requiring PIN entry.

Source: Liveness Detection for Face Recognition

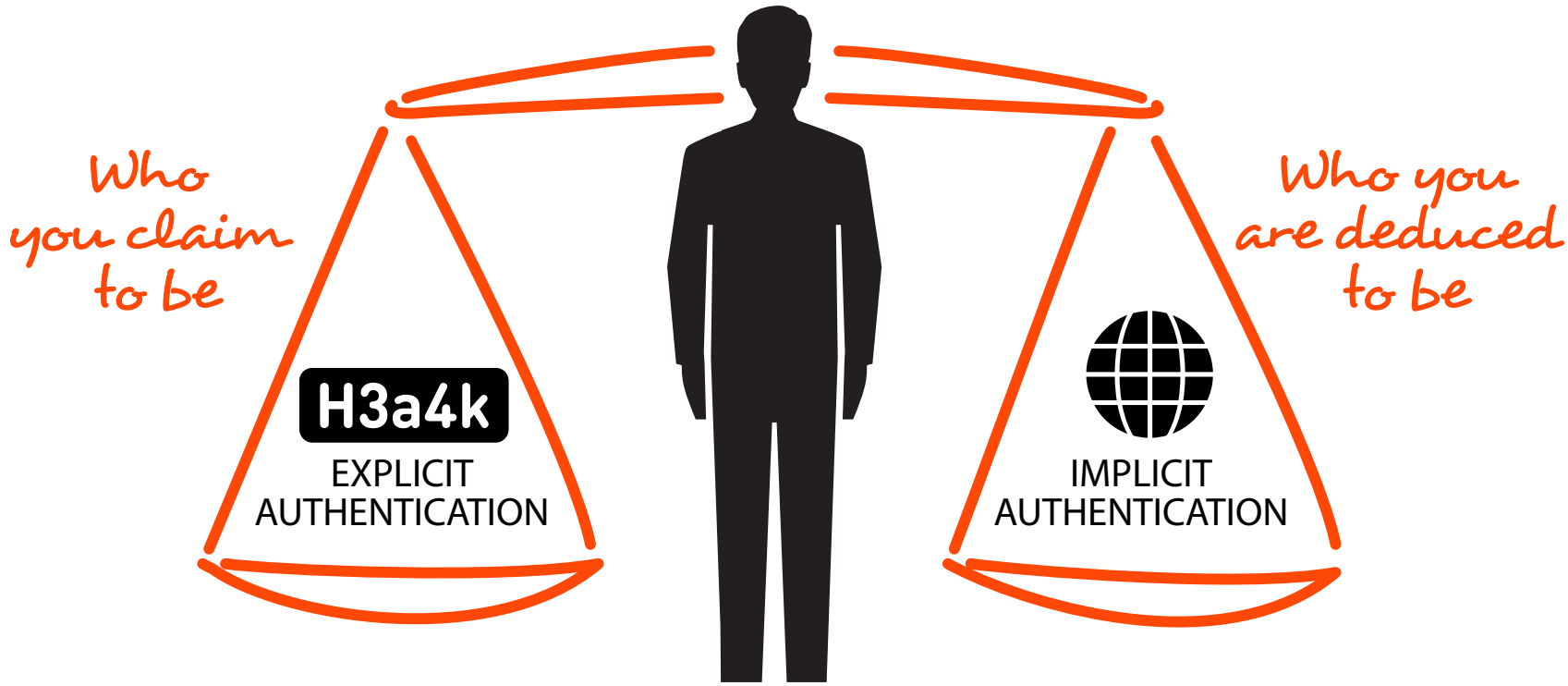


Source: Live Face Detection Based on the Analysis of Fourier Spectra

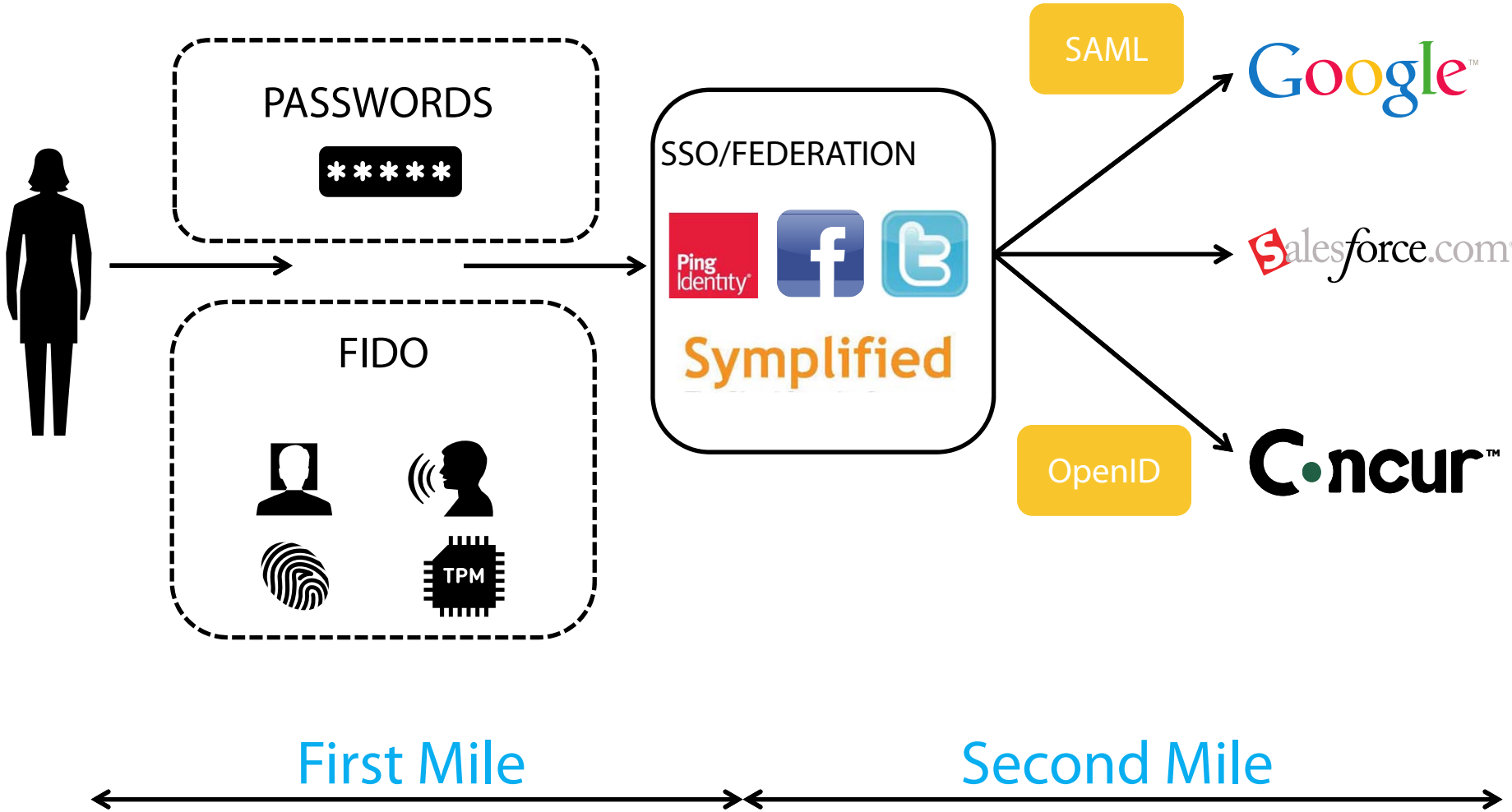
FIDO and IAM


Single Sign-On
Federation
Authentication
User Management
Physical-to-digital identity
Modern Authentication
Passwords
Strong
Risk-Based

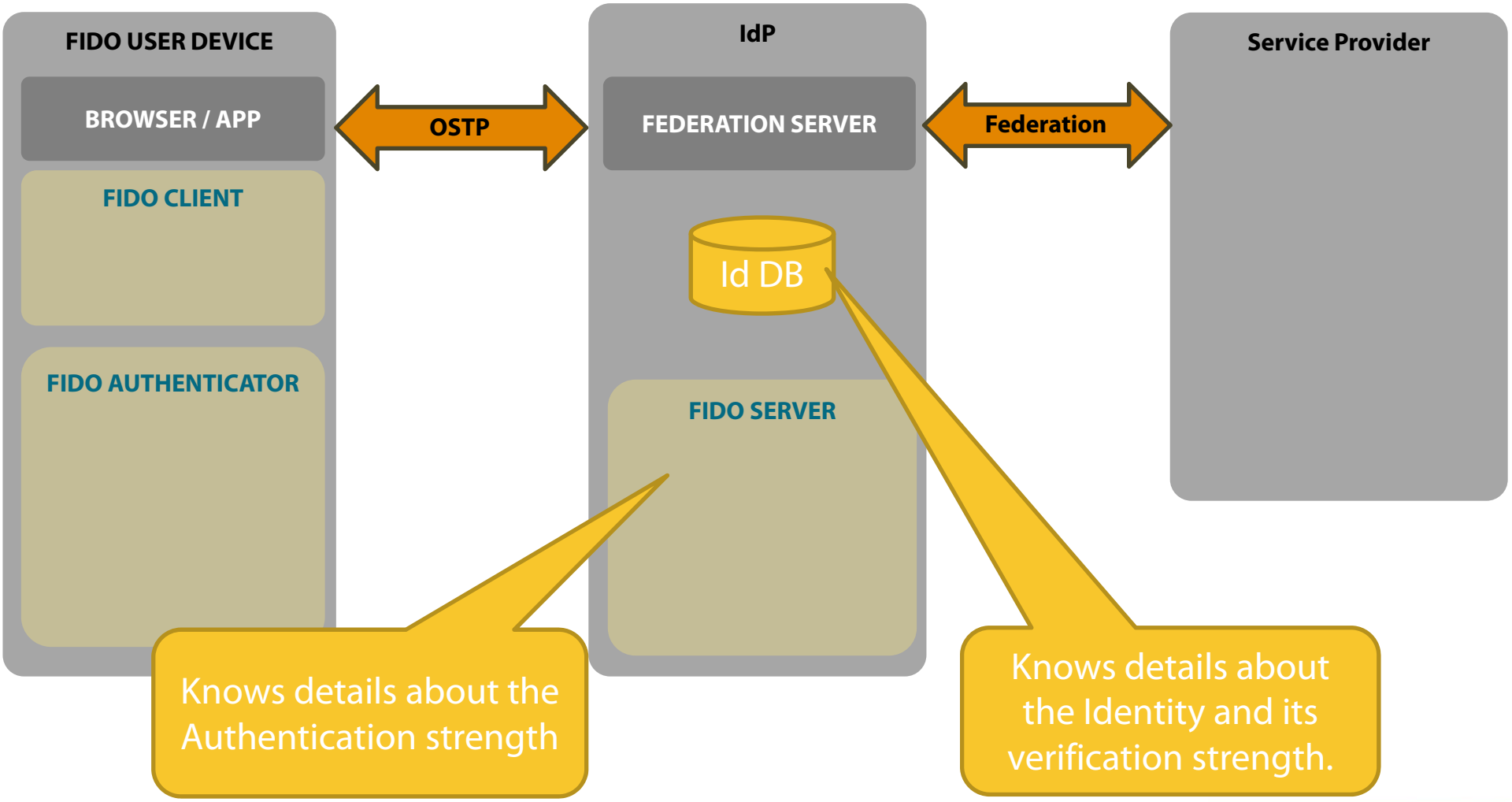
Complementary



FIDO and Federation



FIDO and Federation



FIDO Today

- **Technical Working Groups active**
  - Public Spec Drafts early 2014
  - Early Pilots late 2013
  - Complement existing standards & efforts
    - NSTIC/Federation: OpenID, SAML etc.
- **FIDO Alliance membership is growing**
  - Members set requirements and design the technology
    - Internet Services
    - Client Platform Owners
    - Device & Component Vendors

info@fidoalliance.org | www.fidoalliance.org

FIDO Alliance Members

FOUNDERS

PayPal
lenovo FOR THOSE WHO DO.
Infineon
AGNITIO
validity
Nok Nok LABS

AFTER FEB. 2013

eyeLock
NXP
Allweb Technologies
CROCUS Technology Blossoming future
Google
ENTERSEKT
Egistec
eyeLock
company AKTIV
GO-Trust
BlackBerry
SurePass id
CHECK PROTECT
DIAMOND FORTRESS TECHNOLOGIES
BIO-key Revolutionizing Authentication
OBERTHUR TECHNOLOGIES
CrucialTec
FINGERPRINTS
LG
yubico the key to the cloud
AUTHENTIFY
insyndia imagine. ignite. inspire.
findBIOMETRICS Global Identity Management
ARXAN Protecting the App Economy
FingerQ www.fingerq.com
Ping Identity
MasterCard
MedImpact Delivering · Flexible · Choice
IT'S ME! SECURITY
SECURE KEY
toopher
certus technology systems
Facebanx
CLOUDSECURITY CORPORATION

What's the benefit

For Users

- Easy to use local auth options
- No more worrying about passwords
- Feel safer on the Internet

For Internet Services

- Greatly improved security, Increased user engagement
- User brings own device
- Build server once: leverage all auth methods

For Vendors

- Standardization ignites market
- Solve fragmentation issues with unified framework

Backup

#RSAC

RSA CONFERENCE EUROPE 2013

Summary

- Passwords don't work
- Current alternatives don't scale
- FIDO Alliance works on an open specification separating user verification method from cryptographic authentication protocol
- With that protocol
  - relying parties can define policy for risk appropriate authentication
  - relying parties know the authenticator model and its characteristics through attestation
  - adoption of new authentication methods will be significantly easier

Thank you!

Rolf Lindemann

Nok Nok Labs, Inc.

rolf@noknok.com

www.noknok.com

www.fidoalliance.org

info@fidoalliance.org

#RSAC

RSA CONFERENCE EUROPE 2013