TEMET
end-to-end IT security

The Future of Strong Authentication

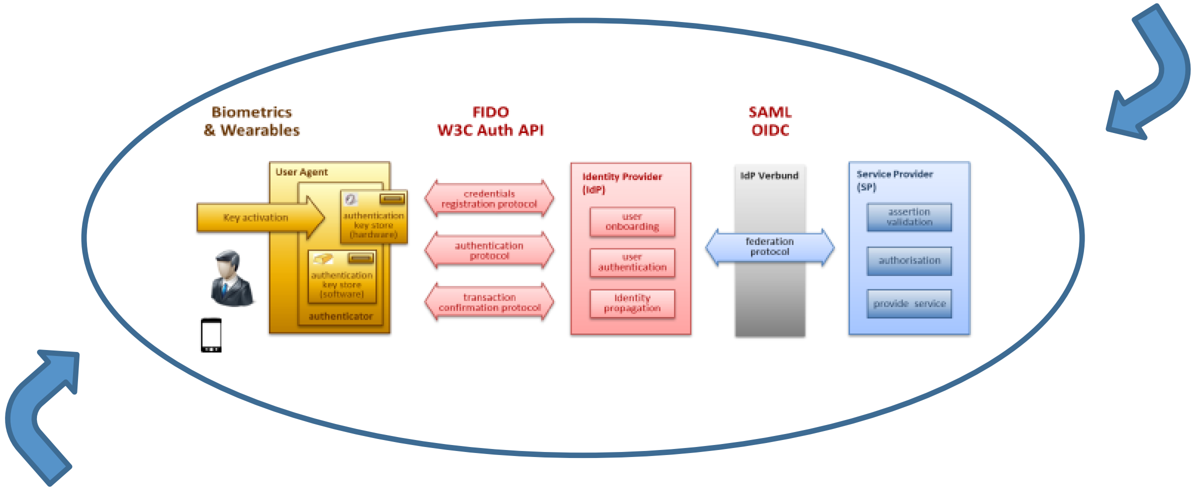
@TEMET 2018

Thomas Kessler | Security Architect | Temet

11.06.2018

Agenda

- It’s time for a change!
- A 3-Tier Model for Future Authentication
- Identity Providers (IdP and Federation



- Trends in Authentication and Key Activation
- Now, what does this mean to me?

Speaker Information

Thomas Kessler

Dipl. Physiker ETH
MAS ZFH in Business Administration

Security Architect, Partner
Works in Information Security since 1991

Core Competencies
Security Architecture and Strategy
Strong Authentiction
Identity Provider (IdP)

Contact
Tel: +41 79 508 25 43
E-Mail: thomas.kessler@temet.ch

It’s Time for a Change (1/3)

- So far, most applications still rely on passwords
  - Most applications with higher security requirements just add another (one-time) password (as for example implemented with mTAN or an OTP generator)
  - Passwords can be copied and misused, and even one-time passwords are vulnerable to phishing or Trojan horse attacks to some degree

- There is a growing need for Strong Authentication due to cybersecurity threats and regulation
  - The Second Payment Services Directive (PSD2) Regulatory Technical Standard (RTS) requires every payment service provider to implement strong customer authentication (SCA)
  - SCA must be based on two or more elements categorised as knowledge, possession and inherence and shall result in the generation of an authentication code (Article 4)
  - The authentication code must be linked to the amount and the payee (Article 5)
  - Breach of one of the elements must not compromise the other elements (Article 9)

It’s Time for a Change (2/3)

- mTAN is facing growing opposition and will eventually loose its predominant position to a plethora of C/R Apps ready to take over
  - There are various approaches to isolate C/R Apps from the OS (and its vulnerabilities)
  - C/R Apps may be used out-of-band or as an SDK integrated with Business Apps
  - Hardware tokens will never really make it for B2C authentication (except for E-Banking)
- Service Providers are getting tired of…
  - … client onboarding and attribute collection;
  - … managing credentials for every client;
  - … implementing authentication servers;
  - … providing support for such commodity functionality.

It’s Time for a Change (3/3)

These factors are driving an architectural shift:

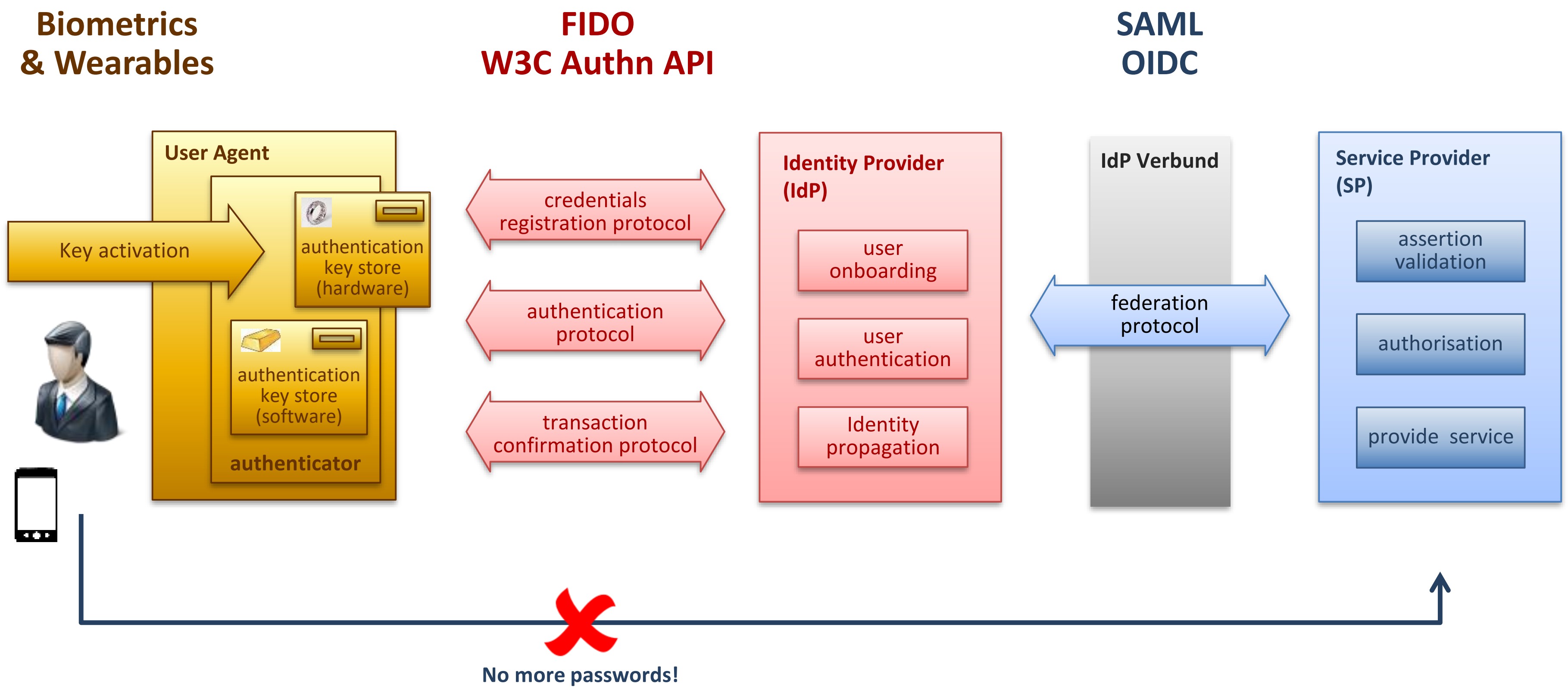
Bring Your Own Identity
BYOID

- So, the real question is: Who will provide you with this identity?
  - Will anybody be able to keep up with Google, Facebook or Apple in the long run?

A 3-Tier Model for Future Authentication

TEMET
end-to-end IT security

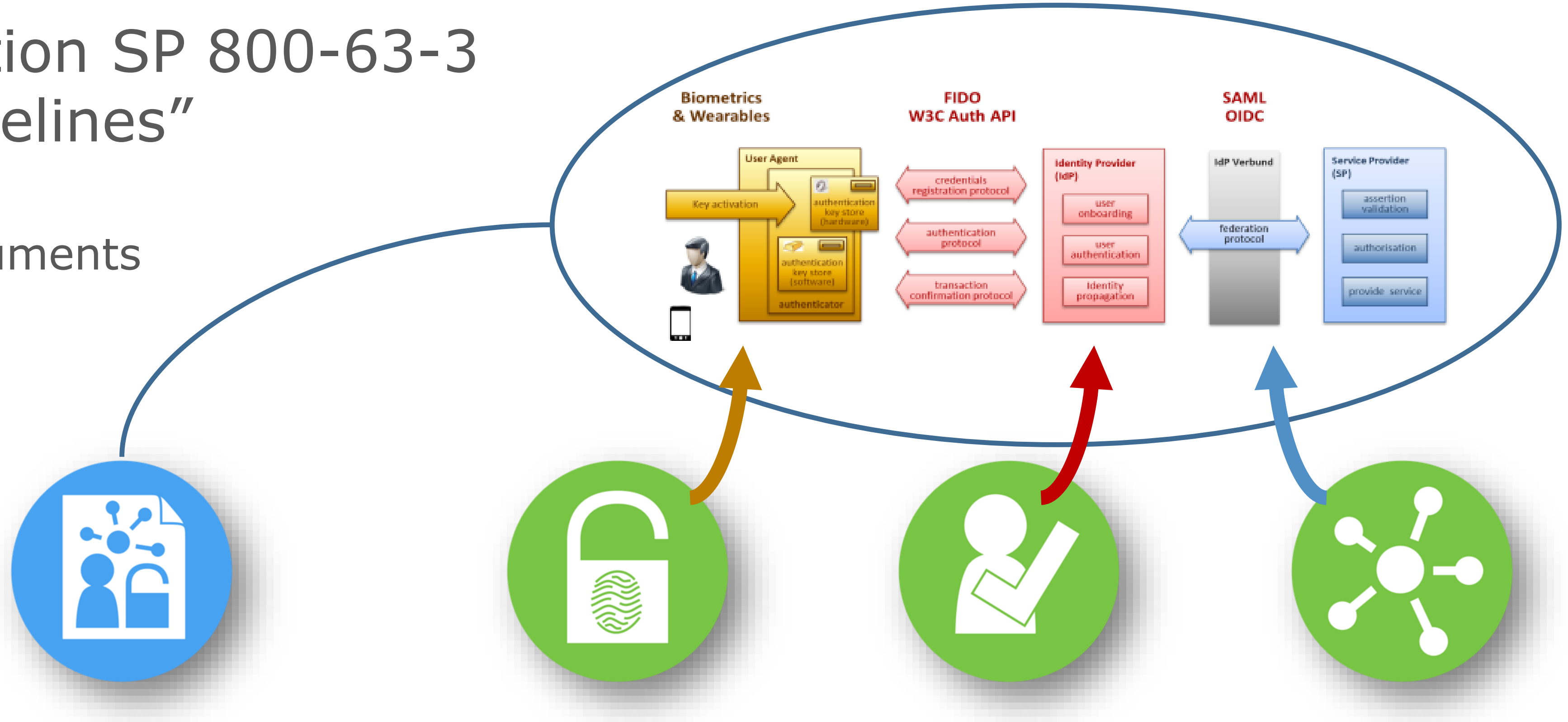
Passwords (including mTAN) will be replaced not by just another mechanism but by a 3-Tier architecture model:



There is a Standard!

NIST Special Publication SP 800-63-3 "Digital Identity Guidelines"

- Published June, 2017
- Consisting of four documents
- 213 pages in total



SP 800-63-3
Digital Identity Guidelines

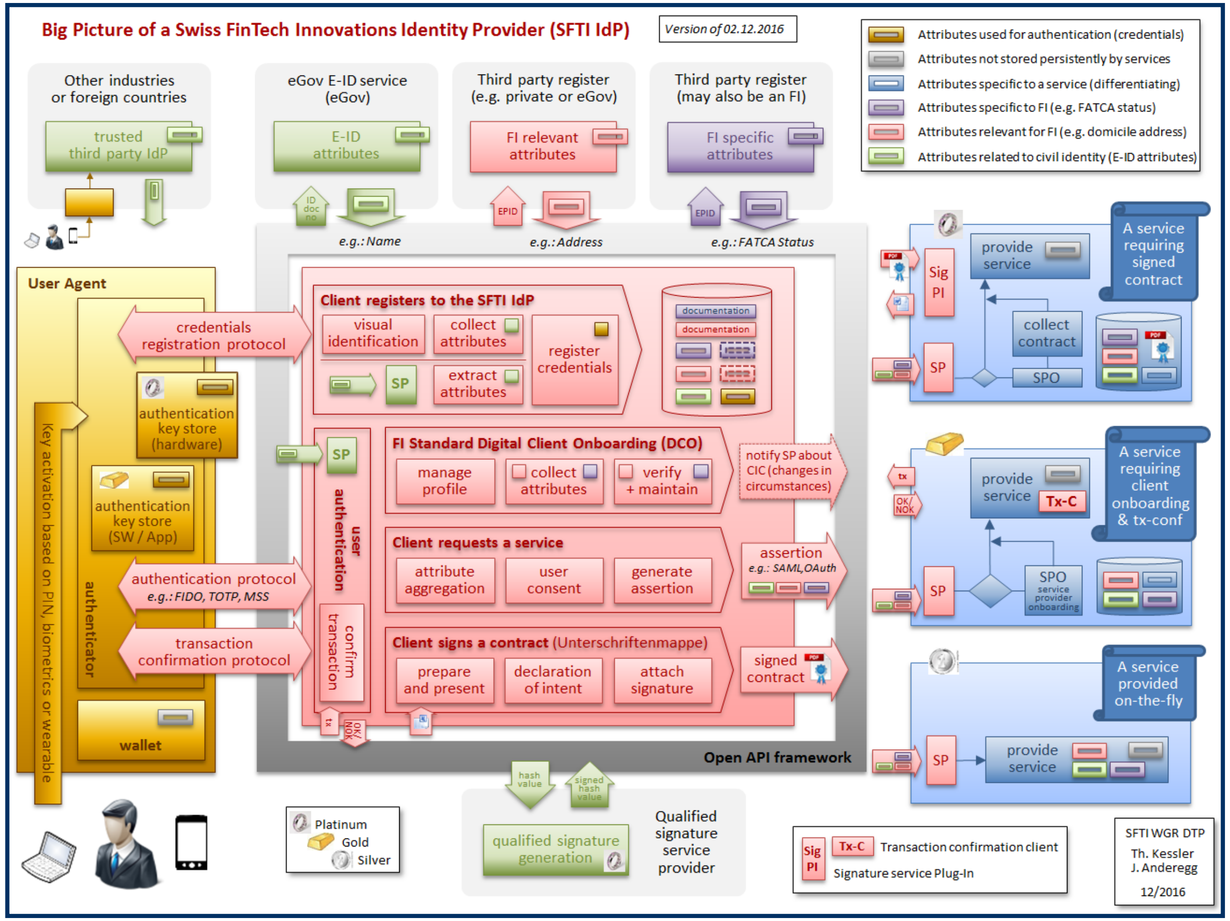
SP 800-63B
Authentication & Lifecycle Management

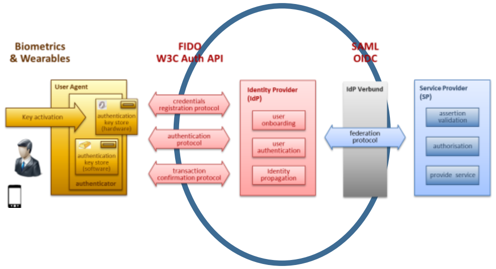
SP 800-63A
Enrollment & Identity Proofing

SP 800-63C
Federation & Assertions

Identity Provider (IdP)

A slightly more complex model of Future Authentication


Big Picture of a Swiss FinTech Innovations Identity Provider (SFTI IdP)
Version of 02.12.2016
Attributes used for authentication (credentials)
Attributes not stored persistently by services
Attributes specific to a service (differentiating)
Attributes specific to FI (e.g. FATCA status)
Attributes relevant for FI (e.g. domicile address)
Attributes related to civil identity (E-ID attributes)
Other industries or foreign countries
trusted third party IdP
eGov E-ID service (eGov)
E-ID attributes
ID doc no
e.g.: Name
Third party register (e.g. private or eGov)
FI relevant attributes
EPID
e.g.: Address
Third party register (may also be an FI)
FI specific attributes
EPID
e.g.: FATCA Status
User Agent
credentials registration protocol
authentication key store (hardware)
authentication key store (SW / App)
authentication protocol
e.g.: FIDO, TOTP, MSS
transaction confirmation protocol
authenticator
wallet
Key activation based on PIN, biometrics or wearable
Client registers to the SFTI IdP
visual identification
collect attributes
extract attributes
register credentials
SP
documentation
documentation
SP
user authentication
confirm transaction
tx
OK/NOK
FI Standard Digital Client Onboarding (DCO)
manage profile
collect attributes
verify + maintain
notify SP about CIC (changes in circumstances)
Client requests a service
attribute aggregation
user consent
generate assertion
assertion
e.g.: SAML, OAuth
Client signs a contract (Unterschriftenmappe)
prepare and present
declaration of intent
attach signature
signed contract
Open API framework
hash value
signed hash value
qualified signature generation
Qualified signature service provider
Platinum
Gold
Silver
Sig PI
SP
provide service
A service requiring signed contract
collect contract
SPO
tx
OK/NOK
SP
provide service
Tx-C
A service requiring client onboarding & tx-conf
SPO
service provider onboarding
SP
A service provided on-the-fly
provide service
Sig PI
Tx-C
Transaction confirmation client
Signature service Plug-In
SFTI WGR DTP
Th. Kessler
J. Anderegg
12/2016

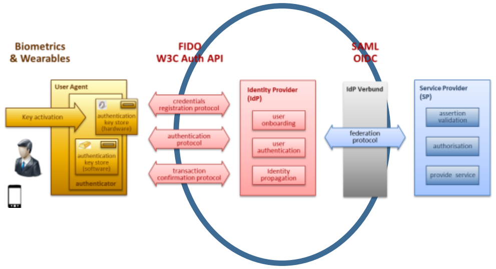


IdP main use cases:

- Client registers to the IdP
- Standard Digital Client Onboarding (DCO)
- Client requests a service
- Client signs a contract
- User authentication

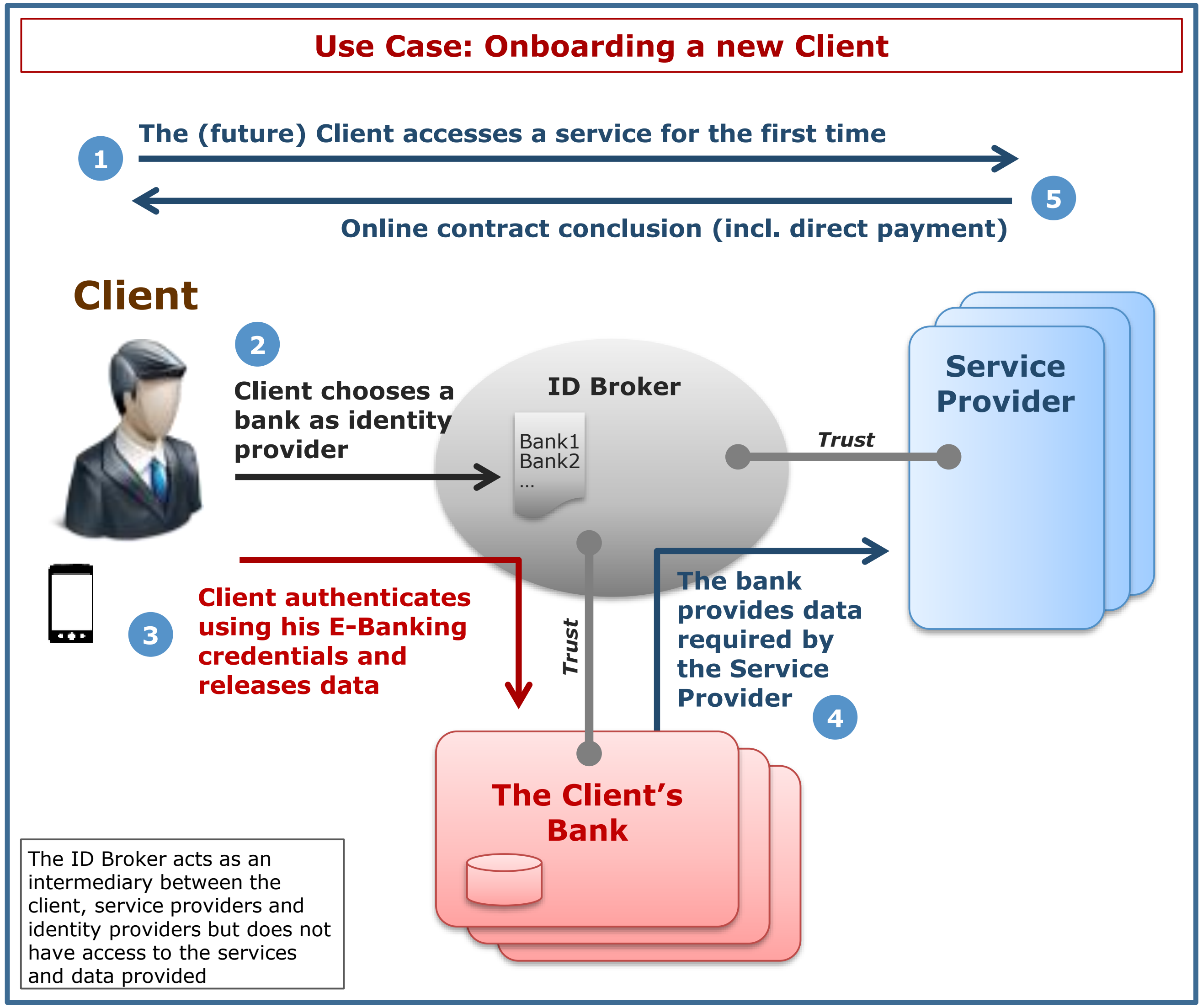
Source:
Position Paper on Digital Identity, Trust and Privacy (SFTI, December 2016)

Identity Provider: (Swiss) Market Overview



- Industry (CUG) Identity Providers
  - BrokerGate for Insurers and Brokers
  - HealthInfoNet (HIN) IdP for Doctors
  - Ofac IdP for Pharmacists
  - SWITCH Swiss edu-ID / SWITCHaai for Students
  - …
- Public Identity Providers
  - Tech Giants / Social Media (Google, Facebook, Apple,…)
  - Governmentally regulated IdP (SuisseID)
  - …
- Swiss government activities
  - E-ID act to enable a regulated marketplace for IdP
  - EPD act requires a certified Identity Provider to access electronic patient dossier
  - IDV Schweiz: An Identity Broker for eGovernment applications

How an IdP Association of Banks may work



Use Case: Onboarding a new Client

1 The (future) Client accesses a service for the first time

5 Online contract conclusion (incl. direct payment)

Client

2 Client chooses a bank as identity provider

ID Broker

Bank1
Bank2
…

Trust

Service Provider

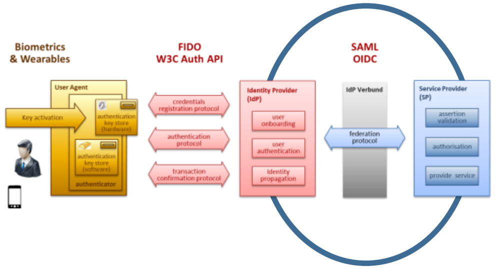
3 Client authenticates using his E-Banking credentials and releases data

Trust

The bank provides data required by the Service Provider 4

The Client's Bank

The ID Broker acts as an intermediary between the client, service providers and identity providers but does not have access to the services and data provided



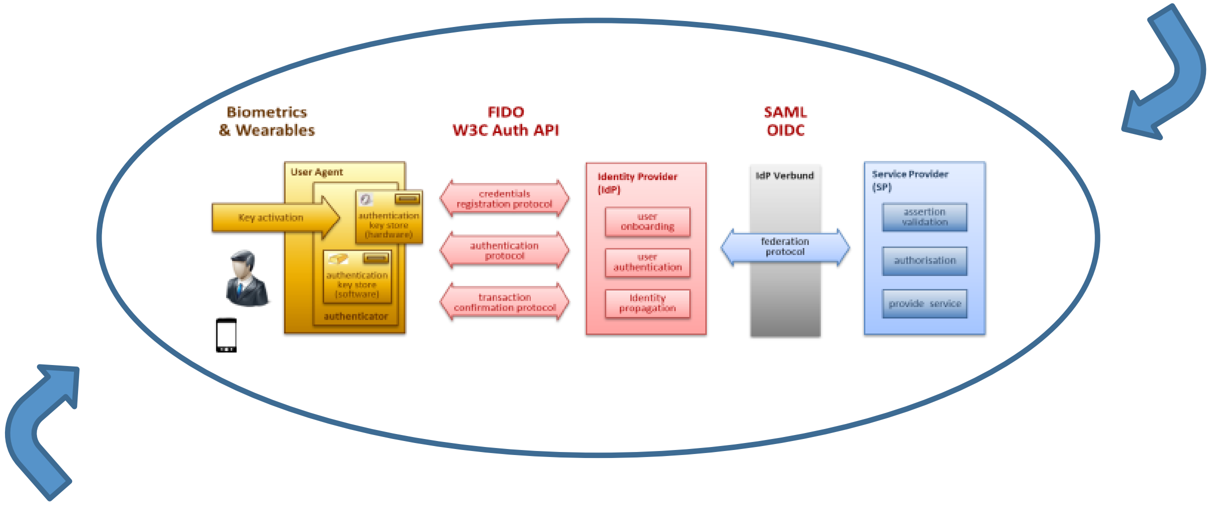
Looking ahead,

Banks (and other trusted entities) in Switzerland have joined forces to participate in a common solution to provide a Swiss Digital Identity.

With SwissID 5, eGovernment and eCommerce Service Providers may leverage proven technology currently used for E-Banking.

Agenda

- It’s time for a change!
- A 3-Tier Model for Future Authentication
- Identity Providers and Service Integration



- Trends in Authentication and Key Activation
- Now, what does all of this mean to me?

Current Situation in B2C Authentication

TEMET
end-to-end IT security

Printed Lists or Grids

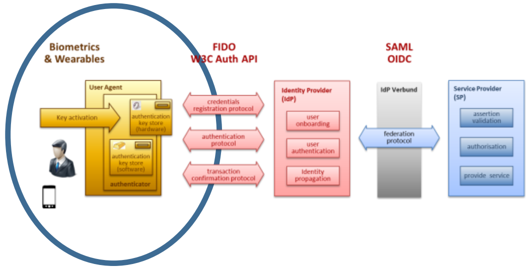
↘

QR-Token

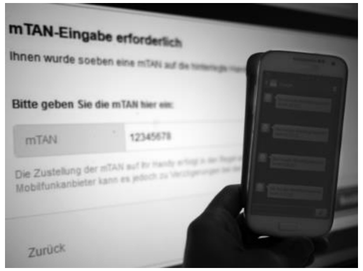
↗

C/R App (online)

↗



mTAN



↘

Mobile Signature Service

↗

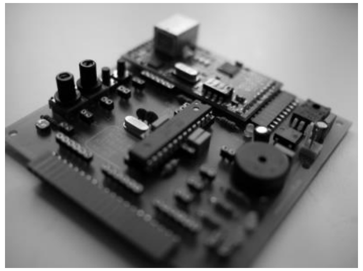
TOTP App (offline)

↗

OTP Token

↘

Trusted Platform Module



↗

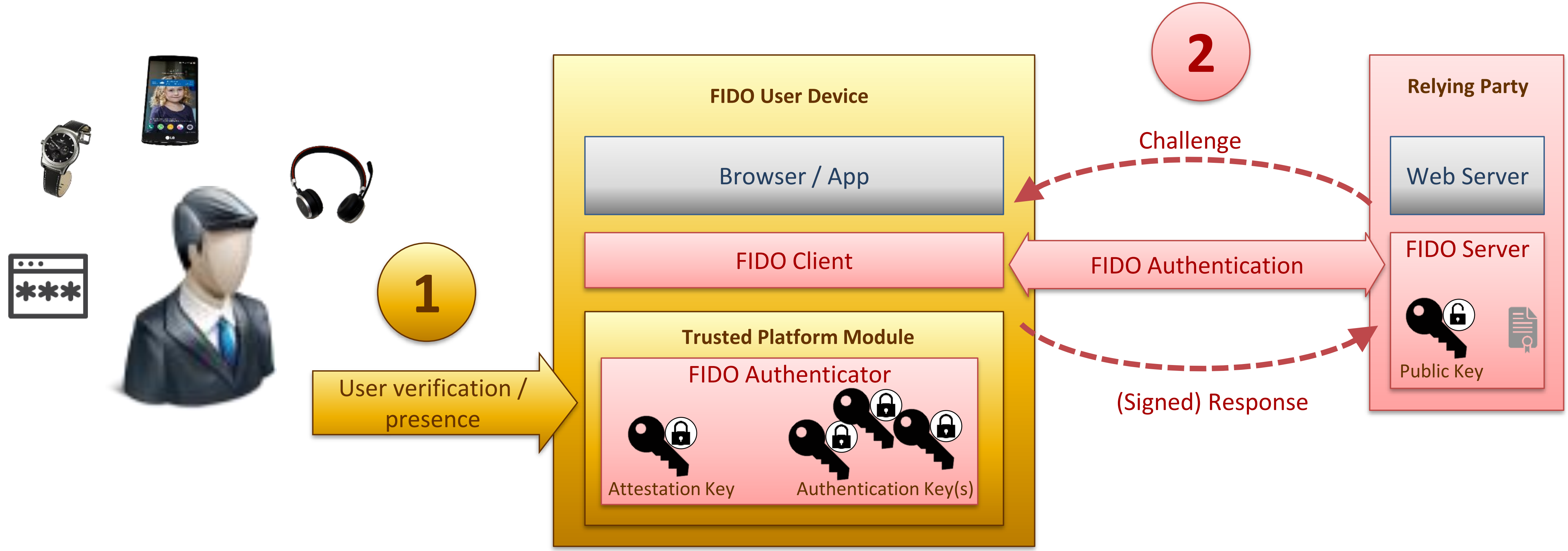
PKI Token

↘

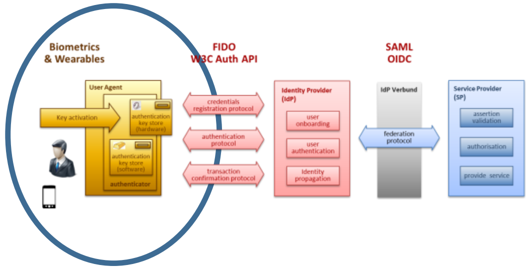
FIDO Universal Authentication Framework

User verification may be based on PIN, Biometrics, Wearables or any combination of sensors.

Once unlocked, the user's private key is used for (mutual) authentication vis-à-vis the FIDO Server.



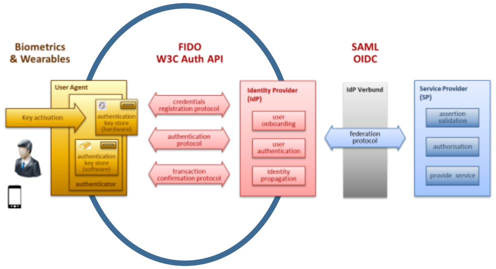
Key Activation Trends



- Biometrics, Wearables and Sensors may eventually replace device PINs
- Biometric data must only be stored decentrally within a (secure) personal authenticator / trusted platform module
- The quality of the mechanisms may be compared to password strength
  - So far, no taxonomy to measure quality of biometric mechanisms is known to the speaker
  - There is an interesting project going on at NIST: SOFA-B (https://pages.nist.gov/SOFA)

⇨ If used to unlock FIDO Authenticators, Biometrics may (finally) become a "game changer" in the authentication industry!

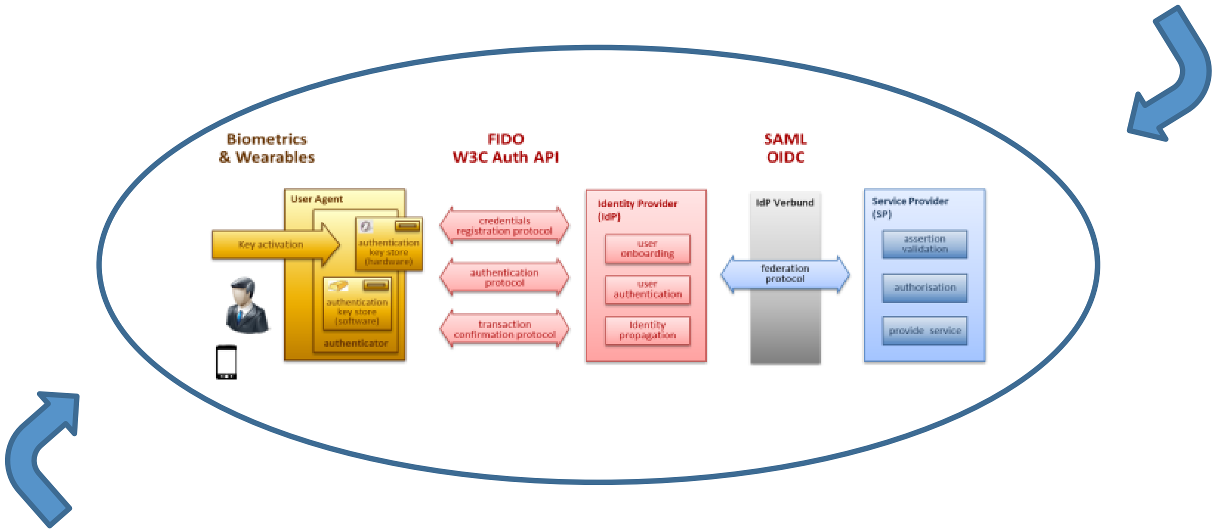
Authentication Protocol Trends



- W3C and FIDO Alliance have announced the new specification for Web Authentication API
- On March 20, 2018 WebAuthn has reached the "Candidate Recommendation (CR)" maturity level and is so close to being recognized as an official W3C web standard.
- The standard defines an API for secure communication between end devices and web services for the purpose of strongly authenticating users
- For Web services with WebAuthn, a secure login to the service without password is possible with compatible browsers in the future
- The big browser manufacturers Google, Mozilla and Microsoft support the standard and want to implement it in their browsers

Agenda

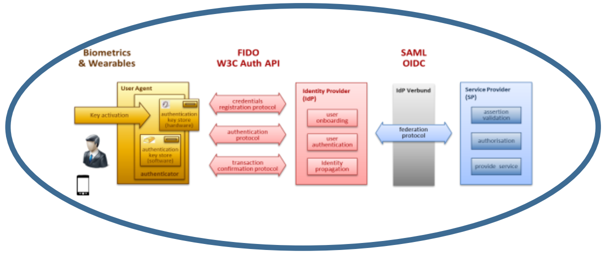
- It’s time for a change!
- A 3-Tier Model for Future Authentication
- Identity Providers and Service Integration



- Trends in Authentication and Key Activation
- Now, what does this mean to me?

Some Strategic Advice (1/2)

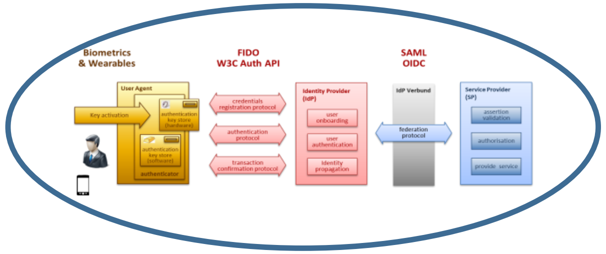
end-to-end IT security



- First of all:
  Decide whether you will be a SP or an IdP

- If you are a Service Provider (SP):
  - Don’t spend much energy on your next authentication mechanism.
  - To keep up with the Joneses, deploy a decent C/R App providing adequate security at reasonable cost. In many cases, some open source Authenticator App may suit your requirements.
  - Concentrate on a comprehensive strategy to integrate with Identity Providers through suitable federation protocols (SAML, OIDC).
  - You may look for strategic partnership with an Identity Provider of choice

Some Strategic Advice (2/2)



Biometrics & Wearables

FIDO W3C Auth API

SAML OIDC

User Agent

Key activation

authentication key store (hardware)

authentication key store (software)

authenticator

credentials registration protocol

authentication protocol

transaction confirmation protocol

Identity Provider (IdP)

user onboarding

user authentication

Identity propagation

IdP Verbund

federation protocol

Service Provider (SP)

assertion validation

authorisation

provide service

- If you are an Identity Provider (IdP):
  - Provide a broad range of authenticators to your customers to cover all kinds of end user devices and use cases.
  - And don’t forget to provide good solutions for special situations such as authenticator replacement or device renewal.
  - Avoid proprietary protocols for end user authentication and federation. Focus on FIDO/W3C Authn API and SAML/OIDC standard interfaces to maintain flexibility.
  - Make it easy for Service Providers to rely on you! Be prepared to compete with Google and other tech giants and therefore consider to join forces with other (national) players.

- And as you are also a User:
  - Look for devices and service providers that support standard interfaces and do not lock you in their proprietary ecosystem by technical restrictions.

… zum Erfolg

TEMET
end-to-end IT security

Besten Dank
für Ihre Aufmerksamkeit!

TEMET AG
Basteiplatz 5
8001 Zürich
044 302 24 42
info@temet.ch
www.temet.ch