From Real-world Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control

A Federated Architecture for Attribute-based and Behavioral Authentication as a High-Assurance Service

Dr. Michael Sirivianos
Cyprus University of Technology

Keynote, Tyrrhenian Workshop 2017: Towards a smart and secure future Internet
Palermo, 19 September 2017

Horizon 2020
European Union funding
for Research & Innovation

Co-funded by the Horizon H2020 Framework Program of the European Union under grant agreement no 653417.

Complacency about authentication security

Flight security in the 60s

ReCRED

Insecure

WIRED

Kill the Password: A String of Characters Won't Protect You

SUBSCRIBE

SHARE

SHARE 15582

TWEET

COMMENT 2

EMAIL

"This summer, hackers destroyed my entire digital life in the span of an hour," says Wired senior writer Mat Honan. ETHAN HILL

This summer, hackers destroyed my entire digital life in the span of an hour. My Apple, Twitter, and Gmail passwords were all robust—seven, 10, and 19 characters, respectively, all alphanumeric, some with symbols thrown in as well—but the three accounts were linked, so once the hackers had conned their way into one, they had them all. They really just wanted my Twitter handle: @mat. As a three-letter username, it's considered prestigious. And to delay me from getting it back, they used my Apple account to wipe every one of my devices, my iPhone and iPad and MacBook, deleting all my messages and documents and every picture I'd ever taken of my 18-month-old daughter.

Password reuse

WIRED

Kill the Password: A String of Characters Won't Protect You

BUSINESS | CULTURE | DESIGN | GEAR | SCIENCE | SECURITY | TRANSPORTATION

SHARE

SHARE 15582

TWEET

COMMENT 2

EMAIL

Our other common mistake is password reuse. During the past two years, more than 280 million "hashes" (i.e., encrypted but readily crackable passwords) have been dumped online for everyone to see. LinkedIn, Yahoo, Gawker, and eHarmony all had security breaches in which the usernames and passwords of millions of people were stolen and then dropped on the open web. A comparison of two dumps found that 49 percent of people had reused usernames and passwords between the hacked sites.

"Password reuse is what really kills you," says Diana Smetters, a software engineer at Google who works on authentication systems. "There is a very efficient economy for exchanging that information." Often the hackers who dump the lists on the web are, relatively speaking, the good guys. The bad guys are stealing the passwords and selling them quietly on the black market. Your login may have already been compromised, and you might not know it—until that account, or another that you use the same credentials for, is destroyed.

Hackers also get our passwords through trickery. The most well-known technique is phishing, which involves mimicking a familiar site and asking users to enter their login information. Steven Downey, CTO of Shipley Energy in

MOST POPULAR

GIFT GUIDE
Father's Day Gift Ideas: Spoil Your Dad This Father's Day With These 1...
MICHAEL CALORE

IN DEPTH
Welcome to Poppy's World
LEXI PANDELL

Horror stories

WIRED Kill the Password: A String of Characters Won't Protect You SUBSCRIBE

information. Steven Downey, CTO of Shipley Energy in Pennsylvania, described how this technique compromised the online account of one of his company's board members this past spring. The executive had used a complex alphanumeric password to protect her AOL email. But you don't need to crack a password if you can persuade its owner to give it to you freely.

The hacker phished his way in: He sent her an email that linked to a bogus AOL page, which asked for her password. She entered it. After that he did nothing. At first, that is. The hacker just lurked, reading all her messages and getting to know her. He learned where she banked and that she had an accountant who handled her finances. He even learned her electronic mannerisms, the phrases and salutations she used. Only then did he pose as her and send an email to her accountant, ordering three separate wire transfers totaling roughly $120,000 to a bank in Australia. Her bank at home sent $89,000 before the scam was detected.

An even more sinister means of stealing passwords is to use malware: hidden programs that burrow into your computer and secretly send your data to other people. According to a Verizon report, malware attacks accounted for 69 percent of data breaches in 2011. They are epidemic on Windows and, increasingly, Android. Malware works most commonly by

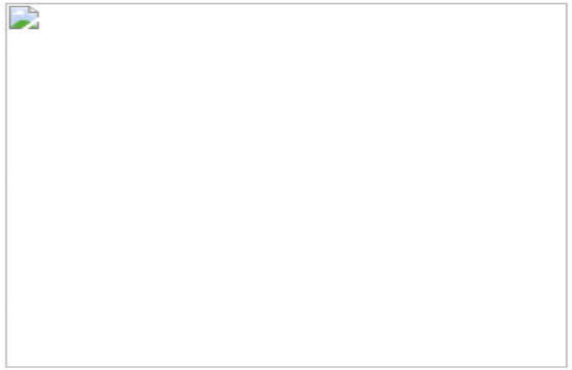
SHARE

SHARE 15582

TWEET

COMMENT 2

EMAIL



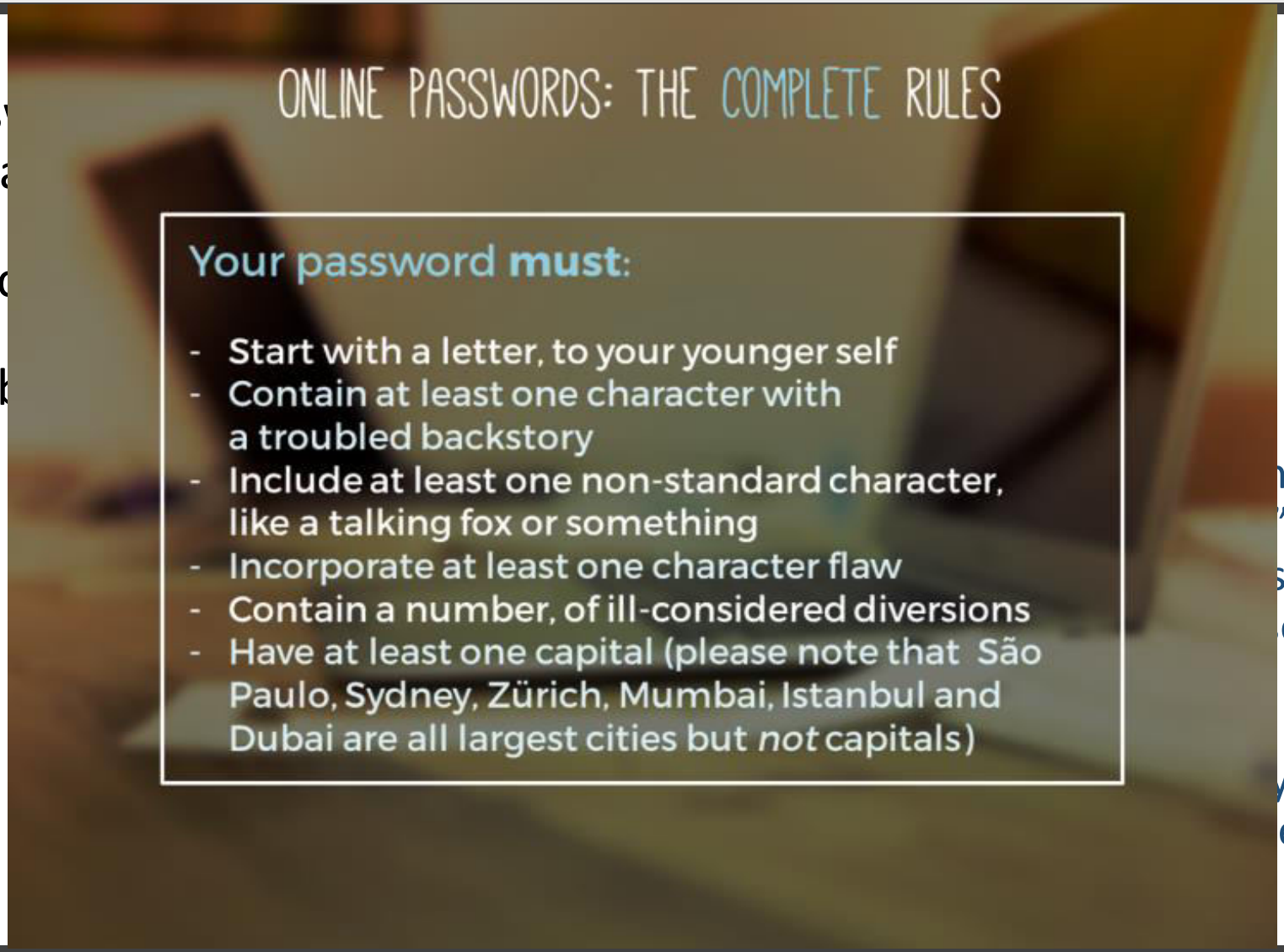
MOST POPULAR

GIFT GUIDE
Father's Day Gift Ideas: Spoil Your Dad This Father's Day With These 1...
MICHAEL CALORE

IN DEPTH
Welcome to Poppy's World
LEXI PANDELL

If secure, then it is not user-friendly

- A secure pass
  dictionary atta
- It should not c
- It should not b



nope Juventus will
'. Then, take the
s and symbols to
e would result in

y adding a random
example:

Something you know -> something you have and you are

WIRED Hack Brief: Password Manager LastPass Got Breached Hard

BUSINESS | CULTURE | DESIGN | GEAR | SCIENCE | SECURITY | TRANSPORTATION

SHARE

SHARE 3931

TWEET

COMMENT

EMAIL

ANDY GREENBERG SECURITY 06.15.15 05:01 PM

HACK BRIEF: PASSWORD MANAGER LASTPASS GOT BREACHED HARD

EXPERTS RECOMMEND PASSWORD managers like LastPass as the easiest way to generate unique, strong security codes for every one of your online accounts—which sounds great, until that password manager itself is cracked, potentially offering attackers access to all the accounts it was designed to protect.

The Hack

On Monday password manager service LastPass admitted it

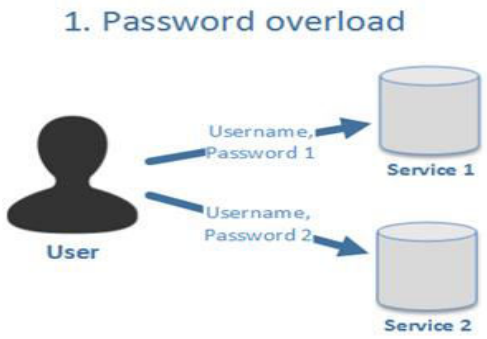
MOST POPULAR

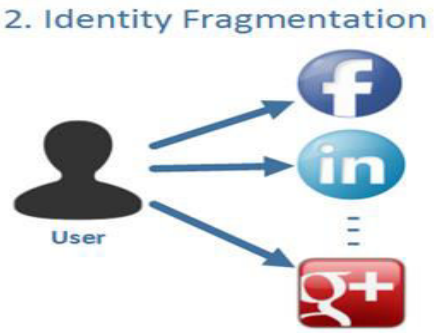
CANTINA TALK
Cantina Talk: You Can Bet Carrie Fisher Would Love *Episode IX*
GRAEME MCMILLAN

WIRED OPINION
Ethical Innovation Means

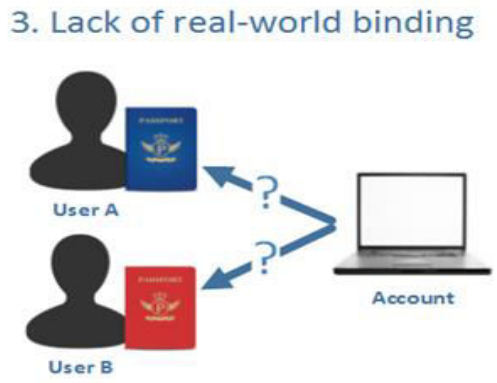
ReCRED's Goal

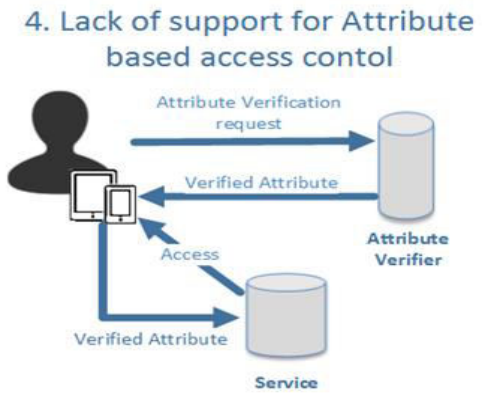
- To promote the user's personal mobile device to the role of a unified authentication and authorization proxy towards the digital world.





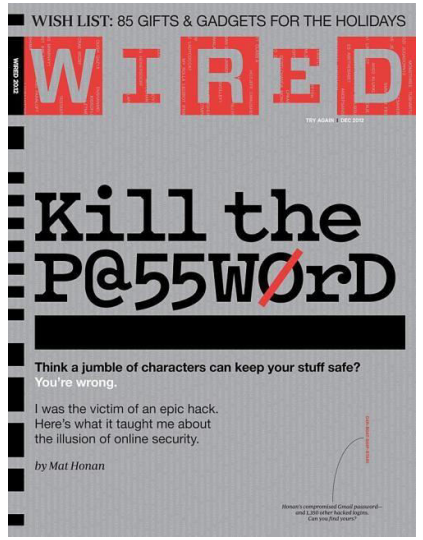
Problems addressed by ReCRED





How do we kill the password?

- Integration between strong device-centric authentication methods and federated login solutions
- Separation of concerns for Identification, Authentication, Authorization and Behavioral Authentication
  - Incremental deployability
  - Wide adoption and compliance with NIST assurance levels
- A novel centralized component that enables:
  - Identity management
  - Account recovery in case of device loss



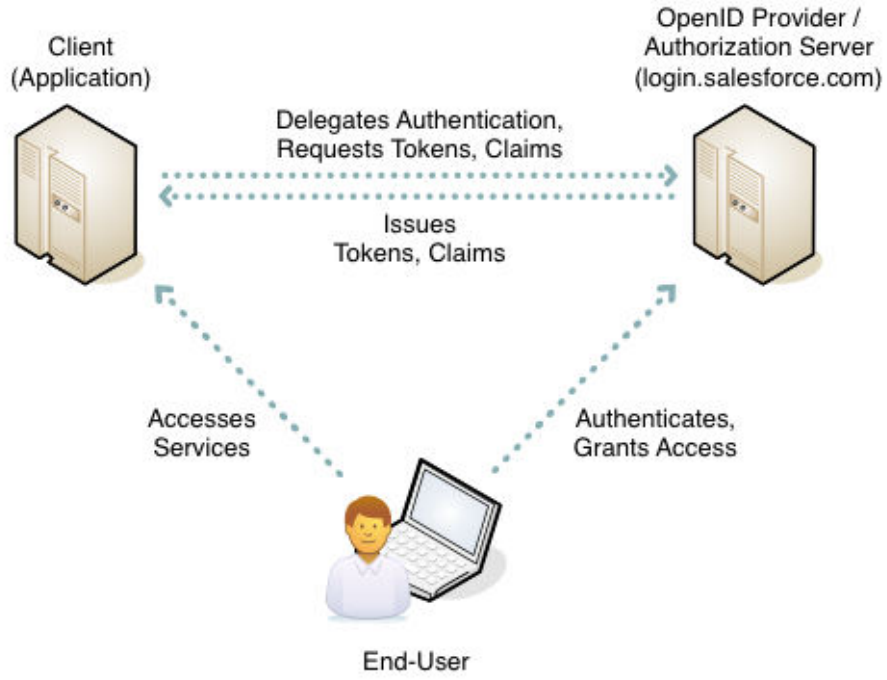
Federated Authentication

Many significant benefits, including, but not limited to:

- **Enhanced UX**
  - A user can be authenticated once and reuse the issued credential at multiple Service Providers
- **Cost reduction** to the end-user (reduction in **authenticators**)
- **Data minimization** and **focus on mission**
  - Service Providers do not need to collect and store personal information
- **Pseudonymous** attribute assertions
  - Service Providers can request a minimized set of attributes

OpenID Connect

- **OpenID Connect** (Single Sign On)
  - Online services authenticate their users by employing **Google**, **Microsoft**, **PayPal**, accounts
  - **Mobile Connect** (Mobile operators as ID providers)
- **OAuth 2.0** (Open standard for Authorization)
  - Issues and uses **access tokens** to be used for **authorization**



OpenID Connect

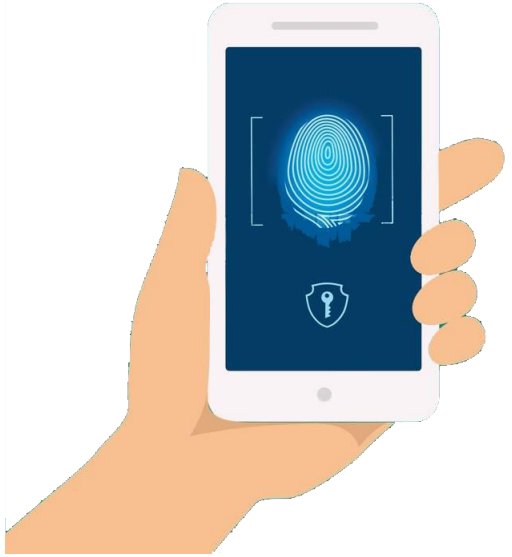
NIST-2017 Assurance Levels

NIST

- Identity Assurance Levels (IAL)
  - Addresses how end-users can register and prove their identities to an identity management system
- Authenticator Assurance Levels (AAL)
  - Addresses how end-users can securely authenticate and access a Service Provider
- Federation Assurance Levels (FAL)
  - Provides requirements and assertions to convey the results of authentication processes and relevant identity information to a Service Provider
  - Privacy-enhancing techniques for identity management
  - Methods for strong multi-factor authentication while the end-user remains anonymous

Why Device-Centric Authentication (DCA)?

- "Something you know" -> "Something you have"
- Solves the password overload problem and introduces high assurance authenticators
- The mobile device of the user is required for:
  - Mobile Connect
  - Behavioral Authentication
  - Privacy-preserving Attribute-Based Access Control (P-ABAC)

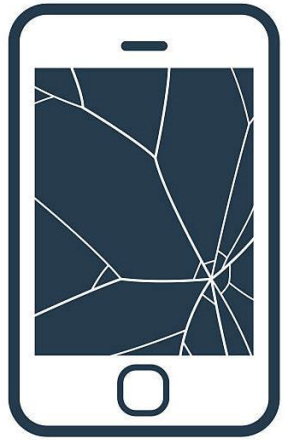


Why DCA needs Federation?

- DCA needs federation for **Identity Management**

- DCA requires **a trusted registry** for reliable Failure Recovery
  - Lack of device failure/loss recovery mechanisms → passwords are still in use

  - To offer failover authentication with Mobile Connect and BAAs



Failure Recovery

- The **main problem** for adoption of various password-replacement schemes
- ID Federation (OpenID Connect) and Consolidation ease recovery
  - Together they support multiple backup factor mechanisms
- Users have to remember only one backup password
  - No need to use it frequently
  - TypTop: Personalized Typo-tolerant Password Checking

Identity Consolidation and Management

- The Identity Consolidator is the **main reference** to a user's identity attributes

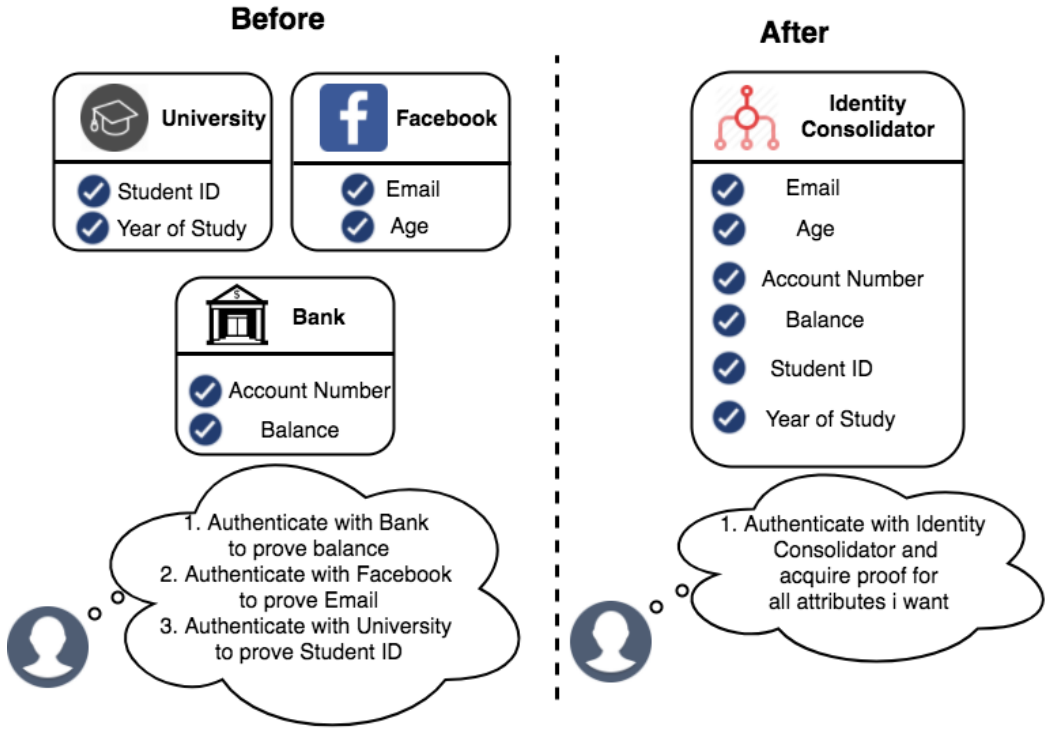
- Main Components:
  - Physical and Online Identity Acquisition
  - Identity Integration
  - Credential Management
  - Identity Management (Profile and Consent Management)
  - Authentication Management
  - Account Management

Why ID Consolidator (IDC)?

- It solves the Identity Fragmentation problem
  - Real to Online identity binding
  - Enables proof of joint attribute ownership
  - Keeps track of all IdPs and BAAs of a user
  - Acts as a consolidated OIDC Identity Provider
- Facilitates the verification of ID attributes
  - by combining multiple soft proofs of identities
  - via statistical correlations (Identity Integration Module)
- Allows for effective Profile and Consent management

Why ID Consolidator?

- Acts as trusted authority able to issue P-ABAC credentials



- Can also acts as a Mobile Connect proxy Identity Provider

Extending the OpenID Connect Protocol

OpenID Connect + FIDO UAF

- Password-less OpenID Connect experience
- Integration of the FIDO UAF server to the OpenID Connect Provider
- Replacement of username/password authentication with biometrics (e.g., fingerprint) or pins

FIDO UAF Authentication

Identity Provider

Identity Consolidator

Service Providers

OpenID Connect + FIDO UAF

Federated identities with OpenID Connect/OAUTH 2.0

Single Sign On

Identity Provider

Single Sign On

Identity Consolidator

Single Sign On

Service Providers

Extending the OpenID Connect Protocol

Extending OpenID Connect to support attribute write on the ID Provider

- Update, delete, transfer of identity attribute between different Identity Providers

- The Service Provider can write attributes to the ID Provider instead of only reading

Extending the OpenID Connect Protocol

OpenID Connect + P-ABAC (Idemix/U-Prove)

- Integration of Cryptographic credentials stacks within the OpenID Connect Provider
- The OpenID Connect Provider acts as an Idemix/U-Prove issuer and verifier

Extending the OpenID Connect Protocol

Attribute combination suggestion based on requested resource

- The Service Provider suggests possible attribute combinations to the OpenID Connect Provider

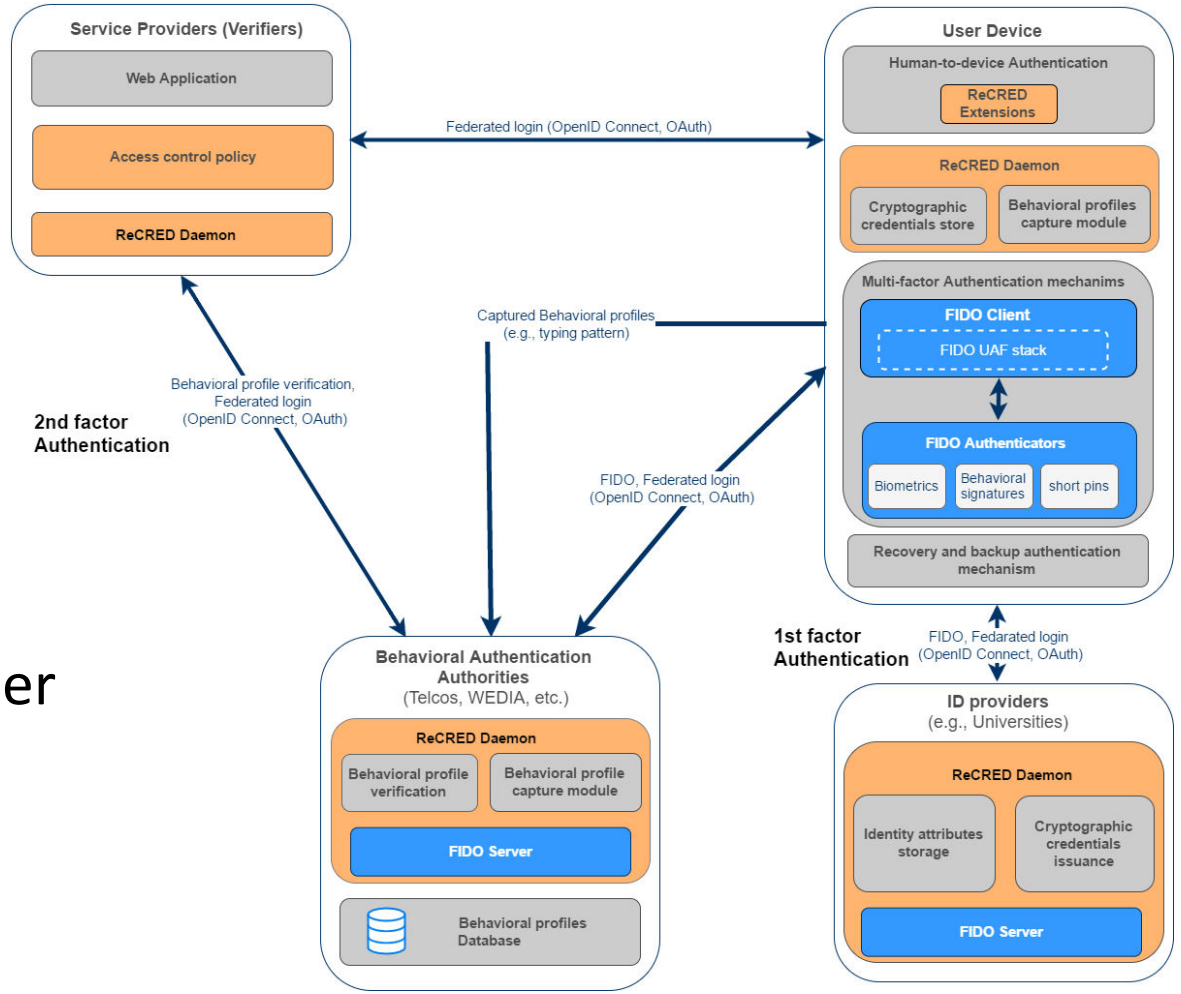
- Offers more flexibility and increased privacy if desired by the user

What is and why do we use Mobile Connect?

- Mobile-based secure universal authentication, authorization, and attribute sharing solution
- Matches the user to his mobile phone
- Provided by a global network of Mobile Network Operators (MNOs)
- **Mobile Connect is required to achieve IAL3**

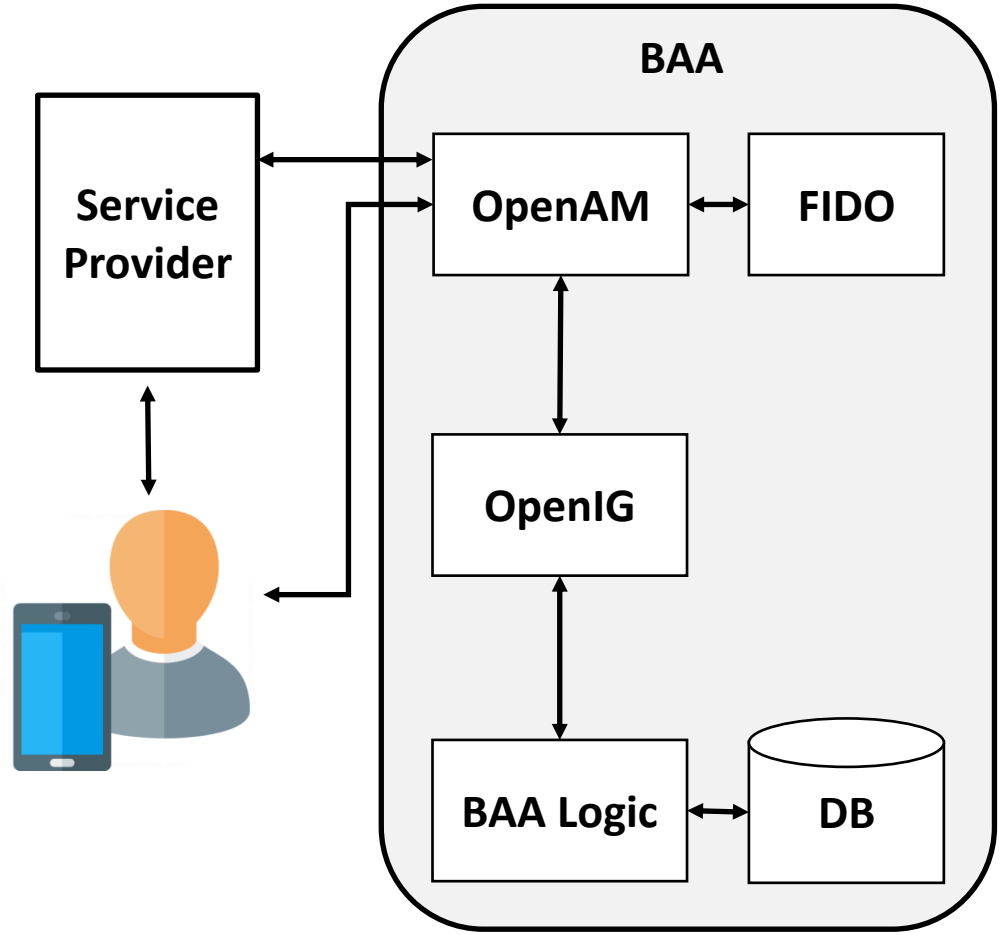
Behavioral Authentication Authority (BAA)

- Provides multi-factor device-to-service authentication based on the user's behavioral biometrics
- Extends the definition of biometric with mobility and traffic patterns
- Acts as an **ID provider** verifying that the user continues to behave as he has normally done in the past



Behavioral Authentication Authority (BAA)

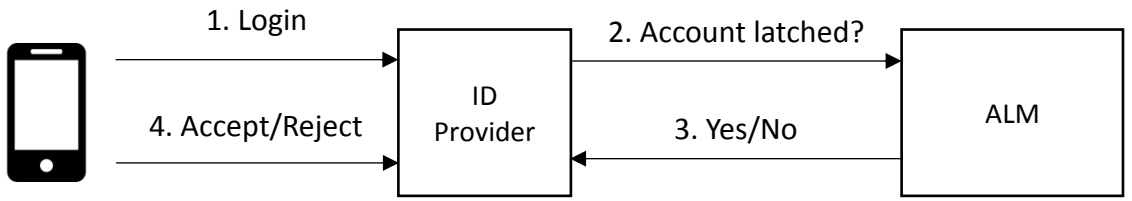
- Abstraction for behavioural authentication modalities
- Provides a common API based on two designs
  - Transparent (Mobility, Weblog)
    →Pull-base
  - Non-transparent (Gait, Keystroke)
    →Push-based
  - BAA as a Service (Stand-alone IdP)
  - Alert ID Consolidator on suspicious behaviour



Account Locking Mechanism (ALM)

- Latch for the online world
  - Real world
    - →Door latched → No entrance, even with right key
  - Online world
    - →Account latched → No login, even with right password (or other credentials)

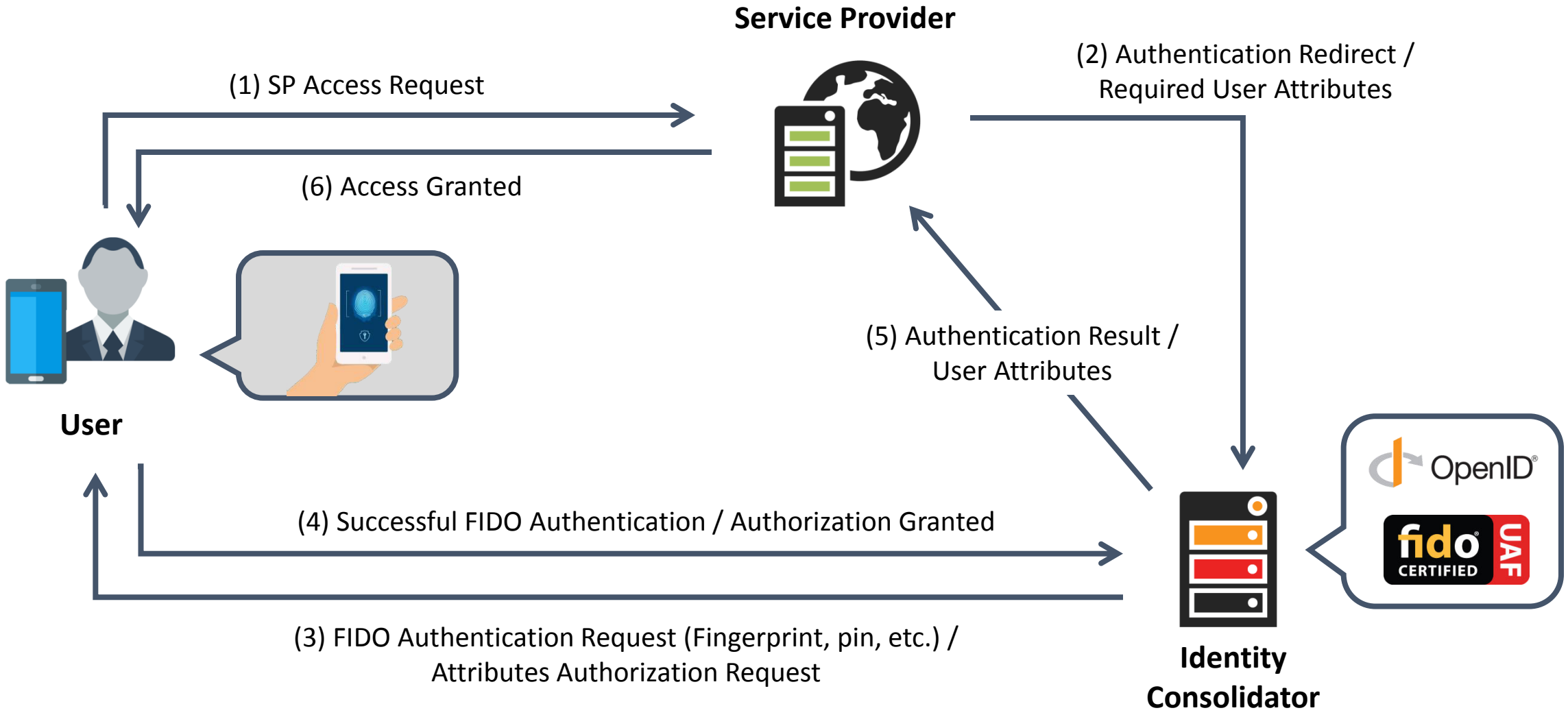
- ALM keeps account "status"
  - User define policies (e.g., latch on at night)
  - Allows for latching based on BAA alerts



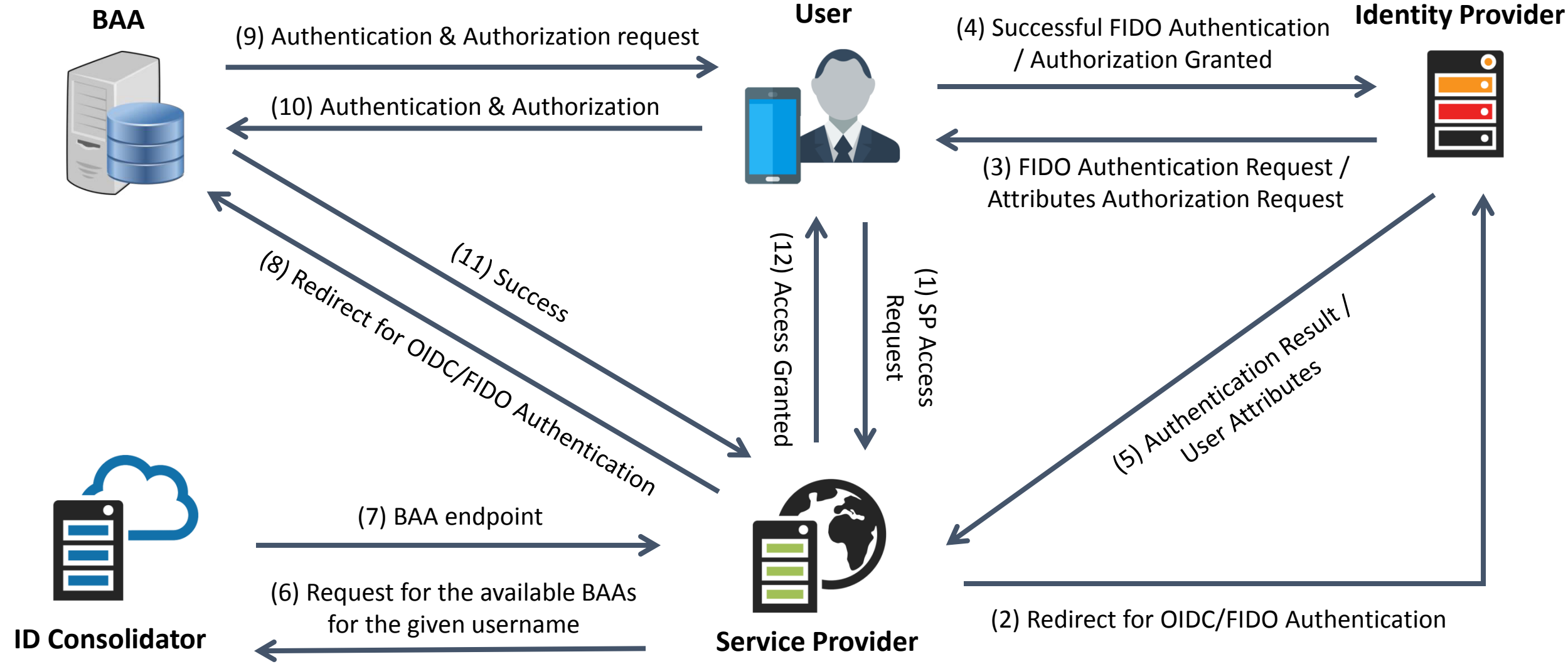
IDC Use Examples

- User authentication to a Service Provider
- Multi-factor Authentication
- IDC as Profile Management Tool

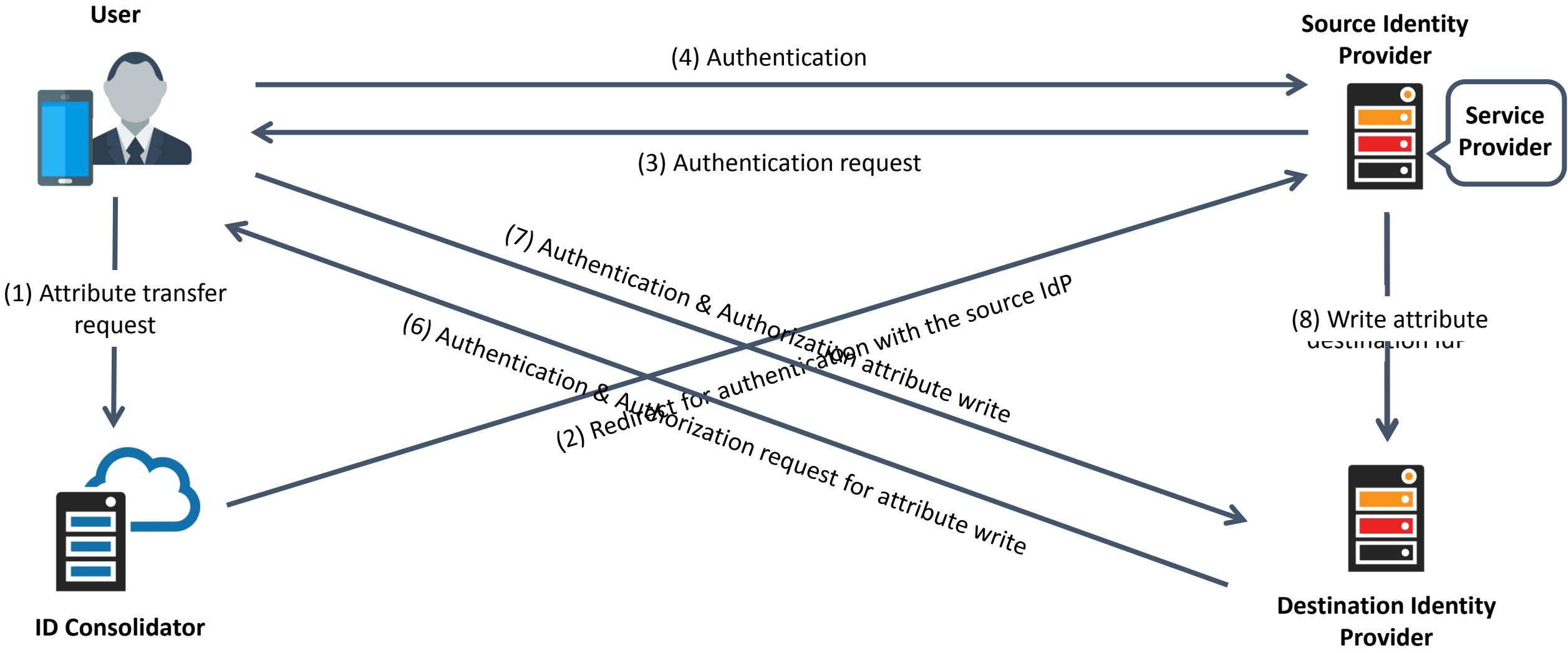
User authentication to an SP (OIDC / FIDO)



Multi-factor Authentication



IDC as a Profile Management Tool



IDC Functionalities Demonstration

- Demo 1 - Physical Identity Acquisition using NFC Technology
- Demo 2 - Transfer of identity attributes between different Identity Providers

Demo 3
BAA on-demand Authentication

- Service Provider (SP) entrusts user authentication to the Identity Provider (IdP)
- IdP provides two authentication factors
  - FIDO and behavioral authentication
- Storyboard
  - User behavior is the expected one
  - User behavior is NOT the expected one
- SP can tailor the service based on the authentication result

BAA continuous Authentication and Account Locking

- SP entrusts user authentication to IdP
- IdP: FIDO + check for account locking status
- Keystroke-based BAA

- Storyboard
  - User authenticates to IdP
    →IdP check for account lock status
  - An adversary takes possession of the user smartphone
  - BAA detects change in behavior and triggers account locking
  - The attacker tries and fails to authenticate to the IdP
    →User account is locked

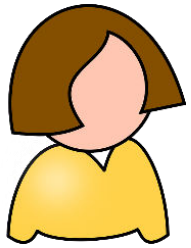
Fail-over Authentication with Mobile Connect and BAA

- The user has lost his device and purchased a new one
  - Tries to regain full access to the IDC by proving his identity
    - → Using Mobile Connect and BAA

- Storyboard
  - User authenticates to IDC with master password
    - → He is granted access in “tentative mode”
  - User proves his identity
    - → Mobile connect (he has acquired a new SIM card with his phone number)
    - → BAA (he has registered the new device to the BAA, also in “tentative mode”)

What is P-ABAC?

- **Privacy-preserving Attribute-based Access Control**



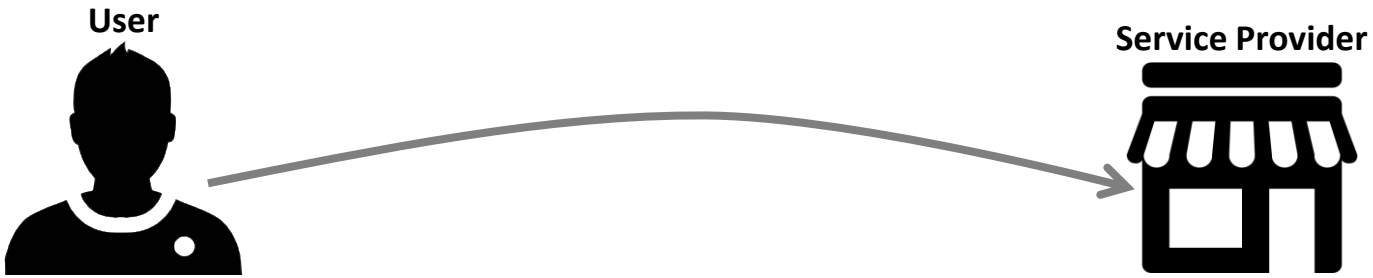
Account-less access through verified identity attributes (e.g., Age, Location, etc.)

idemix
pseudonymity for e-transactions

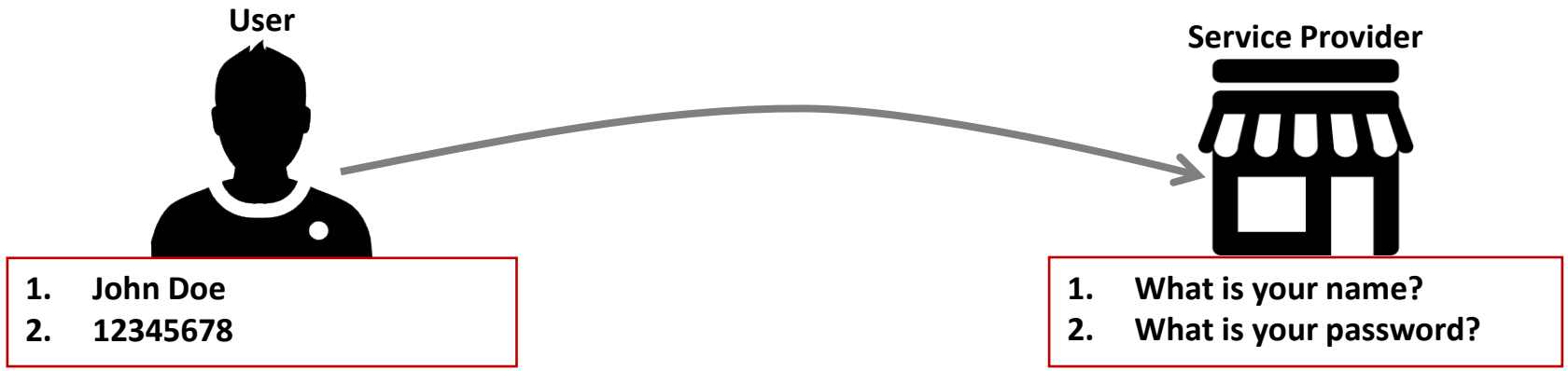
U-Prove

Issue cryptographic anonymous credentials

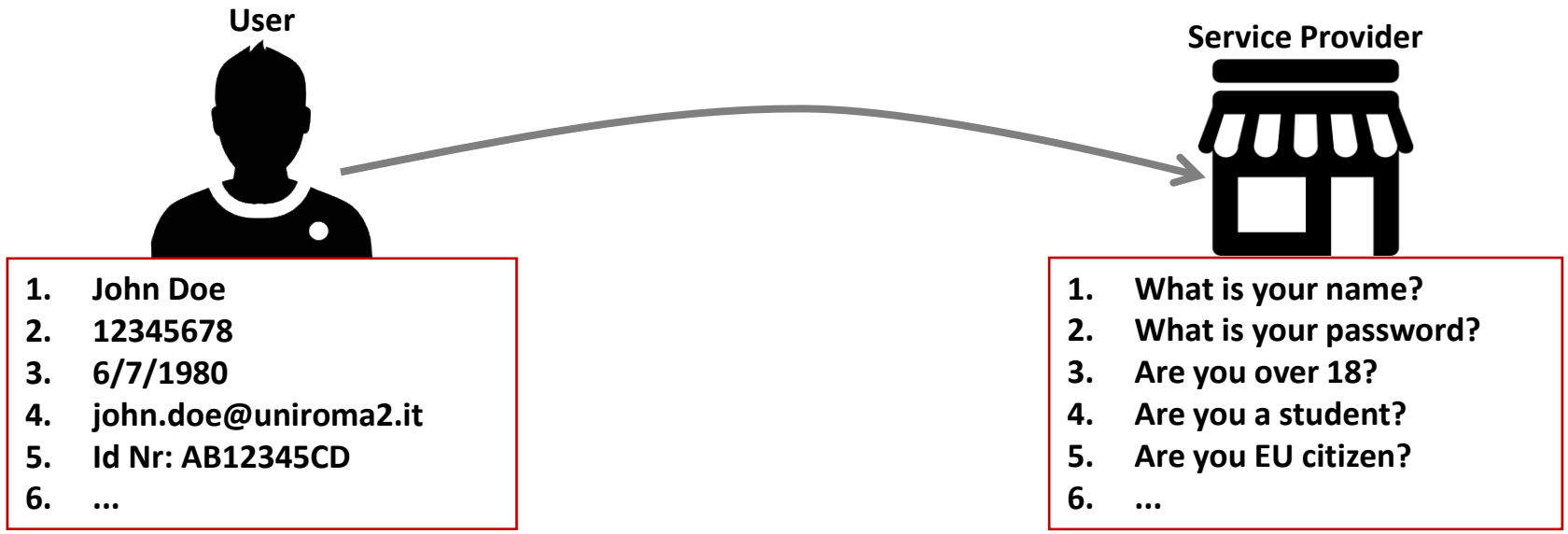
How P-ABAC works?



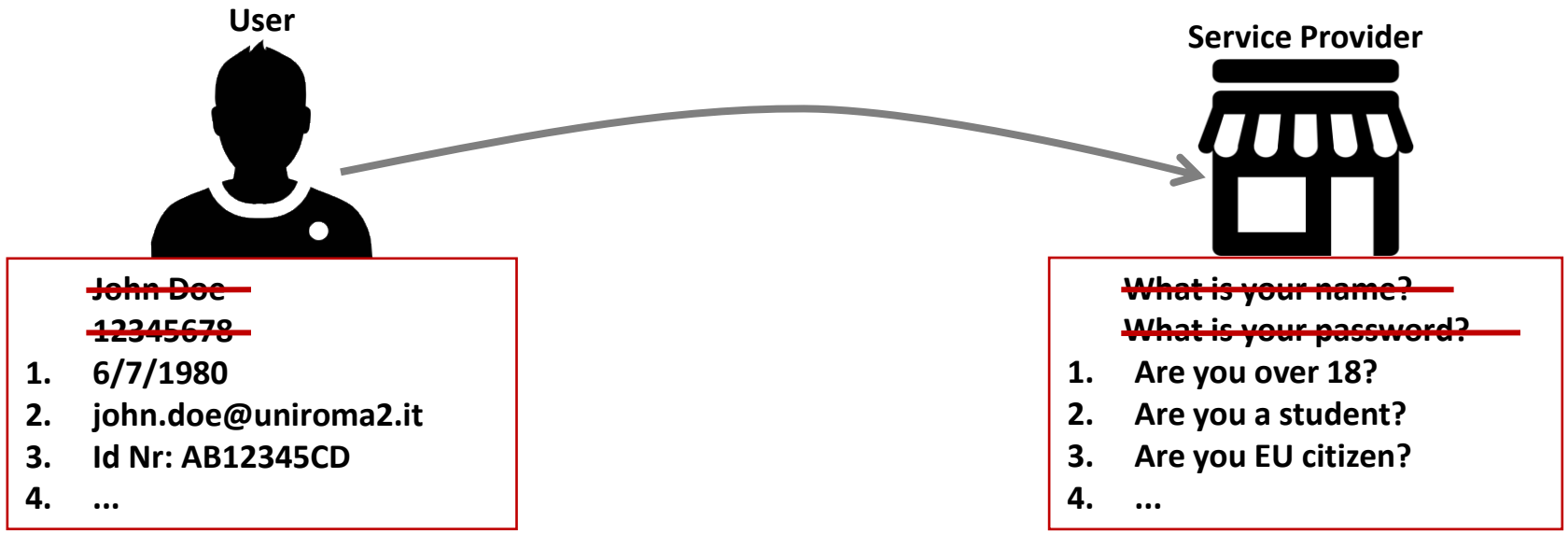
How P-ABAC works?



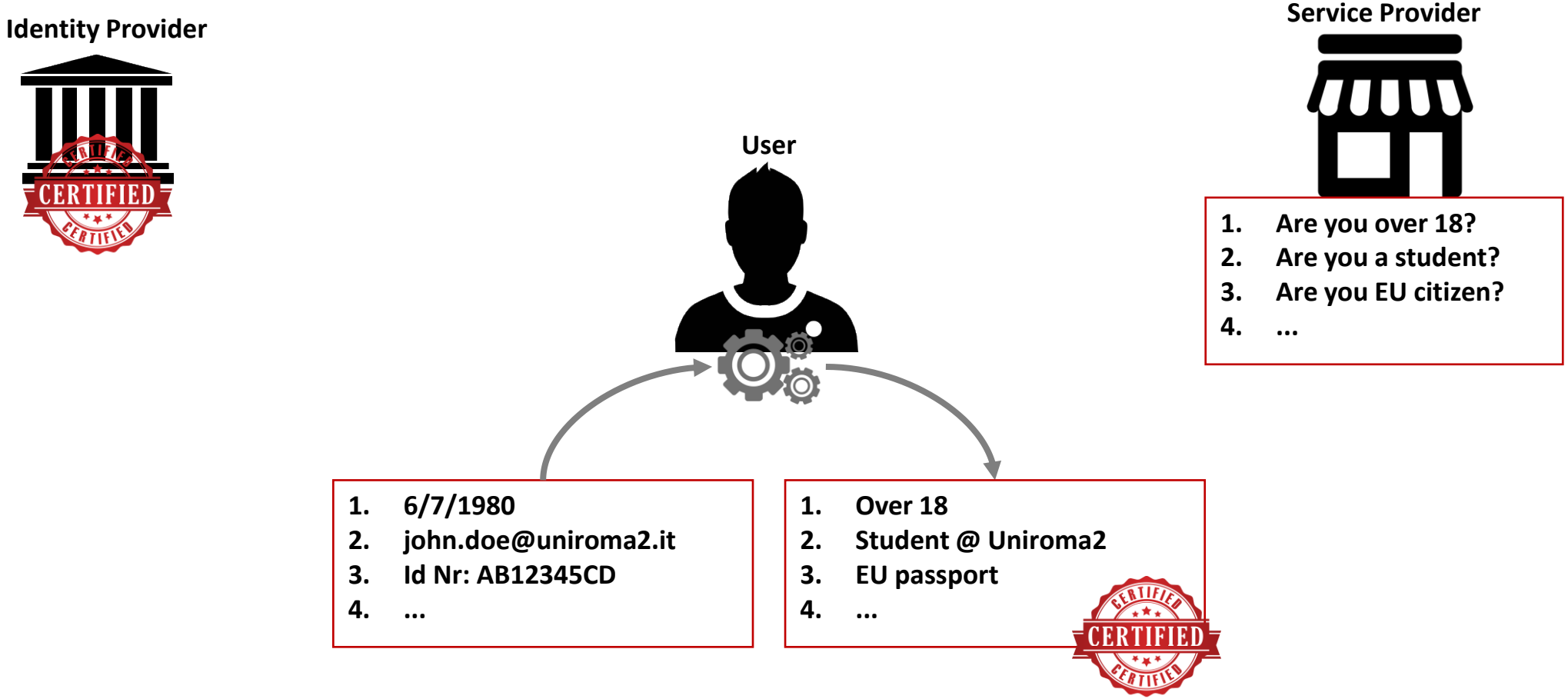
How P-ABAC works?



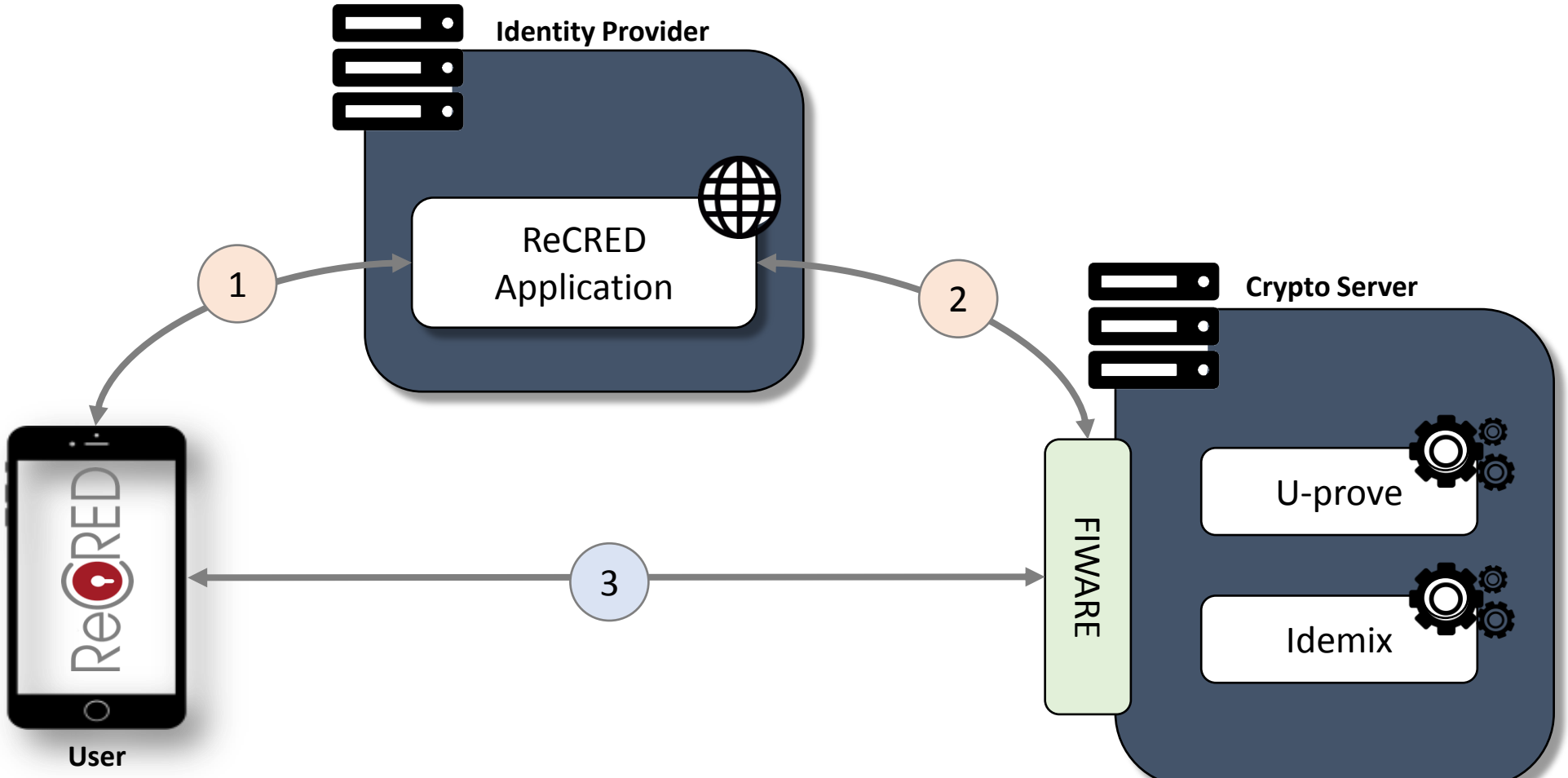
How P-ABAC works?



How P-ABAC works?

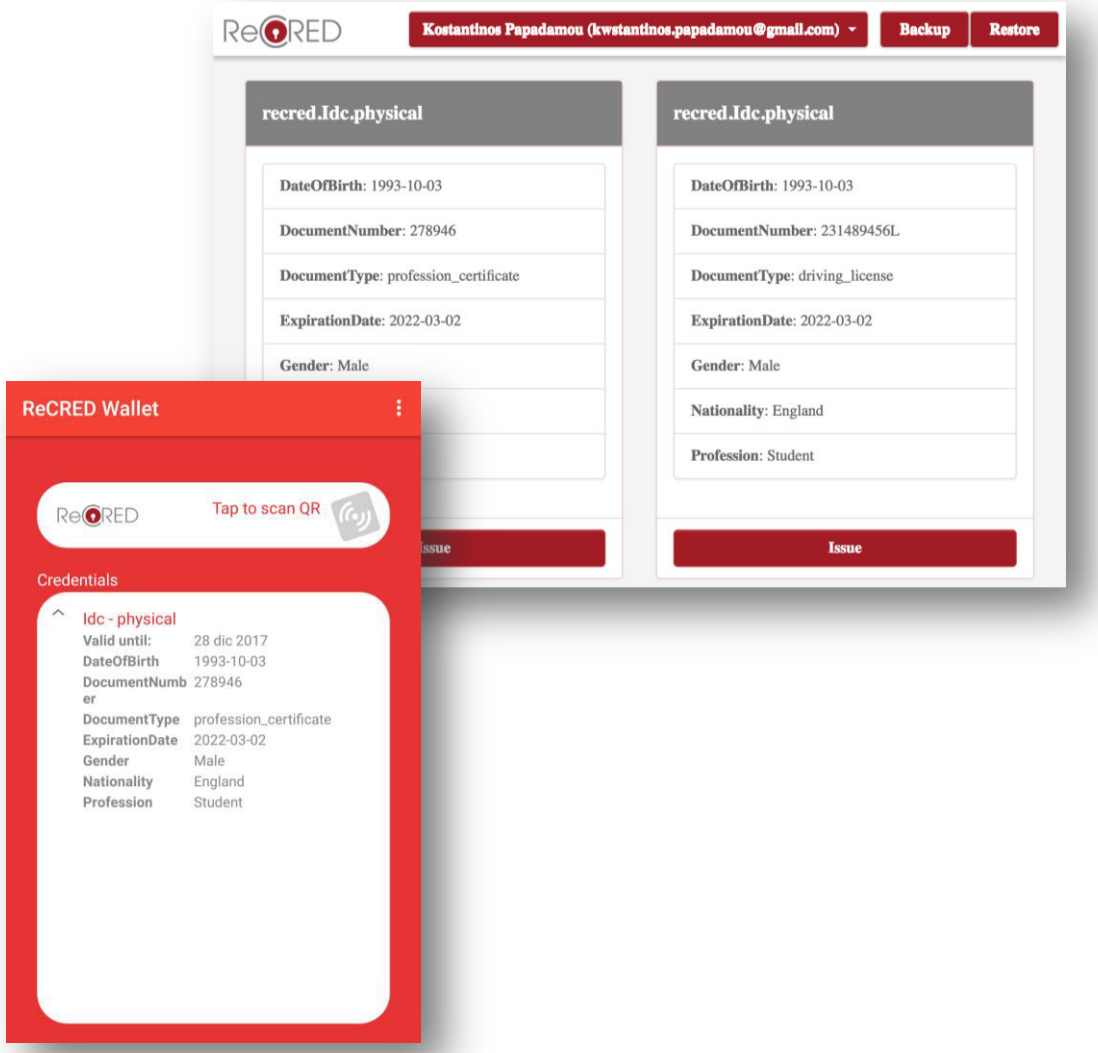


IRMA-like Architecture



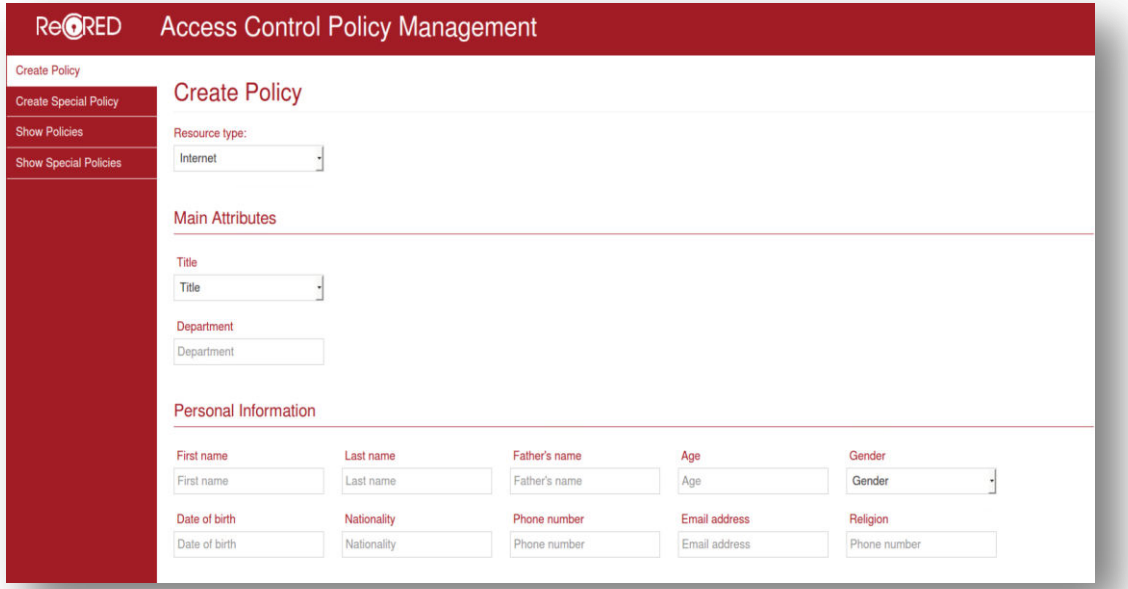
Credential Management

- Credential Management Module
  - P-ABAC Credential Definition
  - P-ABAC Credential Management
  - P-ABAC Credential Issuing
  - P-ABAC Credential Backup & Restore
- ReCRED Wallet Mobile App module
  - P-ABAC Credential Management
  - P-ABAC Credential Backup & Restore



Policy & Consent Management

- ABAC Policy Tools
  - Policy analysis/reasoning mechanisms
  - Policy suggestions for administrators
  - Policy management interface
- Consent Policy Management
  - Specific on P-ABAC credentials
  - Allows the user to define policies for the disclosure of her attributes
- Risk Assessment
  - Assess the risk of privacy leaks



P-ABAC Integration in ReCRED

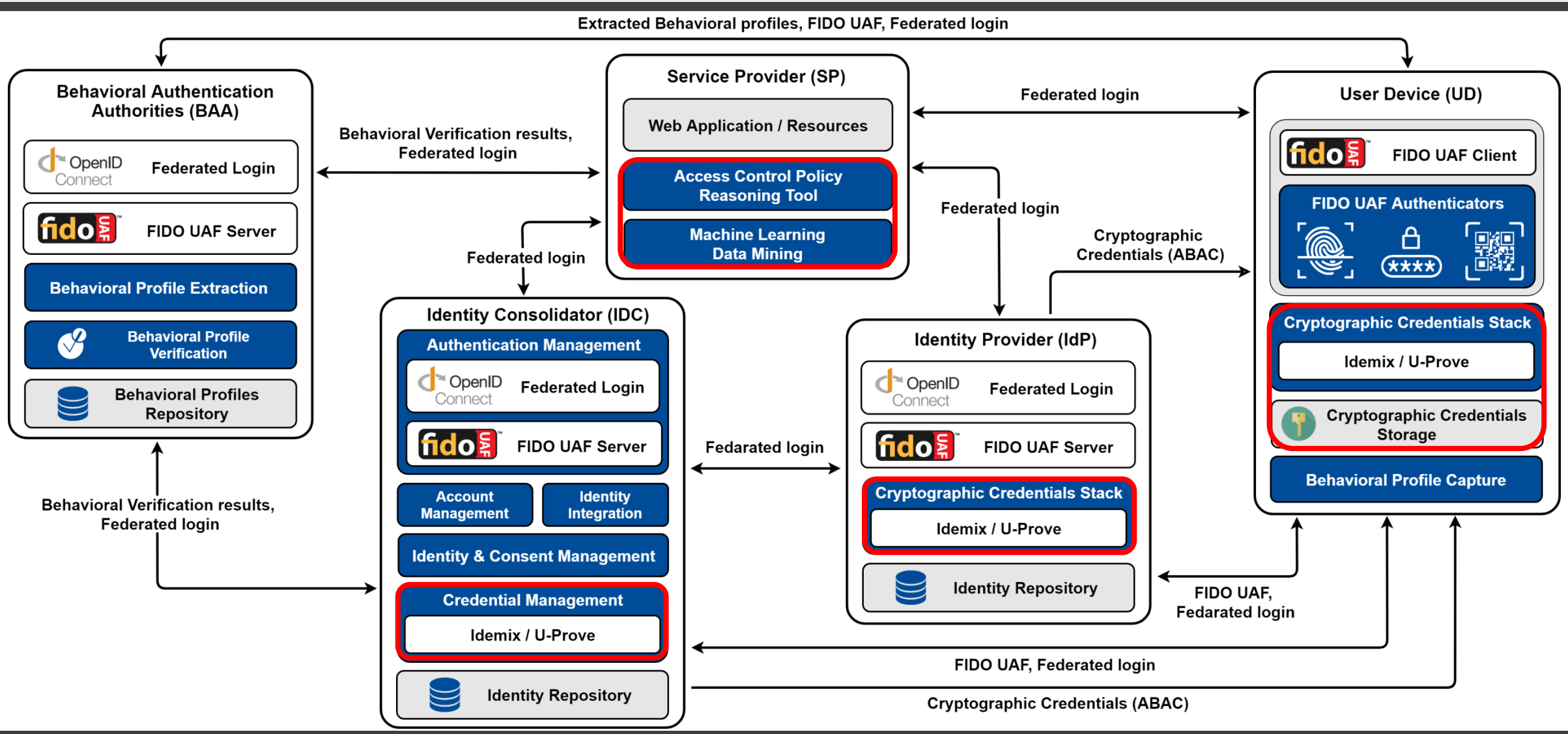
- P-ABAC integration with FIWARE
  - Unifies the interfaces of different underlying P-ABAC engines
- P-ABAC integration with OpenID Connect
  - Allows online services to use P-ABAC seamlessly
- P-ABAC integration with FIDO
  - Allows FIDO-enabled services to use P-ABAC

FIWARE

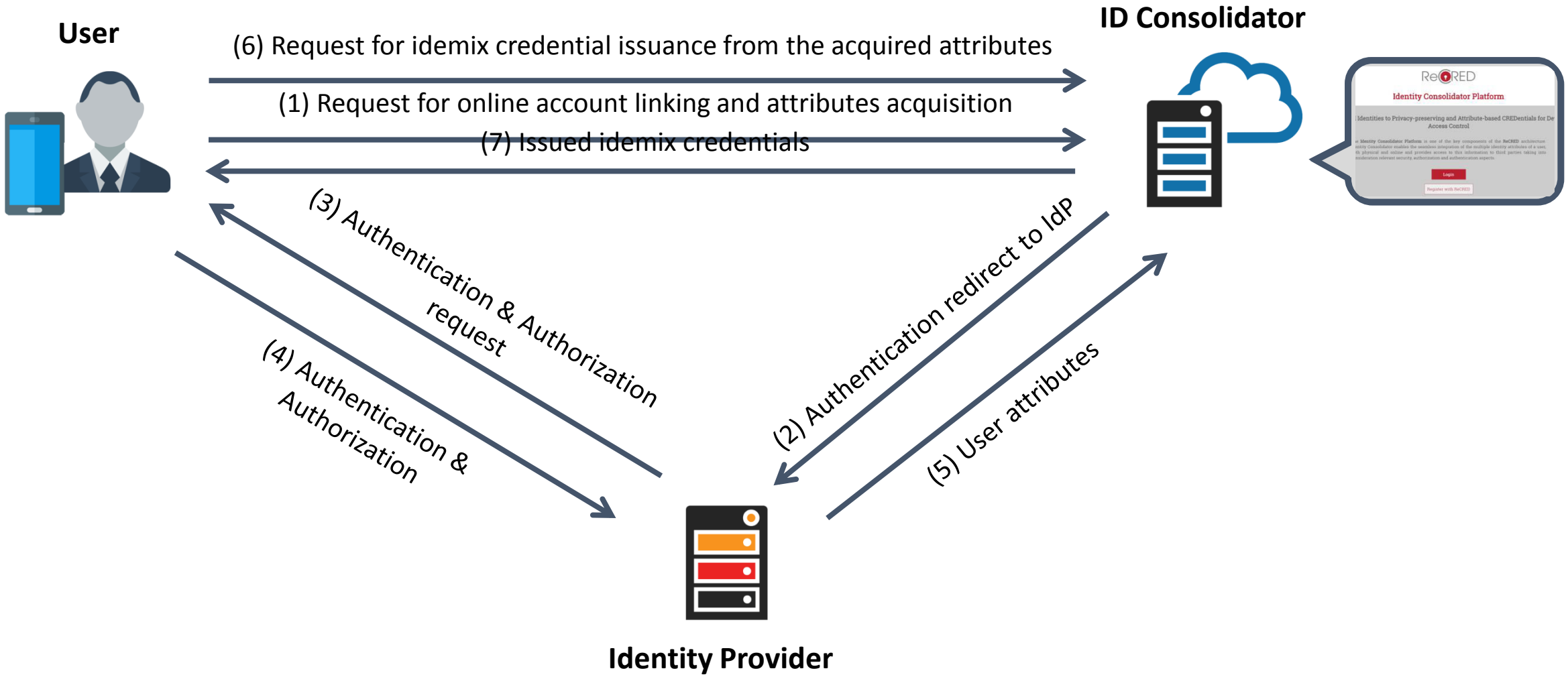
OpenID Connect

fido alliance

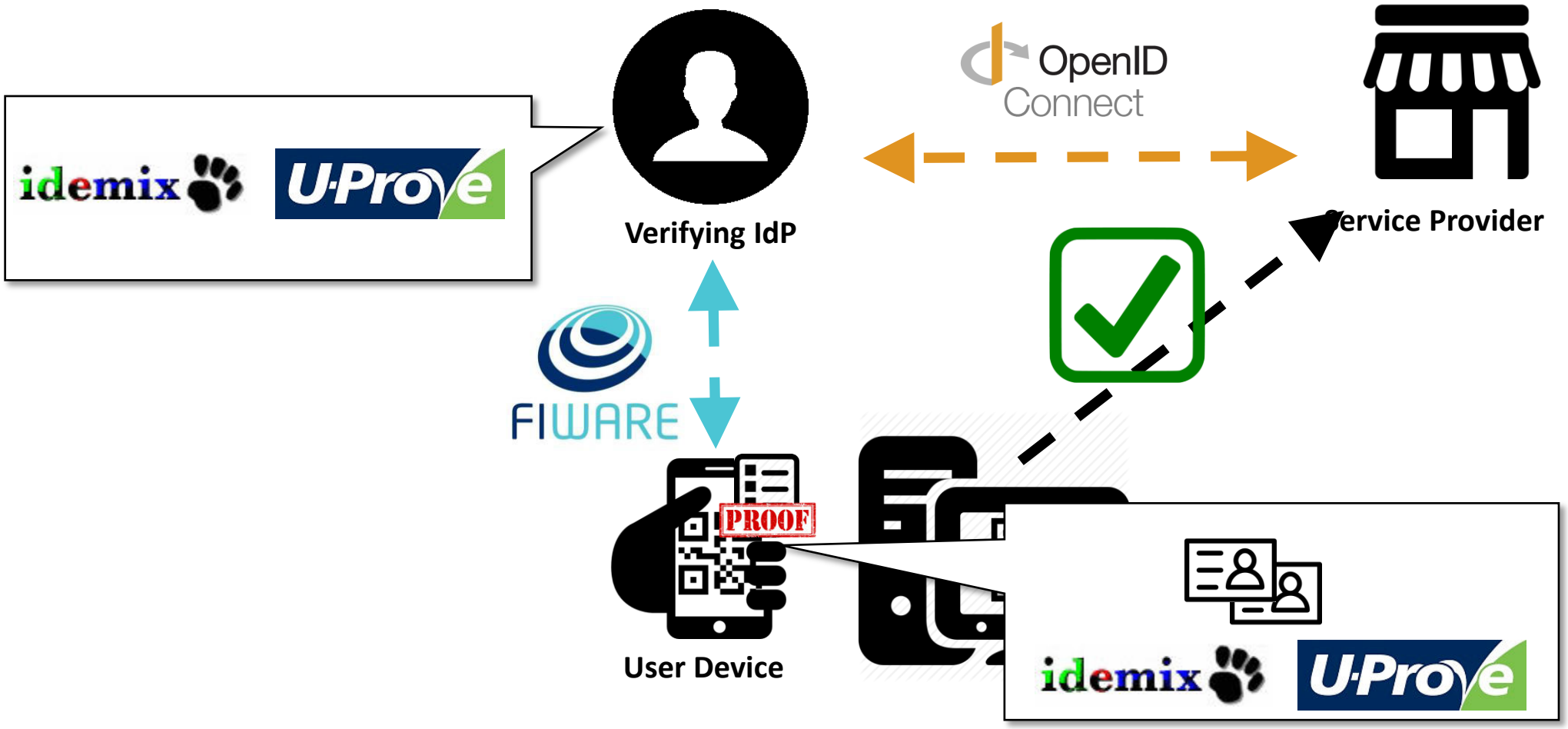
P-ABAC Integration in ReCRED



IDC as P-ABAC Credentials Issuing IdP



P-ABAC with OpenID Connect



P-ABAC Demonstrations

- Demo 6 - Credential Management
- Demo 7 – P-ABAC through OpenID Connect
- Demo 8 – Consent Management & Policy Reasoning Tool

Identity Assurance Levels (IAL)

Identity Assurance Level	Requirements
IAL1	Identity attributes are self-asserted or should be treated as self-asserted
IAL2	Remote or in-person identity proofing
IAL3	In-person identity proofing

How IALs are supported in ReCRED

Identity Assurance Level	Supported with
IAL1	Online registration
IAL2	Physical and Online identity acquisition
IAL3	Mobile Network Operators and Mobile Connect

Authentication Assurance Levels (AAL)

Authenticator Assurance Level	Provides	Requirements
AAL1	Some assurance that the user controls an authenticator registered to the Service Provider	Single-factor authentication
AAL2	High confidence that the user controls authenticator(s) register to the Service Provider	Two-factor authentication
AAL3	Very high confidence that the user controls authenticator(s) register to the Service Provider	Hard cryptographic authenticator + two-factor authentication

How AALs are supported in ReCRED

Authenticator Assurance Level	Supported with
AAL1	Backup Password + Behavioral Authentication
AAL2	Secure SIM (Mobile Connect) + Human to SIM authentication
	Backup password + FIDO
	FIDO
AAL3	Secure SIM + FIDO + Backup Password
	Secure SIM + FIDO

Federation Assurance Levels (FALs)

Federation Assurance Level	Requirements
FAL1	The Identity Provider must sign the assertion using approved cryptography
FAL2	The assertion must be encrypted using approved cryptography such that the Service Provider is the only party that can decrypt it
FAL3	The assertion must be signed using approved cryptography and encrypted to the Service Provider using approved cryptography

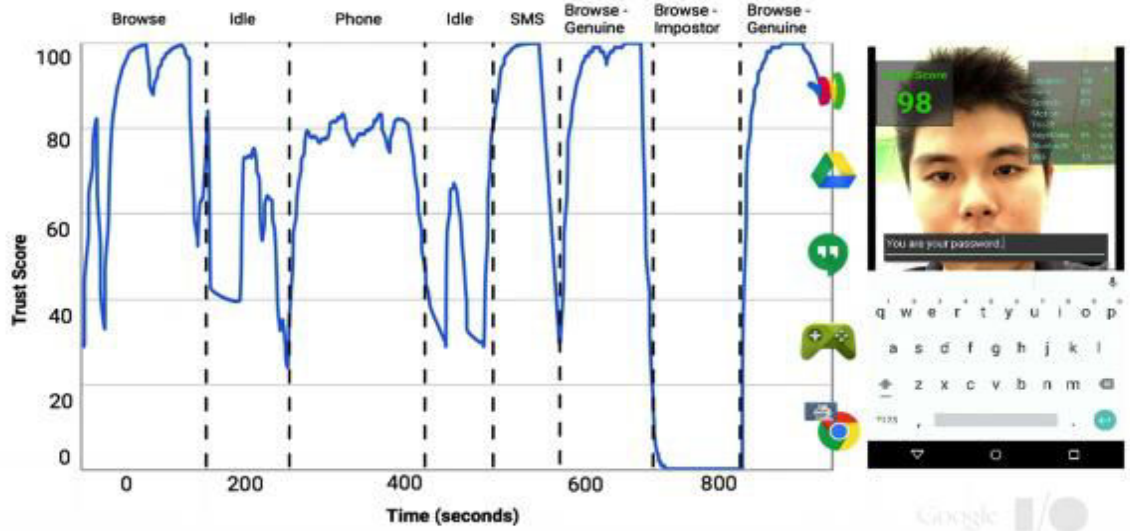
How FALs are supported in ReCRED

Federation Assurance Level	Supported with
FAL1	OpenID Connect
FAL2	OpenID Connect + ID Token encrypted with the public key of the Service Provider
FAL3	OpenID Connect + P-ABAC

Comparison with the State-of-the-art

Google Trust API (ex Abacus)

- Multi-Modal Continuous Authentication System
- Captured attributes
  - Typing patterns
  - Browsing habits
  - Location
  - Face recognition
  - Walking habits
  - Speech recognition
  - Touch dynamics



- Calculates trust score according to captured attributes

ReCRED vs Google Trust API

- **Behavioral profiles** are stored on **BAA**
  - Innovative architectural component
- **Behavioral attributes** are either captured by the **user's device** or directly by the **BAA**
- **Account-wide** lockdown and **device-wide** lockdown

WSO2 Identity Server

- **Open source product** that offers **management of multiple online identities**
- 2 ways of authentication
  - Acts as an **Identity Provider**
  - **Delegates authentication** to other Identity Providers
- **Multi-factor authentication** (FIDO U2F)
- Provides **RBAC** and **ABAC**

ReCRED vs WSO2 Identity Server

- **Physical** Identity **Acquisition** and **Verification**
- **Password-less Authentication** (FIDO UAF)
- **Privacy-preserving** Identity Consolidator
  - Increased privacy if the user desires so

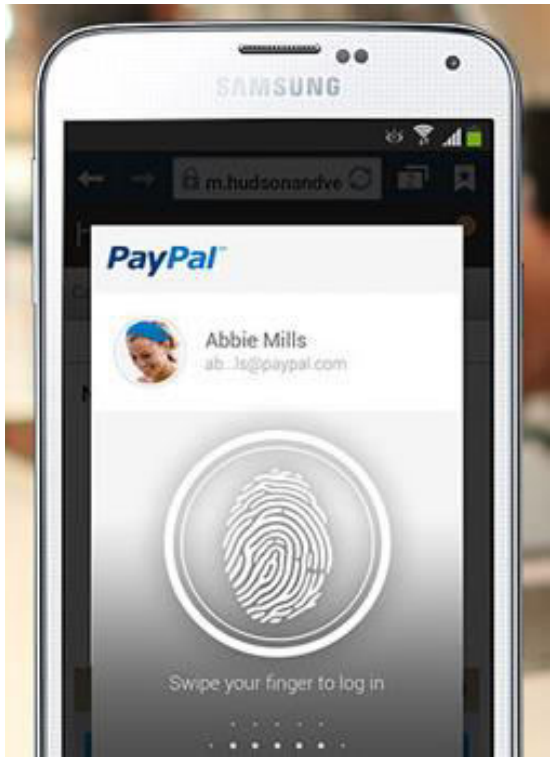
- **Locks online accounts** by performing **behavioral authentication**
- Support for **privacy-preserving ABAC** (Idemix, U-Prove, CP-ABE)

ReCRED vs Trusona

- Enhanced Physical identity acquisition and verification
- Online Identity Acquisition
- Integration with FIDO
- Behavioral continuous authentication
- Integration with **Federated ID systems** (e.g., OIDC) thus, it supports identity attributes storage or exchange

Paypal's FIDO + OpenID integration

- User authentication with FIDO UAF
- Extended OpenID Connect in order to
  - Maintain an authentication token for persistent sign-in
  - No need for re-authentication
- Purchases from multiple apps with one authentication
- Integrated with *Lenovo*, *Samsung devices* as of 2017
- **No source code released**, just a 4-page documentation



In conclusion

- We kill the password with **DCA**
- DCA requires Federation, Identity Consolidation and Behavioral Authentication for efficient **failure recovery** and **identity management**
- Since we have **DCA**, **Federation, and IDC** we can support device-centric **Privacy-preserving ABAC**

Several slides an CUT), **Alberto Caponi** and **Claud lea** (CertSign), **Steven Gevers** (V