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

Device-Centric Authentication for Future Internet

Prof. Christos Xenakis

H2020 Clustering Workshop
Athens, 31 January 2018

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

ReCRED Project – Consortium

- **Project funded by EU under H2020**
- **Call Identifier: H2020-DS2-2014-1**

www.recred.eu

UNIVERSITY OF PIRAEUS

Cyprus University of Technology

verizon

Telefónica I+D

certSIGN

cmit

institute imdea networks

THE PRODUCTIZERS

upcom
Bringing business and IT together

EXUS

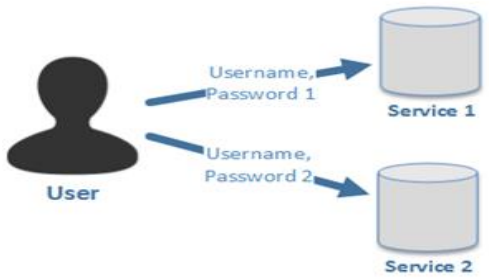
wedia

BAKER & MCKENZIE

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**

1. Password overload

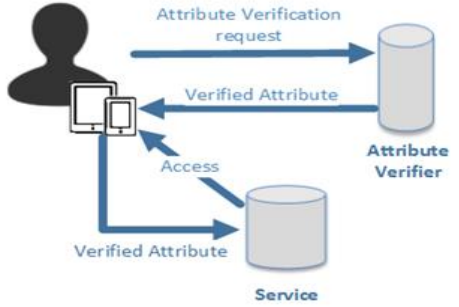


2. Identity Fragmentation

3. Lack of real-world binding

Problems addressed by ReCRED

4. Lack of support for Attribute based access contol



ReCRED's Innovation

- It allows **mobile devices** that users **habitually use** and **carry** to manage all **access control** needs
- It is aligned with **current technological trends** and **capabilities**.
- Integrates **existing** as well **upcoming** techniques of :
  - **Authentication**
  - **Identity management**
  - **Access Control**
  - **Privacy protection**
  - **Trusted computing**

New Digital Landscape

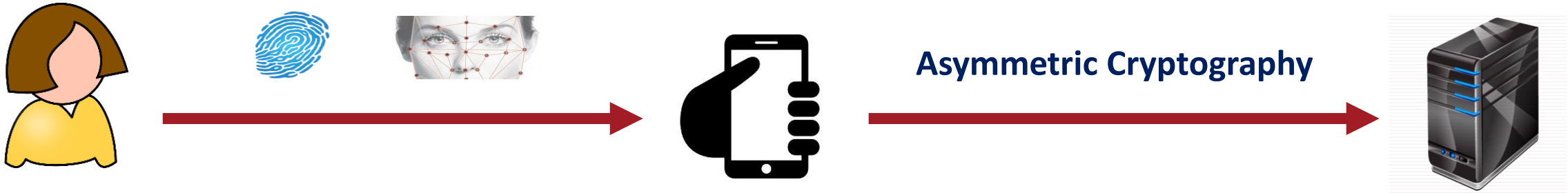
- Nowadays **e-commerce** now exceeds **1 trillion € per annum**
- **Internet of Things** becomes a reality
- **Digital economy** & **digital life require** for **reliable** and **user-friendly authentication mechanisms**
- Currently, **user authentication** relies **on passwords**, a **technology of the '60s**
  - **98%** of the **websites** use **password-based authentication**

Problem 1: What happens with Passwords ?

- Users have the **tendency** to choose **weak** & **easy-to-remember** **passwords**
- Therefore, **passwords** are **easy-to-guess** and **highly insecure**
- Passwords are **highly** **reused** **by users**
- The **security requirements** of **critical services**, such as **e-banking,** are not satisfied by **ordinary passwords**, which can be **easily stolen** or **bypassed**
- Regarding passwords **usability**:
  - **70%** of users **forget their password** **once in a month !**
  - Users **tend to try** on average **2.4 passwords** before they **type the right one !**

Questions arise regarding authentication

- Can I **login** without using **passwords**, **easily** and **securely**
  - **Fast IDentity Online (FIDO)**
  - **Device Centric authentication**
  - By using **strong asymmetric cryptography, transparently to end users**
  - **FIDO members** → Google, Paypal, Microsoft, Visa, Samsung, Intel, American Express, Bank of America, etc.



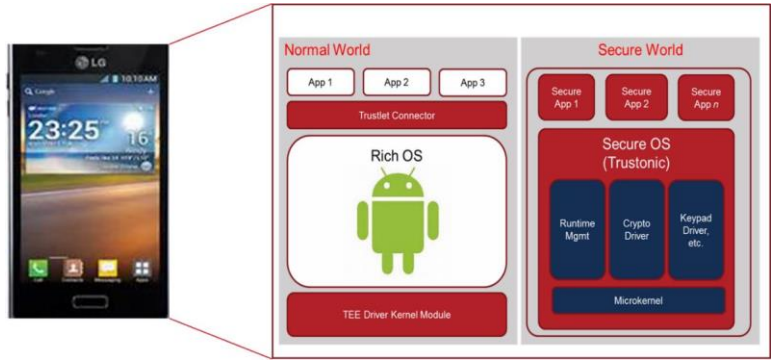
FIDO UAF provide several advantages !!

- It offers **strong authentication** based on **public key cryptography**
- It simplifies both **registration** and **authentication**
- There is **no need** for **maintaining passwords**
  - Dealing with **complex password rules**
  - Going through **password recovery**
- It **enhances users' privacy** since all **identifying info is stored locally**
- **But** the **UAF protocol** relies on the **assumption** that
  - the **UAF authenticator** & **UAF client** are **trusted** and **cannot be tampered**

fido alliance
simpler stronger authentication

Wait a minute… !!!

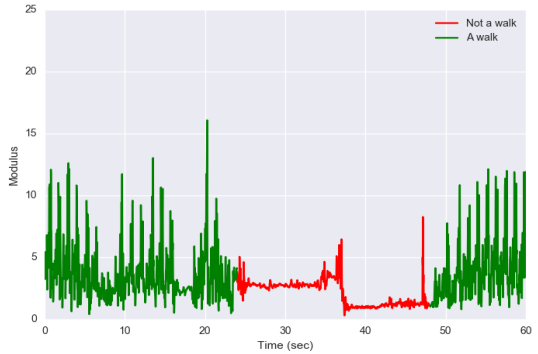
- My mobile device is the **gateway** to my **digital life**
- What If my mobile device is:
  - **Compromised**
  - **Stolen**
  - **Broken**
  - **Lost**
  - **Replaced**

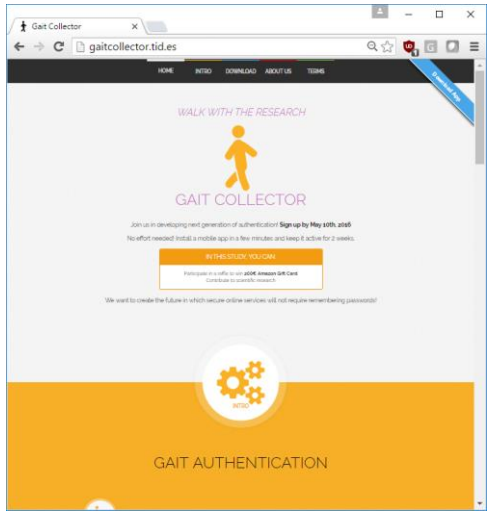


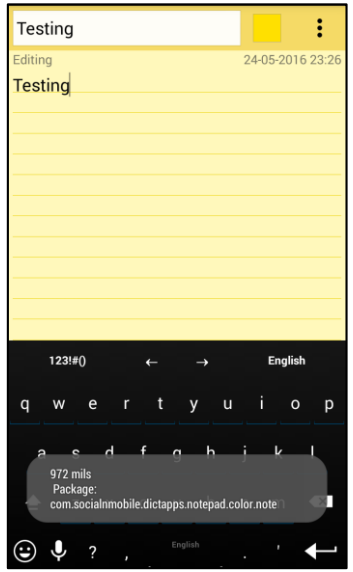
Behavioral Authentication

Behavioral Authentication

- Within **ReCRED**, we have developed **four** different types of **behavioral authentications**:
  - Key stroke
  - Browsing habits
  - Mobility
  - Gait
- Latch for account locking







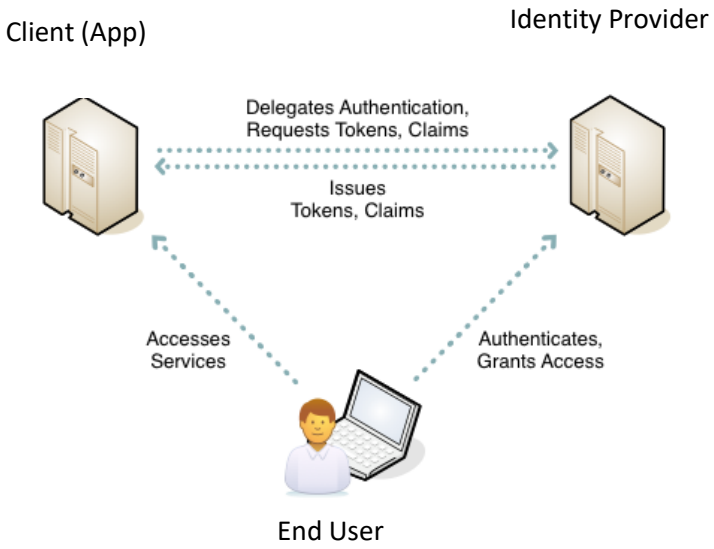
Problem 2: Identity Fragmentation – Online Accounts

- Today's Internet users are registered in **too many online services**
  - **Email** (Gmail, Yahoo), **social media** (Facebook, Twitter, LinkedIn), **e-banking**, **corporate applications**, **cloud providers** (dropbox, office 365).
  - Each one use a **different** **authentication method** & **authentication credentials**

- **Questions arise:**
  - Can I **consolidate** & **manage** **securely** all these **identities & accounts**, **from a single device**
  - Can I **control my privacy** & **give my consent** for using my **personal data (GDPR)**
  - Can I **link** my **online accounts** e.g., facebook with google
  - Can I **link** an **online account** with my **physical identity** e.g., ***e-bay to sell my laptop***

FIDO – Federated authentication - OpenID Connect

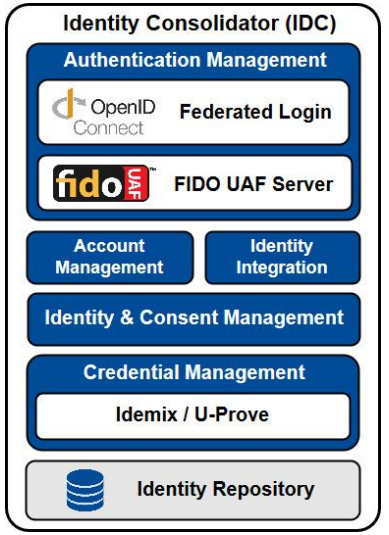
- **OpenID Connect** (federated authentication) delegates authentication
  - Online services authenticate their users by employing **Google**, **Microsoft**, **Twitter**, **LinkedIn** accounts, etc.
- **OAuth 2.0** (Open standard for Authorization)
  - Issues and uses **access tokens** to be used for **authorization**
- **User: less passwords** to remember
- **Service providers:** no need for **password maintenance**
- **ReCRED's approach** = **Fido+(OpenID Connect/OAuth2.0)+BAA**



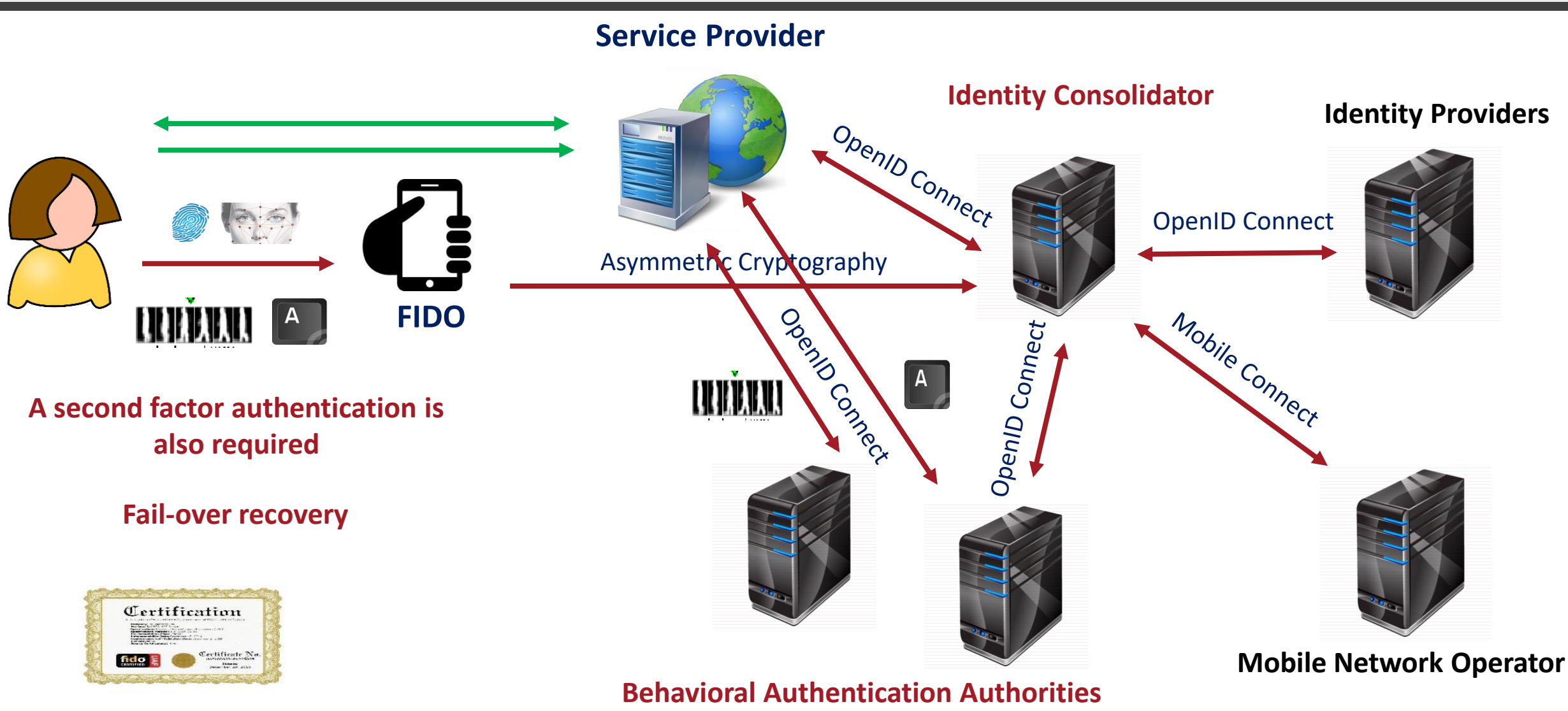
Identity consolidation & management

- **Identity Consolidator** is the central entity of **ReCRED**
  - It is a **identity provider (idp)** , that acts a **trusted third party** and provides **users' authentication**
  - Manages all **access control needs** of the users and supports **federated authentication**

    →Using my **UNIPI account**, **gmail account**, **BAA**, **Vodafon subscription**, etc.
  - It **issues** and **verifies** **cryptographic credentials** *(we will talk about this later on…)*
  - Performs **fail-over recovery** (in case of lost or damaged devices)
  - It horizontally **binds** the **online identities** of a users
  - Collects **identity attributes** from various IdPs **upon user's request**
  - Enable users to **control the level of privacy** on their **personal data**
  - For data usage, **users' consent** **is required**



Device Centric Authentication - DCA



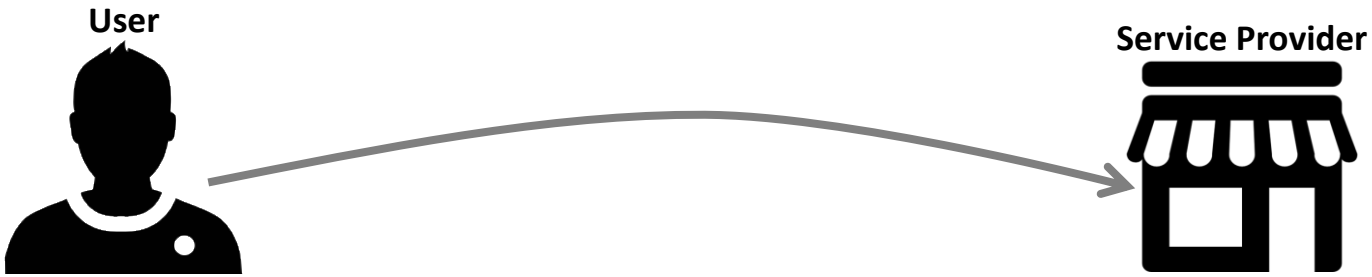
Problem 3 : I want Anonymity

- **But, OpenID Connect** does not provide any **anonymity !!**
- I want to have access to an online bookstore **that has a discount if I have the specific attributes** or **properties:**
  - I am **over 22**
  - I am a **student**
  - I am **EU citizen**
- I want to **ensure my anonymity controlling my privacy**
  - **I do not want to reveal any additional personal information**

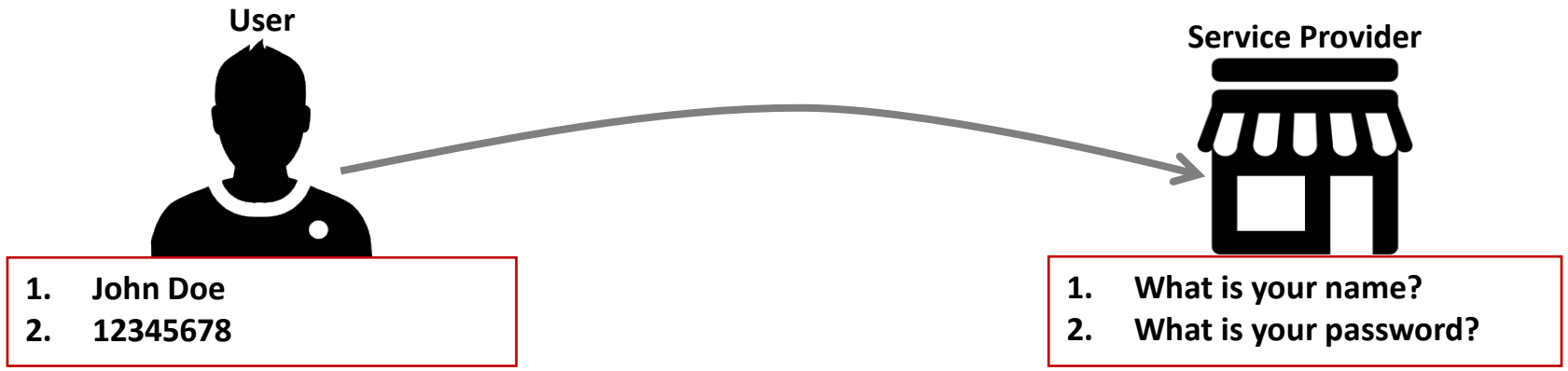
Privacy Preserving Attribute-Based Access Control (P-ABAC)

- **Privacy preserving Attribute-based Access Control - Anonymous Credentials**
  - Authentication with **pseudonyms**
- **Account-less access through verified identity attributes**
  - Age, Location, Affiliation, etc.
- **Reveal** to services **only** the **minimum identity information** that is needed
- **Two implementations**
  - **Idemix by IBM**
  - **U-Prove by Microsoft**
- **Advanced cryptography**
  - Zero knowledge, & blind signatures

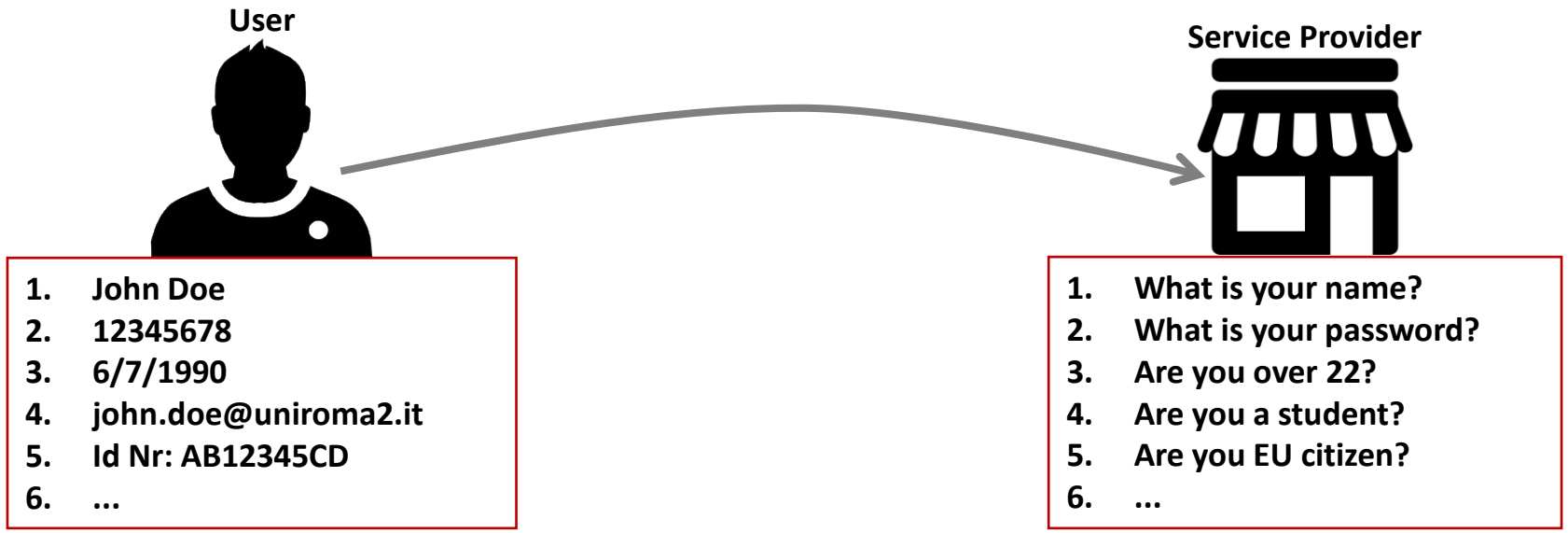
How P-ABAC works? (I)



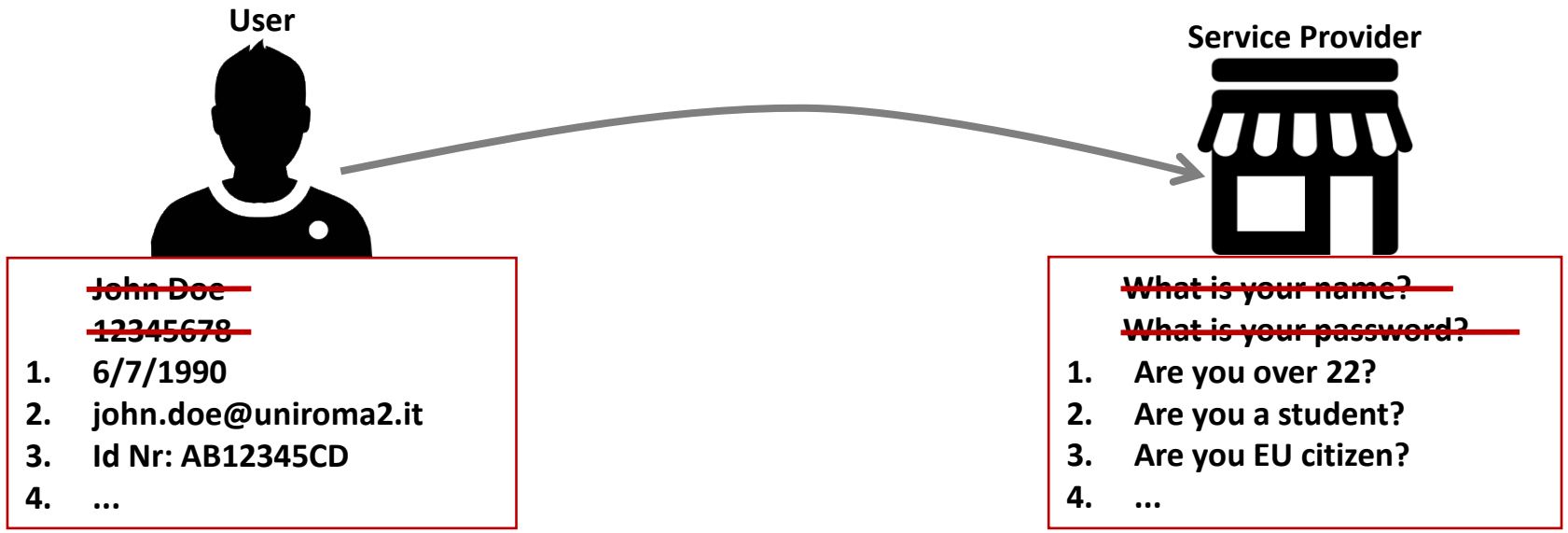
How P-ABAC works? (II)



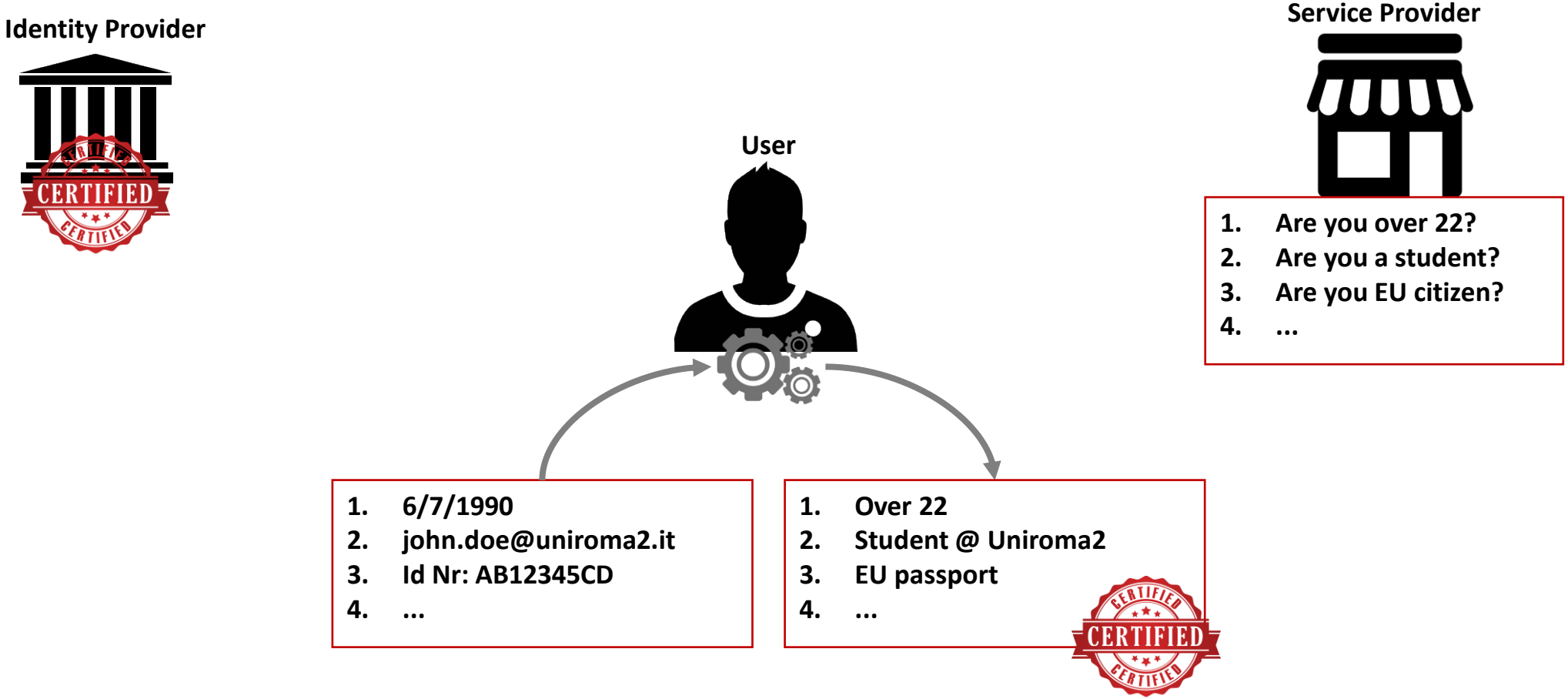
How P-ABAC works? (III)



How P-ABAC works? (IV)



How P-ABAC works? (V)

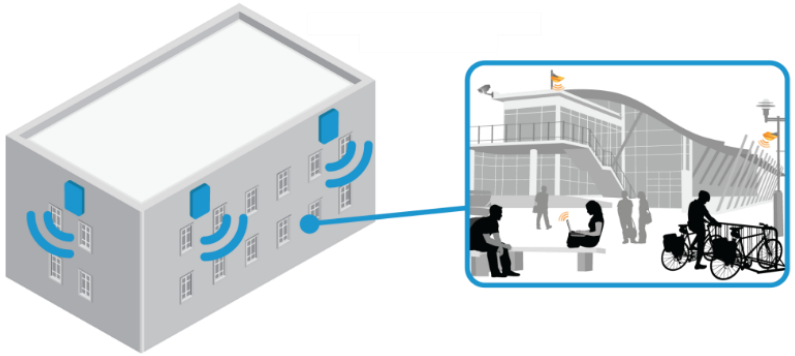


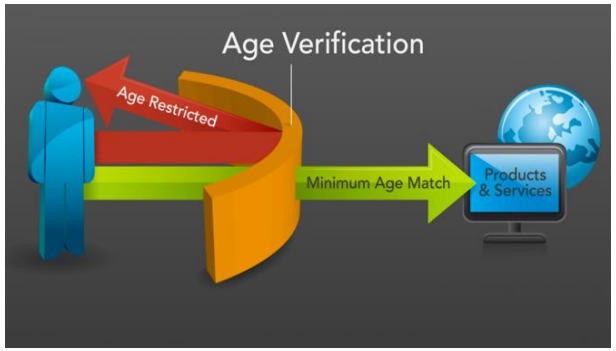
ReCRED's Innovation

- **Standardized** and **secure** authentication using **FIDO**
  - **FIDO protocol implementation**
- **Multifactor** & **easy to use password-less** authentication
  - Both **biometrics** and **behavioral** authentication
- **Security-by-design** by employing the **crypto functions** and **secure storage** of **TEE**
  - Implementation of **secure world applications** with **C programming language**
- **Identity Consolidator** as a **trusted registry** which offers
  - Identity **federation** & **management**, **user consent**, as well as reliable **failure recovery**
- **Privacy-by-design** of **online identities** using **anonymous credentials**
  - **Idemix** and **U-Prove** implementation
  - **Attribute-based Access Control policies**

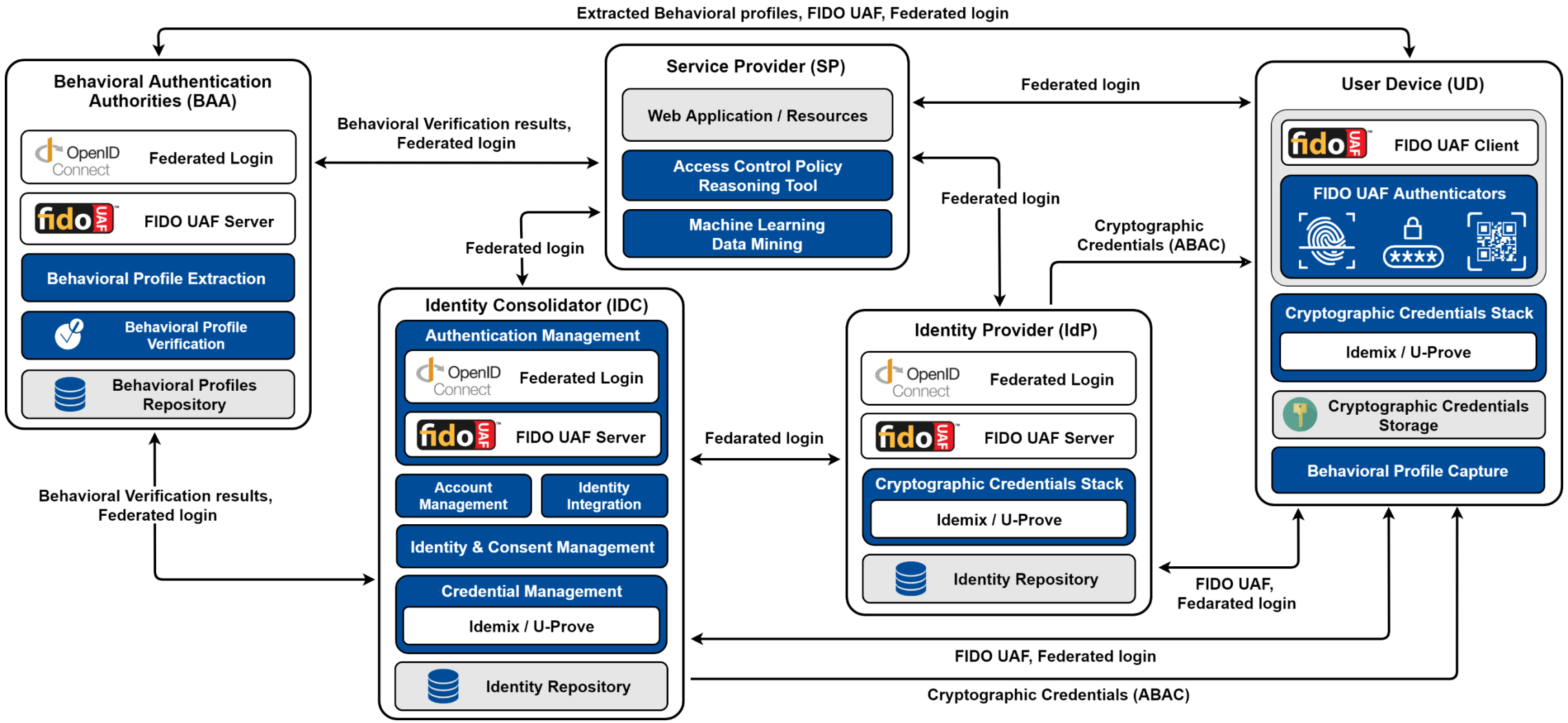
Business Cases

Campus Wi-Fi and Campus-restricted Web Services



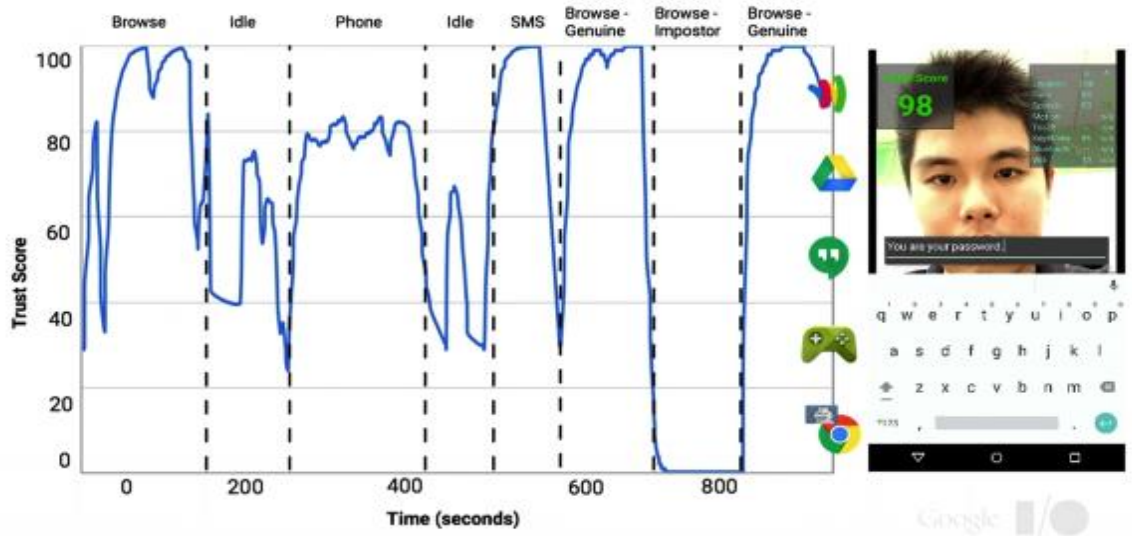


Reference Architecture



Google Trust API (Abacus)

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



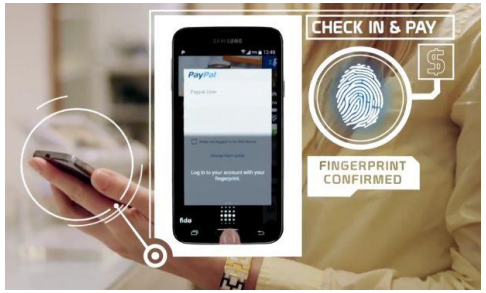
- Calculates trust score according to captured attributes

ReCRED vs Google Trust API

- **Behavioral** profiles are **stored on BAA**
  - **Extra layer of security**
- **Behavioral** attributes are **captured** either by
  - the **user's device**
  - the **BAA**
- **Account-wide lockdown**
- **Device-wide lockdown**

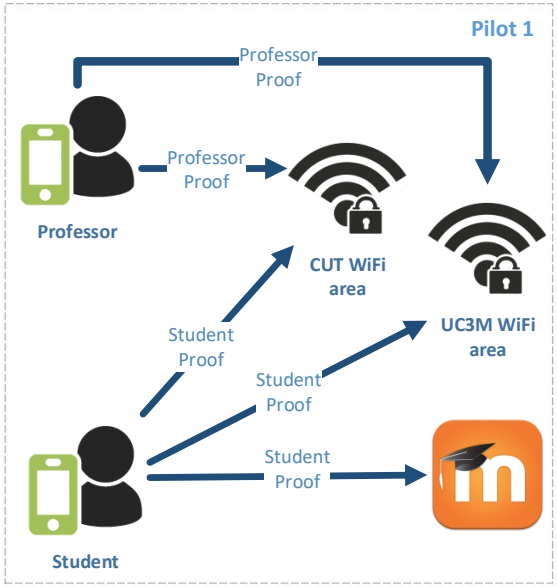
Paypal's FIDO + OpenID integration

- Users 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

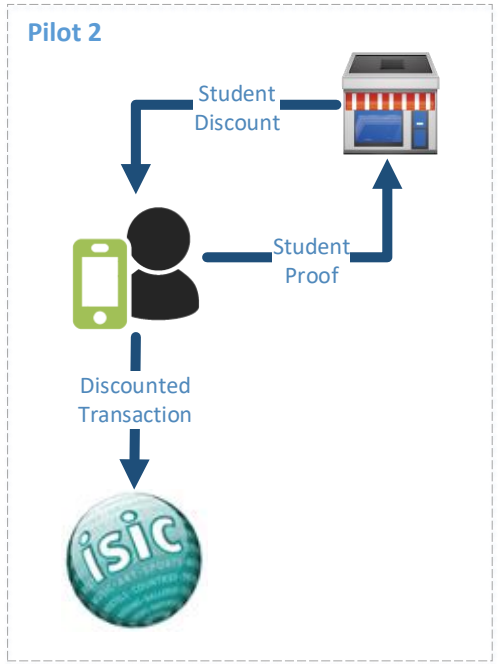


ReCRED's pilots

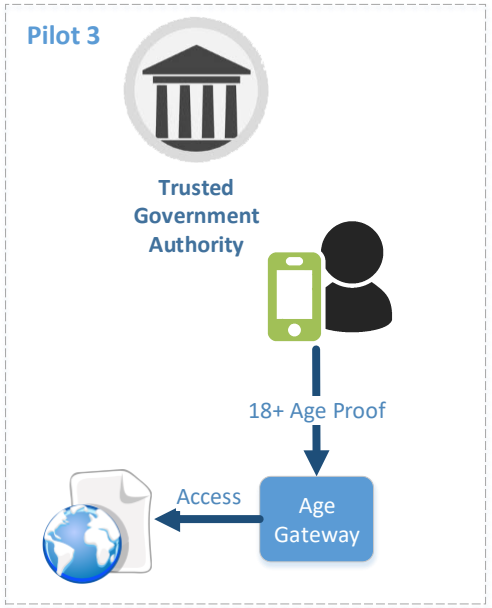
Pilot 1: Device-centric campus WiFi and web services access control



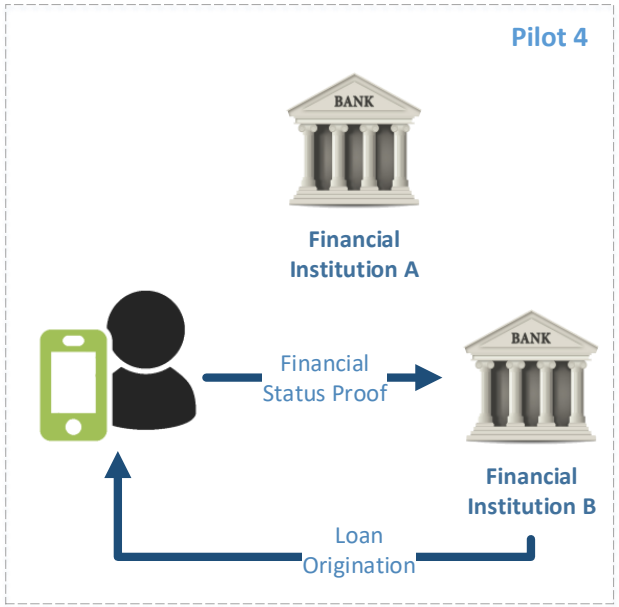
Pilot 2: Student authentication and offers



Pilot 3: Attribute-based age verification online gateway



Pilot 4: Financial services – microloan origination



Christos Xenakis

Systems Security Laboratory

Department of Digital Systems

http://ssl.ds.unipi.gr/

http://cgi.di.uoa.gr/~xenakis/

email: xenakis@unipi.gr

Thank you

https://www.youtube.com/channel/UClVzn8b6g_vE3dxzV1sli0g

https://www.facebook.com/ReCREDH2020/

https://www.linkedin.com/groups/8470632

https://twitter.com/ReCRED_H2020