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

Addressing the problems with passwords: the ReCRED's approach for device-centric access control

Prof. Christos Xenakis
Department of Digital Systems
University of Piraeus Research Center

European Commission
Horizon 2020
European Union funding
for Research & Innovation

ReCRED Project – Consortium

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

wedia

EXUS

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

THE PRODUCTIZERS

verizon

Telefónica
Telefónica I+D

cnit

institute imdea networks

upcom
Bringing business and IT together

certSIGN BY UTI

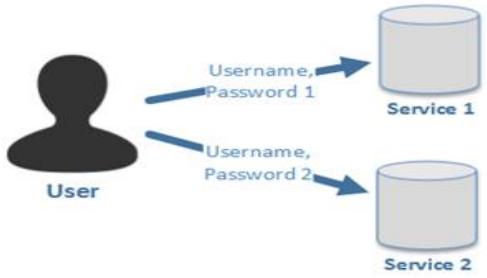
BAKER & McKENZIE

www.recred.eu

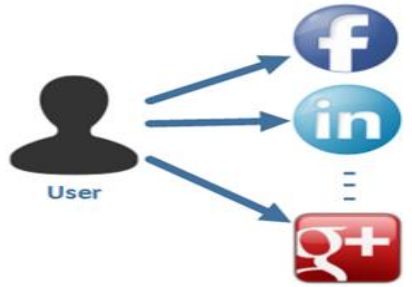
ReCRED's goal

- 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



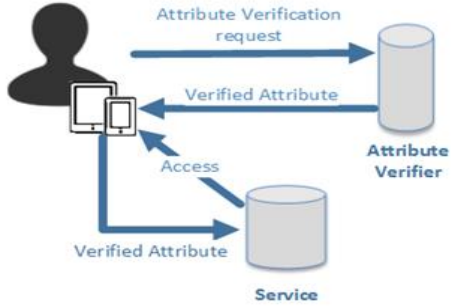
2. Identity Fragmentation



3. Lack of real-world binding

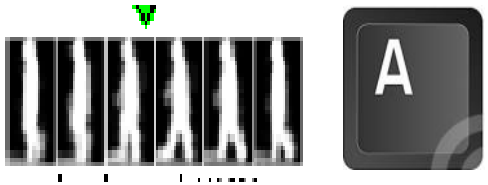
Problems addressed by ReCRED

4. Lack of support for Attribute based access contol



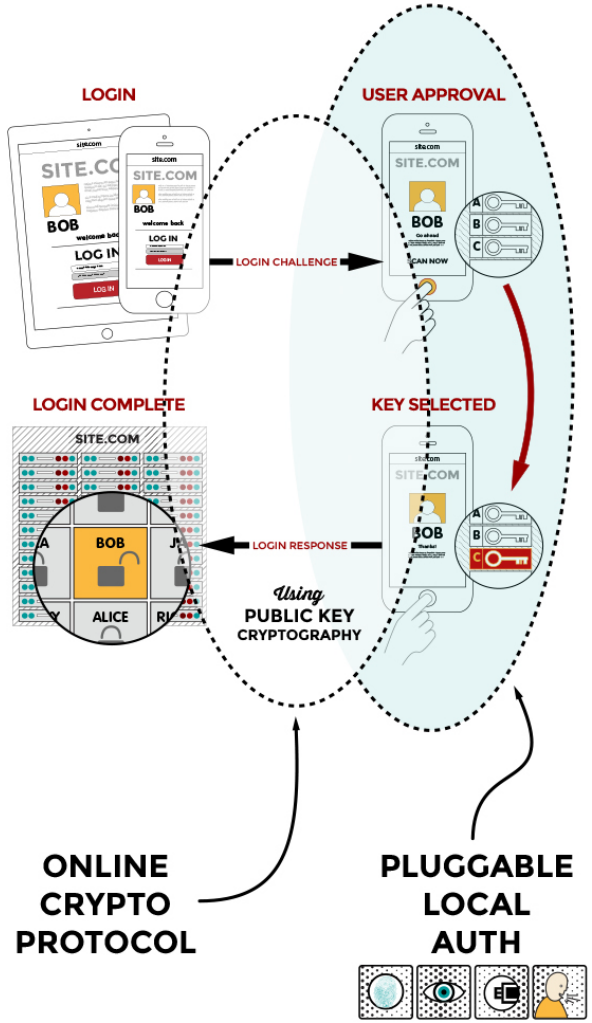
ReCRED's Concepts

- User to Device & Device to Service.



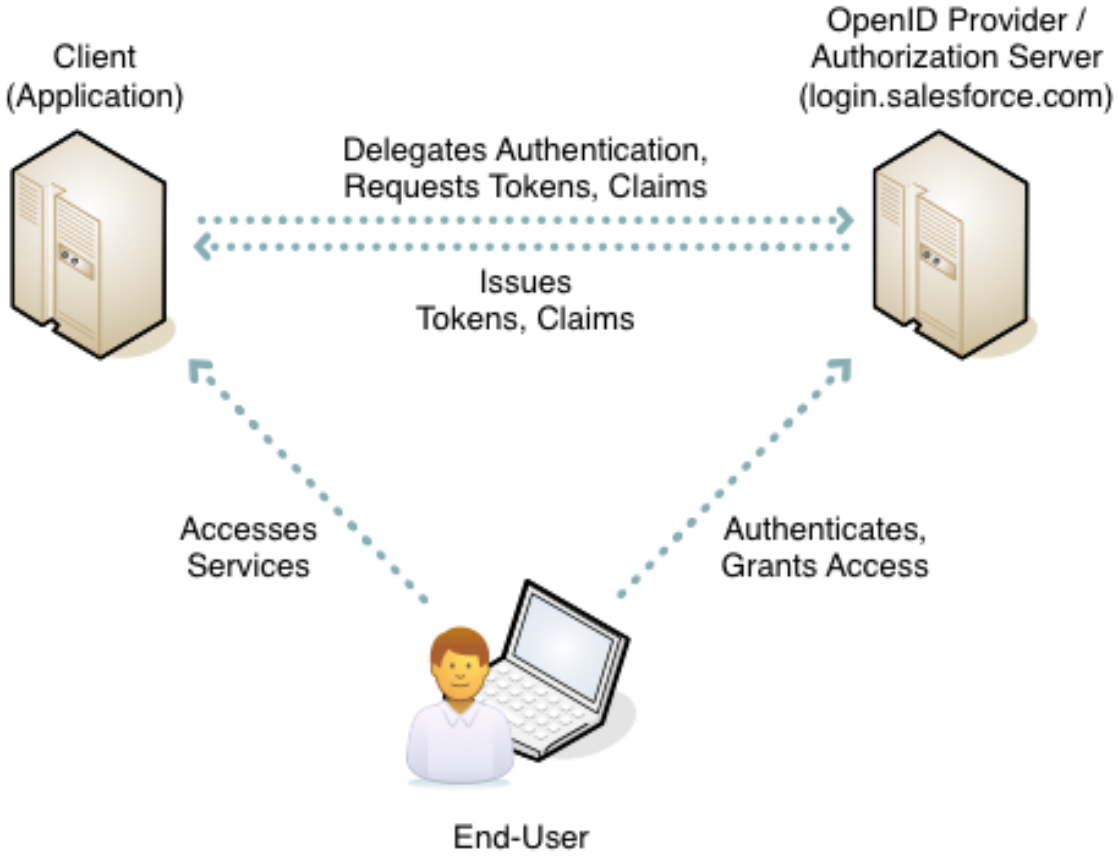
ReCRED's approach - employed technologies

- **FIDO** (Fast IDentity Online)
  - Standardized protocols for password-less authentication



ReCRED's approach - employed technologies

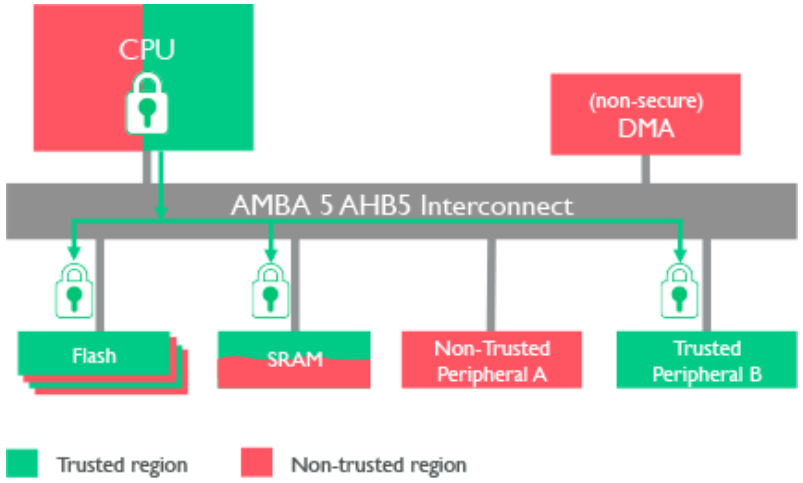
- **OpenID Connect** (Single Sign On)
  - Online services authenticate their users by employing **Google**, **Microsoft**, **PayPal**, accounts
  - **Mobile Connect** (Mobile operators as ID providers)
- **OAuth 2.0** (Open standard for Authorization)
  - Issues and uses **access tokens** to be used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

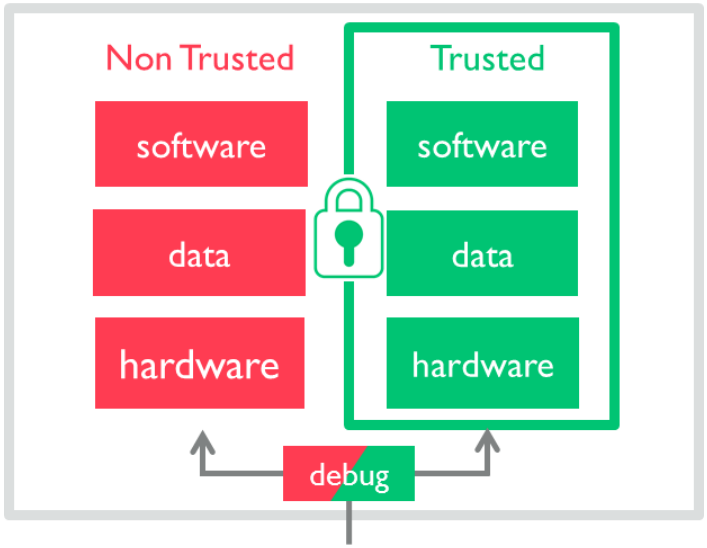


ReCRED's approach - employed technologies

- **Trusted Execution Environment** (TEE)
  - A secure area of the main processor of a smart phone that provides secure storage and cryptographic functions

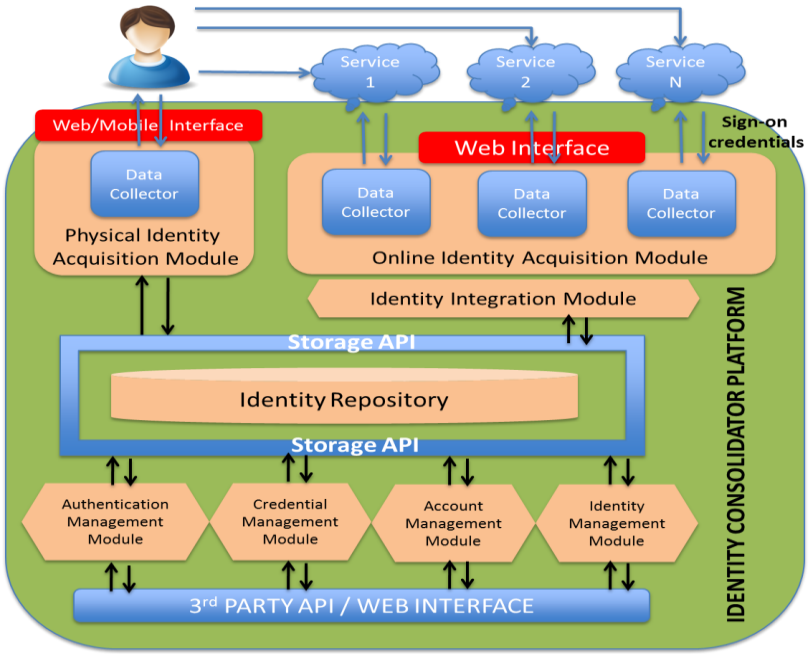
ARM TRUSTZONE
System Security





ReCRED's Concepts

- **ID Consolidator Credential Management Module**
  - Identity Consolidator
  - Real-to-online identity mapping



ReCRED's Concepts

- **Attribute-based Access Control**

idemix
pseudonymity for e-transactions

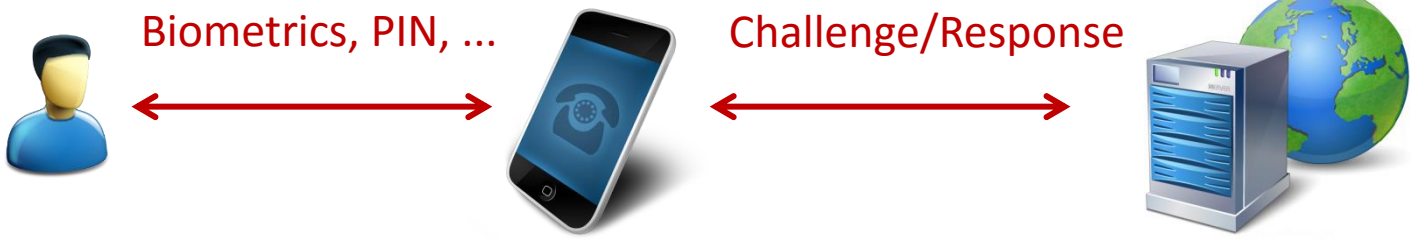
U-Prove

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

Issue cryptographic anonymous credentials

Architecture

FIDO Authentication



Identity Consolidator

Service Provider

Identity Providers

Architecture

Federated identities with OpenID Connect/OAUTH 2.0

Single Sign On

Service Provider

Single Sign On

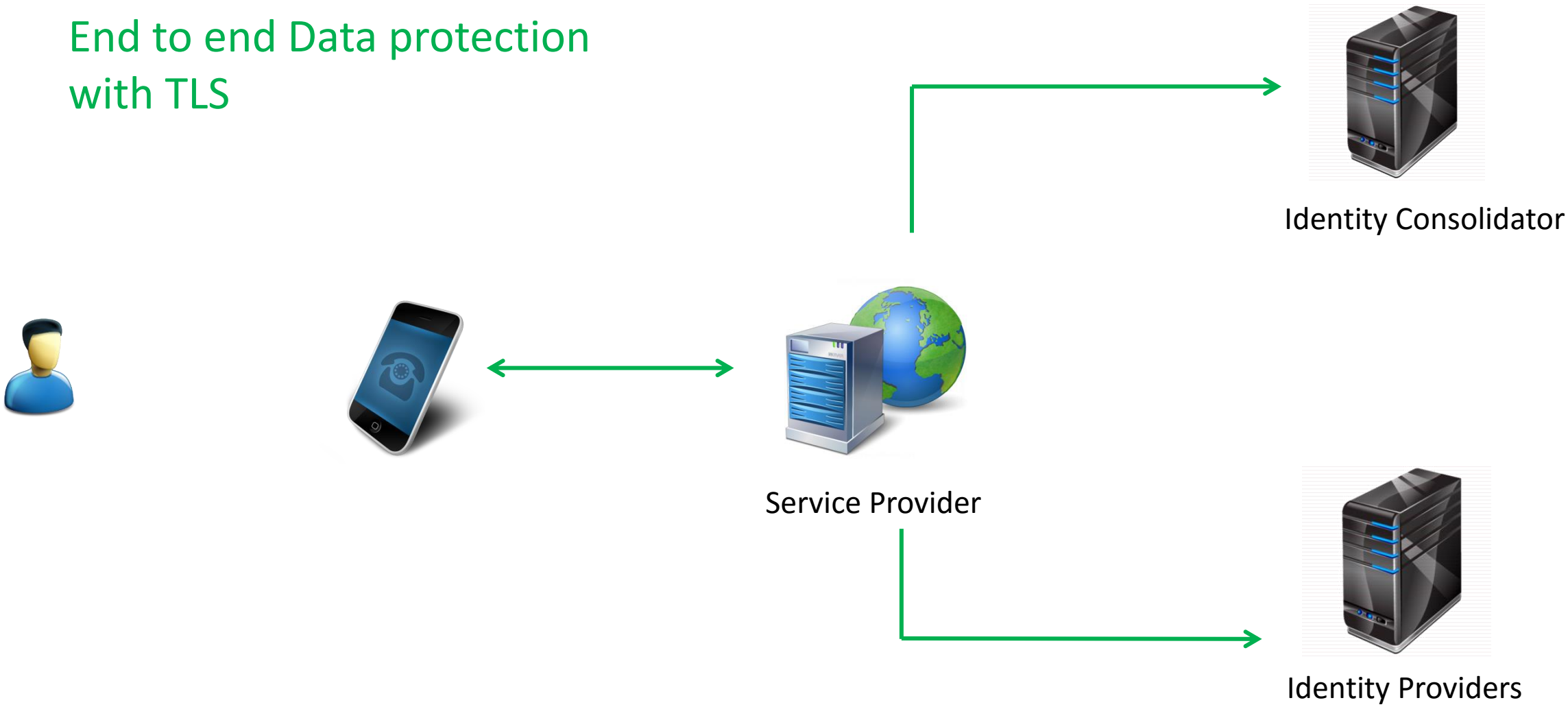
Identity Consolidator

Single Sign On

Identity Providers

Architecture

End to end Data protection with TLS



ReCRED's Innovation

- **Standardized** and secure authentication using **FIDO**
- **Multifactor** & **easy to use** password-less authentication
  - Biometrics and behavioral authentication
- **Single Sign On** (SSO) with federated identities
- Enhanced security & privacy by employing the crypto functions and secure storage of **TEE**
- Privacy of **online identities** using **anonymous credentials**
  - Unlinkability & untraceability
  - **Attribute-based Access Control**

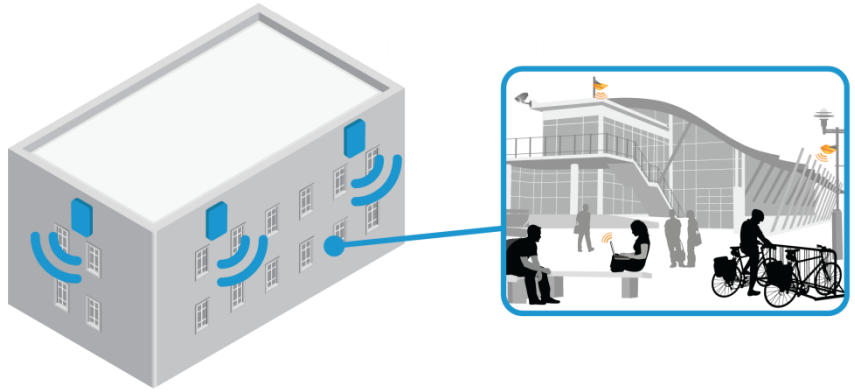
ReCRED's Innovation

- It anchors all access control needs to mobile devices that users habitually use and carry.
- It is aligned with current technological trends and capabilities.
- It offers a unifying access control framework
  - On-line authentication and authorization
  - Using off-the-self mobile devices
- It is attainable and feasible to implement in the existing products.

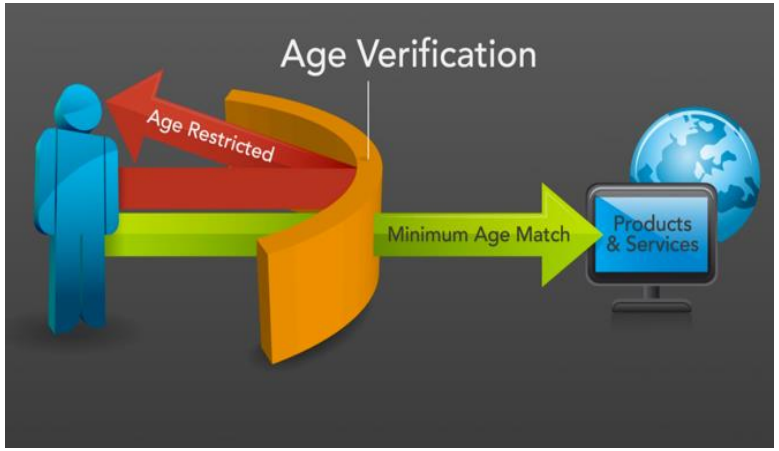
Business Cases

Mobile device data protection

Support to financial services



Campus Wi-Fi and Campus-restricted Web Services

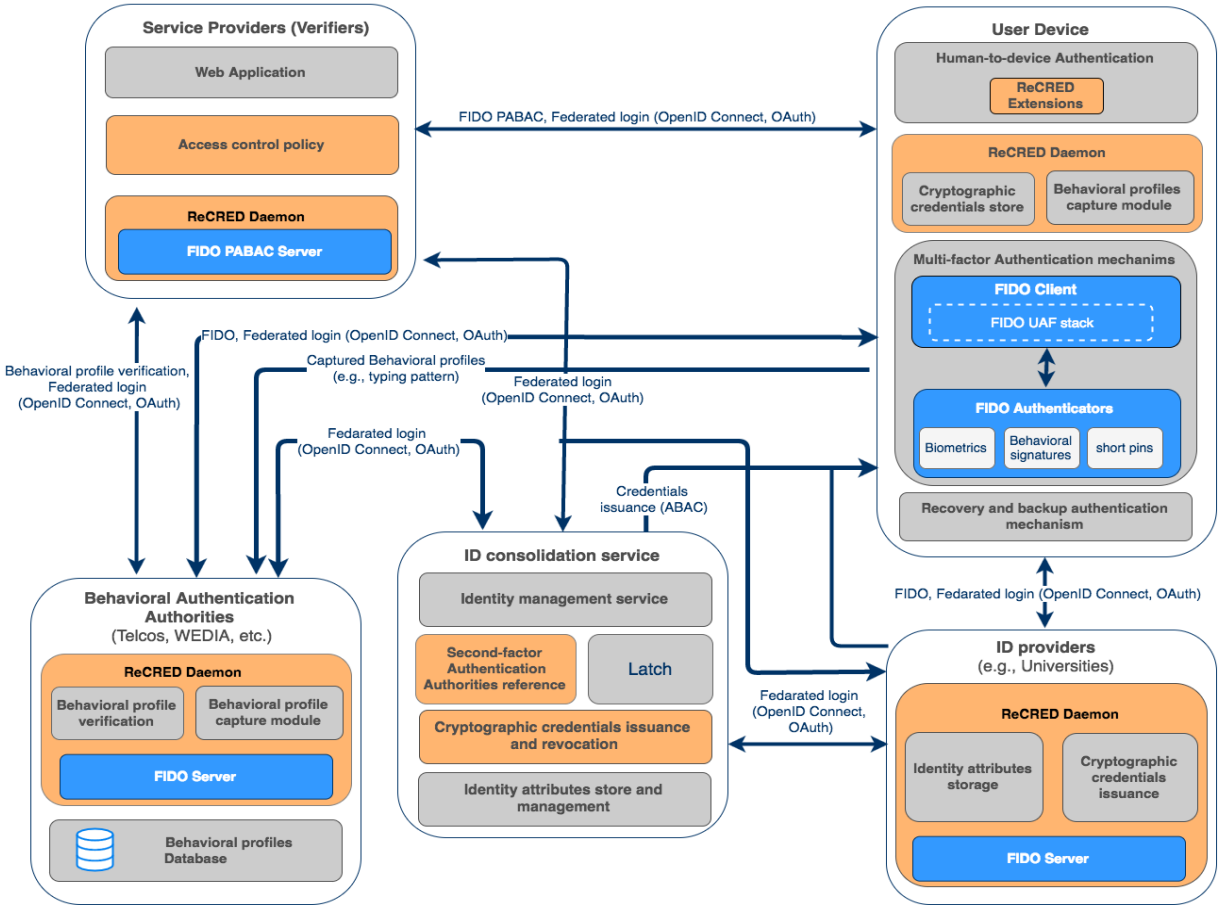


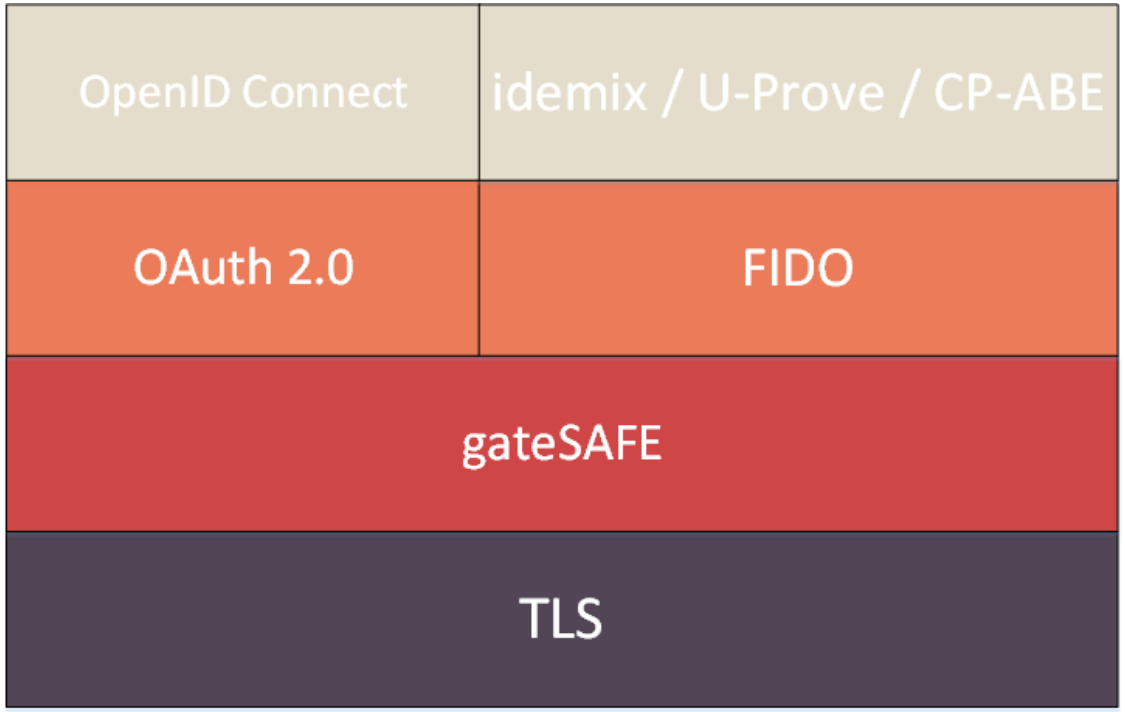
Age Verification

Student Authentication and Offers

Reference Architecture

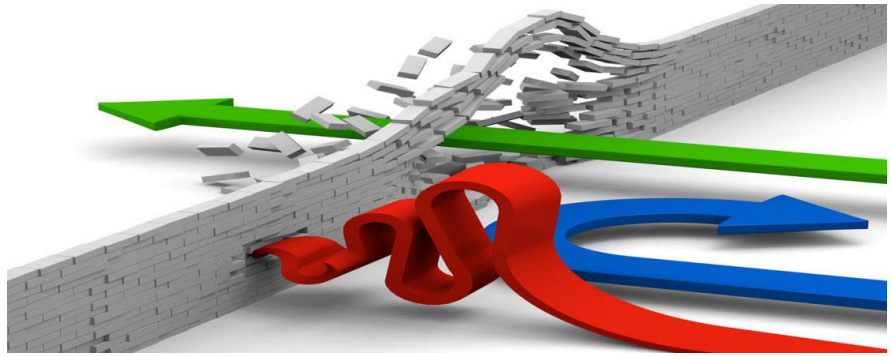
- Definition of the ReCRED architecture





Security and privacy assessment

- Evaluated compliance with **EU directives**
  - 95/46/EC
  - 2002/58/EC
  - 2006/24/EC
- ReCRED is compliant with the **EU legislation**
- Assessment of data privacy and security of ReCRED architecture
- Described process of
  - Code Review
  - Penetration Testing

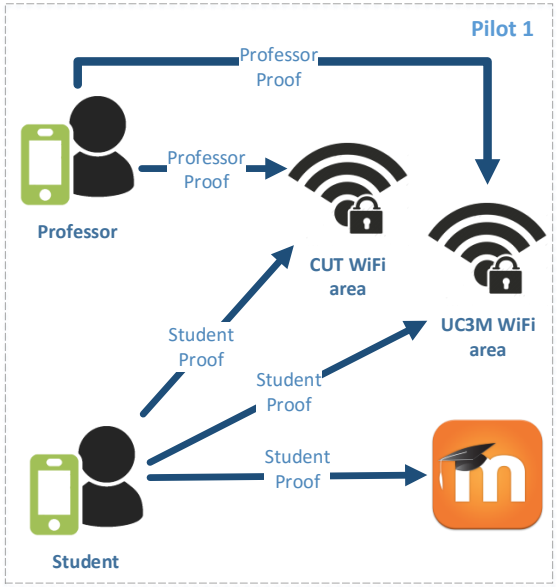


Campus Wi-Fi and Web Services Pilot

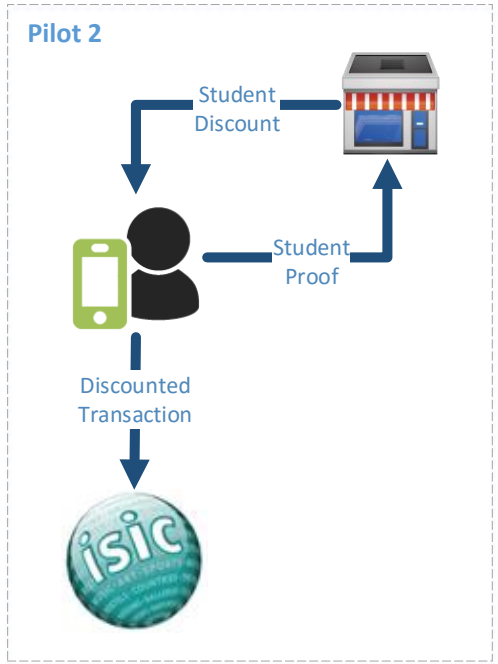
- **First integrated system**
- Started recruiting students from university and library
- Students can access Web Services
  - Device-centric Authentication
  - Password-less experience
  - Fine-grained control of identity attributes to be revealed (ABAC)
- **FIDO + OpenID Connect Integration**

ReCRED's pilots

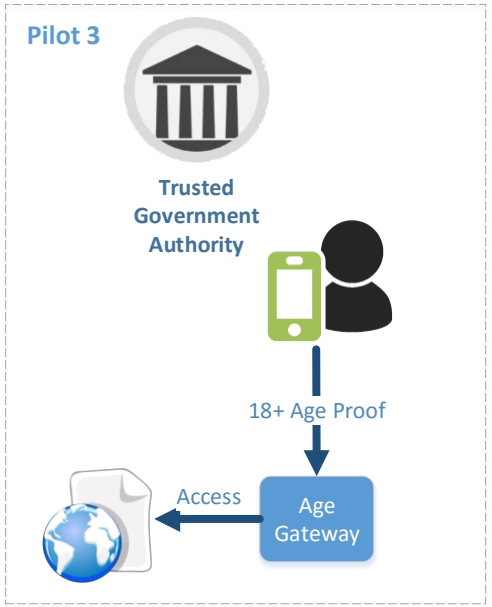
Pilot 1: Device-centric campus WiFi and web services access control



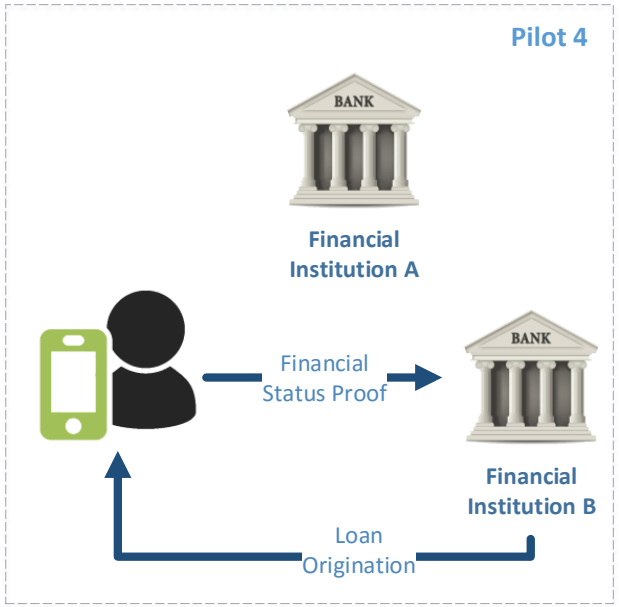
Pilot 2: Student authentication and offers



Pilot 3: Attribute-based age verification online gateway

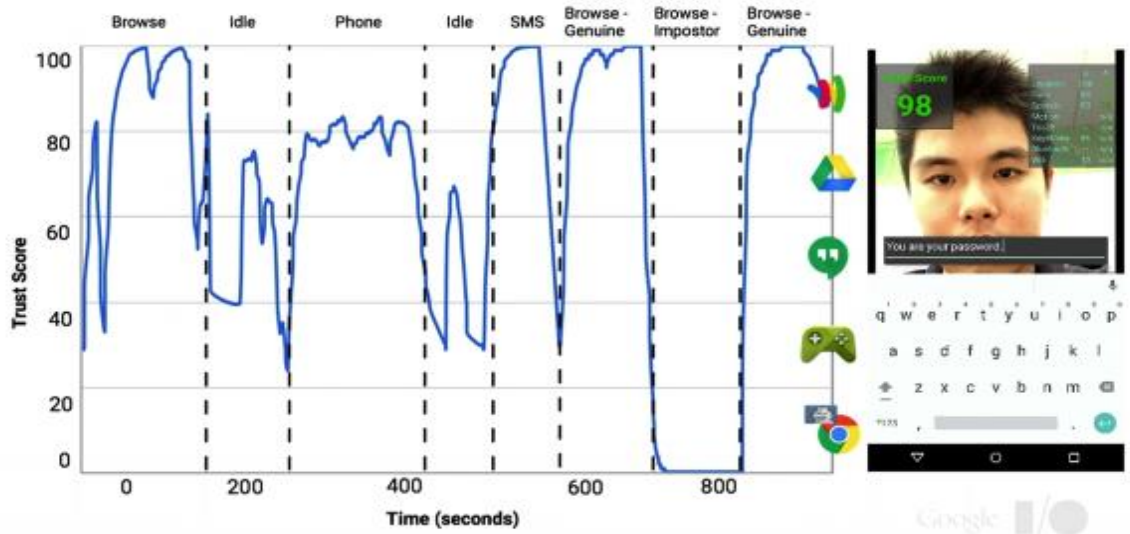


Pilot 4: Financial services – microloan origination



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 Abacus

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

Paypal's FIDO + OpenID integration

- User authenticates with FIDO UAF
- Extended OpenID Connect in order to
  - Maintain an authentication token for persistent sign-in
  - The user doesn't need to re-authenticate

- Purchases from multiple apps with one authentication

- Still a prototype, no source code released, just a 4-page documentation

ReCRED project

is partially an outcome of

Research & Development

in the Field of Security and Privacy

Before R&D !


LEADERSHIP
EDUCATION
SUCCESS
SOCIAL
DREAMS
FREEDOM
INTELLIGENCE
SKILLS
LEARN
tuition
FOCUS
EMPLOYMENT
RESEARCH
COMPETITION
GOALS
FUTURE
INDEPENDENCE
hardwork
OPPORTUNITIES
relationship
SPORTS
GRADUATION
CREDIBILITY
LOANS
AWARDS
commitment
dedication
scholarship
Job
FUN
Hope
STUDY
ASSIGNMENT
test
holidays
technology
IDENTITY
dorm
HOBBY
challenge
pressure
YOUNG
EXPERIENCE
GUIDANCE
SCHOOL
LECTURER
COLLEGE
FRIENDSHIP
achievement
occupation
YOUTH
UNIVERSITY
WORK
class
extracurricular
Laboratory
INNOCENCE
smart
Ambition
hardWORK
books
mentor
WORK
Students
teacher

A few words about us …

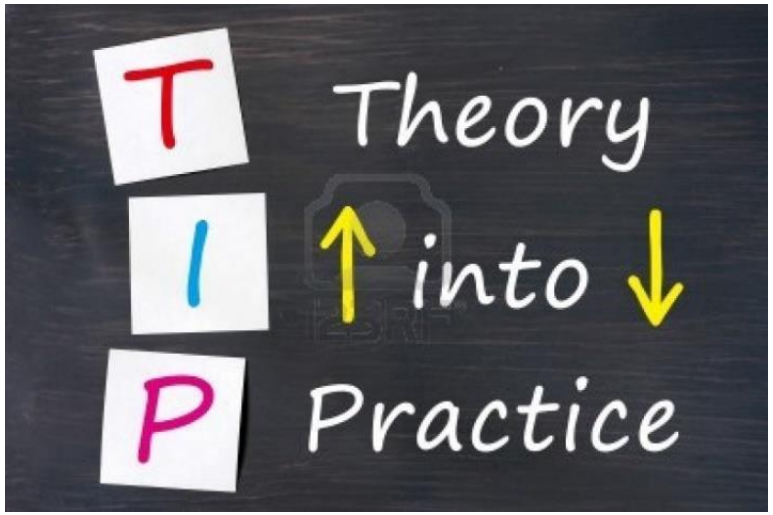
- University of Piraeus, Greece
- School of Information and Communication Technologies
- Department of Digital Systems
- System Security Laboratory founded in 2008
- Research, Development & Education
  - systems security, network security
  - computer security, forensics
  - risk analysis & management
- MSc course on "Digital Systems Security" since 2009

What we do for education

- Undergraduate studies ….
  - Security Policies and Security Management
  - Information Systems Security
  - Network Security
  - Cryptography
  - Mobile, wireless network security
  - Privacy enhancing technologies
  - Bachelor Thesis

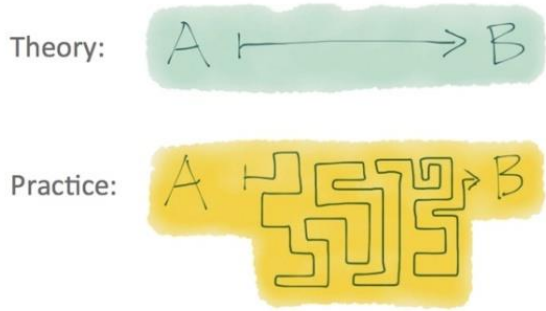
What we do for education

- Postgraduate studies in Digital Systems Security
- 1st semester
  - Security Management
  - Applied Cryptography
  - Information Systems Security
  - Network Security
  - Security Assessment and Vulnerability Exploitation



What we do for education

- Postgraduate studies in Digital Systems Security
- 2nd semester
  - Privacy Enhancing Technologies
  - Mobile Internet Security
  - Digital Forensics and Web Security
  - Advanced Security Technologies
  - Legal Aspects of Security



What we do for education

- Postgraduate studies in Digital Systems Security
- 3rd semester
  - Master Thesis

  - ISO 27001
  - Certified Information Security Manager (CISM)
  - .....

Thank you

Christos Xenakis

Systems Security Laboratory
Department of Digital Systems

http://ssl.ds.unipi.gr/
http://cgi.di.uoa.gr/~xenakis/
email: xenakis@unipi.gr

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS