Device Centric and Attribute Based Access Control in the ReCRED project

Claudio Pisa

<claudio.pisa@uniroma2.it>

consorzio nazionale
interuniversitario
per le telecomunicazioni

ReCRED

cnit consorzio nazionale interuniversitario per le telecomunicazioni

- CNIT (National Inter-University Consortium for Telecommunications)
  - non-profit
  - 37 Italian Universities
    - University of Rome Tor Vergata (uniroma2) among these
  - mission:
    - coordinate and foster basic and applied **research** activities (in cooperation with national and international bodies and industries) and
    - provide advanced **education** and training in the area of **telecommunications**
- Involved in the ReCRED project mostly in:
  - Technical design and implementation
    - Especially Attribute-Based Access Control
  - User Experience assessment

Today

- Password-based access control
  - Security vs. usability
  - Password overload: different passwords for different services
    - In practice: same (weak) password for multiple accounts
  - Google statistics:
    - **70%** of users forget their password once a month
    - **2.4** passwords before the right login
  - Microsoft Security Intelligence Report 17:
    - **98.8%** of users chose a password that is one of the **most common 10,000** passwords
  - Lack of support for attribute-based access control
    - vs. identity or role based
  - Identity fragmentation and lack of real world binding
- Centralized approach
  - vs. decentralized or federated

ReCRED

- H2020 3 years Innovation project
- Aim: supplement basic device-centric authentication with:
  - Multi-Factor Authentication
    - Secure biometrics, i.e. templates:
      - Irreversible
      - Revocable
      - Unlinkable
    - Behavioural authentication
  - Attribute-based access control
  - Privacy-preserving ID consolidation
    - Real to online identity mapping
    - Link different accounts

Participants

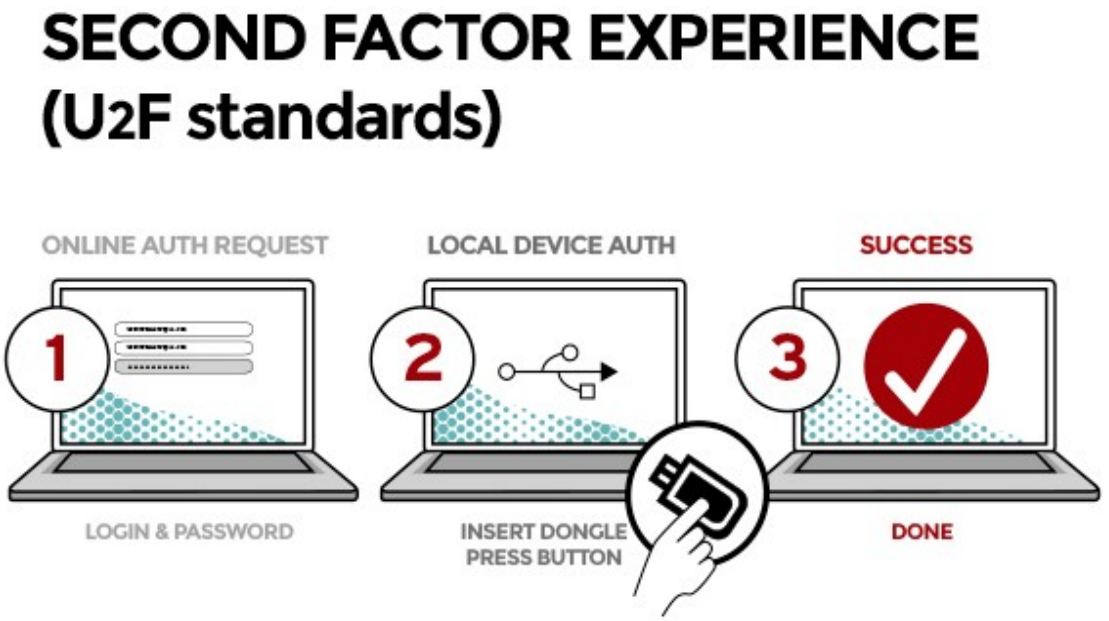
Integration

- ReCRED will integrate existing technologies into a single system. Some of them:
  - FIDO
  - Idemix
  - U-prove
  - Attribute Based Encryption (ABE)

FIDO

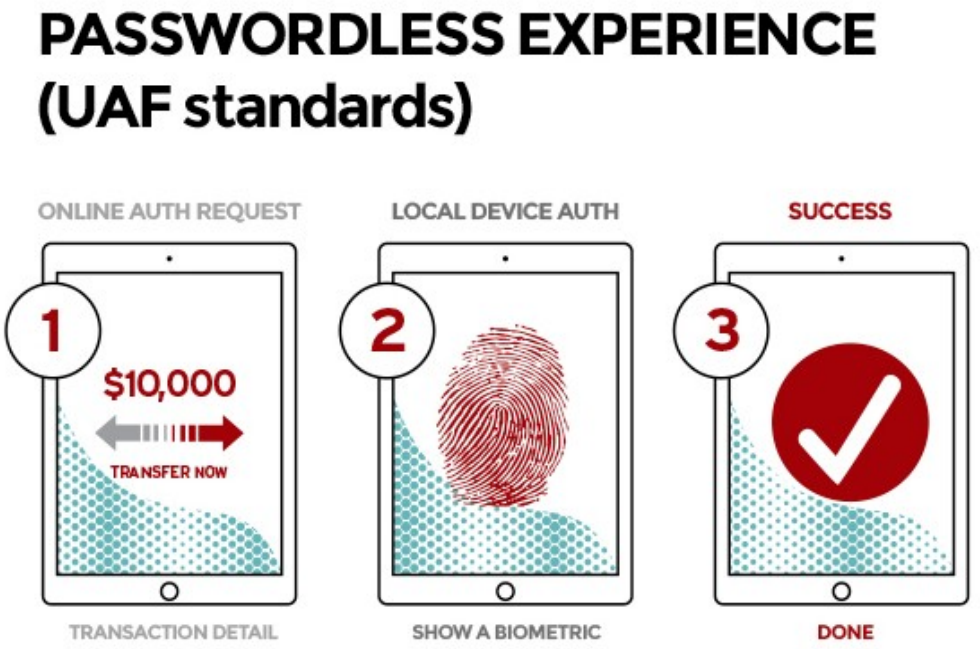
- FIDO alliance
  - More than 200 members
- Standard definition with two protocols:
  - U2F – use device as second factor authentication
  - **UAF** – passwordless (biometric) authentication

FIDO



- User can either:
  - Press a button on a dongle
  - Tap on NFC

FIDO



- User can avoid passwords by using on-device biometric authentication, e.g. fingerprint, looking at the camera, speaking into the microphone, swiping ...

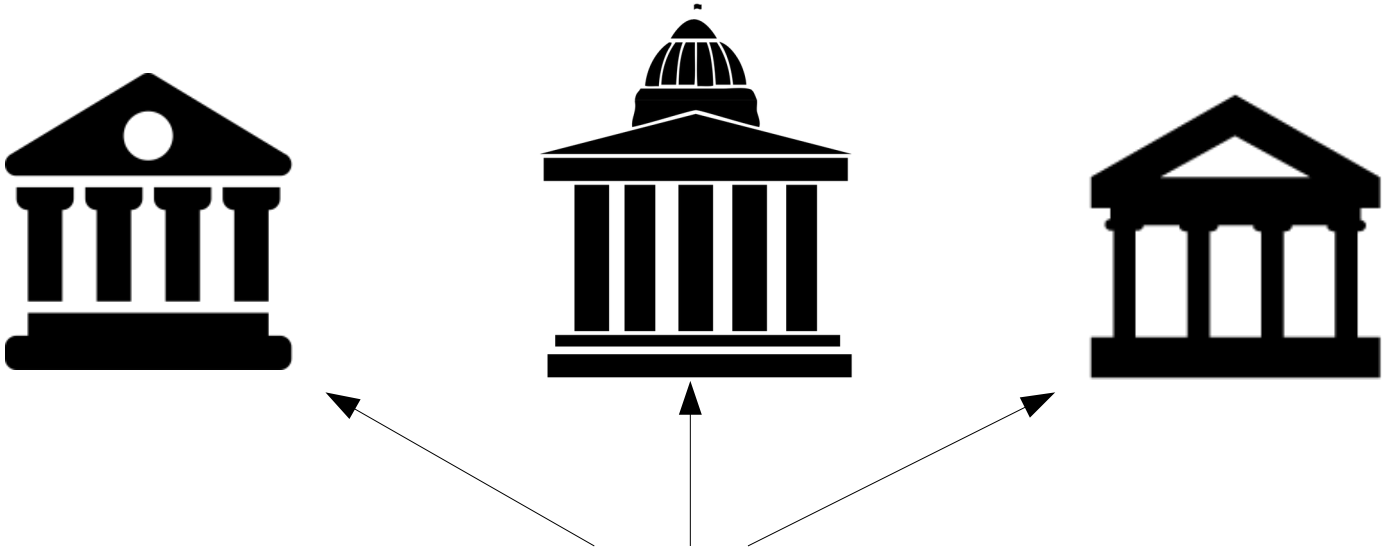
FIDO

- Going beyond FIDO in ReCRED:
  - Behavioral authentication modalities as a second factor authentication
  - Decentralized authentication process

Idemix – identity mixer

- Anonymous Credential System
  - by IBM Zürich Research Labs
- Attribute based access control
- CNIT is working on the integration of idemix in ReCRED

Idemix

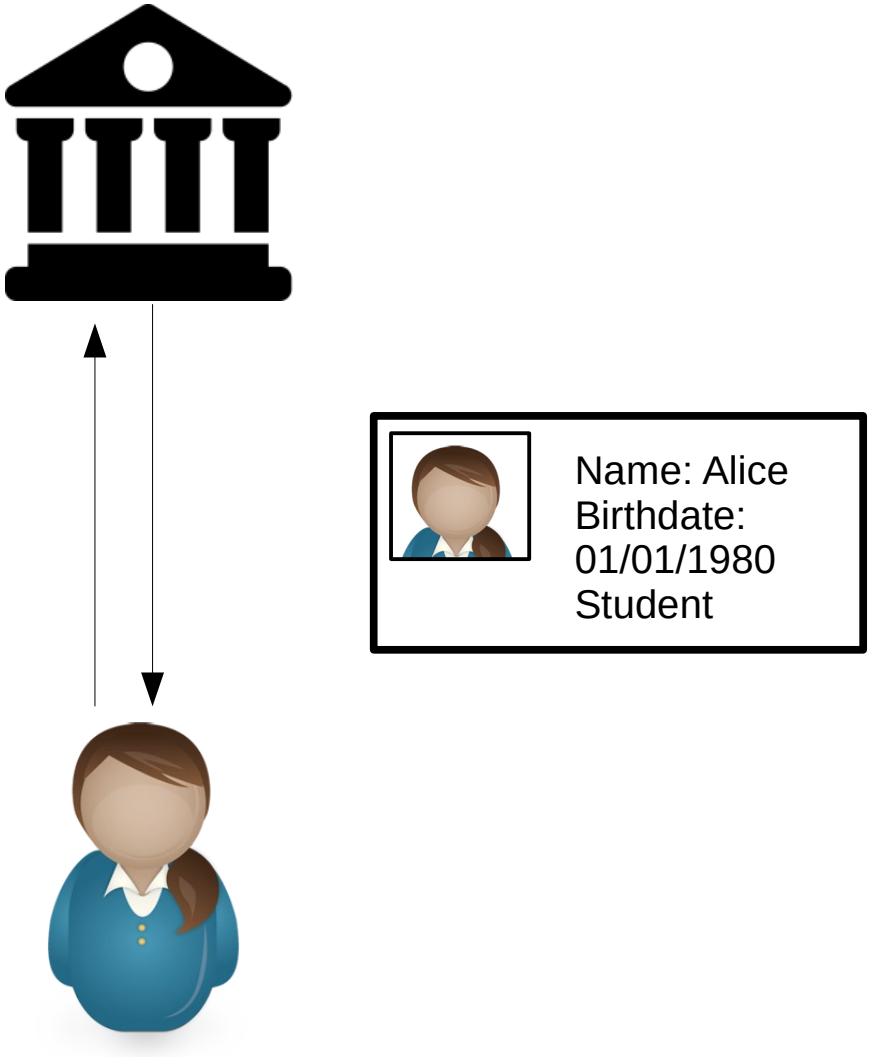


CREDENTIAL ISSUERS

Idemix

Idemix

Idemix



Idemix

SWITCHtube

Idemix

SWITCHtube

Hello. I would like to watch this video

Idemix

SWITCHtube

Hello. To watch this video you must be a student and at least 12 years old

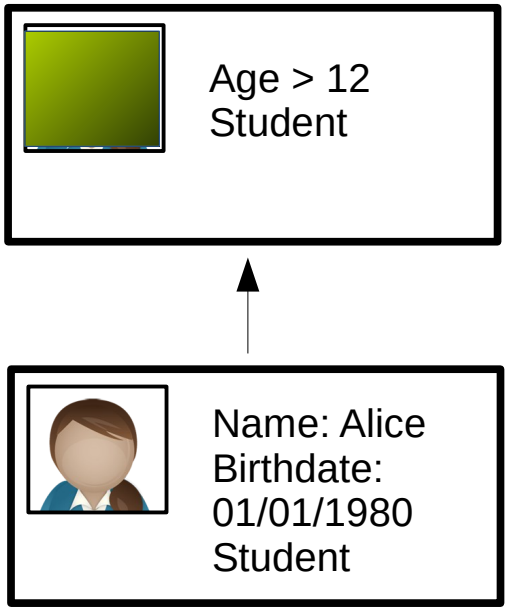
Idemix

SWITCHtube

Name: Alice
Birthdate:
01/01/1980
Student

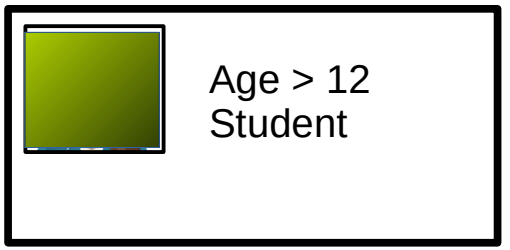
Idemix

SWITCHtube



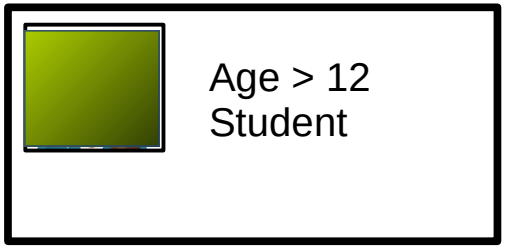
Idemix

SWITCHtube

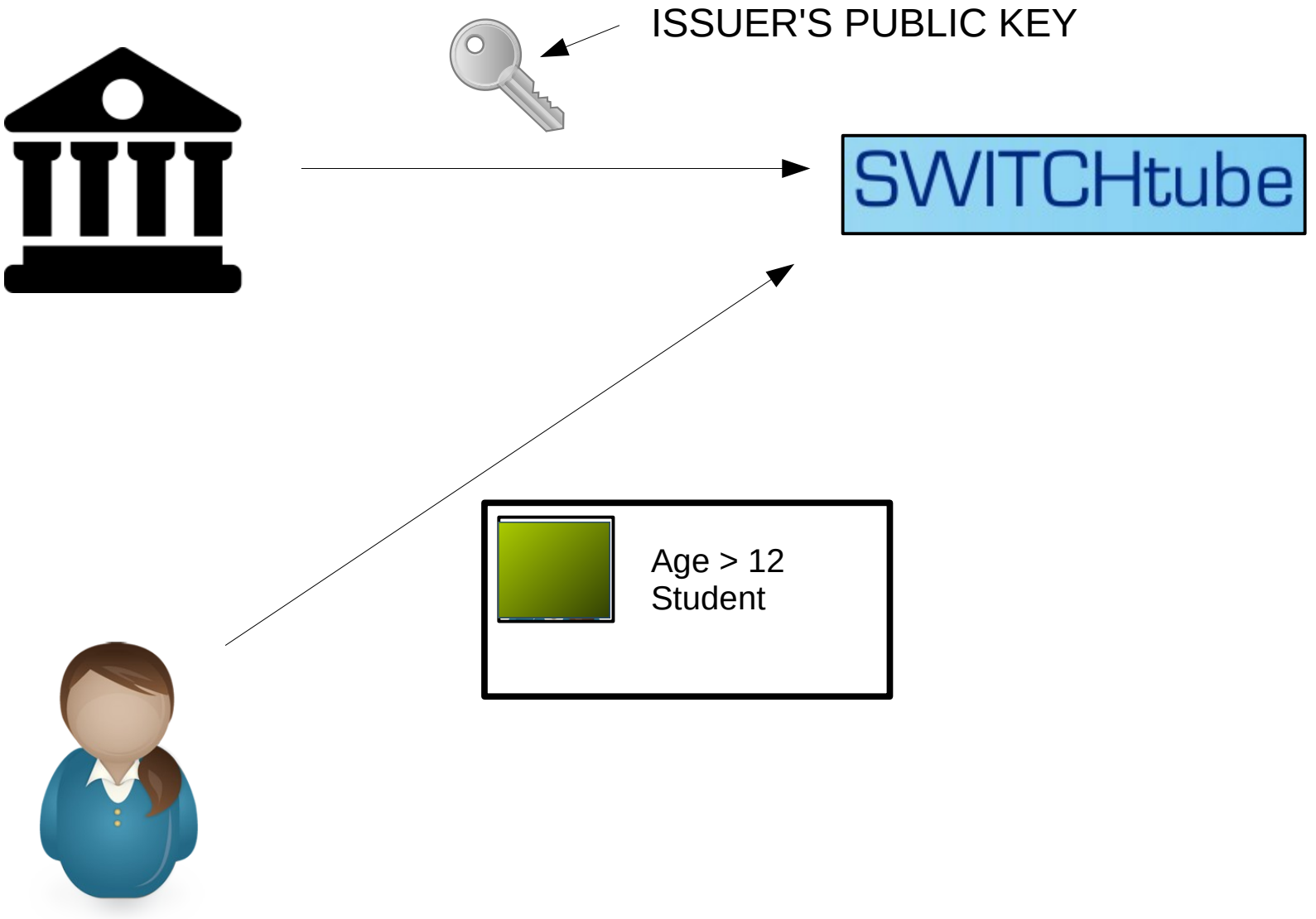


Idemix

SWITCHtube



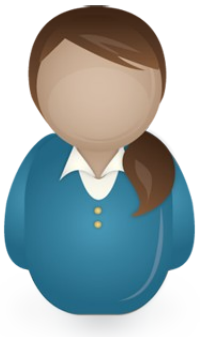
Idemix



Idemix

SWITCHtube

OK! Here is the video you requested



Idemix

- Decentralized system
- Only minimal attribute disclosure
- Properties
  - Zero-knowledge proofs
    - Partial attribute information disclosure (e.g. age > 18)
  - Anonimity
    - Through pseudonyms
  - Untraceability
    - A credential show cannot be linked to the user's identity
  - Unlinkability
    - Two shows of the same credential cannot be linked

U-Prove

- by Microsoft Research (acquired in 2008)
- Similar to idemix, except:
  - Better performance
  - No unlinkability
    - Two credential shows can link to the same user

Attribute Based Encryption (ABE)

- Cyphertext Policy ABE
  - Attribute-based policy embedded in the encrypted data
- Key Policy ABE
  - Attributes embedded in the secret key
- Collusion resistant
- Main drawbacks:
  - Computationally intensive
  - Credential revocation can be non-trivial

Conclusions

- ReCRED advantages (some of them):
  - Integration of different access control technologies into a single system
    - Aiming at going beyond their disadvantages
  - Attribute-based access control
  - Decentralized/Federated credential issuing
  - Device centric access control
    - Beyond passwords
  - Identity defragmentation

Thank you

References

- ReCRED website: http://www.recred.eu
- Pros and cons of u-prove (and Idemix): https://pomcor.com/2011/10/04/pros-and-cons-of-u-prove-for-nstic/
- Idemix: http://www.zurich.ibm.com/idemix/
- Google Project ABACUS: https://www.youtube.com/watch?v=lGrRYnqHegc