THE CENTER FOR CYBERSECURITY OF FONDAZIONE BRUNO KESSLER IN THE LAND OF DIGITAL IDENTITY INFRASTRUCTURES

Silvio Ranise

Director of the FBK Center for Cybersecurity &

Full Professor of Computer Science, University of Trento

Digital identity

What?

Why?

How?

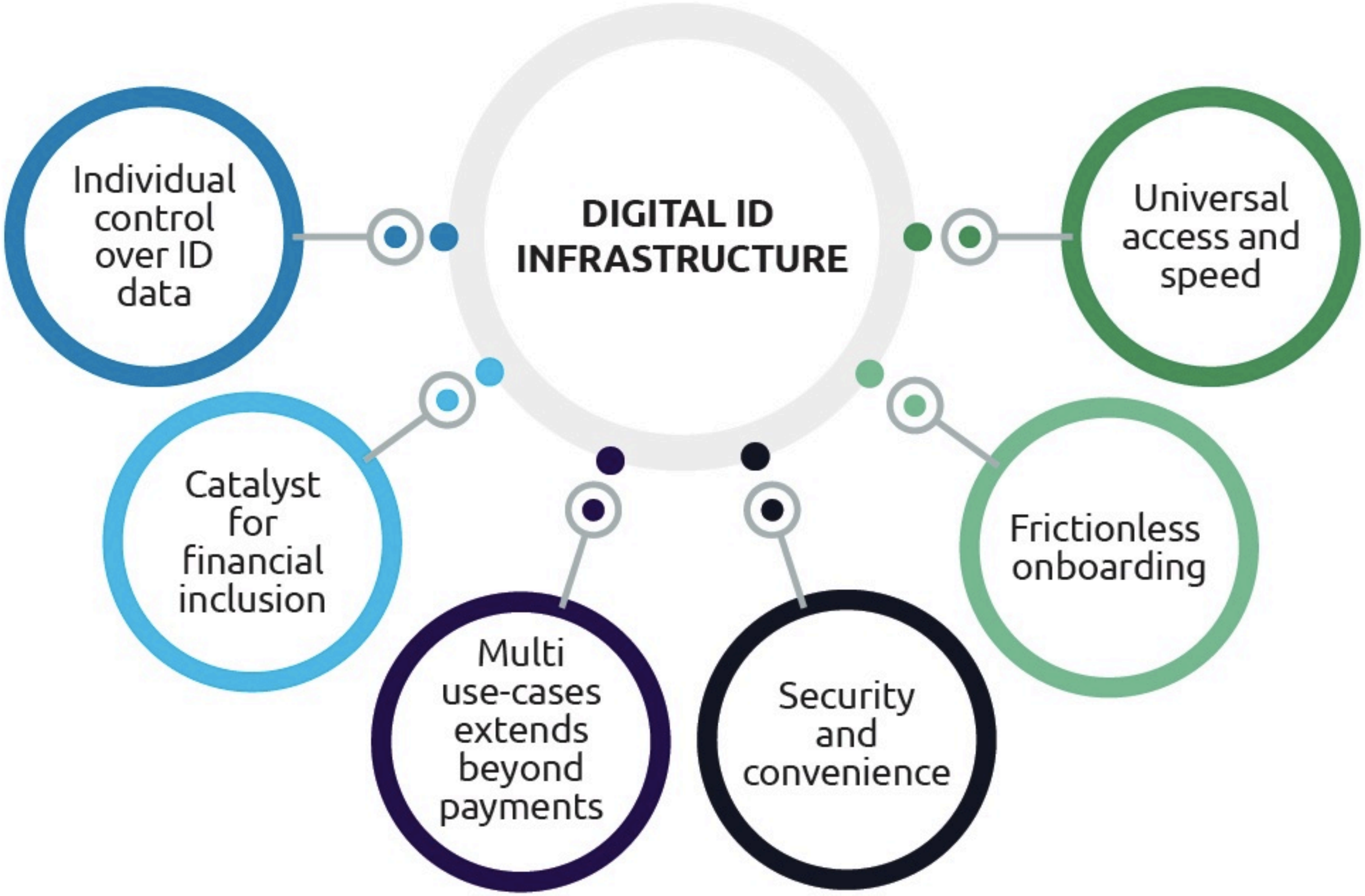
What is digital identity?

- Identity = collection of **attributes** related to an entity
- Attribute = feature or property of an entity allowing for describing its appearance, status or other characteristics

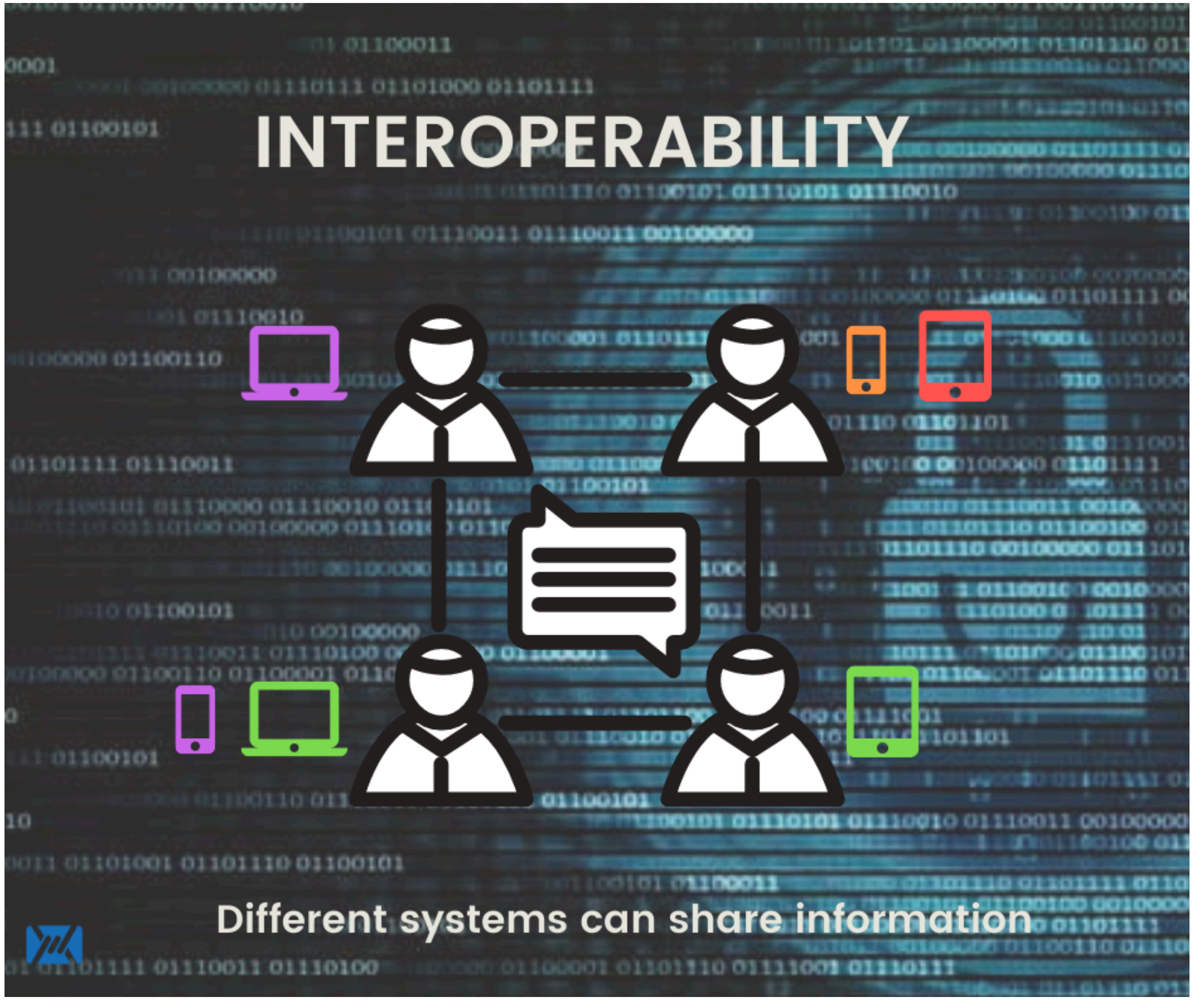
- Digital identity = identity whose attributes are stored, transmitted, and processed in digital format

Why is digital identity important?

Why is there a need for shared and integrated digital ID


DIGITAL ID INFRASTRUCTURE
Individual control over ID data
Universal access and speed
Catalyst for financial inclusion
Frictionless onboarding
Multi use-cases extends beyond payments
Security and convenience

1st Key requirement



SAML v2.0
Security Assertion Markup Language

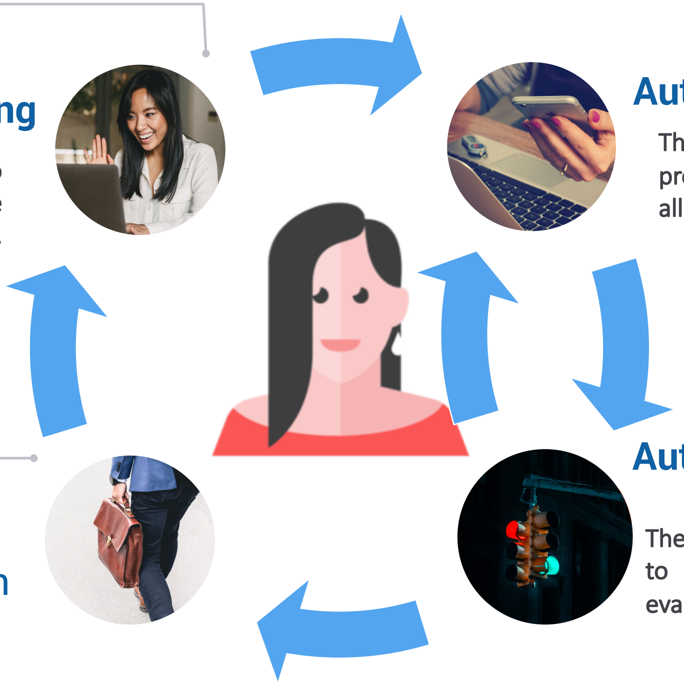
OpenID

Entra con SPID

Cie ID Entra con CIE

eIDAS

The digital identity lifecycle…



Relationship starts

The user receives a credential or authenticator from a *Credential Service Provider* (CSP).

Enrollment/on-boarding

The process through which an applicant applies to become a subscriber of an identity system and the identity system validates the applicant's identity.

Authentication

The process of verifying the identity of a user, process, or device, often as a prerequisite to allowing access to a system's resources.

Authorization/Access control

The process of checking user's permissions to access data, typically automated by evaluating a subject's attributes.

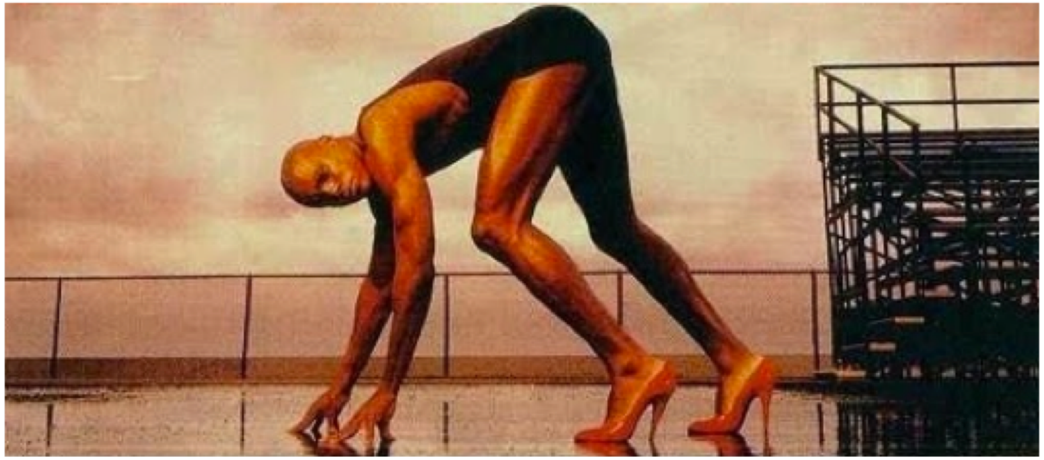
Relationship ends

Deregistration

https://pages.nist.gov/800-63-3/

2nd key requirement

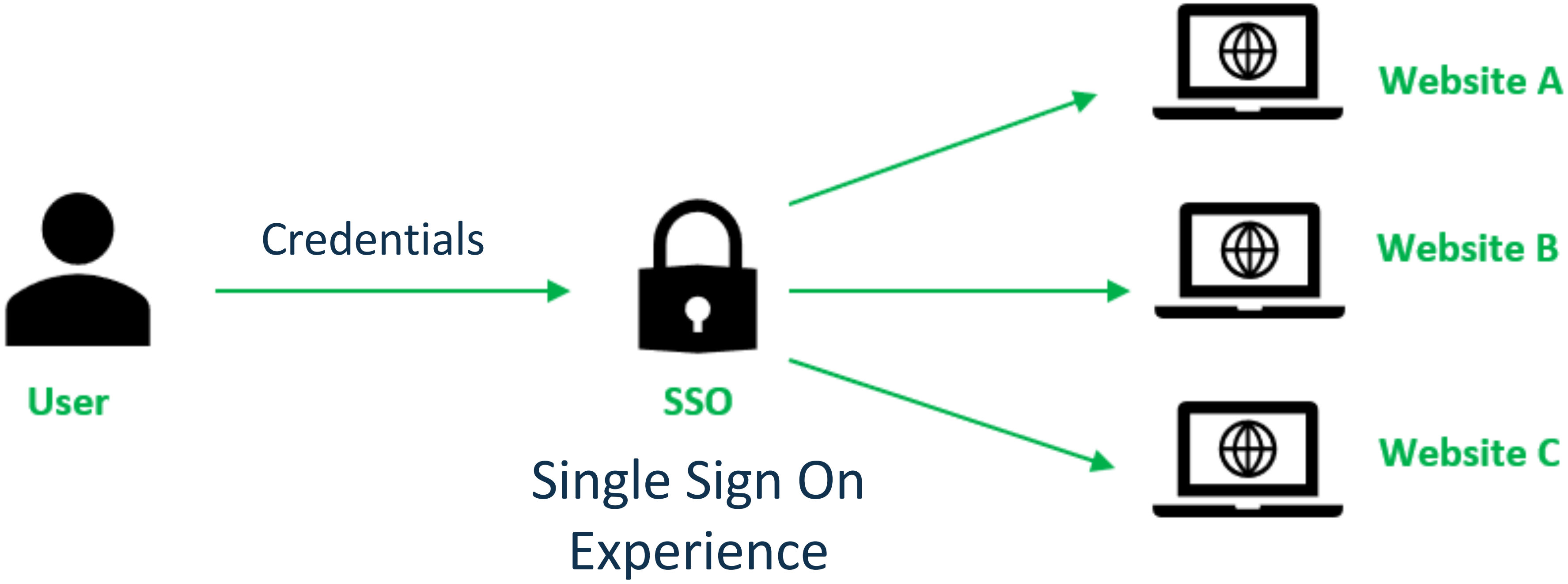
CONTROL IS NOTHING WITHOUT TRUST



Selective disclosure

Trust management

Digital identity infrastructure: main idea



Single Sign On Experience

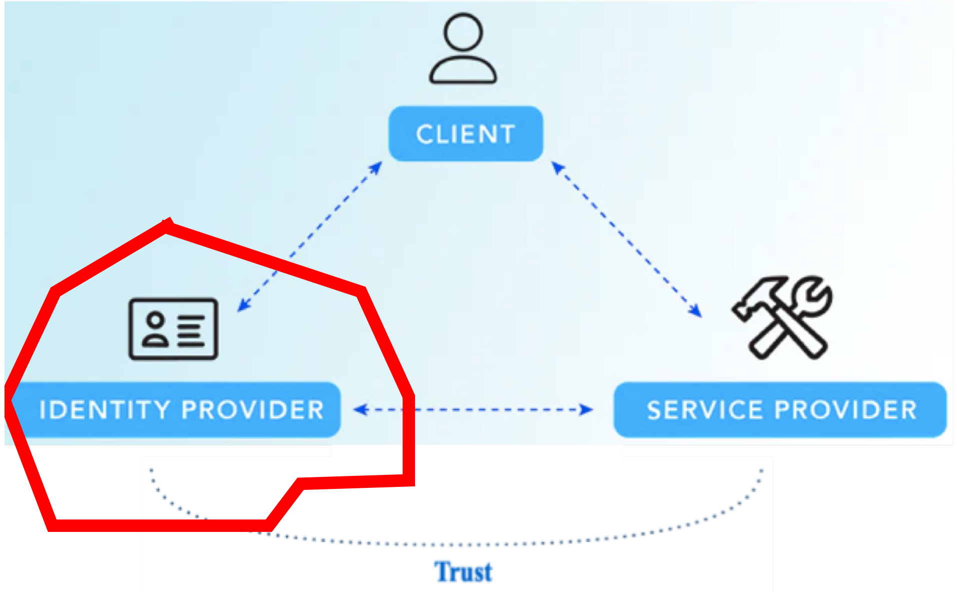
Digital identity

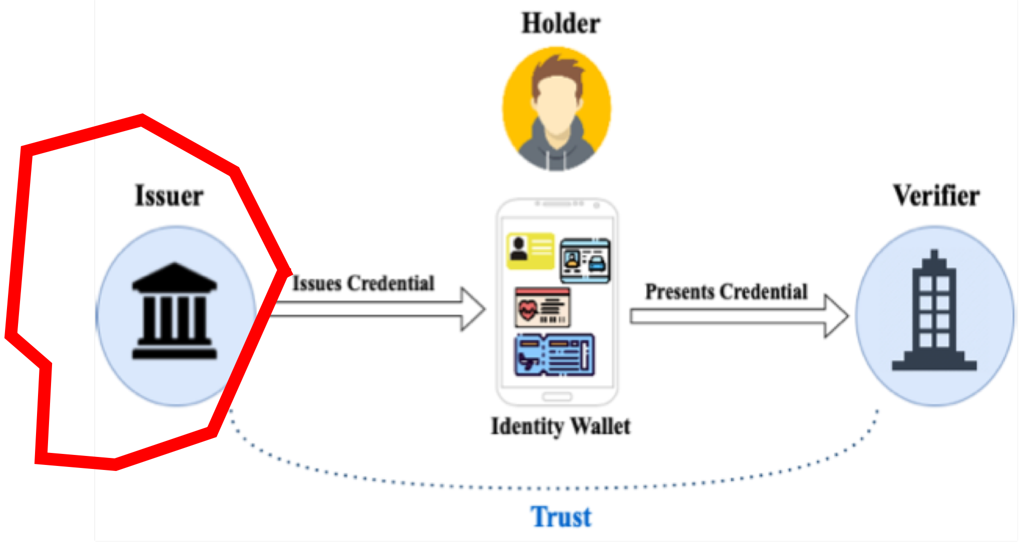
Present and future or reacting to eIDAS revisions

eIDAS (electronic IDentification, Authentication and trust Services) is an EU regulation on electronic identification and trust services for electronic transactions in the European Single Market.

Digital identity infrastructure: architectures

Outsourcing digital identity management to 3rd parties





Centralized

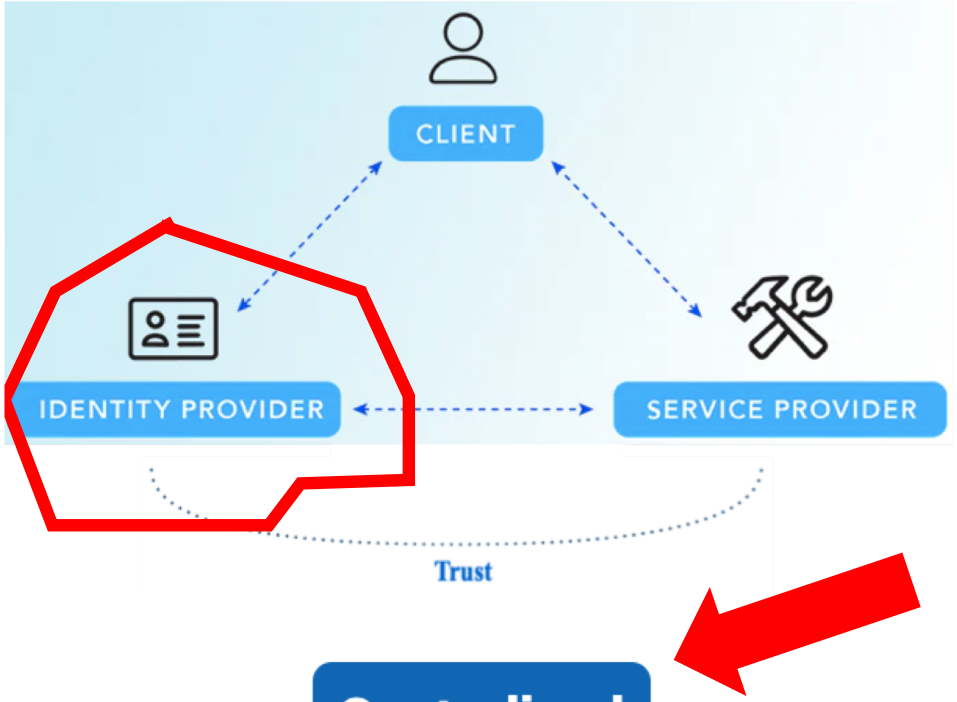
- Single Point of Failure
- Uniform user experience
- User has little control on credentials
- Always online

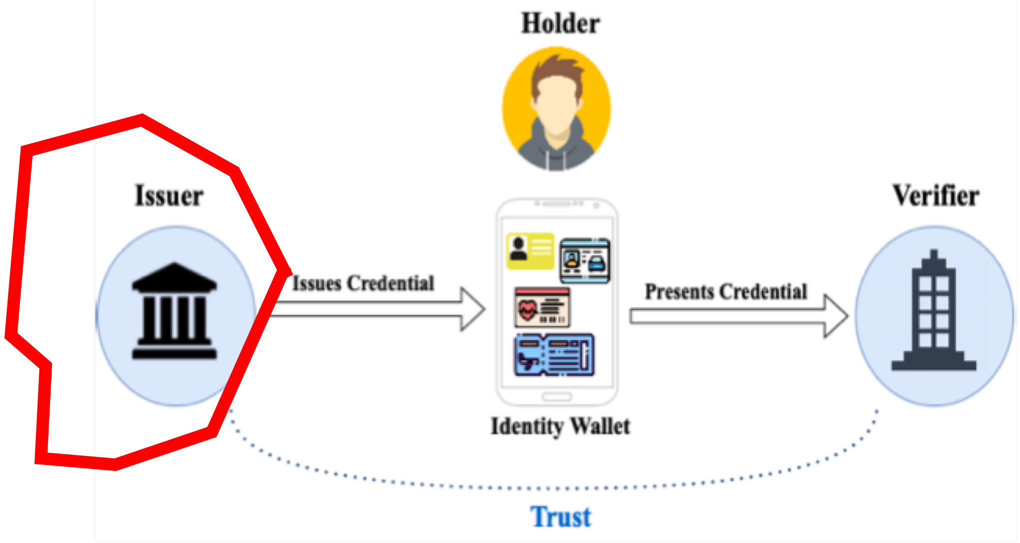
Decentralized

- ~~Single Point of Failure~~
- Uniform user experience
- ~~User has little control on credentials~~
- ~~Always online~~

Digital identity infrastructure: architectures

Outsourcing digital identity management to 3rd parties





Centralized

- Single Point of Failure
- Uniform user experience
- User has little control on credentials
- Always online

Decentralized

- ~~Single Point of Failure~~
- Uniform user experience
- ~~User has little control on credentials~~
- ~~Always online~~

Problems and solutions (by FBK—CS) for the centralized architecture

- Security analysis and risk evaluation in all phases of the development lifecycle
  - Automation, automation, automation, and… yet again automation*!*
- **MuFASA [design]**
  - A Tool for High-level Specification and Analysis of Multi-factor Authentication Protocols
  - https://st.fbk.eu/tools/MuFASA.html
- **Micro-Id-Gym [deployment]**
  - Identity Management Workouts with Container-Based Microservices
  - https://st.fbk.eu/tools/Micro-Id-Gym.html

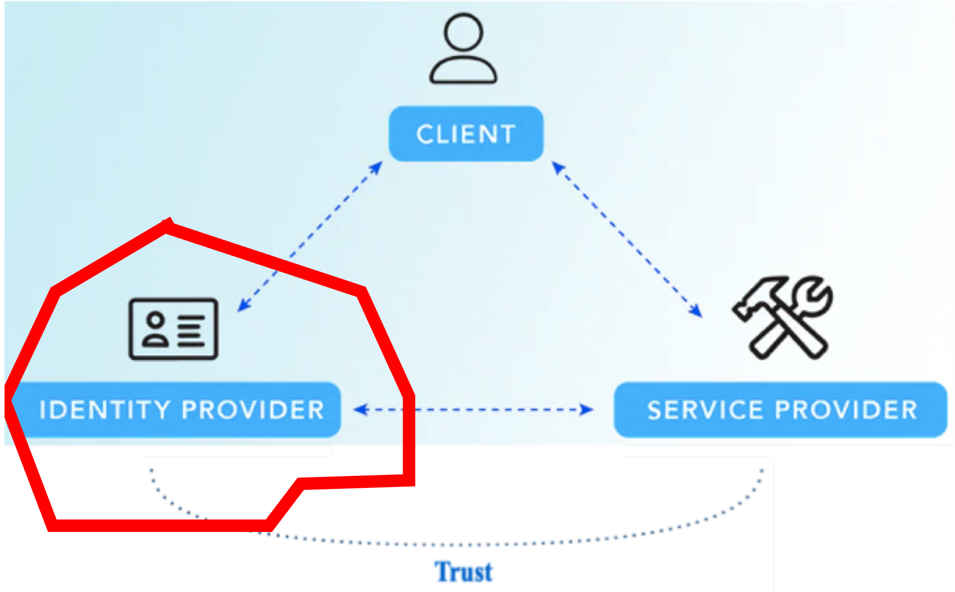
Problems and solutions (by FBK—CS) for the centralized architecture (cont’d)

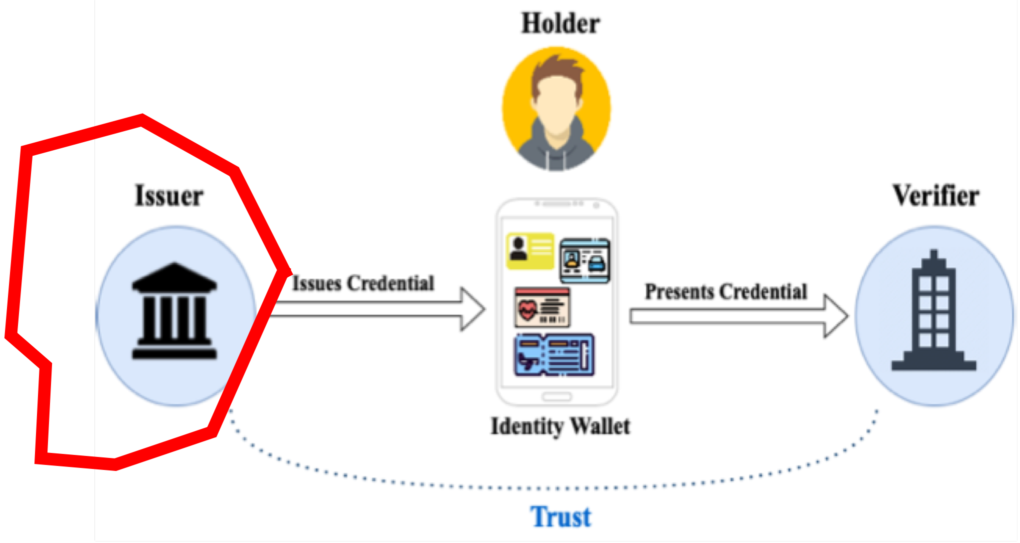
- Difficulty in keeping track of satisfaction of design requirements and compliance constraints when deploying the infrastructure
  - Traceability of requirements across the various phases of the development lifecycle

- **TLSAssistant [deployment]**
  - https://st.fbk.eu/tools/TLSAssistant/

Digital identity infrastructure: architectures

Outsourcing digital identity management to 3rd parties





Centralized

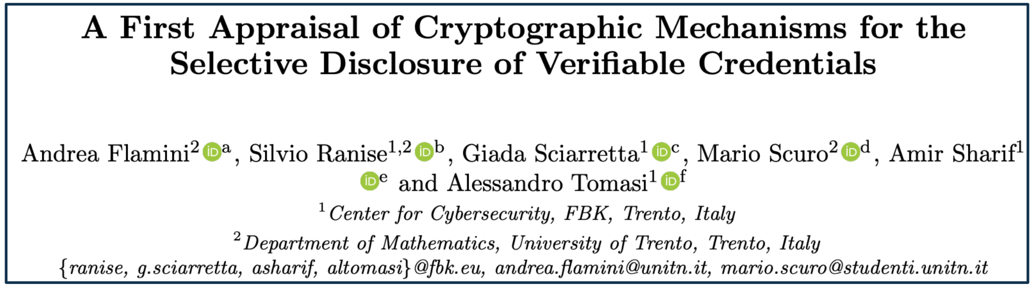
- Single Point of Failure
- Uniform user experience
- User has little control on credentials
- Always online

Decentralized

- ~~Single Point of Failure~~
- Uniform user experience
- ~~User has little control on credentials~~
- ~~Always online~~

Challenge 1
Selective disclosure

- How to share credentials selectively?
- Several possible meanings including
  - A subset of the credentials for data minimization
  - Showing a proof that credentials satisfy a certain condition (e.g., being adult and not exact age) for avoiding to reveal exact data
- Use suitable cryptographic techniques such as
  - hash and signatures
  - Zero Knowledge proofs



A First Appraisal of Cryptographic Mechanisms for the Selective Disclosure of Verifiable Credentials

Andrea Flamini[2][a], Silvio Ranise[1,2][b], Giada Sciarretta[1][c], Mario Scuro[2][d], Amir Sharif[1][e] and Alessandro Tomasi[1][f]

[1] *Center for Cybersecurity, FBK, Trento, Italy*

[2] *Department of Mathematics, University of Trento, Trento, Italy*

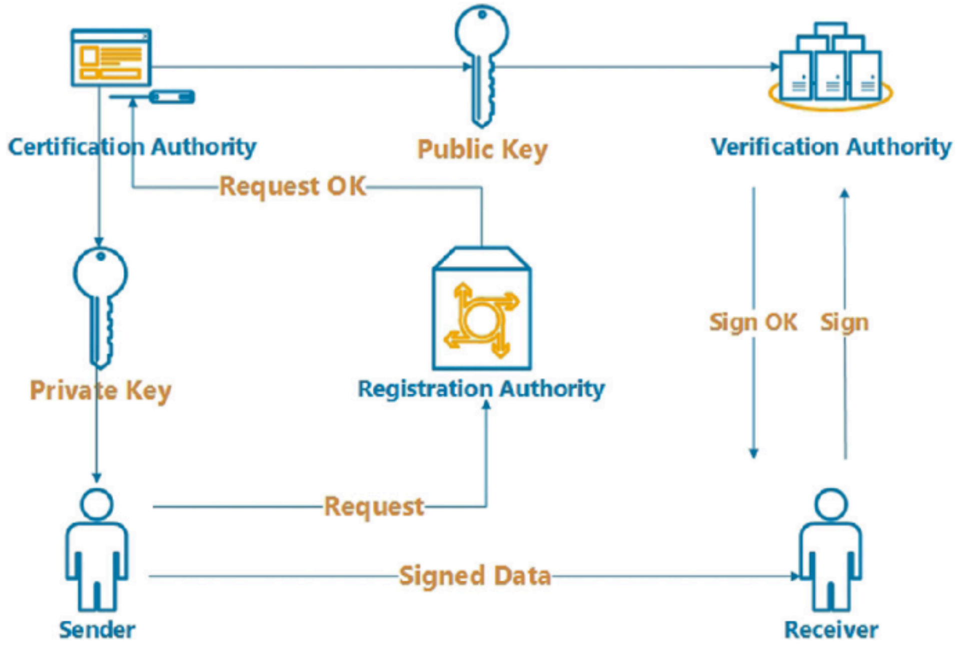
{ranise, g.sciarretta, asharif, altomasi}@fbk.eu, andrea.flamini@unitn.it, mario.scuro@studenti.unitn.it

Challenge 2
Trust management

- How to establish trust in a decentralized architecture?
- Use a Public Key Infrastructure (PKI)
    - Centralized?
    - Decentralized?

OIDC Federation

Blockchain based



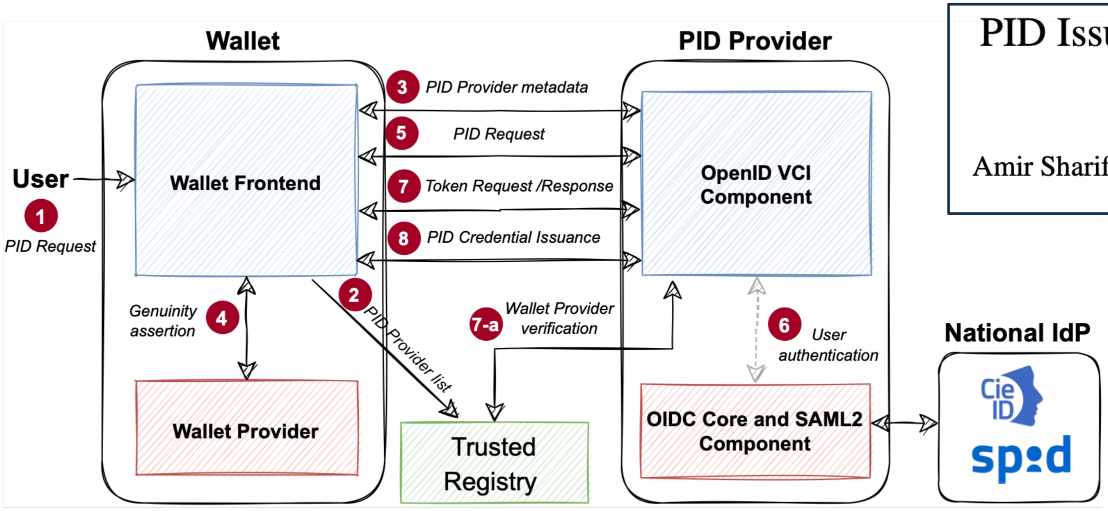
A. Sharif, F. A. Marino, G. Sciarretta, G. de Marco, R. Carbone and S. Ranise. *Cross-Domain Sharing of User Claims: A Design Proposal for OpenID Connect Attribute Authorities.*

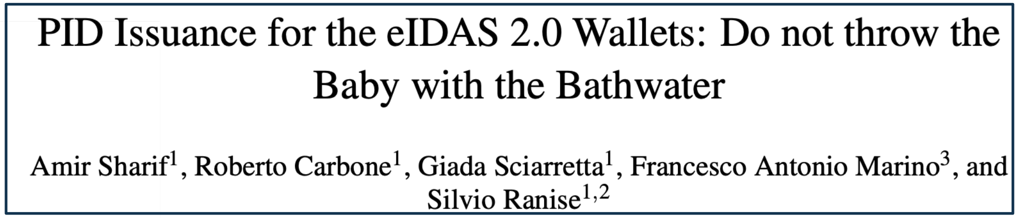
ARES conference
Availability • Reliability • Security

August 29 - September 01, 2023
Benevento, Italy

Challenge 3
Evolving requirements and threats

- What are the threats to wallets?
- Old and new security issues…
- Let us start from the beginning…
  - Wallet activation with Personal Identifiable Information (PID)




PID Issuance for the eIDAS 2.0 Wallets: Do not throw the Baby with the Bathwater

Amir Sharif[1], Roberto Carbone[1], Giada Sciarretta[1], Francesco Antonio Marino[3], and Silvio Ranise[1,2]

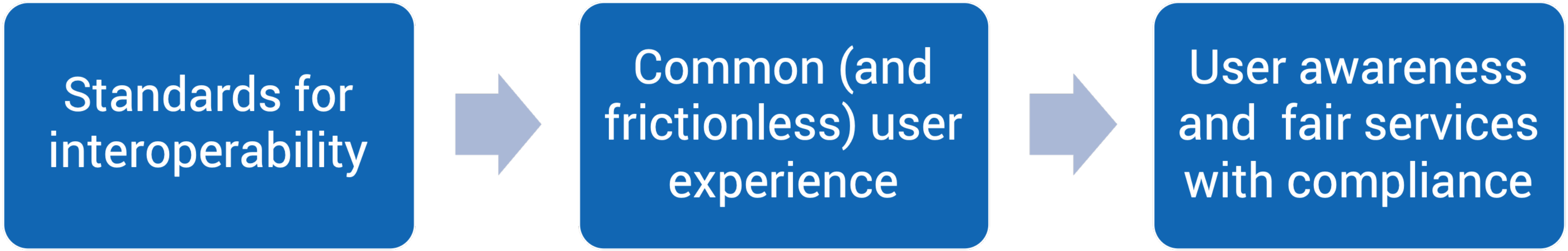
Digital identity

How

ConfGARR23

SAPERI INTERCONNESSI

FBK—CS in the land of digital identity infrastructures



Standards for interoperability

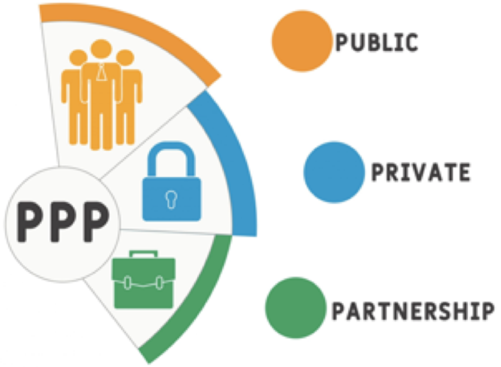
Common (and frictionless) user experience

User awareness and fair services with compliance

- Applied cryptography
- Trust model and establishment
- Evolving requirements and threats

FBK—CS in the land of digital identity infrastructures

What about the business model?



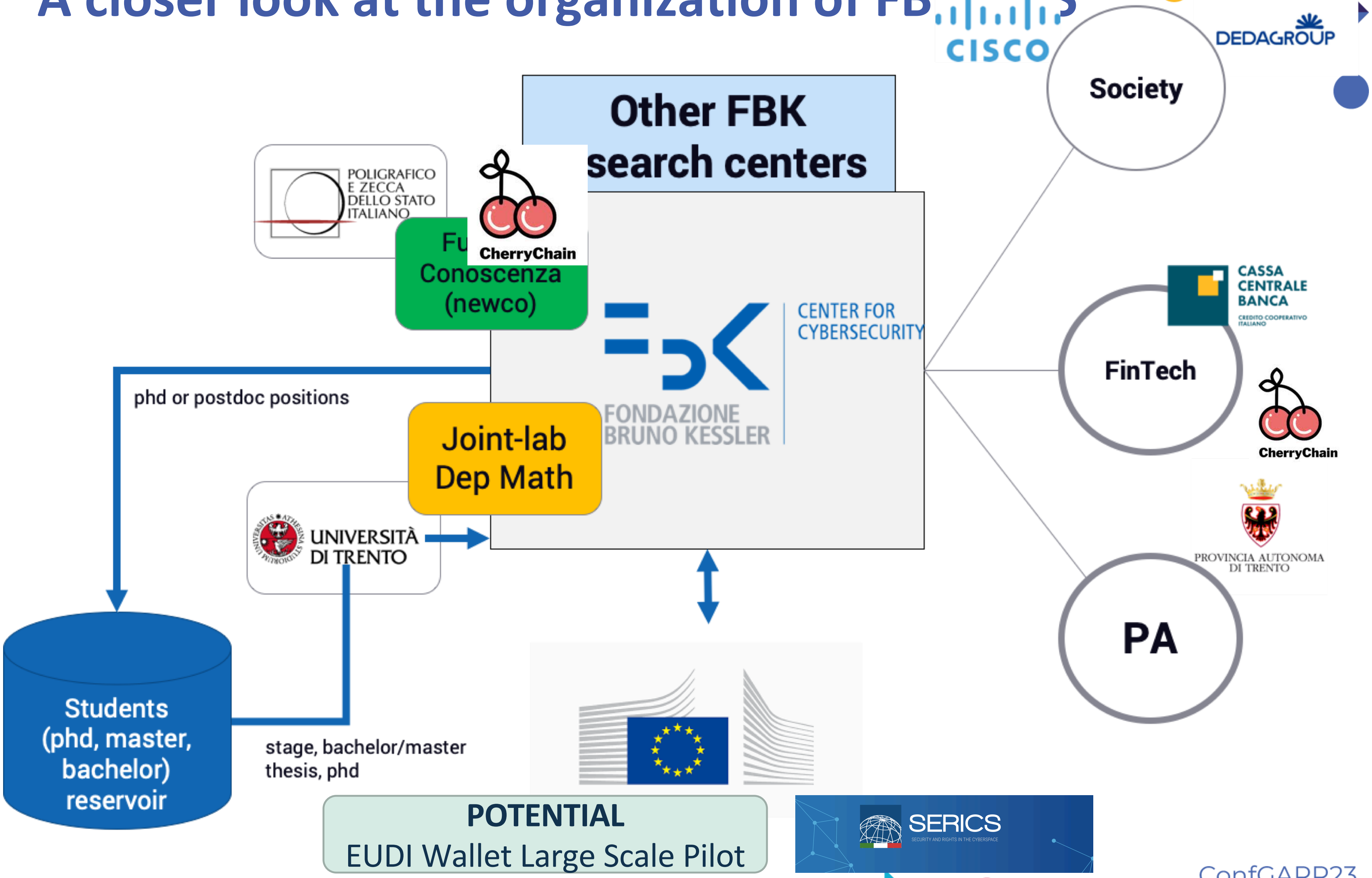
Standards for interoperability

Common (and frictionless) user experience

User awareness and fair services with compliance

- Applied cryptography
- Trust model and establishment
- Evolving requirements and threats

A closer look at the organization of FBK—CS



CISCO

DEDAGROUP

Other FBK research centers

POLIGRAFICO E ZECCA DELLO STATO ITALIANO

Fu Conoscenza (newco)

CherryChain

CENTER FOR CYBERSECURITY

FONDAZIONE BRUNO KESSLER

phd or postdoc positions

Joint-lab Dep Math

UNIVERSITÀ DI TRENTO

Students (phd, master, bachelor) reservoir

stage, bachelor/master thesis, phd

Society

FinTech

CASSA CENTRALE BANCA

CREDITO COOPERATIVO ITALIANO

CherryChain

PROVINCIA AUTONOMA DI TRENTO

PA

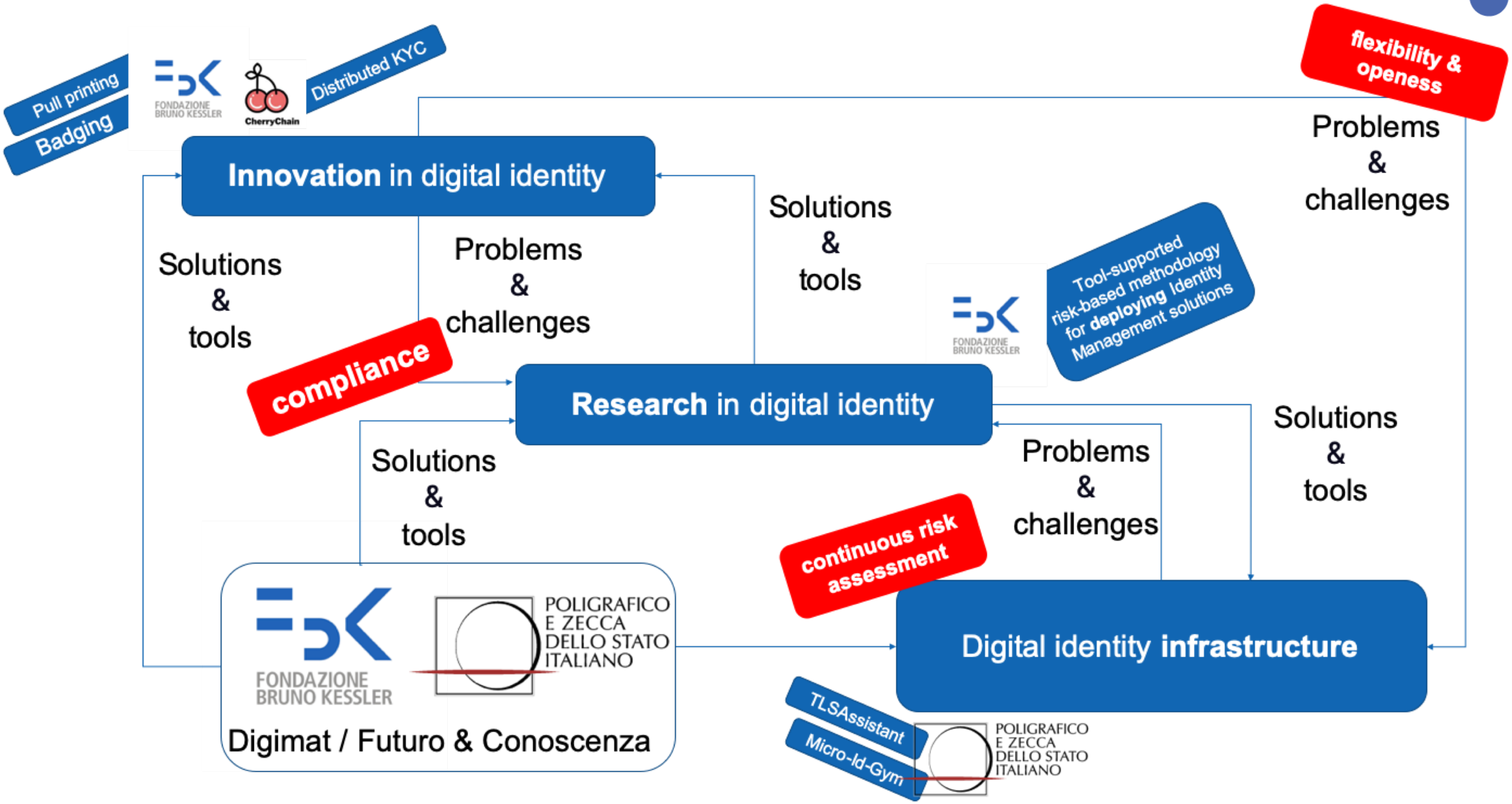
POTENTIAL

EUDI Wallet Large Scale Pilot

SERICS

SECURITY AND RIGHTS IN THE CYBERSPACE

Focus on the collaboration with IPZS


Pull printing
Badging
FONDAZIONE BRUNO KESSLER
CherryChain
Distributed KYC
flexibility & openess
Innovation in digital identity
Solutions & tools
Problems & challenges
Solutions & tools
Problems & challenges
compliance
FONDAZIONE BRUNO KESSLER
Tool-supported risk-based methodology for deploying Identity Management solutions
Research in digital identity
Solutions & tools
Problems & challenges
Solutions & tools
continuous risk assessment
FONDAZIONE BRUNO KESSLER
POLIGRAFICO E ZECCA DELLO STATO ITALIANO
Digimat / Futuro & Conoscenza
Digital identity infrastructure
TLSAssistant
Micro-Id-Gym
POLIGRAFICO E ZECCA DELLO STATO ITALIANO

Remember…

From centralized to decentralized