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

- 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

INTEROPERABILITY

Different systems can share information

SAMLA

OpenID

Entra con SPID

Entra con CIE

eIDAS
The digital identity lifecycle...

Relationship starts

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.

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

Relationship ends

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

2nd key requirement

CONTROL IS NOTHING WITHOUT TRUST

Selective disclosure

Trust management
Digital identity infrastructure: main idea

User → Credentials → SSO

SSO → Single Sign On Experience → Website A
SSO → Single Sign On Experience → Website B
SSO → Single Sign On Experience → Website C
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

- 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/](https://st.fbk.eu/tools/TLSAssistant/)
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\(^2\), Silvio Ranise\(^1,2\), Giada Sciarretta\(^1\), Mario Scuro\(^2\), Amir Sharif\(^3\) and Alessandro Tomasi\(^1\)

\(^1\) Center for Cybersecurity, FBK, Trento, Italy
\(^2\) Department of Mathematics, University of Trento, Trento, Italy
\(^3\) Department of Computer Science, University of 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?

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.
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 Sharif¹, Roberto Carbone¹, Giada Sciarretta¹, Francesco Antonio Marino², and Silvio Ranise¹,²
Digital identity

How
FBK—CS in the land of digital identity infrastructures

- 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

Students (phd, master, bachelor) reservoir

Joint-lab Dep Math

% phd or postdoc positions

FinTech

PA

POTENTIAL EUDI Wallet Large Scale Pilot

Silvio Ranise – FBK & UniTN
Focus on the collaboration with IPZS

Innovation in digital identity

- Solutions & tools
- Problems & challenges

Research in digital identity

- Solutions & tools
- Problems & challenges

Digital identity infrastructure

- Digimat / Futuro & Conoscenza
- TLSAssistant
- Micro-id-Sym

Flexibility & openness

Problems & challenges

Tool-supported risk-based methodology for deploying Identity Management solutions

Pull printing

Badging

Distributed KYC

Compliance

Continuous risk assessment
Remember...

From centralized to decentralized