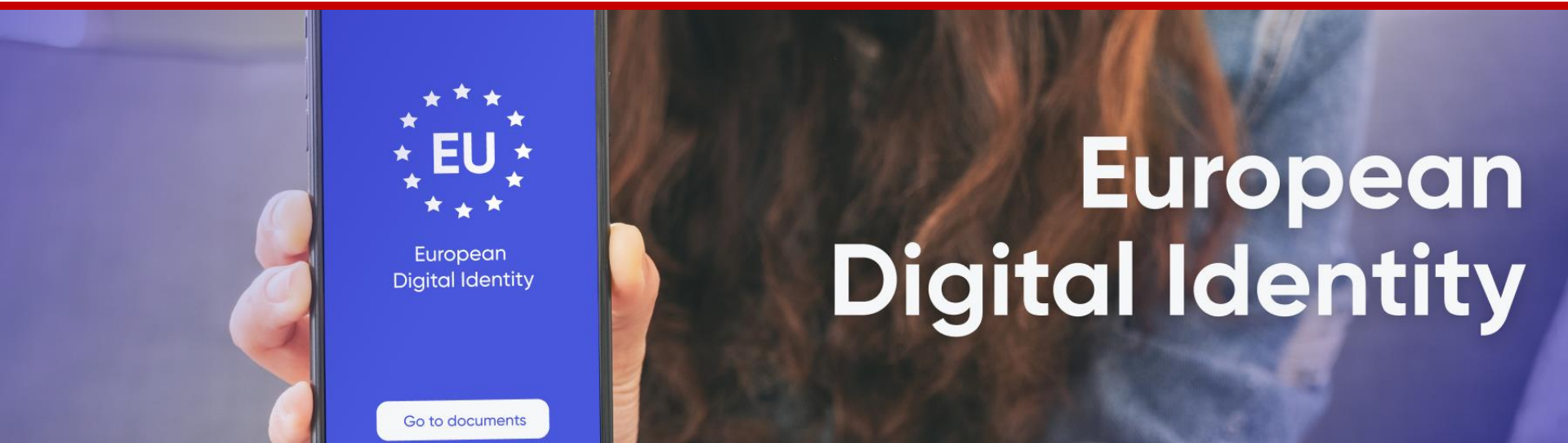
European Digital Identity Wallet

What could go wrong?

Paolo Campegiani
pca@bit4id.com



Subject of the analysis

- The revision of the eIDAS Regulation (eIDAS2) as proposed by the European Commission, and now under the “trialogue” phase

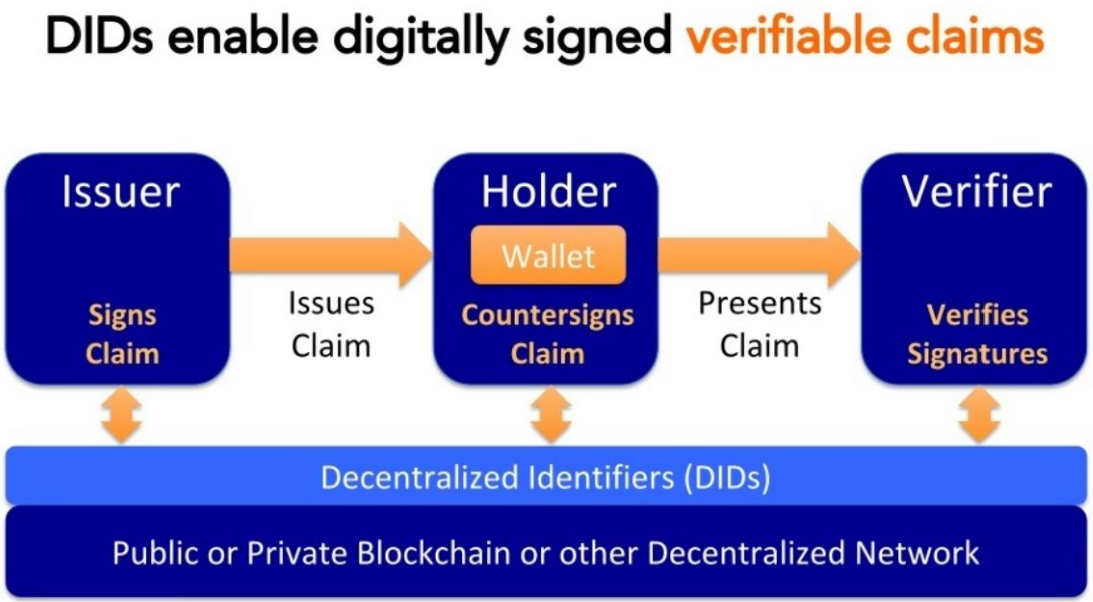
- How we could get (or not get) a vibrant ecosystem that fully realizes the Self-Sovereign Identity paradigm

Is the wallet voluntary? (This is still under discussion)

(28) Wide availability and usability of the European Digital Identity Wallets require their acceptance by private service providers. Private relying parties providing services in the areas of transport, energy, banking and financial services, social security, health, drinking water, postal services, digital infrastructure, education or telecommunications should accept the use of European Digital Identity Wallets for the provision of services where strong user authentication for online identification is required by national or Union law or by contractual

8. The use of the European Digital Identity Wallet by natural or legal persons shall be voluntary. Access to public and private services, access to labour market and freedom to conduct business shall not in any way be restricted or made disadvantageous for natural or legal persons not using European Digital Identity Wallets. It shall remain possible to access public and private services by other existing identification and authentication means.

It’s a chicken, egg AND grassland problem!



We need **three** parties to agree on a set of *semantic* principles:

- Who provides the original data (Issuer)
- Who manages them (Holder)
- Who receives them (Verifier)

Semantic interoperability is hard

- SSI systems designs focus a lot on *transport* interoperability, i.e. how a credential (or a claim) could travel inside the system

- If we want to have an automation of the underlying business processes, we need that the meaning of those attributes is formalized, so we need *semantic* interoperability

- What do you mean by “having a degree in computer science” in one or another European country?

Providing attributes is costly

- The Issuer in a SSI system has a role very similar to an Attribute Authority in a traditional digital identity system
- There are not a lot of Attribute Authorities around here
- This is because the business model of an Attribute Authority is not very clear (who pays for what?)

Managing attributes is not simple

- In a SSI system, the Holder (the User) manages their attributes

- In an ideal world, the User has a lot of attributes about them, and wisely choose a subset to compone a good fit for the service provider that have just requested access to

- In a real world:
  - understanding which attributes are needed and which not could be complex
  - Some attributes overlap or conflict
  - Some attributes are not *strictly* needed but *creatively* requested
  - People do not like to have so many choices

A new technology has new attack vectors

- There are not wide-scale deployments of SSI system, and surely not one that covers 24 languages and 27 countries

- SSI system are based on some innovation in cryptography and other technologies

- What happens if there is a significant data breach?

What we could do to get things right?

1. Private parties are critical for the success of the wallet: let them have a role and a voice

2. Private citizens are the real users and we should talk to them and address their needs and convince their fears (“this is an Orwellian-dystopia!”)

3. Public administrations are the early adopters: give them funds to adapt their systems

4. Regulators (standardizators, …) are not always right in the first time: accept to adapt and change things over time

bit4id.com

Paolo Campegiani
pca@bit4id.com