DIGITAL IDENTITY & VERIFIABLE CLAIMS

HOW CAN BANKS TAKE PART IN THE IMMINENT PARADIGM SHIFT?

Presented by

TOKENIKA

DIGITAL IDENTITY

- A hard approach: basic information allowing to determine who is who, e.g. first name + surname + unique ID (e.g. PESEL or NIP).
- A soft approach: additional information, such as: age, education, qualifications, employment history, medical records, online reputation, company representation / agency etc.

TOKENIKA

THE CURRENT PARADIGM

The subject is not the owner.

The bulk of our personal data is stored in databases owned by unrelated third parties (private companies and public agencies), whose business interests are not aligned with the user's interest.

THE CURRENT PARADIGM

- The information is spread across multiple locations which prevents its subject from having any control about who knows what and how the information is passed to other businesses, re-sold and monetized.
- The system is prone to hacking: there is a great incentive to hack a single database and steal large quantities of personal data, especially when information is linked to real-life identity.
- Our online reputation is non-transferable across systems, it's limited to separate silos. This is the main reason we are still not having a universal digital identity & reputation.
- The current system is very inefficient. Each company needs to verify the same information about its new user by doing it from scratch, as it's hard to share it between businesses.

THE FUTURE PARADIGM

The subject is the owner.

There is no split between the subject of information and the owner of this information.

You, as a user, own your identity, as you own cash.

TOKENIKA

THE FUTURE PARADIGM

- The ultimate control is with the user, i.e. the subject of information. No user profiling is possible without the user being aware of it and giving his explicit consent.
- There is no significant incentive for stealing someone's personal data, as you'd have to hack each individual account separately.
- The system is cheap for the end-user (unlike e.g. certified electronic signature), while there is a clear economic incentive for business entities to contribute to the growth of system.
- Users are incentivized to build their online reputation, as it can be shared across multiple unrelated systems and it works globally, even though no single company controls the system.

MAIN FEATURES

- The information is stored on the user side and the factual correctness is guaranteed by trustworthy third-party entities. Thus the user can make any (reasonable) statement about himself and simultaneously offer a cryptographic proof which certifies that what he says is actually true (i.e. has been confirmed by a trustworthy entity).
- The user can have multiple independent digital identity profiles and some of those profiles can be anonymous (then only the user knows that they belong to the same person).
- The system is not tightly coupled to any particular IT infrastructure, thus multiple identity systems can coexist & cooperate with each other, utilizing each other's power.

KEY CONCEPTS

- Decentralized Identifiers (DIDs)

  A new type of identifier for verifiable, "self-sovereign" digital identity.

- Verifiable Claims (VCs)

  A tamper-proof & cryptographically verifiable statement made by a trustworthy entity about another entity.

- Decentralized Public Key Infrastructure (DPKI)

  The main premise: identities ultimately belong to the entities they represent, thus every identity is controlled not by a trusted third-party, but by its principal owner.

KEY ACTORS

- Owner (a.k.a. Identity Subject)
  An entity about which VCs may be made. In most cases it's a physical person but can also be a legal person.
- Issuer (a.k.a Identity Provider)
  An entity that creates a VC and associates it with a particular Identity Subject. The perceived value of the claim is strictly related to the trustworthiness of its issuer and the claim must be within the business domain of an issuer. Examples: public agencies, banks, insurance companies, employers, education providers.
- Verifier (a.k.a Service Provider)
  An entity that needs to consume a VC about their customer (i.e. Identity Subject) as part of their on-line business model.

BUSINESS CASES

- Simple authentication: user uniqueness is the only aspect that matters (e.g. voting)
- Real identity verification: who you are dealing with does matter (e.g. KYC)
- Verification of factual claims regarding a known user (e.g. employment or AML)
- Verification of factual claims without disclosing who the user actually is (e.g. online auctions)

TOKENIKA

IDENTITY MANAGEMENT

Identity Management is the process of creating & collecting of VCs and then enabling third parties (i.e. SPs) to have a controlled access to those VCs.

- Direct: Identity Subject is the only holder of DIDs & VCs
- Delegated: Identity Subject employs a third party for managing their identity

You, as a user, own your identity, as you own cash, but you can still deposit it with a bank. However, it's a special kind of deposit, because the ultimate control always lies with Identity Subject.

CREDENTIAL REPOSITORY - THE 4TH ACTOR

Credential Repository (CR) is an implementation of Delegated Identity Management.

CR is an entity that facilitates secure and convenient management of DIDs & VCs:

- secure storage & management of DIDs & VCs,
- generation of trustworthy copies of VCs,
- can offer additional services, e.g. 2FA for SPs.

Important: It's a convenience service - the ultimate control is always with Identity Subject.

WHY BANKS CAN PLAY THE ROLE OF CR?

Probable evolution of banks' business domain:

- now: financial services
- in the future: digital identity (which also facilitates financial services)

Banks are in an ideal position to take on the role of Credential Repository:

- have an established reputation and are perceived as trustworthy, as they are licensed & strictly regulated,
- have a big user base (both consumers & businesses) and their services are used on a daily basis.

While financial services are mature & highly competitive (especially after PSD2), digital identity is an emerging opportunity, comparable to the online banking innovation.

MONETIZATION

- Hard identity will most probably be free for all, there'll be no monetization opportunity here.
- Soft identity has commercial value for:
  - Identity Subject (so that he can prove that his statements about himself are true)
  - and/or Service Provider (so that it can do business with Identity Subject)

Thus it's possible to introduce a cryptographic token enabling an economic gratification for identity producers (Identity Issuers) from identity consumers (Identity Subjects and Service Providers).

POSSIBLE EXTENSIONS

As more & more businesses move online and become global, it's hard to imagine the future of Internet without the problem of digital identity being eventually sorted out.

- By-product: Strong Customer Authentication (needed for PSD2)
- Global reputation systems and intention-based economy
- In line with the process of digitalization of all state-issued documents and commercial certificates

THANK YOU

SYGNET
sygnet.eu

Presented by
TOKENIKA

tokenika.io
contact@tokenika.io