NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

Prof. Shamik Sural
Department of Computer Science & Engineering
Indian Institute of Technology Kharagpur

Lecture 43: Identity Management - I

CONCEPTS COVERED

- Basic Concepts of Identity
- Centralized Identity Management
- Introduction to Decentralized Identity Managment

KEYWORDS

- Identity
- Centralized Identity Management
- Single Sign on
- Self-Sovereign Principle
- Decentralized Identifier

What is Identity?

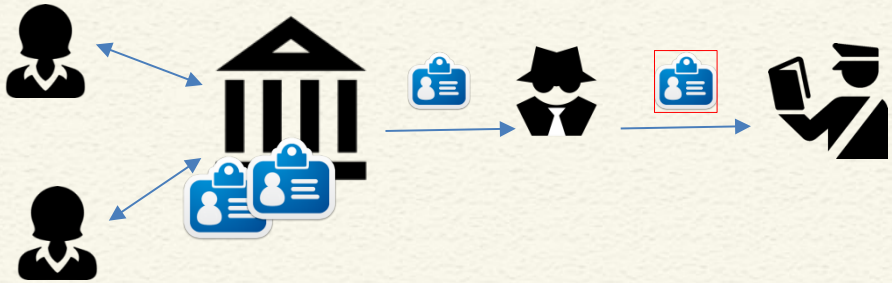
- People are known by their identities - drives every business and social interaction
- Physical Identity is a collection of attributes
  - Name
  - Age
  - Financial history
  - Work history
  - Address history
  - Social history
  - ….

Centralized Digital Identity

- Individuals do not have any control over the information that comprises their identities
- Identity fraud - no visibility over the identity attributes
- Authentication
- Authorization
- Verification

Centralized Digital Identity

- Individuals do not have any control over the information that comprises their identities
- Identity fraud - no visibility over the identity attributes
- Authentication
- Authorization
- Verification



Digital Identity - Single Sign On (SSO)

- Single identity for various purposes
- No need to maintain multiple identity documents
- Widely conceptualized in software industry
- One password to access multiple services
- Single identity provider (IDP) maintains the identity
- Identity consumers (services) use the IDP to authenticate the identity holder
- During authentication, the identity is not exposed to the services

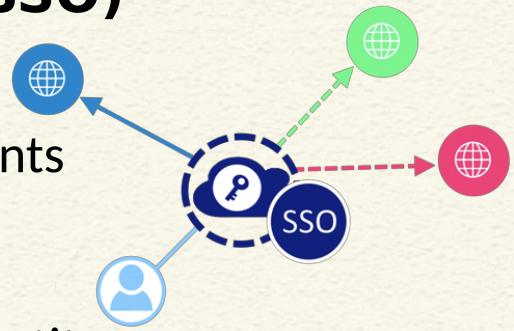
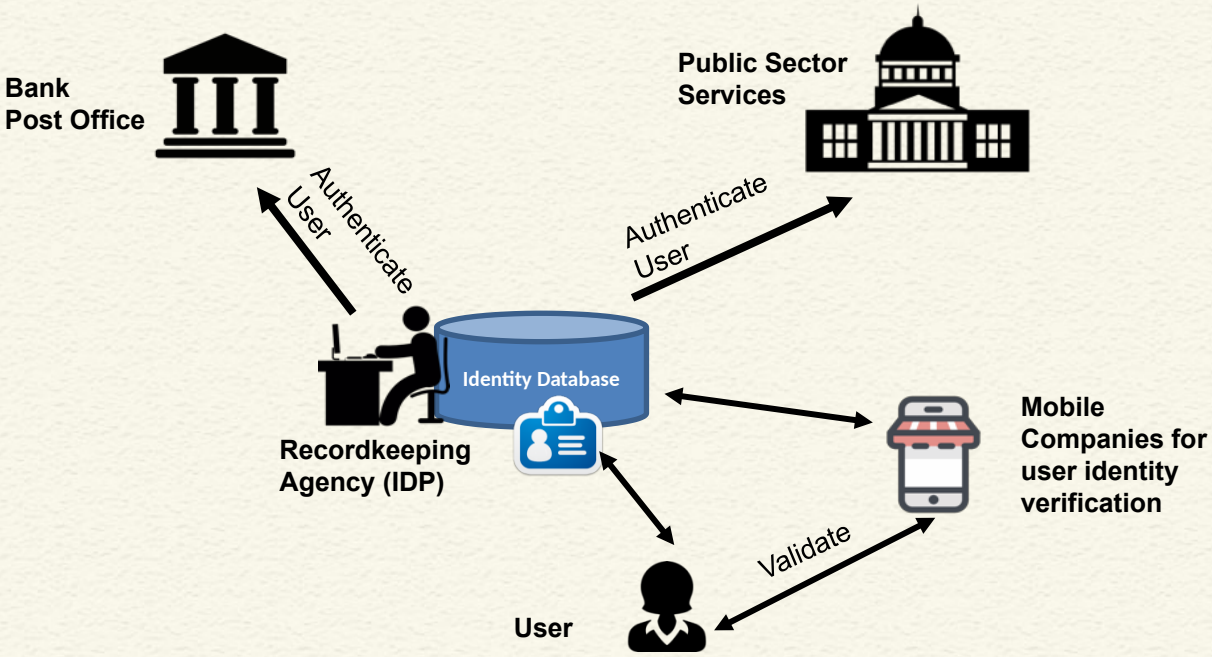


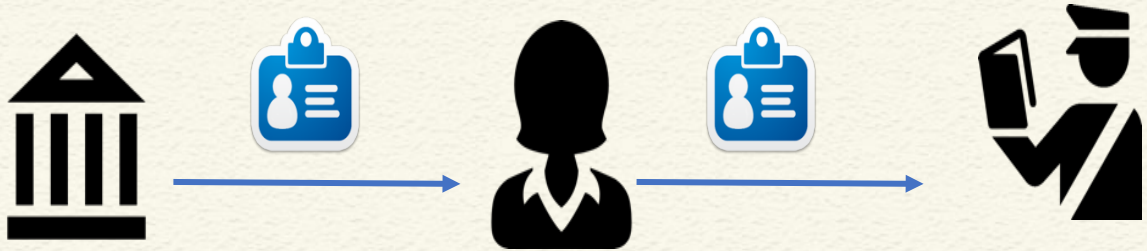
Image Source: https://www.e-spincorp.com/global-theme-and-feature-topics/single-sign-on-sso/

SSO and Decentralization



Decentralizing Digital Identity

- No Centralized Trusted Identity Provider / Registry
- Digital representation of physical identity
- Two major problems:
  - Verifying the **identity issuer**
  - Verifying the **identity holder**



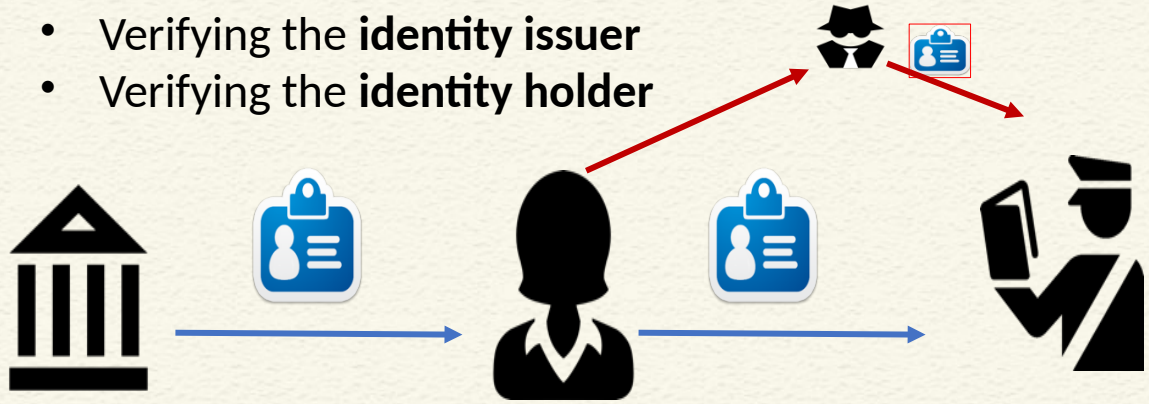
Issuer - Government

Holder

Verifier

Decentralizing Digital Identity

- No Centralized Trusted Identity Provider / Registry
- Digital representation of physical identity
- Two major problems:
  - Verifying the **identity issuer**
  - Verifying the **identity holder**



Fundamental Principles of Digital Identity Management

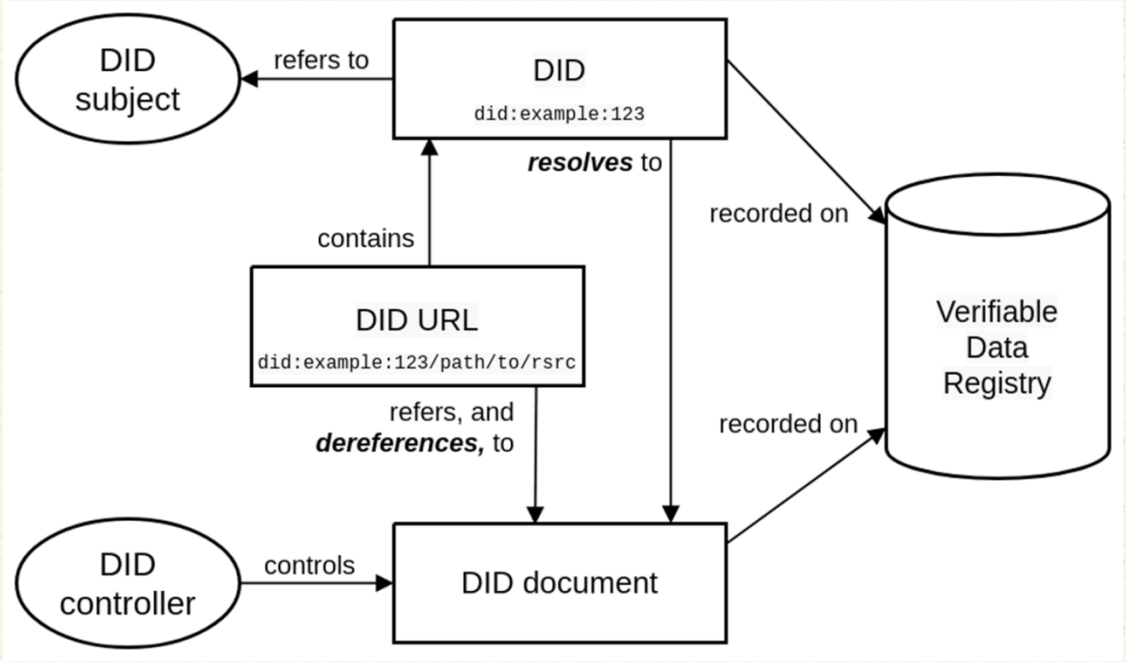
- Self-Sovereign Identity (Privacy Control)
- Individual should have full control and ownership of their identity information
- Individuals can control the usage of their own identity profile for business and social interactions (Consent - agreement for information usage)
- Identical to how we use our physical identity
- Holder possesses the ID
- Holder chooses whom to present the ID
- Burden at individual user?

Decentralized Identifiers (DIDs)

- Provides Verifiable, Decentralized Digital identity
- Designed to be decoupled from:
  - centralized registries
  - identity providers
  - certificate authorities
- Holder of DID can prove its ownership on the DID without the help of any other party
- W3C Proposed Recommendation

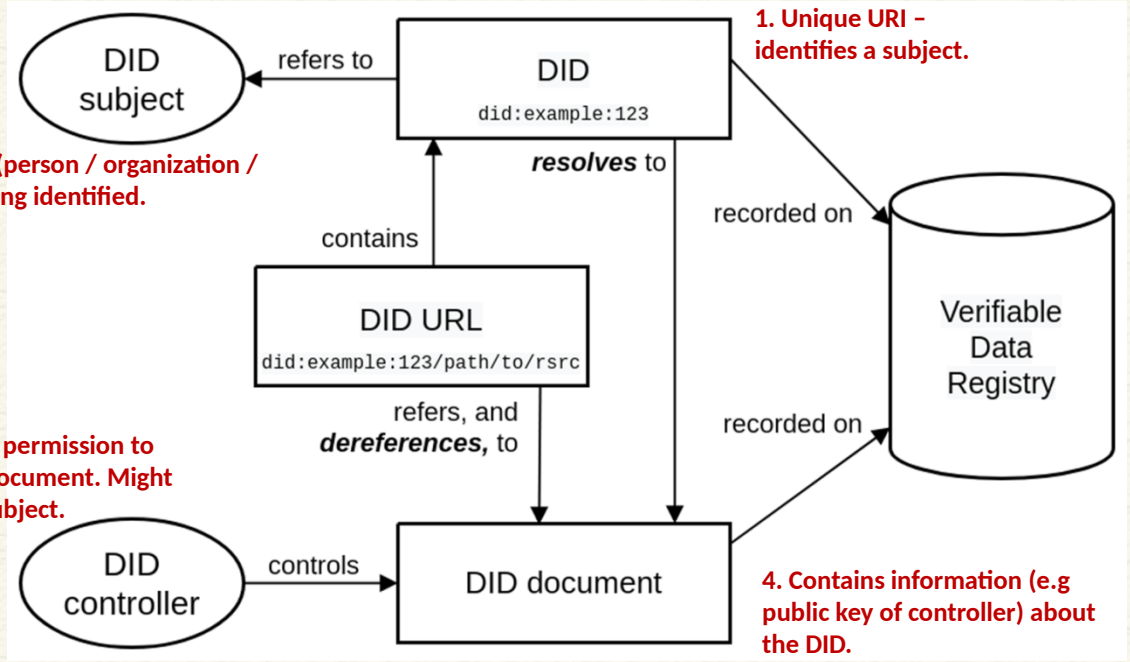
https://www.w3.org/TR/did-core/

DID Architecture



https://www.w3.org/TR/did-core/

DID Architecture



https://www.w3.org/TR/did-core/

CONCLUSIONS

- Introduced the fundamental concepts of identity management
- Centralized vs. decentralized identity management
- DID as a W3C recommendation

REFERENCES

- Web resources as mentioned from time to time


Thank
you