NPTEL ONLINE CERTIFICATION COURSES

Blockchain and its applications

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

Lecture 44: Identity Management - II

CONCEPTS COVERED

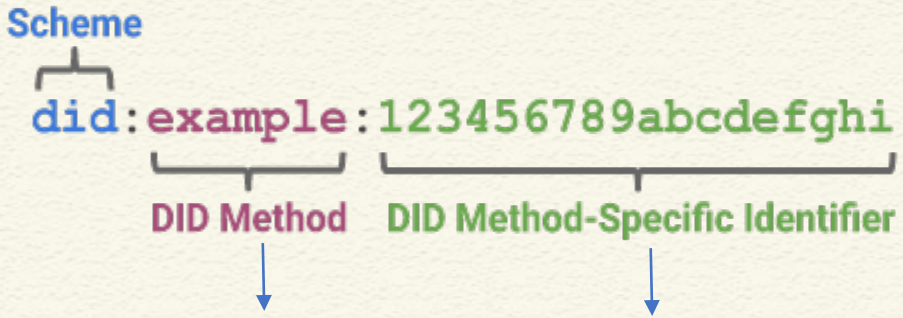
- How DID Works
- DID Work Flow
- Decentralized DID Registry – Use of Blockchain
- Verifiable Credentials

KEYWORDS

- DID
- DID Registry
- Hyperledger Indy
- Verifiable Credential (VC)

DID URI

- Controller controls a **DID Document**.
- A **DID** is a unique address (URI) to the location of that document.



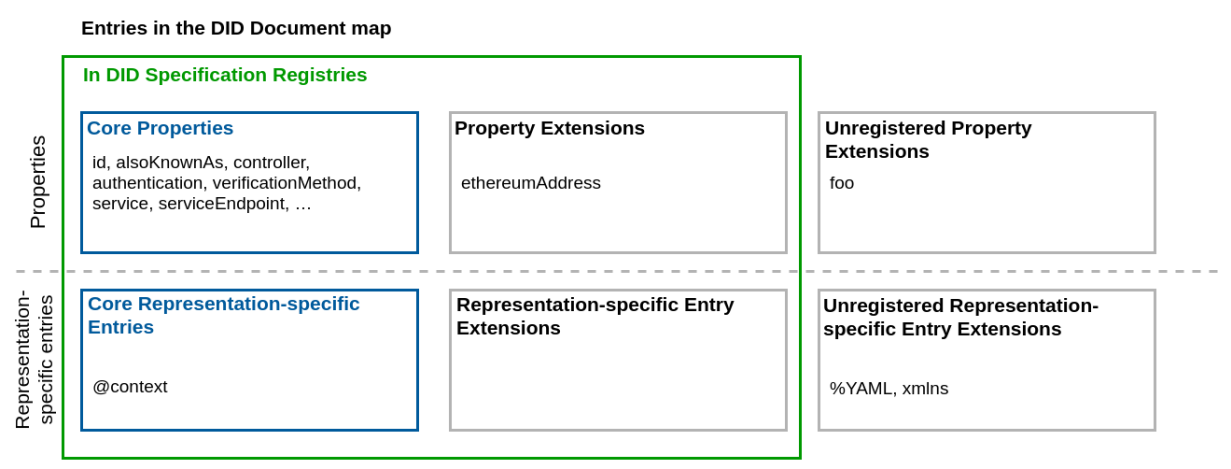
http://www.faqs.org/rfcs/rfc2396.html

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

DID Document

- A set of data describing the DID subject, including mechanisms such as cryptographic public keys, that the DID subject or a DID delegate can use to authenticate itself and prove its association with the DID.
- DID document consists of a map of entries, each entry consisting of a key/value pair.

Representation-specific entries include JSON, XML, etc



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

DID Document Example (JSON)

```
{
    "id": "did:example:123456789abcdefghi",
    "authentication": [{
        "id": "did:example:123456789abcdefghi#keys-1",
        "type": "Ed25519VerificationKey2020",
        "controller": "did:example:123456789abcdefghi",
        "publicKeyMultibase":
          "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
    }],
    "service": [{
      "id":"did:example:123456789abcdefghi#linked-domain",
      "type": "LinkedDomains", // external (property value)
      "serviceEndpoint": https://bar.example.com
     }]
}
```

DID for a particular DID subject

Verification Method specifying how the DID subject can authenticate itself.

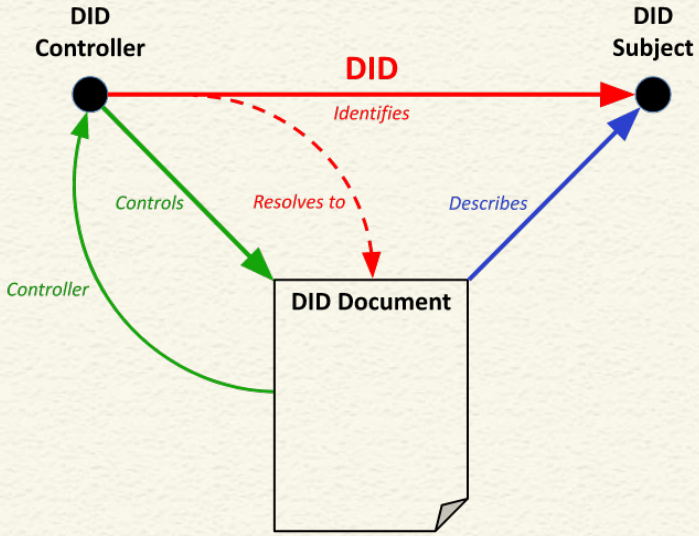
Service Endpoint denoting ways of communicating with the DID subject

It tells how to reach the subject. Otherwise, there is no meaningful use of authentication

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

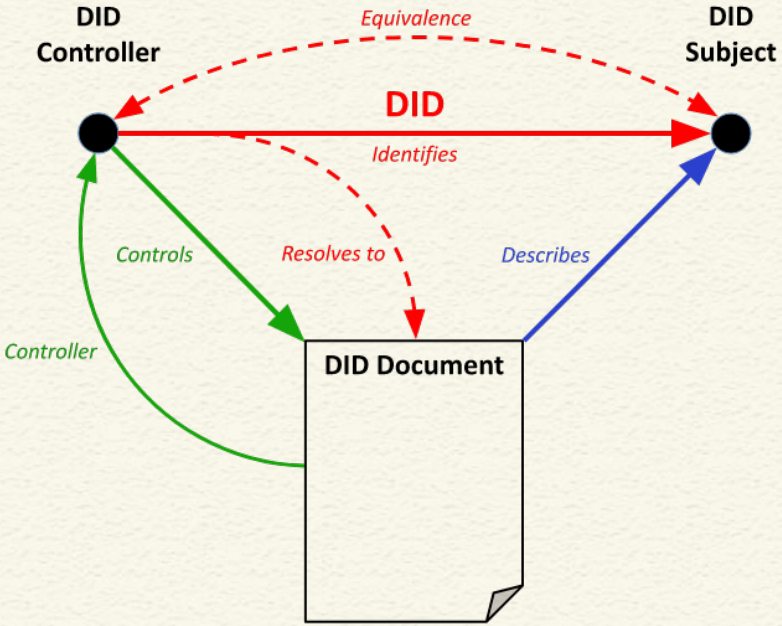
Relationship between Different Components of DID

- A DID is an identifier assigned by a DID controller to refer to a DID subject and resolve to a DID document that describes the DID subject.
- The DID document is an artifact of DID resolution and not a separate resource distinct from the DID subject.
- DID document resides inside verifiable data registry

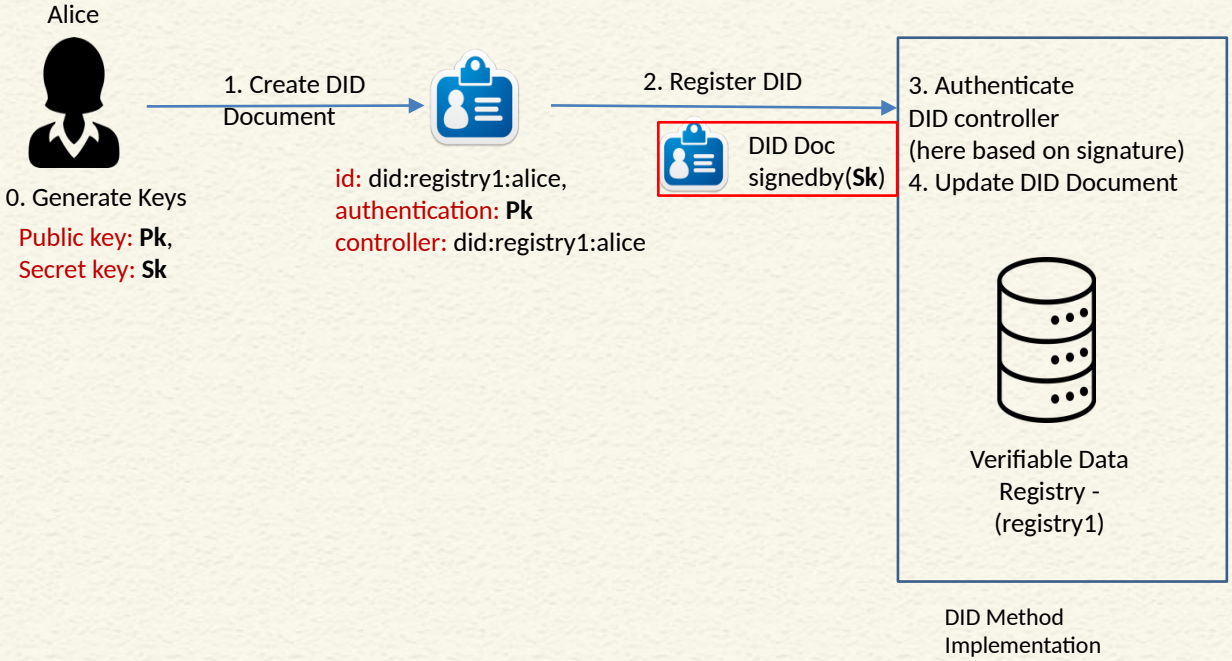


Relationship between Different Components of DID

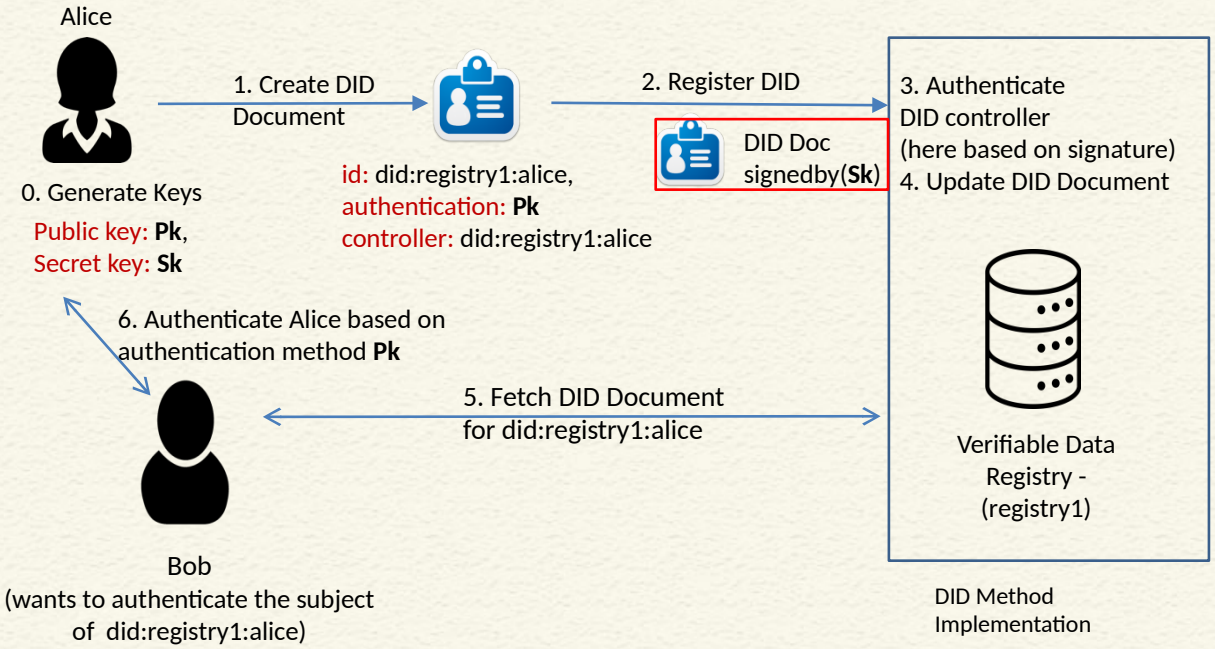
- Often the DID Subject and the DID Controller are the same entity



DID Flow – DID Registration



DID Flow – DID Registration



DID Method Security

- DID Registry ideally enforces DID Method protocols.
- Centralized DID Registry brings in risks
  - Manipulating DID Documents
    - Changing authentication methods
  - Censoring DID Documents
    - Refusing to resolve certain DID Documents
- Lack of Transparency

Verifiable Data Registry - (registry1)

DID Method Implementation

Centralized

Decentralized DID Registry

- Blockchain based Implementation of Verifiable Data Registry
- DID Methods are implemented as smart contracts.
  - Smart contracts enforce how authorization is performed to execute all operations, including any necessary cryptographic processes.
- Transparent Immutable Ledger allows verifiability of DID Documents
  - Any party can validate if a DID Document's creation / updation transactions were authenticated or not.

Verifiable Data Registry

Blockchain based DID Registry

Public permissioned ledger based registry.

- Any party can read the ledger.
- Only selected (registered) parties and write to the ledger.

HYPERLEDGER INDY

https://hyperledger-indy.readthedocs.io/en/latest/

DIF

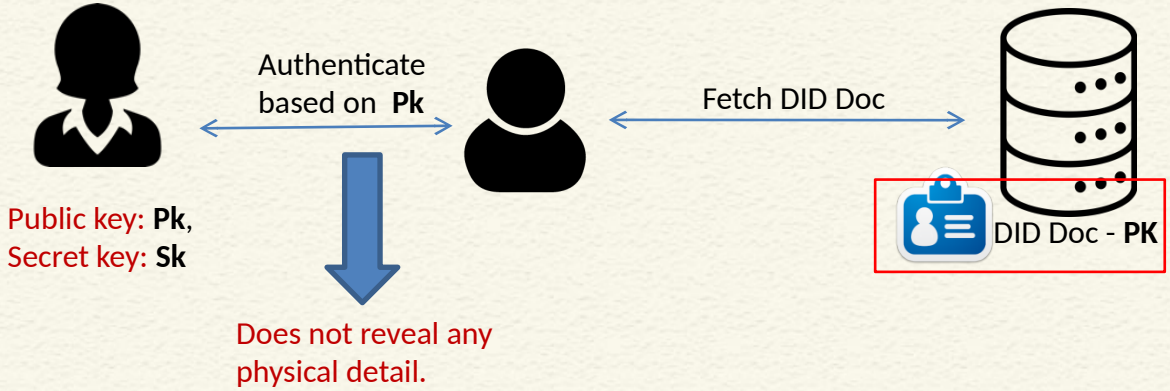
Sidetree

Protocol for creating scalable DIDnetworks that can run atop any existing permissionless blockchain. (e.g. Bitcoin, Ethereum, etc.)

https://identity.foundation/sidetree/spec/

Binding DID to Physical Identity

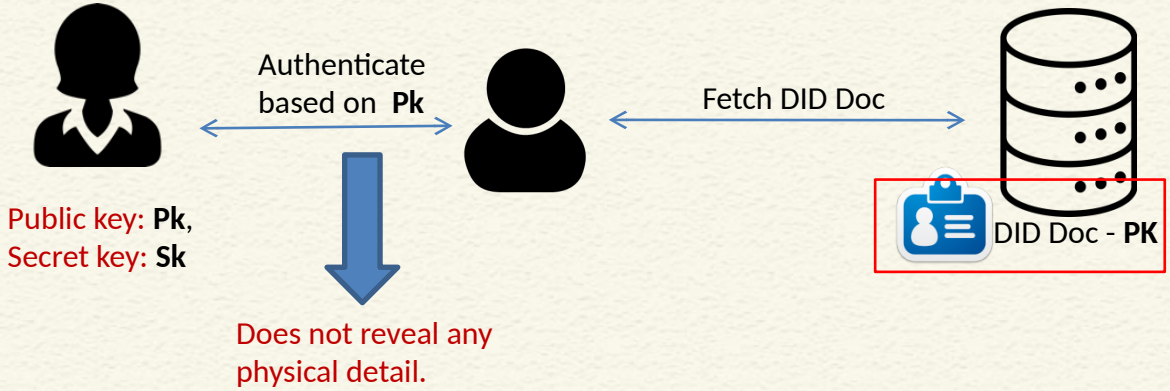
DIDs only allow a DID controller to prove its control over its DID Document.
This is useful to authenticate an entity with respect to its DID



If some physical detail is presented, then that is only self attested by the DID controller, and not any verified information.

Binding DID to Physical Identity

DIDs only allow a DID controller to prove its control over its DID Document.
This is useful to authenticate an entity with respect to its DID



DID are not inherently tied to any physical identity (real world identity).

Verifiable Credentials

- **Verifiable Credentials Data Model** – W3C Recommendation
- Digital Representation of Credentials
  - Driver's licenses - assert that capability of operating a motor vehicle
  - University degrees - assert our level of education
  - Government-issued passports - permit to travel between countries
  - Identity – Birth Certificate, Citizenship Certificate, etc.
- **Decouples Issuer, Holder and Verifier**
- **Cryptographically secure**
- **Privacy respecting**
- **Machine-verifiable**

https://www.w3.org/TR/vc-data-model/

CONCLUSIONS

- Implementation of DID
- Use of blockchain for DID registry implementation
- Verifiable credentials and their relationship with DID

REFERENCES

- Web resources as mentioned from time to time


Thank
you