Verifiable Credentials, Decentralized Identifiers

ITU-WHO Workshop on Smart Vaccination Certificate Exchange, 2021-08-11

Ivan Herman, W3C, ivan@w3.org

These slides: https://iherman.github.io/did-talks/talks/2021-WHO_ITU/#/

About W3C "Leading the Web to its Full Potential"

Tim Berners-Lee, Director of W3C

- Founded in 1994
- ≈ 450 Members, ≈ 60 staff all over the World
- Focuses on the Web Ecosystem: users, developers, browsers, etc.
- Develops standard technologies for the Open Web Platform (e.g., HTML, SVG, CSS, MathML, …)

W3C Recommendations (a.k.a. “Standards”)

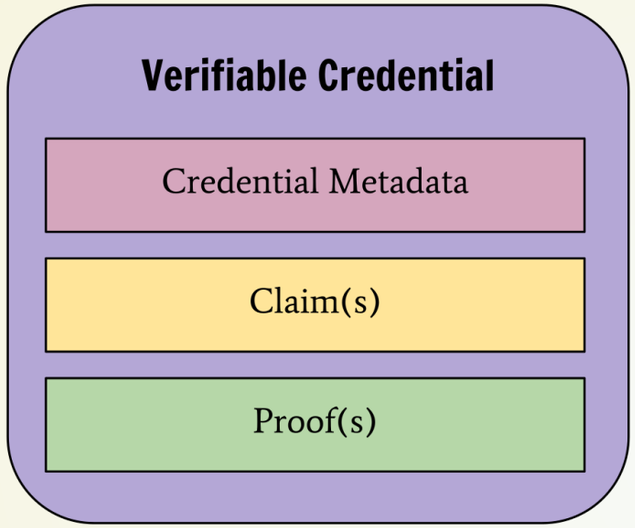
- Specified by *Working Groups*
  - staffed by experts delegated by W3C Members (companies, institutions, universities…)
  - chartered by the W3C Membership
- Final versions voted upon by the W3C Membership
- Developed under the W3C Patent Policy:
  - are freely available to all
  - can be implemented on a Royalty Free basis

Verifiable Credentials

What is a Verifiable Credential?

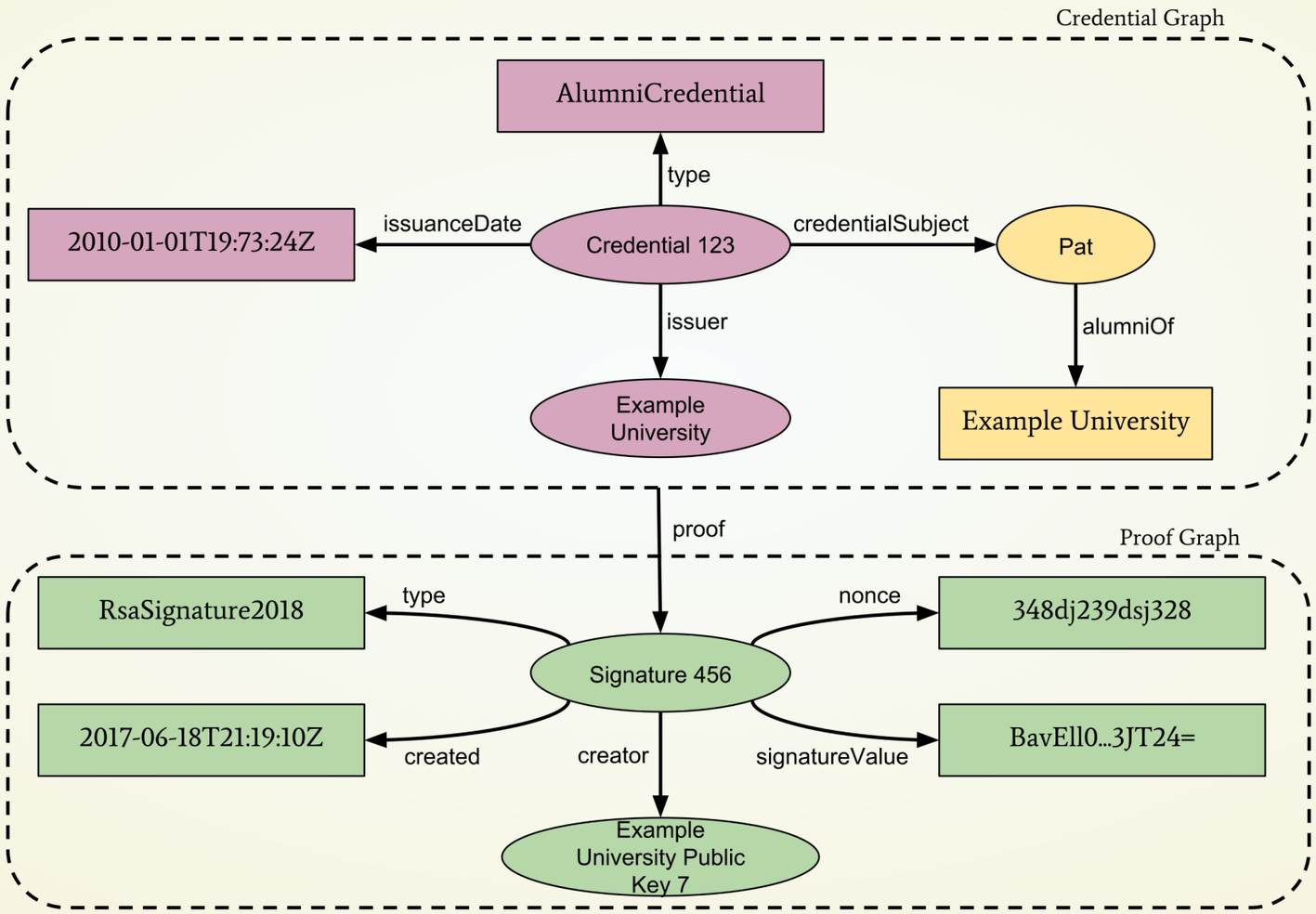
- A digital resource that can hold the same credential data as a physical credential (driving license, university diploma, medical information)
- The resource also includes cryptographic data to make the credential tamper evident and trustworthy (e.g., digital signature)
- It uses digital identifiers to refer to the ”subject”, the ”issuer”, or the “holder” of the credential

Simple View of a Verifiable Credential



- Metadata: contain expiry dates, representative image, identification of the issuer and the subject, etc.
- Proof(s): contain the cryptographic data for, e.g., signatures (keys, signature values, etc.)

Simple View of a Verifiable Credential



The Verifiable Credential standard provides a framework

- The Recommendation itself standardizes terms like "`issuanceDate`" or "`proof`"
- The final application defines the terms like "`alumniOf`" or "`AlumniCredential`"
- This extension mechanism is at the heart of the usage pattern for Verifiable Credentials

Representation of Verifiable Credentials

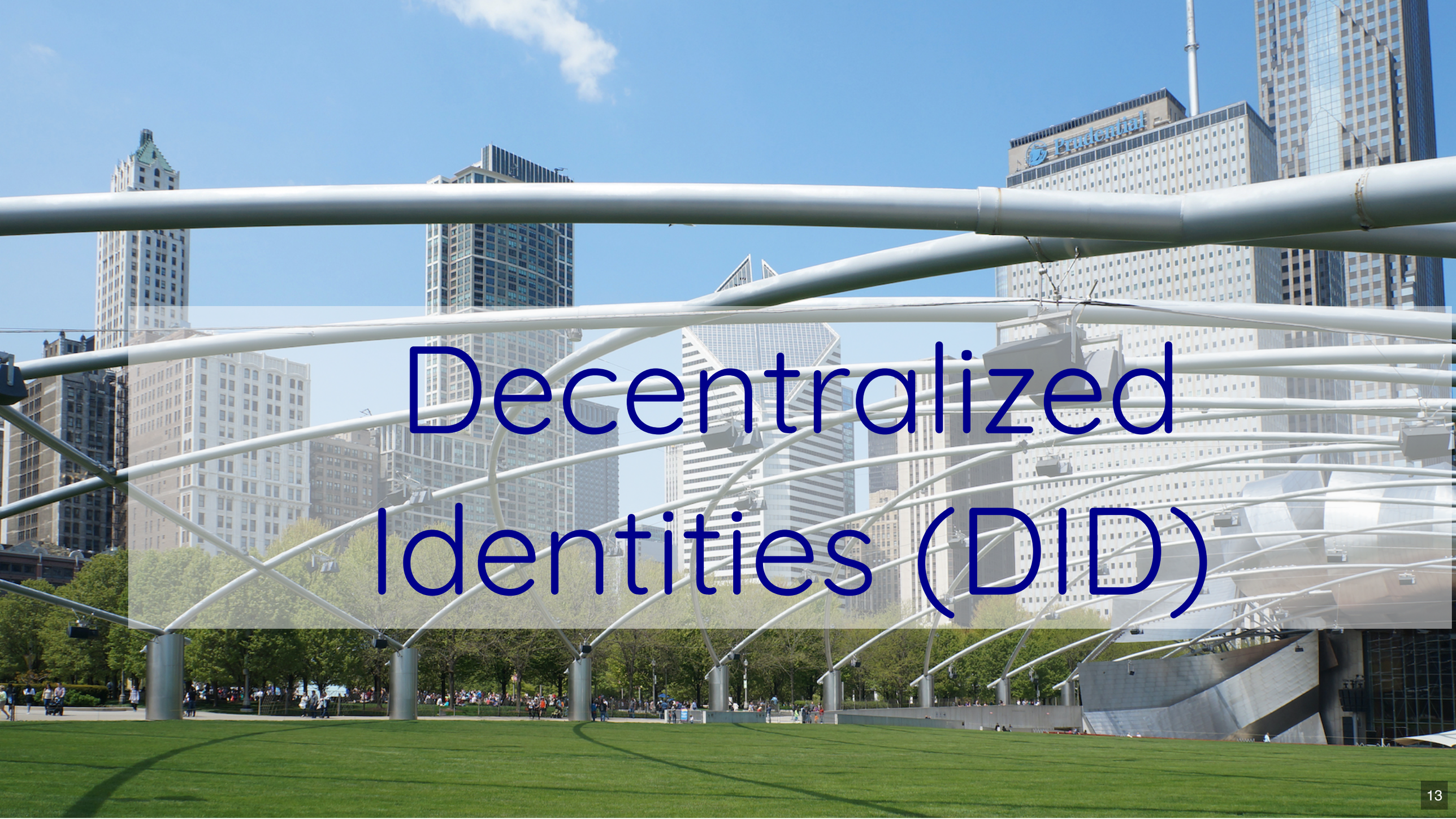
- The abstract model can be "expressed" in JSON, JSON-LD, CBOR,…
  - can then be encoded in, say, a QR code
- The cryptographic data can be expressed in various formats, e.g., JWT, JSON-LD Proofs and Signatures,…
- The standard does not specify the "higher level" functionalities, e.g., the behavior of specialized wallets
  - this is left to implementers and to market forces

Small (incomplete) example

```
{
        "@context": [
                "https://www.w3.org/2018/credentials/v1",
                "https://www.w3.org/2018/credentials/examples/v1"
        ],
        "id": "http://example.edu/credentials/1872",
        "type": ["VerifiableCredential", "AlumniCredential"],
        "issuer": "https://example.edu/issuers/565049",
        "issuanceDate": "2010-01-01T19:73:24Z",
        "credentialSubject": {
                "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
                "alumniOf": {
                        "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
                        "name": "Example University"
                }
        },
        "proof": {
                "type": "RsaSignature2018",
                "proofPurpose": "assertionMethod",
                "verificationMethod": "https://example.edu/issuers/keys/1",
                "jws": "eyJhbGciOiJS...HUdBBPM"
        }
}
```

Identifiers play an essential role in credentials

- Per specification, any digital identifier can be used (based on schemes like `https`, `mailto`, etc.)
- But the control, the reliability, etc, of the identifier may be crucial
- Here is where Decentralized Identity (DID) comes into the picture



Decentralized Identities (DID)

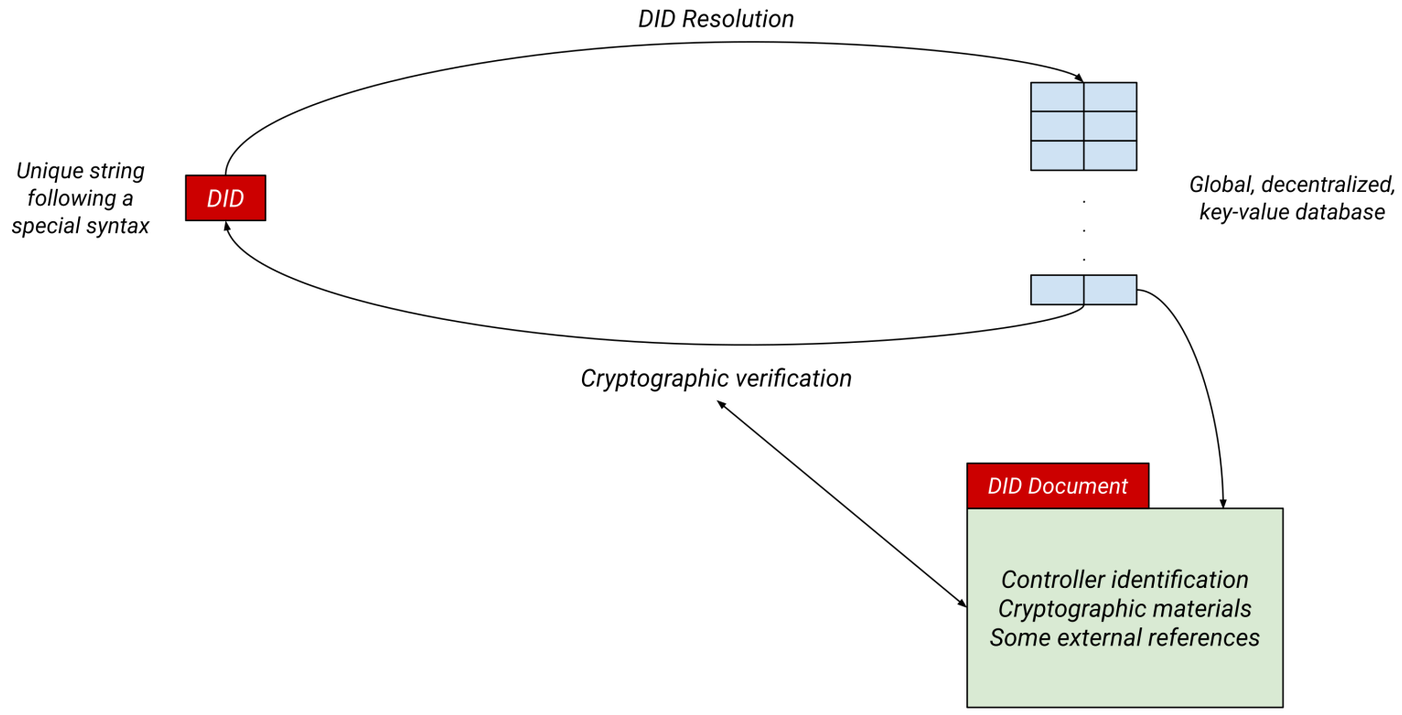
What is DID?

A DID is a self-sovereign identity, i.e., lifetime, portable, and verifiable digital identity that does not depend on any centralized authority

Goals of DIDs

- *Ease of creation*
  - it should be quick and "cheap" to create possibly thousands of DIDs
- *Decentralized*
  - do not depend on centralized registries, identity providers, authorities, etc.
- *Persistent*
  - once created, it is permanently assigned to the subject
- *Resolvable*
  - it is possible to find out basic set of information on the subject
- *Cryptographically verifiable*
  - there is a mechanism to cryptographically prove identity and ownership

High level view: DIDs and DID Documents



“Global, distributed, key-value database”

- Also known as ”Verifiable Data Registry”
- There may be several of those!
  - in the DID world, the term *method* is used for the different approaches and/or implementations
- Different methods can have different approaches
  - may be based on distributed ledgers (generic, like Bitcoin or Ethereum, or custom built)
  - DID documents stored on specialized sites (e.g., GitHub)
  - may be ephemeral DIDs with lighter requirements (e.g., on an intelligent device)
- The choice depends on the relative importance of the requirements for a specific usage

DID Documents

- Contain reference to the "controllers", i.e., entities that may make changes on the DID Document
  - the controller may or may not be identical to the "subject" of the identification
- Include cryptographic data related to the DID subject
  - RSA, various elliptical curve keys, etc.
  - can be expressed using JWK or with DID specific terms
  - can be used for
    - authentication;
    - assertions (e.g., of credentials);
    - key agreement (e.g., to establish secure communication);
    - capability invocation (e.g., authorization to access an API);
    - capability delegation (e.g., delegate an API access to another authority);
    - …

Serialization of DID Documents

- DID Documents are defined via an abstract data model
- Can be serialized as:
  - JSON
  - JSON-LD
  - CBOR
  - other serializations may come to the fore

Documents to read

- *Verifiable Credentials:*
  - Data Model Specification: https://www.w3.org/TR/vc-data-model/
  - Use Cases: https://www.w3.org/TR/vc-use-cases/
- *Decentralized Identifiers:*
  - Core Architecture and Data model: https://www.w3.org/TR/did-core/
  - Use Cases: https://www.w3.org/TR/did-use-cases/
- These slides:
  - In HTML: https://iherman.github.io/did-talks/talks/2021-WHO_ITU/#/
  - In PDF: https://iherman.github.io/did-talks/talks/2021-WHO_ITU/index.pdf

These slides: https://iherman.github.io/did-talks/talks/2021-WHO_ITU/#/