

Decentralized Identifiers (DIDs)

Presentation held for W3C Evangelists , on 2020-04-27

Ivan Herman, ivan@w3.org



Introduction



Importance of identifiers in a digital world

- It is increasingly important to identify persons, concepts, things...
 - any reasoning, control, associations, etc., of resources rely on this ability
- The digital economy relies on proper identification to combine information from different sources
 - it is vital that identifiers are unique

A large crowd of people in traditional Breton costumes, including men in hats and women in bonnets, gathered outdoors.

what are the
problems?

A typical experience

Consider these two scholarly references:

- Tomislav Strinić, Damir Buković, Ljubomir Pavelić, Josip Fajdić, Ivan Herman, Ivica Stipić, Ivan Palada & Ivana Hirš, “Anthropological and clinical characteristics in adolescent women with dysmenorrhea”. *Collegium antropologicum*, 27(2), (2003).
- Ivan Herman, Markus Gylling, “Bridging the Web and Digital Publishing”, *The Journal of Electronic Publishing*, (2015).

- Only one of the two publications is mine...
- The name is not enough; you need a *unique personal identification* to avoid problems with, in this case, homonyms
- This has become even more important in a networked, digital world

Of course, I do have identifiers

- ivan@w3.org
- ivan@ivan-herman.net
- <https://www.w3.org/People/Ivan/>
- <https://www.ivan-herman.net/>
- 0000-0003-0782-2704 (ORCID)
- 89df9321-bf5c-4237-aabc-1f8f202ab5c6 (UUID)

Globally unique identifiers are not only for persons

- They are becoming ubiquitous all around us:
 - companies, institutions,...
 - books, magazines,...
 - retail items
 - genes, proteins, viruses,...
 - stars, galaxies,...
 - vehicles, airplanes,...
 - intelligent home devices, Internet/Web of Things,...

Identifiers are usually context dependent

- Personal identifiers
 - `ivan@ivan-herman.net`
 - `https://www.ivan-herman.net/`
- Professional identifiers
 - `ivan@w3.org`
 - `https://www.w3.org/People/Ivan/`
 - `0000-0003-0782-2704`
- Undecided (depends on its usage)
 - `89df9321-bf5c-4237-aabc-1f8f202ab5c6`

There is a need for many identifiers!

- One person may have to have many different identifiers, depending on the person's various facets in life
 - there should be a very easy way to create as many unique identifiers as needed!
- Are the aforementioned identifiers really the right ones?
 - note that most of them are created for another purpose (email, personal information site) and are “just” used as identifiers...

Problems with current identifiers

- *Ease of creation*
 - <https://www.ivan-herman.net> depends on buying a host name
 - ivan@w3.org is not meant to be an identifier, and an email address is not “cheap”
- *Decentralized*
 - <https://www.ivan-herman.net> depends on a single point of failure; what happens if the hosting site disappears?
 - 0000-0003-0782-2704 depends on the ORCID database. What happens if it is discontinued, hacked, etc?

Problems with current identifiers

- *Persistent*
 - When I leave the W3C then ivan@w3.org disappears...
 - If I do not pay for the ivan-herman.net domain any more, the URL disappears...
- *Resolvable*
 - How can I get more information on what 0000-0003-0782-2704 identifies?
- *(Cryptographically) Verifiable*
 - What about <https://www.ivan-herman.com>? How can one prove that this domain is **not** referring to me?
 - What happens if I stop paying for the domain and somebody else buys it?

Identifiers may fulfill several requirements

- HTTPS URIs are:
 - resolvable
 - verifiable by a human and through HTTPS and certificates
 - *but:* centralized, not persistent, complex to create
- ORCID numbers are:
 - persistent (while ORCID is around, that is), easy to create
 - verifiable by a human but not cryptographically
 - *but:* centralized, only resolvable by turning them into a special URL
- UUID-s are
 - persistent, decentralized, easy to create
 - *but:* not resolvable, not verifiable

No identifiers display
all those
characteristics!

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.
 - the DID has a sovereign controller:
 - the entity identified by the DID (the subject), or
 - whoever else who has the privilege to control the DID (e.g., the owner of a dog “controls” the DID identifying the dog)

Goals of DIDs

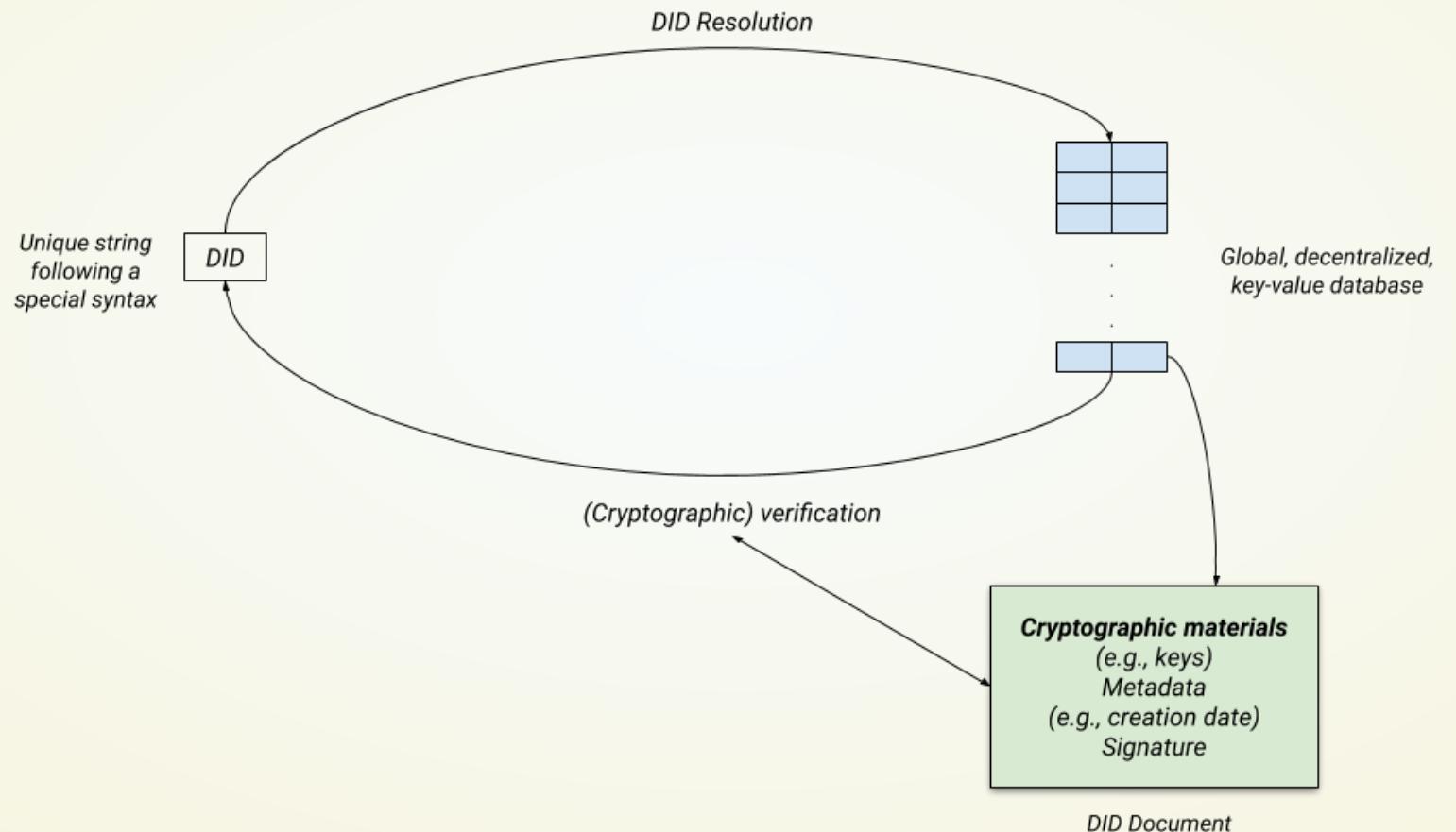
- *Persistent*
 - once created, it is permanently assigned to the subject
- *Resolvable*
 - it is possible to find out basic set of information on the subject
- *Cryptographically verifiable*
 - there is a mechanism to cryptographically prove that it indeed identifies a specific subject (possibly controlled by a separate controller) and nothing else

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

An aerial photograph of the city of Lisbon, Portugal, showing a dense urban area with numerous buildings featuring traditional red-tiled roofs. In the center, there is a large, open public square with a blue construction crane standing prominently. The architecture is a mix of modern and traditional styles, with many multi-story buildings and some larger institutional or commercial structures in the background.

High level view on DIDs

High level view: DidS and DID Documents



“Global, distributed, key-value database”

- There may be several of those!
 - in the DID world, the term *method* is used for the different approaches
- Different methods can have very different characteristics
 - May be based on distributed ledgers (generic or specialized)
 - DID documents stored may be 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 various requirements for a specific usage

DID Documents

- Contain cryptographic information related to the subject (and controller) of the DID
 - verify the control of the DID document, i.e., its authenticity
 - trusted communication
 - the DID documents may be signed
 - information about, e.g., key revocations
- May also include other types of data related to the subject
 - reference to a Web site
 - various services
 - etc.
- May or may not physically “exist” somewhere in the database
 - some methods generate them on-the-fly

DIDs and DID Documents are closely coupled

- DIDs have the right characteristics through the DID Document
 - DID documents are the “representation data and metadata” of a DID in the Web architecture
- A DID Document is tightly bound to the DID it “describes”
- DID+DID Document may be also used as a decentralized cryptographic keychain for various cryptography applications

Serialization of DID Documents

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



Some use cases

There are simple ones

- Securing unique, secure, etc., identities for persons, animals, objects,...
 - unique and unambiguous literature references
 - consistent semantic statements on “resources”
 - identify objects in an internet of “things”
 - etc.
- DID usage is often bound to Verifiable Credentials
 - e.g., life-long credential proving a University Degree, identified with a DID
 - there are (experimental) discussions on using DID+VC as a tool for a COVID-19 proximity checking apps

Find information on purchased goods

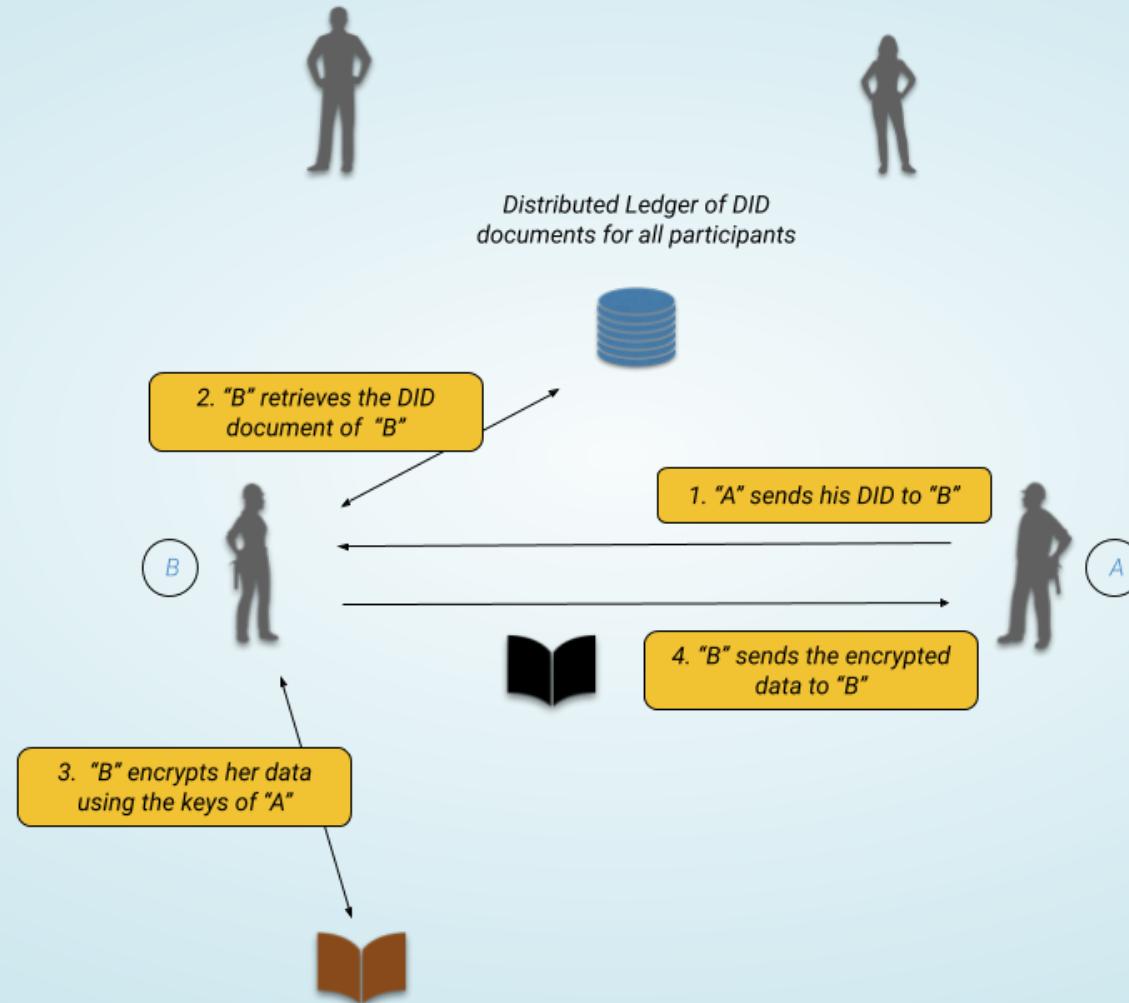


Find information on purchased goods

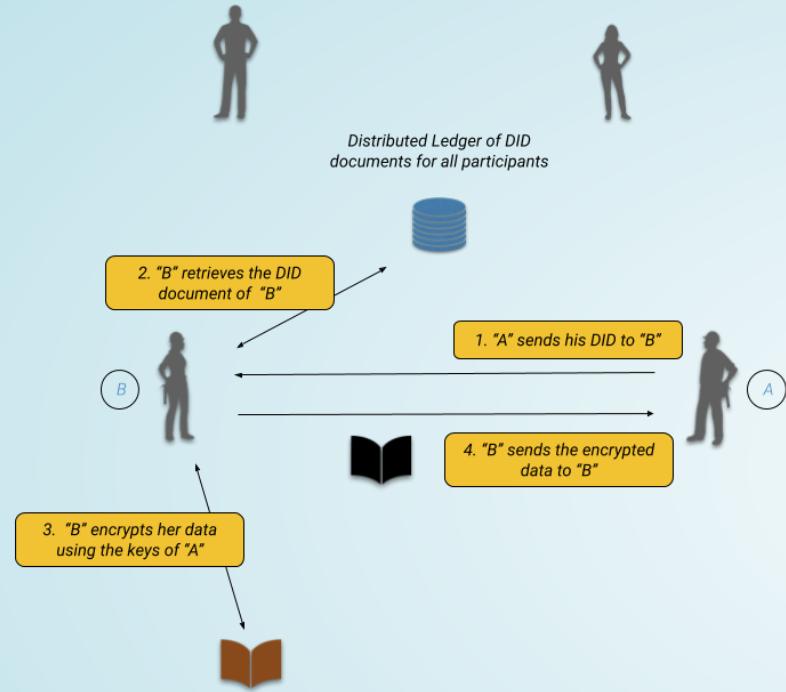


- It is very important that:
 - the identification is unique and persistent
 - the information has not been tampered with
- The same mechanism can be used for constituent parts of goods but the information can remain fully decentralized

Pool of relationships



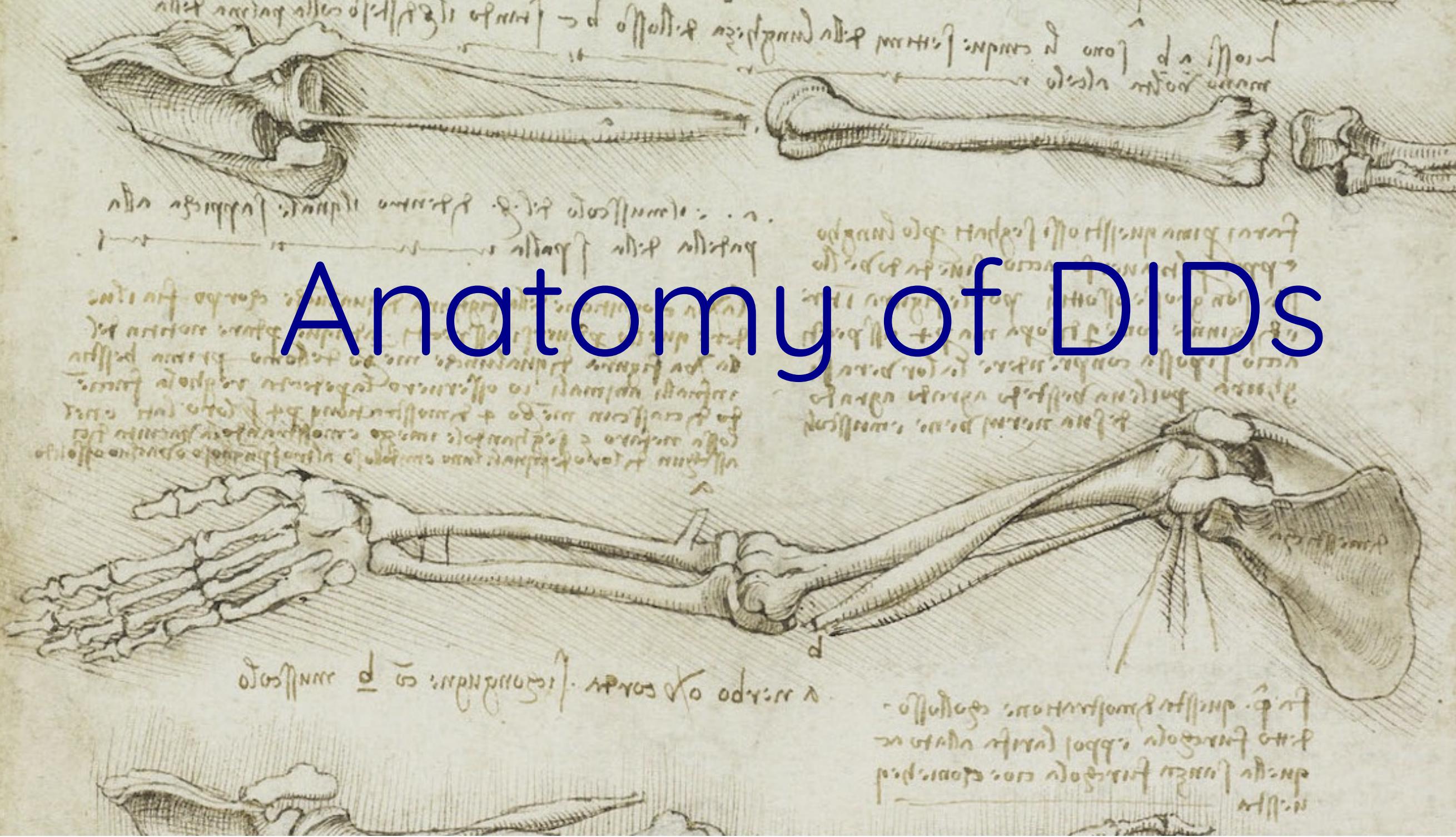
Pool of relationships



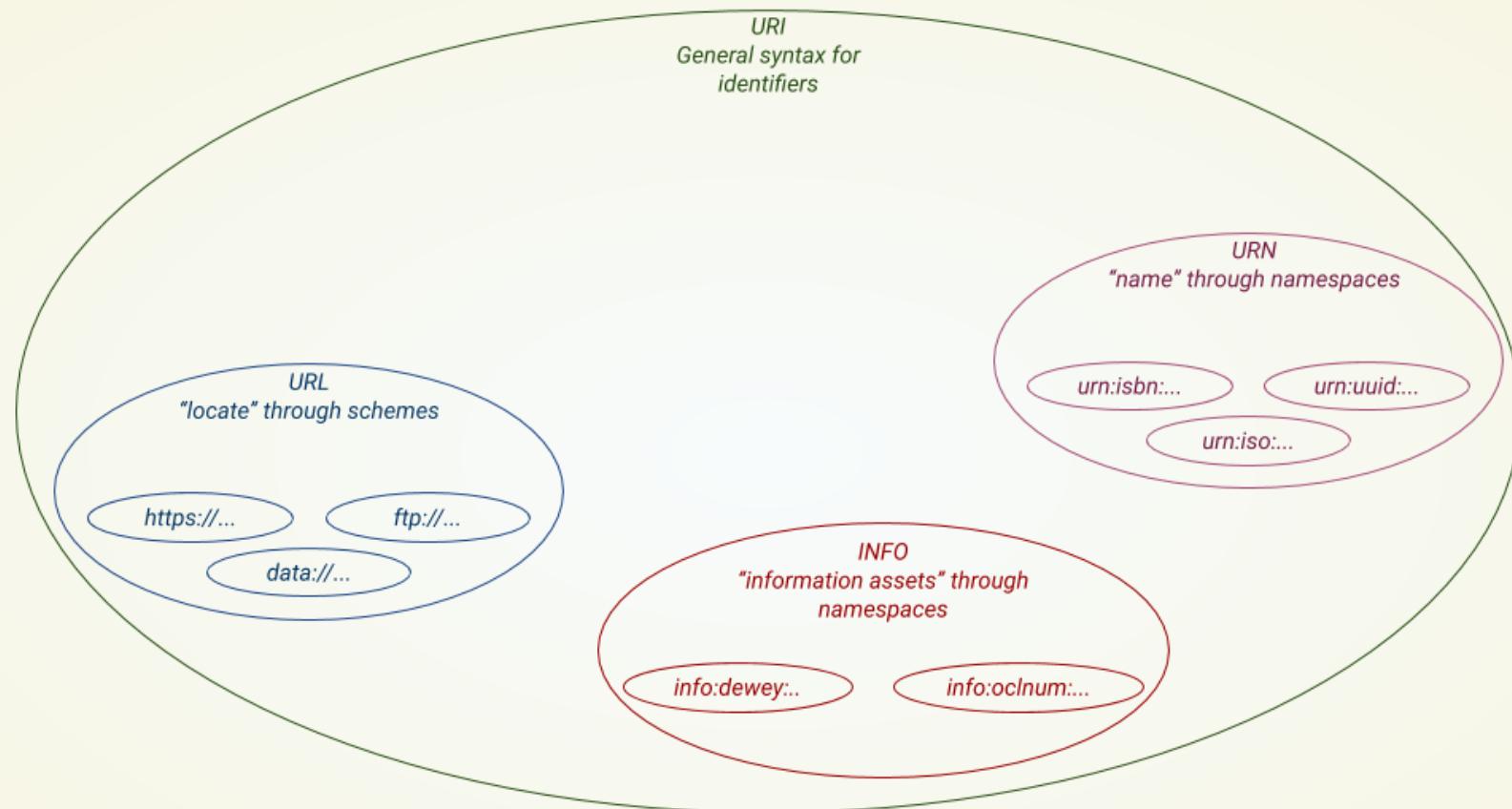
- No need for a complex and centralized key management system
- Both “A” and “B” may remain anonymous

Technical dive in to DIDs

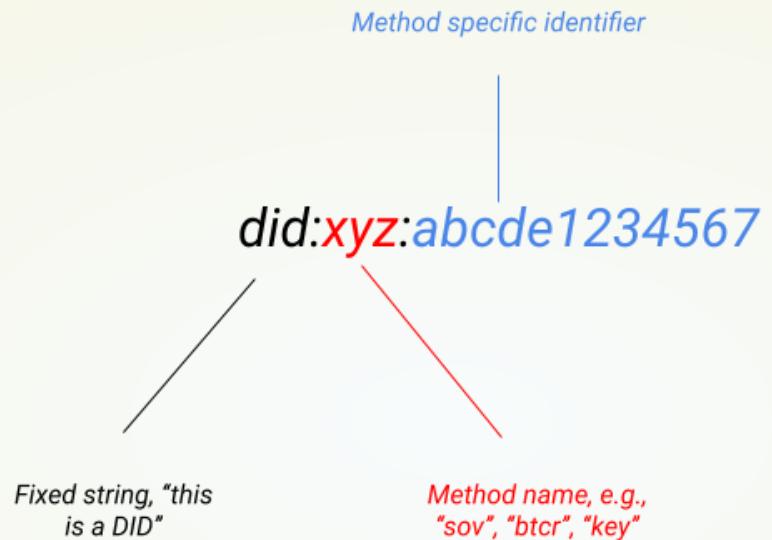
Anatomy of DIDs



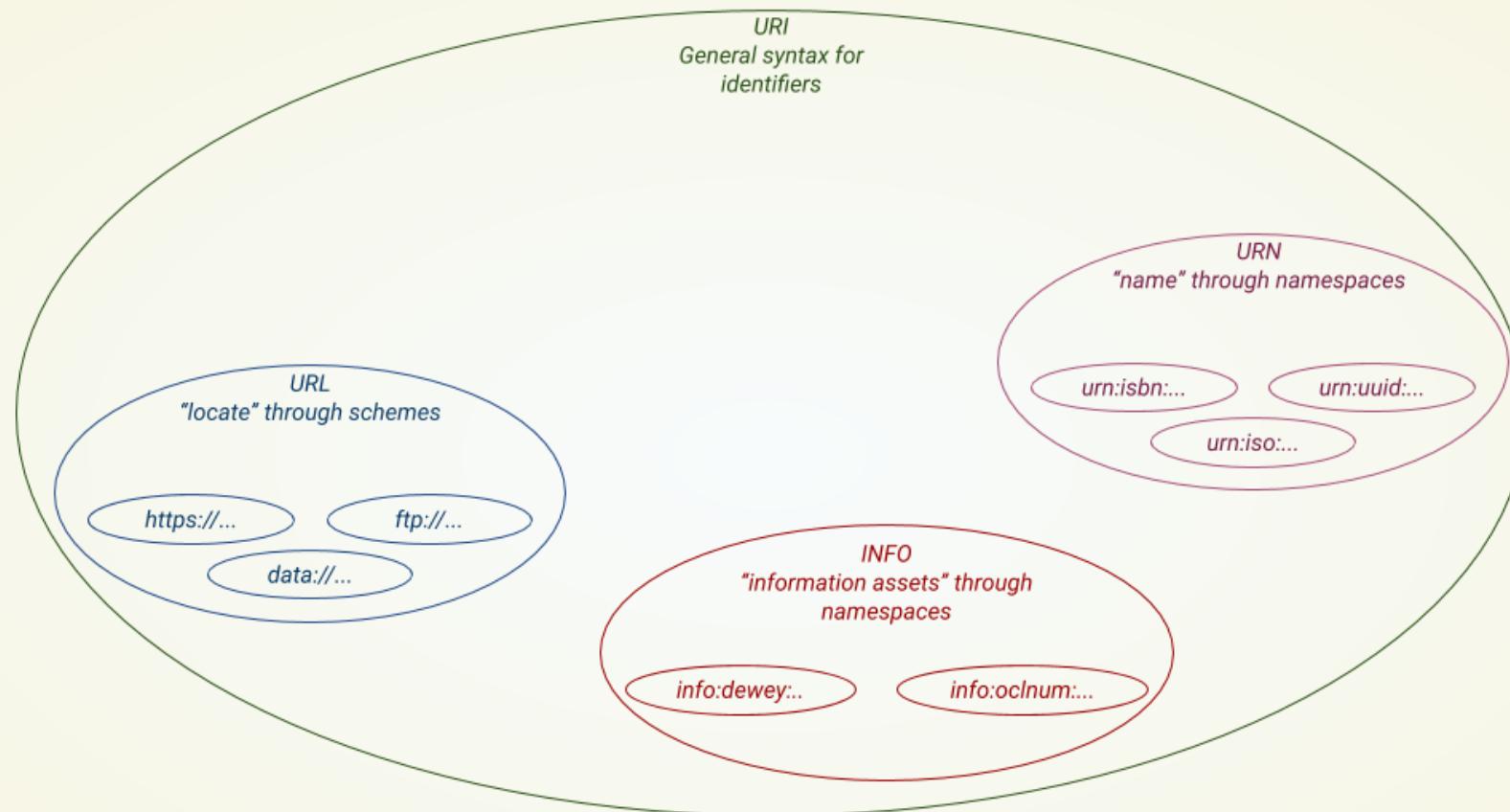
Reminder: URIs, URNs, URLs, ...



DID is a new type of URI



DID is a new type of URI



Why is it important that it is a URI

- DID are within the IETF/W3C world
 - tools, libraries may be used to manage them
 - existing specifications automatically apply to DIDs:
 - "abcd" is valid HTML
 - "<did:btcr:xyv2-xzpq-q9wa-p7t> a rdf:Class." is a valid RDF Turtle statement
- *DIDs are part of the Web*

Examples for ledger based DIDs

- `did:btcr:xyv2-xzpq-q9wa-p7t`
 - built “on top” of the Bitcoin blockchain
 - the method specific identifier is generated from the bitcoin transaction position reference
- `did:sov:mnjk198uipsndg2hdjdjf7`
 - based on a dedicated distributed ledger (Sovrin)
 - the method specific identifier generated from either a simple UUID or the subject’s public keys

Ledger based DIDs

- There are other methods based on generic (e.g., Ethereum), or dedicated (e.g., Veres One) ledgers
- They are generally meant to be general solutions for identity, usable by various applications

Examples for special purpose methods

- **did:key:z6Mki7KaCeTufKQ6...NEv28PhP1PHF35btNN**
 - can be used for single, ephemeral interactions (e.g., IoT)
 - the method specific identifier is an encoded public cryptographic key
 - the DID documents aren't stored; they are generated on demand
- **did:peer:1zQmZMygzYqNwU6Uhmewx...LSwwgf2aiKZuwa**
 - interaction among a fixed number of “peers”, e.g., business relationships
 - the method specific identifier is generated from the DID document
 - the document stores the user's public key(s)
 - all participants have access to the DID documents
 - information in the DID documents are used to exchange encrypted messages among peers

Methods in general

- Lots of experimentation is happening, exploring different methods
 - there is also a need to develop proper user interfaces, applications, etc, to store DIDs in personal wallets, for example
- We can expect to see a convergence of methods to only a few in the coming years

Anatomy of DID Documents

Abstract model of a DID document

- Uniquely related to the DID *subject*, i.e., the entity identified by the DID
- Includes a separate DID for the *controller*
 - identifies an entity that “in charge” of the DID document
- Expresses public cryptographic keys and other verification methods
- May include a separate “proof” section (typically a signature)
- May be extended to include application specific information

DID Document syntaxes

- The specification defines JSON, JSON-LD, and CBOR syntaxes
- The information can be converted from one syntax to the other in a lossless way
 - this means that, for example, only a subset of CBOR is used

Typical DID document structure

```
{  
  "id": "did:example:abcdefgh",  
  "controller": "did:example:xyzwvy",  
  "publicKey": [{ ... }],  
  "authentication": [{ ... }],  
  "proof": [{ ... }],  
  "service": [{ ... }]  
}
```

Public Keys

- List of various public keys
- Their usage is not specified: can be used for DID verification but also for any other application

```
{  
  "publicKey": [ {  
    "id": "keys-1",  
    "type": "RsaVerificationKey2018",  
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"  
  }, {  
    "id": "keys-2",  
    "type": "Secp256k1VerificationKey2018",  
    "publicKeyHex": "02b97c30de767f084ce30...16a3263d29f1450936b71"  
  } ]  
}
```

Authentication

- Keys that can be used for the *authentication* of the controller:
 - can refer to a key listed separately in publicKey
 - can include a full key that can be used for authentication only

```
{  
  "authentication": [  
    "#keys-1",  
    {  
      "id": "#keys-3",  
      "type": "Ed25519VerificationKey2018",  
      "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"  
    }]  
}
```

Proof

- A cryptographic proof of the integrity of the document

```
{  
  "proof": {  
    "type": "LinkedDataSignature2015",  
    "created": "2020-01-16T17:29:20Z",  
    "creator": "did:example:12345#keys-1",  
    "signatureValue": "QNB13Y7Q9...1tzjn4w=="  
  }  
}
```

Documents to read

Use cases and requirements

<https://www.w3.org/TR/did-use-cases/>

Core spec

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

These slides

<https://iherman.github.io/did-talks/talks/2020-evangelists/>

Some more documents to come

Registry

Registry for various terms: crypto terms, methods, additional terms,...

Rubric

Documenting what criteria to look for when choosing a specific method

Implementation guide

Today's Status

- Draft specification was developed in a W3C CG
- Working Group started in September 2019
- Plan is to be technically ready (i.e., Candidate Recommendation) by summer 2020
- Recommendation should be available by summer 2021

Thank you for your
attention!

ivan@w3.org