Current State of DIDs

Markus Sabadello
Danube Tech, Decentralized Identity Foundation, Sovrin Foundation, W3C CCG, OASIS XDI TC

https://danubetech.com/

TIIME – Vienna, 18th February 2019
URNs (Uniform Resource Names, RFC 8141)

Scheme

urn:uuid:fe0cde11-59d2-4621-887f-23013499f905

Namespace

Namespace Specific String

DIDs

Scheme

did:example:123456789abcdefghijk

DID Method

DID Method Specific String

This presentation is released under a Creative Commons license. (CC BY-SA 4.0).
The four core properties of a DID

1. A permanent (persistent) identifier
   It never needs to change

2. A resolvable identifier
   You can look it up to discover metadata

3. A cryptographically-verifiable identifier
   You can prove control using cryptography

4. A decentralized identifier
   No centralized registration authority is required
A DID Method...  

Defines how to perform the **four CRUD operations** on a DID  

1. **Create**: How to generate a new DID  
2. **Read**: How to resolve a DID into a DID document  
3. **Update**: How to write a new version of a DID document  
4. **De-activate**: How to revoke (terminate) a DID so it no longer functions
A DID Document...

Contains metadata for describing and interacting with the DID subject (the entity identified by the DID)

1. **Public keys** or other cryptographic proof material
2. **Service endpoints** for engaging in trusted interactions
3. **Authentication mechanisms** for proving control of the DID
4. **Other metadata**
DID Resolution...

Is the process of using the DID to look up and retrieve a copy of the DID document

- How this is done depends on the DID method
  - Defined by the Read operation
- Different DID methods do this in different ways
- **DID Resolution** is a separate specification
  - **Not in scope** for the W3C DID Working Group
# Comparing DIDs with Domain Names

<table>
<thead>
<tr>
<th><strong>Decentralized Identifiers (DIDs)</strong></th>
<th><strong>Domain Names</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Globally unique</td>
<td>Globally unique</td>
</tr>
<tr>
<td>Persistent</td>
<td>Reassignable</td>
</tr>
<tr>
<td>Machine-friendly identifiers (i.e., long character strings based on random numbers / cryptography)</td>
<td>Human-readable names</td>
</tr>
<tr>
<td>Resolvable using different mechanisms defined by the applicable DID method</td>
<td>Resolvable using the standard DNS protocol</td>
</tr>
<tr>
<td>Associated data is expressed in DID documents</td>
<td>Associated data is expressed in DNS zone files</td>
</tr>
<tr>
<td>Fully decentralized namespaces without delegation</td>
<td>Hierarchical, delegatable namespaces based on centralized root registries for top-level domain names (TLDs)</td>
</tr>
<tr>
<td>Cryptographically-verifiable</td>
<td>Verifiable using DNS security extensions (DNSSEC)</td>
</tr>
<tr>
<td>Fully under the control of the DID controller</td>
<td>Ultimately controlled by ICANN and the registry operator for each DNS TLD</td>
</tr>
</tbody>
</table>

Released under a Creative Commons license. ([CC BY-SA 4.0](https://creativecommons.org/licenses/by-sa/4.0/)).
Comparison with other persistent identifiers
- DID Auth
- OIDC SIOP
- Verifiable Credentials
- DIDComm
- Agents
- Identity Hubs
- Encrypted Data Vaults
- ...

Trust over IP Technology Stack

Trust over IP Governance Stack

<table>
<thead>
<tr>
<th>Metasystem Governance Frameworks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance Authority</td>
</tr>
<tr>
<td>Auditor</td>
</tr>
<tr>
<td>Auditor Accredor</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Credential Governance Frameworks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust Anchor</td>
</tr>
<tr>
<td>Credential Registry</td>
</tr>
<tr>
<td>Insurer</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Provider Governance Frameworks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Developer</td>
</tr>
<tr>
<td>Software Developer</td>
</tr>
<tr>
<td>Agency</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Governance Frameworks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transaction Author</td>
</tr>
<tr>
<td>Transaction Endorser</td>
</tr>
<tr>
<td>Steward</td>
</tr>
</tbody>
</table>
Amsterdam F2F Topics

- Major technical topics:
  - DID Document representations
  - Extensibility and interoperability
  - Metadata
  - Matrix parameters

- Additional topics:
  - Security, IoT, spec structure, rubric, use cases
  - Overlap with DID Resolution
Thank you

Markus Sabadello
Danube Tech
https://danubetech.com/
markus@danubetech.com

W3C DID WG:
https://www.w3.org/2019/did-wg/