Eine Einführung: Dezentrale digitale Identitäten (DIDs)

Markus Sabadello

Danube Tech, Decentralized Identity Foundation,
W3C DID WG, Sovrin Foundation, IDunion SCE

https://danubetech.com/

Digital Society Conference, Berlin

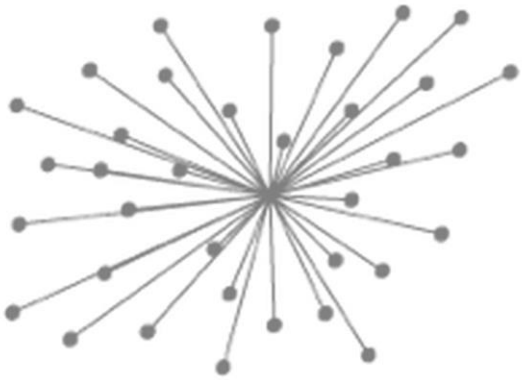
7. Dezember 2023

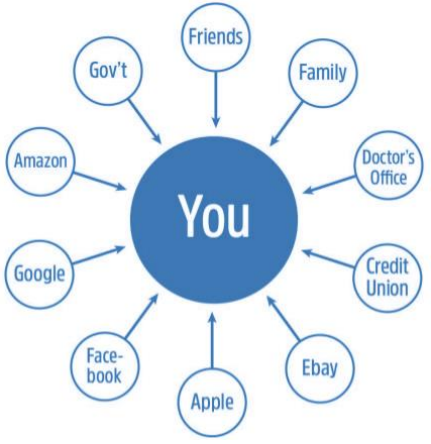
Digital Society Conference
BERLIN 07.-08.12
#Education #Work #Research

DIF

DANUBE TECH GMBH

Dezentrale digitale Identitäten (DIDs) / Self-Sovereign Identity (SSI)

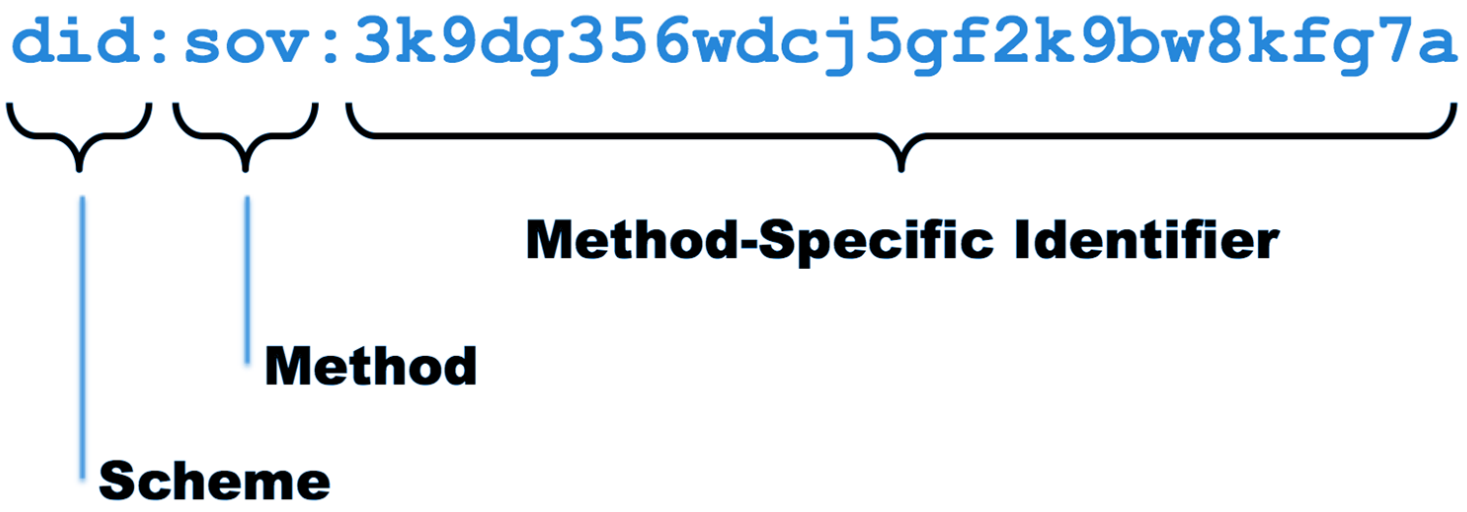




DANUBE TECH GMBH

Decentralized Identifiers (DIDs)

- Self-sovereign identifiers for individuals, organizations, things.
- Decentralized, persistent, cryptographically verifiable, resolvable identifiers.
- Created using blockchain or other decentralized technology.
- Created and managed by identity controller via wallet application.



Syntax and Examples

```
did                = "did:" method-name ":" method-specific-id
method-name        = 1*method-char
method-char        = %x61-7A / DIGIT
method-specific-id = *( *idchar ":" ) 1*idchar
idchar             = ALPHA / DIGIT / "." / "-" / "_" / pct-encoded
pct-encoded        = "%" HEXDIG HEXDIG
```

- did:web:danubetech.com
- did:key:z6MkpTHR8VNsBxYAAWHut2Geadd9jSwuBV8xRoAnwWsdvktH
- did:ion:test:EiAvfKgnZHI-L2UZwx0bzq-IXmp_9rFO6uWFwjH1q_9-zg
- did:indy:idunion:test:H5KH5fSyDRRQ8ZCxB4Qpge
- did:ebsi:zkyJ5CdJJ8GePR6gVh964jx
- did:ethr:goerli:0x03631317a405f68a2b36759553314e1d51e96c88f51ab2aca6663428dc99d7c879
- did:cheqd:testnet:ae129a39-cd24-4be7-888c-634728ab85cc
- did:btco:bwtowpglzpd
- did:web:did-web.dev.godiddy.com:21271ffa-8b50-4474-8c40-be12fcd2121c

DID Resolution

- Enables “trustable” interactions
- DID Resolution: DID → DID Document
  - Identifier
  - Set of verification methods
  - Set of service endpoints
  - Verification relationships (authentication, assertions, encryption, etc.)
- Various metadata about the DID document and resolution process

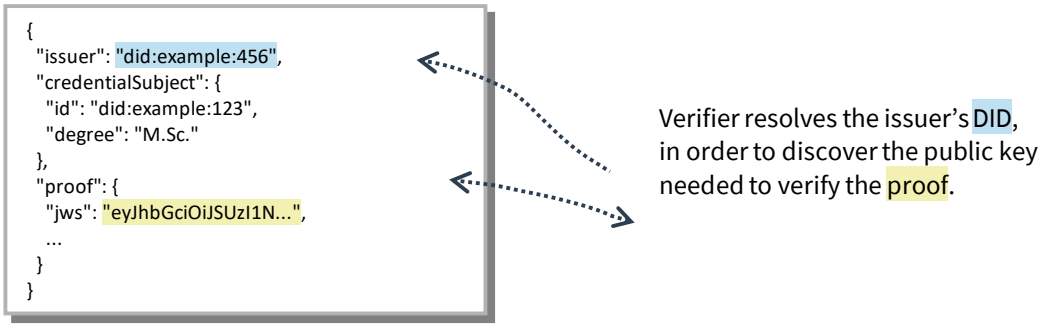
- Example DID Document:

```
{
 "@context": "https://www.w3.org/ns/did/v1",
 "id": "did:ebsi:z25ZZFS7FweHsm9MX2Qvc6gc",
 "verificationMethod": [
  {
   "id": "did:ebsi:z25ZZFS7FweHsm9MX2Qvc6gc#key-1",
   "type": "Ed25519VerificationKey2018",
   "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDmqPV"
  }
 ],
 "service": {
  "type": "DecentralizedWebNode",
  "serviceEndpoint":
  "https://azure.microsoft.com/hub/z25ZZFS7FweHsm9MX2Qvc6gc"
 },
 "authentication": [
  "did:ebsi:z25ZZFS7FweHsm9MX2Qvc6gc#key-1"
 ]
}
```

DANUBE TECH GMBH

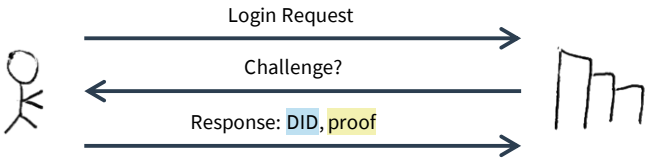
When are DIDs used?

① Verifiable Credentials



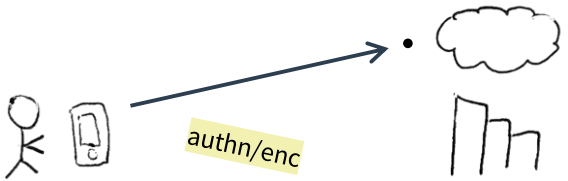
Verifier resolves the issuer's DID,
in order to discover the public key
needed to verify the proof.

② DID Auth



Relying party resolves the user's DID,
in order to discover the public key
needed to verify the proof.

③ Service Discovery



Application resolves a DID,
in order to discover a service for
Interacting via a secure channel.

DANUBE TECH GMBH

Verifiable Credentials

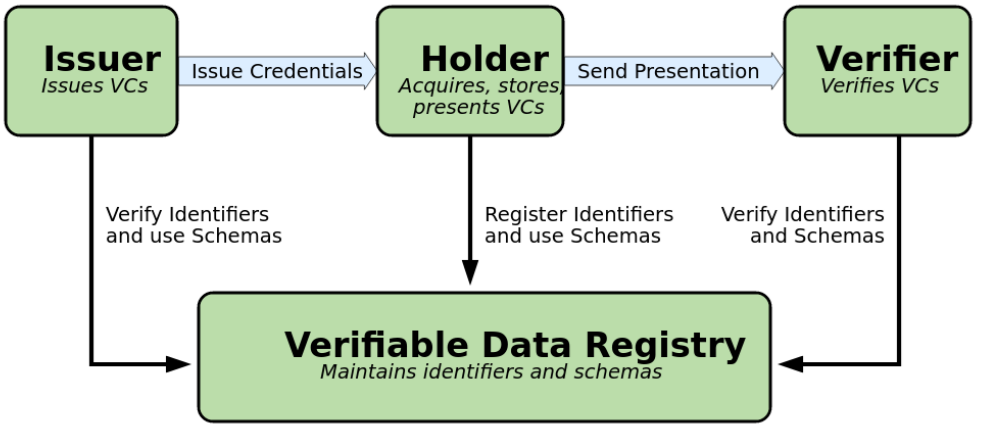
- Example:


```
{
  "@context": [ "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1" ],
  "id": "http://example.edu/credentials/1872",
  "type": ["VerifiableCredential", "NameCredential"],
  "issuer": "did:indy:sovrin:WRfXPg8dantKVubE3HX8pw",
  "issuanceDate": "2010-01-01T19:23:24Z",
  "credentialSubject": {
    "id": "did:btcr:x6lj-wzvr-qqrv-m80w",
    "name": "Markus Sabadello",
    "address": "..."
  },
  "proof": {
    "type": "Ed25519Signature2020",
    "created": "2021-11-13T18:19:39Z",
    "verificationMethod": "did:indy:sovrin:WRfXPg8dantKVubE3HX8pw#key-1",
    "proofPurpose": "assertionMethod",
    "proofValue": "z58DAdFfa9SkqZMVPxAQpic7ndSayn1PzZs6ZjWp1CktyGesjuTSwRdo
            WhAfGFCF5bppETSTojQCrfFPP2oumHKtz"
  }
}
```


Verifiable Credentials Data Model v1.1

W3C Recommendation 03 March 2022

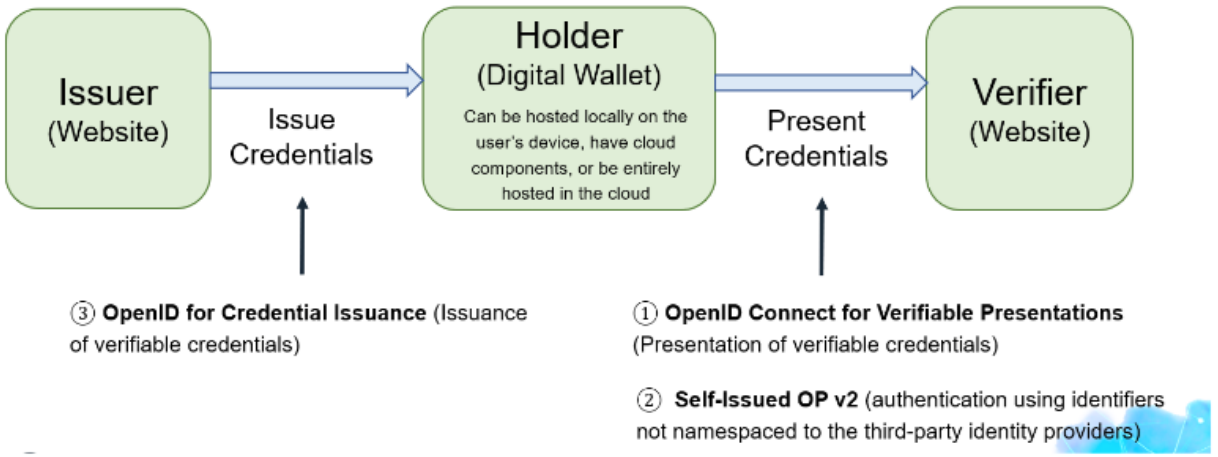
▸ **More details about this document**



DID Auth / OpenID 4 VC

- Prove control of a DID using a cryptographic challenge/response protocol.
- Different architectures and scenarios, e.g. implemented in OIDC 4 VC or DIDComm.

https://openid.net/openid4vc/



Introduction to DID Auth

A White Paper from Rebooting the Web of Trust VI

Markus Sabadello, Kyle Den Hartog, Christian Lundkvist, Cedric Franz, Alberto Elias, Andrew Hughes, John Jordan, and Dmitri Zagidulin

“Wer bin ich?”

“Wer bis du?”

“Ich bin ich!”

Danke

- **Danube Tech GmbH**
- https://danubetech.com/
- markus@danubetech.com