Decentralized Identifiers and the Eclipse Dataspace Connector

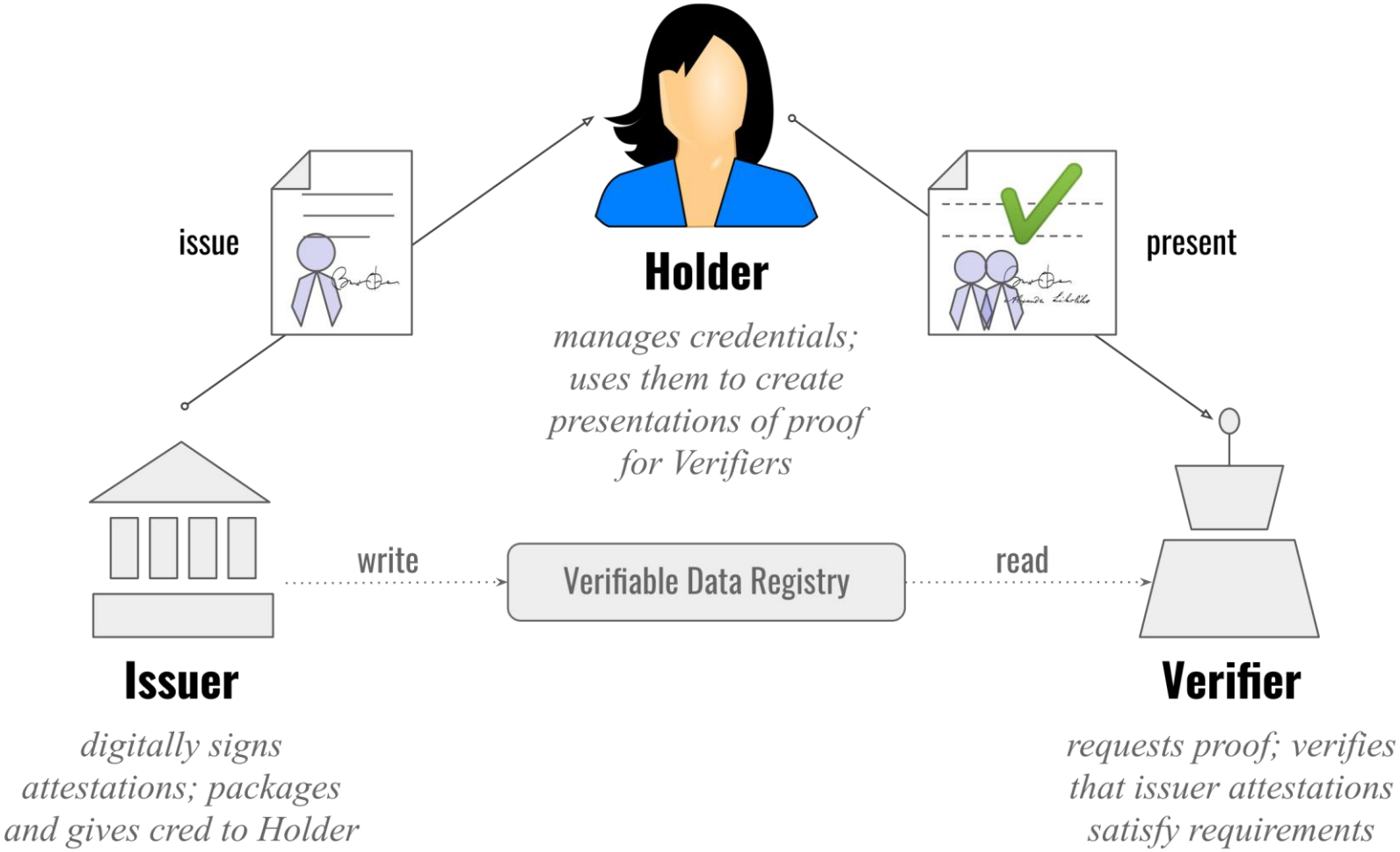
Stefan van der Wiele
Senior Program Manager
Microsoft Identity Division
@wiele

Quick overview

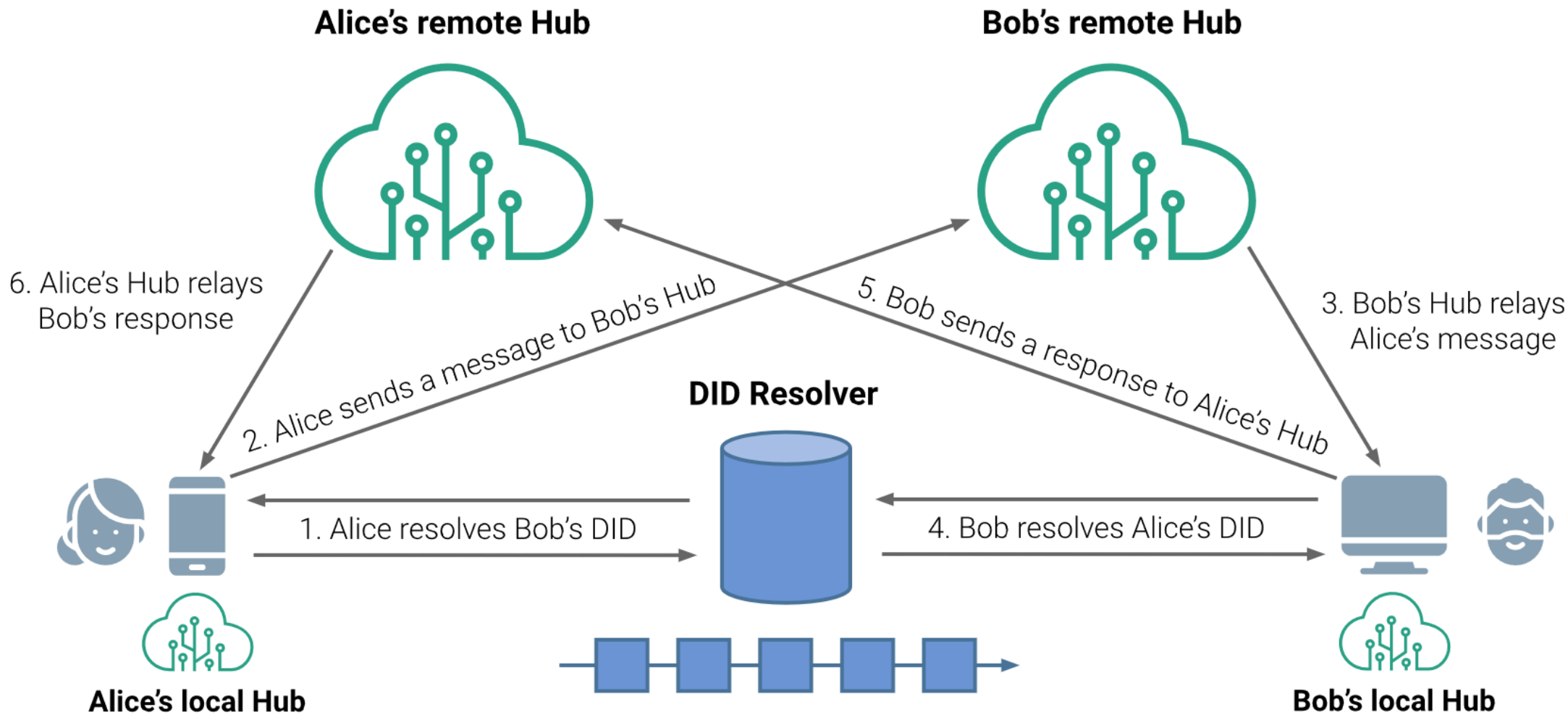
What is a Verifiable Credential, Decentralized Identifier?

What is an Identity Hub?

W3C Verifiable Credentials



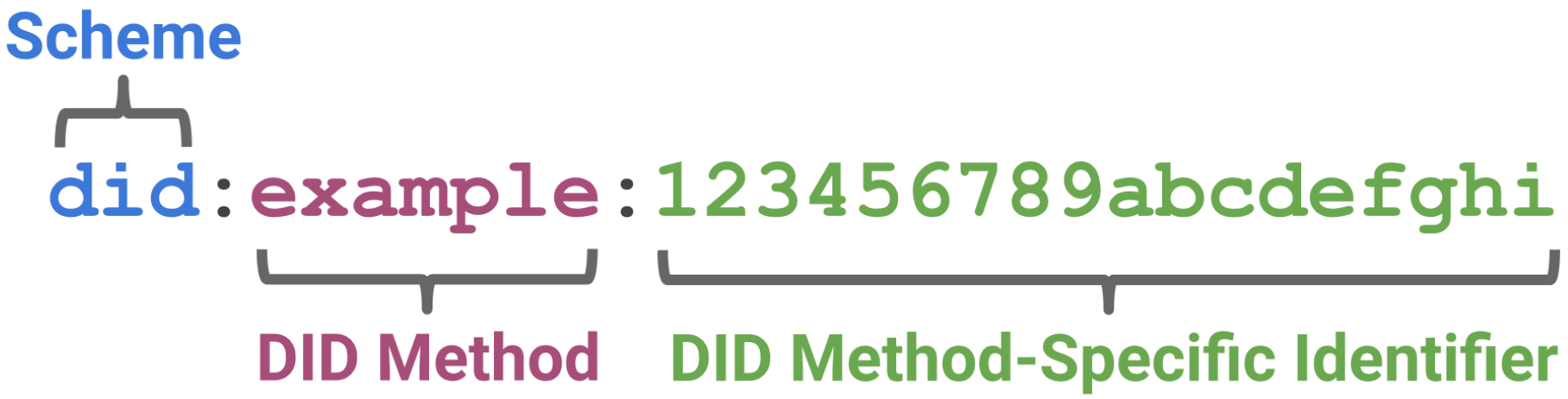
Identity Hub



Decentralized Identifiers

1. **DID** (for self-description)
2. **Set of public keys** (for verification)
3. **Set of auth methods** (for authentication)
4. **Set of service endpoints** (for interaction)
5. **Timestamp** (for audit history)
6. **Signature** (for integrity)

Decentralized Identifiers



Decentralized Identifiers – Document Example


```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ]
  "id": "did:example:123456789abcdefghi",
  "authentication": [{

    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2020",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }]
}
```

Scheme

did:example:123456789abcdefghi

DID Method

DID Method-Specific Identifier

1. Locate DID document

2. Read DID document

1. **DID** (for self-description)
2. **Set of public keys** (for verification)
3. **Set of auth methods** (for authentication)
4. **Set of service endpoints** (for interaction)
5. **Timestamp** (for audit history)
6. **Signature** (for integrity)

Distributed infrastructure

3. Verify VC signature

Verifiable Credential

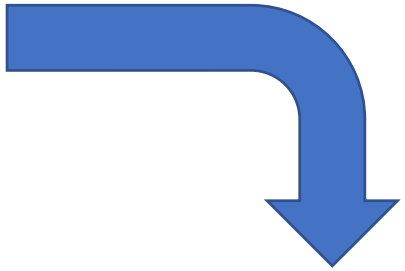
What is did:web?

A new DID method that allows participants to bootstrap trust using a web domain's existing reputation.

{ "@context": "https://www.w3.org/ns/did/v1", "id": "did:web:example.com", "verificationMethod": [{ "id": "did:web:example.com#owner", "type": "Secp256k1VerificationKey2018", "owner": "did:web:example.com", "ethereumAddress": "0xb9c5714089478a327f09197987f16f9e5d936e8a" }], "authentication": ["did:web:example.com#owner"] }

[did:web Method Specification (w3c-ccg.github.io)]

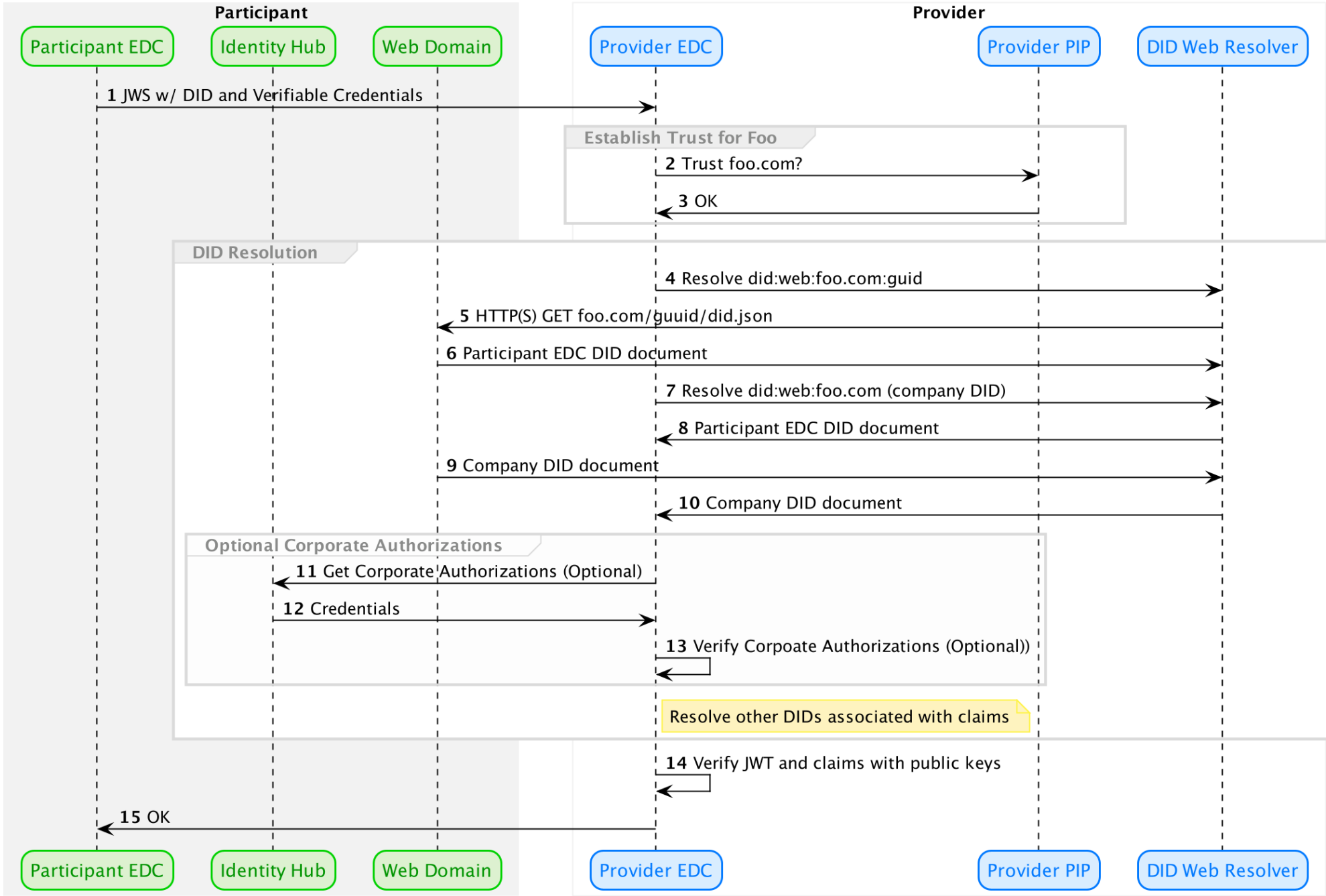
did:web:example.com



https://example.com/.well-known/did.json

EXAMPLE 1: Example did:web DID document

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:web:example.com",
  "verificationMethod": [{
     "id": "did:web:example.com#owner",
     "type": "Secp256k1VerificationKey2018",
     "owner": "did:web:example.com",
     "ethereumAddress": "0xb9c5714089478a327f09197987f16f9e5d936e8a"
  }],
  "authentication": [
     "did:web:example.com#owner"
  ]
}
```


Participant
Provider
Participant EDC
Identity Hub
Web Domain
Provider EDC
Provider PIP
DID Web Resolver
1 JWS w/ DID and Verifiable Credentials
Establish Trust for Foo
2 Trust foo.com?
3 OK
DID Resolution
4 Resolve did:web:foo.com:guid
5 HTTP(S) GET foo.com/guuid/did.json
6 Participant EDC DID document
7 Resolve did:web:foo.com (company DID)
8 Participant EDC DID document
9 Company DID document
10 Company DID document
Optional Corporate Authorizations
11 Get Corporate Authorizations (Optional)
12 Credentials
13 Verify Corpoate Authorizations (Optional))
Resolve other DIDs associated with claims
14 Verify JWT and claims with public keys
15 OK
Participant EDC
Identity Hub
Web Domain
Provider EDC
Provider PIP
DID Web Resolver

Considerations

- DNS Security
  - DNS Over HTTPS
- Optional Path and DID control?

This example:

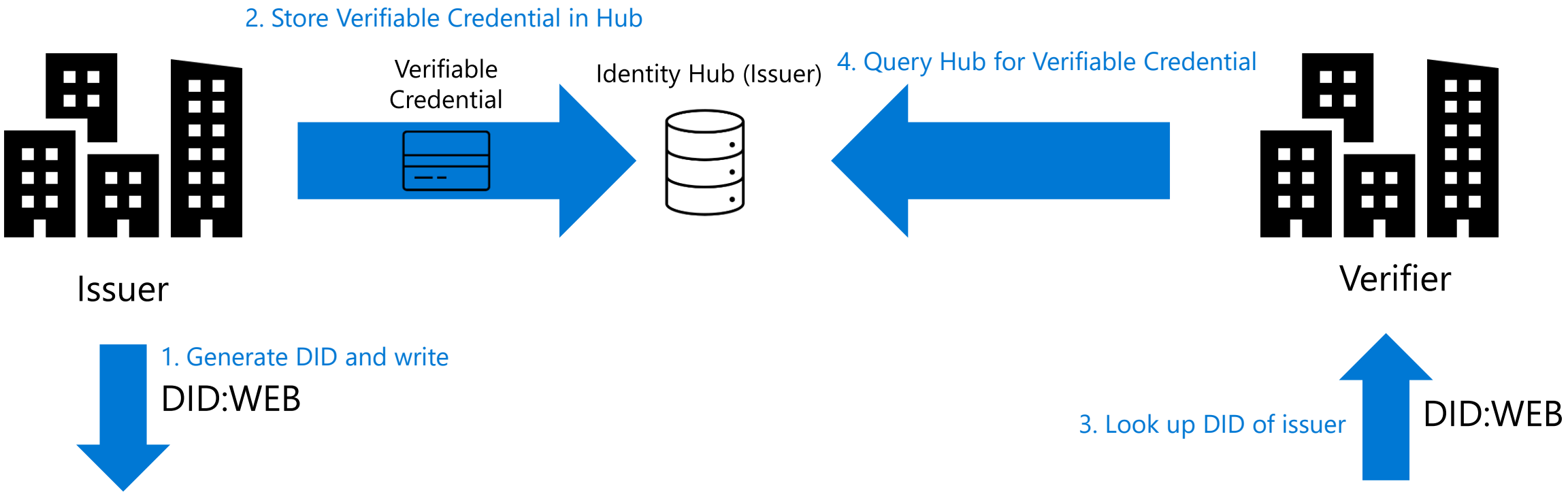
`did:web:example.com:u:bob`

resolves to the DID document at:

`https://example.com/u/bob/did.json`

In this scenario, it is probable that example.com has given user Bob control over the DID in question, and proofs of control refer to Bob rather than all of example.com.

Putting it all together: Using identity hub



"id": "did:example:123456789abcdefghi",
"authentication": [{

"id": "did:example:123456789abcdefghi#keys-1",
"type": "Ed25519VerificationKey2020",

Distributed infrastructure

Resources

- DID-Web
  - did:web Method Specification (w3c-ccg.github.io)
- W3C Verifiable Credentials
  - Verifiable Credentials Data Model 1.0 (w3.org)
- DIF Identity Hub
  - DIF Identity Hub