Decentralized Identity for true Digital Sovereignty

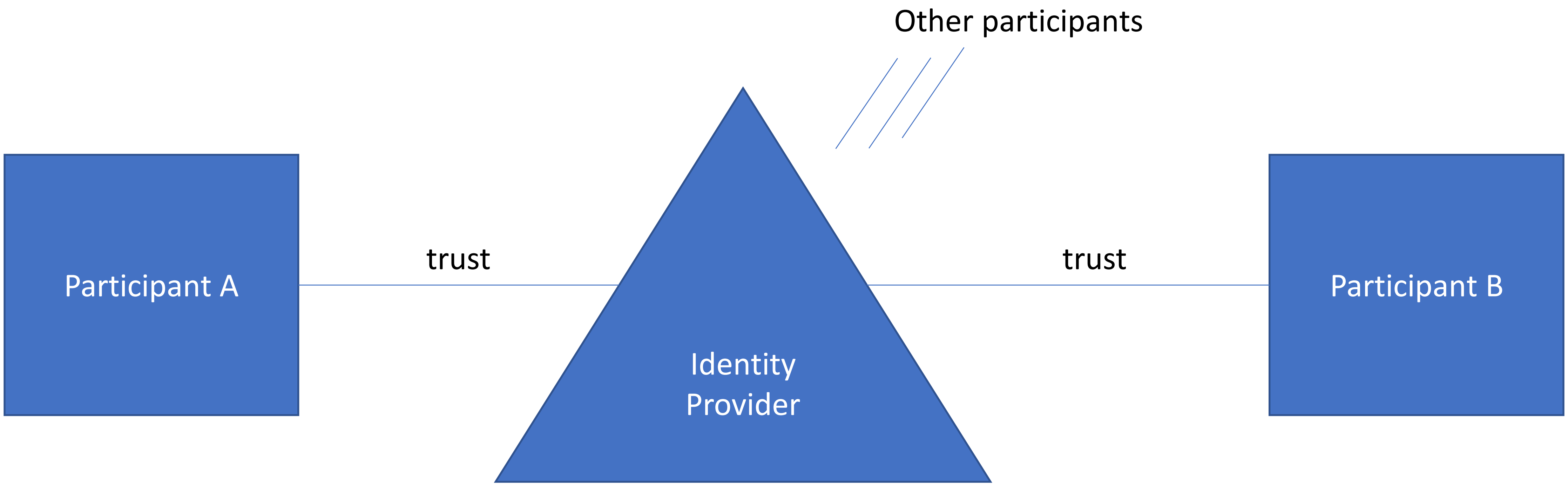
Stefan van der Wiele

Senior Program Manager

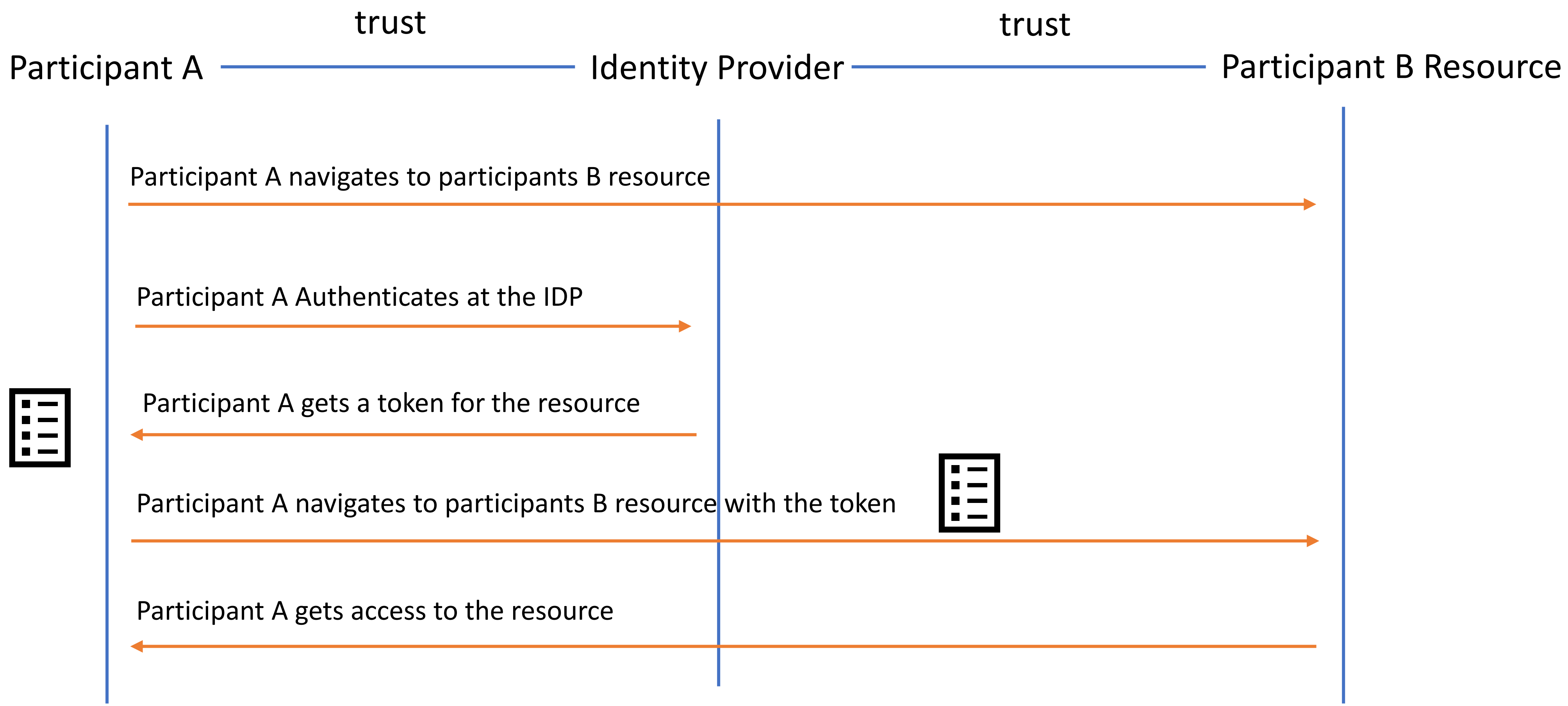
Microsoft identity and network access division

@wiele

Centralized vs. Decentralized



Examples: OpenIDConnect, SAML, WS-Fed



Participant A — trust — Identity Provider — trust — Participant B Resource

Participant A navigates to participants B resource

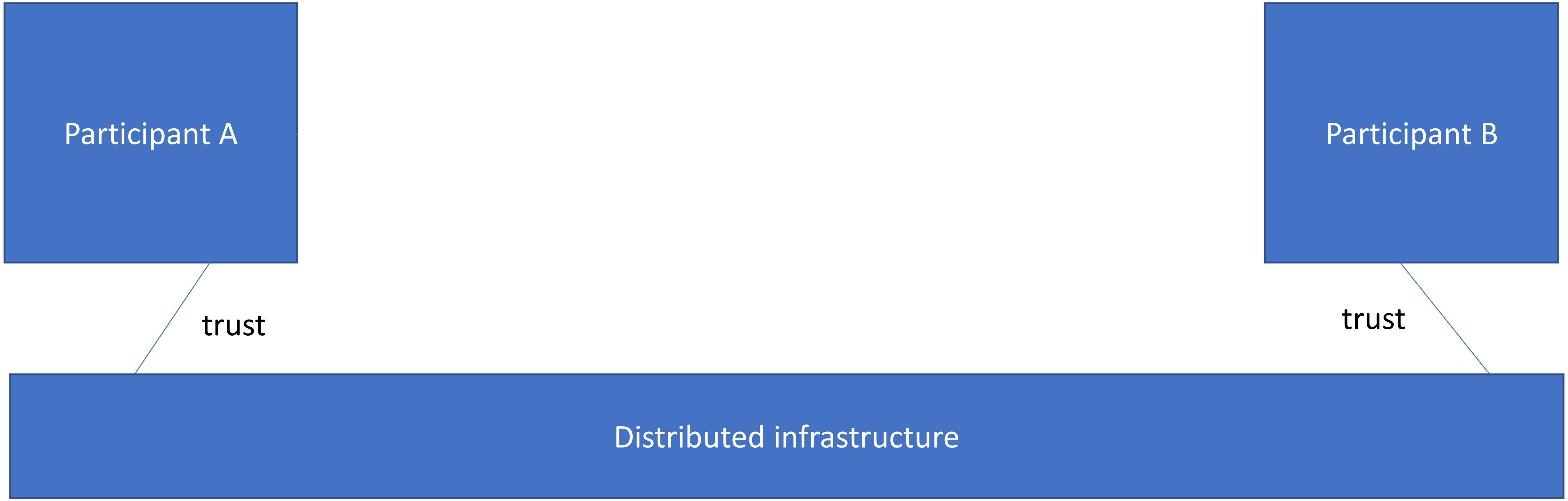
Participant A Authenticates at the IDP

Participant A gets a token for the resource

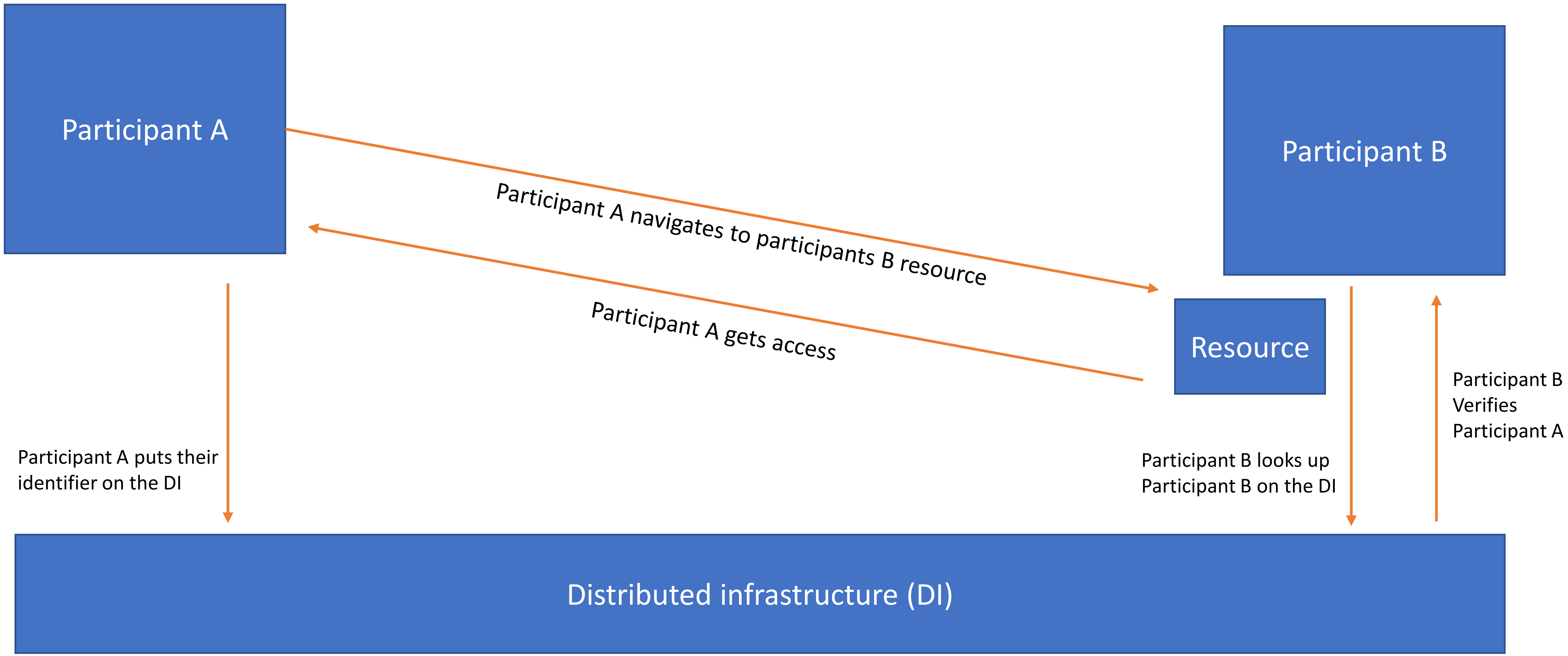
Participant A navigates to participants B resource with the token

Participant A gets access to the resource

Centralized vs. Decentralized



Centralized vs. Decentralized



Participant A

Participant B

Participant A navigates to participants B resource

Participant A gets access

Resource

Participant A puts their identifier on the DI

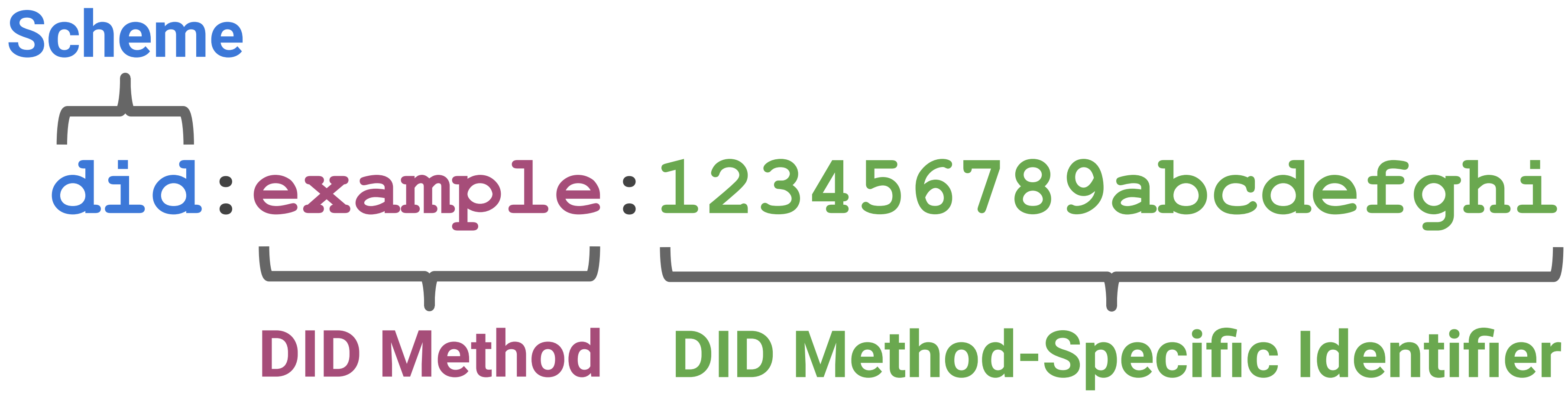
Participant B looks up Participant B on the DI

Participant B Verifies Participant A

Distributed infrastructure (DI)

BLOCKCHAIN HOTEL
Schallplattenbörse
Essen

Decentralized Identifiers



Scheme

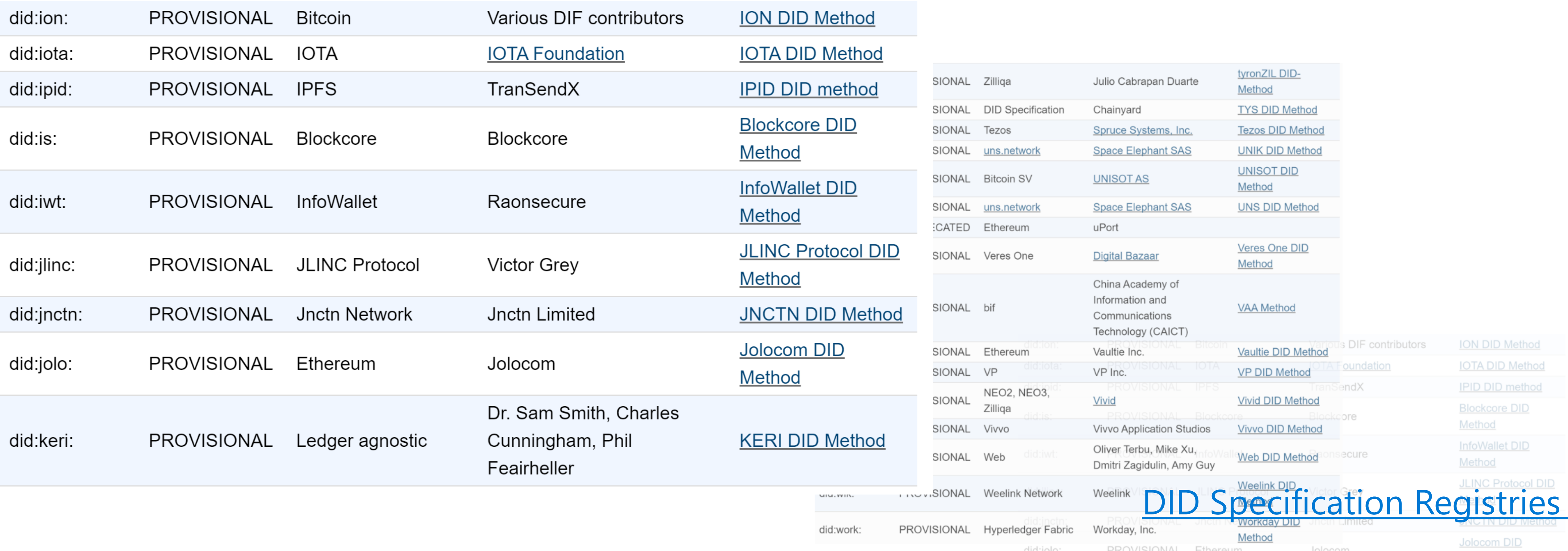
did:example:123456789abcdefghi

DID Method

DID Method-Specific Identifier

Decentralized Identifiers Methods

- Over 80 different methods
- Defines the trusted infrastructure
- How to read and write identifiers to the infrastructure

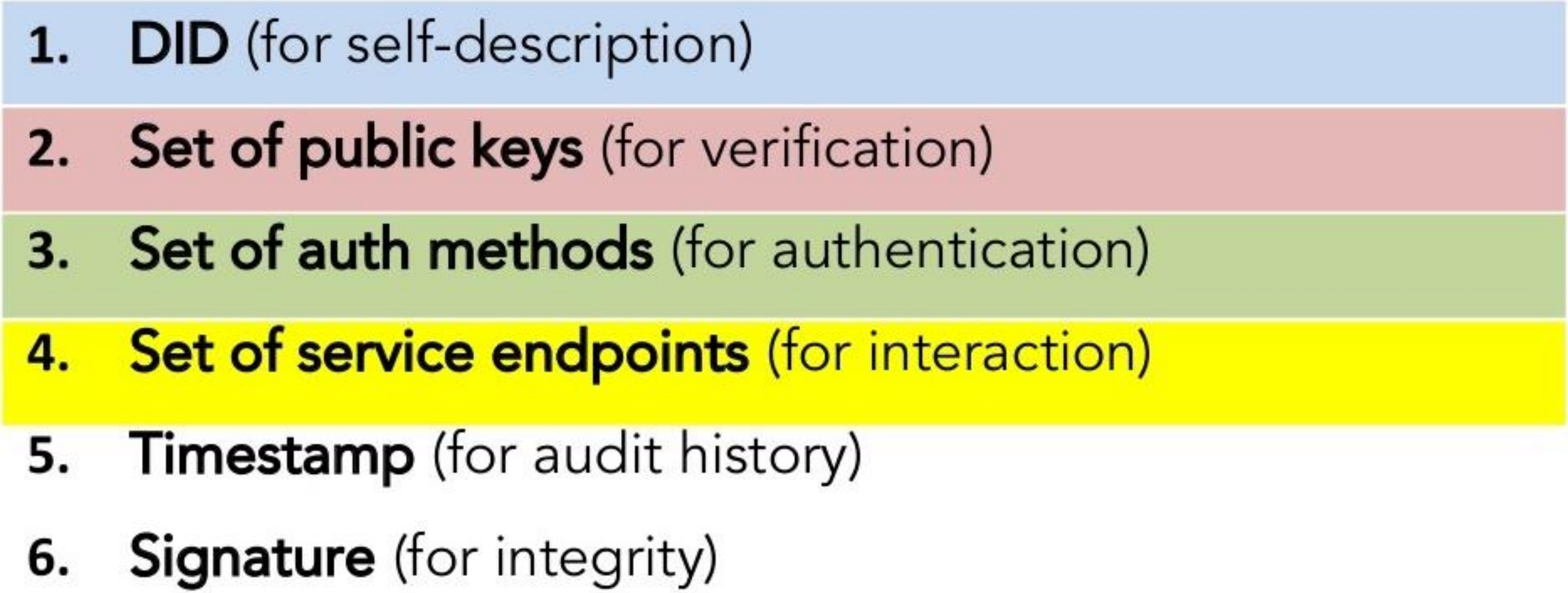


did:ion:	PROVISIONAL	Bitcoin	Various DIF contributors	ION DID Method
did:iota:	PROVISIONAL	IOTA	IOTA Foundation	IOTA DID Method
did:ipid:	PROVISIONAL	IPFS	TranSendX	IPID DID method
did:is:	PROVISIONAL	Blockcore	Blockcore	Blockcore DID Method
did:iwt:	PROVISIONAL	InfoWallet	Raonsecure	InfoWallet DID Method
did:jlinc:	PROVISIONAL	JLINC Protocol	Victor Grey	JLINC Protocol DID Method
did:jnctn:	PROVISIONAL	Jnctn Network	Jnctn Limited	JNCTN DID Method
did:jolo:	PROVISIONAL	Ethereum	Jolocom	Jolocom DID Method
did:keri:	PROVISIONAL	Ledger agnostic	Dr. Sam Smith, Charles Cunningham, Phil Feairheller	KERI DID Method

	SIONAL	Zilliqa	Julio Cabrapan Duarte	tyronZIL DID-Method
	SIONAL	DID Specification	Chainyard	TYS DID Method
	SIONAL	Tezos	Spruce Systems, Inc.	Tezos DID Method
	SIONAL	uns.network	Space Elephant SAS	UNIK DID Method
	SIONAL	Bitcoin SV	UNISOT AS	UNISOT DID Method
	SIONAL	uns.network	Space Elephant SAS	UNS DID Method
	ECATED	Ethereum	uPort	
	SIONAL	Veres One	Digital Bazaar	Veres One DID Method
	SIONAL	bif	China Academy of Information and Communications Technology (CAICT)	VAA Method
	SIONAL	Ethereum	Vaultie Inc.	Vaultie DID Method
	SIONAL	VP	VP Inc.	VP DID Method
	SIONAL	NEO2, NEO3, Zilliqa	Vivid	Vivid DID Method
	SIONAL	Vivvo	Vivvo Application Studios	Vivvo DID Method
	SIONAL	Web	Oliver Terbu, Mike Xu, Dmitri Zagidulin, Amy Guy	Web DID Method
did:wik:	PROVISIONAL	Weelink Network	Weelink	Weelink DID Method
did:work:	PROVISIONAL	Hyperledger Fabric	Workday, Inc.	Workday DID Method

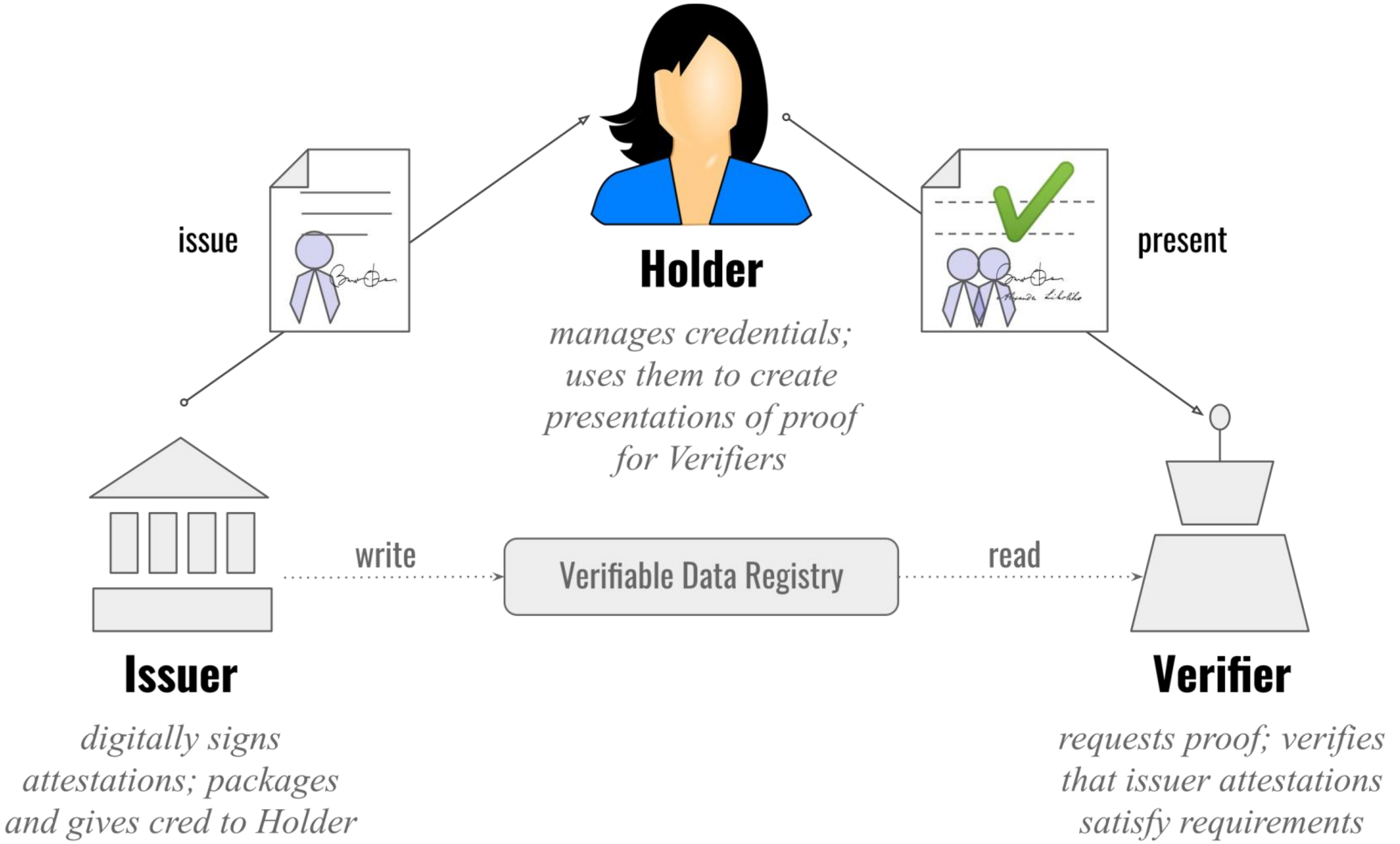
DID Specification Registries (w3.org)

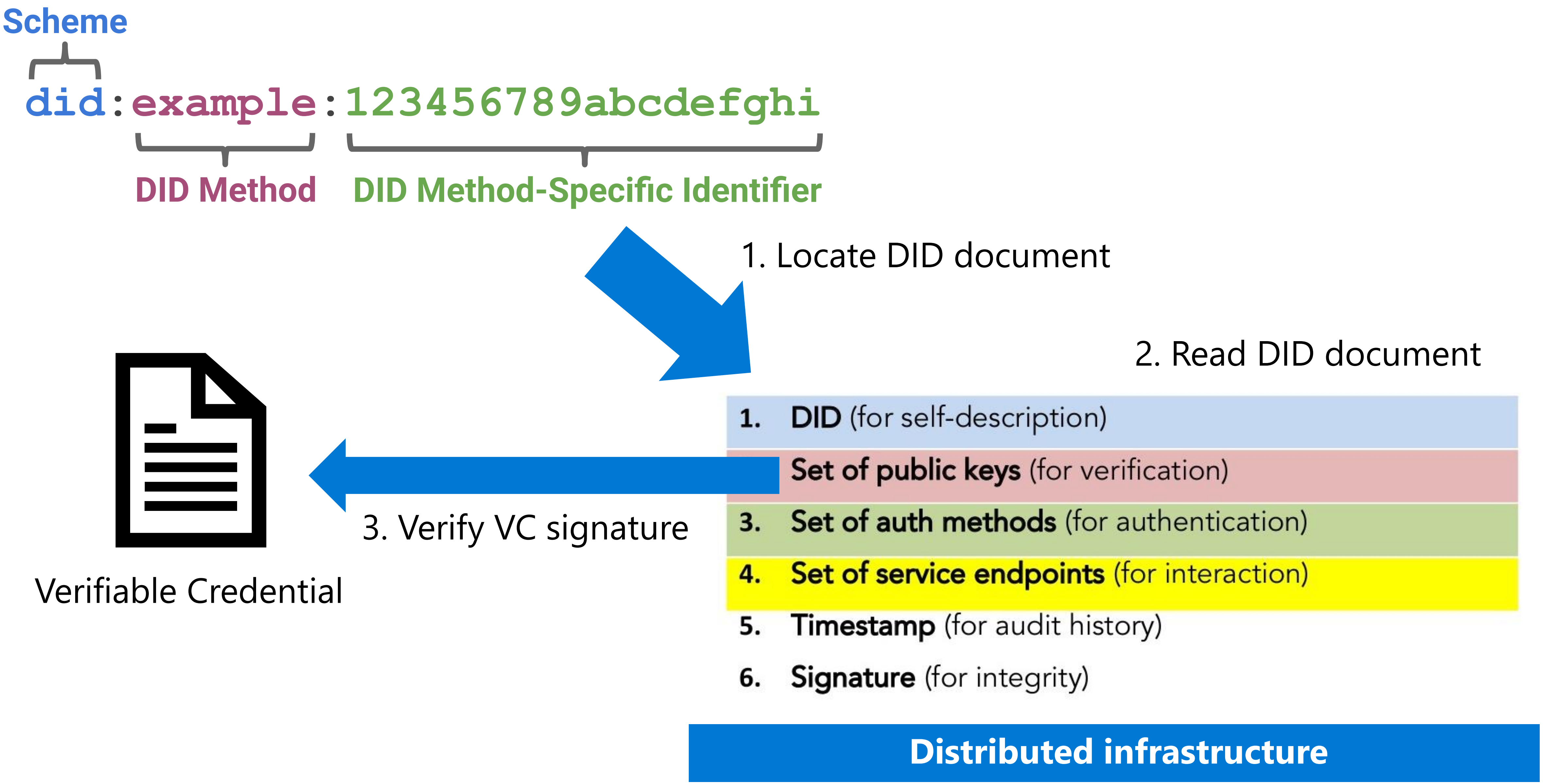
Decentralized Identifiers



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)

W3C Verifiable Credentials


issue
Holder
manages credentials; uses them to create presentations of proof for Verifiers
present
write
Verifiable Data Registry
read
Issuer
digitally signs attestations; packages and gives cred to Holder
Verifier
requests proof; verifies that issuer attestations satisfy requirements



Scheme

`did:example:123456789abcdefghi`

DID Method

DID Method-Specific Identifier

1. Locate DID document

2. Read DID document

1. **DID** (for self-description)

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

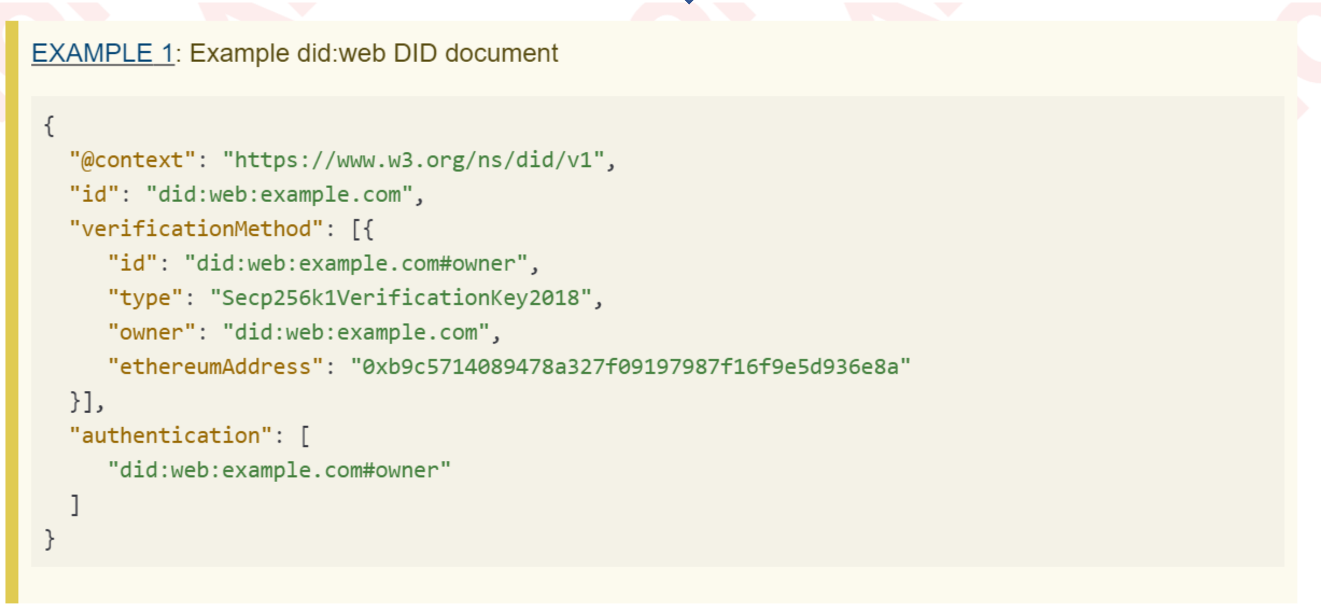
Verifiable Credential

What is did:web?

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

did:web Method Specification (w3c-ccg.github.io) did:web:example.com

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

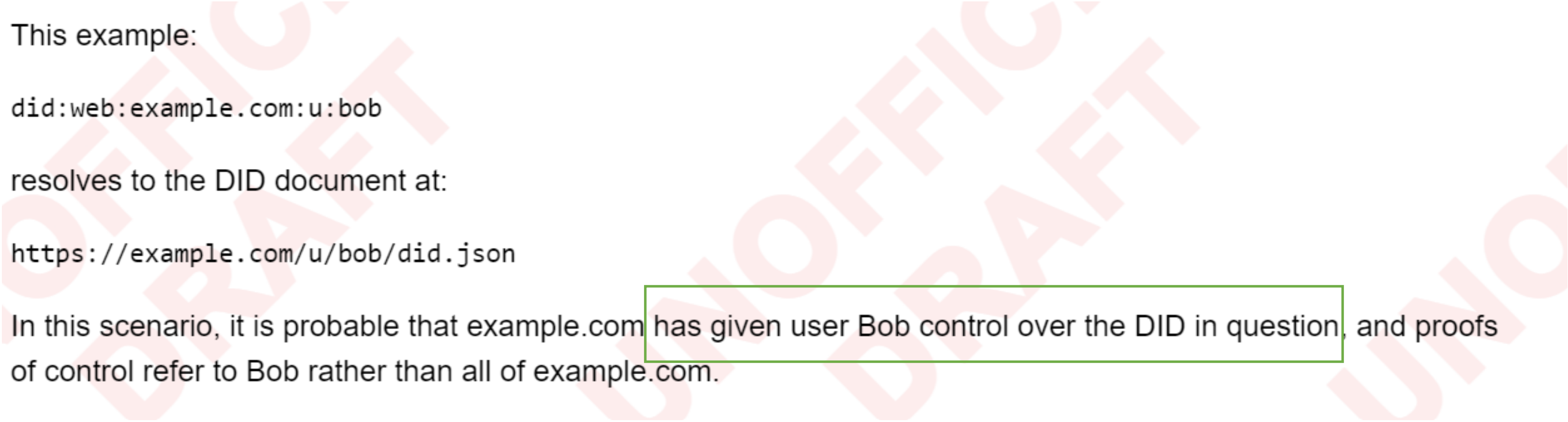


EXAMPLE 1: Example did:web DID document

```
{
  "@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"
  ]
}
```

Considerations

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



This example:

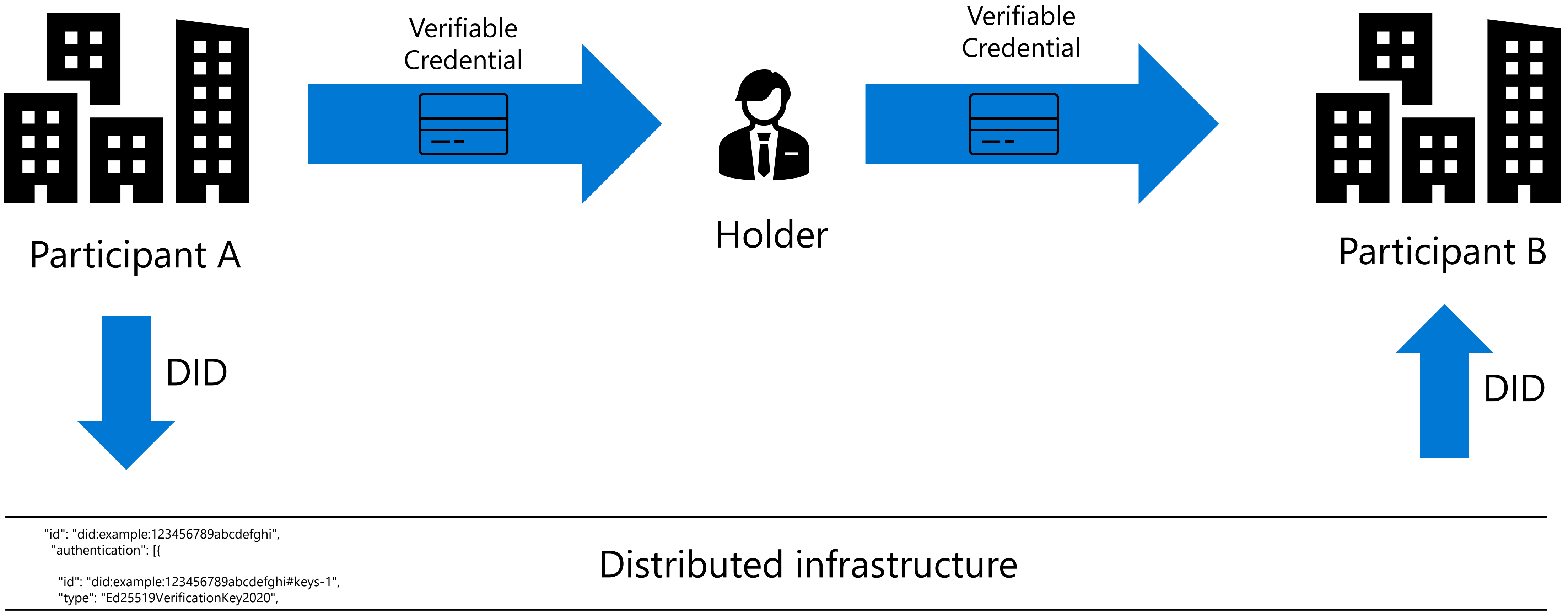
```
did:web:example.com:u:bob
```

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.

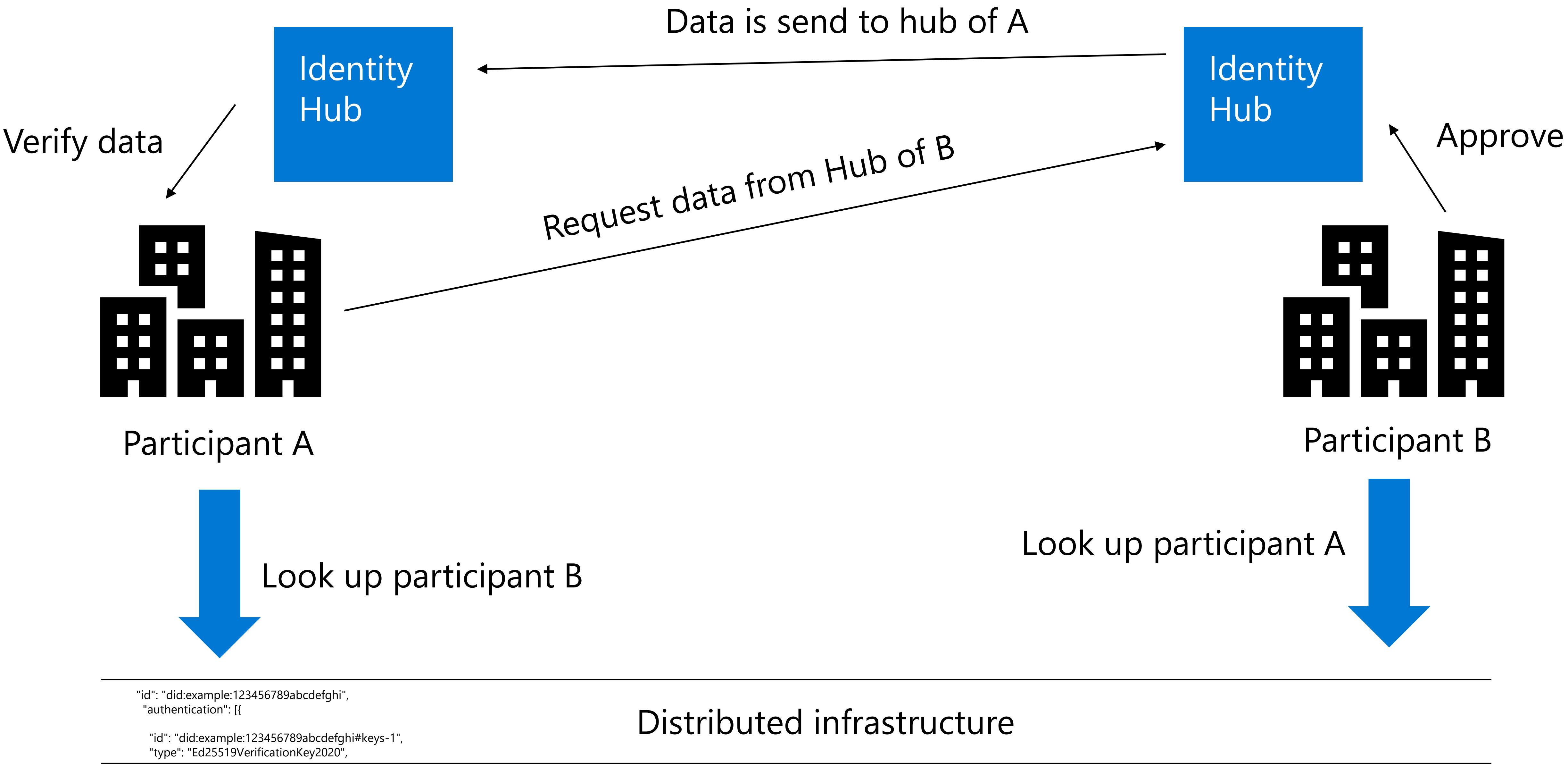
Putting it all together: User initiated



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

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

Introducing: Identity Hub



Data is send to hub of A

Identity Hub

Identity Hub

Verify data

Request data from Hub of B

Approve

Participant A

Participant B

Look up participant A

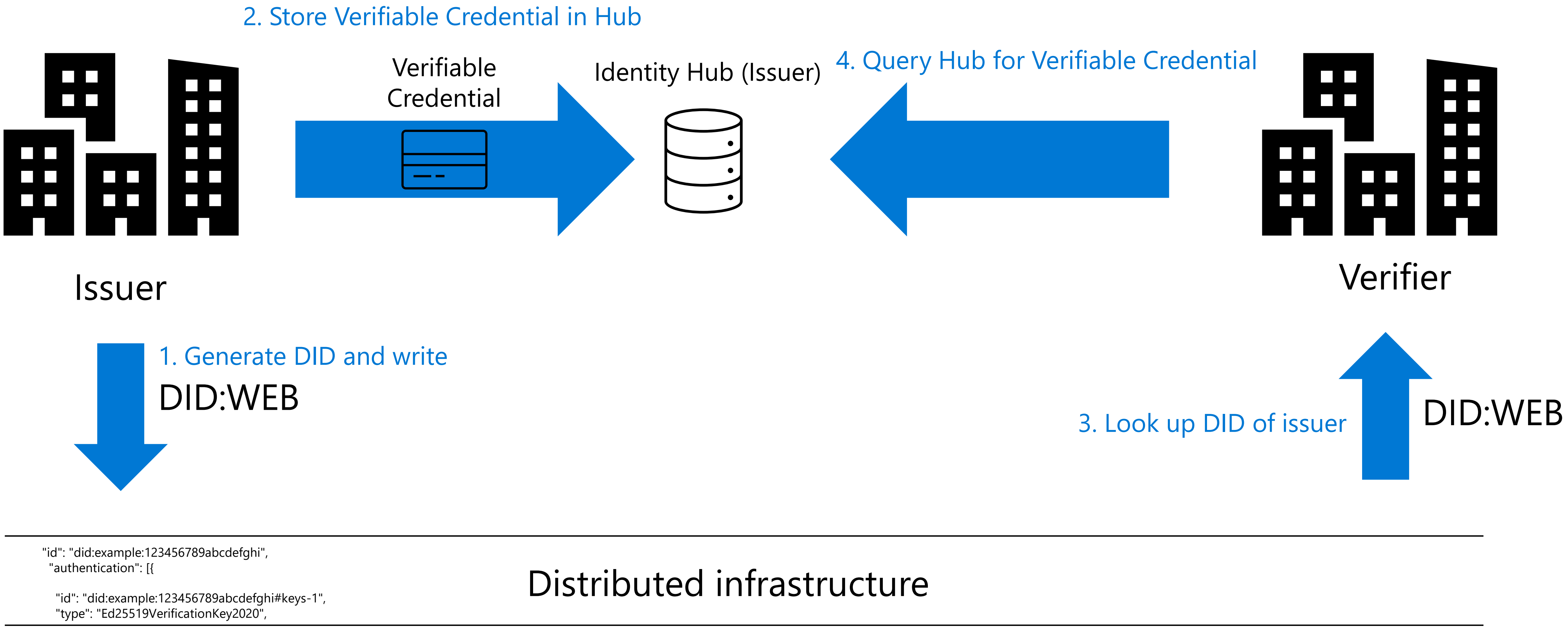
Look up participant B

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

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

Distributed infrastructure

Putting it all together: Using identity hub



2. Store Verifiable Credential in Hub

Verifiable Credential

Identity Hub (Issuer)

4. Query Hub for Verifiable Credential

Issuer

Verifier

1. Generate DID and write

DID:WEB

3. Look up DID of issuer

DID:WEB

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

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

Distributed infrastructure

Current EDC support

Identity Hub

Centralized

oAuth2 – Client Credential Flow

SAML, WS-Fed, Kerberos?

Decentralized

DID:WEB

DID:ION

DID:???

Questions?

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