

did:self A registry-less DID method

N. Fotiou, G.C. Polyzos, V.A. Siris



Decentralized Identifiers

- A W3C recommendation—acting as a framework
- Many individual *DID methods*

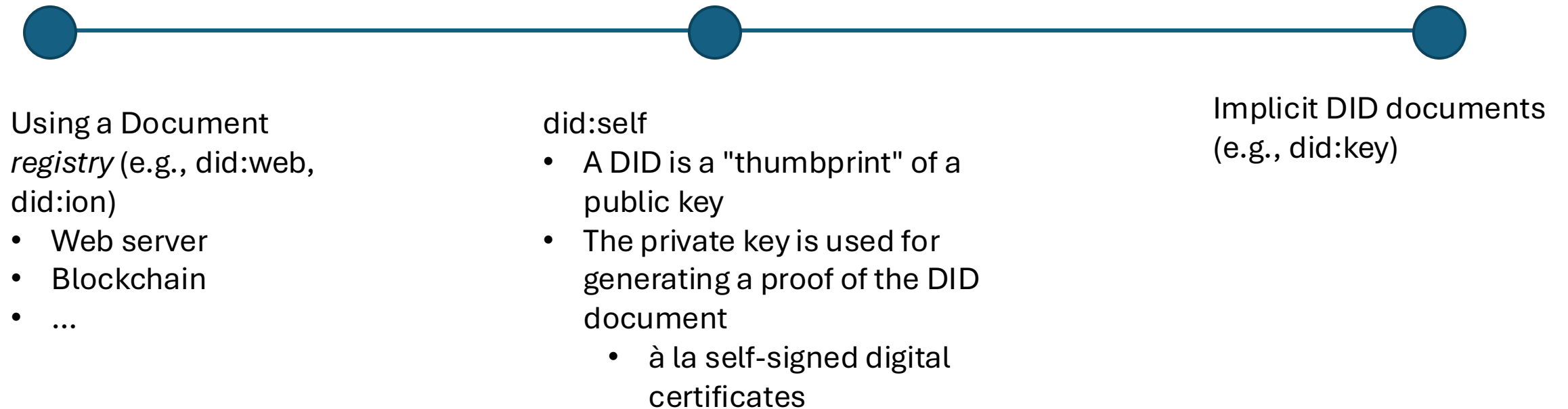
did:web:did.actor:alice



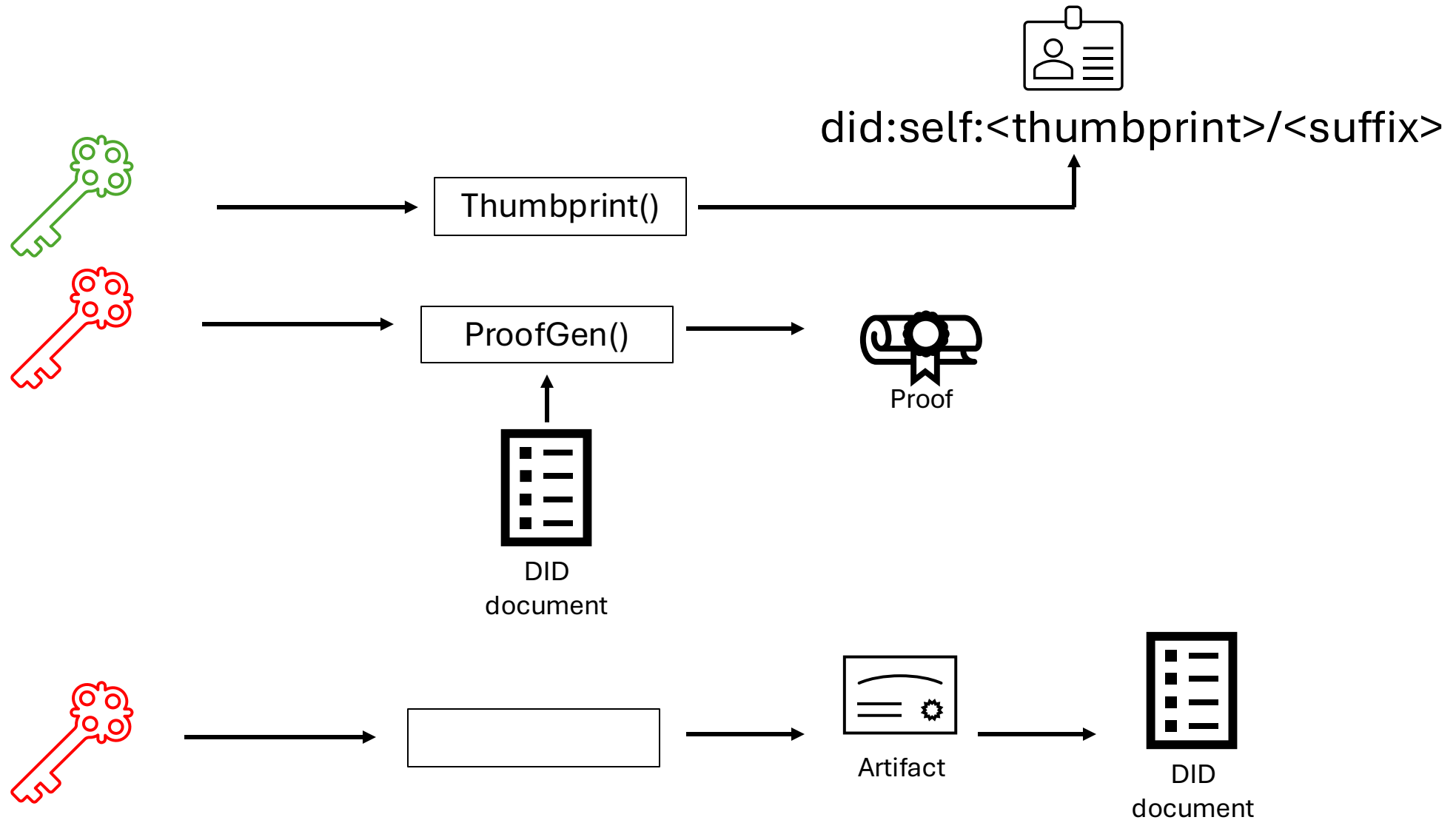
```
{
  "id": "did:web:did.actor:alice",
  "publicKey": [
    {
      "id": "#key1",
      "controller": "did:web:did.actor:alice",
      "type": "Ed25519VerificationKey2018",
      "publicKeyBase58": "DK7uJiq9...FPrk6LSjZ2JRz"
    }
  ],
  "authentication": [
    "did:web:did.actor:alice#key1"
  ]
}
```

DID Document Resolution

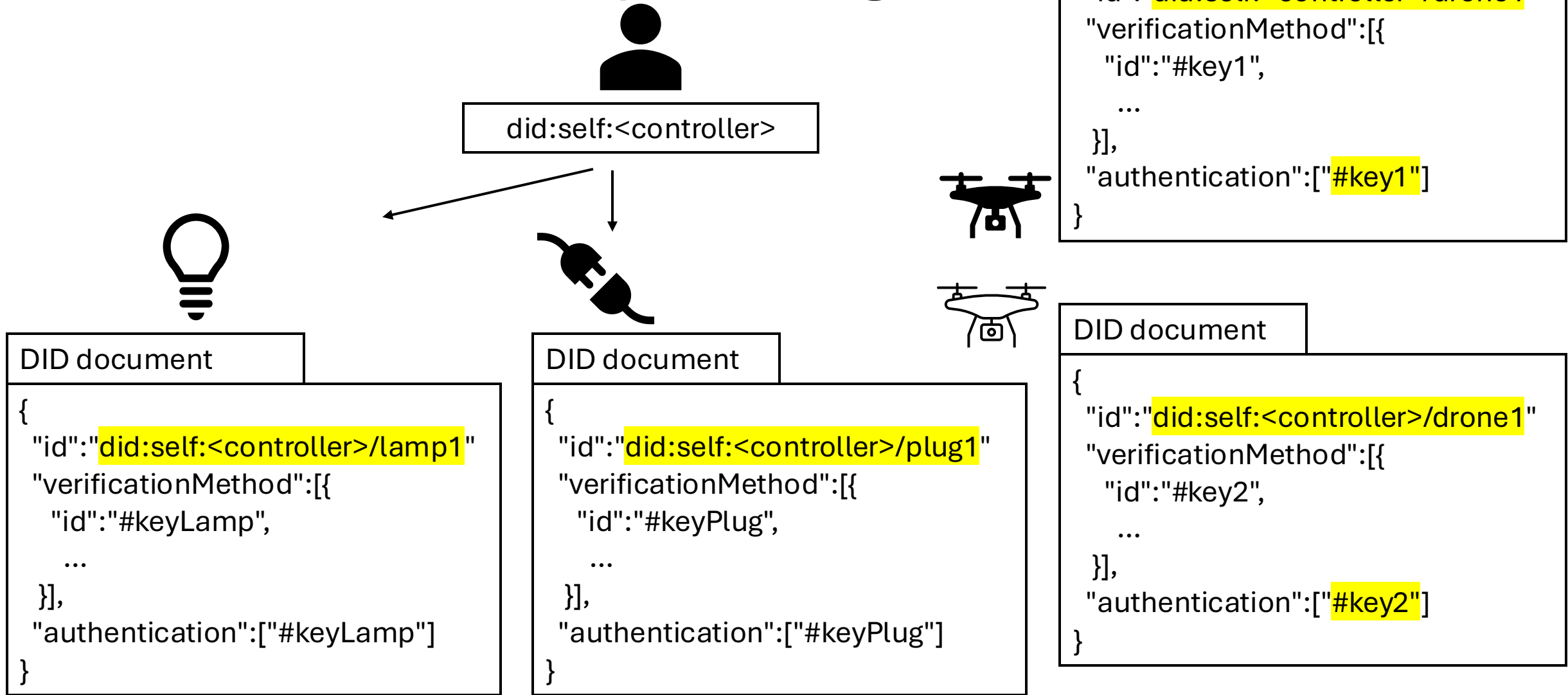
- How a DID document is *resolved*?



did:self Identifier Generation



Controlled Identity Sharing



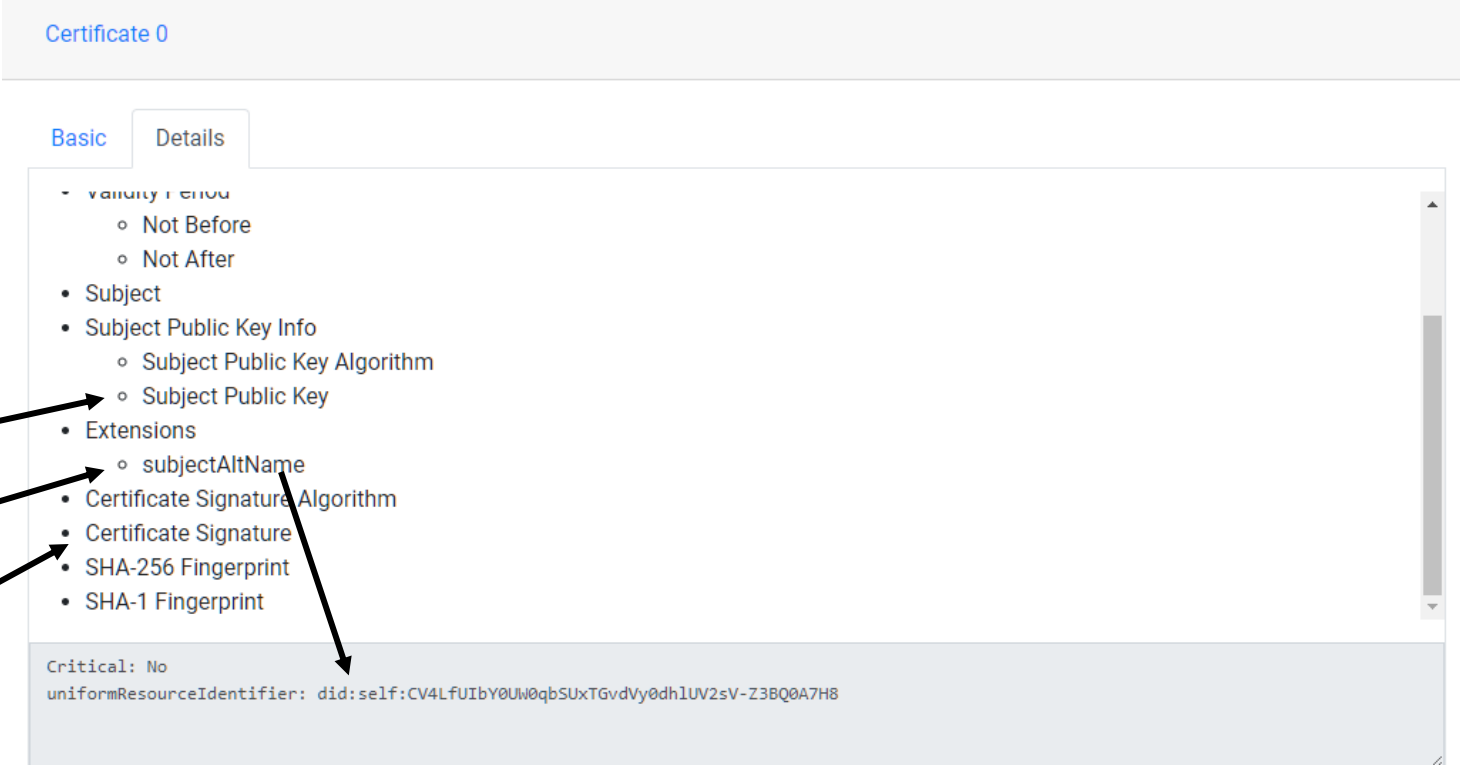
DID documents as JSON Web Tokens

```
1  {
2  "iss": "did:self:iQ9PsBKOH1nLT9FyhsUGvXyKoW00yqm_-_rVa3W7C10",
3  "sub": "device1", ← suffix
4  "cnf": {
5    "jwk": {
6      "kty": "EC", ← authentication verification relationship
7      "crv": "P-256",
8      "x": "YOGmYaMKzwTFytWHN2hGC-2VpPqGqj_sDSckB2IvCgI",
9      "y": "7iWuiXQlLXvROjdMA2WNHhGz0jxu6u41n83YupNteo"
10   }
11  }
12 }
```

controller ←

DID documents as x509 certificate

- Step 1: CA certificate



The image shows a screenshot of a web interface for a 'Certificate 0'. The interface has two tabs: 'Basic' and 'Details'. The 'Details' tab is active, showing a tree view of certificate fields. On the left side of the screenshot, there are three icons: a green key, a person ID card, and a red key. Arrows point from these icons to specific fields in the certificate details: the green key points to 'Subject Public Key', the ID card points to 'subjectAltName', and the red key points to the 'uniformResourceIdentifier' field. The 'uniformResourceIdentifier' field contains the value 'did:self:CV4LfUIbY0UW0qbSUXTGvdVy0dh1UV2sV-Z3BQ0A7H8'.

Certificate 0

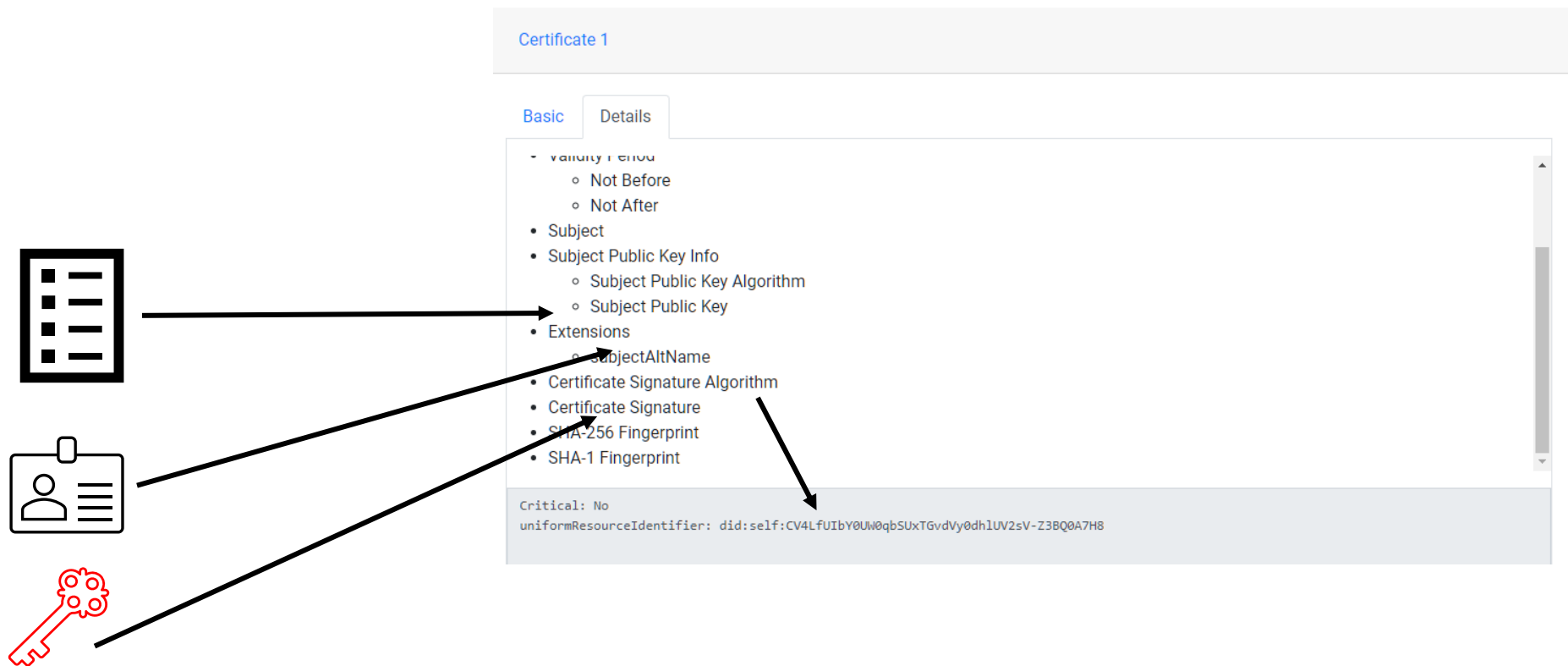
Basic Details

- validity period
 - Not Before
 - Not After
- Subject
- Subject Public Key Info
 - Subject Public Key Algorithm
 - Subject Public Key
- Extensions
 - subjectAltName
- Certificate Signature Algorithm
- Certificate Signature
- SHA-256 Fingerprint
- SHA-1 Fingerprint

Critical: No
uniformResourceIdentifier: did:self:CV4LfUIbY0UW0qbSUXTGvdVy0dh1UV2sV-Z3BQ0A7H8

DID document to x509

- Step 2: Certificate



Takeaways

- did:self does not require any registry, yet it supports DID documents
- did:self allows controlled identity sharing
- Implicit DID documents for did:self allow interoperability with existing standards

Thank you

fotiou@excid.io

<https://github.com/excid-io/did-self>