

Understanding Decentralized Identifiers

Kim Hamilton Duffy

CTO Learning Machine

Co-chair W3C Credentials Community Group

Decentralized Identity Foundation Steering Committee

What is a Decentralized Identifier?

A new type of URL that is:

- globally unique,
- highly available,
- persistent
- cryptographically verifiable, and
- does not require a central admin

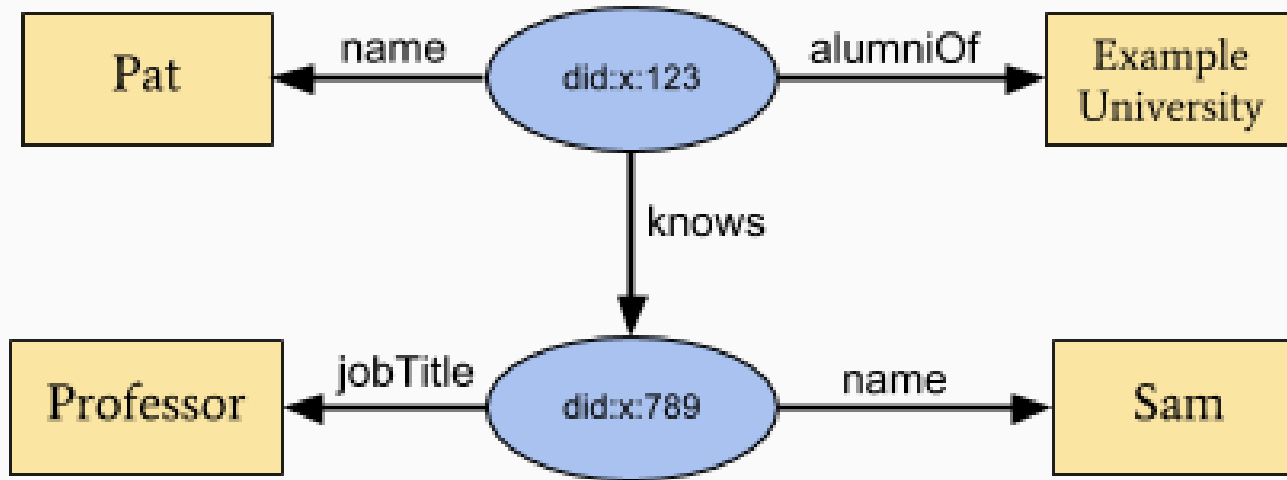


did:btcr:txtest1:8kyt-fzzq-qqqq-ase0-d8

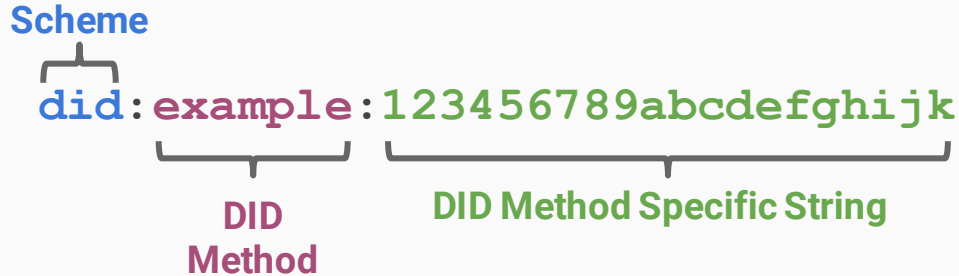
```
{
  "@context": [
    "https://www.w3.org/ns/did",
    "https://w3id.org/did/vc"
  ],
  "id": "urn:uuid:12345678901234567890123456789012",
  "type": "Asymmetric",
  "badge": {
    "id": "urn:uuid:12345678901234567890123456789012",
    "issuer": {
      "type": "Asymmetric",
      "id": "urn:uuid:12345678901234567890123456789012",
      "uri": "https://example.com",
      "name": "Example"
    },
    "type": "Asymmetric",
    "criteria": {
      "narrative": "This is a narrative about the badge."
    },
    "name": "Badge",
    "description": "This is a description of the badge."
  },
  "issuedOn": "2017-06-20T14:58:17.401422+00:00",
  "recipient": {
    "id": "urn:uuid:12345678901234567890123456789012",
    "verificationMethod": {
      "publicKey": "ecdsa-40b11a-pubkey:nadC0buaQ762yp87uckpbAtL9Pg76ieJ",
      "type": "ECDSA",
      "id": "urn:uuid:12345678901234567890123456789012"
    }
  }
}
```



We use DIDs in Verifiable Credentials



DID Implementations (Methods)



Examples:

```
did:v1:nym:BcNkgGmGEpCGSJSMPB4BvWvwVM6YeTR52BSWcZTbzU23  
did:btcr:txtest1:8kyt-fzzq-qqqq-ase0-d8
```

DIDs Resolve to DID Documents

```
{
  "@context": "https://w3id.org/veres-one/v1",
  "id": "did:vl:nym:DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD",
  "authentication": [{
    "type": "Ed25519SignatureAuthentication2018",
    "publicKey": [{
      "id": "did:vl:test:nym:DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD#authn-key-1",
      "type": "Ed25519VerificationKey2018",
      "controller": "did:vl:nym:DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD",
      "publicKeyBase58": "DwkYwcoyUXHNkpj3whn4DgXB4fcg9gj95vKxYN2apkZD"
    }]
  }],
  "service": [{
    "type": "ExampleMessagingService2018",
    "serviceEndpoint": "https://example.com/services/messages"
  }],
  ... more DID-specific information here ...
}
```

1. Authentication Mechanisms

2. Public Key Material

3. Service Discovery

DID RESOLUTION

DID

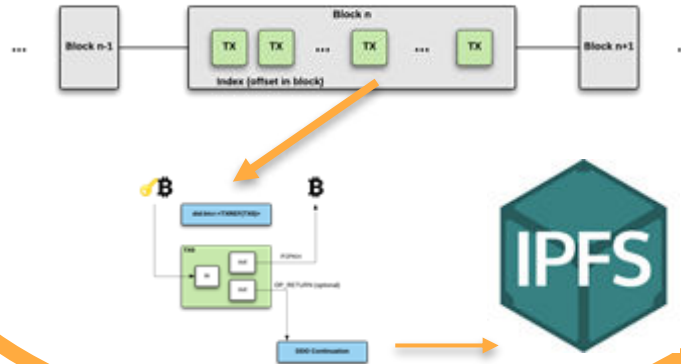
did:btcr:xkyt-fzgq-qq87-xnhn

Universal Resolver

DID Document

[illegible]

DID Method Spec



DID DOCUMENT

```
{
  "@context": "https://w3id.org/did/v1",
  "id": "did:example:123456789abcdefghi",
  "publicKey": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaSigningKey2018",
    "owner": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY-----\r\n"
  }],
  "authentication": [{
    "type": "RsaSignatureAuthentication2018",
    "publicKey": "did:example:123456789abcdefghi#keys-1"
  }],
  "service": [{
    "type": "ExampleService",
    "serviceEndpoint": "https://example.com/endpoint/8377464"
  }],
  "created": "2002-10-10T17:00:00Z",
  "updated": "2016-10-17T02:41:00Z",
  "signature": {
    "type": "RsaSignature2016",
    "created": "2016-02-08T16:02:20Z",
    "creator": "did:sov:8uQhQMGzWxR8ww5P3UWH1j#key/1",
    "signatureValue": "IOmA4R7TfhkYTYW87z640O3GYFIdw0
      yqie9Wl1kZ5OBYNAKOWG5uOsPRK8/2
      C4STOWF+83cMcbZ3CBMq2/gj25s="
  }
}
```

- 1. DID (for self-description)
- 2. Public keys (for verification)
- 3. Auth methods (for authentication)
- 4. Service endpoints (for interaction)
- 5. Timestamp (for audit history)
- 6. Signature (for integrity)

Status

- Incubated at RWOT, IIW
- Currently:
 - Draft report in W3C Credentials Community Group
 - Protocols and prototypes at DIF
 - DID Method Registry
 - DID Auth, DID Resolver
- To Discuss: DID Working Group

DID & VC Architecture Roadmap 2018+

Christopher Allen

Principal Architect & Founder — Blockchain Commons
W3C Credentials CG Chair

Current W3C Standards Track Efforts

- Verifiable Claims WG, Verifiable Credentials
 - Anyone can verifiably say anything about anyone.
 - Identity emerges from evaluating multiple sources of information, across multiple interactions
- Decentralized Identifiers (DIDs), draft WG
 - Anyone can publicly manage provable identifiers without administrative interference
 - Move beyond centrally administered IDs
 - Provide for a plurality of authorities

Decentralized Identity Stack

- DIDs – Root Identifiers
 - DID Universal Resolvers — support interoperability between multiple DID methods.
 - DID Methods – Specific approaches using different blockchains
 - DID Documents – Proof of Control & Service References

+

Decentralized Identity Stack

- DIDs – Root Identifiers ...
- Raw Data – Observed facts & transactions
- Verifiable Credentials – Assertions by knowable authorities
- Profiles / Presentations / Persona – Representations of individuals
- Consent – Records of authorization
- Reasoning – Interpretation & Analysis
- Evaluation – Risk Analysis & Reputation
- Understanding – Internal knowledge representation
- Services – Interactions of value

Potential Standards for Future Work

- DID-Auth (Authn/Authz)
- OCAP (Authz through Object Capabilities)
- Credential Requests & Exchange
- Data Minimization & Selective Disclosure
- Consent & Consent Receipts
- Storage (Identity Hubs) & Internal Representations
- Analytics & Algorithms for Evaluation
- Cryptographic Proofs
 - Signature, Encryption, Signcryption Suites
 - Time-stamping
 - Zero-knowledge proofs

The W3C Credentials Community Group Specification Roadmap (July 2018)

This is a forward looking, high-level overview of the technology and specification roadmap of the W3C Credentials Community Group.

