Verifiable Credentials
and
Decentralized Identifiers
with
DIDKit

Charles E. Lehner / Spruce Systems, Inc.

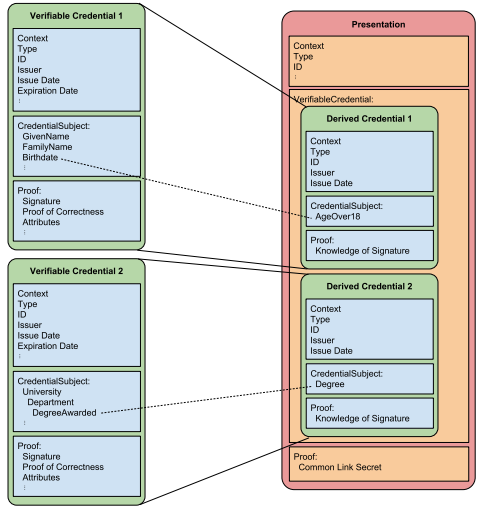
FOSDEM 2022 Web3 Devroom

Verifiable Credentials (VCs)

Verifiable Credentials Data Model v1.1

https://www.w3.org/TR/vc-data-model/

W3C Recommendation



Verifiable Credentials (VCs)

Example 1: A simple example of a verifiable credential

```
{
  // set the context, which establishes the special terms we will be using
  // such as 'issuer' and 'alumniOf'.
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  // specify the identifier for the credential
  "id": "http://example.edu/credentials/1872",
  // the credential types, which declare what data to expect in the credential
  "type": ["VerifiableCredential", "AlumniCredential"],
  // the entity that issued the credential
  "issuer": "https://example.edu/issuers/565049",
  // when the credential was issued
  "issuanceDate": "2010-01-01T19:23:24Z",
  // claims about the subjects of the credential
  "credentialSubject": {
    // identifier for the only subject of the credential
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    // assertion about the only subject of the credential
    "alumniOf": {
      "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
      "name": [{
```

Decentralized Identifiers (DIDs)

Decentralized Identifiers (DIDs) v1.0

https://www.w3.org/TR/did-core/

W3C Proposed Recommendation

Decentralized Identifiers (DIDs)

Example 1: A simple DID document

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ]
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    // used to authenticate as did:...fghi
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2020",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }]
}
```

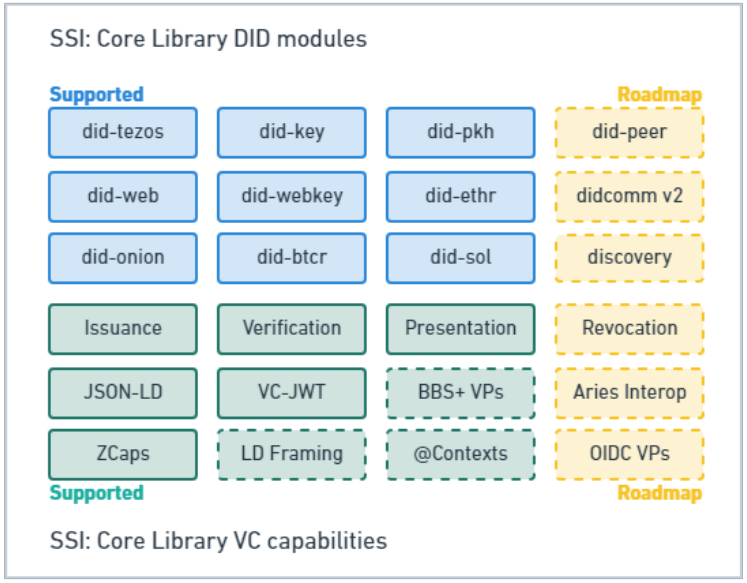
DIDKit/SSI

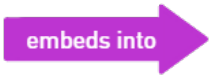
ssi: Core library in Rust

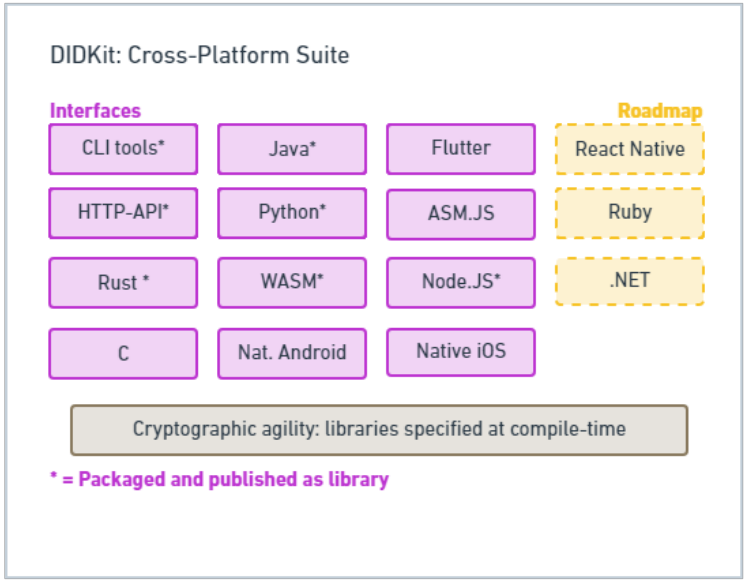
https://github.com/spruceid/ssi

didkit: CLI and bindings

https://github.com/spruceid/didkit







DIDKit

https://github.com/spruceid/didkit/

https://spruceid.dev/docs/didkit/

```
didkit-cli 0.1.1

USAGE:
    didkit <SUBCOMMAND>

FLAGS:
    -h, --help       Prints help information
    -V, --version    Prints version information

SUBCOMMANDS:
    did-auth                      Authenticate with a DID
    did-dereference               Dereference a DID URL to a resource
    did-resolve                   Resolve a DID to a DID Document
    generate-ed25519-key          Generate and output a Ed25519 keypair in JWK format
    help                          Prints this message or the help of the given subcommand(s)
    key-to-did                    Output a DID for a given JWK according to the provided DID method name or pattern
    key-to-verification-method    Output a verificationMethod DID URL for a JWK and DID method name/pattern
    ssh-pk-to-jwk                 Convert a SSH public key to a JWK
    to-rdf-urdna2015              Convert JSON-LD to URDNA2015-canonicalized RDF N-Quads
    vc-issue-credential           Issue Credential
    vc-issue-presentation         Issue Presentation
    vc-verify-credential          Verify Credential
    vc-verify-presentation        Verify Presentation
```

DIDKit - Demo


```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1"
  ],
  "type": [
    "VerifiablePresentation"
  ],
  "verifiableCredential": {
    "@context": [
      "https://www.w3.org/2018/credentials/v1"
    ],
    "type": [
      "VerifiableCredential"
    ],
    "credentialSubject": {
      "id": "did:key:zQ3shVad4rYU4yBPwBrUU6kPFwpwxccQDZUDovcJqYFbGQHX5"
    },
    "issuer": "did:key:z6MkrPSezXuJQ9NXPtrduu4ZtpsuxFjKh9aj2UUTG11oPNsa",
    "issuanceDate": "2022-01-18T15:48:56Z",
    "proof": {
      "type": "Ed25519Signature2018",
      "proofPurpose": "assertionMethod",
      "verificationMethod":
```

Other VC/DID Implementations

https://github.com/transmute-industries/verifiable-data

https://github.com/digitalbazaar/vc-js

https://github.com/danubetech/verifiable-credentials-java

https://github.com/decentralized-identity/did-jwt-vc

https://github.com/hyperledger/aries-cloudagent-python

https://github.com/uport-project/veramo

Community

- World Wide Web Consortium (W3C)
  - Credentials Community Group (CCG)
    - public-credentials@w3.org
  - Decentralized Identifiers Working Group (DID WG)
  - Verifiable Credentials Working Group (VC WG)
- Decentralized Identity Foundation (DIF)
  - Interoperability Open Group
- Internet Identity Workshop (IIW)
- Trust over IP Foundation (ToIP)
- OpenID Foundation
- IEEE SA OPEN

Chat

Matrix: #public-dev:spruceid.com

IRC: #spruce-dev @ Libera.Chat

Email: oss@spruceid.com

Chat

Matrix: @cel:fosdem.org / @cel:spruceid.com

IRC: **cel** @ Libera.Chat / W3C IRC / tilde.chat.

Email: cel@celehner.com / charles.lehner@spruceid.com

OpenPGP: `B8FF 71DA 2A37 5F8F 93FC BBDA 4D2E 8021 3413 F006`

Secure Scuttlebutt: `@f/6sQ6d2CMxRUhLpspgGIulDxDCwYD7DzFzPNr7u5AU=.ed25519`

https://www.w3.org/wiki/User:cel

Thanks