

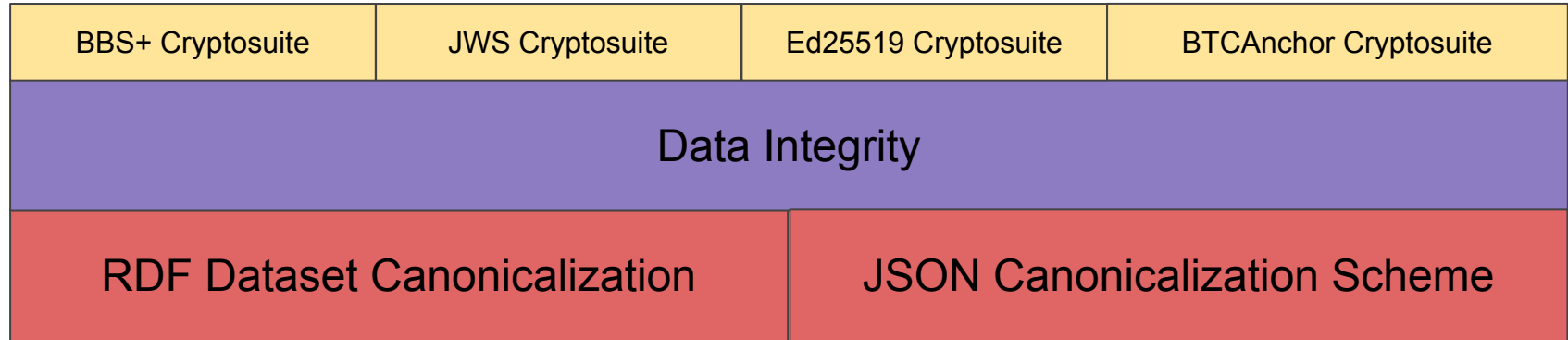


Data Integrity - Multiproofs

Benefits of adding multiple proofs to Verifiable Credentials



The Data Integrity Security Stack (excerpt)



VC with one signature



| | |
|--|-------------|
| <pre>{ "@context": ["https://www.w3.org/2018/credentials/v1", "https://www.w3.org/2018/credentials/examples/v1", "https://w3id.org/security/suites/ed25519-2020/v1"], "id": "http://example.edu/credentials/3732", "type": ["VerifiableCredential", "UniversityDegreeCredential"], "issuer": "https://example.edu/issuers/565049", "issuanceDate": "2010-01-01T00:00:00Z", "credentialSubject": { "id": "did:example:ebfeb1f712ebc6f1c276e12ec21", "degree": { "type": "BachelorDegree", "name": "Bachelor of Science and Arts" } } },</pre> | Information |
| <pre> "proof": { "type": "Ed25519Signature2020", "created": "2022-02-01T01:50:35Z", "verificationMethod": "https://example.edu/issuers/565049#key-1", "proofPurpose": "assertionMethod", "proofValue": "z3zbRkFABmNDAF9SVE14...8WvrLvchpX3yYRMwydH" } }</pre> | Signature |

Benefit: Assert who issued the VC and protect it from tampering.

VC with two signatures in parallel



| | |
|--|---------------|
| <pre>{ "@context": ["https://www.w3.org/2018/credentials/v1", "https://www.w3.org/2018/credentials/examples/v1", "https://w3id.org/security/suites/ed25519-2020/v1"], "id": "http://example.edu/credentials/3732", "type": ["VerifiableCredential", "UniversityDegreeCredential"], "issuer": ["https://example.edu/issuers/565049", "https://example.edu/issuers/748392"], "issuanceDate": "2010-01-01T00:00:00Z", "credentialSubject": { "id": "did:example:ebfeb1f712ebc6f1c276e12ec21", "degree": { "type": "BachelorDegree", "name": "Bachelor of Science and Arts" } } },</pre> | Information |
| <pre> "proof": [{ "type": "Ed25519Signature2020", "created": "2022-02-01T01:50:35Z", "verificationMethod": "https://example.edu/issuers/565049#key-1", "proofPurpose": "assertionMethod", "proofValue": "z3zbRkFABmNdAF9SVE14...8WvrLvchpx3yQYRMwydH"</pre> | Signature (A) |
| <pre> }, { "type": "Ed25519Signature2020", "created": "2022-02-01T01:55:41Z", "verificationMethod": "https://example.edu/issuers/748392#key-5", "proofPurpose": "assertionMethod", "proofValue": "zNdAF9SVE143zbRkFABm...3yQYRMwydH8WvrLvchpX" } }</pre> | Signature (B) |

Benefit: Enable multiple issuers to sign the same data as a single package of information. The order of signatures **DOES NOT** matter.

VC with two signatures in series



```
{
  "@context": ["https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"],
  "id": "http://example.edu/credentials/3732",
  "type": ["VerifiableCredential", "UniversityDegreeCredential"],
  "issuer": ["https://example.edu/issuers/565049", "https://example.edu/issuers/748392"],
  "issuanceDate": "2010-01-01T00:00:00Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6flc276e12ec21",
    "degree": {
      "type": "BachelorDegree",
      "name": "Bachelor of Science and Arts"
    }
  }
},
{
  "proofChain": [{
    "type": "Ed25519Signature2020",
    "created": "2022-02-01T01:50:35Z",
    "verificationMethod": "https://example.edu/issuers/565049#key-1",
    "proofPurpose": "assertionMethod",
    "proofValue": "z3zbRkFABmNdAF9SVE14...8WvrLvchpX3yQYRMwydH"
  }], {
    "type": "Ed25519Signature2020",
    "created": "2022-02-01T01:55:41Z",
    "verificationMethod": "https://example.edu/issuers/748392#key-5",
    "proofPurpose": "assertionMethod",
    "proofValue": "zNdAF9SVE143zbRkFABm...3yQYRMwydH8WvrLvchpX"
  }
}
}
```

Information

Signature (1)

Signature (2)

Benefit: Enable multiple issuers to sign the same data as a single package of information. The order of signatures **DOES** matter.

VC with two different signature approaches



```
{
  "@context": ["https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"],
  "id": "http://example.edu/credentials/3732",
  "type": ["VerifiableCredential", "UniversityDegreeCredential"],
  "issuer": "https://example.edu/issuers/565049",
  "issuanceDate": "2010-01-01T00:00:00Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6flc276e12ec21",
    "degree": {
      "type": "BachelorDegree",
      "name": "Bachelor of Science and Arts"
    }
  }
},
{
  "proof": [{
    "type": "Ed25519Signature2020",
    "created": "2022-02-01T01:50:35Z",
    "verificationMethod": "https://example.edu/issuers/565049#key-1",
    "proofPurpose": "assertionMethod",
    "proofValue": "z3zbRkFADmNdAF90VE14...8Wv1Lvchpx3yQYRMwydH"
  }],
  {
    "type": "BbsBlsSignature2020",
    "created": "2022-02-01T01:50:38Z",
    "verificationMethod": "https://example.edu/issuers/565049#key-2",
    "proofPurpose": "assertionMethod",
    "proofValue": "rQacBr+Lj5yfMdZ...wDQNQxD+hSkpJ8fQ=="
  }
}
}
```

Information

Signature (Ed25519)

Signature (BBS+)

Benefit: Enable an issuer to sign the same data using different cryptographic approaches. Stronger security, better agility, best of multiple approaches.