VC land

demystified

Created by @andresuribe87 on March, 2023

Who this deck is for

If you are:

- A developer.
- New to Verifiable Credentials (VCs)
- Not thrilled about learning through reading specs or RFCs.
- Want to learn *just enough* about VCs in under 15 mins.

Then this is for you.

What is a VC

It's a **graph** of information.

It may have some of the standard **properties**. Some of which are required.

The graph can be encoded using JSON + Proof Format
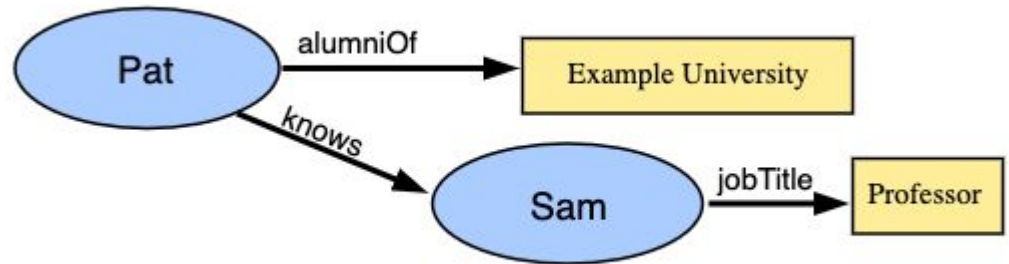
It's defined as a W3C standard

Figure 4 Multiple claims can be combined to express a graph of information.

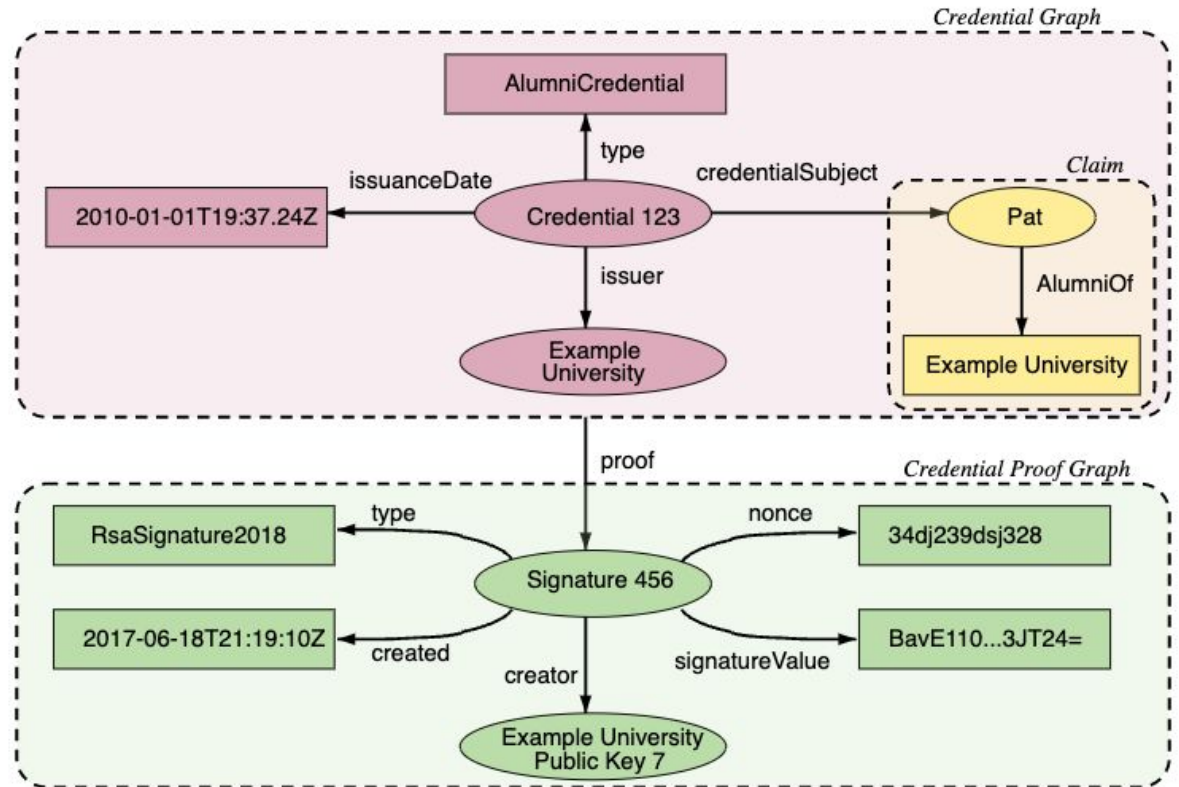# What is a VC

A full graph like what's on the right!

Figure 6 Information graphs associated with a basic verifiable credential.

Examples of VCs

This is what's referred to as a VC with an embedded proof.

It's an *information graph* in JSON!

```
{
  "@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/14",
  "issuanceDate": "2010-01-01T19:23:24Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "degree": {
      "type": "BachelorDegree",
      "name": "Bachelor of Science and Arts"
    }
  },
  "credentialStatus": {
    "id": "https://example.edu/status/24",
    "type": "CredentialStatusList2017"
  },
  "proof": {
    "type": "Ed25519Signature2020",
    "created": "2022-02-25T14:58:43Z",
    "verificationMethod": "https://example.edu/issuers/14#key-1",
    "proofPurpose": "assertionMethod",
    "proofValue": "z3BXsFfx1qJ5NsTkKqREjQ3AGh6RAmCwvgu1HcDSzK3P5QEg2TAw8ufk
tJBw8QkAQRciMGyBf5T2AHyRg2w13Uvhp"
  }
}
```

Examples of VCs

This is what's referred to as a VC with an external proof.

Note that this is a string. It's not even JSON. More accurately, it's a JWT.

You can get JSON from it. Which looks similar to our previous example (but not the same!)

(PD: it's also an *information graph*)

eyJhbGciOiJFUzI1NiIsInR5cCI6IkpXVCJ9.eyJ2YyI6eyJAY29udGV4dCI6WyJodHRwczovL3
d3dy53My5vcmcvMjAxOC9jcmVkZW50aWFscy92MSIsImh0dHBzOi8vd3d3LnczLm9yZy8yMDE4L
2NyZWRlbnRpYWxzL2V4YW1wbGVzL3YxIl0sImlkIjoiaHR0cDovL2V4YW1wbGUuZWR1L2NyZWRl
bnRpYWxzLzM3MzIiLCJ0eXBlIjpbIlZlcmlmaWFibGVDcmVkZW50aWFsIiwiVW5pdmVyc2l0eUR
lZ3JlZUNyZWRlbnRpYWwiXSwiXNzdWVyIjoiaHR0cHM6Ly9leGFtcGxlLmVkdS9pc3N1ZXJzLz
E0IiwiaXNzdWFuY2VEYXRlIjoiMjAxMC0wMS0wMVQxOToyMzoyNFoiLCJjcmVkZW50aWFsU3Via
mVjdCI6eyJpZCI6ImRpZDpleGFtcGxlOmViZmViMWY3MTJlYmM2ZjFjMjc2ZTEyZWMyMSIsImRl
Z3JlZSI6eyJ0eXBlIjoiQmFjaGVsb3JEZWdyZWUiLCJuYW1lIjoiQmFjaGVsb3Igb2YgU2NpZW5
jZSBhbmQgQXJ0cyJ9fSwiY3JlZGVudGlhbFN0YXR1cyI6eyJpZCI6Imh0dHBzOi8vZXhhbXBsZS
5lZHUvc3RhdHVzLzI0IiwidHlwZSI6Ik5yZWRlbnRpYWxTdGF0dXMiXN0MjAxNyJ9fSwiaXNzI
joiaHR0cHM6Ly9leGFtcGxlLmVkdS9pc3N1ZXJzLzE0IiwibmJmIjoxMjYyMzczODA0LCJqdGki
OiJodHRwOi8vZXhhbXBsZS5lZHUvY3JlZGVudGlhbHMvMzczMiIsInN1YiI6ImRpZDpleGFtcGx
lOmViZmViMWY3MTJlYmM2ZjFjMjc2ZTEyZWMyMSJ9.YQKQUu_zreDs69AZ8YqpMGHLl9V_tWH4N
S9P9l67J1wWHf0QCyt5hyuA8ckM4seV-1TRbeiHwdJ3VRkDMcwFcg

Side by Side - diff

```
{
  "vc": {
    "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://www.w3.org/2018/credentials/examples/v1"
    ],
    "id": "http://example.edu/credentials/3732",
    "type": [
      "VerifiableCredential",
      "UniversityDegreeCredential"
    ],
    "issuer": "https://example.edu/issuers/14",
    "issuanceDate": "2010-01-01T19:23:24Z",
    "credentialSubject": {
      "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
      "degree": {
        "type": "BachelorDegree",
        "name": "Bachelor of Science and Arts"
      }
    },
    "credentialStatus": {
      "id": "https://example.edu/status/24",
      "type": "CredentialStatusList2017"
    }
  },
  "iss": "https://example.edu/issuers/14",
  "nbf": 1262373804,
  "jti": "http://example.edu/credentials/3732",
  "sub": "did:example:ebfeb1f712ebc6f1c276e12ec21"
}
```

```
{
  "@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/14",
  "issuanceDate": "2010-01-01T19:23:24Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "degree": {
      "type": "BachelorDegree",
      "name": "Bachelor of Science and Arts"
    }
  },
  "credentialStatus": {
    "id": "https://example.edu/status/24",
    "type": "CredentialStatusList2017"
  },
  "proof": {
    "type": "Ed25519Signature2020",
    "created": "2022-02-25T14:58:43Z",
    "verificationMethod": "https://example.edu/issuers/14#key-1",
    "proofPurpose": "assertionMethod",
    "proofValue": "z3BXsFfx1qJ5NsTkKqREjQ3AGh6RAmCwvgu1HcDSzK3P5QEg2TAw8ufktJBw8QkAQRciMGyBf5T2AHyRg2w13Uvhp"
  }
}
```

What can be done with a VC?

- Can be **presented,** similar to real world credentials like a passport, driver's license, or a university degree.
- Can be **issued**, typically by an organization.
- Its status can be **checked.**
- … and much more!

Life of a single Verifiable Credential

Delete
up to once per Holder

Transfer
repeatable

Holders

Present
repeatable

Issue
exactly once

Verifiers

Issuer

Check Status
Does not preserve privacy
repeatable

Check Status
MAY preserve privacy
repeatable

Revoke
up to once
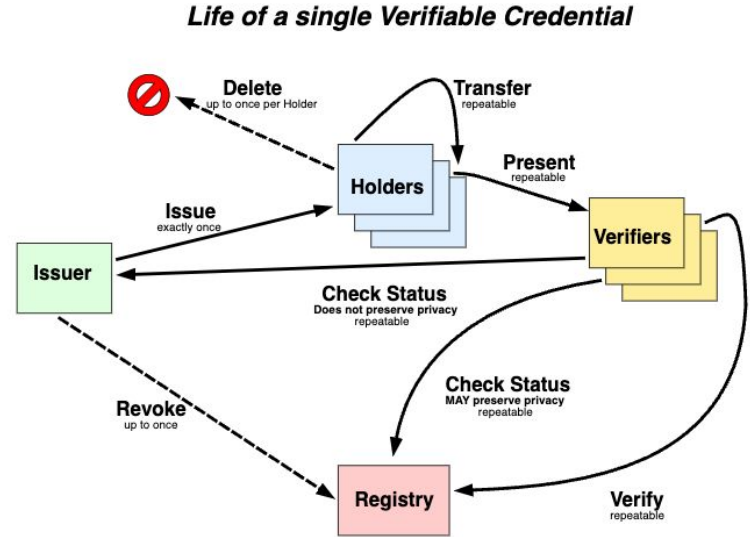
Registry

Verify
repeatable

Figure 10 The roles and information flows for this specification.

Issuance of Credentials using a Credential Manifest

1. Create a CredentialManifest. A good mental model is a Credential Template.
   a. Credential manifests answer the questions:
      i. Who is the issuer of this credential? This is the `issuer` property.
      ii. What information does the issuer need? This is the `presentation_definition` property.
      iii. What information will the credential include? This is the `output_descriptors` property.
      iv. What formats can this be issued in? This is the `format` property.
2. Issue according to the manifest.
3. Win.

Let's focus on this!

What are the different formats?

- Remember: this is about sending information between two parties.
- Information is typically sent as **claims**. This is just a formal way of saying fields and values.
- The possible values are `jwt`, `jwt_vc`, `jwt_vp`, `ldp`, `ldp_vc`, and `ldp_vp`.
- Can you guess what formats our examples have?

What's this format?

- It's a VC
- It has an embedded proof (aka linked data proof `ldp`)
- So it's an `ldp_vc`!

```
{
  "@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/14",
  "issuanceDate": "2010-01-01T19:23:24Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "degree": {
      "type": "BachelorDegree",
      "name": "Bachelor of Science and Arts"
    }
  },
  "credentialStatus": {
    "id": "https://example.edu/status/24",
    "type": "CredentialStatusList2017"
  },
  "proof": {
    "type": "Ed25519Signature2020",
    "created": "2022-02-25T14:58:43Z",
    "verificationMethod": "https://example.edu/issuers/14#key-1",
    "proofPurpose": "assertionMethod",
    "proofValue": "z3BXsFfx1qJ5NsTkKqREjQ3AGh6RAmCwvgu1HcDSzK3P5QEg2TAw8ufk
tJBw8QkAQRciMGyBf5T2AHyRg2w13Uvhp"
  }
}
```

… and this format?

- It's also a VC
- It's a JWT
- So the format is `jwt_vc`!

eyJhbGci0iJFUzI1NiIsInR5cCI6IkpXVCJ9.eyJ2YyI6eyJAY29udGV4dCI6WyJodHRwczovL3
d3dy53My5vcmcvMjAxOC9jcmVkZW50aWFscy92MSIsImh0dHBz0i8vd3d3LnczYy8yMDE4L
2NyZWRlbnRpYWxzL2V4YW1wbGVzL3YxIl0sImlkIjoiaHR0cDovL2V4YW1wbGUuZWR1L2NyZWRl
bnRpYWxzLzM3MzIiLCJ0eXBlIjpbIlZlcmlmaWFibGVDcmVkZW50aWFsIiwiVW5pdmVyc2l0eUR
lZ3JlZUNyZWRlbnRpYWwiXSwiaXNzdWVyIjoiaHR0cHM6Ly9leGFtcGxlLmVkdS9pc3N1ZXJzLz
E0IiwiaXNzdWFuY2VEYXRlIjoiMjAxMC0wMS0wMVQx0ToyMzoyNFoiLCJjcmVkZW50aWFsU3Via
mVjdCI6eyJpZCI6ImRpZDpleGFtcGxl0mViZmViMWY3MTJlYmM2ZjFjMjc2ZTEyZWMyMSIsImRl
Z3JlZSI6eyJ0eXBlIjoiQmFjaGVsb3JEZWdyZWUiLCJuYW1lIjoiQmFjaGVsb3Igb2YgU2NpZW5
jZSBhbmQgQXJ0cyJ9fSwiY3JlZGVudGlhbFN0YXR1cyI6eyJpZCI6Imh0dHBz0i8vZXhhbXBsZS
5lZHUvc3RhdHVzLzI0IiwidHlwZSI6IkNyZWRlbnRpYWxTdGF0dXNMaXN0MjAxNyJ9fSwiaXNzI
joiaHR0cHM6Ly9leGFtcGxlLmVkdS9pc3N1ZXJzLzE0IiwibmJmIjoxMjYyMzczODA0LCJqdGki
0iJodHRw0i8vZXhhbXBsZS5lZHUvY3JlZGVudGlhbHMvMzczMiIsInN1YiI6ImRpZDpleGFtcGx
l0mViZmViMWY3MTJlYmM2ZjFjMjc2ZTEyZWMyMSJ9.YQKQUu_zreDs69AZ8YqpMGHLl9V_tWH4N
S9P9l67J1wWHf0QCyt5hyuA8ckM4seV-1TRbeiHwdJ3VRkDMcwFcg

What about `jwt` and `ldp`?

- There is a subset relationship. Every `jwt_vc` is a `jwt`, but some `jwt` aren't `jwt_vc`.
- So stick in a JWT anything that isn't credential like, and that's what that represents.
- Similar thing to `ldp`! I.e. any JSON that has a proof property, but is not a VC.

Mo' formats

- Note that a format makes sense for *incoming* and *outgoing* data!
- For incoming:
  - `credential_manifest.presentation_definition.format`
- For outgoing:
  - `credential_manifest.format`

I want to learn MORE!

- https://www.youtube.com/watch?v=BxLSSH_EHjo