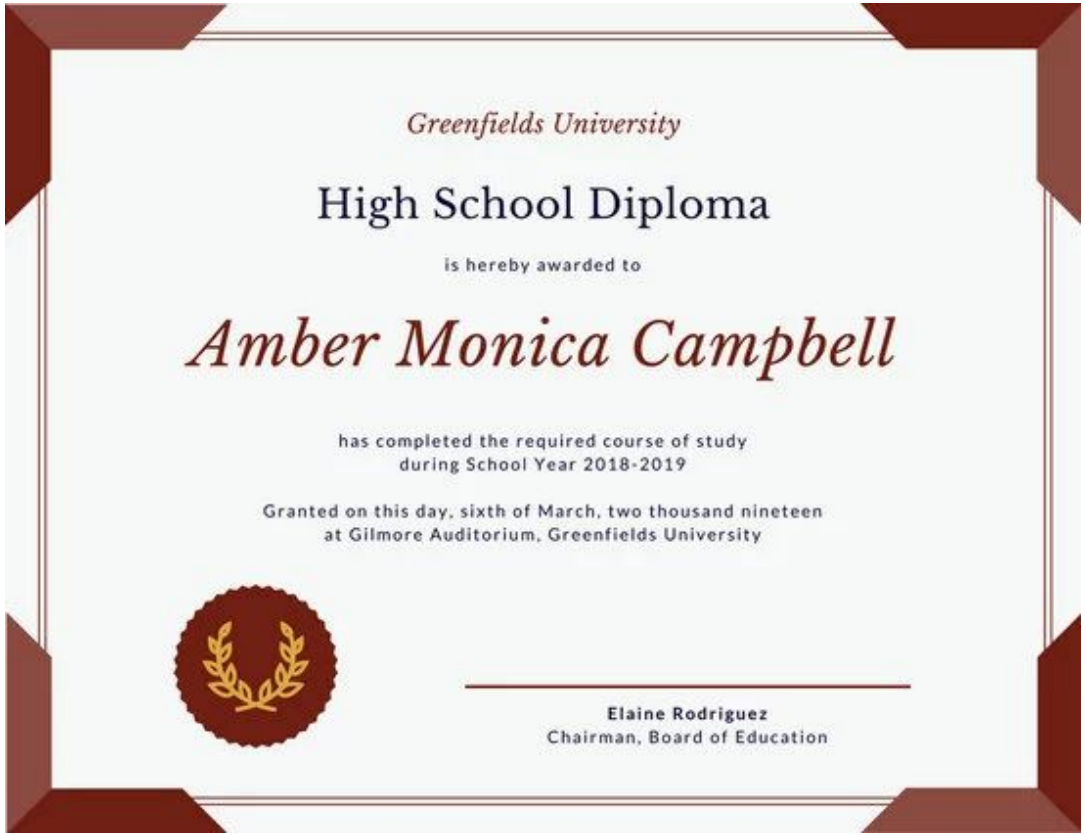
Understanding Verifiable Credentials

Dr. Daniel C. Burnett, PegaSys Blockchain Standards Architect, W3C VCWG Co-chair
W3C Workshop on Strong Authentication & Identity
Redmond, WA, Dec 10-11, 2018

Credentials


Greenfields University

High School Diploma

is hereby awarded to

Amber Monica Campbell

has completed the required course of study
during School Year 2018-2019

Granted on this day, sixth of March, two thousand nineteen
at Gilmore Auditorium, Greenfields University

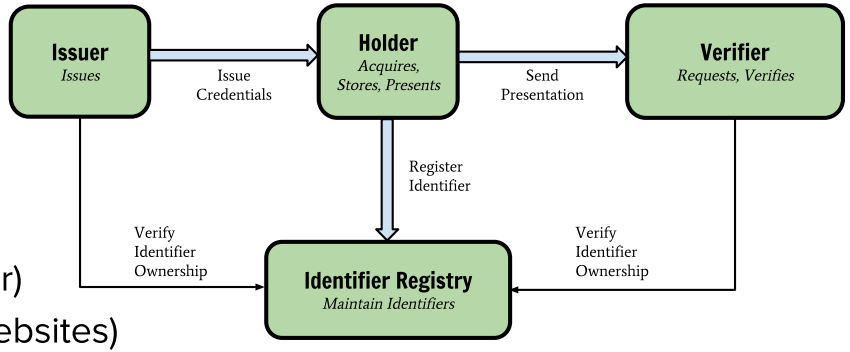
Elaine Rodriguez
Chairman, Board of Education

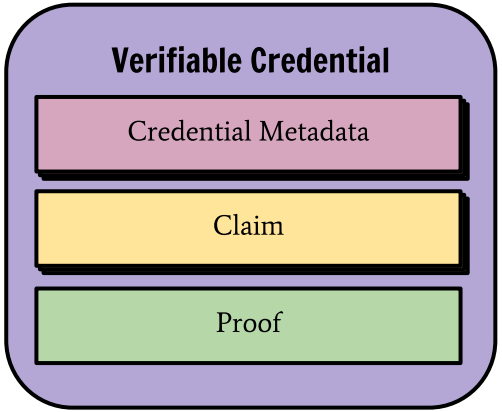
<passport photo>

<driver’s license photo>

(Cryptographically) Verifiable Credentials

- We aim to provide the same thing, but electronically
- A Verifiable Credential is
  - Issued by an *Issuer* (school, corp, govt, ind.)
  - Held by a *Holder* (student, employee, customer)
  - Presented to a *Verifier* (employers, security, websites)
- A Verifiable Credential contains
  - An Identifier
  - Optional metadata
  - One or more claims
  - A proof section
- Identifiers can be cryptographically controlled





Claims & Proofs

- A Claim is
  - One statement about a Subject
- A Claim contains
  - A Subject
  - A Property
  - A Value for the property
- The Proof section contains
  - Signatures over the claims
  - ZKP info (work in progress)

VC Example in JSON-LD syntax

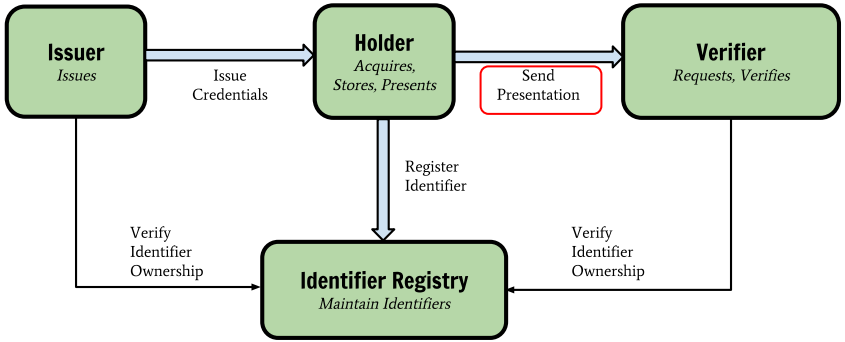
```
{
  "@context": [
    "https://w3.org/2018/credentials/v1",
    "https://example.com/examples/v1"
  ],
  "id": "http://dmv.example.gov/credentials/3732",
  "type": ["VerifiableCredential", "ProofOfAgeCredential"],
  "issuer": "https://dmv.example.gov/issuers/14",
  "issuanceDate": "2010-01-01T19:73:24Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "ageOver": 21
  },
  "proof": { ... }
}
```

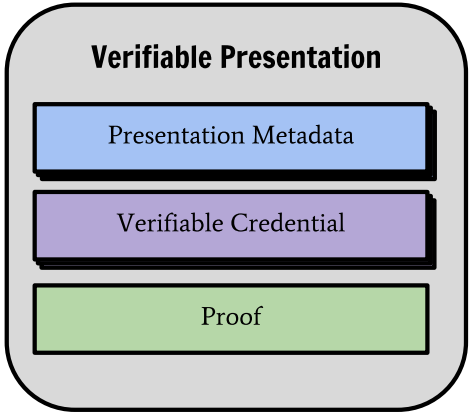
VC - signature-based proof example


```
{ "@context": [...],
  "id": "http://dmv.example.gov/credentials/3732",
  "type": ["VerifiableCredential", "ProofOfAgeCredential"],
  "issuer": "https://dmv.example.gov/issuers/14",
  "issuanceDate": "2010-01-01T19:73:24Z",
  "credentialSubject": {...},
  "proof": {
    "type": "RsaSignature2018",
    "created": "2017-06-18T21:19:10Z",
    "creator": "https://example.com/jdoe/keys/1",
    "nonce": "c0ae1c8e-c7e7-469f-b252-86e6a0e7387e",
    "signatureValue": "BavEll0/I1zpYw8XNi1bgVg/sCneO4Jugez8RwDg/+
      MCRVpjOboDoe4SxxKjkCOvKiCHGDvc4krqi6Z1n0UfqzxGfmatCuFibcC1wps
      PRdW+gGsutPTLzvueMWmFhwYmfIFpbBu95t501+rSLHIEuujM/+PXr9Cky6Ed
      +W3JT24="
  }}
```

Verifiable Presentations

- A Verifiable Presentation is
  - Presented by a Holder to a Verifier
  - Composed from multiple VCs
  - Often from *different Issuers*
  - Often about the *same subject*
- A Verifiable Presentation contains
  - An identifier
  - Optional metadata
  - One or more claims or whole VCs
  - A proof section





Verifiable Credentials are (not)?

Verifiable Credentials allow

- An issuing party to express a statement as a fact, ie “make a claim”
- A holding party to present the statement (in whole or in part) to a third party
- A verifying party to validate the statement hasn’t been tampered with

Verifiable Credentials DON’T

- Represent a “verified truth”

It is the *issuance* of a claim that is verifiable, not the *semantics* of the claim

Standardization: W3C Verifiable Claims Working Group

- **In Scope**
  - Recommend a **data model and syntax(es)** for the expression of verifiable claims, including one or more core vocabularies
  - Create a note specifying one or more of these:
    - How these data models should be used with existing attribute exchange protocols
    - A suggestion that existing protocols be modified
    - A suggestion that a new protocol is required
- **Out of Scope**
  - *Define browser-based APIs for interacting with verifiable claims.* This work may be performed by a future Working Group if there is interest, but is not required for the Working Group to be successful
  - *Define a new protocol for attribute exchange.* This work may be performed by a future Working Group if there is interest, but is not required for the Working Group to be successful
  - *Attempt to address the larger problem of "Identity on the Web/Internet"*
  - Attempt to lead the creation of a specific style of supporting infrastructure, other than a data model and syntax(es), for a verifiable claims ecosystem

VCWG Work Status

- “Verifiable Claims Data Model and Representations” specification
  - FPWD long past, wrapping up ZKP and JWT support
  - Informal reviews already from PING, WAI, others
  - CR expected early 2019
  - Editors’ Draft: https://w3c.github.io/vc-data-model/
  - GitHub: https://github.com/w3c/vc-data-model
- Test Suite
  - Almost all tests written
  - GitHub: https://github.com/w3c/vc-test-suite
- Use cases
  - Editors’ Draft: https://w3c.github.io/vc-use-cases/
  - GitHub: https://github.com/w3c/vc-use-cases

2018 VC Adoption in Commerce (Financial Services)

Deployed Today by:

- Governments
- Banks
- Websites
- DID issuers

Details are W3C Member Confidential

2018 VC Adoption in Commerce (Trade)

Deployed Today for:

- Authorized Importer
- Authorized Exporter
- Certificate of Origin

Details are W3C Member Confidential

Questions?

VCWG Mission and Goals

- It is currently difficult to express claims regarding education qualifications, healthcare data, banking account information, and other sorts of machine-readable personal information that has been verified by a 3rd party on the Web
- VCWG mission is to make expressing and exchanging claims that have been verified by a third party easier and more secure on the Web
- Our charter specifies that education related uses is our first focus but allows that other uses can be addressed such as digital offers, receipts, and loyalty programs and other areas if there is significant industry participation