FIGI Security Clinic

Deploying Decentralised ID Authentication in DFS

Kim Hamilton Duffy
MIT Digital Credentials Consortium

4-5 December 2019
#financialinclusion

Sponsored by

BILL & MELINDA GATES foundation

Organized by

Committee on Payments and Market Infrastructures
BANK FOR INTERNATIONAL SETTLEMENTS

WORLD BANK GROUP

ITU

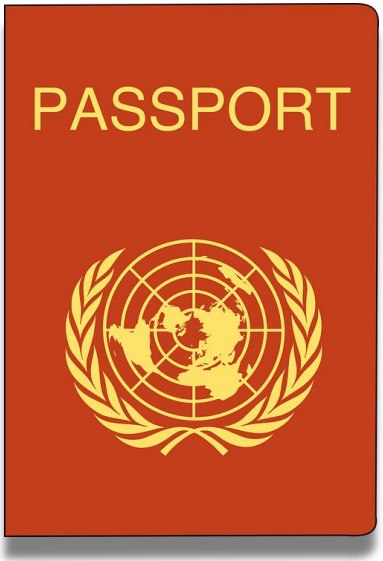
What we'll cover

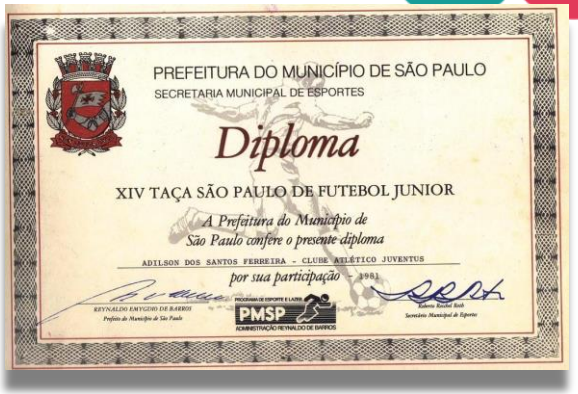
- Intro to Verifiable Credentials
- DIDs and Verifiable Credentials
- Examples

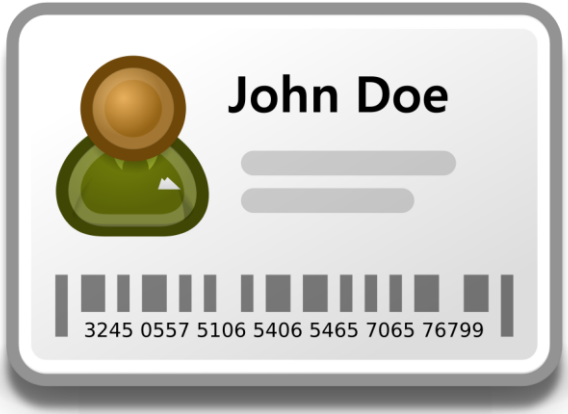
Verifiable Credentials

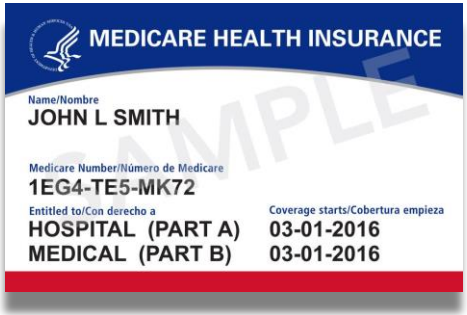
Introduction

What is a Credential?



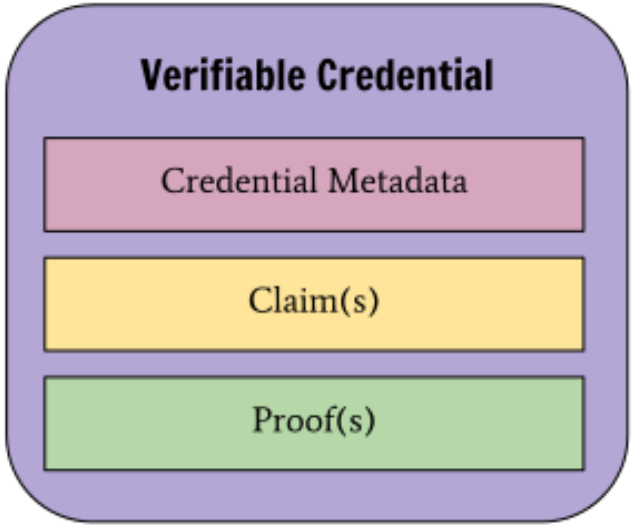






Verifiable Credential

- One or more claims
- Metadata
  - Issuer
  - Expiry date and time
  - Representative image
  - How to verify
  - Revocation mechanism
- Proof
  - Integrity
  - Authenticity



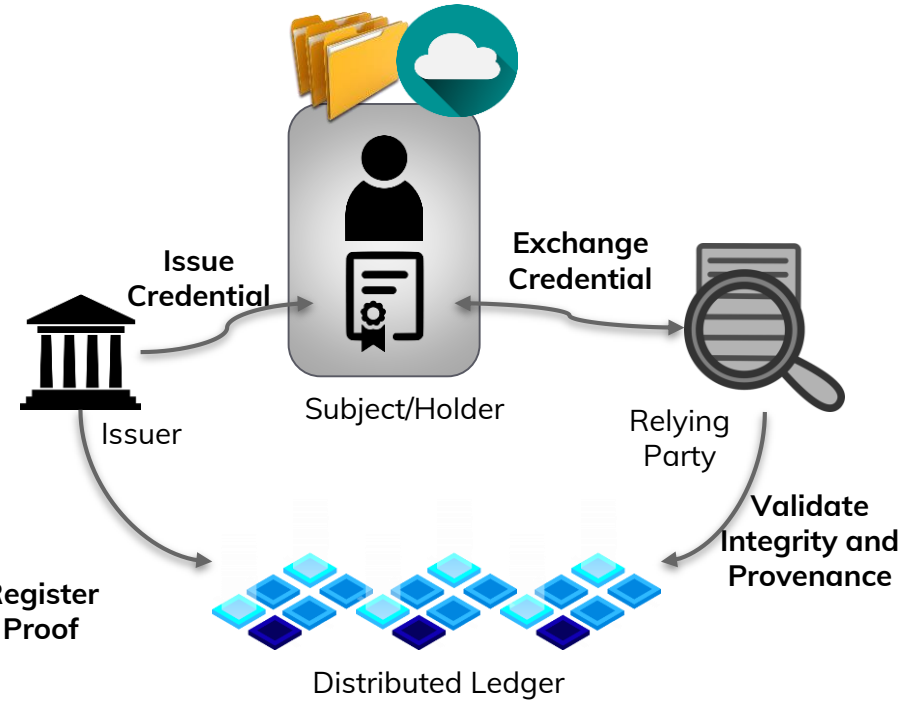
```
{
  "type": ["VerifiableCredential", "UniversityDegreeCredential"],
  "issuer": "did:example:2ec211f712ebc6e1ebfeb6f1c27",
  "credentialSubject": {
          "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
          "degree": {
          "type": "BachelorDegree",
          "name": "Bachelor of Science in Mechanical Engineering"
          }
  },
  "proof": {
          "type": "RsaSignature2018",
          "created": "2017-06-18T21:19:10Z",
          "creator": "did:example:2ec211f712ebc6e1ebfeb6f1c27#keys-1",
          "nonce": "c0ae1c8e-c7e7-469f-b252-86e6a0e7387e",
          "signatureValue":
"BavEll0/I1zpYw8XNi1bgVg/sCneO4Juge...+W3JT24="
  }
}
```

Verifiable Credentials and DIDs

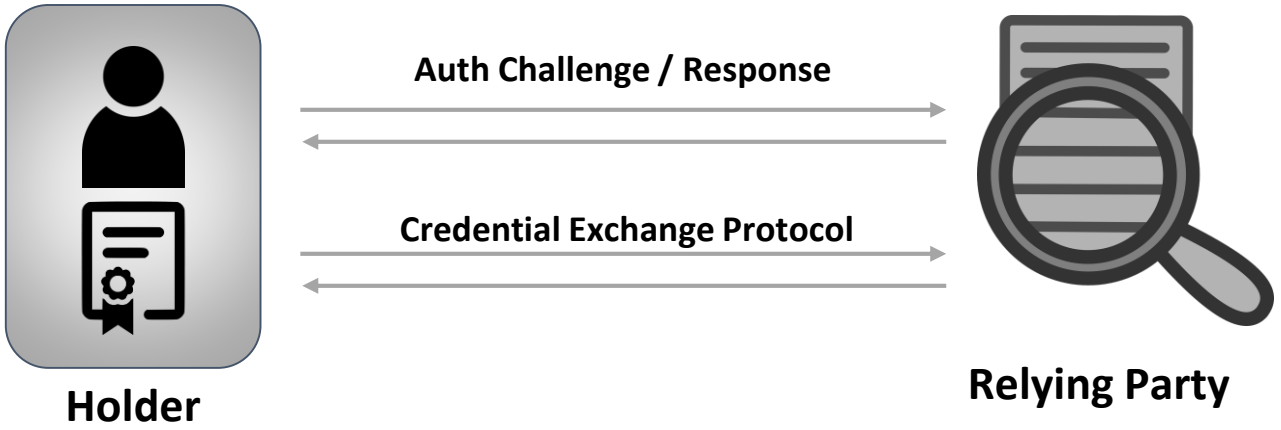
Enabling decentralized trust

with Verifiable Credentials and Decentralized Identifiers

- Individual is center of exchange
- Decentralized storage
  - Controlled by individual
- Decentralized verification



Overview


Auth Challenge / Response
Credential Exchange Protocol
Holder
Relying Party

DIDs resolve to DID Documents

- DID Documents contain:
  - Verification methods
  - Service endpoints for interacting with the DID subject
- Examples:
  - Authentication
  - Requesting a digital signature on a document

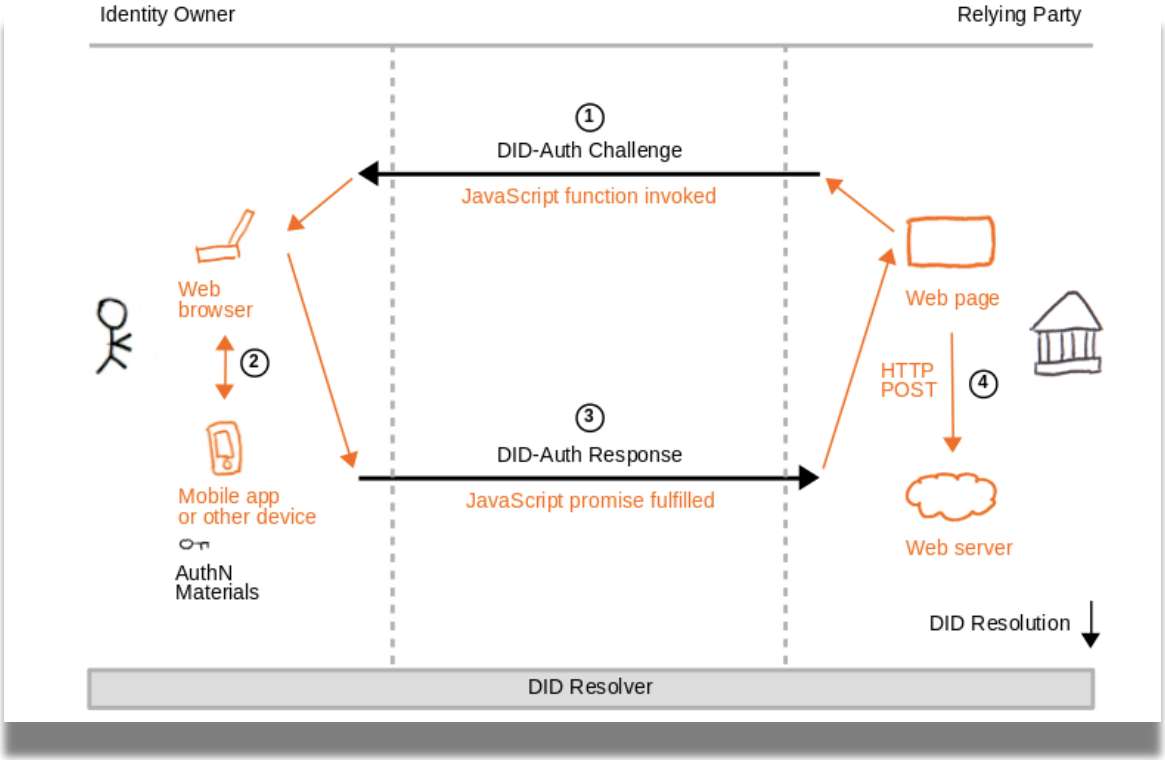
Example DID Document

```
{
  "@context": "https://w3id.org/future-method/v1",
  "id": "did:example:123456789abcdefghi",
  "publicKey": [],
  "authentication": [+],
  "service": [+]
}
```

```
{
  "id": "did:example:123456789abcdefghi#keys-2",
  "type": "Ed25519VerificationKey2018",
  "controller": "did:example:123456789abcdefghi",
  "publicKeyBase58":
"H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
}
```

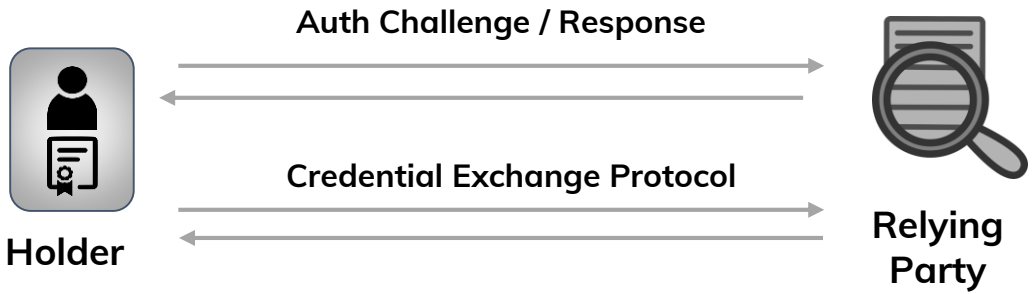
```
{
  "id": "did:example:123456789abcdefghi#oidc",
  "type": "OpenIdConnectVersion1.0Service",
  "serviceEndpoint": "https://openid.example.com/"
}, {
  "id": "did:example:123456789abcdefghi#hub",
  "type": "HubService",
  "serviceEndpoint":
"https://hub.example.com/.identity/did:example:0123456789abcdef/"
}
```

DID Auth with WebAuthn



DID Auth and Verifiable Credentials Relationships

1. DID Auth and Verifiable Credentials exchange are separate
2. Verifiable Credentials exchange is an extension to (or part of) DID Auth
3. DID Auth is a certain kind of Verifiable Credential



Examples

Verifiable Credentials and Decentralized Identifiers

Traditional Learner/Worker Records

- Issuer or Central Authority is needed for verification
  - Bottleneck
  - Failure point
  - Lack of Agency and Control over our data
- Questions
  - How to bootstrap into the system?
  - Leverage existing trust networks?
  - Establish a history?

Learner/Worker Records

- Credential Fraud
  - More than 50,000 PhDs are purchased from diploma mills every year
  - Exceeds the quantity *legitimately* awarded
- Cost to employers
- Cost to learners

  ...who don't necessarily know it's a diploma mill

Digital Academic Credentials

Benefits

- Can cryptographically prove control of credentials
- Layered approach
- Key lifecycle is a first-class concern
- Robust privacy/security spectrum

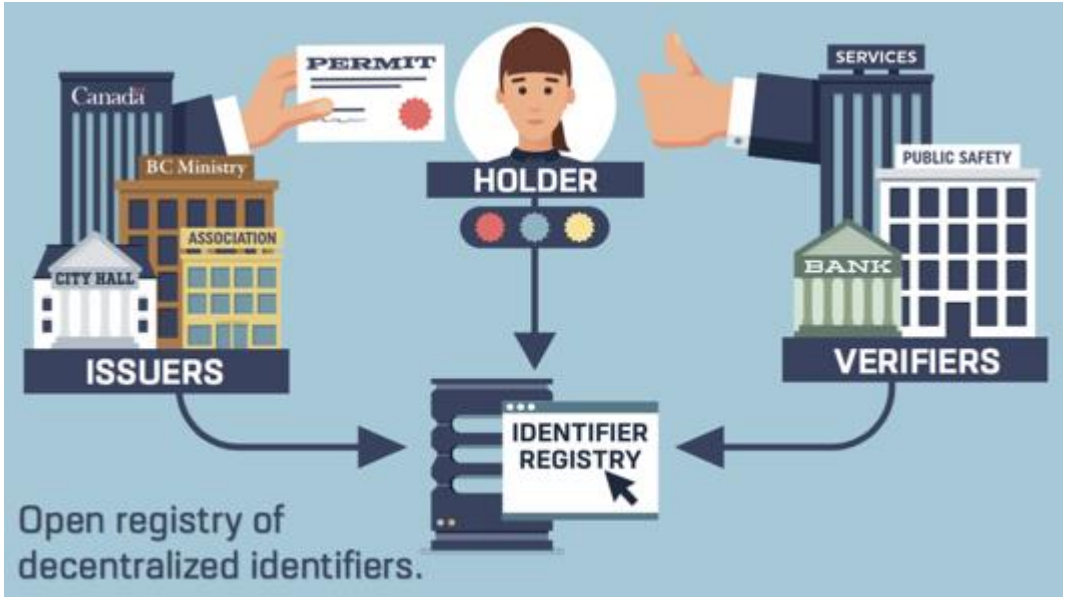
Additional Benefits

- Fraud reduction
- Verifiable history and audit trail
- Individuals control their own records
- Verifiable w/out central authority
- Bootstrap individuals with non-traditional backgrounds

British Columbia VON Project

VON Use Cases

- Streamlined processes for small businesses
- Safe workplace credentials
- KYC




WILEY
Publishers Since 1807
Lumina FOUNDATION
STANFORD
Publishing
Credly
Education
Georgetown University
aetna
workday.
Workforce
Government of Canada
ATB Financial
ups
Insurance
IBM
Financial Services
CULedger
GS1 US
Trade and Logistics
BRITISH COLUMBIA
airbnb
Disney
THOMSON REUTERS
FedEx

Proof of Concept	Use Case	Who's Involved
VON	Business Credentials	British Columbia Government
CU Ledger	Credit Union Banking Security	Sovrin + Credit Union National Association
Building Blocks	Food Aid	World Food Programme (Syrian Refugee Aid)
Dutch Digital ID	Digital ID	TU Delft + Dutch Gov + Others
Walmart Supply Chain	Food Supply Tracking	Walmart + Hyperledger Fabric
TradeLens Shipping	Shipping + Tracking	IBM + Maersk

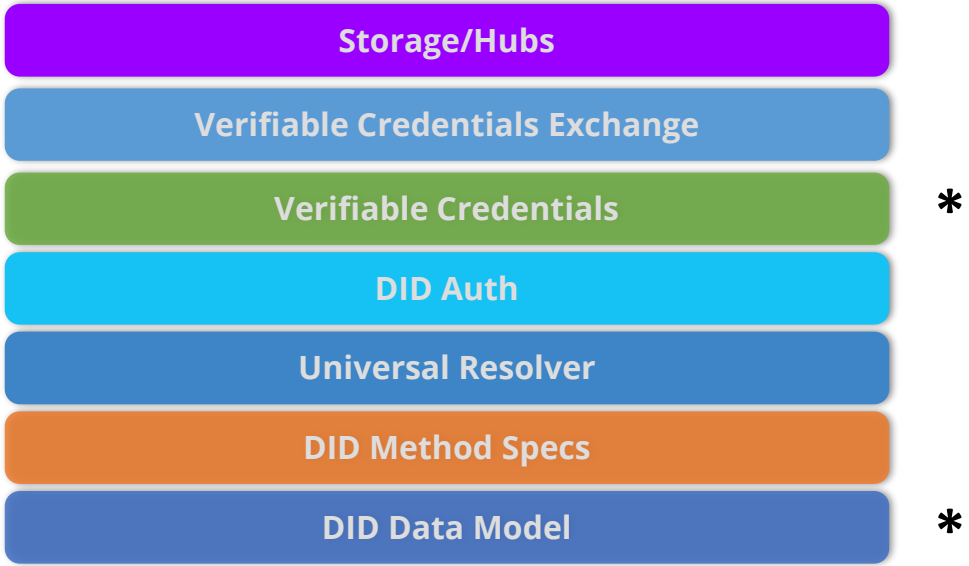
US Government Support

- Improve Supply Chain Management
- Combat Counterfeit Goods

To that end, DHS S&T is pursuing two broad courses of action to encourage a more open and inclusive future for blockchain technology:

1. Support development of globally available specifications (precursor to standards) that are open, royalty free, and free to implement to ensure interoperability across systems while ensuring there is no vendor lock-in.
    a. Decentralized Identifiers (DIDs) via World Wide Web Consortium (W3C) Standardization Process
    b. Verifiable Claims Data Model via W3C Standardization Process
    c. Decentralized Key Management System via TBD (Potentially OASIS)
2. Actively work with and support our DHS Component customers, such as CBP, to understand their potential use cases for blockchain and help them achieve their outcomes with the needed R&D expertise and technologies.

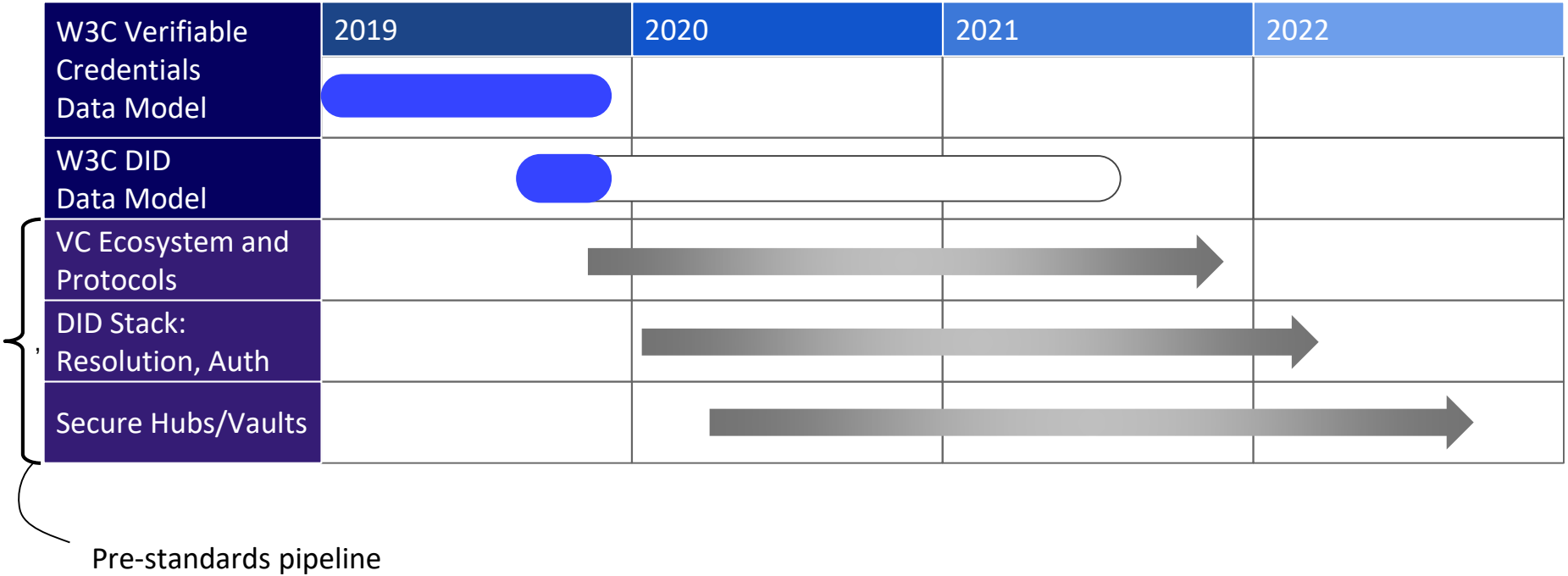
Standards and Specifications



*

*

Standardization Track



References

- DHS Science and Technology Directorate's Testimony before the US House of Representatives, May 8, 2018
  - https://www.dhs.gov/news/2018/05/08/written-testimony-st-house-science-space-technology-subcommittee-oversight-and
- DID Auth
  - https://github.com/WebOfTrustInfo/rwot6-santabarbara/blob/master/final-documents/did-auth.md
  - https://ssimeetup.org/introduction-did-auth-markus-sabadello-webinar-10/
- https://www.wired.com/story/billion-records-exposed-online/

Thank you

Kim Hamilton Duffy
Architect
MIT Digital Credentials Consortium

@kimdhamilton
kimhd@mit.edu