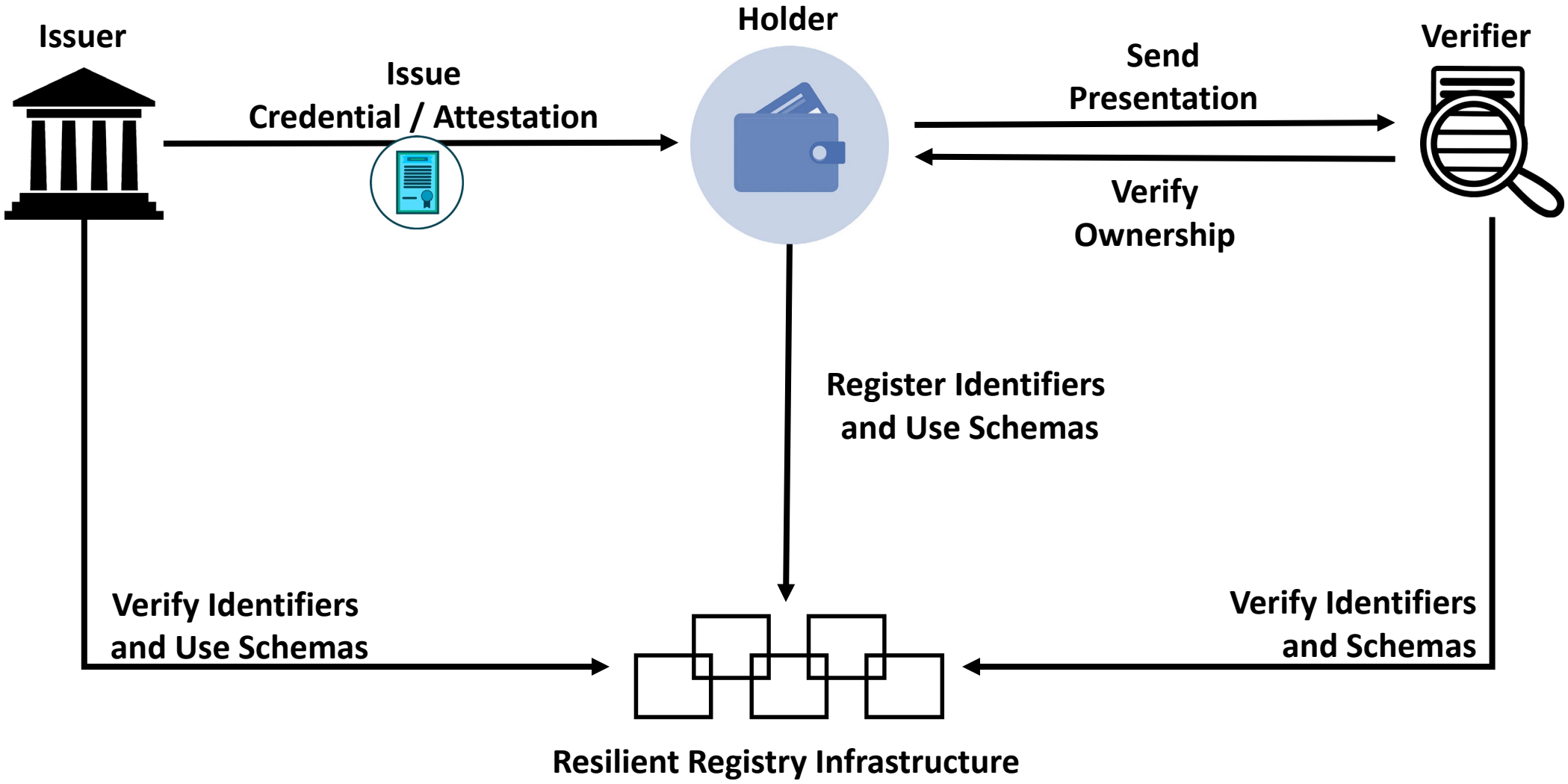
“Absorb what is useful, Discard what is not,
Add what is uniquely your own.”

-- Bruce Lee

ANIL JOHN

Digitally signed by ANIL JOHN
Date: 2021.02.27 13:23:25 -05'00'

# Attestation Issuance & Verification Model



# Real Interoperability REQUIRES Constraints!

## JSON-LD

- Ensures semantic clarity between issuers and verifiers
- Disambiguation between attributes found in different credentials issued by different issuers
- Ability to support language translation on the fly via language maps
- Extensibility model based on RDF
- Future-friendly to AI/ML based analytics i.e., operate on information and not just data

## Selective Disclosure w/ Linked Data Signatures

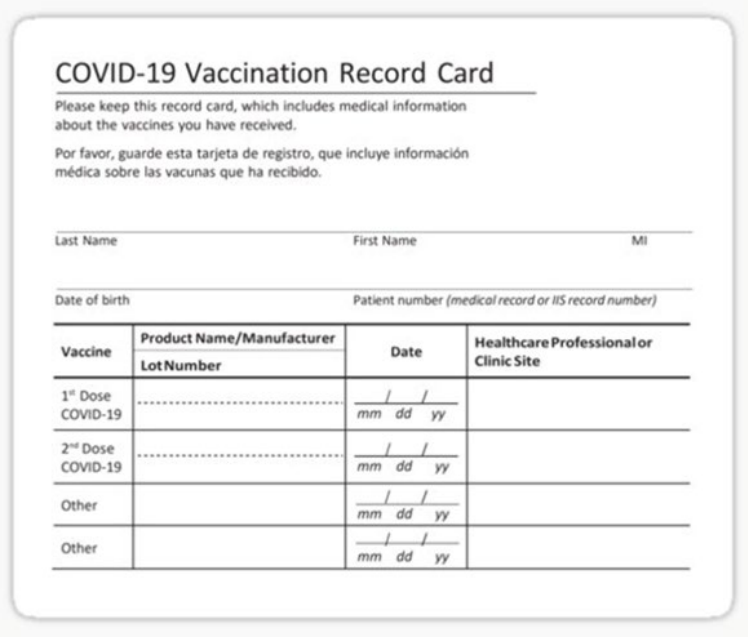
- Interoperable with existing schema technologies via JSON-LD
- Not locked to a specific Ledger
- BBS+ Signatures, which are LD Signatures, are based on pairing-based cryptography*
  - Currently using BLS12-381 curve
- Attributes from credentials issued by different issuers can be combined into a single privacy preserving credential presentation…
- … while fully supporting consent-based selective disclosure

## Refresh & Revocation

- Support for refreshing verifiable credentials that is available to the holder of the credential only – and not the verifier -- to ensure control by and consent of the holder/subject of the credential
- Support for revoking verifiable credentials in a manner that does not compromise holder privacy and mitigates any “phone home” problems

* https://nvlpubs.nist.gov/nistpubs/jres/120/jres.120.002.pdf

# COVID-19 Vaccination Record as a W3C VC



COVID-19 Vaccination Record Card

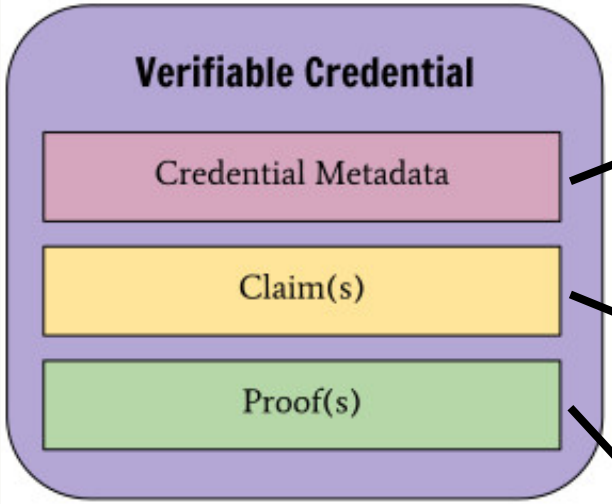
Please keep this record card, which includes medical information about the vaccines you have received.

Por favor, guarde esta tarjeta de registro, que incluye información médica sobre las vacunas que ha recibido.

Last Name | First Name | MI

Date of birth | Patient number *(medical record or IIS record number)*

| Vaccine | Product Name/Manufacturer<br>Lot Number | Date | Healthcare Professional or Clinic Site |
|---|---|---|---|
| 1st Dose COVID-19 | | mm dd yy | |
| 2nd Dose COVID-19 | | mm dd yy | |
| Other | | mm dd yy | |
| Other | | mm dd yy | |




```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://w3id.org/vc-revocation-list-2020/v1",
    "https://w3id.org/vaccination/v1",
    "https://www.uspha.gov/vaxcert/v1"
  ],
  // specify the identifier for the credential
  "id": "https://issuer.uspha.gov/vaxcert/83627465",
  // the credential type which declares what data to expect in the credential
  "type": ["VerifiableCredential", "VaccinationCertificate"],
  // the name of the credential
  "name": "COVID-19 Vaccination Record",
  "description": "COVID-19 Vaccination Record",
  // the entity that issued the credential
  "issuer": "did:web:issuer.uspha.gov:vaxcert",
  // alternate identifier used by the Issuer of the credential
  "identifier": "83627465",
  // when the credential was issued
  "issuanceDate": "2019-12-03T12:19:52Z",
  // when the credential expires
  "expirationDate": "2028-02-26T00:00:00Z",
  // discover current status of the credential
  "credentialStatus": {
    "id": "https://issuer.uspha.gov/vaxcert/status/3#94567",
    "type": "RevocationList2020Status",
    "revocationListIndex": "94567",
    "revocationListCredential": "https://issuer.uspha.gov/vaxcert/status/3"
  },
  // claims about the subject of the credential
  "credentialSubject": {
    "type": "VaccinationEvent",
    "batchNumber": "1183738569",
    "administeringCentre": "FEMA",
    "healthProfessional": "UMD",
    "countryOfVaccination": "US",
    "recipient": {
      "type": "VaccineRecipient",
      "givenName": "JOHN",
      "familyName": "SMITH",
      "gender": "Male",
      "birthDate": "1958-07-17"
    },
    "vaccine": {
      "type": "Vaccine",
      "disease": "COVID-19",
      "atcCode": "J07BX03",
      "medicinalProductName": "COVID-19 Vaccine Moderna",
      "marketingAuthorizationHolder": "Moderna Biotech"
    }
  },
  // digital proof to make the credential tamper-evident
  "proof": {
    // the cryptographic signature suite used to generate signature
    "type": "Ed25519Signature2018",
    // the date the signature was created
    "created": "2020-01-30T03:32:15Z",
    // purpose of the proof
    "proofPurpose": "assertionMethod",
    // the identifier of the public key that can verify the signature
    "verificationMethod": "did:web:issuer.uspha.gov:vaxcert#public-key-1",
    // the digital signature value
    "jws": "eyJhbGciOiJFZERTQSIsI...wRG2fNmAx60Vi4Ag"
  }
}
```

https://www.w3.org/TR/vc-data-model/
https://w3c.github.io/did-core/
https://w3id.org/vaccination

# COVID-19 VaxCert as a W3C VC


```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://w3id.org/vc-revocation-list-2020/v1",
    "https://w3id.org/vaccination/v1",
    "https://www.uspha.gov/vaxcert/v1"
  ],
  // specify the identifier for the credential
  "id": "https://issuer.uspha.gov/vaxcert/83627465",
  // the credential type which declares what data to expect in the credential
  "type": ["VerifiableCredential", "VaccinationCertificate"],
  // the name of the credential
  "name": "COVID-19 Vaccination Record",
  "description": "COVID-19 Vaccination Record",
  // the entity that issued the credential
  "issuer": "did:web:issuer.uspha.gov:vaxcert",
  // alternate identifier used by the Issuer of the credential
  "identifier": "83627465",
  // when the credential was issued
  "issuanceDate": "2019-12-03T12:19:52Z",
  // when the credential expires
  "expirationDate": "2028-02-26T00:00:00Z",
  // discover current status of the credential
  "credentialStatus": {
    "id": "https://issuer.uspha.gov/vaxcert/status/3#94567",
    "type": "RevocationList2020Status",
    "revocationListIndex": "94567",
    "revocationListCredential": "https://issuer.uspha.gov/vaxcert/status/3"
  },
  // claims about the subject of the credential
  "credentialSubject": {
    "type": "VaccinationEvent",
    "batchNumber": "1183738569",
    "administeringCentre": "FEMA",
    "healthProfessional": "UMD",
    "countryOfVaccination": "US",
    "recipient": {
      "type": "VaccineRecipient",
      "givenName": "JOHN",
      "familyName": "SMITH",
      "gender": "Male",
      "birthDate": "1958-07-17"
    },
    "vaccine": {
      "type": "Vaccine",
      "disease": "COVID-19",
      "atcCode": "J07BX03",
      "medicinalProductName": "COVID-19 Vaccine Moderna",
      "marketingAuthorizationHolder": "Moderna Biotech"
    }
  },
  // digital proof to make the credential tamper-evident
  "proof": {
    // the cryptographic signature suite used to generate signature
    "type": "Ed25519Signature2018",
    // the date the signature was created
    "created": "2020-01-30T03:32:15Z",
    // purpose of the proof
    "proofPurpose": "assertionMethod",
    // the identifier of the public key that can verify the signature
    "verificationMethod": "did:web:issuer.uspha.gov:vaxcert#public-key-1",
    // the digital signature value
    "jws": "eyJhbGciOiJFZERTQSIsI...wRG2fNmAx60Vi4Ag"
  }
}
```


Who is the **Issuer (Trust Anchor)** of this credential?

What is the **current status** of this credential?

Who is the **Subject** of the credential?

What does the Issuer
**assert about** the Subject?

How can a Verifier find the Public Key
of the Issuer to **Verify the Digital Signature**
that ensures the integrity and provenance
of the credential?

# VaxCert's Issuer DID resolves to a DID document

did:web:issuer.uspha.gov:vaxcert resolves to a "DID Document" at https://issuer.uspha.gov/vaxcert/did.json

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  // the DID subject
  "id": "did:web:issuer.uspha.gov:vaxcert",
  // the controller authorized to make changes to the DID document
  "controller": "did:web:issuer.uspha.gov:vaxcert",
  // public key(s) associated with the DID subject
  "publicKey": [
    {
      "id": "did:web:issuer.uspha.gov:vaxcert#public-key-1",
      "type": "Ed25519VerificationKey2018",
      "controller": "did:web:issuer.uspha.gov:vaxcert",
      "expires": "2022-02-08T16:02:20Z",
      "publicKeyBase58" : "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
    },
    {
      "id": "did:web:issuer.uspha.gov:vaxcert#public-key-2",
      "type": "Bls12381G1Key2020",
      "controller": "did:web:issuer.uspha.gov:vaxcert",
      "publicKeyBase58": "7cJGQwV5XyzUjJEzY5doVhv62Qqou6qW7GUywgyeDCobiXjN8CnQ7wpWBrGR"
    },
    {
      "id": "did:web:issuer.uspha.gov:vaxcert#public-key-3",
      "type": "JsonWebKey2020",
      "controller": "did:web:issuer.uspha.gov:vaxcert",
      "publicKeyJwk": {
        "kty": "OKP",
        "crv": "Ed25519",
        "x": "VCpo2LMLhn6iWku8MKvSLg2ZAoC-nlOyPVQaO3FxVeQ"
      }
    }
  ],
  // the key used to assert statements as did:web:issuer.uspha.gov:vaxcert
   "assertionMethod": [
    "did:web:issuer.uspha.gov:vaxcert#public-key-1"
  ],
  // the key used to assert statements as did:web:issuer.uspha.gov:vaxcert
  // with selective disclosure support using BBS+ Signatures
   "assertionMethod": [
    "did:web:issuer.uspha.gov:vaxcert#public-key-2"
  ],
  // the key used to authenticate as did:web:issuer.uspha.gov:vaxcert
   "authentication": [
    "did:web:issuer.uspha.gov:vaxcert#public-key-3"
  ],
}
```

The unique identifier (DID) of the Issuer

The public key(s) associated with the Issuer

#public-key-1 to be used to verify digital signatures

#public-key-2 to be used verify selective disclosures

#public-key-3 to be used for authentication

# A Verifier’s Perspective

**Identify the Issuer of the credential and find its public key(s)**

- Find the Issuer's DID
- Resolve Issuer’s DID to DID document
- Pick up the public key used for “assertionMethod” from DID document associated with the Issuer’s DID

**Process the digital proof and credential status check**

- Is the digital signature valid?
- Is the credential valid? i.e. it has not been revoked

**Process Credential Subject Information**

- Find the Subject’s DID in the credential
- Ensure that the Subject has control over its DID
- Process claims about the Subject asserted by the Issuer in the credential