SILICON VALLEY
INNOVATION PROGRAM

Homeland Security
Science and Technology

Interoperability as a First Principle

Encouraging Innovation, Ensuring Diversity, and Enabling a Global Ecosystem

ANIL JOHN | TECHNICAL DIRECTOR

AGENDA

- Introductions
- The DHS standards-based interoperability back-story
- Pivot from Blockchain R&D to enabling standards-based interoperability to support Digital Trade Credentials
- An ecosystem approach to solving operational problems
  - Fund, champion, require and utilize open standards
  - Conduct proof-of-concepts for implementation insights
  - Minimizing risk in operational deployments
- A technical answer to an ICAO use case question
  - Can these open, flexible, global interoperability standards be applied to cross border air cargo digitization?

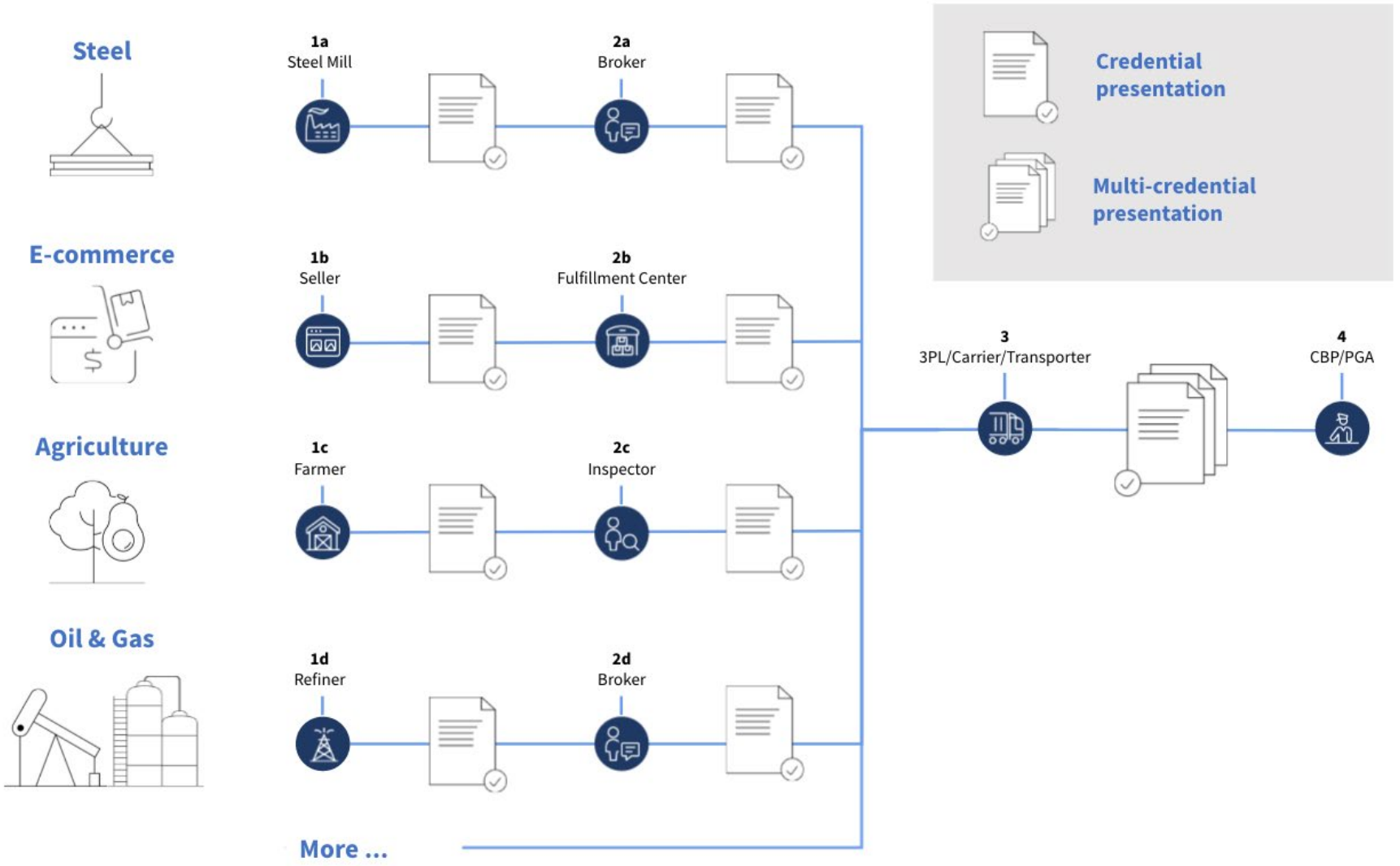
DHS Missions

1. Counter Terrorism and Homeland Security Threats
2. Secure U.S. Borders and Approaches
3. Secure Cyberspace and Critical Infrastructure
4. Preserve and Uphold the Nation's Prosperity and Economic Security
5. Strengthen Preparedness and Resilience
6. Champion the DHS Workforce and Strengthen the Department

DHS **Science & Technology Directorate (S&T)** is the arm of the Department that develops novel and unique technological solutions to protect the Homeland

- Science Advisor to the Department
- Conducts applied research and advanced development as well as testing and evaluation
- Partners with innovation communities globally to adapt, develop and harness cutting-edge technologies via its **Silicon Valley Innovation Program (SVIP)**

Start at the Finish Line -- Global Interoperability of Trade Credentials



- No expectation that all links in the supply chain use the same technology platform or vendor
- All links in the supply chain free to choose the technology stack / platform / vendor of their choice
- Interfaces between systems based on global, open, royalty free and free to use data and protocol standards that ensure multi-platform, multi-vendor, cross-border interoperability

Rewind the Clock to 6 Years Ago -- Is Blockchain Relevant to DHS?

Security and Privacy

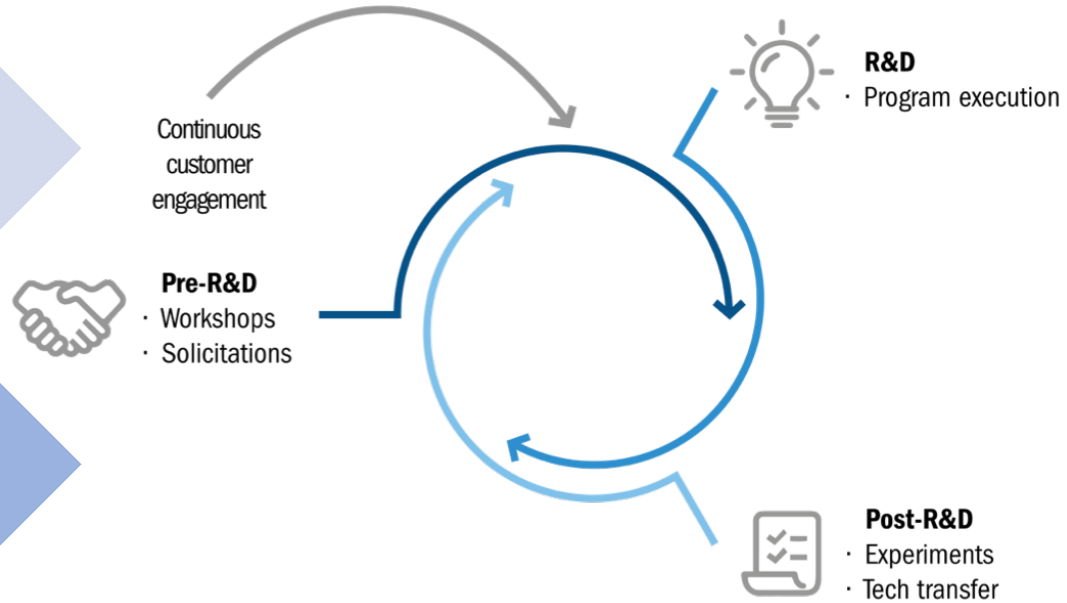
- Confidentiality, Integrity, Availability …
- Pseudonymous Operations, Selective Disclosure …

Integration Approaches & Gain/Pain

- Data Sharing Implications, On Chain vs. Off-Chain
- Storage of Information vs. Validation of Information

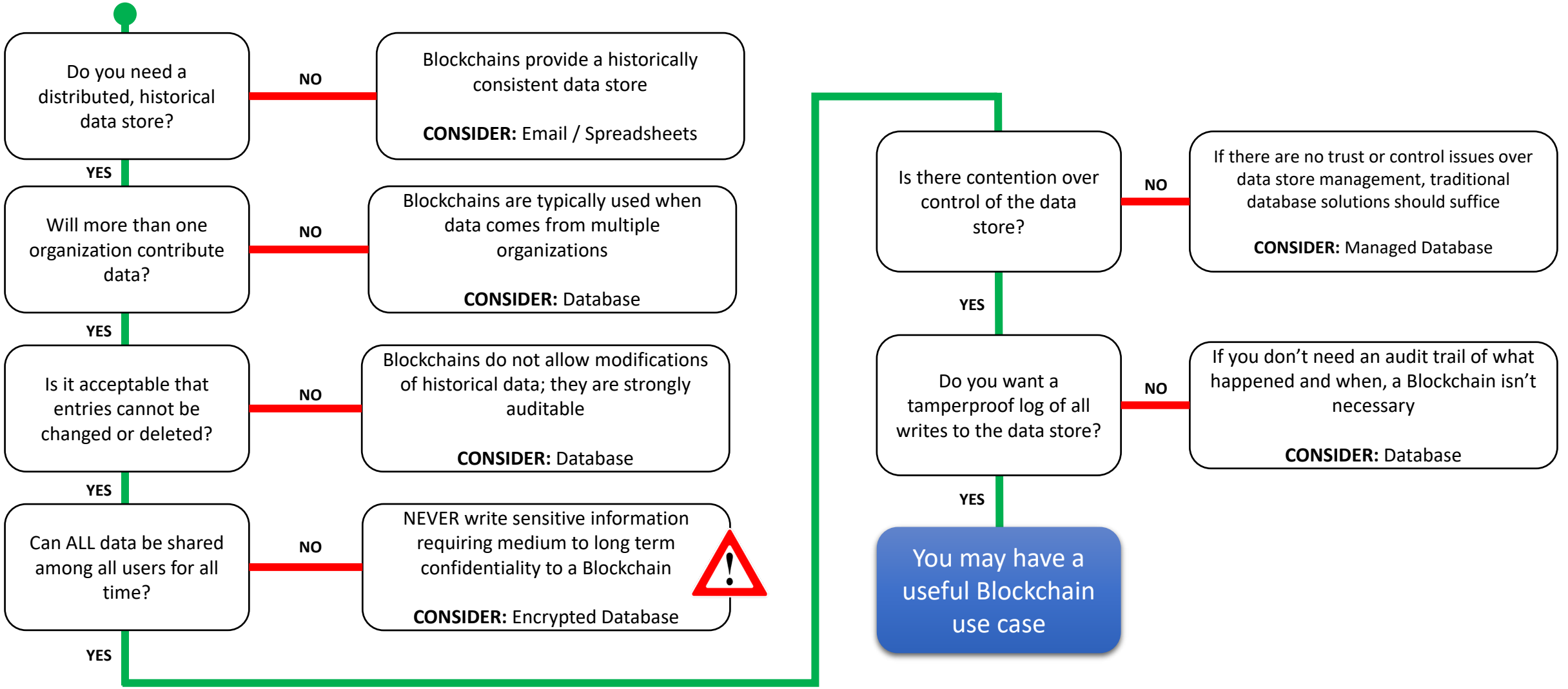
Digital Currency Forensics

- Anonymous Currencies
- Anonymous Networks



Proof of Concept → Pilot Deployment → Operational Deployment

Most Organizations Don’t Need A Blockchain



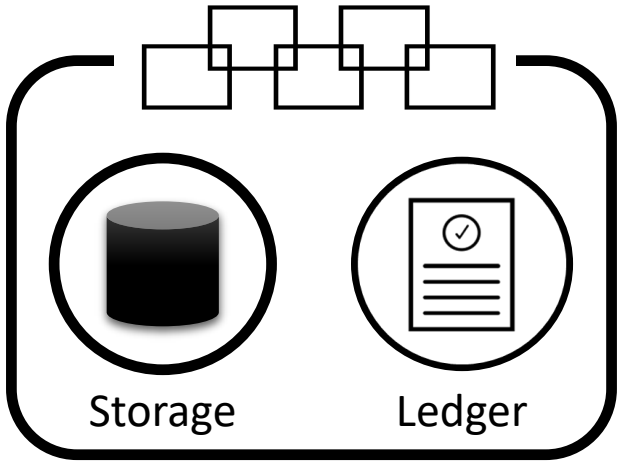
Make Blockchain Useful …

… By Abstracting it Away!

… by layering over it a set of openly developed global standards

… and application programming interfaces (APIs)

… that ensure choice and cross-platform interoperability!



Resilient Registry Infrastructure

Strategic Approach to Ensure a Competitive, Interoperable Marketplace of Solution Providers

1. Help develop and champion interoperability standards and specifications that are patent free, royalty free and free to implement (2016)
2. Invest in business-driven proof-of-concepts to identify scalable integration architectures and determine adoption Gain/Pain ratio (2017)
3. Motivate and shape innovative and potentially risky product development via the S&T Silicon Valley Innovation Program (SVIP) to meet mission challenges (2018)

Develop, Refine, Use and Champion Global Standards to Ensure Interoperability

W3C Verifiable Credentials

- A set of claims made by an issuer about a subject in a manner that is:
  - Tamper evident
  - Cryptographically verifiable
- Digital version of physical credentials/attestations
  - Driver's Licenses
  - Passports
  - Certificates of Origin
  - …

Verifiable Credentials Data Model 1.0
Expressing verifiable information on the Web

W3C Recommendation 19 November 2019

W3C Decentralized Identifiers

- Globally Unique Identifier without the need for a central registration authority
  - Immutable over time
  - Globally resolvable
  - Privacy respecting
  - Cryptographically verifiable

Decentralized Identifiers (DIDs) v1.0
Core architecture, data model, and representations

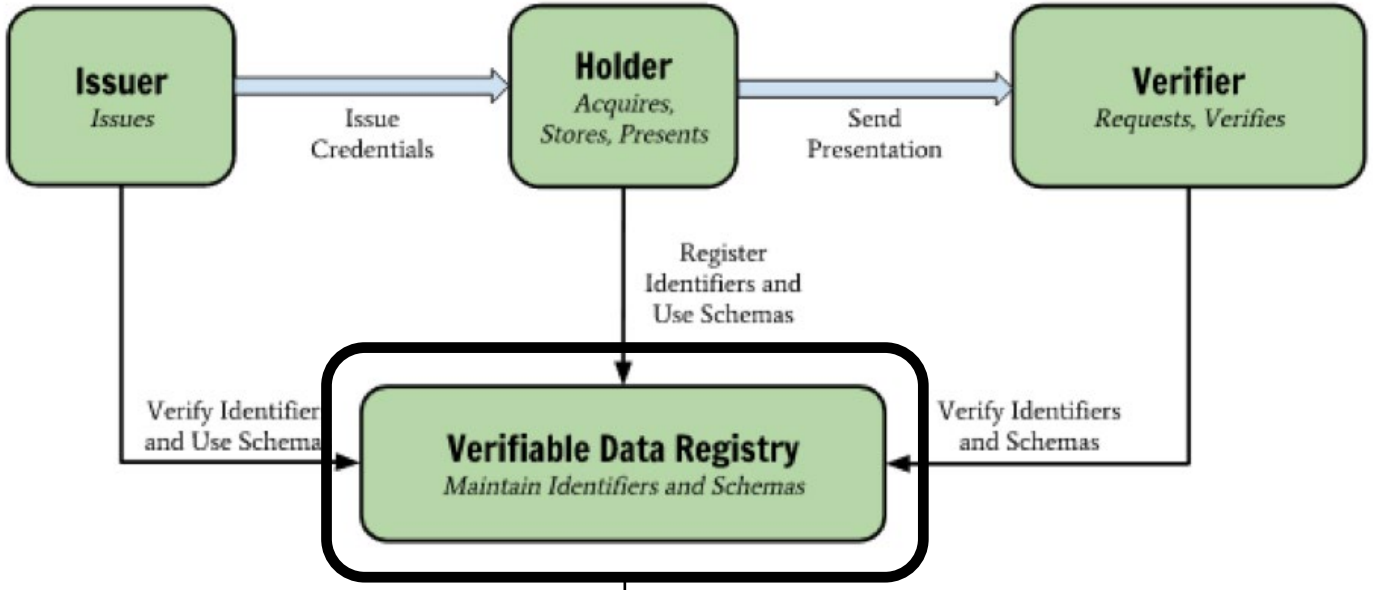
W3C Proposed Recommendation 03 August 2021

Privacy and Credential Lifecycle Management

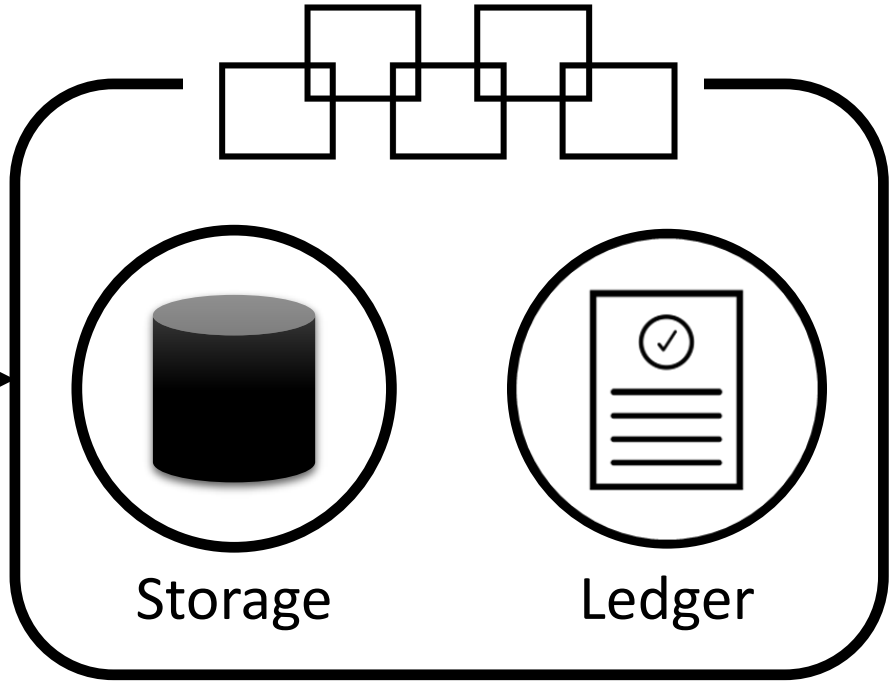
- Tackling the hard challenges of scalable implementation
  - Confidential Storage
  - Data Portability
  - Selective Disclosure
  - Revocation with Herd Privacy
- Path to Standardization via IETF & W3C

Portions of the work on this specification have been funded by the United States Department of Homeland Security's Science and Technology Directorate under contracts HSHQDC-16-R00012-H-SB2016-1-002 and HSHQDC-17-C-00019. The content of this specification does not necessarily reflect the position or the policy of the U.S. Government and no official endorsement should be inferred.

In DHS trusted implementations, if a blockchain / DLT / DAG is used*, the ….



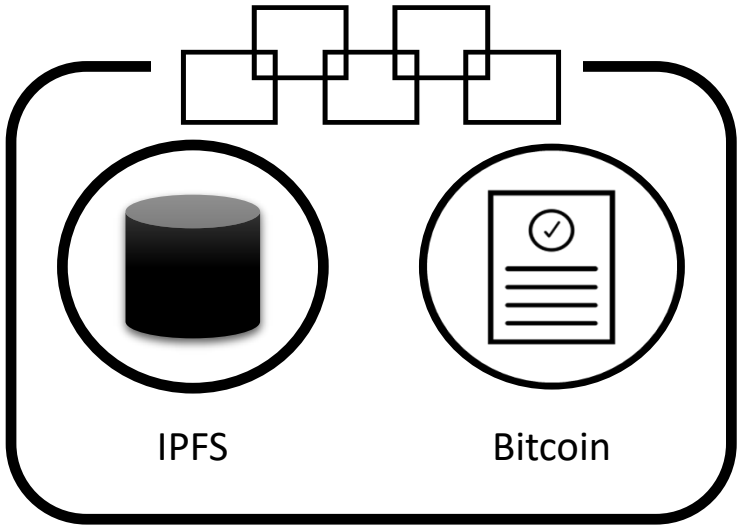
.. MUST support a …



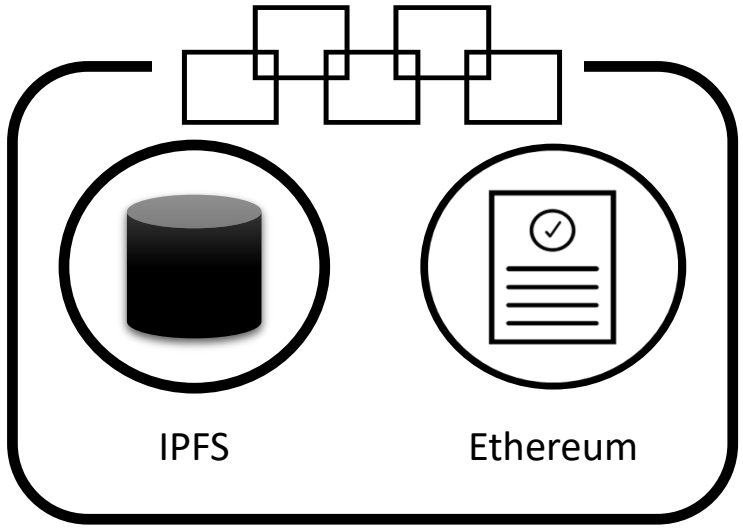
Resilient Registry Infrastructure

* W3C VC/DID standards/specifications do not require, but do support, the use of blockchains, DLTs or DAGs when implementing a Verifiable Data Registry

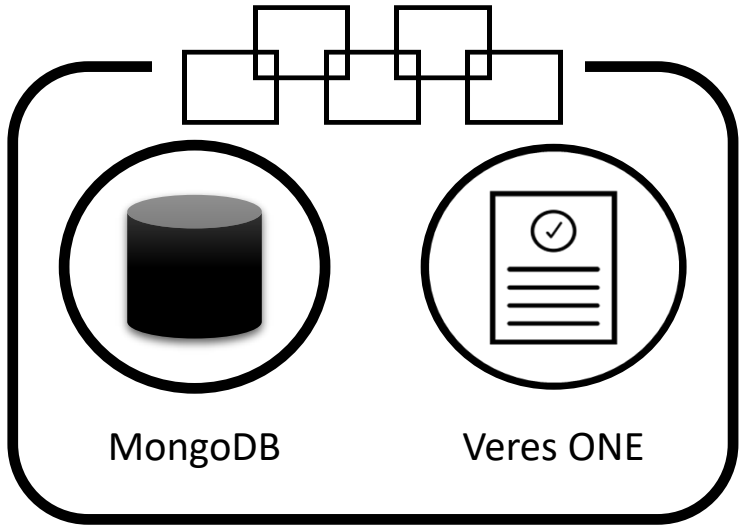
Global support ….



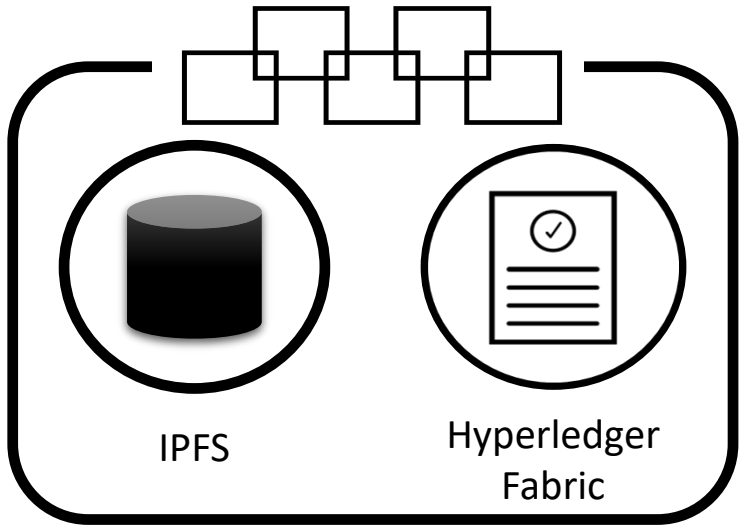
did:ion



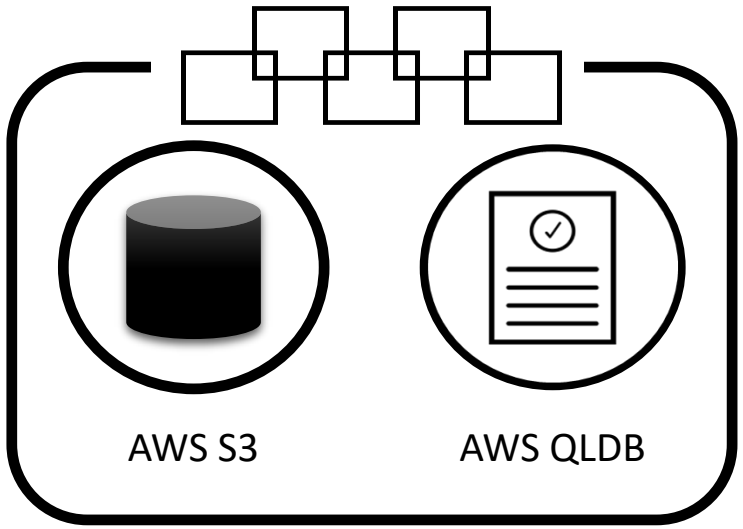
did:elem



did:v1



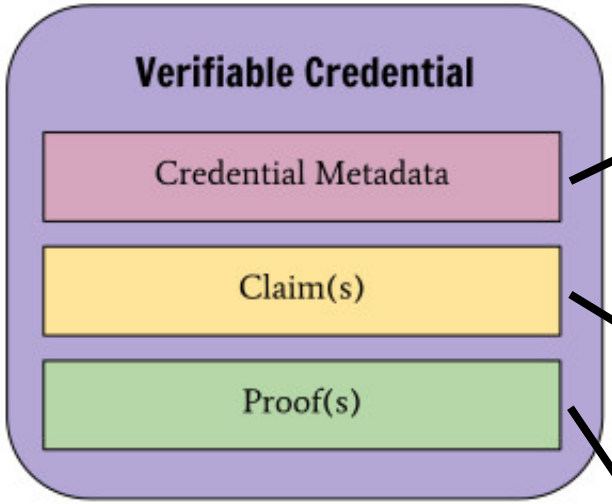
did:trustbloc



did:photon

More ….

A Concrete (Real) Example of Using W3C Standards Digitizing the US Permanent Resident Card




```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://w3id.org/vc-revocation-list-2020/v1",
    "https://w3id.org/citizenship/v1",
    "https://www.uscis.gov/prc/digital/v1"
  ],
  // specify the identifier for the credential
  "id": "https://vc-issuer.uscis.gov/credential/prc/83627465",
  // the credential type which declares what data to expect in the credential
  "type": ["VerifiableCredential", "PermanentResidentCard"],
  // the entity that issued the credential
  "issuer": "did:web:www.uscis.gov:green-card",
  // 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://vc-issuer.uscis.gov/credential/prc/status/3#94567",
    "type": "RevocationList2020Status",
    "revocationListIndex": "94567",
    "revocationListCredential": "https://vc-issuer.uscis.gov/credential/prc/status/3"
  },
  // claims about the subject of the credential
  "credentialSubject": {
    // identifier for the only subject of the credential
    "id": "did:approved-did-method:b34ca6cd37bbf23",
    // assertions about the only subject of the credential
    "type": ["PermanentResident","Person"],
    "givenName": "TEST",
    "familyName": "SPECIMEN",
    "gender": "M",
    "image": "...kJggg==",
    "residentSince": "2015-01-01",
    "lprCategory": "C09",
    "lprNumber": "000-000-204",
    "commuterClassification": "C1",
    "birthCountry": "Bahamas",
    "birthDate": "1958-08-17"
  },
  // digital proof to make the credential tamper-evident
  "proof": {
    // the cryptographic signature suite used to generate signature
    "type": "RsaSignature2018",
    // 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:www.uscis.gov:green-card#public-key-1",
    // the digital signature value
    "jws": "eyJhbGciOiJFZERTQSIsI...wRG2fNmAx60Vi4Ag"
  }
}
```


https://www.w3.org/TR/did-core/
https://www.w3.org/TR/vc-data-model/
https://w3c-ccg.github.io/citizenship-vocab/

US Permanent Resident Card as a W3C VC

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://w3id.org/vc-revocation-list-2020/v1",
    "https://w3id.org/citizenship/v1",
    "https://www.uscis.gov/prc/digital/v1"
  ],
  // specify the identifier for the credential
  "id": "https://vc-issuer.uscis.gov/credential/prc/83627465",
  // the credential type which declares what data to expect in the credential
  "type": ["VerifiableCredential", "PermanentResidentCard"],
  // the entity that issued the credential
  "issuer": "did:web:www.uscis.gov:green-card",
  // 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://vc-issuer.uscis.gov/credential/prc/status/3#94567",
    "type": "RevocationList2020Status",
    "revocationListIndex": "94567",
    "revocationListCredential": "https://vc-issuer.uscis.gov/credential/prc/status/3"
  },
  // claims about the subject of the credential
  "credentialSubject": {
    // identifier for the only subject of the credential
    "id": "did:approved-did-method:b34ca6cd37bbf23",
    // assertions about the only subject of the credential
    "type": ["PermanentResident","Person"],
    "givenName": "TEST",
    "familyName": "SPECIMEN",
    "gender": "M",
    "image": "...kJggg==",
    "residentSince": "2015-01-01",
    "lprCategory": "C09",
    "lprNumber": "000-000-204",
    "commuterClassification": "C1",
    "birthCountry": "Bahamas",
    "birthDate": "1958-08-17"
  },
  // digital proof to make the credential tamper-evident
  "proof": {
    // the cryptographic signature suite used to generate signature
    "type": "RsaSignature2018",
    // 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:www.uscis.gov:green-card#public-key-1",
    // the digital signature value
    "jws": "eyJhbGciOiJFZERTQSIsI...wRG2fNmAx60Vi4Ag"
  }
}
```

Who is the **Issuer** 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?

Public Key Resolver (PKR)

https://www.w3.org/TR/did-core/

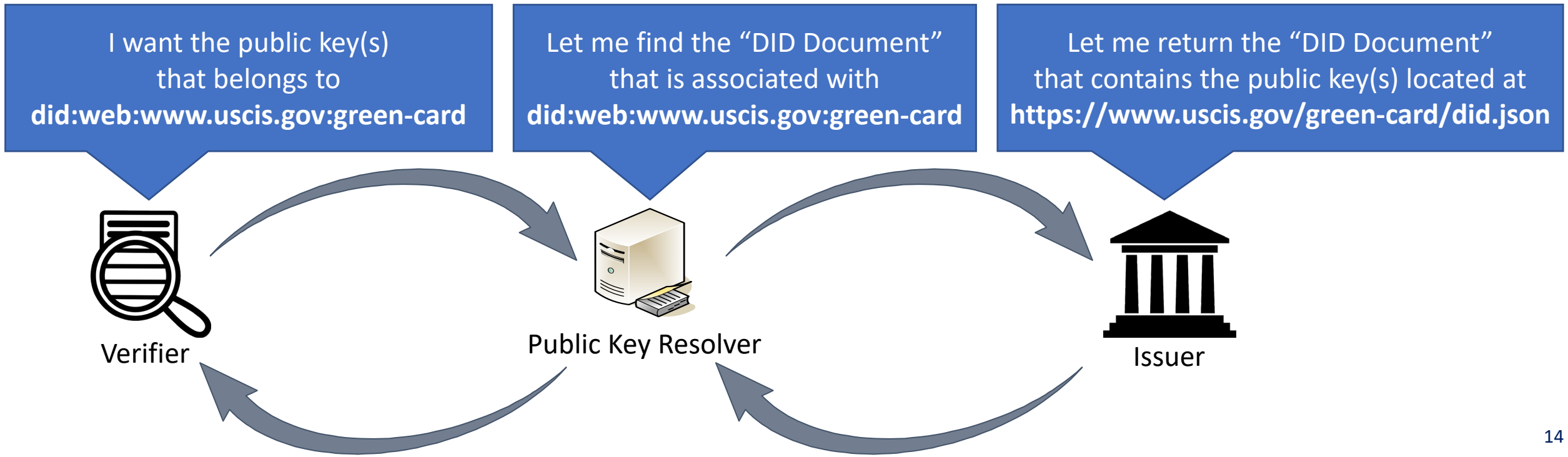
Input	>> A unique decentralized identifier (DID) of an Issuer ---- *ResolveRepresentation(**did**, resolutionOptions)*
Output	>> The location of a text file (DID Document) that is owned/managed by the Issuer that contains its public key(s) ---- *didResolutionMetadata, **didDocumentStream**, didDocumentMetadata*

What is the unique identifier of the Issuer (i.e., the DID representing DHS/USCIS)?

did:web:www.uscis.gov:green-card

What is the identifier of the public key that can verify the digital signature of that Issuer (i.e., a DID URL)?

did:web:www.uscis.gov:green-card#public-key-1



A PKR resolves a DID to a DID document

did:web:www.uscis.gov:green-card resolves to a “DID Document” at https://www.uscis.gov/green-card/did.json


```
{
  "@context": "https://www.w3.org/ns/did/v1",
  // the DID subject
  "id": "did:web:www.uscis.gov:green-card",
  // the controller authorized to make changes to the DID document
  "controller": "did:web:www.uscis.gov:green-card",
  // public key(s) associated with the DID subject
  "publicKey": [
    {
      "id": "did:web:www.uscis.gov:green-card#public-key-1",
      "type": "RsaVerificationKey2018",
      "controller": "did:web:www.uscis.gov:green-card",
      "publicKeyJwk": {
        "kty": "RSA",
        "e": "AQAB",
        "use": "sig",
        "kid": "tNksV42EUs3Xct9AkgZyFWglItRGMxVZ1A1XM68SNq0",
        "n": "kO2d_qQTEBjYFGcoY_da7...FNKtu5E"
      }
    },
    {
      "id": "did:web:www.uscis.gov:green-card#public-key-2",
      "type": "JsonWebKey2020",
      "controller": "did:web:www.uscis.gov:green-card",
      "publicKeyJwk": {
        "kty": "OKP",
        "crv": "Ed25519",
        "x": "VCpo2LMLhn6iWku8MKvSLg2ZAoC-nlOyPVQaO3FxVeQ"
      }
    }
  ],
  // the key used to assert statements as did:web:www.uscis.gov:green-card
  "assertionMethod": [
    "did:web:www.uscis.gov:green-card#public-key-1"
  ],
  // the key used to authenticate as did:web:www.uscis.gov:green-card
  "authentication": [
    "did:web:www.uscis.gov:green-card#public-key-2"
  ]
}
```


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 for authentication

Strategic Approach to Ensure a Competitive, Interoperable Marketplace of Solution Providers

1. Help develop and champion interoperability standards and specifications that are patent free, royalty free and free to implement (2016)
2. Invest in business-driven proof-of-concepts to identify scalable integration architectures and determine adoption Gain/Pain ratio (2017)
3. Motivate and shape innovative and potentially risky product development via the S&T Silicon Valley Innovation Program (SVIP) to meet mission challenges (2018)

Proof of Concepts to understand Gain/Pain

Authenticity and Integrity of IoT Device, Camera and Sensor Data

Lesson Learned

Use of blockchains is overkill WITHIN an Enterprise. There are existing mature technologies and and solutions that are better suited for this purpose.

Enhancing the Entry Submission Process to Streamline International Trade Facilitation

Lesson Learned

Use of common data models based on JSON-LD (e.g., Verifiable Credentials) is viable, critical and developer friendly. Need to separate on-chain (ledger) from off-chain (storage) data

PDF

Enhancing the Registration and Verification of Intellectual Property Assertions of Imported Products

Lesson Learned

Need for standardizing the interfaces to off-chain confidential storage and authorization capabilities that allow for delegated access to information

PDF

Outcome: Adoption of DHS S&T Funded, Developed & Championed Interoperability Standards and Specifications as a US Customs Standard

U.S. Customs and Border Protection

AUG 0 8 2018

MEMORANDUM FOR: John P. Sanders
Chief Operating Officer

FROM: Brenda B. Smith
Executive Assistant Commissioner
Office of Trade

Kathryn Kolbe
Executive Assistant Commissioner
Enterprise Services

Phil Landfried
Assistant Commissioner
Office of Information and Technology

SUBJECT: Setting Standards for Blockchain/Distributed Ledger Technology

DHS S&T has invested over three years of time, money, and effort into researching the specifications necessary to allow multiple blockchains to interact with each other. Interoperability allows the government to remain impartial toward which blockchain software is utilized by our trade partners and removes the need for CBP to continuously build customized Application Program Interfaces to communicate with users of other technology.

Proposed Path Forward:
The Office of Trade (OT) and the Office of Information and Technology (OIT) jointly recommend that:

1. CBP adopt the specifications developed and championed by DHS S&T as a CBP standard.
2. OT and OIT jointly engage other U.S. Government stakeholders, such as the DHS Chief Information Officer (CIO), the White House CIO Council, and others, to push for broader adoption of these standards and to develop an effective "whole of government" approach towards this use-case of blockchain technology.

Strategic Approach to Ensure a Competitive, Interoperable Marketplace of Solution Providers

1. Help develop and champion interoperability standards and specifications that are patent free, royalty free and free to implement (2016)
2. Invest in business-driven proof-of-concepts to identify scalable integration architectures and determine adoption Gain/Pain ratio (2017)
3. Motivate and shape innovative and potentially risky product development via the S&T Silicon Valley Innovation Program (SVIP) to meet mission challenges (2018)

Preventing Forgery & Counterfeiting of Certificates and Licenses (2018)

- DHS Operational Components need to issue, validate and verify entitlements, attestations and certificates
  - Citizenship and Immigration Status
  - Employment Eligibility
  - Essential Work and Task Licenses
  - Organizational Identity & Supply Chain Security

- DHS Operational Components may be both Issuers of Credentials and Validators and Verifiers of Credentials

- Current issuance processes are paper based, non-interoperable and susceptible to loss, destruction, forgery, and counterfeiting

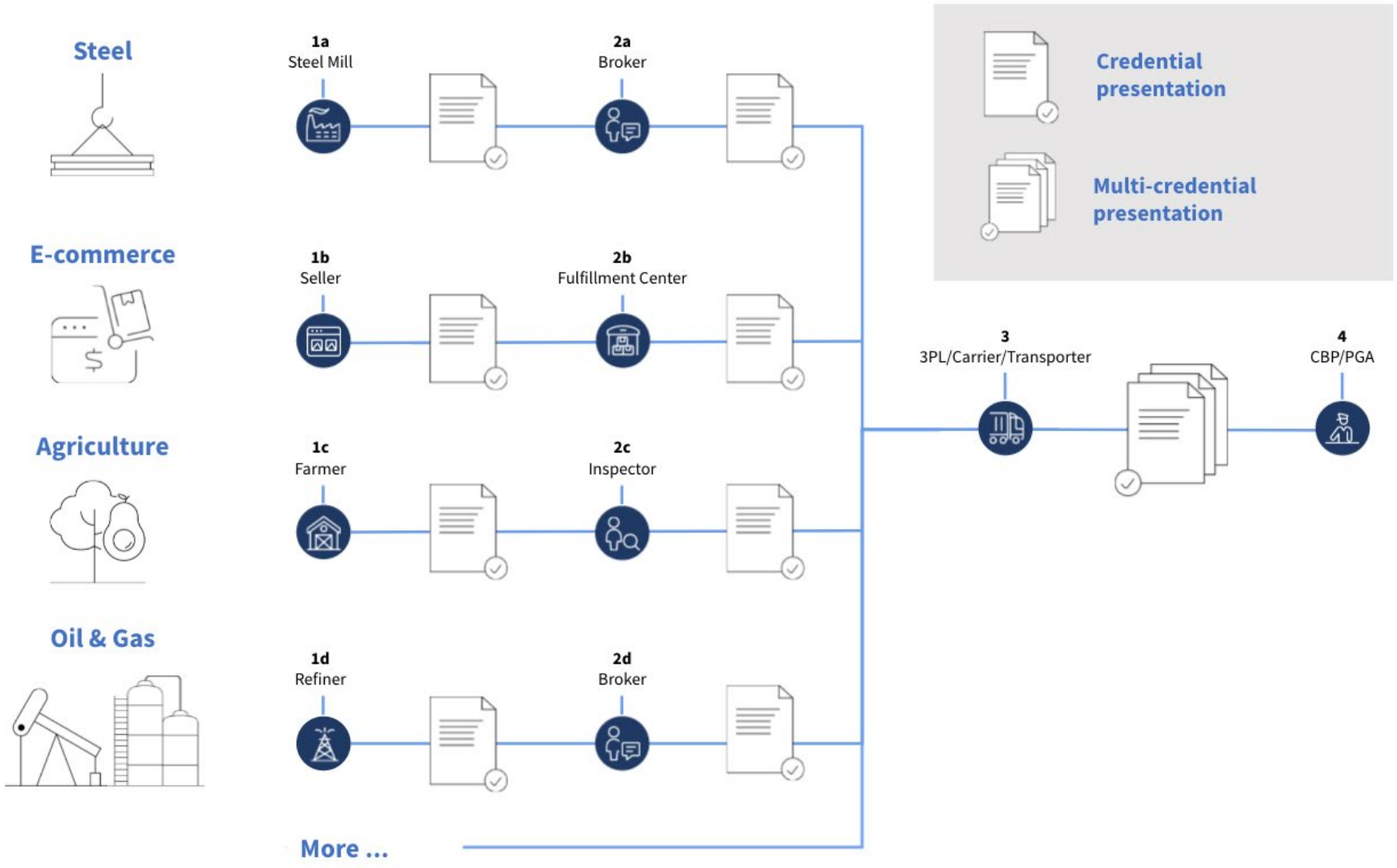
PREVENTING FORGERY & COUNTERFEITING OF CERTIFICATES AND LICENSES

Other Transaction Solicitation Call
70RSAT19R00000002

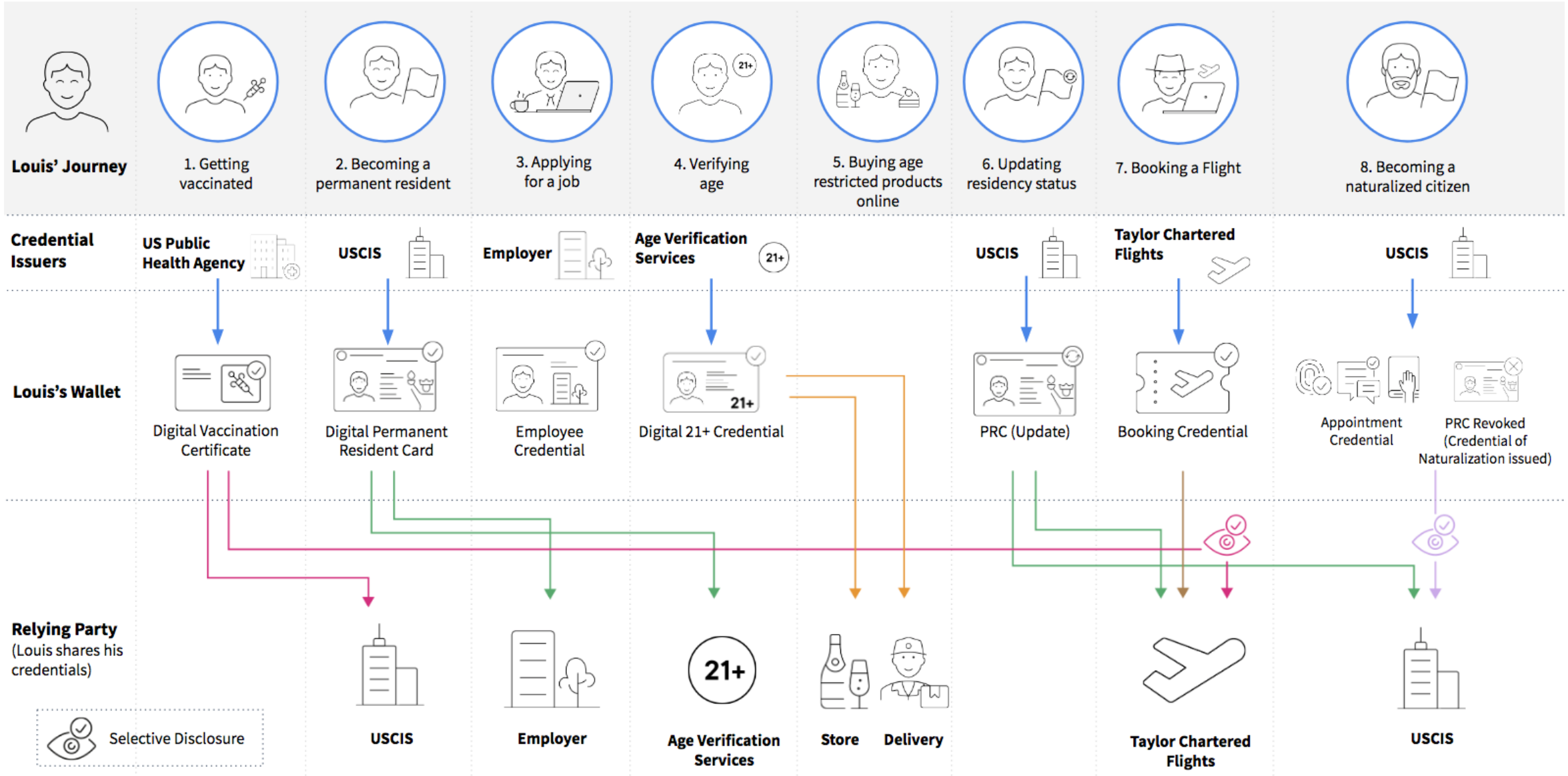
DHS Operational Components & Programs:

- U.S. Citizenship and Immigration Services
- U.S. Customs and Border Protection
- Office of Privacy

Global Interoperability of Trade Credentials



Global Interoperability of Personal Credentials



Ensuring Global Interoperability

Pipe	Payload	Policy
• What are the data exchange protocols that will be used to connect systems? • How do you secure the pipe? • How do you ensure its availability under load and/or duress?	• How do you ensure common understanding of data – across entities that may not share a common authority? • How do you ensure the integrity and provenance of the data? • How do you, if needed, ensure its confidentiality?	• What are the rules of eco-system that everyone needs to agree to? • How do you balance need for commonality with the desire for innovation?

Ensuring Global Interoperability … in Practice!

Pipe	Payload	Policy

• All APIs that are presented to the Issuer and the Verifier SHALL be publicly documented, patent free, royalty free, non-discriminatory, available to all, and free to implement using widely available and supported programming languages.
• Value added services “behind” the open API
 	
More …
	• The solution SHALL incorporate the following emerging and/or mature specifications for interoperability that have been funded, tested and/or championed by DHS:
	  • *Decentralized Identifiers (Standards Development Organization - World Wide Web Consortium / W3C)*
	  • *Verifiable Credentials (Standards Development Organization - W3C)*
	  • *JavaScript Object Notation for Linked Data / JSON-LD (Standards Development Organization - W3C)*
	
	More …
		• The Identity Verification component that is implemented between the Subject/Holder and the Verifier SHALL use standardized, strong authentication technologies that is at least Authenticator Assurance Level 2 (AAL2) compliant as documented in NIST Special Publication 800-63 Revision 3 (or later).
		• The solution SHALL support Federal Information Processing Standard (FIPS) compliant cryptographic algorithms for hashing, encryption, digital signatures, random number generation and any other relevant cryptographic operations that are performed as part of the solution to ensure its ability to be operationally deployable on a US Government network.
		
		More …

Verifying Global Interoperability … in Practice!

Standards Conformance via Automated Test Suites

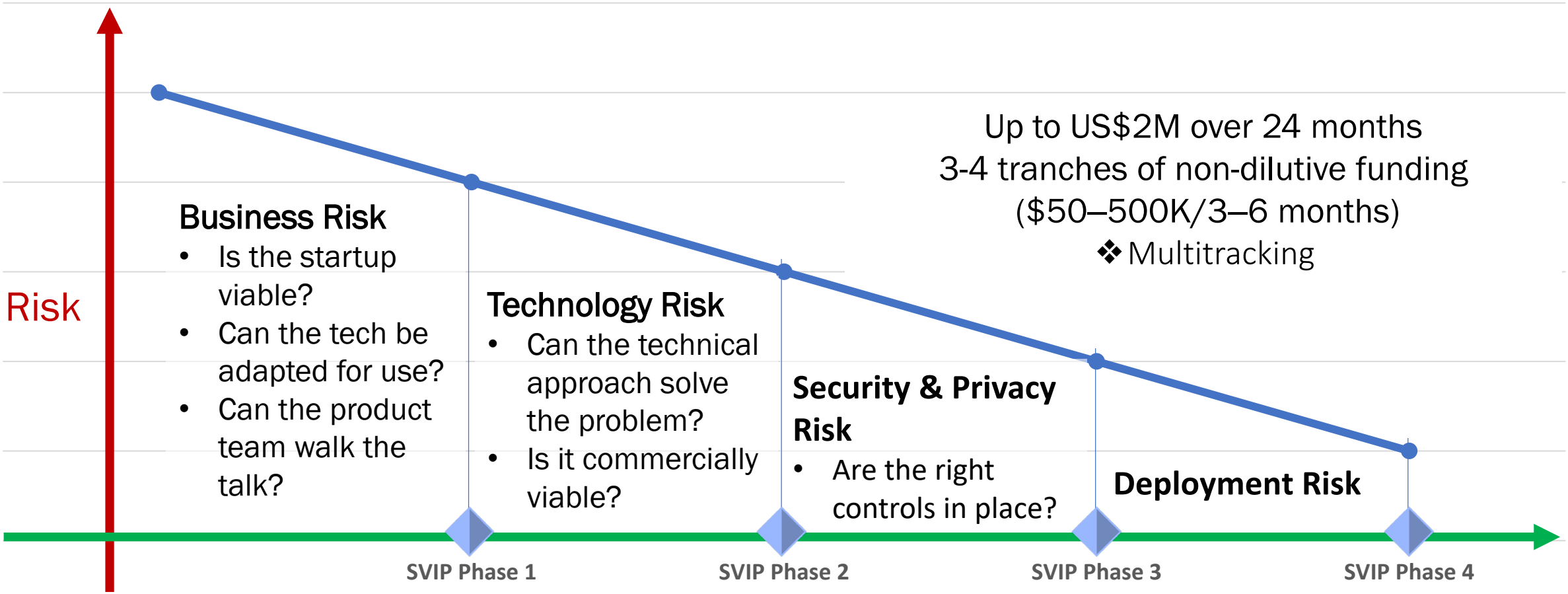
- DHS/SVIP mandates the demonstration of standards compliance using automated conformance test suites
  - Contributed to by DHS/SVIP Performers and many others
  - Developed under the purview of the W3C Credential Community Group (Not DHS)
  - With input sought and accepted from the Global technical community

This is not enough!

Multi-Vendor Interoperability via Plug-fests

- Standards are compromises and as such do not ensure interoperability on their own!
  - Standards allow for multiple ways to accomplish the same thing
  - Standards allow for multiple ways to represent the same thing
- DHS/SVIP mandates the demonstration of interoperability via a NxN matrix testing of the multiple vendors under contract
- Open to working with non-DHS funded entities in a separate “community plug-fest”

Mitigating Operational Transition Risks



DHS/CBP/USCIS/SVIP Multi-Vendor / Multi-Platform Interoperability Testing …

Plugfest 1 May 2020

- JSON-LD
- Linked Data Signatures
- DID Resolution
- VC-HTTP-API https://github.com/w3c-ccg/vc-http-api
- Verifiable Presentation Request https://w3c-ccg.github.io/vp-request-spec/
- Citizenship Vocabulary https://w3c-ccg.github.io/citizenship-vocab/
- Issuer support for multiple mobile/web wallets
- Verifier support for multiple mobile/web wallets
- CHAPI support for mobile/web wallets

Plugfest 2 March 2021

- [Everything Tested in Plug Fest 1]
- Traceability Vocabulary https://w3c-ccg.github.io/traceability-vocab/
- Vaccination Certificate Vocabulary https://w3id.org/vaccination
- FIPS Compliant Cryptographic Primitives
- VC Aggregation and Presentation using Verifiable Presentation (VP)
- VC Revocation with Herd Privacy
- did:web to represent Issuers Only
- VP Support for selective disclosure using BBS+ Signatures

https://docs.google.com/presentation/d/1MeeP7vDXb9CpSBfjTybYbo8qJfrrbrXCSJa0DklNe2k/edit?usp=sharing

Plug-Fest 3+ TBD

- [Everything Tested in Plug Fest 2]
- QR Code w/ CBOR-LD
- Issuer support for VC Refresh by Holder Only
- Issuer support for rich client mobile wallet
- Verifier support for rich client mobile wallet
- Issuer support for OIDC Credential Provider
- More …

W3C Open Vocabulary - Supply Chain Traceability

Traceability Vocabulary v0.0

W3C undefined 11 June 2021

This version:
https://www.w3.org/TR/2021/UNOFFICIAL-traceability-vocab-20210611/

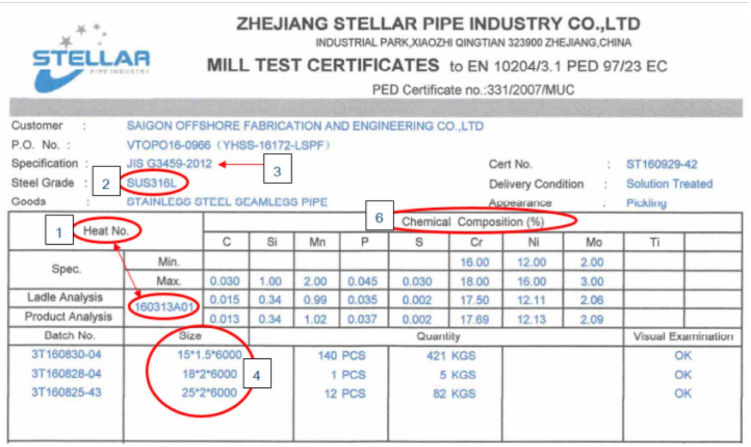
Latest published version:
https://www.w3.org/TR/traceability-vocab/

Latest editor's draft:
https://w3c-ccg.github.io/traceability-vocab

TABLE OF CONTENTS

https://www.w3.org/TR/vc-data-model/
https://w3c-ccg.github.io/traceability-vocab/

Steel Mill Test Report as a W3C VC



ZHEJIANG STELLAR PIPE INDUSTRY CO.,LTD

INDUSTRIAL PARK,XIAOZHI QINGTIAN 323900 ZHEJIANG,CHINA

MILL TEST CERTIFICATES to EN 10204/3.1 PED 97/23 EC

PED Certificate no.:331/2007/MUC

Customer : SAIGON OFFSHORE FABRICATION AND ENGINEERING CO.,LTD

P.O. No. : VTOPO16-0966（YHSS-16172-LSPF）

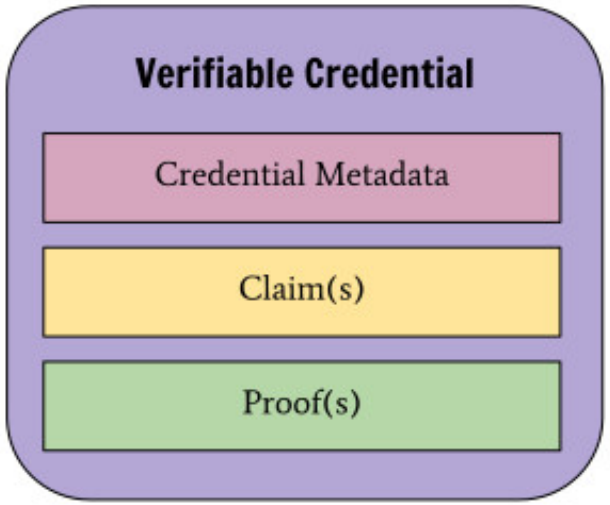
Specification : JIS G3459-2012 (3) Cert No. : ST160929-42

Steel Grade : (2) SUS316L Delivery Condition : Solution Treated

Goods : STAINLESS STEEL SEAMLESS PIPE Appearance : Pickling

(1) Heat No.		(6) Chemical Composition (%)									
		C	Si	Mn	P	S	Cr	Ni	Mo	Ti	
Spec.	Min.						16.00	12.00	2.00		
	Max.	0.030	1.00	2.00	0.045	0.030	18.00	16.00	3.00		
Ladle Analysis	160313A01	0.015	0.34	0.99	0.035	0.002	17.50	12.11	2.06		
Product Analysis		0.013	0.34	1.02	0.037	0.002	17.69	12.13	2.09		

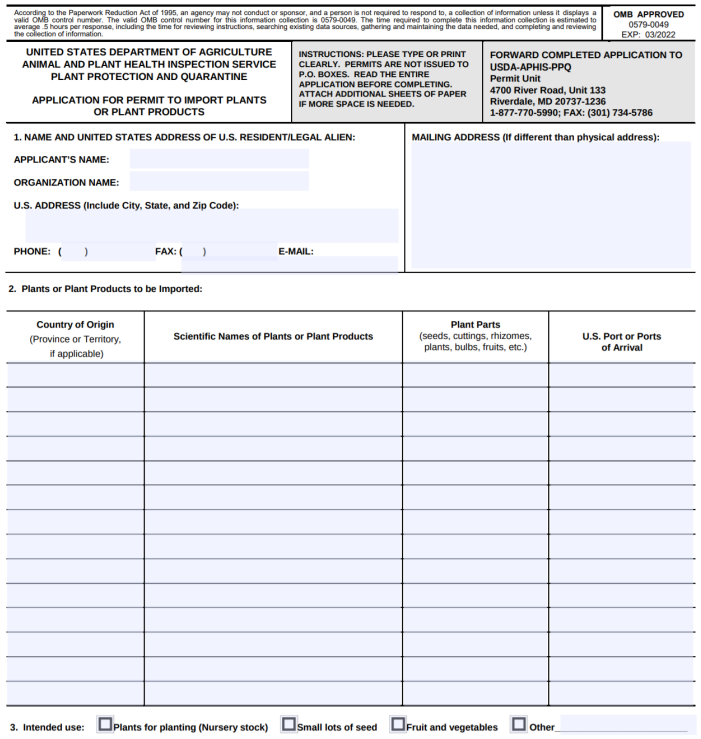
Batch No.	Size	Quantity		Visual Examination
3T160830-04	15*1.5*6000 (4)	140 PCS	421 KGS	OK
3T160828-04	18*2*6000	1 PCS	5 KGS	OK
3T160825-43	25*2*6000	12 PCS	82 KGS	OK




```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://w3id.org/traceability/v1",
    "https://w3id.org/vc-revocation-list-2020/v1"
  ],
  "type": [
    "VerifiableCredential",
    "MillTestReportCertificate"
  ],
  "name": "Certified Mill Test Report",
  "description": "This document includes recommended mill certificate fields.",
  "credentialSubject": {
    "type": [
      "MillTestReport"
    ],
    "manufacturer": {
      "type": [
        "Organization"
      ],
      "name": "Mosciski - Cormier",
      "description": "Right-sized attitude-oriented info-mediaries",
      "email": "Toney_Bradtke74@example.org",
      "phoneNumber": "555-148-7606",
      "faxNumber": "555-564-1276",
      "address": {
        "type": [
          "PostalAddress"
        ],
        "streetAddress": "9329 King Manors",
        "addressLocality": "North Astridview",
        "addressRegion": "New Jersey",
        "postalCode": "51424",
        "addressCountry": "Denmark"
      }
    },
    "product": {
      "type": [
        "SteelProduct"
      ],
      "heatNumber": "36126",
      "specification": "ASTM-85461",
      "grade": "21336",
      "originalCountryOfMeltAndPour": "Denmark",
      "inspection": {
        "type": [
          "InspectionReport"
        ],
        "observation": [
          {
            "type": [
              "Observation"
```


https://www.w3.org/TR/did-core/
https://www.w3.org/TR/vc-data-model/
https://w3c-ccg.github.io/traceability-vocab/

Import Plant/Plant Product Permit as a W3C VC



According to the Paperwork Reduction Act of 1995, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0579-0049. The time required to complete this information collection is estimated to average .5 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information.

OMB APPROVED
0579-0049
EXP: 03/2022

UNITED STATES DEPARTMENT OF AGRICULTURE
ANIMAL AND PLANT HEALTH INSPECTION SERVICE
PLANT PROTECTION AND QUARANTINE

APPLICATION FOR PERMIT TO IMPORT PLANTS OR PLANT PRODUCTS

INSTRUCTIONS: PLEASE TYPE OR PRINT CLEARLY. PERMITS ARE NOT ISSUED TO P.O. BOXES. READ THE ENTIRE APPLICATION BEFORE COMPLETING. ATTACH ADDITIONAL SHEETS OF PAPER IF MORE SPACE IS NEEDED.

FORWARD COMPLETED APPLICATION TO
USDA-APHIS-PPQ
Permit Unit
4700 River Road, Unit 133
Riverdale, MD 20737-1236
1-877-770-5990; FAX: (301) 734-5786

1. NAME AND UNITED STATES ADDRESS OF U.S. RESIDENT/LEGAL ALIEN:

APPLICANT'S NAME:

ORGANIZATION NAME:

U.S. ADDRESS (Include City, State, and Zip Code):

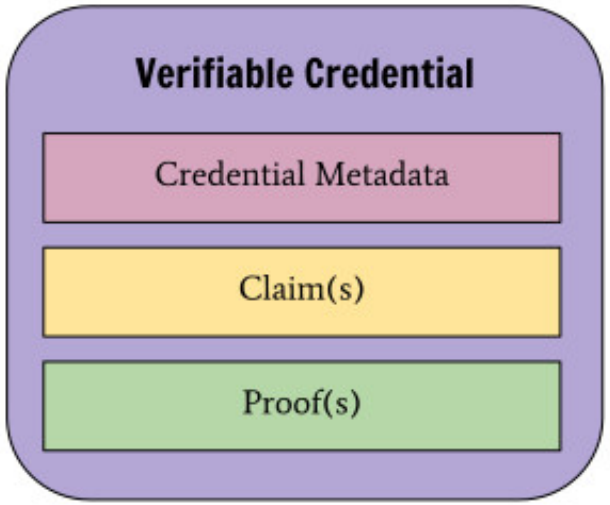
PHONE: ( ) FAX: ( ) E-MAIL:

MAILING ADDRESS (If different than physical address):

2. Plants or Plant Products to be Imported:

Country of Origin (Province or Territory, if applicable)	Scientific Names of Plants or Plant Products	Plant Parts (seeds, cuttings, rhizomes, plants, bulbs, fruits, etc.)	U.S. Port or Ports of Arrival

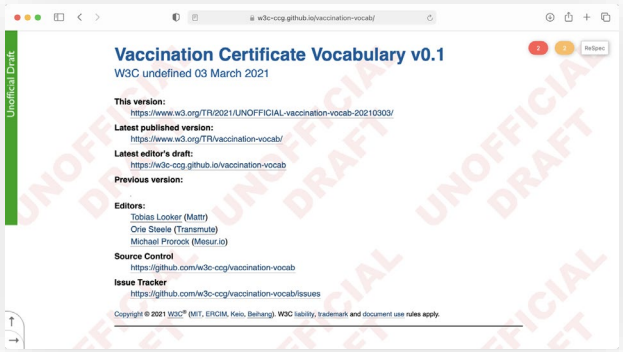
3. Intended use: ☐ Plants for planting (Nursery stock) ☐ Small lots of seed ☐ Fruit and vegetables ☐ Other



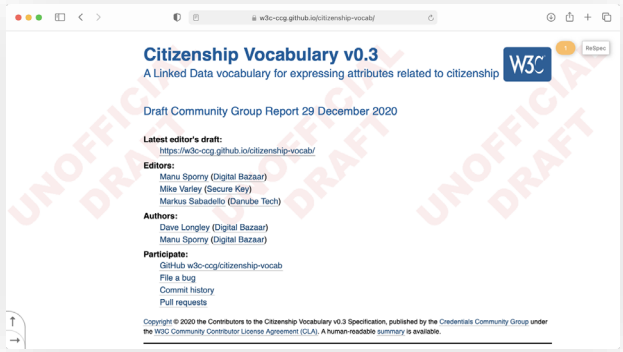

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://w3id.org/traceability/v1"
  ],
  "id": "http://example.org/credentials/",
  "type": [
    "VerifiableCredential"
  ],
  "issuanceDate": "2021-02-04T20:29:37+00:00",
  "issuer": "did:key:z6MktHQo3fRRohk44dsbE76CuiTpBmyMWq2VVjvV6aBSeE3U",
  "credentialSubject": {
    "@context": [
      "https://w3id.org/traceability/v1"
    ],
    "type": "ppq587",
    "facility": {
      "@context": [
        "https://w3id.org/traceability/v1"
      ],
      "type": [
        "Place"
      ],
      "globalLocationNumber": "3744411334251",
      "geo": {
        "type": [
          "GeoCoordinates"
        ],
        "latitude": "-25.1882",
        "longitude": "-8.7921"
      },
      "address": {
        "type": [
          "PostalAddress"
        ],
        "organizationName": "Gusikowski - Boyle",
        "streetAddress": "02675 Reinger Islands",
        "addressLocality": "Jacksonfort",
        "addressRegion": "Nevada",
        "postalCode": "56993",
        "addressCountry": "Sri Lanka"
      }
    },
    "shipment": {
      "@context": [
        "https://w3id.org/traceability/v1"
      ],
      "type": [
        "AgParcelDelivery"
      ],
      "deliveryAddress": {
        "@context": [
          "https://w3id.org/traceability/v1"
        ],
        "type": [
          "PostalAddress"
        ],
        "organizationName": "Tillman, Davis and Welch",
        "streetAddress": "1926 Donald Wall",
        "addressLocality": "Mathildefort",
        "addressRegion": "Illinois",
        "postalCode": "32118-4872",
        "addressCountry": "Czech Republic"
      },
      "originAddress": {
        "@context": [
```


https://www.w3.org/TR/did-core/
https://www.w3.org/TR/vc-data-model/
https://w3c-ccg.github.io/traceability-vocab/

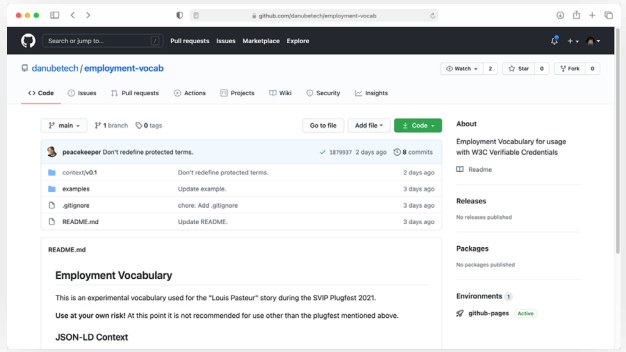
Testing the Payloads - Vocabularies



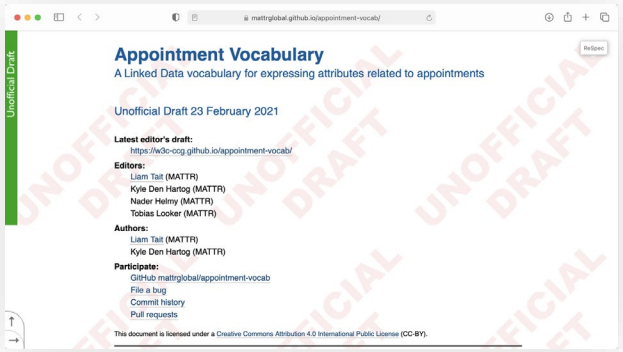
Vaccination [link]



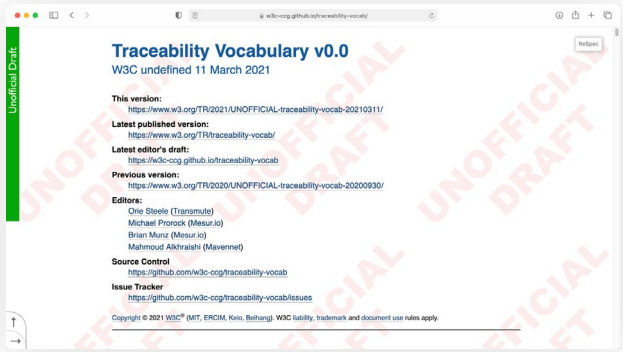
Citizenship [link]



Employment [link]



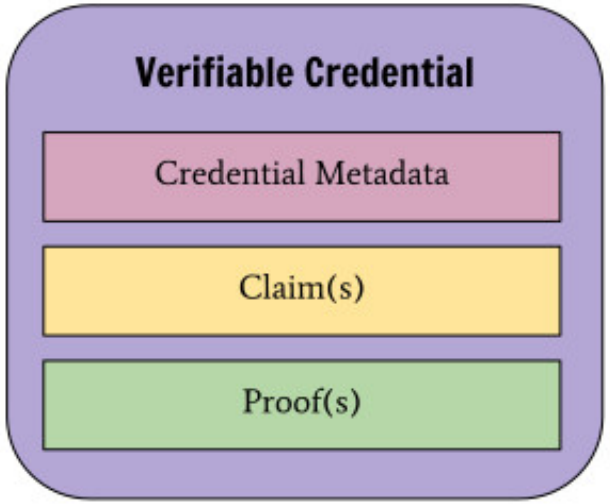
Appointment [link]



Traceability [link]

- **Built referencing existing schema.org definitions**
- **Extensible to incorporate any existing vocabulary elements (for example Traceability Vocab uses GS1 vocabulary elements)**
- **Standardizes the creation of Verifiable Credentials from standardized JSON-LD, which is generated from JSON Schemas**
- **Hosted under the W3C umbrella and open to contributions**

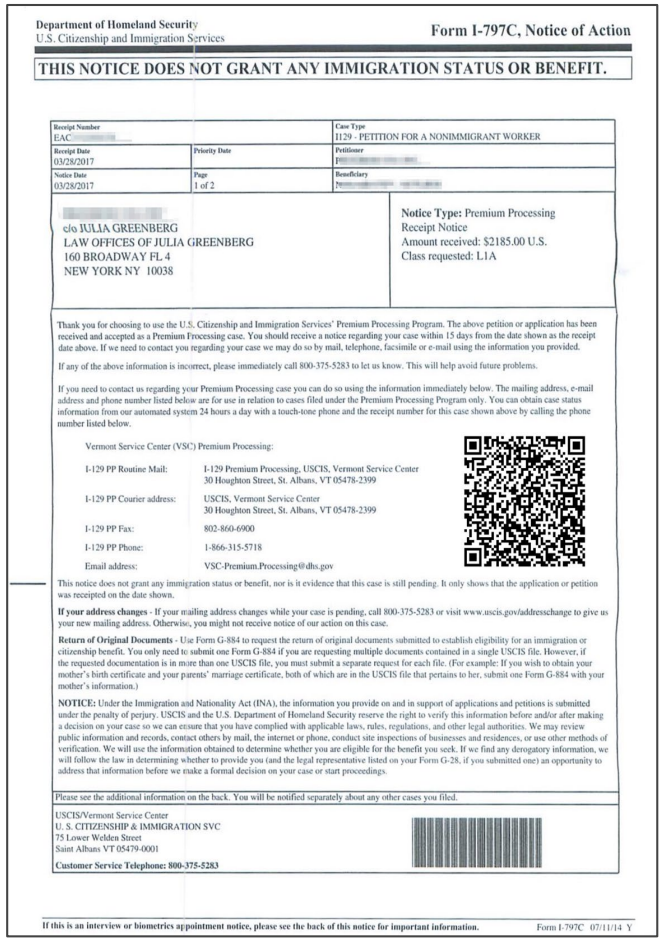
US Permanent Resident Card as a W3C VC




```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://w3id.org/vc-revocation-list-2020/v1",
    "https://w3id.org/citizenship/v1",
    "https://www.uscis.gov/prc/digital/v1"
  ],
  // specify the identifier for the credential
  "id": "https://vc-issuer.uscis.gov/credential/prc/83627465",
  // the credential type which declares what data to expect in the credential
  "type": ["VerifiableCredential", "PermanentResidentCard"],
  // the entity that issued the credential
  "issuer": "did:web:www.uscis.gov:green-card",
  // 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://vc-issuer.uscis.gov/credential/prc/status/3#94567",
    "type": "RevocationList2020Status",
    "revocationListIndex": "94567",
    "revocationListCredential": "https://vc-issuer.uscis.gov/credential/prc/status/3"
  },
  // claims about the subject of the credential
  "credentialSubject": {
    // identifier for the only subject of the credential
    "id": "did:approved-did-method:b34ca6cd37bbf23",
    // assertions about the only subject of the credential
    "type": ["PermanentResident","Person"],
    "givenName": "TEST",
    "familyName": "SPECIMEN",
    "gender": "M",
    "image": "...kJggg==",
    "residentSince": "2015-01-01",
    "lprCategory": "C09",
    "lprNumber": "000-000-204",
    "commuterClassification": "C1",
    "birthCountry": "Bahamas",
    "birthDate": "1958-08-17"
  },
  // digital proof to make the credential tamper-evident
  "proof": {
    // the cryptographic signature suite used to generate signature
    "type": "RsaSignature2018",
    // 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:www.uscis.gov:green-card#public-key-1",
    // the digital signature value
    "jws": "eyJhbGciOiJFZERTQSIsI...wRG2fNmAx60Vi4Ag"
  }
}
```


https://www.w3.org/TR/did-core/
https://www.w3.org/TR/vc-data-model/
https://w3c-ccg.github.io/citizenship-vocab/

USCIS Appointment Letter as a W3C VC



Department of Homeland Security
U.S. Citizenship and Immigration Services

Form I-797C, Notice of Action

THIS NOTICE DOES NOT GRANT ANY IMMIGRATION STATUS OR BENEFIT.

Receipt Number		Case Type
EAC		I129 - PETITION FOR A NONIMMIGRANT WORKER
Receipt Date	Priority Date	Petitioner
03/28/2017		
Notice Date	Page	Beneficiary
03/28/2017	1 of 2	

c/o JULIA GREENBERG
LAW OFFICES OF JULIA GREENBERG
160 BROADWAY FL 4
NEW YORK NY 10038

Notice Type: Premium Processing
Receipt Notice
Amount received: $2185.00 U.S.
Class requested: L1A

Thank you for choosing to use the U.S. Citizenship and Immigration Services' Premium Processing Program. The above petition or application has been received and accepted as a Premium Processing case. You should receive a notice regarding your case within 15 days from the date shown as the receipt date above. If we need to contact you regarding your case we may do so by mail, telephone, facsimile or e-mail using the information you provided.

If any of the above information is incorrect, please immediately call 800-375-5283 to let us know. This will help avoid future problems.

If you need to contact us regarding your Premium Processing case you can do so using the information immediately below. The mailing address, e-mail address and phone number listed below are for use in relation to cases filed under the Premium Processing Program only. You can obtain case status information from our automated system 24 hours a day with a touch-tone phone and the receipt number for this case shown above by calling the phone number listed below.

Vermont Service Center (VSC) Premium Processing:

I-129 PP Routine Mail:	I-129 Premium Processing, USCIS, Vermont Service Center 30 Houghton Street, St. Albans, VT 05478-2399
I-129 PP Courier address:	USCIS, Vermont Service Center 30 Houghton Street, St. Albans, VT 05478-2399
I-129 PP Fax:	802-860-6900
I-129 PP Phone:	1-866-315-5718
Email address:	VSC-Premium.Processing@dhs.gov

This notice does not grant any immigration status or benefit, nor is it evidence that this case is still pending. It only shows that the application or petition was receipted on the date shown.

If your address changes - If your mailing address changes while your case is pending, call 800-375-5283 or visit www.uscis.gov/addresschange to give us your new mailing address. Otherwise, you might not receive notice of our action on this case.

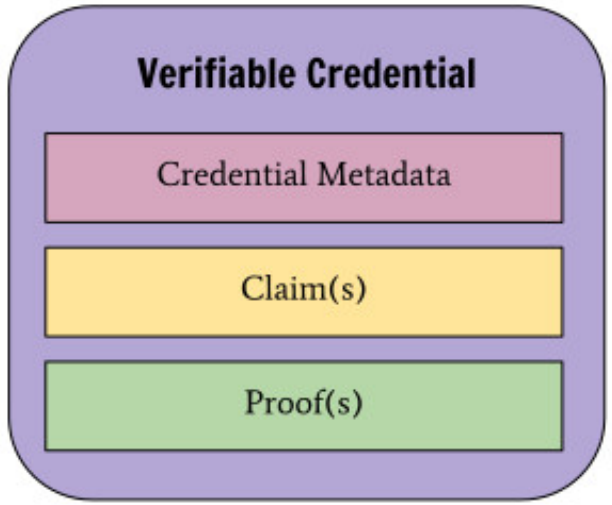
Return of Original Documents - Use Form G-884 to request the return of original documents submitted to establish eligibility for an immigration or citizenship benefit. You only need to submit one Form G-884 if you are requesting multiple documents contained in a single USCIS file. However, if the requested documentation is in more than one USCIS file, you must submit a separate request for each file. (For example: If you wish to obtain your mother's birth certificate and your parents' marriage certificate, both of which are in the USCIS file that pertains to her, submit one Form G-884 with your mother's information.)

NOTICE: Under the Immigration and Nationality Act (INA), the information you provide on and in support of applications and petitions is submitted under the penalty of perjury. USCIS and the U.S. Department of Homeland Security reserve the right to verify this information before and/or after making a decision on your case so we can ensure that you have complied with applicable laws, rules, regulations, and other legal authorities. We may review public information and records, contact others by mail, the internet or phone, conduct site inspections of businesses and residences, or use other methods of verification. We will use the information obtained to determine whether you are eligible for the benefit you seek. If we find any derogatory information, we will follow the law in determining whether to provide you (and the legal representative listed on your Form G-28, if you submitted one) an opportunity to address that information before we make a formal decision on your case or start proceedings.

Please see the additional information on the back. You will be notified separately about any other cases you filed.

USCIS/Vermont Service Center
U. S. CITIZENSHIP & IMMIGRATION SVC
75 Lower Welden Street
Saint Albans VT 05479-0001
Customer Service Telephone: 800-375-5283

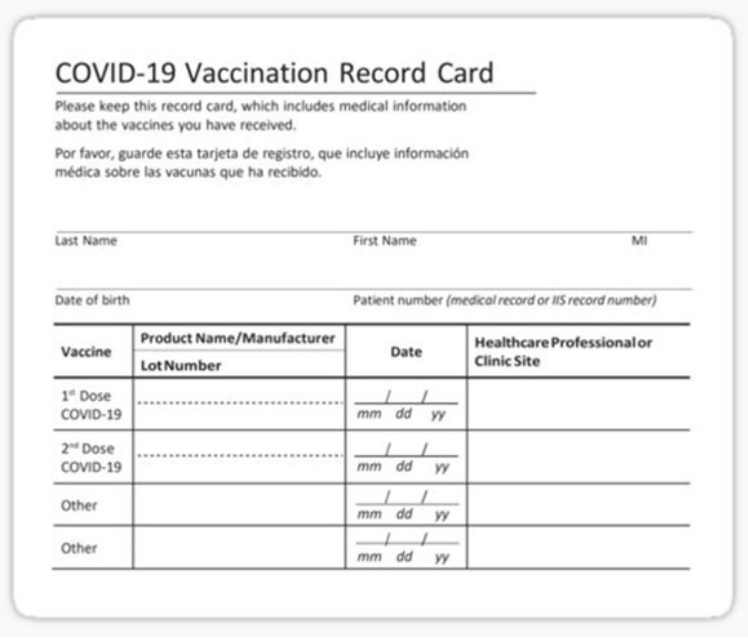
If this is an interview or biometrics appointment notice, please see the back of this notice for important information. Form I-797C 07/11/14 Y




```
"@context": [
  "https://www.w3.org/2018/credentials/v1",
  "https://w3id.org/appointment",
  "https://w3id.org/security/v3-unstable"
],
"id": "https://issuer.oidp.uscis.gov/credentials/83627466",
"type": [
  "VerifiableCredential",
  "Appointment"
],
"issuer": "did:web:issuer.uscis.gov:appointmentcert",
"name": "USCIS Naturalization Interview Appointment",
"description": "An appointment credential to access the online meeting for the fin
"issuanceDate": "2021-02-04T12:19:52Z",
"expirationDate": "2021-03-15T15:00:00Z",
"credentialSubject": {
  "id": "did:example:b34ca6cd37bbf23",
  "type": [
    "USCISAppointmentDetails"
  ],
  "organizer": "did:example:489398593",
  "applicant": "did:example:b34ca6cd37bbf23",
  "startTime": "2021-03-15T14:00:00Z",
  "duration": "PT1H",
  "location": "https://zoom.us/j/5551112222",
  "accountNumber": "768553823129",
  "alienNumber": "000-001-001",
  "receiptNumber": "IOE-21-123-45678",
  "caseType": "N400",
  "appointmentType": "interview"
},
"credentialStatus":{
  "id":"https://issuer.uscis.gov/core/v1/revocation-lists/9e8ea658-b4e4-4e86-bc50-
  "type":"RevocationList2020Status",
  "revocationListIndex":"22",
  "revocationListCredential":"https://issuer.uscis.gov/core/v1/revocation-lists/9e
},
"proof": {
  "type": "https://w3c-ccg.github.io/ldp-bbs2020/context/v1#BbsBlsSignature2020",
  "created": "2021-02-23T02:36:34Z",
  "proofPurpose": "assertionMethod",
  "proofValue": "uNzs/o5PVI/AQyCpadu4aKW5qITzzTicQGR+5wIuZu7YSgqXgn4HUI5v9L8CiXhZR
  "verificationMethod": "did:web:issuer.uscis.gov:appointmentcert"
}
```


https://www.w3.org/TR/did-core/
https://www.w3.org/TR/vc-data-model/
https://mattrglobal.github.io/appointment-vocab/

COVID-19 Proof of Vaccination as a W3C VC



COVID-19 Vaccination Record Card

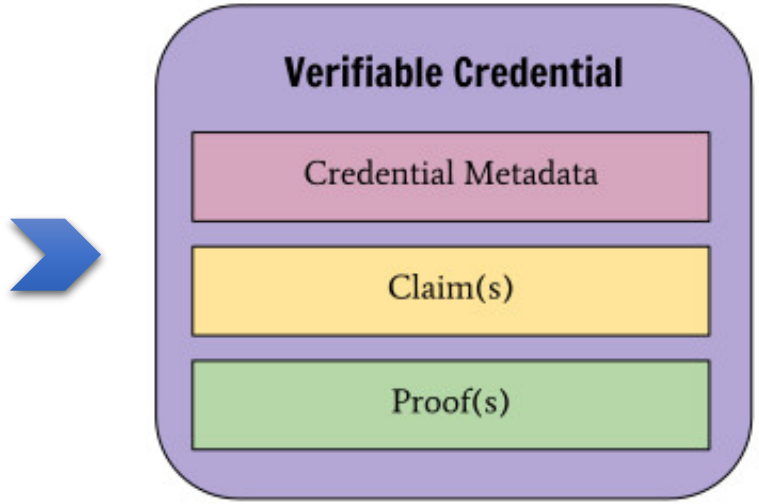
Please keep this record card, which includes medical information about the vaccines you have received.

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

Higher Education Degree as a W3C VC

WU WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

EQUIS ACCREDITED AACSB ACCREDITED AMBA ACCREDITED

CERTIFICATE
MASTER'S DEGREE PROGRAM
IN STRATEGY, INNOVATION, AND MANAGEMENT CONTROL

UJ 066 957 00000000
Student ID number

Ms. Eva Musterfrau, BSc (WU)

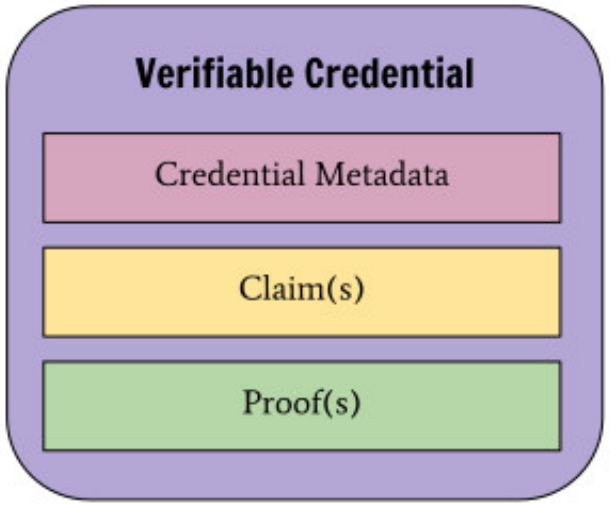
date of birth October 22, 1999

completed the Master's Degree Program in STRATEGY, INNOVATION, AND MANAGEMENT CONTROL, with a Double Degree major in cooperation with Università Commerciale Luigi Bocconi, established according to the curriculum pursuant to the 2002 Universities Act (Universitätsgesetz 2002), Federal Law Gazette I, no. 120/2002, as amended,

on January 04, 2021

with the cumulative grade – passed with honors –

Cumulative grades: passed with honors / passed / failed

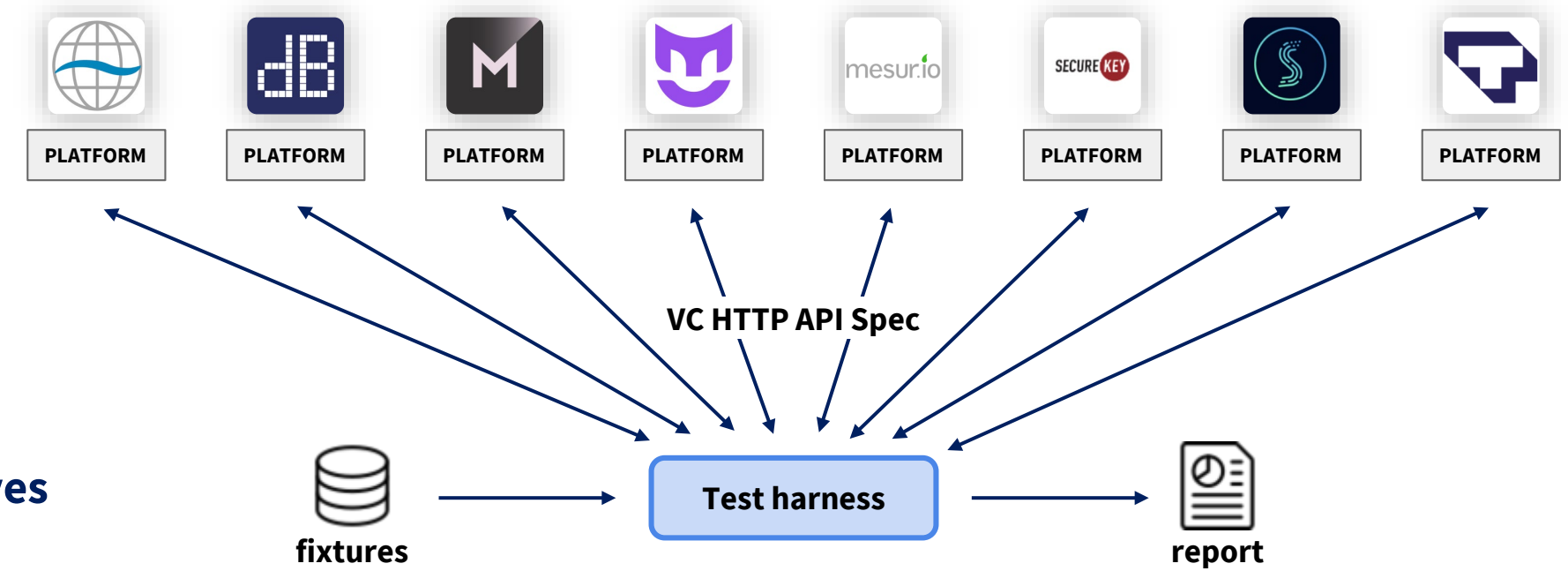



```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://essif.europa.eu/schemas/vc/2020/v1"
  ],
  "type": [
    "VerifiableCredential",
    "VerifiableAttestation",
    "DiplomaCredential"
  ],
  "issuer": "did:ebsi:51rzpDXXCtKExG47boFBahAgd2dtfAZbQxMHM17mYKoq",
  "issuanceDate": "2021-06-10T10:45:13Z",
  "credentialSubject": {
    "type": "Student",
    "id": "did:key:z6Mkk2gs7gfr1F1idzKkjie7eA4pDtRjGfG2GdGcVf9kHgQw",
    "studyProgram": "Master Studies in Strategy, Innovation, and Management Control",
    "immatriculationNumber": "00000000",
    "currentGivenName": "Eva",
    "currentFamilyName": "Musterfrau",
    "learningAchievement": "Master's Degree",
    "dateOfBirth": "1999-10-22T00:00:00.000Z",
    "dateOfAchievement": "2021-01-04T00:00:00.000Z",
    "overallEvaluation": "passed with honors",
    "eqfLevel": "http://data.europa.eu/snb/eqf/7",
    "targetFrameworkName": "European Qualifications Framework for lifelong learning -
(2008/C 111/01)"
  },
  "proof": {
    "type": "EcdsaSecp256k1Signature2019",
    "created": "2021-06-10T10:45:13Z",
    "proofPurpose": "assertionMethod",
    "verificationMethod": "did:ebsi:51rzpDXXCtKExG47boFBahAgd2dtfAZbQxMHM17mYKoq#keys-1",
    "jws":
"eyJiNjQiOmZhbHNlLCJjcml0IjpbImI2NCJdLCJhbGciOiJFUzI1NksifQ..
MEUCIQDDjn4oP8B7L_6E_OSqLqM_Lh3KJZg0YRzmX2uX6MOX8AIgMX0jALizKvFwOq69Q95PJJ2C7aYgJWYQ1SkCm9
LvZnM"
  }
}
```


https://www.w3.org/TR/did-core/
https://www.w3.org/TR/vc-data-model/
https://github.com/danubetech/ebsi4austria-examples

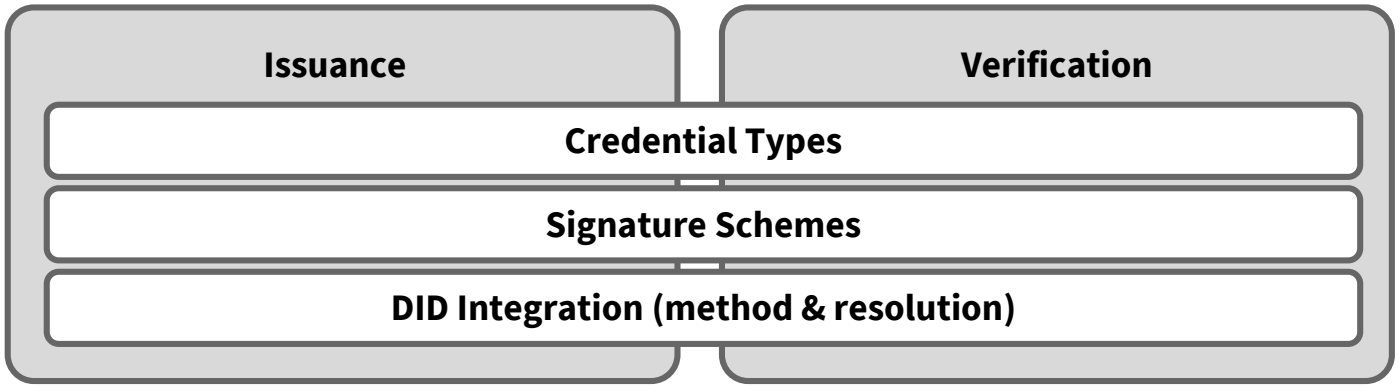
Testing the Pipe -- VC HTTP API Test Suite

Test environment

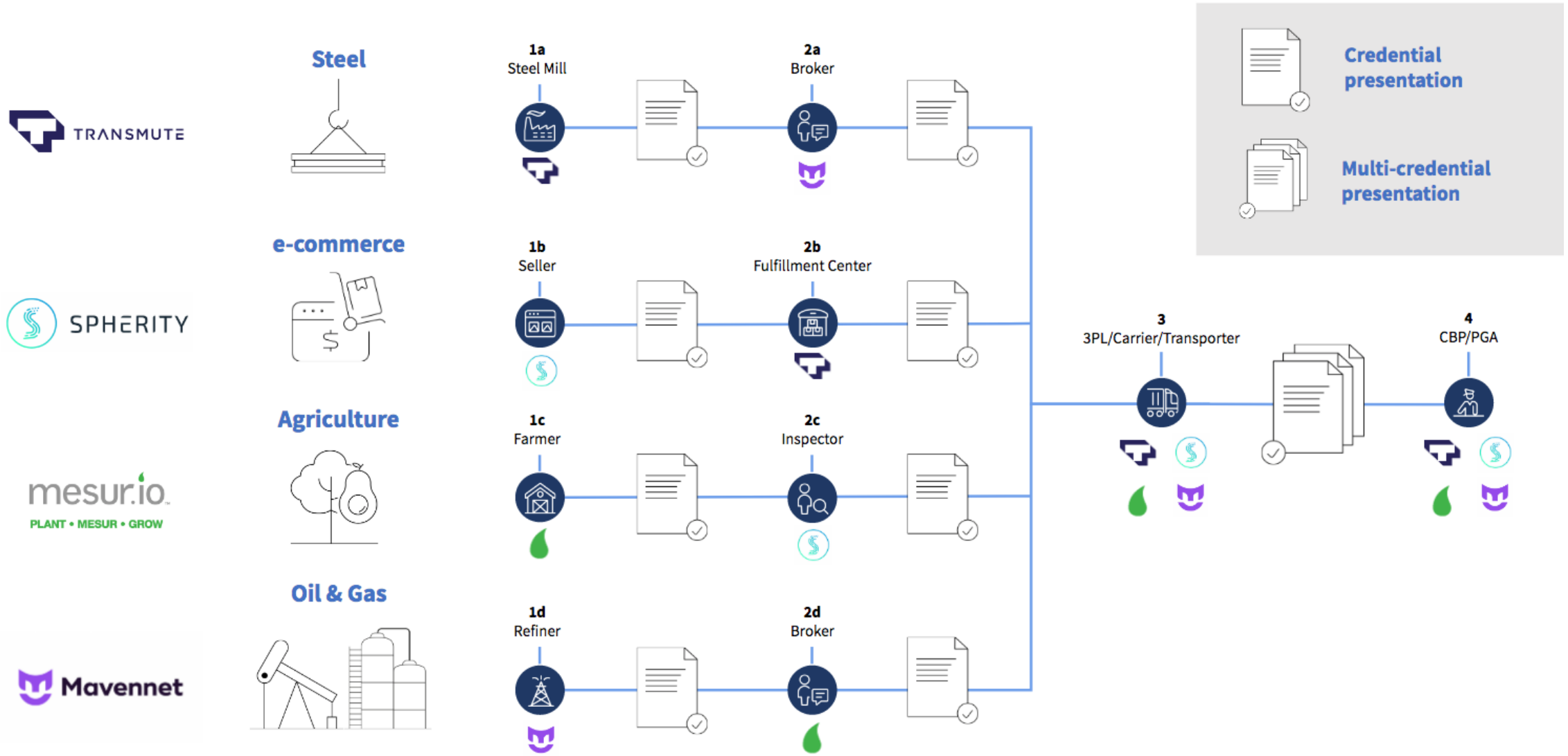


Test objectives

Role of the Test suite
Tests core issuance and verification capabilities for a variety of different credential types against different DID methods and signature suites. “Backend-level testing”



Digital Trade Credentials Interoperability



https://docs.google.com/presentation/d/1MeeP7vDXb9CpSBfjTybYbo8qJfrrbrXCSJa0DklNe2k/edit?usp=sharing

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

Real Interoperability Matters - No Excuses!

- Potential for the development of “walled gardens” or closed technology platforms that do not support common standards for security, privacy, and data exchange. Scalable deployments needs solution diversity to prevent vendor tech lock-in
- Data privacy and data segregation continues to be critical components of any distributed solution, and needs to be addressed up front in the solution architecture and design
- Rip-n-Replace is NOT a successful path to enterprise integration, so interoperability is critically important. Interoperability requires addressing the architecture, protocol, payload and policy aspects of any solution.
- Government has a role in ensuring a competitive, diverse and interoperable eco-system:
  - USG/DHS has invested in extensive R&D to understand the promise, perils, and the gain-to-pain ratio of technology adoption
  - USG/DHS has conducted realistic POCs, Pilots and Implementations that encourage and demonstrate multi-party interoperability and solution diversity
  - USG/DHS has worked in the open, under the W3C umbrella, to develop, utilize and socialize standards conformance test suites, interoperability test suites and verification events (plug-fests) that can be leveraged by anyone!

Answer to a Technical Question from ICAO …

Can this technical approach (using W3C Verifiable Credentials and W3C Decentralized Identifiers) be applied to mitigating cross-border air cargo safety and security risks?

Can this approach be applied to Mitigating Air Cargo Safety and Security Risks? A Possible ICAO Use Case

Global Intent

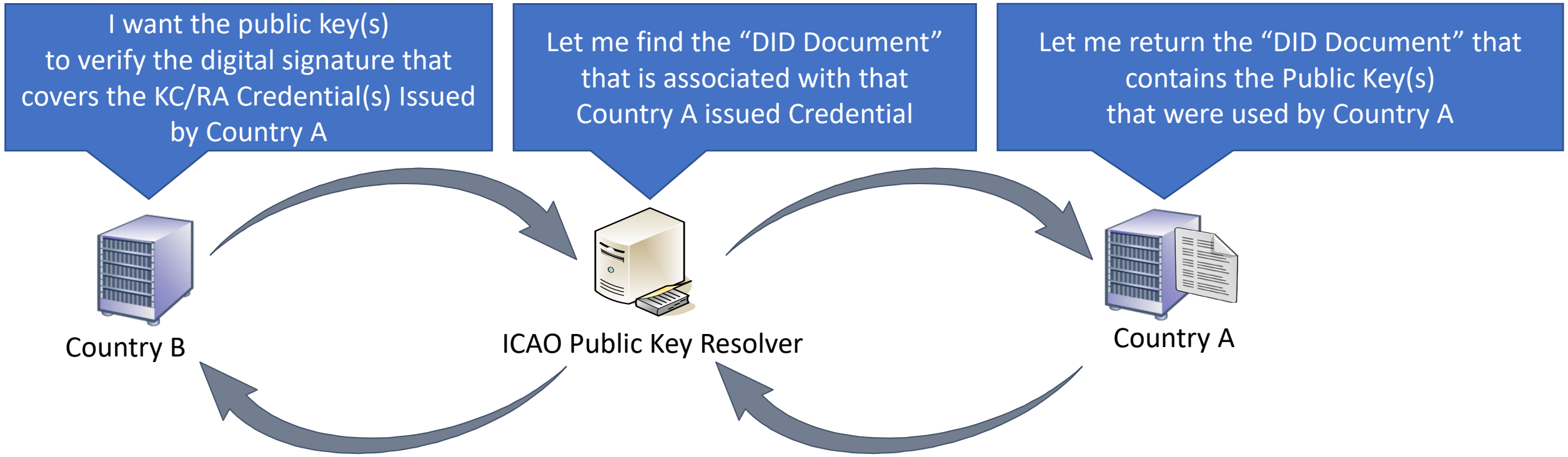
- Increase safety and security measures for air cargo services
- Enhance operational efficiencies for air cargo services
- Collect operational and trade data for analysis and policy decisions
- Support public health goals to mitigate the risks of contamination by COVID-19 across the supply chain
- Utilization of Known Consignor (KC) and Regulated Agent (RA) regimes

Local Implementations

- **USA**: Certified cargo screening program and Air Cargo Advance Screening
- **European Union**: ACC3 Programme
- **Australia**: Regulated Air Cargo Agent and Accredited Air Cargo Agent schemes
- **Hong Kong SAR, China**: Regulated Agent Regime
- **Singapore**: Air Cargo Agent Regime
- **Canada**: Air Cargo Security Programme

However, when the air cargo from Country A arrives in Country B, how does the Country B Customs verify if the entity who has executed the security controls is qualified by the appropriate Country A authority?

Connecting the many “Cylinders of Excellence”



1. A Common Vocabulary for representing KC / RA Credentials
2. An ICAO Managed Public Key Resolver
3. Mutual Recognition (Trust) Framework

PKR - An Issuer's Perspective

- A potential nexus of policy governance and policy enforcement
- No external repository of public keys (e.g., a PKD) to manage, keep up to date, synchronized etc.
- Lifecycle management of keys (e.g., key rotation) under its control with little to no external dependencies
- Choice in which Public Key Resolver to regard as authoritative based on Policy or Trust Framework
  - Single PKR that is globally authoritative
  - A collection of PKRs that are considered authoritative
  - Other governance/policy models?

A Verifier's Perspective

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

- Find the Issuer's unique identifier (i.e., DID) in the credential
- Resolve Issuer's DID to its DID document using a Public Key Resolver
- Pick up the public key used for "assertionMethod" from DID document associated with the Issuer's DID
- Cache locally, if appropriate and per policy

Process the digital proof and credential status check

- Is the digital signature valid?
- Is the credential valid? i.e., has it 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

Homeland Security

Science and Technology

Thank You

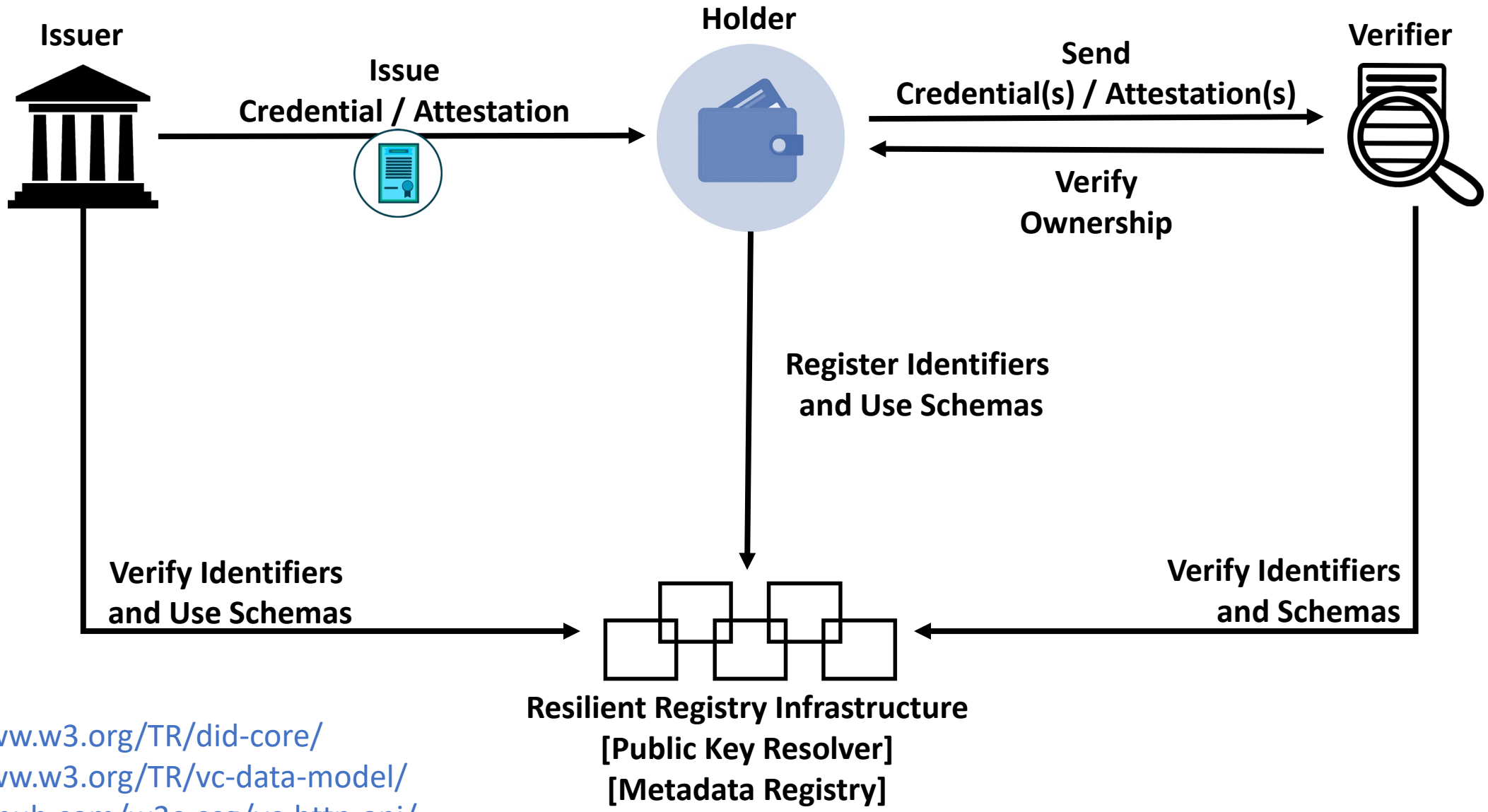
Silicon Valley Innovation Program

DHS-Silicon-Valley@hq.dhs.gov
https://www.dhs.gov/science-and-technology/svip

ANIL JOHN

Digitally signed by ANIL JOHN
Date: 2021.08.23 17:37:52 -04'00'

Credential/Attestation/License/Document Interoperable Issuance & Verification Model



https://www.w3.org/TR/did-core/
https://www.w3.org/TR/vc-data-model/
https://github.com/w3c-ccg/vc-http-api/