Scaling Interoperability

From Principles to Interoperable Implementations

ANIL JOHN | TECHNICAL DIRECTOR

AGENDA

- Introduction
- DHS Operational Need and W3C DID/VC Implementation Patterns
- Implementation Principles
- Standards Profiling Approach
- Q&A

Science and Technology

We are the Department's Science Advisor and research and development arm.

Since 2003, the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) has provided sound, evidence-based scientific and technical perspectives to address a broad spectrum of current and emerging threats.

Delivering Innovative Ideas & Solutions

S&T knows the next ground-breaking idea could come from anywhere. That's why its innovation programs are tailor-made to harness ingenuity and move solutions to the frontlines.

Small Business Innovation Research

Helps small businesses develop and commercialize innovative solutions.

Long-Range Broad Agency Announcement

Provides an open invitation for the innovation community to propose novel solutions for DHS needs.

Prize Competitions

Incentivizes innovation to address homeland security challenges through public crowd-sourcing.

Silicon Valley Innovation Program

Engages the global start-up community to harness commercial R&D for government applications.

DHS Commitment to Working in the Open …

… "Preventing Forgery & Counterfeiting of Certificates and Licenses"

"… in concert with the global technical community, has actively worked together in a public and transparent manner to incubate and move into formal W3C standardization pathways via the W3C Credential Community Group (W3C CCG), a set of emerging specifications that ensure global, multi-vendor interoperability for this technology that is a critical requirement of meeting the needs of DHS.

[…]

It is expected that any company awarded under this [solicitation] will actively participate in and support as relevant to their implementation, these emerging specifications as they mature to become global W3C standards"

PREVENTING FORGERY & COUNTERFEITING OF CERTIFICATES AND LICENSES

Other Transaction Solicitation Call
70RSAT19R00000002

- Open Solicitation on sam.gov in 2018
  - https://go.usa.gov/xexJk
- 200+ applications to the Solicitation
- Highly competitive selection process
- **Multi-tracking 7 Selected Companies**

Solution Shaping and Delivery via Multi-Tracking Competitively Selected Performers

Digital Personal Credentials DHS/USCIS & DHS/PRIV

Danube Tech
Vienna, Austria
https://go.usa.gov/xsqdx

Digital Bazaar
Virginia, USA
https://go.usa.gov/xsqdC

MATTR
Auckland, New Zealand
https://go.usa.gov/xsqdr

SecureKey
Toronto, Canada
https://go.usa.gov/xsqd4
https://go.usa.gov/xsqdT

Digital Trade Credentials DHS/CBP

Mavennet
Toronto, Canada
https://go.usa.gov/xsqpe
https://go.usa.gov/xsqpz

Mesur.io
North Carolina, USA
https://go.usa.gov/xsqpJ

Transmute
Texas, USA
https://go.usa.gov/xsqph

DHS and W3C Standards

W3C Verifiable Credentials Data Model

https://www.w3.org/TR/vc-data-model/#acknowledgements

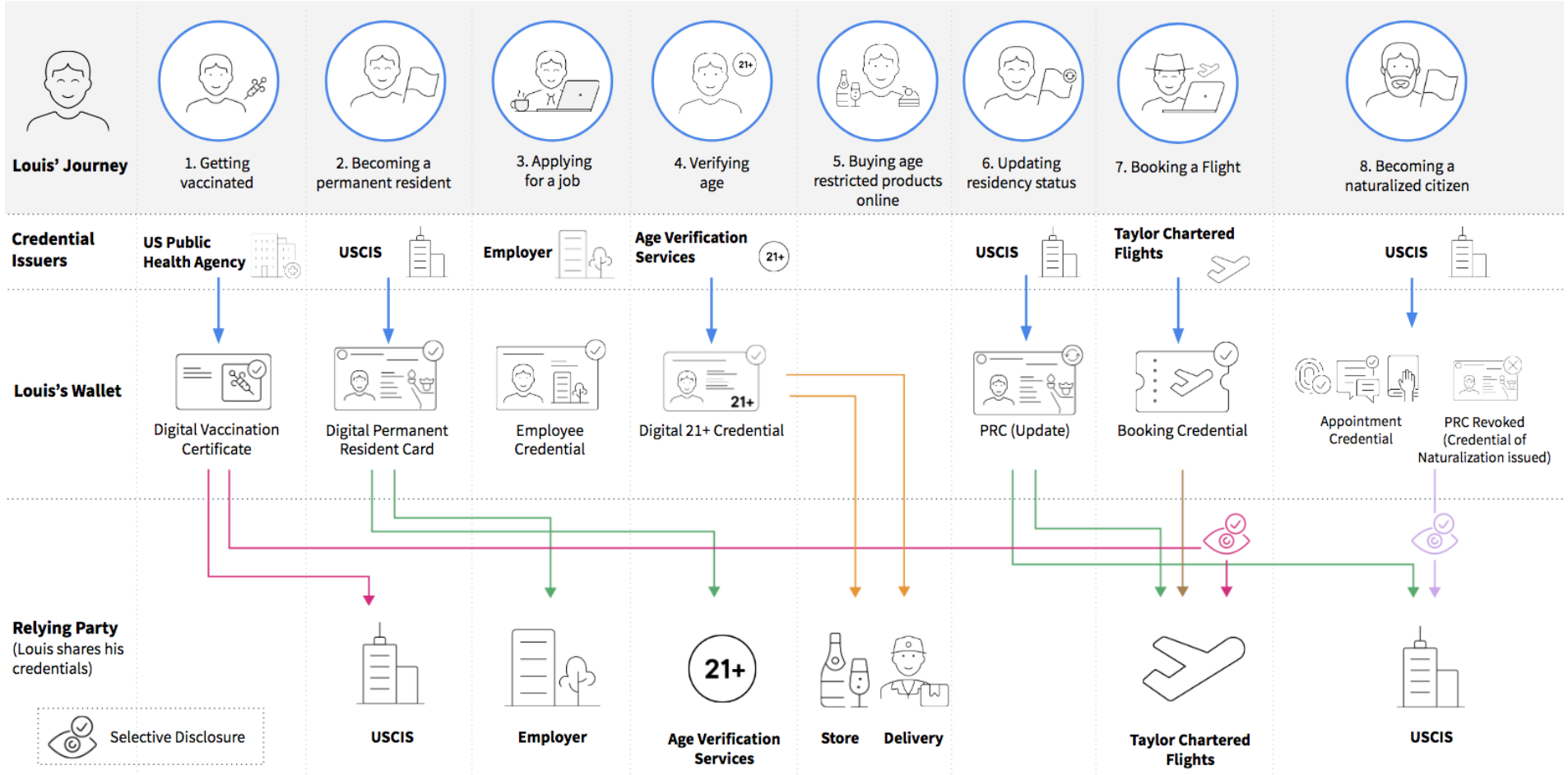
"Portions of the work on this specification have been funded by the United States Department of Homeland Security's Science and Technology Directorate under contract HSHQDC-17-C-00019."

W3C Decentralized Identifiers

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

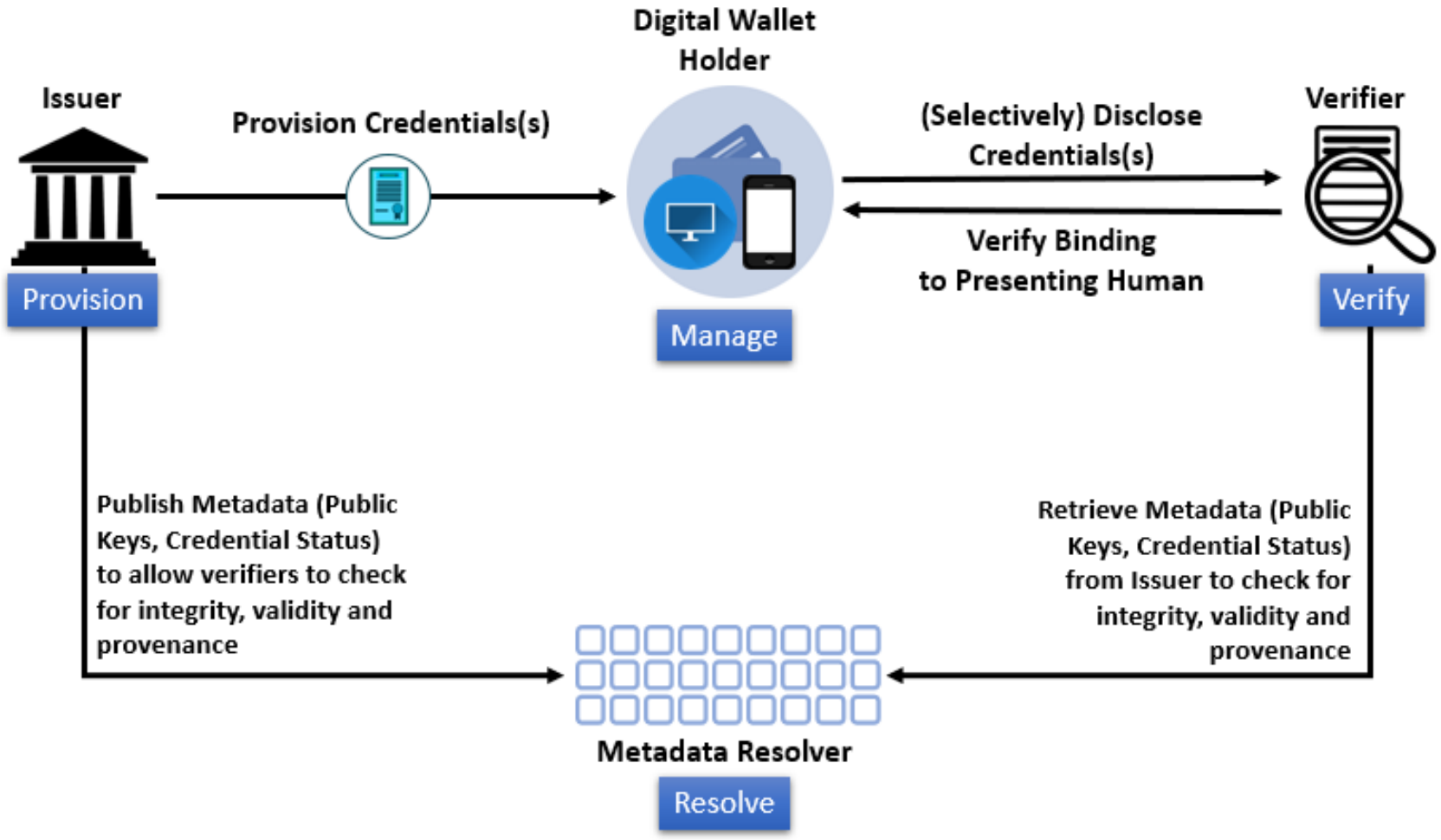
"Portions of the work on this specification have been funded by the United States Department of Homeland Security's (US DHS) Science and Technology Directorate under contracts HSHQDC-16-R00012-H-SB2016-1-002, and HSHQDC-17-C-00019, as well as the US DHS Silicon Valley Innovation Program under contracts 70RSAT20T00000010, 70RSAT20T00000029, 70RSAT20T00000030, 70RSAT20T00000045, 70RSAT20T00000003, and 70RSAT20T00000033."

DHS/U.S. Citizenship and Immigration Services >>
Need for Global Interoperability of US Immigration Credentials



- **Prioritizing privacy and security to ensure individual control and consent over use of data**
- **Equity and access with a bridge to paper to ensure no digital divide**
- **No expectation that everyone uses the same technology platform or vendor**
- **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**

DHS (Personal Credential) Implementation Pattern for W3C VCs & W3C DID Standards

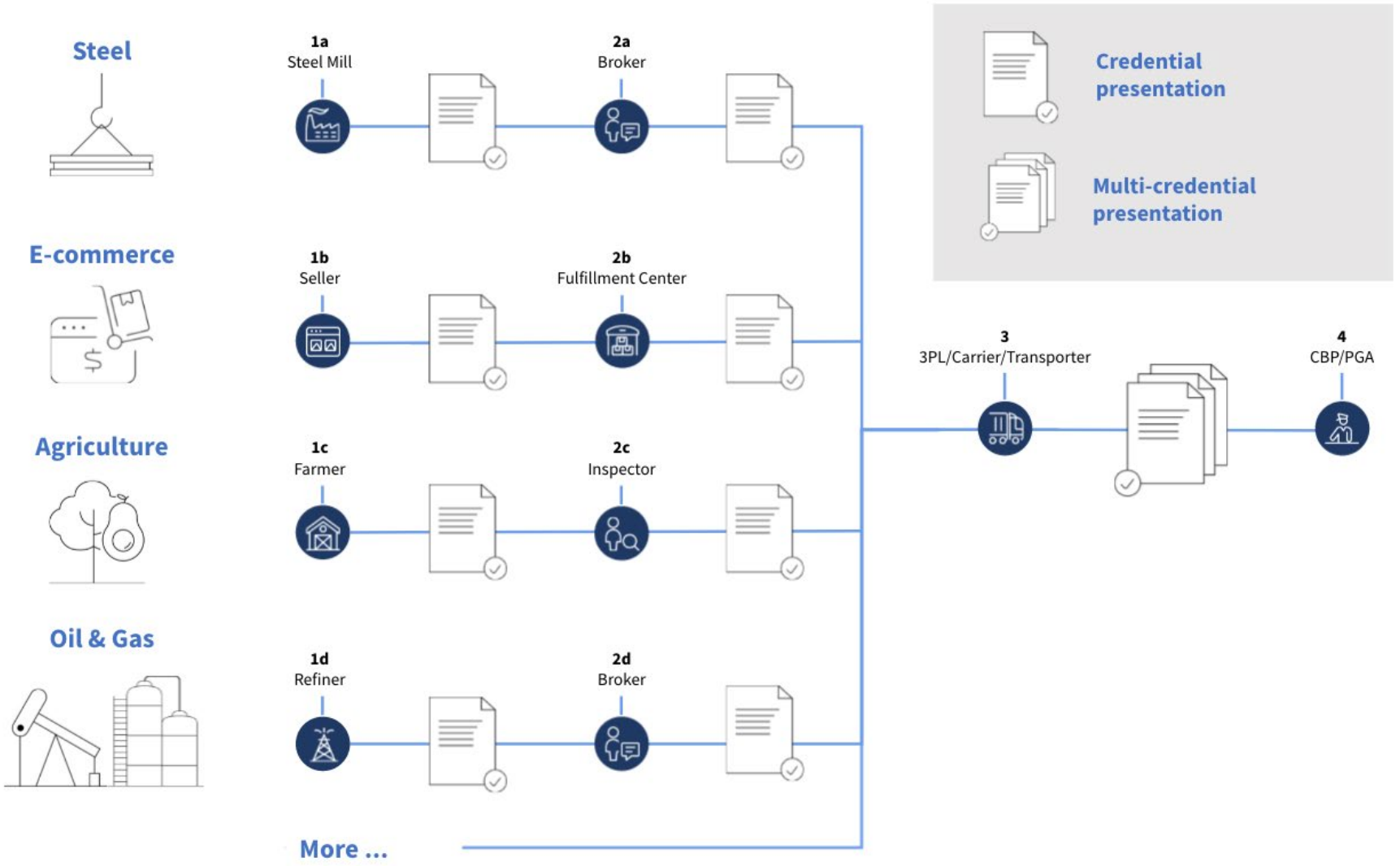


W3C VC/DID architecture is an evolution of existing models that:

- Enables an USG individual customer to have agency and control over their data
- Addresses the "phone home" problem in PKI, SAML, OIDC, App based models
- Provides credential aggregation and selective disclosure with informed consent
- Removes the conflation of identifiers and authenticators when addressing entities
- Supports global resolution of an Issuer's identifier to its public key(s) & their distribution
- Can be profiled to support USG security, privacy and interoperability requirements

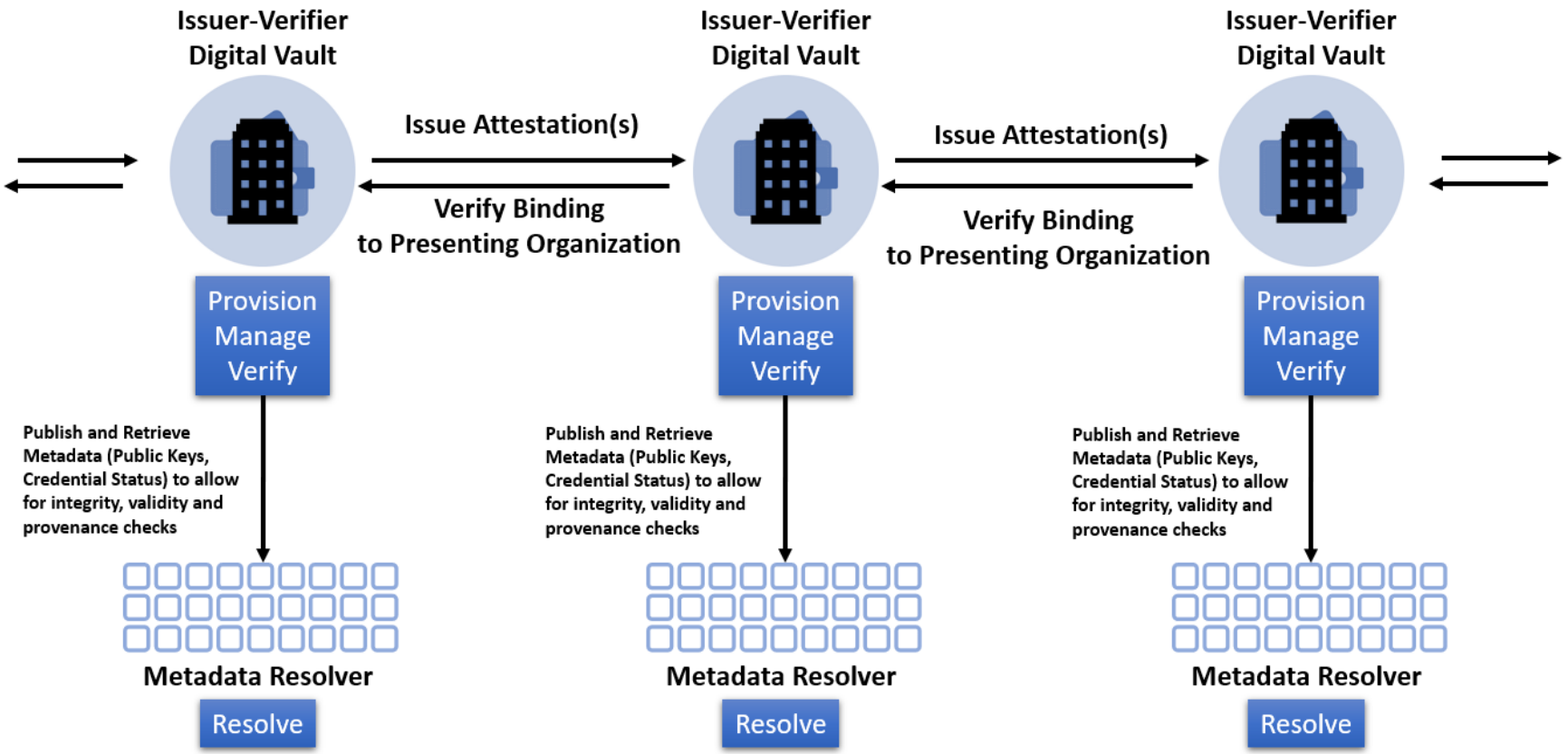
- The W3C VC Data Model Standard identifies an abstract component called a "Verifiable Data Registry" which in our implementation we refer to as a "Metadata (or Public Key) Resolver"
- USCIS supports and requires a Bring-Your-Own-W3C-DID-in-Digital-Wallet for digital immigration credential implementation

DHS/U.S. Customs and Border Protection >>
Need for 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

DHS (Organizational Credential) Implementation Pattern for W3C VCs & W3C DID Standards



W3C VC/DID architecture is an evolution of existing models that:

- Provides supply chain visibility to U.S. Customs using global, open, royalty free and free to use standards
- Enables an organization to mitigate platform/vendor lock-in risk
- Provides credential aggregation and presentation
- Removes the conflation of identifiers and authenticators when addressing entities
- Supports global resolution of an Issuer's identifier to its public key(s) & their distribution
- Can be profiled to support USG security, privacy and interoperability requirements

- The W3C VC Data Model Standard identifies an abstract component called a "Verifiable Data Registry" which in our implementation we refer to as a "Metadata (or Public Key) Resolver"
- U.S. Customs requires visibility and transparency of entities in the supply chain

DHS/Office of Privacy >>
Need for an Alternative Identifier to the SSN

Functional Requirements

- The identifier is meaningless but unique – globally!
- The identifier does not "leak" PII or sensitive information
- Public exposure does not allow its use as an authenticator
- When needed and allowed by policy, can be shared and resolved across systems, agencies and organizations

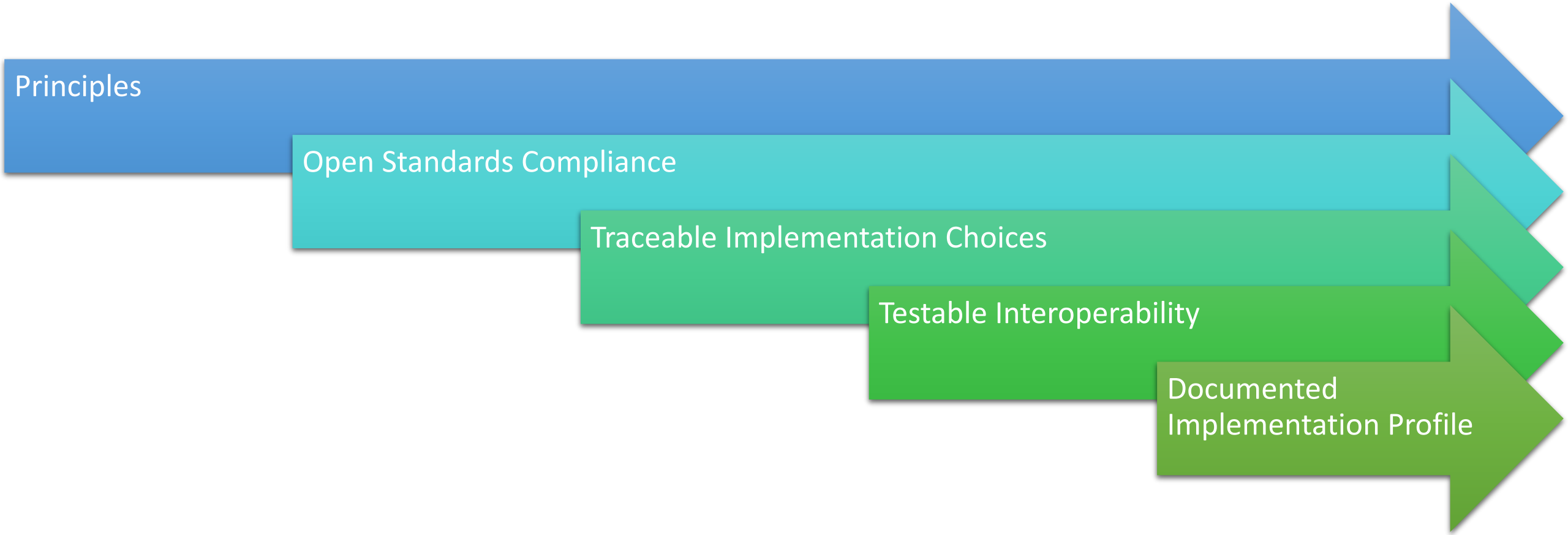
Non-Functional Risk Mitigation

- Implementation needs to add value beyond policy compliance!
- Commercially viable such that DHS and USG are not held hostage to a GOTS O&M long tail
- Global standards-based support to ensure interoperability across and availability within diverse future COTS products

Use Cases

1. An organization, as part of its regular mission / business process, collects an SSN from a person. The collected SSN is immediately replaced with a DID.
   - The SSN is put into an "Encrypted Vault" such that the operational system that collected the SSN no longer has direct access or uses the SSN in its business process.
   - The SSN can only be accessed using a constrained approval workflow process
2. Two separate organizations utilize the mechanism in (1) in order to replace an SSN with a DID. Determine if they are interacting with the same person/SSN.
   - A constrained "comparison / matching" service that provides the ability to discover if the DID assigned by Organization 1 and the DID assigned by Organization 2 map to the same SSN i.e., the same person, without direct sharing of the SSN between the two organizations

Principles > to > Scalable Interoperability



Principles > to > Implementation Choices
((Personal & Organizational Credential Workstreams))

Encourage and support a plurality of **independent, interoperable, standards-based implementations** to counter vendor/technology lock-in and perverse incentives that accrue market power to entities that can result in a gatekeeper functionality between the Government and its customers

- ✓Working in the open (e.g. via the W3C Credential Community Group) to build vocabularies, test suites, APIs and all other artifacts needed to support our deployment
- ✓Ensuring that the artifacts we fund/build encourage and accept contributions from the global technical community and are available freely to anyone who wants to use them
- ✓Require interoperability plug-fests (of companies under contract) to ensure true multi-platform, multi-vendor interoperability AND we share with the global community what choices we are making to enable such interoperability
- ✓DHS will not require and have no plans to support digital wallets/vaults that require a MOU/business relationship with the wallet/vault vendor, and require the use of proprietary digital wallet/vault APIs
- ✓Mitigate business and technology risk by multi-tracking support for innovative companies and communities building and using emerging interoperability specifications and mature standards to enable a competitive, diverse marketplace of potential solutions

Principles > to > Implementation Choices ((Personal Credential Workstream))

U.S. Citizenship and Immigration Services

Not a requirement; **a choice!**

- ✓ Customer receives a physical PRC by mail
- ✓ Insert in the PRC mailer informs Customer about the option to request a digital credential
- ✓ Customer must explicitly request a digital credential using unique code found in the mailer

Eliminate **"phone home"** architecture/technology/implementations

- ✓ Use of the W3C VC architecture breaks the direct link between Issuer (USCIS) and Verifiers
- ✓ Use of herd privacy enabled revocation status check capability (https://w3c-ccg.github.io/vc-status-list-2021/) that blinds the Issuer (USCIS) to Customer interactions using the issued credential

Eliminate **"back-channel" interactions** between verifiers of the credential and the issuer (USCIS) which are not visible to the credential holder (Customer)

- ✓ Issuer (USCIS) WILL NOT implement or respond to credential refresh requests directly from a Verifier
- ✓ Credential refresh WILL require the holder (Customer) to be explicitly in the loop

Support for **selective disclosure capabilities** to provide the holder of the credential (Customer) granular control over what information they can share and when

- ✓ Support for BBS+ Pairing Based Signatures to provide selective disclosure with consent

A (contractually required) Commitment to Standards and Multi-Vendor/Platform Interoperability

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

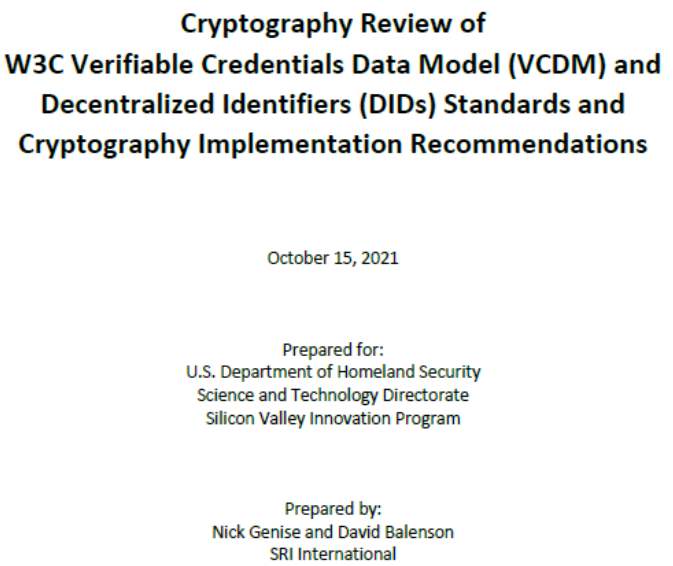
This is not enough!

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”

Beyond Plug-Fests and Implementations

- To scale interoperability beyond the just the plug-fest participants, we are documenting the results and lessons from the DHS sponsored multi-platform, multi-vendor Interoperability Plug-fests to develop a **"DHS Implementation Profile of W3C Verifiable Credentials and Decentralized Identifiers"** to ensure the use of Security, Privacy and Interoperability implementation choices that are acceptable to the USG, and can be utilized by anyone
  - *NOTE: A "profile" of a standard remains fully standard compliant but makes explicit choices within the scope of the standard to satisfy specific security, privacy and interoperability criteria. At a minimum, we are using as input:*
    - W3C Verifiable Credentials Data Model
    - W3C Decentralized Identifiers
    - W3C VC-API + Traceability Extensions
    - …
- Practical Testing of the USG required cryptography as recommended by an independent cryptography review of W3C VC & DID standards
  - http://www.csl.sri.com/papers/vcdm-did-crypto-recs/
- Demonstrate the Incorporation of Digital Wallet UI Prize Challenge Lessons Learned
  - https://github.com/DHS-SVIP/digital-wallet-ui



Cryptography Review of
W3C Verifiable Credentials Data Model (VCDM) and Decentralized Identifiers (DIDs) Standards and Cryptography Implementation Recommendations

October 15, 2021

Prepared for:
U.S. Department of Homeland Security
Science and Technology Directorate
Silicon Valley Innovation Program

Prepared by:
Nick Genise and David Balenson
SRI International

DHS Implementation Profile of W3C Verifiable Credentials Data Model and W3C Decentralized Identifiers (1/4)

- Entity Identifiers
  - Informative
  - Normative
  - Conformance Test
- Entity Metadata Distribution
  - Informative
  - Normative
  - Conformance Test
- Entity Metadata Resolution
  - Informative
  - Normative
  - Conformance Test
- Unlinkability (Personal Credentials)
  - Informative
  - Normative
  - Conformance Test
- Traceability (Organizational Credentials)
  - Informative
  - Normative
  - Conformance Test
- Cryptographic Flexibility
  - FIPS Compliant Cryptography
  - Quantum-Resistant Cryptography
  - Selective Disclosure Cryptography

DRAFT
Work In Progress

DHS Implementation Profile of W3C Verifiable Credentials Data Model and W3C Decentralized Identifiers (2/4)

- Credential Data Model
  - Informative
  - Normative
  - Conformance Test
- Credential Delivery to Digital Wallet
  - Informative
  - Normative
  - Conformance Test
- Credential Delivery to Digital Vault
  - Informative
  - Normative
  - Conformance Test
- Credential Verification
  - Informative
  - Normative
  - Conformance Test

DRAFT
Work In Progress

- Credential Revocation
  - Informative
  - Normative
  - Conformance Test
- Credential Refresh
  - Informative
  - Normative
  - Conformance Test
- Credential Aggregation
  - Informative
  - Normative
  - Conformance Test
- Credential Selective Disclosure
  - Informative
  - Normative
  - Conformance Test

DHS Implementation Profile of W3C Verifiable Credentials Data Model and W3C Decentralized Identifiers (3/4)

- Consent to Share Data with Verifier
  - Informative
  - Normative
  - Conformance Test
- Notification to Credential Holder about Verifier's Intended Use of Shared Data
  - Informative
  - Normative
  - Conformance Test
- Digital Wallet Selector
  - Informative
  - Normative
  - Conformance Test
- Intent Signaling
  - By Issuer
  - By Wallet/Vault
  - By Verifier
- Digital Wallet/Vault Feature Detection
  - Independent Testing
  - Cryptographic Challenge/Response
  - Certification and Accreditation by Third Parties

DRAFT
Work In Progress

DHS Implementation Profile of W3C Verifiable Credentials Data Model and W3C Decentralized Identifiers (4/4)

Workflows / Journeys

- Personal Credential Issuance Workflow
  - A.1 + B.1 + C.1 ….
  - Conformance Test
- Personal Credential Verification Workflow (Remote)
  - X.1 + Y.1 + C.1 …
  - Conformance Test
- Personal Credential Verification Workflow (In-Person)
  - X.1 + Y.1 + C.1 …
  - Conformance Test
- Organizational Credential Issuance Workflow
  - A.2 + B.2 + C.2 …
  - Conformance Test
- Organizational Credential Verification Workflow
  - X.2 + Y.2 + C.2
  - Conformance Test

Vocabularies

- W3C CCG Citizenship Vocabulary
- W3C CCG Traceability Vocabulary
- …

DRAFT
Work In Progress

References

- W3C Verifiable Credentials Data Model
  https://www.w3.org/TR/vc-data-model/
- W3C Decentralized Identifiers
  https://www.w3.org/TR/did-core/
- CCG Citizenship Vocabulary
  https://w3c-ccg.github.io/citizenship-vocab/
- CCG Supply Chain Traceability Vocabulary
  https://w3c-ccg.github.io/traceability-vocab/
- CCG Traceability Interoperability
  https://w3c-ccg.github.io/traceability-interop/
- CCG Verifiable Credentials HTTP API
  https://w3c-ccg.github.io/vc-api/
- W3C VC & W3C DID Cryptography Review
  http://www.csl.sri.com/papers/vcdm-did-crypto-recs/
- BBS Signature Scheme
  https://identity.foundation/bbs-signature/draft-looker-cfrg-bbs-signatures.html
- JSON Encoding for Post Quantum Signatures
  https://datatracker.ietf.org/doc/draft-prorock-cose-post-quantum-signatures/
- Wallet Selector Playground (CHAPI)
  https://chapi.io/

Science & Technology

Thank You

Silicon Valley Innovation Program

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