dhs.gov/science-and-technology/svip

dhs-silicon-valley@hq.dhs.gov

DHS Science & Technology Directorate

SILICON VALLEY INNOVATION PROGRAM

ANIL JOHN | TECHNICAL DIRECTOR

Can Blockchain Help Prevent Forgery and Counterfeiting?

How the DHS mission drives R&D and
how we work with innovative startups globally to solve hard local problems

DHS Missions

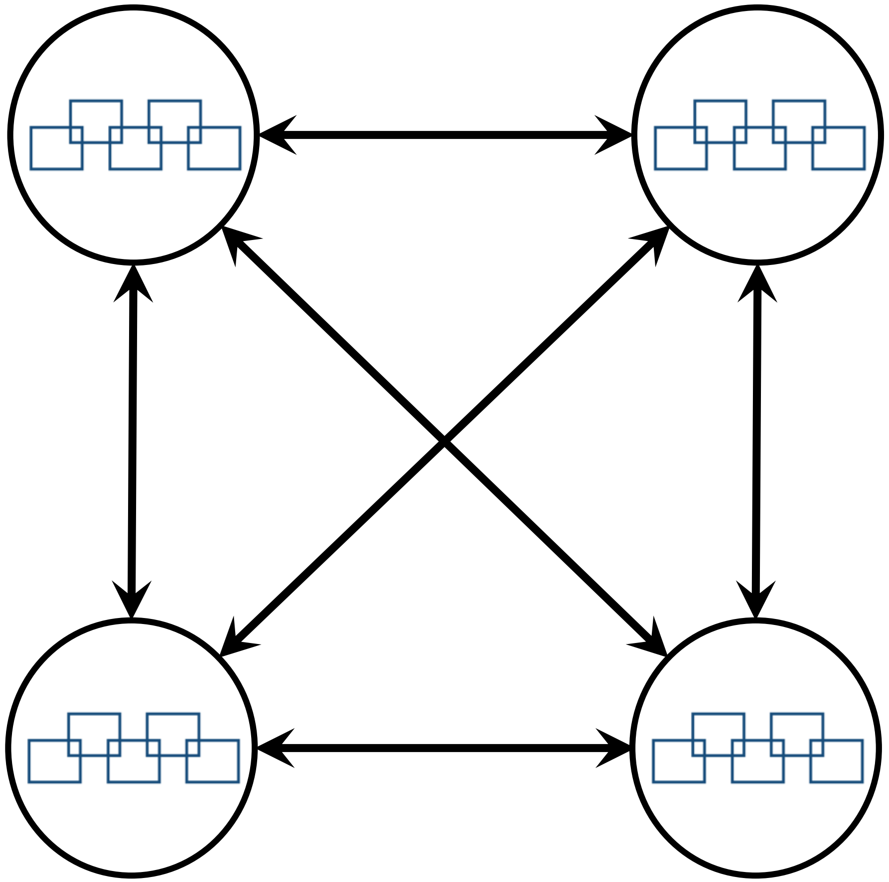
1. Counter Terrorism and Homeland Security Threats
2. Secure U.S. Borders and Approaches
3. Secure Cyberspace and Critical Infrastructure
4. Preserve and Uphold the Nation’s Prosperity and Economic Security
5. Strengthen Preparedness and Resilience
6. Champion the DHS Workforce and Strengthen the Department

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

- 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)**

Blockchain (A Definition for Humans)

- An authoritative book of records …
  - With many copies that are kept synchronized
  - In which multiple parties can create individual records
  - Using consensus to determine the validity and order of written records
  - Where each record is linked to the prior one
  - Ensuring that written records cannot be modified or deleted without alerting the readers of the book



5 Years Ago – Is Blockchain Relevant to DHS?

Security and Privacy

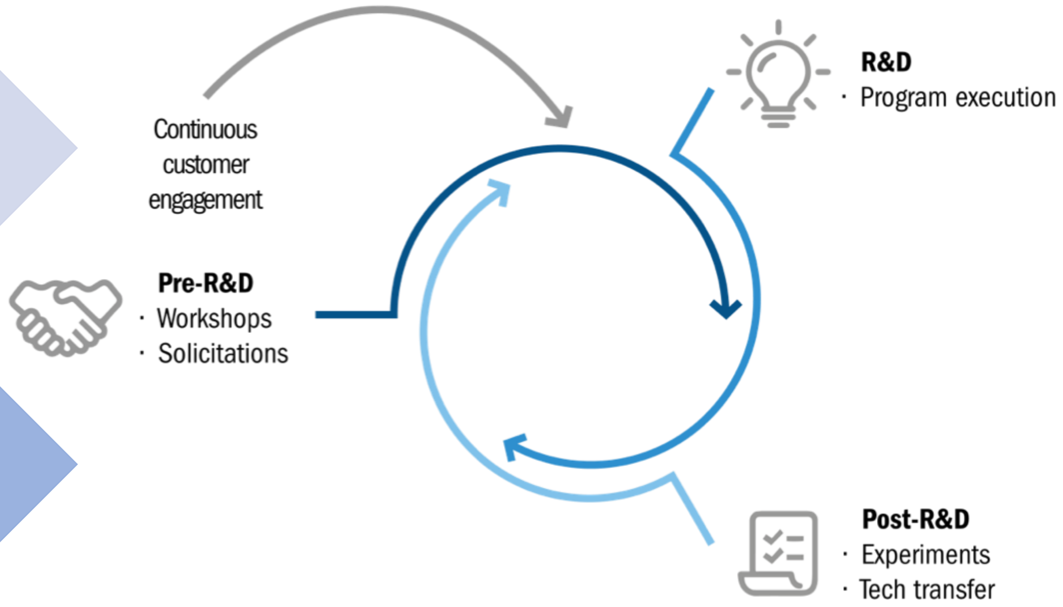
- Confidentiality, Integrity, Availability …
- Pseudonymous Operations, Selective Disclosure …

Integration Approaches & Gain/Pain

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

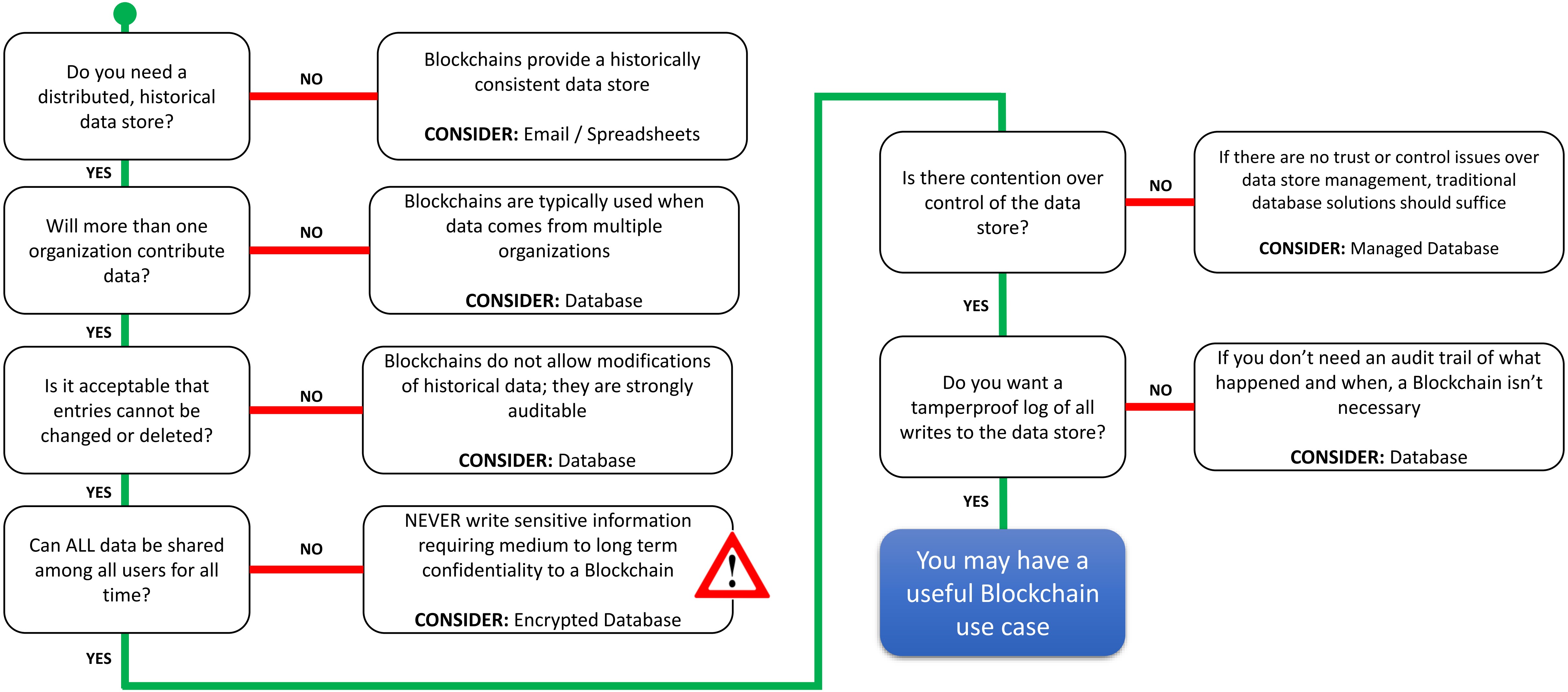
Digital Currency Forensics

- Anonymous Currencies
- Anonymous Networks



Proof of Concept → Pilot Deployment → Operational Deployment

Most Organizations Don’t Need A Blockchain



Do you need a distributed, historical data store?

NO

Blockchains provide a historically consistent data store

CONSIDER: Email / Spreadsheets

YES

Will more than one organization contribute data?

NO

Blockchains are typically used when data comes from multiple organizations

CONSIDER: Database

YES

Is it acceptable that entries cannot be changed or deleted?

NO

Blockchains do not allow modifications of historical data; they are strongly auditable

CONSIDER: Database

YES

Can ALL data be shared among all users for all time?

NO

NEVER write sensitive information requiring medium to long term confidentiality to a Blockchain

CONSIDER: Encrypted Database

YES

Is there contention over control of the data store?

NO

If there are no trust or control issues over data store management, traditional database solutions should suffice

CONSIDER: Managed Database

YES

Do you want a tamperproof log of all writes to the data store?

NO

If you don’t need an audit trail of what happened and when, a Blockchain isn’t necessary

CONSIDER: Database

YES

You may have a useful Blockchain use case

If You Do Need A Blockchain, Be Aware …

- **Architecture and design** cannot be hand-waved away (but often is in the race for market share!)
- There is no one-size-fits-all **ledger data format**, and **standards** for how to create the “data payload” that is written to a ledger are critical to **interoperability** across Blockchain implementations
- Immutability of records combined with encryption as a privacy tool is gated by the reality that **encryption has a time to live** which will eventually run out; this has real privacy and design implications
- **Distributed key management** is not a solved problem, but needs to be for scalable deployment
- **Smart contracts are relatively immature** and the contract execution environment must balance the security needs of the node with providing a richer (more error-prone) language

AND MORE …

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
2. Invest in business driven proof-of-concepts to identify scalable integration architectures and determine adoption Gain/Pain ratio
3. Motivate and shape innovative and potentially risky product development via the S&T Silicon Valley Innovation Program (SVIP) to meet mission challenges

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

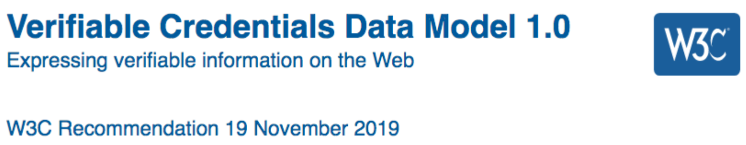
2. Invest in business driven proof-of-concepts to identify scalable integration architectures and determine adoption Gain/Pain ratio

3. Motivate and shape innovative and potentially risky product development via the S&T Silicon Valley Innovation Program (SVIP) to meet mission challenges

Develop and Champion Globally Interoperable Standards and Specifications

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
  - …



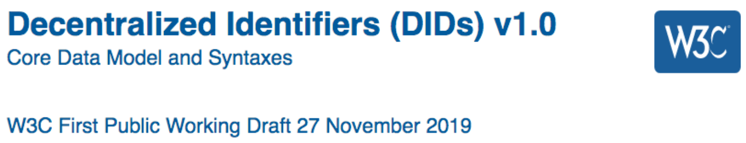
Verifiable Credentials Data Model 1.0

Expressing verifiable information on the Web

W3C Recommendation 19 November 2019

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 Data Model and Syntaxes

W3C First Public Working Draft 27 November 2019

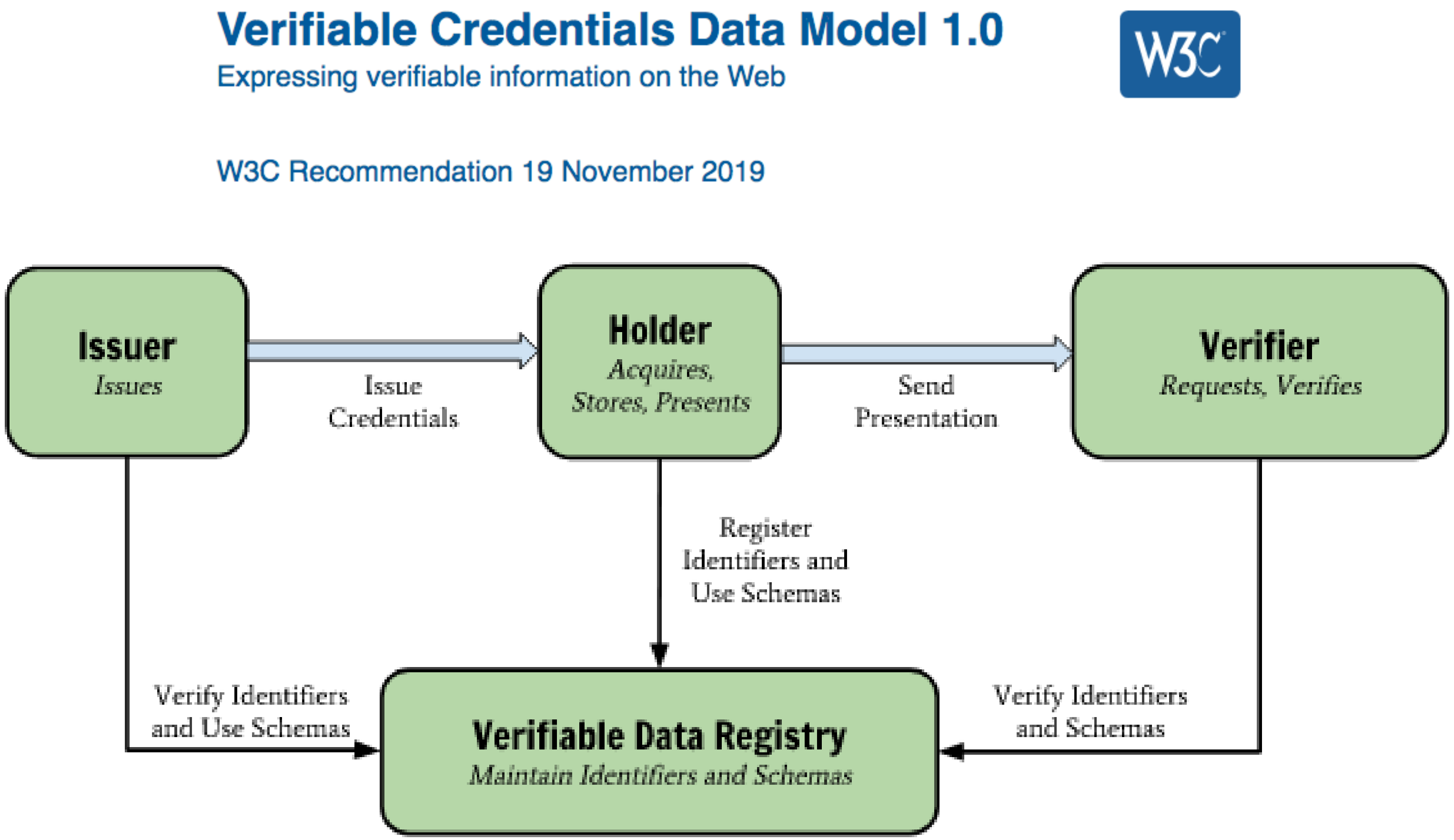
Multi-Party Distributed Key Management

- Tackling the hard challenge of distributed key management
  - Provisioning
  - Revocation
  - Re-Issuance
- Emerging W3C Specifications
  - Secure Data Stores
  - WebKMS
  - Revocation List 2020
- Path to Standardization – W3C

What is a Verifiable Credential (VC)?

A set of claims made by an Issuer about a Subject (Holder of the Credential) in a manner that is:

- Tamper evident
- Cryptographically verifiable
- Privacy respecting



Verifiable Credentials Data Model 1.0

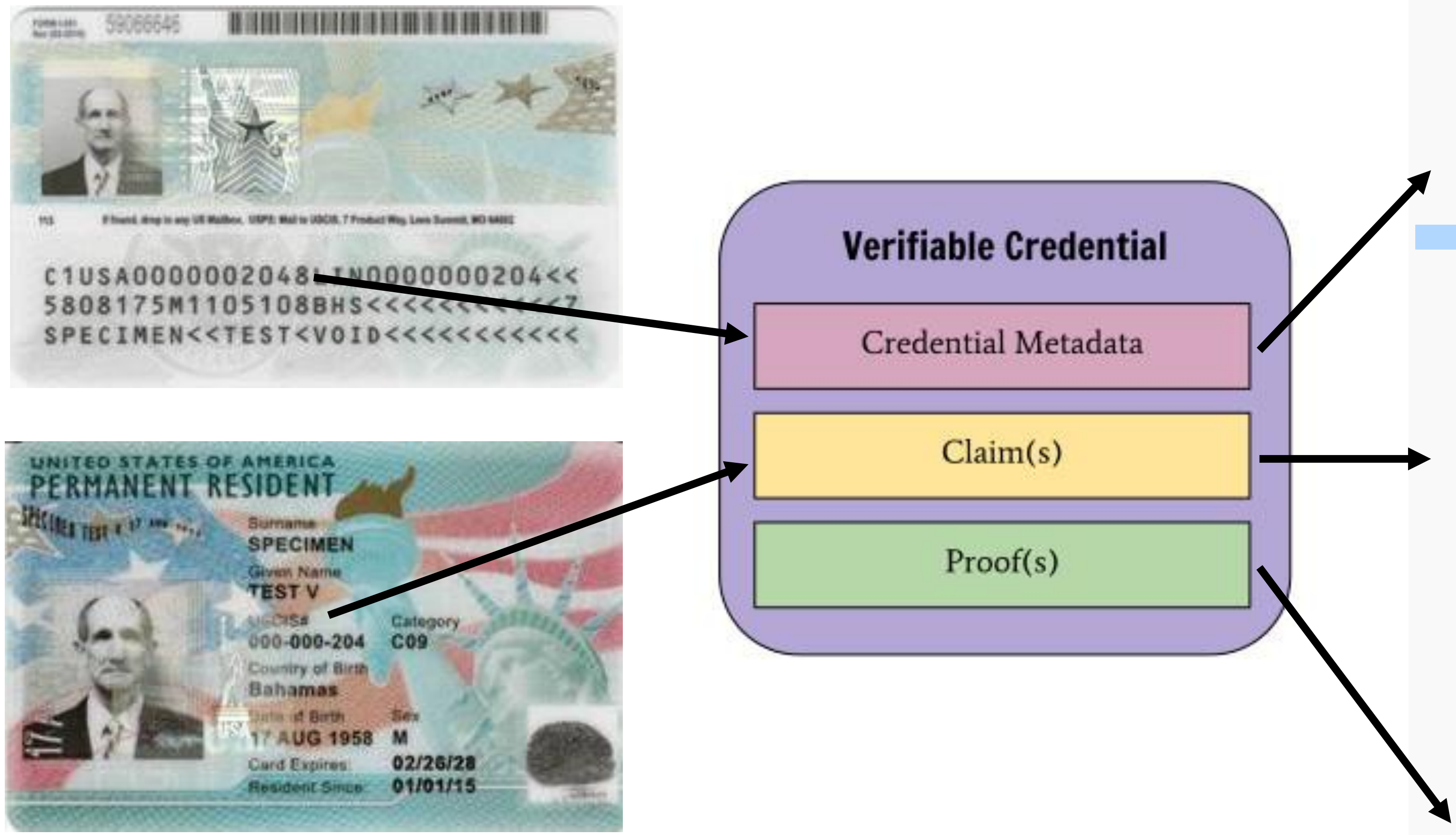
Expressing verifiable information on the Web

W3C Recommendation 19 November 2019

W3C
Issuer
Issues
Issue Credentials
Holder
Acquires, Stores, Presents
Send Presentation
Verifier
Requests, Verifies
Register Identifiers and Use Schemas
Verify Identifiers and Use Schemas
Verifiable Data Registry
Maintain Identifiers and Schemas
Verify Identifiers and Schemas

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

Verifiable Credential Data Model

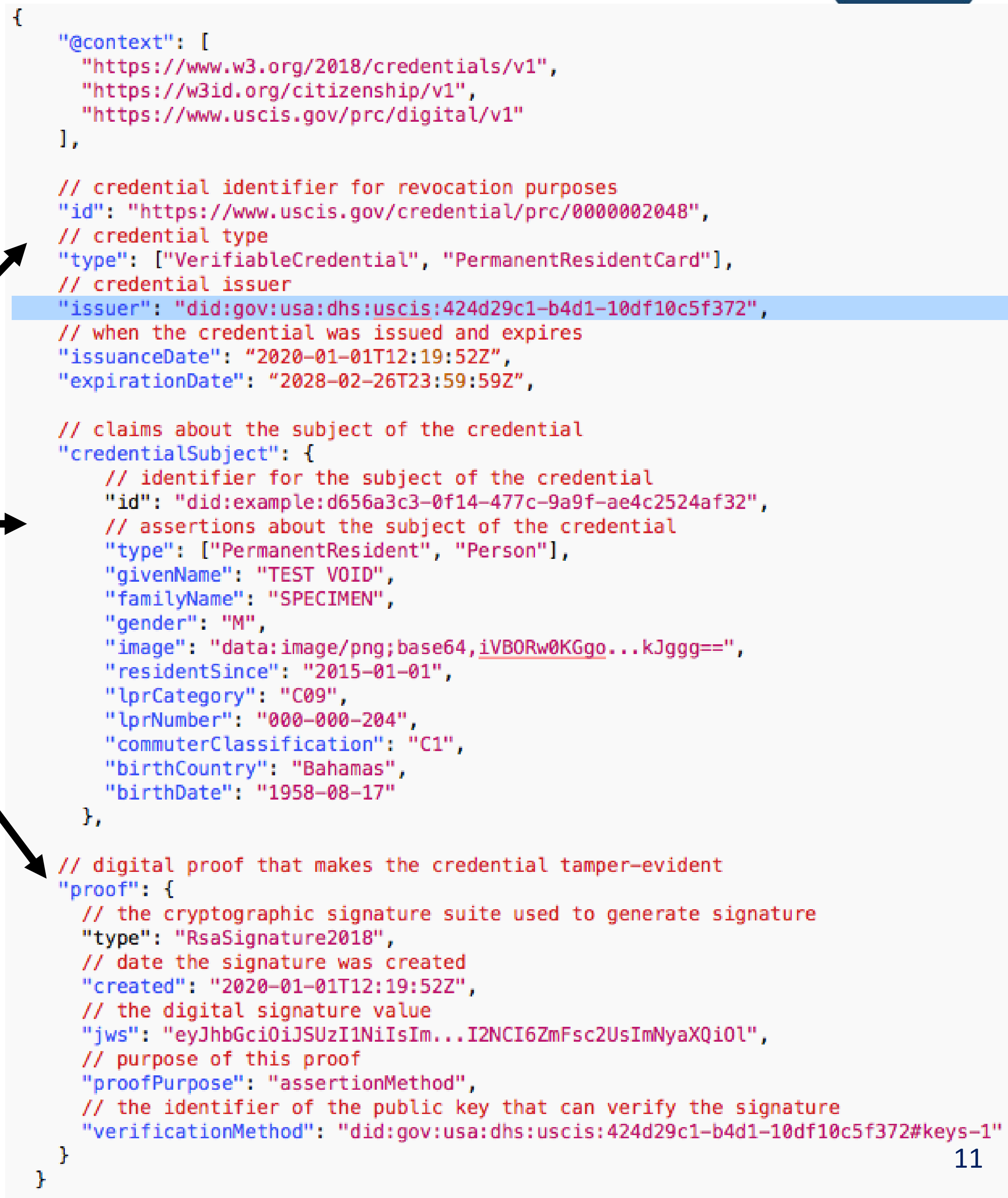


Verifiable Credential

Credential Metadata

Claim(s)

Proof(s)



```
{
    "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://w3id.org/citizenship/v1",
      "https://www.uscis.gov/prc/digital/v1"
    ],

    // credential identifier for revocation purposes
    "id": "https://www.uscis.gov/credential/prc/0000002048",
    // credential type
    "type": ["VerifiableCredential", "PermanentResidentCard"],
    // credential issuer
    "issuer": "did:gov:usa:dhs:uscis:424d29c1-b4d1-10df10c5f372",
    // when the credential was issued and expires
    "issuanceDate": “2020-01-01T12:19:52Z”,
    "expirationDate": “2028-02-26T23:59:59Z”,

    // claims about the subject of the credential
    "credentialSubject": {
        // identifier for the subject of the credential
        "id": "did:example:d656a3c3-0f14-477c-9a9f-ae4c2524af32",
        // assertions about the subject of the credential
        "type": ["PermanentResident", "Person"],
        "givenName": "TEST VOID",
        "familyName": "SPECIMEN",
        "gender": "M",
        "image": "data:image/png;base64,iVBORw0KGgo...kJggg==",
        "residentSince": "2015-01-01",
        "lprCategory": "C09",
        "lprNumber": "000-000-204",
        "commuterClassification": "C1",
        "birthCountry": "Bahamas",
        "birthDate": "1958-08-17"
      },

    // digital proof that makes the credential tamper-evident
    "proof": {
      // the cryptographic signature suite used to generate signature
      "type": "RsaSignature2018",
      // date the signature was created
      "created": "2020-01-01T12:19:52Z",
      // the digital signature value
      "jws": "eyJhbGciOiJSUzI1NiIsIm...I2NCI6ZmFsc2UsImNyaXQiOl",
      // purpose of this proof
      "proofPurpose": "assertionMethod",
      // the identifier of the public key that can verify the signature
      "verificationMethod": "did:gov:usa:dhs:uscis:424d29c1-b4d1-10df10c5f372#keys-1"
    }
  }
```

What is a Decentralized Identifier (DID)?

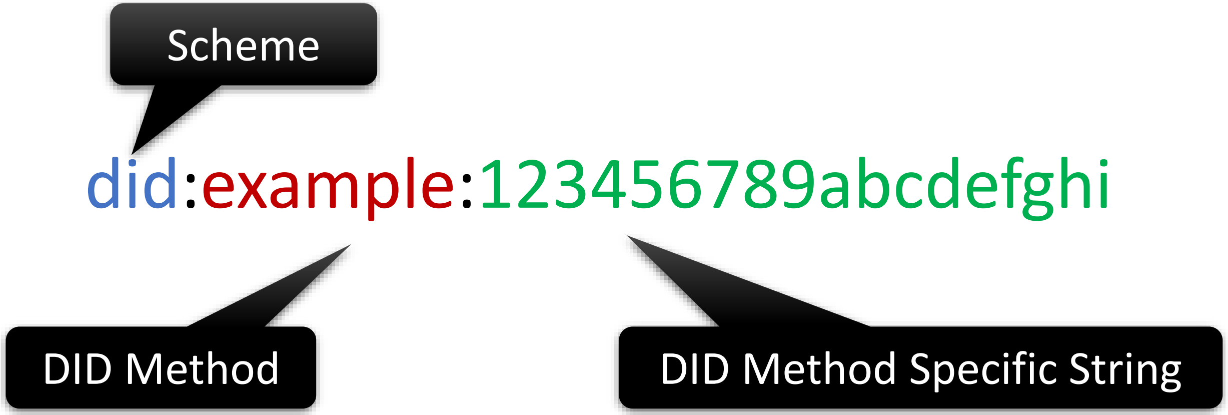
A meaningless but unique identifier that is:

- Immutable over time
- Globally resolvable
- Privacy respecting
- Cryptographically verifiable

DIDs identify
Issuers, Holders and Verifiers

Decentralized Identifiers (DIDs) v1.0
Core Data Model and Syntaxes

W3C First Public Working Draft 27 November 2019

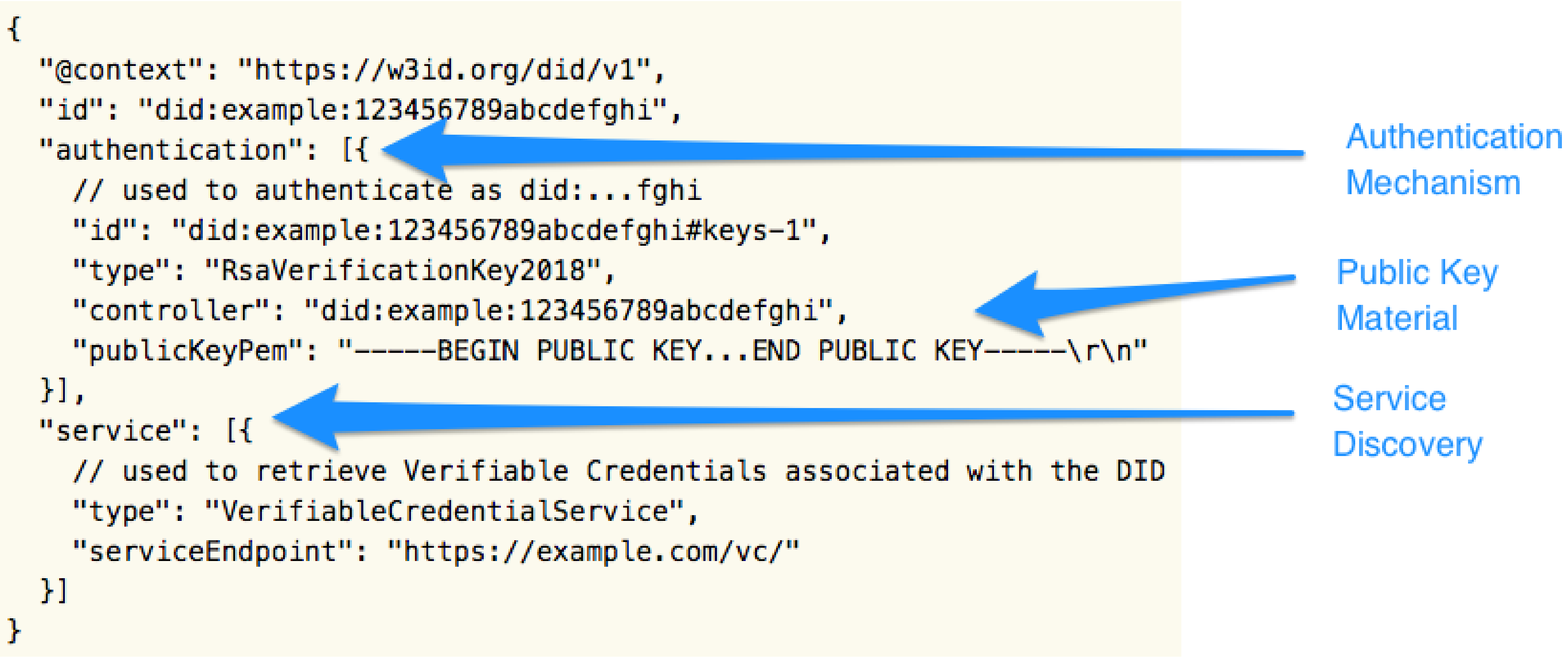


Example(s)

did:gov:usa:dhs:cbp:123abcde
did:gov:usa:dhs:tsa:456abcdfe
did:gov:usa:dhs:uscis:789abcd

https://w3c.github.io/did-core/

DIDs Resolve to DID Documents



```
{
  "@context": "https://w3id.org/did/v1",
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    // used to authenticate as did:...fghi
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "RsaVerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyPem": "-----BEGIN PUBLIC KEY...END PUBLIC KEY-----\r\n"
  }],
  "service": [{
    // used to retrieve Verifiable Credentials associated with the DID
    "type": "VerifiableCredentialService",
    "serviceEndpoint": "https://example.com/vc/"
  }]
}
```

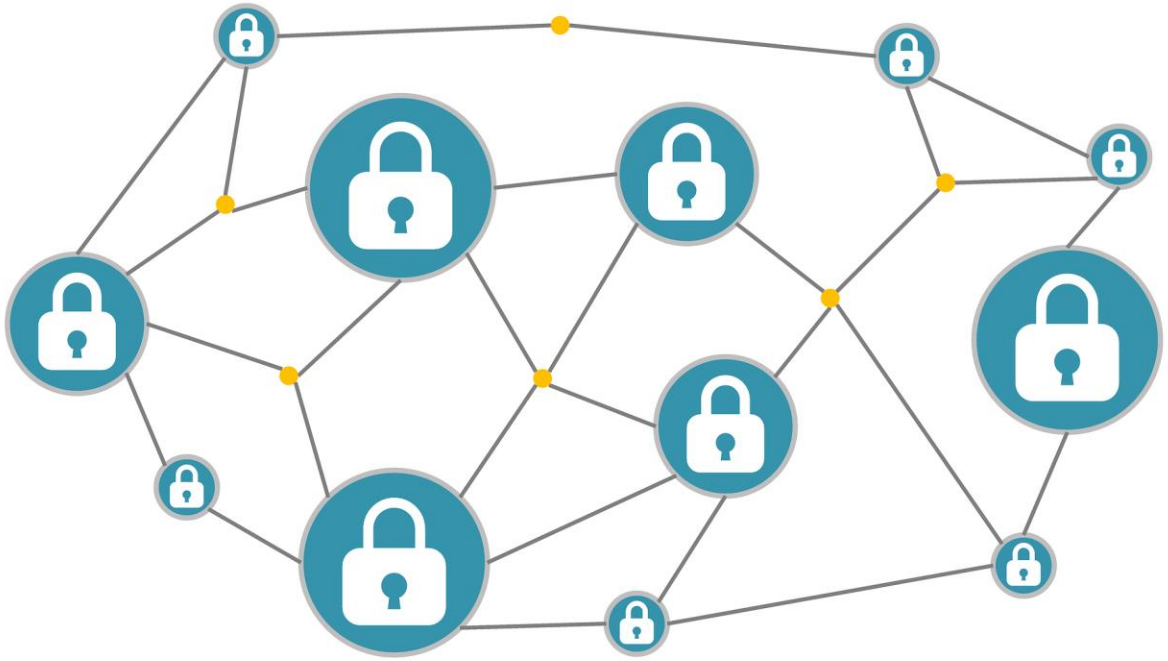
Authentication Mechanism

Public Key Material

Service Discovery

What is Multi-Party Distributed Key Management?

- The hard challenge of distributed key management
  - Provisioning
  - Revocation
  - Re-Issuance
- Supports Cross-Enterprise Managed Deployments
  - Secure Data Stores (Encrypted Data Vaults)
    - https://identity.foundation/secure-data-store/
  - WebKMS
    - https://w3c-ccg.github.io/webkms/
  - Revocation List 2020
    - https://w3c-ccg.github.io/vc-status-rl-2020/
- Potential Path to Standardization – W3C



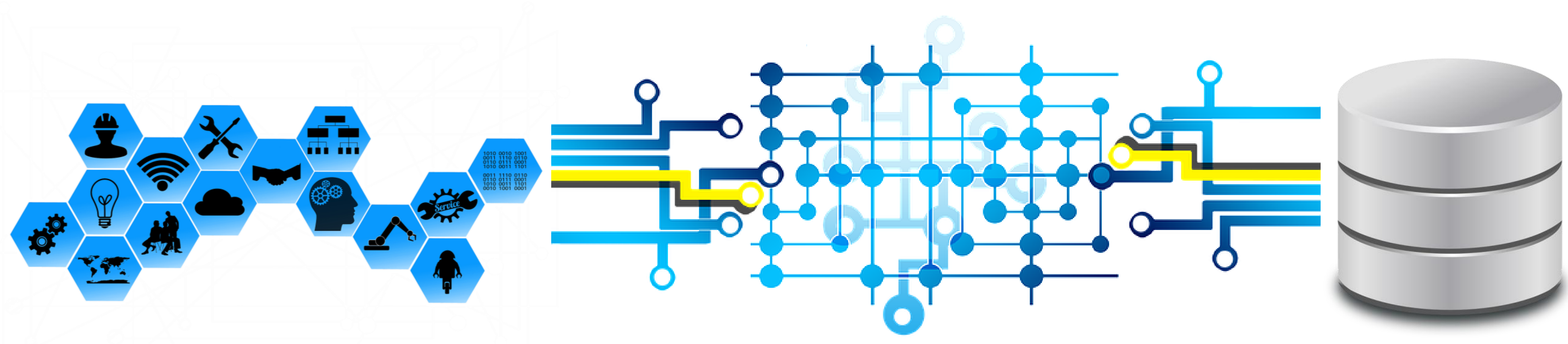
Strategic Approach to Ensure a Competitive, Interoperable Marketplace of Solution Providers

1. Help develop and champion interoperability standards and specifications that are patent free, royalty free and free to implement

2. Invest in business driven proof-of-concepts to identify scalable integration architectures and determine adoption Gain/Pain ratio

3. Motivate and shape innovative and potentially risky product development via the S&T Silicon Valley Innovation Program (SVIP) to meet mission challenges

POC: Authenticity and Integrity of IoT Device, Camera and Sensor Data



SVIP and CBP/Border Patrol proof of concept on implementing anti-spoofing capabilities on cameras and sensors using NPE identity and blockchain technology

This project made clear the architecture choices and design decisions inherent in building an immutable record of data coming from cameras, sensors and IoT devices.

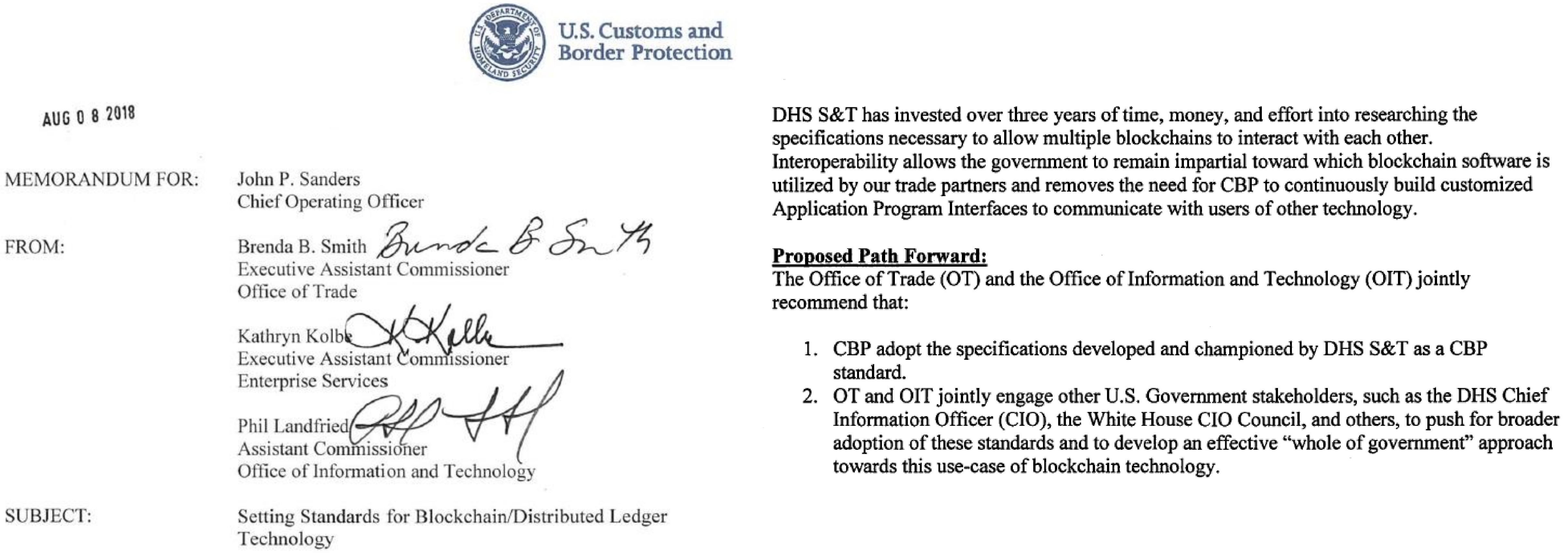
POC: Enhancing the Entry Submission Process to Streamline International Trade Facilitation

- Digital entry submission of Certificates of Origin and implementing their integrity and provenance verification
- Assessment criteria for DHS CBP and S&T included Legal, Policy and Technical aspects
- What we tested and demonstrated:
  - Data level Interoperability across multiple blockchains using emerging specifications combined with mature standards
  - Architecture model that segregates private off-chain and shared non-sensitive on-chain data
  - Fine grained access control allowing US Customs to get real time access to sensitive data owned by trading partners

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

- Increase the ability for CBP Officers, retailers, and end consumers to rapidly and cost effectively determine whether or not a particular product is being legally imported to the country
- What we tested and demonstrated:
  - Data level Interoperability across multiple blockchains using emerging specifications combined with mature standards
  - Cross-blockchain interoperability by the use of blockchain links to point to specific data objects in specific blocks on specific blockchain networks
  - Standards based way for trade participants to register a product’s physical features along with information related to organizations licensed to manufacture and import a product such as limits on quantity or country of manufacture

CBP Adoption of S&T Funded & Championed Blockchain Interoperability 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 Brenda B Smith
Executive Assistant Commissioner
Office of Trade

Kathryn Kolbe K 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

2. Invest in business driven proof-of-concepts to identify scalable integration architectures and determine adoption Gain/Pain ratio

3. Motivate and shape innovative and potentially risky product development via the S&T Silicon Valley Innovation Program (SVIP) to meet mission challenges

What SVIP Does

We help develop and deliver technology that DHS needs while promoting economic development through startup/small-business growth

We enable the global innovation community to tackle the hardest problems faced by DHS's operational missions

CULTIVATE

Educate the innovation community on DHS's mission and challenges

INNOVATE

Leverage commercial investments & adapt to meet government needs

SVIP Application Process

TOPIC CALL

DHS operational agency describes need

APPLICATION

Startup submits 10 page application laying out how their commercial product can be adapted to meet DHS need

PITCH

Select startups invited to provide 15 minute virtual pitch; Courtesy decision provided within 48 hours

AWARD

Other Transaction Agreement (OTA) awarded on average within 45 days

How SVIP Funds

Up to $800K over 24 months

3-4 tranches of non-dilutive funding ❖Multitracking

Performance-based funding steps			
Phase 1	$50-200K	3-6 months	Technology adaptation to address DHS challenge
Phase 2	$50-200K	3-9 months	Full capability build out to demonstrate viability
Phase 3	$50-200K	3-9 months	Capability demonstrations & functional and red team testing
Phase 4	$50-200K	3-9 months	Operational test and evaluation in multiple user scenarios

Benefits to Our Portfolio Companies

Equity-Free

This is a performance-based award. Up to $800K available for every company.

Network

Instant access to DHS public private partnerships and the greater homeland security enterprise, a $544B marketplace.

Mentorship

Learn from the best. We have a deep bench of government and private sector partners who can offer guidance and introductions.

Market Validation

Find market fit through prototype testing and pilot opportunities.

Amplify Your Reach

Demo your product to government, industry and investors from across the world.

Follow-On Funding

Our alumni have received follow-on funding by venture capital investors.

Value Proposition to DHS

Rapid End User Evaluation

Evaluation in operational settings measured in months vs. years

Increased Access to Innovation

Lowered barrier of entry provides DHS access to innovative startups who don’t traditionally engage in Government work

Leveraging Private Investment

$19M+ in DHS awards (to date) leverages more than $500M in private investment

Quick Response to Needs

16 topic calls released addressing key needs including border security, cybersecurity, first responders and aviation security

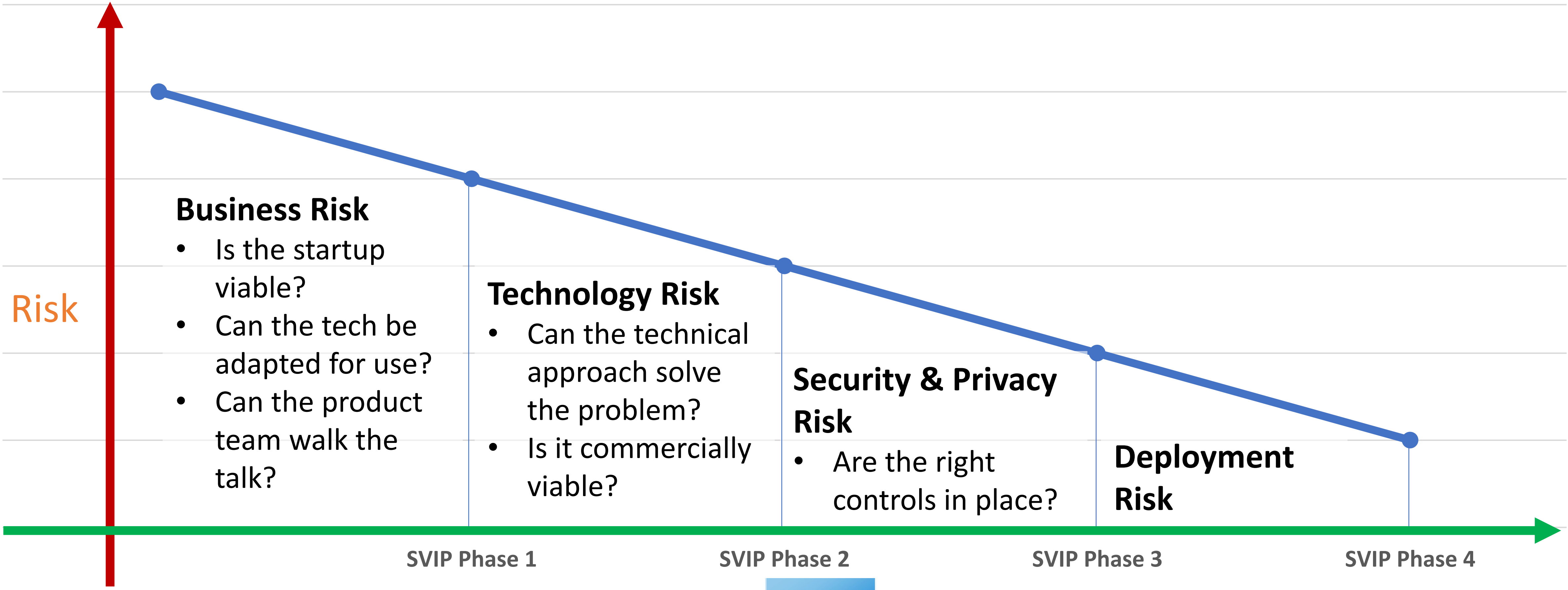
Increased Collaboration

Technology SMEs and Operational End Users work together at every stage

Minimize Financial Risk

Relatively small investments (max $200k / phase) and review gates after each phase ensure projects remain on track and continue to demonstrate mission value

SVIP Mitigates Operational Transition Risks



Business Risk

- Is the startup viable?
- Can the tech be adapted for use?
- Can the product team walk the talk?

Technology Risk

- Can the technical approach solve the problem?
- Is it commercially viable?

Security & Privacy Risk

- Are the right controls in place?

Deployment Risk

SVIP Provides a Pathway to Production Deployment

SVIP Phase 5

- Direct and sole source
- Production deployment to address additional use cases beyond those defined in Phases 1-4
- Requires the deployment to have a prototyping component

Production OT Acquisition

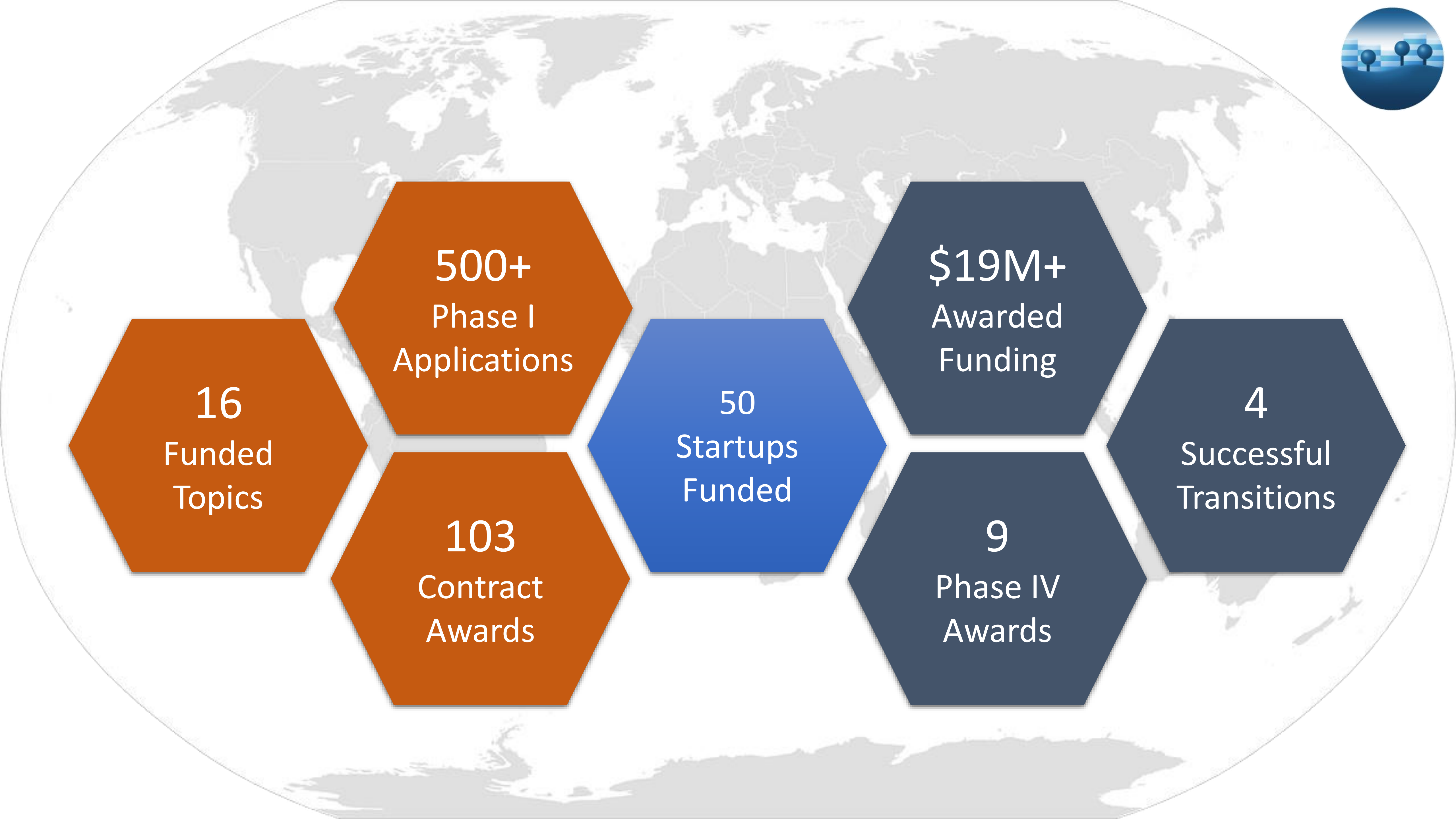
- Direct and sole source
- Production deployment
- DHS Component CO must have OT Warrant
- Requires the use of DHS Component acquisition dollars

Section 880 Acquisition

- Can be direct and sole source if structured appropriately
- DHS Component needs to have delegated 880 authority from DHS OCPO
- Can utilize DHS Component acquisition dollars

Current SVIP Portfolio

- Internet of Things Security
- Big Data
- Identity and Anti-Spoofing
- Fintech Cybersecurity
- Aviation Security
- Seamless Travel
- Drones/sUAS
- K9 Wearables
- First Responder Tech
- Blockchain



16
Funded
Topics

500+
Phase I
Applications

103
Contract
Awards

50
Startups
Funded

$19M+
Awarded
Funding

9
Phase IV
Awards

4
Successful
Transitions

SVIP Call for Solutions: Preventing Forgery & Counterfeiting of Certificate and Licenses

Preventing Forgery & Counterfeiting of Certificate and Licenses

U.S. Citizenship and Immigration Services

U.S. Customs and Border Protection

Transportation Security Administration

- DHS Operational Components (CBP, TSA, USCIS etc.) need to issue, validate and verify entitlements, attestations and certificates
  - Travel
  - Citizenship and Immigration Status
  - Employment Eligibility
  - Organizational Identity & Supply Chain Security
- DHS Operational Components are both Issuers of Credentials (USCIS) and Validators and Verifiers of Credentials (CBP, TSA)
- Current issuance processes are paper based, non-interoperable and susceptible to loss, destruction, forgery, and counterfeiting
- Seeking digital solutions for:
  - Issuance, Validation and Verification of Certificates, Licenses and Attestations
  - Storage and Management of Certificates, Licenses and Attestations
  - Consolidating Decentralized and Derived PIV Credentials

Citizenship, Immigration & Employment Authorization

U.S. Citizenship and Immigration Services

USCIS administers the nation’s lawful immigration system and is responsible for the issuance of documentary evidence of citizenship, immigration, and employment authorization. The application of technologies sought in this topic call could potentially enhance those capabilities by enabling digital representations of those documents that:

- Provide identity protections that allow for disclosure of information under the control of the owner of the credential
- Provide the ability to remotely mange the lifecycle of the credential (electronic document)
- Integrate with the current secure issuance processes

Identity Documents for Travel

Transportation Security Administration

TSA has a responsibility to confirm the identity of each passenger at the TSA security checkpoint and ensure that the identity presented on the digital document matches the identity associated on a confirmed travel reservation […] TSA is moving towards electronic authentication capabilities to strengthen this process in support of TSOs. The application of technologies sought in the topic call could potentially enhance the TSA capabilities to

- Prove the authenticity and provenance of identity documentation at speed
- Ensure that the digital document has counter-fraud protections
- Direct Passengers to certain screening lanes by applicable risk-based screening protocol (e.g., trusted traveler program participant, standard traveler, etc.)

Tribal Identity Documents for Travel

U.S. Citizenship and Immigration Services

Transportation Security Administration

Tribal jurisdictions within the United States have the authority to issue identity documents that TSA may accept for domestic air travel and USCIS may for other uses […] TSA and USCIS have an interest in how the technical implementation of a tribal identity document using the technologies sought in this call could meet the following technical criteria:

- The digital document has counter-fraud protections that are equivalent to the security protections required of physical documents.
- The digital document allows the reliant party to distinguish among tribal documents based on pre-determined criteria (e.g., Federal recognition of the tribe, issuance practices, etc.).
- The implementation has the ability to integrate with the current issuance and validation processes

Identity of Organizations & Organizational Delegates

U.S. Customs and Border Protection

CBP and other DHS Operational Components have various responsibilities regarding supply chain security and intellectual property rights enforcement. These needs require knowing the identity of organizations that are part of a supply chain and understanding who has been delegated to perform a particular function on behalf of an organization. The application of technologies sought in the topic call could potentially enhance the capabilities available to DHS to ensure the ability to:

- Validate the identity of an Organization
- Validate affiliation of a person to a legitimate Organization
- Ensure that the delegated entity is the actual Person performing the actions on behalf of the Organization

Cross-Border Oil Import Tracking

U.S. Customs and Border Protection

Crude oil and oil products crossing the US-Canadian border rely on estimation of pipeline flows for admission and charging of appropriate duties. The same pipeline may be used for different types of oil, with different duties. Additionally, oil imported to Canada may be comingled with Canadian oil for export. The current process for capturing this transaction flow is manual and complex. The application of technologies sought in the topic call could potentially enhance the CBP capabilities to accurate admit oil under USMCA and apply appropriate duties by:

- Accurately tracking the evidence of the flow of oil through pipeline and refinement between the US and Canada
- Attribute oil imports with the accurate composition and country of origin

Origin of Raw Material Imports

U.S. Customs and Border Protection

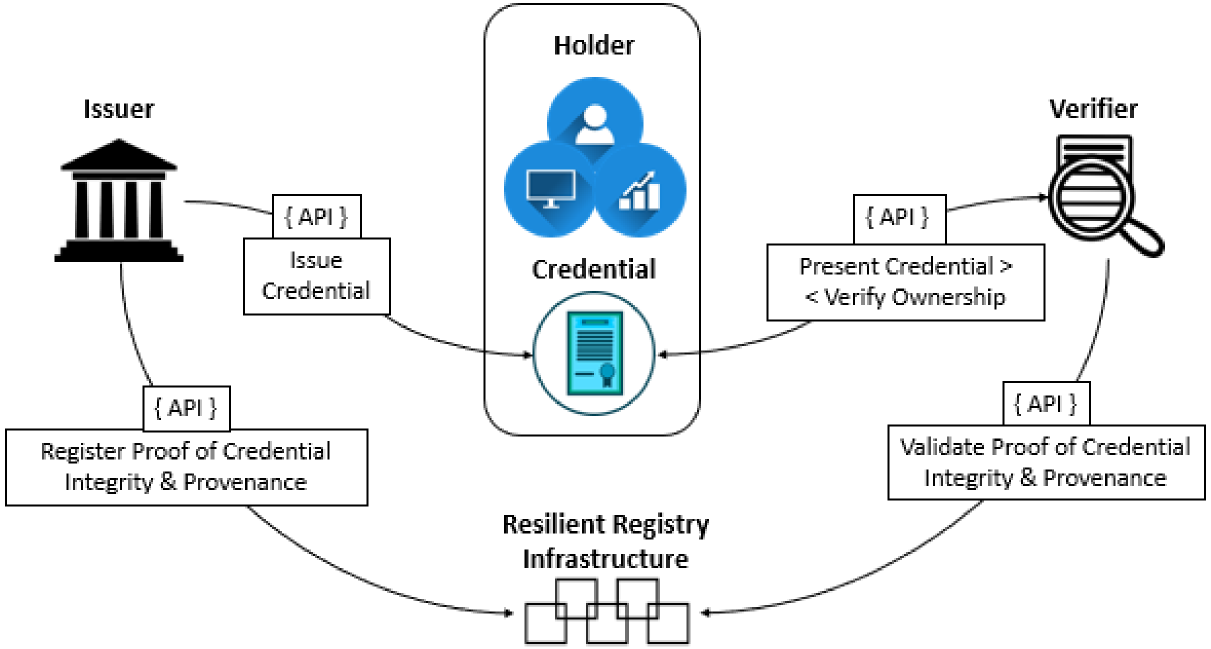
CBP relies on country of origin data from importer documentation. Validating the point of origin for raw materials (ex. timber, diamonds, and precious metals) by CBP requires costly inspection and cannot be implemented at scale. Transit through a nation with a preferential trade agreement could be used to confound the true country of origin, resulting in lost duty revenue and support of illicit activities. The application of technologies sought in the topic call could potentially enhance the CBP capabilities to:

- Track the documentary evidence of the flow of raw materials from the point of extraction
- Enable the application of appropriate duties
- Ensure goods imported to the United States do not come from force labor or fund criminal or terrorist organizations

Scope of Work

DHS is seeking technologies and solutions that address this need via one or more of the following Technical Topic Areas:

1. Issuance and Verification of Certificates, Licenses and Attestations
2. Storage and Management of Certificates, Licenses and Attestations


Holder
Issuer
Verifier
{ API }
Issue Credential
Credential
{ API }
Present Credential >
< Verify Ownership
{ API }
Register Proof of Credential Integrity & Provenance
{ API }
Validate Proof of Credential Integrity & Provenance
Resilient Registry Infrastructure

Interoperability Guidance to Applicants

… **this call will require any proposed solution to incorporate the lessons learned** from DHS investments in R&D, specifications/standards, and proof-of-concepts that has resulted in **our support for existing and emerging standards-based protocols, data exchange formats and security policy frameworks to ensure interoperable integration with enterprise systems.**

The International Organization for Standardization (ISO) uses specific verbal forms to convey clarity on what is a requirement and what is a recommendation or other type of statement.

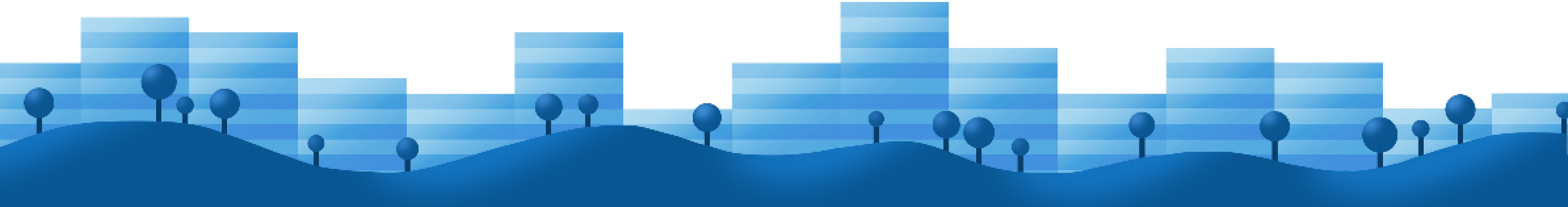
We are adopting and using the following ISO document conventions:

- Requirements - SHALL, SHALL NOT
- Recommendations - SHOULD, SHOULD NOT
- Permission - MAY, MAY NOT
- Possibility and Capability - CAN, CANNOT

Ensuring Interoperability and Open APIs

- 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.
- The solution SHALL incorporate, if appropriate to the particular use case, 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)*

AND MORE …



Objectives for SVIP Phase I

Minimum Viable Product that demonstrates proof-of-concept and supporting documentation inclusive of verifiable test evidence, technical drawings, software or other proof that the technical approach is sound.

Objectives of this phase are to:

- Validate the proposed architecture and design to incorporate interoperability specifications
- Validate digital security criteria equivalency to existing paper based security features.
- Evaluate the design of the APIs
- Articulate a go-to-market commercialization strategy

Homeland Security

DHS S&T Silicon Valley Innovation Program (SVIP)

Phase 1 Multi-Vendor Interoperability Plug Fest

6 -7 May, 2020

PREVENTING FORGERY & COUNTERFEITING OF CERTIFICATES AND LICENSES

Phase 1 Interoperability Plug Fest Test Plan
May 2020

DANUBE TECH GMBH

SICPA

Digital Bazaar

Mavennet

factom

SECURE KEY

Registry Infrastructure Under Test

- Factom
- Hyperledger Fabric
- Hyperledger Indy
- Neoflow
- Transmute for Trade
- Universal Issuer/Verifier
- Veres One

https://lists.w3.org/Archives/Public/public-credentials/2020Apr/0198.html

Why Interoperability in Asset Traceability?

Current State

- Origin documents of raw materials (i.e. Mill Test Reports, Crude Oil Assay, Lumber Export Authorization) are **paper-based**.
- **Proof of origin may be lost when there are multiple transfers/resales**, making it more difficult to validate good origination.
- Different supply chains are siloed, but global trade intersects at multiple points. Customs brokers and border control agencies have to gather data from different parties, **as the number of stakeholders and supply chains increase the problem with authentication intensifies**.

Target State

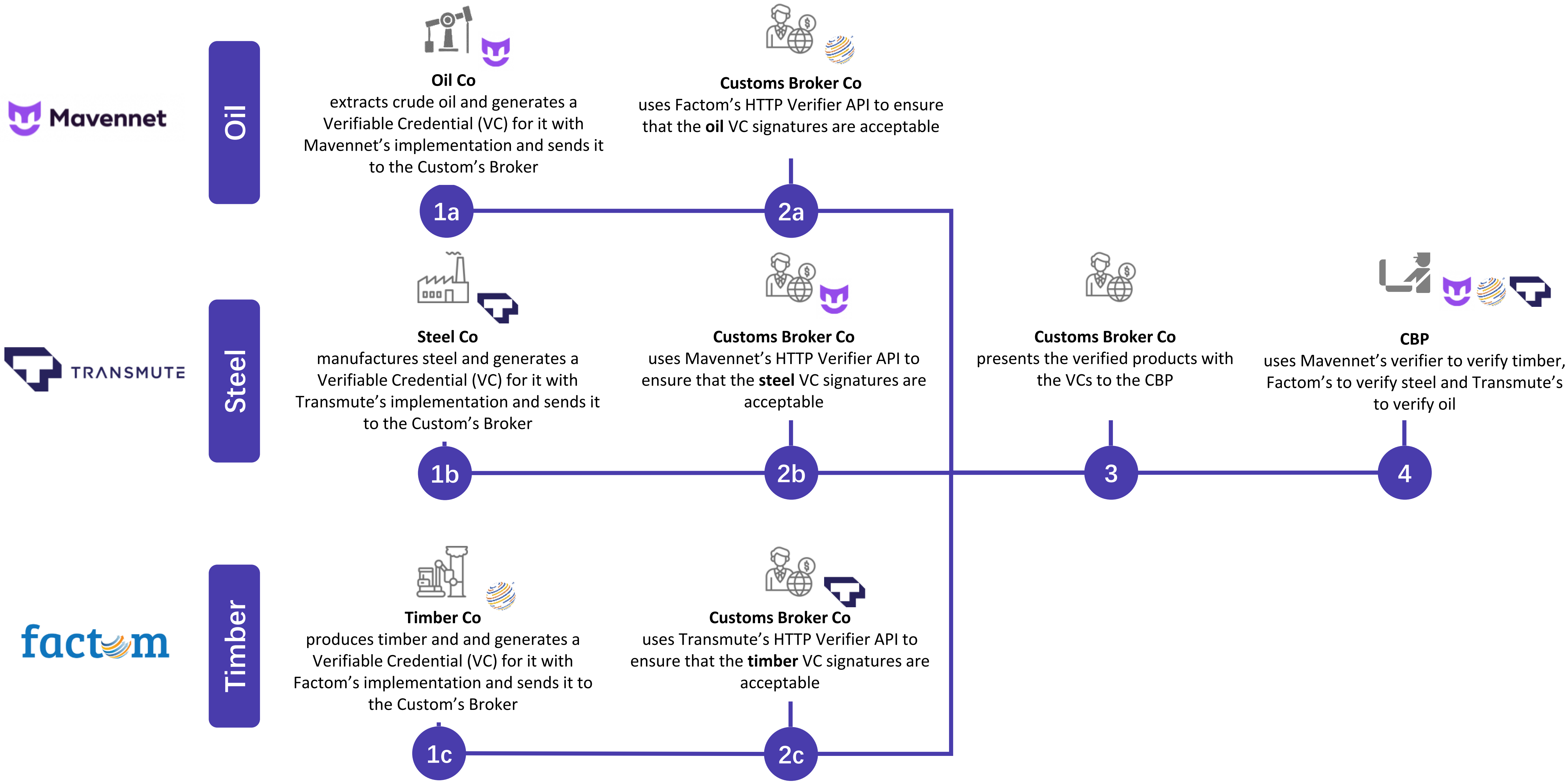
- **DIDs and VCs make origination easier to track and verify and harder to counterfeit.** Such system allows stakeholders on the same network to trust the origin of documents, track, trace and authenticate data end-to-end
- **It is however unrealistic to think all supply chains in the world use the same system or vendor.** At the same time, most supply chains are not linear, but rather a composition supply chains with different materials (e.g. automotive sector is composed of metals, plastic, textile, etc.)
- There is a need for all systems to interoperate in order to guarantee mainstream adoption. **Regulators and border control agencies can verify the origin of products in different systems (i.e. oil, steel, timber, etc.)**

Raw Material Imports Test Scenario

Raw material producers (oil, steel and timber) are using different vendors (Mavennet, Transmute, and Factom) to generate VCs specific to the materials they are producing, i.e. Crude Oil Assay, Mill Test Report, Lumber Export Authorization.

Custom Broker uses different vendors to verify VCs presented by each producer

CBP uses yet another vendor to validate the VCs presented by the Customs Broker



Oil Co extracts crude oil and generates a Verifiable Credential (VC) for it with Mavennet's implementation and sends it to the Custom's Broker

Customs Broker Co uses Factom's HTTP Verifier API to ensure that the **oil** VC signatures are acceptable

Steel Co manufactures steel and generates a Verifiable Credential (VC) for it with Transmute's implementation and sends it to the Custom's Broker

Customs Broker Co uses Mavennet's HTTP Verifier API to ensure that the **steel** VC signatures are acceptable

Customs Broker Co presents the verified products with the VCs to the CBP

CBP uses Mavennet's verifier to verify timber, Factom's to verify steel and Transmute's to verify oil

Timber Co produces timber and and generates a Verifiable Credential (VC) for it with Factom's implementation and sends it to the Custom's Broker

Customs Broker Co uses Transmute's HTTP Verifier API to ensure that the **timber** VC signatures are acceptable

Why Interoperability in Digital PRC Issuance?

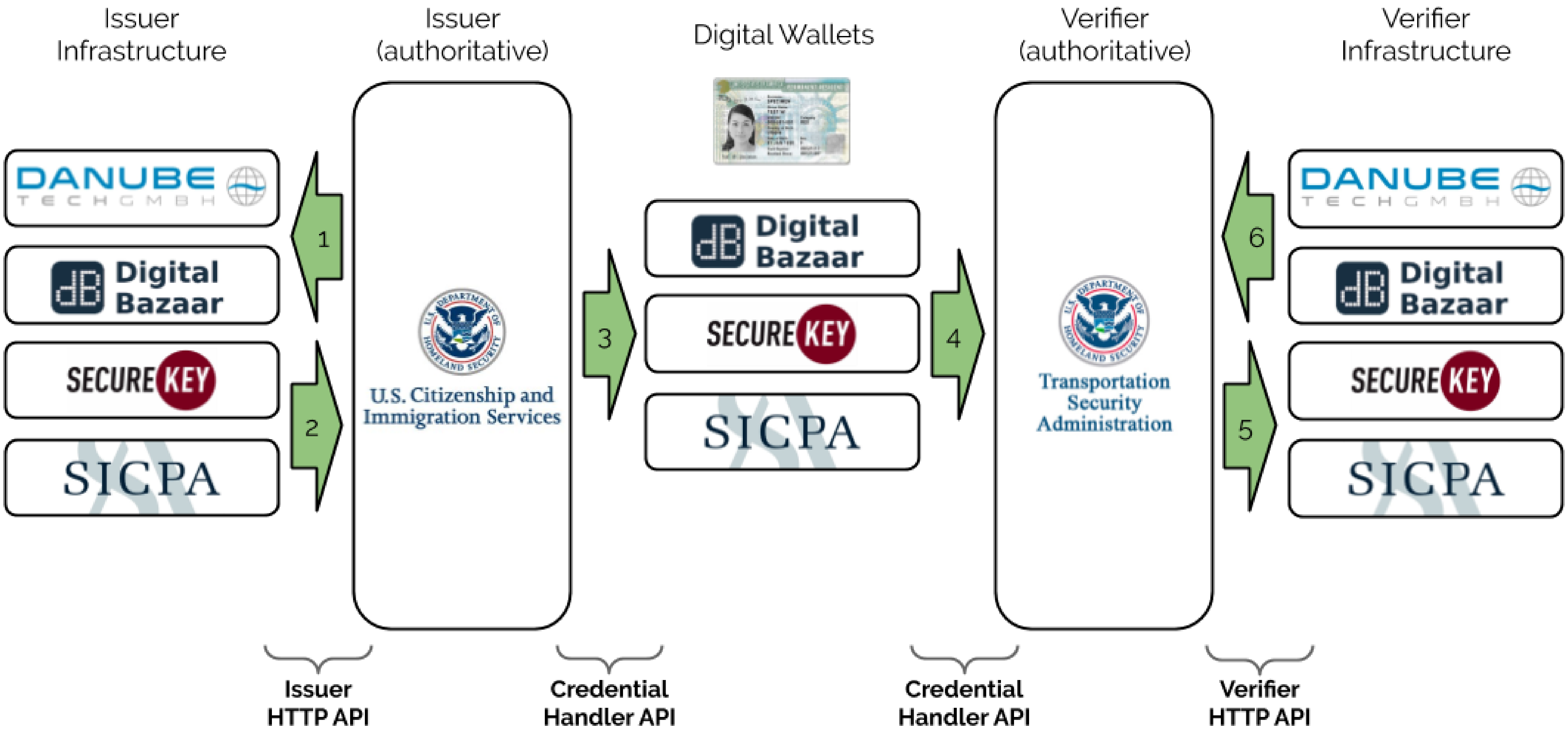
Current State

- USCIS administers the nation's lawful immigration system and is **responsible for the issuance of documentary evidence of citizenship, immigration, and employment authorization**.
- Current issuance processes are **paper based, non-interoperable and susceptible to loss, destruction, forgery, and counterfeiting**.
- Seeking **secure, privacy respecting and interoperable approaches to digital issuance of credentials we are authoritative for** e.g. US Permanent Resident Card, in addition to the currently paper based issuance process.

Target State

- Provide **identity protections that allow for disclosure of information under the control of the owner** of the credential that **meet or exceed current security standards** of paper-based credentials
- **Integrate with the current secure physical credential issuance processes** without any impact on USCIS backend systems
- Provide the ability to remotely manage the lifecycle of the credential as an electronic document
- Enable verification of the Permanent Resident Card (PRC) through verification API and web-based portal (for TSA and employers, respectively)

Digital PRC Test Scenario



Issuer Infrastructure

Issuer (authoritative)

Digital Wallets

Verifier (authoritative)

Verifier Infrastructure

DANUBE TECH GMBH

Digital Bazaar

SECURE KEY

SICPA

1

2

U.S. Citizenship and Immigration Services

3

4

Transportation Security Administration

5

6

Issuer HTTP API

Credential Handler API

Credential Handler API

Verifier HTTP API

Objectives for SVIP Phase II - IV

Phase II

- A working prototype with clearly documented APIs, integrated with a multi-factor authentication mechanism.
- End to end application ready for review and evaluation.

Phase III

- Production ready prototype able to demonstrate all features and functions of the technology.
- Ready for red team testing in a realistic deployment environment with an existing issuer and validator infrastructure.

Phase IV

- Red team feedback incorporated into the technology solution and all development is complete.
- Ready for operational deployment.

Conclusions and Considerations

- 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 Blockchain and DLT eco-system by:
  - Conducting R&D to understand the promise, perils, and the gain-to-pain ratio of technology adoption
  - Conducting realistic POCs, Pilots and Implementations that encourage and demonstrate multi-party interoperability and solution diversity
  - Supporting innovative companies building and using emerging interoperability specifications and mature standards to enable a competitive, diverse marketplace of potential solutions

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

Blockchain/DLT Portfolio Companies

DANUBE TECH GMBH

Universal Issuer and Verifier

“… will integrate interoperability support for multiple credential data formats, blockchains and standardized and open application programming interfaces into their existing decentralized identifier (DID) registrar and DID resolver products for credential issuance and identity verification.“

Digital Bazaar

Interoperable Enterprise Identity and Credential Life-cycle Management

“…will enhance their existing product offering that supports emerging global World Wide Web Consortium (W3C) security, privacy and interoperability standards such as Decentralized Identifiers and Verifiable Credentials with enterprise workforce and credential lifecycle management features.”

factom

Applying Cross-Blockchain Technology to Help Prevent Forgeries or Counterfeiting of Certificates and Licenses

“… a system that provides a way for organizations to manage certificates and licenses associated with tracking raw material imports via an open system that ensures the provenance of issued credentials.”

Mavennet

Blockchain-as-a-Service for Cross-Border Oil Exchange

“… will apply the company’s expertise, gleaned from building a platform enabling real-time auditability of the natural gas trading markets in Canada, to address CBP needs for cross-border oil import tracking. Mavennet’s solution will build a generic end-to-end platform that can be used for any type of commodity that includes automation and integrating application program interface, physical measurement and legacy system capabilities.“

SECURE KEY

Identity Documents Proofing, Presentation and Exchange system

“… will adapt the concepts and code associated with its Verified.Me commercial strength identity network solution that offer availability, disaster recovery, fraud prevention, monitoring and other essential operational controls to support TSA and USCIS needs around the issuance and validation of identity documents for travel and employment authorization.”

Verifiable Provenance, Traceability, and Regulatory Compliance for Raw Material Imports

“… will adapt Transmute ID, its core technology product that leverages centralized and decentralized identity infrastructures to secure individual agency identities and verifiable credentials to ensure that CBP has visibility into the provenance, traceability and regulatory compliance of raw material imports.”

STRANGER LABS

Untangling the New Web of Trust : Digital Credentials Offline

“… enable issuance, exchange and verification of digital credentials in an isolated environment — directly between devices, with no internet, LAN, or cellular connectivity — without sacrificing integrity guarantees or the ability to establish credentials' provenance while simultaneously enabling control of credentials from multiple devices.”

SICPA

Decentralized Digital Identity for Online and Offline Verification

“… will build a flexible, credential-based identity solution that includes the enrollment, creation, issuance and management of secure digital credentials through interoperable, open standards, which will seamlessly coexist with current processes and systems while enabling offline credentials validation.