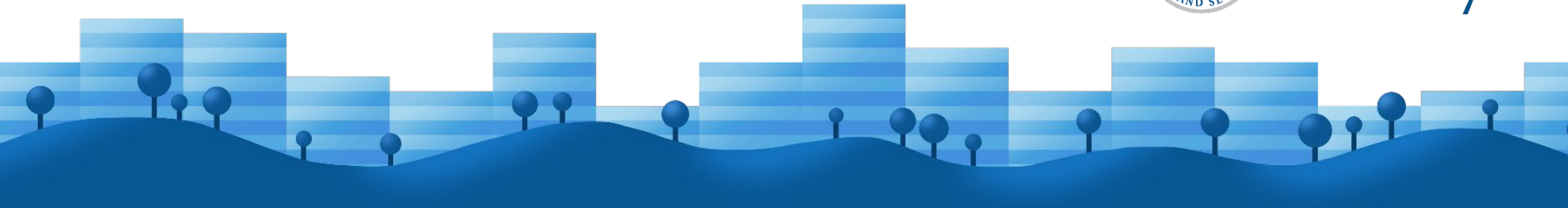
Homeland Security



DHS S&T Silicon Valley Innovation Program (SVIP)

PREVENTING FORGERY & COUNTERFEITING OF CERTIFICATES AND LICENSES

Phase 1 Interoperability Plug Fest Test Plan

May 2020

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

1. Introduction

The U.S. Department of Homeland Security (DHS) is committed to using cutting-edge technologies and scientific talent in its quest to make America safer. The DHS Science and Technology Directorate (S&T) Silicon Valley Innovation Program (SVIP), on behalf of DHS Operational Components, invests in startup companies with viable technologies suitable for rapid prototyping projects from across the nation and around the world to adapt, develop and harness cutting-edge capabilities that are commercially sustainable while simultaneously meeting the needs of DHS Operational Components and Programs.

1.1. DHS Operational Need

Decentralized and Distributed registry and time-stamping implementations such as Blockchain and Distributed Ledger Technology (DLT), from a government perspective, holds the potential for enhanced transparency and auditing of public service operations, greater visibility into multi-party business operations, and automation of paper-based processes to improve delivery of services to organizations and citizens.

DHS Operational Components such as CBP, TSA and USCIS have common needs across their mission sets for potential use of interoperable implementations of these technologies that also support the growth and availability of a competitive marketplace of diverse technology implementations for government and industry to draw upon to deliver cost effective and innovative solutions.

1.2. SVIP Awarded Startups and their Product Delivery Focus

Permanent Resident Card Issuance and Verification (USCIS & TSA Use Cases)

- Danube Tech
- Digital Bazaar
- Securekey Technologies
- SICPA Product Security

Raw Material Import Credentials (CBP Office of Trade Use Cases)

- Factom
- Mavennet Systems
- Transmute Industries

1.3. Interoperability Expectations

Per the DHS SVP Other Transaction Solicitation (OTS) Call 70RSAT19R00000002:

> Interoperability of technology solutions at global scale typically requires a solution provider to address and make specific choices regarding the protocols, payloads and policies supported by their implementations. While novel and innovative solutions are being sought as part of this topic call, DHS S&T and its mission partners have over the last 3+ years conducted extensive R&D, proof of concepts and community engagement to understand, demonstrate and champion a path that accelerates the development and usage of specifications and standards to foster a baseline of interoperability, security and privacy.

> As such, 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.

Selected requirements from the OTS:

- 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)

1.4. Demonstrating Interoperability

All awarded startups, by the end of their Phase 1, need to demonstrate to the Government a Minimum Viable Product that shows the adaptation of their Product to support, among other things and most critically, an interoperable implementation of DIDs/VCs.

How that is demonstrated to the Government is flexible, so what SVIP is resurrecting is the grand tradition (from WAAY back in the SAML and WS-* days) of the Interoperability Plug-Fest.

> *"Interoperability Plug-fests are a safe environment to test your code's degree of conformance with a respective standard, and how well it interoperates with other implementations of the same standard. Ideally, standards would be interpreted identically by all implementers, and hence all implementations would interoperate, but often enough that is utopia (though standards authors work very hard to minimize this). Such situations, where tests fail, the analysis of the failures can discover shortcomings in the standard document itself, illustrate discrepancies in interpretation, or in formal testing settings, errors in the test suite used."*

2. Unified Interoperability Test Plan

This plan outlines the high-level goals for interoperability for companies involved in the 2020 SVIP Blockchain Call cohort. At a minimum, the goals for interoperability are to demonstrate the interoperability at the Wallet, Issuer and Verifier implementations.

2.1. Wallets

- Support for the Verifiable Credentials data model.
  - Why: Supporting the Verifiable Credentials data model enables data portability across Issuers, Wallets, and Verifiers.
- Support create and read operations for at least two different DID methods.

  - Why: Supporting multiple DID methods demonstrates that the product architecture is capable of supporting other DID methods in the future.
- Support CHAPI or DIDComm for DIDAuth with an Issuer front-end website.
  - Why: Supporting DIDAuth demonstrates that the product is capable of a) establishing cryptographic control over a DID - leading to a stronger authentication posture, and b) asserting that the subject of a credential is the same as the entity presenting the credential.
- Support CHAPI or DIDComm for obtaining and storage of Verifiable Credentials.
  - Why: Supporting storage of Verifiable Credentials using a common protocol enables interoperability between Issuers and Wallets.
- Support CHAPI or DIDComm for presentation of Verifiable Credentials.
  - Why: Supporting presentation of Verifiable Credentials using a common protocol enables interoperability between Wallets and Verifiers.
- Support the Ed25519 Cryptographic Suite.
  - Why: Supporting a digital signature cryptographic suite enables interoperability between Issuers, Wallets, and Verifiers.
  - This Suite is widely used in the current Community and offers the best alignment for interoperability across products.
- Support the interaction with multiple Issuer demo sites and multiple Verifier demo sites through CHAPI and/or DIDComm.
  - Why: Specification compliance does not always lead to end-to-end interoperability in the real world due to subtleties in implementations.

2.2. Issuers

- Support for the Verifiable Credentials data model.
  - Why: Supporting the Verifiable Credentials data model enables data portability across Issuers, Wallets, and Verifiers.
- Support the Permanent Resident Card or Raw Materials Credential (data model).
  - Why: This data model was reviewed and approved by DHS/USCIS and represents a real credential in use today.
- Issue a Verifiable Credential to a subject, supporting at least two different DID methods for the issuer DID.
  - Why: Supporting multiple DID methods highlights broader support for the ecosystem than supporting a single DID Method.
- Support the Ed25519 Cryptographic Suite
  - Why: Supporting a digital signature cryptographic suite enables interoperability between Issuers, Wallets, and Verifiers.
  - This Suite is widely used in the current Community and offers the best alignment for interoperability across products.
- Support the Verifiable Credential Issuer HTTP API
  - Why: Issuer demo sites integrating to different implementations of the Verifiable Credential Issuer HTTP API demonstrate the desired functional separation between functional logic and business logic.

2.3. Verifiers

- Support for the Verifiable Credentials data model.
  - Why: Supporting the Verifiable Credentials data model enables data portability

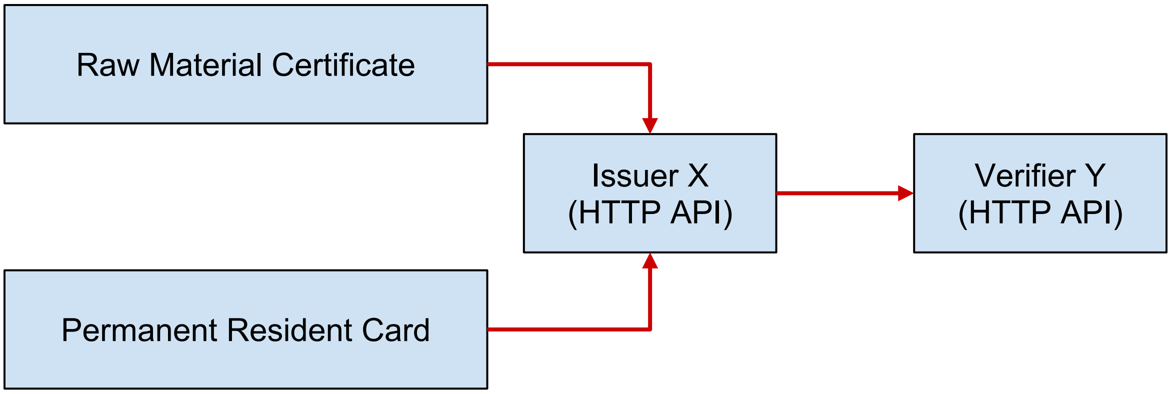
across Issuers, Wallets, and Verifiers.

- Verify a Verifiable Credential, supporting at least two different DID methods for the subject DID.
    - Why: Supporting credential assignment to multiple DID methods ensures portability of Verifiable Credentials between Issuers, Wallets, and Verifiers.
- Verify a Verifiable Presentation, supporting at least two different DID methods for the subject DID.
    - Why: Supporting presentation across multiple DID methods ensures portability of Verifiable Credentials between Issuers, Wallets, and Verifiers.
- Support the Ed25519 Cryptographic Suite.
    - Why: Supporting a digital signature cryptographic suite enables interoperability between Issuers, Wallets, and Verifiers.
    - This Suite is widely used in the current Community and offers the best alignment for interoperability across products.
- Support the Permanent Resident Card or Raw Materials Credential (data model).
    - Why: This data model was reviewed and approved by DHS/USCIS and represents a real credential in use today.
- Support the Verifiable Credential Verifier HTTP API
    - Why: Verifier demo sites integrating to different implementations of the Verifiable Credential Verifier HTTP API demonstrate the desired functional separation between functional logic and business logic.

3. Verifiable Credential HTTP API Test Plan

Test Suite – https://github.com/w3c-ccg/vc-examples/tree/master/test-suite

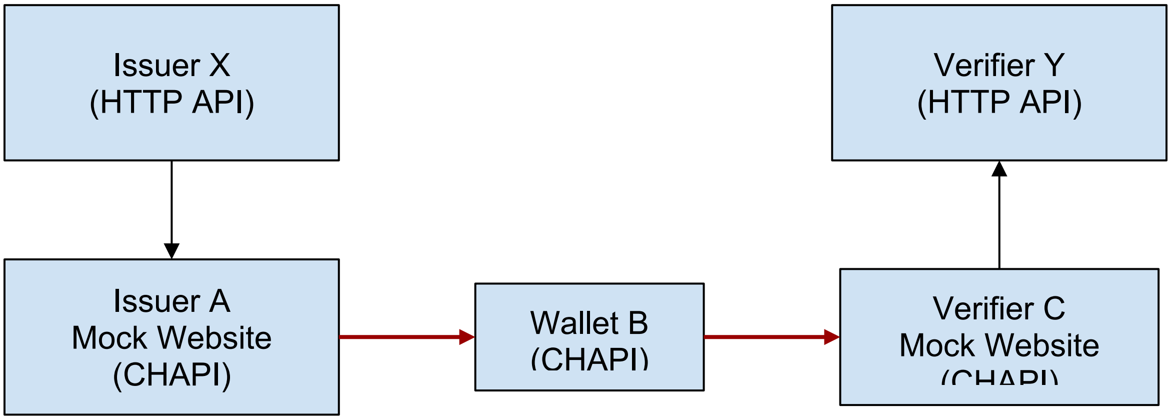
The Verifiable Credential HTTP API Test Suite is designed to test end-to-end conformance to the Verifiable Credential data model standard and the HTTP API pre-standards between Issuer and Verifier products. The general flow of data is shown below:



To establish whether or not Issuer X can interoperate with Verifier Y in the diagram above, an automated test suite is utilized. Red arrows above indicate the flow of data that is tested by the HTTP API Test Suite. The resulting test-report.html is available to determine which products are interoperable with each other. The test suite establishes the basic technical level of interoperability between the use case Verifiable Credentials and the product Verifiable Credential HTTP APIs.

4. Credential Handler API (CHAPI) Test Plan

The CHAPI Test Plan is designed to test end-to-end conformance to the Credential Handler API pre-standard between the Issuer, Wallet, and Verifier products. The general flow of data is shown below:



To establish whether or not Issuer A can interoperate with Wallet B can interoperate with Verifier C in the diagram above, a manual test plan is utilized. Red arrows above indicate the flow of data that is tested by the manual test plan. The black arrows are tested via the automated HTTP API Test Suite mentioned in the previous section. The manual test plan establishes the basic technical interoperability between Issuers, Wallets, and Verifiers utilizing CHAPI or DIDComm to move Verifiable Credentials around the ecosystem.

4.1. CHAPI Flow (Raw Material Credential)

A, B, C = [Transmute, Factom, Mavenet)

1. Company A provides a Wallet to User.
2. User visits Company B, which provides an Issuer, which can provide a Raw Material Credential to the Wallet.
3. User visits Company C and presents Raw Material Credential to a Verifier, where Company C acts as Raw Material Credential Verifier.

4.2. CHAPI Flow (Permanent Resident Card)

Issuers & Verifiers:

- Danube Tech
- Digital Bazaar
- SecureKey
- SICPA

Wallets:

- Transmute
- Veres
- SecureKey

Mock Websites:

- USCIS-db

- USCIS-dt
- Jobs-db
- ERP-mn
- USCIS-sk
- TSA-sk
- TSA-dt

1. Go to Wallet (multiple wallet options), create profile (multiple DID options).
2. Go to mock USCIS site and pick up Permanent Resident Card (multiple backend issuers), store in Wallet.
3. Go to mock jobs site and present Permanent Resident Card (multiple backend verifiers).

Permanent Resident Card and Raw Materials cohorts will specify all CHAPI queries and responses for use in the interoperability plugfest.

5. Off-Line Use Case (Art of the Possible)

Given the virtual nature of the Interop plug-fest in the era of COVID-19, off-line use case interop is not part of this test plan. However, some of the portfolio companies will be demonstrating the ‘art of the possible’ using a combination of video & narration followed by a Q&A.

Digital Bazaar

- QR Code is provided while the Permanent Resident Card (PRC) holder has network connectivity (pre-registration) and then displayed and verified in an offline scenario. There are many variations of what data could be placed into the QR Code. Our focus will be on the prevention of replayability and pulling data from the system of record (or a cache of the system of record).
  - Offline w/ PRC data cache - digitally signed QR Code that provides a look up token to scanning system, which then pulls all necessary information from pre-cached data.
  - Offline w/ no cache - digitally signed QR code asserting PRC number that can be counter-signed by bearer, no image data.

SICPA Product Security

- Demonstration of the ability for a verifier to link a credential to the picture of the holder (captured on moment of enrolment) that is shared out of band (optically), by adding a visual hash of the picture in the credential upon issuance.
- In addition, we plan on demonstrating offline verification of a presentation of the PRC, with relevant information being cached on the verification side in order to do verification through a mobile application. Focus will be on replay attack prevention and graceful degradation in case of low-tech presentation.

6. Appendix

- Interop Test Suite – https://github.com/w3c-ccg/vc-examples/tree/master/test-suite
- Interop Test Report - https://w3c-ccg.github.io/vc-examples/test-report.html
- Verifiable Credentials Data Model - https://www.w3.org/TR/vc-data-model/
- Decentralized Identifiers - https://w3c.github.io/did-core/
- JavaScript Object Notation for Linked Data - https://www.w3.org/TR/2014/REC-json-ld-20140116/

7. References

- SVIP Solicitation - https://beta.sam.gov/opp/bfd1662d1ad9c317e4afae6544abff3a/view?keywords=70RSAT19R00000002&sort=-relevance&index=&is_active=true&page=1

- Awarded Performers participating in the Interop Plugfest
  - Danube Tech https://www.dhs.gov/science-and-technology/news/2019/09/26/news-release-dhs-st-awards-143k-blockchain-interoperability
  - Digital Bazaar https://www.dhs.gov/science-and-technology/news/2019/11/14/news-release-dhs-awards-199k-blockchain-tech
  - Factom https://www.dhs.gov/science-and-technology/news/2019/11/18/news-release-dhs-awards-197k-tracking-raw-material-imports
  - Mavennet https://www.dhs.gov/science-and-technology/news/2019/11/06/news-release-dhs-awards-182k-cross-border-oil-import-tracking
  - SecureKey Technologies https://www.dhs.gov/science-and-technology/news/2019/11/18/news-release-dhs-awards-200k
  - SICPA Product Security https://www.dhs.gov/science-and-technology/news/2019/11/14/news-release-dhs-awards-181k-verify-digital-credentials
  - Transmute Industries https://www.dhs.gov/science-and-technology/news/2019/11/08/news-release-dhs-awards-198k-raw-material-import-tracking