Technical Implementation Requirements for Decentralized Identity

Version 1.0
March 18, 2024

Meeting DHS Operational Needs

1. Counter Terrorism and Prevent Threats
2. Secure and Manage Our Borders
3. Administer the Nation's Immigration System
4. Secure Cyberspace and Critical Infrastructure
5. Build a Resilient Nation and Respond to Incidents
6. Combat Crimes of Exploitation and Protect Victims

U.S. Citizenship and Immigration Services

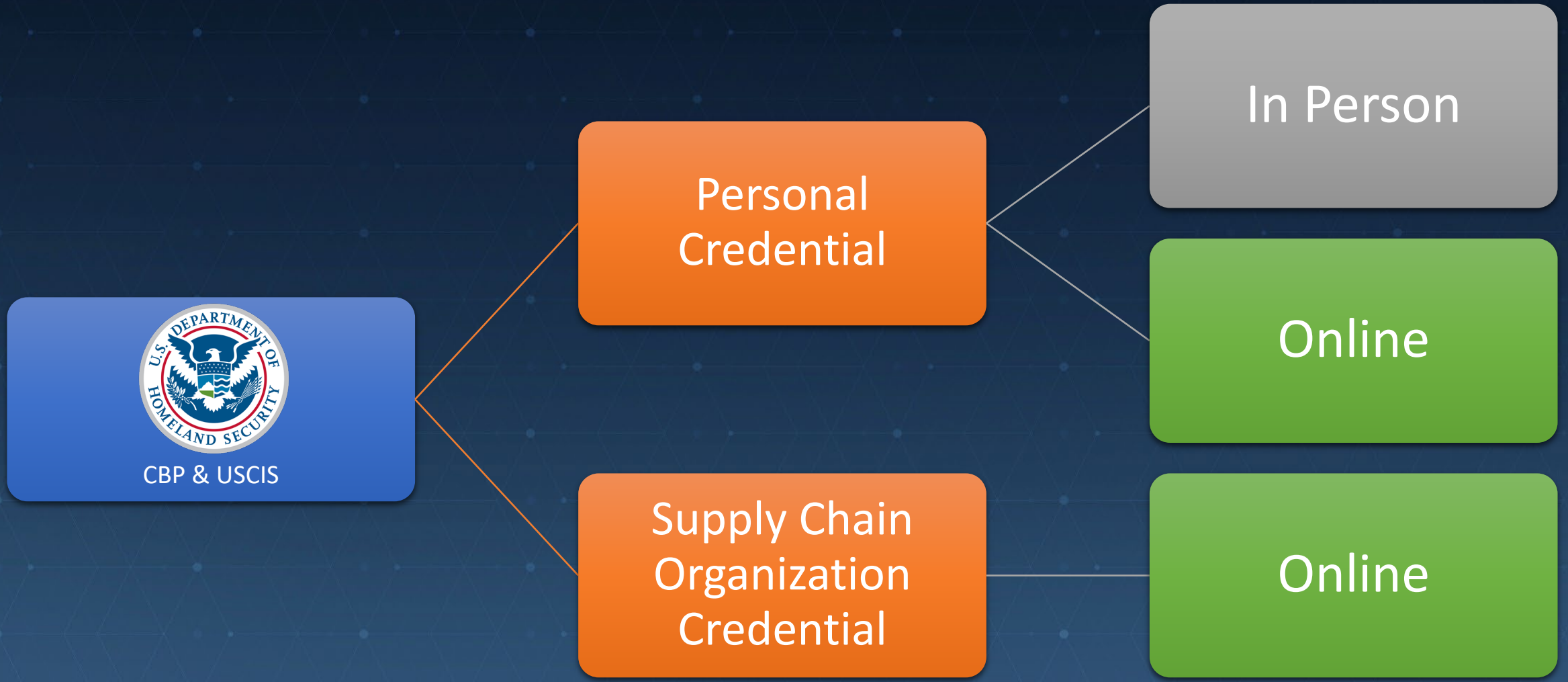
U.S. Customs and Border Protection

Privacy Office

"An implementation should be conservative in its sending behavior, and liberal in its receiving behavior”

~ Postel's Law
a.k.a. Robustness Principle

& not | |


CBP & USCIS
Personal Credential
Supply Chain Organization Credential
In Person
Online
Online

Personal Credential Implementation Principles

- Digital is not a requirement; it is **a choice!**
- **Eliminate "phone home"** architecture/technology/implementations
- **Eliminate "back-channel" interactions** between verifiers of the credential and the issuer, which are not visible to the credential holder
- **Support non-trackable selective disclosure** of information under holder control
- Encourage and support a plurality of **independent, interoperable, standards-based implementations**

Personal Credential Use (In Person)

Read-to-Verify

- **Inclusive**, global usage without the need for a mobile device
- DHS has no awareness of credential usage by a Customer **(No-Phone-Home)**

Scan-to-Verify

- **Inclusive**, global usage without the need for a mobile device
- DHS has no awareness of credential usage by a Customer **(No-Phone-Home)**
- Local Digital Verification of Physical Card Data

Tap-to-Verify

- **Inclusive**, global usage without the need for a mobile device
- DHS has no awareness of credential usage by a Customer **(No-Phone-Home)**
- Streamlined Local Digital Verification of Physical Card Data

In-Person Credential Use: Scan-to-Verify

Digital Signature Payload (Only the data on the card; not the photo)

QR Code on the physical card contains the issuer identifier and digital signature

- **Data attributes already present on the physical card are digitally signed and encoded in CBOR format**
- **Decentralized Identifier (DID) is used to resolve and retrieve the DHS/USCIS public key, which can be used to verify the digital signature**

--------- 2D Barcode Payload ---------

```
IAUSA0000007010SRC0000000701<<
2001012M1105108BRA<<<<<<<<<<<5
SPECIMEN<<TEST<VOID<<<<<<<<<<<
```

+

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

- **Inclusive, global usage without the need for a mobile device**
- **DHS continues to have no awareness of credential usage by a Customer**
- Enhanced content integrity & origin authenticity features on the physical card
- Support for occasionally connected Verifiers – DHS/USCIS public keys can be resolved, downloaded and cached on the verifying device, using the resolver functionality that is part of the W3C Decentralized Identifiers (DID) standard to allow local verification to occur without network connectivity

[W3C-DID]
[CITIZENSHIP-VOCAB]

Distribution and Retrieval of DHS Public Key

I want the public key(s) that belongs to **did:web:www.uscis.gov:green-card**

Let me find the "DID Document" that is associated with did:web:www.uscis.gov:green-card

Let me return the "DID Document" that contains the public key(s) located at **https://www.uscis.gov/.well-known/did.json**

Verifier

Metadata Resolver

Issuer

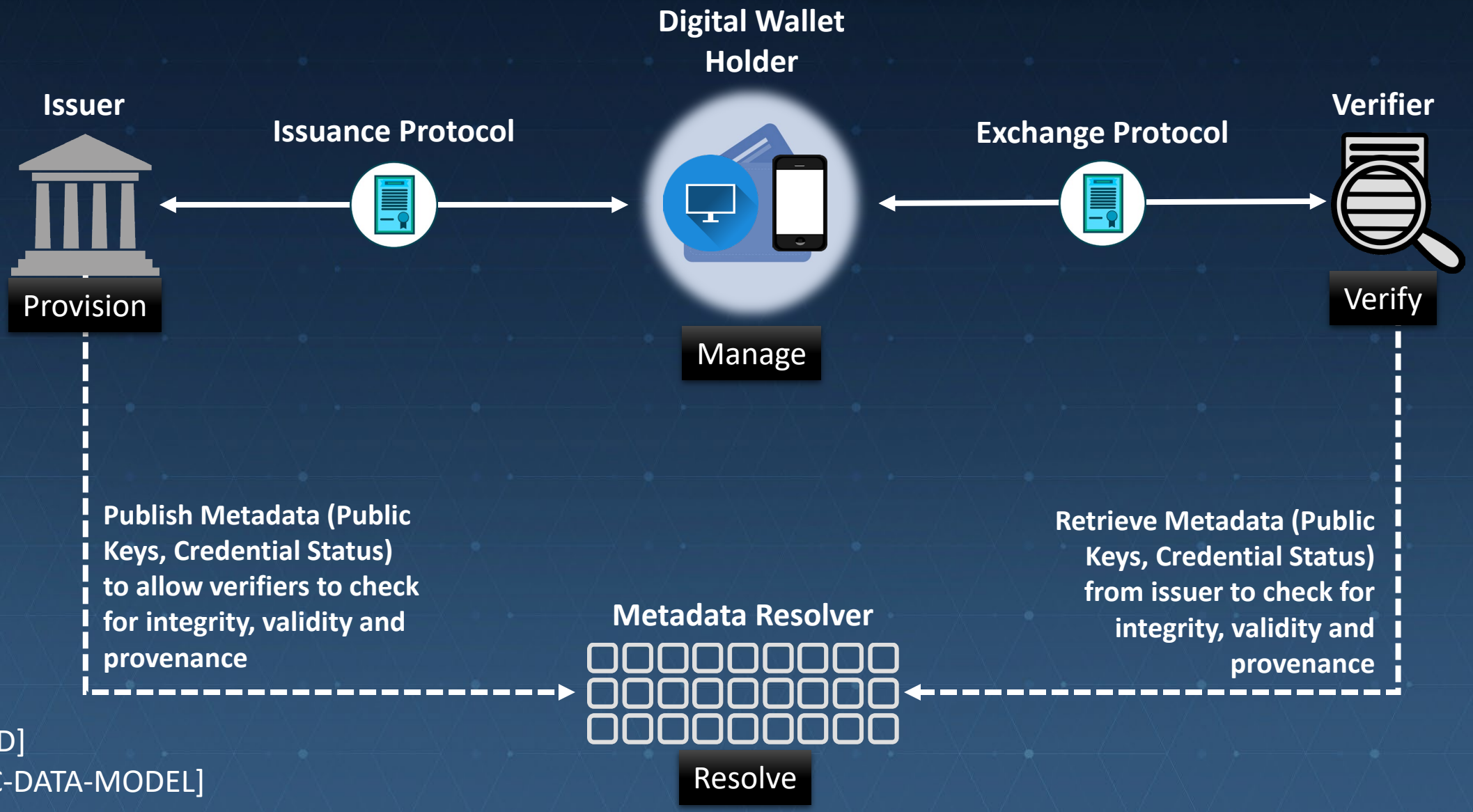
Input >> A unique decentralized identifier (DID) of the Issuer (USCIS) e.g., did:web:www.uscis.gov:green-card
The identifier of the public key used to verify USCIS digital signature from the credential e.g., did:web:www.uscis.gov:green-card#public-key-1

Output >> The location of a metadata file (DID Document) that is owned/managed by the Issuer that contains its public key(s)

Mechanism for publishing public keys which removes the need for a centralized data repository for the distribution and management of public keys

[W3C-DID]

Personal Credential Use (Online)
W3C VCDM & W3C DID Standards



[W3C-DID]
[W3C-VC-DATA-MODEL]

Technical Implementation Requirements

- Conventions Used
- DHS Personal Credential Issuer
  - Accessibility & Openness
  - Platform & Software Security
  - Credential Formats & Digital Signatures
  - Metadata & Vocabulary
  - .gov Binding
  - Issuance Protocol
- DHS Personal Credential Verifier
  - Accessibility & Openness
  - Platform & Software Security
  - Credential Formats & Digital Signatures
  - Metadata & Vocabulary
  - .gov Binding
  - Exchange Protocol
- DHS Personal Credential Holder (Digital Wallet)
  - Accessibility & Openness
  - Platform & Software Security
  - Credential Formats & Digital Signatures
  - Issuance Protocol
  - Exchange Protocol
- Normative References

Conventions Used

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.

The requirements on the following pages adopt and use the following ISO document conventions:

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

DHS Personal Credential Issuer Accessibility & Openness

- SHALL NOT implement capabilities that enable tracking of Holder credential use
- SHALL implement the relevant portions of the W3C Web Content Accessibility Guidelines [W3C-WCAG] to ensure compliance with the Section 508 of the U.S. Rehabilitation Act
  - SHOULD implement the U.S. Web Design System (https://designsystem.digital.gov/)
- SHALL prioritize the implementation of data formats and associated security and privacy mechanisms, inclusive of public facing APIs, that utilize globally available standards and specifications that are openly developed, royalty free and freely available to implement
- SHALL enable the Holder to choose a digital wallet
- SHALL implement support for Holder applications (digital wallets) that use web platform technologies
- SHALL implement support for Holder applications (digital wallets) that use native platform technologies

DHS Personal Credential Issuer Platform & Software Security

- SHALL utilize cryptographic modules validated by the joint U.S. & Canada Cryptographic Module Validation Program [CMVP]
- SHALL utilize [FIPS-140] compliant cryptographic key storage mechanisms
  - MAY utilize an operating system capability
  - MAY utilize an external device capability
  - MAY utilize a remote backend capability
- SHALL provide a Software Bill of Materials (SBOM) containing the details and supply chain relationships of various components used in building the Issuer software
  - SHALL contain the minimum elements for a SBOM as defined in the joint report by the Department of Commerce and the National Telecommunications and Information Administration
    - https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom

DHS Personal Credential Issuer Credential Formats & Digital Signatures

- SHALL implement the [W3C-VC-DATA-MODEL] using the JSON-LD Compacted Document Form
- SHALL implement the embedded proof mechanism defined in [W3C-VC-DATA-INTEGRITY]
- SHALL implement selective disclosure capabilities using [W3C-VC-DATA-INTEGRITY] proof sets to support multiple proofs in a single document
  - SHALL implement a proof that is U.S. Federal Information Processing Standards (FIPS) compliant e.g., ECDSA Cryptosuites
  - SHALL implement a proof based on non-correlatable signatures e.g., BBS Cryptosuites
  - MAY implement additional proofs e.g., PQC
- SHALL implement [W3C-DID]

DHS Personal Credential Issuer Metadata & Vocabulary

- SHALL implement [W3C-BITSTRING-STATUS-LIST] for credential status checks inclusive of revocation checks
- SHALL implement [W3C-DID]
  - SHALL implement the did:web method as the Issuer (Organizational) Identifier
  - SHALL utilize the DID Document as the authoritative metadata distribution mechanism
  - SHALL implement direct DID resolution
  - SHALL implement support for external DID/Metadata resolvers
  - SHALL digitally sign the DID Document with a U.S. Federal Information Processing Standards (FIPS) compliant [W3C-VC-DATA-INTEGRITY] proof to enable integrity and provenance verification
- SHALL implement [CITIZENSHIP-VOCAB]

DHS Personal Credential Issuer .gov Binding - TBD

- .gov is the top-level domain for governments in the U.S., including federal, state, local, tribal, and territorial
- Only verified U.S. Government organizations can register and operate a .gov domain; registration is free to verified USG organizations
  - https://get.gov/domains/eligibility/
- An entity can gain high assurance that a credential is issued or is being verified by a specific USG organization by digitally verifying a cryptographic link between the USG organization's did:web identifier and its .gov domain
- We are currently evaluating various options that utilize existing technologies and standards to demonstrate this linkage without requiring changes to certificate authority governance, browser technology and trust store governance processes

DHS Personal Credential Issuer Issuance Protocol - TBD

- DHS hopes to support multiple issuance protocols
- Issuance protocol SHALL:
  - support required credential format & digital signature mechanisms
  - support required metadata and vocabulary distribution and verification mechanisms
  - enable the Holder to choose a digital wallet
  - disregard (via implementation profiles) external dependencies that are duplicative or not utilized by the DHS Issuer
- Following many-to-many, multi-vendor interoperability testing, DHS will update the requirements for issuance protocols
- Options under consideration include:
  - W3C CCG VC-API
  - W3C CCG VC-API + W3C CCG CHAPI
  - OIDF DCP OID4VCI
  - OIDF DCP OID4VCI + W3C CCG CHAPI

Technical Implementation Requirements

- Conventions Used
- DHS Personal Credential Issuer
  - Accessibility & Openness
  - Platform & Software Security
  - Credential Formats & Digital Signatures
  - Metadata & Vocabulary
  - .gov Binding
  - Issuance Protocol
- DHS Personal Credential Verifier
  - Accessibility & Openness
  - Platform & Software Security
  - Credential Formats & Digital Signatures
  - Metadata & Vocabulary
  - .gov Binding
  - Exchange Protocol
- DHS Personal Credential Holder (Digital Wallet)
  - Accessibility & Openness
  - Platform & Software Security
  - Credential Formats & Digital Signatures
  - Issuance Protocol
  - Exchange Protocol
- Normative References

DHS Personal Credential Verifier Accessibility & Openness

- SHALL NOT implement capabilities that enable Issuer tracking of Holder credential use
- SHALL implement the relevant portions of the W3C Web Content Accessibility Guidelines [W3C-WCAG] to ensure compliance with the Section 508 of the U.S. Rehabilitation Act
  - SHOULD implement the U.S. Web Design System (https://designsystem.digital.gov/)
- SHALL prioritize the implementation of data formats and associated security and privacy mechanisms, inclusive of public facing APIs, that utilize globally available standards and specifications that are openly developed, royalty free and freely available to implement
- SHALL implement in-context explanations that describe who is accessing credentials, what attributes, capabilities or inferences are accessed, for what purpose the credential is needed, and how data will be used, shared and retained
- SHALL enable the Holder to choose a digital wallet
- SHALL implement support for Holder applications (digital wallets) that use web platform technologies
- SHALL implement support for Holder applications (digital wallets) that use native platform technologies

DHS Personal Credential Verifier Platform & Software Security

- SHALL utilize cryptographic modules validated by the joint U.S. & Canada Cryptographic Module Validation Program [CMVP]
- SHALL utilize [FIPS-140] compliant cryptographic key storage mechanisms
  - MAY utilize an operating system capability
  - MAY utilize an external device capability
  - MAY utilize a remote backend capability
- SHALL provide a Software Bill of Materials (SBOM) containing the details and supply chain relationships of various components used in building the Verifier software
  - SHALL contain the minimum elements for a SBOM as defined in the joint report by the Department of Commerce and the National Telecommunications and Information Administration
    - https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom

DHS Personal Credential Verifier Credential Formats & Digital Signatures

- SHALL implement the [W3C-VC-DATA-MODEL] using the JSON-LD Compacted Document Form
- SHALL implement the embedded proof mechanism defined in [W3C-VC-DATA-INTEGRITY]
- SHALL implement selective disclosure capabilities using [W3C-VC-DATA-INTEGRITY] proof sets to support multiple proofs in a single document
  - SHALL implement a proof that is U.S. Federal Information Processing Standards (FIPS) compliant e.g., ECDSA Cryptosuites
  - SHALL implement a proof based on non-correlatable signatures e.g., BBS Cryptosuites
  - SHALL verify all presented proofs in the proof set
  - SHOULD prioritize minimal disclosure of data and metadata by the Holder when negotiating the use of a mutually supported proof, while respecting jurisdictional constraints
  - MAY implement additional proofs e.g., PQC
- SHALL implement [W3C-DID]
- MAY implement additional credential data formats and associated proof mechanisms

DHS Personal Credential Verifier Metadata & Vocabulary

- SHALL implement [W3C-BITSTRING-STATUS-LIST] for credential status checks including revocation checks
- SHALL implement [W3C-DID]
  - SHALL utilize the DID Document as an authoritative source of metadata
  - SHALL implement direct DID resolution
  - SHALL implement support for external DID/Metadata resolvers
  - SHALL digitally verify the U.S. Federal Information Processing Standards (FIPS) compliant [W3C-VC-DATA-INTEGRITY] proof on the DID Document to ensure its integrity and provenance
- SHALL implement [CITIZENSHIP-VOCAB]

DHS Personal Credential Verifier .gov Binding - TBD

- .gov is the top-level domain for governments in the U.S., including federal, state, local, tribal, and territorial
- Only verified U.S. Government organizations can register and operate a .gov domain; registration is free to verified USG organizations
  - https://get.gov/domains/eligibility/
- An entity can gain high assurance that a credential is issued or is being verified by a specific USG organization by digitally verifying a cryptographic link between the USG organization's did:web identifier and its .gov domain
- We are currently evaluating various options that utilize existing technologies and standards to demonstrate this linkage without requiring changes to certificate authority governance, browser technology and trust store governance processes

DHS Personal Credential Verifier Exchange Protocol - TBD

- DHS hopes to support multiple exchange protocols
- Exchange protocol SHALL:
  - support required credential format & digital signature mechanisms
  - support required metadata and vocabulary distribution and verification mechanisms
  - enable the Holder to choose a digital wallet
  - disregard (via implementation profiles) external dependencies that are duplicative or not utilized by the DHS Verifier
- Following many-to-many, multi-vendor interoperability testing, DHS will update the requirements for exchange protocols
- Options under consideration include:
    - W3C CCG VC-API
    - W3C CCG VC-API + W3C CCG CHAPI
    - OIDF DCP OID4VP
    - OIDF DCP OID4VP + W3C CCG CHAPI
    - W3C WICG Digital Credentials API

Technical Implementation Requirements

- Conventions Used
- DHS Personal Credential Issuer
  - Accessibility & Openness
  - Platform & Software Security
  - Credential Formats & Digital Signatures
  - Metadata & Vocabulary
  - .gov Binding
  - Issuance Protocol
- DHS Personal Credential Verifier
  - Accessibility & Openness
  - Platform & Software Security
  - Credential Formats & Digital Signatures
  - Metadata & Vocabulary
  - .gov Binding
  - Exchange Protocol
- DHS Personal Credential Holder (Digital Wallet)
  - Accessibility & Openness
  - Platform & Software Security
  - Credential Formats & Digital Signatures
  - Issuance Protocol
  - Exchange Protocol
- Normative References

DHS Personal Credential Holder (Digital Wallet) Accessibility & Openness

- SHALL NOT implement capabilities that enable Issuer tracking of Holder credential use
- SHALL implement the relevant portions of the W3C Web Content Accessibility Guidelines [W3C-WCAG] to ensure compliance with the Section 508 of the U.S. Rehabilitation Act
  - SHOULD implement the U.S. Web Design System (https://designsystem.digital.gov/)
- SHALL prioritize the implementation of data formats and associated security and privacy mechanisms, inclusive of public facing APIs, that utilize globally available standards and specifications that are openly developed, royalty free and freely available to implement
- SHALL implement in-context explanations that describe who is accessing credentials, what attributes, capabilities or inferences are accessed, for what purpose the credential is needed, and how data will be used, shared and retained
- SHALL enable the Holder to choose a digital wallet
- SHOULD be implemented using web platform technologies
- MAY be implemented using native platform technologies

DHS Personal Credential Holder (Digital Wallet) Platform & Software Security

- SHALL utilize cryptographic modules validated by the joint U.S. & Canada Cryptographic Module Validation Program [CMVP]
- SHALL utilize [FIPS-140] compliant cryptographic key storage mechanisms
  - MAY utilize an operating system capability
  - MAY utilize an external device capability
  - MAY utilize a remote backend capability
- SHALL provide a Software Bill of Materials (SBOM) containing the details and supply chain relationships of various components used in building the Holder software
  - SHALL contain the minimum elements for a SBOM as defined in the joint report by the Department of Commerce and the National Telecommunications and Information Administration
    - https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom

DHS Personal Credential Holder (Digital Wallet) Credential Formats & Digital Signatures

- SHALL implement the [W3C-VC-DATA-MODEL] using the JSON-LD Compacted Document Form
- SHALL implement the embedded proof mechanism defined in [W3C-VC-DATA-INTEGRITY]
- SHALL implement selective disclosure capabilities using [W3C-VC-DATA-INTEGRITY] proof sets to support multiple proofs in a single document
  - SHALL implement a proof that is U.S. Federal Information Processing Standards (FIPS) compliant e.g., ECDSA Cryptosuites
  - SHALL implement a proof based on non-correlatable signatures e.g., BBS Cryptosuites
  - SHALL only present one or more proofs supported by the Verifier
  - SHOULD prioritize minimal disclosure of data and metadata by the Holder when negotiating the use of a mutually supported proof, while respecting jurisdictional constraints
  - MAY implement additional proofs e.g., PQC
- SHALL implement [W3C-DID]
- MAY implement additional credential data formats and associated proof mechanisms

DHS Personal Credential Holder (Digital Wallet) Issuance Protocol - TBD

- DHS hopes to support multiple issuance protocols
- Issuance protocol SHALL:
  - support required credential format & digital signature mechanisms
  - support required metadata and vocabulary distribution and verification mechanisms
  - enable the Holder to choose a digital wallet
  - disregard (via implementation profiles) external dependencies that are duplicative or not utilized by the DHS Issuer
- Following many-to-many, multi-vendor interoperability testing, DHS will update the requirements for issuance protocols
- Options under consideration include:
    - W3C CCG VC-API
    - W3C CCG VC-API + W3C CCG CHAPI
    - OIDF DCP OID4VP
    - OIDF DCP OID4VP + W3C CCG CHAPI

DHS Personal Credential Holder (Digital Wallet) Exchange Protocol - TBD

- DHS hopes to support multiple exchange protocols
- Exchange protocol SHALL:
  - support required credential format & digital signature mechanisms
  - support required metadata and vocabulary distribution and verification mechanisms
  - enable the Holder to choose a digital wallet
  - disregard (via implementation profiles) external dependencies that are duplicative or not utilized by the DHS Verifier
- Following many-to-many, multi-vendor interoperability testing, DHS will update the requirements for exchange protocols
- Options under consideration include:
    - W3C CCG VC-API
    - W3C CCG VC-API + W3C CCG CHAPI
    - OIDF DCP OID4VP
    - OIDF DCP OID4VP + W3C CCG CHAPI
    - W3C WICG Digital Credentials API

Normative References

- [W3C-VC-DATA-MODEL] W3C Verifiable Credentials Data Model
  - https://www.w3.org/TR/vc-data-model-2.0/
- [W3C-VC-DATA-INTEGRITY] W3C Verifiable Credentials Data Integrity
  - https://www.w3.org/TR/vc-data-integrity/
- [W3C-BITSTRING-STATUS-LIST] W3C Bitstring Status List
  - https://www.w3.org/TR/vc-bitstring-status-list/
- [W3C-DID] W3C Decentralized Identifiers
  - https://www.w3.org/TR/did-core/
- [W3C-WCAG] W3C Web Content Accessibility Guidelines
  - https://www.w3.org/TR/WCAG22/
- [CITIZENSHIP-VOCAB] W3C CCG Citizenship Vocabulary
  - https://w3c-ccg.github.io/citizenship-vocab/
- [FIPS-140] Security Requirements for Cryptographic Modules
  - https://csrc.nist.gov/pubs/fips/140-3/final
- [CMVP] Cryptographic Module Validation Program
  - https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program

CBP & USCIS

Personal Credential

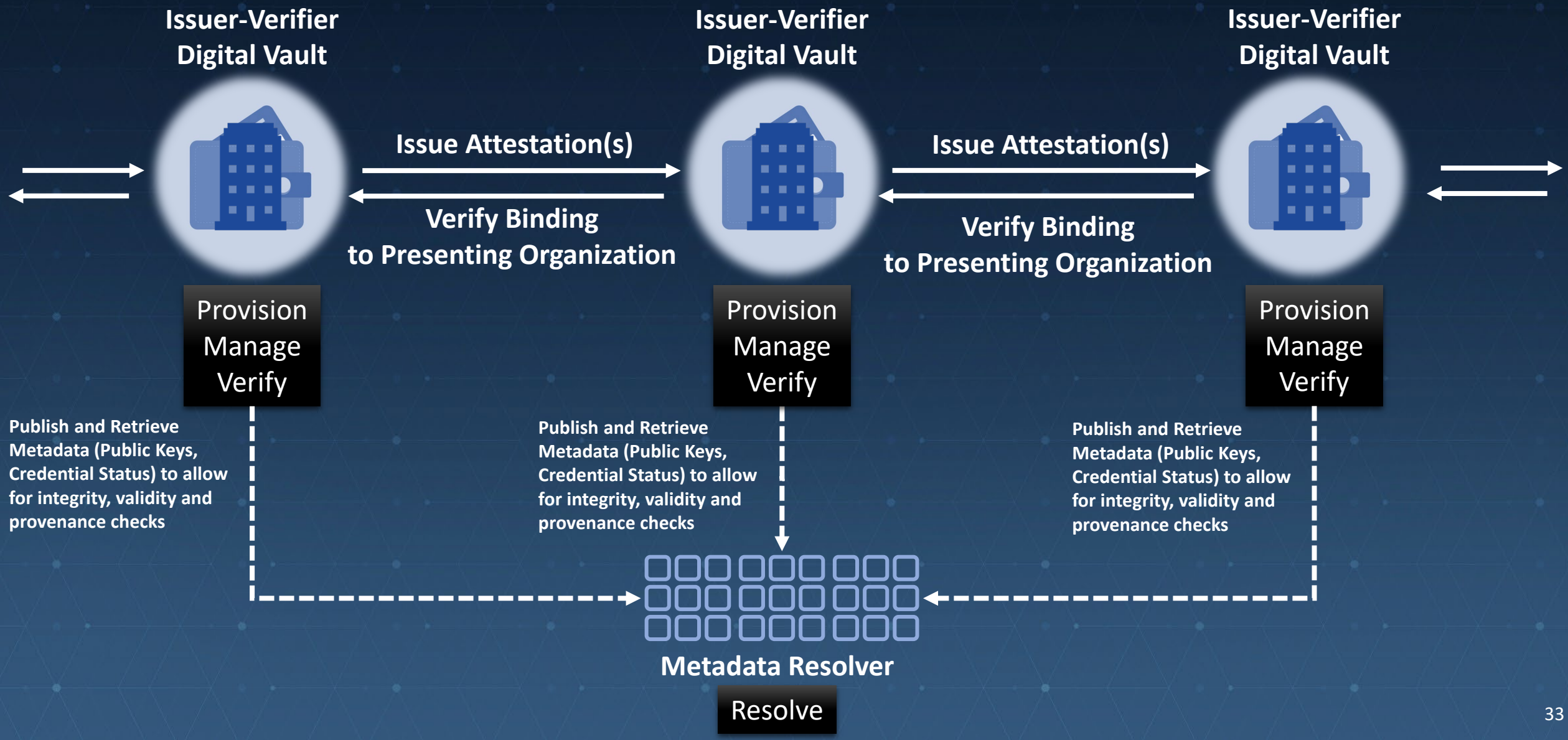
In Person

Online

Supply Chain Organization Credential

Online

Supply Chain Organization Credential Use (Online)
W3C VCDM & W3C DID Standards



Technical Implementation Requirements

- Conventions Used
- CBP/Trade Issuer
  - Credential Formats & Digital Signatures
  - Metadata & Vocabulary
  - Issuance Protocol
- CBP/Trade Verifier
  - Credential Formats & Digital Signatures
  - Metadata & Vocabulary
  - Exchange Protocol
- Normative References

Conventions Used

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.

The requirements on the following pages adopt and use the following ISO document conventions:

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

CBP/Trade Issuer Credential Formats & Digital Signatures

- SHALL implement the [W3C-VC-DATA-MODEL] using the JSON-LD Compacted Document Form
- SHALL implement the enveloping proof mechanism defined in [W3C-VC-JOSE-COSE] with JOSE (Section 3.1.1)
- SHALL implement [W3C-DID]
- MAY implement additional [W3C-VC-DATA-MODEL] compliant proof mechanisms

CBP/Trade Issuer Metadata & Vocabulary

- SHALL implement [W3C-BITSTRING-STATUS-LIST] for credential status checks inclusive of revocation checks
- SHALL implement [W3C-DID]
  - SHALL implement the did:web method as an Organizational Identifier
  - SHALL utilize the DID Document as the authoritative metadata distribution mechanism
  - SHALL implement direct DID resolution
  - SHALL implement support for external DID/Metadata resolvers
- SHALL implement [TRACE-VOCAB]

CBP/Trade Issuer Issuance Protocol

- SHALL implement [TRACE-API]

CBP/Trade Verifier Credential Formats & Digital Signatures

- SHALL implement the [W3C-VC-DATA-MODEL] using the JSON-LD Compacted Document Form
- SHALL implement the enveloping proof mechanism defined in [W3C-VC-JOSE-COSE] with JOSE (Section 3.1.1)
- SHALL implement [W3C-DID]
- MAY implement additional [W3C-VC-DATA-MODEL] compliant proof mechanisms

CBP/Trade Verifier Metadata & Vocabulary

- SHALL implement [W3C-BITSTRING-STATUS-LIST] for credential status checks inclusive of revocation checks
- SHALL implement [W3C-DID]
  - SHALL implement the did:web method as an Organizational Identifier
  - SHALL utilize the DID Document as the authoritative metadata distribution mechanism
  - SHALL implement direct DID resolution
  - SHALL implement support for external DID/Metadata resolvers
- SHALL implement [TRACE-VOCAB]

CBP/Trade Verifier Exchange Protocol

- SHALL implement [TRACE-API]

Normative References

- [W3C-VC-DATA-MODEL] W3C Verifiable Credentials Data Model
  - https://www.w3.org/TR/vc-data-model-2.0/
- [W3C-VC-JOSE-COSE] W3C Securing Verifiable Credentials using JOSE and COSE
  - https://www.w3.org/TR/vc-jose-cose/
- [W3C-BITSTRING-STATUS-LIST] W3C Bitstring Status List
  - https://www.w3.org/TR/vc-bitstring-status-list/
- [W3C-DID] W3C Decentralized Identifiers
  - https://www.w3.org/TR/did-core/
- [TRACE-API] W3C CCG Open API for Supply Chain Traceability
  - https://w3c-ccg.github.io/traceability-interop/openapi/
- [TRACE-VOCAB] W3C CCG Supply Chain Traceability Vocabulary
  - https://w3c-ccg.github.io/traceability-vocab/

Science and Technology

Silicon Valley Innovation Program

dhs.gov/science-and-technology/svip

DHS-Silicon-Valley@hq.dhs.gov

dhsscitech

[W3C-VC-DATA-MODEL] using the JSON-LD Compacted Document Form

W3C Verifiable Credential Data Model

- Information, not data
- Publish & discover
- Built-in versioning & namespaces
- Multi-language support
- Digital signature choices
- Content processing choices
- Dehydrate to binary barcodes

“Dual Signatures” as implemented via [W3C-VC-DATA-INTEGRITY] Proof Sets

- Acceptable and DOES NOT invalidate FIPS 140 validation
  - FIPS 140 validation certificate is allowed to list other algorithms (i.e., “below the line”)
- The format of a dual signature is out of scope for FIPS 140 validation
- Authoritative Reference in the NIST PQC FAQ
  - https://csrc.nist.gov/projects/post-quantum-cryptography/faqs
  - See following slides for a copy of the relevant references

NIST PQC FAQ (1 of 2)

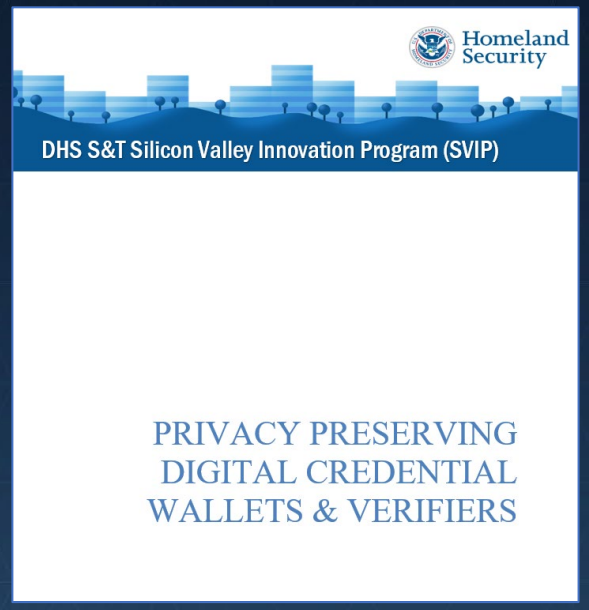
Is it possible for dual signature generation or verification to be performed in a FIPS 140 approved mode of operation? (added 1/28/20)

- "A dual signature consists of two (or more) signatures on a common message. It may also be known as a hybrid signature or composite signature. We will use the term dual signature below. The verification of the dual signature requires all of the component signatures to be successfully verified."
- "Assume that in a dual signature, one signature is generated with a NIST-approved signature scheme as specified in FIPS 186, while another signature(s) can be generated using different schemes, e.g., ones that are not currently specified in NIST standards. Like hybrid key establishment schemes, dual signatures can be accommodated by current standards in "FIPS mode," as defined in FIPS 140, provided at least one of the component methods is a properly implemented, NIST-approved signature algorithm. For the purposes of FIPS 140 validation, any signature that is generated by a non-approved component scheme would not be considered a security function, since the NIST-approved component is regarded as assuring the validity of the dual signature. The format of a dual signature is out of scope for FIPS 140 validation. It is up to the application to specify how to parse signatures and verify them separately."

NIST PQC FAQ (2 of 2)

- Does NIST consider the hybrid key establishment modes and dual signatures to be long-term solutions? (added 1/28/20)
  - “NIST leaves the decision to each specific application as to whether it can afford the implementation cost, performance reduction, and engineering complexity (including proper and independent security review) of a hybrid mode for key establishment or the use of dual signatures. Future experience will help to decide on whether they can be a useful long-term solution. To assist external parties who desire such a mechanism, NIST will accommodate the use of a hybrid key-establishment mode and dual signatures in FIPS 140 validation when suitably combined with a NIST-approved scheme.”

Reducing Cryptographic Implementation Complexity
via our "Privacy Preserving Digital Credential Wallets & Verifiers" work



Open-Source SDKs

A. Cryptographic Tools SDK
B. Sealed Storage SDK
C. Metadata Management SDK
D. Confidentiality and Integrity Protected Computing SDK

"This SDK, when implemented by an issuer, a digital wallet or a verifier makes available to it a suite of cryptographic tools to enable hashing, signing, bulk encryption, streaming encryption, random number generation and more, that can support FIPS compliant cryptography, selective disclosure capabilities, and other privacy preserving cryptographic schemes"

[…]

"It is expected that this module will be developed in a manner that will enable assessment by the Cryptographic Module Validation Program (CMVP) …"