Science and Technology

DHS Implementation Profile of W3C VCs and W3C DIDs

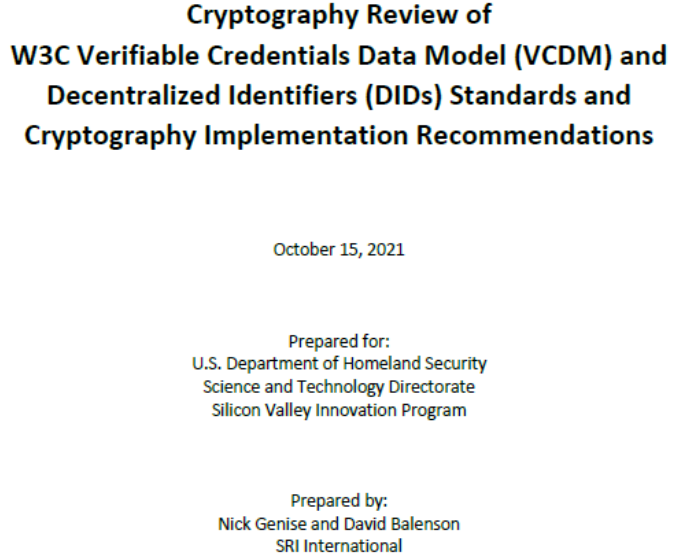
Credential Data Model
Representation Syntax & Proof Format

DRAFT
Work In Progress

WORK IN PROGRESS DATE | 29 September 2022

Guidance to SVIP Performers on Implementation

- To globally scale interoperability, 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 W3C 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
    - …
- Incorporation 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/



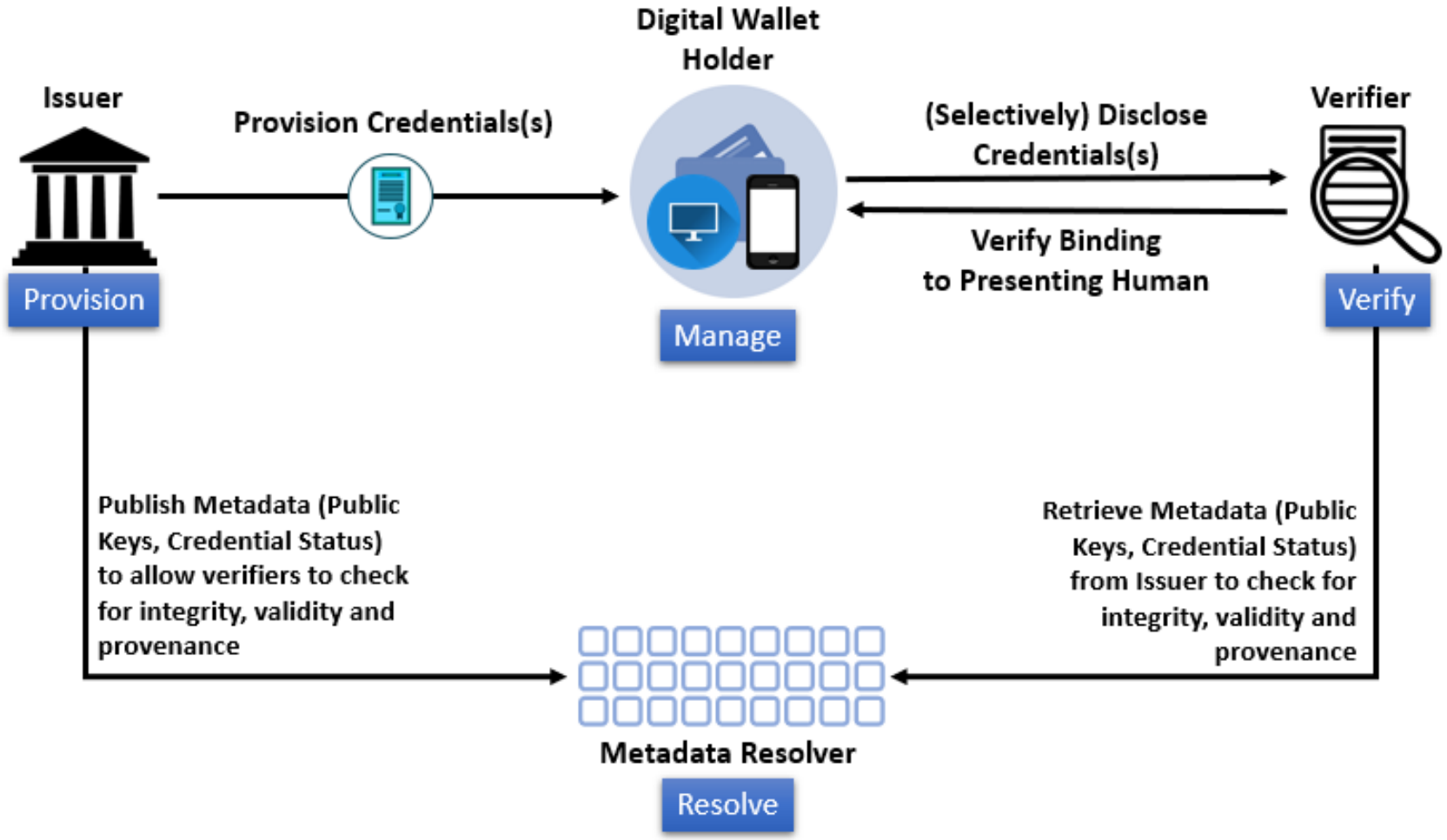
Cryptography Review of
W3C Verifiable Credentials Data Model (VCDM) and Decentralized Identifiers (DIDs) Standards and Cryptography Implementation Recommendations

October 15, 2021

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

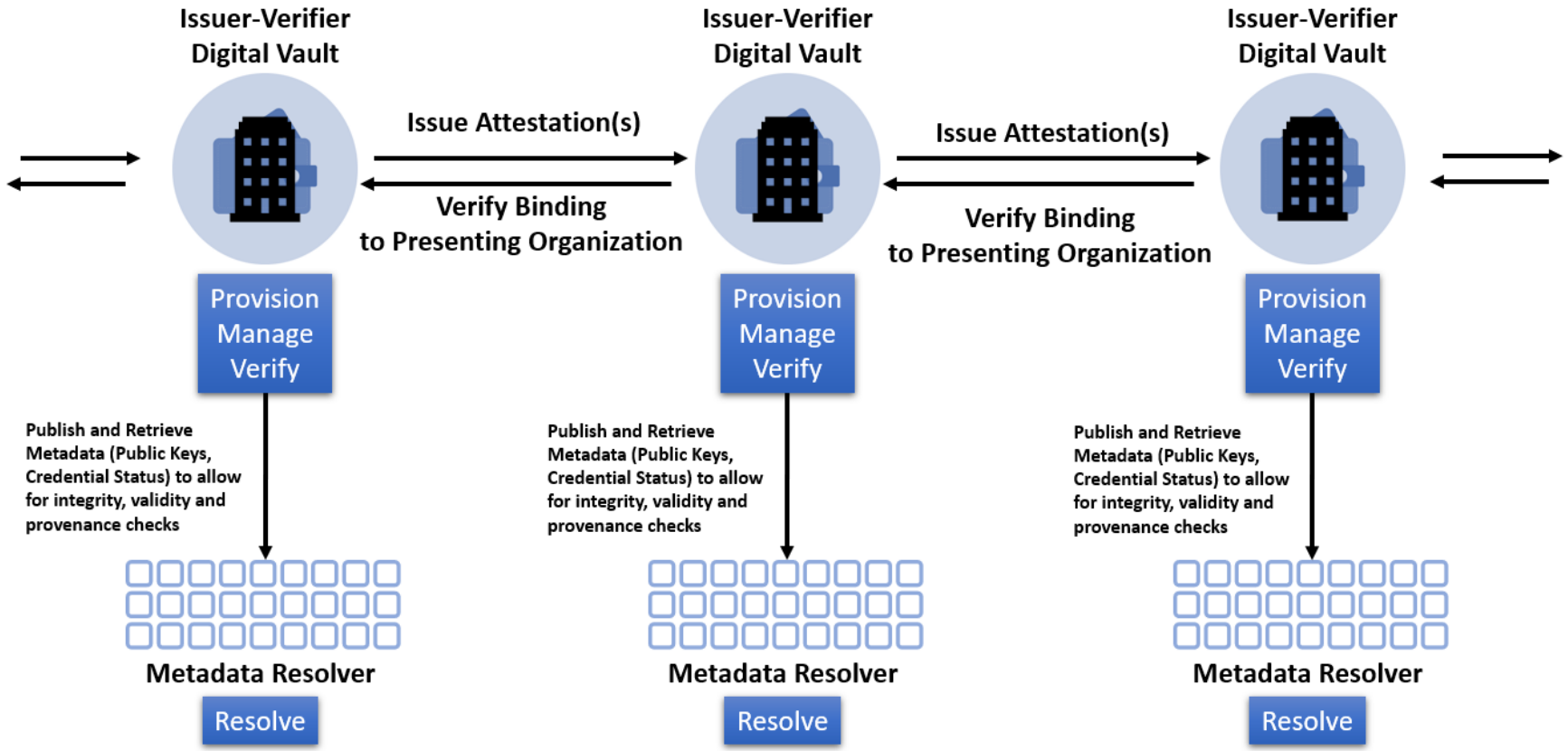
Prepared by:
Nick Genise and David Balenson
SRI International

Digital Wallet Implementation Pattern (Credentials Issued to Individuals)



- 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

Digital Vault Implementation Pattern (Credentials Issued to Organizations)



- 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 Implementation Decision Factors

- Support for a Competitive Ecosystem and Individual Choice
  - Choice of identifiers for individuals
  - Choice of wallets for individuals
  - Enabling market reach via support for complementary work
- Support for Individual Privacy
  - Removing Phone Home and Back-Channel Interactions
  - Enabling selective attribute disclosure
  - Mitigating tracking of individuals and Unlinkability
  - Enabling individual awareness of Verifier use of issued credentials
- Support for Supply Chain Traceability
  - End to end visibility of supply chain hops
  - Denying anonymity to organizations in the supply chain

- Need for Cryptographic Flexibility
  - FIPS Compliant Cryptography
  - Quantum-Resistant Cryptography
  - Selective Disclosure Cryptography
- Availability of Intent Signaling Functionality
  - By Issuer
  - By Wallet/Vault
  - By Verifier
- Availability of Digital Wallet/Vault Feature Detection
  - Independent Testing
  - Cryptographic Challenge/Response
  - Certification and Accreditation by Third Parties

All desired functionality for everyone WILL NOT be technically feasible or possible on Deployment Day 1

Multiple choices/options are in play and maturing in the ecosystem, so the choices we make now may change as the ecosystem matures and best practices for interoperability, security and privacy become clearer!

De-risk via incremental and iterative delivery of capabilities and functionality

Implementation Profile Document Conventions

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

References

Normative

- [VC-DATA-MODEL]
  W3C Verifiable Credentials Data Model
  https://www.w3.org/TR/vc-data-model/
- [DID-CORE]
  W3C Decentralized Identifiers
  https://www.w3.org/TR/did-core/
- [JSON-LD]
  A JSON-based Serialization for Linked Data
  https://www.w3.org/TR/json-ld11/

Informative

- W3C VC & W3C DID Cryptography Review
  http://www.csl.sri.com/papers/vcdm-did-crypto-recs/
- …

Credential Data Model: Representation Syntax

- **Normative**
  - Verifiable Credentials and Verifiable Presentations, as defined in [VC-DATA-MODEL], SHALL be serialized as [JSON-LD] in compacted document form
    - A Verifiable Credential SHALL define all terms using *@context*
    - A Verifiable Presentation SHALL define all terms using *@context*
    - [JSON-LD] SHALL define all types using *@type*
    - [JSON-LD] SHOULD leverage objects instead of strings to refer to Issuers and Holders
    - [JSON-LD] MAY rely on *@vocab* to automatically define terminology
- **Conformance Testing [Informative]**
  - All normative statements will be verifiable via automated testing or other methods
  - Work is in progress on conformance testing and how to verify the desired outcome

Credential Data Model: Proof Format (1/2)

- **Normative**
  - Verifiable Credentials, as defined in [VC-DATA-MODEL], SHALL be signed using the Data Integrity Proof format
    - Data Integrity Proof format SHALL implement mandatory U.S. Federal Information Processing Standards (FIPS) Compliant Cryptography [See FIPS Compliant Cryptography Section of Profile]
    - Data Integrity Proof format SHALL implement interoperable security engineering best practices [See Interoperable Security Section of Profile]
    - Data Integrity Proof format SHALL implement interoperable privacy engineering best practices [See Interoperable Privacy Section of Profile]
  - Verifiable Credentials, as defined in [VC-DATA-MODEL], SHALL NOT be signed using the Camenisch-Lysyanskaya Signature (AnonCreds) Proof format
  - …

Credential Data Model: Proof Format (2/2)

- …
- Verifiable Credentials, as defined in [VC-DATA-MODEL], MAY be signed using the JSON Web Token Proof format
  - JSON Web Token Proof format SHALL implement mandatory U.S. Federal Information Processing Standards (FIPS) Compliant Cryptography [See FIPS Compliant Cryptography Section of Profile]
  - JSON Web Token Proof format SHALL implement interoperable security engineering best practices [See Interoperable Security Section of Profile]
  - JSON Web Token Proof format SHALL implement interoperable privacy engineering best practices [See Interoperable Privacy Section of Profile]

- **Conformance Testing [Informative]**
  - All normative statements will be verifiable via automated testing or other methods
  - Work is in progress on conformance testing and how to verify the desired outcome

Science & Technology

Thank You

Silicon Valley Innovation Program

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