Current State of CCG

August 2024

Agenda

1. VC-API
2. VC 2.0 Test Suite
3. Quantum Safe DI Signature Suite
4. VC Education
5. VC Traceability
6. VC Render Method
7. VC Barcodes
8. Verifiable Issuers and Verifiers
9. DID Linked Resources

Verifiable Credential API (and Verifiable Presentation Request)

Manu, Dave, Ted, Patrick, John, Joe, Eric, and Wes

An API for performing Verifiable Credential lifecycle management

- Supports Issuance, Verification, Presentation, and Status Modification
- Supports OID4 and Workflows/Exchanges
- 11 implementations (varying levels of interoperability)
- Used extensively in VCWG for test suites and canivc.com
- Production deployments (TruAge, CA DMV/OpenCred)
- Most issues have resolutions, PRs are lagging (due to VC 2.0 work)
- Plan is to propose it for standards track soon

VC WG Test Suites

Benjamin Young

VCDM 2.0 - https://w3c.github.io/vc-data-model-2.0-test-suite/
Data Integrity & cryptosuites:

- ECDSA & ECDSA-SD - https://w3c.github.io/vc-di-ecdsa-test-suite/
- BBS - https://w3c.github.io/vc-di-bbs-test-suite/
- EdDSA 2022 - https://w3c.github.io/vc-di-eddsa-test-suite/
- Ed25519Signature 2020 - https://w3c.github.io/vc-di-ed25519signature2020-test-suite/

Bitstring Status List - https://w3c.github.io/vc-bitstring-status-list-test-suite/

JOSE/COSE - https://w3c.github.io/vc-jose-cose-test-suite/

VC JSON Schema - https://w3c.github.io/vc-json-schema-test-suite/

VC WG Test Suites (implementers)

Benjamin Young

VCDM 2.0 - apicatalog.com, Digital Bazaar, OpSecId, SpruceID, VC Issuer Mock
Data Integrity & cryptosuites:

- **ECDSA & ECDSA-SD** - apicatalog.com, Digital Bazaar, SpruceID, bovine
- **BBS** - Digital Bazaar, Grotto Networking, SpruceID
- **EdDSA 2022** - apicatalog.com, Digital Bazaar, OpSecId, SpruceID, Trinsic, bovine
- **Ed25519Signature 2020** - apicatalog.com, Danube Tech, Digital Bazaar, EWF, LearnCard, OpSecId, SourceID, Trinsic

Bitstring Status List - OpSecId, Digital Bazaar

JOSE/COSE - None

VC JSON Schema - Block (TBD)

Quantum Safe DI Signature Suite

Andrea D'Intino - Forkbomb B.V.

- Context:
  - FIPS 203, 204 and 205 (finalized TODAY!), to standardized the winners of NIST PQC https://www.whitehouse.gov/wp-content/uploads/2024/07/REF_PQC-Report_FINAL_Send.pdf)
  - W3C-VC standardization WG: https://w3c-ccg.github.io/di-quantum-safe/
- Implemented:
  - ML-DSA-44 (FIPS 204) and Dilithium2 using PQ-Clean
  - Dyne:did method supports ML-DSA-44 and Dilthium2 pubkeys in base58 (https://dyne.org/W3C-DID/#dyne-org-s-w3c-did-security-vocabulary)
  - Prototype of W3C-VC issuer
  - Prototype of sign/verify ML-DSA-44 microservice with GUI (https://github.com/ForkbombEu/tf-pqcrypto-scripts), runs also on AWS EC2+S2 (https://github.com/ForkbombEu/tf-ncr)
- Missing:
  - Multikey support
  - Data integrity
  - API testing suite

VC Education

xxx

VC Traceability

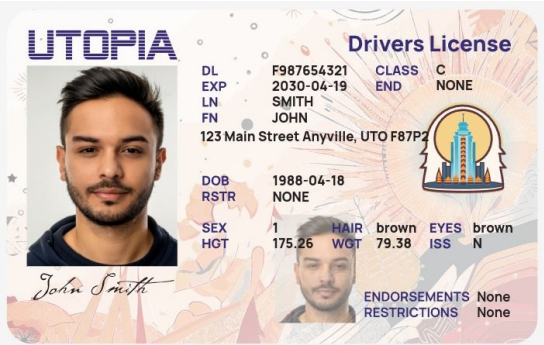
xxx

VC Render Method

Manu, Dmitri, Calvin, Kyle, Patrick

A secure way for issuers to convey how they want their credentials displayed.

- Production deployments in Singapore for Open Attestation Renderer)
- Multiple implementations (none interoperable yet)
- Experimenting with SVG, PDF, and other text-based template formats
- Examples deployed in Playground, standardization ETA 6-12 months



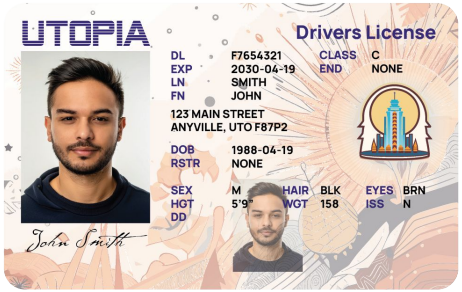
Current state of CCG Aug. 2024

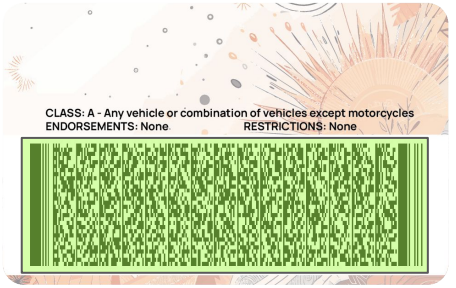
Verifiable Credential Barcodes

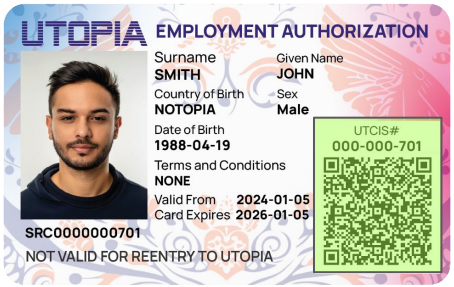
Wes, Manu, Dave, Yash Shah (Credence ID)

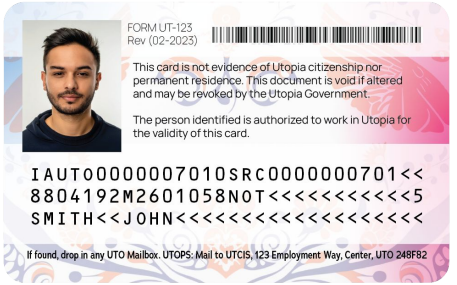
Cryptographic security for physical credentials

- Encode Verifiable Credential in easily-consumable barcode format
- Use new **ecdsa-xi** cryptosuite to digitally sign both the VC and optically readable data on the card (e.g. MRZ)
- Multiple implementations in progress
  - Test vectors available in specification
- Production deployments for CA DMV and DHS in progress
- Plan is to propose for standards-track soon









Current state of CCG Aug. 2024

Verifiable Issuers and Verifiers

Isaac Henderson

- Currently we are working on the data model of the issuer lists and planning to publish the first version by the end of October
- We are on summer break and will start the meeting again in September

DID-Linked Resources

Alex Tweeddale, Ankur Banerjee

Context

- DID-Linked Resources (DLRs) can be used to associate digital files with DIDs, via signing the resource with the verification method keys from a DID Document.
- This is currently being used to store: status lists, trust registries, schemas, policies - in a chronological and sequentially ordered way.

Update

- Draft specification has been published: https://w3c-ccg.github.io/DID-Linked-Resources/
- Review and feedback required by the wider CCG community
- Work underway to build DLRs into the Universal Resolver/Registrar in a standardised way