Credential Formats, Signatures, and Exchange Protocols Drafting Group

Objective

Health Pass compliant implementations must use a standard set of credential formats, digital signature algorithms, and exchange protocols.

Terms of Reference

The primary challenge in designing interoperabile digital credentials of *any* kind is how to standardize the **container** for the data — together with the **digital signature** on the container from the issuer — so that the data inside the container can be trusted by verifiers (and also so it can interoperate across multiple digital wallet implementations).

This standardization challenge was first recognized by the W3C Credentials Community Group in 2015, which incubated the early work that culminated in the establishment of the W3C Verifiable Claims Working Group in 2017. The final approval of the W3C Verifiable Credentials Data Model 1.0 specification followed in September 2019.

There is now strong market momentum toward production usage of verifiable credentials compliant with this W3C standard. This, together with the security, privacy, and data control benefits of decentralized identity architecture, have made W3C verifiable credentials the default choice of the Good Health Pass Collaborative. (See https://www.lfph.io/wp-content/uploads/2021/03/CCI-Paper-Based-VC-Summit-Summary-Report.pdf)

It is, however, important to note that: a) the W3C verifiable credential standard supports several different data container formats as well as multiple digital signature options, and b) the W3C standard does **not** standardize credential presentation and exchange protocols (which were explicitly out of scope for the W3C Working Group charter but were, rather, left for industry to innovate).

Therefore, to achieve global interoperability of Good Health Pass credential implementations, it is necessary to agree on:

1. **The credential data format(s)** (ideally just one).
2. **The credential digital signature suite(s)** (ideally just one).
3. **The credential presentation and exchange protocol(s)** (ideally just one).
4. The **credential revocation mechanism(s)** (ideally just one) for credentials that must be revocable.

Why in each case do we say, “ideally just one”? Because, in the words of Brian Behlendorf, GM of Blockchain, Healthcare, and Identity at the Linux Foundation, “Optionality is never free—it comes at the cost of combinatorial complexity for all implementers.” This cost is redoubled when security and privacy considerations are paramount.

There are many other considerations that go into making these choices, including:

- Performance requirements at airports, airlines, and other travel industry verifiers where reducing travel friction is of critical importance,
- Offline verification requirements in some locales (e.g., no Internet, loss of power, etc.),
- Meeting regulatory requirements for security and privacy,
- Ease of integration with existing systems and solutions, especially legacy travel reservation, security, and check-in systems and procedures,
- Cost and availability

In short, this is one of the most difficult sets of choices that Good Health Pass collaborators must make. Thankfully, excellent work is already being done in this area.

In February 2021, the COVID-19 Credential Initiative (CCI) hosted by Linux Foundation Public Health published a paper by CCI Ecosystem Director Kaliya Young titled Verifiable Credentials Flavors Explained. It explains the differences between the major credential data formats and digital signature algorithm choices (JWT, JSON-LD with LD Signatures, ZKP-CL, JSON-LD with ZKP BBS+). CCI is also currently working on a paper, analyzing the differences between the major credential presentation and exchange protocols, including DIDComm, the Aries Protocol suite, DIF Presentation Exchange, OpenID Self-Issued OpenID Provider (SIOP), and Web/REST using the Credential Handler API (CHAPI).

Responsibilities and Deliverables

Key Interoperability Questions That Must Be Answered:

1. Which verifiable credential format – or formats – compliant with the W3C Verifiable Credentials Data Model 1.0 specification will Good Health Pass systems support?
2. Which verifiable credential signature suite – or suites – compliant with the W3C Verifiable Credentials Data Model 1.0 specification will Good Health Pass systems support?
3. What verifiable credential presentation and exchange protocol or protocols will Good Health Pass systems support?
4. What are the requirements for credential revocation, and how will it be handled so that it is interoperable?
5. How will interoperability with these choices be tested/verified/certified?
6. How will decisions be made if/when additional formats, signature suites, and/or presentation and exchange protocols are developed?
7. How will credentials that don’t comply with the W3C model be addressed?

Chairs/Conveners

- Brent Zundel
- Daniel Bachenheimer
- Kaliya Young

Members

Only members of the Trust Over IP Foundation who have signed the necessary agreements and charters are permitted to participate in this Drafting Group and contribute to its deliverables.

Please add your name to the list below to indicate you have joined the Drafting Group:

- Nuttawut Kongsuwan
- Riley Hughes
- Trev Harmon
- Jim St.Clair

Meeting Schedule

The Drafting Group meets on an alternative schedule. Please see the Calendar of ToIP Meetings.

Meeting Page

Please find agendas, presentations, notes and recordings for all Drafting Group meetings **HERE**.

Communications

The Slack channel for this Drafting Group (trustoverip.slack.com) is #ghp-wg-credential-formats