The COVID-19 Credentials Initiative:

Bringing emerging privacy-preserving technology to a public health crisis.

Kaliya Young, Identity Woman, Co-Founder of the Internet Identity Workshop, Merritt College
Lucy Yang, Co-Chair of the COVID-19 Credentials Initiative

In a major crisis people want to step up and help find and adapt tools for solutions. A technology community building tools based on a W3C standard called **Verifiable Credentials** came together in March to form the COVID-19 Credentials Initiative (CCI). We are submitting this position statement to share an abbreviated case-study of this work and to highlight key challenges that arose in trying to responsibly use new privacy-preserving technologies for this or any crisis.

So what is this emerging technology that is just coming to market with very early adopters and innovators leading the way (including the US government, government of British Columbia, etc.)? It is called Verifiable Credentials (VC or VCs), a data format standard developed and published by the W3C last year. It is a universal data format for one entity (person, organization or thing) to assert something about another entity (person, organization or thing). The issuer packages up the credential and cryptographically signs it to seal the data it contains. It passes this to the subject, or holder so that the subject can share it with the receiver of the credential, the verifier, at that point the receiver is able to use cryptography to check the seal and the validity of the issuer. VC is privacy preserving because the issuer (identity provider) and verifier (relying party) do not form a technical/federated link with each other. Information does not pass directly.

This technology gives people the ability to collect and manage digital credentials similar to the cards we find in our physical wallets in digital wallets. These digital credentials act like paper credentials because individuals do not need to have the verifier directly connect to the issuer. Why is this new? Until now, to have provable information exchanged, the issuer and verifier would need to directly “federate” to exchange information about the data subject.

Immunology is complex science but simplified basics about how it works with some viruses are known. It was based on these simple understandings that possibilities for how VCs might be used by people and institutions to better manage risk began to be explored. One obvious use case was the ability to issue VCs that reflect some type of COVID-19 status, a proof that one:

- Tests positive for antibodies and therefore not infected/or vulnerable to being infected.
- Has recently tested negative therefore the risk of being infected is low and that one could go to work, travel or visit a facility with vulnerable populations.
- Has received a vaccine for COVID-19 and therefore safe to travel or access a large in-person-event.

Some of these use-cases as articulated are not new (e.g. the Yellow Card), it’s just new to digitize them. It makes sense to consider how this simple paper-based technology can be updated to digital. However, the mild hysteria raised about doing things today done on paper via digital means that concerns were triggered without fully understanding or exploring how to use the technology. Some were so concerned that they resigned from organizations whose leadership floated these ideas.

COVID-19 status is currently shared in two forms 1) with the patient via a phone call or text message from the doctor or testing site or 2) in a patient medical record. Neither of these solutions provides a clear way for the subject to prove results to an entity that wants to know this information (e.g. an airline). VCs offer a new innovative format that provides people with information about their COVID-19 status that is under their control and verifiable by a relying party.

The open standards based VC approach is in strong contrast to the CommonPass effort, led by a Rockefeller-Foundation-backed nonprofit, that co-arose in the same time frame. The leadership at CommonPass is connected to the conventional medical records world and proposed the creation of a global system where patient medical records in some as yet to be determined way would be shared with a centralized decision engine that CommonPass would run globally. They held several global meetings with hundreds of people, including government leaders attending to build momentum for their proposed solution. There are also scores of siloed proprietary solutions popping up to solve these data sharing challenges, for example, CLEAR is offering a biometric data sharing solution. In a public health crisis, these non-interoperable solutions are only good when only one of them is widely adopted, which doesn't seem to be the case.

The community that formed around CCI was mostly made up of small early-stage startups who were already implementing VCs for other use-cases and decided to collaborate on exploring COVID-19 use cases. This makeup of the community means that it is not connected to global elites, governments, health departments or healthcare institutions. One exception to this is a startup that had political connections and worked with a California State Legislator to have a bill AB2004 proposed, which opened up a committee to study the use of VCs for COVID-19 medical test results. The bill just passed the senate and is now waiting to be signed by the Governor to become a law. However, the Electronic Frontier Foundation has repeatedly voiced its opposition [1] [2].

CCI has struggled to "raise our voice" and be "heard" by the powers that be who make decisions. The experience of this group raises questions:

- How can emerging technology be "seen" by actors (governments, public health officials, airlines, work places) in the marketplace looking for solutions.
    a) Which technologists are listened to by policy makers?
    b) How are these actors making decisions about the claims these technologists are making?

- How can networks of potential issuers of COVID-19 status credentials be spun up in such a way that the credentials issued are seen as valid by verifiers (airlines, etc.)? This set of challenges around the technology are not technical as much as they are about process and accountability systems.

- How can existing norms of information sharing about people that are paper-based today be translated into digital form in ways that make themselves and those concerned about human rights implications comfortable with the technical deployment?

- How can a new privacy-preserving technology based on open standards be used for public health crises or any other time-sensitive occasions when its deployment and adoption requires a lot of coordination, collaboration and communication? How can these things be facilitated by funders seeking to make a difference?