We need countermeasures against coercion of COVID-19 credentials

Oskar van Deventer (TNO), Alexander Blom (Bloqzone), Line Kofoed (Bloqzone)
14 September 2020

This is a position statement for the “Privacy & Pandemics Workshop”, 27-28 October 2020.

We confirm that we are willing to accept USD 1500 to participate in a relevant workshop session or present a “firestarter” at the virtual event.

Summary
This position statement argues that we need countermeasures against coercion of verifiable credentials, especially COVID-19 credentials. We propose an initial set of countermeasures, which are an amalgamation of technical, governance and legal measures. Our implementation demonstrates the technical feasibility of one of the proposed countermeasures: technically enforced verification of the verifier.

Introduction: 800-pound gorilla asks your credentials
The concept of "self-sovereign" identity presumes that parties are free to enter a transaction, to share personal and confidential information, and to walk away when requests by the other party are deemed unreasonable or even unlawful. In practice, this is often not the case: "What do you give an 800-pound gorilla?", answer: "Anything that it asks for". Examples of such 800-pound gorillas are some big-tech websites, immigration offices and uninformed individuals alleging to represent law-enforcement [1]. Also the typical client-server nature of web transactions reinforces this power imbalance, where the human party behind its client agent feels coerced into surrendering personal data as otherwise they are denied access to a product, service or location.

COVID-19 urgency: coercion of health credentials is bad for society
Efforts to mitigate the effects of the COVID-pandemic using identity technology need strict legislation in order to uphold human rights and dignity.

The UN High commissioner Human Rights recently urged the European Commission to “Enhance the availability, accessibility and effectiveness of redress mechanisms for unjustified decisions made by digital services” [2].

Early September, the California bill “AB-2004 Medical test results: verification credentials” was passed, requiring that “Verifiable credential models should not in any way compromise an individual’s right to privacy, including by means of tracking or reporting the individual’s usage of the verifiable health credential” [3].

Around the same time, in the Netherlands, a special temporary corona-app law was approved, which makes it illegal to enforce the use of a covid-notification app or any other comparable digital means.

The issue of countermeasures against coercion has become more prominent and urgent in the context of the COVID-19 crisis. Here the 800-pound gorillas may be employers demanding health

information that they are not entitled to, or even shops and restaurants, if the sharing of health data has become low friction thanks to verifiable credentials. An extreme case is this: “Even with careful legislation and convenient testing, some uninfected individuals, desperate to return to their daily lives, may deliberately risk infection, betting that they’ll recover and be eligible for the ‘golden ticket’ certifying their immunity” [4].

Countermeasures are governed by governance frameworks

Implementations of one or more potential countermeasures against different types of coercion may be certified within a governance framework. In case of a machine readable governance framework, countermeasures may be automatically enforced, safeguarding its user from being coerced into action by for example unauthorized parties. Different governance frameworks may choose different balances between full self-sovereignty and tight control, depending on the interests that are at play as well as applicable legislation.

Examples of countermeasures: combining technical, governance and legal

The following are examples of potential countermeasures against coercion [5]. The governance framework can stimulate or enforce that some verifiable credentials are only presented when the holder agent determines that certain requirements are satisfied. When a requirement is not fulfilled, the user is warned about the violation and the holder agent may refuse presentation of the requested verifiable credential.

- **Require authoritative verifier**. Verifiers would need to be authorized within the applicable governance framework. A wallet application may technically enforce this governance policy.
- **Require evidence collection**. Requests for presentation of verifiable credentials may hold up as evidence in court, if the electronic signature on the requests is linked to the verifier in a non-repudiable way.
- **Require enabling anonymous complaints**. The above evidence collection may be compromised if the holder can be uniquely identified from the collected evidence. So a governance framework may require the blinding of holder information, as well as instance-identifiable information about the evidence itself.
- **Require remote/proxy verification**. Verification has only value to a holder, if it results in a positive decision by the verifier. Hence a holder should preferably only surrender personal data if this warrants a positive decision. It would save travel, if the requested decision is access to a physical facility. It would in any case prevent unnecessary disclosure of personal data. Some verifiers may consider their decision criteria confidential. Hence, different governance frameworks may choose different balances between holder privacy and verifier confidentiality.
- **Require complying holder agent**. Some rogue holder agents may surrender personal data against the policies of the governance framework associated with that data. Issuers of such data may require verification of compliance of the holder’s agent before issuing.

Demo PoC: “Verify the Verifier”

Subsequent to the Working Group use case “Verify the Verifier” COVID-19 Credentials Initiative [6], one of us (Bloqzone) has built a “Verify-the-Verifier” PoC [7] . In this PoC, the doorman of a home-for-the-elderly requests a volunteering visitor to present specific credentials to gain access to the sbuilding. In the process, the visitor application connects to the doorman application, and the visitor application requests the doorman application for authentication as well for its authorization to request a specific credential, see Figure 1.

Conclusion: Combine technical implementation with legal policy making

We need countermeasures against coercion of verifiable credentials, especially COVID-19 credentials. However, some of the countermeasures may only be effective with the appropriate legal precedence backing. For example, if the collected technical evidence is not accepted in court, it loses force against 800-pound gorillas. We call for a combined technical+governance+legal project to develop solutions and to assure the effectiveness of these in society.

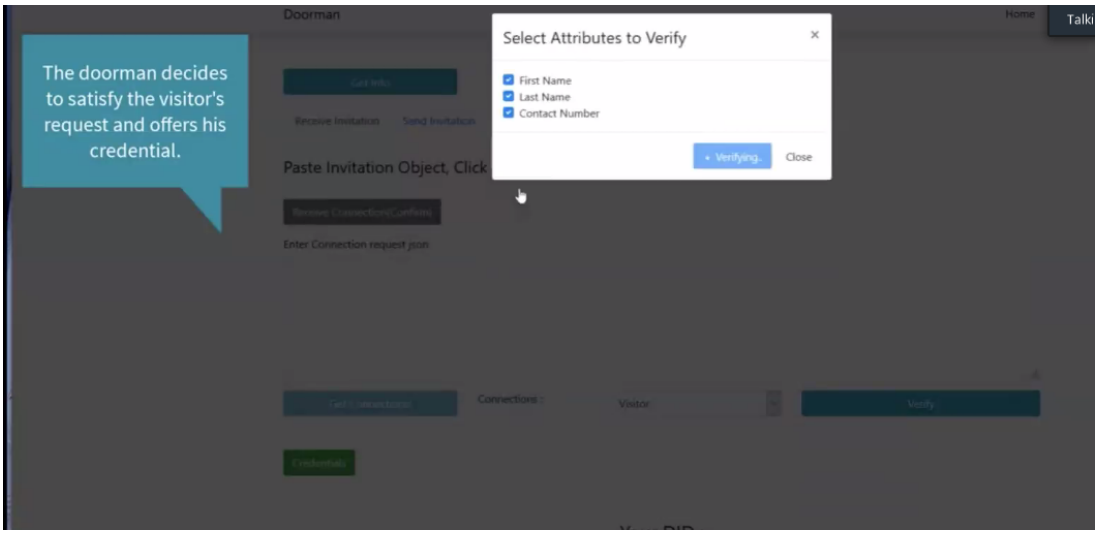

Figure 1: Visitor asks verification of Doorman before presenting a privacy-sensitive COVID-19 credential.

References

[1] Oskar van Deventer et al, "Self-Sovereign Identity - the good, the bad and the ugly", TNO, May 2019, https://blockchain.tno.nl/blog/self-sovereign-identity-the-good-the-bad-and-the-ugly/

[2] UN High Commissioner for Human Rights, Michelle Bachelet, Letter in response to the public consultation on the EU's Digital Services Act, 2020-09-07, https://europe.ohchr.org/Pages/Digital-Services-Act.aspx

[3] Senator Hertzberg et al, "AB-2004 Medical test results: verification credentials.", https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201920200AB2004

[4] Dakota Gruener, "Immunity Certificates: If We Must Have Them, We Must Do It Right", https://ethics.harvard.edu/immunity-certificates

[5] Matthew Davie, Oskar van Deventer et al, "0289: The Trust Over IP Stack", Draft Hyperledger Aries RFC 0289, 2019-2020, https://github.com/hyperledger/aries-rfcs/tree/master/concepts/0289-toip-stack#countermeasures-against-coercion

[6] COVID-19 Credentials Initiative, https://www.covidcreds.com/, Use Case 11 – Verify-the-Verifier, https://docs.google.com/document/d/1PQvDm1ssKypH9X1CV97sStOxfnnSpzLKyDEPJ_bAp7E

[7] Bloqzone, "Who wants to know? Verifying the Verifier", demo PoC mandated verifier identification, https://bloqzone.com/who-wants-to-know/