A Critique of EU Digital COVID-19 Certificates: Do Vaccine Passports Endanger Privacy?

Harry Halpin
Nym Technologies
Neuchâtel, Switzerland
harry@nymtech.net

ABSTRACT

Do COVID-19 vaccine passports come at a fundamental cost for personal privacy? Reviewing proposed COVID-19 credentials from a security and privacy standpoint raises concerns that make deploying COVID-19 digital certificates difficult at best. A closer look into the privacy of the EU Digital COVID-19 certificate presents a fundamental contradiction between two essential security properties: unforgeability and privacy. A substantial reconsideration of the very concept of vaccine passports may be needed to preserve fundamental privacy rights.

CCS CONCEPTS

• **Social and professional topics** → **Patient privacy**; **Personal health records**.

KEYWORDS

COVID-19 certificates, vaccine passports, security, privacy, standards

ACM Reference Format:
Harry Halpin. 2022. A Critique of EU Digital COVID-19 Certificates: Do Vaccine Passports Endanger Privacy?. In *The 17th International Conference on Availability, Reliability and Security (ARES 2022), August 23–26, 2022, Vienna, Austria.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3538969.3544459

1 INTRODUCTION

At the start of 2021, the COVID-19 pandemic has caused a push for globally standardized "vaccine passports" to allow the re-opening of travel and even everyday life. The European Union took the lead in rolling the EU Digital Green Certificate in summer 2021, followed by a series of WHO recommendations. Other countries like the United States have vaccination records issued by their own local authorities, such as the Center for Disease Control (CDC), but do not have a digital version of a vaccine passport, and other countries such as Lebanon have attempted to deploy their own passports.

Given the rush to deployment, there has been both privacy and wider social concerns raised about vaccine passports from the public [6], including questioning whether they should even exist due to their exacerbation of social inequality [8]. Yet unlike the COVID-19 contact-tracing efforts which triggered intensive work and discussion by the academic privacy community [13], there have been little engagement from the academic and wider privacy community on vaccine passports. This is despite the fact that contact-tracing ended up essentially being used by only a negligible percentage of the population in most countries,[1] while vaccine passport uptake was more often legally mandated and so was widely used.

Although the usage of vaccine passports may decline as the COVID-19 pandemic moves to an endemic stage, the broader question remains whether or not these vaccine passports will continue to be used in the context of future pandemics and transition into a permanent feature of daily life.[2] Although it is beyond the scope of this work to determine the answer to the ethical questions such as whether or not the possible privacy violations of COVID-19 digital certificates are justified and whether privacy concerns outweigh the gains in convenience, our goal is outline the privacy concerns and violations as such.

Our review includes the following elements:

- Section 2 reviews both the promise and potential perils of digital vaccine passports, including the necessity for defining clear technical security and privacy goals.
- Section 3 inspects the EU Digital COVID Certificate design for privacy and security considerations.
- Section 4 presents qualitative interviews with a number of the designers and critics of vaccine passports to understand how their judgments around engineering privacy in the design of the EU Digital Certificates.
- Section 5 concludes with a discussion of what lessons can be learned in the case that various nation-states attempt to make the infrastructure around COVID-19 certificates permanent.

2 VACCINE PASSPORTS

A vaccine passport can be thought of as a kind of credential that contains information needed to determine whether or not an individual has been vaccinated or tested for COVID-19. This credential may be a digital credential that can be verified cryptographically, thereby allowing it to be studied from the perspective of cryptographic security properties [2]. Here, we restrict our analysis to cryptographic digital credentials. Note that we will use both the term *vaccine passports* to cover any form of COVID-19 information attached to an identity as the purpose of these credentials is to

ARES 2022, August 23–26, 2022, Vienna, Austria

ACM ISBN 978-1-4503-9670-7/22/08.
https://doi.org/10.1145/3538969.3544459

[1] 'COVID-19 Contract Tracing Apps Reach 9% Adoption in Most Populous countries' from July 2020: https://sensortower.com/blog/contact-tracing-app-adoption
[2] This has been proposed in the United Kingdom in June 2022, see 'A plan for health and social care': https://www.gov.uk/government/publications/a-plan-for-digital-health-and-social-care/a-plan-for-digital-health-and-social-care

restrict mobility to the unvaccinated, although the many systems have re-branded themselves as *vaccine certificates*, and so the two terms will be used interchangeably.[3]

2.1 Goals and Threat Model of Vaccine Passports

The goals of the vaccine passports are, through the restriction of rights of individuals who do not possess them, to allow [10]:

(1) Resumption of in-person activities under conditions that would normally cause the spread of COVID-19.
(2) International travel to resume between countries without spreading COVID-19.

Given the mutation of COVID-19 and its uncertain future trajectory in terms of transmission, as well as the immunity conferred by vaccines and infection [1], it is unclear if these goals can be met by vaccine passports. Vaccine passports raise serious ethical concerns related to rights and autonomy [5]. It is also unclear if vaccine passports are simply performative and so cannot be technically enforced without identity authentication and the promotion of large-scale inequality in vaccination [7].

Assuming somehow that vaccine passports could be effective in determining transmissibility and immunity, one could try to approach the question from a purely technical perspective. Vaccine passports are digital credentials, and whether or not they can be made more or less privacy-preserving is a technical question, even if they should be opposed on social grounds. Therefore, it is necessary to outline precisely the goals of a vaccine passport and its security properties.

2.1.1 Goals. A **digital vaccine passport** should allow someone, the **holder**, to *prove* that they have been vaccinated (within whatever period of time a vaccine ends up lasting) to a third party, a **verifier**. Thus, the desired security and privacy properties of vaccine passports are:

- *Unforgeability*: An unvaccinated person should not be able to persuade a verifier that they have been vaccinated.
- *Privacy Protection*: The verifier should only be able to gain information relevant to vaccination status and not hold this information longer than necessary.

2.1.2 Threat Model. The threats facing the system in terms of unforgeability would be primarily from an *outsider adversary* trying to attest falsely to vaccination status. Note that attacks could also come from an *insider adversary*, such as corrupt vaccination sites producing fake vaccination certificates (perhaps even due to a non-malicious error) or if the key material used in the system is hacked. However, it should be noted that these kinds of attacks by corrupt insiders are common to any public key infrastructure and so will not be taken into consideration. The threat model does not try to take into account a third-party verifier that will simply accept any vaccine passport, e.g. using the entire technical apparatus as a placebo in order to encourage vaccination.

In terms of privacy, one threat could be that of a *local network adversary* that is watching the communication between a local vaccine passport verifier and whatever database it is accessing (possibly not at the same time as it accesses the vaccine passport). A more powerful *global network adversary*, such as an intelligence agency or nation-state, can watch all traffic in and out of every component in the network.

2.2 The (Lack of) Standards in Vaccine Passports

Despite these straightforward goals, there have been a large measure of differing vaccine passport systems deployed without common international interoperable standards. Which vaccine passport system should we inspect for privacy and security properties?

There are many closed-source vaccine passports approaches that do not offer any public documentation, such as CommonPass[4], Commons Project[5] As there are no publicly available technical documentation, these kinds of COVID-19 passes cannot be reasonably thought to be private (or secure) without putting blind trust in the software provider. Other alternative approaches like the NHS COVID-19 app have also been deployed.[6]

There is further fragmentation as a number of airlines have launched blockchain-based solutions of their own accord. The International Air Transport Association have announced IATA Travel Pass, which uses a number of W3C standards like W3C Decentralized Identifiers (DIDs),[7] although the application itself is not open-source. In general, blockchain-based solutions for vaccine passports have been heavily criticized as being insecure and not privacy-preserving, so there is not a clear need to further critique what has already been described as a fundamentally inappropriate design for a vaccine passport [3], although a number of academic papers continue to back such amateur designs for reasons that appear to be based in a monomaniacal desire to publish papers about blockchain technology rather than any pragmatic consideration of security and privacy for actual people [11].

Despite their rather obvious shortcomings, blockchain-based vaccine passports schemes have been sold to airlines in the Middle East by a blockchain startup called Evernym.[8] While most airlines are still using IATA Travel Pass in trial, some like Etihad Airlines claim to be deploying this vaccine passport. Other airlines have been engaged in trials of AOKpass, which is based on the Ethereum blockchain.[9] AOKPass claims to be working with ISO ISO/TC 215 "Health Informatics" which lists two non-public documents in a "preparatory" stage, namely *"Categorical Structure and Data Elements for the Identification and Exchange of Immunization Data"* and *"Interoperability of Public Health Emergency Preparedness and Response Information Systems — Business Rules, Terminology and Data Vocabulary."*[10] As these documents are not available for public

[3]The term 'immunity passport' was originally used frequently as it takes into account a supposed immunity given by infection, however, as time progresses the link between vaccination, immunity, and infection has become less clear [1]. Therefore, we will modestly avoid the term 'immunity.'

[4]CommonPass website: https://thecommonsproject.org/
[5]Open source code is often considered a kind of 'commons,' and closed source projects like the Commons Project are thus the inverse of a commons.
[6]https://github.com/nihp-public/covid19-app-system-public
[7]https://www.evernym.com/travelpass/
[8]https://www.evernym.com/travelpass/
[9]https://www.aokpass.com/en/faq/
[10]https://www.iso.org/committee/54960.html

review, it is rather unlikely they have put forward secure and private vaccine passports. Beyond various national governments and international bodies, various large private companies like Google, Microsoft, and even TicketMaster are also reportedly working on vaccine passports, as well as a host of smaller companies such as OnFido and Evernym. Regardless, the general critiques of blockchain-based vaccine passports have already been shown to be insecure and not preserve user-privacy [3].

With this wide variety of vaccine passport systems remaining unstandardized, it is unclear if vaccine passports can actually be used for international travel efficiently. The most mature and widely deployed vaccine passport system is the open source EU Digital COVID-19 Certificate.[11] A broadly similar digital system has been recommended by the World Health Organization (WHO), via the *"Technical Specifications and Implementation Guidance"* for *"Digital Documentation of COVID-19 Certificates:Vaccination Status"* (DCC:VS).[12] However, the lack of clear international standards has already caused issues: for example, US citizens traveling to the EU can have their rights limited as the US does not issue a digital vaccine passport. Chinese and Russian digital vaccine passports are not guaranteed acceptance from vaccine passports verifiers in the European Union (that decision is left to member states), while those from Israel are accepted. Non-digital CDC vaccine passports from the USA are only accepted in a haphazard manner by European states, and the conversion of a US vaccine passport to an EU digital vaccine one is still done manually. Outside of the EU, there appears to be no automated acceptance of different vaccine passport systems although it is possible a de-facto standard will emerge from the efforts of the EU, IATA and WHO. Therefore, the focus on this paper will be on the primary deployed vaccine passport system by the EU, the EU Digital COVID certificate.

3 EU DIGITAL COVID CERTIFICATE

The *EU Digital COVID Certificate (DCC)*[13] is an exemplary vaccine passport design with widespread usage throughout Europe, whose code is available online[14] and whose information flows have been well-documented.[15] An EU vaccine certificate must contain:

- Full name,
- Date of birth,
- Issuing state,
- Vaccine immunity status.

The 'vaccine immunity status' field includes the vaccine and manufacturer, number of doses administered, and date(s) of vaccination for vaccinated individuals. Other sub-fields may be optionally included if they are related to the above fields. Note that the DCC

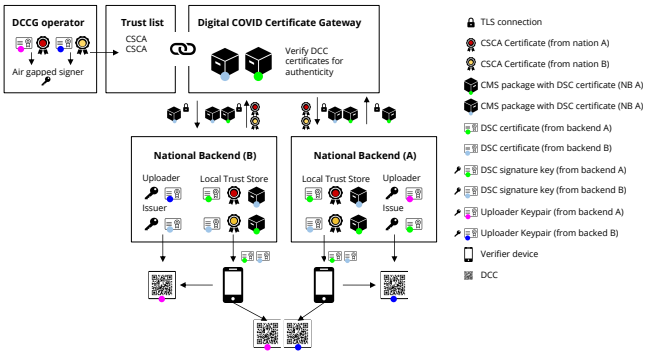

Figure 1: Flow with regards an 'Immunity Passport' (EU-DCC)

can also be used for immunity from recovery as well as verifying test results as the information is broadly similar for individuals that have just been tested (such as the name of the test and results being included) or for those who have been recovered (such as the date of issuance of result with a verification of the antibodies). Note that each vaccination is given an unique identifier, the *Digital COVID-19 Certificate Identifier (DCCI)*, when registered.

This certificate is stored using the IETF COSE standard,[16] which stores key-value pairs similar to the more well-known JOSE standard[17] in a binary format, with the binary format being given in the (unusual) base 45 format. Importantly, this data is all sent through a SHA256 hash function when issued, where the issuer sends the resulting hash to be cryptographically signed by the relevant national authority backend using the IETF CBOR Web Token standard that allows arbitrary COSE payloads to be cryptographically signed.[18] During this process, a uniquely identifying DCCI is given to the vaccination event and the signing authority issues a number called the *Transaction Authentication Number (TAN)* (with a recommended expiration time of two hours) that is returned with the signed EU-DCC. When the certificate is installed on the phone of a holder, the holder types in the TAN to bind it. From the perspective of the holder, the signature of their credential be displayed a QR code that can be verified by anyone with a EUDCC verifier application.

Controlled by the personnel who administer the vaccine, this signature that 'signs' the vaccine certificate is a *Digital Signing Certificate (DSC)*. These DSCs are authorized by a Country Signing Certificate Authority (CSCA) on a per nation-state level. The Europe-wide Digital COVID-19 Certificate Gateway (DCCG) is responsible for exchanging the public keys of DSCs between countries. The list of DSCs and signing key are signed by the are signed the CSCA and uploaded by the national server of national public health authority using the IETF CMS standard.[19] The DCCG signs and publishes all the CSCA keys. This distribution of keys is illustrated by Figure 1 per "Technical Specifications for Digital Green Certificates Volume 5."[20]

[11] https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en
[12] https://www.who.int/publications/i/item/WHO-2019-nCoV-Digital_certificates-vaccination-2021.1
[13] Previously called the "EU Digital Green Certificate" (DGC), not to be confused with another immunity passport scheme with the same name under development in Canada. Given that the technical documentation presented by the EU still uses the terms 'Digital Green' is still used for technical components such as the 'Digital Green Certificate Gateway,' we will continue using this terminology from the official EU documents created by the e-Health network, a group of EU health authorities in https://ec.europa.eu/health/ehealth/covid-19_en.
[14] https://github.com/eu-digital-green-certificates
[15] https://health.ec.europa.eu/ehealth-digital-health-and-care/ehealth-and-covid-19_en
[16] https://datatracker.ietf.org/wg/cose/documents/
[17] https://datatracker.ietf.org/wg/jose/documents/
[18] https://tools.ietf.org/id/draft-ietf-ace-cbor-web-token-15.html
[19] https://datatracker.ietf.org/doc/html/rfc5652
[20] https://ec.europa.eu/health/sites/default/files/ehealth/docs/digital-green-certificates_v5_en.pdf

The information flow is fairly simple. A verifier has a list of CSCA public keys that are signed by the DGCG. The user has a vaccination certificate that was given to them by an issuer, such as a doctor approved by the national public health authority that generates a signature from their DSC key. The traveling citizen (1) first displays their DSC signature to a verifier. Then the verifier (2) checks the signature against each of the CSCA public keys in their local trust store. If the verifier is online (3a), it checks the trust store of its national authority, which has also keys verified by the DGCG. For offline usage when the verifier is not connected to the internet (3b), it downloads the trust store of keys from its national authority. Finally, (4) if the vaccine passport is valid, the signature verifies, otherwise it fails.

3.1 Unforgeability

Are DCCs unforgeable? One trivial way to break unforgeability is for an unvaccinated person to simply copy the correctly signed vaccine credential of a vaccinated person and display the credential as their own. If the verifier does not check any other personal data, the vaccine passport would pass as the vaccination status derives from the signature on the credential. Thus, the unforgeability simply requires the use of an ID card by the holder, including some physically identifiable information such as a photo of their face, that must be manually checked to match the information in the vaccine credential by the verifier. In the case of someone using a vaccine passport that they borrowed or bought online from a hacked vaccine authority, although the credential would pass itself, the manual checks would prevent the misuse of a credential.

The vaccine passport's usage of a digital signature exists only to prevent adversaries from simply freely minting their own vaccine credentials, as the signatures on such fake vaccine credentials would not verify. As all cryptographic security derives from the signature for a DCC, in order to achieve unforgeability in the real-world context of a vaccine credential verification, there must be a check of ancillary personal data, such as an identity card. As such, unforgeability in vaccine passports is not a cryptographic property but a product of an authentication system that is still manual and relies on the efficacy and honesty of the verifier.

Could a DCC be bound to another person's identity *digitally* to prevent simple borrowing and copying of the vaccine credential, or reduce the dependency on manual authentication? This proves to be more difficult than it may first appear. There is a widespread, if erroneous, conception that people can be uniquely identified and bound to their mobile smartphones. Following this well-trodden path, the main way the DCC ties itself to an individual is to not allow the same vaccine event to be tied to more than one vaccine passport stored on a mobile phone is via two-factor authentication using a TAN that uniquely identifies a vaccine event by virtue of being generated when the vaccine is given. As the TAN then binds a DCC on a phone to a particular vaccine event, the TAN cannot be re-used. This would in theory make a single vaccine event and DCC not to be used by more than one person's app on a single phone. However, it should be noted that the approach of using a TAN to authenticate individuals for vaccine passports is not really secure if used in a traditional two-factor via SMS authentication or e-mail flow, which is rightfully being phased out by industry. An outsider adversary with local network adversary powers can obtain a TAN (since it is "sent to the holder via SMS or email".[21] If a TAN is not bound explicitly to a DCC (such as via the DCCI) upon generation, then an adversary could attempt to bind the TAN to their own DCC first, and thus register their own DCC to the vaccine event given by the DCCI and 'lock' the rightful holder out. This could be only prevented if the TAN was given via a secure encrypted channel or printed. Usability also makes these identification of a user with a mobile phone unrealistic, as users may lose devices and have multiple devices.

Lastly, the federated design of the EU DCC does not clearly offer any security benefits over a centralized design and offers only political advantages in terms of national sovereignty. As has been noticed earlier,[22] DSC keys are also signed unnecessarily by a client-signed TLS connection to the DCCG. The use of this TLS client authentication is to prevent the DCCG from being overwhelmed with certain kinds of probing or even denial-of-service attacks by a single client. All DSCs could be signed also by the DCCG rather than a national CSCA and remain cryptographically equivalent. Another reason for this lack of a single signer is that having DCCG sign all keys directly would result in an unnecessary amount of centralization that European nation-states may feel threatens their national sovereignty.

Ultimately, unforgeability appears impossible without some sort of universal (likely cryptographic) digital identity system that authenticates an individual *in the world outside the digital* and then binds them to a vaccination event. The closest that is done by the EU DCC is to problematically bind a DCC to a device via a TAN. However, this seems unnecessary and does not clearly offer advantages over simply using the vaccine passport in conjunction with a national ID card. However, some countries such as the US and the UK do not have national ID cards. Furthermore, the ID cards may themselves be faked or not checked carefully. The entire digital aspect of the DCC relies on a cryptographic infrastructure whose functionality is equivalent to manually checking an identity card, except for being harder to fake vaccine events.

3.2 Privacy Issues

Although we do not perform a full privacy impact assessment of the EU DCC system (as should be done by the EU Data Protection Supervisor), it should be clear that the cost of maintaining unforgeability is to lose privacy as unforgeability presupposes uniquely identifying the holder via disclosing personal data. The ideal vaccine passport would only disclose whether or not a person was sufficiently vaccinated without revealing any further personal information. However, personal data not strictly related to the vaccine event, such as the birth date and full name, is disclosed to the verifier in practice in order to maintain unforgeability. This data is displayed to verify the certificate and the verifier may copy any digital information in the certificate. Copying this personal data may or may not be relatively easy depending on if the credential with this identity data can also be read digitally and so copied.

[21] See the 2022 Version 1.5 'eHealth Network Guidelines on Technical Specifications for EU Digital COVID Certificates Volume 4'.
[22] https://educatedguesswork.org/posts/vaccine-passport-eu/

An insider adversary that can control a verifier can record this personal data and use it for possibly malicious purposes, such as selling certificates (all credentials are multi-show, as the private key on the user's device does not dynamically issue new unlinkable signatures per-usage). Furthermore, as the signature is only generated once and does not rely on any private key material on the user's device (which would be impossible for paper vaccine passports), the entire certificate with signature can be captured by a malicious verifier. The assumption of the current system is that the holder is untrusted while the verifier is trusted, but the DCC is often used for entrance to places such as movie theaters, where the movie theater staff may be not be trained in the finer points of data protection as verifiers. Given the amount of verifiers is expected to be very large and diverse, it is more likely that a verifier become corrupt than any other component of the system, including even the holders themselves. In this case, there is a trade-off between unforgeability and privacy, which is simply a trade-off between a person faking a vaccine passport or a verifier collecting large amounts of personal data.

Worse, the primary problem is that as each certificate is signed by a single key, each usage of any certificate is *linkable* to every other usage of the certificate as the signature is only made once. If the verifiers collaborate to share their copies of a user's DCC, they can easily trace usages of a user as each signature is unique. This is very hard to prevent unless the usage of the DCC is restricted, such as for usage only at international borders (as was originally intended by the EU), and even then the problem of linkability remains. For example, government agencies may collaborate and use the shows of a certificate to track some suspected individual.

While the threat of copying the personal data in a decentralized manner by corrupt verifiers would not affect all holders, at least the design of the DCC does not force all user personal data to be stored in a centralized database, as only the hash of the personal data is signed and stored with a DCCI in a centralized database. It should be remarked that the creation of DCCI seems only related to whether or not a TAN 'activated' a particular DCC, so if TANs were not used, the DCCI could be simply deleted and no centralized database required.

The very semi-centralized federated structure of the DCCG system is ripe for abuse and surveillance by network adversaries watching the centralized components. It is possible for a local network adversary to use traffic analysis on the communications between verifiers and the backend that stores the DSCs if verifiers check an individual user's DCC *online*. This traffic analysis however does not superficially reveal any other personal data than rather a check was done or not, but in conjunction with other data such as readily gathered geolocation data in shopping centers could reveal whether or not someone was vaccinated. [9]. In contrast to a local adversary, a global network adversary that watches a particular user or set of users would be much more dangerous. If verifiers such as restaurants or airports checks the vaccination status by dynamically retrieving any public DSC keys at the time of verification, a person could be tracked throughout their lifetime. To avoid this possible surveillance, all signature checks should happen *offline*. The verifier should be forced to download all the relevant DSC keys in batch on regular intervals. However, this would threaten the unforgeability requirement of vaccine passports, as changes to DSC keys (such as done when a key is compromised) or newly DCCs minted between intervals could not be tracked. Nonetheless, these could be considered edge-cases.

4 INTERVIEWS

In order understand the issues around privacy in context of the EU DCC, including the procurement and creation of various national DCC implementations, a number of interviews were done of experts and critics of vaccine passports. Interviewees were sent a GDPR Information Sheet and Consent Sheet before they were interviewed over a videoconferencing system or in person. They were given the chance to discuss the contents, have those contents verbally explained on the phone, and consent was given before publication. Each interview was composed of the same seven questions.

4.1 Interviewees

Interviewees included:

(1) **Prof. Bart Preneel (Academic, KU Leuven)**: Advisor to Belgium's COVID Safe Pass.
(2) **Javier Ruiz (Civil Society, Open Rights Group)**: Campaigner in the United Kingdom on digital privacy.
(3) **Amelia Andersdotter (Corporate, Sky UK)**: Head of standards and former European Parliament member specializing in digital affairs.
(4) **Dirk-Willem van Gulik (Public Sector, Netherlands)**: During the COVID crisis temporarily hired as the CTO of the Ministry of Public Health, Welfare and Sport of The Netherlands where he lead the design of CoronaCheck system, its international cooperation in general and the EC technical coordination/gateway for the EU DCC in particular and participated in related WHO, EU standardization/exchange and IETF processes[23].
(5) **Eric Rescorla (Corporate, Mozilla)**: CTO of Mozilla
(6) **Anonymous**: University Professor with expertise on Policing, Politics and Urban Space, under conditions of anonymity.
(7) **Dr. Seda Guerses (Academic, TU Delft)**. Privacy expert and critic of vaccine passports [7].

A synthesis of the interviews is presented below, with key quotes taken from each interview.

4.2 Do you see a demand for privacy with regards to COVID-19 vaccine passports and digital services in general?

There was a strong general consensus that privacy was viewed as desirable, but privacy in of itself was not enough. Javier Ruiz noted that *"I think that there is definitely a demand for COVID passports that do not go beyond what they are supposed to do. There is broad concern that COVID passports will become part of something permanent."* Dirk-Willem van Gulik noted that the risks are not in the passport itself as the Dutch passport already supports unlinkability and so privacy, but the main risk is in the *"whole eco-system we had to create."* For example, one risk was *"electronic patient records"*

[23] Outside of the scope of CoronaCheck and wider COVID-19 crisis, Dirk-Willem van Gulik is normally a private sector consultant that works with both public and private bodies.

that were done by organizations that have no prior experience with handling medical records, such as *"supermarket suppliers"* in the Netherlands that may inadvertently create leaks of records or be open to attacks, perhaps via *"people that may sell their access to medical files."* Therefore, privacy is a concern not just for vaccine passports but the entire eco-system and so digital services in general. Bart Preneel made the overarching point that these concerns go beyond privacy and are against the very existence of vaccine passports, as *"people are against these things due to social sorting rather than purely privacy concerns,"* such that *"it's more the purpose they don't like it."*

4.3 If so, who is driving this demand? (the general public, campaign organizations, etc.)

The demand for privacy was thought to come from the general public, insofar as there was demand for vaccine passports. Amelia Andersdotter noted that *"it is not clear to me the public wants COVID passports at all"* but that for those that do, *"there is a general demand for privacy COVID passports"* and that *"COVID passports are not the driving mechanism for the demand for privacy but the demand is definitely there."* The anonymous participant further emphasized that often well-intentioned engineers could be driving this demand due to their concerns on behalf of users, as done in the case for COVID contact-tracing [13], In general, the reaction from campaign organizations was mixed, with the left supporting COVID restrictions such as vaccine passports (even though they often lead to discrimination) and resistance to vaccine passports being linked more to the extreme right or conspiracy theorists.

4.4 To your mind, to what extent has privacy been a concern in the development of Digital COVID Certificates or other COVID-19 vaccine passports and apps?

In most countries privacy was a concern, but not one that was given priority in the development of the app. Bart Preneel noted that privacy *"was low priority"* given the urgency of the situation in most European countries. The anonymous lecturer even stated *"I believe privacy is the very last thing they had in mind."* One exception was the national-level vaccine passport, CoronaCheck, that was built in the Netherlands and focused on privacy in terms of their development, and so diverged from the EU DCC in order to provide stronger privacy protections. Looking back at the development of CoronaCheck, Dirk-Willem van Gulik said that the main risk is *"having to create this industry in too short a time"* means *"that getting privacy right and security right is difficult."* However, the Dutch COVID credential uses a modified version of Idemix anonymous credential technologies such as IRMA [4],[24] of which the Dutch COVID credential is a (fully off-line) variation. So the Dutch vaccine passport indeed took privacy seriously and delivered a privacy-enhanced COVID passport that leaves *"no trace on the device."* However, *"certificates for cross border travel, that follow the EUDCC standard, do not use this type of privacy preserving technology, and they contain both unique identifiers and details, such as the citizen's name."* This means that it *"is possible for a rogue agent to capture this data rather than use it just once. When this data would be combined, it leads to a risk of tracking."*

4.5 To your mind, what are the main privacy risks of COVID-19 vaccine passports? Are you worried about the current Digital COVID certificates in the EU?

Concern over the long-term privacy impacts of vaccine passports and the DCC was widespread among the experts interviewed. Amelia Andersdotter noted these systems were *"a quick hack"* by European governments. Concerns were spread between the data on the vaccine passport itself, its storage in databases, and the wider repercussions on autonomy. One risk, Dirk-Willem van Gulik continues, is that vaccine passports *"contains way more data than needed for its purpose"*[25] including *"a unique identifier that can be used for tracking"* as *"countries are naturally inclined to trust each other...so a lot of citizens have unique identifiers."* The anonymous professor stated that the main risks were that: *"sensitive health data centralizes in state-wide databases makes them a potential way for states to discriminate against their populations, prone to commercial exploitation via subcontracting; and vulnerable to malicious attacks of all kinds."* Seda Guerses said *"privacy is also about the protection of autonomy, in this case, the ability to make decisions and negotiate policy."* This wider issue gets lost *"when you reduce privacy to the information that is revealed by showing a certificate."* This leads to a fundamental critique of even an anonymous credential solution, as imagine *"that you have a super privacy preserving system that revealed only one bit, that said 'yes' or 'no' (with respect to vaccination policy), without revealing any further information, still assumes that you have put in place a technical infrastructure for policy delivery at scale. This system can be used to limit access to (physical) resources, like we use access control in digital systems to access information resources. Most people, when they analyze privacy, they look to minimize the data on the certificate. But they don't analyze the potential problems or consequences of a large scale system that can enforce (access control) policy on physical and digital resources."* Such a system is very powerful and can easily breach privacy as autonomy.

4.6 Do these debates, concerns and critiques relate to the future of digital services (public and commercial) more generally?

In general, there was consensus that this issue of privacy was larger than vaccine passports and permeated all aspects of digital services in both the private and public sphere. Javier Ruiz said that *"most people don't understand the role of providing services such as Yoti. Yoti is a private company, builds an app, they also provide full identity checks."* Dirk-Willem van Gulik simply said that digital services that do not respect privacy should *"not be built as they are against the law."* Note that European privacy regulations such as the General Data

[24] More information on IRMA available at: http://www.cs.ru.nl/B.Jacobs/TALKS/math-irma-6up.pdf

[25] I.e. to assert that the bearer of this (digital) document meets the required medical bar set and that it is sufficiently tied to the bearer in that context (e.g. a border crossing).

Protection Regulation (GDPR) also applies to private companies. In this regard, the battle for privacy in terms of vaccine passports, and the out-sourcing of health data, can be considered just one battle in a larger campaign for the future of these digital services.

4.7 Has GDPR had any influence?

The influence of the GDPR was viewed as mixed. Amelia Andersdotter thought the GDPR had *"no influence"* as it was *"introduced as an emergency measure"* so the *"very mechanism of the GDPR can only have a limited impact on these systems."* In contrast, Bart Preneel said that the GDPR had influence in Belgium's design. The same is true in the UK, although Javier Ruiz noted that while *"at the moment the UK has its adapted version of the GDPR, but anywhere where there was the EU there is now the Ministers,"* that the Ministers are less accountable than EU institutions. Meanwhile, the lecturer noted *"At our time of need, the GDPR was simply ignored."* Dirk-Willem van Gulik said the *"GDPR was helpful, although it's pretty low-level, it at least sets out some basic rules like the technology must be necessary and proportional."*

4.8 What have the procurement processes looked like for these apps? (if you don't know, who should we ask?)

There was general unhappiness with the procurement process in terms of concern for privacy. Dirk-Willem van Gulik noted that we *"asked industry to deliver something like this"*[26] but although seven companies like Accenture and Capgemini got to pitch their idea, but *"the results weren't pretty"* so it became *"clear to society that these big companies that pitched did not have the same interest as society."* In the UK, where the production of vaccine passports was outsourced, Javier Ruiz stated that *"there has been concern about the opacity of the contracts, a huge level of corruption, and privacy has been another concern, how long is data kept, how is it shared"* and even concern as *"Palantir has been involved"* and *"this related to ICT, contact tracing, and data analytics more broadly, not just the COVID passport as such."*

4.9 What should the main criteria be for the procurement processes?

Privacy should have played a much larger role in the procurement process, although the fundamental contradiction of privacy and vaccine passports could mean such procurement never should have happened. In the case of private companies applying to build the Dutch national vaccine passport, Dirk-Willem van Gulik said that privacy experts *"tore them to shreds"* so the public sector had to build the technology itself, as *"all this core technology...there is no viable industry for that, so it was all built directly by the Ministry of Public Health."* Seda Guerses issued similar concerns, noting that *"they should have never built... there is no way you can create and execute such a policy environment and call yourself a democracy,"* although she hopes there is a there is the possibility for a more *"democratic procurement process."* An anonymous lecturer concurred *"They shouldn't be given these contracts in the first place."*

[26] https://www.government.nl/latest/news/2020/04/15/health-ministry-to-hold-digital-event-to-test-coronavirus-apps

4.10 Is privacy something the public sector is willing to pay extra for?

Privacy should be a requirement, rather than a boutique and optional feature. Dirk-Willem van Gulik noted *"If there's no privacy the law says you can't build it"* so *"it has to have privacy."* There are economic advantages to privacy as well, as *"having a proper privacy-enhancing system means the overall building costs were probably lower than a centralized system as there was no personal data there which would have led to making release more complex and slower with more security audits."*

Seda Guerses notes that millions have already been paid in Europe to train experts in privacy and identity management, but *"none of these experts were consulted"*. Seda Guerses noted that *"the right to access physical resources is fundamental to human autonomy"* and expressed concern over a powerful digital access control system to enforce policy and regulate such access.

4.11 How has your experience been with using COVID-19 vaccine passports across borders? Do you think new standards should be developed internationally?

Seda Guerses noted that *"right to enter a physical space is fundamental"* and expressed concern over access control being used in such a system. Bart Preneel also expressed the fact that the issue was also one of government coordination, *"The problem is you have to implement a different proof per country, as they can't agree on the rules."* As a standard expert at the Internet Engineering Task Force (IETF), Eric Rescorla noted that *"this is pretty straightforward technically"* so *"it should probably be an IETF WG rather than in the CFRG. With that said, while I think standardization would be valuable, [it seems to me] that the problem here is a bunch of independent standards proceeding, so I'd want to see some evidence that the various players (EU, VCI, etc.) were interested before starting off."* Dirk Willem van Gulik also positively responded, saying that *"with the worst of the crisis over - this is a good time. Also as it is very likely that this is the time for changes."* This provokes the question: Is it better to attempt to engineer privacy into vaccine passports, or not build them to begin with?

5 CONCLUSION

Of existing vaccine passport deployments, the EU Digital COVID certificate is more privacy-preserving than blockchain-based vaccine passport solutions [3]. Various minor improvements could be made, by minimizing identifiers such as the DCCI and abandoning the use of TANs. However, the primary threat to privacy is that the usages of each certificate are linkable and require the physical authentication of each individual via the disclosure of personal information. Without revealing personal data to the verifier, it is impossible to maintain unforgeability. The requirements of unforgeability and privacy protection are inherently contradictory.

The threat model of vaccine passports assumes untrusted holders and trusted verifiers and issuers, as well as a trusted backend to verify the information. Given the scope of potential abuse of these systems, this does not seem to be the right threat model. After all, it is impossible to prevent replay attacks of vaccine passport

information (where the verifier caches the information and then re-uses it). It seems that abandoning unforgeability, which assumes the holder will want to use a forged vaccine passport, and instead focusing on minimizing the information of verifiers can link is one possibility. For example, the Dutch CoronaCheck system[27] only contains the initial of the first and last name, rather than the full name, and it does not contain the birth year. Furthermore, it displays being negatively tested, vaccinated, or recovered from COVID-19 as equivalent. In order to prevent widespread abuse by state actors, another threat model may trust holders and sacrifice unforgeability and reduce the trust and data collection by verifiers and backend systems. However, if the loss of unforgeability is taken to its logical conclusion, the very concept of vaccine passports could also just be thrown out.

Anonymous credentials (also called 'attribute-based credentials') allows someone to prove statements about themselves without revealing any more personal data than is needed for the proof and the digital representation of the proof is unlinkable between usages [2]. The only usage of these in real-world immunity passports was in the CoronaCheck vaccine passport in the Netherlands. In essence, the QR code and so signature would change with every usage and so be unlinkable, but still be verifiable. Historically this has been done with blind signatures and group signatures, so that the holder can prove that the original certificate (such as an vaccine passport) is genuine but the issuer cannot link its signature to the certificate of the holder given to any given verifier. This can even be done with a set of decentralized validators in a multi-show anonymous credential schemes like Coconut [12], preserving via zero-knowledge proofs the privacy of personal data without putting it on the blockchain or a large centralized data-base.

Yet anonymous credentials do not reconcile the contradiction between unforgeability and privacy. While selective disclosure defends privacy better than simple signed certificates, unforgeability would still require the use of a physical identity card or other more all-encompassing digital identity system. Still, vaccine passports that try to maintain privacy could do much better to prevent the collection of personal and sensitive information from adversaries that watch network flows of data. On the level of network attackers, it would make more sense to build them with better resistance to traffic analysis attacks on the network level, so that the IP address of users and even patterns of access would be hidden using technology like onion-routing and mixnets with dummy traffic, but no vaccine passport uses such network technology. Note that any cryptographic solution, including more complex use of zero-knowledge proofs, would still effectively have to be connected to some part of a verifiable physical identity, leading to dystopian solutions such as WorldCoin that use zero-knowledge proofs of retinal scans.[28]

In conclusion, vaccine passports do present a threat model that inherently trusts governments and verifiers at the expense of the privacy of the population. While the onset of COVID-19 made vaccine passports seem necessary due to a generalized state of exception, given that at the current moment COVID-19 has become widespread, attempts to create a permanent 'health pass' in the UK and Germany from immunity passports should be stopped until further analysis is done on the privacy of these vaccine passports. Ultimately, what vaccine passports require to be unforgeable is a universal identity system capable of authenticating all members of the population. Such an identity system itself poses tremendous threats to privacy, and the precedent set by vaccine passports is the normalization of restricting rights based on identity. Even if our own governments are trustworthy today, there is no guarantee they will be trustworthy guarantors of rights in the future. Identity systems deployed to enforce supposedly temporary restrictions of rights tend to become permanent, and then can easily be instrumentalized to control populations and eliminate dissent. Privacy and fundamental rights should not be sacrificed in the name of public health, as even the most well-intentioned identity system will inevitably endanger the public more than the threat the infrastructure is built to contain.

Acknowledgements: The author has received funding from the European Union's Horizon 2020 Framework Programme for Research and Innovation under grant agreement no. 951972 and grant agreement no. 825268. In addition to the various volunteers for interviews, the author would like to thank Nadim Kobeissi for feedback and Jaya Brekke for helping with interviews.

REFERENCES

[1] Heba N Altarawneh, Hiam Chemaitelly, Houssein H Ayoub, Patrick Tang, Mohammad R Hasan, Hadi M Yassine, Hebah A Al-Khatib, Maria K Smatti, Peter Coyle, Zaina Al-Kanaani, et al. 2022. Effects of Previous Infection and Vaccination on Symptomatic Omicron Infections. *New England Journal of Medicine* 387 (2022), 21–34.

[2] Stefan Brands. 2000. *Rethinking public key infrastructures and digital certificates: Building in privacy.* MIT Press, Cambridge, USA.

[3] Harry Halpin. 2020. Vision: A Critique of Immunity Passports and W3C Decentralized Identifiers. In *Security Standardisation Research*. Springer International Publishing, Berlin, 148–168.

[4] Brinda Hampiholi, Gergely Alpár, Fabian van den Broek, and Bart Jacobs. 2015. Towards practical attribute-based signatures. In *International Conference on Security, Privacy, and Applied Cryptography Engineering*. Springer, Berlin, 310–328.

[5] Daniel Jacob Hemel and Anup Malani. 2020. *Immunity Passports and Moral Hazard.* Technical Report. University of Chicago Coase-Sandor Institute for Law and Economics Research Paper No. 905. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3596569

[6] M Laeeq Khan, A Malik, U Ruhi, and A Al-Busaidi. 2022. Conflicting attitudes: Analyzing social media data to understand the early discourse on COVID-19 passports. *Technology in Society* 68 (2022), 101830.

[7] Stefania Milan, Michael Veale, Linnet Taylor, and Seda Gürses. 2021. Promises made to be broken: Performance and performativity in digital vaccine and immunity certification. *European Journal of Risk Regulation* 12, 2 (2021), 382–392.

[8] Seema Mohapatra. 2020. Passports of privilege. *American University Law Review* 70 (2020), 1729–1763.

[9] Vincent Nguyen. 2018. Shopping for privacy: How technology in brick-and-mortar retail stores poses privacy risks for shoppers. *Fordham Intell. Prop. Media & Ent. LJ* 29 (2018), 535.

[10] Evelyn Paris. 2021. Applying the proportionality principle to COVID-19 certificates. *European Journal of Risk Regulation* 12, 2 (2021), 287–297.

[11] Het Shah, Manasi Shah, Sudeep Tanwar, and Neeraj Kumar. 2021. Blockchain for COVID-19: a comprehensive review. *Personal and Ubiquitous Computing* 8 (2021), 1–28.

[12] Alberto Sonnino, Mustafa Al-Bassam, Shehar Bano, and Sarah Meiklejohn George Danezis. 2019. Coconut: Threshold Issuance Selective Disclosure Credentials with Applications to Distributed Ledgers. In *Proceedings of the Network and Distributed System Security Symposium - NDSS'19*. Internet Society, San Diego. https://www.ndss-symposium.org/ndss-paper/coconut-threshold-issuance-selective-disclosure-credentials-with-applications-to-distributed-ledgers/

[13] Carmela Troncoso, Mathias Payer, Jean-Pierre Hubaux, Marcel Salathé, James Larus, Edouard Bugnion, Wouter Lueks, Theresa Stadler, Apostolos Pyrgelis, Daniele Antonioli, et al. 2020. Decentralized privacy-preserving proximity tracing. (2020).

[27] https://coronacheck.nl/

[28] https://worldcoin.org/