SecureABC: Secure AntiBody Certificates for COVID-19

Chris Hicks*, David Butler*, Carsten Maple and Jon Crowcroft, *Fellow*, *IEEE*

***Abstract*—COVID-19 has resulted in unprecedented social distancing policies being enforced worldwide. As governments seek to restore their economies, open workplaces and permit travel there is a demand for technologies that may alleviate the requirement for social distancing whilst also protecting healthcare services and maintaining human and civil rights. In this work we explore the controversial technique of so-called immunity passports and present SecureABC: a decentralised, privacy-preserving system for issuing and verifying antibody certificates. We consider the implications of immunity passport systems, develop a set of general principles and security requirements for their deployment and show that these may be satisfied in practice.**

***Index Terms*—Authentication, Computer security, Ethical aspects, Privacy, Technology social factors**

I. Introduction

GOVERNMENTS worldwide are currently dealing with the Coronavirus pandemic, an outbreak of the SARS-CoV-2 virus which has already resulted in hundreds of thousands of deaths [1] and has caused unprecedented social changes for billions of people worldwide. Most countries have responded to the pandemic with policies aimed at enforcing social distancing, a technique certain to suppress the transmission of the virus when it is applied uniformly to the whole population [2]. Whilst effective, social distancing measures come at a significant social and economic cost and may not be a feasible long-term policy option in many countries. In addition, it has been noted that the approach may have a disproportionate impact on disadvantaged groups in society [3]. As the effective reproduction rate (R_t) is reduced below 1.0, and the number of COVID-19 cases falls, there are clear benefits to governments seeking technologies that may alleviate the requirement for population-wide social distancing whilst also protecting healthcare services and maintaining human and civil rights. In particular, measures such as intensive testing, contact tracing and selective isolation have been proposed [4].

A promising, but controversial [5], technique for relaxing the need for population wide social distancing is the use of so-called "immunity passports'" or "risk-free certificates'". The general idea is that a test for antibodies to SARS-CoV-2, the virus that causes COVID-19, could serve as the basis for a passport document that frees an individual from the most restrictive social distancing regulations. Assuming that strong correlates of protection to SARS-CoV-2 can be identified, immunity passports could provide a key technology in enabling the transition away from total lockdown. Chile and Estonia have already announced plans to issue and trial such passports, respectively, and policy makers in the USA, UK, Italy and Germany are also considering the approach [6][7]. In light of the interest already shown by several governments, and the emergence of a number of commercial solutions, an academic consideration of immunity passports is called for. In particular it is important that we have a framework for evaluating such systems and understanding the nuanced and complex socio-technical issues that arise. Not only will this facilitate greater understanding and societal confidence in such systems, but it is vital to constructive public debate that a single framework to compare and contrast different solutions is established.

We note that immunity passports are a highly controversial technology that have received attention from many influential organisations including the World Health Organisation (WHO) [8]. We do not claim to advocate for the use of immunity passports as this is a complex policy decision that should only be considered, on a case-by-case basis, after involving all of the relevant stakeholders and experts. We do however think that it is important to provide a detailed technical solution to the problem that can be used to inform any such policy. We complement our reference system with a presentation of four general deployment principles which aim to mitigate many of the concerns surrounding immunity passports.

A. Our Contributions

1. We provide a framework of general principles and a set of security and privacy requirements for immunity passport systems. Our general principles aim to alleviate some of the major concerns relating to such systems, and our requirements provide the basis for ensuring such systems have the correct properties and can be evaluated on common terms.
2. We present SecureABC (Secure AntiBody Certificate

This Manuscript was first received 17 June 2020. This work was supported by The Alan Turing Institute under the EPSRC grant EP/N510129/1.

C. Hicks and D.Butler are with The Alan Turing Institute, London NW1 2DB (email: {chicks,dbutler}@turing.ac.uk). C. Maple is with University of Warwick, Coventry, CV4 7AL (email: cm@warwick.ac.uk). J. Crowcroft is with University of Cambridge, Cambridge, CB3 0FD (email: jon.crowcroft@cl.cam.ac.uk).

scheme), a decentralised and privacy-preserving solution for antibody certificates. We evaluate SecureABC with respect to both our general principles and our security and privacy requirements.

3. We provide evidence that SecureABC is efficient and practical with our proof of concept implementation which includes an Android application for verifying SecureABC QR codes.

B. Outline

First in Section II we review the concerns surrounding immunity passports and derive four general principles that may minimise the risk posed by these systems. Next, in Section III we define our protocol model and introduce the required cryptographic primitives. Section IV presents the full details of our SecureABC system. Then, in Section V, we define our desired security properties for immunity passports and evaluate SecureABC with respect to them. Section VI shows the results of our implementation. Finally, we review related work and other solutions in Section VII before concluding in Section VIII.

II. General Principles for Immunity Passports

In this section we build towards a set of general principles for deploying an immunity passport system. We first provide a general use case for immunity passports to aid and direct our discussion before citing the major concerns that have been raised.

Our motivation for providing this section is to address concerns that immunity passport systems may prove to be counterproductive and could have a net negative impact on society. Evidence is mounting that many nations [6][7] are at least considering immunity passport solutions, so it is important that techniques for minimising the risks posed by such systems are developed. To aid and direct our discussion we begin with a general use case in which citizens wishing to travel on public transport are required to present a certificate affirming that they have some level of protective immunity to the SARS-CoV-2 virus.

Use case 1: basic use case. A healthcare provider will test citizens for antibodies to COVID-19. If antibodies are found, then an immunity passport will be issued. The citizen will now present their passport to the transport service provider who, after establishing the authenticity of the certificate, will allow access to transportation.

A. Immunity Passport Concerns

Immunity passports have attracted significant criticism. We have considered Kofler et al. [5] and the report from the WHO [8] and condensed the main concerns as follows:

1. **Alterations to scientific advice.** As a novel disease, COVID-19 is not yet well understood by the scientific community [9]. For example, the WHO's main concern is that the presence of antibodies is not an accurate indicator of immunity and state that such tests "need further validation to determine their accuracy and reliability" [8].
2. **Discrimination.** Immunity passports will create an attribute for discrimination [7] by establishing a clear distinction between those with immunity and those without. A report by the Ada Lovelace Institute emphasises that "Discrimination and stigmatisation may become commonplace if immunity becomes an element of identity" [12]. This inequality would be exaggerated if tests are not universally and freely available to all – immunity passports, and the associated freedoms, could become a luxury of the rich.
3. **May negatively impact behavior.** An immunity passport could become synonymous with freedom as those in possession could be allowed access to "the post-lockdown world" while those without could remain subject to social distancing policies. This may create a strong incentive for people to attempt to obtain a passport by any means. Coupled with the belief that having, and surviving, the virus corresponds to gaining immunity [10][11], it is hypothesised that immunity passports may actively encourage people to try to become infected. It has also been suggested that believing one has immunity could lead people to behave less cautiously [12].
4. **Feature creep.** In response to COVID-19, Governments are currently exercising a heightened level of control and surveillance over their populations [13][14]. Passporting systems could provide authorities with an opportunity to implement technologies, and to collect data, that could have long-term negative consequences on society [12].

These concerns are persuasive in advocating against immunity passports in the basic use case setting we have described. We are therefore motivated to address these concerns with a set of general principles which aim to mitigate, where possible, the risks associated with immunity passports.

B. General Principles for Immunity Passports

1. Rename, educate and allow revocation. Until there is strong evidence of protective immunity (and its correlates) to COVID-19, the word "immunity" should not be used. This is misleading at best and dangerously inaccurate at worst – creating a false sense of security. We opt for "antibody certificate" as it reflects the function more accurately. We note that in [41] Persad and Emanuel also advocate for a name other than "immunity passports", although we would argue that their "immunity-license" does not quite meet our criteria as it is still somewhat misleading. Moreover, appropriate levels of public education with regard the benefits and limitations of such systems is vital. Indeed, the Information Commissioners Office (ICO) strongly advocate being transparent about the purpose and benefit of the closely related contact tracing technology [15]. Finally, we call for systems which support efficient and fast revocation of certificates and service providers. This is essential to maintain pace with the fast-changing scientific understanding and dynamic policies which relate to COVID-19.

2. **Access to testing and technology.** Wealth, location and demographic profile must not impact access to obtaining or using a certificate. In other words, beyond their specified purpose, antibody certificates must avoid any additional discrimination. The Ada Lovelace Institute report [12] calls for "measures for ensuring vulnerable groups are not excluded from the operation of the system" in relation to immunity passports and in the case of contact tracing, the ICO state that "special consideration for different societal groups" is paramount.
3. **Proportional and necessary use.** As an inherently discriminatory technology we recognise that antibody certificates must be used cautiously. The Lovelace report [12] recommends the development of a strategy for "how immunity certification will be integrated into policy … pertaining to travel, movement, work and schooling". We advocate that such a strategy should ensure, where possible, that any restrictions imposed by antibody certification upon freedom of movement or access to services are both necessary and proportional to the specific risks and harms of COVID-19 transmission in each particular use-case. We note that in their draft Bill [44] Edwards et al. emphasise that proportionality is the key to reducing discrimination. To ensure that verifiers behave according to agreed guidelines on proportionate and necessary use of antibody certificates, we suggest that a user should be able to ascertain that the verifier is authorised before presenting their certificate. Such "mutual authorisation" will provide a higher degree of confidence to users.
4. **Maintain user ownership of data.** An antibody certificate system should be designed in such a way that users can, at all times, control the use of their data. In particular, users must control when and where to use their data to demonstrate their test result. This is supported by the ICO's principle of "giving users control" [15] with regard to contact tracing.

These principles, in particular minimising the restrictions imposed by antibody certification upon freedom of movement or access to services, seemingly diminish the functionality of any system that is in accordance with them. To alleviate this concern, we present two additional use cases that are in accordance with these principles but may still benefit society.

Use case 2: indicating user risk. Consider the basic use case where users of a public transport system are required to show their antibody certificate before making a journey. Under our general principles we advocate that certificates are still checked; however, access is granted to all. In this scenario, antibody certificates can still provide a benefit by allowing testing, cleaning and other mitigatory techniques to be optimised based on the relative use of each service by untested and tested-negative citizens. In [16] this idea is developed further, and technically enforced, by using differential privacy to randomise each user's antibody certificate status whilst still allowing for aggregate statistics to be estimated.

Use case 3: helping vulnerable members of society. When providing food delivery services for elderly people who cannot safely leave their home, preferring the carrier to hold an antibody certificate could reduce the risk faced by the recipient. This scenario, in which the carrier would hold an antibody certificate and her employer verify that it is valid, could represent a reasonable trade-off between restricting access to work and minimising the risk faced by vulnerable groups.

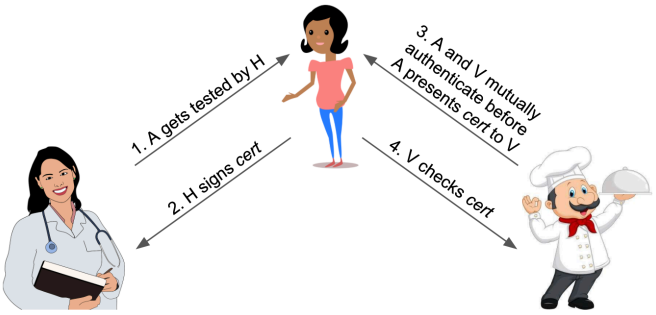

Fig. 1. Our generic model of an antibody certificate scheme run between a healthcare provider, a user and a service provider.

III. Model and Preliminaries

Our antibody certificate scheme model comprises three parties. We denote the Healthcare provider as Harry (H), the citizen or user of the scheme as Alice (A) and the service provider, who Verifies user certificates, as Verity (V). Our general protocol model is outlined in Figure 1: in step (1) A gets tested for antibodies by H. In step (2), if the test detects an appropriate number of antibodies, H signs an antibody certificate which is sent to A. In step (3), after mutually authenticating, A presents her certificate to V and then finally, in step (4), V checks the authenticity (i.e. that is was created by H) and attributes of the certificate (e.g. by matching a photo and name to A). Our system model assumes a root of trust in the system, for example the government, that implicitly authorises both H and V as legitimate entities. A root of trust is needed because a verifier V cannot reasonably be expected to know a priori all of the healthcare providers H that can be trusted to authorise antibody certificates. Similarly, the user A cannot be expected to always know which particular Vs can be trusted to verify their antibody certificates. Moreover, mutual authentication alleviates the "bully on the bus" problem, we discuss this further in the peer indistinguishability property we define in Section V.

A. Preliminaries

SecureABC requires both a secure public key signature scheme and a secure public key encryption scheme. Both of these schemes are made up of three algorithms. The first algorithm generates a public key pair, the second either signs or encrypts and the third verifies the signature or decrypts the ciphertext, respectively. We denote the signature scheme by the tuple: $(key\text{-}gen_{sign},\ sign,\ verify)$ and the encryption scheme by the tuple $(key\text{-}gen_{enc},\ enc,\ dec)$.

We use a signature scheme to allow the healthcare provider to sign antibody certificates and therefore, intuitively, we require the signature scheme to be unforgeable. Specifically, we require

it to be EUF-CMA (Existential Unforgeability under Chosen Message Attack) secure. Rather than define this standard property here, we refer the reader to Goldwasser et al. [17] for the common definition. We note that the standard Elliptic Curve Digital Signature Algorithm (ECDSA) [18] is sufficient for our needs.

We use the encryption scheme in the authentication phase for app-based users. Here the user encrypts their signed certificate such that only an authorized, non-revoked service provider can decrypt it (we discuss this property in more detail when evaluating our scheme in Section V). Our particular use of an encryption scheme means that any public key encryption scheme that is at least IND-CPA secure will suffice. For a standard definition of IND-CPA we refer the reader to Katz and Lindell [19].

IV. SecureABC

In this section we present SecureABC, our secure antibody certificate scheme that realises the model defined in Section III. SecureABC is a distributed, privacy-preserving antibody certificate protocol that allows for both paper-based and app-based user credentials. Providing printable, paper-based credentials is important because even in the most developed countries, the adoption of smartphones is not absolute. Indeed, requiring the use of electronic devices may exclude vulnerable user groups [3] and limit the reach of any deployment. We seek to provide strong privacy guarantees regardless of whether a user has a device capable of displaying a digital passport or not. In particular we seek to replicate the privacy of traditional identity documents, such as driver's licenses, which do not notify the issuer each time they are presented.

As noted in Section III our model assumes a common trust anchor, such as the government, that authorises both H and V as legitimate entities. In practice this means that every time H or V generate a new public key, the government signs it to indicate that it can be trusted. For brevity we implicitly assume this to be the case for all relevant keys.

High level overview of SecureABC. The SecureABC protocol comprises three phases: Setup, Issue and Authentication. The Setup protocol is run by H, who generates the public key pair for the signature scheme he will use to sign antibody certificates. Next, the Issue phase is run between H and A. At the end of the Issue phase A receives an antibody certificate, signed by H, which she can use to demonstrate her antibody status to service providers. Finally, the Authentication phase is run between A and V. This phase allows V to convince A that she is an authorised service provider and allows A to convince V that she has a valid antibody certificate. We provide two Authentication phase sub-protocols which allow A to choose between using either a paper-based or an app-based credential.

The Setup, Issue and Authentication phases of the SecureABC protocol are as follows.

Setup. Harry initialises the set of revoked CID numbers $rev = \{\}$, the set of revoked verifier public keys $rev_V = \{\}$ and generates the public and private key for the signature scheme:

$$(pk_H, sk_H) \leftarrow key\text{-}gen_{sign}(\cdot)$$

Issue. Harry interacts with Alice to issue a signed antibody certificate.

1. Alice is tested for antibodies by Harry, who records the test identity number (TID) that produced the test result. If the test is positive for antibodies, and Alice has not already been issued a certificate, then Harry generates a random Certificate ID (CID), initialises a corresponding revocation bit $b_{\text{CID}} = \texttt{False}$ and specifies a validity period $date_{\text{CID}}$. Harry stores (CID, TID, b_{CID}, $date_{\text{CID}}$) and informs Alice of her test result.
2. Alice provides Harry with a photograph, $photo_A$, and a communication channel, $comm_A$, which will be used to send passport status updates (e.g. upon revocation or test recall). In practice, Alice will choose one of a small number of communication options such as SMS, email or post.
3. Harry appends $comm_A$ to the record he holds for Alice and then sends her the signed antibody certificate $cert_A$ which is computed as follows:

$$cert_A = sign_{pk_H}(name_A, photo_A, date_{\text{CID}}, \text{CID})$$

Certificates can either be paper-based or app-based, in Section VI we show how QR codes can be used to encode such certificates. In the remainder of this paper we assume this encoding.

In the interests of mitigating economic discrimination, we recommend that if a user is unable, or unwilling, to provide a photograph then they are able to obtain one of the required standard for free during the issue phase. One option could be to create a mobile app that can be used by Harry to take such photographs on behalf of each user, it is important however that any such image is deleted by H as soon as the certificate has been issued. All of this could be handled automatically by a suitable audited application.

Authentication. Alice interacts with Verity to demonstrate the authenticity and ownership of her antibody certificate. Authentication must be mutual, that is first Alice must be convinced that Verity is authorised by the government before allowing her to verify her certificate. As certificates are either paper-based or app-based we require two different authentication sub-protocols which correspond to the manual and automated authentication of Verity by Alice, respectively. In both authentication sub-protocols, Verity runs an app which she uses to scan and verify Alice's credential. The app also periodically downloads the list of revoked CID numbers rev and Harry's public key pk_H. The rev list should be signed by Harry to demonstrate its authenticity.

Paper-Based Authentication. Alice has $cert_A$ and Verity has the list of revoked CID numbers rev and the Harry's public key pk_H.

1. Alice must manually convince herself that Verity is a government-authorised service provider, for example

based on context or viewing an identity document. If this step fails Alice aborts the protocol.
2. Alice shows her certificate $cert_A$ to Verity.
3. Verity verifies $cert_A$. That is she confirms $verify_{pk_H}(cert_A) = 1$, and learns $name_A$, $photo_A$, $date_{\text{CID}}$ and CID. She checks that CID has not been revoked i.e. $CID \notin rev$, then compares $photo_A$ to Alice and ensures that $date_{\text{CID}}$ has not elapsed. Optionally, if she deems it necessary for verification, Verity may ask to see a second document bearing $name_A$ --- this process would happen offline[1].

App-Based Authentication. Alice runs an app that stores her antibody certificate $cert_A$ and which periodically downloads a list of revoked verifier public keys, rev_V, from the government. Verity has a list of revoked CID numbers, Harry's public key pk_H and also an encryption public key pair $(pk_V, sk_V) \leftarrow key\text{-}gen_{enc}(\cdot)$.

1. Verity sends pk_V to Alice. In practice, Alice uses the app to scan a QR code or read an NFC tag provided by Verity. Alice verifies pk_V is an authorised public key and is not on the revocation list, i.e. $pk_V \notin rev_V$. If either of these steps fail, then Alice aborts the protocol.
2. Alice computes $cert'_A = enc_{pk_V}(cert_A)$ which is converted to a QR code and scanned by Verity.
3. Verity decrypts Alice's certificate $cert_A = dec_{sk_V}(cert'_A)$ and then proceeds as in Step 3 of the paper-based authentication protocol.

If either the paper-based or app-based authentication protocol succeeds then Verity accepts Alice's antibody certificate, otherwise she does not. It is important to note that the use of encryption in our app-based authentication protocol is an opportunistic enhancement which provides slightly improved security properties for app-users. More details on this point are provided in our evaluation which follows. While not strictly part of the protocol we next detail how revocation would be achieved.

Revocation. Harry periodically computes, signs and distributes rev (e.g. daily) such that it comprises all CID numbers in his private store that have the revocation bit $b_{\text{CID}} = \texttt{True}$. We claim this is sufficient for efficient revocation of certificates and illustrate the exact procedures for different use cases in our evaluation in the next section.

V. Security Properties and Evaluation

First, in this section, we present a theoretical metric with which to evaluate the main technical security properties we require of any antibody certificate protocol. We then evaluate SecureABC with respect to this metric and the general principles we set out in Section II.

A. Desired Security Properties

In this work we do not pursue a rigorous, formal definition for every security property but rather we intend to provide a basic set of terms for evaluating antibody certificate systems. It is unlikely that any scheme can simultaneously satisfy all of these properties as several of them present a trade-off. For example, there is an inherent compromise between the anonymity of user certificates and the binding between the user and their certificate. We provide additional intuition for some properties to help guide the reader.

Forge and Tamper Proof.
We say the system is forge proof if a user cannot create a valid certificate alone. That is valid certificates can only be created by H. Similarly, we say the system is tamper proof if the value of the attributes associated with a certificate cannot be altered by the user after the certificate has been issued.

Binding.
We require that the only certificate a user can successfully use is the one that is assigned to them and which has not been revoked.

Uniqueness.
Uniqueness is satisfied if a user can have at most one valid certificate associated to them at any one time. -- We note, this property is important when binding is imperfect, for example when considering twins who may share a similar photograph but that may not share the same antibody test result.

Peer-Indistinguishability.
We define a peer as an unauthorised service provider (for example, a malicious citizen). We require that a peer cannot learn any information about the user from viewing the certificate. – Intuitively, Peer-Indistinguishability ensures that a user cannot be pressured into revealing their certificate by anyone except an authorised service provider, this alleviates the "bully on the bus" problem.

Unlinkability
We consider unlinkability from the healthcare provider and the service provider in turn.

– (From healthcare provider) *The healthcare provider cannot link a user to their authentication phase interactions*.
– (From service provider) *The service provider cannot link a user to a previous authentication phase interaction*[2].

Revocation of certificates.
We require that a user's certificate can be revoked by the issuer.
Certificates may be invalidated for a number of reasons, we give three examples below:

– (Loss and theft) If a certificate becomes lost or compromised.

[1] We envisage Verity asking for this second factor only if she was unconvinced the photo provided strong binding, or if the situation demanded extra precautions to ensure the user was in fact the holder of the certificate. Entering a care home may warrant such precautions for example.

[2] This property could be satisfied if users were issued anonymous credentials.

	Paper-Based	App-Based
Correctness	✓	✓
Forge-Proof	✓	✓
Binding	✓	✓
Uniqueness	✓	✓
Tamper-Proof	✓	✓
Peer-Indistinguishability	×	✓
Unlinkability by H	✓	✓
Unlinkability by V	×	×
Revocation of Certificates	✓	✓
Revocation of SPs	×	✓

Table 1. Security properties of the paper-based and app-based SecureABC antibody certificates.

– (Error) If a batch of tests are recalled because they were incorrect.
– (Misuse) If evidence of certificate misuse is presented.

Revocation of service providers.
We require that a service provider can be revoked from the list of authorised providers. – We envisage that an authorised service provider may be revoked in the following situations:

– (Change of policy) A change in government policy may mean some service providers are no longer authorised.
– (Sanctioning) If a service provider is deemed to not be following recommended guidelines it may lose its authorised status.

B. Evaluation of SecureABC against Security Properties

Here we evaluate the SecureABC system in relation to the security properties from Section V-A and then with respect our general principles from Section II-B. Table 1 compares the properties observed by the paper-based and app-based authentication mechanisms of SecureABC. As with the previous section we do not aim to provide rigorous proofs of security for each property, only to give the reader an intuitive understanding of why each property is either satisfied or not by SecureABC.

Forge and Tamper Proof.
Here we consider the theoretical enforcement of the forge and tamper proof properties. We make the standard assumption that the underlying signature scheme is EUF-CMA secure. At a technical level the forge proof property is reduced to the unforgeability of the signature scheme. Moreover, the tamper proof property can be reduced to the forge proof property as in order to tamper with the value of the certificate, the user must reconstruct the signature produced by Harry.

Binding.
Alice is bound to her certificate by the photograph and name that are signed by Harry. This can be considered a strong binding property and is in line with current socially accepted verification mechanisms, for example driving licenses.

[3] Here "misuse" can be interpreted in a broad sense. Examples of misuse could be a user allowing others to attempt to use their certificate, or knowledge that some certificates were obtained using bribes to H [39].

Uniqueness.
In the Issue phase Harry checks that to see if Alice currently has a valid certificate. Consequently, uniqueness is satisfied to the degree that it is already assured for medical record keeping.

Peer-Indistinguishability.

– (Paper-based) The paper-based authentication sub-protocol provides poor peer indistinguishability for users. In particular, the protocol only guards against non-technical peers without the ability to scan QR codes.
– (App-based) The app-based authentication sub-protocol realises the peer indistinguishability property. This is achieved by enforcing mutual authentication between Alice and Verity. Here Verity is required to present a valid public key, signed by the government, which has not been revoked. Recall that since Verity's public key is signed using an EUF-CMA secure signature scheme, peer indistinguishability can be reduced to the difficulty of forging a government signature.

Unlinkability.

– (From healthcare provider) SecureABC is decentralized after the issue phase. More precisely, the healthcare provider (or any central authority for that matter) is not involved in the protocol after the issue phase. Consequently to link the user to an authentication the healthcare provider would have to collude with the service providers, we assume this does not happen.
– (From service provider) Since the service provider learns when a user authenticates with them, this property is not satisfied. If multiple service providers collude, then the colluding group all learn the linking.

Revocation of Certificates.
Recall that Harry periodically computes, signs and distributes rev (e.g. daily) such that it comprises all CID numbers in his private store that have the revocation bit $b_{\text{CID}} = \texttt{True}$. Then, for the use-cases in Section II-B, revocation of certificates can be realised as follows:

– (Loss) If Alice's certificate becomes lost or compromised, she must inform Harry. Harry looks up her CID and sets the revocation bit $b_{\text{CID}} = \texttt{True}$ in his private store.
– (Error) If a test result is recalled due to clinical error, Harry uses the TID number to identify the corresponding CID in his private store and then sets the revocation bit $b_{\text{CID}} = \texttt{True}$.
– (Misuse) If evidence of certificate misuse[3] emerges, a trusted authority (e.g. a court) should inform Harry of the CID that was misused. Harry then sets the corresponding revocation bit $b_{\text{CID}} = \texttt{True}$.

Revocation of Service Providers.

– (Paper-based) Our paper-based authentication does not provide technically enforced revocation of service providers. This property can only be obtained if a user is

constantly educated as to which service providers are no longer authorized. For example, daily updates on coronavirus from the UK government have included details on which services and shops are allowed to operate.

– (App-based) This property is satisfied by the app-based authentication sub-protocol. Authentication only succeeds if, in the mutual authentication phase, the service provider sends the user a public key pk_V that is signed by the government and which is not on the list of revoked verifiers rev_V. Since the user encrypts their antibody certificate using pk_V, the verifier must have the corresponding private key pk_V.

C. *SecureABC and the General Principles*

Here we consider SecureABC with respect to the general principles we formulate in Section II-B. Some of the components of the general principles are, naturally, out of scope when considering SecureABC (for example 'educate' and 'testing'), thus here we consider only those aspects that are relevant to the system itself. We keep the same headings for clarity.

Rename, educate and allow revocation. We follow our naming principle; SecureABC provides Secure AntiBody Certificates and implies neither immunity nor freedom of travel. Moreover SecureABC provides efficient and accurate revocation of both user certificates and, for app users only, service providers.

Access to testing and technology. We address digital exclusion in SecureABC by providing both a paper-based and app-based authentication protocol. Moreover, we prescribe that H takes the photo of A in the issue phase. These design decisions ensure that access to, or willingness to use, technology, or in the case of photographs the ability or means to access a "passport photo machine", does not discriminate against certain user groups.

Proportional and necessary use. Whilst this is ultimately a policy decision rather than something that can be technically enforced, we suggest two societally beneficial non-restrictive use cases for SecureABC in II-B.

Maintain user ownership of data. After the initial issue phase, SecureABC is a decentralised system in which users authenticate directly with service providers. This keeps the user in control of when their data is used, and for what purpose, and may both minimise feature creep by governments and facilitate dismantling the system.

VI. Implementation and Performance

In this section we review the implementation and practical considerations of our SecureABC antibody certificate system and present the results of our reference implementation.

QR Codes. In our proof of concept implementation we have chosen to use QR codes to represent the signed antibody certificates that are issued to users. QR codes are a reasonable candidate for this purpose because they are a widely adopted, mature technology that offers both machine-readability and error tolerance. There are a range of libraries suitable for reading and writing QR codes, users understand how to interact with them, and they are resistant to wear and tear when printed. Attacks on QR code systems are surveyed by Krombholz et al. [20].

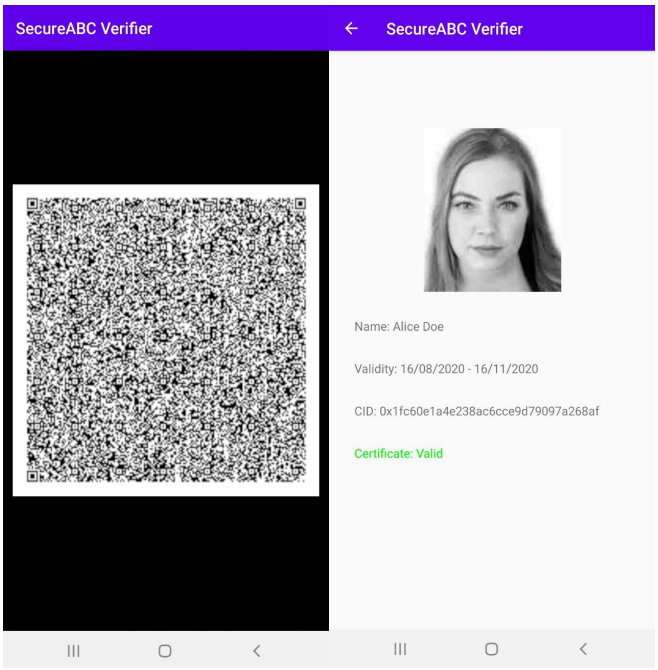

Fig. 2. The SecureABC scanning screen (left) and verification screen (right) from our reference Android implementation. The scanning screen shows a QR code output during the issue phase of our protocol. As shown on the verification screen, this QR code comprises the user image, a name, a CID, a validity period and a 521-bit ECDSA signature.

The storage capacity of a QR code is determined by a "symbol version" number between 1 and 40. Higher symbol numbers correspond to a higher storage capacity. The maximum storage capacity for a standard QR code is 2953 bytes [21]. If a higher storage capacity, for example for a higher resolution user photograph, our SecureABC protocol readily supports alternative technologies such as multi-layered QR codes [22,23] and Microsoft High Capacity Color Barcode (HCCB) [24] are available.

Implementation Proof of Concept. We have created an open source proof of concept implementation of the critical SecureABC components, this can be found at [25]. Firstly, our implementation allows for user credentials to be signed and compiled as a QR code as shown in Fig. 2. This corresponds to the issue phase of our protocol. Secondly, we have implemented an Android application that runs the authentication phase of our protocol. In more detail, the application can read a SecureABC QR code, verify the cryptographic signature and display the user details as shown in Fig. 3. We note we only provide the implementation as a proof of concept; we do not claim it is optimised for performance. However, we feel the performance results given next show SecureABC is both practical and efficient.

Performance and Scalability. Here we first provide benchmarks for our implementation, then highlight some limiting factors and initial learnings regarding optimisation.

Finally, we consider the scalability and usability of our proposal.

SecureABC requires only highly efficient cryptographic algorithms; both signing and verification of antibody certificates are just the standard ECDSA algorithms. Using our unoptimised Python implementation on an Intel Core i9 Macbook, complete end-to-end SecureABC QR code generation takes less than 8 seconds. Recall that this is a one-time operation and, although this performance is already persuasive, we note that less than 2 seconds are spent actually signing the certificate data and the remainder is spent on the generation of the QR code. We discuss this further when detailing optimisations below.

While issuance is a one-time process, user authentication occurs many times and is the more performance critical component. The results of our Android implementation show that a 521-bit ECDSA signature using the NIST standard curve P-521 can be verified in 3 ms using a Samsung Galaxy S9+ smartphone.

Next, we discuss our initial learnings regarding optimisation. Our reference implementation allowed us to both better understand the potential of digital barcode technologies and recognise the specific limitations of QR codes. Firstly, encoding binary data into a QR code is beyond the specification of most standard libraries. This limitation required us to encode the user photograph using a printable representation before writing to a barcode. In particular our Android implementation requires base 64 encoding the user photograph before it is compiled into a QR code. This adds a very significant 33% overhead to the number of bytes that presently need to be included in the QR code. While our current implementation is sufficient to demonstrate the fundamentals of our approach, resolving this limitation would substantially improve the usability of our system by allowing for both smaller QR codes and a higher level of error correction. Experimentally we found that smaller version number QR codes were much faster to read, and less error prone, than their higher capacity counterparts.

Regarding scalability, since our solution is decentralized and offline from any certificate issuer or revocation identity, there are inherently few issues to be considered. Nonetheless, each healthcare provider must maintain a database of user records which includes the CID of their antibody certificate. In practice healthcare providers must already maintain patient records on the same scale as is required for antibody certificates and the addition of an extra field should not be problematic. For revocation, service providers must download the list of revoked CIDs from each healthcare provider and users must download the list of revoked verifiers. This can easily be automated using an app and is also amenable to alternative techniques such as OCSP [27] should the scale of revocation prove to contraindicate basic revocation lists in practice.

Lastly, while conducting usability studies of our approach is outside the scope of this work, we believe that the simple user interface shown in Fig. 2 is encouraging in this regard. We note that key management in SecureABC is, for users, a relatively straightforward matter of looking after their QR code in the same way as they might a photocard driver's license, a bank card or indeed – a mobile phone. Lost or stolen certificates are handled by contacting the healthcare issuer to receive a replacement.

VII. Related Work

Here we review the small number of alternative antibody certificate schemes which have been proposed. To the best of our knowledge, all alternative schemes are either based on a centralised architecture or propose the use of a blockchain. Many of the commercial systems being trialed and implemented by governments [6,7] provide few technical details and cannot be fully understood or reviewed.

In the centralised category Estonia's antibody certificate system [26] enables people to share their so-called immunity status with a third-party using a temporary QR-code that is generated after authentication. Commercially, CoronaPass [28] also propose a centralised antibody certificate solution where service providers verify each user passport against a central database. Whilst security and legal measures can be put in place, in both these solutions, to deter the central authority from misusing the data they hold, it nonetheless represents an avoidable risk and a central point of failure. Involving the central party in each authentication risks large-scale user tracking and feature creep.

Eisenstadt et al. [29] propose an antibody certificate scheme in which W3C-standard "verifiable credentials" [30], the "Solid" platform for decentralised social applications [31] and a federated consortium blockchain are combined. In this system, a hash of each user's certificate is stored in a consortium blockchain which is checked each time that an authentication between a user and verifier takes place. Many commercial antibody certificate solutions also indicate that a blockchain is included. The "Immupass Covid-19 Immunity Certificate" [32] stores details of the tested individual directly in a consortium blockchain. User's present a QR code and their passport to a verifier and the corresponding test result and its validity is retrieved from the blockchain. CERTUS [33] uses a similar approach as does Vottun who are partnering with PwC for a trial in Spain [34].

In the broader security and privacy literature relating to COVID-19, we note that there has been significant debate over the merits of centralised versus decentralised systems for digital contact tracing [35][36][37][38][39]. This is a complex debate because there is a tradeoff between privacy and utility. In particular, centralised contact tracing data may be a valuable tool in tackling the virus. We do not think this debate directly applies here because there is less utility in a centralized record of when and where antibody certificates have used. Consequently, we believe decentralisation is the best approach for antibody certificates.

In relation to the societal implications of immunity passports, and our general principles which we present in Section II-B, the Ada Lovelace Institute published a "Rapid evidence report" [12] which explores how non-clinical measures can be used to attempt to relax current governmental controls and restrictions without an intolerable rise in COVID-19 cases. Finally, we comment that, as we have discussed, the scientific evidence and public understanding of the situation is fast changing, therefore we concur with Eisenstadt et al. [41] who call for regular reviews and oversight of sch processes to be handled by an Ethical Committee.

VIII. Conclusion

In this work we explore the controversial technique of so-called immunity passports and present SecureABC: a decentralised, privacy-preserving system for issuing and verifying antibody certificates. This work is a necessary and important first step towards enabling an open discussion about the technical implications of antibody certificates. We consider the implications of immunity passport systems, develop a set of general principles and security requirements for their deployment and show that these may be satisfied in practice.

Acknowledgement

The authors are grateful to Charles Raab, Markus Kuhn and Joseph Bonneau for their valuable early feedback which has helped to improve this work.

References

[1] E. Dong, H. Du, and L. Gardner, "An interactive web-based dashboard to track COVID-19 in real time", The Lancet Infectious Diseases, vol. 20, no. 5, pp. 533–534, May 2020.

[2] N. Ferguson *et al.*, "Report 9: Impact of non-pharmaceutical interventions (NPIs) to reduce COVID-19 mortality and healthcare demand", Mar. 2020, [Online]. Available: https://www.imperial.ac.uk/media/imperial-college/medicine/mrc-gida/2020-03-16-COVID19-Report-9.pdf. [Accessed: 12- May- 2020].

[3] S. DeLuca, N. Papageorge and E. Kalish, "The Unequal Cost of Social Distancing", Mar. 2020, [John Hopkins University, School of Medicine, Online]. Available: https://coronavirus.jhu.edu/from-our-experts/the-unequal-cost-of-social-distancing. [Accessed 24- May- 2020].

[4] M. Salath et al., "COVID-19 epidemic in Switzerland: on the importance of testing, contact tracing and isolation", Swiss Medical Weekly, Mar. 2020.

[5] N. Kofler and F. Baylis, "Ten reasons why immunity passports are a bad idea", Nature, vol. 581, no. 7809, pp. 379–381, May 2020.

[6] B. Fraser, "Chile plans controversial COVID-19 certificates", The Lancet, vol. 395, no. 10235, p. 1473, May 2020.

[7] A. L. Phelan, "COVID-19 immunity passports and vaccination certificates: scientific, equitable, and legal challenges", The Lancet, vol. 395, no. 10237, pp. 1595–1598, May 2020.

[8] ""Immunity passports" in the context of COVID-19", World Health Organisation, Scientific Brief, Apr. 2020, [Online]. Available: https://www.who.int/news-room/commentaries/detail/immunity-passports-in-the-context-of-covid-19. [Accessed 9- May- 2020].

[9] D. Lewis, "Is the coronavirus airborne? Experts can't agree," Nature, vol. 580, no. 7802, pp. 175–175, Apr. 2020.

[10] "Immune responses in COVID-19 and potential vaccines: Lessons learned from SARS and MERS epidemic", Asian Pacific Journal of Allergy and Immunology, 2020.

[11] M. Galanti and J. Shaman, "Direct observation of repeated infections with endemic coronaviruses", Cold Spring Harbor Laboratory, May 2020.

[12] "Rapid Evidence Review: Exit through the App Store", Ada Lovelace Institute, Apr. 2020, [Online]. Available: https://www.adalovelaceinstitute.org/wp-content/uploads/2020/04/Ada-Lovelace-Institute-Rapid-Evidence-Review-Exit-through-the-App-Store-April-2020-2.pdf. [Accessed 20- May- 2020].

[13] Yamin, Alicia & Habibi, Roojin. "Human Rights and Coronavirus: What's at Stake for Truth, Trust, and Democracy?", Health and Human Rights, 2020.

[14] S. Bernard Stoecklin et al., "First cases of coronavirus disease 2019 (COVID-19) in France: surveillance, investigations and control measures, January 2020", Eurosurveillance, vol. 25, no. 6, Feb. 2020.

[15] "COVID-19 Contact tracing: data protection expectations on app development", Information Commissioners Office (ICO), May 2020, [Online]. Available: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/05/covid-19-contact-tracing-data-protection-expectations-on-app-development/. [Accessed 17- May- 2020]

[16] David Butler, Chris Hicks, James Bell, Carsten Maple and Jon Crowcroft. "Differentially Private Antibody Certificates and Tokens", Jun. 2020, [work in progress]. Available: on request.

[17] S. Goldwasser, S. Micali, and R. L. Rivest, "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks", SIAM Journal on Computing, vol. 17, no. 2, pp. 281–308, Apr. 1988.

[18] "Digital Signature Standard (DSS)", National Institute of Standards and Technology, Jul. 2013.

[19] J. Katz and Y. Lindell, "Introduction to Modern Cryptography", Chapman and Hall/CRC, 2014.

[20] K. Krombholz, P. Frühwirt, P. Kieseberg, I. Kapsalis, M. Huber, and E. Weippl, "QR Code Security: A Survey of Attacks and Challenges for Usable Security", in Lecture Notes in Computer Science, Springer International Publishing, 2014, pp. 79–90.

[21] V. Mavroeidis and M. Nicho, "Quick Response Code Secure: A Cryptographically Secure Anti-Phishing Tool for QR Code Attacks", in Lecture Notes in Computer Science, Springer International Publishing, 2017, pp. 313–324.

[22] J. M. Meruga et al., "Multi-layered covert QR codes for increased capacity and security", International Journal of Computers and Applications, vol. 37, no. 1, pp. 17–27, Jan. 2015.

[23] Z. Yang, H. Xu, J. Deng, C. C. Loy, and W. C. Lau, "Robust and Fast Decoding of High-Capacity Color QR Codes for Mobile Applications", IEEE Transactions on Image Processing, vol. 27, no. 12, pp. 6093–6108, Dec. 2018.

[24] D. Parikh and G. Jancke, "Localization and Segmentation of A 2D High Capacity Color Barcode", in 2008 IEEE Workshop on Applications of Computer Vision, 2008.

[25] https://github.com/alan-turing-institute/SecureABC

[26] "Estonia tests first digital immunity passports for workplaces", Engineering & Technology, The Institution of Engineering and Technology, May 2020, [Online]. Available: https://eandt.theiet.org/content/articles/2020/05/estonia-tests-first-digital-immunity-passports-for-workplaces/. [Accessed 02- Jun- 2020].

[27] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, "RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", June 2013, [Online]. Available: https://tools.ietf.org/html/rfc6960. [Accessed 25- Aug- 2020]

[28] "CoronaPass FAQ", May 2020, [Online]. Available: https://web.archive.org/web/20200609010523/https://resourcesbizagi.azureedge.net/docs/coronapass/CoronaPass-FAQ.pdf. [Accessed 9- Jun- 2020].

[29] M. Eisenstadt, M. Ramachandran, N. Chowdhury, A. Third, and J. Domingue, "COVID-19 Antibody Test / Vaccination Certification: There's an app for that", IEEE Open Journal of Engineering in Medicine and Biology, 2020.

[30] M. Sporny, D. Longley and D. Chadwick, "Verifiable Credentials Data Model 1.0", W3C Candidate Recommendation, Mar. 2019.

[31] E. Mansour et al., 'A Demonstration of the Solid Platform for Social Web Applications', in Proceedings of the 25th International Conference Companion on World Wide Web - WWW '16 Companion, 2016.

[32] "ImmuPass – A simple and secure certificate of COVID-19 immunity" May 2020, [Online]. Available: https://web.archive.org/web/20200615151750/https://www.immupass.org/files/IMMUPASS_V2.1_En.pdf. [Accessed 15- Jun- 2020].

[33] "CERTUS - A novel and simple solution for certificate issuers, holders and verifiers", May 2020, [Online]. Available: https://web.archive.org/web/20200609011043/https://www.certusdoc.com/. [Accessed 9- Jun- 2020].

[34] I. Parker and E. Jones, "Something to declare? Surfacing issues with immunity certificates", The Ada Lovelace Institute, Jun. 2020, [Online]. Available: https://web.archive.org/web/20200609010533/https://www.adalovelaceinstitute.org/something-to-declare-surfacing-issues-with-immunity-certificates/. [Accessed 05- Jun- 2020].

[35] S. Vaudenay, "Centralized or Decentralized? The Contact Tracing Dilemma", Cryptology ePrint Archive, Report 2020/531, May 2020, [Online]. Available: https://eprint.iacr.org/2020/531. [Accessed 12- May- 2020].

[36] "European coronavirus contact tracing app sparks uproar in the privacy community", May 2020, [Online]. Available: https://web.archive.org/web/20200609010523/https://tech.newstatesman.com/security/european-coronavirus-contact-tracing-app-sparks-uproar-in-the-privacy-community. [Accessed 09- Jun- 2020].

[37] "PEPP-PT vs DP-3T: The coronavirus contact tracing privacy debate kicks up another gear", May 2020, [Online]. Available: https://web.archive.org/web/20200609010537/https://tech.newstatesman.com/security/pepp-pt-vs-dp-3t-the-coronavirus-contact-tracing-privacy-debate-kicks-up-another-gear. [Accessed 09- Jun- 2020].

[38] James Bell, David Butler, Chris Hicks and Jon Crowcroft. "TraceSecure: Towards Privacy Preserving Contact Tracing", Apr. 2020, [Online]. https://arxiv.org/abs/2004.04059. [Accessed 17- Jun- 2020].

[39] C. Troncoso *et al.*, "Decentralized Privacy-Preserving Proximity Tracing", May 2020, [Online]. Available: https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf. [Accessed 25- May- 2020].

[40] P. Adepoju, "The yellow fever vaccination certificate loophole in Nigeria. Lancet", 2019, doi:10.1016/S0140-6736(19)31670-8

[41] M. Eisenstadt, M. Ramachandran, N. Chowdhury, A. Third and J. Domingue, "COVID-19 Antibody Test/Vaccination Certification: There's an App for That," Supplementary materials section, in IEEE Open Journal of Engineering in Medicine and Biology, vol. 1, pp. 148-155, 2020, doi: 10.1109/OJEMB.2020.2999214.

[42] G. Persad and E. Emanuel, "The Ethics of COVID-19 Immunity-Based Licenses ('Immunity Passports')." JAMA. May 6, 2020. [Online]. Available: https://dx.doi.org/10.1001/jama.2020.8102 [Accessed: May 20, 2020].

[43] L. Edwards, M Veale, O. Lynskey and R. Coldicutt, "The Coronavirus (Safeguards) Bill 2020: Proposed protections for digital interventions and in relation to immunity certificates.", 2020.