# SecureABC: Secure AntiBody Certificates for COVID-19

Chris Hicks*[1], David Butler*[1], James Bell
Carsten Maple[2], Jon Crowcroft[1],
[1]The Alan Turing Institute , [2]University of Warwick
[1]{chicks, dbutler, jcrowcroft}@turing.ac.uk, [2]cm@warwick.ac.uk

**Abstract**

COVID-19 has resulted in unprecedented social distancing policies being enforced worldwide. As governments urgently seek to reopen society, 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.

## 1 Introduction

Governments worldwide are currently dealing with the Coronavirus pandemic, an outbreak of the SARS-CoV-2 virus which has already resulted in over 375,000 deaths [3] 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 [9]. 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 [15]. 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 reducing the scope of population-wide social distancing and seeking technologies that may alleviate the requirement for 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 [12], 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 [2, 14], respectively, and key policy makers in the UK and Germany are also considering the approach [6]. 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.

We note that immunity passports are a highly controversial technology that has received criticism from many influential organisations including the World Health Organisation (WHO) [12]. We do not claim to advocate 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 solution to the problem that can be used to properly inform any such decision. We complement our solution with a presentation of four general deployment principles which aim to mitigate many of the concerns surrounding immunity passports.

### 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 right properties and can be evaluated on common terms.

2. We present SecureABC, a decentralised and privacy-preserving solution for antibody certificates which is both designed in accordance with our general principles and that meets our security and privacy requirements.

3. We show that SecureABC is efficient and practical with our proof of concept implementation.

**Outline** First in Section 2 we review the concerns surrounding immunity passports and derive four general principles that may minimise the risk posed by these systems. Next, in Section 3 we define our protocol model and introduce our cryptographic primitives. Section 4 presents the full details of our SecureABC antibody certificate system. Then, in Section 5 we define our desired security properties for immunity passports and then evaluate SecureABC with respect to them. Section 6 shows the results of our implementation. Finally, we review related work and other solutions in Section 7 before concluding in Section 8.

## 2 General Principles for Immunity Passports

In this section we build towards a set of general principles for deploying an immunity passport system. We first present the general use case for immunity passports, before citing the major concerns which have been raised. Our motivation for providing this section is to address concerns that immunity passport systems may prove to be counter productive and could have a net negative impact on society. Evidence is mounting that many nations [2, 14, 6] are at least considering immunity passport solutions, so it is important that techniques for minimising the risk posed by such systems are considered.

**Basic use case** We begin our discussion with a 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. In more detail, a healthcare provider will test citizens for antibodies to COVID-19. If antibodies are found then a so-called 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.

**Immunity passport concerns** Immunity passports have attracted significant criticism. The main concerns we are aware of [12, 25] are as follows:

1. **Alterations to scientific advice.** As a novel disease, COVID-19 is not yet well understood by the scientific community [11]. For example, the WHO's main concern is that the presence of antibodies is not an accurate indicator of immunity citing that such tests "need further validation to determine their accuracy and reliability" [12].

2. **Is discriminatory.** Such a system will create an attribute for discrimination [27], creating a clear distinction between those with "immunity" and those without. The Ada Lovelace Institute report emphasises this [22]: "Discrimination and stigmatisation may become commonplace if immunity becomes an element of identity." This inequality would be exaggerated if tests were not universally and freely available to all — immunity passports, and the associated benefits, could be a luxury of the rich.

3. **Incentivises people to get the virus.** Those with immunity passports will be allowed access to "the post-lockdown world" while those without could remain subject to social distancing policy. An immunity passport could become synonymous with freedom, creating a strong incentive for people to attempt to obtain a passport. Coupled with the belief that having (and surviving) the virus corresponds to gaining immunity [20, 18], it is hypothesised that immunity passports could actively encourage people to try to become infected.

4. **Feature creep by governments.** Governments are currently exercising an abnormal level of control and surveillance over their populations [10]. Passporting systems could provide authorities with an opportunity to implement technologies, and to collect data, that could have long-term negative consequences on society [22].

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

### General principles for immunity passports

1. **Rename, educate and revocate.** Until there is strong evidence of protective immunity 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. 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 the principle of being transparent about the purpose and benefit of the closely related contact tracing technology [21]. 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. In the case of contact tracing, the ICO state that "special consideration for different societal groups" is paramount. Moreover the Lovelace report [22] calls for "measures for ensuring vulnerable groups are not excluded from the operation of the system".

3. **No restrictions based on test results.** The Lovelace report 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 strategy should minimise any restriction of access to movement or provision of services. The resulting system will be less discriminatory[1] and therefore will present less incentive to get the virus.

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

[1] Without this the system potentially discriminates against those who have acted responsibly during the lockdown period, have not contracted the virus, and therefore are less likely to test positive for antibodies.

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" [21] with regard to contact tracing.

These principles may appear to reduce the functionality of any antibody certificate system that is in accordance with them. To alleviate this concern we present two additional use cases that are both in accordance with these principles and which may still benefit society:

**Use case 2: Indicating user risk.** Consider the use case given at the start of the section where users of the public transport are required to show their 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 or tested-negative citizens. In the Appendices in Section 8 we now note an early extension to this idea where differential privacy can be used to randomise each users antibody certificate status whilst still allowing for the overall proportion of lower-risk users 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 (based a task scheduling algorithm) the carrier to hold an antibody certificate could provide a way to reduce the risk faced by the recipient. This scenario, in which the carrier would hold an antibody certificate and her employer would be the verifier, could represent a reasonable trade-off between restricting access to work and minimising the risk faced by vulnerable groups.

# 3 Model and Preliminaries

Here we begin the technical part of our paper by first defining the model for our antibody certificate protocol and then introducing the cryptographic primitives we require.

## 3.1 Model

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) H records the result of the test in a certificate which is sent to A. In step (3) A presents her certificate to V and then finally, in step (4), V checks the authenticity and attributes of the certificate to ensures it corresponds to A (e.g. by matching a photo and name to A). Our system model

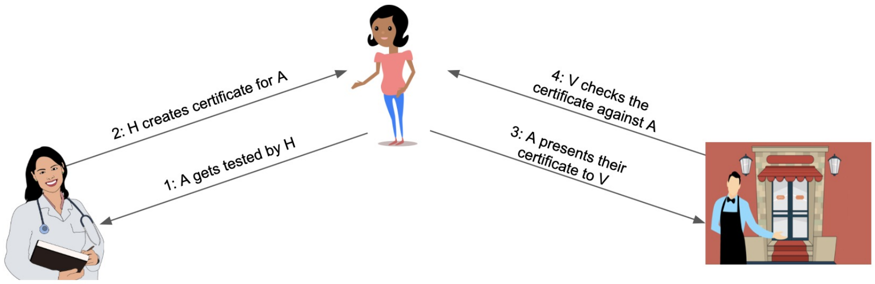
2: H creates certificate for A
1: A gets tested by H
4: V checks the certificate against A
3: A presents their certificate to V

Figure 1: Our general model of an antibody certificate scheme run between a healthcare provider, a user and a service provider.

assumes a root of trust in the system (e.g. the government) that authorises both H and V as legitimate entities.

In our SecuereABC antibody certificate scheme, which we present in Section 4, we map these steps into three protocol phases: an initial setup phase where H generates the public and private system parameters, an issue phase corresponding to steps (1) and (2) where A is tested and issued with a certificate by H and finally an authentication phase corresponding to steps (3) and (4) where A's certificate is verified by V.

## 3.2 Preliminaries

Our SecureABC antibody certificate scheme requires a secure public key signature scheme as well as 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 verifys the signature or decrypts the ciphertext, respectively. We denote the signature scheme by the tuple ($\textit{key-gen}_{sign}$, *sign*, *verify*) and the encryption scheme by the tuple ($\textit{key-gen}_{enc}$, *enc*, *dec*).

We use the 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 [19]. Rather than define this property here, we refer the reader to Goldwasser et al. [19] for the standard definition. We note that the standard Elliptic Curve Digital Signature Algorithm (ECDSA) [16] is a sufficient instantiation for our needs.

We use the encryption scheme in the authentication phase between the user and the service provider. The user will encrypt their signed certificate such that only an authorised service provider can decrypt it. Our particular use of the 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 refer the reader to Katz and Lindell [24] .

# 4 SecureABC

In this section we present SecureABC, our antibody certificate scheme that realises the model defined in Section 3. 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 [15] 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 3 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 H or V generate a new public key, the government signs it to indicate that it can be trusted.

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

## 4.1 The SecureABC Protocol

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

**Setup:** Harry initialises the list of revoked CID numbers $rev = \emptyset$ and generates the public and private key for the signature scheme.

$$(pk_H, sk_H) \leftarrow \mathit{key\text{-}gen}_{sign}(\cdot)$$

**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 $b_{\mathrm{CID}} = \texttt{False}$ and specifies a validity period $date_{\mathrm{CID}}$. Harry stores $(\mathrm{CID}, \mathrm{TID}, b_{\mathrm{CID}}, date_{\mathrm{CID}}, comm_{\mathrm{CID}})$ in a private database

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 prepares and sends Alice the signed antibody certificate $cert_A$ which is computed as follows:

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

In the interests of mitigating economic discrimination, we recommend that provisions are made to ensure that all citizens are able to get a photograph of the required standard. One option could be to create a mobile app that can be used by Harry to take such photographs on behalf of each user.

**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. Since SecureABC allows Alice to present either a paper-based or app-based certificate, 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 and verifies the list of revoked CID numbers $rev$ and Harry's public key $pk_H$.

**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 (e.g. 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 $(name_{\mathrm{A}}, photo_{\mathrm{A}}, date_{\mathrm{CID}}, \mathrm{CID})$. She checks that CID has not been revoked i.e. $CID \notin rev$, then compares $photo_{\mathrm{A}}$ to Alice and ensures that $date_{\mathrm{CID}}$ has not elapsed. Optionally, Verity may ask to see a second document bearing $name_{\mathrm{A}}$.

**App-Based Authentication Protocol:** Alice runs an app that stores her antibody certificate $cert_A$ and which periodically downloads and verifies 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 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 privacy for app-users. More details on this point are provided in our evaluation which follows.

# 5 Security Properties and Evaluation

This section first presents the main technical security properties we require of an antibody certificate protocol before evaluating our SecureABC scheme with respect to them.

## 5.1 Desired Security Properties

In this work we do not pursue a rigorously defined, formal definition for every requirement but rather we intend to provide an unambiguous set of terms for evaluating antibody certificate systems. It is unlikely that any scheme can simultaneously satisfy all of 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 some additional intuition after the definition of each term.

**Correctness:** *If all parties are honest, the service provider will be able to view the certificate produced by the healthcare provider for the user at the end of an execution of protocol.* — Correctness ensures that the protocol computes the expected functionality.

**Soundness:** *A user cannot create a valid certificate alone.* — In other words an adversarial user cannot forge a valid certificate.

**User-Cert Binding:** *The only certificate a user can successfully use is the one that is assigned to them and which has not been revoked.* — This prevents a user from swapping their certificate with that of another user and then succeeding in using it.

**Uniqueness:** *A user can have at most one valid certificate associated to them at any one time.* — This property is important when User-Cert Binding is imperfect, for example when considering twins who may share a similar photograph but that may not share the same antibody test result.

**Cert-Attribute Binding:** *The value of the attributes associated with a certificate cannot be altered by the user.* — In other words, the certificate must be tamper proof.

**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 authorised service providers, this alleviates the "bully on the bus" problem.

**User-Auth unlinkability:**

1. *(From healthcare provider) The healthcare provider cannot link a user to their authentication phase interactions.*
2. *(From service provider) The service provider cannot link a user to an authentication phase interaction.*

This property prevents the healthcare and the service provider, respectively, from learning when and where a users certificate is authorised.

**Revocation of certificates:** *A users certificate can be revoked.* — Certificates may be invalidated in the following situations:

**Loss/Stolen:** If a certificate becomes lost or compromised.

**Error:** If a batch of tests are recalled because they were incorrect.

**Misuse:** If evidence of certificate misuse is presented.

**Revocation of service providers:** *A service provider can be revoked from the list of authorised providers.* — 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.

## 5.2 Evaluation of SecureABC

Here we first evaluate the SecureABC system in relation to the security properties from Section 5 and then with respect our general principles from Section 2. We make the assumption that the healthcare and service providers do not collude. Figure 5.2 summarises and compares the properties observed by the paper-based and app-based versions of SecureABC.

**Correctness:** The correctness of the system is reduced to the correctness of the signature scheme and, optionally for app-based users, the encryption scheme used by our protocol.

**Soundness:** We require that the signature scheme is EUF-CMA secure therefore no forgery of certificates is possible.

**User-Cert-Binding:** Alice is bound to her certificate by the photograph and name that are signed by Harry. Alice would have to go to significant effort to change her appearance and name to match that of another user, and would also face legal and social pressure for doing so.

**Uniqueness:** Harry checks that to see if Alice has already been issued a certificate in the Issue phase, meaning uniqueness is satisfied to the degree that it is already assured for medical record keeping.

**Cert-Attribute Binding:** The certificate is signed by Harry using an EUF-CMA secure signature scheme. As Alice cannot produce any forgery, let alone one with specific attributes, she cannot modify the attributes in her certificate.

**Peer Indistinguishability**

1. (Paper-based) The paper-based authentication sub-protocol provides negligible peer indistinguishability for users. In particular, the protocol only guards against non-technical peers without the ability to scan QR codes.
2. (App-based) The app-based authentication sub-protocol enforces mutual authentication by requiring Verity to present a valid public key, signed by the government, which has not been revoked. As 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.

**User-Auth Unlinkability:**

1. (From healthcare provider) SecureABC is decentralised, meaning the healthcare provider 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.

2. (From service provider) The service provider learns when a user authenticates with them. If multiple service providers collude, then the colluding group all learn the linking.

**Revocation of certificates:** The signed list of revoked certificate CID numbers *rev* is periodically distributed (e.g. daily) to service providers and checked during each authentication. This means a certificate that has been revoked cannot be used successfully. Let Harry periodically compute and distribute *rev* 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 5.1, revocation of certificates can be realised as follows:

1. **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.
2. **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 $b_{\text{CID}} = \texttt{True}$.
3. **Misuse:** If evidence of certificate misuse emerges, a trusted authority (e.g. a court) should inform Harry of the CID that was misused. Harry sets the corresponding revocation bit $b_{\text{CID}} = \texttt{True}$.

**Revocation of service providers:**

1. (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 authorised[2].
2. (App-based) This property is realised in the app-based authentication sub-protocol. Authentication only succeeds if 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 $sk_V$.

**Adherence to our general principles** Here we evaluate SecureABC with respect to the general principles we formulate in Section 2.

1. **Rename, educate and revocate.** Firstly, we follow our naming principle. SecureABC provides Secure Antibody Certificates and implies neither immunity nor freedom of travel. Public education about our system is beyond the scope of this paper, but we do provide efficient and fast revocation of both user certificates and service providers.

[2] For example it may be advertised that a certain class of services (e.g. cinemas) are no longer authorised.

| | Paper-based | Digital |
|---|---|---|
| Correctness | ✓ | ✓ |
| Soundness | ✓ | ✓ |
| User-Cert Binding | ✓ | ✓ |
| Uniqueness | ✓ | ✓ |
| Cert-Attribute-Binding | ✓ | ✓ |
| Peer-Indistinguishability | ✗ | ✓ |
| User-Auth Unlinkability by H | ✓ | ✓ |
| User-Auth Unlinkability by V | ✗ | ✗ |
| Revocation of Certificates | ✓ | ✓ |
| Revocation of Service Providers | ✗ | ✓ |

Table 1: Security properties of our paper-based and app-based user passports.

2. **Access to testing and technology.** We reduce digital discrimination in SecureABC by providing both a paper-based and app-based authentication protocol. This design decision ensures that access to, or willingness to use, technology does not discriminate against certain user groups.

3. **No restrictions based on test results.** Whilst this is a policy decision rather than something that can be technically enforced, we suggest two non-restrictive antibody certificate use-cases in Section 2. In addition, in the Appendices in Section 8 we demonstrate a technique based on differential privacy for hiding individual test results while still allowing aggregate risk estimation.

4. **Maintain user ownership of data.** 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.

## 6 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 SecureABC, users are issued signed antibody certificates which they display to service providers using a QR code representation. QR codes are a suitable technology 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. [26].

The storage capacity of a QR code is determined by a “symbol version” number between 1 and 40. Higher symbol numbers correspond to a greater number of modules, and more modules correspond to higher storage capacity. The maximum storage capacity for a standard QR code is 2953 bytes [29]. If higher storage capacity is needed, alternative technologies such as multi-layered QR codes [30, 35] and Microsoft High Capacity Color Barcode (HCCB) [31] are available.

**Implementation** We have created an open source, reference implementation of our paper-based antibody certificate generation and verification algorithms which can be downloaded from `https://github.com/alan-turing-institute/SecureABC`. We use this implementation to evaluate the suitability of QR codes for this application. In particular, SecureABC antibody certificates comprise a photograph of the user, their name, a validity period, a CID number and a digital signature. Figure 2 shows a QR code that is output by our implementation and which comprises the optimised gray-scale user photograph as shown in Figure 3, the name “Alice Doe”, the validity period “6052020-16082020”, the CID `0x1fc60e1a4e238ac6cce9d79097a268af` and a valid 512-bit ECDSA signature.

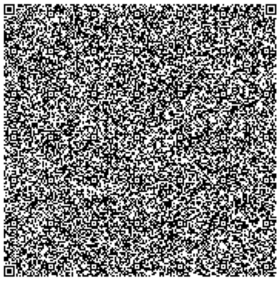

Figure 2: An example of a standard “version 40” QR code that is output by our reference implementation.

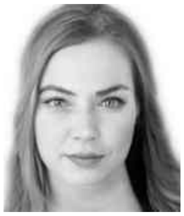

Figure 3: An example image, initially generated by the NVidia StyleGAN [23], that has been optimised to a size of 2157 bytes. This image, a name, a CID, a validity period and a 512-bit ECDSA signature is included (with 7% error correcting codes) in the standard QR code shown in Figure 2.

Our implementation shows that it is possible to provide both a high level of security (512-bit ECDSA) and reasonable user-cert-binding, in the form of a photo, using a standard version 40 QR code. Verification of antibody certificates is highly efficient and is just the standard ECDSA verification algorithm.

# 7 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 trialled and implemented by governments [2, 14] provide few technical details and cannot be fully understood.

In the centralised category Estonia's antibody certificate system that is being trialled by the "Back to Work" non-governmental organisation [14] 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 [13] 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 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. [17] propose an antibody certificate scheme in which W3C-standard "verifiable credentials" [33], the "Solid" platform for decentralised social applications [28] and a federated consortium blockchain are combined. In this system, a hash of each users 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" [7] 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 [1] uses a similar approach as does Vottun who are partnering with PwC for a trial in Spain [32].

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 [34, 5, 8]. In digital contact tracing, users' phones continually broadcast ephemeral identities which are used to determine which users have come into contact and risked infection. Decentralised contact tracing systems [4] have the advantage of allowing users to compute which interactions may have risked infection locally, denying this information to a central authority. Analogously in our SecureABC scheme, users authenticate directly with service providers and the healthcare provider is denied certificate usage information.

In relation to the non-technical implications of immunity passports, and our general principles which we present in Section 2, the Ada Lovelace Institute published a "Rapid evidence report" [22] 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.

## 8 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. 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.

**Acknowledgements** The authors are grateful to Charles Raab, Markus Kuhn and Joseph Bonneau for their valuable early feedback which has helped to improve this work. This work was supported by The Alan Turing Institute under the EPSRC grant EP/N510129/1.

## References

[1] CERTUS - A novel and simple solution for certificate issuers, holders and verifiers. Online, Accessed 19 May 2020, Available at: `https://www.certusdoc.com/`.

[2] Chile to issue world's first 'immunity passports' to recovered coronavirus patients. Online, Accessed 16 May 2020, Available at: `https://nypost.com/2020/04/21/chile-to-issue-worlds-first-immunity-passports-to-recovered-coronavirus-patients/`.

[3] COVID-19 Tracker. Online, Accessed 23 May 2020, Available at: `https://www.bing.com/covid/`.

[4] Decentralized Privacy-Preserving Proximity Tracing. Online, Accessed 12 May 2020, Available at: `https://github.com/DP-3T/`.

[5] European coronavirus contact tracing app sparks uproar in the privacy community. Online, Accessed 20 May 2020, Available at: `https://tech.newstatesman.com/security/european-coronavirus-contact-tracing-app-sparks-uproar-in-the-privacy-community`.

[6] 'Immunity passports' could speed up return to work after Covid-19. Online, Accessed 12 May 2020, Available at: `https://www.theguardian.com/world/2020/mar/30/immunity-passports-could-speed-up-return-to-work-after-covid-19`.

[7] ImmuPass - A simple and secure certificate of COVID-19 immunity. Online, Accessed 11 May 2020, Available at: https://www.immupass.org.

[8] Pepp-pt vs dp-3t: The coronavirus contact tracing privacy debate kicks up another gear. Online, Accessed 19 May 2020, Available at: https://tech.newstatesman.com/security/pepp-pt-vs-dp-3t-the-coronavirus-contact-tracing-privacy-debate-kicks-up-another-gear.

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

[10] The new normal: China's excessive coronavirus public monitoring could be here to stay. The Guardian, Online, Accessed 19 May 2020, Available at: https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay.

[11] What we don't know about COVID-19. The New Yorker, Online, Accessed 18 May 2020, Available at: https://www.newyorker.com/science/medical-dispatch/what-we-dont-know-about-covid-19.

[12] WHO Scientific Brief - ”Immunity passports” in the context of COVID-19. Online, Accessed 9 May 2020, Available at: https://www.who.int/news-room/commentaries/detail/immunity-passports-in-the-context-of-covid-19.

[13] CoronaPass FAQ. Bigazi, Online, Accessed 15 May 2020, Available at: https://resourcesbizagi.azureedge.net/docs/coronapass/CoronaPass-FAQ.pdf, 2020.

[14] Estonia tests first digital immunity passports for workplaces. E&T editorial staff, Online, Accessed 02 June 2020, Available at: https://eandt.theiet.org/content/articles/2020/05/estonia-tests-first-digital-immunity-passports-for-workplaces/, May 2020.

[15] Stefanie DeLuca, Nick Papageorge, and Emma Kalish. The unequal cost of social distancing. John Hopkins University, School of Medicine, Online, Accessed 24 May 2020, Available at: https://coronavirus.jhu.edu/from-our-experts/the-unequal-cost-of-social-distancing, 2020.

[16] Digital Signature Standard (DSS) (FIPS 186-4). Technical report, National Institute of Standards and Technology, July 2013.

[17] 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*, pages 1–1, 2020.

[18] Marta Galanti and Jeffrey Shaman. Direct observation of repeated infections with endemic coronaviruses. *medRxiv*, 2020.

[19] Shafi Goldwasser, Silvio Micali, and Ronald L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, 17(2):281–308, 1988.

[20] The Guardian. WHO warns against coronavirus immunity passports. Online, Accessed 10 May 2020, Available at: `https://www.theguardian.com/world/2020/apr/25/who-warns-against-coronavirus-immunity-passports`.

[21] ICO Information Commissioners Office. COVID-19 contact tracing: data protection expectations on app development, 2020. Online, Accessed 17 May 2020, Available at: `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/`.

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

[23] T. Karras, S. Laine, and T. Aila. A style-based generator architecture for generative adversarial networks. In *2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, pages 4396–4405, 2019.

[24] Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography (Chapman & Hall/Crc Cryptography and Network Security Series)*. Chapman & Hall/CRC, 2007.

[25] Natalie Kofler and Françoise Baylis. Ten reasons why immunity passports are a bad idea. *Nature*, 581(7809):379–381, May 2020.

[26] Katharina Krombholz, Peter Frühwirt, Peter Kieseberg, Ioannis Kapsalis, Markus Huber, and Edgar Weippl. QR Code Security: A Survey of Attacks and Challenges for Usable Security. In *Human Aspects of Information Security, Privacy, and Trust*, pages 79–90, Cham, 2014. Springer International Publishing.

[27] The Lancet. COVID-19 immunity passports and vaccination certificates: scientific, equitable, and legal challenges. Online, Accessed 6 May 2020, Available at: `https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(20)31034-5/fulltext`.

[28] Essam Mansour, Andrei Vlad Sambra, Sandro Hawke, Maged Zereba, Sarven Capadisli, Abdurrahman Ghanem, Ashraf Aboulnaga, and Tim Berners-Lee. A demonstration of the solid platform for social web applications. In *WWW (Companion Volume)*, pages 223–226. ACM, 2016.

[29] Vasileios Mavroeidis and Mathew Nicho. Quick Response Code Secure: A Cryptographically Secure Anti-Phishing Tool for QR Code Attacks. In *Computer Network Security*, pages 313–324, Cham, 2017. Springer International Publishing.

[30] Jeevan M. Meruga, Carly Fountain, Jon Kellar, Grant Crawford, Aravind Baride, P. Stanley May, William Cross, and Randy Hoover. Multi-layered covert QR codes for increased capacity and security. *International Journal of Computers and Applications*, 37(1):17–27, 2015.

[31] D. Parikh and G. Jancke. Localization and Segmentation of A 2D High Capacity Color Barcode. In *2008 IEEE Workshop on Applications of Computer Vision*, pages 1–6, 2008.

[32] Imogen Parker and Elliot Jones. Something to declare? Surfacing issues with immunity certificates. Online, Accessed 05 June 2020, Available at: `https://www.adalovelaceinstitute.org/something-to-declare-surfacing-issues-with-immunity-certificates/`.

[33] M Sporny, D Longley, and D Chadwick. Verifiable credentials data model 1.0. *W3C, W3C Candidate Recommendation, March*, 2019.

[34] Serge Vaudenay. Centralized or decentralized? the contact tracing dilemma. Cryptology ePrint Archive, Report 2020/531, 2020. `https://eprint.iacr.org/2020/531`.

[35] 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*, 27(12):6093–6108, 2018.

# Appendix

The following section introduces an extension to the use case we give in Section 2 in which users are not restricted access to services or transportation on the basis of their antibody certificate value. We show that differential privacy may provide a way to enforce non-discrimination, by randomising antibody certificate statuses, whilst still allowing for aggregate risk to be estimated.

# Differentially Private Antibody Certificates

Briefly, here we consider the use of antibody certificates strictly as a tool for analysing risk rather than asserting immuno-priviledge. In particular we apply techniques from differential privacy such that individual antibody test results are randomised, and remain hidden from service providers, but still allow for aggregate risk estimates to be calculated. Randomising each users antibody certificate result means that it cannot, and will not, be used to restrict access to services or freedom to travel. This also means that users will be less motivated to fraudulently acquire a certificate which has not been issued to them. Finally, this frees us from the need to ensure user binding by including a photograph and name in each certificate.

In this work non-binding, randomised and differentially private antibody certificates are used as a tool for estimating the aggregate risk of multiple users who use a particular service over short to medium timeframes. We expect that users may be motivated to use this tool voluntarily as a way of reducing the need for more restrictive social policy in the fight against COVID-19.

## 8.1 Protocol

Our protocol consists of three phases, issue, check and aggregate. The issue phase is congruent to the issue phase from SecureABC; here however we employ differential privacy techniques to output the 'status' of a certificate. The check phase is conducted between a user and a service provider. Finally the aggregate phase allows the service provider to reconstruct the underlying risk profile of the 'checked' users.

We use a DP protocol to produce a randomised 'user status' value in certificate, we denote this by $protocol_{DP}$, but do not go into details about it here.

### Issue

1. A goes to H to get tested for antibodies. Let the test result be $i$.
2. Let the test result be $i$.
3. H and A compute $i_{out} \leftarrow protocol_{DP}(i)$.
4. H computes and signs the value $i_{out}$ to form the certificate — $cert = \{i_{out}\}_{sgn_H}$.

### Check

1. A presents their certificate to V before accessing a service.
2. V checks the signature on the certificate is from H (verifies the certificate is valid) and records the value $i_{out}$.

### Aggregate

1. V find the frequency $f$ of each element of $I$ amongst the $i_{out}$ it has received
2. V debiases the frequency estimates as per Equation **??** to get an unbiased estimate of the the sum of the $i$

## 8.2 Evaluation: error and threat model

**Evaluation of error** The introduction of differential privacy means some error is introduced in the reconstruction of the underlying distribution collected by service providers.

**Evaluation of threat model** Our method here does not bind a user to a certificate, moreover the certificate value is someone meaningless on its own — it is only meaningful when aggregated. Therefore there is a decreased incentive for users to fraudulently obtain a certificate.

We now discuss two possible attacks to the proposed system.

- **Sybil attack** As certificates are bound to a user an adversary can flood the network with multiple identical valid certificates. While this Sybil-type attack is possible, we argue such an attack, while feasible, is unlikely as an adversary must corrupt a high percentage of users to use the same certificate.
- **Service providers track users** Certificates are still signed by the healthcare provider. Thus it is possible for a service provider to track a user by the signature value on their certificate. **Note this is an issue but not as bad as SecureABC.**

  it is possible that the User signature values could be used to determine behaviour over time. Risk expands with collaboration

## 8.3 Error in Aggregation

Assuming that every value submitted came from different people or duplicates were removed from the dataset the following estimates on the errors hold. The standard deviation of $\hat{f}$ is given by

$$\sigma := \sqrt{\mathbb{E}((\hat{f} - f)^2)} = \frac{\exp(\epsilon/2)}{\exp(\epsilon) - 1}\sqrt{\frac{k-1}{n}}.$$

The expected absolute error is then up to leading order

$$\mathbb{E}(|\hat{f} - f|) = \sqrt{\frac{2}{\pi}}\sigma.$$

An approximate 95% confidence interval, for the truth, is given be all values within $2\sigma$ of the output.

We have also verified our expected error experimentally, as shown in Figure 4, by simulating our protocol 100 times for each number of users ranging from 1 to 500.

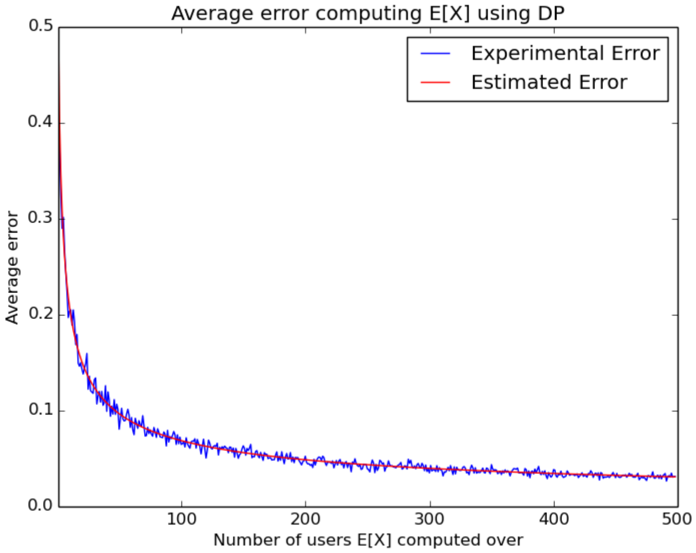

Figure 4: Experimental average error between the real antibody presence ratio and that which is recoverable after applying our DP protocol.

## 8.4 Threat Modelling

Here we draft our initial discussion relating to the potential threats and mitigations in relation to this system.

- **Lack of user-cert binding** Compared to SecureABC, there users are not strongly bound to their certificate using a photograph and name. Users may be incentivised to use fraud to obtain a certificate. An adversary may be incentivised to attack the system using many user certificates that have been stolen. Replay attacks might be a problem. We mitigate this by randomising the antibody certificate status, eliminating it's value as a currency for special access or freedom.

- **Testing distribution affects risk measurement** If governments are not motivated to uniformly at random test the population then the aggregated risk may be biased. It could be, however, that this system may provide an additional incentive for uniform testing so that the aggregate user antibody statistics are accurate.

- **Service providers track users** User signature values could be used to determine behaviour over time. Risk expands with sets of collaborating service providers. Healthcare provider signatures on certificates could also be misused to unfairly profile users. Anonymous credentials could mitigate this risk although they would also worsen the system's resistance to malicious users.