Open Identity Exchange

UK Government – Cabinet Office

COVID-Status Certification Review – Call for Evidence

March 2021

OIX Response

29th March 2021

Version 1.0

Author/Editor: Nick Mothershaw, Chief Identity Strategist
Email: nick.mothershaw@openidentityexchange.org
Mobile: 07885 618523

1 What is the Open Identity Exchange?

The Open Identity Exchange (OIX) is a community for all those involved in the ID sector to connect and collaborate, developing the guidance needed for interoperable, trusted identities. Through our definition of, and education on Trust Frameworks, we create the rules, tools and confidence that will allow every individual a trusted, universally accepted, identity.

Our Vision:
A world where we can all prove our identity and eligibility anywhere, using a simple universally trusted ID

Our Purpose:
To create a community for all those involved in the ID sector to connect and collaborate. Together we create the rules, tools and confidence to support the acceptance of universally trusted IDs and eligibility information

How we Achieve this:
We are uniquely dedicated to ID Trust. We are a membership organisation, offering education, information and collaboration around the topic of universally trusted identity. We bring together buyers of ID Services (reliant organisations or relying parties) with ID Service organisations such as tech vendors, consultancies, along with regulators and market influencers to work together to drive adoption of ID Trust.

Our papers and guides form the bedrock of Trust Frameworks that supports the creation and use of inter-operable, universally trusted identities.

OIX has a wide programme of events, thought leadership and working groups.

Through the OIX Guide to Trust Frameworks and associated Papers, members build an understanding of the wider ecosystem required tocreate and rely upon trusted identities. The OIX Directory explains where member services sit within this ecosystem.

OIX is a global organisation based in the United Kingdom. Members include: Microsoft, International Airlines Group, Sopra Steria, Barclays, Lexis Nexis, Experian, Thales, Trans Union, GB Group, Nat West Group, Forgerock, YOTI and numerous small to medium size identity services organisations and Trade Bodies.

2 About this Document

This response was compiled through a series of workshops with OIX members.

OIX's focus in this paper in on Legal and Operational / Delivery considerations for Covid Certificates. It extracts from an upcoming OIX paper on challenges for Covid Certificates.

3 Three Challenges for Covid Certificate delivery

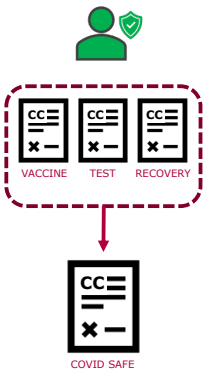
A Covid Certificate, in the context of this paper, could be a proof of vaccine, proof of test or proof of having had covid. The use of the word "certificate" is not intended to imply any particular technical solution. The word credential could have equally been used.

OIX sees three major challenges regarding the issue and presentation of covid certificates. These are essentially standard challenges for:

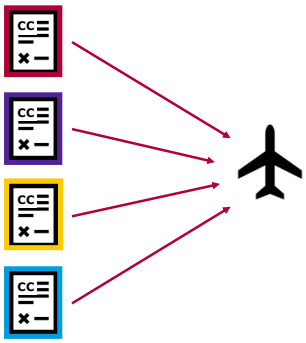
- the establishment of trust in a user and connecting certified data to them
- allowing the user to easily present this to an organisation that requires this information
- allowing organisation to receive information in a consistent format.

1. User Trust and Certificate Issue.
How to ensure the Covid Certificate is given to the person who received the covid vaccine or test

2. Certificate Collation and Status Determination
How to allow the user to collate together certificates to meet the needs of different organisations



3. Certificate Interoperability.
How to allow organizations to read different "flavours" of Covid Certificates issued by many different healthcare providers



A key focus of this paper is challenge 1, User Trust and Certificate Issue, as this seems to be the unsolved area in this space. For example, the European Union is leaving this challenge to member states to solve.

Challenge 2, Certificate Collation and Status Determination can be solved by allowing users to collate certificates from different issuers in a single "digital wallet" or against a single trusted Digital Identity. This enables the user to collate an NHS issued vaccine and a recent private sector Covid Test to prove to an airline they are safe to fly. The user can then present these as a package, or as a determined status such as "covid safe", to meet the needs of the organisation. Digital wallets could be issued for particular purposes, such as air travel in the case of the IATA Travel Pass, or be generic digital wallets that the user can use for many purposes.

Challenge 3, Certificate Interoperability, can be met by the definition of common data standards for the Covid Certificates and then either:
Determining a

a) single delivery protocol or,

b) implementing protocol translation services within organisations receiving covid certificates.

It does not seem like option (a) is likely as divergence is already occurring, so option (b) is most likely to be required.

In any event, to solve all the challenges a **Trust Framework** is required. The trust framework defines the roles and rules within a trust ecosystem. For instance:

- How is trust established in the user?
- How does a covid certificate issuer link the certificate to the correct user? This is often referred to a "binding"
- What data should be in the covid certificate? How is the data formatted?
- How can the user store and manage their certificates?
- How can the user collate certificates and present them to organisations?
- How are certificates delivered to organisations in a consistent manner?
- How can organisations trust the certificate is genuine?

As this is a global problem there will need be alignment between many collaborating global and regional trust frameworks. These are likely to fall into two types:

- Healthcare based trust frameworks for certificate issue. These will be regional.
- Sector based trust frameworks for organisational certificate consumption: Airlines, Events Venues, Employers, other Healthcare Providers. Both regional and global.

OIX is a specialist in Trust Frameworks and Interoperability and seeks to assist the UK Government in solving these key challenges in whatever way it can.

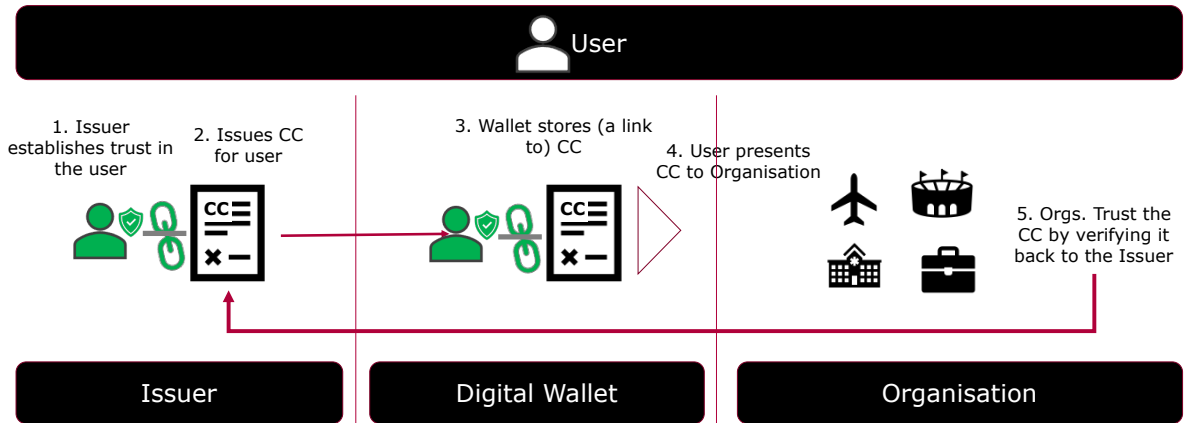
4 User Trust and Certificate Issue

User Trust can be established by two parties in a trust framework:

a) The issuer of the covid certificate
b) A separate trusted Identity Provider.

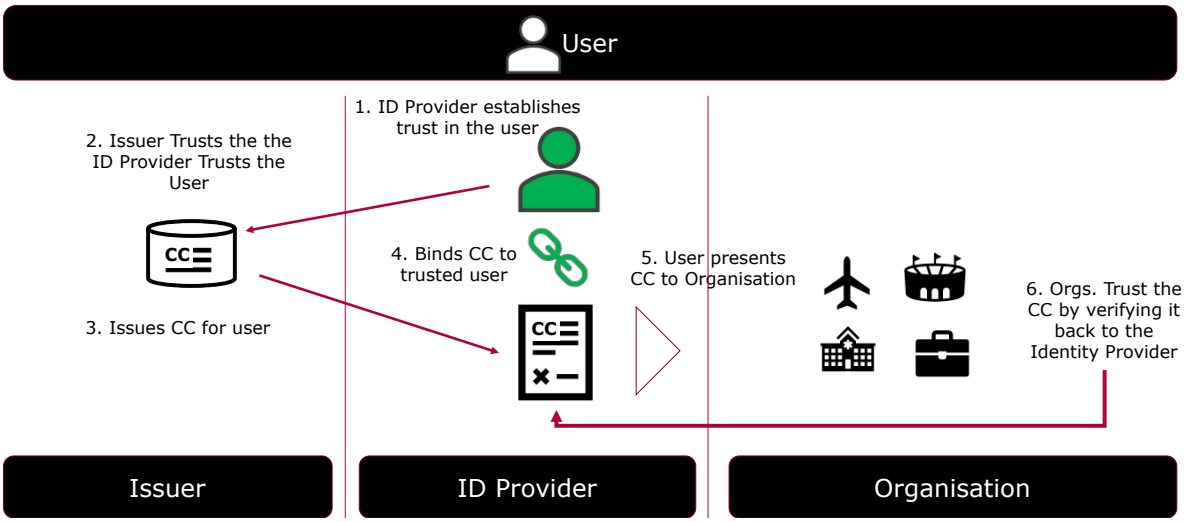
The organisation who then receives the certificate will need to trust that the Issuer or the ID Provider verified that this user is the correct user to be issued the certificate, depending on which scenario is implemented.

a) User Trust Established by the issuer of the covid certificate



CC = Covid Certificate

b) User Trust Established by and separate Identity Provider



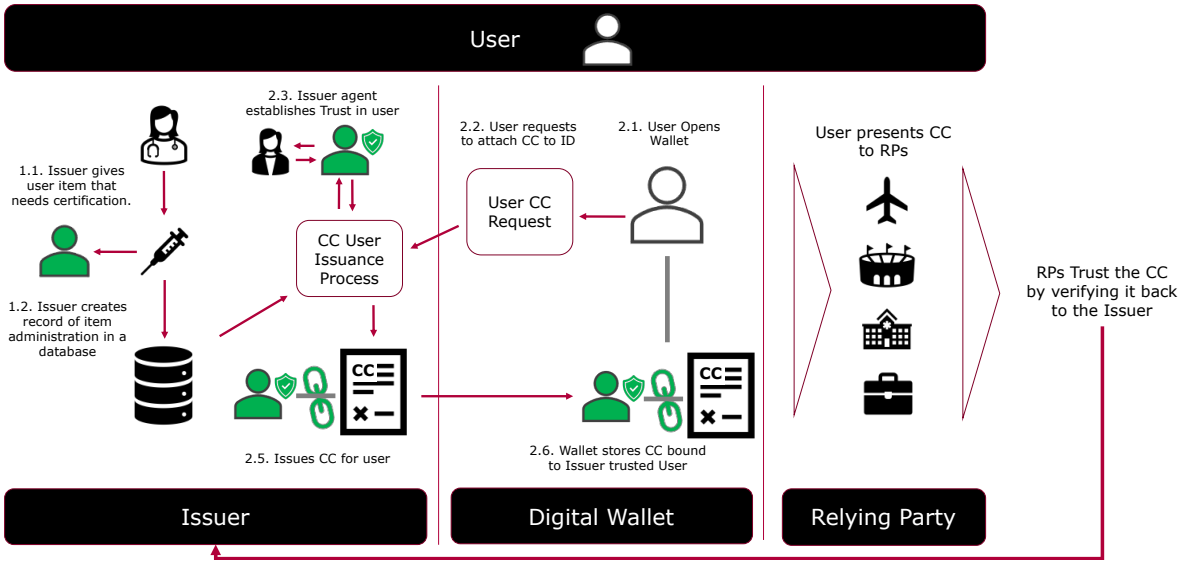
Option B requires a trust framework that supports separate ID providers. Thats is – separate from the issuers of the covid vaccine or test. This can be a government ID, such as in Estonia, or a third party trusted ID, such as in Canada or the Nordics.

The UK does not have a separate non-healthcare identity provider that could be used in this context. Until the UK Trust Framework is implemented this will remain the case.

The challenge for the UK is compounded by the fact that, at point of writing, 30 million vaccines have already been issued to UK citizens. So, associating a covid certificate for the vaccine at point of issue with a user's digital identity, or placing it in their digital wallet, is not an option.

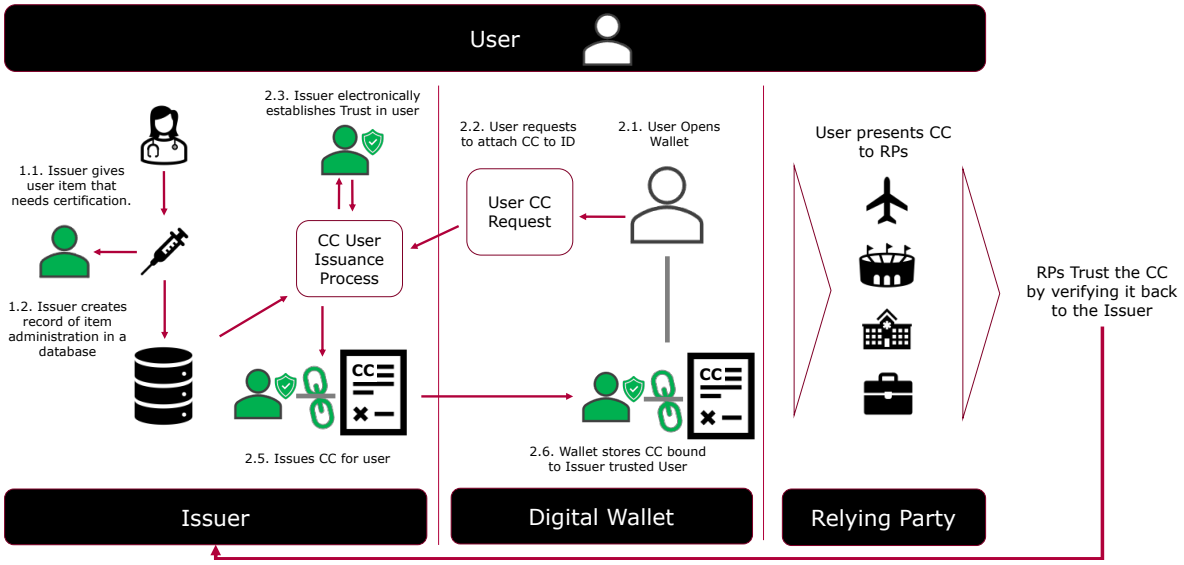
OIX has 5 different scenarios for covid certification issue that will appear in its forthcoming paper. However, given that the UK does not have separately trustable ID providers, and has already issued millions of vaccines, there is only one of these options the OIX can see working in the short term, with 2 derivatives:

Manual ID Proofing: The vaccine has already been administered and is stored in a database (the users health record). When the user asks for their certificate digitally, the healthcare provider Issuer manually ID proofs the user (e.g., by a doctor's receptionist) and then issues them with the Covid Certificate. The Covid Certificate is looked up using verified attributes provided by the user (e.g., name, Dob, Address) along with their NHS number. The Covid Certificate is linked to the users self-created ID wallet for them to present to organizations that need to see the certificate.



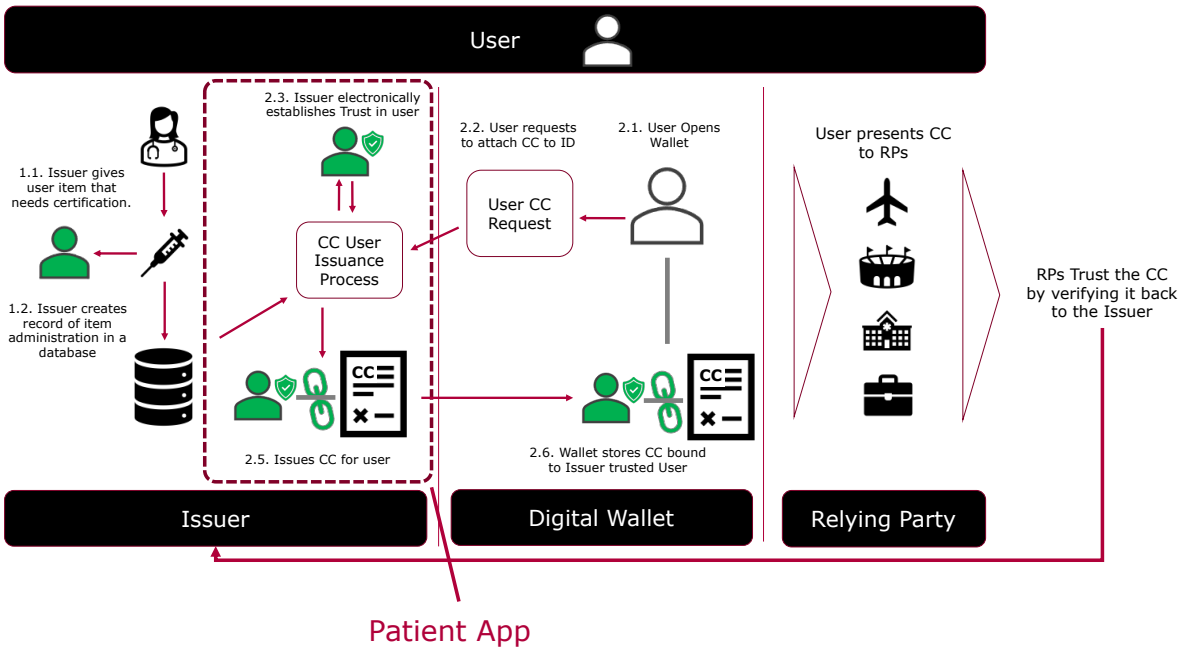
Electronic ID Proofing: The vaccine has already been administered and is stored in a database (the users health record). Healthcare Issuer electronically ID proofs the user and then issues them with the Covid Certificate. The Covid Certificate is looked up using verified attributes provided by the user (e.g., name, Dob, Address) along with their NHS number.

The Covid Certificate is linked to the users self-created ID wallet for them to present to organizations that need to see the certificate.

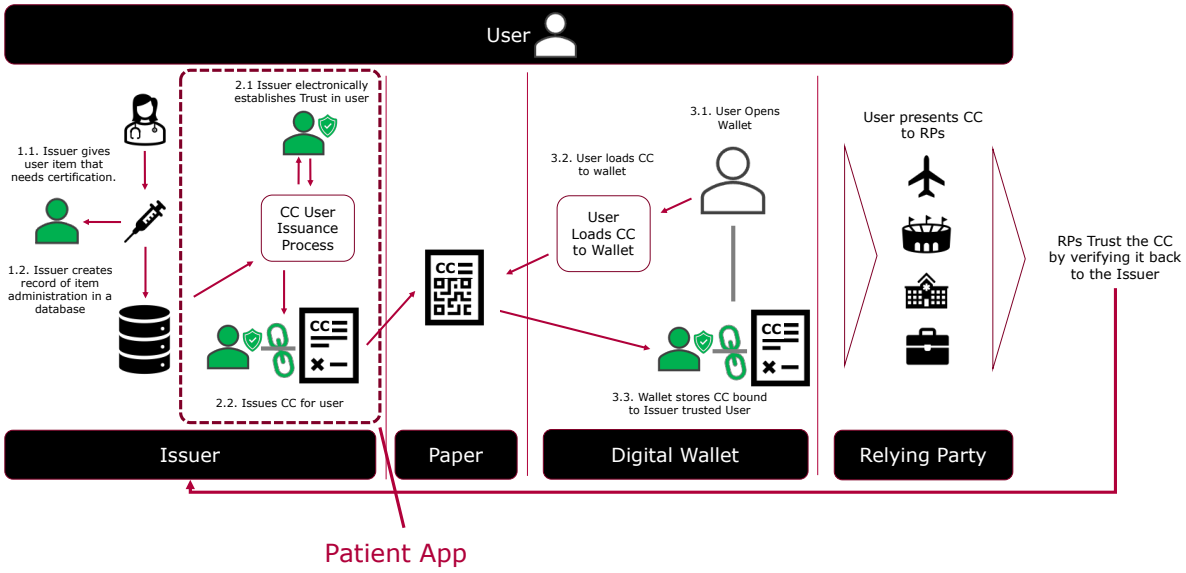


Clearly the manual option is not desirable due to cost and inconvenience but may be useful to support inclusion.

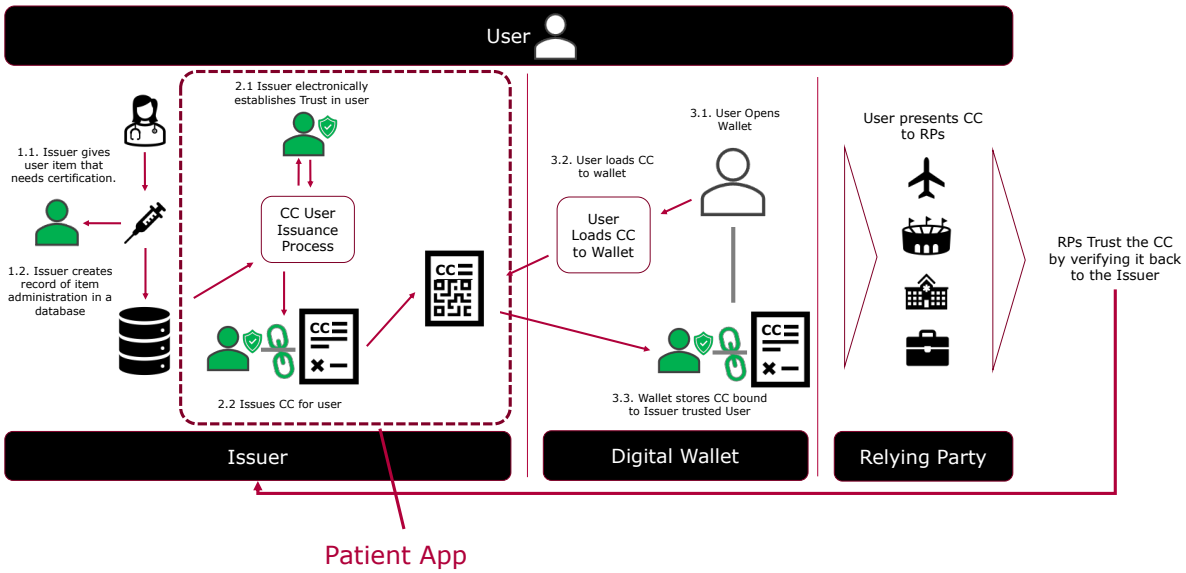
The second option involves the implementation of an electronic ID proofing process by the issuer – the NHS. Fortunately, the NHS has proxies for this today: GP patient apps systems, or the NHS app. These already establish trust in the user and so could be used as a way to issue the user a certificate that can be stored in the user's wallet and then collated with other certificates, such as private covid tests, to meet the needs of organisations:



The Patient App need not issue an electronic certificate directly into the user's digital wallet. A paper form of the certificate could be issued with a QR code that can be scanned by the user to create a copy of the Covid Certificate in their wallet:



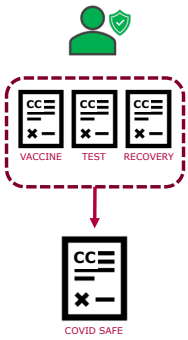
Equally, a QR code could be displayed on a screen in the Patient App to allow the user to create a copy of the Covid Certificate in their wallet:



5 Certificate Collation and Status Determination

Different use cases will require users to have different covid certificates. For example, an events venue may only require evidence of a vaccine, whereas an Airline may require evidence of a vaccine plus evidence of a recent negative independent covid test.

The user will therefore need gather several covid certificates together and present them to different organisations. The user can do this by managing them within a digital wallet or via trusted digital identity:



The digital wallet / identity should be smart. It should make the process simple for the user and the consuming organisation. If the consuming organisation simply wants to know the user is covid safe, the digital wallet / identity could make that determination on behalf of the organisation and issue results of its determination to the organisation. This requires that the organisation trusts the digital wallet / identity can make this determination properly and accurately – the digital wallet / identity provider must be part of the trust framework.

An implication of the wallet being smart and making determinations is that it must trust who the user is, either by proxy by using the trust established in the user by the issuers of the certificates, or independently through its own ID verification process. Which option is acceptable would be a matter for the trust framework to determine.

A “chain of trust” is therefore required:

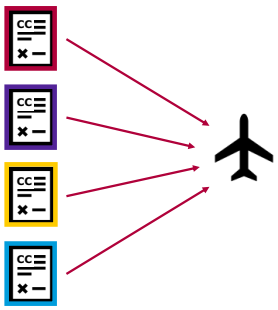
- The organisation trusts the digital wallet / identity to make determinations, such as covid safe on its behalf.
- The organisation trusts who the user is, based on trust established by the Digital ID provider, digital wallet provider or the issuer(s) of covid certificates.
- The organisation trusts the covid certificate is genuine as it comes from a bonafide issuer.
- The organisation trusts the covid certificate belongs to the user as it has been “bound” to the user by an issuer or a trusted identity provider.

To enable this chain of trust possible a Trust Framework is required.

The NHS would therefore need be part of this trust framework in the role of an Issuer of covid certificates as a minimum.

6 Certificate Interoperability

A key challenge will be how to allow organizations to read different “flavours” of Covid Certificates issued by many different healthcare providers:



Certificate interoperability comes in two parts:
1. The definition of common data standards for the Covid Certificates and then,
2. Determining and agreeing either a
    a) single protocol delivery protocol or,
    b) implementing protocol translation services within organisations receiving covid certificates.

In terms of a common data standard, this is vital. There is an existing ICAO Digital Travel Credential standard that could be extended. Also, the European Union eHealth network has defined the data attributes to be collected for vaccines, tests and proof of recovery. The World Health Organisation is pursuing a software neutral Smart Vaccination Certificate approach will focus on establishing key specifications, standards, trust framework for a digital vaccination certificate.

The UK Government should ensure the data content provided by the NHS is any covid certificates is to agreed international standards, and should be actively engaging with those who are seeking to set these standards.

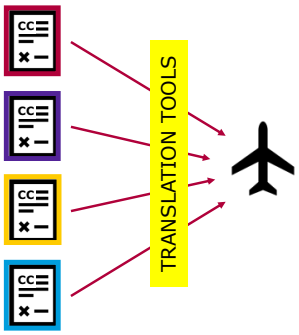
In terms of a single delivery protocol, it does not seem like option (a) is likely as divergence is already occurring, so option (b) is more likely to be required.

The EU is settling on traditional “digital certificates” for its Green Heath Pass, whilst most other global solutions, such as IATA Travel Pass and Good Health Pass, are focussing on the newer Verifiable Credential standard from W3C. This new standard however has several sub-flavours as it is in early stages of maturity.

If the result is several different “flavours” of protocol are acceptable and are in the market, protocol translation will be required.

When selecting a “flavour” of protocol, consideration should be given as to whether it can be operated digitally but offline: consider border staff, or events staff, who cannot rely on network connectivity at the point they need to read a covid certificate and verify its authenticity.

If protocol translation is done by the organisation receiving the credentials, then that becomes an adoption burden for them. They may need multiple ways for users to present credentials to them, at least paper and QR code electronic. They will then need protocol reading and data interpretation tools.



The problem of translation could be pushed to the digital wallet or digital identity provider. The organisation could insist that derived certificates at least are delivered to them in a protocol and format of their choice. However, if a digital wallet or digital identity provider is going to manipulate data before it is passed to the organisation, the rules for this must be agreed and followed; a trust framework is once again required.

7 Conclusion

UK Government, and the NHS, should consider the following:

- Issue citizens with digital covid vaccine certificates through existing technology: Patient Apps.

- Deliver data within the certificates in a recognised international standard format. International standards are still emerging – UK Government be part of their definition.

- Select a certificate protocol that will be internationally accepted and will work offline.

- Prepare to be an "Issuer" in a trust framework that allows the organisations to consume covid certificates or information derived from then. Be part of the chain of trust.

- Work with the identity industry, either directly or through OIX, to:

    - Determine use cases where covid certificates will be required.

    - Determine the rules for each use case. Or at least provide guidance. Private sector is calling for government guidance on this – abdicating responsibility to the private sector is going to result in slow take up and inconsistent citizen experiences.

    - Ensure users can get their covid certificates into their digital wallets or associated with a digital identity.

- Consider whether a specific trust framework is needed for use of covid certificates in the UK, for example entrance to venues or use in employment. Should the UK government put in place rules for the use of covid certificates and a trust framework to govern these rules?

- Whilst this document focusses on digital covid certificate delivery, machine readable paper based versions of certificates should also be able to be issued. These should be able to be digitised into a user's digital wallet or digital identity if the user wishes, to allow them to be easily presented to organisations.