Identity Binding

Introduction

For a health credential to be trustable at the point of presentation, the verifier must be able to determine the level of confidence that the presenter of the Health Pass is the legitimate subject of the Health Pass (i.e. is it really Jane Doe presenting Jane Doe's health status?). Identity binding describes the process for how the subject and the Health Pass are linked. This section describes the identity binding across three zones. These zones deal with identity disambiguation - that not all issuers will know all verifier's identity requirements - to enable a framework for trust in the actions of a 3rd party.

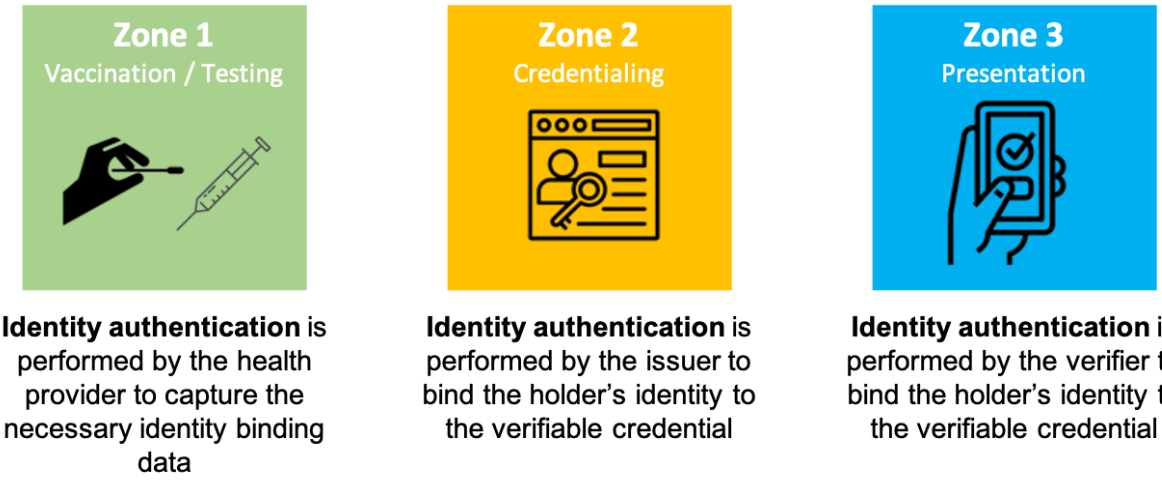


Figure 1: Identity binding and authentication zones in the Good Health Pass ecosystem

In Zone 1, the Good Health Pass ecosystem must be able to accommodate the complete spectrum of identity binding strength—from no identity binding at all (e.g., giving a free Coronavirus Disease of 2019 (COVID-19) test to a refugee) to authenticating a patient with full biometrics and an extensive Electronic Health Record at a modern hospital. The strength of this initial binding can be described through, what is called, the **Authenticator Assurance Level**. Levels of assurance are described in various national and international standards documents including: 1) ISO/IEC 29115, 2) Pan-Canadian Trust Framework, 3) eIDAS, and 4) the NIST 800-63 series. The latter establishes some of the most widely referenced standards for Level of Assurance (LoA) for identity proofing, the Identity Assurance Level (IAL) as described in NIST-800-63A and the Authenticator Assurance Level (AAL) described in NIST-800-63B. The document presented in Zone 1, typically a government issued document, has an **Identity Assurance Level** associated with it based on the corresponding identity proofing process undertaken at issuance (i.e., a Passport has a higher IAL than a Grocery Store Affinity card).

Identification is not needed to provide care, in Zone 1. The healthcare provider will undertake appropriate identity verification to adequately bind the event (e.g. vaccination or test) to the recipient in their records. Moving identity binding farther to the left increases the confidence and reduces the risk of fraud.

In Zone 2, which may be coincident with Zone 1, Good Health Pass credential issuers must perform identity authentication of the holder to a sufficient AAL [based on the destination country's rules - where applicable] prior to issuance of the credential. If Zones 1 and 2 are separated, it is incumbent on the process to ensure chain of custody - that the health information is bound to the correct individual. It is recommended that the Good Health Pass credential include identity document information and both the IAL of the document presented and the AAL achieved when authenticating the identity claim; i.e., identity binding.

In Zone 3, Good Health Pass credential verifiers validate the Good Health Pass credential by checking the Authenticity, Integrity, and Revocation status of the credential and then determining if the presenter of the credential is the legitimate subject of the credential. This can be done with virtual or physical identity credentials where the verifier may use biometric information in the credentials and may also review the issuers levels of assurance during the identity process to ensure that it meets the required IAL and AAL - if applicable.

Whilst tools exist to provide high levels of assurance, such as biometric authentication, it needs to be recognized that primary considerations for healthcare may make such tools difficult if not impossible to implement:

- inclusion and accessibility needs mean that low, or no tech solutions must work alongside high-tech means
- those with limited evidence of their identity must be served with equivalence to those with the strongest forms
- public health needs may require remote and self-administered testing to provide greatest impact and reach
- primary systems for recording data are established health systems that extend far beyond the purpose of a health pass service

This section of the blueprint positions the challenge and how risks can be mitigated or accepted by the development of standards that allow confidence in identity binding to be assessed by verifiers.

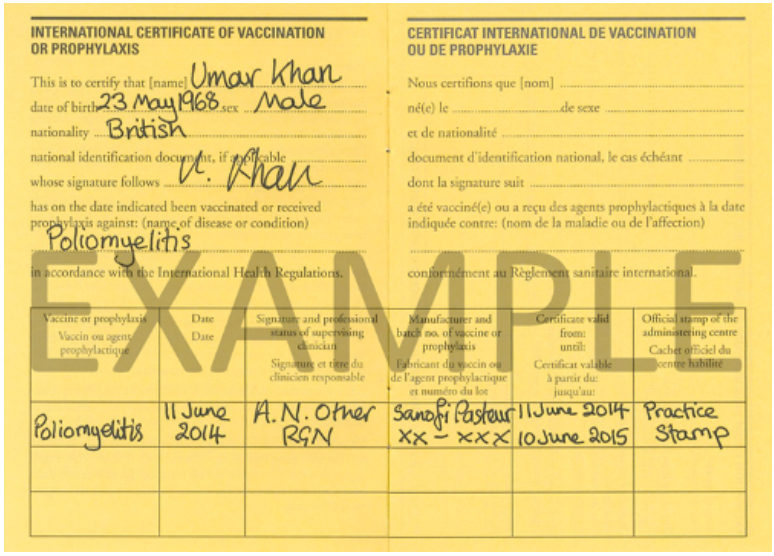
How the world works

During the COVID-19 pandemic, governments have implemented requirements for passengers arriving at their border to provide health information such as: vaccination status, or a negative result of a type of SARS-CoV-2 test within a given time period. For example, a polymerase chain reaction (PCR) Test meeting given criteria no older than 72 hours.

In this case, how the results are presented and how they are bound to the identity of the passenger can also be prescribed. This follows established standards from the International Health Regulations and the model for an International Certificate of Vaccination. The model certificate recommends binding to the identity of the individual by their name, date of birth, gender, nationality and national identification document. A passport or travel document number can also be added by the individual, though there is no requirement for this to be presented for checking.

https://apps.who.int/iris/rest/bitstreams/1031116/retrieve

The International Certificate of Vaccination, or Yellow Card, has been used for passengers arriving at a country's border by the identity data it contains being cross-referenced with the identity data contained on the passenger's passport. This is an example of two internationally recognised and accepted documents being used in concert to bind health data along with identity data and authorization.



INTERNATIONAL CERTIFICATE OF VACCINATION OR PROPHYLAXIS

This is to certify that [name] Umar Khan
date of birth 23 May 1968 sex Male
nationality British
national identification document, if applicable
whose signature follows U. Khan
has on the date indicated been vaccinated or received prophylaxis against: (name of disease or condition) Poliomyelitis
in accordance with the International Health Regulations.

CERTIFICAT INTERNATIONAL DE VACCINATION OU DE PROPHYLAXIE

Nous certifions que [nom]
né(e) le ..... de sexe .....
et de nationalité .....
document d'identification national, le cas échéant .....
dont la signature suit .....
a été vacciné(e) ou a reçu des agents prophylactiques à la date indiquée contre: (nom de la maladie ou de l'affection)
conformément au Règlement sanitaire international.

EXAMPLE

Vaccine or prophylaxis / Vaccin ou agent prophylactique	Date / Date	Signature and professional status of supervising clinician / Signature et titre du clinicien responsable	Manufacturer and batch no. of vaccine or prophylaxis / Fabricant du vaccin ou de l'agent prophylactique et numéro du lot	Certificate valid from: / until: / Certificat valable à partir du: / jusqu'au:	Official stamp of the administering centre / Cachet officiel du centre habilité
Poliomyelitis	11 June 2014	A.N. Other RGN	Sanofi Pasteur xx - xxx	11 June 2014 10 June 2015	Practice Stamp

Whilst for international travel it is perfectly reasonable to ask individuals to provide proof of identity - or more specifically their passport - before undertaking vaccination and issuing their certificate, the same is not true for general inoculations and more broadly access to health care provision.

Taking a high-level look at enrolment and authentication processes in the United Kingdom highlights how identity in healthcare operates today, and how COVID-19 vaccinations and testing are being addressed. It is important to note that other countries' health care systems work very differently. Identity binding for health passes needs to operate within these different constructs.

National Health Service – Patient Enrolment

Patients in the U.K. obtain first-line healthcare through a General Practitioner (GP). GP surgeries are private businesses contracted to the National Health Service through their local Clinical Commissioning Group. Patients are enrolled onto the list of their local GP surgery. Whilst GPs will often ask for proof of identity and address, there is no formal requirement for identity verification. Indeed, GPs cannot decline to register a patient due to a lack of proof of identity or address.

https://www.nhs.uk/nhs-services/gps/how-to-register-with-a-gp-surgery/

Once enrolled, when attending an appointment in-person, the patient will be required to confirm their name and date of birth. Again, there is no requirement for identity verification nor any authentication other than matching the self-asserted information with the patient record.

Why is this important?

- Vaccinations obtained in the course of public health programmes, such as the COVID-19 vaccination rollout, may have no demonstrable identity verification for some Users.

- Health Pass providers cannot assume Users have been rigorously authenticated at the point of care.

Digital Health Records

Patients are able to access online services such as:

- contacting their GP for advice and support
- ordering repeat prescriptions
- seeing parts of their health record, including information about medicines, vaccinations and test results
- seeing communications between their GP surgery and other services, such as hospitals
- booking, checking or cancelling appointments

There are two ways in which patients can enrol for access to online services.

1. They enrol for an NHS ID online by proving their ID using a government document – their verified data is then matched against their patient record, and they get credentials (username, password and mobile OTP) for future access.
2. They go via their GP who registers them for online access, making the link to their patient record and issuing them with credentials for access.

Why is this important?

- Credentials obtained from a health record should contain identity data that can be matched with the identity proofing undertaken by the Health Pass provider.

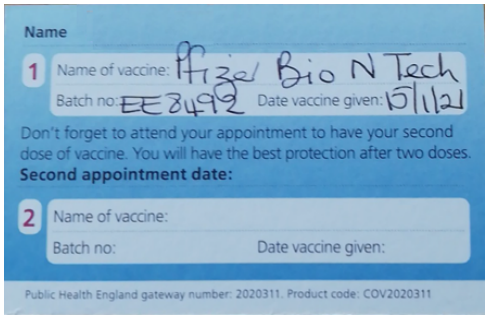
COVID-19 Vaccinations

COVID-19 vaccinations are offered for free, with rollout prioritising the most clinically vulnerable. Patients are contacted by their GP surgery as, based on their patient record, they fall into the priority grouping being called forward on a national basis. Once invited, patients register either online or by phone giving their details to match to their patient record. Vaccinations are being provided through:

- local hubs covering multiple GP surgeries
- mass vaccination centres
- satellite locations in premises such as pharmacies

This means that for the majority of patients, they will be vaccinated somewhere other than the GP surgery they are registered at.

The NHS has produced a COVID-19 vaccination record card which is issued to the patient when they attend for their vaccination. The card acts as a reminder for their second appointment for a two-dose regime. It is not intended to be used as evidence of being vaccinated. The name of the patient is the only identity binding on the record. The name of the vaccine given, the batch number and the date given is recorded.



As well as being provided with the physical card, the details are electronically recorded against their NHS patient record.

Why is this important?

- The use of identity tools provided by Health Pass applications should not expect to be included within a public health care process.

- Proof of vaccination may be obtained from the health care systems post the point of treatment.

COVID-19 Testing

Public Health testing is available through an online or phone booking system. This is available through a network of testing centres offering drive-up or walk-up service, additionally home testing is provided by post. In areas with surges of cases or where new variants are of concern, testing with no prior appointment is also available. Patients applying online must provide their name, plus a mobile number to receive their results. An email address is also required for a home testing kit. Public Health testing is not to be used for activities that require proof of a negative test.

Why is this important?

- Public health testing should be assumed to be for the identification of positive cases rather than proof of a negative test. Therefore, the requirements for identity binding may not be of primary concern should a credential be issued.

Testing for proof of a negative result for international travel purposes is provided by the private sector. Governments have published criteria for providers of these tests to develop “Trust Lists” that passengers must obtain their test results from.

https://www.gov.uk/guidance/self-declare-as-a-private-sector-covid-19-testing-provider
https://www.cdc.gov/coronavirus/2019-ncov/travelers/testing-international-air-travelers.html

These private sector providers offer both in-person and at home testing services. The personal data required varies from provider to provider. Some require only limited contact information, name and email, where others also request passport details.

Why is this important?

- Health Pass providers may need to provide the ability for private sector testing providers to authenticate the User (e.g. by securely displaying a photo, name and date of birth of the User) of the Health Pass.

- Private sector health providers may need to align their own identity proofing and authentication processes, where used, with those of the Health Pass providers.

- Health Pass providers may need to support the use of identification evidence related to the use case for which the credential is being obtained (e.g. a Passport for a travel use

case, a proof of age card for a hospitality use case, matching attributes such as name and age for an event use case).

- Health Pass providers may need to support facial biometric binding to the individual where the technology requirements allows to include those without provable identity.

Coronavirus testing before you travel to England

International arrivals to the UK are required to complete a Passenger Locator Form.

Passengers are required to have proof of a negative test result. This proof can be in the form of a printed document or an email or message that can be shown on a phone. The test result must be in either English, French or Spanish. Translations are not accepted.

The original test result notification must include the following information:

- your name, which should match the name on your travel documents
- your date of birth or age
- the result of the test
- the date the test sample was collected or received by the test provider
- the name of the test provider and their contact details
- confirmation of the device used for the test, or that the test was a PCR test

https://www.gov.uk/guidance/coronavirus-covid-19-testing-for-people-travelling-to-england

Why is this important?

- Health Pass providers should be able to meet the identity binding policy of the use case for which the health credential is being used.

What do we mean by interoperability and why is it important?

To achieve global interoperability, ecosystem partners must either all agree on what data is required, how it is interchanged, how it is secured, and how it is to be used (as was done by ICAO and its members for Passports) or, because different countries, regions, or other jurisdictions may have differing requirements, there must be a way for them to publish their requirements so that others can obtain country-specific requirements and process accordingly.

In the case of identity binding requirements, countries may specify minimal IAL and AAL which would need to be known prior to receiving health care so that the subject can bring the requisite identity information and the health care provider / issuer can perform the requisite identity authentication and binding - and record it in the Good Health Pass credential.

In order for identity binding to be interoperable the process used by the Heath Pass providers for health credential must be available to and understandable to the Verifier.

Zone 1: Identity authentication of the user to obtain the identity data needed for the identity binding

As we have seen from the example of the United Kingdom, the identity authentication of the user is varied within the health care process itself. Whilst the application of a high assurance, robust identity assurance process may be desired by the Verifier as the beneficiary of the health credential, this may not be in the best interests of the health care provider or the patient. It would be exclusionary and against the needs of public health to require patients to present a passport in order to access testing or vaccinations.

Where testing or vaccination is being sought specifically for the purposes of international travel, as a passport is a requirement of the use case, concerns over exclusion are mitigated should the Health Pass provider make this a requirement.

Why is this important?

- Health Pass providers must fill the gaps of identity binding in public health care processes for the fulfilment of private sector use cases.

- Health Pass providers may support no or low identity and authentication provided that this information is conveyed to the Verifier.

- The requirements of the Verifier should, where known, be accounted for in the Issuance process particularly where the health credential is being obtained for that purpose.

Zone 2: Authentication of the user to the identity binding in order to issue the credential

Having performed identity proofing of the User; e.g., the passport issuing authority, authentication is then used to establish the health credential is being issued to the correct User. Health care providers may issue the credential using technology integrated in to the Health Pass provider (e.g. a QR code scanned by the Health Pass application), via SMS or email, via the health care systems (e.g. digital health records), or using paper records.

This chain of custody for the vaccination or testing process needs to be accounted for. The level of authentication assurance will vary depending on how the health process is administered. Identity authentication, undertaking the vaccination or test, and issuance of the credential could all be conducted in an uninterrupted process. The person administering the vaccine in the patient's arm being the identity authenticator and credential issuer creates a tightly controlled process with limited scope for the credential being issued to the wrong subject.

With home testing, strong identity authentication could be required in order to obtain the test kit, though the chain of custody for who the kit is used on is far weaker. Without remote supervision being used for the entirety of the process, there is scope for fraud to occur. This can be mitigated to some degree by requiring authentication of the user to accept the test kit. For example, using possession of a mobile device as an authentication factor so that the results of the test are only issued to a specific device.

The use of multi-factor authentication with a biometric factor of a facial match to the photo from a passport may be desirable for an international travel use case. Consideration should be given to the required technology to do this. This could be facilitated by a User with a smartphone or requires investment in technology by Issuers and Verifiers for Users with low or no tech requirements.

It should be recognized that the issuance of the credential need not occur at the time of the health process being undertaken. As described in the U.K. example, a record of vaccination may exist within the health system. A patient should be able to access their own health record and obtain a credential as proof of prior vaccination.

Why is this important?

- Health Pass providers may need to match the identity data from its own proofing process with identity data in a credential obtained from a health system.

- Health Pass providers may need to account for the chain of custody in the information presented to the Verifier in order that they can implement their own risk mitigations.

Zone3: Authentication of the user to the identity binding in order to accept the credential

The level of assurance associated with authentication against an identity document with an IAL commensurate with the verifier's requirements and an irrefutable chain of custody for the vaccination or testing process provides useful information for the Verifier. Being able to determine what has occurred from the point of health care be provided and the issuance of the corresponding Good Health Pass credential enables the implementation of business / operational policy within the Verifier domain. Additional risk mitigations and where suitable, risk acceptance, can be used to supplement the steps undertaken by the Issuer.

Leveraging the authentication used to issue the credential at the time of presentation can ensure that the subject of the credential is known and can be trusted. In one implementation, if the Issuer has established multi-factor authentication with a biometric factor that is bound to the User, the Verifier can require the User to authenticate through the same means in order to prove they are the subject of the credential. An alternate option can use the identity information bound to the credential to match with their own data or the additional presentation of an identity document. For a travel use case, this could be the passenger named on the boarding card or the details of a passport.

Why is this important?

- Health Pass applications should allow the Verifier to understand, to the extent possible, what identity binding has occurred in Zones 1 and 2.

- Verifiers should expect to fill gaps in the identity binding process, particularly for no/low assurance and no/low technology implementations. For example, manual cross reference of the health credential with a physical identity document at the point of acceptance.

The purpose of identity binding and how it can be achieved

Identity binding is the ability to link the presenter of an identity claim to the claim itself. In the context of verifiable health credentials this is typically done when:

1. **Issuing an identity credential**. In many instances this is a government function where an identity proofing process is used to:
    - Resolve a claimed identity to a single, unique identity within the context of the population of users
    - Validate that all supplied evidence is correct and genuine
    - Validate that the claimed identity exists in the real world
    - Verify that the claimed identity is associated with the real person supplying the identity evidence

The way in which the identity proofing process is conducted is often categorized by the **Identity Assurance Level (IAL)** which relates to associated identity fraud which may be acceptable by relying parties. Refer to NIST 800-63A Section 4.7 or ISO 29115 Section 6.5 for examples of Identity Assurance Levels.

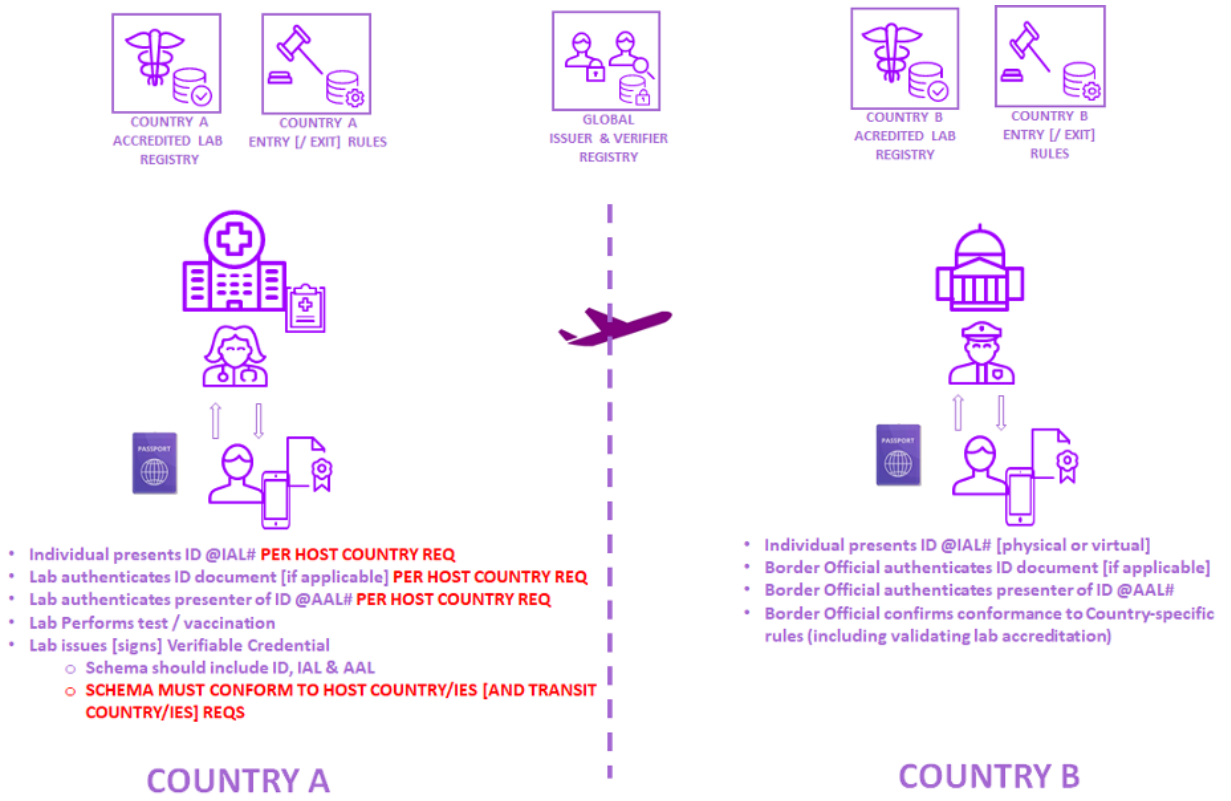
Identity credentials with relatively high Identity Assurance Levels are National ID cards and Passports where identity proofing is done in-person, typically with biometric identifiers to deduplicate within the population, and breeder documents are source-checked. Conversely, shoppers' affinity cards are very low (IAL). The acceptable IAL for an identity credential is a business decision based on the risk appetite of the relying party.

2. **Presenting an identity credential** to receive a service. In the context of verifiable health credentials, this may be at the point of vaccination or test, the border crossing point, at an employer's facility, at an educational institution, etc.

The viability of the verifiable health credential relies on the accreditation of the issuer AND their ability to authenticate the identity of the subject to the level required by down-stream verifiers.

Authentication, like identity proofing, has varying levels of assurance depending on the methods used, in this case **Authenticator Assurance Level**, the strongest of which are the best at minimizing identity fraud. Refer to NIST 800-63B Sections 4.1, 4.2, and 4.3 or ISO 29115 Section 6.5 for examples of Authenticator Assurance Levels.

Authentication processes with relatively high Authenticator Assurance Levels are in-person (or remote supervised), may include one or more biometric, may include one or more cryptographic devices. Conversely, a 4-digit PIN corresponds to a relatively low (AAL). The AAL best suited for authenticating an identity claim is a business decision based on the risk appetite of the relying party.



A typical scenario, as depicted above, has a subject (passenger) arriving at the vaccination or test facility where they are asked to prove their identity. The passenger may present a Passport, A driver's license, a Health ID, etc. The relative trustworthiness of the credential provided (as quantified by the associated IAL) is described above.

In a high-risk environment, the authenticity of the credential presented is determined using various means (optical, visual, electronic, etc.).

The next step in the process is to determine if the presenter of the identity credential is the authorized holder of the credential. An example in a high-risk environment would biometrically match the presenter to the cryptographically authenticated photo contained in the credential. In any event, the relative trustworthiness of the authentication process (as quantified by the associated AAL) is described above

Recommendations for Stakeholders

Regulators

(Governments)

- **Establish acceptance policy for identity proofing and authentication:** take measures to ensure that Users are not excluded due to a lack of provable identity or access to technology when defining requirements for presentation of health credentials

Standard Bodies Organizations (SBOs) / Industry Groups

(WHO, ISO, W3C, VCI, Linux PH, ID2020, ToIP, DIF, IATA, ICAO)

- **Set data standards for identity binding:** ensure that identity proofing and authentication is part of the credential data definition
- **Set data standards for personal data:** ensure that Good Health Pass providers can match the User whose identity is authenticated by them with the subject of a credential issued by the health care provider
- **Set data standards for chain of custody:** so that issues that cannot be dealt with by identity binding (such as home testing) can be accounted for

Issuers - Public

(Public health providers)

- **Include identity information of the subject:** comply with data standards for health credentials issued to Good Health Passes

Issuers – Private

(Private health providers)

- **Align their own identity processes with Health Passes:** utilise identity processes provided by or aligned to those of the Good Health Pass providers
- **Include identity information of the subject:** comply with data standards for health credentials issued to Good Health Passes

Verifiers / Buyers of Health Pass solutions

(Airlines, Airports, Border Controls)

- **Set risk mitigation policies:** understand the complexities for issuance of health credentials and the variations in the level of confidence they can take from identity binding
- **Check Identity Binding:** in compliance to the requirements of the governing trust framework

Everyone

- **Commit to identity binding requirements:** outlined in this blueprint
- **Consider risks:** consider identity risks in granularity - what documents were provided, which authentication process was used, etc.
- **Collaborate on policy:** to mitigate risk and reduce fraud from the system

Recommendations for Providers of Health Pass solutions

In understanding the way that the world works, it becomes clear that identity binding is primarily a concern of the providers of Health Pass solutions. There is no single solution to this if Health Passes are to be inclusive. It must be recognised that:

- Health Care providers, particularly in the public health domain, cannot present unjust barriers based on a patient's ability to prove their identity, or their access to or capability to use technology

- Access to health care is the primary concern, ability to provide proof downstream is secondary. This may create undesired circumstances for the Verifier of a Health Pass credential that they will have to mitigate. Health Pass providers need to give them the information to enable them to do so.

- There is more ability to influence Identity binding for health credentials obtained for the specific purpose of the Verifier use case – for example obtaining a COVID-19 test prior to international travel.

Providers of Health Pass solutions should implement identity proofing and authentication to perform identity binding between the credential and the Holder of the Health Pass. The use of facial biometric authentication can provide a useful foundation from which identity binding can be layered as required for the use of the Health Pass.

Health Pass providers need to operate with the health care system, not the other way round. This means that they will have to fill gaps in identity proofing and authentication undertaken in the healthcare domain through innovative controls in their own domain. They can fill these gaps by providing matching of identity data from their own proofing process with the identity data received from the health care systems.

Recommendation 1

Implement identity binding into Health Pass solutions by offering identity proofing and authentication capabilities to fulfil variations and gaps that exist in health care providers and Verifiers across the three Zones described.

Recognition is needed that solutions requiring higher end-technology needs to interoperate with low or no technology solutions at the Issuer and Verifier ends of the

journey. The same is true for solutions that provide higher standards of identity proofing and authentication, these must equally interoperate with low assurance implementations.

Lower assurance identity binding may require the Verifier to take additional actions, such as cross referencing the identity details of the subject of the health credential. Solutions leveraging tools such as smartphones, document verification and biometric facial matching can provide a more seamless Verifier experience. Health Pass solutions offering this three-way binding between the User, their identity evidence and the health credential are desirable, though need to allow for interoperability with more simple Health Passes, including those utilising paper as the means of presentation.

Recommendation 2

Provide Verifiers with information on the identity binding that has taken place. Allow Users to step-up from no or low levels of identity binding as required to meet the needs of the use case they require proof for.

Health Pass providers can also offer tools and services to the health care provider, such as the ability for the user to show or share their verified identity details in an easy to integrate way. Similarly, they also need to provide ease of integration into the Verifier systems.

Health care is a multi-provider domain. Health Pass providers need to ensure that identity binding is implemented consistently across the industry so that Issuers in the both the public and private health care sectors and Verifiers in all sectors can reliably utilise whichever Health Pass solution a User presents.

Recommendation 3

Collaborate on identity standards for Health Passes so that there is consistency on the presentation of the level of confidence that a Verifier should take from the identity binding performed.

Appendix

Term	Definition
Identity Authentication	The process of providing assurance about the identity of an entity interacting with a system
Identity Proofing	The process of verifying the claimed identity of an applicant by authenticating the identity source documents and information provided by or obtained in relation to the applicant.
Identity Binding	The process of associating credentials related to an entity and their verified (to a given level of assurance) identity. It's purpose is to link the presenter of an identity claim to the claim itself.