Getting Ready for Digital Identity

OPEN IDENTITY EXCHANGE

CONTENTS

1.

Introduction

Today, users end up repeating the same process again and again with each organization they deal with resulting in 100s of separate IDs

This model has a number of challenges for both users and the organization they are dealing with:

User Challenges	Organization Challenges
100s of usernames and passwords	Forgotten authenticators lead to loss of customers and high recovery costs
Verification is undertaken again and again with each new organization	Cost to maintain own tailored ID verification and management solutions
Millions of ID documents are lost every year	Organizational impact of losing ID documents or data
User are victims of ID fraud as IDs are stolen	ID Fraud is high and growing

Leads to complex onboarding journeys which result in abandonment

Is there a better way of doing this? **Yes - a Digital Identity!**

A Digital Identity enables a user to provide trust in their identity and information to any organization.

A user can have a single trusted Digital ID that they can use with many organizations

The Digital Identity has the following advantages for users and organizations:

User Benefits	Organization Benefits
Single set of authenticators	No more forgotten authenticators - Improves returning user rates
Can more easily provide each new organization the ID and Eligibility information they need	Reduces onboarding costs
Can use a single ID to access different organizations when they deal with them again	Reduces user management costs
Removes risk of lost documents	No need to handle and store user ID documents
In control of their own identity and information	Opportunity for broader digital engagement and services with customers

Reduces Abandonment and Identity Fraud

Digital Identity aims to replicate the presentation of a user's passport, ID card or similar in the physical world but online. Just as in the physical world organizations will rely on the visual inspection of a document, a digital Identity will allow a service provider to achieve the same in an online engagement.

The difference being, that by using a digital identity, the user and services provider can gain benefits performing engagements with each other from the digital world. Such benefits can be:

- Faster more convenient transactions
- Safer transactions
- Lower costs of transactions

To realise these, and other benefits online, a digital equivalent of the physical world's traditional identity documents and data needs to be created. This creation process will tap into authoritative sources and physical documents for checking against agreed standards. This activity can be carried out by an organization who creates Digital IDs to a known and approved standard. These standards define the trustworthiness of the checks and allow an organization to 'rely' on the digital version of the identity in the transaction.

2.

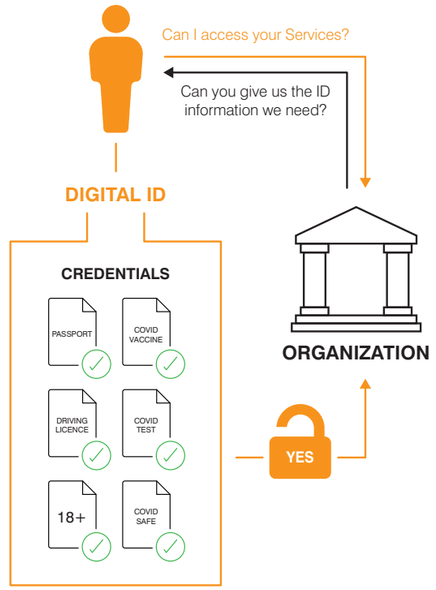
I What is Digital ID?

A digital identity:

- is a collection of digital credentials that have been verified. Credentials can include identity credentials, such as an ID card, passport or driving licence, and eligibility credentials such as education certificates, covid tests or covid vaccines records.
- should use a recognised standard to verify evidence of an identity presented by a user in an online verification cycle.
- might derive information from users credentials, such as the user being 'Over 18' or 'Covid Safe' that the user can share securely.

The Digital ID can use a number of methods to gather credentials such as direct access to the credential issuer, document scanning, selfie capture, chip reading in documents, biometric matching. In some cases documents and data captured can come from or be checked against the issuer where this service is available. For example, today UK passport validity can be checked with the HMPO. US driver licencing authorities are starting to issue digital "mobile driving licences", and digital covid certificates are being issued to users by governments and health providers.

Once basic information on a user is captured this can be used to obtain further information on the user from online data services such as credit reference agencies, electoral regististers, births and death registers, court judgements etc. During the cycle of creating a digital identity the set of credentials that are required to meet an identity standard can be collected together, and if the collected evidence is checked in accordance with the standard, the Digital identity might create derived credentials and further attest that the checks have been performed by them to the relevant standard.

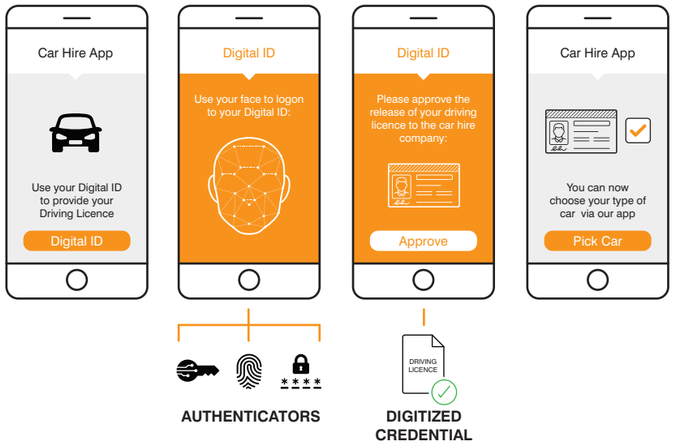


Once this identification cycle has been completed by the identity provider the user can use their digital identity in transactions where the user is requested, by an organization, to present their digital identity containing their credentials. Moreover, the user can then use their Digital ID with many organizations without the need to go through ID proofing again and again.

- A Digital ID is a set of verified digital Credentials.
- Examples of Credentials include:
  - Digitized real world credentials: Driving licence, Passport, Vaccine Certificate
  - Derived Credentials: Over 18, Covid Safe

The simplest use of a Digital ID is to provide a Digitized version of a real-world Credential, such as a passport, driving licence, covid vaccine or qualifications.

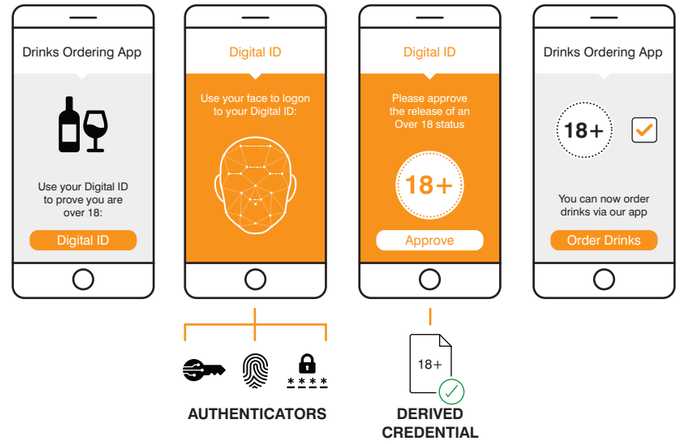
The example below shows a user sharing their digitized driving licence with a car hire company:



Authenticators such as biometrics, passwords or devices are used to identify the user as the owner of the Digital ID.

The driving licence Digitized Credential must have been verified as belonging to the user when it was associated with the Digital ID.

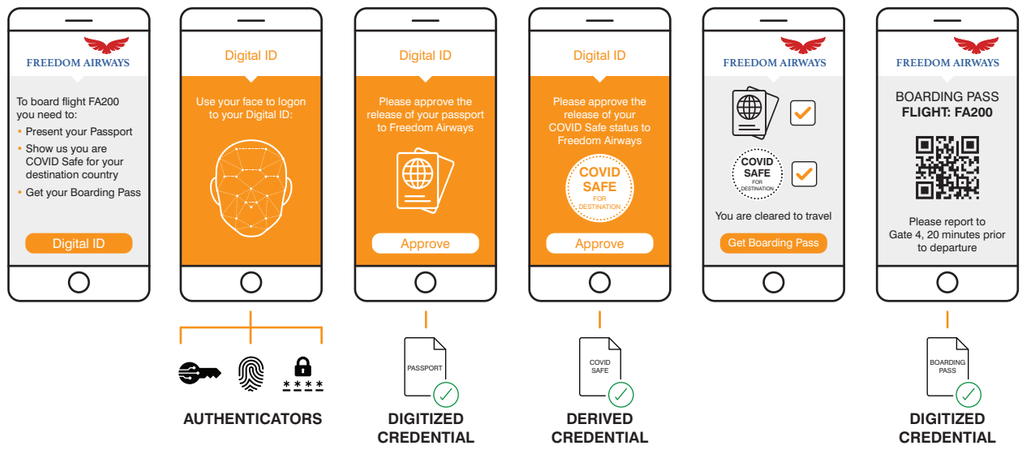
The Digital ID can also derive credentials about the user. For example, the fact that a user is over 18 can be derived from the user's driving licence to prove the user's age. There is no need to share the whole driving licence data and unnecessarily disclosing the user's address:



The Digital ID needs to know the rules required to meet an organization's ID needs. For example, to determine the person is over 18 the Digital ID must do so from a government issued ID document, verified as belonging to the user and accessed by strong authenticators.

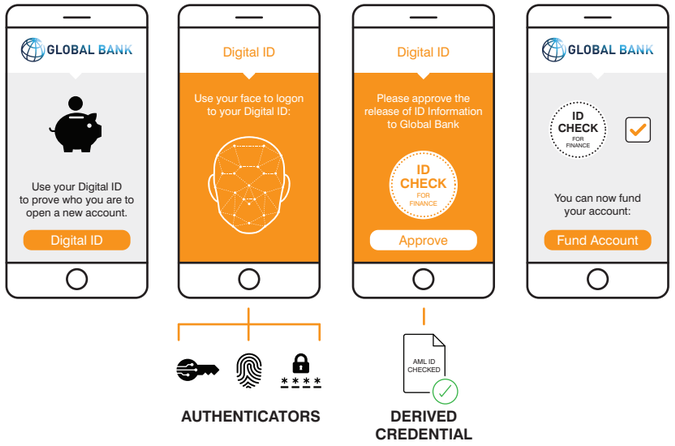
Another example of a derived credential is a Covid Safe status. The rules for Covid Safe vary by use case. They may require the user to simply be vaccinated, or they may also require them to have had a recent test of a specific type.

Our example below shows select screens the user checking in to board a flight might use:

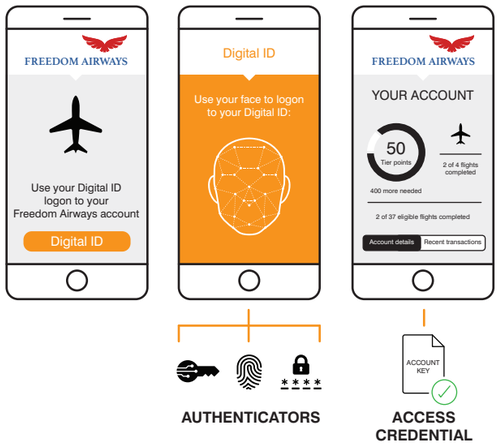


The Digital ID provides the user's passport, a Covid Safe status to the required rules and then also allows the user to store their boarding pass as a new digitized credential.

These rules can be sophisticated. Digital ID ecosystems often define levels of trust for a user, known as Levels of Assurance. These are essentially complex derived credentials. For example, the complex rules required for Anti-money laundering ID proofing can be defined as a Level of Assurance. The example below shows that despite this being a complex process from the Digital IDs and organization point of view, from the user point of view it can be very simple, allowing quick and easy access to services:



Finally, the Digital ID can also be used to allow users to access an account with an organization again and again. The organization relies on the trust and the authenticators established in the users Digital ID, saving the organization having to issue and manage its own authenticators (e.g. passwords) to the user. Here we see the user logging in to their airline app using their Digital ID:



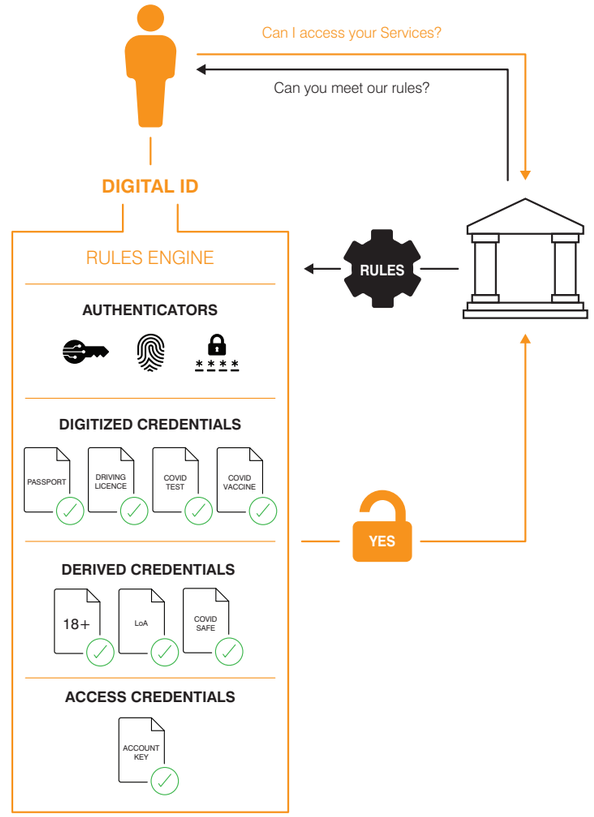
Putting that all together results in a Digital ID that can allow users to confirm who they are, and share other important information about themselves, to many different organizations who they want services from.

The Digital ID works out what a user needs to meet an organizations business rules using a rules engine, and helps the user gather, derive and present credentials to meet the organizations needs.

A Digital ID can carry digitized versions of existing credentials, such as a passport, driving license, vaccine certificate or relevant qualifications.

It can also derive credentials that show users meet the business rules of an organization, such as being over 18, COVID safe or meeting a specific “level of assurance”.

Organizations can also choose to allow users to use their Digital ID to access an account they hold with you. Thus, removing the need for you to issue your own logon authenticators (e.g., user IDs and passwords).



As an organization, you choose which of these Digital features to access and use:

- Digitized Credentials
- Derived Credentials
- Access Credentials

Organizations can use Digital IDs in several different ways:

Method of Use	Purpose	Digital ID Features Used
One and done transactions	To determine eligibility and access users data.	Digitized Credentials Derived Credentials
Opening an account for a new user	To determine eligibility and access users data.	Digitized Credentials Derived Credentials
Re-access to an account	Using the Digital ID’s authenticators instead of issuing your own authenticators.	Access Credentials
Ongoing eligibility	A user is still eligible for services, or are they eligible for new services.	Digitized Credentials Derived Credentials

Some organizations might only use a Digital ID to ensure they know who the user is and what they are eligible to do. Others might only use it for re-access to accounts. Many organizations might use it for both.

3.

How will the Digital ID market work?

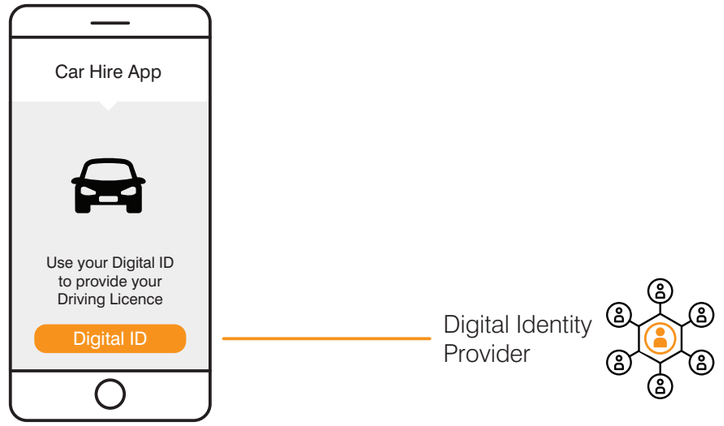
In some countries there will be a single Digital ID issued to all users by the state. States such as Estonia and India have already gone down this route. Many US states are now issuing their users with Digital driving licenses as a form of ID.

In many other countries, such as the UK, a market of private sector Digital ID providers is being established. The user will choose a Digital ID provider based on factors such as:

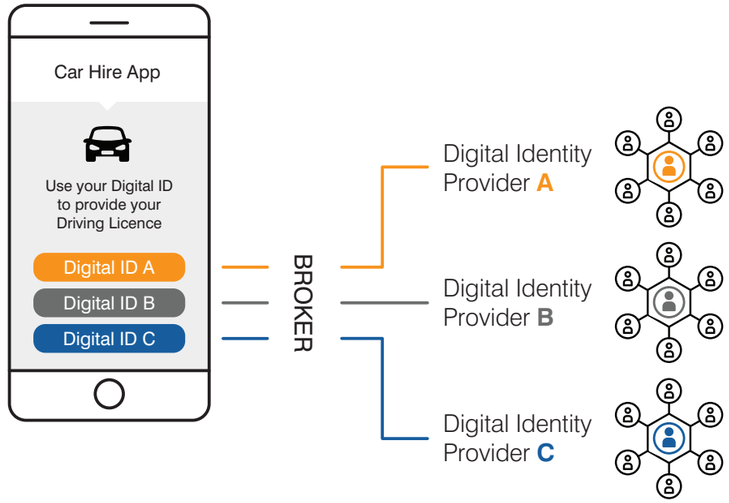
- Where they can use this Digital ID i.e. which sectors and how many organizations can accept the Digital ID
- Services they receive from the Digital ID
- Brand of the Digital ID provider

This approach ensures the user has choice in their Digital ID provider and also control of their data. ID Data is then also not stored in a single central database.

It may be that one Digital ID provider can give you access to a critical mass of users and data to meet your needs:



In order to access a sufficient number of Digital IDs to obtain good user coverage, you may choose to connect to multiple Digital ID providers:



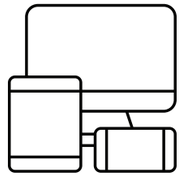
This may sound like an integration and commercial nightmare, but that is where standards come into play. When there are multiple Digital ID providers in a market it's vital they all offer consistent technical interfaces and minimum levels of service. Standards are usually enforced through a governance mechanism referred to as a Trust Framework. OIX is a specialist in Trust Frameworks and we will explain more about them in a later section of this document.

Commercially, ID Brokers are likely to be present in the market, providing a single commercial access point to many Digital ID providers, along with technical integration services.

4.

Why now is the time for Digital ID?

To make Digital ID a reality, various factors need to come together in a perfect storm. That storm is now on the horizon.

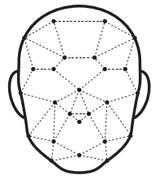


Shift to Digital

During the 2020/21 pandemic the requirement to perform services remotely was clearly demonstrated. Users were confined but needed to continue business, living at home and contacting family and friends. This brought increased demand on existing online services and created the need for new ways of working to ensure economic and social continuity. As users were driven into new online channels, some for the first time in their lives, the need for smooth engagement with new customers was, and remains, imperative.

As the registration cycle is front and center of the ‘first time engagement’ phase of a user using a service, if it is smooth and easy to use the user will return. This benefits both organizations and users.

Using a solution that allows rapid and trusted identification of users will lubricate the rails in the shift to digital.



Biometrics maturity

Today there are many organizations that have developed biometric solutions which can be deployed in many services. These solutions vary in capability from those used by law enforcement agencies, deriving evidence admissible in court, to those used for simple device access. Biometric solutions are able to provide a unique identification of an individual but does not provide an answer to who a person is. Today when users register a fingerprint to a phone, it is self asserted to the device and device account but this is not checked against a source that can state that any given fingerprint belongs to ‘Joe Smith’. Digital ID will enable a person’s biometric to be verified as belonging to them and then to be safely used to prove who the user is. Digital ID biometrics do not need to be tied to a single device and can support multiple different types of biometric. Biometric accuracy has now reached a level of maturity that means they can be reliably used, to the extent that standards are now available that ensure robust and ethical management.

Use of digital credentials

Alongside biometrics the creation of digital credentials allows for data from the physical world to be made digital (digitized) and for other digital data to be derived such as age from a date of birth. Further additional data from other digital sources can be associated with the individual as evidence of their identity. A Digital presentation of a passport would provide an organization with the same data presented in a passport whilst also including decryption of the passport issuer’s key and therefore enhance the trust in the passport credentials. Covid vaccination certificates are being made available as digital credentials which the user could store in their Digital ID. The user could then simultaneously present their passport and covid status to board a plane. Some countries are now issuing digital versions of driving licenses which users will be able to associate with their Digital ID. We expect that digitized credentials will have equal legal status to their paper equivalents.

Regulatory readiness

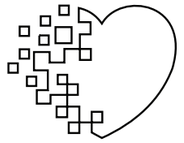
As the remote or digital engagement with customers has increased due to the 2020/21 pandemic the need for current regulations in industry sectors to be updated to allow Digital IDs to be relied on in transactions has been highlighted. This was evidenced in 2020 by the UK Money Laundering Regulations which were extended allowing organizations to use digital identities in their processes for identifying and ensuring that customers are real. The EU has just extended eIDAS to require member states to accept Digital IDs as equivalent to paper IDs for a whole range of use cases. In the US the Improving Digital Identity bill is being progressed. In the UK, the government is creating a Trust Framework for Digital ID and Attributes.

Technical standards

In technology, standards underpin the interoperability of different vendors' products and services. Mobile phones illustrate how technical standards allow a phone maker to sell a phone to work in almost any country and connect it to a network. The same objective prevails for Digital IDs. Any Digital ID created, in accordance with an accepted technical standard must be able to be used, in accordance with a governance standard such as a trust framework, by any relying party with confidence. Governments and industry bodies, such as the OIX, have developed standards for Digital IDs. The UK, US and EU governments have all defined guidelines or standards for identity proofing and authentication. These are currently evolving as the needs for all participants are fully understood.

Government Frameworks

Government issued trust frameworks are established to indicate to industry how digital identity should operate and what the roles and expectations of the actors in the framework can expect from using Digital IDs. Frameworks for Digital IDs are a set of rules and standards that different organizations agree to follow. This includes legislation, standards, policies and Good Practice Guides (GPGs). Governments around the globe are defining trust frameworks for Digital ID, including EU, UK, Canada, Australia and India.



Sector adoption

The adoption of Digital IDs will progress at differing rates in different sectors determined by the benefits of their use. These benefits will range from improved costs for services, safer services and faster transactions. During the summer of 2021 Digital IDs were being used in the home buying and selling process where a property buyer establishes a Digital ID and uses it to prove their identity to all the organizations involved in the buying cycle, such as mortgage brokers, estate agents solicitors etc. This saves time and obviates the need for home buyers to provide the same information many times. Similar projects are exploring the use of Digital ID with finance, pensions, employment vetting, age verification, payments and education. With a Digital ID created for one purpose, it is an easy step to use that ID in other sectors where the trust in the Digital ID generated can be transferred.

Race to invest

As Digital IDs become more widely used to deliver the benefits discussed, organizations are competing to provide or manage a user's digital identity as a way of increasing engagement with their products and services and are investing to achieve this dominance.

Apple's use of TouchID and FaceID have driven the social acceptance of biometrics and, as a result, these biometric credentials are increasingly being used by third party organizations as an authentication option for their own services. Apple's investment in owning ID is demonstrated by their increasing number of patents in this area. Other players that are investing to be at the center of the ID eco-system are telcos, tech giants, banks, governments and disruptors so as to be well positioned to benefit from the growth in the usage of Digital IDs.

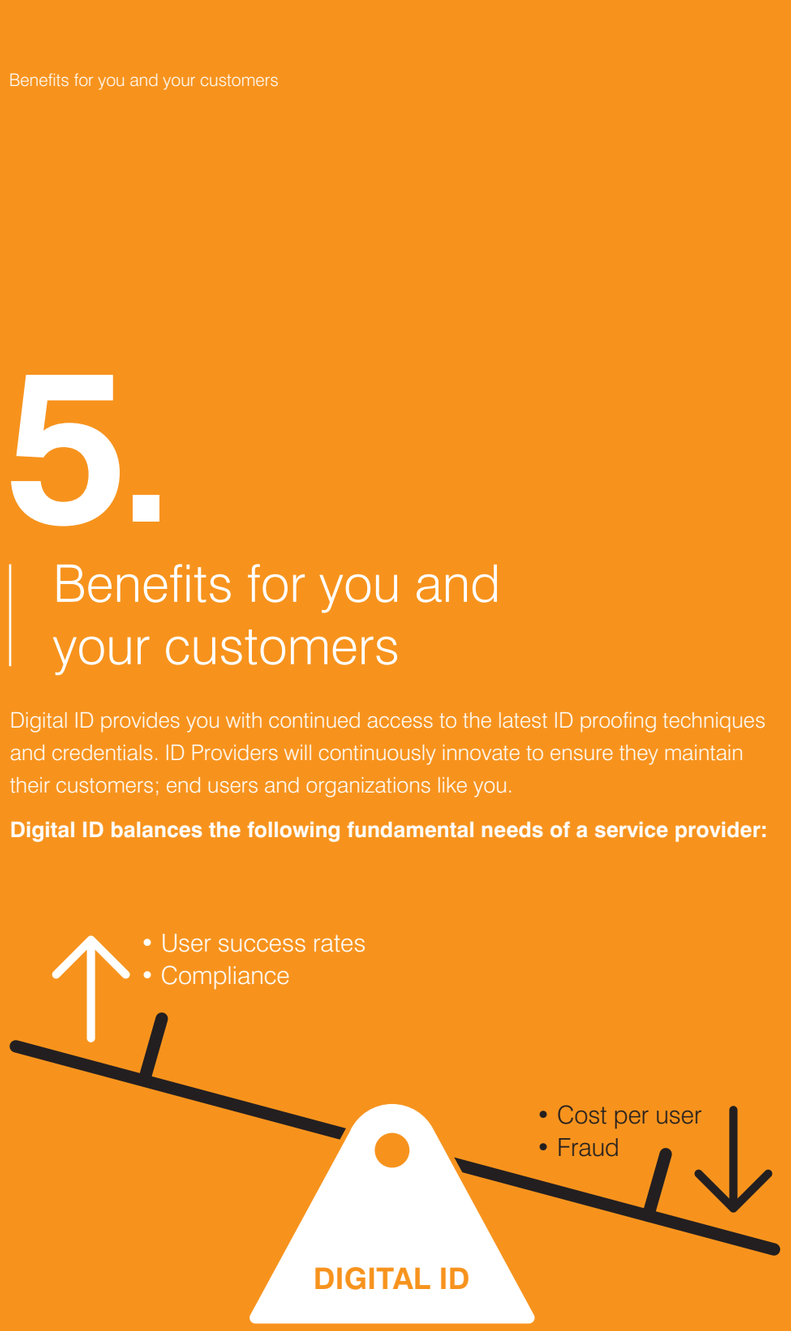
The Canadian Government's use of bank ID to login to services and the Scandinavian BankID service are live services showing the appetite for banks to dominate this space. As in all technology ecosystems there will be disruptive organizations with innovative technology and business models aiming to capitalise on the digitisation of businesses and the need for trusted identities as part of this process.

5.

Benefits for you and your customers

Digital ID provides you with continued access to the latest ID proofing techniques and credentials. ID Providers will continuously innovate to ensure they maintain their customers; end users and organizations like you.

Digital ID balances the following fundamental needs of a service provider:



There are a number of key stakeholders in your organization who need to buy into the adoption of Digital ID. They are the people responsible for the key performance indicators that Digital ID will improve:

			Key Stakeholders			
Benefits of Digital ID	How does Digital ID help?	£ Benefit?	Customer Acquisition and Retention (Sales / Product / Marketing)	CFO / Fraud Manager	CRO / Compliance Officer	Operations
Digital UX Success Rates – Onboarding	Increases	Yes	Yes	-	-	Yes
Digital UX Success Rates – Returning	Increases	Yes	Yes	-	-	Yes
Identity Fraud	Reduces	Yes	-	Yes	-	-
Improved Compliance	Increases	-	-	-	Yes	-
Compliance Cost	Reduces	Yes	-	-	Yes	Yes
Cost per User	Reduces	Yes	Yes	-	-	Yes
Time limited services involving people / call centres	Reduces	Yes	Yes	-	-	Yes

Building a business case for adoption will be based on the projected achievement of these benefits. It will be important to understand your current measures for the above and set a realistic benefit target for each area that Digital ID should improve.

In addition, any Digital ID implementation must also satisfy the following organizational stakeholders:

Supporting Stakeholder	What they need from Digital ID
Security	Industry standards, encryption, cyber security, strong authenticators
Technical	Ease of integration and maintenance
Legal	Liability, Record Keeping, Redress, Data Protection
Operational Risk	Audit, MI, Risk and Data Management

But most importantly, why is Digital ID good for your customers?

With a Digital ID your customers:

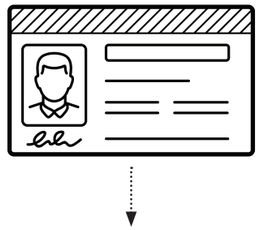
- Gain instant access to your services
- Move away from forgettable passwords
- Do not have to find and provide you with paper ID documents
- Only provide you with the data that you need
- Can easily share updates with you when their data changes

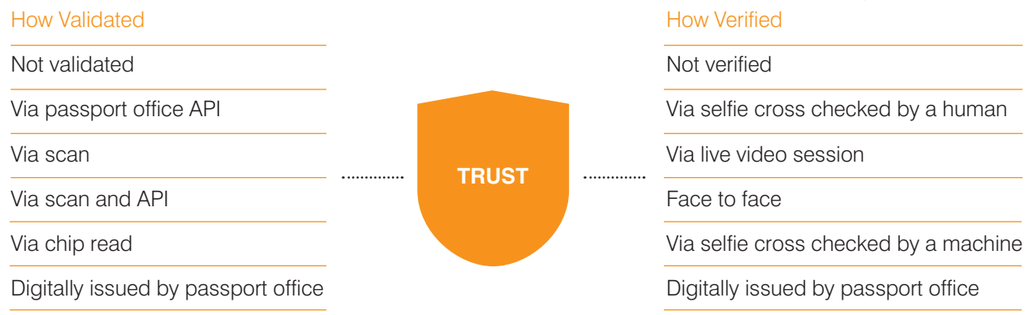
6.

Trust Frameworks - ensuring a Digital ID meets your rules

It's important that organizations receive the right information from a Digital ID to meet their rules for dealing with individuals. These rules might be internal risk based rules, or they may be rules set by your regulator.

For example, if you are going to accept a digitized passport as a form of ID, how was the digital version of the passport created?





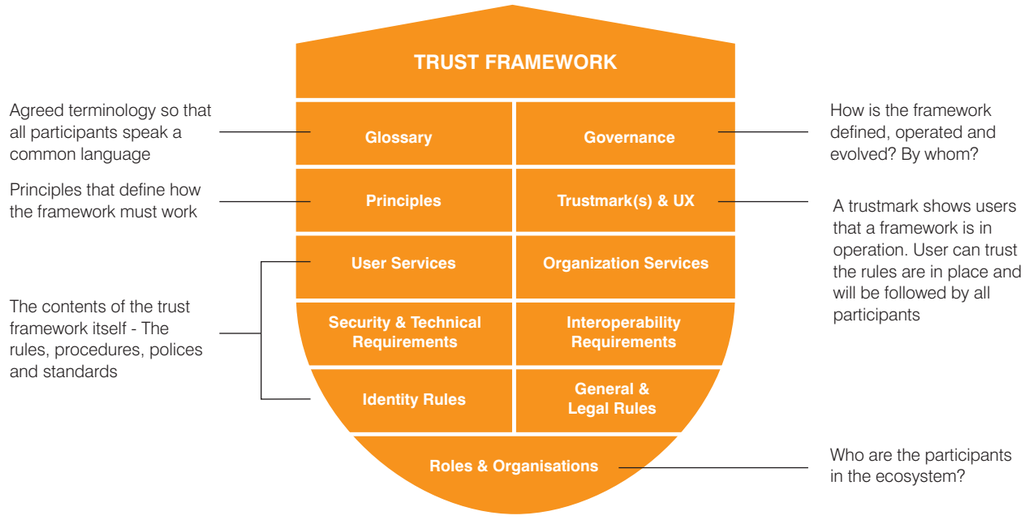
Different methods of validating the passport and verifying it belongs to the user result in increasing levels of trust that the passport is genuine.

This principle applies to all forms of credential:

- How was it validated?
- How is the credential verified as belonging to the user?

You must be confident that a Digital ID is working to the rules you require. This is part of the role of a Trust Framework and Trust Schemes.

A Trust Framework will set the rules for Digital ID. Not just the credential validation and verification rules, but legal, technical, operational and governance rules too:



Trust Schemes will then add extra rules to the framework for specific geographies, sectors and use cases. For example a scheme might define specific rules for COVID Safe for Travel or Age Verification for Online Services. Look for Schemes that support your specific area of business and the rules you need to follow.

What should a good trust framework do for you, as the consuming organization of IDs?

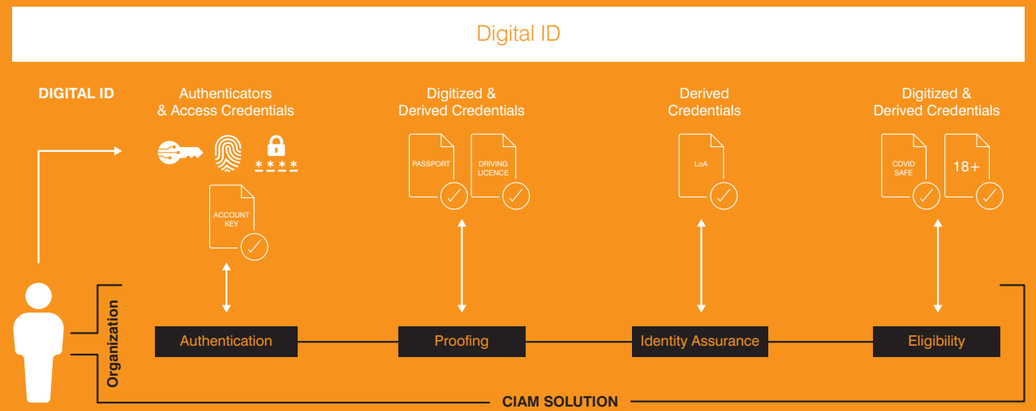
Feature	Highlights
Confidence in Users	Users are validated and verified to a level that you can trust to allow them to access, and re-access your services.
Critical Mass of Users	Provide access to millions of users with trusted IDs.
Users can be confident you are a genuine organization	One of the features of the trust framework is a verifiable 'trustmark' that allows users to be sure that you are a legitimate organization. This makes organization impersonation more difficult.
Manages ID Fraud	The rules of the framework should ensure ID fraud is defended against by all parties, so your fraud numbers decline.
Eligibility Information	You should be able to receive more than just proof of who the user is. You should also be able to receive trusted information about the user, such as financial or education information.
Inclusion	Provide access to more ways to digitally proof users, supported by Assisted Digital and Vouching within the Digital ID ecosystem.
Support and Redress	If there is a problem with an ID, or the service from an Digital ID provider, there should be support; from Helpdesk all the way through to Redress.
Deliver data in a single format	Where there are many Digital ID providers in a market, the framework should ensure you receive the same data from each different ID provider. Including the credentials you may need as evidence to support your processing.

Trust Frameworks will usually certify participants, such as Digital ID Providers, as being compliant with the framework and therefore permitted to show a Trustmark. The framework will make clear to certified parties what the consequences will be if they breach the rules of the framework. Certified parties may be held liable for losses incurred as a result of breaches of rules, and may even have their certification removed as a result.

7.

How does Digital ID integrate into your processes?

As discussed there are a number of different ways a Digital ID can be utilised by an organization. This will affect how the Digital ID is integrated into your systems. The example below shows the touchpoints between a typical Customer Information Access Management (CIAM) solution and a Digital ID.



You might simply use Digital ID as an access mechanism to your accounts, in which case it integrates into your authentication modules

You might use Digital ID to collect credentials, such as a passport, driving licence or the results of data verification APIs to use in your own ID proofing processes, and make an Identity Assurance - user trust - decision yourself.

The process of determining whether you can trust a user might be outsourced to the Digital ID, creating an integration point at your Identity Trust decision point. The Digital ID provider will provide you with a level of assurance.

FInally, you could use Digital ID to determine not (just) who the user is, but what they are eligible to do. Can they access elements of your services, such as are they COVID safe or are they over 18.

8.

What can you do next?

- Join OIX as a member to influence how Digital ID evolves to make sure it meets your current and future needs.
- Is there a Scheme in your sector? If not, Start one!
  OIX can help bring together expert organizations in your sector to start adoption of Digital ID.
- Talk to suppliers in the Digital ID Market.
  The OIX Directory lists members and their services categorized by type of service.
- Understand more about Trust Frameworks.
  The OIX Guide to Trust Frameworks explains the content and objectives of a trust framework and is the gateway to a series of guides on the more detailed framework elements.
- Respond to government consultations and calls for help. Either through OIX or directly.
- Get involved in pilots.
  Trust Frameworks and Schemes are looking for innovative first adopters who see the benefits of being first to market with Digital ID for their users.
- Undertake a proof of concept.
  Many Digital ID providers will offer free trials. See the OIX Directory.
- Follow OIX on Twitter and LinkedIn for ongoing updates.

OPEN IDENTITY EXCHANGE

Open Identity Exchange UK Europe
Suite 1, 3rd Floor
11-12 St James's Square
London SW1Y 4LB

Email: info@openidentityexchange.org
Web: openidentityexchange.org