OIX OPEN IDENTITY EXCHANGE

Trust Frameworks for Smart Digital ID

An OIX Guide | March 2022 | Version 1.1

Produced by:

Nick Mothershaw, with the input of the members of the
Open Identity Exchange Trust Framework Working Group

OPEN IDENTITY EXCHANGE

The Open Identity Exchange vision is a world where we can all prove our identity and eligibility anywhere, using a simple universally trusted ID

We 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

We are uniquely dedicated to ID Trust. We are a membership organization, offering education, information and collaboration around the topic of universally trusted identity.

We bring together buyers of ID Services (reliant organizations or Relying Parties) with ID Service organizations such as tech vendors, consultancies, along with regulators and market influencers to work together to drive adoption of ID Trust.

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

OIX has a wide programme of events, thought-leadership and working groups. Members access a suite of resources including support for Pilot Projects and Business Case Development.

Contact:

Nick Mothershaw, Chief Identity Strategist

nick.mothershaw@openidentityexchange.org

DOCUMENT HISTORY

Version	Date	Key Changes	Author
0.1 BETA	July 2020	First issue	Nick Mothershaw
0.2 BETA	February 2021	Update to bring principles in line with new guide	Nick Mothershaw
0.3	September 2021	Updated BETA to first release post working group feedback	Nick Mothershaw
1.0	January 2022	Updated to Version 1.0 after extensive enhancement to support SSI and Rules Engines.	Nick Mothershaw, Richard Thompson
1.1	March 2022	Updated SSI alignment section with simplified introductory diagrams	Nick Mothershaw

CONTENTS

1 INTRODUCTION

The guide is designed to provide an expert view on what a ***Trust Framework*** to enable Smart Digital ID should look like, by detailing its salient components: the principles, content, roles and responsibilities.

It builds upon the OIX 2017 paper "Trust Frameworks for Identity Systems", which attained worldwide acceptance; becoming a benchmark guide used by global organizations defining rules and standards for trust. This new guide incorporates lessons learnt from existing national and international frameworks including eIDAS in Europe, Verify in the UK, the PCTF in Canada and Aadhaar in India.

OIX provides comprehensive, practitioner informed descriptions along with real-world examples of all the potential components in a trust framework by defining it within the following context:

- Principles and ***Trustmarks***
- Trust rules (e.g. ***Proofing, Authentication, Identity assurance***)
- User services (e.g. Consent, Multiplicity, ID creation)
- Organizational services (e.g. User access, Liability, SLAs)
- General and Legal rules (e.g. Data Management, Record Keeping, Fraud Controls)
- Security and Technical Requirements (e.g. Schemas, Chain of Trust)
- Governance (e.g. ***Certification***, Enrolment, Operations)
- ***Interoperability***

Additionally, it defines and details the roles and responsibilities within a framework, outlining the functions, input and outputs of each party within the framework. This is critical for potential new entrants to determine how they can participate, contribute to, or derive the most benefit from a trust framework.

The guide is intended to provide a clear guide to trusted identity and ***Attributes*** for both users and organizations, in line with the OIX mission to present the human end of identity as opposed to a solely technical viewpoint. To this end, the guide is technology agnostic providing the neutrality to allow providers of trust frameworks to implement frameworks in accordance with their own specific technical needs. The trust framework presented in this guide is suitable for the governance of both decentralised and centralised ID ecosystems, including those supporting federation of IDs.

In the context of this guide a Digital ID could be for:

- An individual acting in their personal capacity
- An individual acting on behalf of an organization.
- A thing that is controlled by an individual or an organisation.

For all the above scenarios a User controls the Digital ID. Sometimes the user must be involved every time a Digital ID is used. Other times, for example for the Digital ID of a thing, users might only be involved to set up and manage the thing on a more occasional basis with the things Digital ID acting on its behalf the rest of the time.

This guide describes Digital ID in the context of users controlling a Digital ID that is asserted to an organization that consumes the Digital ID for the provision of products and services.

It is recognised that there are Digital ID solutions which create Digital IDs that identify an organization. This allows an organization to assert their 'organizational Digital ID' so that individuals can trust an organization, enabling them the be sure of the entity they are transacting with.

It will allow regulators to comprehend the relevance of trust frameworks when defining appropriate regulations for areas such as anti-money laundering.

As stated above, this guide draws on previous OIX work on trust frameworks, in particular:

Paper	Date Published	Authors
Trust Frameworks for Identity Systems	Jun 2017	Esther Makaay – SIDN Tom Smedinghoff - Locke Lord LLP Don Thibeau - Open Identity Exchange
Establishing a Trusted Digital Identity Ecosystem	Oct 2019	Ewan Villars, Innovate Identity

The identity community uses a plethora of specialist terminology. In order to try and standardise the vernacular OIX has created a separate Glossary of Identity Terms, including common synonyms.

How is the guide being evolved?

This guide links to further, more detailed, reference guides on the previously mentioned topics. These reference guides will detail what needs to be accomplished in order to deliver the high-level contents and what considerations need to be given to ensure the success and interoperability of any resulting trust framework or scheme.

2 WHO IS THE INTENDED AUDIENCE?

The guide will be of use to a broad audience:

- **Individuals (users)** - explains how trust frameworks can provide them with portable, re-usable, ubiquitous identities through the focus on interoperability between trust frameworks which will allow individuals to use their trusted digital identities and attributes across sectors and borders. The framework emphasises that Digital IDs need to understand the rules of complex processes and help the users through those processes; the Digital ID must be smart. This guide is not intended to provide an end-user explanation of trust frameworks, but should enable expert users, with an IT and identity background, to understand how they are put together.
- **Organizations (Relying Parties, as the consumers of trust)** – explains how trusted identities work and what roles and governance they should expect to see in the ecosystem. Why can they trust a Digital ID? How should a Digital ID work for them in terms of working to their rules. The OIX directory can be used to find trusted suppliers of IDs: ***Credential Issuers***, ***Identity Providers*** or ID ***Brokers***. The OIX directory provides a single reference point for ***Trust Schemes***, trust providers and their associated certification.
- **Framework Creators** – provides a Guide to creating frameworks that then ensures any framework created is following proven best practice and should be interoperable with other frameworks. The OIX directory will list other frameworks for reference.
- **Global Identity Influencers** - Brings together their already largely aligned thinking into a single, high level, easy to understand web-reference.
- **Existing Framework Operators -** Defines how interoperability between frameworks can work.
- **OIX ID Services Members** - The OIX Directory positions each member's services against the framework based on their role (or sub-role) in the ecosystem.

3 SMART DIGITAL ID

Using a Digital ID must be delightful, not painful.

Creating digital identities, or wallets, full of digitized versions of real-world credentials and then leaving the user to work out which credentials, or parts of credentials, are needed for each transaction is not sufficient.

The user's Digital ID must be intelligent! It must be Smart!

It must be able to accept 'the rules' for a transaction and work out how to fulfil those rules on behalf of the user. If that means getting a credential the user does not currently have, the Smart Digital ID should assist the user to get it. If it means combining information from several credentials to meet data minimised needs, the Smart Digital ID must do that safely and with the user's consent.

Users cannot be expected to need to understand 'the rules' – the rules are too complicated! Try working out the rules for a 'covid safe' status for instance? The user's Smart Digital ID must be their assistant to help them through the process.

The Smart Digital ID is a service the user depends on to ensure they can prove who they are and what they are eligible to do as they go about their day to day lives. The Smart Digital ID must seamlessly provide trust in who the user is and what they can do.

A Smart Digital ID could be delivered to the user via a Smart Wallet on their device or it could be securely hosted in the cloud.

This guide explores the components a Digital ID needs to be Smart, and defines how trust frameworks can be designed to support Smart Digital ID.

4 IDENTITY TRUST

4.1 The Need for Identity Trust

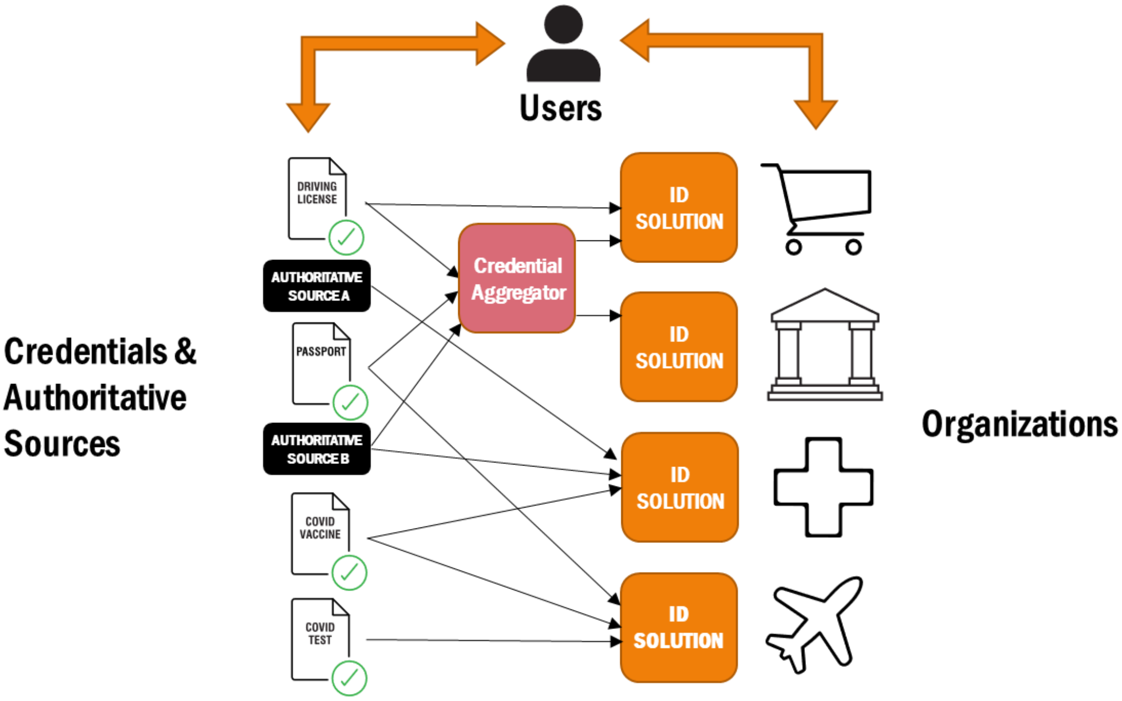
For many types of transaction, digital or otherwise, organizations need to know who they are dealing with and what that person is able, or eligible, to do. The rise of Identity Theft means that organizations cannot rely on a person simply claiming to be who they are, independent verification and risk checks are required. Equally, genuine individuals may try to present false information about themselves in order to gain access to goods, services or environments that they do not have the ***Eligibility*** for. Examples where trust is needed, and the risks to be mitigated are:

Scenario where trust is needed	**Risks needing mitigation**
Access to age restricted goods / services	Underage access
Agreeing to deliver goods to an address	Identity Theft Avoidance of payment
Opening a financial services account	Identity Theft Money Laundering
Accessing benefits	Identity Theft Eligibility for benefit
Travel	Identity Theft Terrorism Lack Permission to visit (VISAs) Infection (COVID)
Employment	False qualifications Right to work Access to Vulnerable people
Housing	Right to reside
Healthcare	Access to sensitive personal information.

Users need to trust organizations they present their ID information to are genuine. The user's Digital ID should only work with reputable organizations who are part of the trust framework.

4.2 How Organizations establish identity trust today

Users interact with many different types of organization online, for many different purposes:

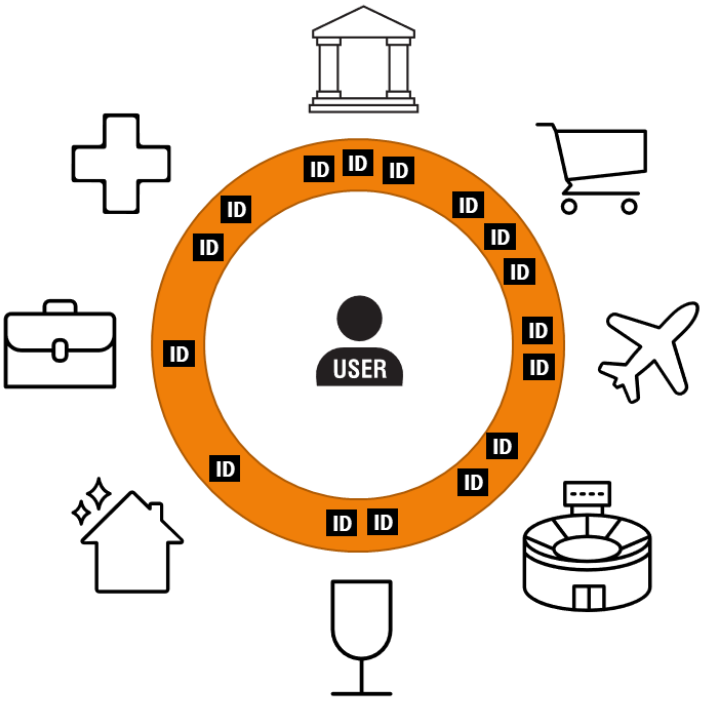


In order to simplify the sourcing of Credentials, ID solutions may take credential services from an organization that creates and markets 'packages' of credentials, a 'credential aggregator'. These credentials must have been created in accordance with the framework.

Organizations providing services to users typically have their own tailored ID Solution that enables them to:

- Ensure that the user is who they are claiming to be. This is done on a risk mitigation basis and / or to a standard that is prescribed, usually on a per-sector basis (e.g. finance). Organizations often leverage external ID proofing, verification and risk services from credential issuers or authoritative sources to establish the user is who they are claiming to be.
- Ensure the user is eligible for the goods, services or environments they are trying to access, such as is the user Over 18 or COVID safe.
- Issue the user with organization specific authenticators to enable them re-access the organization on an ongoing basis (e.g. a username and password). The authenticators used are, again, usually determined on a risk-based approach, but increasingly also by sector-based regulation (e.g. PSD2 SCA for the finance sector).
- Manage the user's privileges, accesses and entitlements within that organization.

The user ends up repeating the same process again and again with each organization they deal with, and has many usernames and passports:

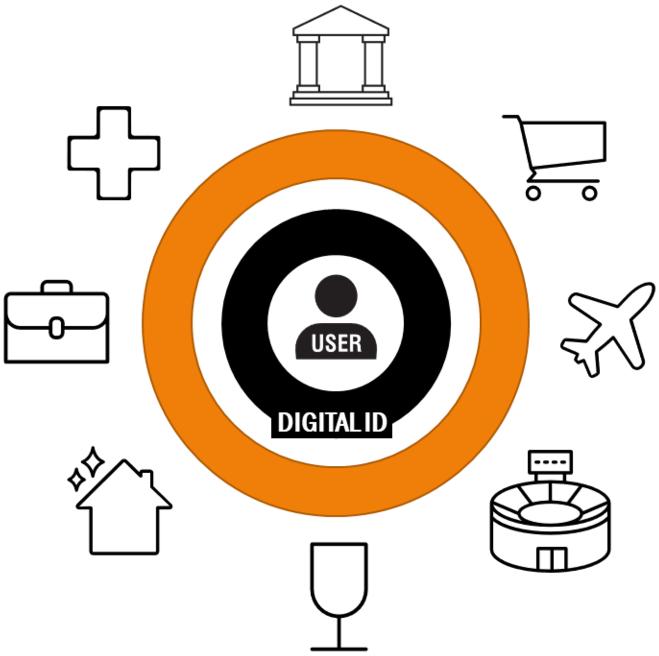


This model has a number of challenges for each party:

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 solutions.
Leads to complex onboarding journeys which lead to abandonment	

4.3 A better way of doing this – a Digital Identity?

A Digital Identity may enable a user to provide trust in their identity to any organization.



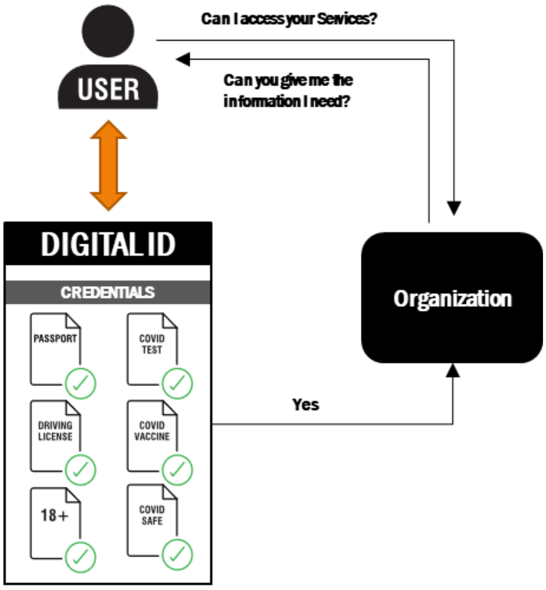
The Digital Identity has the following advantages for users and organizations:

User Advantages	Organization Advantages
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
Reduces Identity Fraud	

4.4 What is a Digital ID?

A Digital ID is a set of verified digital ***Credentials***. Examples of Credentials include:

- Digitized real world credentials such as Driving license, Passport or Vaccine Certificate
- and derived credentials such as Over 18, Covid Safe or a ***Level of Assurance***

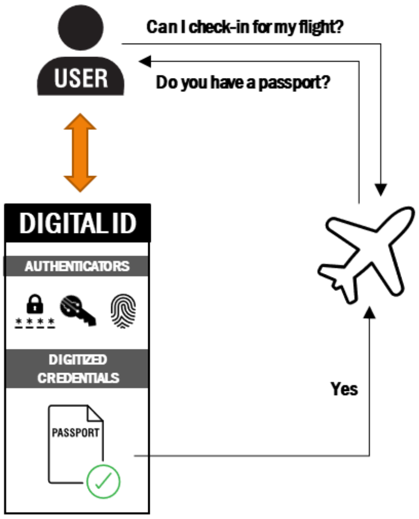


A user will approach an organization for services and will provide the organization with the information they need to do business with the user using their Digital ID.

The user might then use their Digital ID to access an account they set up with that organization.

The Digital ID will come from a provider that the user trusts to give them the tools to manage their ID. The Digital ID might be in the form of a 'wallet' that allows the user to collect and manage credentials. The wallet might be on a user mobile device or managed in the cloud.

Let's start with a simple example of how this works – providing a passport to an airline:

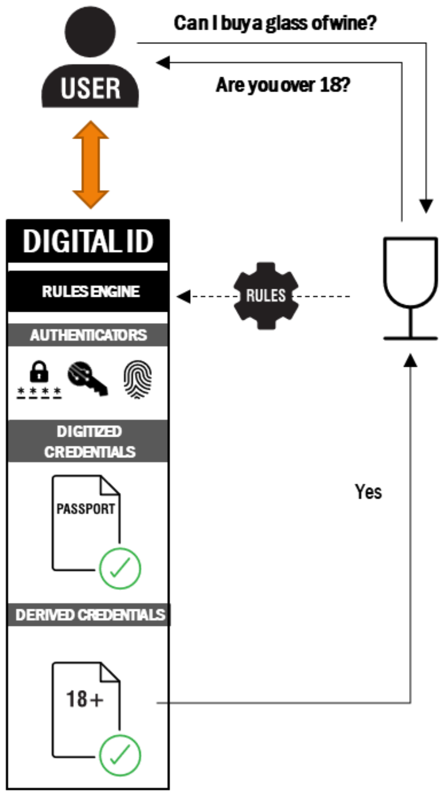


The simplest implementation of Digital ID is where the user is providing a Digitized version of a real-world Credential, such as a passport, driving license, covid vaccine or qualifications.

The ***Digitized Credential*** must have been verified as belonging to the user.

Authenticators are used to identify the user is the owner of the Digital ID and Digitized Credential.

If we consider what also seems like a simple example – proving the user is Over 18 - we quickly see that the Digital ID must have some level of sophistication if it is to help the user prove who they are for everyday tasks. It must be a Smart Digital ID:



Organizations might not ask the user for a specific Digitized Credential but might ask for information that can be derived from one or more credentials.

For example, the user can provide a ***Derived Credential*** that says they are Over 18.

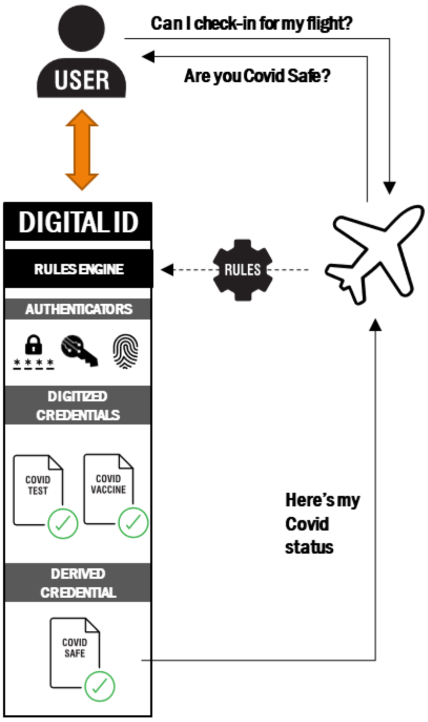
This could be derived programmatically by the Smart Digital ID from a digitized credential that has been verified as belonging to the user. The digitized credential itself does not need to be shared with the wine seller.

The Rules for deriving Over 18 are determined by a ***Rules Engine***. For instance, a rule might be that a) the Over 18 proof must be derived from a government issued credential and b) the government credential must have been verified as belonging to the user to an agreed standard and c) the user has used authenticators to access the digital ID that prove this is the genuine user.

Organizations must be able to set their own rules.

To answer an organizations question, a complex set of rules might be required that may require several digitized credentials to be gathered.

Another example is proving a user is Covid Safe:



The rules for a COVID Safe status might be: a vaccine course from a list of approved types completed within the last 12 months PLUS a negative test from a list of approve types within the last 72 hours.

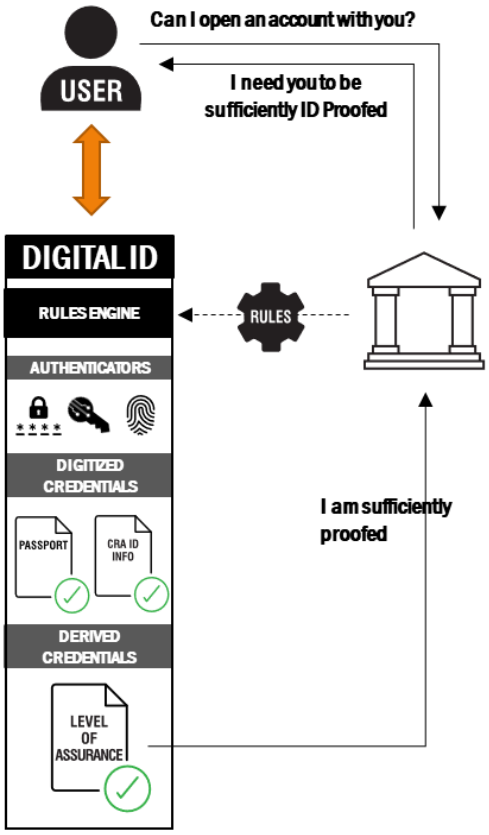
Rules may vary by use case, trust framework or individual organization

Many Derived Credentials are point-in-time and need to re-assess at the point of next request.

Also, Digitized Credentials may expire or be revoked. In which case and other credentials derived from them may no longer be valid.

Many Trust Frameworks will define what's known at ***Levels of Assurance***. These show that a user has been identity proofed to a predefined level and has sufficiently robust authenticators associated with the Digital ID to assert that Level of Assurance to an organization.

Using a finance example, to open an account with a financial services provider the user might need to prove they have a sufficient level of assurance:



Trust that the user is the genuine individual is derived from the credentials gathered by the user.

For example, a photo from a passport or driving license cross checked with a selfie of the user, can be used to verify that this is the genuine user. Or a logon to online banking.

Higher levels of assurance usually also need multiple robust Authenticators to be “bound” to the users as part of the proofing process, to provide multi-factor ***Authentication***.

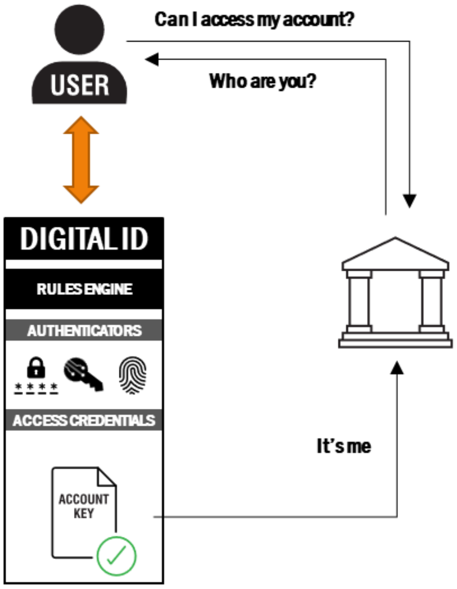
A Level of Assurance is a form of Derived Credential. Levels of Assurance are dynamic and need to be continually re-assessed as the users' credentials expire and fraud risks are re-assessed.

The process is handled by the Rules Engine. The user sees that they are asked to gather certain credentials and set up specific authenticators. They will not usually be aware they have achieved a specific Level of Assurance.

A user may have many different Levels of Assurance for different use cases and organizations.

Some trust frameworks may also require that the credentials used to derive a level of assurance are shared with the organization, as a form of ***evidence.***

Finally, users may use their Digital IDs to logon to an organizational account again and again. This does not just mean financial accounts, but any organization the user has an ongoing relationship with:



Users already use Facebook, Apple and Google IDs to do this as a form a Digital ID, but with no level of assurance expressed.

The organization would issue the User with an ***Access Credential*** that is their Account Key for that organization.

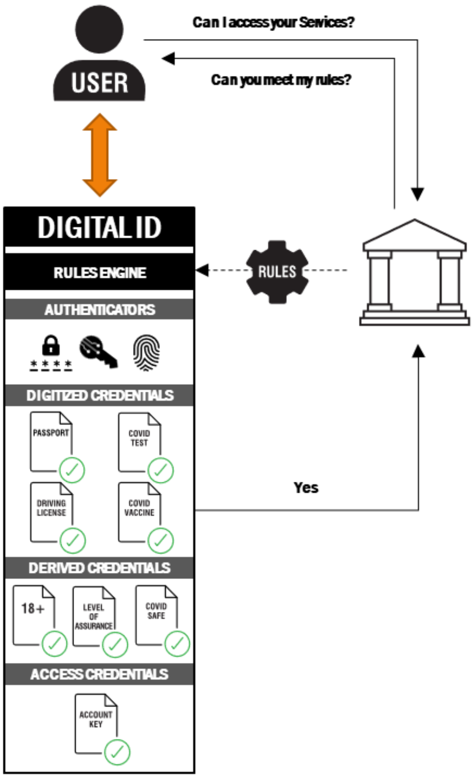
Or many organizations could rely on a generic ***Account Key*** created by the Digital ID.

Next time the user interacts with the organization they present them with their Account Key to show them who they are.

The organization may require authenticators of a particular type or level of quality to trust the Digital ID.

4.5 The 4 key features of a Smart Digital ID

Putting the examples we have looked at so far together gives us a complete view of a Smart Digital ID.



Rules Engine. The Smart Digital ID **works out what a user needs** to meet an organizations business rules using a rules engine or rules agent, and helps the user gather, derive and present credentials to meet the organization's needs. The Digital ID must be smart. It must make the users life easier. To do so it must interpret organizations rules on behalf of the user. The user cannot be expected to understand and process the complex rules that organizations must work to. The Digital ID should work out whether the user have right information or credentials required. If they don't have them, it should help them get them. It should combine credentials if necessary to created derived credentials that meet the organizations rules, removing processing and data handling burden from organizations. It should apply the principle of data minimisation, only sharing the information organization require to meet their needs; no more, no less.

Digitized versions of Credentials – The Digital ID can carry **credentials** such a passport, driving license, vaccine certificate or relevant qualifications.

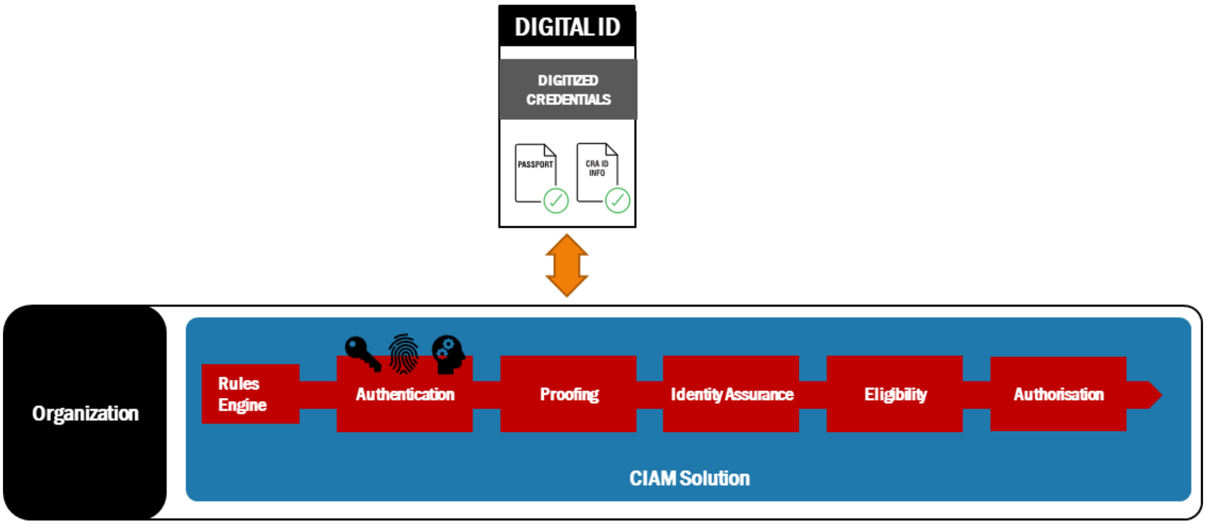
Derived credentials – The Digital ID can also work out that users meet the business rules of an organization, **such as being over 18, COVID safe** or meeting a specific **"level of assurance".**

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

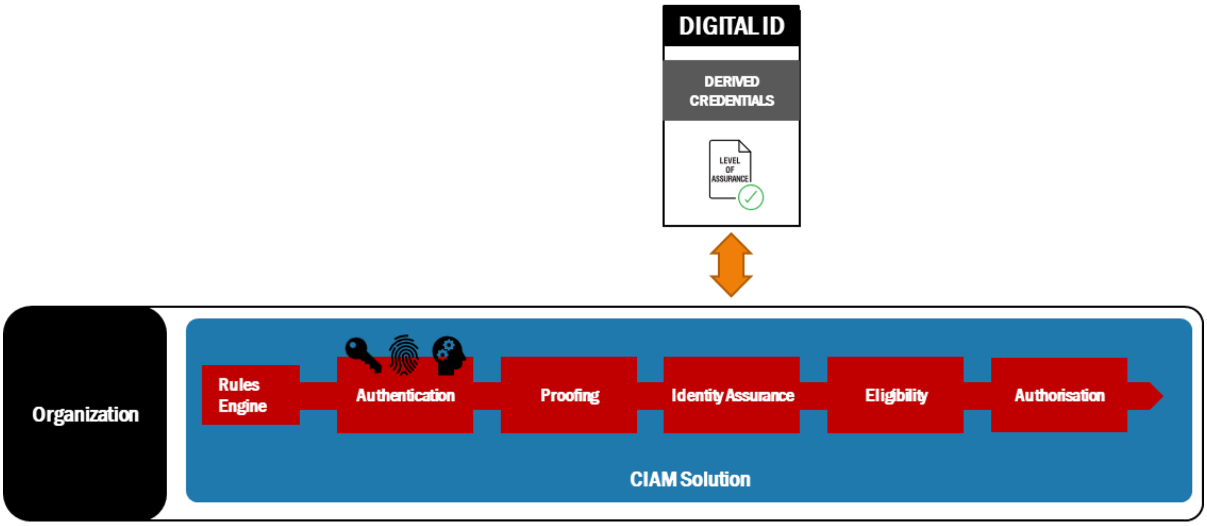
4.6 How will Digital ID be adopted?

Firstly – this is likely to be an evolution, not a revolution. Organizations will move towards using Digital Identities over time. Organizations might use Digital IDs in all ways described below, or just one.

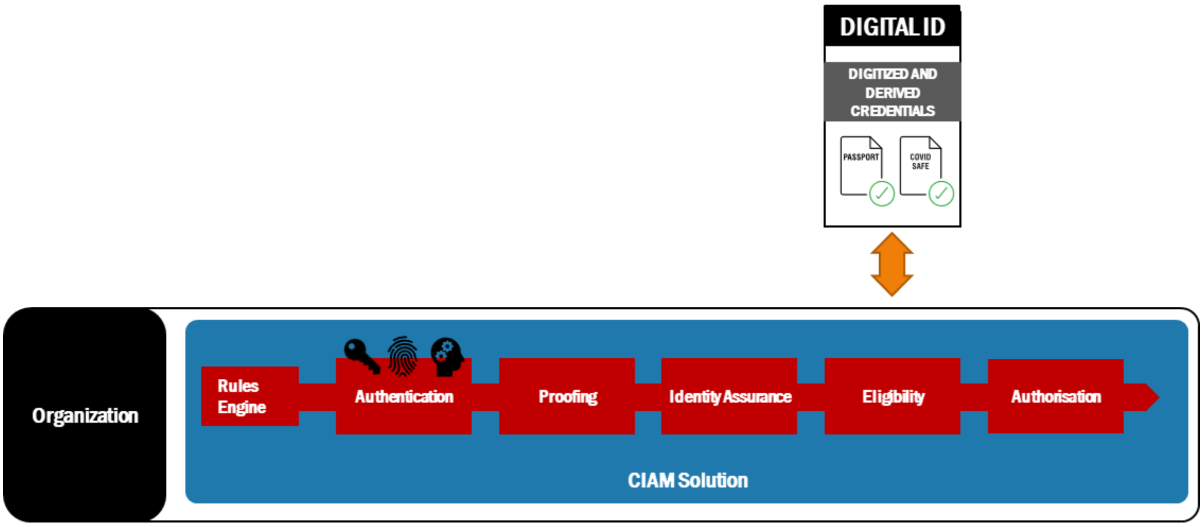
Some organizations might only use a Digital ID to gather credentials to proof the user themselves and will continue to issue the user with their own organization-specific authenticators.



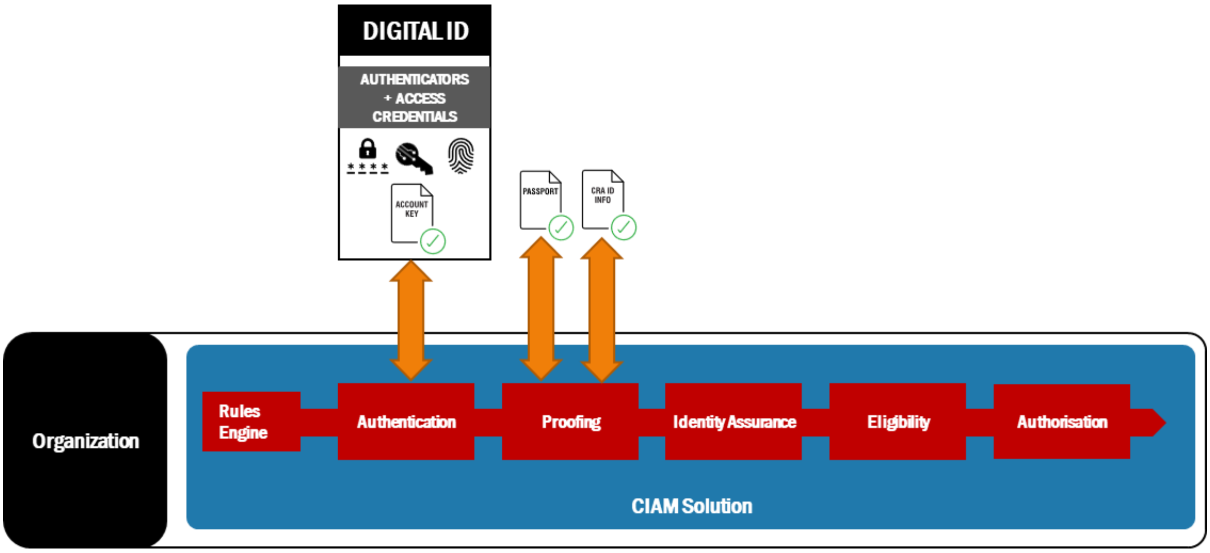
Some organizations will rely on the Digital ID to make complex rule-based decisions for them, leveraging derived credentials such a Level of Assurance or Over 18. (



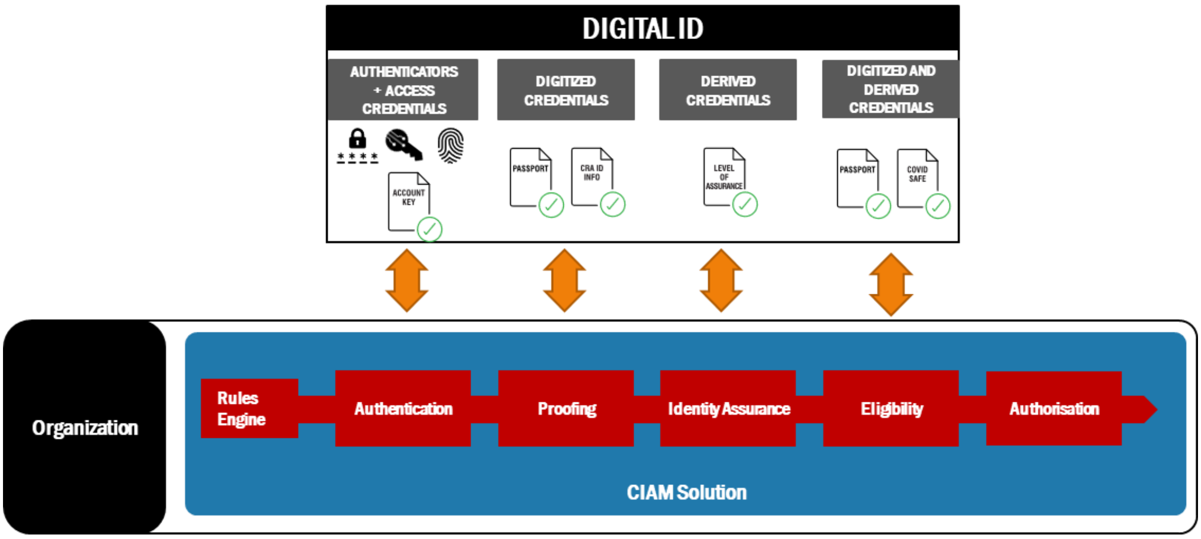
Other organizations might issue their own authenticators and do their own ID proofing, but use a Digital ID to only provide eligibility information, such as a COVID Safe status or eligibility to travel (passport):



Other organizations might user a Digital ID solely as an access method, as many organizations do with OpenID Connect today, to save issuance and management of their own authenticators. The organization would continue to get their proofing and eligibility information directly.:

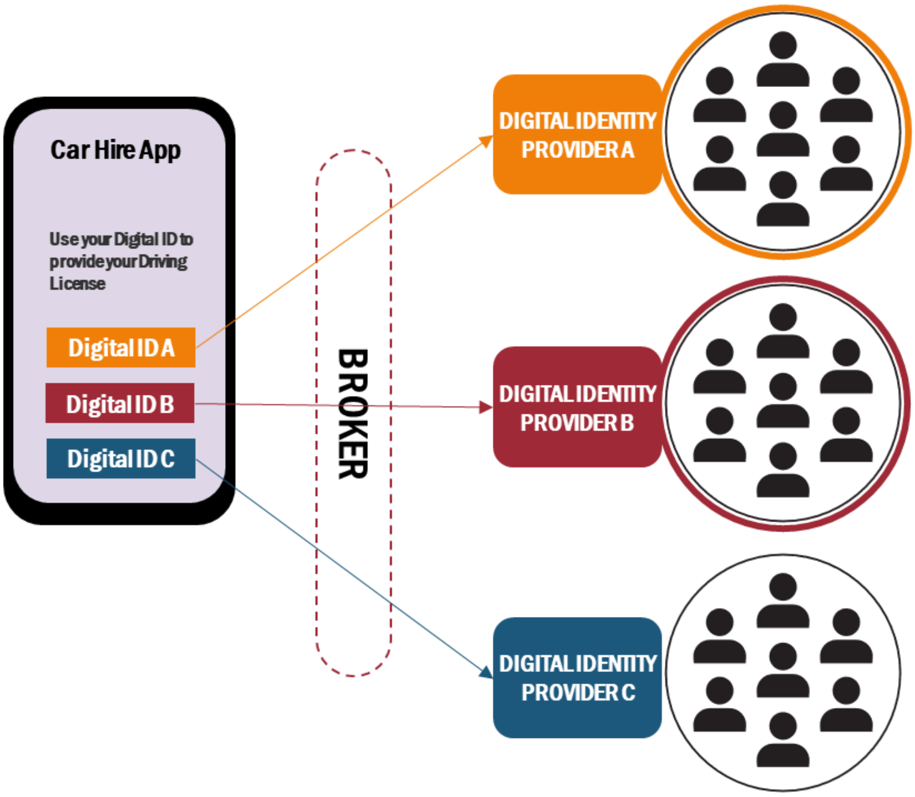


Finally, some organizations might move to fully embrace the use of Digital Identities for both account opening and ongoing account access. (Digital ID access to accounts).



Organizations will still need their own ID Solution – often referred to as a Customer Identity Access Management (CIAM) Solution - to manage their interaction with the Digital ID and determine the user's privileges within that organization.

There may be multiple ***Identity Providers*** in a particular market. This may be enforced to ensure a competitive market, or driven by market forces alone and consumer choice. Or an ID market might be formed by a consortium of companies who already issue IDs to a critical mass of users, such as Banks or Telcos.


Car Hire App
Use your Digital ID to provide your Driving License
Digital ID A
Digital ID B
Digital ID C
BROKER
DIGITAL IDENTITY PROVIDER A
DIGITAL IDENTITY PROVIDER B
DIGITAL IDENTITY PROVIDER C

Organizations will not want to contract with, and separately interface to, Digital Identities from different Identity Providers, so ***Brokers*** are likely to emerge, who aggregate Identity Providers and / or credential issuers into single services.

5 THE GOVERNANCE REQUIRED

To establish Trust within an identity ecosystem, rules are required to which all parties subscribe that enable organizations, or Relying Parties, to consume identities and their associated information with confidence.

Accordingly, some form of governance framework is required.

5.1 Governance Frameworks

Governance frameworks are not a new concept. They are commonly used outside of the world of digital identities, to govern a variety of multi-party systems where participants desire the ability to engage in a common type of transaction with any of the other participants, and to do so in a consistent and predictable manner. In such cases, they are proven to work and scale. Common examples include credit card systems, electronic payment systems, and the internet domain name registration system, which all rely on a set of interdependent specifications, rules, and agreements. This set of specifications, rules and agreements is referred to by various names, such as “operating regulations,” “scheme rules,” or “operating policies.”

In the world of identity systems, we refer to the governance framework as the “trust framework.”

5.2 The Basic Concept of a Trust Framework

“Trust framework” is a generic term often used to describe a legally enforceable set of specifications, rules, and agreements that govern a multi-party system established for a common purpose, designed for conducting specific types of transactions among a community of participants, and bound by a common set of requirements. Examples include credit card systems (such as Visa or MasterCard), electronic payment systems (such as SWIFT or NACHA), the domain name registration system (ICANN), and identity systems. They all share a variety of common characteristics, including the fact that each participant needs assurances that each other participant will follow the same set of rules applicable to its particular role.

The set of specifications, rules, and agreements that govern such multi-party systems are referred to by various names. For example, the Visa payment card system refers to them as “Operating Regulations”; the NACHA electronic funds transfer system calls them “Operating Rules”; some identity systems do refer to them as a “trust framework”, such as Australia’s DTA, Canada’s DIACC framework, India’s Aadhaar service and eIDAS) others refer to them as “Scheme Rules.” Other identity systems call them “Common Operating Rules”, “Operating Policies.” or similar descriptions.

OIX uses the term “trust framework,” as that is the term most commonly used in the field of digital identity management.

A “trust framework” means an environment for identity transactions governed by a set of rules where users, organizations, services, and devices can trust each other. A trust framework involves:

a) a set of rules: roles, principles, policies, procedures and standards,

b) a group of participating entities,

c) governing the collection, verification, storage, exchange, authentication, and reliance on credentials about an individual person, a legal entity, device, or digital object, for the purpose of facilitating trusted identity transactions.

6 THE TRUST FRAMEWORK

6.1 Contents of the Trust Framework

A trust framework comprises:

Governance approach. How is the framework established, evolved and operated? How are parties certified to the framework?

Principles. Key principles that the framework must support

Trust mark. How is the trust framework communicated and to end users and relying to parties? What are the user experience rules around the Trust mark.

Interoperability requirements. How is multi use case ID interoperability going to be achieved, within and across frameworks.

The different Roles within the trust framework.

The Rules of the trust framework.

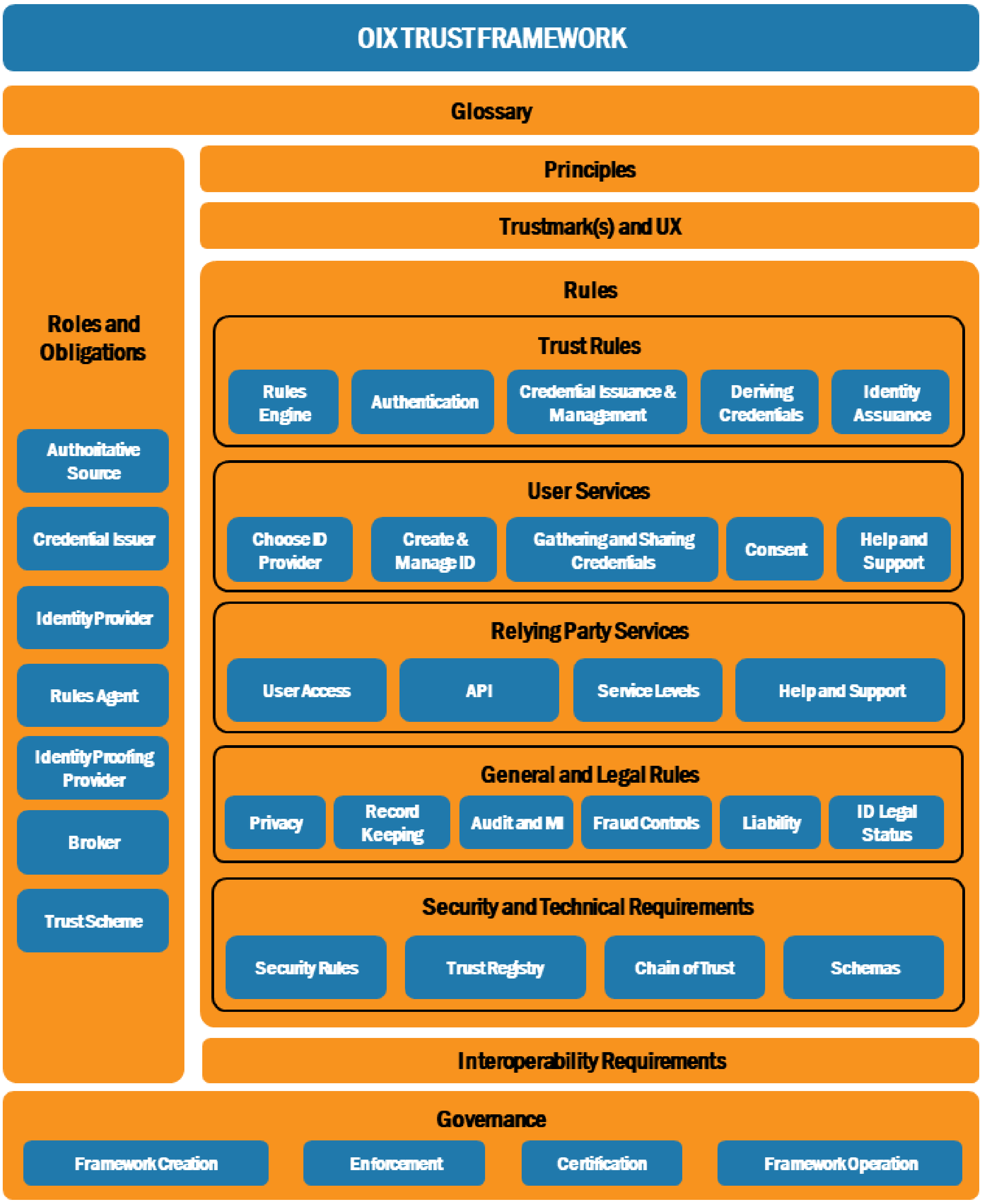
In this guide the rules of a trust framework are deliberately organised as follows:

- From the top down we start with the user led Principles required, then the Trustmark required to communicate the framework to the user.
- Then come the Trust Rules in the framework, the fundamental elements of ID credential issuance and management, deriving credentials, authenticators, and identity assurance.
- Next come the services required by the Users of a Digital ID, followed by the Organization, or ***Relying Party***. If we get these two keys endpoints of user and Relying Party right, the framework is more likely to be a success.
- Then, General, and legal rules applying to all parties are then covered: fraud controls, liability, record keeping, audit and MI.
- Finally, the technical and security rules to ensure the framework is managed securely, delivers data in a consistent format and can be held to account.

A key objective OIX is seeking to achieve is interoperability across frameworks. This is referenced throughout the guide but is also called out as a separate contents section for specific consideration.

The contents suggested in the guide are a super-set of the contents any individual framework might need to implement. Each framework is likely to implement a sub-set of these contents suitable to meet its own specific needs.

This trust framework diagram shows the more detailed contents at the rule area level:



Subsequent sections of this document explore, at a high level, these rule level contents and roles.

Within each content area the appropriate policies, procedures, rules and standards need to be defined. These have been identified and listed in a table for each framework content area.

The obligations defined by these documents then need to be mapped to each role within the ecosystem. This can then be used to formulate a contract for each actor within the ecosystem.

Note that this OIX guide to trust frameworks does not address many purely commercial matters between the parties, in particular pricing. It is expected that each framework implementation will address commercial matters in a way that suits the parties and the implementation structure of that particular framework.

6.2 Glossary

The identity community uses a plethora of specialist terminology. In order to try and standardise the vernacular OIX has created a separate Glossary of Identity Terms.

The glossary identifies common synonyms for the terms used by OIX. It also includes the rationale for choosing to use some key terms and the list of alternatives considered.

Throughout this guide all terminology used is consistent with this glossary.

Terms used this this document that are defined in the glossary are shown in ***bold italics***.

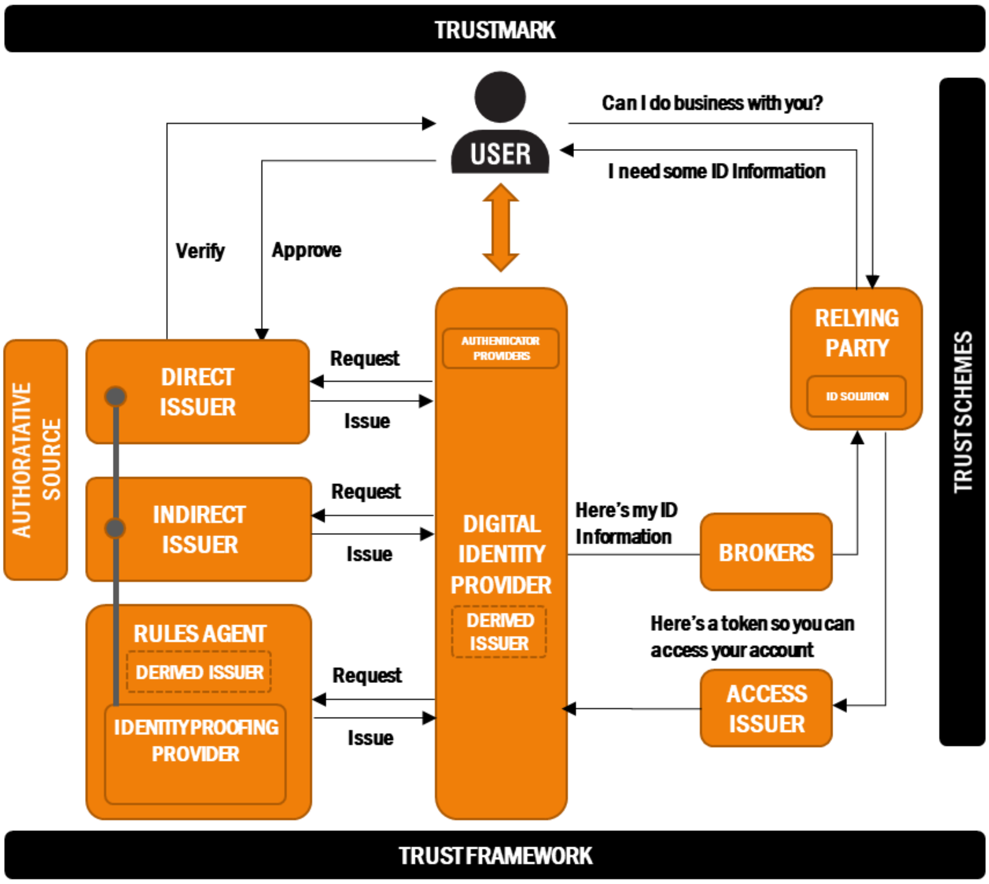
7 ROLES AND OBLIGATIONS

7.1 Roles

The identity ecosystem can involve many different roles. The roles differ between each implementation – for example, centralised and federated models will differ, as will self-certified / self-sovereign models, and one person or organization (an ‘actor’ or ‘participating entity’) may perform more than one role.

An overview of the roles that could be involved is shown below. This model assumes a single trust framework and Trustmark. It supports the implementation of the framework though trust schemes that specialise the framework for specific sectors or use cases.

Not all framework implementations will have all of these roles. A key design choice for when creating a framework is which roles to implement; this choice will be influenced by whether the body defining the framework is creating an open market approach to identity trust, or creating a single implementation of a framework and scheme for a territory.



A brief explanation of each different role is shown below:

Role	Explanation
Trust Framework	A trust framework is a set of specifications, rules and agreements often referred to by various names, such as “operating regulations,” “scheme rules,” or “operating policies.”. The framework is likely to include a certification process by which other roles in the eco-system can be shown to be compliant with the trust framework. Each trust framework is likely to need some form of governance or oversight authority to maintain and oversee compliance with the framework.
Authoritative Source	An organization that is regarded as the definitive authority for identity or eligibility information, often in law. Examples of authoritative sources include government agencies (passports, driving licenses), banks, educational institutions, healthcare providers.

Issuer	Issues some form of credential that proves who the user is and / or what they are eligible to do. This could be: electronic issuance of ID documents (e.g. passport, driving license), certificates of education, qualifications, entitlements, medical information, proof of social / societal activity, ID fraud risk assessments through to a confirmation of the users age bracket (e.g. over 18) or a determination of the Level of Assurance. They could be, or could get data from, a trusted “authoritative source” to allow the credential they issue to be validated. The provision of eligibility data is sometimes referred to as an “attribute service”.
Direct Issuer	Issues the user with a digitized credential after verifying directly that the user is who they claim to be.
Indirect Issuer	Issues the user with a digitized credential. Relies on the Identity Provider to verify who the user is. A provider of an API call from a Digital Identity Provider to validate information provided by the user is an example of an indirect issuer.
Derived Issuer	Derives a new status from credential(s) gathered for a user, such as Over 18 or a Level of Assurance. An Identity Provider will often play the role a Derived Issuer, or an external Rule Agent might play this role.
Access Issuer	Issues an Access Credential to an account in a Relying Party to allow the user to logon to that Relying Party again and again. Relying Parties are often an access issuer.
Identity Provider	Creates and maintains a Digital Identity for users that they can present to Relying Parties to prove who they are and what they are eligible to do. The Digital Identity must comply with the overall rules of the trust framework and of any sector-specific trust schemes. In the self-sovereign model, the provider of an app or wallet to hold verifiable credentials is the Identity Provider. An Identity Provider has a rules engine that allows it to determine a Relying Parties requirement through an RP Credential Request, and assist the user through the process of gathering any required credentials and applying the rules to those credentials to derive new ones to meet the Relying Parties needs. They may ‘outsource” Credential Request (for complex use cases) to a Rules Agent. Issues the user with Authenticators to allow them to reidentify themselves to the Identity Provider so that they can reuse their Digital Identity again and again.
Identity Proofing Provider	The ID Proofing Provider understands ID Proofing models and will work directly with the user to take them through the ID Proofing process. At the end of the process the ID Proofing Provider will share the Digitized Credentials gathered as part of the proofing process and the result of the proofing process, a Derived Credential representing the level of ID assurance achieved, back to the Digital ID.
Rules Agent	A specialist in applying a set of rules to create a derived credential, such as a level of assurance or a complex finance assessment on the user.
Authenticator Provider	A specialist in providing authenticators, such as biometrics, leveraged by an Identity Provider to issue and manage a user’s authenticators. Banks may be particularly suitable to play this role as they must issue strong authenticators to their customers as part of meeting regulatory standards.
Broker	In a market where there are multiple Identity Providers, a broker allows a Relying Party to enter a single contract and single technical integration to access a critical mass of digital identities or eligibility information from different Identity Providers or credential issuers. A Broker may retain Evidence relating to a Digital ID transactions on behalf of the Relying Party, but this retention shall be performed in accordance with any Scheme operational rules.
Trust Scheme	Defines an implementation of the framework within the overarching rules defined by the trust framework. Implementations could be sector specific, territory specific or global-multinational. For example, sector-specific use cases, requiring a separate trust scheme, might be: online age verification using zero knowledge proofs, anti-money-laundering checks, or air travel. These sector-specific schemes will often contain the actual implementation of local or global regulations specific to that sector. Schemes may further define, extend or omit optional elements of the trust framework to tailor the identity service to the needs of the specific implementation. For example, the trust scheme might define the ID Proofing requirements for a specific sector within the overarching requirement set by the trust framework. Where the line between trust framework and trust scheme is drawn needs careful consideration.
Trustmark	Communicates trust and compliance with the framework and schemes to the end user and Relying Parties. Indicates that a participating entity is associated with a particular trust framework and allows an individual to verify that is the case.
ID Solution	Each Relying Party a user deals with will need a solution to record the Identity Provider, and / or credential issuer services that are used. The Relying Party may also record permissions or access rights against an identity that are specific to that Relying Party. Many Relying Parties will use a Customer Identity Access Management (CIAM) system to achieve this.
Relying Party	Someone providing goods or services that the user wants to access, who requires some level of trust in who the user is, or what they are eligible to do. Also, who may want the user to re-access their services from time to time. The Relying Party might become a form of issuer to enable re-access, issuing an Access Credential. A Relying Party could be an organization but could also be another person or a “thing”.

The role definitions above can also be found in the OIX Glossary of Terms.

It is important to note that in many cases these different roles can be played by one ‘actor’, or party. For example:

- An Identity Provider will often issue its own credentials and have its own rules engine, thus having no need for an Authenticator Provider or a Rules Agent.
- The issuance and validation of a credential might be done by the same party playing the role of credential issuer and authoritative source.
- A single party might play the role of Identity Provider and credential issuer, taking in from various authoritative sources and to create a trusted Digital Identity
- A government might choose to play all these roles itself by digitally issuing trusted national IDs directly to its citizens.
- The roles of trust framework definition, trust scheme implementation, Trustmark and broker could all be played by a single commercial entity, who brings together the identities from multiple Identity Providers.
- A Relying Party might issue Relying Party-specific identities directly to its users, playing the role of Identity Provider to its own customers. It would assemble information from credential issuers that it requires to meet its identity needs, in line with a trust framework / scheme relevant to its business.

7.2 Obligations

When designing a framework, it is important that the obligations that will be put on each party playing a role in the framework is considered. The applicability of each policy, procedure, rule and standards to each role needs to be determined.

In each of the following sections regarding the different elements of the framework, the roles that are obligated to fulfil that element are identified. Those constructing and managing frameworks can use these references to construct contracts for specific roles, or parties, within the implementation of a framework.

Tables in the contents section of this guide have a column entitled “Who?” that indicates the obligated roles for each element of the framework. The following abbreviations are used:

Role	**Abbreviation**
Trust Framework	Fwk
Authoritative Source	AS
Issuer (applied to any of the below)	Iss
- Direct Issuer	DirIss
- Indirect Issuer	IndIss
- Derived Issuer	DerIss
- Access Issuer	AccIss
Identity Provider	IdP
Rules Agent	RA
Authenticator Provider	AuthP
Broker	Bkr
Trust Scheme	Sch
Trustmark	Tmk
Identity Solution	IdS
Relying Party	RP

8 PRINCIPLES

Establishing the key principles that the trust framework needs to follow is vital to how the detail of the framework is written. Every aspect of the framework should be true to these principles.

To ensure the needs of the different parties are considered, OIX suggest that principles are split between the following, in order of precedence:

1. Users - the most important principles to meet are those concerning the User.
2. Relying Party – the next most important are those concerning the ***Relying Party***.
3. Framework - and finally, those concerning the rest of the framework.

This does not imply that any Relying Party principle should be compromised in favour of a User principle, rather that in the design of a detailed trust framework the implementation should ensure the User principle is met first.

Principles should be written in plain language, particularly those aimed at the User.

OIX has undertaken a review of principles implemented in different trust frameworks and has produced the following User principles written in plain language. These principles are the 4 Cs:

User Principle	User Principle Element	Who?
CONVENIENCE	A digital identity I set up can be used in lots of different places – I don't need different digital identities to access different kinds of services, unless, I choose to do so	Bkr, IdP, Sch, Fwk
	I need to know where I can use my digital identity	Bkr, IdP, Sch, Fwk
	I need to understand why I am sometimes asked for further evidence to prove my identity	IdP
CHOICE	I am able to choose who manages my digital identity for me and change this at any time	Bkr, Sch, Fwk
	I can have more than one digital identity	Bkr, IdP, Sch, Fwk
	My digital identities are free.	Sch, Fwk
	I am able to create a digital identity directly for myself, or find assistance to help me create and manage it	Bkr, IdP, Sch, Fwk
	I can choose an alternative to a digital identity, if I am unable or unwilling	Sch, Fwk
	If I choose to, I can create a digital identity, whoever I am, whatever my background.	Sch, Fwk
CONTROL	It's my digital identity and data.	Bkr, IdP, Sch, Fwk
	I agree who my data is shared with	IdP
	I can see a record of who my data has been shared with, and request for it to be returned and removed if I want.	Bkr, IdP, RP
	I am able to change my data at any time and choose who is informed of that change.	IdP, Bkr, RP
	My data will only be used in ways that I have agreed to, at the point of need	IdP, RP
CONFIDENCE	My digital identity and data is protected from fraud and those who might use it illegitimately.	Bkr, IdP, Sch, Fwk
	If something goes wrong, I need to know how I can seek help, support or independent redress from a trusted governance body	Bkr, IdP, Sch, Fwk

The User principles should be shared with end users. The Trustmark is a good way afford users access to, and to explain, these principles.

These user-based principles map to a set of architectural and governance principles for the Digital ID Trust Framework:

User Principle	Trust Framework Principles
CONVENIENCE	**Works for the user.** The digital ID enables the user to answer the questions organization pose of them, interpreting the organizations rules and information needs and assisting the user to fulfil organizational requests. It provides simple explanations of an organization's requirements. **Visible.** A Trustmark shows the user, and organizations, that the trust framework is in operation. I**nteroperability.** A single Digital ID works for multiple use cases. Users do not need different IDs for different use cases. Organization's get consistent information about users regardless of which digital Identity Providers the user has chosen.
CONTROL	**User Control and Privacy.** The Digital ID and credentials belong to the user. The user's information can only be accessed, processed and shared through legally permitted methods, such as consent and legitimate interest. The user can see where they shared their data. The user has the right to be forgotten. **Data Minimization.** Only the data required to fulfil an organizations request need be shared, including deriving summary statuses such as Over 18 where appropriate.
CHOICE	**Inclusion.** All users who choose to do so are able to obtain and use a Digital ID. **Choice**. A user has a choice of Digital Identity Providers and is able to move their credentials to any suitable alternative Identity Provider of their choice.
CONFIDENCE	**Security.** The digital ID is secure and safe from fraud. It can only be used with organizations which are part of the trust framework. **Support**. The user, and organizations relying on a Digital ID, must have somewhere to go when there is a problem and are guaranteed that their problem will be resolved promptly

	Transparency. The trust framework rules. Operation and governance are open and clear to all parties. **Accountability.** Parties providing services follow follow the rules of the framework. Any party that is found to be at fault of the rules can be held liable for any damages caused to other parties.

The following trust framework rule documents are required to support the implementation of Principles:

Document	Type
User, Relying Party and Framework Principles	Principles

9 TRUSTMARK

A ***Trustmark*** is a recognizable signal that the trust framework is in operation. The signal could be a phrase, word, symbol or logo that is easily recognizable.

The main parties who need to see and understand the Trustmark and what it implies are:

- Users: Need to know that their data is safe, that their ID will be accepted by many Relying Parties and that if anything goes wrong, they are protected. Essentially that the User principles of the trust framework will be met.
- Relying Parties: Need to be confident that the services they consume from brokers, Identity Providers or credential issuers are compliant with the trust framework
- Credential ***issuers***: Need to know that the credentials the issue will be handled in a proper manner.

Analogous examples of trust marks that offer similar services, for both users and Relying Parties, to those that are required for identity can be found in payments: VISA, Mastercard, AMEX.

Interoperability between frameworks might be signalled to users and Relying Parties by creating an overarching Trustmark and / or by listing mutual agreements between frameworks when the Trustmark information is displayed.

The Trust Framework should set rules on:

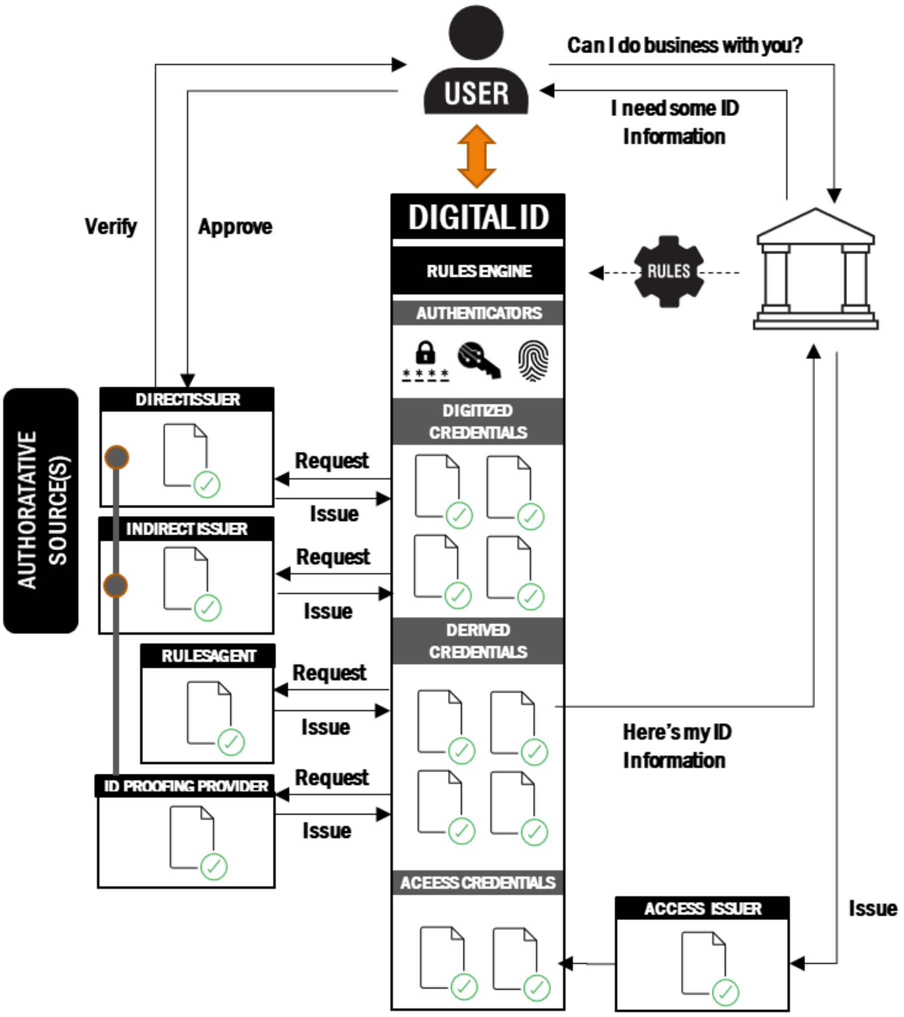
Trustmark Rule	Requirement	Who?
Single Trustmark for the framework?	The conceptual challenges of online identity, privacy and security are amplified by an overabundance of trustmarks. Too many marks or too much granularity hinders rather than helps user's decision-making processes. A single Trustmark per Trust Framework is recommended. Although some frameworks may elect to allow trust schemes to set their own Trustmark, in which case an overarching framework Trustmark, such as a standard symbol or icon, should be considered to convey to parties that a trust scheme is part of the trust framework.	Fwk, Sch
Where and how trust marks should be presented	When and how should the user see the Trustmark? How should direct issuers, brokers and IdPs display the Trustmark in a B2B context?	Bkr, IdP, RP, DirIss
What happens when a user clicks on the Trustmark	Is the user taken to a central site the communicates what the Trustmark is and what it does? Or must the participating entity implement informational services to support the Trustmark	Fwk, Sch
What information is displayed "behind" a Trustmark	Display of the following information should be considered: ● Who backs the Trustmark and how it is governed? ● User principles in plain language. ● Who is certified to participate in the framework, perhaps by role. ● Where a user can use their ID, either by sector or through a list of Relying Parties that accept IDs from the framework ● How this framework interoperates with other frameworks: where else are users ID accepted and, for Relying Parties, which IDs from other frameworks could they accept. ● Explanations of any framework level rules or levels of assurance, and why users must go through step up and sometimes cannot get to the required level. ● Where a user can go for help and support. ● What compensation is available and how to access it.	Bkr, IdP, RP, DirIss

To support these Trustmark rules the following policies, procedures or standards are required:

Document	Type
Trustmark Brand and UX usage policy	Policy

10 TRUST RULES

The following diagram show the different elements of a Digital ID and how they interact with those involved in providing and receiving trust in the Digital ID ecosystem:



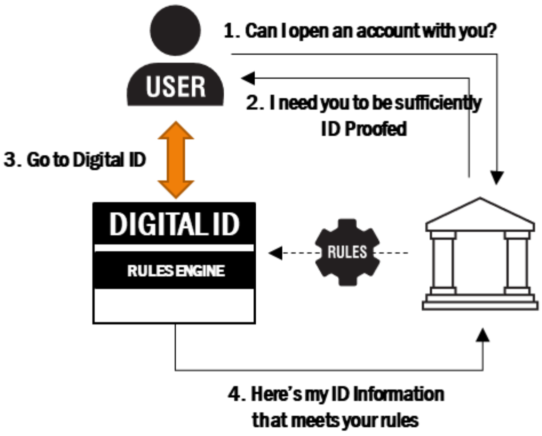
This section on Trust Rules defines how each component part of the Digital ID works, and how each part interacts with the other roles in the ecosystem to form a Smart Digital ID.

10.1 Rules Engine

A Digital ID needs to be able to interpret the rules required to meet the needs of a particular use case. The rules might be:

- Relying Party specific rules
- Rules defined by the framework, scheme or Identity Provider as part of their services.
- Handling Relying Party Credential Requests.
- Rules contained in an RP Credential Request might:
    - Require specific type of Digitized Credential is required, e.g. a passport from an ICAO recognized passport authority.
    - Define how a Derived Credential is determined e.g. Over 18 must come from a passport or driving license issued to the user by a Direct Issuer.
    - Define that specific Authenticators are required: e.g. 2 factors from one of possession, inherence or knowledge.
    - Define a level of assurance determined using an ***Identity Assurance*** Policy.

A Digital ID will typically have a Rules Engine to allow it to interpret Credential Requests and provide appropriate responses .


1. Can I open an account with you?
USER
2. I need you to be sufficiently ID Proofed
3. Go to Digital ID
DIGITAL ID
RULES ENGINE
RULES
4. Here's my ID Information that meets your rules

		Who?
Rules Engine		
Rules Engine	The Digital ID must have a Rules engine, or leverage a third party ***Rules Agent*** to implement rules. Rules Agents are often only required for more sophisticated rules. A specialist version of a Rules Agent is an ID Proofing Provider who specialises in the derivation of a level of assurance through an Identity Assurance process. Most Digital IDs will have at least their own rudimentary rules engine.	IdP
Accepting Relying Party Rules	The Credential Request from a Relying Party must contain the credentials needed and instructions to run a set of rules. This could be an instruction to meet a level of assurance for the user or could be a specific set of rules for the particular use case, or even this specific call. For example, the Credential Request could be that the RP requires: • a covid vaccine from an approved list, but not specific batch numbers, • a PCR test from this attached list of approved test providers with whom the RP has a contract.	IdP, RA, IdPP
Helping the user follow the rules.	The user must be assisted in the achievement of the rules by the digital ID. The user should not need to know the details of the rules, this is the job of the rules engine. The rules engine should determine the best way to fulfil the rules for a particular user, gathering relevant credentials, leveraging the right authenticators, and offering the users a choice of options when possible.	IdP, RA, IdPP

10.2 Authentication

Authentication happens when the user wants to:

- use their Digital Identity to gather digitized credentials, derive credentials or present credentials to a Relying Party,
- maintain their Digital Identity.

The user uses the ***Authenticators*** to allow them to be re-recognized to use the Digital Identity, or an element of the Digital ID, for example a specific credential.

Some frameworks will implement a separate role of ***Authenticator Provider*** that allows a third party, such as a bank, to provide authenticators to the Digital ID. The separate authenticator provider issues, manages and revokes the users' credentials.

		Who?
Authentication		
Authenticator Types	Rules must be set for authenticator types required. Authenticators fall into 3 types: ● Possession. Something the user has, such as a token or device. ● Inherence. Something unique about the user themselves, such as a biometric. ● Knowledge. Something the user knows, such as a secret (e.g. a pin or password).	Fwk, Sch, RP
Authenticator Strengths	Rules must be set for authenticator strengths required. Different authenticators have different strengths. A facial biometric is stronger than a password as it is harder to falsely present a facial image than it is to falsely present a password.	Fwk, Sch, RP
No. of Authenticators (Factors)	Rules must be set for the number of authenticators required. As risk increases, it is then wise to use 2 authenticators (or factors) to allow users to re-access services. As risk increases further, the 2 authenticators used should be from different types, for example requiring both a biometric and a token for access to more secure services.	Fwk, Sch, RP
Assess Authenticators Required	The first step is to assess the correct authenticators required for the rules of a transaction and determine if the user has suitable authenticators, possibly bound to a requested ***Level of Assurance*** or a ***Trust Anchor***. This could be done by assessing whether the user has previously achieved a defined level of assurance that meets the Relying Party's needs, or it could be achieved dynamically by the rules engine based on credentials and authenticator types requested by the Relying Party. If the user does have the authenticator required, the Identity Provider must determine what authenticators are required to meet the rules and ask the user to set up new authenticators.	IdP
Binding Authenticators to Credentials	When the user gathers or derives a credential, it may be appropriate to ensure the credential can only be accessed and shared when a specific (set of) authenticator(s) are used. In this case the credential is BOUND to authenticator(s). This might happen for ● A single digitized credential, such as a passport. ● A derived credential, such as Over 18 or a specific level of assurance.	IdP
Establishing a **'Trust Anchor'**	An Identity Provider might rely on the fact that a Direct Issuer has verified the user to issue them a Digitized Credentials and leverage this as a 'root of trust' to assign – or BIND – authenticators for the Digital ID to the user, creating a 'trust anchor'. For example, the user might get a digitized version of a Driving License from an issuer and at that point it is gathered the Identity Provider will bind authenticators to the credentials, or the ID in general, to allow the user to access the credential and present it to others in future. Once this is established the user has a 'root of trust', based on the Digitized Credential (the driving license) used to bind the Digital ID authenticators to the user. This 'Trust Anchor' can now be used to by the user to gather other credentials, often from indirect issuers.	IdP

Assert and Check Authenticators	The user will be asked to assert authenticators to meet the needs of the Relying Party or trust framework / scheme rules. Authenticators are checked for validity and are fraud risk assessed to mitigate against account takeover attacks.	IdP
Ongoing Monitoring	It is important that trust in the user is kept up-to-date. Most credentials do not have an infinite period of validity. Credentials such as a user's qualifications is long lived, but may still be revoked. Credentials such as passports and driving licenses have expiry dates. Other credentials such as an identity risk assessment, is only really valid at the point it is created. In additional the user may change their circumstances, such as change their name, or move address. Each time the Digital Identity is asserted, and the authentication process occurs, the validity of any trusted credential relied upon must be checked and the credentials must be reverified and updated if necessary, before the users identity can be asserted to the Relying Party.	IdP

10.3 Credential Issuance and Management

A Digital ID must help the user gather ***Digitized Credentials*** to meet the rules of the organizations the user is interacting with. A good digital ID will help the user through the process, guiding them to gather credentials to meet the often-complex rules of organizations.

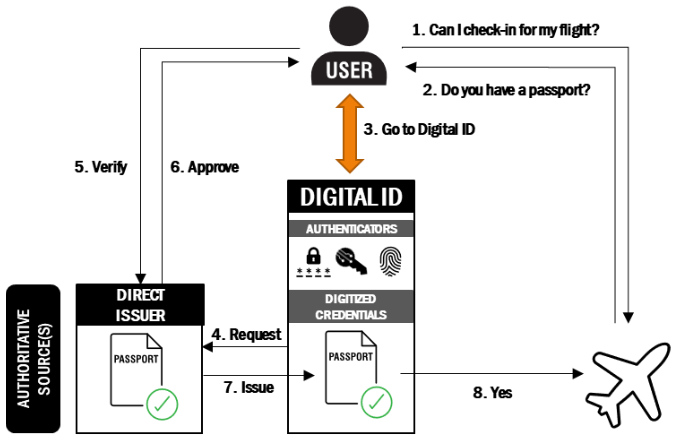
If a user does not have a credential that is required by an organization, they can get a Digitized Credential from an Issuer.

The issuer could be the ***Authoritative Source*** of the credential, such as a government passport office, or a third party that creates a trusted credential using the source issued document and / or data.

Third party credential issuers may act as an aggregator for several authoritative sources of the same information, such as passport agencies, licensing agencies or educational institutions.

In circumstances where a third party issuer issues a credential, derived from an Authoritative Source, and subsequently it is deemed inaccurate or untrustworthy due to the third party issuer's processing errors, the Authoritative Source would be held accountable for this error in digitized credential issuance.

In the below example case the ***Credential Issuer*** interacts DIRECTLY with the user to verify who they are before issuing the credential to them – thus we call them a ***Direct Issuer***:



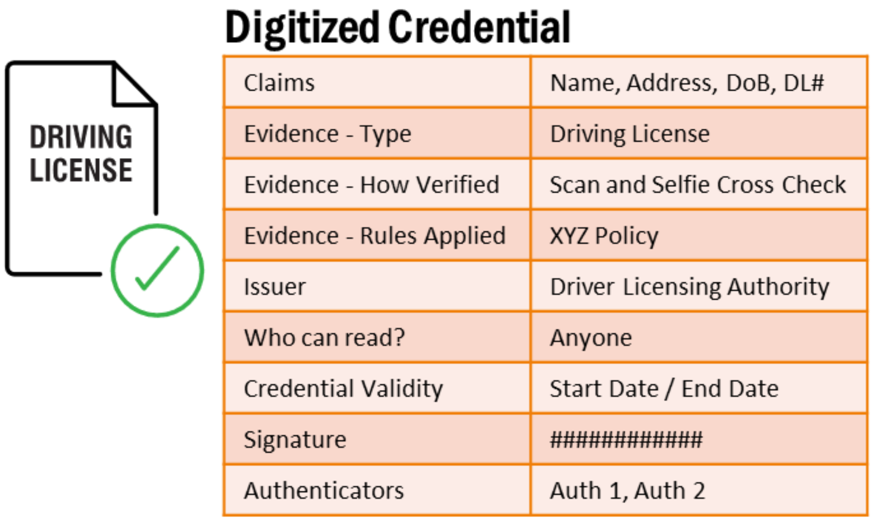
The trust in the credential can be traced back to the Direct Issuer.

Credentials will contain ***Claims***, ***Evidence*** and who the issuer is.

It will be digitally signed so that who the issuer is can be traced and it's integrity is ensured.

A credential may also contain restrictions on who can read it, including allowing it to only be read if the reader is in the possession of the right cryptographic key.

It will also contain any authenticators required to be used by the user to access and present the credential:


DRIVING LICENSE

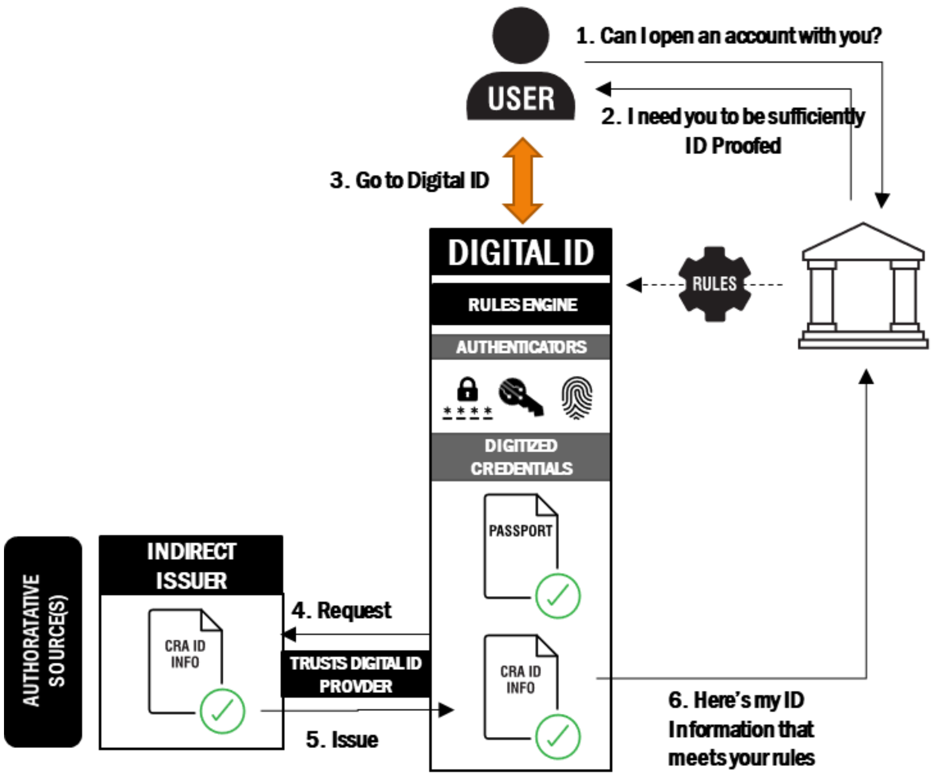
Digitized Credential

Claims	Name, Address, DoB, DL#
Evidence - Type	Driving License
Evidence - How Verified	Scan and Selfie Cross Check
Evidence - Rules Applied	XYZ Policy
Issuer	Driver Licensing Authority
Who can read?	Anyone
Credential Validity	Start Date / End Date
Signature	############
Authenticators	Auth 1, Auth 2

The ***claims*** are the actual information about the user the credential contains, such as name, date of birth, education details, health information.

The ***evidence*** will show the type of the claim, how it was verified as belonging to the user, the rules applied to undertake that verification and who the issuer of the credential is.

The Digital ID might get a credential for the user from a credential Issuer that trusts that the Digital Identity Provider trusts the user, as per the below example:

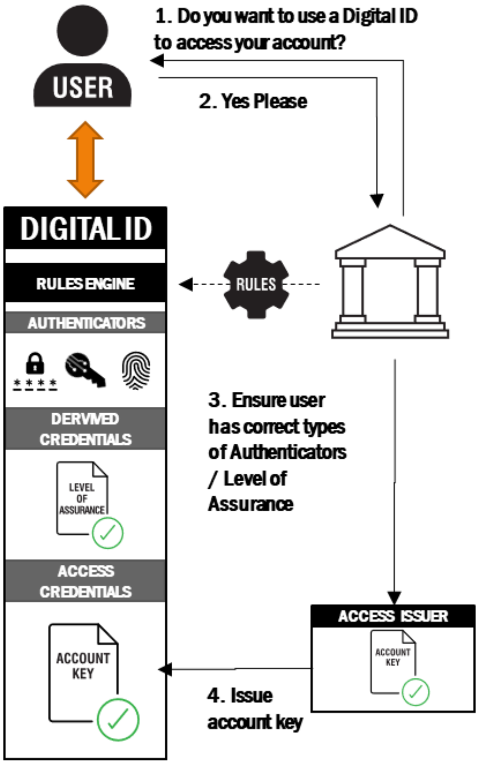


In this case the credential issuer does not interact directly with the user to verify who they are, they trust the Digital Identity Provider has verified the user - thus we call them an ***Indirect Issuer*****.**

The Indirect Issuer does not verify who the user is themselves.

The user may not give explicit consent for indirect access to credentials, instead some other legal permission such as legitimate interest may be used.

Another type of credential is an access credential. When a Relying Party wants to allow a user to access their services again and again, they might issue an access credential to the user which links their Digital ID to their account:

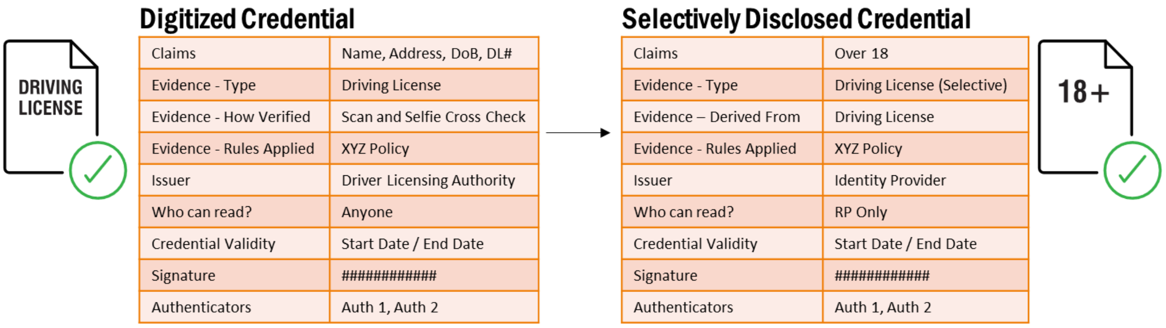


The user may need to have the right strength of Authenticators to meet the organization's needs. Our example here shows the organization issuing the trusted user with an account key that would be unique to the user and only presentable via that users Digital ID. The Account Key will contain the access Authenticator requirements for the Organization. The Organization is effectively the credential issuer for the Account Key. We call this an ***Access Issuer***.

10.3.1 Selective Disclosure

To support the principle of data minimization, where only the information vital to complete a transaction is shared by the user with a Relying Party, selective disclosure may be implemented.

The original issuer of the credential issues a cut down, or summarized, credential that only contains the information required to fulfil a specific transaction. For example, proving the user is over 18:



Digitized Credential

Claims	Name, Address, DoB, DL#
Evidence - Type	Driving License
Evidence - How Verified	Scan and Selfie Cross Check
Evidence - Rules Applied	XYZ Policy
Issuer	Driver Licensing Authority
Who can read?	Anyone
Credential Validity	Start Date / End Date
Signature	############
Authenticators	Auth 1, Auth 2

Selectively Disclosed Credential

Claims	Over 18
Evidence - Type	Driving License (Selective)
Evidence – Derived From	Driving License
Evidence - Rules Applied	XYZ Policy
Issuer	Identity Provider
Who can read?	RP Only
Credential Validity	Start Date / End Date
Signature	############
Authenticators	Auth 1, Auth 2

This credential may be re-used with many Relying Parties who have the same informational need, or restricted the relying party for whom it is issued (as per the example above).

If the process of creating the selective disclosed credential is implemented by the Digital ID itself, or a Rules Agent, they become the issuer of the selectively disclosed credential. In this instance the selectively disclosed credential would be regarded as a Derived Credential.

10.3.2 User Provided "Self-Asserted" Credentials

This Framework guide recognizes that users should have the ability to include self-asserted credentials into their Digital ID where this would improve engagement with organizations they are interacting with.

In this case the user themselves may have a level of trust that is achieved through an identity assurance process (see later). Thus the user may be trusted, but their self-asserted credential is not verified by an issuer of any form. The self-asserted credential could be regarded as self-issued.

However, the inclusion of these credentials is considered out of scope of this framework guide and inclusion could be a service capability delivered as a 'value-add' option or feature implemented by a digital identity scheme. Consequently, the responsibility for any reliance on User provided/asserted Credentials by a scheme would be subject to the commercial terms between the Scheme and that Relying Party.

The level of reliance on the trusted User's self-asserted credentials would have to be decided by the Relying Party and be a function of the risk levels in the transaction. For example, the provision of a mobile phone number, the equivalent of the national insurance number used in the UK or an e-mail address. The Relying Party should not place a level of assurance on the trusted User to a trust level above that which the User has achieved themselves.

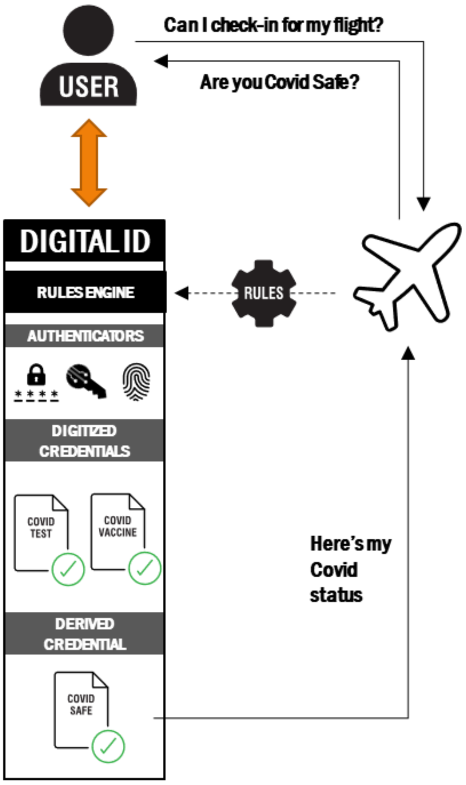
		Who?
Credential Issuance and Management		
Recognition of Authoritative Sources	The trust framework or scheme is likely to give more credence to credentials that come from, or a verified against, an authoritative source. Issuers may be an authoritative source themselves, such as a passport agency, or may be a third party who accesses an authoritative source to validate and verify the user information.	Fwk, Sch
Direct Issuers – User Verification	Must verify the user is who they are claiming to be, often to rules prescribed by the trust framework, before issuing the user with a Digitized Credential.	DirIss
Indirect Issuers – User Verification	Can contractually assume the Identify Provider has, or will establish, trust in the user. The purpose of the call to an Indirect Issuer might be as part of establishing a level of assurance for a user, and therefore may be prior to trust establishment,	IndIss
Direct Issuers – User Consent	Must obtain and retain consent from the user to create and release the Digitized Credential to the Identity Provider.	DirIss
Indirect Issuers – User Verification	Can contractually assume the Identify Provider has the legal right (e.g. consent from the user, legitimate interest) to call the Indirect Issuer. This may be via a general consent for "ID proofing and Fraud" checks, rather than explicit consent to call that indirect issuer.	IndIss

Access Issuers	Need to be able to issue Access Credentials and have them bound to the user with the appropriate authenticators.	AccIss
Binding Authenticators	Any type of issuer might bind appropriate authenticators, or authenticator types, to the credential that the user must use to access and present the credential.	Iss
Revocation	Any type of issuer needs to be able to revoke a credential they have issued at any time.	Iss
Dealing with Revocation	When a credential is revoked this may have knock on effects on Relying Parties who have relied upon that credential, possibly through a derived credential. The IdP must have a process to determine who is affected by a revocation, inform them of the revocation and determine next steps.	IdP
Ongoing Monitoring	It is important that trust in the user is kept up to date. Most credentials do not have an infinite period of validity. Credentials such as a user's qualifications are long lived, but may still be revoked. Credentials such as passports and driving licenses have expiry dates. Other Credentials, such as an identity risk assessment, is only really valid at the point it is created. In addition the user may change their circumstances, such as change their name, or move address. Each time the credential is used, the validity of the credential must be checked, and the credential must be reverified and updated, before it can be presented or used to derive another credential.	IdP

10.4 Deriving Credentials

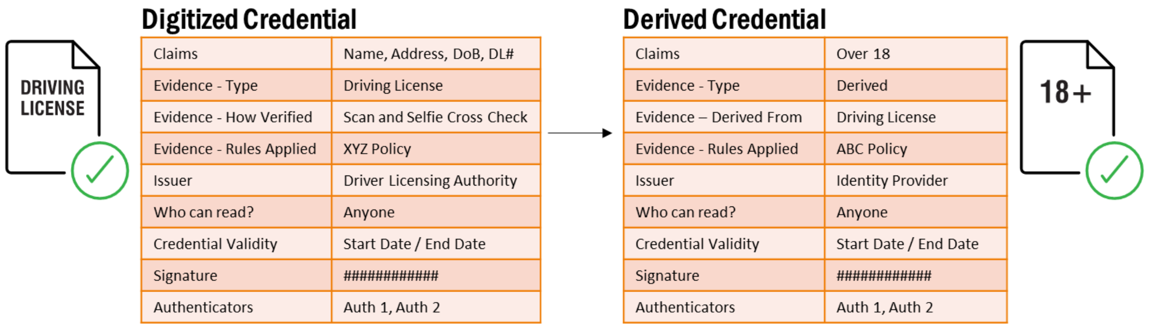
A Digital ID must help derive credentials to meet the rules of the organizations the user is interacting with. A smart Digital ID will help the user through the process, guiding them to gather credentials to meet the often-complex rules of organizations.

For example, the Digital ID rules engine may combine the credentials, direct and indirect, to create a ***Derived Credential*** that is of the level of assurance the organization requires. The creation of Derived Credentials must be executed by a trustworthy organization through the application of the rules for the Framework.



Here a Derived Credential for COVID Safe is created. Two digitized credentials have been used to derive the COVID Safe status, a Covid Vaccine and a Covid Test. The Digital ID provider is the issuer of the new Derived Credential.

A Derived Credential might be derived from a single Digital Credential, for example an Over 18 credential could be derived from a Driving License:



Digitized Credential

Claims	Name, Address, DoB, DL#
Evidence - Type	Driving License
Evidence - How Verified	Scan and Selfie Cross Check
Evidence - Rules Applied	XYZ Policy
Issuer	Driver Licensing Authority
Who can read?	Anyone
Credential Validity	Start Date / End Date
Signature	############
Authenticators	Auth 1, Auth 2

Derived Credential

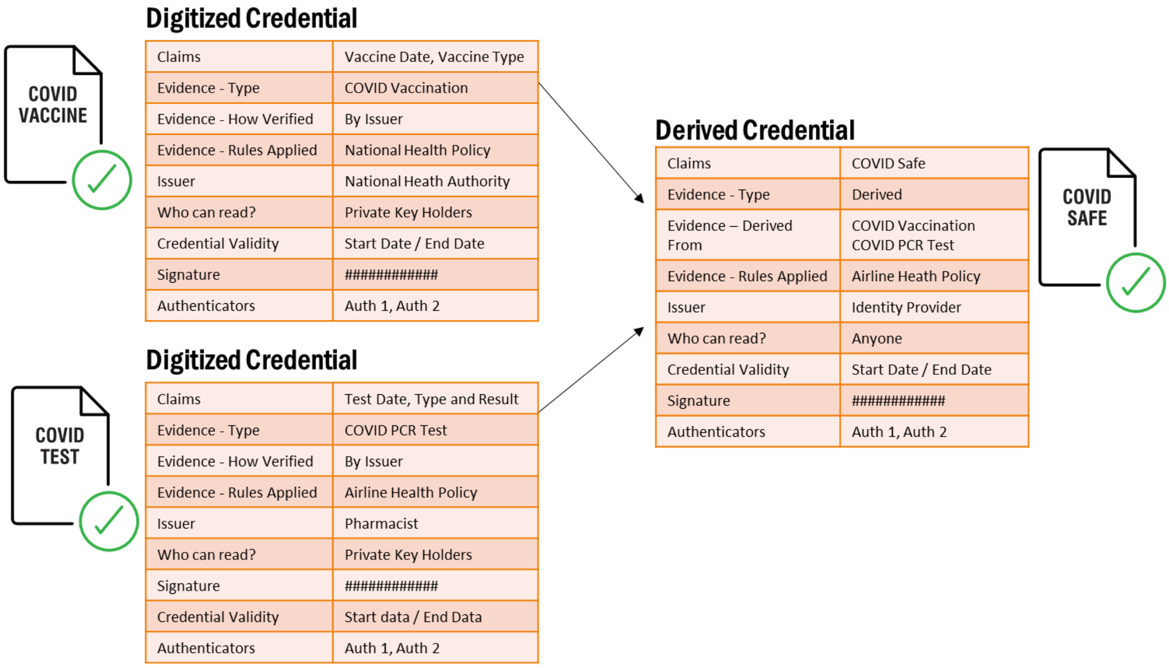
Claims	Over 18
Evidence - Type	Derived
Evidence – Derived From	Driving License
Evidence - Rules Applied	ABC Policy
Issuer	Identity Provider
Who can read?	Anyone
Credential Validity	Start Date / End Date
Signature	############
Authenticators	Auth 1, Auth 2

This derivation could be done by the Identity Provider, making them the issuer of the Derived Credential, or could be done by the original issuer of the credential, in this example the Driver Licensing Authority.

The Derived Credential will have authenticators bound to it that must be used to access and present the credential.

Zero Knowledge Proofs, where a cryptographic method is used to link the Derived Credential back to the Digitized Credential may be desirable to ensure that the original issuer of the credential is hidden from the party to whom the Derived Credential is issued, but is still legally traceable if required by the IdP.

Or a Derived Credential could be derived from multiple Digitized Credentials:



Digitized Credential

Claims	Vaccine Date, Vaccine Type
Evidence - Type	COVID Vaccination
Evidence - How Verified	By Issuer
Evidence - Rules Applied	National Health Policy
Issuer	National Heath Authority
Who can read?	Private Key Holders
Credential Validity	Start Date / End Date
Signature	############
Authenticators	Auth 1, Auth 2

Digitized Credential

Claims	Test Date, Type and Result
Evidence - Type	COVID PCR Test
Evidence - How Verified	By Issuer
Evidence - Rules Applied	Airline Health Policy
Issuer	Pharmacist
Who can read?	Private Key Holders
Signature	############
Credential Validity	Start data / End Data
Authenticators	Auth 1, Auth 2

Derived Credential

Claims	COVID Safe
Evidence - Type	Derived
Evidence – Derived From	COVID Vaccination COVID PCR Test
Evidence - Rules Applied	Airline Heath Policy
Issuer	Identity Provider
Who can read?	Anyone
Credential Validity	Start Date / End Date
Signature	############
Authenticators	Auth 1, Auth 2

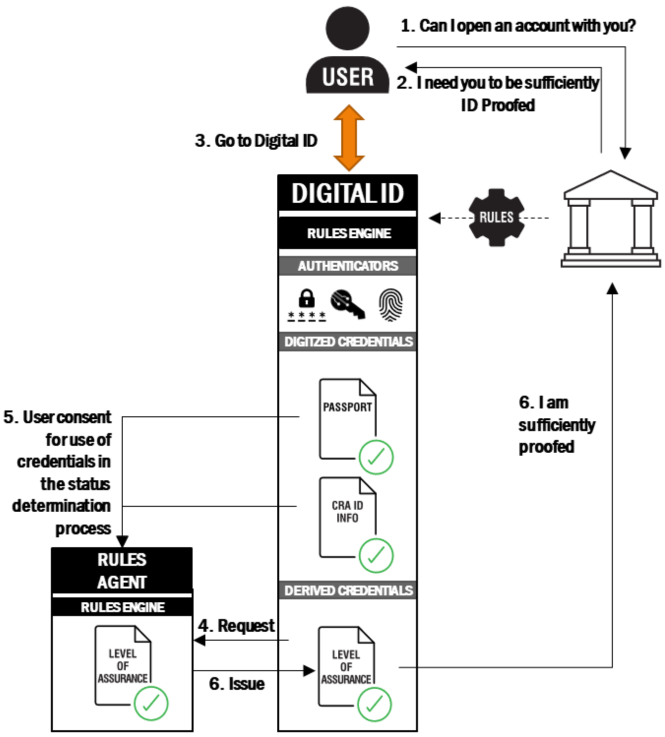
Here the issuer is the Identity Provider, using rules provided via an Airline Health Policy.

		Who?
Derived Credentials		
Apply Rules	The IdP, Rules Agent or ID Proofing Provider , must apply the correct rules to derive a credential, as defined by the trust framework, scheme or the Relying Party themselves.	IdP, RA, IdPP
Zero Knowledge Proofs	A trust framework or scheme might feel it's appropriate to implement zero knowledge proofs to allow for data minimised delivery of derived credentials.	IdP, DirIss

Choice of Rules Agent	The Relying Party might be able to define who their preferred Rules Agent, or ID Proofing Provider is.	RP
User Verification	Must verify the user is who they are claiming to be, often to rules prescribed by the trust framework, before issuing the user with a Derived Credential. For example, they may need to have achieved a certain level of assurance before the ID can be issued.	IdP
Direct Issuers – User Consent	Must obtain and retain consent from the user to create the Derived Credential.	IdP
Binding Authenticators	Must bind appropriate authenticators, or authenticator types, to the Derived Credential that the user must use to access and present the credential.	IdP
Revocation	A Derived Credential must be able to be revoked at any time. The trigger for this would most likely be the revocation of a Digitized Credential on which the Derived Credential was based.	Iss
Dealing with Revocation	When a credential is revoked this may have knock on effects on Relying Parties who have relied on upon that Derived Credential. The IdP must have a process to determine who is affected by a revocation, inform them of the revocation and determine next steps.	IdP
Ongoing Monitoring	Most derived credentials do not have an infinite period of validity. Credentials such Over 18 are long lived but may still be revoked. Credentials such as COVID Safe statuses have a finite period of validity, often a few hours. Other Credentials, such as a level of assurance assessment, are only really valid at the point it is created. In additional the user may change their circumstances, such as change their name, or move address. Each time the credential is used, the validity of the credential must be checked, and the credential must be reverified and updated before it can be presented.	IdP

10.4.1 Rules Agents

A Derived Credential may not be created directly by the Digital ID, but may be created by a separate ***Rules Agent:***



The Rules Agent reads Digitized Credentials to derive the new credential

Like with the Indirect Issuer, the user may not interact directly with the Rules Agent. The Digital Identity Provider may call the Rules Agent directly with the user's consent, passing them the required credentials to make the determination.

Who the Rules Agent is could be a preference of the Relying Party asking for the ID information.

10.5 Identity Proofing and Assurance

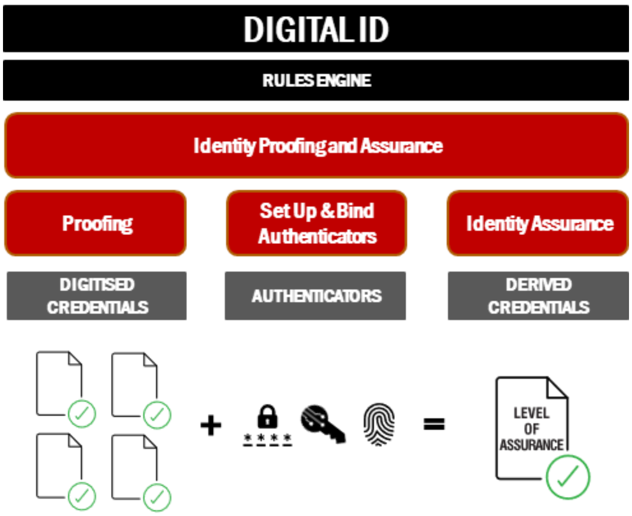
Identity Proofing and Assurance involves 3 steps:

- **Proofing -** the process of gathering and establishing trust in credentials for the user, and undertaking identity risk checks.

- **Set up Authenticators –** make sure the user has the right types of authenticators available to meet the Level of Assurance (see above).

- **Identity Assurance –** assigning a Level of Assurance from the credentials and identity risk checks gathered, and authenticators available. Binding the authenticators to the to the level of assurance.

The combination of these steps may be referred to as an Identity Assurance Model, or Identity ***Assurance Policy***.



The Rules Engine (or Rules Agent) will determine what needs to happen in each step depending on the level of assurance being determined using an assurance policy:

- What types of credentials are acceptable for proofing to this Level of Assurance?
- Does the user already have some of these? If not,
- Do they need to go and get them from a Direct Issuer?
- Can the Digital ID get them from Indirect Issuers?
- What types of authenticators are acceptable for this Level of Assurance?
- Does the user already have some of these? If not,
- What options are available to the user to set up a new authenticator?

Inclusion must be considered by trust frameworks to ensure the maximum number of users can access identity services. Techniques such as ***Vouching*** and manual evidence checking should be considered.

10.5.1 Proofing

There are three techniques generally used in the ***Proofing*** process. A process for scoring the different data and methods used within each technique should also be considered:

		Who?
Proofing Techniques		
Validation	Validating that the user exists. Validation uses credentials that the user can provide to prove who they are such as a passport, driving license or bank account. The strength of the credential should be taken into account. For example, a passport is likely to be regarded as higher strength credential than a utility bill. The credential must be validated to make sure that it is genuine. Validation is typically done via a Credential issuer with access to, an authoritative source. Validation might also include checking for evidence of User Activity at the address they provide or via the use of some other form of credential they provide, such as a social media.	Iss, IdP, RA, IdPP
Verification	Verifying that this user is the person they are claiming to be. This might be by checking possession of a credential presented by the user either through a face-to-face check, via video, via an electronic token or via biometric cross match (e.g. selfie to passport photo). The user might also be verified as genuine by the collection of separate verification-specific credentials, such as the ability to answer knowledge-based questions. The verification of a user as the genuine holder of a piece of credentials might be done by the same issuer who validated that evidence, or be done by a separate issuer. The Identity Provider may also play the role of credential verifier in this respect, linking pieces of evidence together to create a single piece, or collection of, more robust evidence.	Iss, IdP, RA, IdPP
Identity Risk *Assessment*	Assessing whether there are any risk factors present that indicate identity fraud. This might include entries in known fraud risk, mortality or change of address registers, or lack of evidence of the user in expected data sources (such as voter registers, evidence of device use abnormalities, presentation of inconsistent data.)	IdP, RA, IdPP
Proofing Scores		
Proofing Scores	Each different method and data combination used within a proofing technique could be allocated a score to reflect its value in an identity assurance assessment. For example, an NFC read of a passport and with photo cross match to a selfie of user would score more highly than evidence of a user's name and address from a utility account.	Fwk, Sch
Applying and recording Proofing Scores	The scoring model defined for proofing scores should be applied by the party undertaking ID proofing. This could be part of credential issue or applied as part of deriving a credential. Who applied the proofing must be recorded as part of the chain of trust for the digital ID.	Iss, IdP, Ra, IdPP

A single credential might have one or more of the proofing techniques applied to it. For example, as passport might be used for both validation and verification. Credentials used for identity risk assessments might be deliberately independent from credentials used for validation or verification.

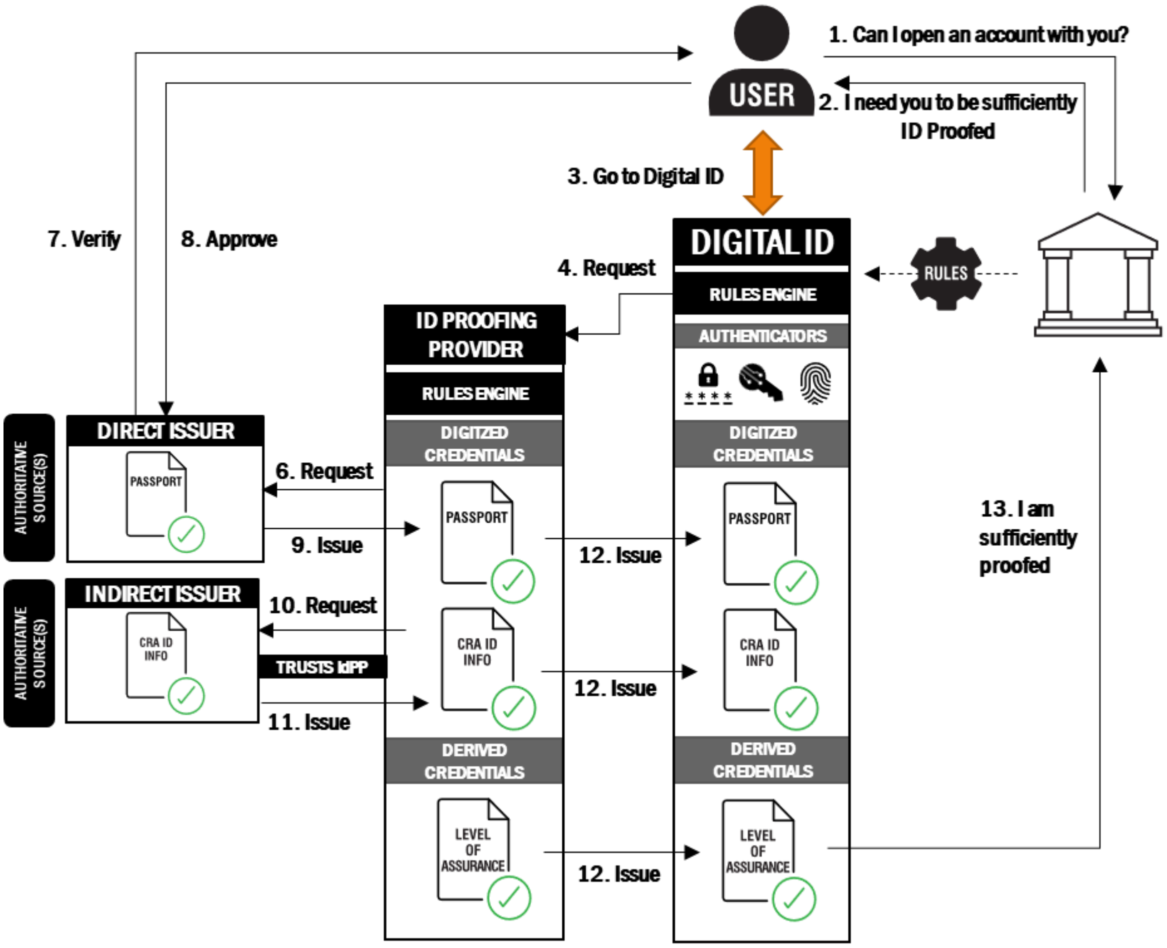
The result of the proofing process is a collection of trusted credentials, which can then be shared with, or presented to, Relying Parties. The collection of trusted credentials can also be used in an identity assurance process to achieve a level of trust, or assurance, to be presented to a Relying Party.

From trusted credentials, ***trusted claims*** can be drawn. For example, trust in a person's name address and date of birth can then be drawn from a passport.

Interoperability between frameworks might be achieved by aligning proofing scores or determining equivalence between proofing scores across different frameworks.

10.5.1.1 Identity Proofing Providers

A more sophisticated form of a Rules Agent is an ***Identity Proofing Provider*** (IdPP).



The ID Proofing Provider understands ID Proofing models and will work directly with the user to take them through the ID Proofing process.

At the end of the process the ID Proofing Provider will share the Digitized Credentials gathered as part of the proofing process and the result of the proofing process, a Derived Credential representing the level of ID assurance achieved, back to the Digital ID.

Note that is role addresses the ID proofing process only, not the full identity assurance process outlined below. The party who binds authenticators to the ID is the one who undertakes Identity assurance.

10.5.2 Identity Assurance

Identity Assurance is the process of establishing trust in the user themselves.

Different use cases will demand different levels of trust in a user's identity. The level of trust required is often dependent on the risk and value of the transaction. For example, more surety in a user's identity is required to allow them to board a plane than to deliver a low value retail item to their address.

The level of trust achieved in an identity is a function of the amount and quality (proofing score) of the credentials collected about the user.

For example, a basic level of trust might be established by an issuer checking the user's self-declared address against a database of known addresses. This might be a sufficient level of trust to deliver goods to this person's address.

To board a plane however, trust in the user's identity is required to be more strongly established:

- A passport or ID card might be needed, along with another separate proof of the user's address to validate the user.
- Verification that the user is the genuine holder of the passport or ID card would be required.
- A comprehensive Identity Risk check must be undertaken to mitigate against identity fraud.

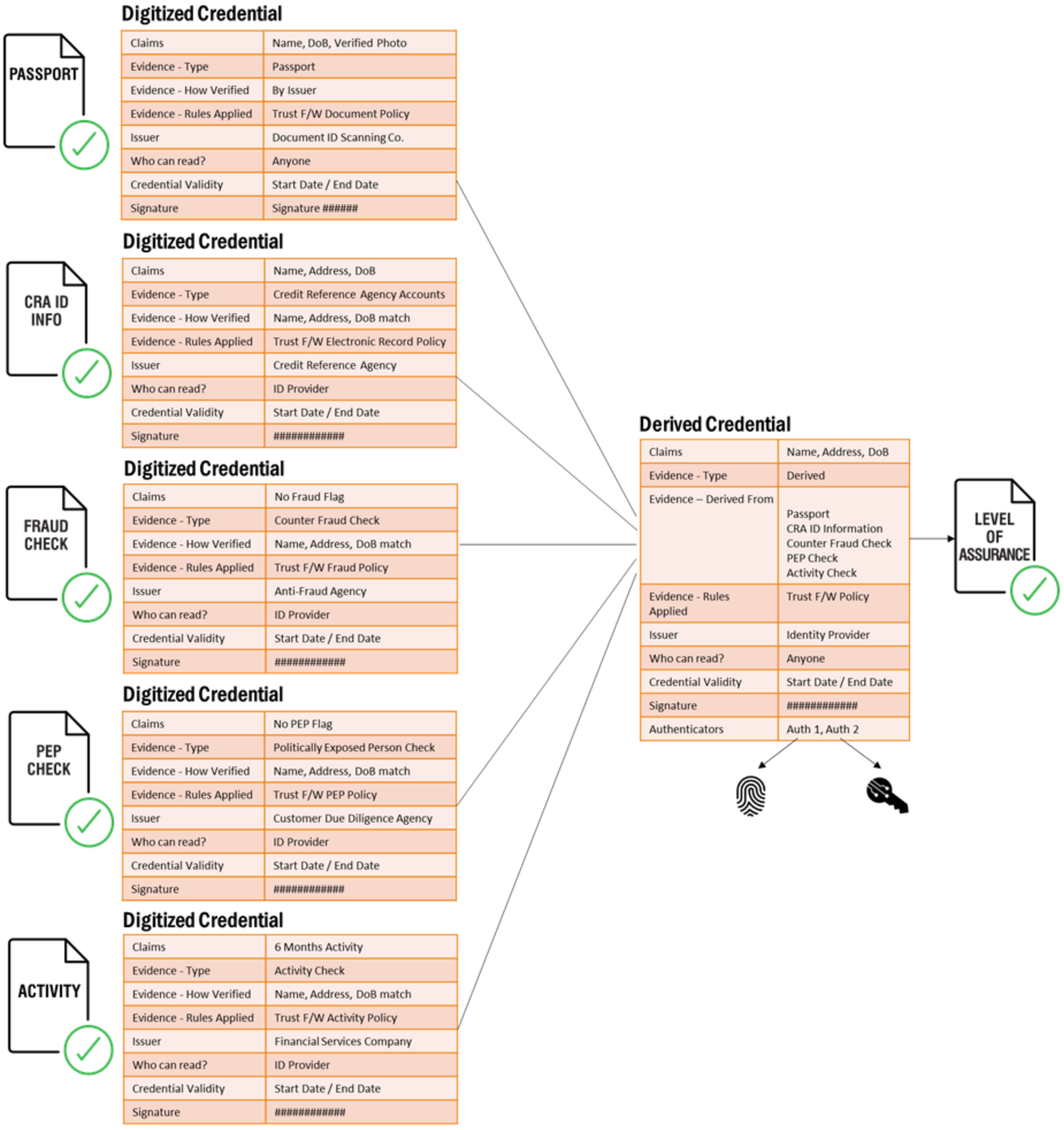
The trust framework, or a trust scheme, might define the level of identity trust that Relying Parties in a particular sector require, or might choose to use, to meet their regulatory requirements. This is called a ***Level of Assurance.***

As the assurance level increases, then the quality and mix of authenticators used to allow re-assertion of that level of assurance should also increase.

The following table describes the identity assurance process:

		Who?
Identity Proofing and Assurance		
Definition of Level(s) of Assurance	A level of assurance can be determined by an ***Assurance Policy*** that defines the types and amounts of trusted credentials required to achieve that level of assurance, along with the proofing scores required to be achieved for validation, verification, and identity risk. It may also define the type, strength and number authenticators required to re-access a Digital Identity to assert and manage that level of assurance.	Fwk, Sch
Proofing	The IdP should allow the user to achieve a Level of Assurance required by a Relying Party. Ideally the Identity Provider should do this in a way that does not require the user to understand the assurance policy. For instance, the rules engine should work out against the assurance policy what trusted credentials the user already has that will allow them to achieve a specific level of assurance, and what the gaps are. The rules engine should then work out the smartest way to fill these gaps, guiding the user through the process. Alternatively, the Relying Party could undertake this process for the user themselves using the Assurance Policy.	IdP, RA, IdPP Or RP
Trusted Claims	From trusted credentials, trusted claims can be drawn. For example, trust in a person's name address and date of birth can the drawn from a passport. For chain of trust purposes, it may be necessary to record which trusted credential(s) provided which trusted claim. A single trusted claim such as first name, could be affirmed by several different trusted credentials.	IdP, RA Or RP
Set Up Authenticators	The user should set up to the authenticators that are appropriate to manage and assert the Digital Identity as defined in the Assurance Policy. The user may have already set up some authenticators to manage their Digital ID; these may be appropriate for the level of assurance required, or additional authenticators may need to be set up. Alternatively, the Relying Party could undertake this process for the user themselves using the Assurance Policy.	IdP or RP
Binding Authenticators	The authenticators of the level of quality and type required to meet the assurance policy should be attached to the ID in the same transaction as the identity proofing is achieved in order to establish the level of assurance – this is known as "binding". Alternatively, the Relying Party could undertake this process for the user themselves using the Assurance Policy.	IdP Or RP
Issue Derived Credential	The users should be issued with a derived credential that contains the assurance level and trusted claims derived as part of the level of assurance, and evidence of how the credential was derived i.e. the other credentials on which it is based. This may be a point in time assessment of the level of assurance as some of the credentials used in its establishment may be dynamic and may need to be re-assessed before the credential can be issued again i.e. the Identity Risk credentials will be point in time.	IdP Or RP

The following diagram shows a derived credential for a Level of Assurance linked to the bound authenticators and linked back to the credentials used in its establishment:



Digitized Credential

Claims	Name, DoB, Verified Photo
Evidence - Type	Passport
Evidence - How Verified	By Issuer
Evidence - Rules Applied	Trust F/W Document Policy
Issuer	Document ID Scanning Co.
Who can read?	Anyone
Credential Validity	Start Date / End Date
Signature	Signature ######

Digitized Credential

Claims	Name, Address, DoB
Evidence - Type	Credit Reference Agency Accounts
Evidence - How Verified	Name, Address, DoB match
Evidence - Rules Applied	Trust F/W Electronic Record Policy
Issuer	Credit Reference Agency
Who can read?	ID Provider
Credential Validity	Start Date / End Date
Signature	############

Digitized Credential

Claims	No Fraud Flag
Evidence - Type	Counter Fraud Check
Evidence - How Verified	Name, Address, DoB match
Evidence - Rules Applied	Trust F/W Fraud Policy
Issuer	Anti-Fraud Agency
Who can read?	ID Provider
Credential Validity	Start Date / End Date
Signature	############

Digitized Credential

Claims	No PEP Flag
Evidence - Type	Politically Exposed Person Check
Evidence - How Verified	Name, Address, DoB match
Evidence - Rules Applied	Trust F/W PEP Policy
Issuer	Customer Due Diligence Agency
Who can read?	ID Provider
Credential Validity	Start Date / End Date
Signature	############

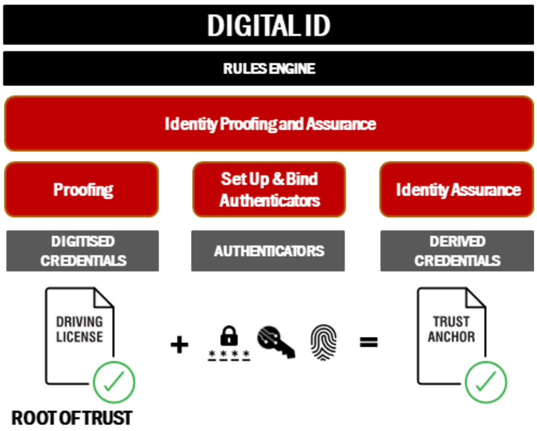
Digitized Credential

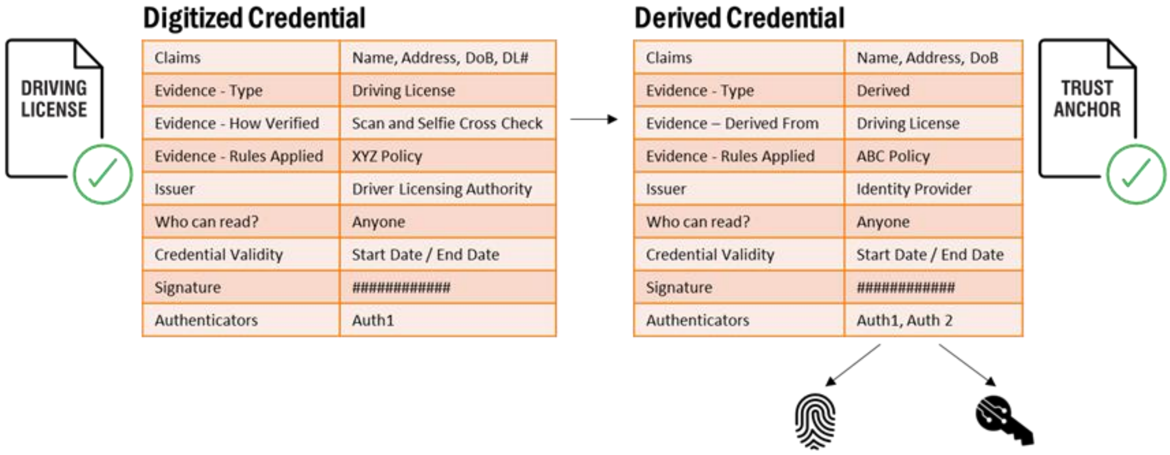
Claims	6 Months Activity
Evidence - Type	Activity Check
Evidence - How Verified	Name, Address, DoB match
Evidence - Rules Applied	Trust F/W Activity Policy
Issuer	Financial Services Company
Who can read?	ID Provider
Credential Validity	Start Date / End Date
Signature	############

Derived Credential

Claims	Name, Address, DoB
Evidence - Type	Derived
Evidence – Derived From	Passport CRA ID Information Counter Fraud Check PEP Check Activity Check
Evidence - Rules Applied	Trust F/W Policy
Issuer	Identity Provider
Who can read?	Anyone
Credential Validity	Start Date / End Date
Signature	############
Authenticators	Auth 1, Auth 2

A ‘trust anchor’ method uses a single trusted credential as the ‘root of trust’ for binding authenticators to the user. This is essentially the same process as the Identity Proofing and Assurance process. The process is illustrated by the following diagrams:





Digitized Credential

Claims	Name, Address, DoB, DL#
Evidence - Type	Driving License
Evidence - How Verified	Scan and Selfie Cross Check
Evidence - Rules Applied	XYZ Policy
Issuer	Driver Licensing Authority
Who can read?	Anyone
Credential Validity	Start Date / End Date
Signature	############
Authenticators	Auth1

Derived Credential

Claims	Name, Address, DoB
Evidence - Type	Derived
Evidence – Derived From	Driving License
Evidence - Rules Applied	ABC Policy
Issuer	Identity Provider
Who can read?	Anyone
Credential Validity	Start Date / End Date
Signature	############
Authenticators	Auth1, Auth 2

The result of this process is a trusted user with an assured identity. In some implementations of trust frameworks the level of assurance achieved is recorded against the user and can be presented to the Relying Party as an indicator of trust in the user.

Interoperability between frameworks might be achieved by aligning levels of assurance or determining equivalence between levels of assurance across different frameworks.

10.5.3 Trust Framework Rules Documents

The following are required to support the Trust Rules:

Document	**Type**
identity proofing	Standard
identity assurance	Standard
identity authentication	Standard
eligibility	Policy

11 USER SERVICES

Users Services that the framework should consider are:

		Who?
Choosing a Digital Identity		
Choosing an Identity Provider	The user should be able to understand which Identity Providers are best suited to meet their needs. For example, what ID documents will they need to prove who they are with different Identity Providers. Inclusion is a key consideration – users with little documentary or electronic evidence of their ID must still be able to get an ID, perhaps through a credential issuer who is operating as a vouching service.	Bkr, Tmk
Finding an existing Digital ID	Users may already have an Digital ID with one or more providers. When users first go to a new Relying Party and need to choose a Digital ID to use. Highlighting the provider(s) the user already has an ID with will make the transaction easier for the user and therefore more likely to be successful. Where the user has more than one ID, and a particular level of assurance is required, the IDs with the right level of assurance should be prioritized.	Bkr, IdP
Ensuring the same Digital ID is used when returning to a Relying Party	Consideration needs to be given to how a user might re-access a Relying Party that they have used an ID to establish an account with. This is particularly important where that Relying Party relies upon the ID for on-going access to the Relying Parties' services. Users should be guided to re-use the same ID for subsequent transactions with the same Relying Party. An Access Credential makes this link between a Digital ID and the Relying Party.	RP, Bkr, IdP
Creation and Management of a Digital Identity		
Creating an ID	The user should be able create a Digital Identity. Typical stored data is name, address, date of birth, contact information and any credentials the user gathers to prove their identity and their entitlements.	IdP
Authenticators	Once the user has created a Digital Identity the user should set up some forms of authenticator (e.g. secret, biometric or a token) that only they can use to allow them to re-access their Digital Identity. Additional authenticators of specific types and quality may be required to be set up to allow the user to access and present specific credentials and achieve certain levels of assurance.	IdP
Account Recovery	The user must be able to recover a Digital Identity that they have with an Identity Provider.	IdP
Privacy Policy	The user must understand and agree how the data they provide and store within the Digital Identity is used.	IdP
Maintaining up to date data	The user must be able to update the data held in their Digital Identity at any time. Credentials that expire and need renewing should trigger a reminder to the user. Any changes in the user's data may lead to the need for re-proofing or validation.	IdP
Sharing updates with Relying Parties	The user may be offered a service where they can choose which Relying Parties to send updated verified information to (e.g. a new address). Relying Parties may choose to subscribe to this service.	IdP, RP
Accessibility	All user services should include accessibility options.	IdP
Delegated Authority	The ability for users to be represented by a delegated authority (another user) or advocate of their choice should be considered.	IdP
Closing a Digital ID	The user must be able to close their Digital Identity at any time. Consideration needs to be given to how a user might re-access a Relying Party that they establish an account with using the ID now being closed. This is particularly important where that Relying Party relies upon the ID for ongoing access to the Relying Party's services. Is a replacement ID from another Identity Provider offered?	IdP
Achieving and Presenting Trust		
Gather credentials	The user should be able to collect credentials and store these against their Digital Identity.	IdP, DirIss, IndIss
Establish Trust in digitized credentials	The user should be able to establish trust in their credentials through a Direct Issuer, an Indirect Issuer and / or an identity proofing and assurance process.	IdP, DirIss, IndIss

Interpreting a Relying Parties Rules	The Digital Identity should allow the user to fulfill a Relying Parties rules, or the rules of a trust scheme or framework. It should do this in a way that does not require the user to understand the detail of a rule, be that getting a Digitized Credential from the right type of issuer or deriving a credential to meet more complex rules.	IdP, RA, IdPP
Create Derived Credentials	The Digital ID should be able derive a credential required by a Relying Party. Ideally the Identity Provider should do this in a way that does not require the user to understand the detail of the rule request. For instance, the Identity Provider should work out what digitized credentials the user already has that will allow them to achieve the rule request, and what the gaps are. The Identity Provider should then work out the smartest way to fill these gaps, guiding the user through the process. The IdP solution may ask the user to choose authenticators to use appropriate to rules. The user may need to set up additional authenticators because specific types, and quality of authenticator may be required to allow the user to achieve certain rules. The result may be recorded by the Identity Provider as a Derived Credential.	IdP, RA, IdPP
Achieve a Level of Assurance	For Trust frameworks or schemes that define levels of assurance, the Digital ID should allow the user to achieve this. A Level of Assurance is a special form of Derived Credential the process to create one is the same as above. A The user may not know about level of assurance(s) as this may confuse them.	IdP, RA
Authentication	The user must be able to present to the Relying Party the level of assurance required. This will be by accessing their ID using the appropriate authenticators, refreshing any expired credentials, and then sharing trusted information (including the confirmation of their identity) to the Relying Party.	IdP, AuthP
Access ***Eligibility Credentials***	The Identity Provider should be able to access eligibly credentials for a trusted user and attach this to the user's digital identity for them to present to the Relying Party as trusted *eligibility credentials. This could come from direct or indirect issuers.*	IdP, DirIss, IndIss.
Sharing Trust with a Relying Party	The user should be able to share trusted information from their ID with Relying Parties This includes digitized and derived credentials and (where used) levels of assurance. Selective Disclosure may be applied to credentials so that only the information needed to fulfill a transaction is shared (i.e. Data minimization)	IdP
Accessing Relying Parties again	The user should be able to use their Digital ID to re-access their account with the Relying Party. This could be using an Access Credential issued to them by the Relying Party.	IdP, RP
Data Minimization	The user should not supply an rules agent with more data than is needed to complete the rule assessment process, or supply or share with any Relying Party more data that is necessary to fulfil the purpose of a transaction. Derived Credentials play a major role in data minimization.	IdP, RA
Consent		
Consent	Data must only be shared with a Relying Party using appropriate legal reasons. This is often with the user's consent. When obtaining the users consent best practice is to list the data to be shared with the Relying Party. As this point, the user should be asked to check that the information being shared is accurate and up to date. The user should have an option to change their data at this point; any changes may lead to the need for re-proofing. Subject to local data protection laws, a user's consent for sharing could be one, all or any of the following,: - For many organizations eg a group of organizations in multiple locations - Long lived consent: User consent over time cannot be assumed to continue if the context when consent was acquired changes and consent should be re-requested. An example would be for a time-bounded offer that has expired. - Explicit consent via general terms: the User signifies agreement to share either by a statement in a privacy policy to which they agree - Explicit consent via affirmative action: the User signifies agreement to share by a clear affirmative action at point of data sharing. The reference here to 'consent' is not intended to prevent the processing of data under other legal basis under data protection laws or the use of processors to support those that control data – rather, it is about ensuring that the user is in control when its data is transferred to a Relying Party.	IdP
Consent History	Users should be able to see who their data was shared with, what data was shared, and when.	IdP

Right to be forgotten	Users could request that their data is removed from the records of a Relying Party they have shared their data with. Relying Parties may choose to subscribe to this service.	IdP, RP
Help and Support		
Help	The user should have access to some form of help services, such as a helpdesk or chat service, in order to answer and solve their queries.	IdP, IdPP, DirIss, Bkr
Fraud Detection by the User	The user may detect or suspect that their identity has been stolen. Users should be able to report this to the appropriate party in the framework	Bkr, IdP, IdPP, DirIss, Sch, Fwk.
ID replacement	The user should be able to change Identity Provider at any time. Consideration needs to be given as to what, if any, credentials can be passed from the old IdP to the new IdP. Consideration needs to be given as to how any links maintained (by Access Credentials) between and Relying Parties and the ID are passed over, to maintain continuity of access to those Relying Parties.	RP, Bkr, IdP
ID repair	If the users ID is compromised by a fraudster, or through data breach, comprehensive and swift ID repair procedures must be followed, including notification to the user and any Relying Parties who may have been or could be compromised as a result. Closing down the user’s ID and issuing them with a new ID with new Authenticators if necessary.	IdP
Complaints	There should be a place for users to complain about any issues they feel are not being handled correctly. Complaints should initially be directed at the party the users are interacting with, but escalation is required to the Scheme and possibly Framework level. There needs to be some ultimate arbiter, possibly an independent body.	RP, IdP, IdPP, Bkr, Sch, Fwk
Disputes	Any disputes must be handled swiftly and fairly. An ultimate arbiter is needed: the Scheme, the Framework or an independent body.	RP, IdP, IdPP, Bkr, Sch, Fwk
Compensation	Is there any compensation due to a user if their ID is stolen or they are unable to use it? Each Trust Framework, or maybe more especially trust scheme, will need to consider whether a compensation mechanism is required. The inclusion of compensation could be driven by regulatory requirements or as a commercial feature to attract / assure users and Relying Parties.	RP, IdP, IdPP, Bkr, Sch Fwk

To support these user services the following policies, procedures or standards are required:

Document	**Type**
Privacy Policy	Policy
Creating and Maintaining a Digital Identity	Procedure
Collecting and Presenting credentials	Procedure
Help and Support Procedure	Procedure
User Support Record Keeping	Policy
Complaints Procedure	Procedure
Dispute Procedure	Procedure
Identity Repair Procedure	Procedure
Compensation Policy	Policy
Compensation Procedure	Procedure

12 RELYING PARTY SERVICES

Relying Party Services that the framework should consider are:

		Who?
User Access to Identity Service		
Allowing the user to access services in the framework.	The Relying Party should enable the user to select to use a service from the framework as part of their on-boarding or logon processes. The Trustmark will be used to communicate use of the framework to the user. The Relying Party must comply with the rules for presentation and use of the Trustmark. To make this as easy as possible for the Relying Party, an SDK might be offered.	Bkr, IdP, Ver.
Requests and Responses (API)		
Credential Request.	The Relying Party should be offered a consistent way to request services from the framework. Request types might include: 1. Specific Digitized Credentials 2. Derived Credentials – zero knowledge 3. Derived Credentials - with evidence 4. Rules to apply to derive a credential: RP own rules or IdP offered rules.	Bkr, IdP, Iss. Ver
Credential Request Response.	The Relying Party should receive a response to their requests in consistent way, regardless of the user's choice of Identity Provider or credential issuer, or any different technical implementations within the ecosystem. The response should include (depending on the request): ● Credentials, including claims, and their verification status ● Other Credentials used to create a Derived Credential ● Assurance Model, Policy Used and Evidence to support assurance	Bkr, IdP, Iss. Ver
Relying Party Based Identity Assurance		
Assessment of Strength of Identity	Where the Relying Party is undertaking this process for the user themselves, they will need access to the assurance policy. Ideally the Relying Party should so this in a way that does not require the user to understand the assurance policy. For instance, the Relying Party ID solution should work out against the assurance policy what trusted credentials the user already has that will allow them to achieve that level of assurance, and what the gaps are. The Relying Party ID solution should then work out the smartest way to fill these gaps, guiding the user through the process.	Fwk, Sch.
Set Up Authenticators	Where the Relying Party is undertaking this process for the user themselves, they will need access to the assurance policy. The user should set up to the authenticators that are appropriate to manage and assert their Relying Party specific identity as defined in the assurance policy.	Fwk, Sch.
Bind Authenticators	Where the Relying Party is undertaking this process for the user themselves, they will need access to the Assurance Policy. The authenticators of the level of quality and type required to meet the assurance policy should be attached to the ID in the same transaction, as the identity proofing is achieved in order to establish the level of assurance – this is known as "binding".	Fwk, Sch.
Liability		
Liability Model	The Relying Party needs to know whether, or not, any other party will take any liability in the event of various failure scenarios occurring. These include, but are not limited to: data breach, theft of an identity, unavailability of service. The higher the risk and value of the Relying Party's transaction, the more likely that the Relying Party will seek some form of acceptance of liability in the event of failures by the parties in the framework. This may be "fault based" liability, where if the party with a failure can demonstrate that it followed all the rules of the framework, it will not be held at fault. Thus, liability would only be placed on that party in the event any rules are proven to have been breached. Liability, if in place, may also be subject to caps. Liability is a commercial matter that a trust framework might be fairly neutral upon, and leave to a trust scheme to implement.	Fwk, Sch.
Liability Claims	In the event of a failure the Relying Party will need a procedure to follow in order to pursue a claim. The details of the procedure may vary depending on the type, scale and value of the claim. An escalation path to an ultimate arbiter in the framework is required, before deferral to the legal framework in the territory of the claim.	Bkr, IdP, IdPP, Ver, Fwk or Sch
Service Levels		

Service Level Agreement	In order to offer a consistent level of service to users, Relying Party must have some surety of system availability, support availability (incl help desk) and response times. This may be a competitive feature offered by trust schemes or individual brokers.	Sch, Bkr, IdP, IdPP, Iss Ver
Service Level Monitoring	Management information on service performance should be provided to the Relying Parties through their prime contract points within the trust framework ecosystem.	Bkr, IdP, IdPP, Ver.
Compensation for poor service	Frameworks, or trust schemes, should consider whether any compensation should be offered to Relying Parties who receive poor service. This may also be a competitive feature offered by trust schemes or individual brokers.	Bkr, IdP, IdPP, Ver.
Help and Support		
ID replacement	The user should be able to change Identity Provider at any time. Any links that are maintained between a Relying Party and ID must be updated in order to maintain continuity of access to accounts within Relying Parties.	Bkr, IdP,
Relying Party Fraud Detection	A Relying Party may detect that an identity it is relying upon has been stolen. It should be able to report this to the appropriate party in the framework	Bkr, IdP, Iss, Sch, Fwk Ver
Complaints	There should be a place for Relying Party to complain about any issues they feel are not being handled correctly. Complaints should initially be directed at the party the Relying Party is interacting with, but escalation may be required to the Scheme and possibly Framework level. There needs to be some ultimate arbiter, possibly an independent body.	IdP, IdPP, Bkr, Sch, Fwk
Disputes	Any dispute must be handled swiftly and fairly. An ultimate arbiter is needed: the Scheme, the Framework of an independent body.	IdP, IdPP, Bkr, Sch, Fwk
Compensation	Is there any compensation due to a Relying Party if IDs that it relies on are compromised or the service is unavailable? IDs might be compromised through ID theft or data breach. Each trust framework, or maybe more especially trust scheme, will need to consider whether a compensation mechanism is required. Its inclusion could be driven by regulatory requirements or as a commercial feature to attract / assure users and Relying Parties.	IdP, IdPP, Bkr, Sch, Fwk

To support these Relying Party services the following policies, procedures or standards are required:

Document	Type
Liability Policy	Policy
Liability Claims Procedure	Procedure
Request and Response Standards	Standards
Level of Assurance determination by Relying Party	Procedure
Service Levels	Policy
Service Level Monitoring	Procedure
Help and Support Procedure	Procedure
Complaints Procedure	Procedure
Dispute Procedure	Procedure
Identity Replacement Procedure	Procedure

13 GENERAL REQUIREMENTS

The following general requirements support the User and Relying Party services, and align with the Trust Rules.

The framework should consider general requirements around:

		Who?
Privacy		
Respecting Users Privacy	The trust framework must include appropriate privacy protection and controls for the user and their data, including terms required to support compliance with applicable data protection laws	IdP DirIss IndIss RA, IdPP RP
Privacy Policy	The framework must create a model privacy policy, or model terms, that framework participants are required to implement.	IdP DirIss IndIss RA, IdPP RP
Record Keeping		
Record Keeping	Records should be kept of the credentials gathered by the user and how these were used to create derived credentials. Records of what authenticators were connected to the user for what purpose should be also kept. This would include any updates to the user's Digital Identity. Records keeping forms a history of how the user created, managed and used their Digital Identity. Access to this information might be vital in terms of fraud investigation or dispute resolution. The period of retention for records the user owns should be able to be managed by the user, taking any overarching data protection legislation into account. The method of retention might be dependent on technical implementation: some implementations might write records (or pointers to records) to a block chain for instance, whilst others may keep them separately in the cloud.	IdP IdPP DirIss IndIss RA
Record Keeping – for Relying Parties	Relying Parties may require that an Identity Provider, issuer or rules agent keeps records of the credentials gathered by for derived for the user. The period of retention for records should be agreed, taking into account any overarching data protection legislation, user choice, and the period of time the Relying Party needs to rely on the identity (evidence).	IdP idPP DirIss IndIss RA
Record Keeping – User Help and Support	Appropriate records of any support interaction with the user should be kept. Records may be required to support investigations into fraud or prove user actions / decisions.	IdP, IdPP. Bkr, DirIss, Sch, Fwk
Audit and MI		
Audit Trial	In order to track movement of data through the ecosystem and ensure the integrity of the trust framework each role must keep appropriate audits records including: creations, updates, deletions, credential gatherings and presentations, assurance assessments, authenticator issue and use.	Bkr, IdP, IdPP, DirIss, IndIss, RA.
Liability		
Liability Model	The Relying Party needs to know whether, or not, any other party will take any liability in the event of various failure scenarios occurring. These include, but are not limited to: data breach, theft of an identity, unavailability of service. The higher the risk and value of the Relying Party's transaction, the more likely that the Relying Party will seek some form of acceptance of liability in the event of failures by the parties in the framework. This may be "fault based" liability, where if the	Fwk, Sch.

	party with a failure can demonstrate that it has followed all the rules of the framework, it will not be held at fault. Thus, liability would only be placed on that party in the event any rules are proven to have been breached. Liability, if in place, may also be subject to caps. Liability is a commercial matter that a trust framework might be fairly neutral upon, and leave to a trust scheme to implement.	
Liability Claims	In the event of a failure the Relying Party will need a procedure to follow in order to pursue a claim. The details of the procedure may vary depending on the type, scale and value of the claim. An escalation path to an ultimate arbiter in the framework is required, before deferral to the legal framework in the territory of the claim.	Bkr, IdP, IdPP, Ver, Fwk or Sch
Fraud and Cyber Controls		
General Considerations	The whole ID ecosystem represented within the framework needs to be protected from cyber-attack and identity fraud. Bringing identity services into a single framework where a user has reusable identities that can access many different Relying Parties generates a "honey pot" for fraudsters and cyber attackers – so the defenses implemented within the framework must be robust. But they must also be proportionate – data sharing for fraud prevention purposes must be minimized to that which is necessary to ensure fraud defense. Most of the roles in the ecosystem will have some responsibility in managing fraud and cyber risk. Consideration should be given to a separate role of Fraud Management within the framework. This could be a central operational function collating and disseminating fraud attack information across the ecosystem and dealing with detected frauds. This could be an operational function of the trust framework, trust scheme or at a broker level.	Fwk, Sch
Cyber-attack detection	Any system or service vulnerability or externally accessible point of the ecosystem must have appropriate cyber-attack controls in place, which have been implemented in accordance with a recognised cyber security standard.	Bkr, IdP, IdPP, DirIss.
Fraud attack detection	A set of robust fraud detection and prevention tools should be installed across the system. Types of fraud to the considered would be: Identity Fraud - including ID theft, muling and synthetic IDs. Points in the process to be covered: ● Registration ● Account Management ● Logon Particular attention should be paid to any fraud vulnerabilities in non-happy-paths, such as pausing then resuming the ID proofing process or account take over through the helpdesk. The following data should be considered for assessment for fraud risk: user provided PII, user provided evidence for proofing and eligibility, ID Risk indicators, meta-data about the transaction (such as device footprints).	Bkr, IdP, IdPP, DirIss
Relying Party Fraud Detection	A Relying Party may detect that an identity it is relying upon has been stolen. It should be able to report this to the appropriate party in the framework	Bkr, IdP, IdPP, DirIss, Sch, Fwk
Informing Relying Parties about a detected fraud.	When a fraud is detected, if the ID is relied upon by any Relying Party they must be informed about the fraud. A procedure of what action needs to be taken needs to be defined.	Bkr, IdP, IdPP, DirIss, Sch, Fwk
User Fraud Detection	A user may detect or suspect that their identity has been stolen. They should be able to report this to the appropriate party in the framework	Bkr, IdP, IdPP, DirIss, Sch, Fwk
Informing a User about a detected fraud.	When a fraud is detected, any users effected must be informed. The ID repair procedure in User Services should be followed.	Bkr, IdP, IdPP, DirIss, Sch, Fwk

Sharing attack information across the ID ecosystem	Fraudsters will attack different points in the ecosystem to find and exploit vulnerabilities. Sharing of attack information between Identity Providers, brokers and credential issuers helps find and defend these vulnerabilities.	Bkr, IdP, IdPP, DirIss, Sch, Fwk
Sharing attack information with other sectors / agencies	Fraudsters will not only attack this trust framework ecosystem. They already attack traditional Relying Party-based ID solutions today. Consideration should be given to sharing attack information with other groups or agencies that work to prevent fraud across the whole digital and non-digital ecosystem for a territory.	Bkr, IdP, IdPP, DirIss, Sch, Fwk
Responding to and Investigating Incidents	When a fraud is suspected or found, the affected parties will need to support the investigation process, take action to close digital identities down and inform other affected parties, and also provide evidence from their records for investigatory and possibly prosecution purposes.	Bkr, IdP, IdPP, DirIss, Sch, Fwk
ID Legal status		
Paper vs Digital	Today paper ID documents, issued by governments, provide individuals of evidence of legal status in a nation state. As these documents are prepared and issued by governments, in accordance with internationally recognized standards, this provides trust that others can rely on in the identification of an individual. The framework has to be able to provide the same trust representation from a Digital ID by articulating how a Digital ID is created to the same trustworthy manner as paper ID documents. To achieve this there may be statutory or regulatory changes in nation states to make Digital IDs, created under frameworks, legally admissible.	

To support these general requirements the following policies, procedures or standards are required:

Document	**Type**
Record Keeping	Policy
Audit	Policy
Supporting an Investigation	Procedure
Fraud and Cyber Controls	Policy and Procedure

14 TECHNICAL AND SECURITY RULES

The following Technical and Security requirements support the User and Relying Party Services and align with the Trust Rules and General Requirements:

		Who?
Security Rules		
Security Policy Definition	The rules applicable to each party in the framework need to be defined, from Relying Party through to issuer These need to include rules for: • Data at rest • Data in transit • Operational Security management Implementation of an ISO27001 standard Information Security Management System (ISMS), or similar (such as NIST Cyber Security Framework, COSO Integrated Framework or the NCSC Cyber Assessment Framework), should be considered for key parties such as Identity Providers, Credential Issuers and Brokers.	Fwk, Sch
Security Policy	All operational parties in the eco-system must comply with a Security Policy that has been approved by the Trust Framework through internal certification processes.	IdP, DirIss, IndIss, RA, IdPP, Bkr, RP.
Trust Registry of eco-system participants		
Trust Registry	The implementation of some form of registry to control who can participate in the ID ecosystem governed by the trust framework will ensure mutual trust between parties at a technical-transactional level, and will protect the ecosystem from bad-actors.	Fwk, Sch
Trust Registry Entries	All operational parties in the ecosystem must be entered onto the Trust Registry. The role of the party should be recorded.	IdP, IdPP, AuthP, DirIss, IndIss, RA, Bkr, RP.
Trust Registry Checking	Each transaction must check the Trust Registry to ensure the parties involved are permitted and are playing the role assigned to them.	IdP, IdPP, Iss, Ver, Bkr, RP.
Recording and Presentation of Chain of Trust		
Chain of Trust Recording Policy	How the Chain of Trust and evidence are recorded, in terms of the gathering, deriving, and presenting credentials should be defined. The user of cryptographic techniques to ensure evidence cannot be tampered with should be considered.	Fwk, Sch
Chain of Trust Recording	Parties creating, deriving, and presenting credentials must record this in a secure consistent way.	IdP, Ver.
Recording Proofing Scores	Where a scoring model is used as part of proofing a record should be kept of who determined the score for each credential used in the Assurance Policy.	IdP, RA
Request and Response Schemas		
Schema Definition	In order to ensure credentials are delivered to Relying Parties in a consistent way, standard request and response schemas should be defined. This is particularly important in a framework that supports multiple Identity Providers, or multiple issuers who issue the same type of credential Consideration should be given to globally defined schemas from organizations such as The Open Identity Foundation ID Assurance profile and W3C Verifiable Credentials. However, localization will almost certainly be required for many credential types. The framework should implement a clear curator for locally applicable schemas.	Fwk, Sch
Request / Response Schemas	Identity claims and evidence should be in a consistent format across the framework, regardless of the technical protocol used to deliver the credentials	IdP, Ver.

To support these Technical and Security Services the following policies, procedures or standards are required:

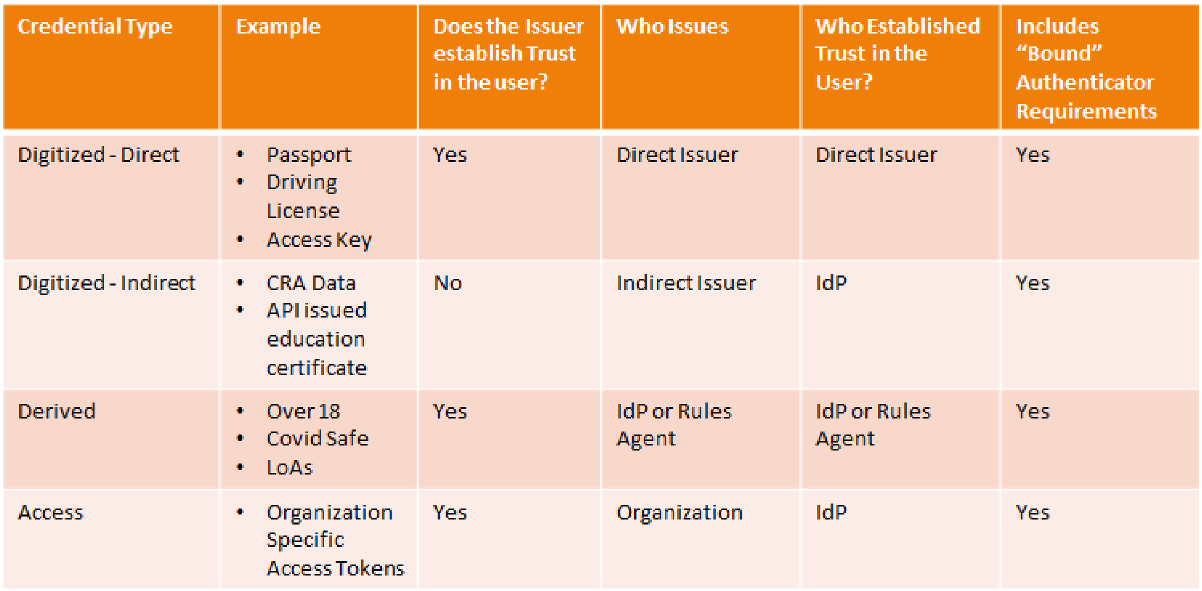
Document	Type
Security Policy	Policy
Proofing Policy	Policy
Trust Registry	Procedure
Request and Response Schemas	Standard

14.1 Chain of Trust

There are two questions that need to be answered when tracing the chain of trust for a credential:

- Who issued the credential?
- Who established trust in the user?

The tracing of trust varies depending on the type of credentials issued. The following table highlights the 4 types of credentials defined in this guide, and how the chain of trust works for each:



Credential Type	Example	Does the Issuer establish Trust in the user?	Who Issues	Who Established Trust in the User?	Includes "Bound" Authenticator Requirements
Digitized - Direct	• Passport • Driving License • Access Key	Yes	Direct Issuer	Direct Issuer	Yes
Digitized - Indirect	• CRA Data • API issued education certificate	No	Indirect Issuer	IdP	Yes
Derived	• Over 18 • Covid Safe • LoAs	Yes	IdP or Rules Agent	IdP or Rules Agent	Yes
Access	• Organization Specific Access Tokens	Yes	Organization	IdP	Yes

15 INTEROPERABILITY REQUIREMENTS

When considering interoperability, there are two dimensions to consider - internal interoperability within the framework and external interoperability with other frameworks.

15.1 Internal Interoperability

One of the key purposes of a Trust Framework is to achieve interoperability of identity services across different use cases and sectors, principally ensuring a User can present their identity to many different organizations in a simple, seamless way.

When constructing the framework, a key design choice is whether to include the concept of schemes and whether those schemes are separately administered from the framework.

If a separately administered trust scheme model is implemented, then to ensure interoperability the framework will need to set some rules that all schemes must adhere to. Rules to consider setting at the framework level include:

- Application of Principles
- Trustmark Rules
- Trust Rules and model, but perhaps leave the setting of acceptable scores within the model for particular use cases to the trust scheme.
- Technical Rules such as used of common levels of Security and common schemas

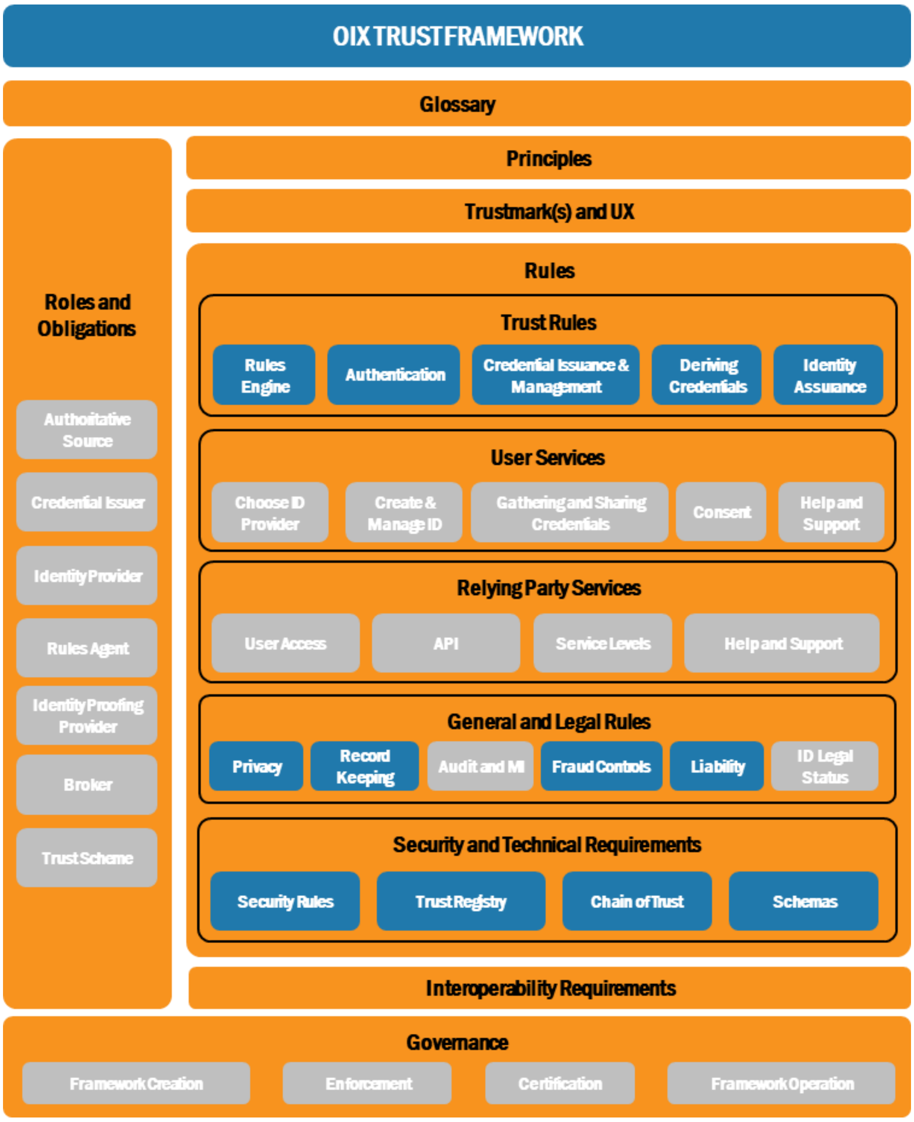
Interoperability can also be achieved through parties such as Identity Providers or credential issuers becoming compliant with more than one trust scheme.

15.2 External Cross Framework Interoperability

External interoperability with other trust frameworks can be achieved in three ways:

- Bilateral agreements between frameworks to mutually recognize the trust that they ensure.
- Through a node approach, where some agent enables many frameworks to trust each other through independently assessing their alignment and compatibility.
- Through parties such as Identity Providers or credential Issuers becoming compliant with more than one trust framework.

The node approach is a more efficient way of ultimately achieving mass interoperability between frameworks as it only requires each framework to align to commonly agreed rules. The node approach essentially creates an overarching trust framework, or a “framework of frameworks”.



The key areas that need to be designed and implemented with interoperability between frameworks in mind are:

- Application of Framework Principles
- Trustmark Rules
- Trust Rules
- Privacy Rules
- Record Keeping
- Fraud Controls
- Liability
- Request and Response Schemas
- Trust Registry
- Chain of Trust
- Security Standards

16 GOVERNANCE OF THE TRUST FRAMEWORK

16.1 Creation and Management of a Trust Framework

Someone (a person, an entity, a group, or a committee) must be charged with the task of writing the Trust Framework, and someone (not necessarily the same person or group) should be assigned responsibility thereafter for updating and maintaining it as necessary to meet future needs.

The authorship and control over the content of a Trust Framework is often a function of the nature and structure of the Trust Framework implementation itself. In some cases, this may be assigned to the legal entity establishing the framework, or a separate legal entity charged with the task of managing it. In other cases, a trust framework may be written by a consortium of participating entities that mutually agree on rules and regulations, or by a committee of participants elected to oversee accountability and governance.

Common examples of possible authors for a Trust Framework include the following:

- **Independent Governing Entity:** For some Trust Frameworks, an independent entity may be formed or designated for the specific purpose of developing, maintaining, and enforcing an appropriate trust framework. This typically occurs in the case of a large-scale identity system that includes numerous Identity Providers and Relying Parties. Such an entity is commonly referred to as a Trust Framework provider, operator or authority. An example is the Digital ID and Authentication Council of Canada (DIACC) a non-profit coalition of public and private sector leaders. DIACC defines and manages the Pan-Canadian trust framework.
- **Consortium of Participating Entities:** In other cases, a group consisting of some, but not necessarily all, of the participating entities will convene to draft, and update as needed, the appropriate Trust Framework. An example of this is provided by the CA/Browser Forum, which consists of a group of browser vendors and certification authorities that jointly agrees upon the trust framework for a system focused on recognition of trust roots for website server and related domain name owner identification.
- **Single Participant Governing Entity:** In some cases, a single existing organization (typically an entity acting as either the sole Identity Provider or the sole relying organization) both establishes the Trust Framework and acts as a participant for its own specific purposes. As the strong central entity, it dictates the architecture, policies and contractual structure of the trust framework, and may also manage and operate a technical platform, which supports the interactions among the participants. Examples include single Identity Provider systems, such as those operated by Google and Facebook, and single Relying Party systems, such as those operated by the US government's Login.gov program or the UK government's GOV.UK Verify program.
- **Non-Governing Standards or Certification Organization:** In some cases, an independent entity may be established to develop (and update from time-to-time) standard rules for a Trust Framework , but such entity will not itself actually govern the operation of a framework. It may, however, certify participants (particularly Identity Providers) as compliant with its system rules. Examples of this approach include the identity assurance Framework issued by the Kantara Initiative, and the tScheme Approval profiles issued by tScheme.
- **Mutual Agreement Among All Participants:** In smaller scale Trust Framework, system rules can be jointly negotiated by the participants (or written by a dominant participant), and memorialized in a mutual agreement. In such case there is no separate governing entity, but simply an agreement between and among all of the participants.

16.2 Enforceability of a Trust Framework

A Trust Framework is of no value unless the participants in the identity system that it purports to govern are legally obligated to follow the rules set out in the trust framework – i.e., it must be enforceable

In some cases, the rules of the Trust Framework can be made binding by law or regulation. Likewise, depending on the technologies and procedures specified by the Trust Framework, policies may also be enforced by systems, software and applications. But in most cases, the rules of a trust framework are private law that can be made enforceable only by voluntary agreement of the parties.

Thus, once a Trust Framework is written, a key challenge is establishing a mechanism to ensure that all participants within the scope of its rules are legally bound in a manner that makes the portion of the rules relevant to their role enforceable against them. And ideally, each participant should be legally obligated to follow the rules of the framework for the benefit of all other affected participants in the framework (including the end users) even though each participant will not enter into a separate contract directly with all such other participants. This is usually accomplished as follows:

- In the case of the private sector, the governing trust framework is usually made enforceable by some sort of contractual mechanism. Many approaches can be used, although one of the more common approaches is to develop a master set of framework rules (set out in one or more documents), which all parties agree to through the use of a simple form contract that references or incorporates the rules by reference.
- In the case of government sector or government-sponsored frameworks, the governing trust framework may take the form of a statute or regulation. In such cases, the terms of the trust framework are binding on the participants by law.
- Trust frameworks for public-private partnerships might rely on a contract-based approach, or a hybrid form might be used, where the foundation and main principles are based in law, but certain specific role-related requirements are enforceable through agreements.

In some cases, trust frameworks are not made legally binding on certain roles, such as end users or credential issuers, although the trust framework may regulate the conduct and responsibilities of other participants relative to those roles. For example, in some cases users do not contractually agree to the terms of the trust framework itself. However, the trust framework may impose on Identity Providers an obligation to enter into a contract with such users that contains certain terms or imposes certain requirements.

16.3 Certification to a Trust Framework

Participating entities in the framework may need to be certified in some way to demonstrate that they are compliant with the obligations the framework defines for the role(s) that that participating entity is playing. Types of approval include:

- **Self-Assessment.** The participating entity self declares compliance with the framework.
- **Verified Self-Assessment.** An independent body or automated tool verifies the participating entities self-assessment. The independent body is not a formal certification body and takes no liability for that verification.
- **Approved.** The participating entity demonstrates how it meets the requirements of the trust framework through documentation, demonstration and inspection by an independent body.
- **Certified.** The participating entity demonstrates how it meets the requirements of the trust framework through documentation, demonstration and inspection and is formally certified by an independent body.

The type of approval required will depend on what level of regulatory compliance, and protection against fraud and financial risk, the framework is offering the user and Relying Party.

16.4 Operation of a Trust Framework

The need for one or more operational roles depends on the complexity and maturity of the trust framework implementation.

At a minimum, someone must be responsible for developing and maintaining the trust framework itself, and amending it when changes are required, or new issues arise.

In more complex frameworks, with a large network and many types of participating entities offering many different services, there may also be a need to provide for additional governing roles to address a variety of other governing functions, such as:

- **Governance and Policy Development:** Developing and amending legislation; policies; decision-making; stakeholder-facilitation; managing standards and procedures; accountability mechanisms.
- **Policy Enforcement:** Ensuring compliance with existing policies; enforcement mechanisms; performing assessments or audits; managing changes and releases.
- **Participating Entity Management:** Administration and enrolment of participating entities; Certification and trust marks; support; dispute resolution; billing.
- **Network Evolvement:** Growing and supporting the network; marketing; communication and; developing strategy.
- **Trust Framework Operations:** Offering central services to the participating entities and/or public, e.g. fraud management, information and discovery services.

In many cases these functions can be addressed by a designated separate legal entity (like Visa, Inc. does for the Visa credit card system). In other cases, a cooperative consortium might fill one or more of the governing roles or a committee established by the participating entities.

The roles tasked with performing these functions are sometimes referred to as a Trust Framework Provider, Trust Framework Authority, Policy Authority, or Trust Framework Operator (depending on their specific functions).

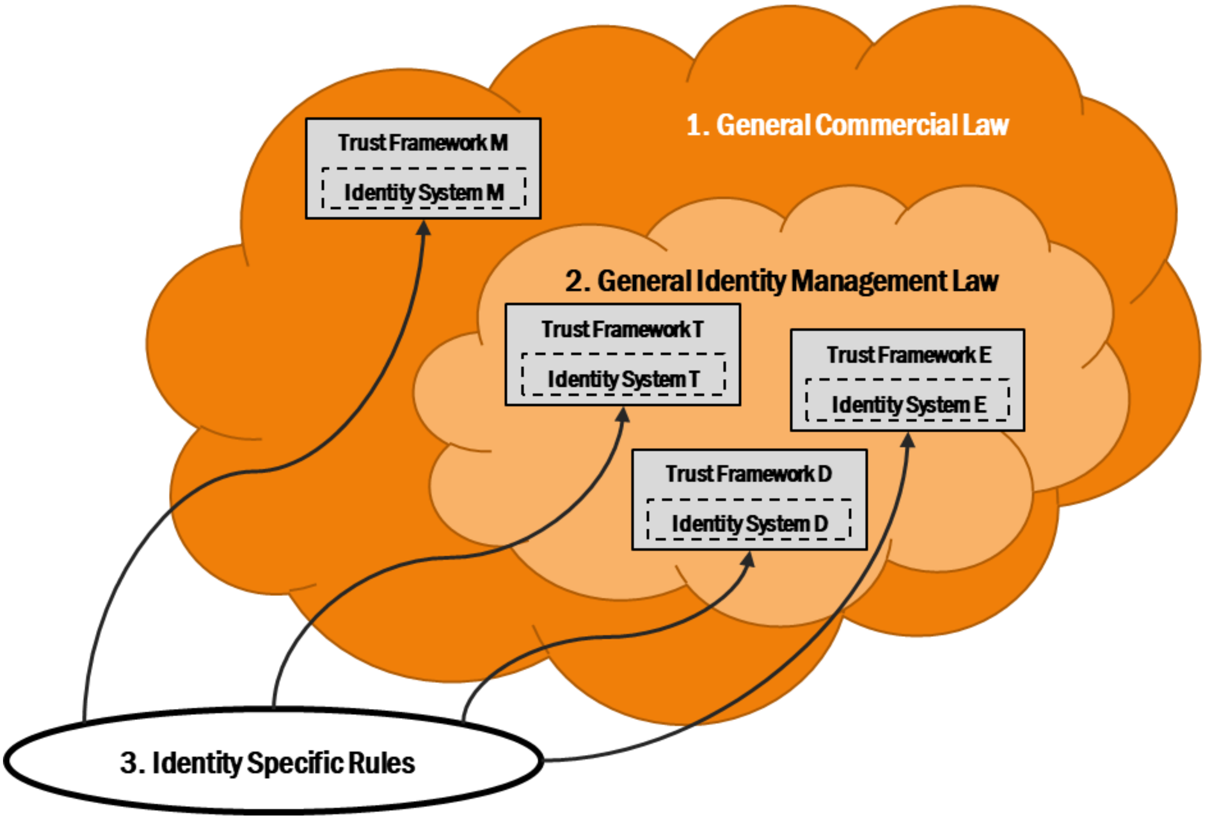
17 THE LEGAL CONTEXT OF AN IDENTITY TRUST FRAMEWORK

The role of a Trust Framework in the overall legal framework for identity is much like the role of a sales contract in the overall legal framework governing the sales of goods. That is, it is written to address the specific issues of a particular identity system, but is also subject to, and governed by, more general higher-level law.

Identity systems and identity transactions, like most commercial systems and commercial transactions, are typically governed by up to three levels of different legal rules. These legal rules may be generally described as follows:

- **Level 1 - General Law:** The first (and foundational) level of legal rules applicable to identity systems and transactions is existing general law. This consists of the rules enacted as statutes by legislatures, adopted as regulations by government agencies, or determined by judicial decision. Such law was not written for identity systems, but is frequently applied to them to the extent it relates generally to the activities that take place within the identity system. General law includes contract law, tort law, privacy law, export control law, warranty law, consumer protection law, antitrust law, and the like. Such law is public law (i.e., written by governments), applies to all identity systems and their participants by the authority of the government, and is enforceable in the courts. Unfortunately, because it is not written for identity systems, it may not be a good fit, or may yield unanticipated or inappropriate results.
- **Level 2 – Identity Management Law:** The second level of legal rules applicable to identity ecosystems and transactions consists of identity management law. This law (where it exists) is new, is written specifically to govern all identity systems within its scope, and is designed to address one or more of the specific issues that arise in the context of the operation of such identity systems (e.g., participant liability). Very little such law currently exists, but projects are underway in several jurisdictions to develop such Level 2 law for the purpose of encouraging and/or regulating identity systems and identity transactions. An example of such Level 2 law is the Virginia Electronic Identity Management Act. Level 2 law is also public law, and applies to all identity systems and identity system participants that operate within its scope by the authority of the government, and is enforceable in the courts.
- **Level 3 –** Trust Framework **-- Identity System-Specific Rules:** The third level of legal rules applicable is Trust Framework. A trust framework is usually necessary in some form regardless of whether that identity system is operated by a government or a private sector entity. In the case of private sector identity systems (and some public-private identity systems) the trust framework typically takes the form of contract-based rules (i.e., private law) drafted by one or more participants in, or the governing body of, the specific identity system and voluntarily agreed to by the participants. In the case of government operated identity systems, the trust framework typically takes the form of statutes or regulations adopted by the operating government body (most often a country's national ID system, or e.g., the eIDAS Regulation in the EU). In either case, however, these framework-specific identity system rules apply only to the specific identity system for which they were written. Thus, there will be many such trust frameworks. Contract-based trust frameworks must, of course, also comply with the governing legal rules in Level 1 and Level 2. In the case of trust frameworks that exist in contract form, they are binding only on those parties that voluntarily agree to the terms of the applicable contracts. If such rules exist as a statute or regulation, they are binding only on those who are expressly within their scope. In either case, such trust frameworks only apply to one particular identity system.

This legal framework is depicted in the diagram below. As this diagram illustrates, portions of the legal framework for any private-sector identity system (i.e., the Level 3 trust framework portion) are under the control of the developers of that identity system, and other portions (i.e., Levels 1 and 2) are outside of their control. That is, the operators of an identity system are free to make up the Level 3 system rules (so long, of course, as the participants contractually agree to be bound by them), but at the same time, the private contracts that make these system rules binding on the participants are supplemented (and in some cases superseded) by existing laws and regulations. As such, the Level 3 system rules must interface with existing law – a challenge made all the more difficult for identity systems that cross jurisdictional boundaries. Moreover, any issues not addressed by the Level 3 trust framework will be determined by the public law at Level 1 (and Level 2 if it exists).

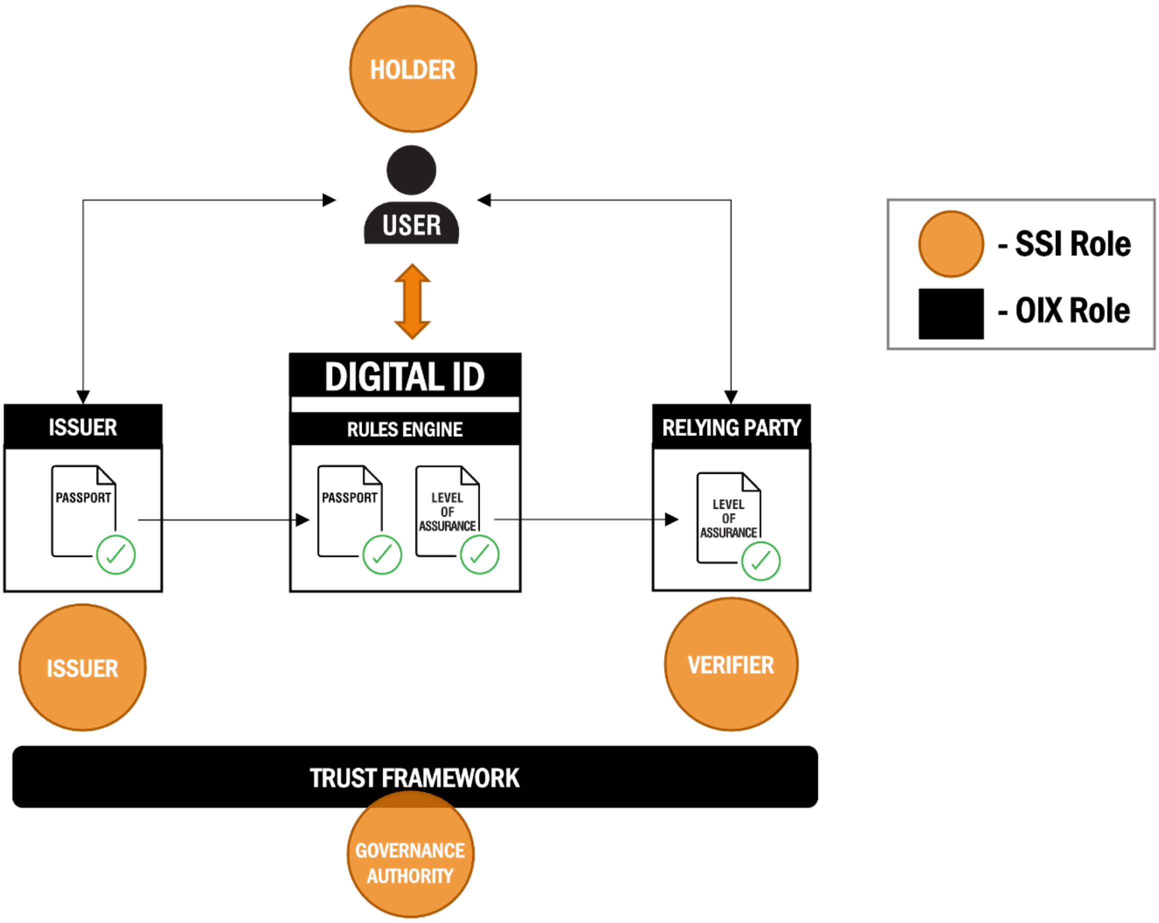


18 MAPPING SELF SOVEREIGN IDENTITY MODELS TO THE TRUST FRAMEWORK

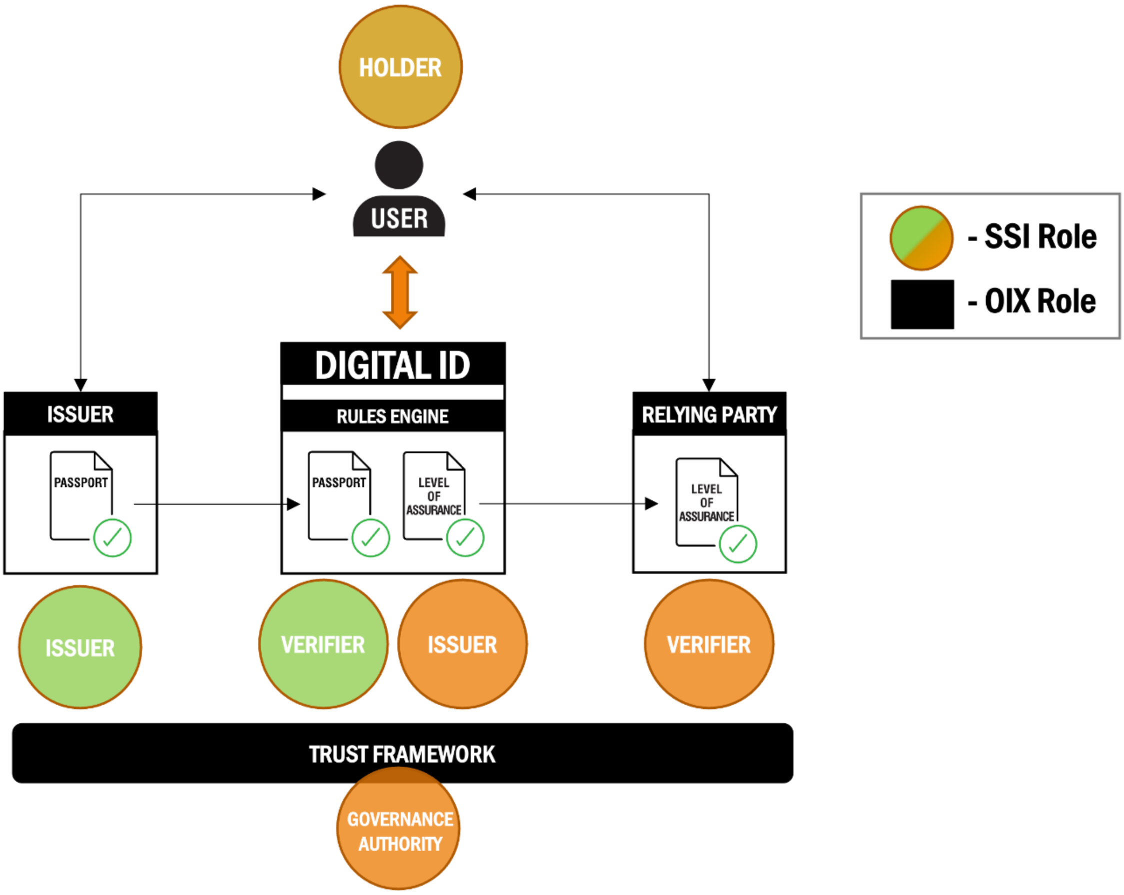
OIX has ensured that this framework model addresses the needs of both 'traditional' centralised identity models and newer Self Sovereign privacy-centric digital identity models.

In the Self Sovereign model the provider of the Wallet the user, or holder, utilises to manage their Digital Identity is likely to take the role of the Identity Provider as described in this guide. Accordingly, a 'Smart Wallet' is required that works for the user to enable the rules of the Relying Party to be easily fulfilled.

The below diagram shows how the roles and constructs used in Self Sovereign models map to a Digital ID as described in this guide:



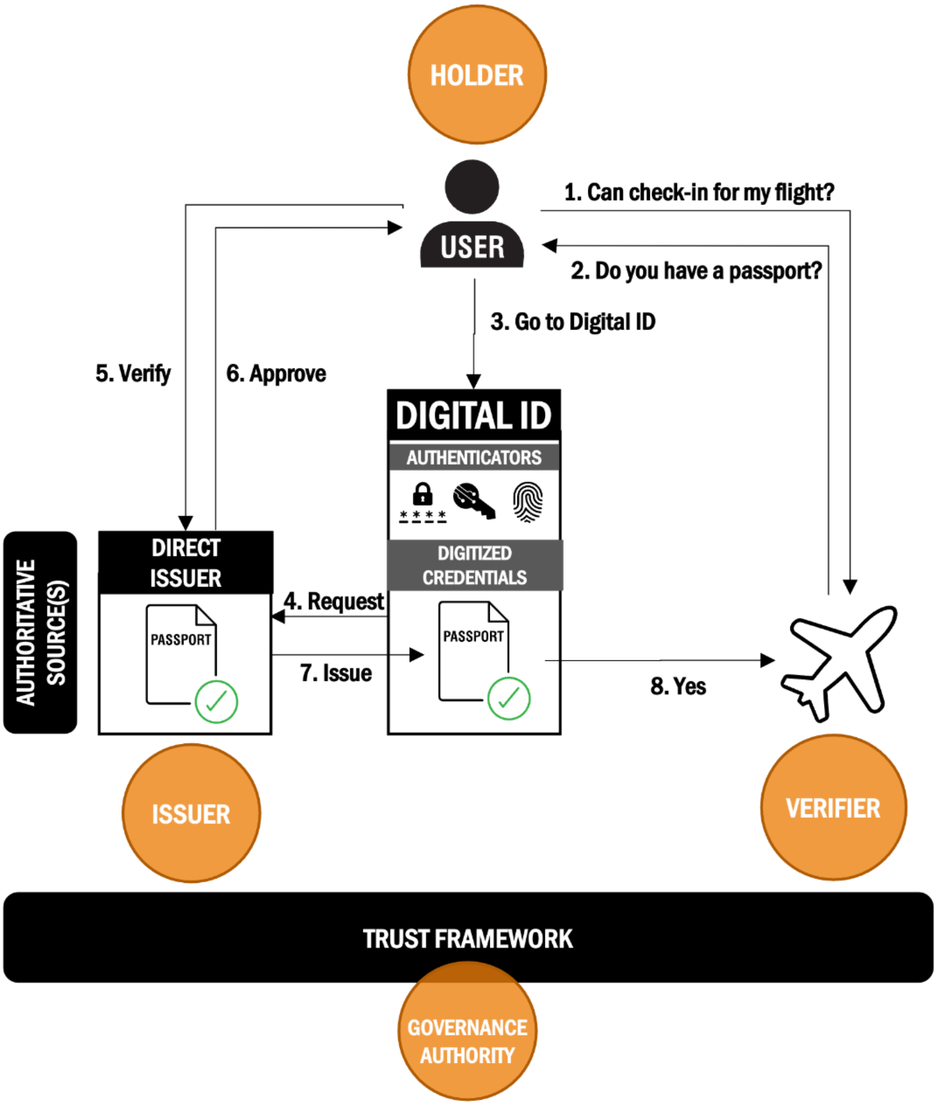
The Digital ID may also play the role of verifier and issuer. For example, when a Derived Credential is issued by a Digital ID after it has verified the Digitized Credential from which the new credential was derived:



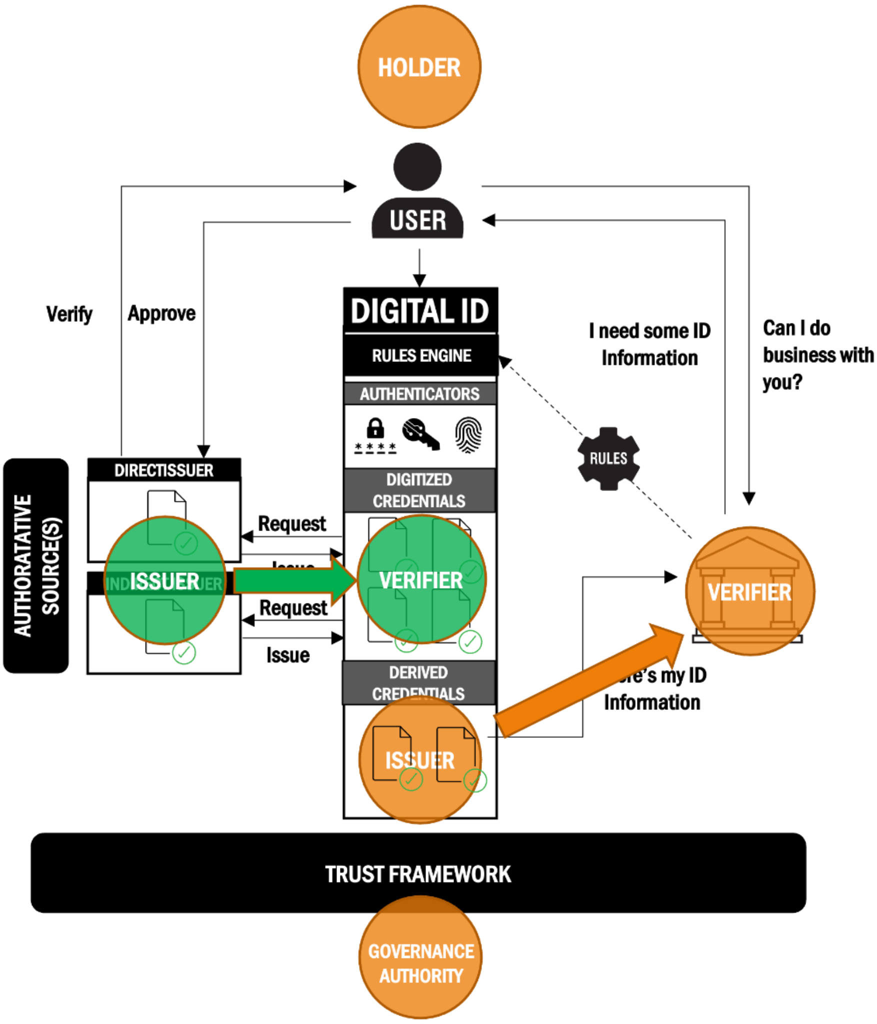
The role of issuer can also be played by a Rules Agent, ID Proofing Provider, or in the case of an Access Credential, the Relying Party.

The below diagrams explore how SSI roles overlay on some of the examples of how a Digital ID works referred to earlier in this guide.

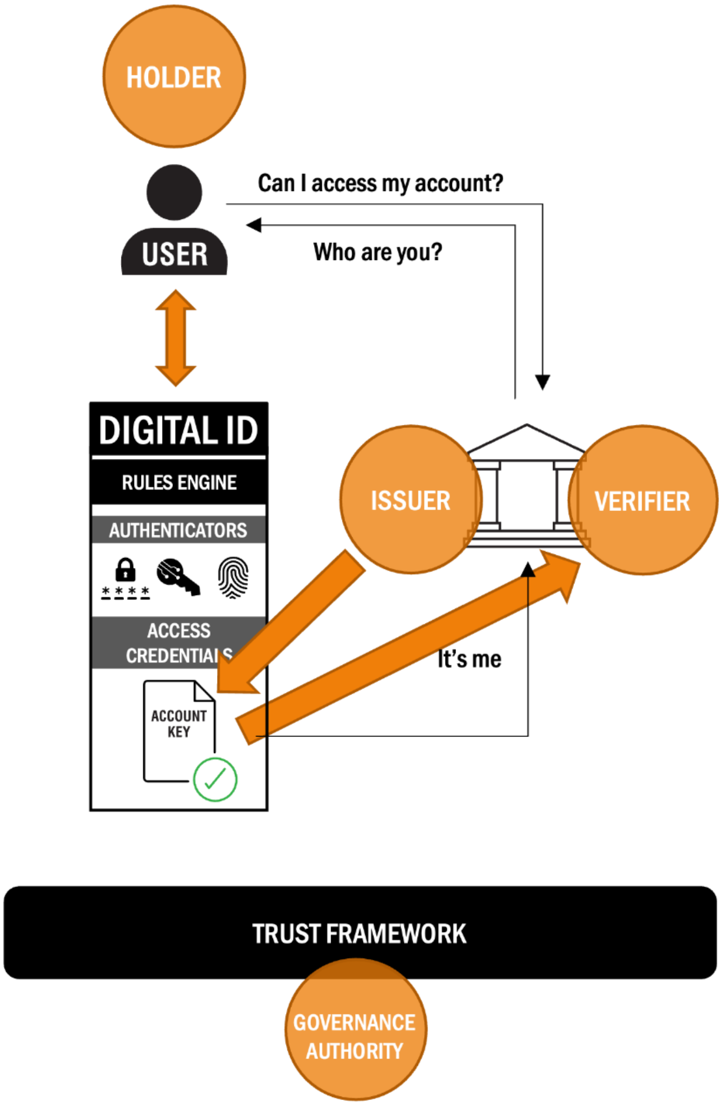
The use of a Passport Digitized Credential is a good example of a single layered self-sovereign transaction:



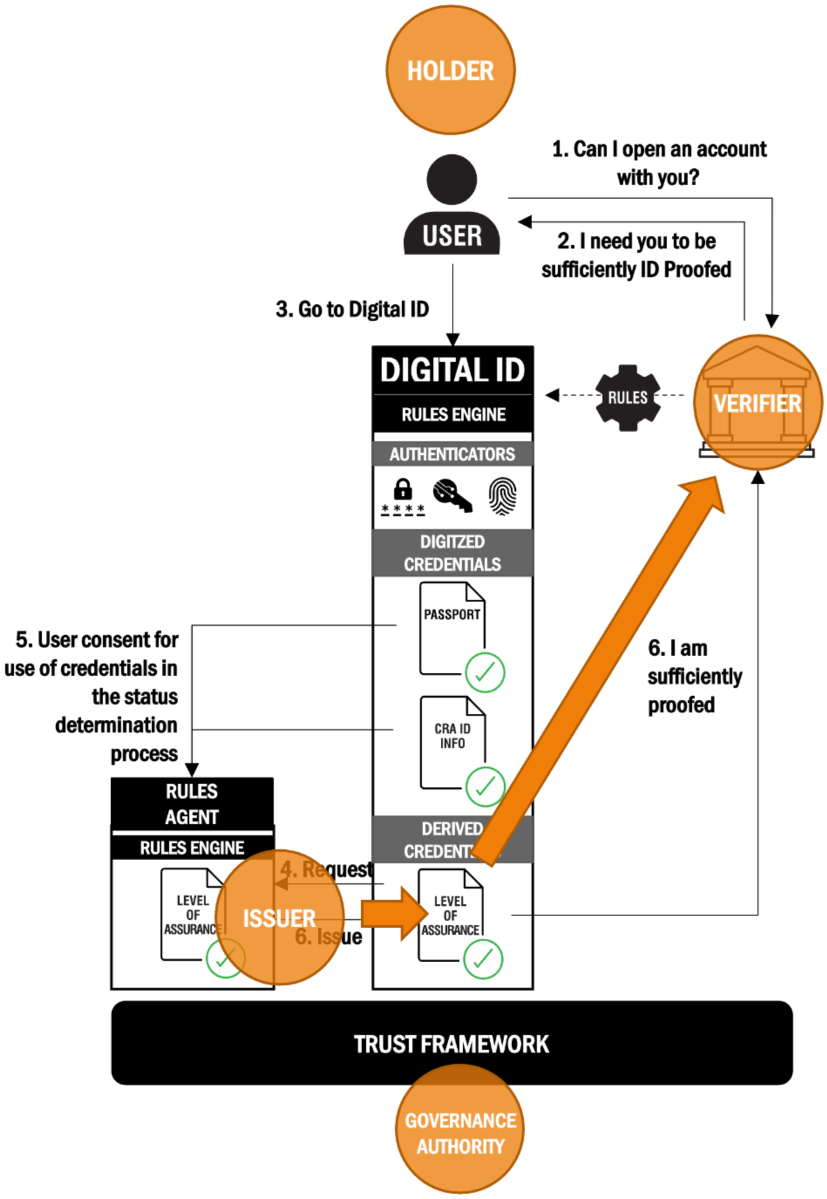
However, once the Digital ID starts to derive credentials, it also plays the role of verifier and issuer, resulting in a more complex picture:



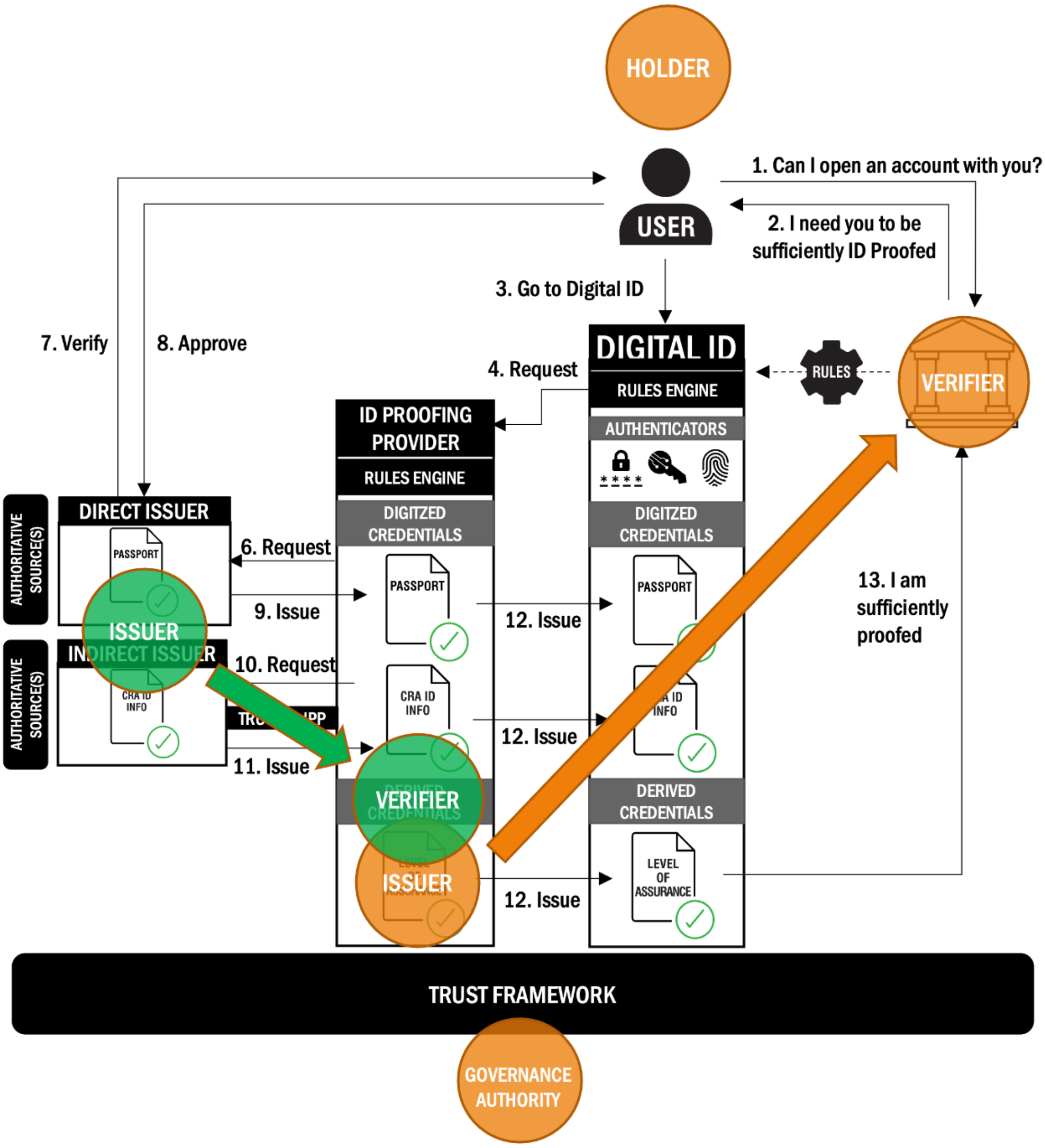
The Relying Party is also an Issuer when it creates an Access Credential for the user to use to access their account with that Relying Party. So it also becomes the verifier of its issued credential:



When a Rules Agent derives a Credential, it becomes the issuer of the Derived Credentials having verified Digitized Credentials:



Equally when an ID Proofing Provider derives a Level of Assurance, it becomes the issuer of the Derived Credential. The ID Proofing Provider is also often the party who triggers the issue of Digitized Credentials on which is the derived Level of Assurance is based:


HOLDER
USER
1. Can I open an account with you?
2. I need you to be sufficiently ID Proofed
3. Go to Digital ID
4. Request
7. Verify
8. Approve
DIGITAL ID
RULES ENGINE
AUTHENTICATORS
DIGITZED CREDENTIALS
PASSPORT
CRA ID INFO
DERIVED CREDENTIALS
LEVEL OF ASSURANCE
RULES
VERIFIER
ID PROOFING PROVIDER
RULES ENGINE
DIGITZED CREDENTIALS
PASSPORT
CRA ID INFO
DERIVED CREDENTIALS
LEVEL OF ASSURANCE
VERIFIER
ISSUER
AUTHORITATIVE SOURCE(S)
DIRECT ISSUER
PASSPORT
ISSUER
INDIRECT ISSUER
CRA ID INFO
AUTHORITATIVE SOURCE(S)
TRUSTED APP
6. Request
9. Issue
10. Request
11. Issue
12. Issue
12. Issue
12. Issue
13. I am sufficiently proofed
TRUST FRAMEWORK
GOVERNANCE AUTHORITY