OIX GUIDE TO TRUST FRAMEWORKS

September 2021

Nick Mothershaw and others
Open Identity Exchange

Version 1.0

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 organisation, offering education, information and collaboration around the topic of universally trusted identity.

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

Our 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, Chair & Chief Executive

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
1.0	September 2021	Updated BETA to first release post working group feedback	Nick Mothershaw

CONTENTS

1 INTRODUCTION

The guide is designed to provide an expert view on what a good ***trust framework*** might 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 organisations 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:

- User services (e.g. Consent, multiplicity, ID creation etc.)
- Organizational services (e.g. User access, ID Assurance, Liability, SLAs etc.)
- Trust rules (e.g. ***Proofing***, ***authentication***, assurance etc.)
- General rules (e.g. MI, audit, fraud controls etc.)
- Security and Technical Requirements
- Governance (e.g. ***Certification***, enrolment, operations etc.)
- ***Trustmarks***
- ***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, jargon-free guide to trusted identity and ***attributes*** for both users and organisations, 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.

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. 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 how the OIX directory can be used to find trusted suppliers of IDs: ***credential issuers***, ***identity providers***, ID ***brokers*** or ID Tech Component Providers. 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 IDENTITY TRUST

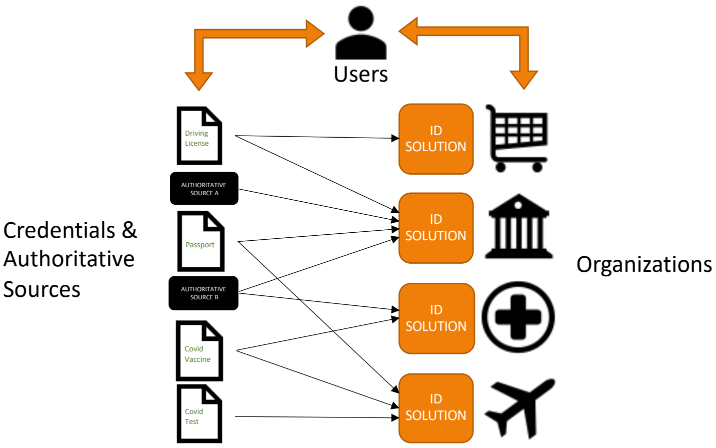
3.1 The Need for Identity Trust

For many types of transaction, digital or otherwise, organisations 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 organisations 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.

3.2 How Organisations establish identity trust today

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

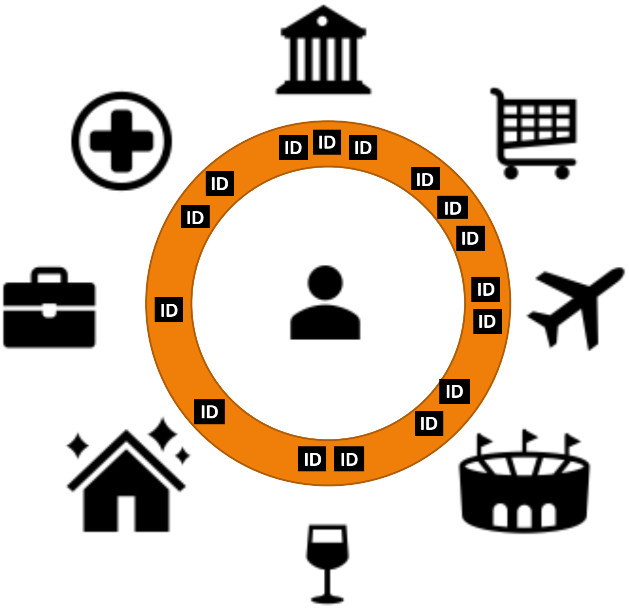


Organisations providing services to users typically have their own tailored ID Solution that enables them to:

- 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). Organisations 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 organisation specific ***authenticators*** to enable them re-access the organisation 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 organisation.

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	Organisation 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 organisation.	Cost to maintain own tailored ID solutions.
Leads to complex onboarding journeys which lead to abandonment	

3.3 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.

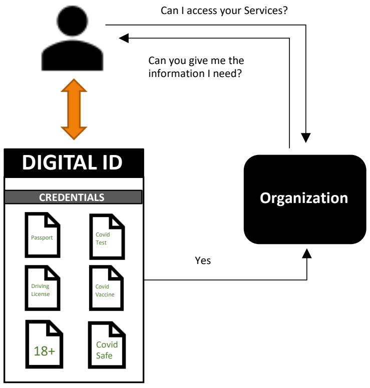
The Digital Identity has the following advantages for users and organizations:

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	

3.4 What is a Digital ID?

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

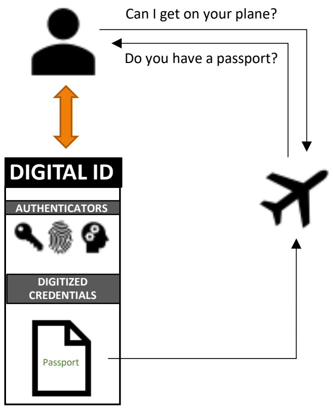
Digtized real world credentials such as Driving license, Passport or Vaccine Certificate and derived credentials such as Over 18, Covid Safe or a Level of Assurance:



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.

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

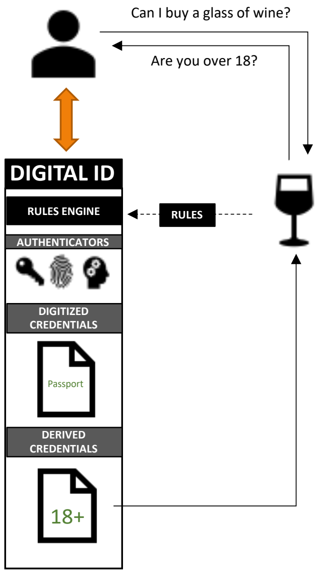


The simplest implementation of Digital ID is where the user is providing a Digitized version of a real-world Credential, such as a passport, driving license, covid vaccine or qualifications.

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.

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:



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.

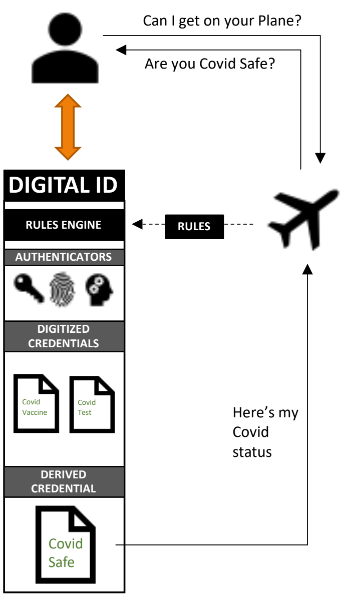
This could be derived programmatically from a digitized credential that has been verified as belonging to the user. The digitized credential itself does not need to be shared with the wine seller.

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 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.

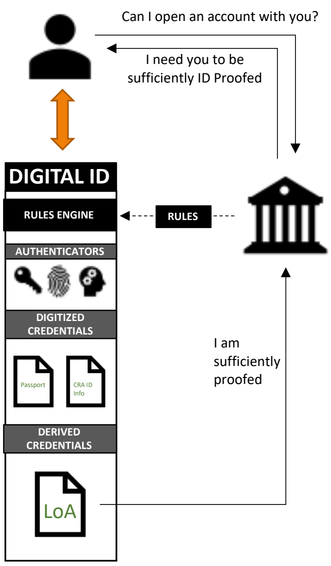
Rules may vary by use case, trust framework or individual organization

Many Derived Credentials are point-in-time and need to re-assessed at 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 pre-defined 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**.

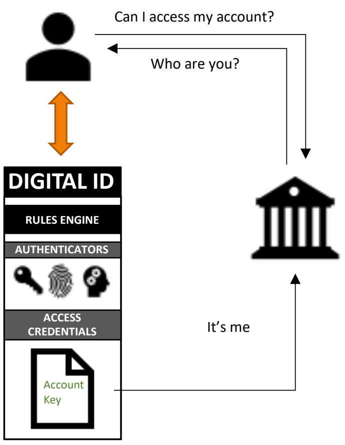
A Level of Assurance is a form of Derived Credential. Levels of Assurance are dynamic and need to be continually re-assessed as the users' credentials expire and fraud risks are re-assessed.

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 derived a level of assurance are shared with the organization.

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



Users use Facebook, Apple and Google IDs to do this all the time – they are acting 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.

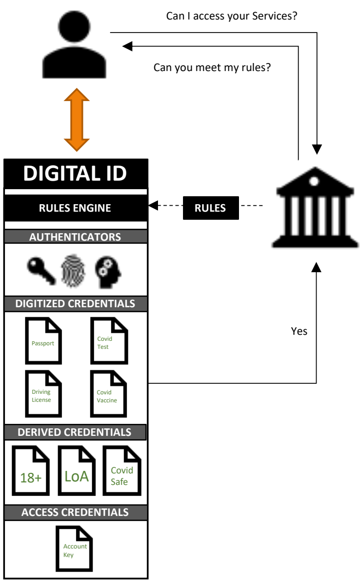
Or many organizations could rely on a generic Account Key created by the Digital ID.

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.

3.5 What is a Digital ID? – 3 Modes of use

Putting the examples, we have looked at so far all together gives us the complete view of a Digital ID:



The 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 organizations needs.

Mode 1 – The Digital ID can carry **digitized versions of existing credentials**, such a passport, driving license, vaccine certificate or relevant qualifications.

Mode 2 – The Digital ID can also **derive credentials** that show users meet the business rules of an organization, **such as being over 18, COVID safe** or meeting a specific **"level of assurance".**

Mode 3 - Organizations can also choose to allow users to use their **Digital ID to access an account** they hold with you. Thus, removing the need for you to issue your own logon authenticators (e.g., user IDs and passwords).

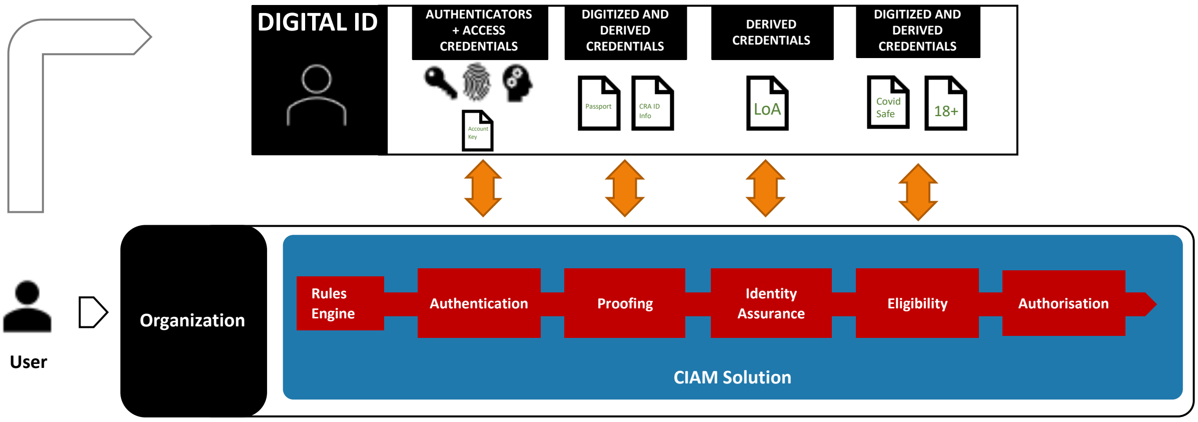
3.6 How might this market evolve?

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

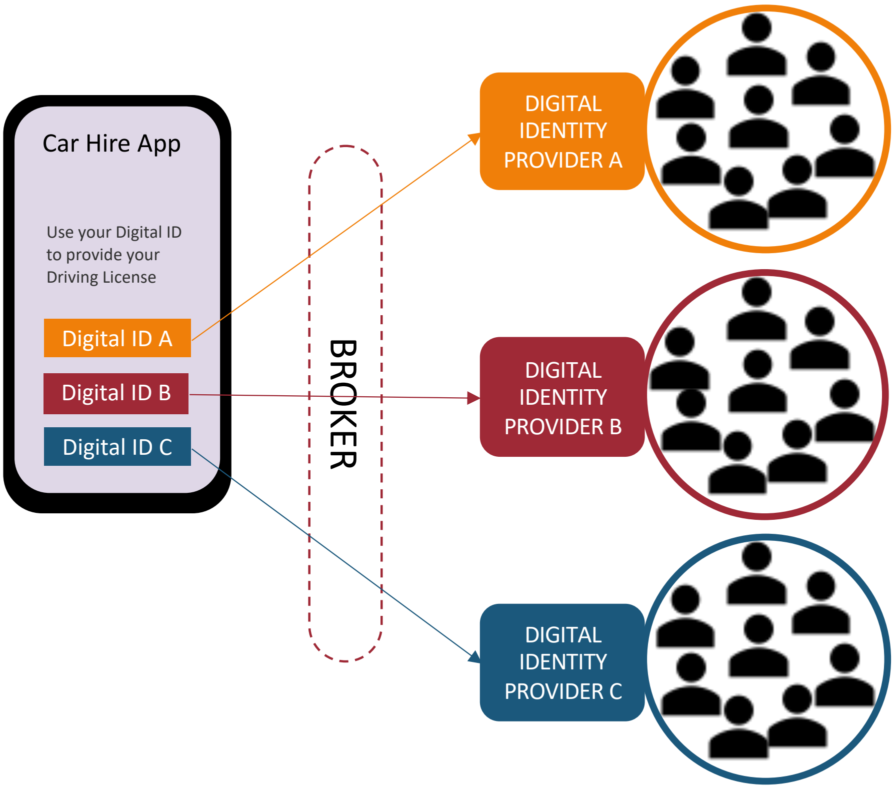
- Some organisations might only use a Digital Identity from an ***identity provider*** to onboard of the user and will continue issue the user with their own organisation-specific ***authenticators.*** Of these,
- Some organization will rely of the Digital ID to make complex rule bases decisions for them, generating derived credentials such a Level of Assurance or over 18. (Mode 2)
- Other organizations might use a Digital ID to provide digitized credentials to make their own decisions upon (Mode 1)

Other organisations might move to fully embrace the use of Digital Identities for both account opening and ongoing account access. (Mode 3).]

Organisations 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 organisation:



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

Organisations will not want to contract with, and separately interface to, Digital Identities from different ***identity providers***, so ***brokers*** (3) are likely to emerge, who aggregate ***identity providers*** and / or ***evidence issuers*** into single services.

4 THE GOVERNANCE REQUIRED

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

Accordingly, some form of governance framework is required.

4.1 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***."

4.2 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 deployed in the U.S. refer to them as a "***trust framework***", whereas identity systems in the UK (e.g., the GOV.UK Verify program) refer to them as "Scheme Rules." Other identity systems call them "Common Operating Rules" or "Operating Policies."

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, organisations, services, and devices can trust each other. A ***trust framework*** involves:

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

b) applicable to 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,

d) for the purpose of facilitating trusted identity transactions.

5 THE TRUST FRAMEWORK

5.1 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.

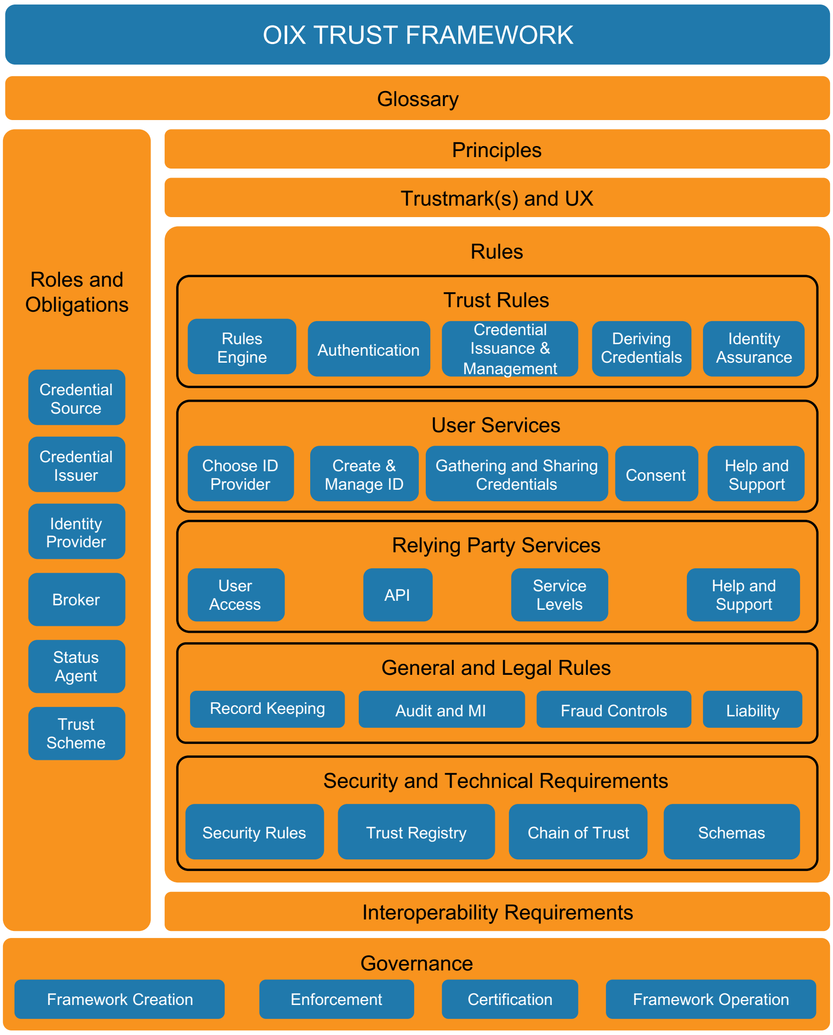
In this guide the rules of a ***trust framework*** are deliberately organised as follows:

- 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.
- General and legal rules applying to all parties are then covered: fraud controls, liability, record keeping, audit and MI.
- Finally, the Technical 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.

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.

5.2 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.

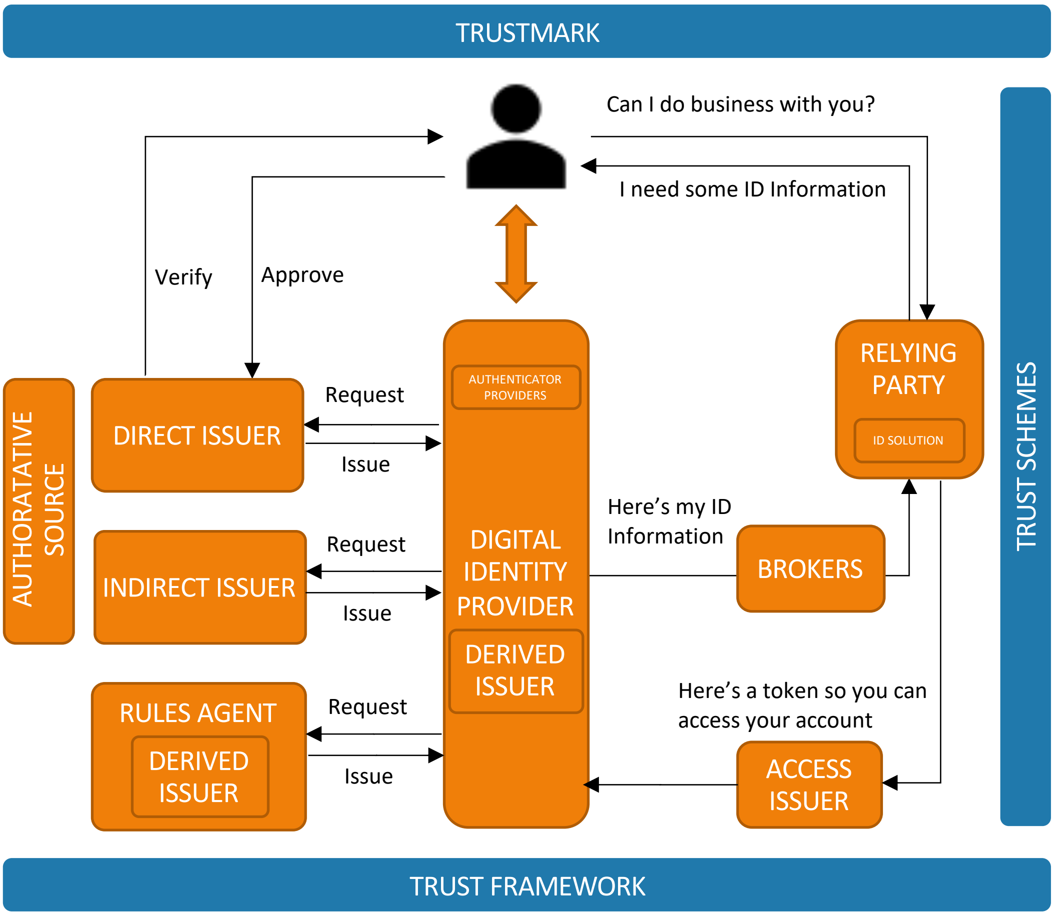
6 ROLES AND OBLIGATIONS

6.1 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 organisation (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.


TRUSTMARK
Can I do business with you?
I need some ID Information
Verify
Approve
TRUST SCHEMES
RELYING PARTY
ID SOLUTION
AUTHENTICATOR PROVIDERS
AUTHORATATIVE SOURCE
DIRECT ISSUER
Request
Issue
INDIRECT ISSUER
Request
Issue
DIGITAL IDENTITY PROVIDER
DERIVED ISSUER
Here’s my ID Information
BROKERS
RULES AGENT
DERIVED ISSUER
Request
Issue
Here’s a token so you can access your account
ACCESS ISSUER
TRUST FRAMEWORK