OIX GUIDE TO TRUST FRAMEWORKS

July 2020

Nick Mothershaw and others
Open Identity Exchange

Version 0.1 BETA

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

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.)
- Organisational 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 will the guide be developed?

During the course of 2020 this guide will link 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 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.
- **Organisations (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: ***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

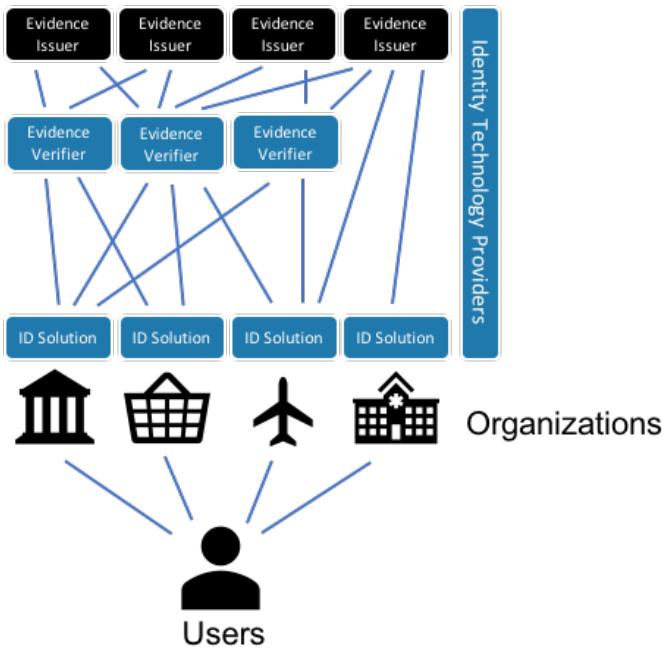
3.1 The Need for Identity Trust

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:

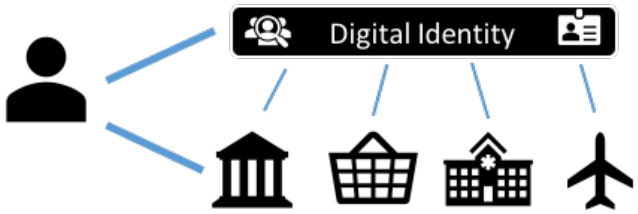
- Ensure that the user is who they are claiming to be. This is done on a risk mitigation basis and / or to a standard that is prescribed, usually on a per-sector basis (e.g. finance). Organisations often leverage external ID ***proofing, verification*** and risk services from ***evidence issuers*** or ***evidence verifiers*** 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.
- 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.

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 organisation.



The Digital Identity can help organisations do two key things:

- facilitate access to verified trusted information about the user, known as ***attributes*** or ***claims***, that are supported by ***evidence.***
- also allow the organisation to trust that the user is who they claim to be

A Digital Identity can help to enable a user to explicitly consent to or permit sharing of information about themselves that may be held digitally.

When a user interacts with an Organisation they can use their Digital identity to provide access to verified ***attributes*** and ***evidence*** of who they are and/or what they are eligible to do. This may be by providing access to different elements of verified ***evidence***, or by providing a ***level of assurance*** based on collected ***evidence***, that meets the needs of that organisation. The minimum amount of information required to fulfil the transaction should be provided.

For ongoing access to the Organisation's services, instead of issuing each user with organisation specific ***authenticators*** (e.g. a username and password), the organisation could choose to rely on a trusted Digital identity.

The Digital Identity enables the user to prove who they are, to many different Organisations:

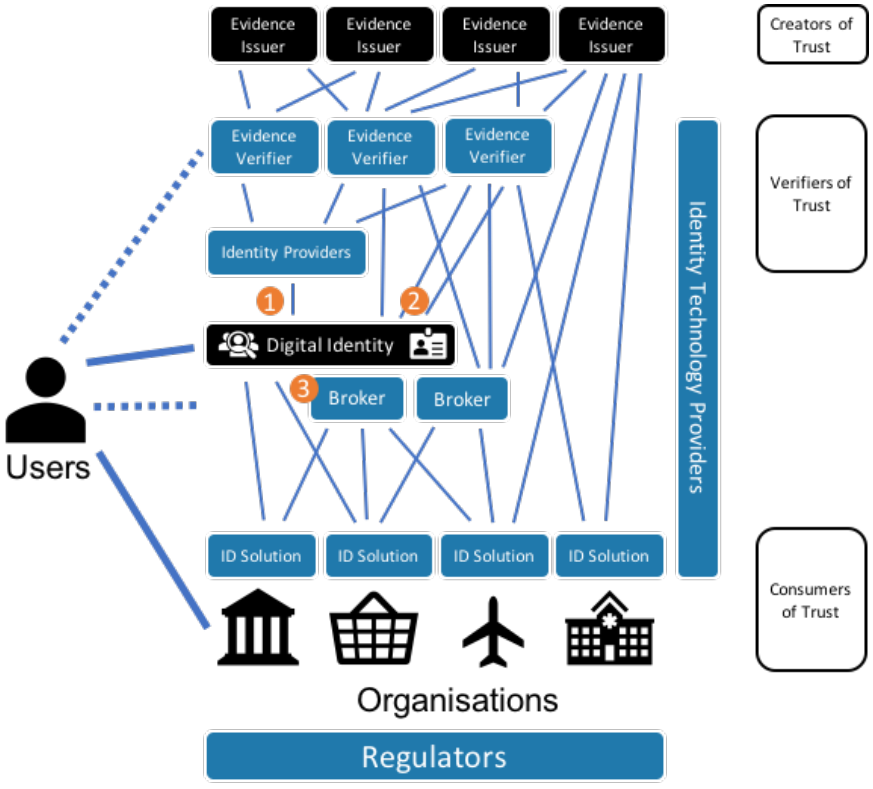
- The user's verified personal information can be passed to each Organisation (with the user's consent) to save the user repeatedly entering the same personal information into different Organisation's sites.
- The user does not need a logon and password for each organisation, their Digital Identity becomes their way to authenticate to all accepting organisations.

3.4 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.

- Some organisations might only use a Digital Identity from an ***identity provider*** to onboard the user and will continue issue the user with their own organisation-specific ***authenticators.***
- Other organisations might move to fully embrace the use of Digital Identities for both account opening and ongoing account access.
- Whilst another set of organisations not rely upon a Digital Identity, but may still work with the commonly agreed (or mandated) rules and standards applicable to their sector whilst continuing to issue users with their own organisation-specific identity. Drivers for this include brand protection, high volume transactions and high-risk transactions. These organisations might choose to access the service of ***evidence issuers*** or ***evidence verifiers*** either directly or through a ***broker*** who offers access to these services.

Organisations may also still need their own ID Solution to manage the user's privileges within that organisation.



Users may use an ***identity provider*** to create and manage their Digital Identity (1), or might create and manage it themselves (2) (although this will often be via some form of Digital Identity Wallet, where arguably the wallet provider is the ***identity provider***).

An ***identity provider*** might allow a user to collect ***trusted evidence*** about themselves that they can then share with organisations. An ***identity provider*** may go further and establish a level of trust in the user to a ***level of assurance*** that the organisation then relies upon.

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.

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.

Evidence issuers offer two types of ***evidence***: ***identity evidence*** and ***eligibility evidence***. ***Evidence verifiers*** ensure the evidence collected is genuine, belongs the user and also assess identity fraud risk. Organisations might choose to use a Digital Identity to access some pre-obtained and verified ***identity evidence*** for a User, then access other ***evidence issuers*** or ***evidence verifiers,*** directly or through a ***broker,*** for additional ***identity evidence*** or ***eligibility evidence***.

The reliance on third parties to undertake identity services on behalf of an organisation means that contracts will be required between the different parties. All parties will need to work to commonly agreed rules and standards that meet the trust needs of different organisations.

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 ***identity evidence*** 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

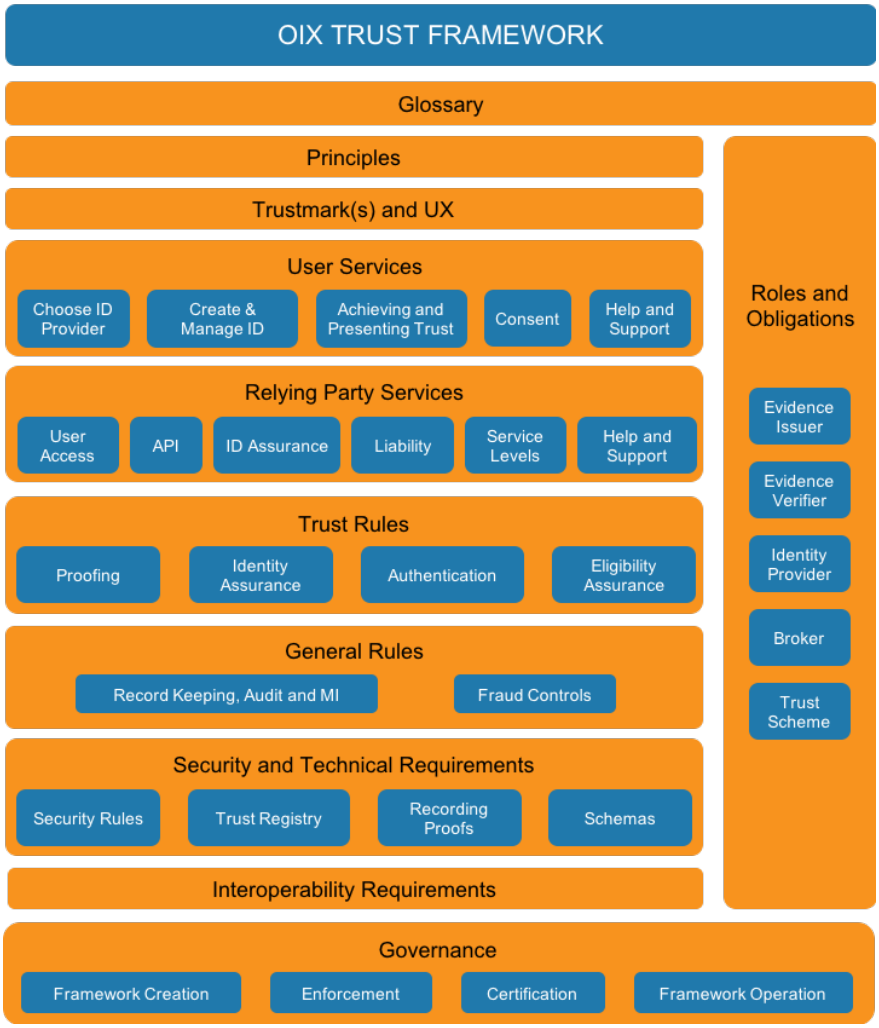
In this guide the contents of a ***trust framework*** are deliberately organised in a user centric way:

- From the top down we start with the user led Principles required, then the ***Trustmark*** required to communicate the framework to the user, and next the services a user might be offered through the implementation of the framework.
- We then move on to the services required by the next most important party, the Organisation, or ***relying party***. If we get these two key end-points of user and ***relying party*** right, the framework is more likely to be a success.
- Next come the Trust Rules in the framework, the fundamental elements of ID ***proofing***, ***authentication*** and assurance.
- Finally, the General and Technical rules to ensure the framework is managed securely and can be held to account.
- This is then underpinned by recommendations on the operational Governance approach to ***trust framework***s.

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.

The ***trust framework*** has the following contents:



Subsequent sections of this document explore, at a high level, these 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

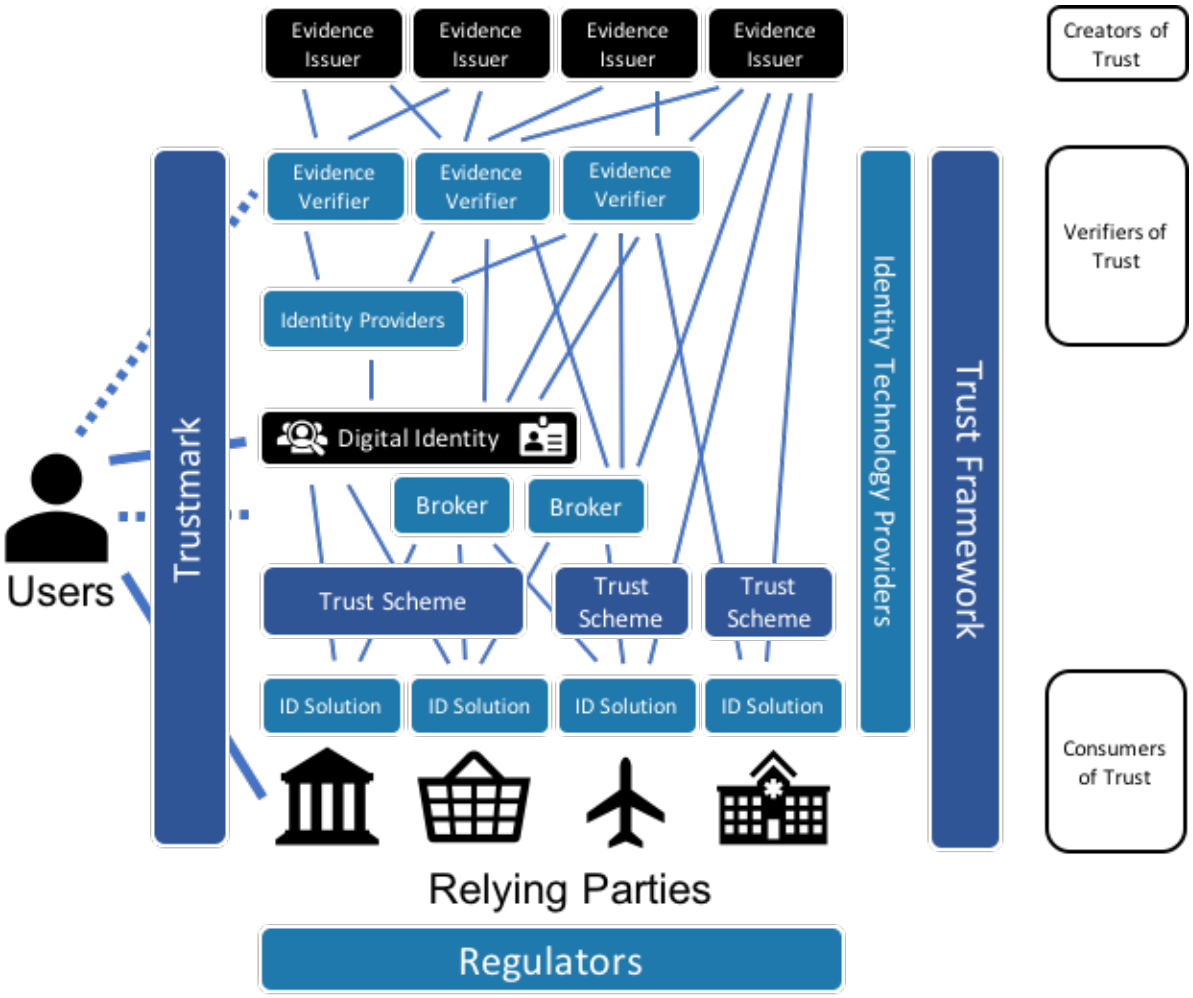
The identity ecosystem can involve many different roles. The roles differ between each implementation – for example, centralised and federated models will differ, as will self-certified / self-sovereign models, and one person or organisation (an 'actor' or 'participating entity') may perform more than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

An overview of the roles that could be involved is shown below. This model assumes a single ***trust framework*** and ***Trustmark***, with several ***brokers***, ***trust schemes***, and ***regulators*** in the ecosystem.

It also includes a specific role for ***evidence issuers***, who are an ***authoritative source*** that provides ***evidence*** and ***verification*** services around an individual's ID.

In this model, organisations might use their own tailored ID Solutions to meet the requirements of a framework and scheme, or might rely on an ***identity provider***(s) to do this for them. We are not assuming there is always a Digital Identity in use, as it is going to take some time to evolve to that state.

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.
Identity Technology Provider	A technical or service component used as part of establishment and provision of trust in the identity. Types include: ID ***proofing*** and ***verification***, ID ***authenticators***, Fraud controls, Identity Access Management, Aggregators.
Evidence Issuer	Issues some form of ***evidence*** that proves who the user is and / or what they are eligible to do. This could be: electronic issuance or ***verification*** 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 simple confirmation of the users age bracket (e.g. over 18). They could be, or could provide data to, a trusted "***authoritative source***" to allow the ***evidence*** they issue to be ***validated***. The provision of ***eligibility*** data is sometimes referred to as an "attribute service". In a self-sovereign identity model, this role in combination with the ***evidence verifier*** is referred to as the "Issuer".
Evidence Verifier	***Validates*** some form of ***evidence*** that proves who the user is and / or what they are eligible to do, and then ***verifies*** the ***evidence*** belongs to the User This could be by accessing an ***evidence issuer*** as, or via, an "***authoritative source***", to validate the ***evidence.*** They can be services that interact directly with the user, including ***vouching*** services. This role uses the rules for identity ***proofing*** and records the process of such as ***verified evidence*** and ***claims***. In a self-sovereign identity model, this role in combination with the ***evidence issuer,*** is referred to as the "Issuer".
Identity Provider	Creates and maintains a Trusted Digital Identity for users that they can present to ***relying parties*** to prove who they are. Trust is established through ***proofing***. The Trusted 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 to hold verifiable credentials, provide the user with bound ***authenticators***, and present credentials to ***relying parties*** could be a proxy for the ***identity provider***.
Broker	In a market where there are multiple ***identity providers***, a ***broker*** allows a ***relying party*** to enter into a single contract and single technical integration to access a critical mass of digital identities or ***eligibility*** information from different ***identity providers*** or ***evidence issuers***.
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 an participating entity is associated with a particular ***trust framework*** and allows an individual to verify that is is the case.
ID Solution	Each ***relying party*** a user deals with will need a solution to record the ***identity provider***, and / or ***identity evidence*** 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. This could be an organisation but could also be another person or a "thing".
Regulators	Those that set the regulation to which any role in the scheme must comply. This could be general regulation such as data protection, or more specific regulation related to identity such as money laundering or age restriction regulation.

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:

- The issuance and ***verification*** of a piece of ***evidence*** might be done by the same party playing the role of ***evidence issuer*** and ***evidence verifier***.

- A single party might play the role of ***identity provider*** and ***evidence verifier***, taking in ***identity evidence*** from various different 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 ***evidence issuer***s that it requires to meet its identity needs, in line with a ***trust framework*** / ***scheme*** relevant to its business.

6.2 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
identity technology provider	ITP
evidence issuer	Iss
evidence verifier	Ver
identity provider	IdP
broker	Bkr
trust scheme	Sch
Trustmark	Tmk
identity solution	IdS
relying party	RP
regulators	REg

7 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 framework*****s** and has produced the following User principles written in plain language. These principles are the 4 Cs:

User Principle	User Principle Element	Who?
CONVENIENCE	An ID I set up can be used in lots of different places – I don't need different IDs to access different kinds of services, unless I choose to do so	Bkr, IdP, Sch, Fwk
	I need to know where I can and cannot use my ID.	Bkr, IdP, Sch, Fwk
	I need to understand why I am sometimes asked for further verification of my ID.	IdP
CHOICE	I can choose who manages my ID for me and change this at any time.	Bkr, Sch, Fwk
	I can have more than one ID.	Bkr, IdP, Sch, Fwk
	My IDs are free.	Sch, Fwk
CONTROL	It's my ID and data.	Bkr, IdP, Sch, Fwk
	I need to agree who my data is shared with.	IdP
	I can see a record of this, and request for it to be returned and removed if I want.	Bkr, IdP, RP
	I can 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	IdP, RP
CONFIDENCE	I need to know my ID and data is safe from ID fraud and those who might use it illegitimately.	Bkr, IdP, Sch, Fwk
	If something goes wrong, I need to know I will be OK, and the problem will be resolved.	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.

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

Document	Type
User, ***Relying Party*** and Framework Principles	Principles

8 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 ***evidence issuers*** are compliant with the ***trust framework***
- ***Evidence issuers***: Need to know that their ***evidence*** 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 signaled 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?
Is there a 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 ***evidence issuers***, ***brokers*** and IdPs display the ***Trustmark*** in a B2B context?	Bkr, IdP, RP, Ver
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 different levels of assurance, and why users have to 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, Ver

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

Document	Type
Trustmark Brand and UX usage policy	Policy

9 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 an ***evidence verifier*** who is a ***vouching*** service.	Bkr, Tmk
Finding an existing Digital ID	Users may already have an ID with one or more providers. When users first go to a new ***relying party*** and need to choose a Digital ID to use. Hghlighting 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.***	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 ***evidence*** 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 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. 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 ***evidence***	The user should be able to collect ***evidence*** about their ID, both ***identity evidence*** and ***eligibility evidence***, and store this against their Digital Identity.	IdP, Ver
Establish Trust in the ***Evidence***	The user should be able to establish trust in their ***evidence*** through ***validation*** and ***verification*** of the ***evidence.***	IdP, Ver

Establish Trust in the User – Identity Assurance	The should be able to achieve a level of trust required by a ***relying party***. Ideally the ***identity provider*** should do this in a way that does not require the user to understand the identity ***assurance model***. For instance, the ***identity provider*** should work out what ***truestd evidence*** the user already has that will allow them to achieve that level of trust required, 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 the level of trust required. 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 levels trust. The level of trust achieved may be recorded by the ***identity provider*** as a ***level of assurance***. The user may not know about ***level of assurance(s)*** as this may confuse them.	IdP
Authentication	The user must be able to present to the ***relying party*** the level of trust required. This will be by accessing their ID using the appropriate ***authenticators***, refreshing any expired ***evidence***, and then sharing trusted information (including the confirmation of their identity) to the ***relying party***.	IdP
Access ***Eligibility Evidence***	Th ***identity provider*** should be able to access ***eligibly evidence*** for a trusted user and attach this to the user's digital identity for them to present to the ***relying party*** as trusted ***eligibility evidence.***	IdP
Sharing Trust with a ***Relying Party***	The user should be able to share trusted information from their ID with ***relying parties*** This includes ***trusted claims***, ***trusted identity and eligibility evidence,*** and (where used) ***levels of assurance.***	IdP
Data Minimization	The user should not supply an ***identity provider*** or ***evidence verifier*** more data than is needed to complete ID ***proofing***, or supply or share with any ***relying party*** more data that is necessary to fulfil the purpose of a transaction.	IdP, Ver, RP
Consent		
Consent	Data must only be shared with a ***relying party*** with the user's 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.***	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, 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, Ver, 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, ID ***Proofing*** information can be passed from the old IdP to the new IdP. Consideration needs to be given as to how any links maintained between an Organisations 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, 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, 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, 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 ***evidence***	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

10 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)		
Request.	The ***relying party*** should be offered a consistent way to request services from the framework. Request types might include: • Identity ***claims*** • Trusted Identity ***claims*** • Trusted Identity ***claims*** with ***evidence*** • ***Identity evidence*** check • (minimum) level of ***identity assurance*** with No-evidence • ***identity assurance*** with ***evidence*** • Identity ***eligibility*** check Several request types might be combined in a single request.	Bkr, IdP, Iss. Ver
Response.	The ***relying party*** should receive a response to their requests in consistent way, regardless of the user's choice of ***identity provider*** or ***evidence verifier***, or any different technical implementations within the ecosystem. The response should include (depending on the request): • Identity ***claims***, and their ***verification*** status • ***Identity assurance*** • ***Identity evidence*** • ***Eligibility evidence***	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 ***identity assurance*** Model. Ideally the ***relying party*** should so this in a way that does not require the user to understand the ***identity assurance*** Model. For instance, the ***relying party ID solution*** should work out against the ***identity assurance model*** what ***trusted evidence*** 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 ***identity assurance model.*** The user should set up to the ***authenticators*** that are appropriate to manage and assert their ***relying party*** specific identity as defined in the ***identity assurance model***.	Fwk, Sch.
Bind ***Authenticators***	Where the ***relying party*** is undertaking this process for the user themselves, they will need access to the ***identity assurance model.*** The ***authenticators*** of the level of quality and type required to meet the ***identity assurance model*** 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, Ver, Fwk or Sch
Service Levels		
Service Level Agreement	In order to offer a consistent level of service to users, ***relying parties*** 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, 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, Ver.
Compensation for poor service	Frameworks, or ***trust scheme***s, 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, 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 parties*** 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, 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, Bkr, Sch, Fwk
Compensation	Is there any compensation due to a 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, Bkr, Sch, Fwk

To support these ***relying party*** services the following policies, procedures or standards are required:

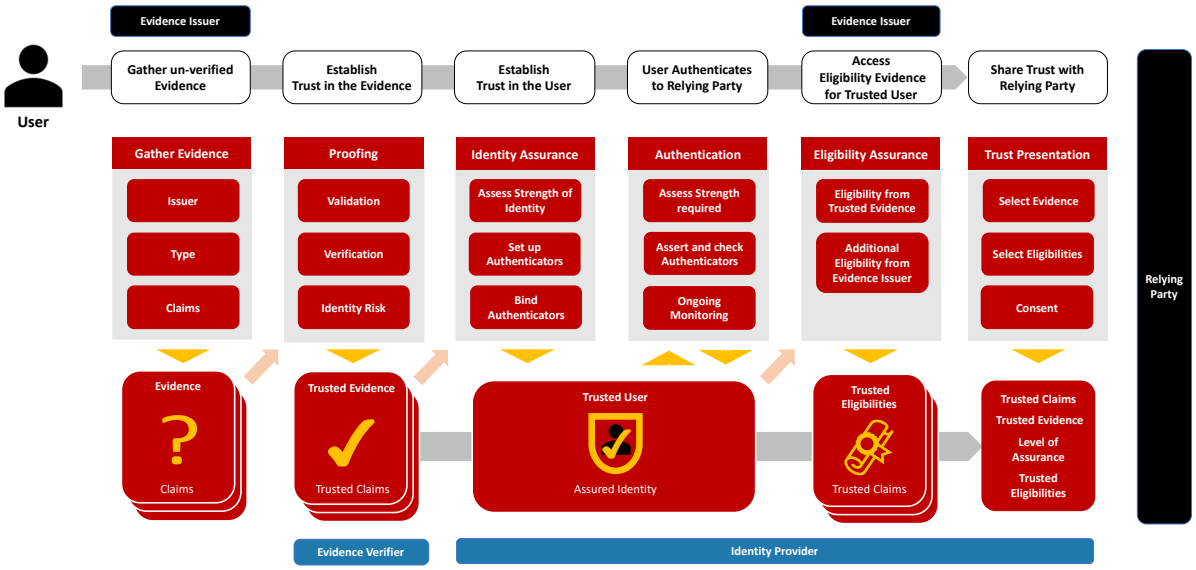
Document	**Type**
Liability Policy	Policy
Liability Claims Procedure	Procedure
Request and Response Standards	Standards
Level of Assurance determination by ***relying party***	Procedure
Service Levels	Policy
Service Level Monitoring	Procedure
Help and Support Procedure	Procedure
Complaints Procedure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

11 TRUST RULES

A structured approach to ***proofing*** and identity trust is required to ensure consistency and ***interoperability*** within a ***trust framework***, and for ***interoperability*** across ***trust frameworks***.

The framework should consider rules around ***proofing***, ***identity assurance, authentication***, and ***eligibility assurance***. Keeping trust up to date for a user's identity and ***eligibility*** is also a key consideration.

The following diagram shows the process of achieving and presenting trust in the user. Additionally, it shows the roles involved in this part of the process:



Once the user is trusted, they may present that trust, along with ***trusted evidence*** and ***trusted eligibilties*** to the relying party.

11.1 Proofing

Proofing is the process of establishing trust in ***identity evidence*** gathered by, or about, the user. ***Evidence*** comes from an ***evidence issuer***.

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.

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 evidence that the user can provide to prove who they are such as a passport, driving license or bank account. The strength of the evidence should be taken into account. For example, a passport is likely to be regarded as higher strength evidence than a utility bill. The ***evidence*** must be validated to make sure that it is genuine. ***Validation*** is typically done by an ***evidence verifier***. ***Evidence verifiers*** may be, or have 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 ***evidence*** they provide, such as a social media.	Ver

Verification	Verifying that this user is the person they are claiming to be. This might be by checking possession of ***evidence*** 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 ***evidence***, such as the ability to answer knowledge-based questions. The ***verification*** of a user as the genuine holder of a piece of ***evidence*** might be done by the same ***evidence verifier*** who validated that ***evidence***, or be done by a separate ***evidence verifier***. The ***identity provider*** may also play the role of ***evidence verifier*** in this respect, linking pieces of ***evidence*** together to create a single piece, or collection of, more robust ***evidence.***	Ver
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.)	Ver
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

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

The result of the ***proofing*** process is a collection of ***trusted evidence.*** This can then be shared with, or presented to, ***relying parties.*** It 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 evidence***, ***trusted claims*** can be drawn. For example, trust in a person's name address and date of birth can the drawn from a passport.

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

11.2 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 ***evidence*** collected about the user.

For example, a basic level of trust might be established by checking the user's self-declared address against a database of known addresses by an ***evidence verifier***. 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 must 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 ID fraud.

The ***trust framework***, or a ***trust scheme***, might define the level of identity trust that ***relying parties*** in a particular sector are required to achieve in order to meet certain regulatory requirements. This is called a ***Level of Assurance.***

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

The following table describes the ***identity assurance*** process:

		Who?
Identity Assurance		
Definition of Level(s) of Trust	A level of trust can be determined by an ***identity assurance model*** that defines the types and amounts of ***trusted evidence*** required to achieve that lelve of trust, 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 trust. A level of trust might be referred to, and communicated as, a ***level of assurance***	Fwk, Sch
Authenticator Types	***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 user knows, such as a secret (e.g. a pin or password).	Fwk, Sch
Authenticator Strengths	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
No. of ***Authenticators*** (Factors)	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
Assessment of Strength of Identity	The IdP should allow the user to achieve a level of trust required by a ***relying party***. Ideally the ***identity provider*** should do this in a way that does not require the user to understand the ***identity assurance model***. For instance, the ***identity provider*** should work out against the ***identity assurance model*** what ***trusted evidence*** the user already has that will allow them to achieve that level of trust, 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. Alternatively, the ***relying party*** could undertake this process for the user themselves using the ***identity assurance model***.	IdP 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 ***identity assurance model***. The user may have already set up some **authenticators** to manage their Digital ID; these may be appropriate for the level of trust required, or additional ***authenticators*** may need to be set up. Alternatively, the ***relying party*** could undertake this process for the user themselves using the ***identity assurance model.***	IdP Or RP
Bind ***Authenticators***	The ***authenticators*** of the level of quality and type required to meet the ***identity assurance model*** 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 ***identity assurance model.***	IdP Or RP

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.*

11.3 Authentication

Authentication happens when the user wants to:

- use their Digital Identity to present a level of trust, ***evidence*** or ***eligibility*** to a ***relying party***,
- maintain thier Digital Identity.

The user uses the ***authenticators*** that are bound to their Digital Identity that allow them to re-recognized to use the Digital Identity.

	Who?
Authentication	

Assess Trust Required	The first step is to assess the strength of trust required for this transaction and determine if the user has that level of trust, possibly stored as a ***level of assurance***. This could be done by assessing whether the user has previously achieved a defined level of trust that meets the ***relying party's*** needs, or it could be achieved dynamically based on ***trusted evidence*** and ***authenticator*** types requested by the ***relying party.*** If the user does have the level of trust, the ***identity provider*** must determine what ***authenticators*** are required to assert that level of trust. If the user does not have the required level of trust, they will need to establish this by going through part or all of the ***proofing*** and ***identity assurance*** processes. This is often referred to as "step-up" at point of ***authentication.***	IdP
Assert and Check ***Authenticators***	The user will be asked to assert ***authenticators*** to meet he level of trust required. 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 ***evidence*** does not have an infinite period of validity. ***Evidence*** such as a user's qualifications is long lived, but may still be revoked. ***Evidence*** such as passports and driving licenses have expiry dates. Other ***evidence***, 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 evidence*** relied upon must be checked and the ***evidence*** must be reverified and updated if necessary, before the users identity can be asserted to the ***relying party.***	

11.4 Eligibility Assurance

Eligibility Assurance is the process of assessing whether the user is able, or is allowed, to access the ***relying party's*** services.

This might be by presentation of a passport to board a flight, presentation of qualifications to gain employment, or proof of living alone to gain access to benefits.

All these may be achieved through the collection, ***validation*** and ***verification*** of ***eligibility evidence***, by the user.

		Who?
Eligibility Assurance		
Eligibility from ***Trusted Evidence***	The ***proofing*** process can be used to ***validate*** and ***verify eligibility evidence***. Some ***eligibility evidence*** may already be trusted as it was used as part of the ***identity assurance*** process e.g. a passport. In this case the ***trusted evidence*** that results from the ***proofing*** process can also be used as ***eligibility evidence.***	IdP
Eligibilty from ***Evidence Issuers***	Once a sufficient level of trust has been established in the user it may be possible to go straight to an ***evidence issuer*** to collected additional ***evidence*** without the need for further ***verification*** of the user. The ***evidence issuer*** would trust that the ***identity provider*** has followed the rules of the framework or scheme to achieve trust in the user. The ***identity provider*** would then simply call an ***evidence*** service provided by the ***evidence issuer***, and the results of this would be added the user's digital identity as ***trusted eligibility***. An example might he accessing a user's inoculation record held by a health provider and attaching this as a ***trusted eligibility*** to the digital identity.	IdP

From ***trusted eligibility***, further ***trusted claims*** can be drawn. For example, trust in a person's passport number, nationality or inoculation date.

11.5 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

12 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?
Record Keeping and Audit Trail		
Record Keeping	Records of the ***evidence*** gathered by the user and how this was used in ***identity assurance*** and ***authentication*** should be 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 Bkr Ver
Record Keeping – for ***Relying Parties***	***Relying parties*** may require that an ***identity provider***, ***broker*** or ***evidence verifier*** keeps records of the ***evidence*** gathered by 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 Bkr Ver
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, Bkr, Ver, Sch, Fwk
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, ***evidence*** gatherings and presentations, assurance assessments, ***authenticator*** issue and use.	Bkr, IdP, Ver.
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 externally accessible point of the ecosystem must have appropriate cyber-attack defenses.	Bkr, IdP, Iss, Ver.

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, Ver.
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
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, Iss, Sch, Fwk, Ver
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, Iss, Sch, Fwk. Ver
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, Iss, Sch, Fwk, Ver
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 ***evidence issuers*** helps find and defend these vulnerabilities.	Bkr, IdP, Iss, Sch, Fwk, Ver
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, Iss, Sch, Fwk, Ver
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, Iss, Sch, Fwk,Ver

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

13 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 ***evidence verifier***. 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) should be considered for key parties such as ***identity providers***, ***evidence issuers*** and ***brokers***.	Fwk, Sch
Security Policy	All operational parties in the eco-system must comply with a Security Policy.	IdP, Ver, 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 eco-system must be entered onto the Trust Registry. The role of the party should be recorded.	IdP, Iss, Ver, 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, Iss, Ver, Bkr, RP.
Recording and Presentation of *evidence* Proofs		
Proof Recording Policy	How ***evidence*** proofs are recorded, both in terms of the gathering, creating and presenting ***evidence*** should be defined. The user of cryptographic techniques to ensure ***evidence*** cannot be tampered with should be considered. Consideration should be given to support for "zero knowledge proofs", which allow a ***relying party*** to trust a derived ***assertion*** of ***evidence*** (such as proof of a person's age) without the need for the ***relying party*** to see the supporting ***evidence*** behind this ***assertion.***	Fwk, Sch
evidence Proof Recording	Parties creating and presenting ***evidence*** proofs must record this in a secure consistent way.	IdP, Ver.
Request and Response Schemas		
Schema Definition	In order to ensure the ***identity evidence*** and ***eligibility*** information is 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 ***evidence issuers*** who issue the same type of ***evidence***. Consideration should be given to globally defined schemas from organisations such as The Open Identity Foundation and W3C. However, localization will almost certainly be required for many ***evidence*** types. The framework should implement a clear curator for locally applicable schemas.	Fwk, Sch
Request / Response Schemas	Identity data and ***evidence*** collected and presented should be in a consistent format across the framework.	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 INTEROPERABILITY REQUIREMENTS

When considering ***interoperability***, there are two dimensions to take into account: internal ***interoperability*** within the framework and external ***interoperability*** with other frameworks.

14.1 Internal Interoperability

One of the key purposes of a 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 Organisations 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 ***evidence verifiers*** becoming compliant with more than one ***trust scheme***.

14.2 External Interoperability

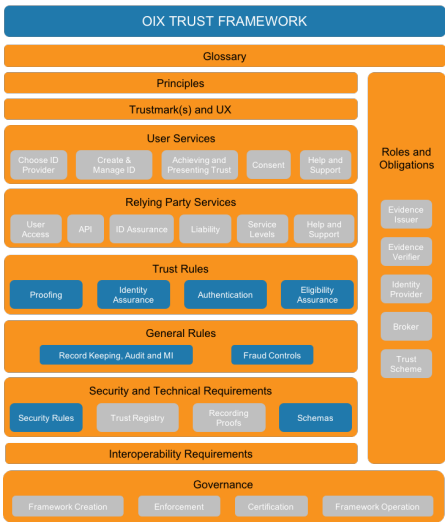
External ***interoperability*** with other ***trust frameworks*** can be achieved in three ways:

- Bilateral agreements between frameworks to mutually recognise 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 ***evidence verifiers*** 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
- Record Keeping
- Fraud Controls
- Response Schema
- Security Standards



15 GOVERNANCE OF THE TRUST FRAMEWORK

15.1 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 ***trust framework***, or a separate legal entity charged with the task of managing the ***trust framework***. 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 organisation (typically an entity acting as either the sole ***identity provider*** or the sole relying organisation) 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* Organisation:** 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 Initiative8, and the tScheme Approval profiles issued by tScheme9.
- **Mutual Agreement Among All Participants:** In smaller scale ***trust frameworks***, 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.

15.2 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 ***trust 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 ***trust 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 ***evidence 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.

15.3 Certification to a Trust Framework

Participating entities in the framework may need to be certified in some way to show 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***.

15.4 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 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).

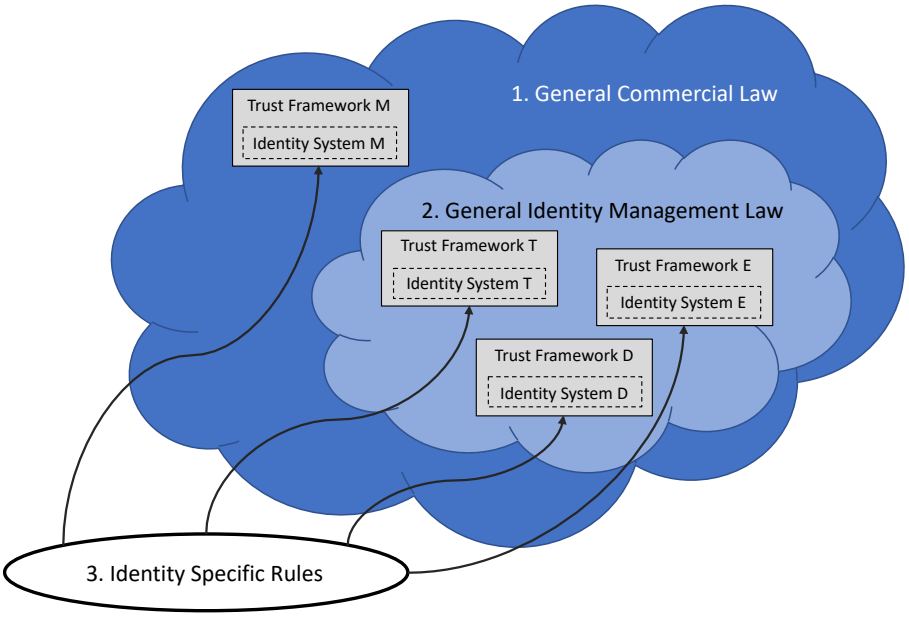
16 THE LEGAL CONTEXT OF AN IDENTITY TRUST FRAMEWORK

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 the ***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 system-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).

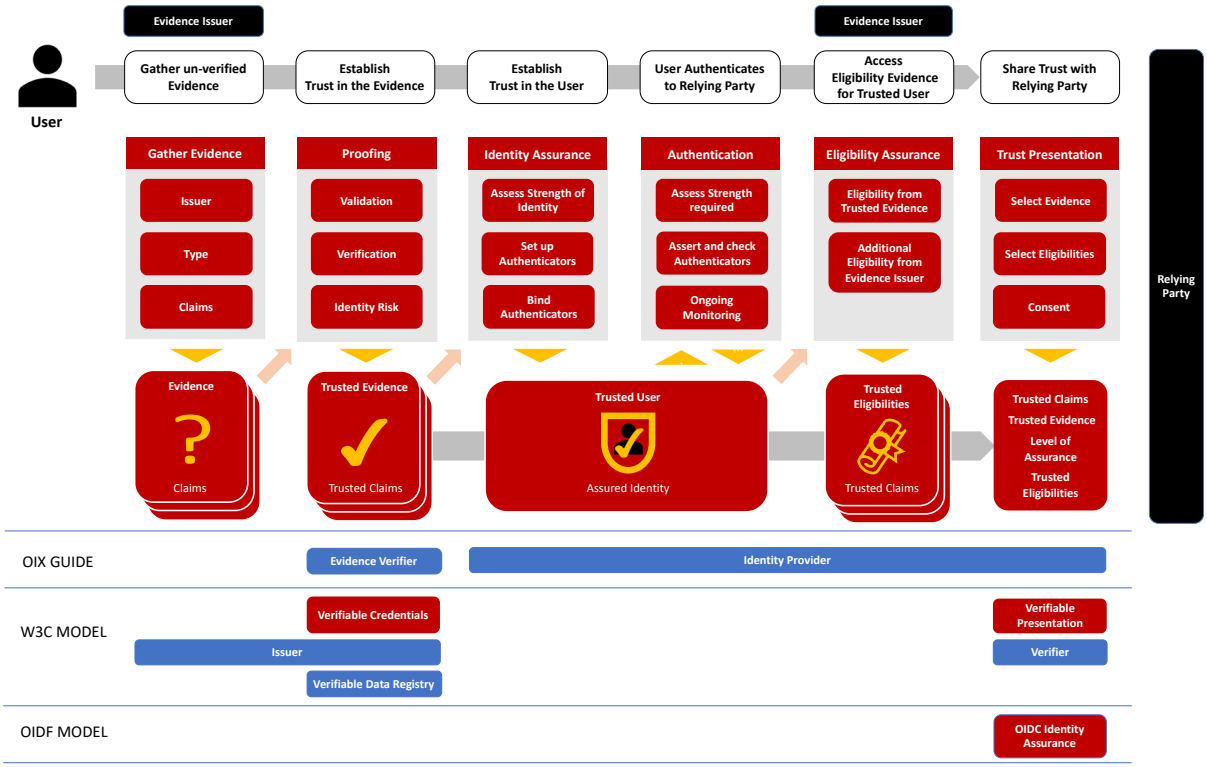


17 MAPPING SELF SOVEREIGN IDENTITY MODELS TO THE TRUST FRAMEWORK

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.

The below diagram shows how the roles and constructs used in Self Sovereign models map to the Trust and presentation process in this framework guide.

It also shows where the Open Identity Foundations ID Assurance schema would be used.



It is important to note that in many implementations the ***identity provider*** may also play the role of ***identity verifier***.

It is also worth noting that in the Self Sovereign model the wallet the user, or holder, uses to manage their identity may be playing part of the role of the ***identity provider*** as described in this guide.