Guide to Identity Trust Frameworks

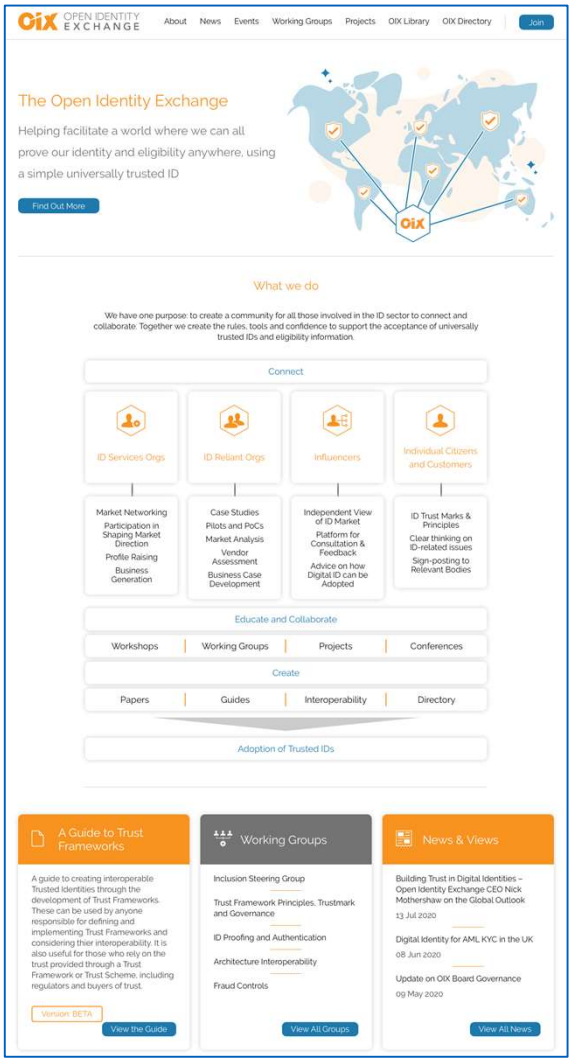
LAUNCH WEBINAR

15th July 2020

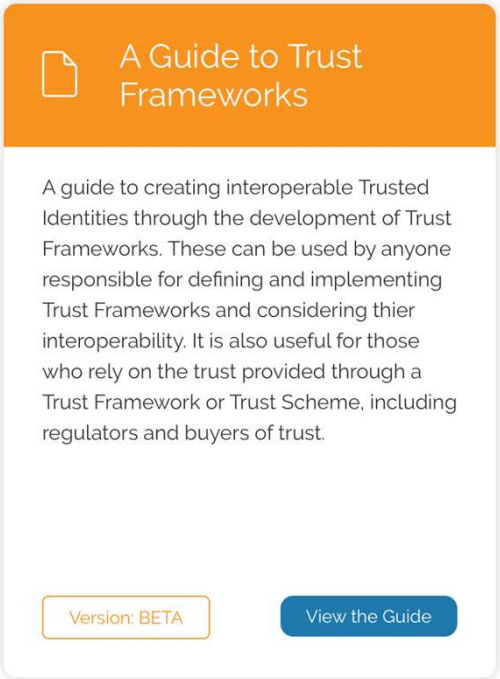
Nick Mothershaw, OIX

The New OIX Website

- New Vision
- New Purpose
- Guide to Trust Frameworks
- Working Groups
- OIX Library
- Members access
- OIX Directory



The OIX Guide to Trust Frameworks



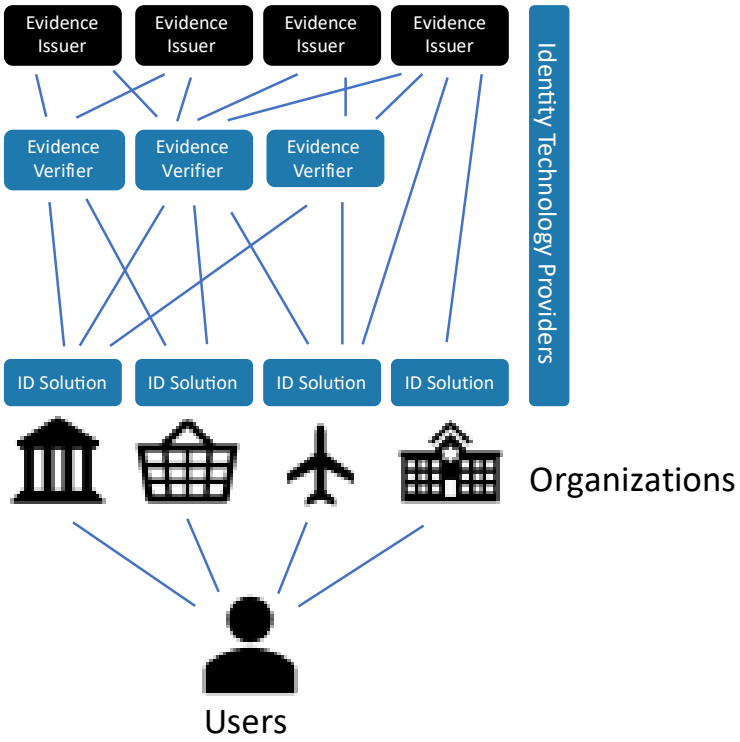
- Build on the work OIX has done over the last 10 years
- Focus on the rules, rather than the tools
- Focus on interoperability
- Be technology and ID implementation “flavour” neutral.
- Centric to user and relying party needs.
- A high-level guide, under which more detailed guides to specific areas will be added
- Use consistent terminology
- Will evolve as more detailed guides are added

Who is the guide aimed at?

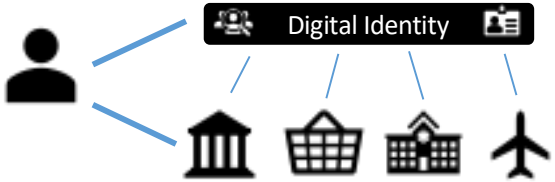
Who	Benefit
Global Identity Influencers	Brings together their already largely aligned thinking into a single –high level – easy to understand web-reference.
Existing Framework Operators	Defines how interoperability between frameworks can work.
Framework Creators	A Guide to creating frameworks that ensures any framework created is following proven best practice and will be interoperable with other frameworks. The OIX directory will list other frameworks for reference.
Relying Parties	Understand how trusted identities and access to eligibility works. Relying Parties can then use the OIX directory to find trusted suppliers of IDs: ID Providers, ID Brokers or ID Tech Component Providers.
OIX ID Services Members	Enables members to understand the ecosystem and position thier services against the framework based on their role (or sub-role) in the ecosystem.
Individuals	Explains how trust frameworks can provide them with portable, re-usable, ubiquitous identities that are interoperability between trust frameworks. *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.*

The Story – an evolution

Today: Organisation Centric ID

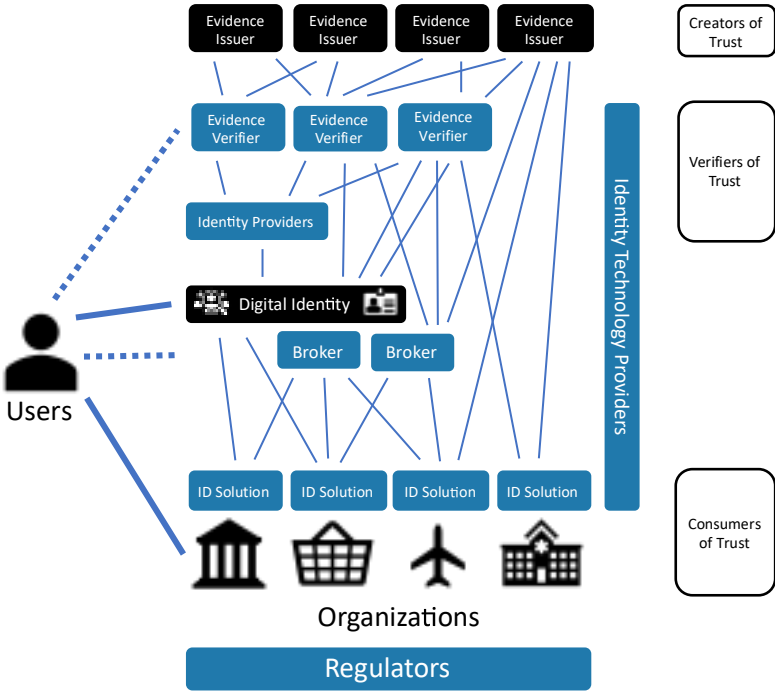


The Vision: Trusted Digital ID and Eligibility

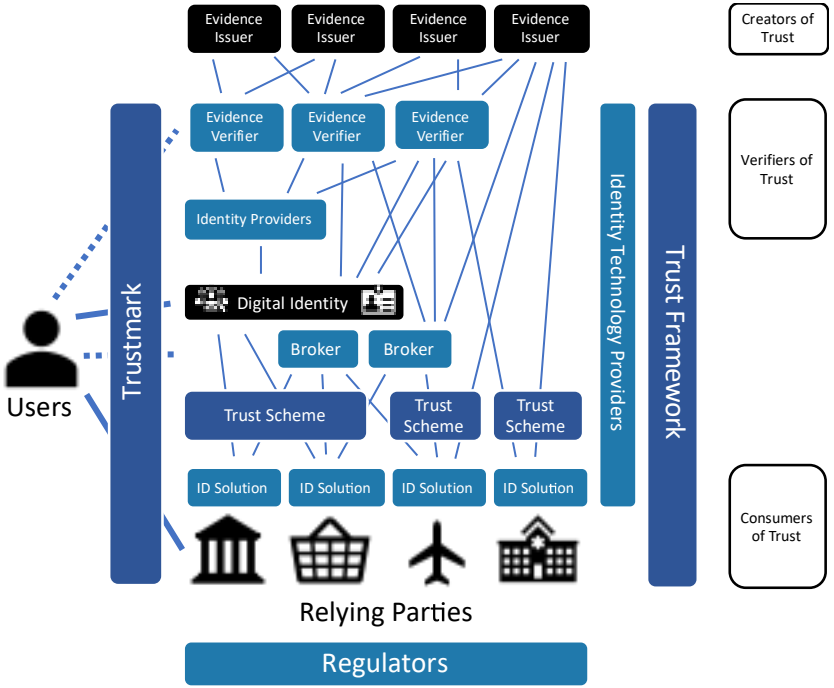


The Story – an evolution

1 - 5+ years: An Evolving Market



The Need: Governance of Trust



The OIX Guide to Trust Frameworks - Glossary

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.

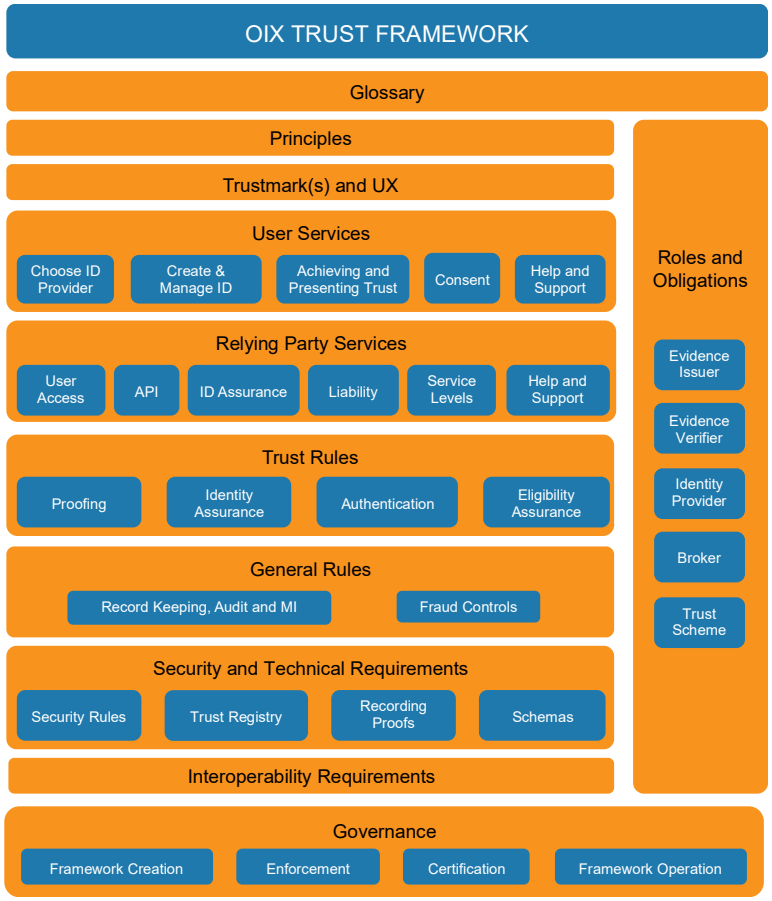
Throughout this guide all terminology used is consistent with this glossary.

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

Term	OIX definition	Common synonyms
Account Recovery	An individual must be able to recover credentials and / or an account that they have with a provider in the trust framework.	
Assertion	A collection of Attributes specific to a single Entity in response to a valid Authentication request and any additional metadata related to that response.	
Assurance Model	An Identity Assurance Model defines the types of evidence and methods for scoring each type in order to achieve a Level of Assurance for each of the different Identity Evidence Types: Validation Evidence, Verification Evidence and Identity Risk Evidence. It may also define the Authenticators required to re-access an account to assert and manage that level of assurance.	
Attestation	An Attestation is when a third-party Entity validates that according to their records, that Claims are true. For example, a University may attest to the fact that someone studied there and earned a degree. An attestation from an Authoritative Source is more robust than a proof, which may be forged.	
Attribute	A quality or characteristic inherent in or ascribed to someone or something, such as their name, or date of birth, passport number, qualifications, inoculations.	Claim
Authentication	A process that either enables the electronic identification of a natural or legal person.	
Authenticator	A trusted way to re-identify the user to allow them access and assert their Digital Identity. Different authenticators have different strengths and can be combined to create even greater strength. Typically, Authenticators fall into different types: Possession - something the user has, such as a token or device. Inherence - something unique about the user themselves, such as a biometric. Knowledge - something the user knows, such as a secret (e.g. a pin or password). Context - consider where the individual is, when they are transacting, what they are doing or may have done in conjunction with the Relying Party that both know i.e. historic, recent transactions	

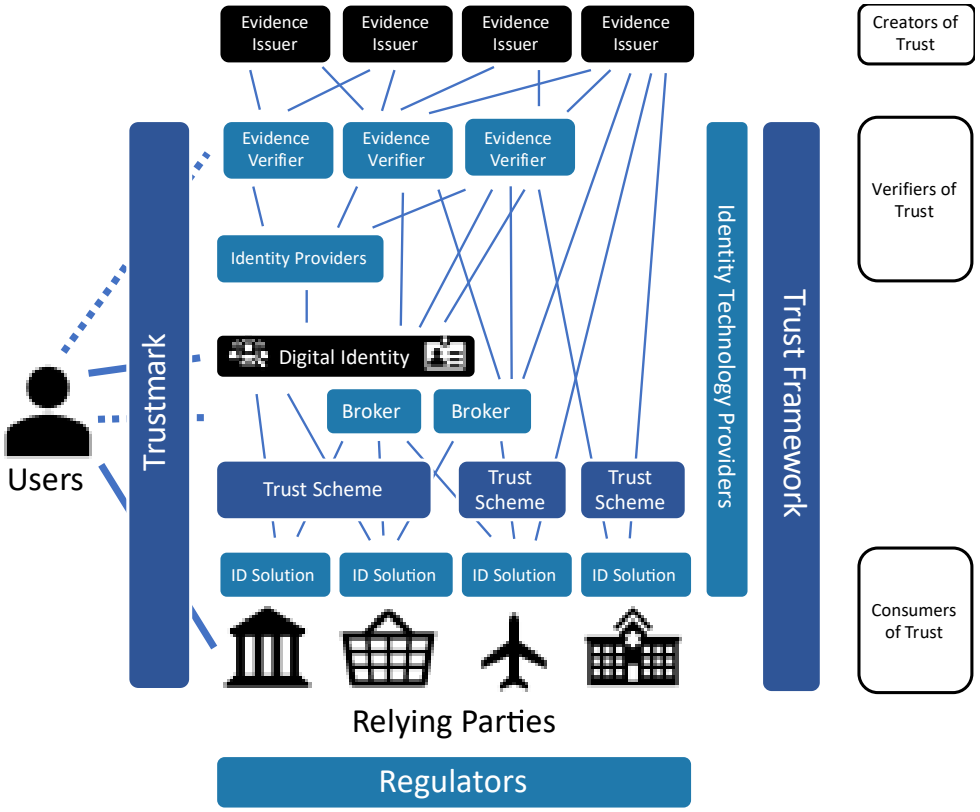
- Contains Synonyms
- Glossary terms in the guide are in ***bold italic***
- Some key decisions:
  - Evidence
  - Evidence Issuer
  - Evidence Verifier
  - User
  - Relying Party
  - Credential

The OIX Guide to Trust Frameworks - Contents



- User and Relying Party centric
- Focusing on the Rules, rather than the tools
- Each Orange Box is a section
- Each Blue Box is a sub-section

The OIX Guide to Trust Frameworks - Roles



- Real World Roles
- ID Operational Roles
- Governance Roles

- Roles will often be combined in any one trust framework implementation

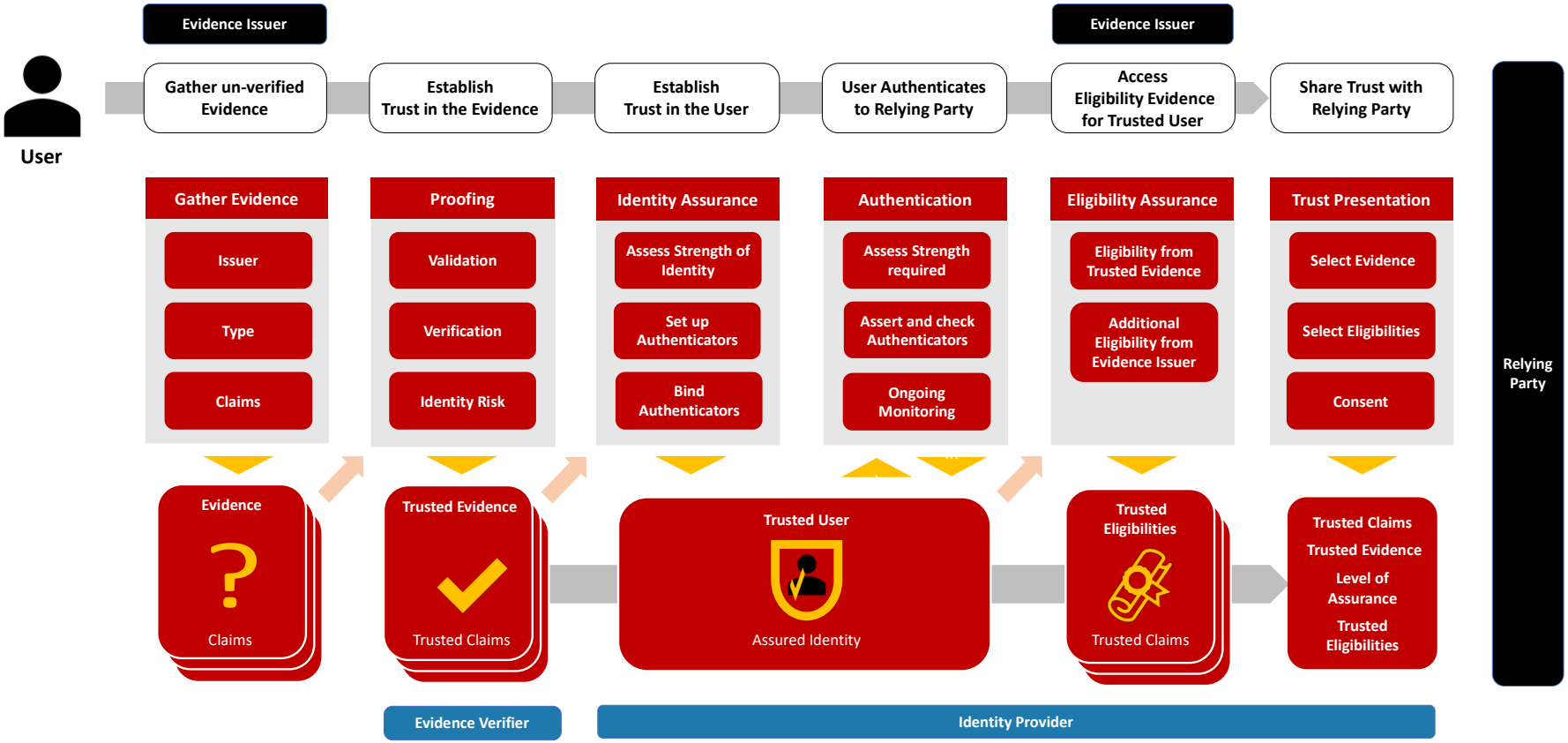
- One size does not fit all, even in one market

The OIX Guide to Trust Frameworks - Obligations

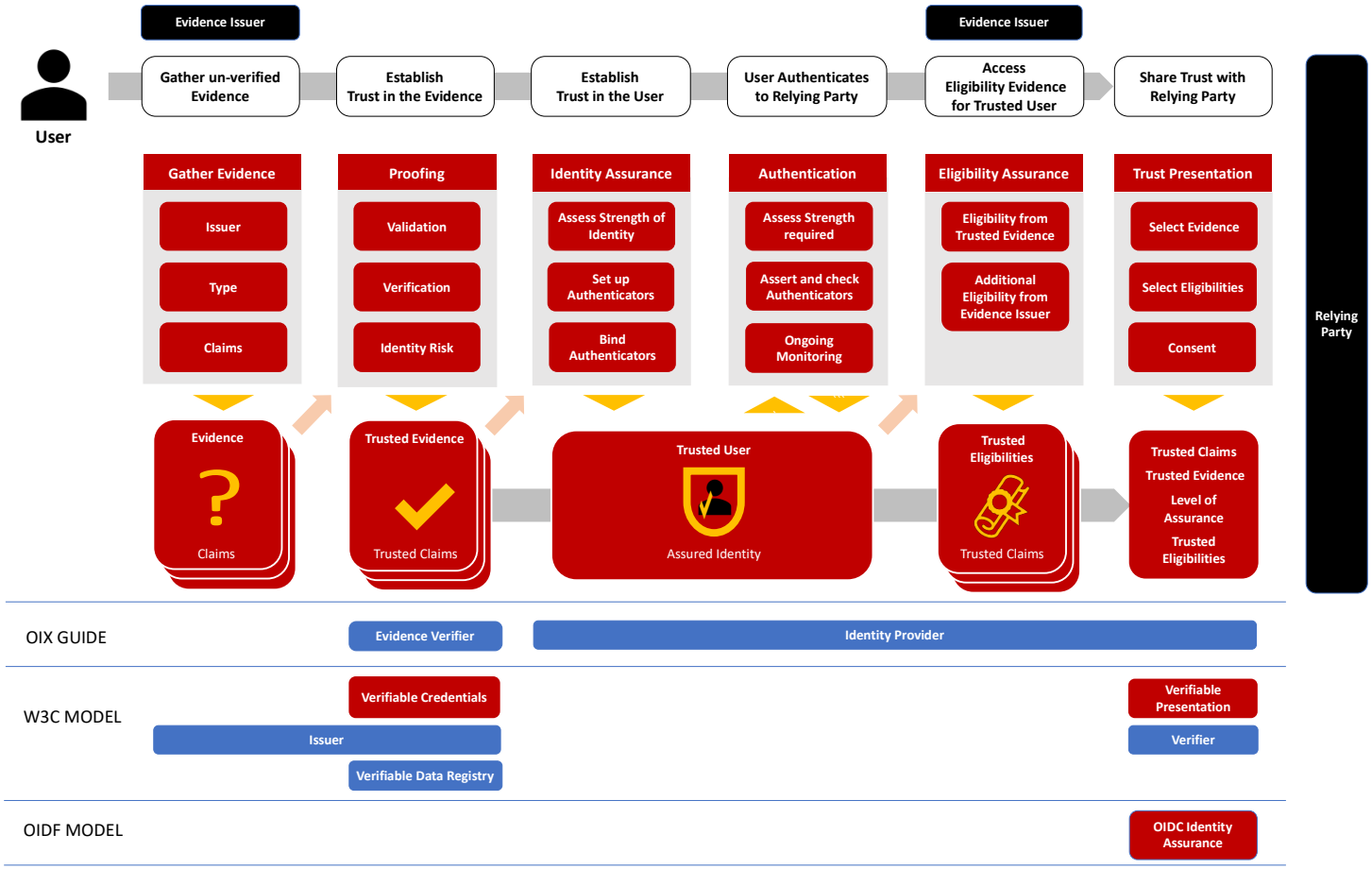
		Who?
Identity Assurance		
Definition of Level(s) of Trust	A level of trust can be determined by an ***identity assurance model*** that defines the types and amounts of ***trusted evidence*** required to achieve that lelve of trust, along with the ***proofing*** scores required to be achieved for ***validation***, ***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 role responsible for **defining** key rules is identified.
- By default, all rules are for consideration by the framework implementor.
- The role responsible for **complying** with each rule is identified
- There are often choices dependent on the way the framework is to be implemented.

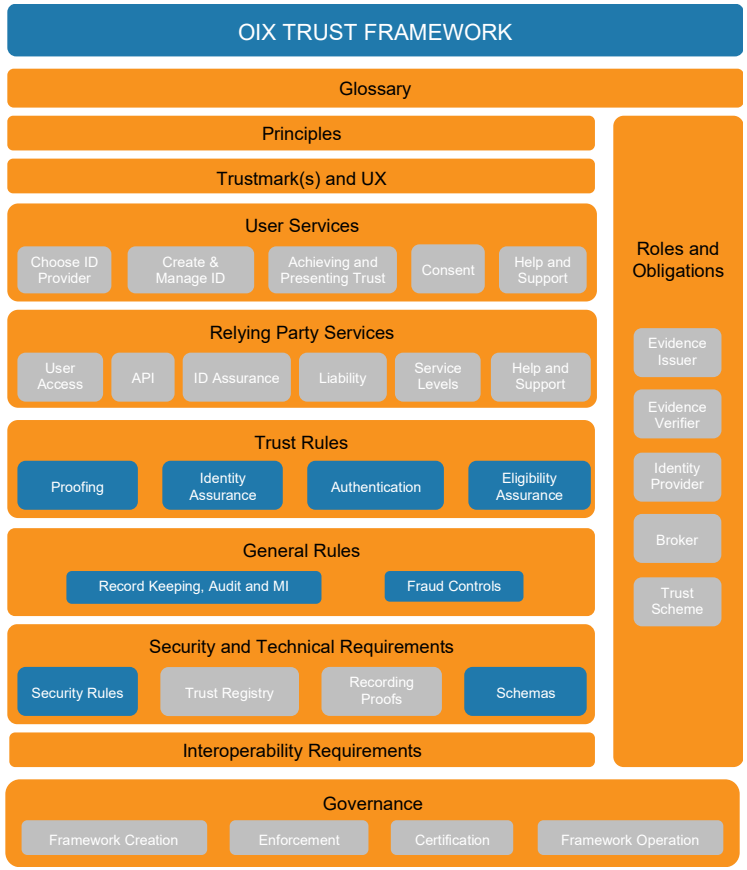
The OIX Guide to Trust Frameworks – Trust Rules



If OIX is about the “rules”, where do the “tools” fit?

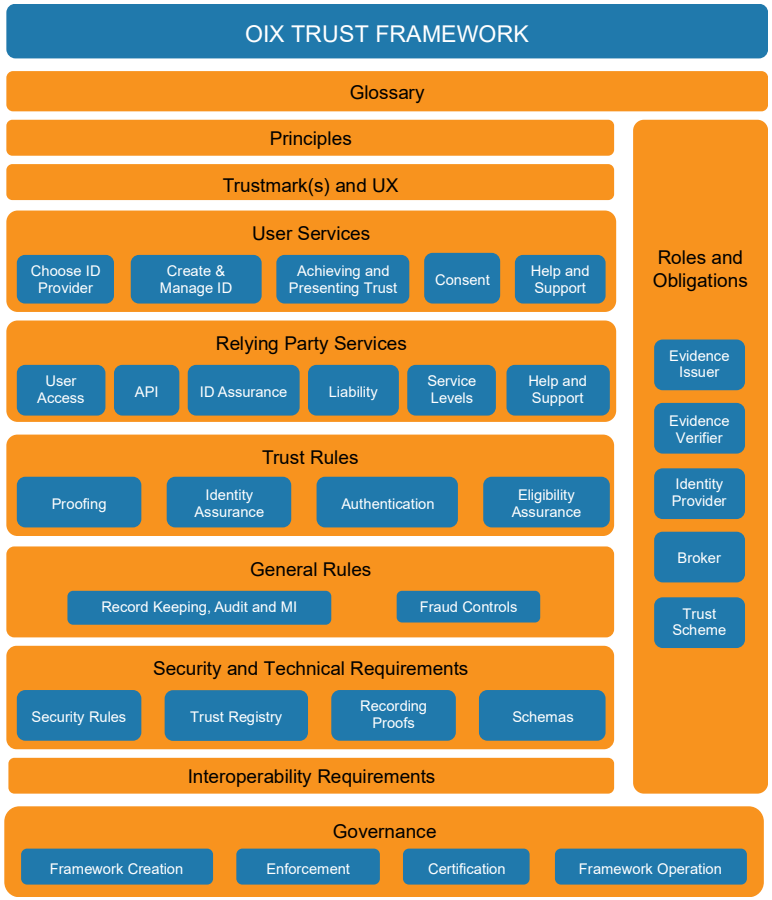


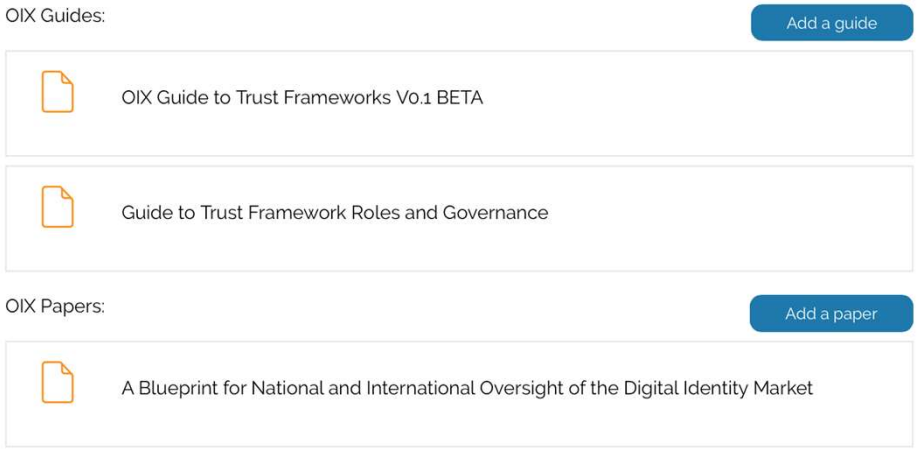
The OIX Guide to Trust Frameworks - Interoperability



- Key areas for cross-framework interoperability identified so far are:
  - Trust Rules
  - Record Keeping and Audit
  - Fraud Controls
  - Security Rules
  - Schemas

Accessing Detail behind the Web Guide





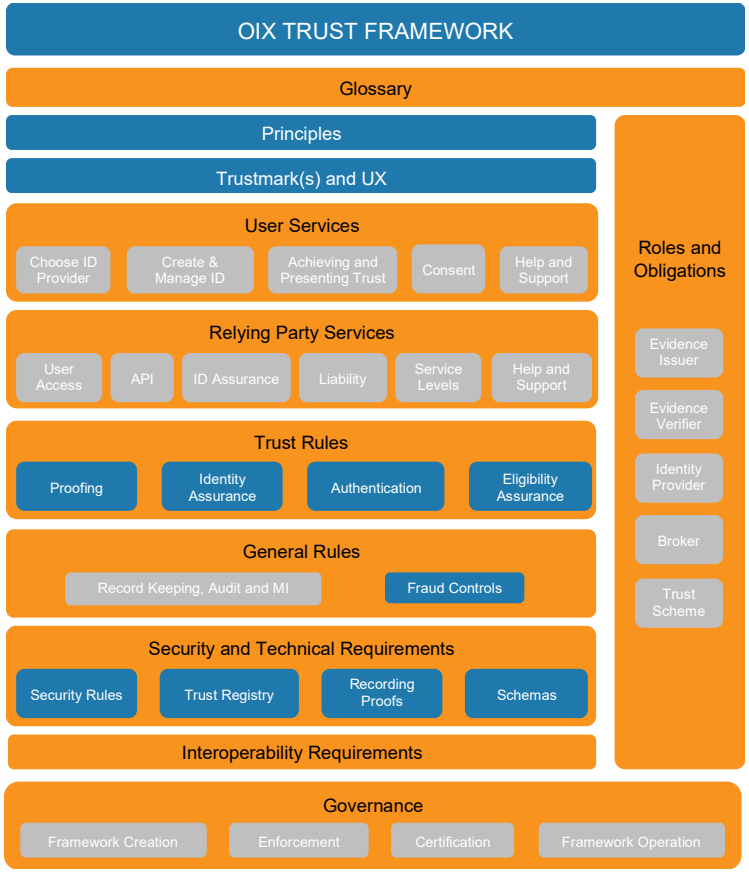
Key guides / papers attached so far:

- Paper version of the OIX Guide to Trust Frameworks
- OIX Glossary of Terms
- A Blueprint for National and international Oversight of the Digital Identity Markey
- Digital Identity – Approach to Liability

Guide to Identity Trust Frameworks

WEB GUIDE DEMONSTRATION

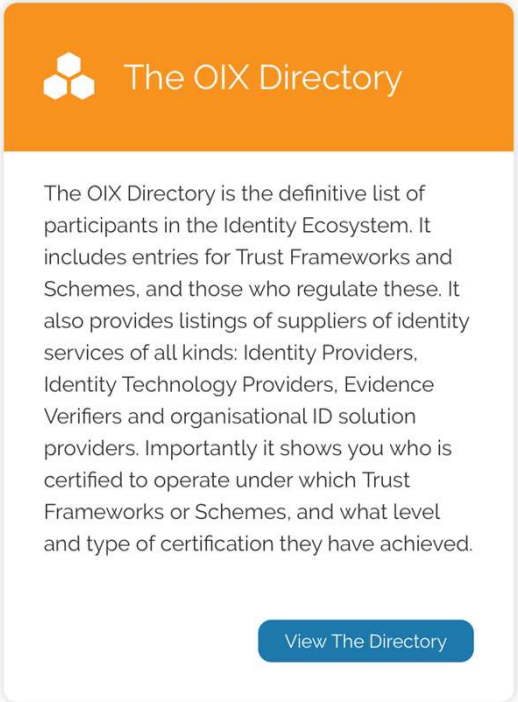
Adding Detail to the Guide – Working Groups



Producing new more detailed Guides:

Working Group	Guides
Trust Frameworks: Design, Principles and Trustmark	• OIX Guide to Trust Frameworks • Trust Framework Principles • Guide to Trustmark's
ID Proofing and Authentication	• Guide to ID Proofing and Authentication • Guide to ID Proofing and Authentication Interoperability.
Fraud Controls (with TISA)	• Guide to Digital Identity Fraud Controls
Architecture Interoperability (with TechUK)	• Paper or Guide on key considerations for interoperability across ID ”flavours” and technical standards.

The OIX Directory



- List Trust Frameworks and Schemes
- List ID supplier services:
  - Identity Providers, Brokers, IAM Providers, ID Verification, ID Authentication, ID Aggregators, ID Consultants, any other IDtech.
- Show who is certified to what standard, Trust Scheme or Trust Framework.
- Free supplier entries for Members
- Non-member suppliers can pay for entries
- Members will now be populating the OIX directory for launch in September 2020

Guide to Identity Trust Frameworks

LAUNCH WEBINAR

QUESTIONS