innovate identity™

experts in id

OPEN IDENTITY EXCHANGE

OIX Trust Framework Guide

Identity Proofing and Authentication Interoperability Guide

Project Aims and Outcomes

To develop a structured approach to assessing interoperability across the various elements of identity proofing and authentication including:

- A structured framework to assessing equivalency / compatibility.
- The key considerations for an assessment.
- A way to communicating the degree of interoperability.

Intended outcomes:

- Enable an assessor of interoperability, a trust framework operator, standard setter, identity provider or a relying party to understand how an interoperability assessment may be structured, and what proofing and authentication issues or processes an assessment should include.
- To enable practitioners to have a means to communicate or understand an assessed level of interoperability, and for that to be acted upon.
- To ensure the approach could be used as the basis for a full detailed assessment methodology to be developed, or upon which a trust mechanism (such as certification or formal recognition) could be based.

Defining Interoperability

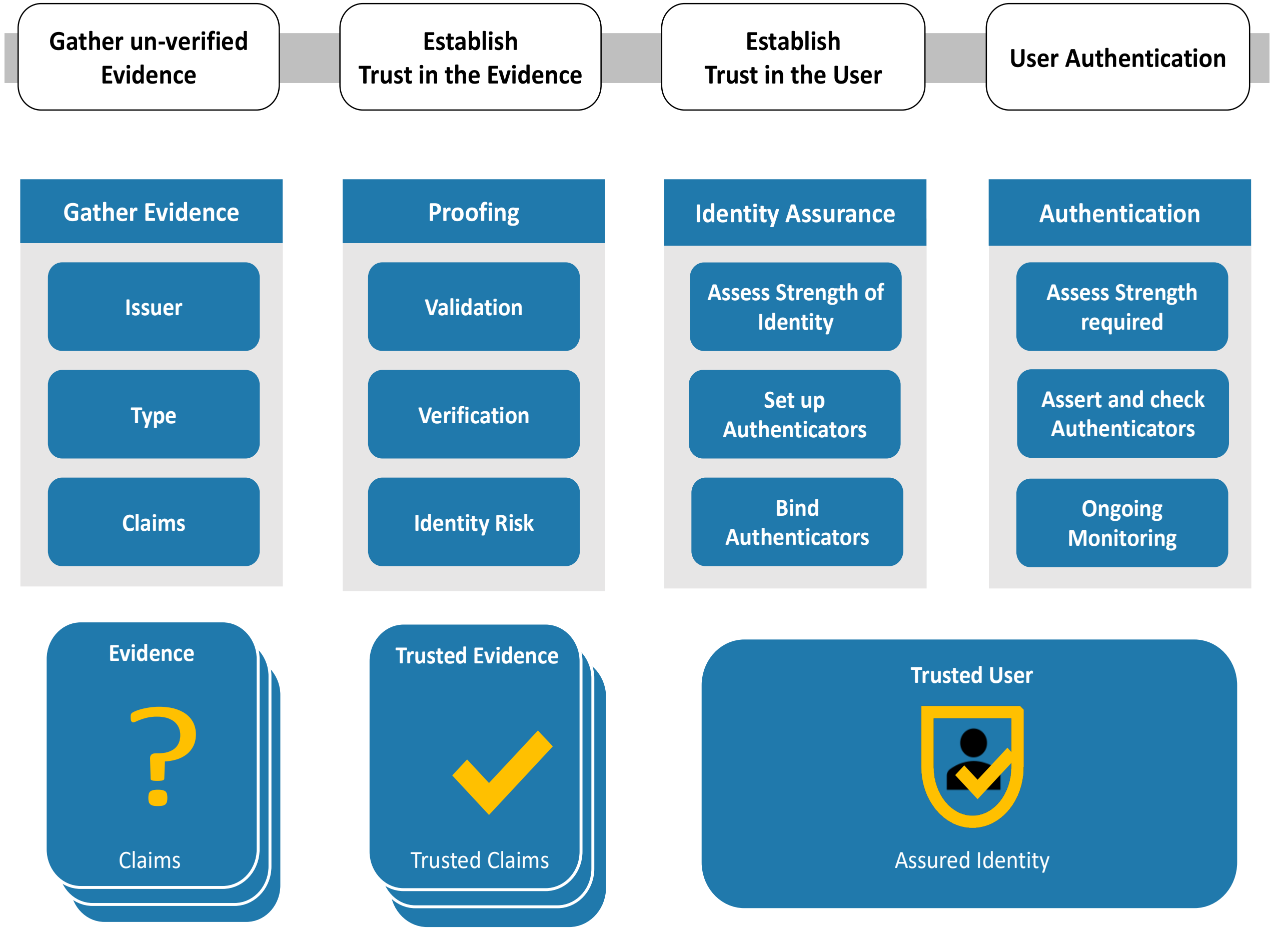
> *“the ability of two systems to exchange and make use of data”*
>
> *“the seamless, secure and controlled exchange of data between different applications and technologies”*

Interoperability for Identity Proofing and Authentication:

- The degree of compatibility and equivalence between different trust frameworks or identity levels - concerning the evidence and processes used to create the identity (and the results of those processes).
- The degree to which an effective exchange of data is possible - in this case identity data, and the evidence concerning how the identity was proofed and authenticated.
- The degree to which intervention is necessary to utilise the identity data, and the level of risk associated utilising it – there should be no ambiguity or mis-translation.
- The degree to which the data is actionable – the identity data’s format and value must be understood, and the level of assurance or risk mitigation needs to be clear to the recipient.

CATEGORY	DEFINITION
Technical Interoperability	The ability of two or more participants in a market to accept data from each other and perform a given task in an appropriate and satisfactory manner. A measure of the compatibility and connectivity between two technical systems.
Syntactic Interoperability	The comparability and degree of similarity of how data is formatted, packaged and exchanged between different systems. This can be accomplished by following common standards, and via the exchange of data describing the evidence (metadata). This factor is often combined with semantic interoperability (below).
Semantic Interoperability	Ensuring that the various participants within a market are able to exchange information with an unambiguous, shared meaning and value. This can be enhanced through the use of common or comparable scoring frameworks, and linking data to a controlled or shared vocabulary, or via the identification of synonymous terms and definitions.
Organisational Interoperability	Ensuring that objectives and principles that guide the actions of the various participants are aligned, or to assess the degree of their compatibility. This ensures that data can be exchanged with clear and aligned purposes in mind. In some interoperability models this factor may include the legal and governance factors, but here they are split into separate categories, below.
Legal Interoperability	The degree of alignment between two or more national or state legal and regulatory trust frameworks, and the compatibility of the legal requirements and obligations placed on parties operating within the two trust frameworks.
Governance Interoperability	The equivalence of the manner in which the trust frameworks and the constituent elements of the identity creation and monitoring processes are overseen. The degree to which the governance and oversight mechanisms may be considered equivalent in terms of the degree of oversight, the type and strength of oversight mechanisms utilised (such as certification or audit regimes) and the degree of independence of that process.
User Interoperability	Ensuring users can access a service and as part of doing so assert their identity in a manner which is a) familiar, b) trusted, and c) efficient. For example, whether there a comparable user experience or interface, common rules and consumer protections, or a recognised consumer-facing trustmark of some kind.

Identity Proofing and Authentication – Key Elements



Gather un-verified Evidence

Establish Trust in the Evidence

Establish Trust in the User

User Authentication

Gather Evidence
- Issuer
- Type
- Claims

Proofing
- Validation
- Verification
- Identity Risk

Identity Assurance
- Assess Strength of Identity
- Set up Authenticators
- Bind Authenticators

Authentication
- Assess Strength required
- Assert and check Authenticators
- Ongoing Monitoring

Evidence ? Claims

Trusted Evidence ✓ Trusted Claims

Trusted User – Assured Identity

The Approach Structure

- Utilising the generic key elements set out in the end-to-end identity model.
- Cross-referencing the steps against the different interoperability factors.
- This approach is adaptive and individual interoperability factors can be weighted as appropriate.
- This provides a generic structure and approach to assessing and then communicating the level of interoperability, and where a greater degree of misalignment may be an issue.
- The assessment approach is able to adapt to different identity solution architectures – not all steps need to be present or enacted in sequence to enable an assessment to be made.

User Considerations (see next slide)

- A wide-ranging series of detailed points for an interested party to consider for each key element when undertaking or considering the results of an interoperability assessment.
- Aligned to 7 interoperability factors.

CONSIDERATIONS **Step 1. Evidence and Claims**	
Technical	• What claims and security features are present for each corresponding evidence type? • How is the identity evidence recorded and transmitted? • Does it align to international or national standards?
Syntactic	• How are claims (attributes) data formatted (e.g. name, address, date of birth)? • How are issuing organisations categorised and that information represented in the evidence? • How is metadata ordered and packaged?
Semantic	• How is evidence described and categorised? What relative strength is given to each? • How are the types of evidence defined? How are security features described? • Do they align to recognised standards?
Organisational	• Is evidence collected for the same purpose? • Are principles concerning the use of personal data aligned? • Are use case risks understood and mitigated in the same way?
Legal	• Are there local regulated types of evidence required in either trust framework? Do they compare? • Are there local restrictions as to the evidence that can or cannot be presented? • How it is recorded (e.g. consent, privacy, data sharing rules)?
Governance	• Is the data collection process governed and overseen or audited in some way? • Is the adherence to process or issuance standards certified or in any other way assured? • How do these processes align?
User	• Are the means by which evidence is gathered from users similar? • Are there comparable rules regarding the user experience and expectations for this process? • Are there comparable arrangements for accepting non-standard forms of evidence, for example for thin-filed or vulnerable users?

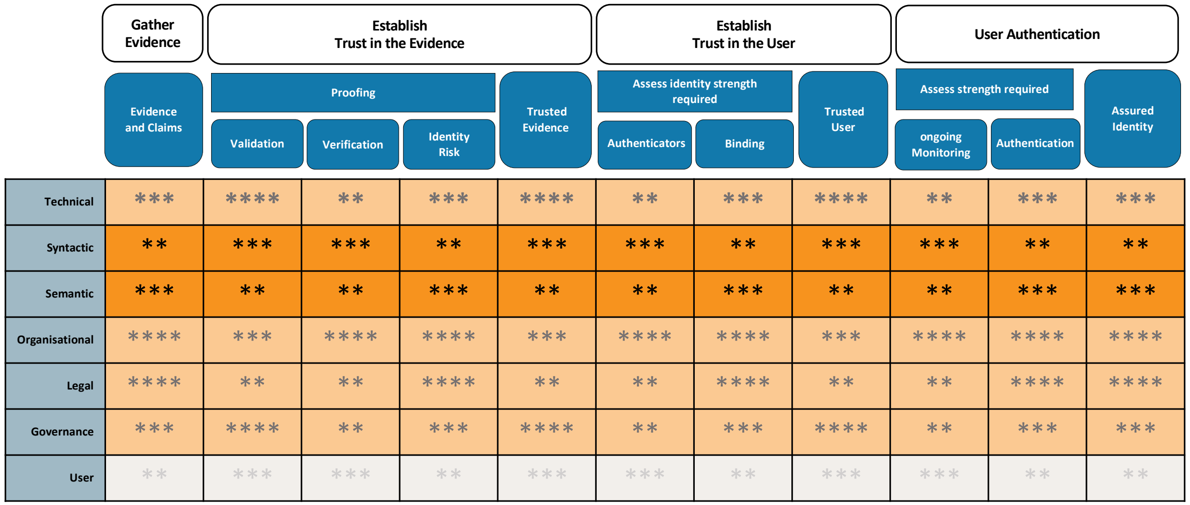
The Approach in Practice (1)

	Gather Evidence	Establish Trust in the Evidence				Establish Trust in the User			User Authentication		
		Proofing				Assess identity strength required			Assess strength required		
	Evidence and Claims	Validation	Verification	Identity Risk	Trusted Evidence	Authenticators	Binding	Trusted User	ongoing Monitoring	Authentication	Assured Identity
Technical											
Syntactic											
Semantic											
Organisational											
Legal											
Governance											
User											

Stage One: Interoperability Assessment

1. Select the interoperability factors applicable on the matrix (vertical axis).
2. Select the identity proofing and authentication steps applicable (horizontal axis). This may first require comparing the trust framework’s use of key terms and definitions to the OIX Identity Proofing and Authentication Guide.
3. Assess the relevant importance of each matrix cell (primary, secondary, inconsequential).
4. For each cell of primary or secondary importance, compare the two trust frameworks using available policies, procedures, standards and specifications.
5. Score each cell using the identity interoperability assessment-adapted SPICE model.

The Approach in Practice (2)



	Gather Evidence	Establish Trust in the Evidence				Establish Trust in the User			User Authentication		
	Evidence and Claims	Proofing			Trusted Evidence	Assess identity strength required		Trusted User	Assess strength required		Assured Identity
		Validation	Verification	Identity Risk		Authenticators	Binding		ongoing Monitoring	Authentication	
Technical	***	****	**	***	****	**	***	****	**	***	***
Syntactic	**	***	***	**	***	***	**	***	***	**	**
Semantic	***	**	**	***	**	**	***	**	**	***	***
Organisational	****	***	****	****	***	****	****	***	****	****	****
Legal	****	**	**	****	**	**	****	**	**	****	****
Governance	***	****	**	***	****	**	***	****	**	***	***
User	**	***	***	**	***	***	**	***	***	**	**

Stage Two: Considering Interoperability Assessment Outcomes

The completed assessment matrix populated with the assessment score indicates:

- The relative importance of each of the interoperability factors to identification proofing and authentication, depicted by the shading.
- The degree of correlation between the approaches to identification within each trust framework.
  - Low scores indicate areas of significant differences in the approaches to identification between the two trust frameworks; a low degree of alignment. High risk. High intervention.
  - High scores indicate the steps at which the two approaches are closely correlated, providing the basis for an interoperable model to be established; a high degree of alignment. Low risk. Low intervention.

The Approach in Practice (3)

	Gather Evidence	Establish Trust in the Evidence				Establish Trust in the User			User Authentication		
	Evidence and Claims	Proofing			Trusted Evidence	Assess identity strength required		Trusted User	Assess strength required		Assured Identity
		Validation	Verification	Identity Risk		Authenticators	Binding		ongoing Monitoring	Authentication	
A to B											
B to A											

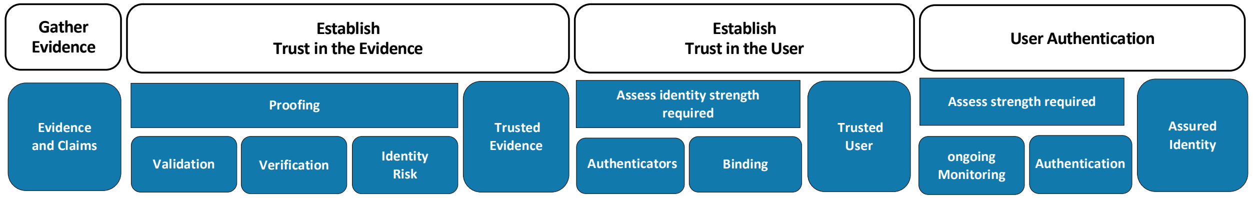
Stage Three: Comparative Strength Assessment
This is a detailed and technical assessment of each relevant step in identification set out in each of the two trust frameworks being compared, that will determine the degree of equivalence.

1. For each cell, analyse supporting material such as the policies, procedures, standards and specifications
2. Determine the relative strength of the approach comparing one trust framework to another.

Considerations include:

- Equivalence of claims data, security and robustness of identity evidence and its sources
- Equivalence of performance, security, risk and level of confidence associated with checking processes
- Equivalence of inputs and level of risk mitigation and assurance associated with identity levels

The Approach in Practice (4)



	Evidence and Claims	Validation	Verification	Identity Risk	Trusted Evidence	Authenticators	Binding	Trusted User	ongoing Monitoring	Authentication	Assured Identity
A to Model	▨	🟦	🟦	🟦	🟦	▨	🟦	🟦	🟦	▨	▨
B to Model	🟨	▨	🟨	🟦	🟨	🟦	🟦	🟨	▨	🟦	🟨
C to Model	🟨	🟨	🟨	🟧	🟧	🟦	🟨	🟨	🟦	🟦	🟧

Stage Four: Comparative Strength Assessment Outcomes

1. The higher the number of equal strength cells, the greater the equivalency between identification steps in the two trust frameworks and their outcomes.
2. Cells which indicate a lack of equivalence will need to be addressed.

Measures may need to be considered to resolve this lack of equivalence – requiring additional/stronger checks, additional/stronger evidence or a higher identity level.

- Steps that are indicated as having weaker or significantly weaker strength in one of the trust frameworks require particular attention, due to the lower level of risk mitigation this presents.
- Steps that are indicated to be stronger or significantly stronger in one of the trust frameworks may also require attention, such as to minimise the volume, type or sensitivity of the data used.