OIX INTEROPERABILITY GUIDE: IDENTITY PROOFING AND AUTHENTICATION

December 2020

Version 1.0

Authors: Ewan Willars and Rob Laurence
Innovate identity

CONTENTS

Document Version History

Name of Document / version	Version Number	Date
First release	1.0	December 2020

1. INTRODUCTION

Section One Overview
Section One introduces the interoperability guide, explains how it is meant to be used, and by which audiences. It sets out how the guide is structured, and an overview of what is included.

The OIX Interoperability Guide provides 'how to' guidance for anyone interested in assessing how different identity ecosystems interact. It sets out a clear, adaptable approach to assessing ***interoperability*** of ***identity proofing*** and ***authentication*** carried out in different regional or national ***trust frameworks***.

Building on the evidence of approaches to assessing and communicating interoperability taken in other sectors, and building on the preceding ***Guide to Identity Proofing and Authentication***, the Interoperability Guide provides a structured approach to assess interoperability between identity trust frameworks, and to assess the equivalency of ***identity levels*** across different trust frameworks, covering all of the key elements of identity proofing and authentication.

The Interoperability Guide:

- Defines interoperability for digital identity proofing and authentication, based on previous applications, including from other sectors.
- Sets out the key considerations for anyone carrying out or acting on the results of ***interoperability assessment***, such as relying parties, standard setters, identity providers, trust framework operators, authorities or assessment practitioners.
- Provides guidance on a specific approach to assessing interoperability, including an assessment structure for assessing compatibility between trust frameworks, and the degree of equivalency between identity levels.
- Gives guidance on methods to communicate the degree of interoperability.
- Provides guidance for interpreting and acting on interoperability assessment scores.

The outcomes intended for the Interoperability Guide are to:

1. Enable an assessor of interoperability (whether standard setter, authority, relying party or identity provider) to understand how an identity proofing and authentication interoperability assessment should be approached, and what issues and processes such an assessment should include.
2. Provide the means to communicate the results of an identity proofing and authentication interoperability assessment, and the considerations for potential actions based upon it.
3. Provide a structure and approach to inform a full and detailed interoperability analysis.
4. Enable different parties to understand how to achieve a high degree of interoperability, and to identify where and why interoperability may be currently compromised.

Using the Interoperability Guide
When reading the guide:

- Dotted grey boxes contain overviews of different aspects or sections of the guide.
- Blue Considerations boxes provide examples of the main issues to focus on at each stage, the questions that different parties should consider when approaching interoperability assessment, and the actions they may consider as a result. These considerations are expanded step-by-step in the Appendix.
- Text in '***bold italics'*** link to the terms and definitions set out in the ***OIX Glossary***. For further terms and definitions and an introduction to the principal concepts of identity proofing and authentication, please read the ***OIX Guide to Identity Proofing and Authentication.***

Section Two defines interoperability and its principal component factors. Section Three sets out a structure for interoperability assessment of proofing and authentication, and an assessment matrix for assessing inter-trust framework interoperability, and the equivalence of identity levels. Section Four sets out methods to communicate the results of an assessment, and how to act on the data that provides. A four-stage implementation plan is included in Section Five of the guide.

The Interoperability Guide will not:
- Provide a specification.
- Provide detailed assessment evaluation criteria.

The OIX Digital Identity Trust Framework Guides
Other areas of identity, including the guide to proofing and authentication plus guidance on identity management, storage and maintenance, the roles of different organisations, how identity ecosystems may be governed and how trust frameworks can be developed are covered in a series of separate but connected publications.

- OIX GUIDE TO TRUST FRAMEWORKS AND INTEROPERABILITY [i]
- **LINK TO GUIDE TO IDENTITY PROOFING AND AUTHENTICATION (TBC)**

2. INTEROPERABILITY OF IDENTITY PROOFING AND AUTHENTICATION

Section Two Overview
Section Two defines the concept of interoperability, its various factors, and how these relate specifically to identity proofing and authentication. It explains why an approach to interoperability is required, provides guidance on the key challenges for readers to be aware of, and some of the major considerations involved in assessing interoperability for different parties. It sets out the fundamental features that an interoperability assessment needs to have in order to be effective.

Interoperability has a range of definitions, varying by context and subject. In each case this has an impact on how interoperability is assessed, and how that degree of interoperability is then best expressed. Any interoperability assessment approach needs to be founded upon a clear understanding of what interoperability means in that specific context.

In this section interoperability will be defined in terms of what it means for digital identity, and for proofing and authentication specifically. A multi-layered model for interoperability assessment will be presented in a way that can help to represent the different challenges and practical considerations involved in an assessment, providing a highly practical as well as conceptually sound underpinning for the approach.

Defining Interoperability
The simplest generic definition of interoperability belies its complex nature:

> "*the ability of two systems to exchange and make use of data*".

With a little more nuance, a definition used in the education sector describes interoperability as being:

> "*the seamless, secure and controlled exchange of data between different applications and technologies*[ii]."

Combined, these two simple definitions capture the important elements of interoperability for identity, and for proofing and authentication in particular.

- Firstly, that there is an effective and secure exchange of data, i.e., the identity data, and the evidence concerning how the identity was proofed and authenticated.
- Secondly, it requires as little intervention as possible (the 'seamless' requirement).
- Finally, it needs to be actionable. For that to be the case, the data's format and value needs to be described, understood and acted upon by the recipient.

The level of intervention required, the chance of problems occurring, and the level of risk involved in a transaction decrease as the level of interoperability increases.

Interoperability Challenges

There are a range of issues that create a more challenging environment for interoperability to be established. Issues such as:

- **Legal Diversity** – while there are some relevant standards and guidance that are recognised internationally (e.g., FATF Financial Crime and AML guidance, or data protection standards such as GDPR), there is a wide diversity of legal frameworks in practice, that vary in terms of their requirements, the terms and definitions they use, and how they impact on the practical implementation and use of digital identities.
- **Different Delivery Architectures** – different national or state-level identity ecosystems may each encompass a range of identity approaches, from decentralised and self-sovereign identity to highly centralised and federated systems. Comparing 'apples to oranges' can be a complicated process unless there is a common structure or standard that can be applied to all solutions.
- **Range of Technologies** – the technologies that underpin identity solutions and how they record, store, process and present data can vary widely, such as via blockchain, various registries and databases, cloud-based solutions, and via different devices and channels.
- **Semantic and Syntactic Diversity** – OIX research has demonstrated the lack of alignment between the terms and definitions used across different trust frameworks, and the formatting and values used to describe identity data. Creating a common nomenclature, such as that provided by the ***OIX Identity Glossary***, and other shared syntactic approaches, such as those presented by international standard setters, are both important steps towards interoperability.

To address the interoperability challenges, it is necessary to assess the impact they have on the alignment, compatibility and equivalence of identities created within different trust frameworks. By firstly understanding the degree of existing interoperability, actions can be taken to better align trust frameworks, and the proofing and authentication steps.

A successful approach will:

- Enable the degree of interoperability to be assessed for all interoperability factors.
- Be adaptable enough to encompass a range of technologies and local delivery approaches, while being ordered in a manner than enables direct comparison of alignment, equivalence and comparative strength to be made.
- Due to the nature of identity and how identities are created, it may be necessary to consider interoperability at both a) a granular level, assessing equivalence at a high level of detail at every step, such as specific types of identity evidence and processes used, and b) at an outcome level, for example assessing equivalence between different levels of assurance or risk mitigation.
- Provide a framework against which certification or other trust mechanisms could be developed, such as by an independent authority or standard setter.
- Provide a means to communicate the assessed level of interoperability in some way, and by doing so to identify the steps where action may be needed to increase interoperability, enabling a relying party to utilise an identity with a sufficient range of data and degree of risk mitigation.

In summary, combining all of these success factors, a successful interoperability assessment approach should be:

- **Structured**
- **Adaptable**
- **Repeatable**
- **Comparable**
- **Actionable**

Interoperability of Identity Proofing and Authentication

The degree of interoperability of identity proofing and authentication carried out in different trust frameworks can be critical information for a range of parties.

Some of the main considerations are set out below.

CONSIDERATIONS

For Relying Parties:

- Can the identity be trusted?
- Was it created in a trust framework that is comparable with the local trust framework in terms of its quality of governance, how it defines identity evidence, and how the user's identity has been proofed and authenticated?
- Does the identity evidence used to create the identity equate to the type of identity evidence locally required? Has it been assessed as being of equivalent strength?
- Will using the identity mitigate the relying party's identity risk proportionate to the level of risk associated with the use case? How do the levels of assurance align to assurance levels in another trust framework?

For Identity Providers and Brokers:

- Do the types of identity evidence used provide the required data about the user?
- How do the identity levels in the trust framework in which an identity was created align to other trust frameworks?
- If an identity level falls short of the equivalent local requirements, can it be stepped up? Is it possible to:
    - Collect or assert additional or stronger identity evidence?
    - Undertake additional, more robust identity proofing processes?
    - Use stronger authenticators or authentication methods?
- Does the user have access to another identity of higher strength?

For Authorities:

- Is the trust framework, within which an identity was created, trusted?
- Does the trust framework operate with equivalent standards, governance, privacy and security arrangements?
- Are local levels of assurance recognised by a competent authority? If so, are the levels of strength or assurance requirements equivalent across different legal or regulatory environments?
- Can the assessment of interoperability be trusted? Has it been carried out according to a structured, robust, repeatable approach?

- Are users and other parties protected by equivalent liability arrangements or reciprocal legal protection?

For Standard Setters:

- Are the standards aligned to those in other jurisdictions or trust frameworks?
- Do the standards and how they are presented lend themselves to delivering and assessing cross-framework interoperability – e.g., are definitions in line with common usage elsewhere?
- Are evidence types aligned to common or recognised standards?

Categorising Different Interoperability Factors

Interoperability can be broken down into a number of ***interoperability factors***, which helps to provide a structure to assessing and analysing it in practice, as well as conceptually. The first four factors set out in Figure 1 frequently appear in a number of interoperability models, i.e., technical, syntactic, semantic and organisational factors.[iii]

For identity there are further factors that need to be considered and that have been explored by OIX research previously, i.e., governance, legal, and user factors.[iv]

FIGURE 1: Interoperability Factors

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.

The factors provide a means to categorise a range of interoperability issues and the structure for an assessment approach.

For assessing interoperability of proofing and authentication specifically, and based on the context within which the assessment is being made (such as the type of use intended for the identity transaction), some of the factors will be of relatively greater or lesser importance.

For example, semantic interoperability will be a key area of focus when comparing two trust frameworks and the degree to which data might be exchanged between them, commonly understood and then utilised. Terms and definitions can vary widely (and sometimes subtly) between trust frameworks. It is necessary to understand how they compare, and where necessary intervene to translate or align them.

Certain interoperability factors are of lesser importance for proofing and authentication but vital in another area of assessment. For example, user interoperability may be less important for proofing and authentication than it is for assessing interoperability in the way an identity is transmitted or asserted by its owner.

This will be an important consideration in the next section where weighting or prioritising certain data may be necessary when undertaking a detailed assessment analysis.

Some of the main considerations for each of the interoperability factors are explored below.

CONSIDERATIONS

Technical Interoperability

- Are the processes used to validate, verify and record evidence of a comparable technological base – are they technically compatible?
- Can data pass seamlessly between the systems?
- Do the trust framework participants adhere to recognised technical standards?
- Is the technology comparably mature? Are required performance levels similar?
- Is the level of technical security comparable?

Syntactic Interoperability

- Is the identity evidence generated at each step of proofing and authenticating the identity comparable to that in another trust framework?
- Is the data formatted in a manner appropriate to the use case and comparable to that used in a second trust framework?
- Is the value expressed in a comparable format and data types?
- Are evidence and metadata formats and values aligned?

Semantic Interoperability

- Can the terms and definitions used in different circumstances be aligned?
- Are evidence types and checking processes called the same thing?
- Are assurance or level of confidence measured in a comparable way?
- Are different evidence processes valued in the same way?
- Where terms and definitions differ are synonyms identified?
- Are processes categorised in the same manner?

Organisational Interoperability

- Is the range of intended end uses comparable?
- Is risk calculated in the same way?
- Are identities created and used for similar purposes?
- Are the underlying principles of the trust frameworks compatible, and aligned?

Legal Interoperability

- Are the legal frameworks aligned, in terms of the requirements and obligations expected of the various parties?
- Are regulatory standards common, or aligned across the two jurisdictions?

Governance Interoperability

- Is there a trusted authority or organisation to assess or guarantee interoperability for the user and market participants?
- Are the trust framework rules set by comparably independent or overseen organisations? Are trust mechanisms of a similar type?

User Interoperability

- Are similar user guarantees or equivalent consumer protections in place?
- Is there a shared or equivalent user-facing trustmark?
- Are the requirements to access use cases similar?

3. ASSESSING INTEROPERABILITY

Section Three Overview
Section Three provides guidance on the structured approach to assessing interoperability and the degree of alignment between trust frameworks, as well as interoperability between identity levels across different trust frameworks, focused on the proofing and authentication steps involved.

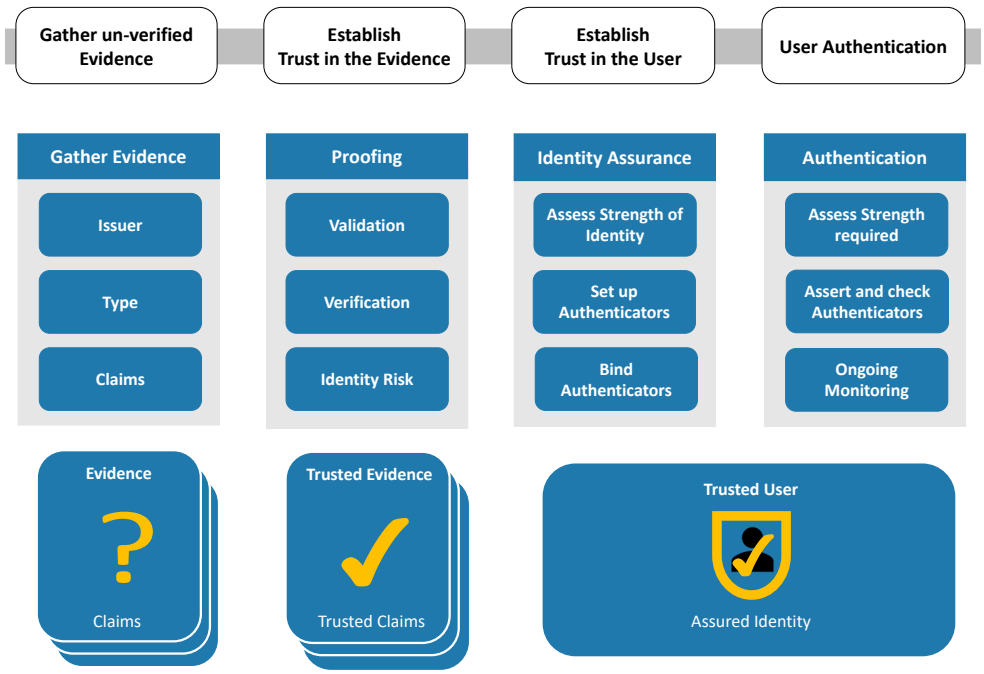
In this section, the guidance sets out a logical, clear and repeatable structure for the assessment of interoperability between trust frameworks, and in considering the relative strength of respective identity levels.

The approach is adaptable and able to accommodate a comparable assessment in a range of contexts and for a wide variety of identity architectures.

A Structured Approach
The ***OIX Guide to Identity Proofing and Authentication*** provides detailed guidance on the individual elements of proofing, authentication and assurance, and how they combine to deliver trusted, assured identities and confidence that the person asserting an identity is its rightful owner. The way that the guide sets out the steps involved, and the core elements and how they are categorised provides a frame upon which OIX approach is based.

The illustration below shows the end-to-end steps that go towards creating and asserting an identity – here the proofing and authentication steps are shown in blue. Broken down into its individual steps, it provides the underlying categorisation of the assessment approach.

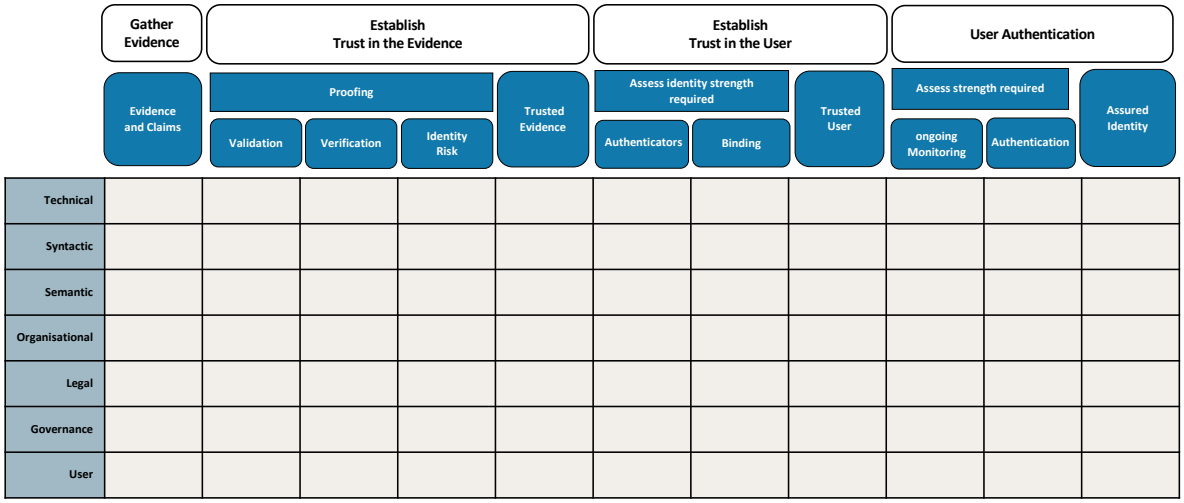
FIGURE 2: Identity Proofing and Authentication – key elements



A. FRAMEWORK-TO-FRAMEWORK INTEROPERABILITY ASSESSMENT

For assessing interoperability between trust frameworks, the various proofing and authentication steps (set out across the horizontal axis) combine with the seven interoperability factors (set out in the vertical axis) provide the basic structure for the Identity Proofing and Authentication Interoperability Assessment Matrix.

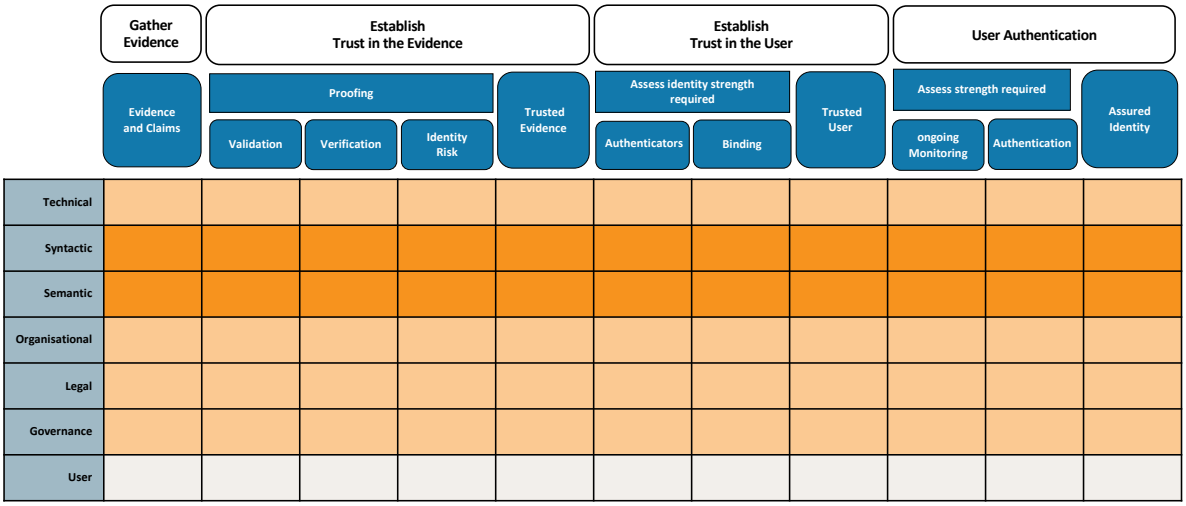
FIGURE 3: Identity Proofing and Authentication Interoperability Assessment Matrix



When considering an assessment of proofing and authentication interoperability, the most relevant of the seven interoperability factors are considered primary factors, shown in the following matrix in orange.

Secondary factors are shown in a lighter colour, and user interoperability is the least important factor – however it is retained in the matrix (light grey).

FIGURE 4: Interoperability Assessment Matrix: Weighted Factors



Practitioners can adapt how different factors are weighted in the matrix to reflect the context and purpose of the interoperability assessment being carried out. However, in the absence of further adaption, the primary and secondary factors identified in Figure 4 above provide a functional starting point.

Assessment Inputs

An assessment between trust frameworks is a bilateral assessment model. At a cross-framework level, interoperability is a measure of compatibility between the two systems (in this case two identity trust frameworks). It is a measure of the degree to which data can be exchanged and used without unnecessary intervention, mistakes or risks.

The data in this case comprises:

- Evidence used to create the identity.
- Claims provided by the evidence.
- Provenance of the evidence.
- Processes that have been carried out (validation, verification, fraud risk assessment) and their outcomes.
- The data that can connect a specific person with the identity (the authenticator/s bound to the identity).
- Processes used to match a person to the authenticator (authentication).
- How the data combines to generate a degree of trust (assurance) at a number of steps (trusted evidence, trusted user, assured identity).

This guide provides the foundation and structure for an assessment, and how to communicate and act on the results of that assessment. It provides a starting point and structure for a full interoperability analysis upon which a certification, trustmark or interoperability audit could be based.

Undertaking the initial analysis of interoperability between trust frameworks or between identity levels begins with a granular assessment of each step along the horizontal axis in full detail. Alternatively, an assessment focused less on the inputs and processes, and instead on the outcome achieved at each step can be utilised. This is often associated with a more mature ecosystem with a range of recognised standards in place.

Granular Assessment Approaches

For assessing the interoperability of each step of proofing and authenticating an identity, a granular assessment will need to consider the comparability and compatibility of inputs, the checking processes undertaken, and the evidence generated at each step (including both the outputs and outcomes).

Questions may include:

- Are the inputs of similar strength or robustness?
- Do they operate with a comparable process, security or robustness of output?
- What is the relative success rate of the process, for example the proportion of successful versus unsuccessful or falsely matched results?
- Are the results compatible in how they are formatted and structured, valued, communicated and transmitted?

Outcome-based Assessment Approaches

An alternative method is to undertake an outcome-based assessment approach, focused on the outcomes achieved at each step, and the confidence one may have in the information provided (somewhat) regardless of the process used to get there.

This method particularly focuses on the steps where assurance is assessed, and how this is communicated in the evidence:

- Is the relative strength of the identity evidence used to create identities known – based on the type of organisation it was sourced from, and the application and delivery process, the security features present, and how hard it is to copy, amend or replicate the evidence?
- Is the range of claims presented by the evidence types the same in each trust framework?
- Given the processes used to validate, verify, authenticate and carry out fraud checks, are the relative success / failure rates and residual levels of risk known?
- Do the processes conform to recognised standards that set out the minimum level of successful operation, or (for example) process security?
- How are levels of assurance calculated, expressed and overseen?

Undertaking an outcome-based assessment between trust frameworks needs to consider how the outcomes are reached. Are processes (and the rules that govern them) based on similar requirements? Do they conform to comparable recognised standards?

For example, do the minimum matching rate requirements for a facial recognition process conform to similar minimum positive/negative matching rates in each trust framework?

If standards are not present or have not been conformed with, the relative process success rates may be demonstrated by testing, or by assessing its operation in practice. However, the more effective method is by comparing processes that conform to recognised and comparable standards, usually present in more mature markets.

For outcome-based assessments, comparing processes that conform to recognised standards provides the most efficient and trusted method of assessing interoperability.

Considerations for each Proofing and Authentication Step

For each step of proofing and authenticating an identity, assessing interoperability between two frameworks raises a number of considerations for practitioners to be mindful of. These considerations provide a starting point from which a fully detailed analysis specification could be developed. Figure 5 is included as an exemplar – a detailed set of considerations for each step is included in the appendix at the end of the guide.

FIGURE 5: Considerations for Assessing the Interoperability of 'Evidence and Claims'

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 and what relative strength is given to each? • What are the types of evidence called? 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, and 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?

Guidance on how to score and communicate the degree of interoperability, and what this means in practice for different parties, is included in Section 4.

B. IDENTITY LEVEL INTEROPERABILITY ASSESSMENT

As well as understanding the degree of interoperability between identity trust frameworks, interested parties frequently wish to know the degree of interoperability between the identity levels. Rather than assessing compatibility or alignment, this is focused on assessing if the identity levels are of equivalent 'strength'. In practice this includes:

- The extent of the claims or trusted information provided by the identity.
- The degree of confidence in the identity itself, and that it belongs to the person claiming it.
- The degree of risk mitigation this provides to a relying party.

This assessment can involve either an identity level set out in trust framework standards, or an identity for which the processes used to create it are known, but that does not conform to a recognised standard, such as some proprietary or self-sovereign identities.

CONSIDERATIONS
For assessing interoperability between proofing and authentication of different identity levels, considerations include: - Is the type of evidence used to create the identity in question, or the range of evidence types required by a standard in one trust framework equivalent to those in the second? - Are the claims from different types of identity evidence the same? - Are the means of validating and verifying evidence, assessing the degree of risk and the checks undertaken to achieve that of equivalent strength and reliability? - Are the authenticators and how they were recorded, stored and bound to the identity of a comparable strength to those required by another trust framework? - Is the means of authenticating the user of equivalent strength and reliability? - Is the level of strength or confidence in the trusted evidence, the trusted user and assured identity equivalent to that set out in another trust framework, or sufficient to mitigate a relying party's risks?

The same steps used in the interoperability assessment matrix for comparing trust frameworks are also used to create a structured approach to assessing two or more identity levels. However, the seven interoperability factors are not part of the identity level assessment matrix.

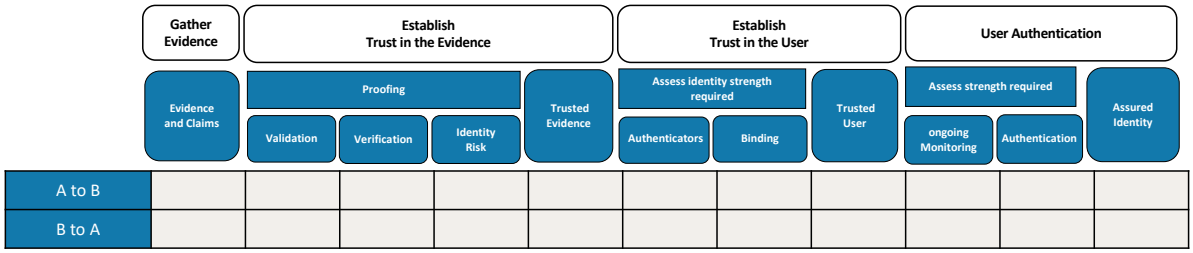
Bilateral or Multilateral Assessment

A comparative assessment of interoperability based on comparing identity levels can be undertaken in three different ways:

- A bilateral assessment of the comparative strength of identity levels across two trust frameworks.
- A multilateral assessment where three or more identity levels are compared against each other.
- A bilateral or multilateral assessment where identity levels are compared against a model standard.

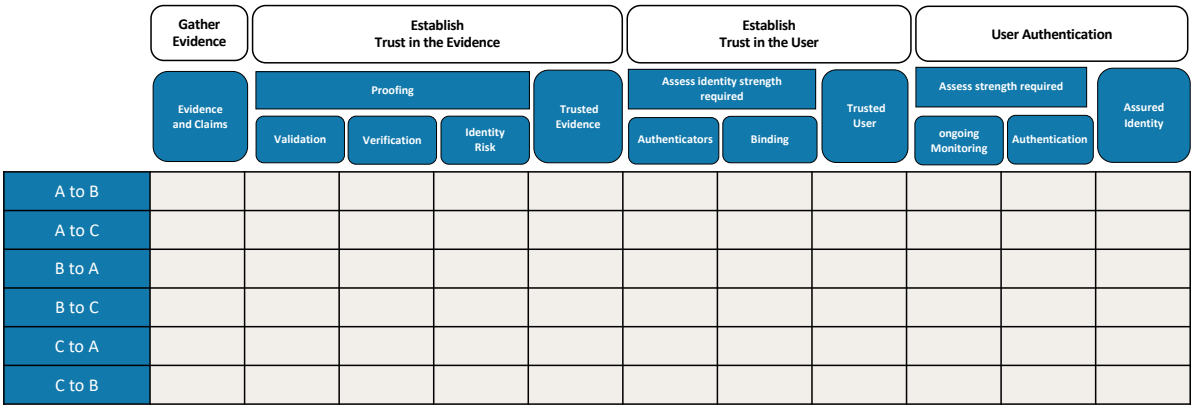
The identity level assessment matrix can be adapted to accommodate any of these assessment methods.

FIGURE 6: Bilateral (2-framework) Identity Level Assessment Matrix



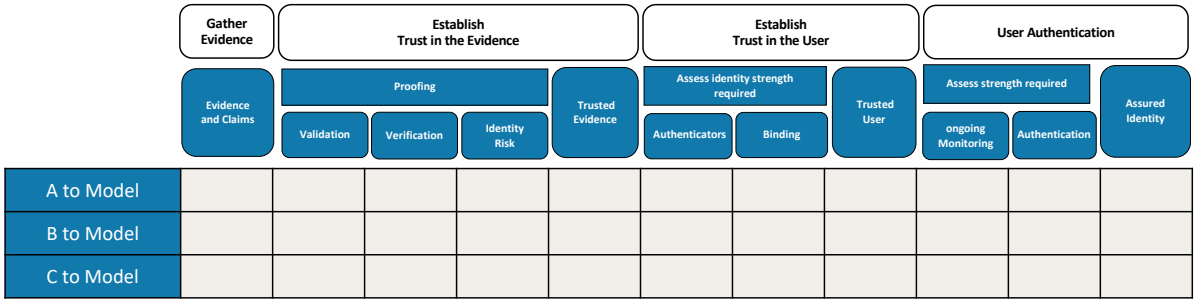
In a simple bilateral assessment, the relative strength of one identity level compared to another is reflected in an entry for each process step (set out across the horizontal axis of the table). In Figure 6, the upper row sets out the interoperability assessment results as to whether the identity level (proofing and authentication) from Framework A is stronger, weaker or equivalent to an identity level in Framework B. The lower row sets out the converse assessment result at each step, comparing Framework B to Framework A.

FIGURE 7: Multilateral (3-framework) Identity Level Assessment Matrix



The Multilateral Assessment Matrix, illustrated in Figure 6, is a simple extension to the bilateral example, with additional trust framework lines added. However, for an assessment involving a number of identity levels, this can become complex and cumbersome to use.

FIGURE 8: Multilateral (3-framework-to-model) Identity Level Assessment Matrix



More mature well-ordered markets (particularly those of processes or technologies of systemic importance) often feature a standard or model approach recognised by an international authority of some type.

Where this is present, the model standard is used as a common reference point for a multilateral interoperability assessment. This provides a more efficient assessment approach where a large number of comparisons need to be undertaken.

Outcome-based Identity Level Assessments

As well as granular identity level assessments, as with the comparison of trust frameworks, another method to undertake an efficient interoperability assessment is to use an outcome-based assessment, rather than a granular assessment of each individual step, input and checking process.

As with assessment against a common standard, an outcome-based identity level analysis is best undertaken where there are recognised standards and known success/failure rates for different processes. This enables a comparison of the relative success rates and degree of confidence that provides, rather than the component inputs and process detail.

- Can the resulting evidence be trusted to the same degree?
- Has it has been assessed to reach a comparatively strong level of assurance?
- Does it provide a required or comparable level of risk mitigation?
- Are the operational outcomes of the processes used within tolerance levels?

An outcome-based identity level assessment is therefore focused on fewer individual steps:

- The Evidence and Claims step, to ensure the required claims are present, and due to the fact some trust frameworks or standards require the use of one or more specific types of standard evidence
- The three steps where an assessment of assurance takes place – the Trusted Evidence, Trusted User, and Assured Identity steps.

In the absence of recognised standards, the relative degree of risk mitigation and strength of outcome associated with a particular checking process can be assessed via robust testing on a case-by-case basis. However, comparing outcomes that have been demonstrated and/or certified to conform to a known standard is a more efficient assessment method.

CONSIDERATIONS

In an outcome-based assessment, considerations include:

Evidence and Claims

- Does the evidence gathered to create the identity level conform to a standard of sufficient strength (e.g., a passport that conforms with the relevant ICAO standard)?
- Are the required claims present?
- Whether the security features included in the evidence are similarly robust.

Trusted Evidence

After validating and verifying the identity evidence and undertaking a fraud risk assessment:

- Is there is sufficiently strong likelihood that the identity evidence is not fake or invalidated in any way?
- Is there a sufficiently strong likelihood that the identity evidence is not being presented fraudulently and that the level of confidence associated with the claimed identity is sufficiently high?
- Is the assessed level of identity risk associated with the claimed identity sufficiently low?

Trusted User

Following the recording of authenticators and the binding of them to the claimed identity:

- Are the authenticators capable of providing accurate matches at a sufficiently high level?
- Is the risk of false matching sufficiently low given the authenticator type?
- Is the recorded authenticator sufficiently robust and secure to ensure it was not spoofed, adapted or replaced in any way?
- Has the authenticator been bound to the identity in a way that is sufficiently secure and resilient to interference or compromise?

Assured Identity

Given the factors above, and the outcome of the Trusted User step:

- Is the choice of authenticator sufficiently strong in terms of the confidence one may have in the result of the comparison to the person claiming the identity?
- Is there sufficiently high degree of confidence that the evidence originally used to proof the identity is still valid, and that its status has not changed since the last time it was checked?

4. COMMUNICATING THE LEVEL OF INTEROPERABILITY (AND HOW TO USE THAT INFORMATION)

Section Four Overview
Section Four provides guidance on an approach to scoring and communicating the degree of interoperability following an assessment between trust frameworks, and to compare the relative strength of two or more identity levels. It sets out key considerations for those seeking to assert the results of an interoperability assessment, and considerations for those seeking to act on this information.

In this section, the guide provides detailed guidance on the considerations surrounding the presentation of interoperability assessment results, both for cross-framework assessments, and for those between identity levels. Each of the two assessment methods require different scoring approaches, and both are set out in the guide.

The way that interoperability scores are set out must also be relevant to a range of parties, enabling them to gain insights into the degree of interoperability, including areas where interoperability is weaker, or stronger, and provide a stimulus for the various actions that can take place. The two assessment matrices set out in the previous section provide the structures needed to identify the specific areas of interoperability, and areas of strength and weakness.

The guide presents a range of potential actionable insights that can be identified via both assessment and scoring methods. It considers how the interoperability assessments can be utilised by authorities and standards setters, as well as trust framework operators and relying parties. It provides a detailed basis for considering if a trust framework aligns to another, and whether specific identities may be utilised, and with what degree of risk or type of intervention required.

A. RATING FRAMEWORK-TO-FRAMEWORK INTEROPERABILITY LEVELS

For an assessment of interoperability between two trust frameworks, the measure of interoperability needs to communicate the degree of alignment and compatibility between them. Drilling down further, this means in practice:

- The degree of intervention may be required to successfully exchange usable data between the trust frameworks.
- The likelihood of problems emerging due to the level of interoperability.
- The level of risk that parties may be exposing themselves to by proceeding to utilise the data without intervention.

The scoring method is based on the SPICE ('Software Process Improvement and Capability d'Etermination') model, which is adapted from its basic form to provide an interoperability score specifically relevant to assessing identity trust frameworks.[v]

Following the assessment of interoperability, the results are communicated via a 5-star scoring model. These results can be derived from a detailed analysis of the trust frameworks that follows the approach set out in this guide.

Framework-to-Framework Interoperability Scale:

* **Isolated**: total incapacity of interoperation.
** **Initial**: interoperability may require great efforts.
*** **Executable**: possibility of interoperability exists but the risk of proceeding with existing incompatibility is high.
**** **Connectable**: interoperability, differences exist but can be aligned.
***** **Interoperable**: enterprise-level interoperability, with low risk of encountering problems.

The SPICE-based 1-5 star interoperability scale for each category communicates the degree of intervention required to interoperate successfully between the two trust frameworks, the likelihood of problems emerging should intervention not take place, and level of risk concerned.

This approach is applied to each identity proofing and authentication step. The resulting score is set out in the Interoperability Assessment Matrix, with a single 1-5 star score being shown for each step, based on the assessment of inputs, processes and outcomes, and the evidence generated at each step.

FIGURE 9: Scores shown in the Interoperability Assessment Matrix: *

	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	**	***	***	**	***	***	**	***	***	**	**

** The scores indicated above are intended to be illustrative only.*

As with the interoperability assessment itself, different steps and interoperability factors may be more or less important, given the context under which the assessment is taking place, and weighted in line with this.

In the Interoperability Assessment Matrix set out in Figure 9 above, the syntactic and semantic interoperability factors have been highlighted as the primary interoperability factors concerning proofing and authentication, with secondary factors also displayed.

This may be adapted by practitioners based on the use case and assessment context.

Actionable Data
Parties in receipt of the results of an interoperability assessment between trust frameworks have a strong indicator of the degree of comparability and alignment for each individual step involved in proofing and authentication.

This provides the basis for further investigation into areas of particular weakness, where interoperability is scored at a low level. The acceptability of different scores can also be considered in light of the risk tolerance and appetite of the relying party, or against the expectations set out in local regulation or trust framework rules.

Given the indication of the compatibility of the two trust frameworks, and the likely level of intervention and residual risk involved in exchanging and utilising data between them, the interoperability scores become actionable for a variety of parties.

CONSIDERATIONS

For various recipients of an identity proofing and authentication interoperability assessment between two trust frameworks, a number of actions may be considered:

Relying Parties

- Could a minimum level of interoperability be set in order for identities from a given trust framework to be used, particularly for regulated or high-risk use cases?
- If the syntactic and semantic interoperability scores are low is there a standard against which the definitions and formatting could be mapped to help align them across the two trust frameworks?

Identity Providers and Brokers

- Can the data be normalised or harmonised to the requirements of the receiving trust framework prior to transmission and/or use?
- Can processes and outputs be aligned to recognised standards, particularly those utilised in other trust frameworks?

Standard setters

- Could the principles underpinning use of identity data be aligned different trust frameworks?
- Could the terms and definitions and syntax requirements be aligned across the trust frameworks?

Authorities

- Can the two trust frameworks successfully interoperate? Is the level of reliability and risk mitigation sufficient given any concerns regarding the degree of compatibility?
- Might additional requirements need to be put in place to reduce the residual risk involved in exchanging and utilising identity data between the trust frameworks before relying parties may be permitted to use it?

B. RATING THE EQUIVALENT STRENGTH OF IDENTITIES

Scoring an interoperability assessment carried out based on the strength of identity levels, seeks to communicate the degree of equivalency between the inputs, processes, outcomes and evidence generated in each case.

In practice, this means:

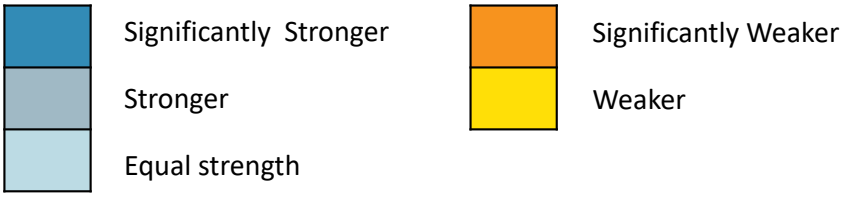
- Are the inputs, processes and (in particular) outcomes at each step equivalent?
- Do they provide an equivalent set of claims (attributes) and are the types of evidence assessed to be the same strength in each case?
- Do they provide the same degree of certainty regarding whether the person claiming the identity is its rightful owner?
- Do they mitigate risk to the same degree?

Assessing the interoperability of the proofing and authentication steps of different identity levels can be carried out in a granular manner encompassing inputs, processes and outcomes at each step. In a mature, standards-driven ecosystem this assessment may be carried out based solely on the outcomes achieved at the Evidence and Claims, Trusted Evidence, Trusted User and Assured Identity steps.

The results of an assessment must be able to convey equivalency, as well as any areas of comparative strength or weakness.

The scoring model set out below is based on a colour-coded 5-point scale. Practitioners may wish to set out further gradation of results based on their detailed assessment methodology.

Identity-to-Identity Interoperability Scale

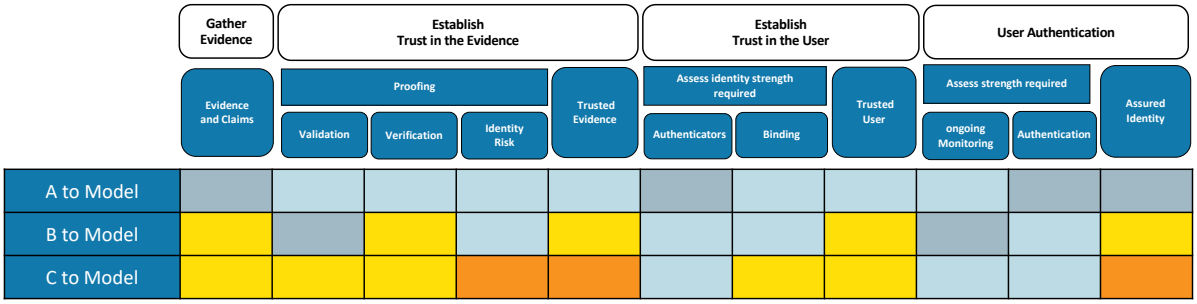


In the scale, the term ‘weaker’ or ‘stronger’ reflects the comparative strength of identity evidence and the range of attributes provided, the level of risk mitigation and the level of confidence in the accuracy of the data or outcome.

The 5-point equivalency scale provides a clear indication of relative strength, and therefore a quick way to review the results of an assessment, and to highlight areas of possible concern to be investigated, or action to be undertaken.

This can be applied whether comparing between two or more identity levels directly, or identity-to-model standard assessments. This is illustrated in Figure 10 via a three-identity-to-model comparative strength assessment.

FIGURE 10: Scores shown in an Identity Level Assessment Matrix: *



** The interoperability scores indicated above are intended to be illustrative only.*

Actionable Data

A score provides an indication of the detailed equivalency assessment carried out and indicates areas where the strength of two or more identity levels may differ, and therefore the areas that may require intervention to raise or lower the strength of an identity, or to better align identity level requirements between trust frameworks and their standards.

CONSIDERATIONS

Following an interoperability assessment, a number of actions may be considered:

Relying Parties

- If the assured identity is assessed to be of equivalent strength this is a positive indicator that it meets the same degree of risk mitigation as the compared identity or identity standard could it be used in across both trust frameworks?
- If the assured identity is of at least equivalent strength, are there more granular elements – individual steps – where the identity is assessed to be of weaker strength? Do these steps require further investigation?
- If the assessed level of interoperability is weak, can the identity be 'stepped up', for example by gathering additional, or stronger identity evidence, or undertaking additional checks?

Identity Providers

- If the identity is assessed to be weaker at some steps, does the owner of the claimed identity have additional evidence on file, or that can be gathered to step up the identity strength?
- Are additional, stronger processes or steps be used – for example to more confidently verify the data to the individual, or by utilising stronger form of authenticator or authentication process?
- If the identity is stronger than the required equivalent, are there data minimisation concerns?
- Can the identity being used be 'stepped down' to remain proportionate to the requirements of the relying party or receiving trust framework?

Standard setters and Framework Operators

- If assessed to be weaker, are there particular steps set out in scheme rules or standards in the originating trust framework that need to be amended, or upgraded in some way?
- Can the data underpinning the identity be augmented in some way to provide a 'bridge' to better align the two trust frameworks, for example by mandatory step ups, or process enhancements?

Authorities

- For authorities overseeing organisations participating in the receiving trust framework, if the identity or identity standard is of at least equivalent strength, is there sufficient confidence in this assessment to consider recognising the originating trust framework in some way?
- If the identity level is judged to be weaker, should it be considered incompatible for specific regulated use cases?

5. PUTTING THE APPROACH INTO PRACTICE

Section Five Overview

Section Five sets out a four-stage practical toolkit for applying the approach to interoperability assessment in practice.

- *Stage One provides an overview of how to select the most relevant interoperability factors, consider their weighing and score the assessment.*
- *Stage Two provides guidance on interpreting and acting on the results of an interoperability assessment between trust frameworks.*
- *Stage Three provides an overview of how to structure a comparative strength assessment between two or more identity levels.*
- *Stage Four provides guidance on interpreting and acting on the results of a comparative strength analysis between two identity levels.*

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.

** Note, this will require a set of detailed evaluation criteria for each cell based on the considerations set out in the Interoperability Guide.*

	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											

- **At cell level, the outcome will show the degree of interoperability for each step of identity proofing and authentication.**
- **It identifies specific areas where interoperability may require further alignment between the trust framework.**
- **Taken together, it presents a holistic view of the degree of compatibility between the approaches to identification set out in the two trust frameworks.**

Stage Two: Considering Interoperability Assessment Outcomes

The completed assessment matrix populated with the assessment score indicates:

1. The relative importance of each of the interoperability factors to identification proofing and authentication, depicted by the shading.
2. The degree of correlation between the approaches to identification within each trust framework. *
3. Low scores indicate areas of significant differences in the approaches to identification between the two trust frameworks: a low degree of alignment.
    - The steps at which there is a higher level of risk involved in exchanging and making use of data between the trust frameworks.
    - The steps where a higher degree of intervention is likely to be required to normalise data between the trust frameworks.
4. 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.
    - The steps at which there is a lower level of risk involved in exchanging and making use of data between the trust frameworks.
    - The steps where a lower degree of intervention is likely to be required to normalise data between the trust frameworks.

** Note. This needs to be balanced to take account of the relevant importance of each interoperability factor. How significant is a low degree of correlation for an inconsequential factor? Are the factors of primary importance given sufficient weighting?*

	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	**	***	***	**	***	***	**	***	***	**	**

- **Where there is a high degree of correlation, the comparative strength assessment of the identification steps can be performed – Stage 2.**
- **Where there is a low degree of correlation, is intervention needed to better align the trust frameworks, or is correlation achieved at a different step?**

Stage Three: Comparative Strength Assessment

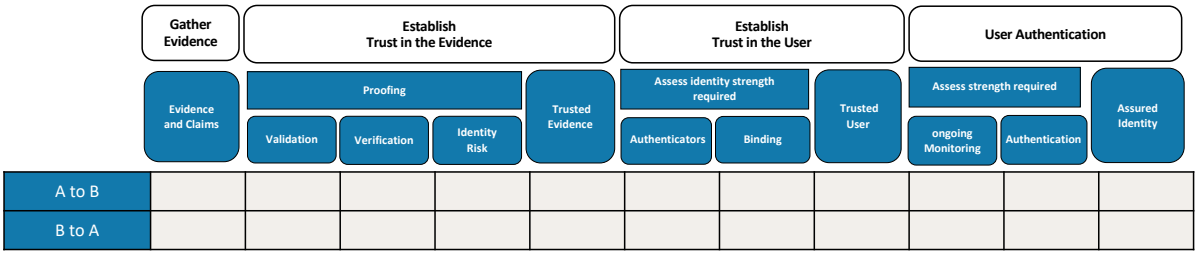
This is a detailed and technical assessment of each relevant step in identification set out in each of the two trust frameworks being compared, that will determine the degree of equivalence.

1. For each cell, analyse supporting material such as the policies, procedures, standards and specifications within the trust frameworks in question
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.

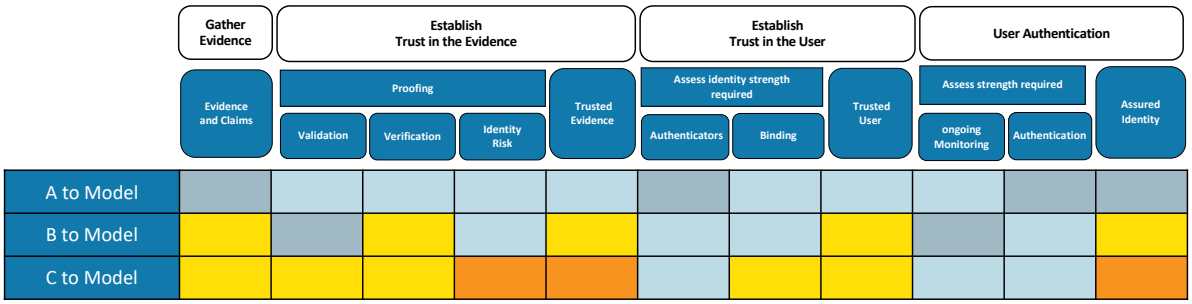
** Note, this will require a set of detailed evaluation criteria for each cell based on the considerations set out in the Interoperability Guide.*



- **The outcome will show the comparative strengths (and weaknesses) of the two trust frameworks, leading to a determination of equivalence for each step of identification.**

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 introduced to resolve this lack of equivalence.
    - 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 being used.



- **To reach this point, the degree of correlation of each of the primary and secondary (i.e., important) interoperability factors between the identity levels will have been determined.**
- **A high degree of correlation between interoperability factors does not indicate equivalence between each of the identification steps.**
- **Where there is a variance, this will need to be addressed.**
- **Baseline changes to identification within a trust framework may be necessary, or changes to the evidence or processes required for an identity, in order to deliver a comparative degree of risk mitigation.**

APPENDIX 1

Step-by-Step Considerations for Inter-Framework Interoperability Assessment
For each of the identity proofing and authentication steps, a series of considerations are set out to guide practitioners, based on the seven interoperability factors. These considerations are applicable to a bilateral assessment between two trust frameworks.

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 and what relative strength is given to each? • What are the types of evidence called? 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, and 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?

CONSIDERATIONS Step 2. Validation	
Technical	• Are the security features included in different evidence types comparable in terms of their resilience to tampering, or similar levels of protection from fraudulent reproduction of evidence? • Are technical processes to confirm the validity of evidence and the requirements for the success and failure rates of these checks comparable?
Syntactic	• How are validity checking results included in the evidence package? • What is the format of validity metadata, and how is this categorised? • What standards are used to order the transmitted validity data?
Semantic	• Is there a correlation between the way or ways that validity is defined, and the terms used to describe its various aspects? • How are the checks used to determine validity described and named?
Organisational	• Are the intended purposes of undertaking validity checks the same or comparable? • Are the organisational roles different parties may take in a validation exercise, understood in a consistent and comparable way? • Are the ways that non-valid evidence is acted upon comparable?
Legal	• Are there legal obligations or restrictions regarding how validity of identity evidence is checked or how that data is used? • If so, are they comparable?
Governance	• Are validation processes comparably well-governed in terms of their resilience to influence or compromise, and the degree of risk involved in using them? • Are the validation processes subject to audit or certification or similar by the trust framework operators?
User	• Do the validation checks require information (for example privacy notices) to be provided to the user? • Is a user's consent required and is it recorded, and by who? • How are these obligations expressed?

CONSIDERATIONS Step 3. Verification	
Technical	• Are the verification methods used comparable? For example, the mix or knowledge, possession or inherence-based factors? • Are there technical requirements for the type of verification processes permissible, or key features they must include, or how many factors should form part of the verification? • How is the verification process outcome specified and included in the metadata or evidence packet? Does this conform to common or recognised standards?
Syntactic	• In each framework how is the verification process outcome data formatted, categorised, packaged and/or encrypted?
Semantic	• Are verification and different verification factors defined in the same way? • Is there a correlation or sufficiently aligned range of terms and definitions and how they are set out? • How is the degree of confidence the verification process provides that the user is the rightful owner of the identity evidence scored and how is this described?
Organisational	• Are there principles set out concerning verification, and are they compatible? • Is the process of verification carried out for the same purpose in each trust framework? • Are the roles of the various parties involved in verifying identity evidence comparable?
Legal	• Are there any legal obligations or restrictions that may impact on verification, how it is undertaken, who by, and whether and how it is shared across trust frameworks and national borders? • How do these issues correlate across the two trust framework jurisdictions?
Governance	• What service level or performance expectations are tested and how? • How do the expectations compare?
User	• How do the user experience expectations with regard to verification compare? • How is inclusion addressed in terms of the options users have to verify themselves? • Are the processes presented to the user in a comparable way, and via a similar range of channels and devices?

CONSIDERATIONS Step 4. Identity Risk	
Technical	• Are registries and trusted sources of risk data comparable in terms of the underlying technical architecture, the types of source organisations, and the functionality of the data interface used? • When comparing data sources, is the population coverage of similar quality and quantity? • Are algorithms used to assess the level of risk comparable in the way they identify potential risk?
Syntactic	• Is the level and type of potential identity risks described in the evidence and metadata in a similar format? • Are data types and values formatted and communicated according to common or recognised standards?
Semantic	• How are different types of identity risks categorised and defined? • Do they correlate? • Is the level or degree of risk described in a comparable manner?
Organisational	• How are the impacts of risk on different parties categorised and communicated to wider stakeholders? • Is risk assessment carried out for the same reasons and with comparable objectives?
Legal	• What is the legal basis and requirements for customer due diligence – is it risk- or standards-based?
Governance	• Is the level of potential risk calculated involving similar means of oversight? • Are algorithmic and automated processes calibrated and assured by an independent third party? • Is there guidance available on comparable instruction and level of detail and sophistication? Do the standards align?
User	• Are comparable safeguards in place to prevent the communication of risk factors to users?

CONSIDERATIONS Step 5. Trusted Evidence	
Technical	• How do the methods or calculations used to assess and weight the strength of the component elements of trusted evidence compare? • Via what technical process is metadata recorded to describe the trusted evidence package? • Are similar standards applied to the assessment of trust in the evidence?
Syntactic	• How are the results of the previous steps and the combined assessment of the evidence generated at each of the previous steps set out, formatted and packaged? • Are the data forms used to describe this comparable?
Semantic	• What terms and definitions are used to describe the combined level of strength or trust in the evidence? • How do the levels of trust, and their hierarchical strength communicated or scored, compare? • Is the guidance provided to the various parties on the subject similar or aligned?
Organisational	• In assessing the level of trust in the evidence, its ownership and validity, are the same goals being worked towards? • How is the level of trust understood with regard to its relationship with the level of organisational risk?
Legal	• Is the regulatory standing of the standards, the rules or methods used to assess or score the level of trust in the evidence and its validation and verification, comparable? • Are there obligations on relying parties, identity providers or other parties involved in the trust framework to provide, record or vouch for the trust in the identity evidence comparable?
Governance	• How is the overall assessment of trust in identity evidence, its validation, verification (and the level of identity risk) overseen? • By what type of organisation or mechanism – are they similar, and comparably robust? • What are the liability arrangements for problems emerging, and for which parties?
User	• Is the user able to know, store or choose to assert the specific data regarding the degree of trust assessed for the identity evidence they have presented, and the assessed level of risk associated with the identity? • How is user consent obtained and stored if this data is to be shared? • Via what channel or device is the user able to do this, and are the user experience expectations comparable?

CONSIDERATIONS Step 6. Authenticators	
Technical	• How is the authenticator data stored and transmitted? • Do the authenticators conform to recognised standards? • By what process were they collected and stored? • What security does the process of recording the authenticator data rely on? • What comparable margin of error is involved in the authenticator recording/replicating processes?
Syntactic	• How is the authenticator data expressed in the different evidence types? • How does the framework require the authenticator data to be formatted, and is this consistent with the requirements of the second framework?
Semantic	• Are the range of types of authenticators named and described in the same way? • On what type of scale is the strength of the authenticator measured? • Are the hierarchical strengths given to different authenticators comparable between the trust frameworks?
Organisational	• Has the authenticator been collected for the same purpose or intended use? • Is there consumer or trust framework participant protection based on the use of the authenticator and is it comparable?
Legal	• Is the data protection regime equivalent, in terms of protecting the individual, and the processor of data? • Is the use of the authenticator permissible under law? • Are there legal restrictions regarding how personal (e.g., biometric data) is recorded and stored?
Governance	• How was the collection of the authenticator and its authenticity assured, and by who? • Has the collection and strength of the authenticator assessed or certified? If so, how and by what organisation? Can the authenticator collection process be audited?
User	• Does the trust framework have a similar means for a user to supply the authenticator data, if it is not derived directly from identity evidence? • Is the user given a choice of which authenticator to provide and use? • How is inclusion ensured in the provision of authenticators? • Via what processes, channels and devices is this possible? • Is the user experience comparable?

CONSIDERATIONS Step 7. Binding	
Technical	• How do the technical binding processes compare? For example, are they both cryptographic in nature? • Are there standards relating to the binding processes used? • How do the various binding methods allowed within the trust framework compare in terms of their security and strength?
Syntactic	• How is the data concerning evidence of the type or strength of the binding process and who undertook the process formatted and packaged?
Semantic	• How are different binding processes named and described? • How are they grouped or characterised within the trust frameworks?
Organisational	• Is binding undertaken for a comparable purpose or objective? • Are the risks concerning the binding processes understood in the same terms, and impact on the parties involved?
Legal	• Are there legal requirements or restrictions regarding the encryption of personal data, who can undertake this, and the auditability of the data by authorities?
Governance	• How is the binding process overseen, and by who within each trust framework? • If the data is auditable, under what process or arrangement?
User	*(Note: the User is not involved in the binding process directly)*

CONSIDERATIONS Step 8. Trusted User	
Technical	• How do the methods or calculations used to combine the trusted evidence with the strength of authenticator and binding to create a level of assurance regarding the 'trusted user', compare between frameworks? • To what extent are the different elements weighted in a comparable or aligned way?
Syntactic	• Is the combined data bringing together the trusted evidence with the strength of authenticator and its binding expressed in a comparable or compatible manner? • Is it the formatting and categorisation aligned? • Does the data conform to common or recognised standards?
Semantic	• How does the measure of strength of confidence or trust expressed by the evidence and metadata at this step compare? • How is strength or assurance described and defined? • Is the guidance in each trust framework aligned?
Organisational	• Is the bringing together of trusted evidence and authenticator data undertaken for a comparable reason? • Are use cases comparable between the trust frameworks? • Are the principles concerning how Trusted User data is assessed and used compatible?
Legal	• Is there a legal or regulatory recognition, or requirements and obligations, concerning Trusted User data? • Are liability, data protection legislation, consent obligations and security requirements aligned?
Governance	• Is the assessment of the level of confidence or assurance in the Trusted User overseen and, if so, by a comparable type of organisation? • Is a comparable standard or trust mechanism such as trustmark, certification or attestation for the parties involved in the assessment of Trusted User data? And for the processes they perform?
User	• How is the level of assurance associated with a Trusted User's identity communicated to them? • Is the user able to store and/or assert the Trusted User data in a comparable way? • Are similar consumer-facing messages projected concerning how and for what use cases their Trusted User data may be asserted?

CONSIDERATIONS Step 9. Monitor Risk	
Technical	• Are registries and trusted sources of data to check the validity of identity evidence of a similar technical model? • Are processes used to check and update the user's identity risk data comparable at the point of use? • Is the quality and quantity of the data coverage similar?
Syntactic	• Is the data concerning the re-validation of identity evidence and other fraud monitoring checks formatted in an aligned way? • Are data types and values formatted and communicated according to common or recognised standards?
Semantic	• How are different types of risk and validity checks and monitoring procedures categorised and defined? Does it correlate across the two trust frameworks? • Are the data and processes described in a consistent manner?
Organisational	• How are the impacts of finding indicators of non-valid evidence similar, what actions are required, by whom, and are they comparable? • Is risk monitored, and evidence and checks revalidated for the same reasons, and with comparable objectives?
Legal	• What is the legal basis and requirements for customer due diligence – is it risk- or standards-based? • Are digital identity standards or specific trust frameworks legally recognised? • Is there a correlation between the levels of assurance and confidence in a Trusted User for comparable use cases? Are these levels recognised in a similar way and by a similar type of organisation?
Governance	• Are risk monitoring and revalidation processes calibrated and assured by an independent third party? • Are common or recognised standards conformed to, and do they align?
User	• Does the revalidation of identity evidence and ongoing monitoring of risk factors require user input, or consent? • Is the user experience similar?

CONSIDERATIONS Step 10. Authentication	
Technical	• Is there a correlation in the range of authentication methods and how they are carried out? • How do the tolerances for mistakes and relative success rates compare?
Syntactic	• How is the data resulting from an authentication check set out and formatted? Does it differ between frameworks? • Is this data encrypted, and in what form? • How much confirmatory data is required by the relying parties in each trust framework?
Semantic	• Are the various types of authentication checks known by comparable names, are they defined and described in the same or similar way? • How are the results considered in terms of their relative strength, or the factors that are considered to set them apart?
Organisational	• Is this step undertaken for a comparable and aligned purpose? • Are the roles of different parties understood and consistent? • Who undertakes the authentication, and under what arrangement is it relied upon?
Legal	• Are there regulatory requirements regarding the type, strength and frequency that authentication is required to be carried out, and how this is balanced against the level of assurance of the trusted user? • Is an authentication allowed to persist under law, or must it be carried out at every use? • Are there data protection or privacy laws relevant, and how do they compare?
Governance	• How are the results of authentication overseen? • Is this carried out in a comparable way, and by an equivalent type of organisation?
User	• What is the range of devices and channels able to be used by a user to authenticate themselves? • Are users given comparable means to address failed authentication attempts? • How is inclusion in how authentication is undertaken ensured? • What are the comparable user experience expectations?

CONSIDERATIONS Step 11. Assured Identity	
Technical	• Does the assured identity conform to common or recognised standards, and how do they compare? • Via what technology and data exchange process is the data transferred, and is this compatible between the trust frameworks?
Syntactic	• How is the combined data from the proofing and authentication processes structured and formatted? • Does it conform to common or recognised standards, and to what extent do they align?
Semantic	• How is the proofing and authentication data and the combined level of assurance or degree of trust defined, and are comparable terms used to describe the strength of the identity?
Organisational	• Are use cases and the intended purpose of sharing an assured identity comparable? • Is the risk associated with different use cases comparable across similar uses and types of organisation? • Are the principles regarding the use of an assured identity aligned across the trust frameworks?
Legal	• How do any legal or regulatory requirements regarding the strength of an assured identity compare? • Are there specific regulated use cases set out in local legislation or regulation? Are they aligned?
Governance	• To what extent are liability arrangements and dispute mechanisms in place, and the requirements, processes and outcomes for the various parties involved similar or aligned? • Is there a trustmark, certification or oversight regime, who operates it, and is the level of oversight comparable?
User	• What consumer protection is in place, how is it communicated, and is this aligned? • Is the user experience comparable? • How does a user raise any problems with the identification process, and how are these addressed from the user's perspective – to what extent is this comparable across trust frameworks? • What level of consumer support is available?

[i] https://openidentityexchange.org/guide-trust-frameworks-interoperability
[ii] https://www.edsurge.com/news/2019-11-12-data-interoperability-provides-a-path-toward-equity-4-lessons-learned

[iii] https://ec.europa.eu/isa2/eif_en

[iv] https://openidentityexchange.org/networks/87/item.html?id=55

[v] http://ceur-ws.org/Vol-1182/paper9.pdf