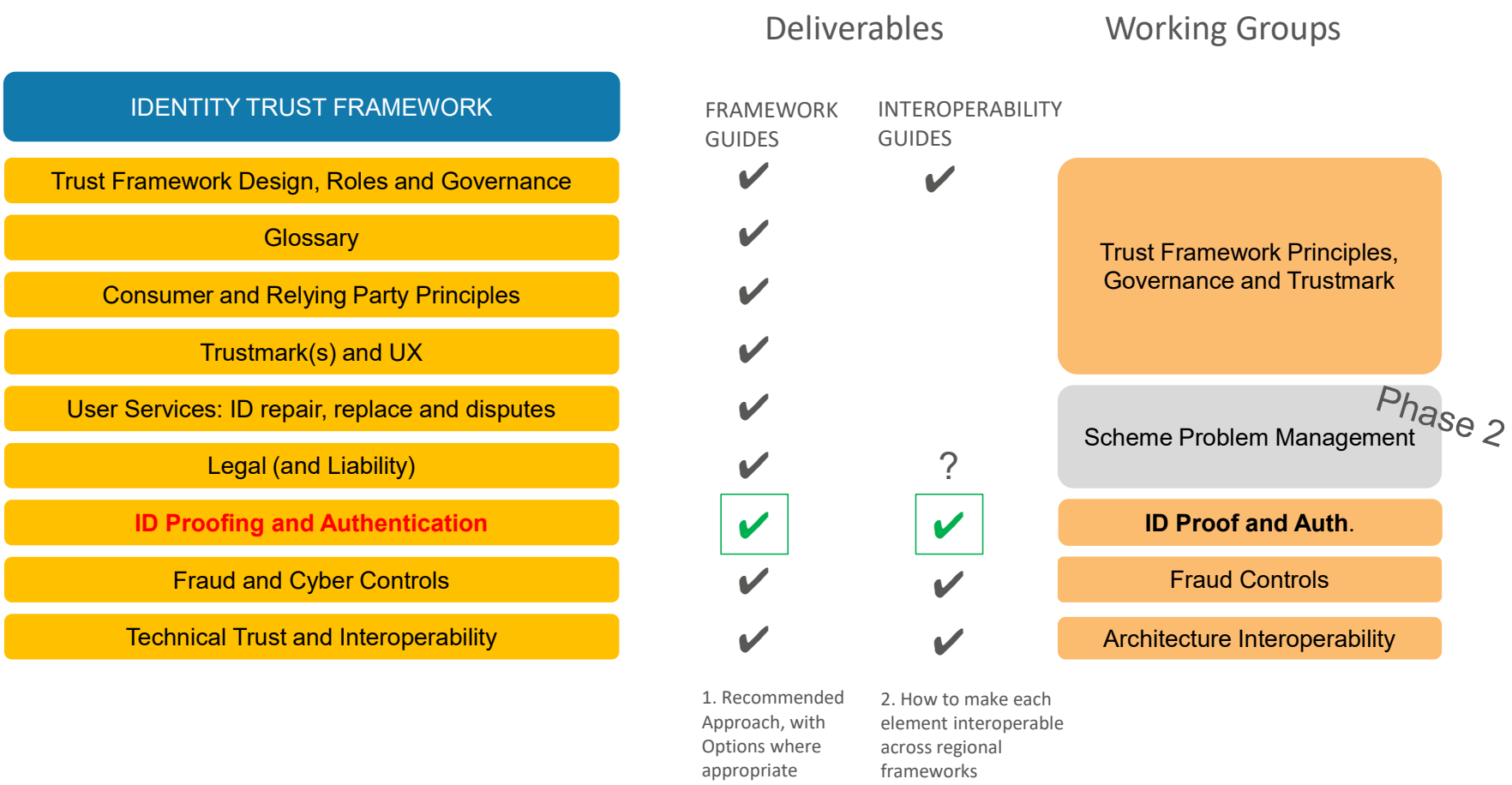
OIX Trust Framework Guide

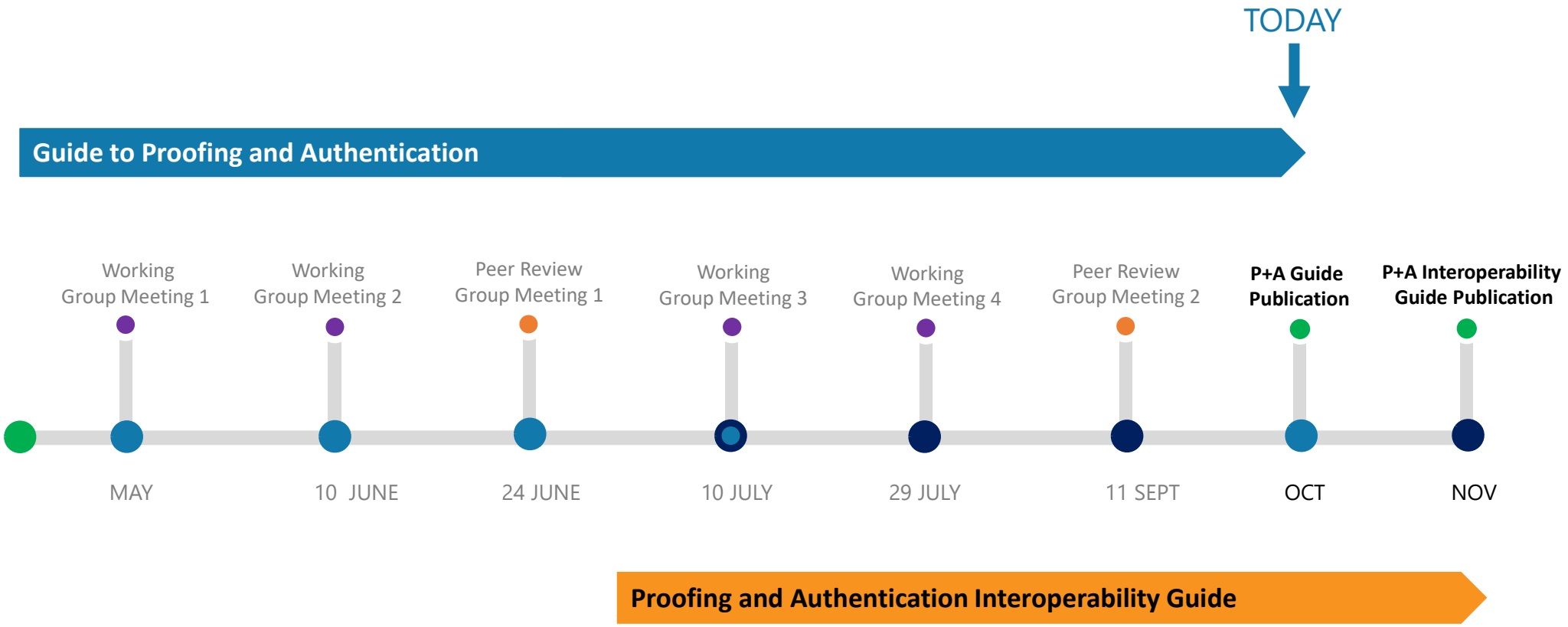
Identity Proofing and Authentication

Thursday 15 October 2020

The OIX Trust Framework Guides



Timeline

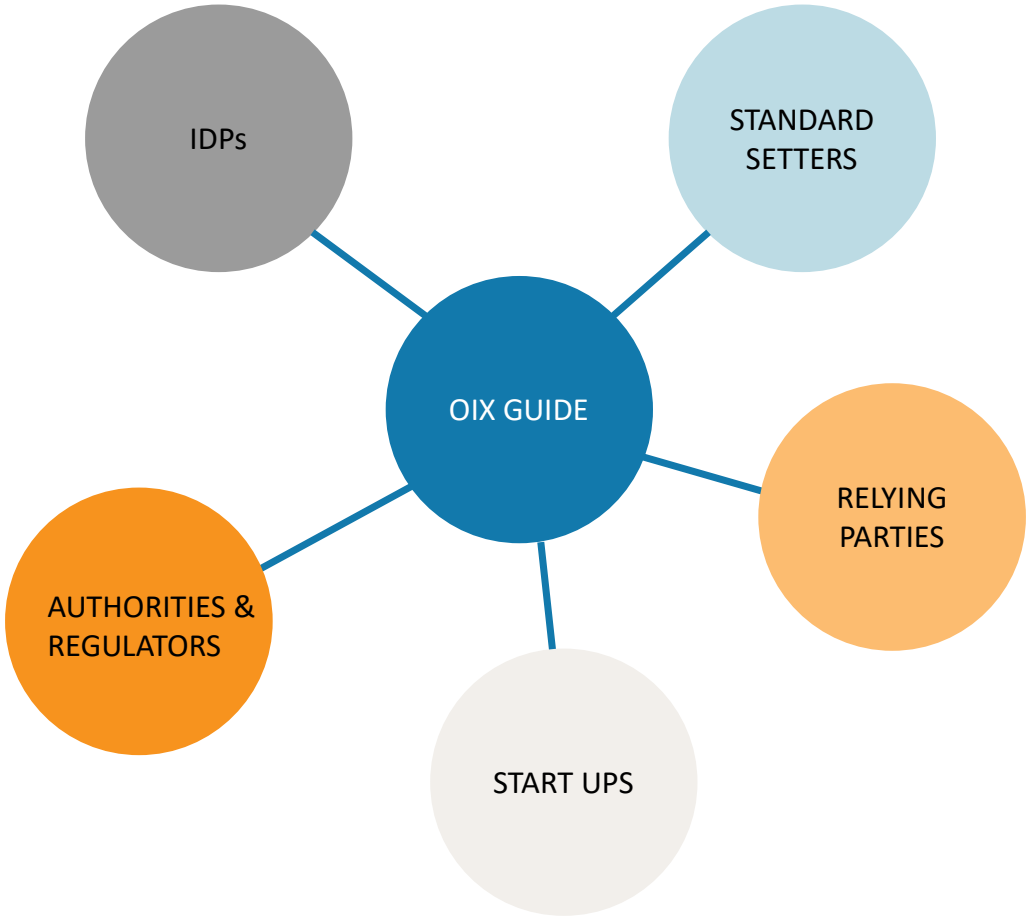

TODAY
Guide to Proofing and Authentication
Working Group Meeting 1
Working Group Meeting 2
Peer Review Group Meeting 1
Working Group Meeting 3
Working Group Meeting 4
Peer Review Group Meeting 2
P+A Guide Publication
P+A Interoperability Guide Publication
MAY
10 JUNE
24 JUNE
10 JULY
29 JULY
11 SEPT
OCT
NOV
Proofing and Authentication Interoperability Guide

Objectives

Define and publish a high-level structured approach to both identity proofing and authentication through analysis of the ways this has been done across different regional trust frameworks.

Define how this structured approach will allow interoperability to be assessed between trust frameworks.

Audiences



Audience

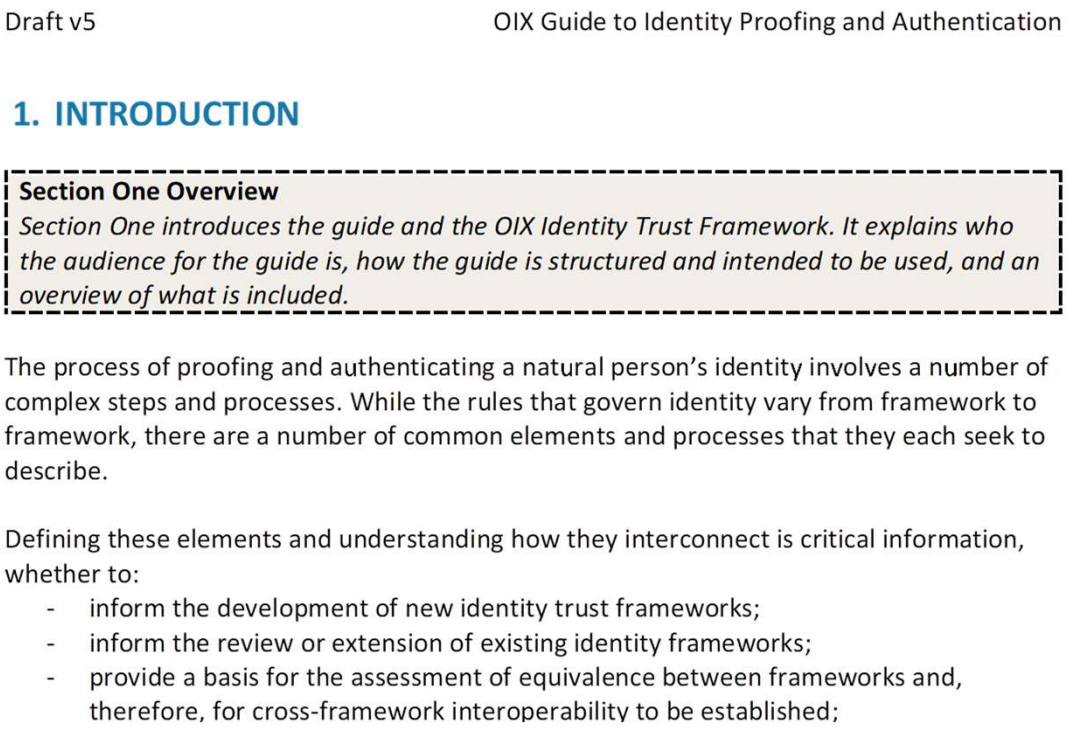
- Diverse potential audiences
- Some specialist, many not
- The Guide does not presume identity or technical expertise

The guide is relevant to anyone considering or actively involved in the creation and ongoing development of a digital identity framework, and specifically for those tasked with developing standards or guidance for identity proofing and authentication.

Challenges

1. To be relevant to all trust frameworks and national circumstances.
2. To be agnostic of solution type, whether proprietary, federated or self-sovereign.
3. To cater for a wide range of audiences – from lay to expert.
4. To be informative and practical – could we make a guide ‘actionable’?
5. To co-ordinate across multiple working groups and areas of focus.
6. To provide an underlying structure and approach to interoperability assessment.

Guide Presentation



Draft v5 OIX Guide to Identity Proofing and Authentication

1. INTRODUCTION

Section One Overview
Section One introduces the guide and the OIX Identity Trust Framework. It explains who the audience for the guide is, how the guide is structured and intended to be used, and an overview of what is included.

The process of proofing and authenticating a natural person's identity involves a number of complex steps and processes. While the rules that govern identity vary from framework to framework, there are a number of common elements and processes that they each seek to describe.

Defining these elements and understanding how they interconnect is critical information, whether to:

- inform the development of new identity trust frameworks;
- inform the review or extension of existing identity frameworks;
- provide a basis for the assessment of equivalence between frameworks and, therefore, for cross-framework interoperability to be established;

Style and Format

- Demystify proofing and authentication
- Provide an end-to-end structure that is adaptable to a range of architectures and frameworks
- Identify generic, underlying steps, a logical flow
- Present a hierarchy of content - accessible introductions leading to increasing technical detail

Guide Presentation

When combined, the evidence creates a level of confidence, expressed as a degree of assurance in the identity.

CONSIDERATIONS
Before considering the processes that make up identity proofing in more detail, a relying party would be expected to have performed a risk analysis and determined: - the degree of risk if a person they are transacting with is not who they say they are, and - the degree of confidence or strength of identity that will be required to sufficiently mitigate that risk. The second point may be determined by a regulator or other competent authority, set out within a ***trust framework***, or decided by the relying party themselves.

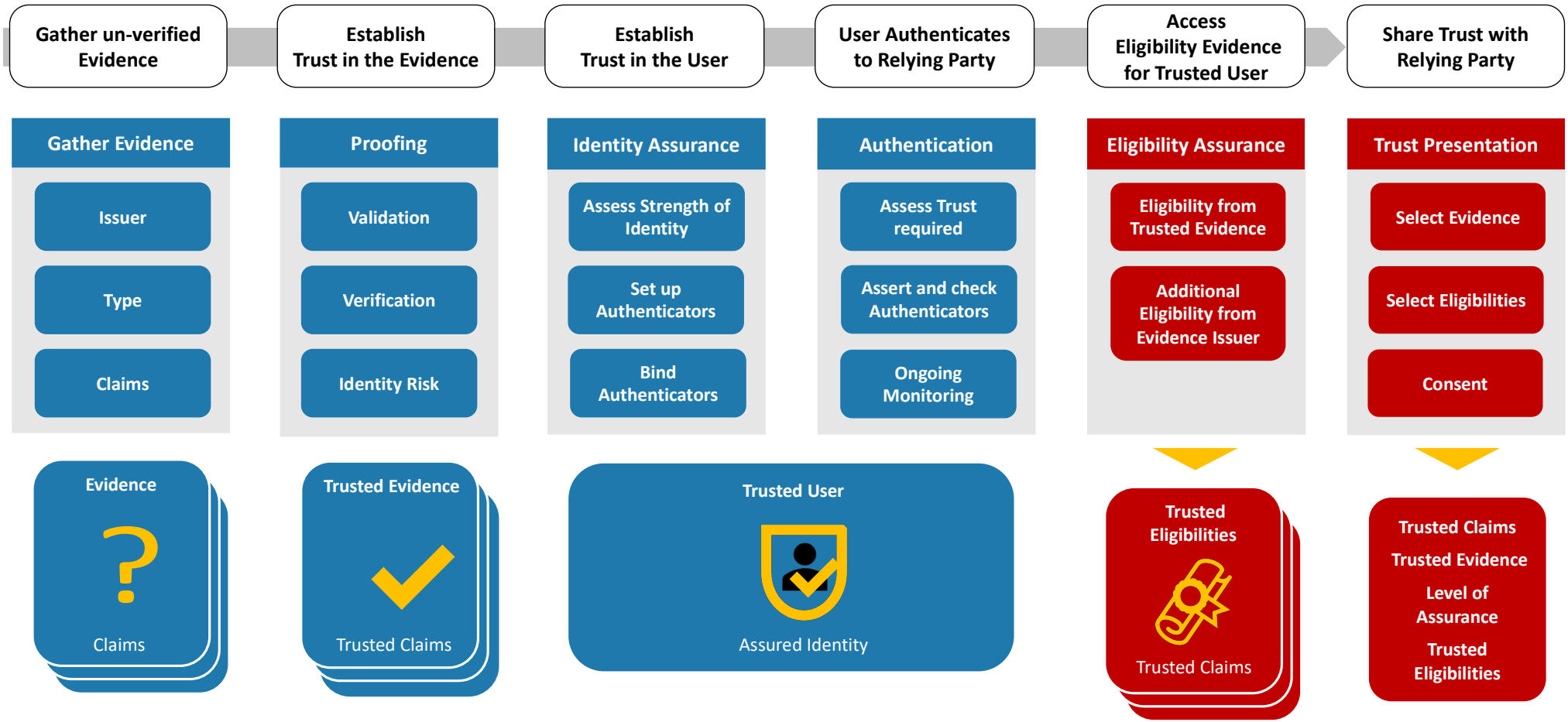
A. IDENTITY EVIDENCE

The first step in an identity proofing process involves gathering evidence of the identity being claimed. Evidence may be physical, a digital representation of a physical piece of evidence, or digital by design. The person may present it themselves or it may be extracted from a trusted database.

Style and Format

- 'Considerations' – user-centric challenges and questions to consider
- Links to other OIX Guides, particularly the Glossary

Proofing and Authentication



Proofing and Authentication

IN OR OUT OF SEQUENCE?

The illustrated process may suggest a linear, stepped process (l-r). In many cases, this will be the case. However, it is vital to note that some identity approaches do not use all of the steps set out in the diagram above. It may be the case that there is a break between steps, most typically between the binding of authenticators and the subsequent authentication of the individual when they later seek to assert their assured identity.

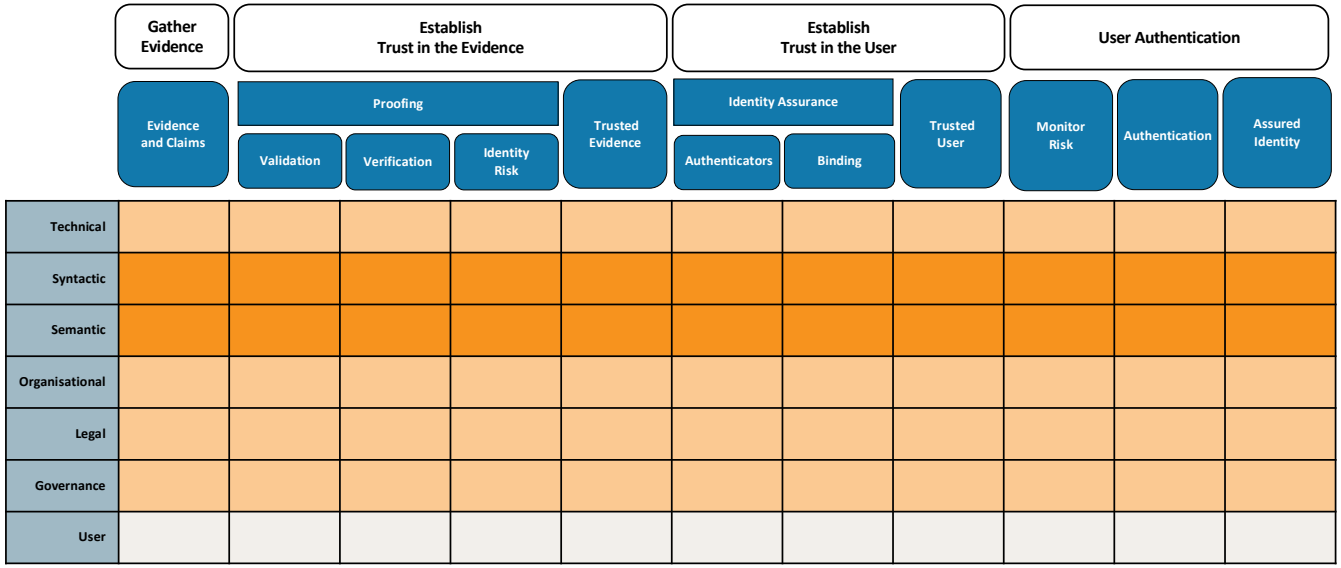
Self-sovereign journeys may start with authentication, but subsequently return to proofing, for example to step up the level of trust or the range of claims they are able to provide to a relying party. There are occasions where steps are repeated, such as the re-validation of evidence used to create the identity, or to monitor ongoing risk indicators.

However, while specific journeys and sequencing may differ in practice, the fundamental building blocks remain consistent.

Proofing and Authentication - a structured approach

THE STEPS PROVIDE…

- An underlying structure to help define and explain identity proofing and authentication
- A structure for the guide
- A structural underpinning for the interoperability assessment matrix



Guide Contents

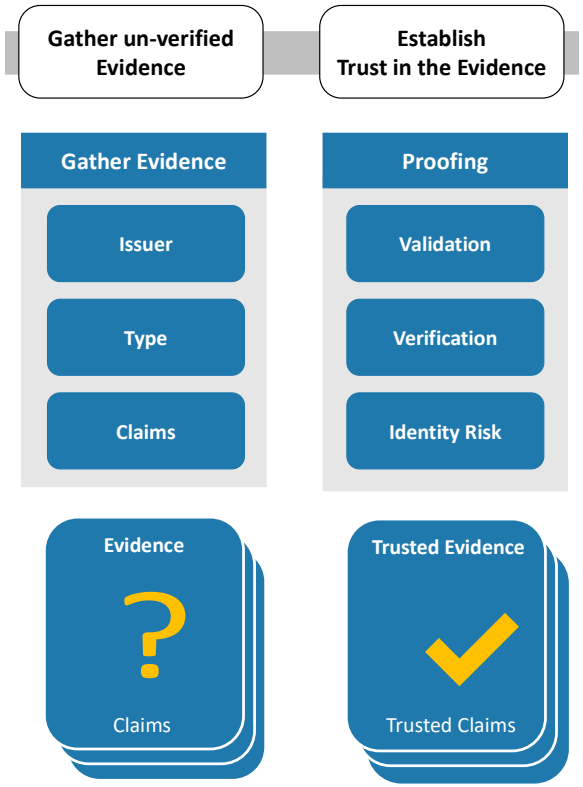
Guide Contents: Establishing a person's identity

INTRODUCTION

ESTABLISHING A PERSON'S IDENTITY

- Official vs social identity vs personas
- Defines digital vs other forms of identity
- Explains the range of use cases, and how they differ (risk/assurance and claims)
- Entitlements vs authorisations
- Introduces the end to end diagram and the various steps involved
- Introduces Proofing and Authentication as concepts – what they are and what they do
- Introduces calculating a level of assurance – how and why

Guide Contents: Identity proofing



IDENTITY PROOFING

A. Identity evidence

- Attributes provided by identity evidence
- Assessing the strength of identity evidence
- Non-standard evidence

B. Validation

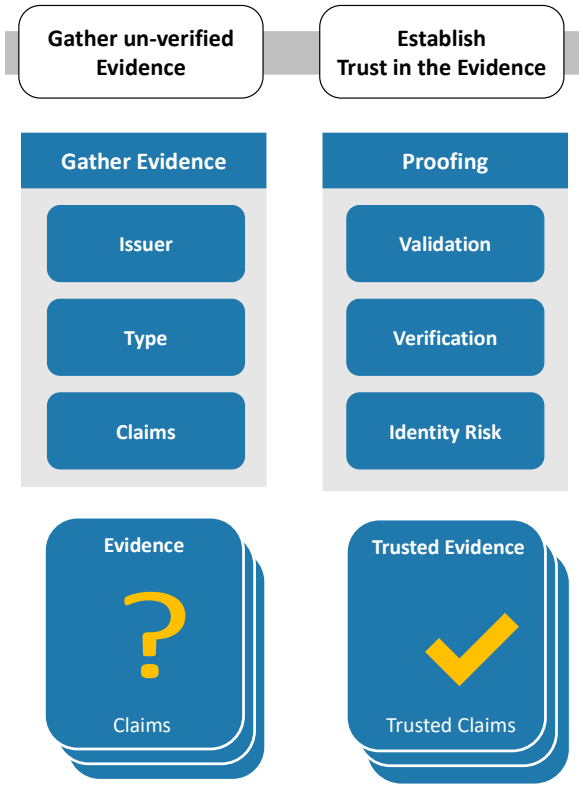
- In person vs remote validation techniques
- Checking with authoritative sources

Guide Contents: Identity proofing

CONSIDERATIONS
When gathering Identity evidence, there are a number of considerations: - How many pieces of identity evidence are presented? - What are the sources of evidence? Are they from an authoritative source? - What are the attributes they provide? Is the personal information consistent between separate pieces of evidence? - How 'strong' is the evidence? What types of checks were undertaken by the issuer of the evidence, and what security features does the evidence contain?

CONSIDERATIONS
When checking the validity of identity evidence, considerations include: - Whether physical or digital evidence, is it original? Is it a certified scan or copy? - Are the features expected to be there present? Are there any mistakes, or other anomalies? - Is the information presented consistent within the piece of evidence? - Can the evidence be matched against the record held by an authoritative source, or by the issuer of the evidence? - Can it be demonstrated that the security features are correct, and have not been tampered with? - Have the validation checks been carried out in a controlled environment and/or by appropriately trained staff?

Guide Contents: Identity proofing



C. Verification

- Knowledge–based verification techniques
- Possession-based verification
- Biometric verification
- Facial matching techniques

D. Identity fraud risk (assessment and mitigation)

- Explains contra-indicators
- When to check for identity fraud risk
- What happens when indicators are present

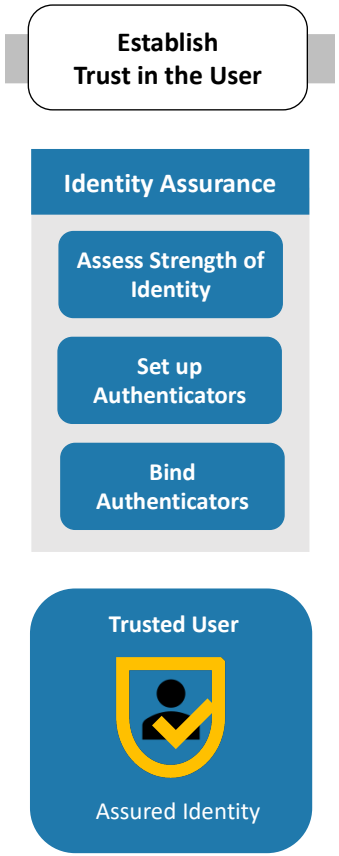
Guide Contents: Identity proofing

CONSIDERATIONS
When verifying a claimed identity, considerations include: - Is a knowledge-based challenge, or biometric verification either using photo-matching or another biometric factor, most appropriate? - If using knowledge-based verification, do the *challenges* involve static information, or more dynamic content? - What is the likelihood that the information being asked for could be known by someone other than the rightful owner of the identity? Is it publicly available? - Who has supplied the information involved in the challenge – was it a regulated or statutory body, or otherwise trusted source? Is the organisation independent from your own organisation? - If verifying the identity using biometric information contained in the evidence, what type of biometric information is present? - If photo-matching by person, is this being done by an appropriately trained person under controlled conditions? - Is the person claiming the identity present, or being matched remotely? - Are methods being used to ensure that the image of the person claiming the identity is not pre-recorded, re-used or tampered with? - If verification involves other biometric information such as fingerprints, is the biometric from strong identity evidence? - Are the likely number of false matches and non-matches of the technique being used to match the records known? - Are controls used to ensure that the person claiming the identity is not trying to *spoof* the test? Is there a *liveness test* being employed? - How effective and inclusive are algorithms that carry out remote visual checks? - What happens if a remote automated visual check does not provide a match?

Guide Contents: Identity proofing

CONSIDERATIONS
When checking an identity for potential fraud, considerations may include: - Has the evidence used to establish the identity been reported as lost, stolen or previously used in a fraudulent way? - Is there a lack of expected records and historical evidence that could indicate that the identity may be synthetic? (*note many SSI solutions may share no activity history by design, to ensure user privacy)* - Have fraud checks been made with authoritative and independent sources? - Is the individual likely to be at higher risk of being impersonated, such as politically exposed or high-profile persons? - Is the user in the expected geo-location (country or region)?

Guide Contents: Authenticators

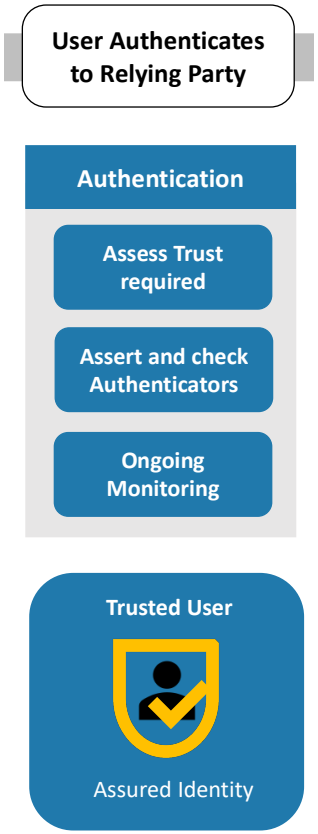


AUTHENTICATORS

- Provides examples of authenticators
- Describes the different categories of authenticator
- Explains binding process, and why it is important
- Describes 'credentials' and why this might be confusing!

Possession: Something the person has in their possession, such as a token or device (for example a smart phone).
Inherence: Something unique about the person themselves, such as a biometric (for example their fingerprint).
Knowledge: Something the person knows, such as a secret (for example a password or PIN number).
Context: Information concerning where the person is, how they have transacted, what they are doing or have done (risk-based authenticators)

Guide Contents: Identity Authentication



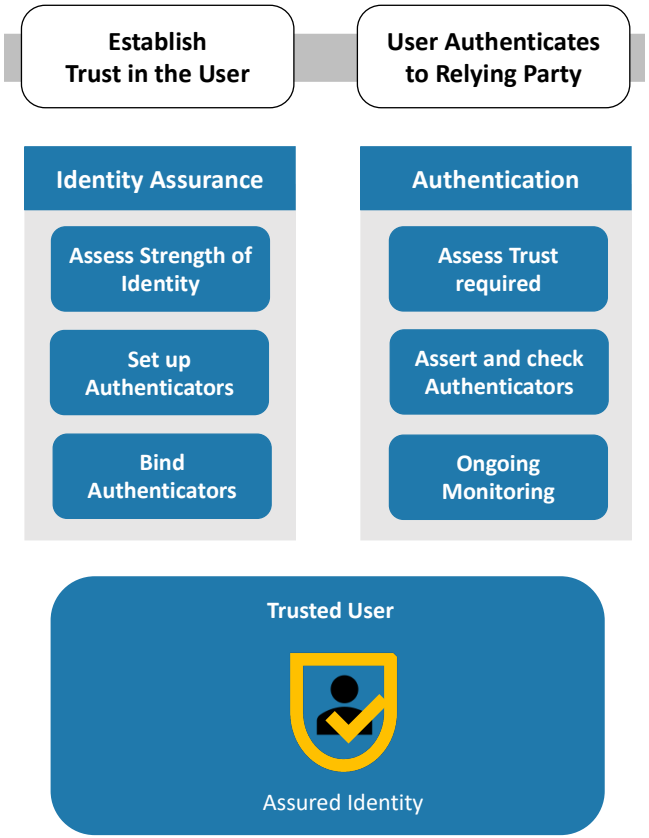
IDENTITY AUTHENTICATION

- The importance of assessing the level of trust a relying party or use case requires.
- Defines different authentication approaches:
  - Single vs multifactor authentication
  - Real-time and continuous authentication
  - Offline authentication
- Expresses the need for ongoing monitoring

Guide Contents: Identity Authentication

CONSIDERATIONS
When authenticating a person asserting an identity, considerations include: - What form of authenticator or authenticators will be used? - Will it be necessary to authenticate users offline? - Has the relative strength of different authenticators or authentication processes been taken into consideration? - If using knowledge-based authentication, do the challenges involve static information, or more dynamic content? Is this strong enough to provide sufficient assurance? - What is the likelihood that the information being asked for could be known by someone other than the rightful owner of the identity? Is it publicly available? - If authenticating the identity using biometrics, what type of biometric information is present? - Is the percentage of false-match and non-match rates, with the biometric technique being used to authenticate the user known and acceptable? Does it conform to a recognised standard? - Are appropriate checks in place to prevent spoofing?

Guide Contents: Identity Assurance



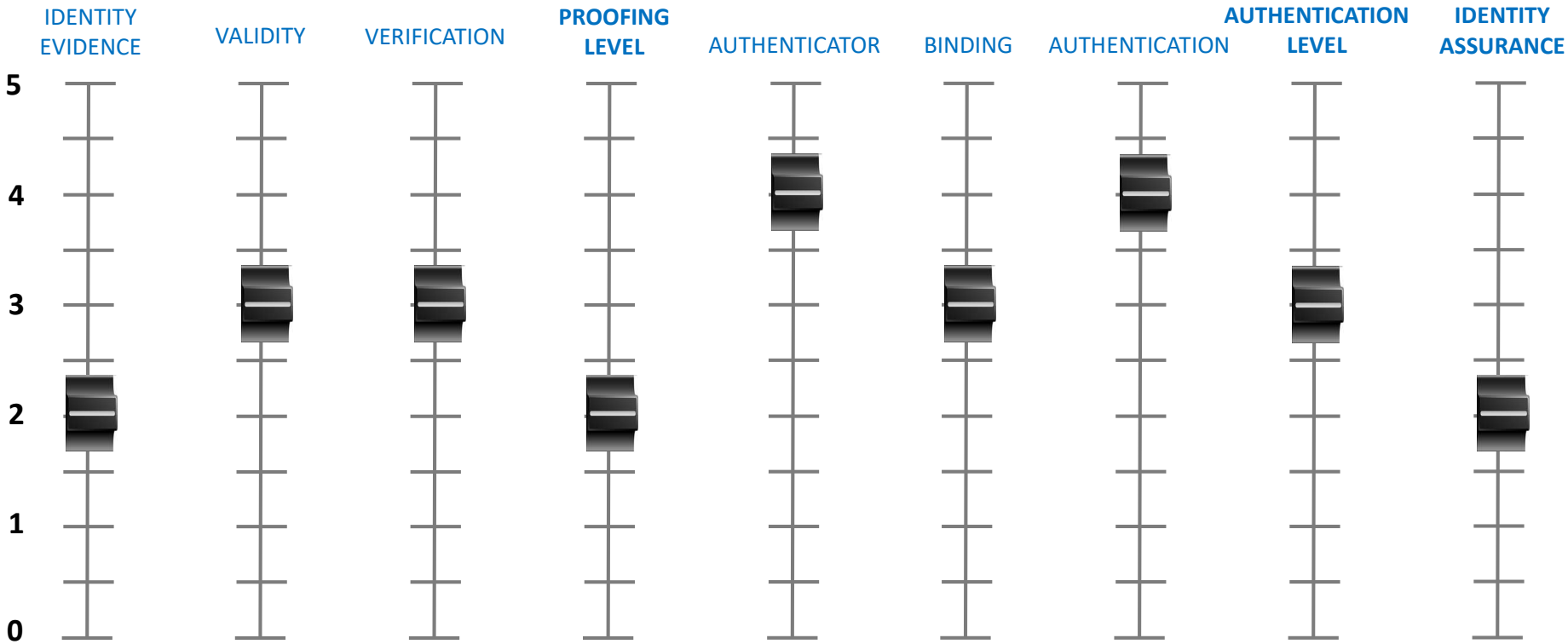
ASSESSING THE STRENGTH OF AN IDENTITY

- Why assessing the strength of an identity is important and what that means in practice
- How assurance or confidence may be assessed at different steps
- Different requirements by sector and use case
- Scoring and communicating identity trust
- Levels of assurance
- Balancing assurance and risk

APPENDIX

- Using digital identity for regulated customer due diligence
- Based on new FATF Guidance
- Stresses importance of standards

Guide Contents: Identity Assurance



Guide Contents: Identity Assurance

CONSIDERATIONS
When contemplating the strength of an identity and whether it is sufficient, considerations include: - What were the strengths of the individual elements of proofing and authentication? - What type of organisation has made the assessment of identity strength, and to what standards? - What is the level of identity risk involved in the transaction the identity user is seeking to make? - Has the relevant competent authority, regulator of trust framework stipulated a minimum strength of identity required for this transaction, or is the choice of identity strength made on a case-by-case risk-assessed basis? - With the identity be assessed on the basis of the strength of its component elements (for example as might be the case with a self-sovereign identity), or on the basis of a combined level of assurance?

What Next?

PUBLICATION

Proofing & Authentication Interoperability Guide (November)

FURTHER RESEARCH?

- Mapping vs different trust frameworks and solutions?
- Devising a full methodology and detailed analysis?

Questions and Discussion

Contacts

Ewan Willars

ewillars@innovateidentity.com

Rob Laurence

rlaurence@innovateidentity.com

www.innovateidentity.com