OIX GUIDE TO IDENTITY PROOFING AND AUTHENTICATION

October 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	October 2020

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 define and 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.
- Understand why identities can be trusted.
- Implement identity proofing and authentication internally in an organisation, particularly in the absence of a recognised trust framework.

a) Introducing the OIX Guide to Identity Proofing and Authentication
In the absence of an established international authority for digital identity, there is no accepted international guide to identity proofing and authentication, nor a universally established nomenclature for describing the core elements of those processes.

This guide forms part of the journey towards establishing them.

- The guide provides both an overview and more detailed explanation of the key elements of identity proofing and authentication, agnostic of technology, solution architecture or the specific approach taken by individual trust frameworks.
- It links to the ***OIX Glossary*** of the main terms and definitions, and to other OIX Digital Identity Trust Framework guides.

b) The intended audience
The guide will be of value to anyone seeking to understand how identities are established and checked. By explaining the terminology and processes involved in accessible language, the guide will introduce lay readers to the subjects of identity proofing and authentication.

For those seeking to use identity solutions to identify the users of their services, this guide provides an invaluable introduction to the main elements of identity proofing and authentication, and a guide to how the relative strength of an identity can be matched against the nature of the use case.

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.

The guide will be relevant to organisations and individuals interested in how digital identities might interoperate between different identity frameworks, and across national borders. The guide will aid those seeking to assess the equivalence of the terms used, the degree of alignment between identity standards, and how the strength of identity and proofing and authentication processes are described.

The guide has been written for a range of stakeholders, to be accessible and practical, and to provide links to further information.

c) Using the guide

The guide is written in a format that will allow the reader to easily navigate the information and link to other OIX and external sources.

- At the beginning of each section of the guide there is a grey text box; this provides an overview of what the reader can expect the section to cover.
- In each section there are one or more blue text boxes; these provide a series of questions for organisations to consider in applying the factors described.
- Within the main body of text, where a word or words are in '***bold italics***', they link to the OIX Glossary where a formal definition of the term can be found.

d) Scope

The range of approaches to establishing and sharing identities and how this is governed vary widely between and within different nations and regions. Guidance provided at national or regional level tends to directly reflect the specific approach to identity taken within that particular framework or circumstance.

However, identity is increasingly a global issue, which transcends different frameworks and technical implementations. Having a simple, overarching, non-framework-specific guide is increasingly important.

This document is intended to provide guidance on the processes of identity proofing and authentication in a manner that is relevant to all approaches, frameworks and solutions, applicable in any local context or circumstance. It is one of a series of guides that make up the OIX Digital Identity Trust Framework Guides.

e) The OIX Guide to Trust Frameworks and Interoperability

Other areas of identity, including 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 guides.

- **OIX GUIDE TO TRUST FRAMEWORKS AND INTEROPERABILITY** [i]

2. ESTABLISHING A PERSON'S IDENTITY

Section Two Overview
Section Two introduces and defines the concept of identity, some of the different forms identity can take, and explains how identity may be used. It briefly describes what attributes are and introduces the concepts of identity proofing and authentication.

a) What is identity?

This is a question that causes much debate as there can be many answers. Identity is how a person is known to their family, friends, work colleagues, the State and other organisations. A known identity may therefore differ according to circumstance and personal preference.

b) Different forms of identity

i) Official identity

The State may know a person, from the start of their lives, by their full name and date of birth that they were registered with, provided by a parent and vouched for by a medical professional at the place of their birth. Other data is captured, such as parents' names and the place of birth to make the registration unique. In some countries a unique identifier will also be issued at this point.

This is sometimes known, particularly in legal contexts, as a person's ***official identity*** – issued by government, and unique within the population. A person can change aspects of their official identity only through a formal process, such as marriage, divorce or by deed poll.

ii) Social identity

A person may choose to be known amongst family, friends, work and social groups with one or more variants of this or, indeed, by a completely different identity (such as a pseudonym). These may be called civic or ***social identity***.

iii) Attributes

A person's identity can include characteristics that make them unique. The information or characteristics that are ascribed to an identity are referred to as identity ***attributes*****.** Some of the more common or core identity attributes include a person's name, their date of birth, and their address, but attributes may include a far wider range of information that collectively are unique to that person. Attributes might also include their preferences, values, or their physical characteristics (physical characteristics are commonly called ***biometric information***).

iv) Personas

Another form of identity are ***personas***. Personas are how people choose to project their role or character in a certain context. Individuals may have a work or business persona, separate from their personal persona which they may choose to project amongst friends or in more informal circumstances.

In slightly more technical terms, personas are another way of describing a person's identity (whether official, or social) in combination with one or more attributes that are used to distinguish or describe them.

c) Digital identity

Digital identity describes a variety of ways to express a trusted and re-usable identity in a digital manner, and which can include attributes, records of the type of evidence used to create it, and ways used to prove the individual is the rightful owner.

The key concept of digital identity is that its rightful owner can use it to provide trust in their identity to any organisation.

The digital identity contains proofs of the user's identity, and these are stored for that user in some way as verified and trusted information, with supporting evidence. The digital identity may be afforded a level of trust, based upon the reliability of the information and processes used to create it, and this may be described as a ***level of assurance***.

The digital identity and other user information and attributes might be held and managed by the individual on their own device or managed by an identity provider.

d) Identity uses

Identity needs to be considered within the context it is being used. Is an identity being used for an interaction with the State, a bank, to travel or buy something, or with a social group? Each type of use case carries a different risk to the person and, in particular, to whoever they are interacting with based on the type of transaction, and whether the identity has been established, and to what degree of certainty – this can be described as identity risk.

For a social group, proving one's identity may not be that important, for the State or a bank it becomes much more important, and for areas of national security it may be extremely important. An identity assumes different levels of importance in different contexts, determined by the level of identity risk involved.

The higher the risk, the more confident in a person's claimed identity the organisation needs to be. How identities are checked, and how the level of confidence or trust is established is the focus of this guide.

e) Eligibilities and authorisations

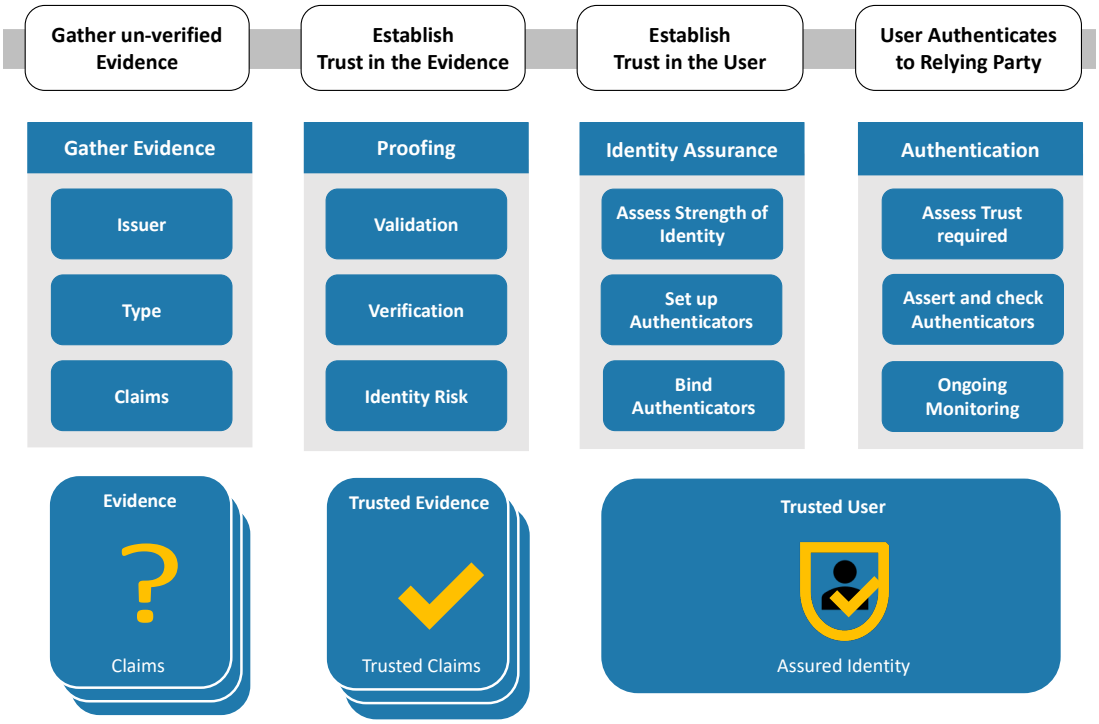
An ***eligibility*** describes a right to do or have something, which may also involve an approval process by a third party (an ***authorisation***).

An authorisation is the permission that needs to be given in order for a person to do or have something that they are entitled to.

For example, at the local minimum driving age, a person may be entitled to apply for a driving licence (their eligibility) but have to pass a test to then be approved to drive on public roads (the authorisation process).

Authorised eligibilities may be applicable in two different contexts. The first of these is as identity evidence. The second is to provide attributes that may belong to an identity. An authorised eligibility, such as a passport for international travel, could be used in both contexts.

The fundamental elements of proofing and authentication



The illustration above demonstrates the range of generic proofing and authentication elements that are used in the creation and assertion of a digital identity.

IN OR OUT OF SEQUENCE?
The illustrated process above 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.

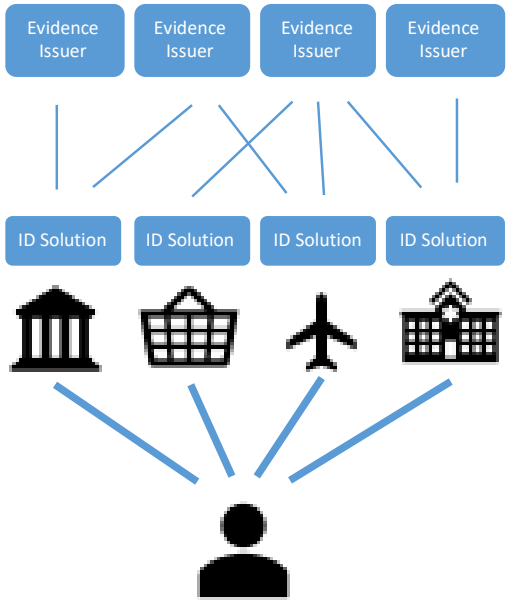
Self-sovereign journeys may start with authentication, but subsequently return to proofing, for example to step up the level of trust or the range of claims they are able to provide to a relying party. There are occasions where steps are repeated, such as the re-validation of evidence used to create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

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

f) Identity proofing and authentication
Organisations that wish to control access to their systems or services typically establish an individual's identity (***identity proofing***), and check that a person seeking to re-engage with the organisation in future is who they claim to be (***identity authentication***).

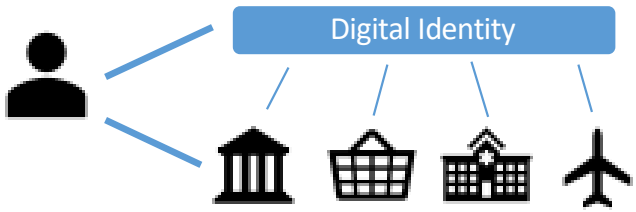
Organisations have often built their own identity proofing and authentication systems and processes. This approach can result in a number of challenges, both for the user and for the organisation.

For the user, they may have to remember an ever-growing number of passwords and usernames, and repeatedly undergo the sometimes-lengthy processes of proofing and authenticating their identity across multiple organisations.



For organisations, this results in having to manage lost or forgotten passwords and account details for their customers, higher abandonment rates, and added cost and vulnerability due to managing bespoke processes and systems.

A digital identity can provide a solution to these challenges by enabling its owner to reuse the same trusted identity across a range of organisations and use cases, providing a more efficient way to confirm an individual's identity. The collection of organisations that share the same approach to identity is often described as an ***identity ecosystem***.



Digital identity remains a rich and varied topic, with a range of approaches and solutions present in each market. This includes the emergence of ***self-sovereign identity*** approaches, which enable a person to store (and often to validate and verify) identity evidence on their own device or in the cloud, which they can share with organisations of their choosing.

The concept of ***data minimisation***, i.e. sharing only the minimum information that is necessary to identify the person and to gain access to a given service, is often a feature of identity ecosystems. Asserting an identity to gain access to a service does not necessarily

require a user to share all of the required attributes with a third party – for example, it is possible for a person to gain access to an age-restricted service by using their identity to prove that they are over 18, but without sharing their exact date of birth, omitting unnecessary fields of information. This is known as providing a ***zero-knowledge proof***.

g) Calculating a level of assurance

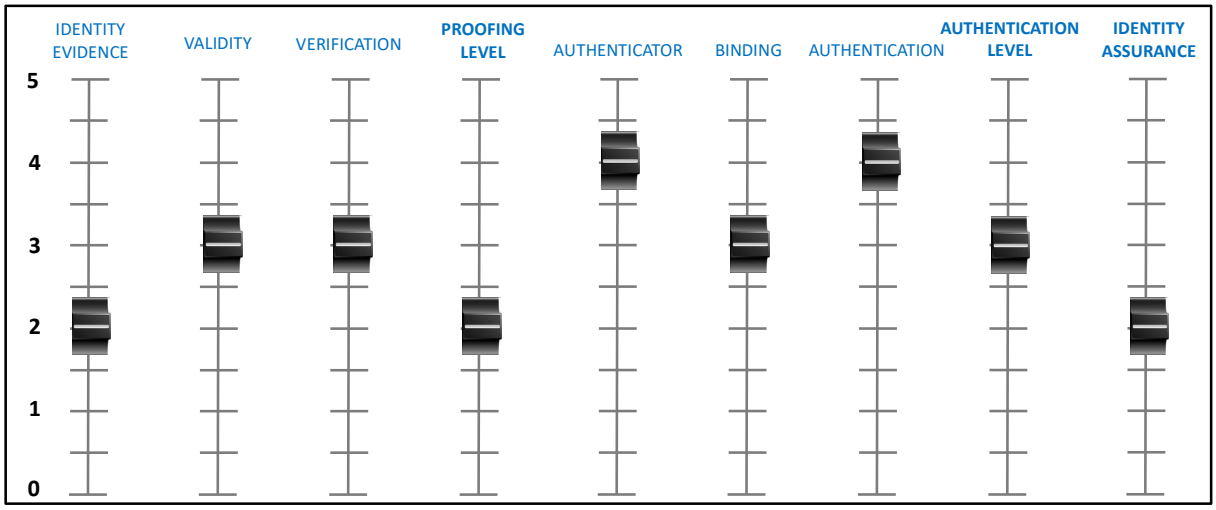
Information on the strength and characteristics of the evidencing and checks that have been undertaken can be shared in raw form to a relying party, or the data can be assessed to a ***level of assurance*** – the degree of trust associated with the identity.

The level of assurance is determined by scoring each step, and then combining them, or assessing them against requirements for the levels of assurance set out by a trust framework. The assessed results or one or multiple steps may be communicated to a relying party.

To utilise this information effectively, the relying party needs to first consider the level of assurance that they require in order to sufficiently mitigate the level of risk related to the use case, and to satisfy their legal or regulatory requirements.

The image below uses the analogy of a series of scales, represented here as a 'mixing desk', to show the different strength of each individual element, and how they can come together to result in proofing, authentication and identity assurance levels.

Relatively 'weaker' elements may limit the overall level of assurance that is capable to be achieved – in such a case it may be necessary to step up the identity by gathering stronger evidence or undertaking further checks. In other circumstances, evidence of stronger steps elsewhere in the profile may be considered to mitigate weaker relatively steps.

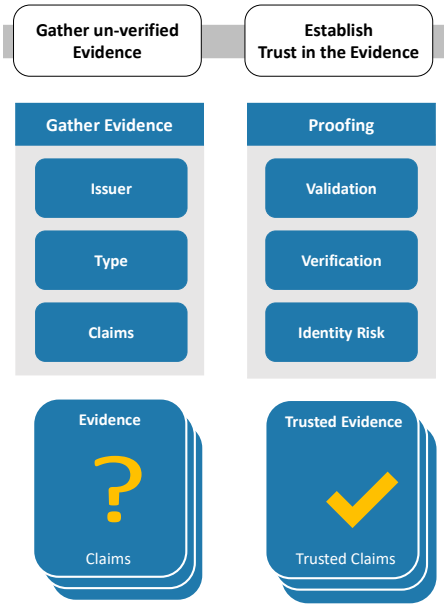


Recording evidence is vital to develop trust, and to enable specific identities and how they have been checked and created to be reviewed or audited should this be required.

The sections below set out the proofing, authentication and identity assurance steps in greater detail.

3. IDENTITY PROOFING

Section Three Overview
Section Three provides detailed guidance on identity proofing, its key elements and how they fit together – i.e. evidence gathering, validation, verification and fraud checking. It will define and explain the processes that are typically involved, using the resulting evidence to establish confidence in an identity, and expressing this within identity frameworks.



In order to check and have a degree of trust in an identity, it is necessary to undertake identity proofing. This encompasses a number of steps which when combined can identify an individual with a degree of certainty, and in a structured and auditable manner.

Ensuring a structured, measurable outcome is important when it's needed to communicate the strength of an identity, for a ***relying party*** to choose whether to accept an identity, and when governments, industry or regulators seek to set identity standards, particularly for their use by regulated industries.

Identity proofing is not dependent on one specific set of checking processes, whether digital or physical in nature. Proofing identity can involve a combination of both in-person and remote processes.

It can also take place over a period – it does not all have to be undertaken at one time.

The steps which together make up identity proofing are:

A. Gathering evidence of a person's identity.
B. Checking that the evidence is valid.
C. Verifying the identity belongs to the person claiming it.
D. Checking the identity is not being claimed fraudulently.

Each step that forms part of identity proofing, and the outcome of each check should be evidenced, and the ***meta-data*** captured during the proofing process can be shared with other parties to enable them to understand what processes have been carried out to establish the claimed identity, who this was done by, to what standard or outcome, when, and potentially other data.

Fraud controls feature throughout the proofing process, in various forms, and then during the identity's ongoing use.

When combined, the evidence creates a degree of trust or confidence, often expressed as the identity's level of assurance.

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 trust or strength of identity assurance 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 sourced from a trusted database.

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?

a) Attributes provided by identity evidence

At least some of the following attributes should be present in the evidence:

- The claimed identity's name.
- The claimed identity's address.
- The claimed identity's date of birth.
- The claimed identity's biometric information.
- A unique reference number.

b) Assessing the strength of identity evidence

Typically, the greater the number of attributes that are present, the stronger the identity evidence. Additional features that affect the strength of a piece of evidence include:

- The physical or digital security features present.
- The strength of checks undertaken by the organisation that issued the evidence.
- The security of the process that was used by the issuer to provide the evidence to the applicant.
- The nature of the issuing organisation and whether it can be considered an authoritative source.

Evidence of official identity - for example, passports that meet the relevant international standards, driving licences that have been issued to agreed state or national standards, or government-issued identity cards - are given a higher strength rating relative to many other

types of identity evidence. This is due to the security features employed, the nature of organisation issuing the evidence, and the strength of the checks they undertake to establish the identity of an applicant.

Identity evidence issued by regulated organisations that follow high standards of customer due diligence, such as financial institutions, are other examples of evidence considered to have a high strength.

c) Where standard evidence is not present
When evidence of official identity or other high strength evidence is not available, other types of evidence may be used alone or in supplement. This can include evidence such as birth or marriage certificates, local government issued evidence, or proof of an account with an established (and usually regulated) organisation.

In the absence of any standard identity evidence, particularly in cases where access to a service is an inclusion issue, ***vouching*** may be another source of evidence of a claimed identity.

The relative strength or weakness of each piece of evidence should be considered on a case by case basis.

B. VALIDATION

Once identity evidence has been gathered, it is necessary to undertake some form of check to ensure that each piece of evidence is valid. ***Validation*** is a process to ensure that the evidence is real, that is not a counterfeit or forgery, that there is a record of the identity evidence being issued and that it has not expired, been cancelled or otherwise become compromised, such as by theft or loss.

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?

a) In person versus remote/digital checks and security features
Validity checks, like the identity evidence they are being performed on, can be either remote digital processes, or they can be carried out in person.

In-person checks can include visual inspection of the evidence. Comparisons can be carried out against known templates and design features, and infrared or ultraviolet features checked. Non-visual checks include data supplied by embedded chips that can confirm the document information, that it has not been tampered with and its date of issuance. Remote visual checks are also possible, typically using automated algorithms to identify a match.

Cryptographically protected information included in the evidence can also be checked, such as by using a secure key.

b) Checking with authoritative sources

Information presented by the evidence can be checked against records held by authoritative sources or by a trusted issuing organisation (such as via a ***Document Checking Service***).

C. VERIFICATION

Identity verification involves checking to ensure that the identity belongs to the person claiming it. This is to prevent impersonation and the risk of someone gaining access to a service by pretending they are someone else. There are a number of ways commonly used to achieve this, typically using knowledge-based or possession-based techniques, or by comparing the user against a previously verified image of them, such as a passport photo.

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?

a) Knowledge-based verification

Knowledge-based verification checks involve asking the person claiming the identity to provide information that only the rightful owner of the identity should know.

The relative strength of knowledge-based checks depends on a number of factors, such as the number of questions asked, whether the information being requested is static (such as a reference number) or a more dynamic check involving uniquely generated or more secure information.

The source of the information is also important to assessing the relative strength of the verification check, including the independence and type of organisation. For example, challenges involving information from statutory or regulated organisations are likely to be more secure and therefore stronger than using information from many other sources.

b) Possession-based verification

Possession-based verification is used to ensure that the person who is claiming the identity has within their possession something else that is considered secure, and that they might be expected to have access to. For example, this can be via a software or hardware-based security token.

c) Biometric verification

Other verification checks involve checking the person claiming the identity against biometric information contained in the evidence they are presenting. As with a knowledge-based challenge, the type of organisation that issued the evidence containing the biometric information is an important consideration.

The most common types of biometric checks used to verify a user involve their image, such as photo matching, whether in person or remotely (such as via a live web link), or via automated forms of facial recognition.

d) Photo matching

Comparing a person's face against a facial image included in the evidence being used to claim an identity can be undertaken either in person or remotely, for example via a web link. This commonly involves comparing a person against the photo included in official identity evidence, such as a passport, driving licence or identity card.

Whether remotely or in person, photo matching can be done by a person, often appropriately trained and under controlled conditions, or by digital facial recognition software.

Non-automated processes, i.e. those undertaken by a person, are stronger if the person carrying out the comparison is trained appropriately, undertakes the check in controlled conditions, and applies measures designed to prevent the process being compromised, such as ensuring that a remote image is live and not pre-recorded or tampered with.

e) Automated facial recognition
Automated facial matching, increasingly using Artificial Intelligence (AI), can be a strong method of undertaking image-based verification. However, it is reliant on the process or software having known and acceptable rates of success, and a sufficiently low likelihood of false positive or negative matches being made.

D. IDENTITY FRAUD RISK ASSESSMENT AND MITIGATION

Carrying out checks during the validation and verification stages to make as sure as possible that the identity is not being claimed fraudulently is an important part of the proofing process.

Identity fraud is a significant factor in a range of wider fraud and financial crimes, such as money laundering, terrorist financing, fraudulent push payments, account takeovers and improper access to services. Fraud that has been facilitated in some way by an identity being falsely created, or compromised, is a significant and growing fraud vector, with cumulative costs to the global economy equal to many tens of £billions.

Some of the principle reasons people seek to commit identity fraud include:
- Gaining access to property, benefits or services they are not entitled to.
- To steal information from other identities.
- To support organised crime.
- To evade detection by authorities.

During the validation step, checks may include ensuring the identity evidence presented is genuine. These could include validating algorithms, checksums and format, and cross-checking consistency of data across different sources of identity evidence.

During the verification step, checking for ***contra-indicators***, i.e. signs of an increased risk that the evidence used to create an identity or how it has been used may be fraudulent, is important. In practice, fraud monitoring typically involves a combination of processes, carried out at different stages of the identity lifecycle.

As well as checking for 'negative' signs that may indicate a higher risk of fraud, a range of the proofing and authentication processes covered in this guide can be seen as 'positive' checks, looking for indicators that suggest that the identity being claimed is more likely to be genuine.

This includes the checks to validate identity evidence and check it is real, as well as the checks used to verify the owner of the identity, and to check any future uses of the identity are by its rightful owner.

Another form of check which is used to counter fraud is to examine the persistence and historic use of the evidence being presented in support of an identity. The analysis of the ***activity history*** or historic record of the evidence may include how long evidence has existed, and whether it has been used in an expected manner.

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)?

a) When to check for fraud risk

Identifying factors that may indicate an elevated risk of identity fraud can happen throughout the identity lifecycle:

- When the identity is first created and proofed.
- Any time that an identity is used, to ensure it is being used by its rightful owner.
- Any time an identity is updated.
- Over time, to ensure the evidence that has been used to support the identity remains valid, and has not been compromised, lost or stolen.
- To identify if the identity itself has been compromised or used in an unexpected or potentially fraudulent manner.

This can involve a wide variety of checking processes, some of which have already been explored in other sections. They can also encompass checking trusted registries that indicate mortality or changes of address, if there is a lack of the expected evidence of the individual in data sources such as voter registers, evidence of device use abnormalities, or the presentation of inconsistent or inaccurate data.

b) What happens when fraud indicators are present?

If indicators of potential fraud risk are found, or if the positive checks do not present the supporting data one might expect, action is taken. This is true whether they are found during the proofing of an identity, or its subsequent use.

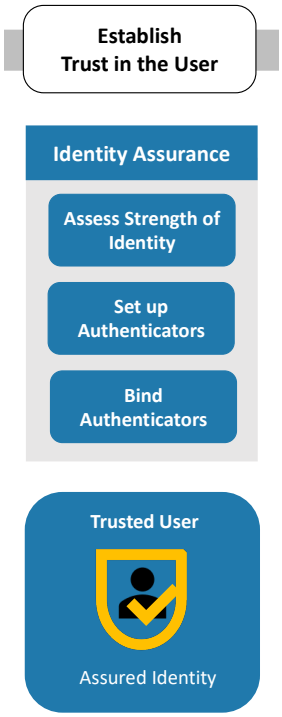
The response will typically form one of a number of actions, dependent on the level of risk:

- Asking for additional or stronger identity evidence.
- Making additional verification checks.
- Temporarily/permanently suspending the use and access to the identity account.
- In federated identity systems, within what is required and permissible within local legislation, to share fraud signals with other organisations, including appropriate law enforcement authorities.
- In SSI solutions seek additional supporting evidence from a number of other sources.

The actions identified above are only indicative – each organisation taking part in creating or using an identity should have specific policies and actions plans in place to set out what actions should be taken if a fraud risk is identified, based on their obligations and to protect themselves and other parties against that risk.

4. AUTHENTICATORS

Section Four Overview
Section Four describes the authenticators that enable the user to be recognised as a known user. It defines the different types of authenticator, describes how an authenticator can be bound to an identity, and the creation of a credential.



Each user typically has one or more authenticators connected to their identity.

An ***authenticator*** is information which can be subsequently checked against anyone claiming the identity to ensure they are its rightful owner.

Authenticators are connected to an identity via a ***binding*** process, securely linking the authenticator to the identity. The binding of an authenticator to an identity creates a ***credential***.

The type or strength of an authenticator is usually dictated by the strength of the identity, having assessed the strength of the evidence and the checks undertaken. A strong identity requires an equally strong authenticator or mix of authenticators (such as a biometric) to subsequently retain the requisite level of assurance.

A single relatively weak authenticator (a 'secret' for example) may limit the overall level of assurance associated with the identity.

a) Types of authenticator

Authenticators can cover a range of different data, usually falling into one of four main categories:

- **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 (for example geo-locational data).

b) Binding

Binding is a process to authoritatively link a verified identity with one or more authenticators. A binding may also link a range of other attributes to the verified identity, and the identity to an account within a system. Regardless of the number or type of authenticators, the binding process ensures that it is connected to the verified identity.

Binding typically takes place following an identity proofing process, and additional bindings can occur over the lifetime of an identity once it has been established.

Binding is an important process and can be a determining factor in how strong an authentication process is, and how much trust can be placed in the identity itself. Strong factors elsewhere will be weakened by an insufficiently robust or reliable binding.

c) Credentials

The term credential is used in a variety of ways in different contexts which can cause some confusion:

- In common usage, a credential can refer to a document that attests who someone is, the organisation they represent, or a qualification they have achieved. Examples include an identity card, passport, driving licence, birth certificate or a letter of introduction. The credential may exist physically, digitally or in both states. Credentials of these types are often used as identity evidence within an identity proofing process and are presented to relying parties as proof of a user's identity or eligibility.
- A credential is also a term used within an identity authentication context. When a verified identity is bound to an authenticator, this derives a credential. A credential defined in this way can also include attributes bound to the verified identity, as well as the authenticator/s. A credential of this kind can be used to provide the basis for a login process. **This OIX guide references this form of credential.**
- A credential, or verified credential, is also a term used with a specific meaning in the field of access management, where a credential can be used to determine a subject's authorisation to carry out an action.

d) Authenticators

i) Knowledge: Something the user knows

A commonly used form of authenticator involves something that the user knows, and that should only be known to both the user and the party initiating the authentication process.

These secrets most often take the form of passwords, or PIN numbers, and may involve checking whether the user can provide information that only the rightful owner of the identity should know, called ***knowledge-based authentication***. The type of knowledge being sought can determine the strength of a knowledge-based authentication, depending on the likelihood that the information may be insecure or publicly available, and based on the number of challenges being presented.

Passwords and PIN numbers are information that can be subject to compromise – people may write down their secrets or share them with others. Passwords may be predictable, and records of authenticators can be hacked and made available to those seeking to commit identity theft.

As a result of their inherent weaknesses, knowledge-based authenticators are often paired with another form of authenticator.

ii) Possession: Something the user has
Even before the advent of the smartphone, checking that a person has in their possession a physical artefact (or token) was already a common form of authenticator; for example, using a device or card reader to access a bank account.

Since the widespread adoption of the smartphone, they have been an increasingly common form of authenticator, with the phone effectively being used as the token. The phone is checked to be in the user's possession, for example through the issuing of a single-use time-limited code sent to the phone.

Tokens can also be entirely digital in nature, such as a unique authentication code or digital certificate.

Possession-based authenticators vary in strength, depending on the type of device or digital form being used. However, all possession-based authenticators have inherent weakness when used alone. Artefacts can be lost or stolen. However, combining a possession-based authenticator with an inherence-based authenticator can form a strong combination.

iii) Inherence: Something the user is
Inherence-based authenticators are based on unique biographic information. This is primarily the user's physical or biological characteristics, or their behavioural characteristics, such as their haptic information (the specific way they type on a keyboard, for example).

As well as facial matching techniques outlined in a previous section, there are a range of other biometric identifiers that can be used to authenticate a user, although some are much more widely used than others. Biometric identifiers can be anything that can be measured and that is unique to that person and their being – the person's DNA, their patterns of behaviour, fingerprints, the way they walk or type, their iris pattern, the mapping of veins under their skin, or their voice.

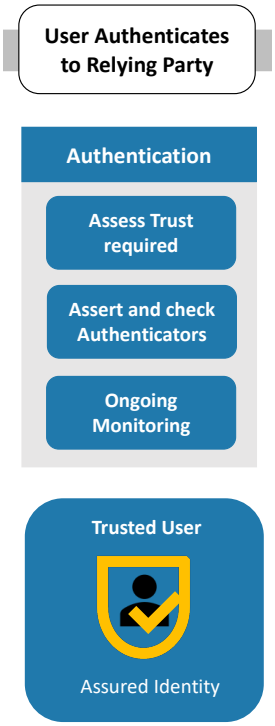
When considering the strength of an authentication process, it is important to consider if it features safeguards to recognise if the biometric record has been tampered with or otherwise compromised, and that the person claiming the identity is not presenting artificial or recorded evidence to provide a match.

Whether a biometric authentication process conforms with recognised standards will also help to define the relative strength of the authentication, and the level of confidence that the person claiming the identity is its owner. Biometrics typically represent a strong authentication method, particularly when paired with another category of authenticator.

v) Context: Risk-based assessment involving a variety of data types
Using contextual data as a means to provide a dynamic risk-based assessment of the likelihood that a person is who they say they are is a relatively recent approach. It can utilise a very wide-ranging data sets from a variety of sources to enable authentication risk to be accurately assessed, such as locational data, internet connectivity data, or other communications records.

5. IDENTITY AUTHENTICATION

Section Five Overview
Section Five describes the process of authenticating a person asserting a previously verified identity to ensure they are who they claim to be. It describes how authenticators are used to re-recognise a known user.



Authentication is carried out to make sure that the person in possession of an identity is the rightful owner.

This takes place whenever the owner of an identity seeks to ***assert*** their identity, whether to identify themselves to access a service or product, or simply to access their account details.

Performing an online login is a very simple everyday example of an authentication process – it enables an organisation to re-recognise a previously verified user via an authentication when they return to access their account.

Stronger forms of authentication that provide greater certainty the person is who they claim to be are usually employed for identity checking.

a) Assess Trust Required
A relying party must first have assessed the level of trust it requires for a given transaction, normally based on the level of identity risk involved, and any regulatory requirements.

It can then be determined if the user has that level of trust, possibly stored as a level of assurance.

This can be undertaken by assessing whether the user has previously achieved a defined level of trust or level of assurance that meets the relying party's needs. Alternatively, it may be achieved dynamically based on the trusted evidence and authenticator types requested by the relying party, and available to the user.

The ***identity assurance*** process defines how this assessment is made. This process is explored in more detail in the next section.

If the user does have the level of trust associated with their identity, it must be determined, typically by the identity provider, what authenticators are required to assert that level of trust.

If the user does not have the required level of trust, they will need to establish this by going through part or all of the proofing and identity assurance processes. Undertaking a process to increase the level of trust or assurance in an identity is often referred to as a 'step-up'.

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?

b) Authentication approaches

i) Single- and multi-factor authentication

Using just one authenticator to demonstrate rightful ownership of an identity, or ***single factor authentication***, has inherent weaknesses, as any compromise can allow direct access to a person's identity. A combination of two or more separate authenticators, or ***multi-factor authentication***, is considered to be a much stronger approach, particularly when the two factors are from separate categories, one of which is usually an inherence-based factor.

ii) Real-time or continuous authentication

An authentication approach that is becoming more frequently applied is continuous authentication, sometimes called ***real-time authentication***. This process, rather than requiring a single or small number of authenticators to be checked, uses contextual data from a number of sources, each of which goes towards giving a person a score in real-time (or close to).

For example, this can include triangulating the geolocational data from a person's mobile with their known movements and transactional data, as well as social media, logins and other account activity; almost any verifiable data can be used in principle.

The individual data points, although insufficient to strongly authenticate a person when used alone, when combined can provide a collective strength that can provide considerable confidence that the person is who they claim to be.

iii) Offline authentication

Many authentication processes require internet access or some form of bandwidth for the check to be performed. This is obviously not always possible, and locally held approaches have now been developed that enable ***offline authentication*** of a user to take place in a

trusted manner, requiring no internet or other forms of connectivity at the time the authentication takes place.

As with the elements of identity proofing, the authentication process is also usually assessed in terms of its strength, based on the nature of the authenticators used and the process of checking this against the person asserting the identity.

This is usually given a score, which may also be expressed as an ***authentication assurance level*****.** Assurance and assessing the strength of an identity is explored in detail in the next section.

c) Ongoing monitoring

It is important that trust in the user is kept up to date.

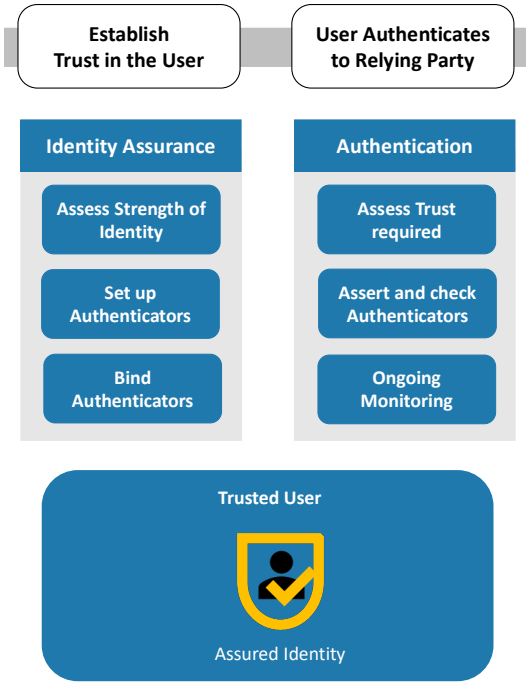
Most evidence does not have an infinite period of validity. Some evidence, such as a user's qualifications may be long lived, but may still be revoked.

Other evidence types such as passports and driving licenses have expiry dates, while evidence such as that provided by an ***identity risk assessment*** may only be valid at the point it is created. In addition, the user may change their circumstances, such as changing their name or address.

Each time the digital identity is asserted, and the authentication process occurs, the validity of any trusted evidence relied upon may need to be checked, and the evidence be reverified and updated if necessary, before the user's identity can be asserted to the relying party.

6. IDENTITY ASSURANCE

Section Six Overview
Section Six explains why it is necessary to assess the strength of an identity based on the evidence, the principles involved in assessing identity assurance (both individual elements that make up proofing and authentication, and as a whole), and the need to match the level of trust in an identity to the risk involved in a given use case.



It is vital that the relying party has determined the level of risk involved in a transaction, and therefore the strength of trust or identity assurance that will be required to mitigate the risks they face.

The confidence or assurance of an identity should be proportionate to the level of identity risk.

Identity assurance
Being able to describe the strength of the proofing and authentication processes used to establish an identity is vital, in order for parties to communicate and understand the degree of trust that has been established, or the level of assurance the identity has been assessed against.

This requires a structured and evidential approach to be used to establish and assess the strength of the individual elements of proofing and authentication – the strength of identity evidence used, the relative strength of the validation, verification and anti-fraud checking processes, and of the authenticators, the binding process and the authentication technique.

The digital identity, the evidence of the claims and checking processes and the associated metadate can communicate the strength of the proofing and authentication evidence to a relying party in a consistent and auditable manner.

This is important for the relying party, as the strength of an identity required should be in proportion to the risk involved in the transaction or process being undertaken, and it may be necessary to demonstrate that at a later date, for example to a regulator. The higher the ***identity risk*** involved in a transaction, the higher the level of trust in the identity should be. Many identity ecosystems also develop approaches that enable the constituent elements to be assessed together, and in balance, using an ***identity assurance model***.

Identity assurance models
An identity assurance model defines the types and amounts of trusted evidence, and the proofing scores required to be achieved for validation, verification and identity risk necessary to achieve a level of trust.

It may also define the type, strength and number of authenticators required to re-access, manage or assert a digital identity in order to maintain the level of trust. A level of trust might be referred to, and communicated as, a level of 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?

Knowing the level of trust in an identity is important across different sectors and use cases.

- **Public Services** – identity is used to gain access to government or public services, which often involves the transfer of private or sensitive information (such as health data, or regarding the registration of voters, for example), or of a financial nature (such as welfare applications).
- **Travel** – particularly for cross-border and air travel, knowing with confidence who the person is that has booked the tickets and is then boarding the means of transport can be an important consideration for national security.
- **Health** – the provision of health information, making sure it pertains to the intended individual, and in particular that it is then delivered to the correct person is considered highly private and sensitive, and identity strength is therefore a key consideration.
- **Financial Services** – identifying an individual is one of the important checks that financial service organisations, and many others, are required by law to undertake to prevent money laundering and terrorist financing. Providing access to a person's account or applying for products that include credit of some type are also financially risky transactions requiring considerable confidence in a person's identity to be established.
- **Retail** – allowing a customer to purchase a product or service online varies in risk, depending primarily on the value of the product or service being provided. Before an expensive item is delivered, a retail organisation may wish to be confident that the address is correct and linked to the person making the purchase.

Other services or transactions may require confidence in a person's identity for other reasons, such as physical safety or security – for example, when agreeing a transaction in the social economy, booking a late-night taxi, or renting out an empty property.

a) Scoring and communicating identity strength

There are a range of factors involved in assessing the relative strength of the different elements of identity proofing and authentication. Evidence of these different elements and processes allows parties to describe the degree of trust of each element via a score.

Many of these factors are summarised in the table below.

CONSIDERATIONS
Indicators of identity strength: **Identity Evidence** - The nature of the organisation that issued the identity evidence – whether a statutory body, a regulated organisation covered by an anti-money laundering regime, or another form of authoritative source. - Whether the evidence is of a legal or official identity, or another form of identity evidence. - The nature of the security features present in the piece of evidence. - The types and strength of the checks undertaken by the issuing organisation, and the way that the evidence was transmitted to the recipient and how secure that process was. - The number of individual pieces of evidence presented. **Validation Evidence** - Whether a piece of evidence is original, or a certified copy of some sort. - The range of identity information or attributes that the evidence includes. - The strength of the validation checking processes being undertaken – and whether by software, or a person adequately trained and in a controlled environment. - If a certified copy, who the certifying person or organisation was, and the checks they may have undertaken. - Whether there are any mistakes or anomalies, and the consistency of the information contained in the piece of evidence. - Whether the evidence can be matched against the record held by an authoritative source, or by the issuer of the evidence. - Whether the security features expected to be present are correct and have not been tampered with. **Evidence of Fraud Checks** - Whether there are any signs that the evidence used to establish the identity has been reported as lost, stolen or used in a fraudulent way. - Whether checks have been made to ascertain if the identity has been identified as being synthetic. - Whether the checks have been made against records held by an authoritative source, and one that is also independent. - If the identity has been checked to ensure it belongs to someone who is alive, and where a record can be found of that identity with organisations that would be expected to know the individual.

- Whether the owner of the identity may themselves be at higher risk of being impersonated, such as a politically exposed or high-profile person.

Verification Evidence

- Whether the verification factor is knowledge-based, versus via a compared photo, or other form of biometric record.
- Whether there is a single factor or multiple factors used to verify the identity.
- If knowledge-based, whether the challenges involve static or dynamic information, and how easy it may be for the information to have been compromised in some way.
- The source of the knowledge being used as the basis for the challenge.
- The strength of the processes used to capture a biometric record by the issuing organisation, and the status of the issuing organisation (whether a statutory or regulated organisation, for example)
- The strength of the verification process itself. If photo matching, whether this has been undertaken by a trained person under controlled conditions and, if biometric matching or via software-based facial recognition processes, the likely level of false positive or negative matches.
- The relative strength of the piece of evidence from which a biometric record has been supplied.
- If remotely verified, whether a liveness test and anti-spoofing techniques are present.

Authenticator Assurance

- The form of authenticator being used.
- The relative strength of the binding process used.
- If using knowledge-based authentication, whether the challenges involve static information, or more dynamic content.
- The likelihood that the information being asked for could be known by someone other than the rightful owner of the identity.
- The nature of the controls used to prevent spoofing.
- If using biometric authenticators, the type of biometric information, and nature of controls present to identify or prevent tampering.
- The expected rate of false matches and non-matches created by the authenticating process.
- Whether the authentication processes conform to relevant and recognised standards.

Authentication Factors

- How many authenticators are required?
- What type and quality of authenticators are acceptable?

Identity trust frameworks usually recognise and adopt guidance or standards that provide a detailed scoring mechanism that encompass these factors, and any other issues affecting the strength of the evidence of identity proofing and authentication. This prevents the need for all organisations to make their own assumptions and assessments of relative strength.

It facilitates interoperability by enabling the level of confidence to be communicated effectively and consistently within an ecosystem, either at a granular level, element-by-element, or as a combined score.

b) Levels of assurance

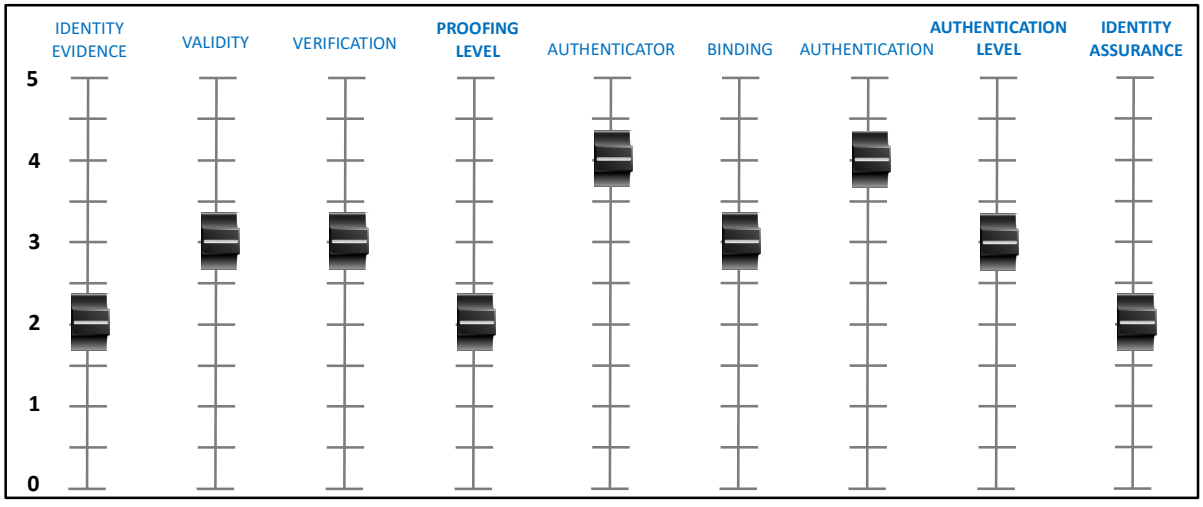
While a granular, elemental approach to scoring identity provides a method of communicating he degree of trust in the individual elements of identity, many identity frameworks also provide a way to assess this more holistically. This involves assessing the various component elements and their scores together, to be able to assign a level of trust, often called the identity's level of assurance.

For organisations that are part of an identity trust framework or defined identity ecosystem, a standardised and accepted approach to assigning levels of assurance - an identity assurance model - enables a more efficient market to be developed. It can negate the need for relying parties to examine each identity at a granular level, instead accepting it on the basis of its level of assurance. An identity assurance model requires that a level of assurance and how it is calculated is agreed amongst the participants in the framework and has processes in place to generate trust in how the score has been assessed, such as via ***certification*** or the use of a ***trustmark.***

An identity assurance model provides a means to assess the various elements of identity proofing and authentication to provide a level of assurance. The details may vary, but there are some principles that are commonly used to form the basis for this calculation.

One method (a more granular approach) may stipulate that certain factors *must* be present in order for an identity to reach a given score or overall level of assurance. This may stipulate that a particular type of evidence is required, such as evidence issued by a Government body, or those with certain security features present. Or it may stipulate using a type of authenticator that meets a minimum standard of operation.

It may therefore be decided that the overall level of proofing or authentication assurance, or the combined level of identity assurance, can only be as strong as its weakest component.



An example is shown in the previous diagram. Here, the identity evidence score is 2, resulting in a proofing level that can be no higher than that, despite relatively stronger validation and verification checks being recorded.

This also flows through to the overall identity assurance score.

Identifying common and recognised levels of assurance provides additional efficiency and certainty for relying parties, particularly those undertaking regulated ***customer due diligence***.

Recognised assurance levels (such as those set out in recognised guidance or standards) also provide a way for relying parties, regulators or competent bodies that oversee sectors to recognise specific levels of assurance as being a minimum or accepted requirement for a given service or transaction, based on its level of risk.

c) Balancing identity strength with the level of risk

Different transactions or use cases carry different levels of risk, for the user, and for the relying party.

For example, applying for credit will require a greater level of identity strength or assurance level than making an online retail purchase. Identifying a passenger before they travel on a plane will need to be more stringent than the strength of identity required to open up an account with a library.

Using an insufficiently strong identity for a transaction means that the identity risks involved are not sufficiently mitigated by the identity – there are inappropriately high risks that the person using the identity may not be who they claim to be, or the information may be incorrect.

However, requiring too high a strength or level of assurance can create problems for identity users, by setting too high a bar and therefore unnecessarily restricting access to services, potentially adding to financial or social exclusion.

As well as understanding the strength of an identity, accurately assessing the level of risk involved in a transaction is vital if the two are to be held in balance, and an appropriate level of assurance or trust identified for a use case.

APPENDIX: USING DIGITAL IDENTITY FOR REGULATED CUSTOMER DUE DILIGENCE

The international anti-money laundering (AML) regime is founded upon assessing the risk involved in a transaction or a business relationship and ensuring that the checks undertaken to identify the individual (part of customer due diligence) match the level of risk.

The greater the level of risk, the stronger and more secure the checks need to be. This includes the proofing and authentication of the individual.

The Financial Action Task Force (FATF) is the global money laundering and terrorist financing watchdog. This inter-governmental body sets international policies and guidance that aim to prevent these illegal activities and the harm they cause to society, and this is reflected in the AML legislation present in the majority of states.

FATF has published Digital Identity Guidelines that stress the importance of a number of factors when considering if a digital identity can be used for undertaking customer due diligence and identifying an individual.

1. **Is the digital identity system authorised by government or a competent authority for use in customer due diligence?** If so, the relying party can utilise a digital identity at the appropriate level of assurance.

2. **If not, is the robustness and assurance level of the digital Identity system known, and either certified or audited by Government, or by Government-approved processes?**

3. **And, does the digital identity system provide a sufficient assurance level for the associated money laundering or terrorist financing risk?**

For regulated entities in particular, being able to assess the risk involved in a transaction and understand (and trust) the level of assurance associated with an identity, are both critical to being able to use a digital identity to identify an individual as part of customer due diligence.

For further information on how to utilise digital identities for regulated customer due diligence, please review the Financial Action Task Force's Digital Identity Guidance:

https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html

[i] https://openidentityexchange.org/guide-trust-frameworks-interoperability