Glossary of Terms

An OIX Guide | January 2022 | Version 1.0

Produced by:

Nick Mothershaw, with the input of the members of the
Open Identity Exchange Working Groups

CONTENTS

1. INTRODUCTION

The identity community uses a plethora of specialist terminology. In order to try and standardise the vernacular OIX has created a separate Glossary of Identity Terms.

The glossary identifies common synonyms for the terms used by OIX. It also includes the rationale for choosing to use some key terms and the list of alternatives considered.

When a glossary term is used in an OIX document they are shown in bold italics.

2. GLOSSARY

Term	OIX definition	Common synonyms
Access Issuer	Issues an Access Credential to an account in a relying party to allow the user to logon to that relying party again and again. Relying Parties are often an access issuer.	
Account Recovery	An individual must be able to recover credentials and / or an account that they have with a provider in the trust framework.	
Agent	A person who is dealing directly with an end user on behalf of one of the participants in the trust framework	
Assertion	A presentation of an identity or credentials to to a relying party	
Identity Assurance Model	An Identity Assurance Model defines: **Proofing** - the process of gathering and establishing trust in credentials for the user, and undertaking identity risk checks. **Set up Authenticators** – make sure the user has the right types of authenticators available to meet the level of assurance (see above). **Identity Assurance** – Assigning a level of assurance from the credentials and identity risk checks gathered, and authenticators available. Binding the authenticators to the to the level of assurance.	Identity Assurance Policy
Attribute	A quality or characteristic inherent in or ascribed to someone or something, such as their name, or date of birth, passport number, qualifications, inoculations.	Claim
Authentication	A process that enables the electronic identification of a natural or legal person. Usually the assertion via bound authenticators of one or more credentials.	
Authenticator	A trusted way to re-identify the user to allow them access and assert their Digital Identity and Credentials. Different authenticators have different strengths and can be combined to create even greater strength. Typically, Authenticators fall into different types: Possession - something the user has, such as a token or device. Inherence - something unique about the user themselves, such as a biometric. Knowledge - something the user knows, such as a secret (e.g. a pin or password). Context - consider where the individual is, when they are transacting, what they are doing or may have done in conjunction with the Relying Party that both know i.e. historic, recent transactions	Credential
Authenticator Provider	A specialist in providing authenticators, such as biometrics, leveraged by an Identity Provider to issue and manage a user's authenticators. Banks may be particularly suitable to play this role as they must issue strong authenticators to their customers as part of meeting regulatory standards.	

Term	OIX definition	Common synonyms
Authoritative Source	An organization that is regarded as the definitive authority for identity or eligibility information, often in law. Examples of authoritative sources include government agencies (passports, driving licenses), banks, educational institutions, healthcare providers.	
Binding	Binding is a process to authoritatively link a verified credential with one or more authenticators.	
Broker	In a market where there are multiple identity providers, a broker allows a relying party to enter a single contract and single technical integration to access a critical mass of digital identities or eligibility information from different identity providers or credential issuers. A Broker may retain Evidence relating to a Digital ID transactions on behalf of the relying party, but this retention shall be performed in accordance with any Scheme operational rules.	Ochestrator
Certification	Certification allows Entities to prove their compliance to the requirements of the Trust Framework by means of assessment either formally by an accredited 3rd party or by means of a self-assessed or partially self-assessed method agreed by the members of the Trust Framework.	
Claim	A quality or characteristic inherent in or ascribed to someone or something, such as their name, or date of birth, passport number, qualifications, inoculations. If the intention is also to impart the status of the claim then metadata regarding the provenance and quality of the claim should also be provided as Evidence.	Attribute.
Credential	A Credential describes something about the user, either about their identity or what they are eligible to do. A credential contains claims and evidence. It comes from an issuer and has a period of validity. It has authetenticators bound to it that musr be used to access and share the credential. This could be: ID documents (e.g. passport, driving license), certificates of education, qualifications, entitlements, medical information, proof of social / societal activity, ID fraud risk assessments through to a simple confirmation of the users age bracket (e.g. over 18). Credential will contain claims, evidence, who the issuer is. It will be digitally signed to that who the issued is understood and it's integrity is ensured. It will also contain any authenticators required to be used by the user to access and present the credential:	
Derived Issuer	Derives a new status from credential(s) gathered for a user, such as Over 18 or a Level of Assurance. An Identity Provider will often play the role a Derived Issuer, or it an external Rule Agent might play this role.	
Direct Issuer	Issues the user with a digitized credential after verifying directly that the user is who they claim to be.	
Eligibility	Eligibility is the process of assessing whether the user is able, or allowed, to access the organization's services.	
Eligibility Assurance	Eligibility Assurance is the process is ensuring eligibility evidence gathered or accessed for the user is genuine.	

Term	OIX definition	Common synonyms
Eligibility Credentials	Credentials that proves what the user is eligible to do. This could be: ID documents for specific purposes (e.g. passport, driving license), certificates of education, covid vaccines or tests, qualifications, medical information.	
Evidence	The part of a credential that provides confidence in it's providence: who issued it, how was it verified and with what information, when was it checked, key reference numbers that allow the evidene to be traced back to the issuer records, when was it issued.	
Indirect Issuer	Issues the user with a digitized credential. Relies on the Identity Provider to verify who the user is. A provider of an API call from a Digital ID provider to validate information provided by the user is an example of an indirect issuer.	
Issuer	Issues some form of credential that proves who the user is and / or what they are eligible to do. This could be: electronic issuance of ID documents (e.g. passport, driving license), certificates of education, qualifications, entitlements, medical information, proof of social / societal activity, ID fraud risk assessments through to a confirmation of the users age bracket (e.g. over 18) or a determination of the Level of Assurance. They could be, or could get data from, a trusted "authoritative source" to allow the credential they issue to be validated. The provision of eligibility data is sometimes referred to as an "attribute service".	Issuing sources Issuer (in Self Sovereign)
Identity Assurance	Identity Assurance is a combination of the Identity Verification and Proofing process and the trust imparted by the means of authentication as measured against a set of criteria and levels as adopted by the Trust Framework.	
Identity Credentials	Credentials that proves who the user is. This could be: electronic issuance or verification of ID documents (e.g. passport, driving license), proof of social / societal activity, ID fraud risk assessments through to a simple confirmation of the users age bracket (e.g. over 18).	
Identity Proofing and Verification	The process that validates and verifies documents, data and risk assessments.	
Identity Provider (IDP)	Creates and maintains a Digital Identity for users that they can present to relying parties to prove who they are and what they are eligible to do. The Digital Identity must comply with the overall rules of the trust framework and of any sector-specific trust schemes. In the self-sovereign model, the provider of an app or wallet to hold verifiable credentials is the identity provider. An Identity Provider has a rules engine that allows it to determine a relying parties requirement through an RP Credential Request, and assist the user through the process of gathering any required credentials and applying the rules to those credentials to derive new ones to meet the relying parties needs. They may 'outsource" Credential Request (for complex use cases) to a Rules Agent. Issues the user with Authenticators to allow them to reidentify themselves to the identity provider so that they can reuse their Digital Identity again and again.	

Term	OIX definition	Common synonyms
Identity Proofing Provider	The ID Proofing Provider understands ID Proofing models and will work directly with the user to take them through the ID Proofing process. At the end of the process the ID Proofing Provider will share the Digitized Credentials gathered as part of the proofing process and the result of the proofing process, a Derived Credential representing the level of ID assurance achieved, back to the Digital ID.	
Identity Solution (ID solution)	A combination of technology and business processes that meet the needs of an organisation for the purpose of identity verification, authentication and access (privilege) management.	
Interoperability [between frameworks]	To achieve practical operational interoperability a contractual agreement combining trust, legal, commercial, technical and operational areas between two or more Trust Frameworks will be required. i.e. eiDAS is an example of an overarching Trust Framework between the EU member states	
Level of Assurance	A level of assurance is a set of outcome-based requirements and processes that must be met in order for the trust implied by an assertion of identity to be easily recognised as part of an authentication process. Various standards for levels of assurance currently exist e.g. those provided by ISO/IEC 29115, NIST 800.63.3, eIDAS Regulation.	
Metadata	Structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use, or manage an information resource. Metadata is often called data about information or information about information.	
Proofing	Proofing is the process of establishing trust in evidence collected by, or about, the user.	
Relying Party	An Entity that depends on identity and eligibility data provided to it as being correct, valid, current and complete.	Organization Verifier
Rules Agent	A specialist in applying a set of rules to create a derived credential, such as a level of assurance or a complex finance assessment on the user.	
Trust Framework	A Trust Framework is a set of specifications, rules and agreements often referred to by various names, such as “operating regulations,” “scheme rules,” or “operating policies.”. The framework is likely to include a certification process by which other roles in the eco-system can be shown to be compliant with the trust framework. Each trust framework is likely to need some form of governance or oversight authority to maintain and oversee compliance with the framework.	
Trust Policy	A documented policy that defines, for a specific framework, scheme or relying party: • what ID proofing is required, • which authenticators should be used • what fraud controls should be run • how are any fraud indicators handled.	
Trust Scheme	Defines an implementation of the framework within the overarching rules defined by the trust framework. Implementations could be sector specific, territory specific or global-multinational. For example, sector-specific use cases,	

Term	OIX definition	Common synonyms
	requiring a separate trust scheme, might be: online age verification using zero knowledge proofs, anti-money-laundering checks, or air travel. These sector-specific schemes will often contain the actual implementation of local or global regulations specific to that sector. Schemes may further define, extend or omit optional elements of the trust framework to tailor the identity service to the needs of the specific implementation. For example, the trust scheme might define the ID Proofing requirements for a specific sector within the overarching requirement set by the trust framework. Where the line between trust framework and trust scheme is drawn needs careful consideration.	
Trusted Claim	A quality or characteristic inherent in or ascribed to someone or something, such as their name, or date of birth, passport number, qualifications, inoculations that has been validated and verified. If the intention is also to explain the trusted status of the claim, then metadata regarding the provenance and quality of the claim should also be provided via Trusted Evidence.	
Trusted Eligibility	Eligibility Credentials that has been through an eligibility assurance process.	
Trusted Evidence	Evidence that has been through the proofing process, or that has been accessed directly from an Evidence Issuer on behalf of a trusted user. Includes metadata regarding the provenance and quality of evidence (e.g. how it validated and verified, who the evidence issuer was.).	
Trustmark	Communicates trust and compliance with the framework and schemes to the end user and relying parties. Indicates that an Entity is associated with a particular Trust Framework and allows an individual to verify that is is the case.	
Validation	Validating that the user exists. Validation uses credentials to prove the user exists such as a passport, driving license, bank account. The strength of the credential should be taken into account. For example, a passport is likely to be regarded as higher strength evidence than a utility bill. The credential must be validated to make sure that it is genuine. Validation is can be done by an Issuer, a Rules Agent, an ID Proofing Provider or by the Identity Provider. Validation might also include checking for evidence of user Activity at the address they provide or via the use of some other form of evidence they provide, such as social media.	
Verification	Verifying that this user is the person they are claiming to be. This might be by checking possession of a credential presented by the user either through a face to face check, via video, via an electronic token or via biometric cross match (e.g. selfie to passport photo). The user might also be verified as genuine by the collection of separate verification-specific credentials, such as the ability to answer knowledge-based questions. The verification of a user as the genuine holder of a credential might be done by the same party who validated that evidence, or be done by a separate party, such as the ID Proofing Provier or Identity Provider.	
Vouching	The process of manually validating and verifying evidence, or the whole identity, by an independent person or organisation, rather than through data or via a machine. The person or	

Term	OIX definition	Common synonyms
	organization might be afforded special legal status as trusted party to undertake this role, such as a notary.	

3. RATIONALE FOR CHOICE OF TERMS

Within the identity community there are often many alternatives terms used to the describe the same thing. In order to be consistent within OIX documentation the follow key terms have been chosen from a list of alternatives by an OIX members working group.

The rational for these choices is documented here so that the reader can understand why a particular term was chosen:

<table>
<tr><th colspan="3">What do we need a term for?</th></tr>
<tr><td colspan="3">Someone who needs to trust IDs / ID information</td></tr>
<tr><th>Alternative Term</th><th>English Language Observations</th><th>Potential Alignments or Confusions</th></tr>
<tr><td>Organization</td><td>Covers most business and government use.
Does not cover peer-to-peer</td><td></td></tr>
<tr><td>Verifier</td><td>Covers business and government use. Covers peer-to-peer. Covers things.</td><td>Aligns with W3C SSI models
Confusion with other roles / processes in the OIX trust framework</td></tr>
<tr><td>Relying Party</td><td>Covers business and government use. Covers peer-to-peer. Covers things.</td><td>Term used by OIX to date. Aligns with OIDF standards.
Identerati speak!</td></tr>
<tr><th colspan="3">Chosen Term</th></tr>
<tr><td colspan="3">Relying Party</td></tr>
</table>

<table>
<tr><th colspan="3">What do we need a term for?</th></tr>
<tr><td colspan="3">Someone who has a Digital Identity and accesses a Relying Party</td></tr>
<tr><th>Alternative Term</th><th>English Language Observations</th><th>Potential Alignments or Confusions</th></tr>
<tr><td>User</td><td>Covers personal and business use. Possibly OK for things.</td><td>Accessibly term that buyers of ID services will understand</td></tr>
<tr><td>Holder</td><td>Covers personal and business use. Possibly OK for things.</td><td>Aligns with W3C SSI models</td></tr>
<tr><td>Individuals</td><td>Covers personal and business use. Not so good for things.</td><td></td></tr>
<tr><th colspan="3">Chosen Term</th></tr>
<tr><td colspan="3">User</td></tr>
</table>

<table>
<tr><th colspan="3">What do we need a term for?</th></tr>
<tr><td colspan="3">A collective name for:
• Forms of Identity (e.g. passport, birth certificate, ID card, driving license, identity data footprints, KBA question services)
• Identity Risk Assessments
• Eligibilities (e.g. passport, driving license, qualifications)
• Service Information (e.g. Payment information)</td></tr>
<tr><th>Alternative Term</th><th>English Language Observations</th><th>Potential Alignments or Confusions</th></tr>
<tr><td>Credentials</td><td>A fair description of forms of identity and eligibility. Also payment credentials.</td><td>Used for logon credentials and tokens by NIST, which we would call Authenticators.</td></tr>
<tr><td>Evidence</td><td>A fair description of forms of identity and eligibility. Also payment credentials.</td><td>In W3C Verifiable Credentials and OIDF ID Assurance is used to describe the Evidence that supports the verified claims: the form of identity itself, how an who verified it.</td></tr>
<tr><td>Attributes</td><td>I would not describe a passport as an attribute of a person</td><td>In IT this usually implies a granular data item: name, address, DoB. “a piece of information which determines the properties of a field or tag in a database or a string of characters in a display.”.</td></tr>
<tr><td>Claims</td><td>A claim is “an assertion that something is true.” So this is also a fair English description.</td><td>Used for atomic claims in W3C and OIDF: name, address, date of birth.</td></tr>
<tr><th colspan="3">Chosen Term</th></tr>
<tr><td colspan="3">Credential</td></tr>
</table>

<table>
<tr><th colspan="3">What do we need a term for?</th></tr>
<tr><td colspan="3">A body that provides verification, validation or trusted information on Evidence</td></tr>
<tr><th>Alternative Term</th><th>English Language Observations</th><th>Potential Alignments or Confusions</th></tr>
<tr><td>Issuer</td><td>Covers the action of issue of Forms of ID and Entitlements, but not verification. This body need to provide TRUST in <thing> into the ID ecosystem the Risk assessments as a verification of risk, payment services need to be verified.</td><td>Aligns with W3C standards</td></tr>
<tr><td>Verifier</td><td>Covers the action of verification of Forms of ID and Entitlements. Risk assessments as a verification of risk, payment services need to be verified.</td><td>W3C standards use this for what we might describe as Relying Party.
Aligns with OIDF ID Assurance “verified claims"</td></tr>
<tr><td>Provider</td><td>Generic</td><td></td></tr>
<tr><td>Authoritative Source</td><td>Those playing this role will be, or need access to, an authoritative source to verify the <thing> was issued by them / exists.</td><td>This could be a separate role that is accessed by this role to perform validation / verification. For example, a Document Checking Service from an ID issuing source, a government department, or a CRA.</td></tr>
<tr><td>Trust Issuer, Verifier or Provider</td><td>The word Trust describes what this body is doing as a component role contribution to the eco-system.</td><td></td></tr>
<tr><th colspan="3">Chosen Term</th></tr>
<tr><td colspan="3">Issuer and Verifier where chosen as separate roles.
Authoritative Source is also separately defined.</td></tr>
</table>

4. USE OF THE TERM CREDENTIAL

The term credential has many different meanings with the identity community. OIX uses credential as outline below:

Use of Term Credential	OIX term
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.	Credential
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,	Authenticator
A verified credential is a term used within self-sovereign identity implementations to refer a document that has been validated and verified as belonging to that user.	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.	Access Credential