OIX GLOSSARY OF TERMS

July 2020

Nick Mothershaw

Version 0.1 BETA

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
Account Recovery	An individual must be able to recover credentials and / or an account that they have with a provider in the trust framework.	
Assertion	A collection of Attributes specific to a single Entity in response to a valid Authentication request and any additional metadata related to that response.	
Assurance Model	An Identity Assurance Model defines the types of evidence and methods for scoring each type in order to achieve a Level of Assurance for each of the different Identity Evidence Types: Validation Evidence, Verification Evidence and Identity Risk Evidence. It may also define the Authenticators required to re-access an account to assert and manage that level of assurance.	
Attestation	An Attestation is when a third-party Entity validates that according to their records, that Claims are true. For example, a University may attest to the fact that someone studied there and earned a degree. An attestation from an Authoritative Source is more robust than a proof, which may be forged.	
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 either enables the electronic identification of a natural or legal person.	
Authenticator	A trusted way to re-identify the user to allow them access and assert their Digital Identity. 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
Authoritative Source	Any source irrespective of its form that can be relied upon to provide accurate data, information and/or evidence that can be used to verify a claim made by an Entity.	
Broker	A Broker allows relying parties to enter into a single contract and single technical integration to access a critical mass of IDs and entitlement information from different Identity Providers or Evidence Issuers. An intermediary that would typically be defined by the specific Trust Framework.	

Term	OIX definition	Common synonyms
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.
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.	
Eligibility Evidence	Evidence 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, qualifications, medical information.	
Evidence	Some form of evidence that proves who the user is and / or what they are eligible to do. 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).	Claim
Evidence Issuer	Issues some form of evidence that proves who the user is and / or what they are eligible to do. This could be: electronic issuance or verification 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 simple confirmation of the users age bracket (e.g. over 18). They could be, or could provide data to, a trusted “authoritative source” to allow the evidence they issue to be validated. The provision of eligibility data is sometimes referred to as an “attribute service”. In a self-sovereign identity model, this role in combination with the evidence verifier is referred to as the “Issuer”.	Issuing sources Issuer (in Self Sovereign)
Evidence Verifier	Validates some form of evidence that proves who the user is and / or what they are eligible to do, and then verifies the evidence belongs to the User This could be by accessing an evidence issuer as, or via, an “authoritative source”, to validate the evidence. They can be services that interact directly with the user, including vouching services. This role uses the rules for identity proofing and records the process of such as verified evidence and claims. In a self-sovereign identity model, this role in combination with the evidence issuer, is referred to as the “Issuer”.	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 Evidence	Evidence 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	

Term	OIX definition	Common synonyms
	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. Trust is established through evidence issuers. The Trusted 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 to hold verifiable credentials, provide the user with bound authenticators, and present credentials to relying parties could be a proxy for the identity provider.	
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.	
Identity Technology Provider	A technical or service component used as part of establishment and provision of trust in the identity. Types include: ID proofing and verification, ID authenticators, Fraud controls, Identity Access Management, Aggregators.	
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
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 Scheme	Defines an implementation of the framework for Identity 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 Evidence that has been through the 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 evidence that the user can provide to prove who they are such as a passport, driving license, bank account. The strength of the evidence should be taken into account. For example, a passport is likely to be regarded as higher strength evidence than a utility bill. The evidence must be validated to make sure that it is genuine. Validation is typically done by an evidence verifier. Evidence verifiers may be, or have access to, an authoritative source. 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 evidence 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 evidence, such as the ability to answer knowledge-based questions. The verification of a user as the genuine holder of a piece of evidence might be done by the same evidence verifier who validated that evidence, or be done by a separate evidence verifier. The identity provider may also play the role of evidence verifier in this respect, linking pieces of evidence together to create a single piece, or collection of, more robust evidence.	

Term	OIX definition	Common synonyms
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 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:

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

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

What do we need a term for?		
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)		
Alternative Term	**English Language Observations**	**Potential Alignments or Confusions**
Credentials	A fair description of forms of identity and eligibility. Also payment credentials.	Used for logon credentials and tokens by NIST, which we would call Authenticators.
Evidence	A fair description of forms of identity and eligibility. Also payment credentials.	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.
Attributes	I would not describe a passport as an attribute of a person	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.”.
Claims	A claim is “an assertion that something is true.” So this is also a fair English description.	Used for atomic claims in W3C and OIDF: name, address, date of birth.
Chosen Term		
Evidence		

What do we need a term for?		
A body that provides verification, validation or trusted information on Evidence		
Alternative Term	**English Language Observations**	**Potential Alignments or Confusions**
Issuer	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.	Aligns with W3C standards
Verifier	Covers the action of verification of Forms of ID and Entitlements. Risk assessments as a verification of risk, payment services need to be verified.	W3C standards use this for what we might describe as Relying Party. Aligns with OIDF ID Assurance “verified claims"
Provider	Generic	
Authoritative Source	Those playing this role will be, or need access to, an authoritative source to verify the <thing> was issued by them / exists.	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.
Trust Issuer, Verifier or Provider	The word Trust describes what this body is doing as a component role contribution to the eco-system.	
Chosen Term		
Issuer and Verifier where chosen as separate roles. Authoritative Source is also separately defined.		

4 USE OF THE TERM CREDENTIAL

The term credential has many different meanings with the identity community. As a result of the diverse use of this term OIX has decided not to use the term credential in its documents, and instead uses the terms in the table below for each different definition:

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.	Evidence
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.	Trusted Evidence
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.	Not used