## **eKYC & IDA Working Group Charter**

#### **1) Working Group name**

eKYC and Identity Assurance Working Group

#### **2) Purpose**

Maintain OpenID Foundation specifications for providing Relying Parties with identity information, i.e. verified Claims, along with an explicit attestation of the verification status of those Claims (what, how, when, according to what rules, using what evidence). These specifications are aimed at enabling use cases requiring strong identity assurance, for example, to comply with potential regulatory requirements such as Anti-Money Laundering laws or access to health data, risk mitigation, or fraud prevention.

Build upon OpenID Foundation specifications for providing Relying Parties with identity information with particular focus on:

* Attachment of binary elements (needed for conveying identity evidence in some use cases)
* Representation of when a subject has authority to act for another entity such as person authorised to act for a legal entity or person authorised to act for another person
* Extension to enable RPs to request that the return data be data minimised in specific ways

**Terminology**

**[SOURCE: ISO/IEC 24760-1:2011, 3.1.2, modified – entity has been replaced by subject, added mapping of attribute to claim]**

*identity information verification*

process of checking identity information and credentials against issuers, data sources, or other internal or external resources with respect to authenticity, validity, correctness, and binding to the entity

*verification*

process of checking information by comparing the provided information with previously corroborated information

*verifier*

actor that corroborates identity information

*person*

human being

*subject*

person whose identity is being proofed

*identity*

set of attributes related to a subject

*identifying attribute*

attribute that contributes to uniquely identifying a subject within a context

Note: in the context of OpenID Connect represented as a “Claim”.

*supporting attribute*

attribute that is used in identity proofing but not as an identifying attribute

*identity information*

set of values of attributes optionally with any associated metadata in an identity

*evidence of identity (EOI)*

evidence that provides a degree of confidence that a subject is represented by the identity being claimed

*authoritative evidence*

holds identifying attribute(s) that are managed by an authoritative party

Note: A point in time copy of the identifying attribute(s) is liable to become out of date and therefore becomes corroborative evidence.

Note: This is one type of evidence of identity.

*authoritative party*

entity that has the right to create and responsibility to own and directly manage an identifying attribute

Note: Law sometimes nominates a party as authoritative. It is possible that such a party is subject to legal controls.

*corroborative evidence*

holds identifying attribute(s) that are not managed by an authoritative party

Note: The identifying attributes in corroborative evidence may not be as up-to-date or accurate as authoritative evidence.

Note: This is one type of evidence of identity.

*proofing information*

information collected for identity proofing

*proofing party*

party that performs identity proofing of a subject

*Authority (or authority to act)*

From [Britannica Dictionary](https://www.britannica.com/dictionary/authority) "the power or right to direct or control someone or something" Note: the "someone" for the purposes of this specification is a "natural person", and the "something" is a "legal entity". That power or right will often clarify any ambiguity around the scope or purpose of the action allowed.

#### **3) Scope**

* Maintenance of OpenID for Identity Assurance Specifications
* Development of profiles of the OpenID for Identity Assurance with work on a mechanism for registering re-usable values at key parts of the Identity Assurance metadata
* A mechanism to represent, request and provide claims about the authority a natural person may have to act for another natural or legal person
* Development of a specification that enables attachment of binary objects into an identity assurance payload
* Extension to the request - response capabilities of OIDC to allow for more granular data minimisation
* Not making breaking changes to existing OpenID Connect specifications

**Out of Scope:**Legal or regulatory advice, Identity Proofing, identity information verification

#### **4) Proposed specifications**

OpenID Attachments 1.0

OpenID for Authority 1.0

OpenID Connect Advanced Syntax for Claims 1.0

#### **5) Anticipated audience or users**

* Identity Verifiers
* Application Developers (acting as RPs)
* Age assurance providers
* Ecosystem architects and designers
* Identity Providers (IDPs) or Claims Providers
* Trust Framework operators

#### **6) Language**

English.

#### **7) Method of work**

Mailing list and telephone/internet conference calls combined with F2F (where needed) and  
information sharing/collaborative working via online tools.

#### **8) Basis for determining when the work is completed**

WG consensus based on implementation experience. The work will be completed once it is apparent that maximal consensus on the drafts have been achieved, consistent with the purpose and scope.