Workgroup: connect
Internet-Draft: assurance-levels-00
Published: 3 April 2020
Intended Status: Standards Track
Authors: A. Pulido *Santander*, V. Herraiz, Ed. *Santander*, J. Oliva *Santander*

Assurance Levels

Abstract

This specification defines a new member attribute that allows the process of requesting a minimum assurance level in relation to an existing claim. In the response to this request, the OP SHOULD provide extended information about the assurer and the resolved level.

1. Introduction

Within the current OpenID Connect specification [OIDC], when returning claims to the RP - with the exception of email and telephone - there is no a way to declare and differentiate the claims that have been validated by the OP as part of their current customer due diligence or onboarding processes.

The concept around level of assurance, which has an associated degree of liability based on contractual conditions of the service and the relevant legislation for the OP, is attached too. For instance, banks currently perform KYC and AML checks as part of the onboarding process. In this case, some of the claims provided by the bank could be tied to a particular level of assurance or trust framework.

With this extension proposal, requested claims by the RP can refer to a desired level of assurance. If the OP can meet that level for the claim, and the user consents to share the relevant information, the data will be included in the response. If this level of assurance cannot be met, the claim will not be returned.

1.1. Notational conventions

The key words "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "MAY", and "CAN" in this document are to be interpreted as described in "Key words for use in RFCs to Indicate Requirement Levels" [RFC2119]. These key words are not used as dictionary terms such that any occurrence of them shall be interpreted as key words and are not to be interpreted with their natural language meanings.

1.2. Terminology

This specification uses the terms "Claim", "Claim Type", "Claims Provider","ID Token", "OpenID Provider (OP)", "Relying Party (RP)", and "UserInfo Endpoint" defined by OpenID Connect [OIDC]

Other terms:

- IAL: Identity Assurance Level
- Assurer: Entity responsible for the verification of the level of assurance for a specific claim.

2. Request

This specification defines a generic mechanism to request an assurance level over claims using the new OPTIONAL member `ial`. This new member will be used as part of the claims elements within `id_token` or `userinfo`, as specified in section 5.5 of [OIDC]. It will contain one of the values of the level of assurance as defined by the OP.

Any other member already supported by OpenID specifications remains valid, including members that are defined for every claim.

Here is a non normative example:

```
{
"id_token": {
    "given_name": {
      "purpose": "This is why the RP requires your name",
      "essential": true,
      "ial": "2"
    }
}
```

IAL values are specified by the OP as an ordered enumeration and represented as `string` values. Therefore, the comparator operations are defined and every verification level contains the previous one excluding the first level.

Claim requests with an invalid `ial` member SHOULD not be included in the response. Returning the claim in this case could be misleading.

Every claim MAY have a identity assurance level based on the level of OP verification of the actual data provided in the given claim. The IAL of the actual data at the OP MUST be equal to or greater than the IAL in the request. If the OP cannot provide the level of assurance that has been requested, the claim will not be returned.

The values and meaning for the IALs supported by the OP MAY represent the legal framework the OP operates in, or at least the adherence to standard ways to attest the validity of the data being returned. Here is an example for the IAL values with similarity to some standards such as NIST or eIDAS:

- "1": There is no requirement to link the applicant to a specific real-life identity. Any attributes provided in conjunction with the subject's activities are self-asserted or should be treated as self-asserted. Self-asserted attributes are neither validated nor verified.
- "2": Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL2 introduces the need for either remote or physically-present identity proofing.
- "3": Physical presence is required for identity proofing. Identifying attributes must be verified by authorized and trained representatives.

3. Response

The request will return the resulting claims that match the assurance levels (IALs) requested by the RP.

Implementers SHOULD return an object for each claim inside the `ial_claims` element with the following fields:

- `level` REQUIRED. This is the level of assurance provided by the OP - it MUST be equal to the level requested.
- `assurer` OPTIONAL. The `id` and `name` of the assurer (the entity assuring the data level). This id MUST be unique.

The following is a non normative example of the response:

```
{
    "given_name": "Joe",
    "address": {
        "street_address": "1234 Hollywood Blvd.",
        "locality": "Los Angeles",
        "region": "CA",
        "postal_code": "90210",
        "country": "US"
    },
    "ial_claims": {
        "given_name": {
            "level": "2",
            "assurer": {
              "id": "SANUK",
              "name": "Santander UK PLC"
            }
        },
        "address": {
            "level": "2",
            "assurer": {
              "id": "SANUK",
              "name": "Santander UK PLC"
            }
        }
    }
}
```

4. OP Metadata

The OP SHOULD advertise their capabilities with respect to the assertion claims in their `openid-configuration` (see [OIDC.Discovery]) using the following new elements:

- `ial_claims_supported`: Boolean value indicating the support of any level of assurance claims.
- `ials_definition_supported`: List of supported IALs by the OP

Non normative example:

```
{
  "ial_claims_supported": true,
  "ials_definition_supported": {
    "1": {
      "description" : "There is no requirement to link the applicant to a specific real-lif
      "reference_trust_framework" : "NIST.800-63A"
    },
    "2": {
      "description" : "Evidence supports the real-world existence of the claimed identity a
      "reference_trust_framework" : "NIST.800-63A"
    },
    "3": {
      "description" : "Physical presence is required for identity proofing. Identifying att
      "reference_trust_framework" : "NIST.800-63A"
    }
  }
}
```

5. IANA Considerations

To be done.

6. Normative References

[OIDC] Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, "OpenID Connect Core 1.0 incorporating errata set 1", 8 November 2014, <http://openid.net/specs/openid-connect-core-1_0.html>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", March 1997, <https://tools.ietf.org/html/rfc2119>.

[OIDC.Discovery] Sakimura, N., Bradley, J., Jones, M., and E. Jay, "OpenID Connect Discovery 1.0 incorporating errata set 1", 8 November 2014, <https://openid.net/specs/openid-connect-discovery-1_0.html>.

Appendix A. Notices

Authors' Addresses

Alberto Pulido Moyano, Ed.
Santander
Email: alberto.pulido@santander.co.uk

Victor Herraiz Posada
Santander
Email: victor.herraiz@santander.co.uk

Jorge Oliva Fernandez
Santander
Email: Jorge.OlivaFernandez@santander.co.uk

Table of Contents