OpenID Connect 4 Identity Assurance

February, 2020

Torsten Lodderstedt

CTO – yes.com
OpenID & Identity Assurance

• OpenID Connect increasingly being used in scenarios requiring higher identity assurance levels

• Examples:
  – Anti-Money Laundering
  – Telecomunication
  – eGovernment
  – Access to Health Data
  – Risk mitigation
  – Fraud prevention
Challenges

• Typically used with **implicit** attestation based on the context
  – RP determines trust framework based on IDP it connects to

• Ambiguous
  – What claims in result set are verified, what are not?

• Lack of metadata and evidence
  – Needed for mapping between regulatory/legal contexts, dispute resolution, and auditing

```json
{
  "sub": "24400320",
  "email": "max@mustermann.de",
  "email_verified": true,
  "given_name": "Max",
  "family_name": "Mustermann",
  "birthdate": "1956-01-28",
  "place_of_birth": {
    "country": "DE",
    "locality": "Musterstadt"
  }
}
```
New: Identity Assurance Specification

• OpenID Connect for Identity Assurance
  – https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html

• Representation for verified claims and associated metadata & evidence

• Enables legal compliance for mentioned use cases
Explicit Attestation

- Trust framework the IDP complies with
- Time of verification
- Verifier: what party verified the user’s identity
- Evidence: which evidence where used
- Verification Method: how were the evidence verified
Verification Data Structure (Example)

```
"verification":{
  "trust_framework":"de_aml",
  "time":"2016-04-23T18:25:43.511+01",
  "verification_process":"e53ffebe-3219-45ee-a103-2c9d917f142e",
  "evidence":[
    {
      "type":"id_document",
      "method":"pipp",
      "verifier":{
        "organization":"Deutsche Post",
        "txn":"2ee7c266-802d-4f8b-b3d7-95fc07506a98"
      },
      "document":{
        "type":"idcard",
        "issuer":{
          "name":"Stadt Musterstadt",
          "country":"DE"
        },
        "number":"53554GJM4",
        "date_of_expiry":"2022-04-22"
      }
    }
  ]
}
```

- **External Verifier on behalf of IDP**
- **German Anti-Money Laundering Act**
- **Physical In-Person Proofing**
- **Proofing via ID Card**
International

• Working group members and contributions from UK, US, CA, CZ, SE, FR, ES, DE, and JP
• Looking for even broader group of participants!
• Specification can be used across jurisdictions
• Wiki page documents (growing number) of identifiers for
  – Trust frameworks, e.g. eIDAS, NIST 800-63A, Japanese & German AML
  – Identity documents, e.g. ID Card, Passport, Driving Permit
  – Verification Methods, e.g. „Physical In-Person Proofing and „Supervised remote In-Person Proofing“
• and use cases
No Ambiguities

• Claims with attestation are represented in data structure along with verification metadata

• Also allows to use existing OpenID Connect Claims alongside verified claims in the same transaction
Example

```
{
  "sub": "24400320",
  "email": "max@mustermann.de",
  "email_verified": true,
  "verified_claims": {
    "verification": {
      "trust_framework": "de_aml",
      "time": "2016-04-23T18:25:43.511+01",
      "verification_process": "e53ffeba-3219-45ee-a103-2c9d917f142e",
      "evidence":[...]
    },
    "claims": {
      "given_name": "Max",
      "family_name": "Mustermann",
      "birthdate": "1956-01-28",
      "place_of_birth": {
        "country": "DE",
        "locality": "Musterstadt"
      }
    }
  }
}
```

Privacy Preserving

• RP asks for individual Claims and Verification data elements
• Purpose of inquiry can be conveyed (per transaction or individual claim)
Example Request

```
{
    "userinfo": {
        "verified_claims": {
            "verification": {
                "trust_framework": {
                    "value": "eidas_ial_substantial"
                },
                "evidence": [
                    {
                        "type": {
                            "value": "id_document"
                        },
                        "method": null
                    }
                ],
                "claims": {
                    "given_name": null,
                    "family_name": null,
                    "birthdate": {
                        "purpose": "To send you best wishes on your birthday"
                    }
                }
            }
        }
    }
}
```

Required trust framework: eIDAS Identity Assurance Level "substantial"

Requested user claims

evidence type and verification method but not the evidence itself
Versatile

- Representation can be used in a variety of channels (even beyond OpenID Connect):
  - ID Token
  - User Info
  - Access Tokens
  - Token Introspection Responses

- Support for aggregated and distributed claims allows combination of claims from different claims sources
Status

• 1st Implementers Draft approved in 11/2019
• Dedicated eKYC-IDA working group set up in 01/2020
  [https://openid.net/wg/ekyc-ida/](https://openid.net/wg/ekyc-ida/)
• 2nd Implementers Draft approved on 05/18/2020
• Several implementations (e.g. Connect2id, Authlete, id4me, yes®, ...)

[OpenID Logo]
2nd implementers draft features

• Assertions may contain multiple „verified_claims“
  – Claims from different sources or verified using different trust framework/processes/evidence in the same assertion

• Clarification and simplification of request syntax and processing

• JSON Schema for requests and assertions

• IANA registry entries for new claims (JWT Claims Registry)

• Identifier extensibility based on namespaces
  – Trust frameworks, verification methods, id documents
  – Overview page on openid.net/wg/ekyc-ida/identifiers
Outlook

• Conformance Tests
• Additional Claims for mobile phone number and age verification
• Expression Language
• Work with potential adopters (TISA, European Commision, ETSi)
• Support Legal Entities