eKYC & Identity Assurance Working Group

October, 2020

Torsten Lodderstedt

CTO – yes.com
Objective

• Develop OpenID Connect extensions for communication of assured identity information
• Verified claims along with information about how the verification was done and how the respective claims are maintained
• Current Spec: OpenID Connect for Identity Assurance https://openid.net/specs/openid-connect-4-identity-assurance-1_0.html
Status Quo

- eGovernment
- Health Data
- Anti Money Laundering
- Fraud Prevention
- Telecommunications
- Risk Mitigation

Identity information

```json
{
  "sub": "112183889",
  "email": "john@doe.example",
  "email_verified": true,
  "given_name": "John",
  "family_name": "Doe",
  "birthdate": "1955-03-12",
  "address": {
    "country": "BE",
    "locality": "Examplecity"
  }
}
```

Rules?

When verified?

Evidence?

Who verified?

How verified?
OpenID Connect for Identity Assurance

- Representation for verified claims and verification information
- Enables
  - mapping between regulatory and legal contexts
  - dispute resolution
  - auditing
OpenID Connect 4 Identity Assurance - How?

```
{
    "verified_claims":{
        "verification":{
            "trust_framework":"de_aml",
            "evidence":[
                {
                    "type":"id_document",
                    "method":"pipp",
                    "time": "2012-04-22T11:30Z",
                    "verifier": {
                        "organisation": "National Post"},
                    "document":{
                        "type":"idcard",
                        "date_of_expiry": "2020-03-22"}
                }
            ],
            "claims":{
                "given_name": "John",
                "family_name": "Doe"
            }
        }
    }
}
```
Main Concepts

• Explicitness
  – Trust Framework, Time & method of verification, Evidence

• Clarity
  – Clear distinction between claims with and without attestation
  – Can be used together with existing OpenID Connect Claims

• Versatility

• Preservation of Privacy
  – Relying party can express fine-grained data requests
  – Asks for individual Claims and verification data elements
  – Purpose of request can be conveyed
## International Standard

→ Identifiers for...

<table>
<thead>
<tr>
<th>Trust Frameworks</th>
<th>Identity Documents</th>
<th>Verification Methods</th>
</tr>
</thead>
<tbody>
<tr>
<td>eIDAS &amp; NIST 800-63A</td>
<td>ID Card &amp; Passport</td>
<td>Physical In-Person Proofing</td>
</tr>
<tr>
<td>Japanese &amp; German AML</td>
<td>Driver’s License</td>
<td>Supervised remote In-Person</td>
</tr>
</tbody>
</table>

Full list: [https://bitbucket.org/openid/ekyc-ida/wiki/identifiers](https://bitbucket.org/openid/ekyc-ida/wiki/identifiers)

→ Extensible

→ Contributions welcome!
Current Status

→ 2nd Implementer’s Draft approved in May 2020
→ Several implementations exist
→ 3rd Implementers Draft in Preparation
   → New: Age Verification, MISDN, Alias
   → ID Document Images (Evidence)
   → Editorial improvements
Outlook

→ Aiming for final publication after Implementers Draft 3
→ Work with potential adopters, e.g. TISA, European Commission, ETSi
→ Conformance Tests
→ New Topics
  → Expression Language
  → Support for Legal Entities
Contributions welcome!

WG page: https://openid.net/wg/ekyc-ida/
WG meeting weekly on Wed (4pm CEST)