OpenID Connect & FAPI Overview

2020-10-28
OIDF Workshop - FAPI
OpenID Connect: Selective Claims Provision Protocol

Which also forms Basis for ABAC.
An Identity Layer provides:

<table>
<thead>
<tr>
<th>Who</th>
<th>• is the user that got authenticated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Where</td>
<td>• was he authenticated</td>
</tr>
<tr>
<td>When</td>
<td>• was he authenticated</td>
</tr>
<tr>
<td>How</td>
<td>• was he authenticated</td>
</tr>
<tr>
<td>What</td>
<td>• attributes he can give you</td>
</tr>
<tr>
<td>Why</td>
<td>• he is providing them</td>
</tr>
</tbody>
</table>
Identity = Set of Claims related to an entity

```json
{
    "iss": "https://server.example.com",
    "sub": "248289761001",
    "aud": "example.net",
    "acr": "https://tf.example.com/gold",
    "iat": 1311280970,
    "exp": 1311281970,
    "nonce": "n-0S6_WzA2Mj"
}
```
Interoperable

Simple & Mobile Friendly

Flexible

Secure
## Interoperable

<table>
<thead>
<tr>
<th><strong>Standard scopes</strong></th>
<th>• openid, profile, email, address, phone</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Method to ask for more granular claims</strong></td>
<td>• Request object and claims</td>
</tr>
<tr>
<td><strong>ID Token</strong></td>
<td>• Info about the authenticated user</td>
</tr>
</tbody>
</table>
| **UserInfo endpoint** | • Get attributes about the user  
  • Translate the tokens |
Simple & Mobile Friendly

JSON Based

REST Friendly

In simplest cases, just copy and paste

Mobile & App Friendly

e.g., ID Token is signed JSON
{
  "iss": "https://client.example.com",
  "user_id": "24400320",
  "aud": "s6BhdRkqt3",
  "nonce": "n-0S6_WzA2Mj",
  "exp": 1311281970,
  "iat": 1311280970,
  "auth_time": 1311280969,
  "acr": "2",
  "at_hash": "MTIzNDU2Nzg5MDEyMzQ1Ng"
}
Security Scalability

OAuth 2.0
(RFC6749 & RFC6750)

OpenID Connect
+ ID Token (JWS/JWT)
+ Hybrid Flow
+ JAR

FAPI
+ mTLS
+ PKCE
+ JARM
+ CIBA etc.
FAPI - Financial-grade API Security Profile

Designed for higher security

For transactions with higher values at stake or to exchange sensitive data.

Formally Verified

Security Properties Formally verified against Web Attacker Model.
Flexible

**Granular Request**
- Through Request Object (JSON)
- Data Minimization

**Aggregated Claims**
- Does not disclose data recipients to data sources

**Distributed Claims**
- Decentralized Data Storage
FAPI - Ver1 & Ver2

FAPI ver.1 is to become final specification this year.

- Formally verified
- Open Banking UK
- Open Banking AU - [https://consumerdatastandardsaustralia.github.io/infosec/#2-overview](https://consumerdatastandardsaustralia.github.io/infosec/#2-overview)
- FDX North America coming onboard on FAPI ver.1

FAPI ver.2 is in the making.

- Streamlining
- Clearer security target
- Yet to be Formally Verified
- OBIE, AU CDR, FDX will contribute in ver.2
- Part 1 - Baseline (was Read Only)
- Part 2 - Advanced (was Read & Write)
- Part 3 - CIBA Profile
- Part 4 - JARM
• Grant/Consent Management
• Event Notification.
• etc
Conformance Test
Create the future together.