Introduction to the OpenID Foundation, OpenID Connect & Financial-grade API (FAPI)
OpenID Foundation

A non-profit international standardization organization founded in 2007.

Specialized in the standardization of internet identity layer and API access management.
OpenID Foundation Members

Members spread over 36 countries.
Instrumental in the creation of standards including:

- OpenID Connect 1.0
- OAuth 2.0
- JSON Web Signature (JWS)
- JSON Web Token (JWT)
- Client Initiated Backchannel Authentication (CIBA)
- Financial-grade API Security (FAPI)
- OpenID Connect for Identity Assurance 1.0 (eKYC)
- Shared Signals and Events

... and more
3B Users Worldwide

Apple, Google, Microsoft, Verizon, UK Open Banking, Australian CDS, BankID (Norway), itsme (Belgium), GSMA, etc.
OpenID Connect: Selective Claims Provision Protocol

Which also forms Basis for ABAC.
Identity = Set of Claims related to an entity

{
  "iss": "https://server.example.com",
  "sub": "248289761001",
  "aud": "example.net",
  "acr": "https://tf.example.com/gold",
  "iat": 1311280970,
  "exp": 1311281970,
  "nonce": "n-0S6_WzA2Mj"
}
<table>
<thead>
<tr>
<th><strong>An Identity Layer Provides</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Who</strong></td>
</tr>
<tr>
<td><strong>Where</strong></td>
</tr>
<tr>
<td><strong>When</strong></td>
</tr>
<tr>
<td><strong>How</strong></td>
</tr>
<tr>
<td><strong>What</strong></td>
</tr>
<tr>
<td><strong>Why</strong></td>
</tr>
<tr>
<td>Standard scopes</td>
</tr>
<tr>
<td>-----------------</td>
</tr>
<tr>
<td>Method to ask for more granular claims</td>
</tr>
<tr>
<td>ID Token</td>
</tr>
<tr>
<td>UserInfo endpoint</td>
</tr>
</tbody>
</table>
Simple & Mobile Friendly

e.g., ID Token is signed JSON

```
{
    "iss": "https://client.example.com",
    "sub": "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)
+ ID Token (JWS/JWT)
+ Hybrid Flow
+ JAR

OpenID Connect
+ mTLS
+ PKCE
+ JARM
+ CIBA etc.

FAPI
### Flexible

<table>
<thead>
<tr>
<th>Granular request</th>
<th>Through request object (JSON) – data minimization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aggregated claims</td>
<td>Does not disclose data recipients to data sources</td>
</tr>
<tr>
<td>Distributed claims</td>
<td>Decentralized data storage</td>
</tr>
</tbody>
</table>
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
How do you know if it was implemented correctly?
Conformance Test
Create the future together

openid.net