OpenID Connect Focus Scenarios

1.  Web SSO
2.  Simple Social Networking
3.  Claims-Based Authorization
4.  Resource Sharing
5.  Multiple Levels of Assurance
6.  Claims Aggregation from Multiple Sources
1. Web SSO

- Providing user identifier and optional IdP-provided claims to RPs
- Reduce number of places you're using your password
- (OpenID 2.0 already used for this)

- Target Market: Same as OpenID 2.0
2. Simple Social Networking

• Access to basic profile information
• APIs for more advanced interactions
• High security not a requirement

• Target Market: Social Web
3. Claims-Based Authorization

• Using authoritative claims to authorize access
  – Based on claims about the identity

• For example:
  – People acting as employees or members
  – Power of attorney with scope
  – People acting in a role

• Target Market: Enterprises and individuals
4. Resource Sharing

• Person-to-person delegation of your services
• Also person-to-organization delegation
• For example:
  – Calendar sharing
  – Medical records sharing with a doctor
  – Medical records sharing with a medical practice

• Target Market: Enterprises and individuals
5. Multiple Levels of Assurance

• Enable using of range of assertion levels from low to high
  – With a common user experience

• *Target Market:* Wanted by governments
6. Aggregating Claims from Multiple Sources

• Enabling use of verified claims from multiple authoritative sources
  – Including potentially personal data stores

• Without always requiring individual user-visible interactions with all claim sources
  – But still with user consent

• **Target Market:** Commercial or government RPs needing sets of verified attributes
OpenID Connect Spec Diagram

OpenID Connect Protocol Suite
31 October 2011

http://openid.net/connect
Standards Requirements from OpenID Connect Scenarios

<table>
<thead>
<tr>
<th>Requirement \ Scenario</th>
<th>JWT Token Format</th>
<th>Signing &amp; Encryption (in JOSE)</th>
<th>OAuth JWT Assertion Profile</th>
<th>SWD Discovery</th>
<th>Dynamic Client Registration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web SSO</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes for open systems</td>
<td>Yes for open systems</td>
</tr>
<tr>
<td>Social Networking</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes for open systems</td>
<td>Yes for open systems</td>
</tr>
<tr>
<td>Claims-Based Authorization</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes for open systems</td>
<td>Yes for open systems</td>
</tr>
<tr>
<td>Resource Sharing</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes for open systems</td>
<td>Yes for open systems</td>
</tr>
<tr>
<td>Multiple LoAs</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes for open systems</td>
<td>Yes for open systems</td>
</tr>
<tr>
<td>Aggregated Claims</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes for open systems</td>
<td>Yes for open systems</td>
</tr>
</tbody>
</table>