OpenID AB/Connect Working Group

Mike Jones

April 7, 2025

Working Group Highlights Since Last Workshop in October 2024

- Security analysis for OpenID Federation performed
  - Vulnerability in JWT audience for Authorization Server identified
- Certification tests for OpenID Federation being developed
- Interop event for OpenID Federation to occur at SUNET later this month
- OpenID Federation Wallet Architectures adopted
- OpenID Connect Relying Party Metadata Choices adopted
- OpenID Provider Commands adopted

Vulnerability in JWT audience for Authorization Server (1)

- Found by University of Stuttgart researchers during OpenID Federation security analysis
- Described in public disclosure
  - https://openid.net/notice-of-a-security-vulnerability/
- OpenID Federation fixed
- OpenID Connect Core errata in progress
- FAPI 2.0 fixed
- FAPI 1.0 errata in progress
- CIBA Core errata in progress
- Several OAuth specs being updated by rfc7523bis specification

Vulnerability in JWT audience for Authorization Server (2)

- Fix is requiring that audience value of JWTs sent to the authorization server be ***solely the authorization server issuer identifier***
- Previously, audience values were all over the map, providing ambiguity that attackers could exploit
- For instance, this was the PAR [RFC 9126] audience text:

Due to historical reasons, there is potential ambiguity regarding the appropriate audience value to use when employing JWT client assertion-based authentication (defined in Section 2.2 of [RFC7523] with `private_key_jwt` or `client_secret_jwt` authentication method names per Section 9 of [OIDC]). To address that ambiguity, the issuer identifier URL of the authorization server according to [RFC8414] **SHOULD** be used as the value of the audience. In order to facilitate interoperability, the authorization server **MUST** accept its issuer identifier, token endpoint URL, or pushed authorization request endpoint URL as values that identify it as an intended audience.

OpenID Federation Interop Event

- Hosted by SUNET in Stockholm, Sweden, April 28-38, 2025
- ~25 participants
- ~dozen implementations
- Will include testing the existing certification tests
  - https://openid.net/certification/federation_testing/
- Will test interoperation of implementations with each other
- Testing using topologies with multiple trust anchors planned

OpenID Connect Core

- Draft with fix to audience vulnerability published
  - https://openid.net/specs/openid-connect-core-1_0-36.html
  - Intent is to publish it as “OpenID Connect Core 1.0 incorporating errata set 3”
- It makes sense to wait for OAuth spec updates before publishing errata
  - OAuth updates being made by
    - https://datatracker.ietf.org/doc/draft-ietf-oauth-rfc7523bis/
  - Changes being made to reduce its scope, based on discussions at IETF 122

OpenID Connect Native SSO for Mobile Apps

- https://openid.net/specs/openid-connect-native-sso-1_0.html
- Updates being considered to remove reuse of ID Token

OpenID Federation Extended Subordinate Listing

- https://openid.net/specs/openid-federation-extended-listing-1_0.html
- Extends OpenID Federation to provide efficient methods to interact with a potentially large number of registered Entities
- Motivated by open finance use cases in Australia, etc.

- ***Implementations and feedback wanted!***

OpenID Federation Wallet Architectures

- https://github.com/peppelinux/federation-wallet/
- Defines entity types for trust establishment with OpenID Federation for wallet ecosystems

- ***Implementations and feedback wanted!***

OpenID Connect Relying Party Metadata Choices

- https://openid.net/specs/openid-connect-rp-metadata-choices-1_0.html
- Enables RPs to express a set of supported values for some RP metadata parameters, rather than just single values

- *Time for an Implementer's Draft?*

OpenID Provider Commands

- https://openid.net/specs/openid-provider-commands-1_0.html
- Complements OpenID Connect by introducing set of Commands for an OP to directly manage an end-user Account at an RP

Plans for OpenID Federation

- https://openid.net/specs/openid-federation-1_0.html
- Gather feedback from interop event in April and apply to the spec
- Gather feedback from certification tests and apply to the spec
- Create a more complete set of certification tests
  - and test the tests
- Progress to be a Final Specification

Inactive Specifications

- Several adopted specs appear to not be being actively worked on
  - OpenID Connect Claims Aggregation
    - No updates since draft -02 in September 2021
  - OpenID Connect UserInfo Verifiable Credentials
    - No updates since draft -00 in May 2023
  - Self-Issued OpenID Provider v2
    - No updates since draft -13 in November 2023

- ***Should any of these be officially marked as being discontinued?***

Bonus Update – Enhanced Authentication Profile (EAP) WG

- https://openid.net/wg/eap/specifications/
- Token Bound Authentication – Applying Token Binding to ID Tokens
  - Abandoned at Implementer's Draft stage
- OpenID Connect Extended Authentication Profile (EAP) ACR Values
  - Updated in March to enable registration of ACR values as IANA LoA Profiles
  - ACR registrations in place at https://www.iana.org/assignments/loa-profiles/
    - "`phr`" – Phishing-Resistant Authentication
    - "`phrh`" – Phishing-Resistant Hardware-Backed Authentication
  - WGLC for Final status concludes tomorrow
- Once EAP ACR Values is Final, our intent is to close the working group

Your Turn!

- What would you like the OpenID Connect working group to know?