AB / Connect & Federation

Mike Jones

WG Highlights Since Last Workshop in October

- OpenID Federation 1.0 became final, February 2026
- OpenID Federation 1.1 specifications created, separating protocol-independent and Connect-specific functionality into two specs, December 2025 - *Vote to approve final specs today!*
- OpenID Federation Interop Event at TIIME in Amsterdam, February 2026
- OpenID Connect RP Metadata Choices became final, March 2026
- Second security analysis for OpenID Federation approved, March 2026
- WGLC for OpenID Connect Ephemeral Subject Identifier, April 2026
- OpenID Federation Entity Collection 1.0 specification adopted, April 2026
- Frederik Krogsdal Jacobsen became co-chair, April 2026

OpenID Federation 1.0

- Enables trust establishment for multilateral federations
  - Core functionality protocol-independent
  - Also contains OpenID Connect-specific profile
- https://openid.net/specs/openid-federation-1_0.html
- Became final in February 2026
- Result of numerous interop events and deployments
- Incorporating feedback from implementers at each step of the journey
- Conformance tests are in development
  - Trust chain evaluation tests have been well tested & used in interoperability
  - Registration tests are available and would benefit from feedback
  - Input on test descriptions from GÉANT Incubator, FBK in progress

1.1 OpenID Federation Specifications

- The two 1.1 specs together are exactly equivalent to OpenID Federation 1.0
- OpenID Federation 1.1
  - Protocol-independent functionality from OpenID Federation 1.0
  - https://openid.net/specs/openid-federation-1_1.html
- OpenID Federation for OpenID Connect 1.1
  - Protocol-specific functionality from OpenID Federation 1.0
  - https://openid.net/specs/openid-federation-connect-1_1.html

- Vote to approve them today!
  - https://openid.net/foundation/members/polls/406

OpenID Federation for Wallet Architectures 1.0

- Defines how to perform trust establishment for Wallet ecosystems with OpenID Federation
  - Defines entity types for Issuer, Wallet, Verifier
  - Parallel to what OpenID Federation for OpenID Connect does for OpenID Connect
- Corresponds to usage in Italian EUDI Wallet
- Also used for Swedish Wallet
- https://openid.net/specs/openid-federation-wallet-1_0.html
- Spec progressed as a result of feedback during interop at TIIME in February

Interop Event in Amsterdam at TIIME in February 2026

- 12 people, 9 implementations, 9 countries
  - Croatia, Finland, Greece, Italy, Netherlands, Poland, Serbia, Sweden, US
- Read about it at https://self-issued.info/?p=2807

- *This one organized by the community – not the OpenID Foundation!*

Security Analysis of Final OpenID Federation 1.0

- By University of Stuttgart security researchers
- Began April 2026
- Follows security analysis of last Implementer's Draft in 2024

Findings from 2024 OpenID Federation Security Analysis

- Actionable vulnerability in audience values of Client Registration JWTs detected
  - https://openid.net/notice-of-a-security-vulnerability/
- Applies to:
  - OpenID Federation
  - OpenID Connect private_key_jwt registration
  - RFC 7523 (JWT Client Authentication)
  - RFC 9126 (Pushed Authorization Requests)
  - Client-Initiated Backchannel Authentication (CIBA)
- All have been or are being updated to address the vulnerability

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
- Became final in March, 2026
- Used by OpenID Federation specs

OpenID Connect Ephemeral Subject Identifier

- https://openid.net/specs/openid-connect-ephemeral-subject-identifier-1_0.html
- Specifies an ephemeral subject identifier type that prevents correlation of the subject identifier across multiple visits
- Working Group Last Call for Final status, April 2026

OpenID Federation Entity Collection

- Defines an additional federation endpoint to retrieve a filterable list of all resolvable entities of a given type in a (sub-)federation.
- Can be used to populate home realm discovery user interfaces
- Adopted April 2026
- Repository https://github.com/openid/federation-entity-collection
  - Publication at openid.net/specs planned shortly

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.
- Recently updated to make pagination placeholders more general

OpenID Provider Commands

- https://openid.net/specs/openid-provider-commands-1_0.html
- Complements OpenID Connect by introducing a set of Commands for an OP to directly manage an end-user Account at an RP
- Updated to incorporate WG feedback since adoption in March 2025

OpenID Connect Enterprise Extensions

- https://openid.net/specs/openid-connect-enterprise-extensions-1_0.html
- Specifies a number of common or desirable extensions to OpenID Connect
- Reviews and implementations wanted

OpenID Connect Key Binding

- Specifies how to bind a public key to an OpenID Connect ID Token
  - https://openid.net/specs/openid-connect-key-binding-1_0.html
- Active discussions of features
- Editor's draft recently updated

OpenID Connect Native SSO for Mobile Apps

- https://openid.net/specs/openid-connect-native-sso-1_0.html
- Updates being considered to replace reuse of ID Token
- Please discuss during IIW

OpenID Connect Claims Aggregation

- https://openid.net/specs/openid-connect-claims-aggregation-1_0.html
- Many issues recently addressed
- Reviews wanted
- Please discuss at IIW

OpenID Connect Core

- Third Errata Set work under way
- Draft with fix to audience vulnerability published
  - https://openid.net/specs/openid-connect-core-1_0-36.html
- 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
- Other minor errata corrections also merged
- Intent to publish result as “OpenID Connect Core 1.0 incorporating errata set 3”

Your Turn!

- Working group resources
  - https://openid.net/wg/connect/
  - https://openid.net/wg/connect/specifications/

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