AB/Connect and Federation

Mike Jones



WG Highlights Since Last Workshop in April

- OpenID Federation 1.1 specifications, separating protocol-independent and Connect-specific functionality into two specs, became final, May 2026
- OpenID Federation Subordinate Events Endpoint became Implementer's Draft, September 2026
- OpenID Federation Extended Subordinate Listing became Implementer's Draft, September 2026
- OpenID Connect Native SSO for Mobile Apps 2nd Implementer's Draft Published September 2026
- OpenID Connect Key Binding became Implementer's Draft, September 2026
- OpenID Connect Ephemeral Subject Identifier became final, October 2026
- Second security analysis for OpenID Federation under way
- OpenID Federation Entity Collection 1.0 WGLC for Implementer's Draft status, October 2026 - *open now*

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

- eduGAIN migrating to OpenID Federation after successful pilot

OpenID Federation Conformance Tests

- Initial tests for Trust Chains and Registration developed in 2025
  - Used at Federation Interop event in Stockholm, April 2025
- Additional conformance tests currently being developed by others
  - GÉANT Incubator project developing Trust Mark tests
  - FBK used AI to read spec and automatically generate tests
  - Investigating how to integrate both into the conformance suite

1.1 OpenID Federation Specifications

- 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

- Became final May 2026

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
- Actively being progressed towards Implementer's Draft status

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
- Active discussions of what the specification guarantees between the security researchers and the working group

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

IETF spec closing OAuth vulnerabilities almost an RFC

- “Updates to OAuth 2.0 JSON Web Token (JWT) Client Authentication and Assertion-Based Authorization Grants”
  - https://datatracker.ietf.org/doc/draft-ietf-oauth-rfc7523bis/
- Once done, time to finish applying fixes to OpenID Connect and CIBA
- Current errata drafts starting this work
  - https://openid.net/specs/openid-connect-core-1_0-36.html
  - https://openid.net/specs/openid-client-initiated-backchannel-authentication-core-1_0-06.html

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
- Became final October 2026

OpenID Federation Subordinate Events Endpoint

- https://openid.net/specs/openid-federation-extended-listing-1_0.html
- Provides a mechanism for Trust Anchors and Intermediates to publish historical events related to their Immediate Subordinates, such as registration, revocation, and updates of their Federation Entity Keys
- Motivated by Italian deployments
- Implementer’s Draft published in September 2026

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.
- Was updated to make pagination placeholders more general
- Implementer’s Draft published in September 2026

OpenID Federation Entity Collection

- https://openid.net/specs/openid-federation-entity-collection-1_0.html
- 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

- WGLC for Implementer's Draft status currently open
  - Responses needed!

OpenID Connect Native SSO for Mobile Apps

- https://openid.net/specs/openid-connect-native-sso-1_0.html
- Enables native applications by the same vendor to share login information
- Second Implementer's Draft published September 2026
- Updates being considered to replace reuse of ID Token
- Please discuss during IIW

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
- Implementer’s Draft published in September 2026

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 Claims Aggregation

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

Future Work Items

- Providing guidance for transition to post-quantum cryptography
  - Slack channel #interest-group-pqc-readiness
  - Blog post https://openid.net/post-quantum-openid-connect/
  - Also see upcoming discussion
- Providing guidance for transition from SAML to OpenID Connect
  - Slack channel #interest-group-saml-to-oidc-readiness

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?