Trust Establishment with OpenID Federation

April 18, 2024

Mike Jones and John Bradley

Internet Identity Workshop

What is Trust Establishment?

- Determining whether two parties that would like to interact share a common trust infrastructure
- Examples:
  - Do an OpenID Provider and an OpenID RP belong to a common federation?
  - Is a Verifier eligible to have a Credential presented to it by a Wallet?
  - Do two parties belong to the same Open Banking ecosystem?

OpenID Federation Specification

- OpenID Federation specification
  - https://openid.net/specs/openid-federation-1_0.html
- Enables trust establishment and maintenance of multi-party federations
  - Applying lessons learned from large-scale SAML federations
  - Can be used for OpenID Connect, OAuth 2.0 deployments, Wallet ecosystems
- Renamed from “OpenID Connect Federation” to reflect broader role
  - Can be and is used both with and without OpenID Connect
- Defines hierarchical JSON-based trust establishment data structures for participants
  - Enables trust to be established independent of Web PKI

Specification Progress & Status

- OpenID Federation work begun in July 2016
- Three interop events were held in 2020
- Current specification is draft 34
  - https://openid.net/specs/openid-federation-1_0-34.html
- In production use in Italy, Australia, Sweden
- Have resolved most open issues
  - *Last Implementer's Draft planned in this quarter*
  - *Then advancement to Final status later this year*
- Planning for Certification testing started

Tour of Federation Features (1)

- Entities
  - Leaf, Intermediate, Trust Anchor
  - https://openid.net/specs/openid-federation-1_0-34.html#name-introduction
- Entity Statement
  - Self-signed JWT declaring properties about an entity
  - https://openid.net/specs/openid-federation-1_0-34.html#name-entity-statement

Tour of Federation Features (2)

- Trust Chain
  - Sequence of Entity Statements used to establish trust
  - Starts with a Leaf, contains Intemediates, ends at a Trust Anchor
  - https://openid.net/specs/openid-federation-1_0-34.html#name-trust-chain
- Entity Types
  - The role(s) that an entity plays in a Federation
  - Examples: OP, RP, Wallet, Verifier, Federation Entity
  - https://openid.net/specs/openid-federation-1_0-34.html#name-entity-type-identifiers

Tour of Federation Features (3)

- Metadata
  - Declarations metadata for entity types
  - For example, OP metadata, RP metadata
  - https://openid.net/specs/openid-federation-1_0-34.html#name-metadata
- Metadata Policy
  - Enables superiors to provide and constrain metadata values
  - For example, constraining signing algorithms within Federation
  - https://openid.net/specs/openid-federation-1_0-34.html#name-metadata-policy

Tour of Federation Features (4)

- Trust Marks
  - Statements of conformance by sets of criteria by an accredation authority, which are signed JWTs
  - Can be included in Entity Statements
  - https://openid.net/specs/openid-federation-1_0-34.html#name-trust-marks
- Automatic Registration
  - Enables identifying OAuth Clients/RPs using Entity Identifiers
  - No explicit registration needed
  - https://openid.net/specs/openid-federation-1_0-34.html#name-automatic-registration