Certification Testing for OpenID Federation

Michael B. Jones

December 29, 2024

# Modes of Testing Federation Implementations

There’s value in testing both deployed federations and federation software. Some tests can be run on production federations to validate that they are correctly following aspects of the specification. However, “negative tests”, which test how an implementation handles misbehaviors, such as bad signatures, require interacting with test federations supplied by the certification testing software that can perform both positive and negative tests. Some positive tests also require participating in test federations so that a full range of inputs can be generated and tested against.

Therefore, I propose these modes of testing Federation implementations and deployments:

* **Deployed Single Entity Testing:**  Tests the properties of an Entity deployed in a Federation in detail. Obviously, only features used by the Entity can be tested.
* **Deployed Entire Federation Testing:** Tests the properties of an entire deployed Federation graph. These tests walk the Federation graph using authority\_hints values and Subordinate Listings, validating the relationships between the Entities. Obviously only limited information can be logged so that the log sizes for Federations with thousands of Entities do not become unwieldy.
* **Entity Joined to Test Federation:** Tests the behavior an Entity within a custom federation created for certification testing purposes. Both positive and negative tests can be run in this manner. There will be some tests applicable to all Entity Types and some specific to particular Entity Types.

# OpenID Federation Certification Profiles

## Profiles for Deployed Single Entity Testing

* **Deployed Federation Entity:** Tests that the Entity has a valid Entity Configuration and consistent relationships with its superiors and subordinates.

## Profiles for Deployed Entire Federation Testing

* **Deployed Federation Structure:** Tests that the relationships been Entities in an entire deployed Federation graph are internally consistent and that all Entities have valid Entity Configurations. Logs superior and subordinate relationships and pass/fail status for each Entity with reasons for any failures.

## Profiles for Entities Joined to Test Federations

* **Complete Federation Entity:** Tests both positive and negative conditions applicable to any Federation Entity. Includes tests in **Deployed Federation Entity** profile and more.
* **Metadata Resolution:** Tests that the Entity creates correct Resolved Metadata for a Trust Chain. Requires that the Entity either have a Resolve Endpoint or be an OP supporting Explicit Registration.
* **Trust Anchor:** Tests additional requirements applicable to Trust Anchors.
* **Trust Mark Issuer:** Tests requirements for Trust Mark Issuers.
* **Trust Mark Verifier:** Tests that Entities using Trust Marks correctly validate them.
* **OP Using Automatic Registration:** Tests Automatic Registration functionality for OPs.
* **RP Using Automatic Registration:** Tests Automatic Registration functionality for RPs.
* **OP Using Explicit Registration:** Tests Explicit Registration functionality for OPs.
* **RP Using Explicit Registration:** Tests Explicit Registration functionality for RPs.