Course by Consortium GARR and Reti Business & IT Consulting

OIDC
What's more

OIDC primer - a course on OpenID Connect

Credits: Roland Hedberg, Ioannis Kakavas

OpenID Connect Federation

a work in progress...

OpenID Connect Federation 1.0 - draft 01

openid-connect-federation-1_0

R. Hedberg, Ed. [independent]
R. Gulliksson [UmU]
M. Jones [Microsoft]
J. Bradley [Ping Identity]
September 9, 2016

http://openid.net/specs/openid-connect-federation-1_0.html

OpenID Connect Federation - @GÉANT

GN4-2 JRA3 T1.A

Carry out development based on OpenID Connect (OIDC), specifically for extending the standard to make OIDC “federation and interfederation capable” (i.e. OIDC metadata, discovery, etc.), including engaging with and contributing to the IETF and developing a potential OIDC profile for eduGAIN.

https://wiki.geant.org/display/gn42jra3/GN4-2+JRA3

OpenID Connect Federation - the problem, a solution

The OpenID Connect standard specifies **how a Relying Party (RP) can discover metadata about an OpenID Provider (OP)**, and then register to obtain client credentials. During discovery and registration there is no automated mechanism for the OP or the RP to verify the information exchanged during this process. **All the information is self-asserted**.

In an identity federation context this is not sufficient. The participants of the federation must be able to trust information provided about other participants in the federation.

This document describes **how an identity federation can be built around a trusted third party, the federation operator**.[1]

[1] openid-connect-federation-1_0

OpenID Connect Federation - over self-assertion

This document **extends Signed Metadata**, as introduced by OAuth 2.0 Authorization Server Metadata [I-D.draft-ietf-oauth-discovery], to create so called **metadata statements**. Metadata statements together with the use of a trusted third party (that verifies and enforces some common policy), **can be used to transfer verified data and trust** in the data between clients and servers.[1]

[1] openid-connect-federation-1_0

OpenID Connect Federation - Metadata components

signing_keys OPTIONAL. A JSON Web Key Set (JWKS) [RFC7517] representing the public part of the entity's signing keys.

signing_keys_uri OPTIONAL. Location where a JWKS representing the public part of the entity's signing keys can be found[...]

metadata_statements OPTIONAL. JSON array containing a list of metadata statements.

metadata_statement_uris OPTIONAL. JSON object where the names are the federation identifiers and the values are URLs pointing to metadata statements connected to each federation.

signed_jwks_uri OPTIONAL. This is the signed version of the jwks_uri parameter defined in OpenID Connect Dynamic Client Registration 1.0 [...]

[1] openid-connect-federation-1_0

OpenID Connect Federation - Metadata Statements

A set of metadata statements, together **describe an entity** are brought together using the metadata_statement parameter.

The following is a non-normative example of a compounded metadata statement. Also note that the **the metadata_statement MUST be a signed JWT**. In this example, the only the parts of the signed JWT payload pertinent to the example are shown.[1]

```
{
  "redirect_uris": ["https://example.com/rp1"],
  "metadata_statements": [
    {
      "scope": "openid eduperson",
      "response_types": ["code"],
      "metadata_statements" : [
        {
          "contacts": ["dev_admin@example.com"],
          "logo_uri": "https://example.com/logo.jpg",
          "policy_uri": "https://example.com/policy.html",
          "tos_uri": "https://example.com/tos.html"
        }
      ]
    }
  ]
}
```

[1] openid-connect-federation-1_0

OpenID Connect Federation - Trust model

The **trust model** is based on **linking together signing keys**, referred to in the metadata statements and represented as JWK Sets [RFC7517]. **Each signature chain is rooted in the trusted third party's signing keys**. By verifying such signature chains, the entities can establish trust in the metadata.[1]

trusted third party --> Federation Operator

[1] openid-connect-federation-1_0

Links

- OpenID Connect Federation 1.0 - draft 01
  http://openid.net/specs/openid-connect-federation-1_0.html

- Fedoidc - Test Implementation
  https://github.com/OpenIDC/fedoidc/

- GN4-2 JRA3 T3.1A OpenID Connect Federation
  https://wiki.geant.org/display/gn42jra3/GN4-2+JRA3

Q&A

Thanks for your attention!