Building an Identity federation using OpenID Connect

Roland Hedberg@TNC16, Prague

According to Wikipedia

- A **federation** (information technology) is a group of computing or network providers agreeing upon standards of operation in a collective fashion.

- The term "**identity federation**" is by design a generic term, and is not bound to any one specific protocol, technology, implementation or company. One thing that is consistent, however, is the fact that "federation" describes methods of identity portability which are achieved in an open, often standards-based manner – meaning anyone adhering to the open specification or standard can achieve the full spectrum of use-cases and interoperability.

What to expect from a federation ?

- Trust fabric
- Enforced policies

OIDC facilities useful in a federation context

- Dynamic server configuration discovery
- Dynamic client registration
- Support for key roll-over
- Information (JWT) signing/encryption

Building trust fabric (sort of PKI)

- Chain of signed keys

- Signing keys belonging to an entity are represented as a JWK Set

- A JWK Set if packed into a JWT which is signed by an entity higher up in the chain.

- The federation operator is the root of the trust chain

Signed Jason Web Token (JWS) basics

- 3 base64encoded parts separated by '.'

  1. Header

  2. Message body

  3. Signature

Players

Federation Operator

- RP Owner (RPO)
- RP Administrator (RPA)
- RP

- OP Owner (OPO)
- OP Administrator (OPA)
- OP

RPO Request

```
{
  "contacts": [
    "dev_admin@example.com"
  ],
  "logo_uri": "https://example.com/logo.jpg",
  "policy_uri": "https://example.com/policy.html",
  "signing_key": {
    "e": "AQAB",
    "kid": "1vjOgVk9D2KxBj0sJsaRUpa04_n3Ociu16d0jjTwE6M",
    "kty": "RSA",
    "n": "nugdp2hmgtZV5K26EecYLqeB5_iiyDkqFlGixtC1_twZdKxfq90f_YX2hcL9
AhimU7lJD5NEVRlfO2Jt7ozaw_2Nf9su4uu_5D9NA6uqseSinLKrBE7qBkVuDjsRWeOijT
3HBuvq170L8HEFagGl6KCfJwqrkCaKQFXBVeXqkL4XzYBkRopLs2Y9CI6z7ezym63e4F-F
o2Ghe-iQ0U_ULYlc0L52Pvi9E3sLO2eP_TDc-3fqRN2hOhvJhQtRTm8puTgR59HwkLU-gn
-9epZE9gBf5icgEsfaPmb3fruNIrATWqWEGV8HnSBQbMI_tfEQMqEAZ123K6zZGY0SsPcx
zQ",
    "use": "sig"
  },
  "tos_uri": "https://example.com/tos.html"
}
```

RPO Software statement

```
{
  "contacts": ["dev_admin@example.com"],
  "exp": 1465849214,
  "iat": 1465849214,
  "iss": "https://swamid.sunet.se/",
  "jti": "606ca2e2a6e8434bbe13083044d714a2",
  "kid": "sjZwsrAG1AoVx-3TDUVC3_9OolCmdpVgMRiPEM7hJvE",
  "logo_uri": "https://example.com/logo.jpg",
  "policy_uri": "https://example.com/policy.html",
  "response_types": [”code", "code id_token”, "token"],
  "scopes": ["openid","email","phone"],
  "signing_key": {
    "e": "AQAB",
    "kid": "1vjOgVk9D2KxBj0sJsaRUpa04_n3Ociu16d0jjTwE6M",
    "kty": "RSA",
    "n": "nugdp2hmgtZV5K26EecYLqeB5_iiyDkqFlGixtC1_twZdKxfq90f_YX2hcL9
AhimU7lJD5NEVRlfO2Jt7ozaw_2Nf9su4uu_5D9NA6uqseSinLKrBE7qBkVuDjsRWeOijT
3HBuvq170L8HEFagGl6KCfJwqrkCaKQFXBVeXqkL4XzYBkRopLs2Y9CI6z7ezym63e4F-F
o2Ghe-iQ0U_ULYlc0L52Pvi9E3sLO2eP_TDc-3fqRN2hOhvJhQtRTm8puTgR59HwkLU-gn
-9epZE9gBf5icgEsfaPmb3fruNIrATWqWEGV8HnSBQbMI_tfEQMqEAZ123K6zZGY0SsPcx
zQ",
    "use": "sig"
  },
  "token_endpoint_auth_method": "private_key_jwt",
  "tos_uri": "https://example.com/tos.html"
}
```

’Russian doll’ #1

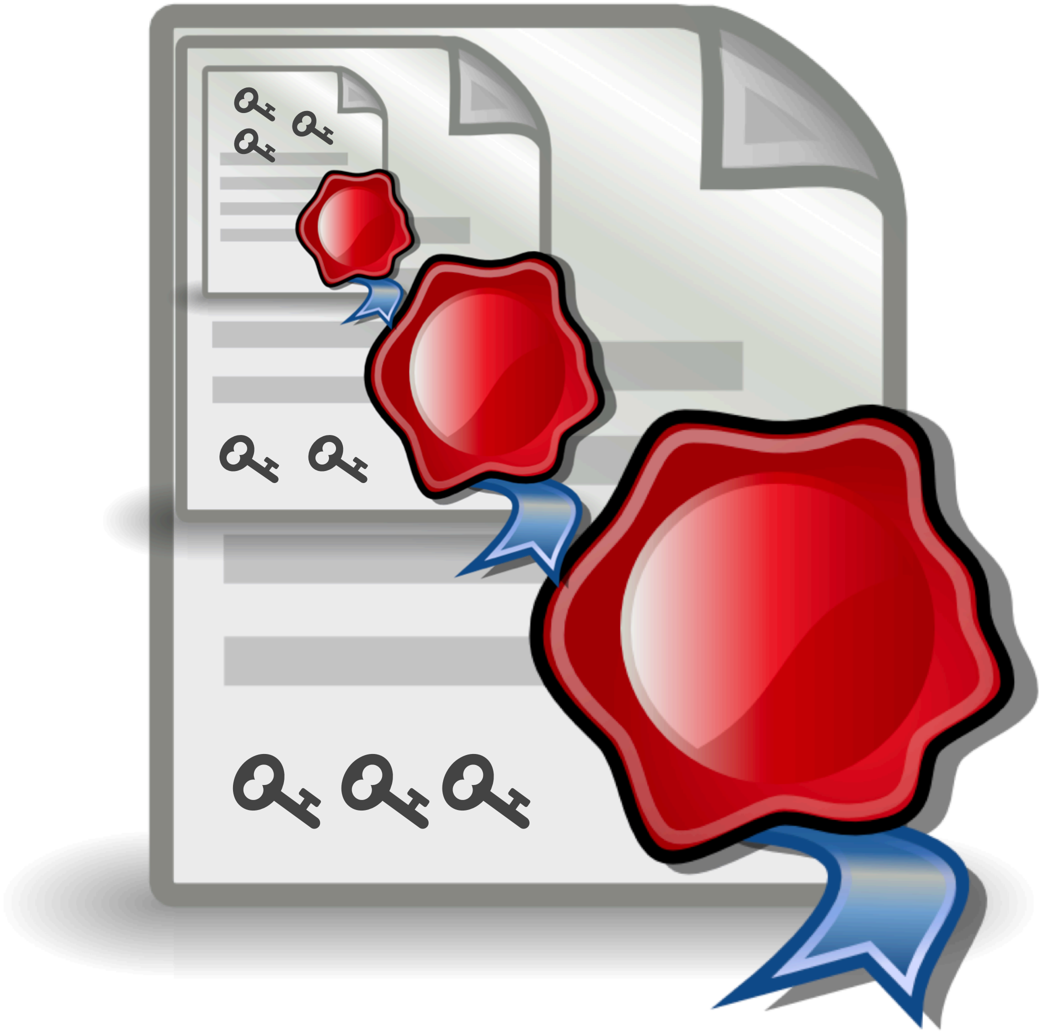
RPO request (FO sig)

’Russian doll’ #2

RPA request (RPO sig)

’Russian doll’ #3

RP request (RPA sig)



Enforcing behavior policy - OP

- scopes_supported
- response_types_supported
- subject_types_supported
- token_endpoint_authn_methods_supported
- claims_supported
- id_token_signing_alg_values_supported

Enforcing behavior - RP

- response_types
- subject_type
- id_token_signed_response_alg
- token_endpoint_auth_method
- default_max_age
- *’allowed_scopes’*
- *’allowed_claims’*

A child can register less or equal to what a parent has allowed.

scopes_supported in OP provider configuration response

Federation Operator	**openid,** profile, email, phone, address, offline_access
OP operator	**openid,** email, phone, offline_access
OP	**openid,** email, address

So what have we gained/can we gain ?

- Complete independence of transport protocol for message security.

- The federation can allow the operators to spin up new instances of RPs/OPs without involving the FO.

- Federation policy can be enforced.

If you want to be part of the discussion

Last version of the draft:

https://github.com/rohe/pyoidc/blob/master/oidc_fed/oidcfed.txt

Mailing lists:

oidc@lists.geant.org

openid-specs-ab@lists.openid.net