How to model Policy Frameworks into OIDC?

Davide Vaghetti (GARR)
GÉANT OIDCFed Team (GN4-2 JRA3 Task 3 1.A)

TNC2018
Trondheim, June 14th, 2018

Target

OIDC entities should be able to signal compliance to and support for policy frameworks.

~~Five Ws and~~ How

~~**W**ho? *many actors*~~

~~**W**hat? *isn't it OIDC policy framework support signaling?*~~

~~**W**here? *many places as well*~~

~~**W**hen? *ASAP!*~~

~~**W**hy? *do we really want or need to answer this one?*~~

How?

Policy frameworks and requirements

REFEDS R&S Entity Category https://refeds.org/research-and-scholarship

- Metadata requirements: Tagging only.
- In band requirements: none.

REFEDS Sirtfi https://refeds.org/sirtfi

- Metadata requirements: Tagging and security contact.
- In band requirements: none.

GÉANT Data Protection Code of Conduct https://wiki.refeds.org/x/MIAY

- Metadata requirements: Tagging, UI, Privacy Policy and required attributes.
- In band requirements: none.

Signaling compliance and support

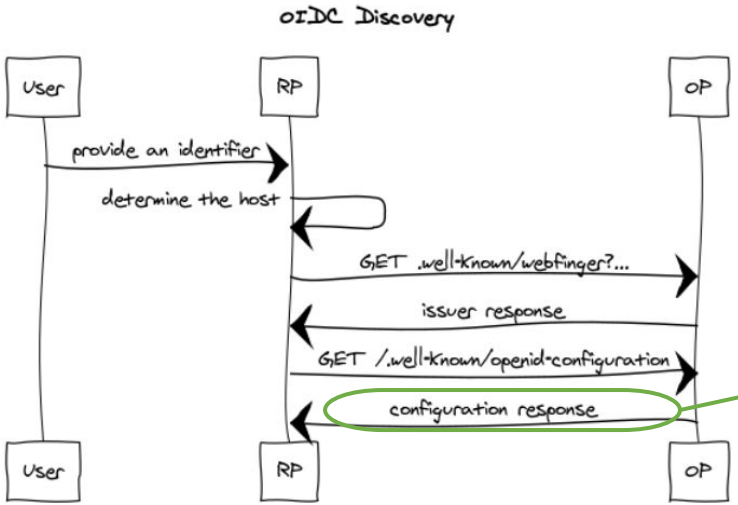
Metadata tagging: In SAML R&E Identity Federations, compliance to and support for policy frameworks is signalled through entity metadata tagging (extension or attribute).

Trust anchor: The trust anchor is the Federation Operator.

Signature: The trust is enforced through metadata signing.

OpenID Connect Provider metadata

*OPs metadata (openid-configuration) are sent **in band** through the OIDC discovery*




```
{
   "issuer":
     "https://server.example.com",
   "authorization_endpoint":
     "https://server.example.com/connect/authorize",
   "token_endpoint":
     "https://server.example.com/connect/token",
    [..]
   "op_policy_uri":
     "https://server.example.com/op_policy",
   "op_tos_uri":
     "https://server.example.com/op_tos"
}
```

OIDC OPs metadata claims for policy

op_policy_uri

URL that the OpenID Provider provides to the person registering the Client to read about the OP's requirements on how the Relying Party can use the data provided by the OP. The registration process SHOULD display this URL to the person registering the Client if it is given.

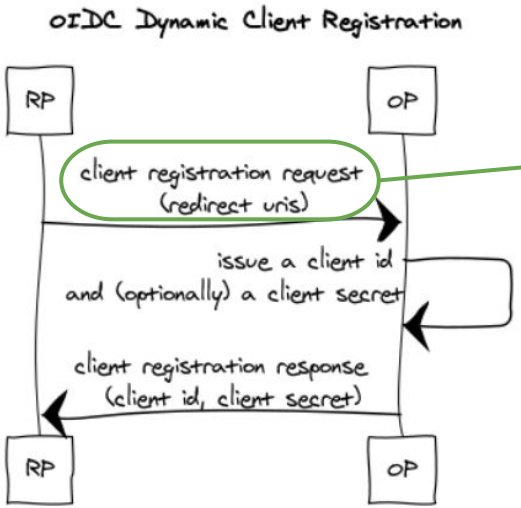
op_tos_uri

URL that the OpenID Provider provides to the person registering the Client to read about OpenID Provider's terms of service. The registration process SHOULD display this URL to the person registering the Client if it is given.

https://openid.net/specs/openid-connect-discovery-1_0.html

OpenID Connect Client metadata

*Clients metadata are sent **in band** as a client registration request*




```
{
    "application_type": "web",
    "redirect_uris":
      ["https://client.example.org/callback",
       "https://client.example.org/callback2"],
    [..]
    "contacts":
       ["info@example.org",
        "helpdesk@example.org"],
    "policy_uri":
      "https://client.example.com/policy",
    "tos_uri":
      "https://client.example.com/tos"
}
```

OIDC clients metadata claims for policy

policy_uri

URL that the Relying Party Client provides to the End-User to read about the how the profile data will be used. The value of this field MUST point to a valid web page. The OpenID Provider SHOULD display this URL to the End-User if it is given [..]

tos_uri

URL that the Relying Party Client provides to the End-User to read about the Relying Party's terms of service. The value of this field MUST point to a valid web page. The OpenID Provider SHOULD display this URL to the End-User if it is given [..]

https://openid.net/specs/openid-connect-registration-1_0.html

OIDC OPs and clients metadata

Metadata tagging

OP's op_policy_uri and op_tos_uri as well as client's policy_uri and tos_uri are not array, they cannot be overloaded.
-> Possible solution: craft a new claim like policy_framework_uris?

Trust anchor and signature

OIDC Federation metadata statements

The standard allow for multiple metadata statements, so the trust anchor can be the Federation or another party as well (independent authorities)

Policy frameworks and OIDC

REFEDS R&S Entity Category

- support/compliance (symmetric): new metadata claim (policy_frameworks?)

REFEDS Sirtfi

- compliance: new metadata claim (policy_frameworks?)
- security contact:
  - **[ISSUE]** *no contacts claims for OP and contacts for clients is an array*
  - **[SOLUTION]** *a new claim? security_contact?*

GÉANT Data Protection Code of Conduct

- support/compliance (symmetric): new metadata claim (policy_frameworks?)
- privacy policy: op_policy_uri
- required attributes:
  - **[ISSUE]** *no standard claim to signal them in the metadata*
  - **[SOLUTION]** *new claims? required_claims/required_scopes?*

Let’s start the discussion

Davide Vaghetti
davide.vaghetti@garr.it

GÉANT
Networks · Services · People
www.geant.org

This work is part of a project that has applied for funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).