

Kantara OTTO

Open **T**rusted **T**axonomy for federation **O**perators

<https://github.com/kantarainitiative/wg-otto>

What problem does OTTO Solve?

1. Leverage the federation trust model for OAuth protocols
2. Reduce duplication of data during inter-federation
3. Make federation metadata more searchable
4. Define common data model to generically describe federation stuff
5. API's to standardize entity-to-federation communication
6. Support OpenID and SAML first, but allow for extension
7. Simple, extensible, open and interoperable...

We talked to a lot of federation experts...

- Leif Johansson

- “The biggest problem is not that we haven't deployed MDQ. The biggest problem is the aggregator-aggregator communication is too slow, too cumbersome, doesn't scale well. Need an asynchronous update mechanism... the problem of who talks to who, and how and what are the data types are incidental.”

- Ian Young, co-author of MDQ

- “Exchanging metadata is analogous to DNS v. hosts files. But DNS is small--just an IP address--whereas the average SAML IDP metadata is 7k, and some may contain multiple certificates.”

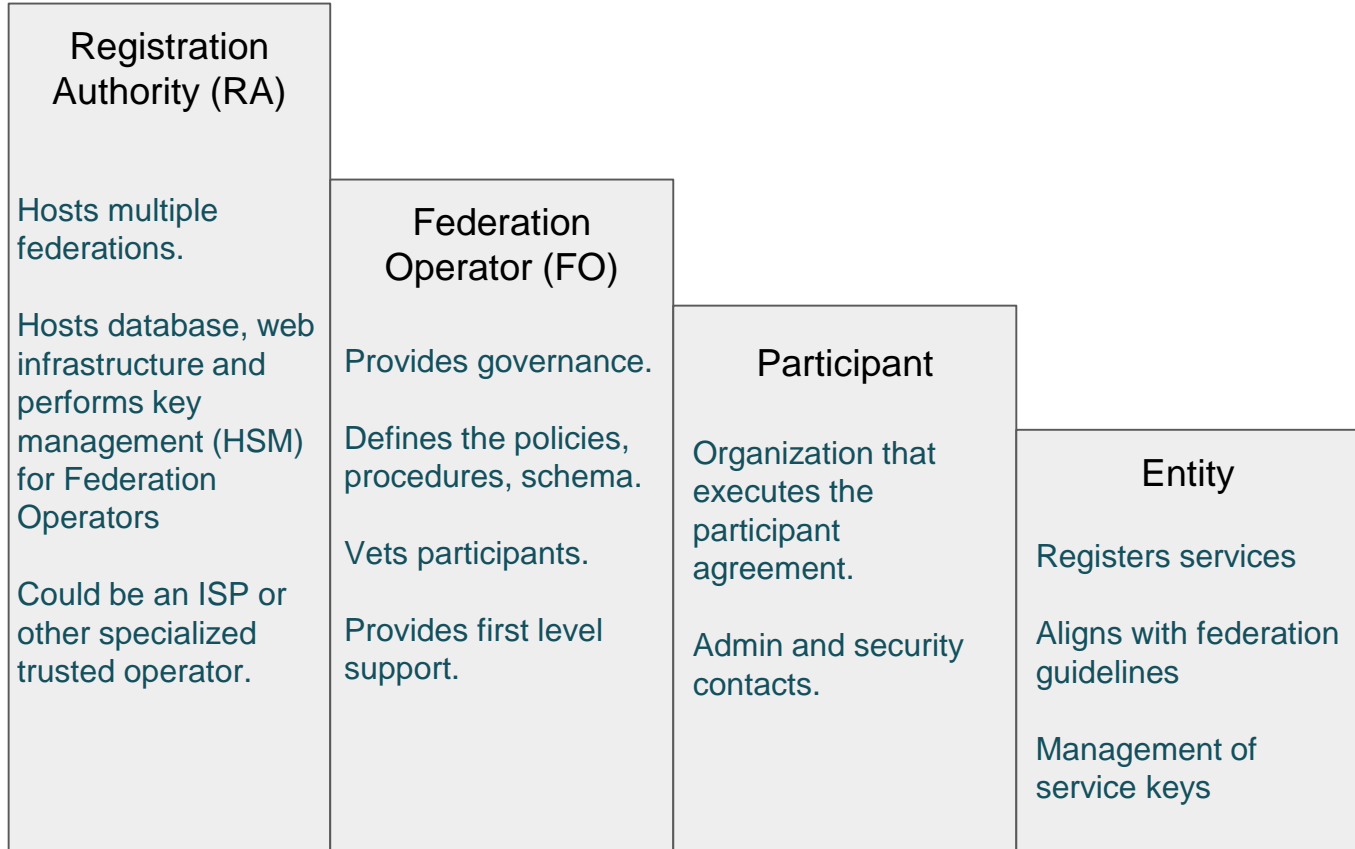
- Roland Hedberg, co-author OpenID Connect federation

- “One of the unique approaches of this federation draft is the use of "metadata statements", which include information about a federation participant, and the services it offers.”

- Rhys Smith, JISC Federation API developer

- “Automation is needed by a larger federation, and especially by participants who manage many entities. If a participant needs to update 300 certificates, it can be a challenge for both the member and the federation. An automated process to perform this task would be more accurate and less expensive.”

OTTO Federation Actors



OTTO API endpoints

- Configuration endpoint `.well-known/otto-configuration`
- Federation endpoint
- Participant endpoint
- Entity endpoint
- Metadata endpoint
- Schema endpoint

JSON-LD vocabulary

CORE

- Registration Authority
- Federation
- Participant
- Entity
- Schema
- Metadata

OpenID

- OpenID Provider
- OpenID RP
- User Claim
- Scope
- Metadata Statement
- Categories

SAML

- Saml Entity
- Entity Descriptor
- SP
- IDP
- Attribute Authority

```
{  
  "@id": "openid:OpenIDProvider",  
  "@type": "rdfs:Class",  
  "rdfs:subClassOf":  
    {  
      |   "@id": "otto:Entity"  
    }  
},
```

More info

API standard

<https://gluu.co/otto-api>

Core Vocab

<https://gluu.co/otto-vocab>

OpenID Vocab

<https://gluu.co/otto-openid>

SAML Vocab

<https://gluu.co/otto-saml>

Github Code

<https://github.com/GluuFederation/otto-node>

Swagger-UI

<http://otto-test.gluu.org/swagger>

::
:
:
:
:
::