Proof of concept - JWT Federations

Notice: *This is experimental proof of concept software used to experiment and learn about building trust between OpenID Connect and OAuth entities. Can not be used for any production systems.*

JWTFed is a Node.js library that implements creating and signing entity statements, validation of entity statements, validation of trust chains, Webfinger client fetching entity statements, resolving protocol specific metadata and more.

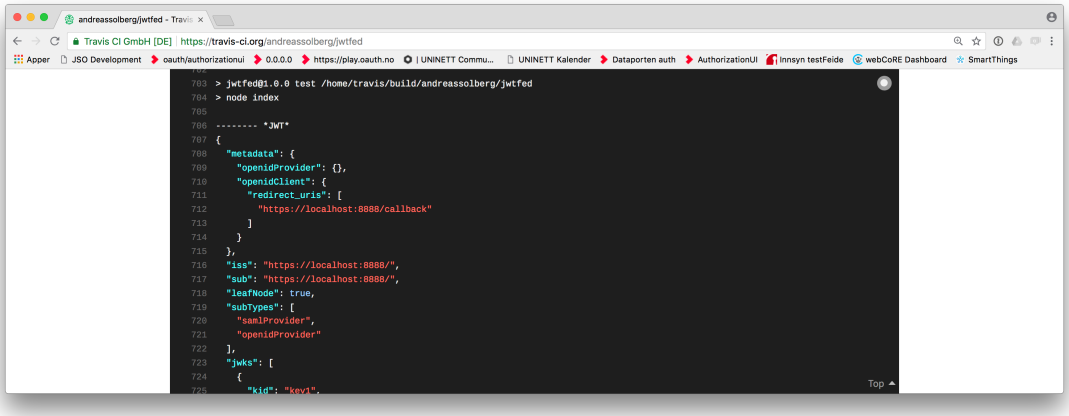
- jwtfed at github (https://github.com/andreassolberg/jwtfed)
- jwtfed NPM package (https://www.npmjs.com/package/jwtfed)

There is a demo script that generates a chain of entity statements and then validates it.

- Look at the demo script output at Travis CI (https://travis-ci.org/andreassolberg/jwtfed)

JWTserver is a Node.js server that can act as a federation issuing statements about clients, providers or other federations. It also implements the WebFinger lookup points needed for both clients and providers to serve their own metadata.

- jwtserver at github (https://github.com/andreassolberg/jwtserver)
- jwtserver docker image at docker hub (https://hub.docker.com/r/andreassolberg/jwtserver/)
- Kubernetes configuration for 4 demo entities (https://github.com/andreassolberg/jwtserver/blob/master/deployment.yaml)



Demo deployment

Here are a few entities that is currently running and can be used for experimentation and demoing.

```
https://serviceprovider.andreas.labs.uninett.no/application1007
https://ntnu.andreas.labs.uninett.no/
https://feide.andreas.labs.uninett.no/jwtfederation
https://edugain.andreas.labs.uninett.no/openid
```

Copy

Copy

Self issued statement from serviceprovider

- WebFinger request to get self issued statement
  - https://serviceprovider.andreas.labs.uninett.no/.well-known/webfinger?rel=http://oauth.net/specs/federation/1.0/entity&resource=https%3A%2F%2Fserviceprovider.andreas.labs.uninett.no%2Fapplication1007 (https://serviceprovider.andreas.labs.uninett.no/.well-known/webfinger?rel=http://oauth.net/specs/federation/1.0/entity&resource=https%3A%2F%2Fserviceprovider.andreas.labs.uninett.no%2Fapplication1007)
- Referred signed JWT
  - https://serviceprovider.andreas.labs.uninett.no/federation-api/entitystatements?entity=https%3A%2F%2Fserviceprovider.andreas.labs.uninett.no%2Fapplication1007 (https://serviceprovider.andreas.labs.uninett.no/federation-api/entitystatements?entity=https%3A%2F%2Fserviceprovider.andreas.labs.uninett.no%2Fapplication1007)
- Decoded version of the JWT
  - https://serviceprovider.andreas.labs.uninett.no/federation-api/entitystatements?entity=https%3A%2F%2Fserviceprovider.andreas.labs.uninett.no%2Fapplication1007&decoded=1 (https://serviceprovider.andreas.labs.uninett.no/federation-api/entitystatements?entity=https%3A%2F%2Fserviceprovider.andreas.labs.uninett.no%2Fapplication1007&decoded=1)

NTNU issues statement about serviceprovider

- WebFinger request to get self issued statement
  - https://ntnu.andreas.labs.uninett.no/.well-known/webfinger?rel=http://oauth.net/specs/federation/1.0/entity&resource=https%3A%2F%2Fserviceprovider.andreas.labs.uninett.no%2Fapplication1007 (https://ntnu.andreas.labs.uninett.no/.well-known/webfinger?rel=http://oauth.net/specs/federation/1.0/entity&resource=https%3A%2F%2Fserviceprovider.andreas.labs.uninett.no%2Fapplication1007)
- Referred signed JWT
  - https://ntnu.andreas.labs.uninett.no/federation-api/entitystatements?

entity=https%3A%2F%2Fserviceprovider.andreas.labs.uninett.no%2Fapplication1007
(https://ntnu.andreas.labs.uninett.no/federation-api/entitystatements?
entity=https%3A%2F%2Fserviceprovider.andreas.labs.uninett.no%2Fapplication1007)

- Decoded version of the JWT
  - https://ntnu.andreas.labs.uninett.no/federation-api/entitystatements?
    entity=https%3A%2F%2Fserviceprovider.andreas.labs.uninett.no%2Fapplication1007&decoded=1
    (https://ntnu.andreas.labs.uninett.no/federation-api/entitystatements?
    entity=https%3A%2F%2Fserviceprovider.andreas.labs.uninett.no%2Fapplication1007&decoded=1)

Feide issues statement about NTNU

- WebFinger request to get self issued statement
  - https://feide.andreas.labs.uninett.no/.well-known/webfinger?
    rel=http://oauth.net/specs/federation/1.0/entity&resource=https%3A%2F%2Fntnu.andreas.labs.uninett.no%2F
    (https://feide.andreas.labs.uninett.no/.well-known/webfinger?
    rel=http://oauth.net/specs/federation/1.0/entity&resource=https%3A%2F%2Fntnu.andreas.labs.uninett.no%2F)
- Referred signed JWT
  - https://feide.andreas.labs.uninett.no/federation-api/entitystatements?
    entity=https%3A%2F%2Fntnu.andreas.labs.uninett.no%2F (https://feide.andreas.labs.uninett.no/federation-
    api/entitystatements?entity=https%3A%2F%2Fntnu.andreas.labs.uninett.no%2F)
- Decoded version of the JWT
  - https://feide.andreas.labs.uninett.no/federation-api/entitystatements?
    entity=https%3A%2F%2Fntnu.andreas.labs.uninett.no%2F&decoded=1 (https://feide.andreas.labs.uninett.no/federation-
    api/entitystatements?entity=https%3A%2F%2Fntnu.andreas.labs.uninett.no%2F&decoded=1)

eduGAIN issues statement about Feide

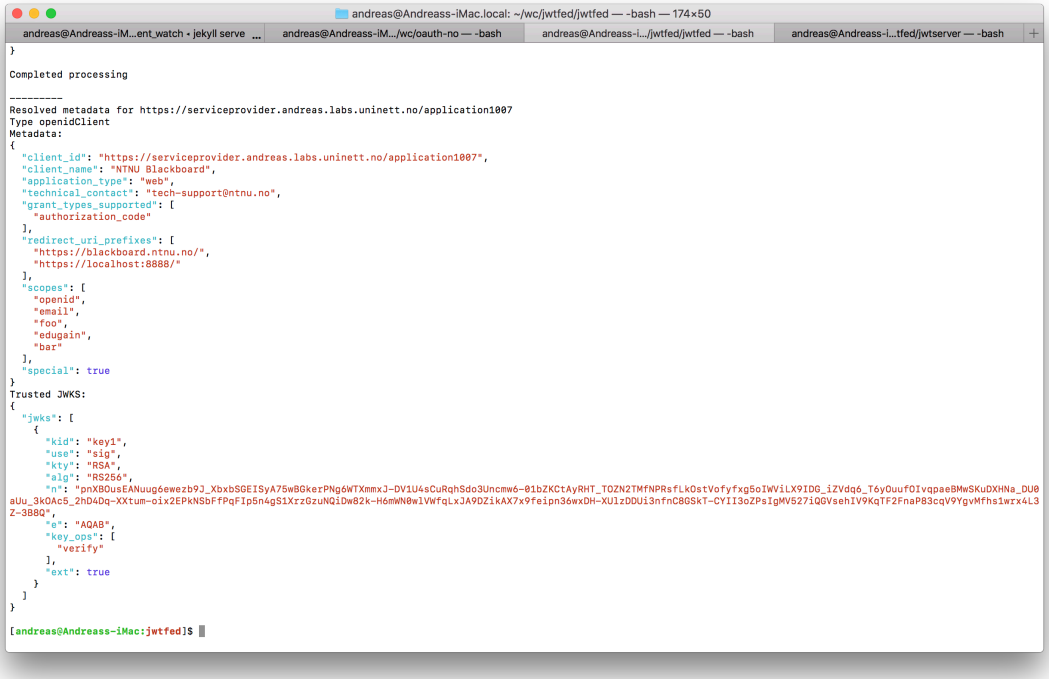
- WebFinger request to get self issued statement
  - https://edugain.andreas.labs.uninett.no/.well-known/webfinger?
    rel=http://oauth.net/specs/federation/1.0/entity&resource=https%3A%2F%2Ffeide.andreas.labs.uninett.no%2Fjwtfederation
    (https://edugain.andreas.labs.uninett.no/.well-known/webfinger?
    rel=http://oauth.net/specs/federation/1.0/entity&resource=https%3A%2F%2Ffeide.andreas.labs.uninett.no%2Fjwtfederation)
- Referred signed JWT
  - https://edugain.andreas.labs.uninett.no/federation-api/entitystatements?
    entity=https%3A%2F%2Ffeide.andreas.labs.uninett.no%2Fjwtfederation
    (https://edugain.andreas.labs.uninett.no/federation-api/entitystatements?
    entity=https%3A%2F%2Ffeide.andreas.labs.uninett.no%2Fjwtfederation)
- Decoded version of the JWT
  - https://edugain.andreas.labs.uninett.no/federation-api/entitystatements?
    entity=https%3A%2F%2Ffeide.andreas.labs.uninett.no%2Fjwtfederation&decoded=1
    (https://edugain.andreas.labs.uninett.no/federation-api/entitystatements?
    entity=https%3A%2F%2Ffeide.andreas.labs.uninett.no%2Fjwtfederation&decoded=1)

Running a test

You can clone the jwtfed repository (https://github.com/andreassolberg/jwtfed) and run a CLI command to lookup the OpenID Connect Client metadata for our demo client, with a locally configured edugain trust root, like this:

```
clear; node lookup.js openidClient https://serviceprovider.andreas.labs.uninett.no/application1007
```

Copy Copy



OAuth.no · UNINETT AS (http://www.uninett.no) · Andreas Åkre Solberg (https://no.linkedin.com/in/andreassolberg) · erlang (https://twitter.com/@erlang)