

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>)

```

763 > jwtfed@1.9.0 test /home/travis/build/andreassolberg/jwtfed
764 > node index
765
766 ----- *JWT*
767 {
768   "metadata": {
769     "openidProvider": {},
770     "openIdClient": {
771       "redirect_uris": [
772         "https://localhost:8888/callback"
773       ]
774     }
775   },
776   "iss": "https://localhost:8888/",
777   "sub": "https://localhost:8888/",
778   "leafNode": true,
779   "subTypes": {
780     "samlProvider",
781     "openidProvider"
782   },
783   "jws": {
784     {
785       "kid": "key1",

```

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

```

[red] [green] [yellow] [blue] andreas@Andress-iMac.local: ~/wc/wtfed/jwtfed -- -bash -- 174x50
andreas@Andress-iMac-ent-watch : jekyll serve ... andreas@Andress-iMac:/wc/oauth-no -- -bash andreas@Andress-iMac:/wc/wtfed/jwtfed -- -bash andreas@Andress-iMac:/wc/wtfed/jwtserver -- -bash
}

Completed processing

-----
Resolved metadata for https://serviceprovider.andreas.labs.uninett.no/application1007
Type openidClient
Metadata:
{
  "client_id": "https://serviceprovider.andreas.labs.uninett.no/application1007",
  "client_name": "NTNU Blackboard",
  "application_type": "web",
  "technical_contact": "tech-support@ntnu.no",
  "grant_types_supported": [
    "authorization_code"
  ],
  "redirect_uri_prefixes": [
    "https://blackboard.ntnu.no/",
    "https://localhost:8888/"
  ],
  "scopes": [
    "openid",
    "email",
    "foo",
    "edugain",
    "bar"
  ],
  "special": true
}
Trusted JWKS:
{
  "jwks": [
    {
      "kid": "key1",
      "use": "sig",
      "alg": "RS256",
      "n": "pnXBOusEAnuq6ewezb9J_XbxbSGEIyA7SwB0kerPng0Wtmxx3-DV1U4sCuRqhSdo3Uncm6=81bZKCTAyRHt_TOZN2TMfNPnrSflk0StVoFYxg5oIWvIX9IDG_iZVdq6_T6yOuufQ1vpaaBMsKuDXHNa_DUaUu_3kOAcB_Zhd4Dq-XXtum-oixZEpkNSdFPpqIpsNagS1XrzGzuQNdW82k-H6mWN0w1VwfLxJA9DZ1kAX7x9epIn36wxDH-XUL0uz33nrcnCBOSkt-CYII3oZPs1gMW5Z7lQ0vseh1Dw9KqT2FnaPB3cqV9YgmFhs1wrzXLZ-3880",
      "e": "AQAB",
      "key_ops": [
        "verify"
      ]
    },
    {
      "ext": true
    }
  ]
}
}

[andreas@Andress-iMac:~]$

```