



## Federation Provider

Ömer M. Ilhan, TUB SNET

Mathias Slawik, TUB SNET

Usecases Hackathon, 15.11.2016



**H2020-ICT-644925 – CYCLONE**

**Complete Dynamic Multi-cloud Application Management**

# Federation Provider



Personal Open source Business Explore

Pricing Blog Support


This repository

Search

Sign in

Sign up

 [cyclone-project](#) / [cyclone-federation-provider](#)

 Watch

19


 Star

1

 Fork

0

 Code

 Issues 1

 Pull requests 0


 Projects 0

 Pulse

 Graphs

CYCLONE Federation Provider, based on RedHat Keycloak

 46 commits

 2 branches

 0 releases









 2 contributors

Branch: master ▾

New pull request

Find file

Clone or download ▾

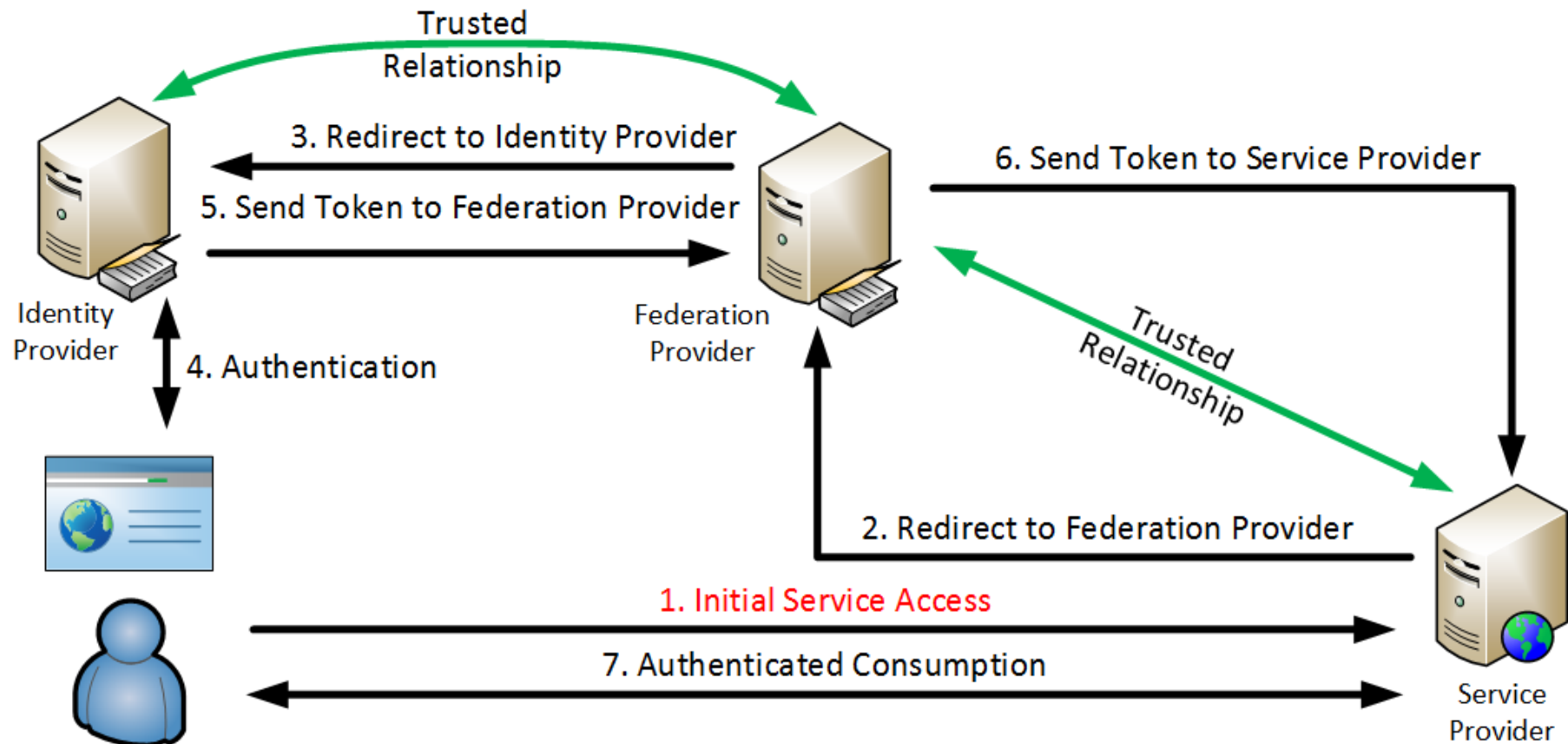
 omer-ilhan	add ids to eduPersonTargetedID filter, fix #3	Latest commit 555c5ec on 11 Oct
 components	add ids to eduPersonTargetedID filter, fix #3	a month ago
 data/keycloak/exports	extended configurability and added proper persistency	10 months ago
 docs	Add diagram of the architecture	7 months ago
 .gitignore	Add README and update gitignore to do not track database files	8 months ago
 README.md	Add diagram in README.md	7 months ago
 docker-compose.override.yml	add cron scripts through volumes	a month ago
 docker-compose.yml	split docker-compose.yml	a month ago

[github.com/cyclone-project/cyclone-federation-provider](https://github.com/cyclone-project/cyclone-federation-provider)

# Federation Provider

- open-source Components and standard protocols
  - Keycloak ([keycloak.org](https://keycloak.org))
  - OpenID-Connect ([openid.net/connect](https://openid.net/connect))
  - SimpleSamlPHP ([simplesamlphp.org](https://simplesamlphp.org))
  - SAML 2 ([oasis-open.org](https://oasis-open.org))

# Federation Provider



# OpenID Connect Authorization Code Flow

1. Client prepares an Authentication Request containing the desired request parameters.
2. Client sends the request to the Authorization Server.
3. Authorization Server Authenticates the End-User.
4. Authorization Server obtains End-User Consent/Authorization.
5. Authorization Server sends the End-User back to the Client with an Authorization Code.
6. Client requests a response using the Authorization Code at the Token Endpoint.
7. Client receives a response that contains an ID Token and Access Token in the response body.
8. Client validates the ID token and retrieves the End-User's Subject Identifier.

# JSON Web Token (JWT)

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ0eXAiOiJCZWFyZXIiLCJzdzWliOiIxMjM0NTY3ODkwIiwicHlwciJmVycmVkaX3VzZXJuYW1lIjoiaSm9obiBEb2UiLCJlbWFpbCI6ImouZG9lQGV4YW1wbGUub3JnIn0.CrYguTP4MZ3vcPzZgeUyRYu  
mbI7v236R8d\_gRTHgfiA

- Dot-separated
- Base64Url-encoded

## Header:

```
{  
  "alg": "HS256",  
  "typ": "JWT"  
}
```

## Payload:

```
{  
  "typ": "Bearer",  
  "sub": "1234567890",  
  "preferred_username": "John Doe",  
  "email": "j.doe@example.org"  
}
```

Signature: HMAC

- User visits protected resource
- Unauthenticated
- Redirect to Federation Provider

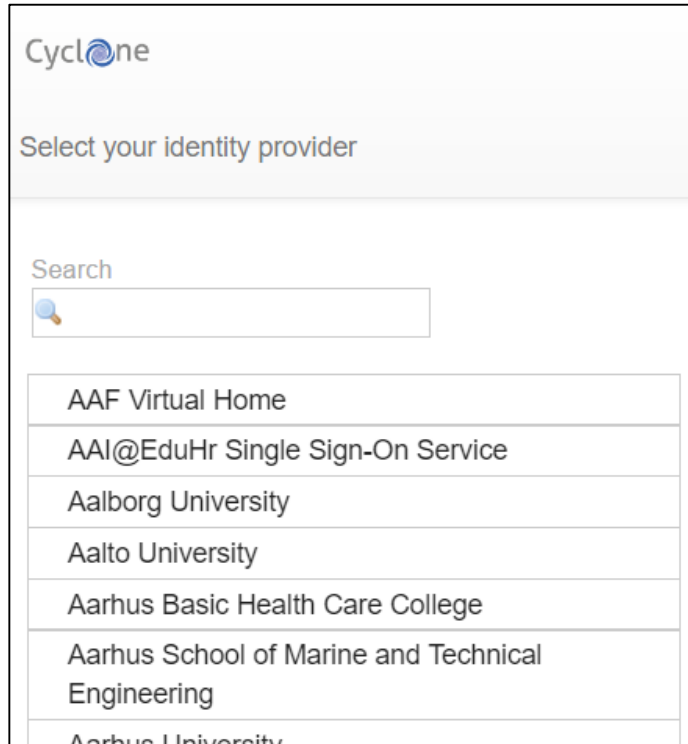
# Federation Provider

- Reachable at [federation.cyclone-project.eu](https://federation.cyclone-project.eu)
- Example Auth URL:  
federation.cyclone-project.eu  
/auth/realms/master  
/protocol/openid-connect  
/auth?  
client\_id=cnrs\_ifb  
&redirect\_uri=app/auth\_callback  
&response\_type=code





# Federation Provider



The screenshot shows the Cyclone Federation Provider selection interface. At the top, the Cyclone logo is displayed. Below it, the text "Select your identity provider" is shown. A search bar with a magnifying glass icon is present. Below the search bar, a list of identity providers is displayed, including AAF Virtual Home, AAI@EduHr Single Sign-On Service, Aalborg University, Aalto University, Aarhus Basic Health Care College, Aarhus School of Marine and Technical Engineering, and Aarhus University.

Cyclone

Select your identity provider

Search

AAF Virtual Home

AAI@EduHr Single Sign-On Service

Aalborg University

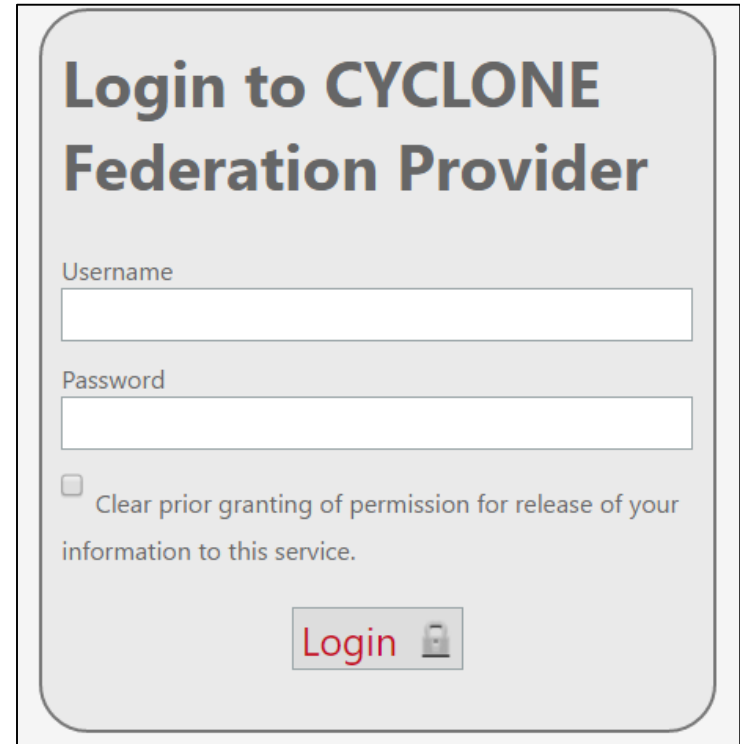
Aalto University

Aarhus Basic Health Care College

Aarhus School of Marine and Technical Engineering

Aarhus University

Select Home Institution



The screenshot shows the Cyclone Federation Provider login interface. At the top, the text "Login to CYCLONE Federation Provider" is displayed. Below this, there are input fields for "Username" and "Password". A checkbox labeled "Clear prior granting of permission for release of your information to this service." is present. At the bottom, there is a "Login" button with a lock icon.

Login to CYCLONE Federation Provider

Username


Password

☐ Clear prior granting of permission for release of your information to this service.


Login

Login at Home Institution IDP

- Ask for User Consent
- Return to redirect\_uri with code



FEDERATION PROVIDER



**CNRS IFB**

Do you grant these access privileges?

Personal Info: Full name, commonName, Given name, schacHomeOrganizationType, eduPersonScopedAffiliation, eduPersonTargetedID, mail, Username, Family name, Email

[CNRS IFB'S TERMS AND CONDITIONS](#)

# Federation Provider

- Application uses code to retrieve tokens

POST

/auth/realms/master/protocol/openid-connect/token

Content-Type:

application/x-www-form-urlencoded

grant\_type: authorization\_code

code: (code)

redirect\_uri: (redirect\_uri)

client\_id: (client\_id)

Response:

Response:

```
{  
  "access_token": (JWT),  
  "expires_in": (time),  
  "refresh_token": (JWT),  
  "refresh_expires_in": (time),  
  "token_type": "bearer",  
  "id_token": (JWT),  
  "not-before-policy": (policy),  
  "session-state": (session-state)  
}
```

# Federation Provider

- 3 JWTs: access, id & refresh\_token
- Attributes depend on the IDP
- Min. 1 identifying attribute, i.e. eduPersonUniqueID, eduPersonTargetedID, eduPersonPrincipalName or mail
- Keycloak OpenID-Connect Endpoints:  
[keycloak.gitbooks.io/securing-client-applications-guide/content/topics/oidc/oidc-generic.html](https://keycloak.gitbooks.io/securing-client-applications-guide/content/topics/oidc/oidc-generic.html)

# Federation Provider

- No need to reinvent the wheel, libraries are available
- Keycloak Client Adapters for  
Java (JBoss, Tomcat, Spring, ..), Javascript, NodeJS, ...
- mod\_auth\_openidc for Apache  
[github.com/pingidentity/mod\\_auth\\_openidc](https://github.com/pingidentity/mod_auth_openidc)
- And more: [openid.net/developers/libraries/](https://openid.net/developers/libraries/)

## Example: mod\_auth\_openidc

```
OIDCRedirectURI http://${HOSTIP}/example/redirect
OIDCCryptoPassphrase pass
OIDCClientID slipstream
OIDCClientSecret secret
OIDCProviderMetadataURL https://federation.
cyclone-project.eu/auth/realms/master/.well-
known/openid-configuration
```

```
<Location /example/>
  AuthType openid-connect
  Require valid-user
</Location>
```

More information and (code) examples on github

[github.com/cyclone-project](https://github.com/cyclone-project)

Thank you for your attention!

Questions?