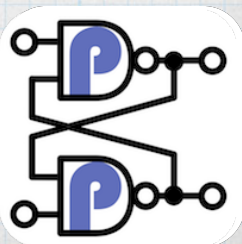


# Keycloak Workshop

Trust and Internet Identity Meeting Europe 2018

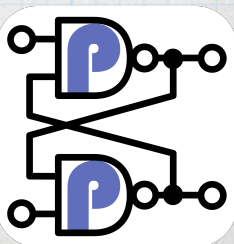
Peter Pfläging  
[pflaeging.net](http://pflaeging.net)  
[peter@pflaeging.net](mailto:peter@pflaeging.net)





# Agenda

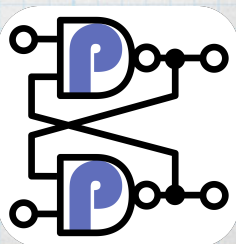
- \* What is Keycloak?
- \* Where to use?
- \* Usability
- \* Short demo, ...





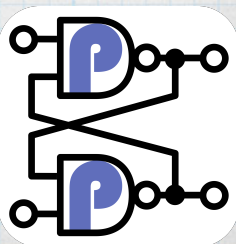
# Keycloak: Features

- \* Identity Provider
- \* Good protocol support
  - \* SAML2, OpenID-Connect, OAuth2
  - \* LDAP, Active Directory
- \* Themeable
- \* Social Login support
- \* Cascadable





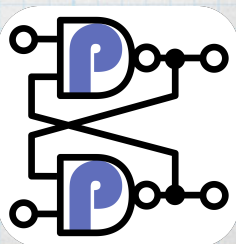
- \* Central Management through Web GUI or CMD line
- \* Clustering and HA
- \* Good workflow support
- \* Support for OTP build in
- \* Password policy support
- \* Security: break-in prevention





# Keycloak: Advantages

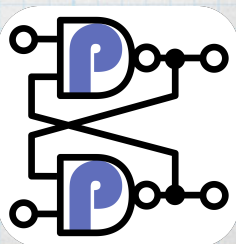
- \* Easy and fast install
- \* secure
- \* Configuration over programming
- \* Good protocol support
- \* Fairly good documented
- \* Deep rights management
- \* Multi tenant and instance support





# Keycloak: Disadvantages

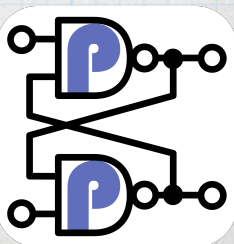
- \* Sometimes complex configuration
- \* Complex java programming if you hit the wall ;-)
- \* Rights management complex
- \* Theming not very comfortable
- \* Large universal product, ...





# Typical use case

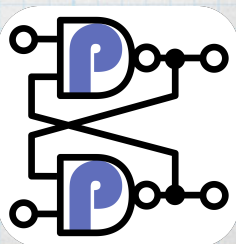
- \* Keycloak as IdP with LDAP or AD in Org.
- \* Keycloak in front of WebApps
- \* Keycloak as User integration platform





# Keycloak as IdP in Org.


- \* Fast setup with
  - \* LDAP
  - \* Kerberos
  - \* Active Directory
- \* Base for
  - \* other IdP's
  - \* Applications with OIDC, SAML2 or OAUTH2 support
  - \* Easy self service portal with workflows





# Example Login

id.fairkom.net



**E-Mail**

**Passwort**

[Passwort vergessen?](#)

☐ Angemeldet bleiben [Anmelden](#)

---

Noch keine fairlogin ID? [Registrieren](#)

Oder Anmeldung mit einem der folgenden ID Provider, sofern Sie diesen vertrauen und kein neues Passwort möchten.


[Sign in with Bürgerkarte Austria](#)

[More Social Identity Providers](#)

[Sign in with Google](#)

[Sign in with GitHub](#)

[Sign in with Twitter](#)

 Deutsch


fairlogin is provided  
by fairkom.eu



# Example App Dashboard


fairapps

Peter Pfläging




fairchat

fairchat is world's first fair and sustainable messenger. Read, create or join public groups.




GitLab

The swiss knife for agile sprints: git file repository, issue tracker, scrum board and wiki.




fairchat meet

Instant video chat for one or more participants. With chat, common writing board and screen sharing.




GroupOffice

The office in the cloud: Calendar, email, contacts and mail that syncs with your mobile.




ownCloud

Save and share your data safely and have access from any device.




board.net

Quick notes on the web, write simultaneously. The page name is your common password.



Sandstorm Apps


More webtools: Forms, Slides, Edit, Draw, Calc, Store, Ideation, ...

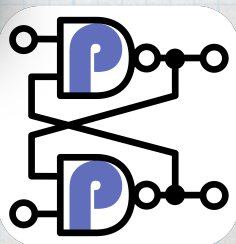


fairkom DokuWiki

Documentation on fairkom services.

Imprint. Powered by fairkom Gesellschaft.

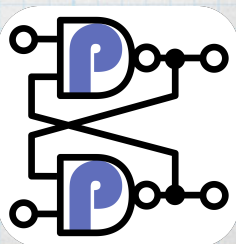
  
TIIME





# Keycloak in front of WebApps

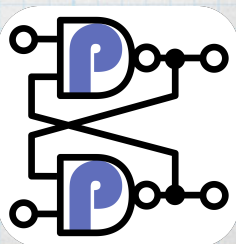
- \* Get the users out of the Apps
- \* Role & group management
- \* Attribute rewriting is very strong
- \* Support of different federations
  - Social and enterprise





# Keycloak as user integration platform

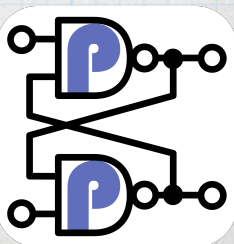
- \* Start with Keycloak early in dev or deployment
- \* Don't mess with local user-DB's
- \* Easy expand with new services
- \* —> Keycloak Workshop





# Demo: Flow

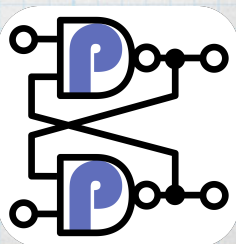
- \* Setup 2 Keycloak - infrastructures
- \* Deploy 2 Apps in Keycloak
- \* Deploy second Keycloak instance
- \* Connect the 2 instances





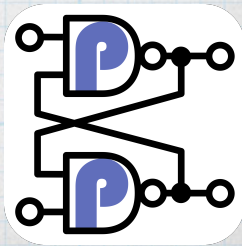
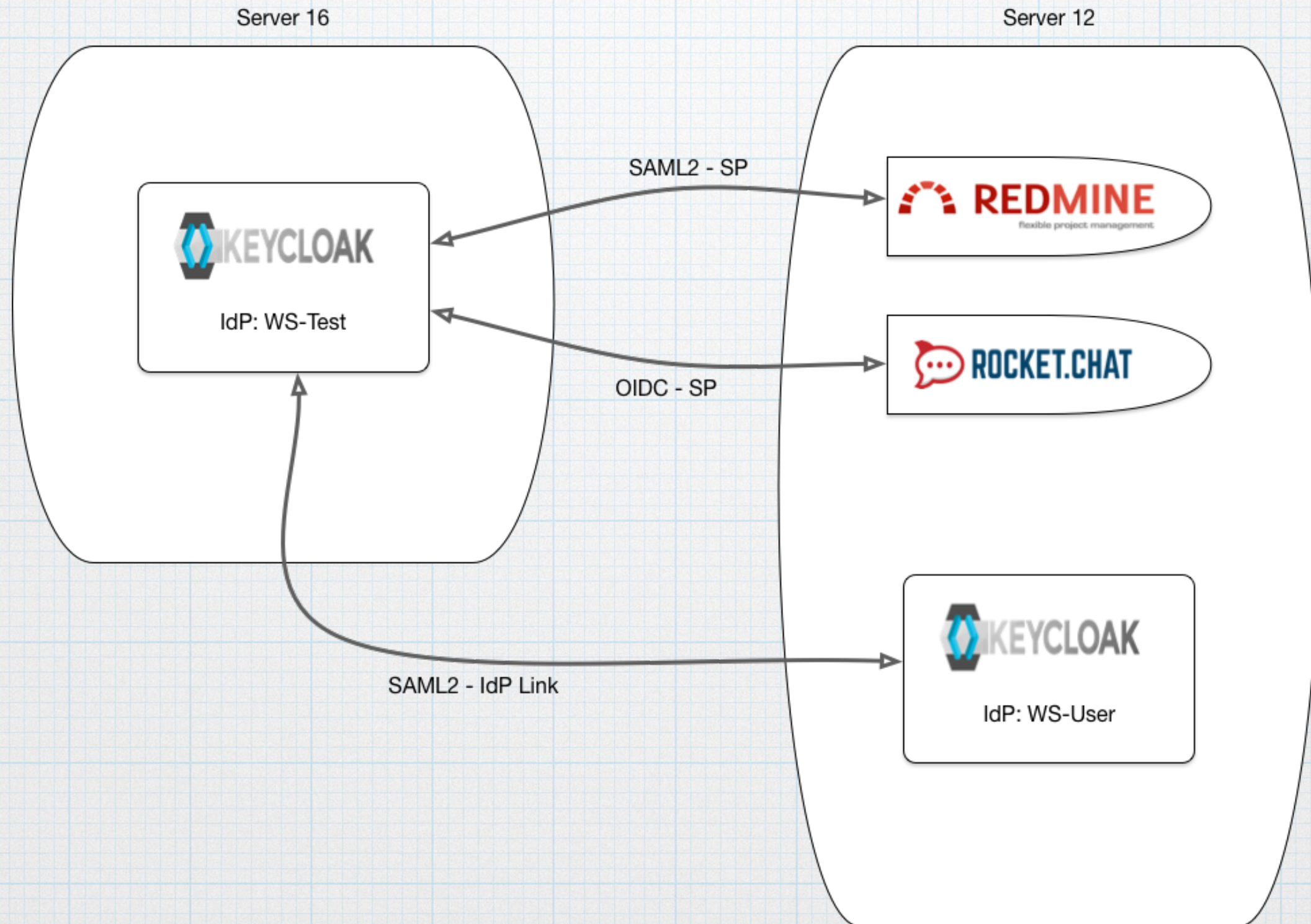
# Docker-Compose for Keycloak

- \* Required: docker & docker-compose
- \* Repo: <https://github.com/pflaeging/keycloak-ws>
- \* Complete Keycloak Environment
- \* „Nearly“ production ready ;-)



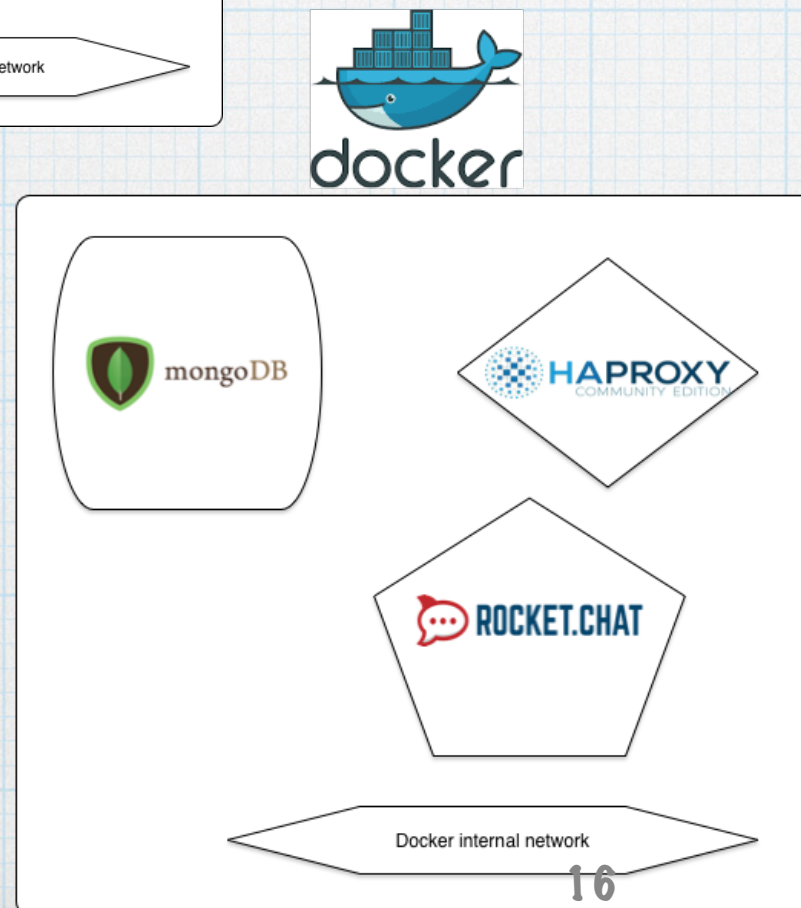
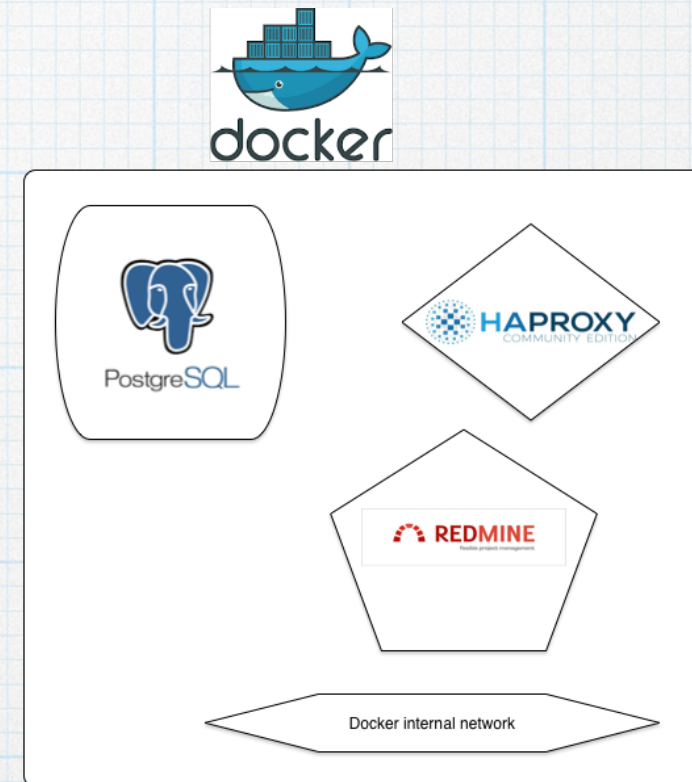
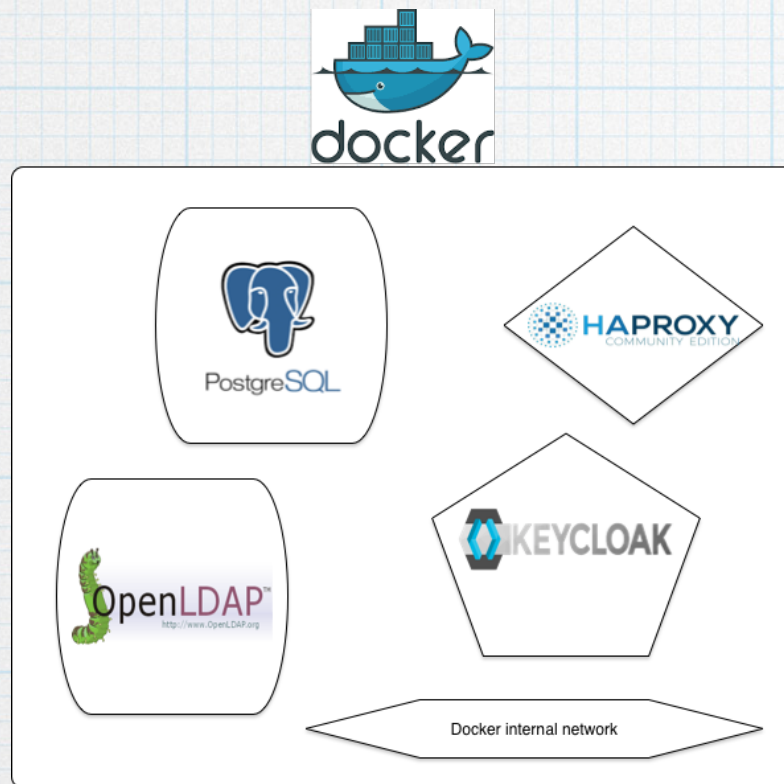


# Complete scenario





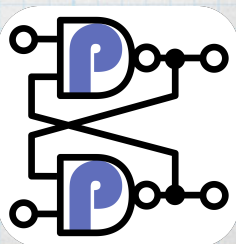
# Components





# Demo URLs

- \* Keycloak WS-Test (master)  
<https://server16.pflaeging.net:20443/auth>
- \* Rocket.Chat  
<https://server12.pflaeging.net:21443/home>
- \* Redmine with SAML2 plug-in  
<https://server12.pflaeging.net:22443/>
- \* Keycloak WS-User (second instance)  
<https://server12.pflaeging.net:20443/auth>





# Additional

- \* Repo: <https://github.com/pflaeging/keycloak-ws>
- \* Additional Tools:
  - \* Apache Directory Studio
  - \* Docker
  - \* Docker-compose
  - \* Portainer
  - \* SAML-tracer (Firefox)
  - \* SAML Message decoder (Chrome & Chromium)

