Keycloak

Dies ist die technische Anleitung primär zum Einbinden neuer Dienste. Suchst Du vielleicht die Anleitungen/Single Sign-On?

Keycloak

Keycloak ist eine Identity Management Software, in Java geschrieben. Wir setzen sie seit August 2025 auf auth.ping.de ein.

Deployed als docker container auf hafen. Für die User aus der Ping- und Prima-Mitglieder Datenbank haben wir den Realm PING angelegt.

Der Datenexport aus den Datenbanken erfolgt über Perl-Scripte, die hier auch mal dokumentiert werden sollten.

Unter der URL https://auth.ping.de/realms/PING/account können Mitglieder z.B. 2FA konfigurieren.

Es gibt in dem Realm zwei Gruppen "ping" und "prima", so dass gewisse Dienste auf diese Gruppen eingeschränkt werden können (wenn Daten nicht existieren für alle User u.s.w.).

Neue Anwendung zu Keycloak hinzufügen

Wenn man dann eine Software hat, die sich via OIDC an ein Single Sign-on dranflanschen lässt, dann geht das wie folgt:

1. Im Keycloak **im Realm PING** einen neuen Client anlegen.
   Meist findet man eine Anleitung, welche Parameter dabei zu beachten sind.
   Vermutlich wollt ihr unter "capability config" den Punkt "client authentication" einschalten.
   Darum geht es schließlich.
   Tragt auch die richtige URL des Clients unter *Root URL* ein.

2. Nachdem ihr den Client angelegt habt, findet ihr in dessen *Client details* unter *Credentials* das *Client secret*. Das braucht ihr für die Anwendung, die angebunden werden soll.
3. In der Anwendung könnt ihr bei der Konfiguration des OIDC vielleicht den Erkennungsendpunkt angeben. Der lautet

   https://auth.ping.de/realms/PING/.well-known/openid-configuration

Gruppen aus Keycloak in der Anwendung

Wenn ihr jetzt noch Rollen für besondere Berechtigungen vom Keycloak in eure Anwendung übernehmen wollt, dann könnt ihr im Keycloak noch Client Roles definieren, Usern diese zuweisen und dann in einem *Client scope* für den Client die Rollen mappen. Dazu legt ihr einen *token mapper* vom Typ *user client roles* an. Dort ist vermutlich die Checkbox "Add to ID token" wichtig, also aktiviert die.

Viel Erfolg.

Im Keycloak konfigurierte Dienste:

- conf.ping.de BigBlueButton greenlight-v3 UI 2026-04
- wiki.ping.de Bookstack 2026-03
- poz.ping.de wordpress 2026-04
- weiterbildung.ping.de wordpress 2026-04
- matrix anmeldung 2026-03
- code.ping.de forgejo git repo
- milla apache geschützter Bereich 2026-03
- cloud.ping.de nextcloud
- ki.ping.de open-webui

Revision #2
Created 2026-01-31 17:05:11 UTC by Daniel Hess
Updated 2026-04-20 20:33:29 UTC by Sven Neuhaus