



Single Sign-On (SSO)

Daniel Högerle, Jannik Pongratz, Lukas Butscher



Inhalt

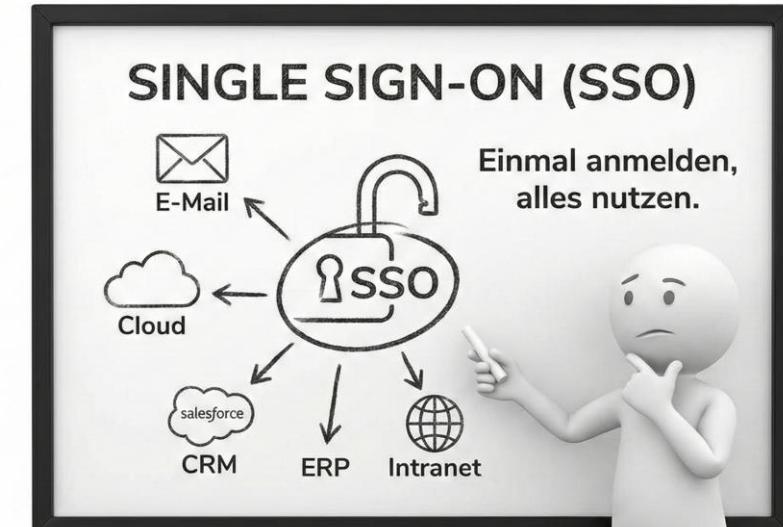
- 1) Überblick: Single Sign-On**
- 2) Nutzen von Single Sign-On**
- 3) Zielsetzung**
- 4) Umsetzung & Projektmethode**
- 5) Technische Realisierung**
- 6) Ergebnis & Demo**
- 7) Fazit**



Was ist Single Sign-On

Einführung

- Zentrale Authentifizierung für mehrere Dienste
- Ein Login für verschiedene Anwendungen
- Identitätsverwaltung über einen zentralen Dienst



“ Single Sign-On ermöglicht es einem Benutzer, sich einmal anzumelden und anschließend mehrere Systeme ohne erneute Anmeldung zu nutzen.

Nutzen von Single Sign-On

Für Benutzer

- Nur ein Benutzername / Passwort
- Bessere Benutzerfreundlichkeit
- Weniger Passwortprobleme

Für Administratoren

- Zentrale Benutzerverwaltung
- Einheitliche Sicherheitsrichtlinien
- Geringerer Verwaltungsaufwand

Zielsetzung des Projekts

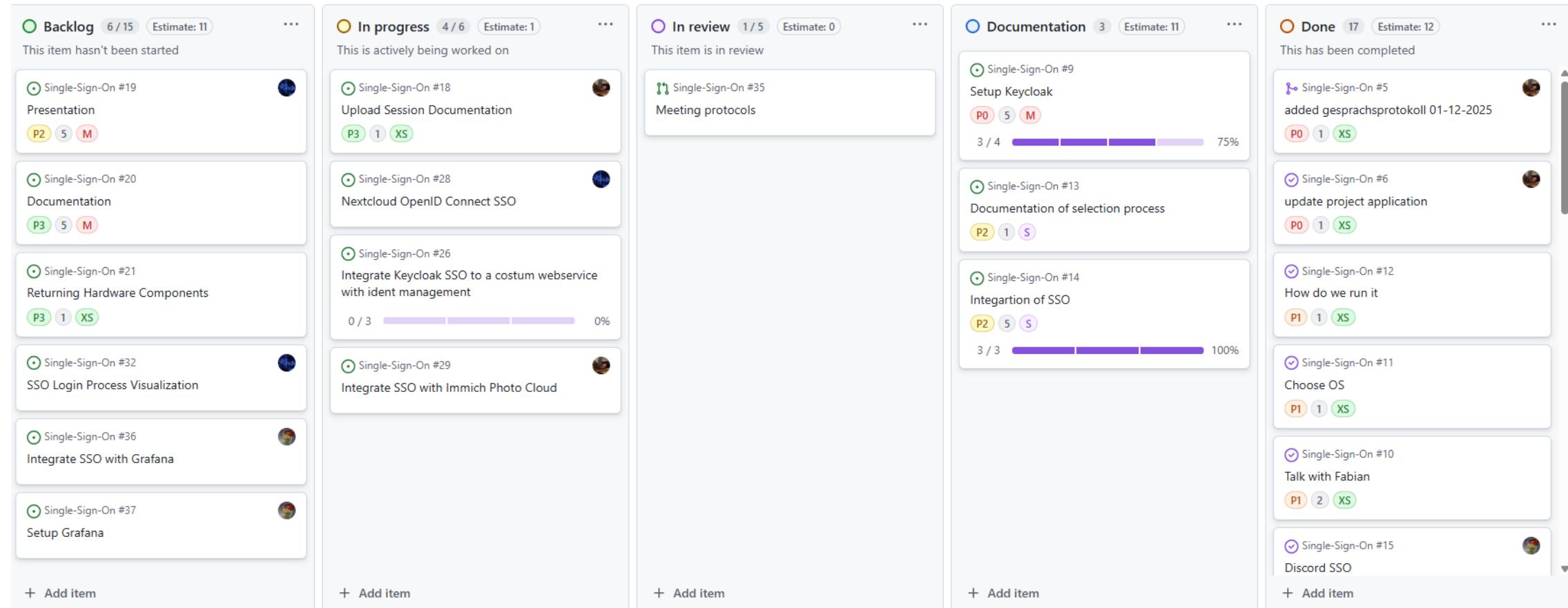
- Aufbau eines zentralen SSO-Dienstes mit Keycloak
- Einbindung bestehender Anwendungen
- Nutzung moderner Authentifizierungsstandards
- Funktionsfähige Anmeldung in der Demo



Umsetzung / Projektvorgehen

Projektmethode: Kanban

■ Nutzung von GitHub Projects als Kanban-Board



The screenshot shows a GitHub Projects Kanban board with five columns:

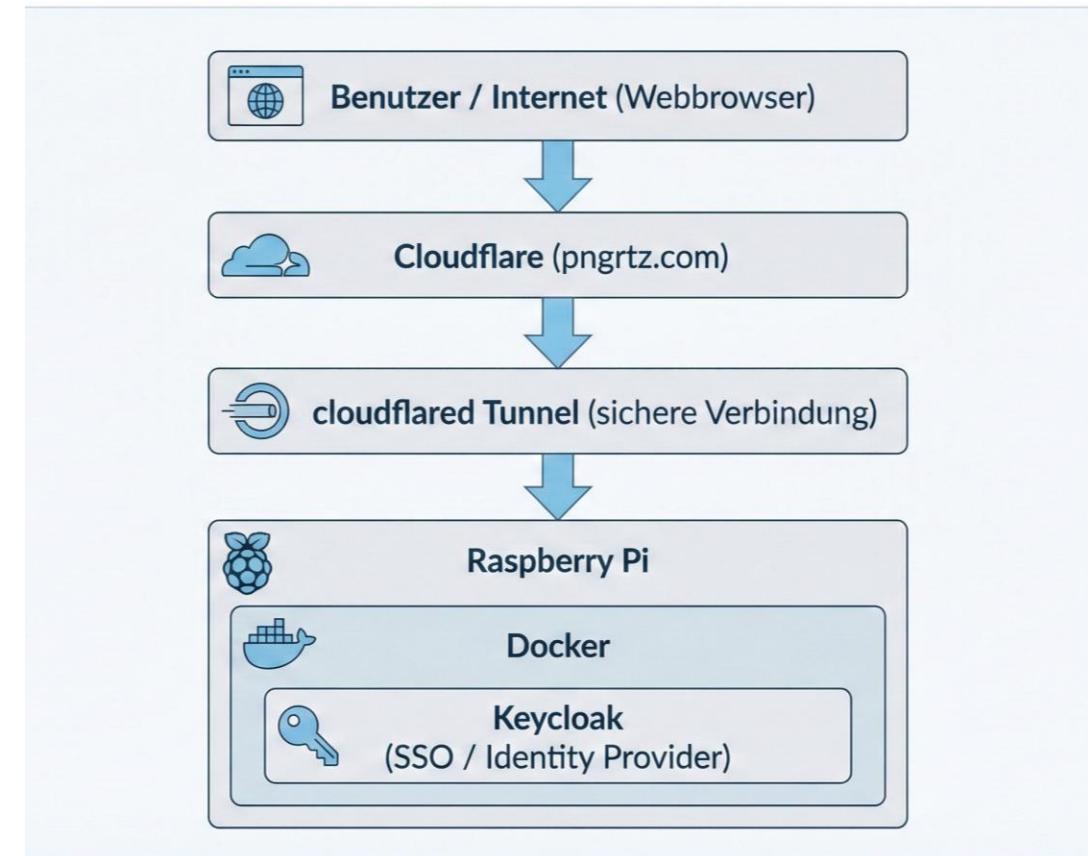
- Backlog**: 6 / 15 Estimate: 11. Sub-tasks include Single-Sign-On #19 (Presentation, P2, 5, M), Single-Sign-On #20 (Documentation, P3, 5, M), Single-Sign-On #21 (Returning Hardware Components, P3, 1, XS), Single-Sign-On #32 (SSO Login Process Visualization, P1, 1, XS), Single-Sign-On #36 (Integrate SSO with Grafana, P1, 1, XS), and Single-Sign-On #37 (Setup Grafana, P1, 1, XS).
- In progress**: 4 / 6 Estimate: 1. Sub-tasks include Single-Sign-On #18 (Upload Session Documentation, P3, 1, XS), Single-Sign-On #28 (Nextcloud OpenID Connect SSO, P1, 1, XS), Single-Sign-On #26 (Integrate Keycloak SSO to a costum webservice with ident management, P1, 1, XS), and Single-Sign-On #29 (Integrate SSO with Immich Photo Cloud, P1, 1, XS).
- In review**: 1 / 5 Estimate: 0. Sub-tasks include Single-Sign-On #35 (Meeting protocols, P1, 1, XS).
- Documentation**: 3 / 3 Estimate: 11. Sub-tasks include Single-Sign-On #9 (Setup Keycloak, P0, 5, M, 75%), Single-Sign-On #13 (Documentation of selection process, P2, 1, S), and Single-Sign-On #14 (Integration of SSO, P2, 5, S, 100%).
- Done**: 17 / 12 Estimate: 12. Sub-tasks include Single-Sign-On #5 (added gesprächsprotokoll 01-12-2025, P0, 1, XS), Single-Sign-On #6 (update project application, P0, 1, XS), Single-Sign-On #12 (How do we run it, P1, 1, XS), Single-Sign-On #11 (Choose OS, P1, 1, XS), Single-Sign-On #10 (Talk with Fabian, P1, 2, XS), Single-Sign-On #15 (Discord SSO, P1, 1, XS), and Single-Sign-On #30 (P1, 1, XS).

Each card includes a plus icon to add new items.

Systemarchitektur (Übersicht)

Wo läuft was? Wie ist es erreichbar?

- Keycloak läuft auf Raspberry Pi
- Betrieb in Docker-Container
- Öffentliche Erreichbarkeit über Domain
- Sicherer Tunneling mit cloudflare



Eingebundene Dienste

Zentrale Komponente

- Keycloak (Identity Provider)

Angebundene Dienste (Clients)

- Nextcloud
- Grafana
- Immich
- Keycloak Demo Service

Externe Identity Provider

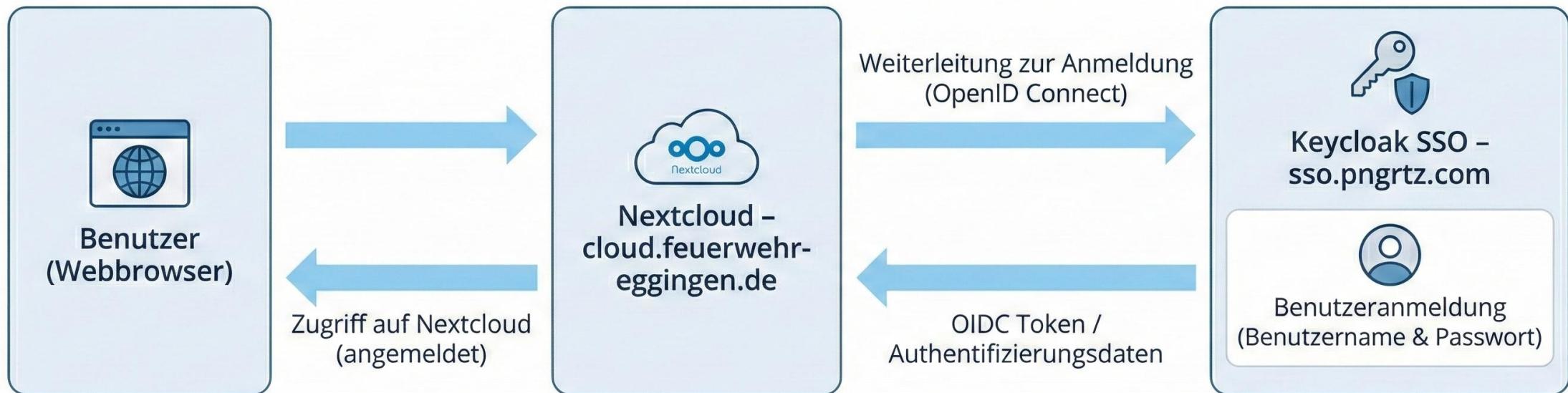
- GitHub
- Discord

“

Keycloak fungiert als zentrale Anlaufstelle für die Anmeldung aller angebundenen Dienste.

Der SSO-Login Prozess

Am Beispiel Nextcloud





Live Demo

Herausforderungen & Schwierigkeiten

1 / 2

Bedienung & Übersichtlichkeit von Keycloak

- Umfangreiche Benutzeroberfläche
- Einstellungen sind tief verschachtelt
- Hohe Einstiegshürde für neue Nutzer
- Fehlermeldungen teilweise wenig aussagekräftig

Benutzer- und Rollenverwaltung

- Admin-Benutzer hatte nicht die erwarteten Rechte
- Unklare Rollen- und Berechtigungsstruktur
- Fehlkonfiguration: zwang zur Neuinstallation
- Lösung: Admin Benutzer beim Setup

Herausforderungen & Schwierigkeiten

2 / 2

Integration von Nextcloud

- Nextcloud benötigt exakt definierte Attribute
- Falsche oder fehlende Attribute führten zu Login-Fehlern
- Automatische Benutzeranlage in Nextcloud ist standartmäßig aktiviert

Abstimmung zwischen Diensten

- Jeder Dienst hat eigene Anforderungen an OIDC
- Unterschiedliche Redirect-URIs
- Schrittweises Testen jedes einzelnen Clients notwendig

Fazit

- Projektziel erreicht
- Zentrale Single-Sign-On-Lösung mit Keycloak umgesetzt
- Mehrere bestehende Dienste erfolgreich angebunden
- Praxisnahe Erfahrung mit Identity & Access Management gesammelt
- Teamarbeit und Organisation mit Kanban erfolgreich umgesetzt



Thank You



ENDE

