RBS
Robert-Bosch-Schule

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

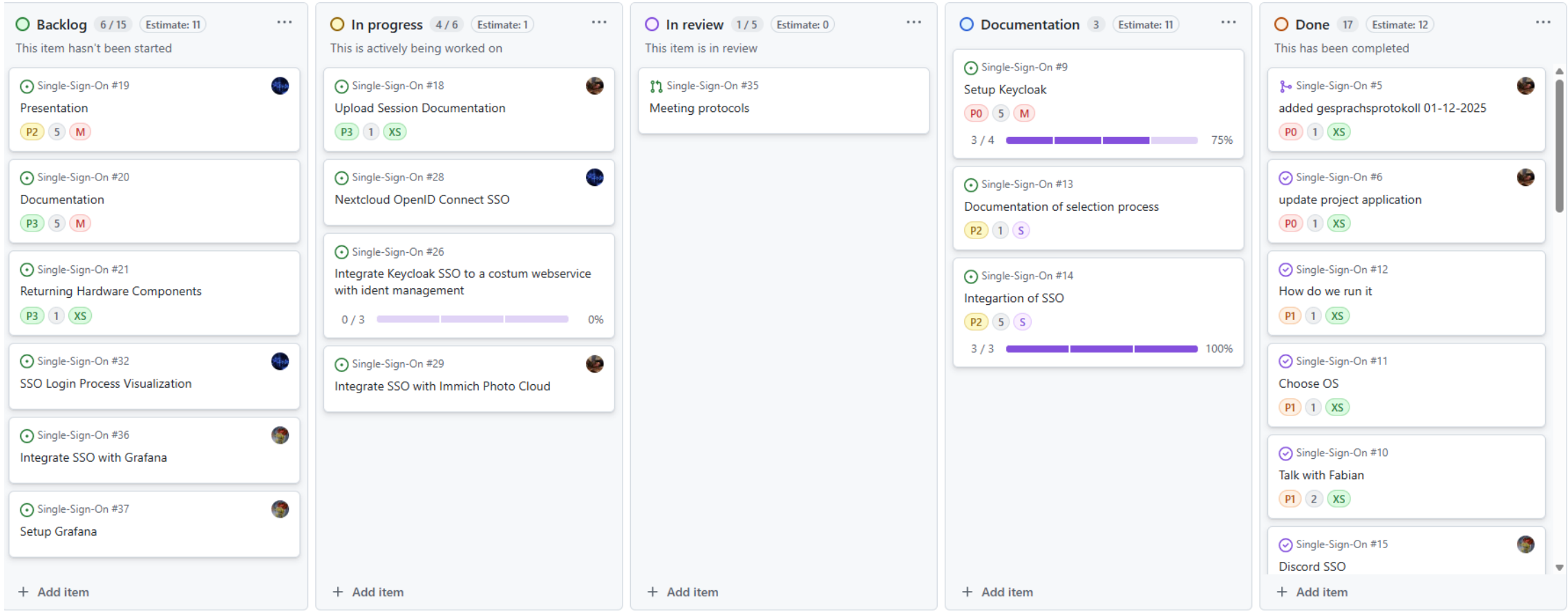
Zielsetzung des Projekts

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

Umsetzung / Projektvorgehen

Projektmethode: Kanban

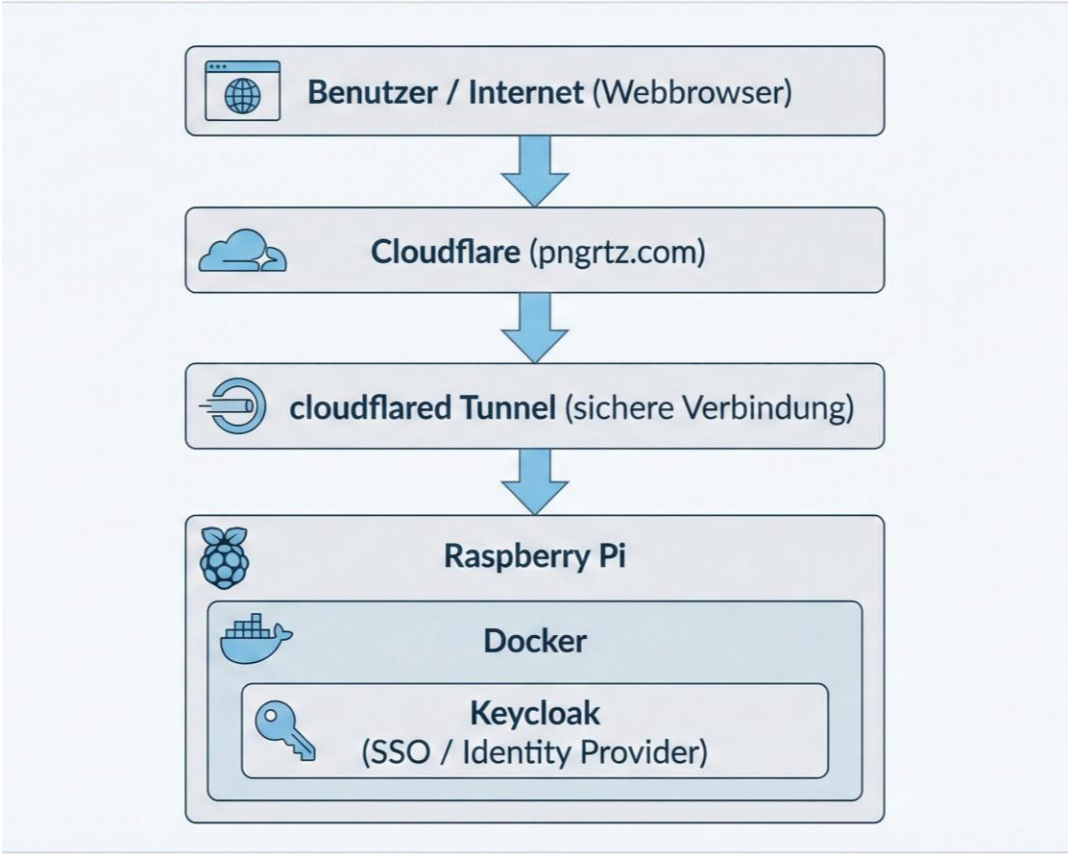
- Nutzung von **GitHub Projects** als Kanban-Board



Systemarchitektur (Übersicht)

Wo läuft was? Wie ist es erreichbar?

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



Eingebundene Dienste

Zentrale Komponente

- Keycloak (Identity Provider)

Angebundene Dienste (Clients)

- Nextcloud
- Grafana
- Immich
- Keycloak Demo Service

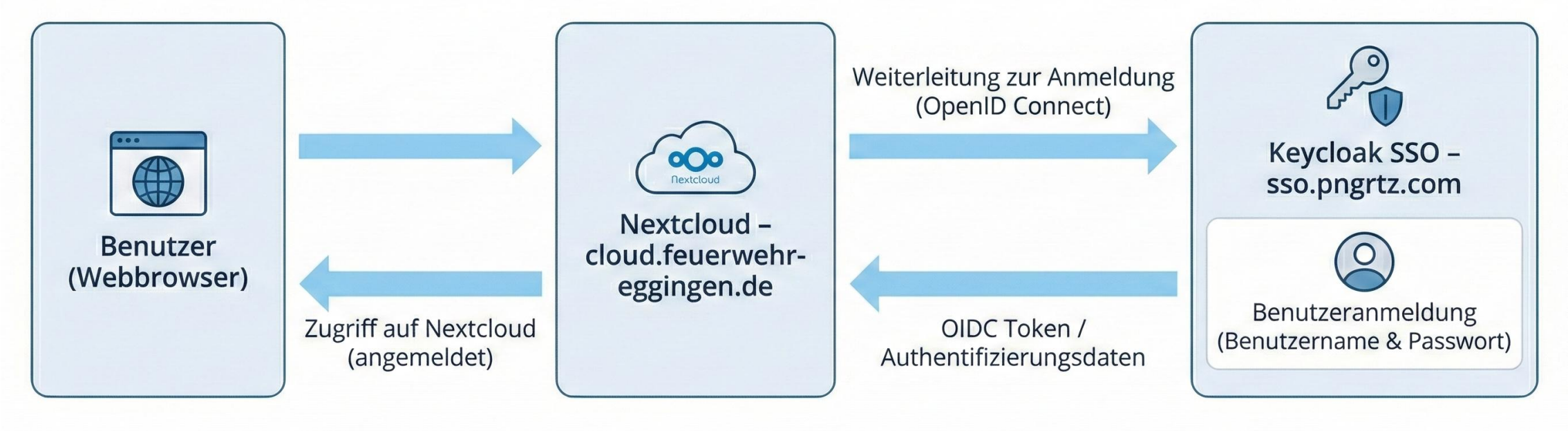
Externe Identity Provider

- GitHub
- Discord

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

Der SSO-Login Prozess

Am Beispiel Nextcloud




Search...
SSO
Username
Password
Login
Forgot your password?
LIVE
LIVE

Live Demo

Herausforderungen & Schwierigkeiten

RBS Robert-Bosch-Schule

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

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

RBS
Robert-Bosch-Schule