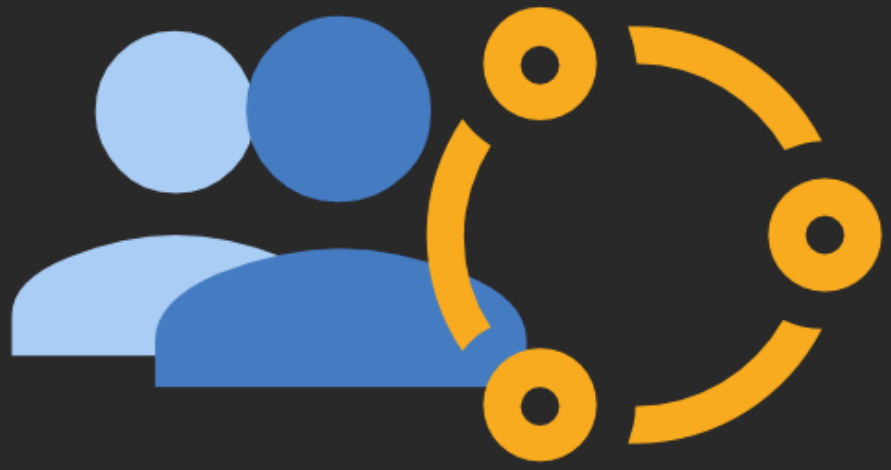
Single-Sign-On für TYPO3

Externer Login für EntraID, Keycloak und andere IdP

Die b13 Single-Sign-On ist die komplette Lösung, um Website-Nutzer oder TYPO3-Redakteure und -Administratoren über einen externen Identity Provider zu authentifizieren.

Die Authentifizierungsmethode basiert auf der SAML Technologie (verschlüsselter / signierter XML-Austausch) und kann mit Microsoft Entra ID, Keycloak oder SAP Cloud Platform Identity verwendet werden.



Vorteile von Single-Sign-On mittels externen IdP bei TYPO3

Mit einer externen Haltung von Benutzerzugriff kannst du die zentralen Login-Daten deines Unternehmens, die du in der Regel in einem zentralen System steuerst, an TYPO3 anbinden, und gleichzeitig die feingranulare Rechteverwaltung in TYPO3 behalten.

Dabei wird dein zentraler Identity Provider (IdP) mit Hilfe der SAML Authentifizierungsmethode an TYPO3 angebunden. Über den IdP können weitere Funktionen wie Single-Sign-On in weitere Anwendungen, Support für Multi-Factor-Authentifizierung (MFA) und einfache Offboarding-Prozesse von internen Benutzern gesteuert werden.

Dabei dient TYPO3 stets als Service Provider (SP) und kann mit der b13 Single-Sign-On Lösung einen *SP-initiated Login*, *einen SP-initiated Logout* oder einen *IdP-initiated Logout* verarbeiten.

Wie funktioniert's?

Die **b13 Single-Sign-On** Lösung basiert auf einer TYPO3-Erweiterung sowie einer SAML-Bibliothek. Der Application Server stellt ein Zertifikat und einen Private-Key aus, welche dann für die Signierung und Verschlüsselung der XML-Daten dienen.

Die TYPO3-Erweiterung erlaubt es, den Login (Authentifizierung) über eine YAML-Datei oder XML-Datei zu steuern.

Neben der MetaData URL, werden auch Funktionen konfiguriert:

Just-in-Time-Provisioning / Federation

Es ist möglich, nur bestehenden TYPO3-Benutzern den Login zu erlauben oder auch neue Benutzer-Datensätze im TYPO3 über die Anbindung zu erstellen.

Separation von Website-Besuchern und Redakteure

Je nach Anwendungsfall im TYPO3 Projekt wird entschieden, ob der, Single-Sign-On für einen internen Bereich der Website verwendet wird oder den Zugriff für Redakteure im Backend verwaltet. Selbst beides ist parallel möglich, da Single-Sign-On auch pro Site in einem Multisite-Projekt konfiguriert werden kann.

Weitere Funktionen

Mapping von Gruppen-Berechtigungen und Attributen

Die bestehende Konfigurationsdatei erlaubt es, ein statisches Gruppen-Mapping für die Zuordnung der Berechtigung durchzuführen bzw. weitere SAML-Attribute wie E-Mail-Adresse, Adresse / Land oder Organisationshoheit für die Benutzer aus dem Identity Provider zu setzen.

Hybrid-Login möglich

TYPO3-Benutzer, die über Single-Sign-On gesteuert werden, beinhalten keine Credentials wie Passwort mehr im TYPO3-System. Es ist jedoch auch möglich, sowohl native TYPO3-Benutzer als auch Single-Sign-On gesteuerte Benutzer in einem System parallel zu betreuen.

Mögliche Anbindungen

Die b13-Single-Sign-On Lösung für TYPO3-Frontend und TYPO3-Backend wurden bereits erfolgreich mit folgenden im Produktionseinsatz getestet:

- Microsoft Entra ID (Azure Entra ID)
- Keycloak
- SAP Cloud Platform Identity Authentication Service

Anforderungen

Die **b13 Single-Sign-On** Lösung auf SAML Basis besteht aus einer TYPO3-Erweiterung sowie einer Dokumentation und einem Onboarding Call von ca. 1h für die Einrichtung.

Systemanforderungen:
- TYPO3 v12 LTS / v13 LTS in Composer—Mode
- PHP 8.2+ mit openssl Extension
- URL oder XML-basierte Metadaten-Information für SAML

Beispiel-Konfigurationen für eine simulierte lokale Entwicklung auf Basis von Keycloak mit DDEV können bereitgestellt werden.

Es ist möglich, pro TYPO3-Environment (Development, Testing, Production) andere IdPs zu konfigurieren.

Kosten & Zugang

Kosten / Jahr: 999€
Einmalige Bereitstellung und Onboarding: 299€

Nach Zahlung der Rechnung wird ein Zugang zu einem privaten Git-Repository mit der TYPO3 Erweiterung und Dokumentation bereitgestellt.

Updates für neuere TYPO3-Versionen und Bugfix Releases sind im jährlichen Update-Zyklus enthalten.

Der Zugang wird automatisch um 12 Monate verlängert, wenn nicht spätestens 8 Wochen vor Ablauf schriftlich gekündigt wird.

made with ❤ by b13