Single-Sign-On For TYPO3

External login for Entra ID, Keycloak and other IdPs

The b13 Single-Sign-On is a complete solution for authenticating website users, TYPO3 editors, and administrators through an external Identity Provider.

The authentication method is based on SAML technology

(encrypted
/ signed XML exchange) and can be used with Microsoft Entra ID, Keycloak, or SAP Cloud Platform Identity.

Advantages of Single-Sign-on With an External Idp in TYPO3

With external management of user access, you can connect the central login credentials of your organization—usually controlled in a central system—to TYPO3 while still maintaining fine-grained permission management within TYPO3.

Your central Identity Provider (IdP) is connected to TYPO3 using the SAML authentication method. Through the IdP, additional features can be controlled, such as Single-Sign-On for other applications, support for Multi-Factor Authentication (MFA), and simplified offboarding processes for internal users.

In this setup, TYPO3 always acts as the Service Provider (SP) and, with the b13 Single-Sign-On solution, can process an SP-initiated login, an SP-initiated logout, or an IdP-initiated logout.

How Does It Work?

The **b13 Single-Sign-On** solution is based on a TYPO3 extension and a SAML library. The application server issues a certificate and a private key that are used to sign and encrypt the XML data.

The TYPO3 extension allows the login (authentication) to be configured via a YAML file or an XML file.

In addition to the metadata URL, further functions can be configured.

Just-In-Time Provisioning / Federation

It is possible to allow login only for existing TYPO3 users
or to automatically create new user records in TYPO3 through the IdP connection.

Separation of Website Visitors and Editors

Depending on the use case within the TYPO3 project, you
can decide whether Single-Sign-On should be used for an internal area of the website or to manage editor access in the backend. Both can also run in parallel, since
Single-Sign-On can be configured per site in a multisite project.

Additional Functions

Mapping of Group Permissions and Attributes

The existing configuration file allows static group mapping to assign permissions. Additional SAML attributes such as email address, address or country, or organizational ownership can also be assigned to users based on information from the Identity Provider.

Hybrid Login Possible

TYPO3 users managed through Single-Sign-On no longer store credentials such as passwords in the TYPO3 system. However, it is also possible to manage both native TYPO3 users and Single-Sign-On users within the same system.

Possible Integrations

The b13 Single-Sign-On solution for the TYPO3 frontend and backend has already been successfully tested in production with the following systems:

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

Requirements

The **b13 Single-Sign-On** solution based on SAML consists of a TYPO3 extension, documentation, and an onboarding call of about one hour for setup.

System requirements:

- TYPO3 v12 LTS / v13 LTS in Composer mode
- PHP 8.2+ with OpenSSL extension
- URL-based or XML-based SAML metadata information

Example configurations for a simulated local development environment using Keycloak with DDEV can be provided.

It is also possible to configure different IdPs for each TYPO3 environment (development, testing, production).

Costs & Access

Cost per year: 999€
One-time setup and onboarding: 299€

After payment of the invoice, access will be provided to a private Git repository containing the TYPO3 extension and documentation.

Updates for newer TYPO3 versions and bug-fix releases are included in the annual update cycle.

Access is automatically renewed every 12 months unless cancelled in writing at least 8 weeks before the end of the current term.

made with ❤ by b13