INSTITUTIONELLES IDENTITÄTS-MANAGEMENT MIT SHIBBOLETH IN OJS 3

OJS-de.net

Im Rahmen des institutionellen Identitäts-managements in OJS 3 bekommen Nutzer/innen die Möglichkeit, sich mit einem Single-Sign-On-Verfahren über ihre Institution als Identity Provider bei einer OJS-Zeitschrift anzumelden.

Diese Anleitung wurde auf Basis folgender Software-versionen erstellt.

OJS Code-Version: 3.1.2

OJS Database-Version: 3.1.2

Shibboleth-Plugin: 1.0.0.0

Inhalt

Das Shibboleth Konsortium stellt Open-Source-Lösungen zur verteilten Authentifizierung und Autorisierung von Webanwendungen, inklusive institutionellem Identitäts-management und Single-Sign-On (SSO), zur Verfügung.

Shibboleth Konsortium

Die Authentifizierung erfolgt dabei über die Institution (Identity Provider, IdP) der Nutzer/innen. Sollen mehrere IdPs einbezogen werden, kann das schnell zu einem erheblichen Einrichtungsaufwand führen. Daher können die IdPs zu sogenannten Föderationen zusammengefasst werden. Ein zusätzlicher Erkennungsdienst „Where Are You From"/Discovery-Service (WAYF/DS-Dienst) identifiziert dann die für den Benutzer/die Benutzerin zuständige Institution.

Im deutschsprachigen Raum stehen dafür im wissenschaftlichen Bereich die Authentifizierungs- und Autorisierungs-Infrastrukturen (AAIs) des Vereins Deutsches Forschungsnetz e.V. (DFN-AAI) oder die Schweizer Stiftung SWITCH (SWITCHaai) zur Verfügung.

DFN-AAI

SWITCHaai

Die Hauptelemente eines web-basierten SSO-Systems sind:

Das Shibboleth Single-Sign-On-Verfahren

- **Web Browser** – repräsentiert den Benutzer/die Benutzerin, der/die auf eine geschützte Ressource zugreifen will;
- **Ressource** – der geschützte Inhalt, auf den zugegriffen werden soll (z.B. OJS-Webseite)

- **Identity Provider (IdP)** – die Institution, die den Benutzer/die Benutzerin identifizieren kann
- **Service Provider (SP)** – Applikation, die den SSO-Prozess imitiert (z.B. Shibboleth-Plugin von OJS)
- **„Where Are You From"/Discovery-Service (WAYF/DS-Dienst)** – optional – fragt Benutzer/innen (basierend auf einer Auswahlliste) nach ihrem Identity Provider (Heimatinstitution)

Der Identity Provider stellt den Single-Sign-On-Authentifizierungsprozess für einen spezifischen Benutzer/eine spezifische Benutzerin zur Verfügung und erweitert damit deren Reichweite über die Heimatinstitution hinaus. Er verifiziert Benutzer/innen anhand der in der Institution verfügbaren Verfahren und kann damit kontrollieren, welche Informationen über sie an den Service Provider weitergegeben werden.

Der Identity Provider

Der Service Provider erkennt den Zugriff eines Benutzers/einer Benutzerin auf eine geschützte Ressource und initiiert den SSO-Prozess. Er leitet die Authentifizierungsanfrage entweder direkt an einen vorkonfigurierten Identity Provider weiter, oder schickt den Benutzer/die Benutzerin zu einem konfigurierten WAYF/DS-Dienst.

Der Service Provider

Es ist nicht ungewöhnlich, dass Service Provider mit Kund/innen aus verschiedenen Institutionen oder Identity Provider mit verschiedenen Dienstleistungseinrichtungen zusammenarbeiten möchten. Diese schließen sich dann zu einer sogenannten Föderation zusammen, welche die SPs und IdPs identifiziert und die Vertrauensbasis für die Zusammenarbeit bildet (Federated-SSO).

Shibboleth Federations

IdP-Föderationen und der IdP-Erkennungsdienst

In diesem Fall schickt der Service Provider den Benutzer/die Benutzerin zunächst zum WAYF/DS-Dienst der Föderation (z.B. DFN-AAI oder SWITCHaai), welcher den für die spezifische Person zuständigen IdP identifiziert (meistens durch Auswahl des IdPs aus einer Liste von registrieren IdPs durch den Benutzer/die Benutzerin). Anschließend wird der Benutzer/die

Benutzerin zur Autorisierung an den gewählten IdP weitergeleitet.

Den Ablauf des Single-Sign-On-Verfahrens mit Shibboleth verdeutlicht ein von SWITCHaai veröffentlichtes Schema (Abbildung 1). Dabei werden, je nach verwendetem Erkennungsdienst, zwei Verfahren unterschieden. Während das WAYF-Verfahren eine komplexe, multilaterale Kommunikation beinhaltet, ist die Kommunikation beim Discovery-Service-Verfahren wesentlich vereinfacht.

Der Ablauf des SSO-Verfahrens

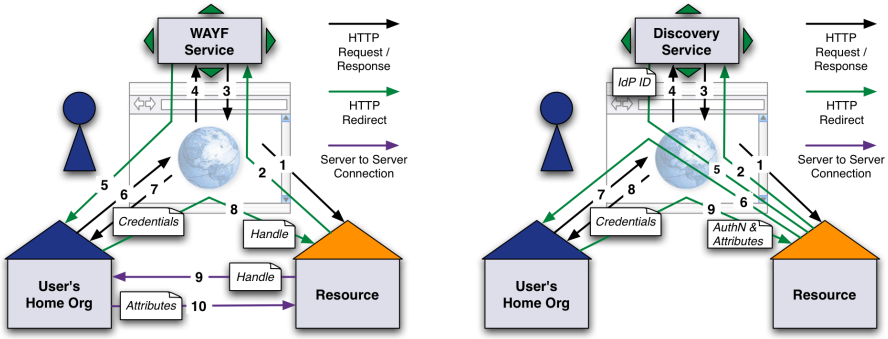

Abbildung 1 Schema des Single-Sign-On-Verfahrens mit „Where Are You From"-Service (WAYF, links, Shibboleth 1.x default) und Discovery-Service (rechts, Shibboleth 1.x default). User's Home Org: Identity Provider, Resource: Ressource und Service Provider. Quelle: SWITCHaai.

Um Shibboleth mit OJS 3 nutzen zu können, müssen Sie zunächst das Shibboleth Service Provider Modul für den von Ihnen genutzten Webserver installieren und konfigurieren.

Shibboleth SP3 Documentation

Aktivierung von Shibboleth in OJS 3

Der Shibboleth Service Provider (SP) 3.0 Configuration Guide von SWITCH stellt dafür eine sehr gute Anleitung zur Verfügung.

Nach erfolgreicher Installation des Shibboleth Service Providers installieren Sie das Shibboleth-Plugin über die Plugin-Galerie von OJS 3 und aktivieren Sie es. Gehen Sie in die Plugin-Einstellungen und konfigurieren Sie das Plugin wie in Abbildung 2 gezeigt. Im Feld „Shibboleth SP path" geben Sie bitte die URL zum WAYF/DS-Dienst Ihrer Shibboleth-Föderation ein.

Damit ist das Plugin eingerichtet.

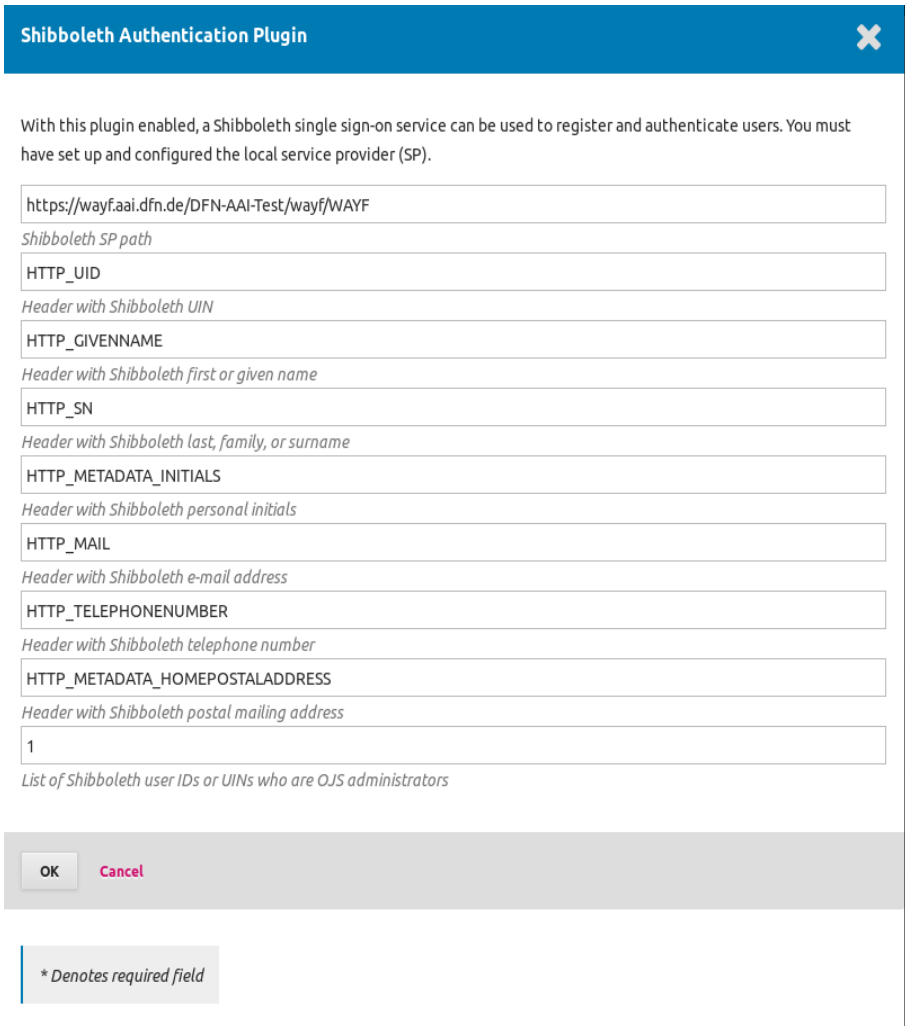

Abbildung 2 Einstellungen des Shibboleth-Plugins