

# Shibboleth® – ein modernes Single Sign On System

Petra Berg | petra.berg@cms.hu-berlin.de

## Shibboleth – Funktion

Viele webbasierte Dienste der Humboldt-Universität sind auf eine Authentifizierung ihrer Nutzer und häufig auch auf deren Autorisierung angewiesen. Momentan implementieren die meisten Dienste eigene Anmeldefunktionen, was zur Folge hat, dass der Nutzer täglich mit mehreren verschiedenen Web-Oberflächen zur Anmeldung konfrontiert wird.

Eine für den Nutzer leichter handhabbare Lösung bietet das Shibboleth-System, welches ihm erlaubt, sich nur einmal je Sitzung zu authentifizieren und innerhalb dieser Sitzung alle an Shibboleth angebundenen Dienste ohne weitere Authentifizierung zu nutzen. Ermöglicht wird diese Funktion durch Technologien des Browsers auf Nutzerseite und der zentralen Authentifizierung im Shibboleth-System. Als Sitzung wird dabei der Zeitraum zwischen dem Öffnen des Browsers und dem Schließen der letzten offenen Instanz des Browsers bezeichnet. Ein Logout in der Web-Anwendung beendet die Shibboleth-Sitzung ebenfalls, aber ohne Schließen des Browsers.

Zusätzlich zur Authentifizierung des Nutzers kann das Shibboleth-System sogenannte *Attribute* für die Autorisierung des Nutzers an den Dienst liefern. Attribute sind Informationen zum Nutzer, die vom Identitätsmanagement bereitgestellt werden. Dazu wird im Shibboleth-System vorher einmalig festgelegt, welcher Dienst welche Attribute benötigt. Diese werden unter der Voraussetzung der Zustimmung durch den Nutzer nach erfolgreicher Authentifizierung an den Dienst übertragen. Die

eigentliche Autorisierung des Nutzers übernimmt der Dienst auf Grundlage der übertragenen Attribute selbst.

Für den Nutzer ergeben sich folgende Szenarien für den Zugriff auf webbasierte Dienste innerhalb einer laufenden Sitzung:

### Erster Zugriff

Der Nutzer öffnet seinen Browser und wählt die Adresse des gewünschten Dienstes (siehe Abbildung 1: 1 Starte Dienst). Auf dem Server des Diensteanbieters, Service-Provider (SP) genannt, leitet das Shibboleth-SP-Modul den Browser an den zentralen Shibboleth-Server, den sogenannten Identity-Provider (IdP) weiter (Abbildung 1: 6 Umleitung), denn dieser kennt den Nutzer. Der IdP präsentiert dem Nutzer im Browser die Login-Seite, in die er seinen Nutzernamen und das Passwort eingeben muss (Abbildung 1: 7 Login? und 8 Login.).

Mit Nutzernamen und Passwort schaut der IdP in seine definierte Menge von Identitätsdaten (bereitgestellt von einem Identitätsmanagement), ob ein Nutzer mit dem angegebenen Account und Passwort existiert. Ist er vorhanden, ist der Nutzer authentifiziert. Kommt er hingegen in keinem Eintrag vor, hat er sich vielleicht vertippt und bekommt im Browser die Login-Seite erneut präsentiert.

Ist der Nutzer authentifiziert, legt der IdP eine Shibboleth-Sitzung für den Nutzer an und schreibt deren Kennung in ein sogenanntes Browser-Cookie, das wie ein Merkzettel im Browser funktio-

*Webbasierte Dienste innerhalb der Universität sowie in deren Umfeld gewinnen immer mehr an Bedeutung. Im Zuge dessen wird es immer wichtiger, webbasierte Systeme zur Authentifizierung und Autorisierung zentral bereitzustellen. Shibboleth ist ein solches System. Es verwirklicht Single Sign On (SSO) zur Authentifizierung und stellt unter Berücksichtigung datenschutzrechtlicher Aspekte Informationen zum Nutzer (Attribute) zur Autorisierung bereit. Zusätzlich ermöglicht Shibboleth das Bilden von Vertrauensgruppen, den sogenannten Föderationen, die eine gegenseitige Nutzung von Diensten erlauben. Nachfolgender Beitrag beschreibt die Funktion von Shibboleth aus Sicht des Nutzers sowie die technische Umsetzung aus Sicht des Administrators.*



Für den ersten Zugriff innerhalb einer laufenden Sitzung geht also die erste Umleitung vom SP-Modul zum sogenannten *Discovery Service* (DS) (Abbildung 1: 2 Umleitung). Dieser fragt über eine Seite im Browser den Nutzer nach der Heimateinrichtung (Abbildung 1: 3 Heimateinrichtung?). Diese merkt sich der DS auch in einem Browser-Cookie. In manchen Fällen fragt der DS den Nutzer nicht, sondern gibt die Heimateinrichtung zurück, über den der Nutzer im Internet angemeldet ist (in deren IP-Bereich sich der Nutzer gerade befindet). Dann fallen die Wege 3 und 4 in der Abbildung 1 weg. Liegt dem DS die Heimateinrichtung vor, schickt er diese an das SP-Modul zurück (Abbildung 1: 5 Umleitung).

Die weiteren Schritte sind identisch zum Verlauf der Anmeldung in den anfänglich beschriebenen Szenarien (siehe oben).

## Technische Umsetzung

Für die Funktion von Shibboleth spielen sogenannte *Metadaten* eine wesentliche Rolle. Die Metadaten eines an Shibboleth teilnehmenden Dienstes sind zugleich Ausweis und Eintrittskarte und müssen daher besonders geschützt werden. Sie enthalten wichtige Informationen über unterstützte Services, deren Adressierung sowie die Zertifikate, die zum Verschlüsseln und Signieren verwendet werden.

Die Metadaten werden aus der Konfiguration der Shibboleth-Komponente mit Hilfe eines enthaltenen Generators oder manuell erzeugt. Diese Metadaten müssen allen Identity-Providern der Föderation bekannt sein. Da die Metadaten hierarchisch organisiert sind, können sie zentral gesammelt und bereitgestellt werden.

Jeder Shibboleth-Teilnehmer, sowohl Service-Provider (Dienst) als auch Identity-Provider, kann beliebig viele Quellen für Metadaten konfigurieren und so Mitglied in mehreren Föderationen sein. Wichtig ist, dass die Metadaten immer von einer verlässlichen Quelle

stammen und dies durch eine gültige digitale Signatur bezeugen. Zusätzlich sollten Metadaten aus Sicherheitsgründen eine begrenzte Gültigkeit haben, die jeweils vor Ablauf erneuert wird.

Damit die Nutzer das Shibboleth-System optimal nutzen können, müssen möglichst alle Web-Dienste mit Authentifizierung an der Humboldt-Universität auf Shibboleth umgestellt werden.

Für die Umstellung von Web-Diensten der HU sind im Allgemeinen folgende Schritte vom Dienstanbieter nötig:

1. Vorlage eines vom Datenschutzbeauftragten bestätigten Sicherheitskonzeptes für den Web-Dienst
2. Mitbestimmungsantrag an die zuständigen Personalräte, mit Vorlage des bestätigten Sicherheitskonzeptes zur Kenntnisnahme
3. Installation des Shibboleth-SP-Moduls auf dem Web-Server
4. Konfiguration des Shibboleth-SP-Moduls entsprechend der Shibboleth-SP-Konfigurationsanleitung
5. Erstellen der Metadaten zum SP mit bereitgestellter Web-Anwendung
6. Zentrale Freischaltung der SP-Metadaten und damit des Dienstes

Schritt 1 ist dabei als selbstverständlich zu betrachten, da ein solches Sicherheitskonzept für jeden Web-Dienst an der Humboldt-Universität vorliegen muss.

Schritt 2 ermöglicht den zuständigen Personalräten, von ihrem Recht auf Mitbestimmung Gebrauch zu machen.

Schritt 3 umfasst das Laden und Installieren des Shibboleth-SP-Moduls, welches als Debian Package unter den Bestimmungen der Apache Licence 2.0 verfügbar ist.

Für Schritt 4 steht eine ausführliche Anleitung zur Verfügung, die wiederum Schritt für Schritt die nötigen Konfigurationen für das Shibboleth-SP-Modul enthält. Die Konfiguration wird durch im Installationspaket enthaltene Vorlagen erleichtert, die nur geeignet angepasst werden müssen.

Schritt 5 ist der wichtigste Schritt zur Nutzung von Shibboleth aus Sicht des Web-Dienst-Anbieters. Über eine speziell für diesen Zweck implementierte Web-Anwendung werden die Metadaten des betreffenden SPs aufge-

nommen bzw. erzeugt. Anschließend werden die resultierenden Metadaten auf Korrektheit und Vertrauenswürdigkeit geprüft. Sind die Daten korrekt und vertrauenswürdig, können sie als Metadaten exportiert werden.

In Schritt 6 werden die SP-Metadaten zentral in die Menge der Metadaten aller Teilnehmer eingetragen. Damit ist der betreffende Dienst freigeschaltet und kann am Shibboleth-System teilnehmen.

## Fazit

Der Einsatz von Shibboleth birgt wesentliche Vorteile in Bezug auf die Nutzung von Web-Diensten. Punkt eins ist die Vereinfachung von Authentifizierung und Autorisierung für Web-Dienste aus Sicht des Nutzers. Punkt zwei ist die Möglichkeit, innerhalb von Föderationen Web-Dienste einem größeren Nutzerkreis zur Verfügung zu stellen und so eine umfangreiche Kooperation der Einrichtungen untereinander zu schaffen.

## Literatur

- [1] INTERNET2: *Shibboleth*.  
<http://shibboleth.internet2.edu/>
- [2] DFN-AAI – *Authentifikations- und Autorisierungs-Infrastruktur*.  
<https://www.aai.dfn.de/>