Einsatz von Shibboleth im Bereich Wissenschaft und Lehre

Universitätsbibliothek Freiburg, DFN-Verein Berlin, 01.07.2008

Wozu Shibboleth?

Problem

Anbieter möchten aus verschiedenen Gründen den Zugriff auf ihre Ressourcen auf bestimmte Benutzer oder Benutzergruppen einschränken oder die Inhalte dem Benutzer personalisiert anbieten. In beiden Fällen bedarf es einer Authentifizierung und Autorisierung. Bisherige Systeme werden den aktuellen Anforderungen kaum gerecht:

Probleme aus Sicht des Anbieters:

- Aufwändige Registrierung und Verwaltung der Benutzer bei jeder Ressource
- Ressourcen bleiben ungeschützt, da der Aufwand für einen geeigneten Schutz zu groß ist

Probleme aus Sicht der Einrichtung:

- Hoher Aufwand für die Einbindung neuer Anbieter in das eigene Angebot
- Hoher Aufwand für den Schutz eigener Ressourcen (zum Beispiel E-Learningmodule)

Probleme aus Sicht des Benutzers:

- Benutzer müssen sich für jeden Dienst neu authentifizieren
- Benutzer benötigen verschiedene Benutzerkennungen und Passworte für verschiedene Dienste
- Bei vielen Ressourcen ist der Zugriff nur innerhalb der eigenen Einrichtung möglich

Basierend auf dem Verfahren **Shibboleth**[1], das im Rahmen des Internet2-Projektes entwickelt und gepflegt wird, wurde in der vergangen Jahren eine deutschlandweite Infrastruktur zur Lösung dieser Probleme aufgebaut. Unter dem Namen DFN-AAI bietet der DFN-Verein, Berlin, alle notwendigen Dienste und Unterstützung an.

Was ist Shibboleth?

Lösung

Shibboleth ist eine frei verfügbare Software, welche auf bekannte Standards beruht und die Nutzung beliebig verteilter Ressourcen mit einem einzigen Account ermöglicht. Shibboleth verwendet einen föderativen Ansatz: Die Einrichtung verwaltet und kontrolliert die Identität ihre Mitglieder, und der Anbieter kontrolliert den Zugang zu seinen Ressourcen. Shibboleth bietet folgende Vorteile:

Vorteile aus Sicht des Anbieters:

- Der Aufwand für den Schutz von Ressourcen ist vergleichsweise gering
- Es ist keine Benutzerverwaltung erforderlich

Vorteile aus Sicht der Einrichtung:

- Die Einbindung neuer Ressourcen in das eigene Angebot ist sehr einfach
- Mitgliedern anderer Einrichtungen kann leicht Zugriff auf eigene geschützte Ressourcen gewährt werden, falls entsprechende Zugriffsrechte vorhanden sind

Vorteile aus Sicht des Benutzers:

- Die Nutzung der Ressouren ist unabhängig von Standort und Zugriffsweg möglich
- Der Benutzer muss sich für den Zugriff auf verschiedene Resourcen nur einmal authentifizieren (*Single Sign-On*)
- Die Anforderungen des Datenschutzes werden respektiert

Wie funktioniert Shibboleth?

Funktionsweise

Die Funktionsweise von Shibboleth lässt sich am einfachsten anhand des folgenden Szenarios erklären:

Was möchten Sie?
Ein Benutzer möchte auf eine geschützte Ressource zugreifen. Der Anbieter nimmt die Anfrage entgegen und prüft, ob der Benutzer bereits authentifiziert ist. Wenn nicht, wird er zu einem Lokalisierungsdienst weitergeleitet.

Woher kommen Sie?
Der Lokalisierungsdienst bietet eine Auswahl von Einrichtungen an. Der Benutzer wählt seine Heimateinrichtung aus und wird zu dieser weitergeleitet.

Wer sind Sie?
Die Heimateinrichtung prüft, ob der Benutzer bereits authentifiziert ist. Ist dies nicht der Fall, wird der Benutzer aufgefordert sich zu authentifizieren (zum Beispiel mit Benutzerkennung und Passwort oder Chipkarte). Die Heimateinrichtung stellt einen ,,digitalen Ausweis“ aus und leitet den Benutzer zum Anbieter zurück.

Welche Rechte haben Sie?
Der Anbieter prüft den Inhalt des digitalen Ausweises. Benötigt der Anbieter weitere Informationen um zu entscheiden, ob der Benutzer auf die gewünschte Ressource zugreifen darf (zum Beispiel die Fakultätszugehörigkeit), so fragt er bei der Heimateinrichtung des Benutzers nach.

Dürfen Sie zugreifen?
Der Anbieter prüft über das eigene System oder einen externen Rechteserver, ob der Benutzer auf die Ressource zugreifen darf und gestattet den Zugriff oder lehnt ihn ab.

Was ist notwendig, um Shibboleth einzusetzen?

Voraussetzung

Für Shibboleth können fast beliebige lokale Authentifizierungssysteme verwendet werden, gegebenenfalls auch IP-Kontrolle. Die für die Einbindung notwendigen Software-Komponenten laufen auf allen gängigen Plattformen, sie stehen als Open Source-Produkte kostenfrei zur Verfügung. Da die Einrichtung die Verantwortung für eine Authentifizierung ihrer Mitglieder übernimmt, ist der Einsatz eines zuverlässigen Identitäts-Management-Systems (IdM) erforderlich. Auf Benutzerseite ist keine besondere Software notwendig.

Was ist eine Föderation?

DFN-AAI

Eine Föderation ist der Zusammenschluß von Einrichtungen und Anbietern. Die Teilnehmer unterschreiben einen Vertrag, um das notwendige Vertrauensverhältnis zwischen den Teilnehmern zu garantieren. Für wissenschaftliche Einrichtungen in Deutschland bietet der DFN-Verein und dem Namen ”DFN-AAI[2]“ einen umfassenden Dienst zur technischen Unterstützung bei Installation und Betrieb an.

Wie verbreitet ist Shibboleth?

Shibboleth weltweit

Shibboleth basierte Authentifizierungs- und Authorisierungssysteme werden heute schon weltweit eingesetzt. In den USA und Europa existieren bereits landesweite Föderationen im Hochschulbereich. Shibboleth wird auch bereits von einer Reihe namhafter Anbieter wie EBSCO, Elsevier, JSTOR, Proquest (CSA), OVID, GBI, DIPF, etc.[3] unterstützt, weitere Anbieter haben eine Unterstützung angekündigt. Es ist davon auszugehen, dass Shibboleth sich weltweit als Standard für die verteilte Authentifizierung und Autorisierung durchsetzen wird.

[1] http://shibboleth.internet2.edu/
[2] http://www.aai.dfn.de/
[3] Stand Juli 2008

Kontaktadressen

Universitätsbibliothek Freiburg
Platz der Universität 2
79098 Freiburg

Ansprechpartner:
Ato Ruppert

DFN-Verein
Stresemannstr. 78
10963 Berlin

Ulrich Kähler