Shibboleth

Informationen zum Thema Shibboleth

Derzeit wird in Deutschland ein Netzwerk einer neuen europaweit abgestimmten Infrastruktur für Authentifizierung- und Autorisierungsdienste aufgebaut. Basis dieser neuen Technik ist ein Open Source Softwarepaket namens "Shibboleth".

Shibboleth wird mittelfristig die bisherige IP-Nummern-basierte Autorisierung beim Zugriff auf lizenzierte Materialien ablösen. Ab März wird bereits der Zugriff für Privatpersonen auf die Materialien der Nationallizenzen darüber geregelt werden.

- **Authentifizierung** bedeutet dabei: zweifelsfreie Identifizierung eines Anfragenden (Wer bist Du?)
- **Autorisierung** bedeutet dabei: Erlaubnis oder Verbot des gewünschten Zugriffs der zuvor authentifizierten Person (Was darfst Du?)

Shibboleth verfügt über zwei Module zur Abbildung dieser beiden Funktionalitäten, den sog. "**Identity Provider**" (IdP) und den "**Service Provider**" (SP). Bei der Einführung von Shibboleth werden diese beiden Funktionen logisch sehr viel stärker separiert, als das bisher bei den derzeit verwendeten Verfahren der Zugriffssteuerung der Fall ist. Dies bedeutet, dass die Erlaubnis, ob eine zugriffsbeschränkte Quelle einzusehen ist, nicht mehr an den Rechner (via IP-Freigabe) gebunden wird, sondern an die tatsächlich zugreifende Person. Das Ziel ist eine Trennung von Personendaten und Services, ein verteiltes, organisationsübergreifendes (föderatives) Identity Management (IdM).

Zur Inbetriebnahme von Shibboleth müssen die Universitäten/Bibliotheken eine Instanz des Identity Providers bereitstellen. Die Serviceanbieter wie z.B. Verlage, Datenbankhosts müssen dagegen den Service Provider von Shibboleth betreiben. Für die Serviceanbieter entfällt jedoch damit das aufwendige Verwalten von Access-Listen für jede Universität.

Etwas verkürzt dargestellt läuft der Shibboleth Mechanismus wie folgt ab: Der Kunde kann über eine beliebige Internetverbindung eine geschützte Quelle anfordern. Der Service-Provider (Host) fragt zunächst eine Mittelinstanz, den sog. "Where Are You From"-Dienst (WAYF), um die Heimatorganisation des Anfragenden zu ermitteln. Anschließend wird er zur Authentifizierung an die Identity Provider-Instanz seiner eigenen Universität überstellt, um sich dort anzumelden. Diese ermittelt, ob die anfragende Person, wirklich diejenige ist, die vorgibt anzufragen. Das Ergebnis wird dem Service Provider mitgeteilt, der anschliessend beim Identity Provider anfragen kann, welcher Nutzergruppe die Person zuzuordnen ist. Anschliessend kann der Service Provider anhand der abgesprochenen Policy allein entscheiden, ob der Zugriff rechtmäßig ist oder nicht. Die Authentifizierung- und Autorisierungsinformationen werden während der Browsersitzung über ein Token (Cookie) gespeichert und können so ein Single-Sign-On generieren, so dass weitere Anmeldungsschritte bei dritten Service Providern für den Kunden nicht mehr notwendig sind.

Um eine universitätsweit einheitliche Instanz des Identity Providers anbieten zu können, muss zuvor ein Identity Management eingerichtet werden, dass gewisse übergeordnete Qualitätskriterien aufweist. Einfachste Basis kann ein funktionierender Verzeichnisdienst, wie etwa LDAP sein.

Der formale und rechtliche Rahmen des organisationsübergreifenden IdM wird durch eine derzeit vom DFN aufgebaute sog. "**Föderation**" gebildet. Die Föderation des DFN soll alle universitären Identity Provider und alle zugehörigen Service Provider in einer Dachorganisation vereinen, die die vertraglichen und organisatorischen Standards des Shibboleth-Verfahrens einmal für alle Mitglieder regelt. Weiterhin wird der DFN für die gesamte Föderation den WAYF-Dienst betreiben. Alle Mitglieder des DFN können dann diesen Bedingungen beitreten.

VZG & Shibboleth

Die VZG ist seit Dezember 2007 Mitglied der DFN Föderation und dort als IdP mit der Einzelnutzerverwaltung (IdP) und als SP mit einem Proxy für die Nationallizenzen angemeldet.

Projekte in Bibliotheken

SuUB Bremen:

Zugang zu lizenzierten Medien der UB für Angehörige der Universität Bremen via Shibboleth:
im Testbetrieb mit Ebsco, Springerlink/Metapress, Elsevier/Sciencedirect bereits voll funktionsfähig - Manfred Nölte, Martin Blenkle</p>

HSU Hamburg:

Zwei LDAP Server und zwei SQL Datenbanken werden momentan als LDAP Directory abgefragt. Der Benutzerstatus im LBS kann neben der Institutszugehörigkeit aus dem Hochschuldirectory zur Belegung der Attribute herangezogen werden. Die Lösung ist hochflexibel und kann dynamisch ohne Betriebsunterbrechung erweitert werden. Ideen sind etwa Auswertung des Ablaufdatums eines LBS Accounts, Abfrage von Mahnstufen.. Ulrich Hahn

Vorträge

- Vergleich Penrose und MyVD "Virtual Directory als Attributquelle" für einen Schibboleth IdP. Vortrag aus dem 10. Shibboleth Workshop am 7.4.2010.
- Umsetzung mit Pnrose "Shibboleth und Penrose". Vortrag im Rahmen der DFN Betriebstagung am 26.10.2010

Wichtige Quellen

- http://shibboleth.internet2.edu/
- Shibboleth (Wikipedia)
- Projekt Authentifizierung, Autorisierung und Rechteverwaltung (AAR) (Uni Freiburg)
- DFN-AAI – Authentifizierungs- und Autorisierungs-Infrastruktur im DFN
- Switch-AAI