

---

## Abschlussbericht zum Entwicklungsprojekt „Rechtmanagement mit Shibboleth“

Der Bibliotheksverbund Bayern (BVB) und der Kooperative Bibliotheksverbund Berlin-Brandenburg (KOBV) unterzeichneten Ende Dezember 2007 eine Vereinbarung zur Begründung einer langfristigen Entwicklungspartnerschaft. Dabei wurde die Einführung des Single-Sign-On-Verfahrens (SSO) Shibboleth<sup>1</sup> zur Authentifizierung und Autorisierung in den Verbundbibliotheken als eines der ersten gemeinsamen Entwicklungsprojekte im Rahmen dieser strategischen Allianz definiert.

Das primäre Merkmal des SSO-Verfahrens ist durch eine besondere Zugangskontrolle zu lizenzierten Ressourcen gekennzeichnet: Im Gegensatz zu den bisherigen Methoden (IP-Prüfung, Benutzererkennung und Passwort) erfolgt die Authentifizierung standortunabhängig und nur ein Mal pro Session.<sup>2</sup> Vorrangiges Ziel ist somit die Vereinfachung des Zugangs zu lizenzierten Angeboten einer Bibliothek, ohne dass Sicherheitsrisiken entstehen.

Shibboleth liegt als Open-Source-Implementierung vor. Die Vorteile des Verfahrens wurden sowohl in Deutschland als auch international durch eine breite Nutzergemeinschaft getestet: In Deutschland haben unter Anderem die Universitätsbibliotheken Freiburg und Regensburg in Zusammenarbeit mit dem DFN-Verein eine landesweite Infrastruktur zur Authentifizierung und Autorisierung (AAI) auf der Basis von Shibboleth erarbeitet – die DFN-AAI.<sup>3</sup>

Der DFN-Verein legt darüber hinaus deutschlandweit den organisatorischen und technischen Rahmen für die Einführung und den Betrieb von Shibboleth fest und bestimmt die Richtlinien für die Teilnahme an der deutschlandweiten Föderation. Bereits eine Vielzahl von Anbietern auf der einen Seite und Institutionen auf der anderen Seite sind der DFN-AAI beigetreten und es ist mit einer stetig wachsenden Teilnehmerzahl zu rechnen. Daher lag es für die strategische Allianz von BVB und KOBV auf der Hand, ihr Shibboleth-Entwicklungsprojekt auf diesen Richtlinien aufzubauen.

Aus organisatorischer Sicht teilte sich das Projekt in zwei Phasen auf:

- In der ersten Projektphase (April 2008 – April 2009) stand die Bedarfsermittlung und Informationsarbeit mit dem Ziel der Gewinnung von Pilotpartnern im Vordergrund.
- In der zweiten Projektphase (April 2009 – April 2010) erfolgte die Bereitstellung der Verbunddienstleistungen als Shibboleth-fähige Serviceleistungen.

Der folgende Bericht beschreibt die Vorgehensweise sowie die Ergebnisse der beiden Projektphasen.

### Erste Projektphase: Bedarfsermittlung und Informationsarbeit sowie Shibbolethisierung in den Bibliotheken

Um die Bedürfnisse der einzelnen Bibliotheken besser einschätzen zu können und die lokalen Bedingungen kennen zu lernen, wurde vom 25.06 bis zum 11.08.2008 eine **Umfrage zum Thema Rechtmanagement** unter den BVB- und KOBV-Bibliotheken sowie der zuständigen Rechenzentren durchgeführt. Ziel der Umfrage war die Ermittlung

- potenzieller Pilotpartner,
- des Ist-Zustandes in Bezug auf den Einsatz von Zugangskontrollen sowie
- des Soll-Zustands in Bezug auf die Shibbolethisierung der Zugangskontrollen

---

<sup>1</sup> Definition siehe: [http://de.wikipedia.org/wiki/Shibboleth\\_\(Internet\)](http://de.wikipedia.org/wiki/Shibboleth_(Internet))

<sup>2</sup> Ausführlich dazu siehe: <http://shibboleth.internet2.edu/>

<sup>3</sup> Homepage der DFN-AAI: <https://www.aai.dfn.de/>

Von den 106 Verbundbibliotheken antworteten 38 auf die Umfrage. Die Ergebnisse lauten im Einzelnen:

- Potenzielle Pilotpartner: 27 Bibliotheken bekundeten ihr grundsätzliches Interesse am Rechtmanagement-Projekt im Rahmen der Strategischen Allianz von BVB und KOBV. Davon setzten bereits 18 Bibliotheken ein eigenes Identity-Management-System ein. Neun Bibliotheken erklärten ihre Bereitschaft zur Pilotpartnerschaft. Fünf dieser Bibliotheken organisierten ihren Beitritt zur DFN-AAI mithilfe ihres lokalen Rechenzentrums selbst. Die verbliebenen vier Einrichtungen wurden nach Auswertung der Umfrage kontaktiert.
- Ist-Zustand: Die bisher am meisten verbreiteten Methoden der Zugangskontrolle sind IP-Prüfung und Authentifizierung mit Passwort. Sie werden für die Regulierung des Zugangs zu lizenzierten Datenbanken, CD-ROM-Datenbanken, Nationallizenzen, EZB, Publikationsservern, bestimmten OPAC-Funktionen, elektronischen Semesterapparaten u.ä. verwendet.
- Soll-Zustand: Die Soll-Erhebung ergab eine weitgehende Übereinstimmung des Einsatzes bisheriger Zugangskontrollen mit dem Bedarf an zu shibbolethisierenden Diensten

Damit konnte gezeigt werden, dass ein grundsätzlicher Bedarf sowie ein Interesse am Einsatz von Shibboleth vorhanden ist. Es wurde jedoch in der Umfrage deutlich, dass durch fehlende lokale Voraussetzungen sowie durch bereits anderweitige Projekte der Kreis potenzieller Pilotpartner stark eingeschränkt ist.

Zur Verifizierung der Umfrageergebnisse sowie zur weiteren Einbindung möglicher Pilotpartner erfolgten von Oktober 2008 bis März 2009 **Gespräche mit den projektinteressierten Bibliotheken**. Die Ergebnisse der Umfrage konnten in den Gesprächen vertieft werden. In den Gesprächen zeichnete sich zunehmend ab, dass aufgrund personeller und technischer Gegebenheiten die Bibliotheken nur in enger Zusammenarbeit mit den lokalen Rechenzentren die Einführung von Shibboleth leisten können. Technische Herausforderungen sowie organisatorische Umstände scheinen eine Entscheidung für den Einsatz von Shibboleth zu erschweren.

Weitergehende, persönliche Gespräche mit den Hauptakteuren der potenziellen Pilotpartner zur **Informationsarbeit und Einbindung in das Projekt** führten zu folgenden Ergebnissen:

- Bibliothek und Rechenzentrum des Leibniz-Zentrums für Agrarlandschaftsforschung (ZALF) e. V. Müncheberg: Nach mehreren Gesprächen ab September 2008 erfolgte der Beitritt des ZALF zur DFN-AAI im April 2009. Die Zugänge zu diversen Verlagsangeboten, u.a. Springer Metapress oder de Gruyter, wurden erfolgreich shibbolethisiert und bieten den ZALF-Mitarbeitern bis zum heutigen Tag einen komfortablen Service.
- FHW Berlin: In Gesprächen im September 2008 kristallisierte sich heraus, dass ein Beitritt zur DFN-AAI auf Basis des Entwicklungsprojekts aufgrund von Planungen zur Auslagerung der sehr heterogenen, hochschulweiten Nutzerverwaltung nicht praktikabel erscheint.
- BVB: UB Regensburg und UB Passau wurden als potenzielle Pilotpartner im November 2008 kontaktiert. Dem starken Interesse am Entwicklungsprojekt widersprachen mangelnde personelle und technische Ressourcen. Dies galt ebenso für die aus Gesprächen mit dem DFN-Verein hervorgegangenen weiteren potenziellen Pilotpartner FH Kempten, Universität Eichstätt und Hochschule Neu-Ulm.

Somit stand zum Abschluss der ersten Projektphase trotz intensiver Bemühungen mit dem ZALF lediglich ein Pilotpartner zur Verfügung. In konzentrierter Form erfolgte die Einbindung in das Projekt, die Zufriedenheit wurde im Rahmen der Projektzusammenarbeit immer wieder geäußert.

## Zweite Projektphase: Bereitstellung und Implementierung der shibbolethisierten Verbunddienstleistungen

Von den zahlreichen KOBV- und BVB-Nutzerdienstleistungen wurden einige zentrale zur Shibbolethisierung ausgewählt. Im Rahmen der zweiten Projektphase stellte sich die UB der FU Berlin als Projektpartner für Verbunddienstleistungen zur Verfügung.

Im Folgenden werden die Auswahl, Probleme und Testergebnisse als Übersicht aufgeführt. Die detaillierte Beschreibung der vorgenommenen Installationen und Konfigurationen sind dokumentiert und im internen KOBV-Wiki<sup>4</sup> zugänglich.

**KOBV:** Eine der wichtigsten Nutzer-Dienstleistungen des KOBV ist die Recherche in MetaLib, einer Portalsoftware. Die KOBV-Zentrale hostet MetaLib als Konsortialportal für sieben Institutionen (u.a. UBs der FU Berlin, HU Berlin, TU Berlin). Primo, eine ebenfalls aus dem Hause ExLibris stammende Neuentwicklung für Portalsoftware, wird von der KOBV-Zentrale im Test- und Produktivbetrieb gehostet (u.a. für die UBs der FU Berlin, HU Berlin, TU Berlin). Die UBs von FU Berlin, HU Berlin und TU Berlin verwenden zusätzlich Aleph als lokales Bibliothekssystem. Alle drei genannten Systeme setzen den Patron Directory Service (PDS) von ExLibris als Authentifizierungskomponente ein.

Für die drei genannten Dienste wurde ein Konzept für eine gemeinsame Authentifizierungsplattform entworfen, als Testsystem aufgesetzt und implementiert. Ein SSO-Verfahren für MetaLib und Primo konnte in dieser Testumgebung realisiert werden. Das Aleph-Lokalsystem der FU Berlin sollte in einer eigenen Umgebung durch die FU-Berlin getestet werden. Hierzu muss allerdings noch die produktive Inbetriebnahme des Identity-Providers durch die FU Berlin geleistet werden.

Um ein shibbolethisiertes Zugangssystem des KOBV in den produktiven Betrieb zu überführen, sind folgende Arbeitsschritte notwendig:

- Test der Anbindung an Aleph mit FU Berlin
- Aufnahme des Produktivbetriebs der Service-Provider (in Abhängigkeit vom Stand des lokalen Identity-Providers)
- Anbindung weiterer Identity-Provider anderer Bibliotheken (HU Berlin, TU Berlin)

**BVB:** Die zur Anbindung an Shibboleth vorgesehenen Dienste waren das Gateway Bayern, der Inhaltsverzeichnisdienst sowie die Online-Fernleihe. Da nur wenige Bibliotheken einen lokalen Identity-Provider betreiben, dient ein regionaler Identity-Provider zur Authentifizierung der Benutzer.

Eine Besonderheit des Inhaltsverzeichnisdienstes und der Fernleihe ist der Schutz durch Lazy-Session: Die Anwendungen führen die Authentifizierung bei Bedarf selbst aus. Lazy-Session bietet den Vorteil, dass parallel zu Shibboleth die bisherigen Authentifizierungsmethoden (IP-Check bzw. Anmeldung am AV-Server) weiter betrieben werden können. Das Login am Gateway Bayern wurde auf den regionalen Identity-Provider umgelenkt. Nur bei einer erfolgreichen Authentifizierung wird die Anmeldung am Gateway initiiert. Zur Umsetzung des Konzepts wurden diverse ServletFilter implementiert.

Der regionale Identity-Provider ist kein Identity-Provider im eigentlichen Sinn. Er stellt keine Verbindung zur Nutzerverwaltung *einer* Institution dar, sondern bildet die Schnittstelle zu den Nutzerdaten vieler Bibliotheken. Ein Beitritt zur DFN-AAI ist in dieser Form ausgeschlossen, da dieser nur Institutionen mit eigener Nutzerverwaltung ermöglicht wird. Seit April 2010 betreibt der DFN-Verein die DFN-AAI-Basic, eine Föderation mit weniger restriktiven Bedingungen als die DFN-AAI. Ein Beitritt des regionalen Identity-Providers als auch der Service-Provider zur DFN-AAI-Basic ist anzustreben.

Um ein shibbolethisiertes Zugangssystem des BVB in einen *produktiven* Betrieb zu überführen, sind abschließend folgende Arbeitsschritte notwendig:

- Übernahme der notwendigen Anpassungen an den Produktivsystemen
- Anmeldung des regionalen Identity-Providers sowie der Service-Provider für Fernleihe, Gateway Bayern und Inhaltsverzeichnisdienst bei der DFN-AAI-Basic

---

<sup>4</sup> Informationen und Dokumentationen zum Entwicklungsprojekt:  
<https://wiki.kobv.de/confluence/display/Entwicklungsprojekte/Rechtemanagement>

## Öffentlichkeitsarbeit

Das Projekt wurde mehrmals dem interessierten Fachpublikum vorgestellt:

- "Shibboleth: SingleSignOn statt Multi-Accounting" (Vortrag auf dem 6.KOBV-Forum am 16.06.2008 in Berlin)
- „Aktueller Stand des BVB-KOBV-Entwicklungsprojekts“ (Vortrag auf dem DFN-AAI-Workshop am 7.10.2008 in Cottbus)
- „SingleSignOn für Bibliotheken“ (Vortrag vor dem AK MetaDirectory am 18.02.2009 in Würzburg)

Ein Austausch mit dem DFN-Verein fand außerdem im Rahmen weiterer DFN-Veranstaltungen statt, zuletzt beim 10. Shibboleth-Workshop am 07.04.2010 in Hamburg,

Die Zusammenfassung der *technischen* Dokumentation erfolgt durch Hinterlegung im Projektwiki, während eine allgemeinverständliche Darstellung des Einsatzes von Shibboleth in Bibliotheken mit Projektrückblick durch eine Veröffentlichung eines Artikels in einer bibliothekarischen Zeitschrift erfolgt (angedacht: ABI Technik; Einreichung im 3.Quartal).

Berlin, 7. Juli 2010

Dr. Wolfgang Peters-Kottig, Gunar Maiwald