



SWITCH E-Infrastructure for E-Science Projekt BFH.1

Sharepoint-Moodle e-Learning-Plattform Phase 1

Sharepoint-Moodle e-Learning-Plattform Phase 1:
Voranalyse AAI-Anbindung Sharepoint-Server

Schlussbericht

Auftraggeber	Christian Schmid, HDEL
Projektleiter	Matthias Hutter, BFH-ITS
Autor	Matthias Hutter, BFH-ITS
Letzte Änderung	17. August 2010

Über dieses Dokument

Dieser Schlussbericht ist das eigentliche Produkt des Projekts *Sharepoint-Moodle e-Learning-Plattform Phase 1: Voranalyse AAI-Anbindung Sharepoint-Server*. Er dokumentiert die geleisteten Arbeiten, die dabei gemachten Erfahrungen und die daraus gewonnenen Erkenntnisse sowie Empfehlungen zu Produktwahl und weiterem Vorgehen.

Versionskontrolle

Version	Bemerkung	Autor	Datum
1.0	Initiale Version	Matthias Hutter	29. Juli 2010

Tabelle 1: Versionierung

Inhaltsverzeichnis

1	Management Summary	4
2	Ausgangslage	5
2.1	Ziele	5
2.2	Wahl der Produkte	5
2.3	Vorstellung der getesteten Produkte	6
2.3.1	ActiveShareFS 2007	6
2.3.2	Shib4moss	7
3	Durchgeführte Arbeiten	8
3.1	Aufbau der Testumgebung	8
3.2	Installation der Produkte	8
3.2.1	ActiveShareFS 2007 Pro	8
3.2.2	shib4moss	9
3.3	Tests	10
4	Erkenntnisse	12
4.1	Systembedingte Schwierigkeiten	12
4.1.1	Attribute statt Gruppen	12
4.1.2	Keine umfassende User-Datenbank	12
4.1.3	Ad-hoc Gruppen	12
4.1.4	Zombies	13
4.2	Vergleich der Produkte	13
4.2.1	Installation	13
4.2.2	Gruppenverwaltung	14
4.2.3	Funktionsumfang	15
4.2.4	Support durch den Lieferanten	16
4.2.5	Preis	16
5	Empfehlung	17
5.1	Produktwahl	17
5.2	Weiteres Vorgehen	17
6	Ausblick Phase 2	19

1 Management Summary

Es wurden zwei Produkte, welche Logins via Shibboleth auf einen Sharepoint-Server ermöglichen evaluiert und getestet. Bei *ActiveShareFS* von 9Star Research handelt es sich um ein kommerzielles Produkt und *shib4moss*, das Ergebnis einer Zusammenarbeit der Universität Pierre et Marie Curie und Microsoft Frankreich, steht unter einer Open Source Lizenz.

Die Installation läuft bei beiden Produkten ähnlich ab. Bei der Konfiguration zeigen sich aber deutliche Unterschiede. *ActiveShareFS* setzt auf ein eher umständliches GUI-Programm zur Konfiguration¹, während *shib4moss* komplett mit Konfigurationsdateien parametrisiert wird. Der Funktionsumfang ist *ActiveShareFS* sehr gross. Es funktioniert fast alles, was mit Domain Logins auch möglich ist. *Shib4moss* hingegen bietet nicht viel mehr als das reine Login auf den Server. Allerdings ist *ActiveShareFS* kostenpflichtig und eigene Änderungen sind im Gegensatz zu *shib4moss* nicht möglich.

Wie sich gezeigt hat, sind für eine effektive Integration von Sharepoint in AAI vor allem konzeptionelle Probleme zu lösen. Für eine saubere Integration mit anderen, shibboleth-geschützten Ressourcen (Stichwort: Portal) müssten beide Produkte noch massiv ausgebaut werden. Bevor also mit einer Phase 2 des Projekts *Sharepoint-Moodle e-Learning- Plattform* fortgefahren wird, muss genau geklärt werden, ob der zu erwartende Nutzen den grossen Aufwand rechtfertigt. Die Berner Fachhochschule plant bis auf weiteres keine Phase 2. Dies vor allem aufgrund mangelnder personeller Ressourcen.

Kurz vor Abschluss des Projekts erschien eine neue, komplett überarbeitete Version von *ActiveShareFS*. Aus Zeitgründen konnten die Tests mit der neuen Version nicht wiederholt werden.

¹In der neuesten Version verbessert. Siehe Abschnitt 2.3.1

2 Ausgangslage

Grundlage für das Projekt *Sharepoint-Moodle e-Learning-Plattform Phase 1: Voranalyse AAI-Anbindung Sharepoint-Server* bildet der entsprechende Projektantrag vom 11.11.2009. Er beschreibt die Endziele sowie das grobe Vorgehen.

Vorgehen für Phase 1 (Auszug aus dem Projektantrag):

Es wird eine Marktanalyse und ein Produktvergleich, inkl. Testinstallationen stattfinden, um herauszufinden welches Produkt das Endziel (e-Learning Plattform mit Sharepoint auf AAI und Integration von Moodle-Quiz in Sharepoint) am besten unterstützt. Anhand der getesteten, einander gegenüber gestellten Produkte, wird ein Entscheid getroffen werden und das weitere Vorgehen bestimmt. Als Ergebnis der Analyse werden die folgenden Varianten z. Hd. Phase II erwartet:

- a Abbruch des Vorhabens mit Begründung. Für weitere Phasen werden keine Projekt-Anträge erfolgen.
- b Volle AAI-Integration von Sharepoint (auch User ohne einen AD-Account können sich auf dem entsprechenden Sharepoint-Server über AAI einloggen).
- c Teil-AAI-Integration von Sharepoint: Es können sich vorerst User mit AD-Account der Hochschule die den Sharepoint Server betreibt einloggen.

Die Varianten B und C werden nur weiterverfolgt, wenn das Vorhaben aufgrund der Vor- und Machbarkeitsstudie (Phase I) nicht abgebrochen wird (=Variante A).

2.1 Ziele

Die Ziele des Projekts sind ebenfalls dem Projektantrag zu entnehmen:

- o Die Möglichkeiten Sharepoint in AAI einbinden zu können sind geprüft und die Varianten-Entscheide sind gefällt.
- o Die Single Sign On -Möglichkeiten (SSO/Integrated Authentication) von Sharepoint sind geklärt.
- o Das Produkt für die Einbindung von Sharepoint in AAI ist gewählt.
- o Entscheid Projektantrag für Phase II ist gefällt.

2.2 Wahl der Produkte

Die Markterforschung zu Beginn des Projekts förderte ausser *Active Directory Federation Services* keine Produkte zu Tage, welche nicht schon im Projektantrag bekannt waren. Also wurden die Produkte kurz analysiert, um ihre grundsätzliche Funktion und die Features abschätzen zu können. Aufgrund dieser Voranalyse wurde beschlossen, die Produkte in folgender Priorisierung zu testen:

1. *ActiveShareFS 2007* von 9Star Research, Inc.
2. *shib4moss*, das Ergebnis einer Kooperation von Microsoft Frankreich und der Universität Pierre et Marie Curie
3. *CICme*, eine Eigenentwicklung der University of Illinois
4. *Active Directory Federation Services*, die Lösung von Microsoft für Federated Access Control

Begründung

ActiveShareFS schien das am weitesten entwickelte und sofort einsetzbare Produkt zu sein, also sollte es zuerst getestet werden. Shib4moss, als Open Source Software unter CeCILL verfügbar bot sich für den Schulbetrieb an und hatte eine ausführliche Dokumentation. Daher der zweite Kandidat.

CICme hat als einzige öffentliche Dokumentation eine Präsentation, welche an einem Internet2-Treffen gezeigt wurde. Darin wird es als Lösung für einen sehr spezialisierten Use Case dargestellt. Active Directory Federation Services benötigt immer eine direkte Beziehung zwischen Service- und Identity-Provider, welche einzeln eingerichtet werden muss. Das skaliert schlecht in der Switch AAI Federation. Daher für diese Produkte die Plätze drei und vier.

2.3 Vorstellung der getesteten Produkte

Aus Zeitgründen konnten nur die beiden ersten Produkte getestet werden. Im folgenden Abschnitt werden die beiden getesteten Produkte kurz vorgestellt.

2.3.1 ActiveShareFS 2007

ActiveShareFS (ASFS) ist ein kommerzielles Produkt, welches ermöglicht, via Shibboleth auf einen Sharepoint-Server einzuloggen. Hergestellt wird ASFS von der Firma 9Star Research. 9Star Research ist eine amerikanische Softwarefirma, welche sich auf Single-Sign-On-Lösungen auf der Basis von Shibboleth spezialisiert hat. Auf der Produkt-Homepage² wird ASFS folgendermassen beschrieben:

Using ActiveShareFS, SharePoint administrators can now enable Shibboleth/SAML based authentication for their SharePoint server and facilitate user access using SharePoint Roles. As a result, SharePoint administrators are able to provision access for their SAML authenticated users simply by using the SharePoint PeoplePicker or by configuring ActiveShareFS rules.

Im Projekt wurde *ActiveShareFS 2007 Professional* verwendet und getestet. Kurz vor Abschluss des Projekts erschien eine neue Version von ActiveShareFS, die *ActiveShareFS 2007 SSO Cloud Solution*. Aus Zeitgründen konnten jedoch die Tests mit dieser Version nicht wiederholt werden. Hingegen wurde die neue Version im Rahmen einer Desktop-Sharing-Session durch 9Star Research vorgestellt und erklärt. Deshalb finden sich an einigen Stellen

² <http://www.9starresearch.com/products/activesharefs>

im Dokument Anmerkungen, wo die Funktionalität der neuen wesentlich von der getesteten Version ASFS abweicht.

2.3.2 Shib4moss

Shib4moss ist das Produkt einer Zusammenarbeit von Personen der Universität Pierre et Marie Curie und Microsoft Frankreich. Es ist ein Starterkit, welches Shibboleth-Logins in Sharepoint möglich macht, oder wie es die Projekt-Homepage³ beschreibt:

shib4moss is a starter kit project that demonstrates the integration of Microsoft Sharepoint with Shibboleth identity federation.

The kit comes with a document discribing how Shibboleth works and integrate with Sharepoint. It gives some points on Shibboleth installation and configuration. It explains how to install the binary, Shib4MOSS.dll, and how to configure the Sharepoint web.config.

Shib4moss steht unter der *CeCILL-B* Lizenz frei zur Verfügung. Die französische *CeCILL*-Lizenz wird von der Free Software Foundation als GPL-kompatible Lizenz anerkannt. Vor allem weil shib4moss freie Software ist, wurde es als zweiter Testkandidat ausgewählt.

³ <http://sourcesup.cru.fr/shib4net/shib4moss/shib4moss.html>

3 Durchgeführte Arbeiten

3.1 Aufbau der Testumgebung

Die Testumgebung besteht aus einer virtuellen Maschine pro Produkt. Somit musste die Grundinstallation nur einmal gemacht werden, danach wurde die Maschine für die Installation der Produkte jeweils geklont.

Die Grundinstallation orientierte sich an der produktiven Sharepoint-Farm der BFH. Folgende Software wurde in der Grundinstallation aufgespielt:

- Windows 2003 Standard Edition R2
- Microsoft Office Sharepoint Server 2007 mit Service Pack 1, Installationsoption "Basic", d.h. mit lokalem MS SQL 2005 Express Edition Datenbankserver
- SharePoint Language Packs German und French
- MOSS Server Language Packs German und French

3.2 Installation der Produkte

Vor der Installation des jeweiligen Produkts wurde ein Klon der Grundinstallation erstellt.

3.2.1 ActiveShareFS 2007 Pro

Die Installation von ASFS folgte dem "ActiveShareFS 2007 Installation Guide-3.1"⁴, (nachfolgend "ASFS-Guide").

1. Shibboleth SP (Guide Kap. 4)

Der Shibboleth SP wurde gemäss "Deployment of Shibboleth Service Provider (SP) 2.3.1 on Windows with IIS"⁵ von Switch (nachfolgend "Switch-Guide") für die Switch AAI Federation aufgesetzt und in der Resource Registry mit der EntityID <https://sps-asfs.bfh.ch/shibboleth> registriert. Dabei wurde die Setup-Anleitung im ASFS-Guide im Hinterkopf behalten, um die Vorgehensweise und Einstellungen aus dem Switch-Guide wo nötig an die Bedürfnisse von ASFS anpassen zu können.

2. Erweiterung Sharepoint Web Application

Entsprechend dem ASFS-Guide Kapitel 3.2 wurde die bestehende Sharepoint Web-Application um eine "Extranet" Zone erweitert, welche dann mit ASFS ausgestattet werden sollte. Hier wurde statt eine neue Application zu erstellen, die bestehende Sharepoint-Application erweitert. So steht unter beiden Adressen (Intranet und Extranet) der gleiche Inhalt zur Verfügung. Diese Zone wurde anschliessend im IIS Manager

⁴Alle Dokumentationen von 9Star Research sind vertraulich und werden dem Kunden nur mit der Software zusammen zur Verfügung gestellt.

⁵<https://www.switch.ch/aai/docs/shibboleth/SWITCH/2.3/sp/deployment/windows-iis.html>

entsprechend ASFS-Guide Kapitel 3.3 auf eine eigene IP-Adresse und mit SSL konfiguriert. Als SSL-Zertifikat wurde das vom Shibboleth-Installer erzeugte Self-Signed Zertifikat verwendet.

3. Shibboleth Konfiguration

Konfiguration von Shibboleth (in shibboleth2.xml) gemäss ASFS-Guide Kapitel 5.2

4. Installation und Konfiguration von ASFS 2007 (ASFS-Guide Kap. 6)

ASFS wurde mittels Installer installiert. Anschliessend wurde die Extranet Zone in der Sharepoint Central Administration entsprechend angepasst: Authentication Type, Membership Provider und Role Provider wurden eingetragen, die "Client Integration" wurde aktiviert. Danach wurden die beschriebenen Änderungen in web.config und shibboleth2.xml gemacht.

5. Konfiguration mittels ActiveShareFS Tools (Guide Kap. 8)

Zunächst musste auf dem SQL Server eine Datenbank für die ASFS-Konfiguration erstellt werden. Anschliessend wurde mit "ASFS Database Manager" diese DB angehängt. Schliesslich konnte ASFS mittels "ActiveShareFS Manager" konfiguriert werden.⁶ Diese Konfiguration stellte sich als sehr komplex heraus und konnte nicht ohne Hilfe des 9starresearch-Supports (via Webex) gelöst werden.

6. Erstellen der Business Rules (Guide Kap. 10)

Auch die Business Rules konnten nicht ohne Hilfe vom 9starresearch-Support realisiert werden. Es wurden Business Rules erstellt, welche die User gemäss ihren Shibboleth-Attributen in passende Sharepoint-Gruppen buchen. Beispiele solcher Gruppen sind "BFH Studenten", "VHO-Angehörige" oder "Studenten".

7. Anpassung Logout-Templates

Nachdem der Login in Sharepoint via AAI klappte, wurden die Templates für die Seiten "Sign Out" und "Sign in as a different user" gemäss ASFS-Guide Kapitel 7.1 resp. 7.2 angepasst, um die User in geeigneter Form auf die Modalitäten von Shibboleth-Logins aufmerksam zu machen.

3.2.2 shib4moss

Die Installation von shib4moss folgte dem (französischen) Dokument "Kit de démarrage Extension Web SSO fédéré Shibboleth pour les technologies SharePoint" sowie der (englischen) Kurzanleitung "Shib4MOSS Installation & configuration documentation". Beide Dokumente sind Teil des Shib4moss-Download-Pakets.⁷

1. Shibboleth SP (Etape 1)

Auch hier wurde als erstes der Shibboleth SP mit Hilfe des Switch-Guides installiert. Wo nötig wurde ebenfalls das Vorgehen an die Bedürfnisse von shib4moss angepasst.

⁶Die neue Version ASFS wird in einer zentralen XML-Datei konfiguriert. Der "ASFS Manager" wird also nicht mehr benötigt.

⁷ <https://sourcesup.cru.fr/frs/download.php/2625/Shib4MOSS.zip>

Diese Installation wurde als EntityID `https://sps-shib4moss.bfh.ch/shibboleth` in der Resource Registry eingetragen.

2. **Erweiterung Sharepoint Web Application** (Etape 2)

Die Erweiterung der Sharepoint Web Application wurde entsprechend der Shib4moss-Anleitungen vorgenommen. Zusätzlich wurde wie schon bei ASFS die Extranet Zone im IIS Manager für SSL konfiguriert.

3. **Konfiguration der Extranet Zone** (Etape 3)

Entsprechend der Anleitungen von shib4moss wurden die Anpassungen in der Sharepoint Central Administration für die Extranet Zone gemacht: Single Sign On wurde aktiviert sowie Membership- und RoleProvider eingetragen. Anschliessend wurden die dokumentierten Änderungen an den verschiedenen web.configs gemacht und die Binaries (shib4moss.dll) ins jeweilige bin-Verzeichnis der Web Sites kopiert. Auch der Shibboleth.sso Ordner wurde erstellt.

Wie sich leider erst später herausgestellt hat, hätte bei den einzufügenden Konfigurationsabschnitten der Text "Umpc" überall durch "Upmc" ersetzt werden müssen, damit die Konfiguration lauffähig wird.

4. **Konfiguration der Shibboleth Web SSO Extension** (Etape 4)

Bei den zuvor eingefügten Konfigurationsabschnitten mussten abschliessend die entsprechenden Passagen durch reale Werte ersetzt werden. Diese Werte wurden weitgehend aus den Beispielen in der Shib4moss-Dokumentation übernommen und wo nötig an die bei SWITCHaai genutzten Attributnamen und Werte angepasst.

Leider stellte sich die so erhaltene Konfiguration als nicht lauffähig heraus: User konnten sich zwar über Shibboleth einloggen, erhielten aber danach immer die Fehlermeldung "Access denied", obwohl sie anhand ihrer Berechtigungen hätten auf die Seite zugreifen dürfen. Erst mit der Hilfe des Projektverantwortlichen von shib4moss, Jean Marie Thia von der UPMC konnte das Produkt zum Laufen gebracht werden. Dazu stellte Herr Thia eine virtuelle Maschine mit seiner Konfiguration zur Verfügung. Diese wurde auf der Testplattform installiert und gestartet. Durch Vergleichen der beiden Konfigurationsdateien gelang es schliesslich eine funktionierende Konfiguration zu machen.

3.3 Tests

Die Schwerpunkte der Tests waren:

- Möglichkeiten für Logins via Active Directory Domain und SWITCHaai
- Berechtigungskonzept: Zusammenfassen der User in sinnvolle Gruppen und Rechtevergabe auf diese Gruppen
- Integration der Microsoft Office Client-Anwendungen: Dokumente direkt ab Sharepoint öffnen und wieder abspeichern.

- Management-Funktionen: Delegierbarkeit der User-Einteilung in Gruppen und der Vergabe von Berechtigungen, Benachrichtigung der User per Mail usw.

Nicht getestet wurden die Sharepoint-Workflows und die Integration des Outlook Web Access WebParts. Beide Features werden in der BFH zur Zeit nicht genutzt.

Detaillierte Informationen zu den Tests finden sich in den folgenden Dokumenten:

- Testszenarien
- Testbericht ActiveShareFS 2007
- Testbericht shib4moss

4 Erkenntnisse

4.1 Systembedingte Schwierigkeiten

Die Integration von Sharepoint in eine Shibboleth-Federation stellt einige Herausforderungen, welche unabhängig vom gewählten Produkt sind. Diese Probleme werden im Folgenden erläutert.

4.1.1 Attribute statt Gruppen

Sharepoint-Rechte werden an Gruppen vergeben, z.B. erhält die Gruppe "BFH-Studenten" Leserechte auf einen bestimmten Kurs. Shibboleth-User sind aber per se nicht Mitglied von irgendwelchen Gruppen. Sie verfügen stattdessen über Attribute, z.B. "ist Student" sowie "Account hat BFH als Heimorganisation". Ein Problem das dementsprechend alle Integrationsprodukte lösen müssen, ist das Umlegen von Attributen auf entsprechende Gruppenzugehörigkeiten.

Diese Abbildung von Attributen auf Gruppenzugehörigkeiten ist meist mündlich sehr einfach zu formulieren: "Die Gruppe BFH-Studenten sind alle Shibboleth-User, deren Account von bfh.ch stammt und welche das Zugehörigkeitsattribut Student haben." Dies technisch umzusetzen erfordert aber meist einen hohen Konfigurationsaufwand, welcher zudem immer vom Systemadministrator geleistet werden muss: Er muss die entsprechende Gruppe in Sharepoint erstellen und die Regeln des Integrationsprodukts so anpassen, dass die richtigen User in diese Gruppe gebucht werden.

4.1.2 Keine umfassende User-Datenbank

Ein Shibboleth Service Provider (also eine Applikation mit Shibboleth-Login) kennt nie seine gesamten potenziellen Nutzer, da er keine Möglichkeit hat, die Nutzerliste der Institutionen in der Shibboleth-Federation abzufragen. Ebenso existiert kein (maschinenlesbares) Verzeichnis, welche der Institutionen welche Attribute bereitstellen können.

Stattdessen loggen die User irgendwann zum ersten Mal auf den Service ein und präsentieren ihre Attribute. Der Service erstellt dann typischerweise automatisch einen (lokalen) Account für den Nutzer und identifiziert ihn beim nächsten Besuch anhand eines eindeutigen Attributs. Dieser Account bleibt meist beim Service gespeichert und ist in Folge dort greifbar und kann mit Rechten ausgestattet werden.

Dementsprechend kann sich kein Dienstanbieter eine Liste der zum Zugriff berechtigten Personen anzeigen lassen⁸.

4.1.3 Ad-hoc Gruppen

Die (vom Administrator eingerichteten), attribut-basierten Gruppen wie "Alle Studenten" oder "BFH Dozenten" mögen für die Berechtigung eher allgemeiner Sites genügen. Es gibt aber immer wieder Sites wie z.B. Projektgruppen, welche Personen aus verschiedensten

⁸ Es sei denn, er berechtigt die Accounts einzeln und nicht aufgrund ihrer Attribute, siehe Abschnitt 4.1.3

Departementen und Institutionen enthalten, wo aber nur ein genau definierter Personenkreis berechtigt werden soll.

Es muss also möglich sein, einzelne Benutzer in einer Gruppe zusammenzufassen und zu berechtigen. Dieses Vorhaben wird durch das Fehlen einer vollständigen User-Datenbank (siehe 4.1.2) zusätzlich erschwert. Die Person, welche berechtigt werden soll, ist zum entsprechenden Zeitpunkt eventuell im Sharepoint-System noch gar nicht bekannt.

Hier sind die Integrationsprodukte besonders gefordert. Im Idealfall sollten Personen in die berechtigte Gruppe eingeladen werden können, welche im Sharepoint-System noch gar nicht bekannt sind. Sonst muss der Site-Administrator seine zukünftigen Benutzer bitten, sich vorgängig am Sharepoint Server anzumelden, damit die Accounts in Sharepoint bekannt werden und berechtigt werden können. Eine gute Möglichkeit für solche Einladungen und Gruppen-Management bietet das "Group Management Tool"⁹ von Switch.

4.1.4 Zombies

Ein anderes Problem von dem sämtliche Shibboleth Service Provider betroffen sind, sind die sogenannten "Zombies". Dies sind Accounts von Usern, welche ihre Heimorganisation verlassen haben, die aber im angebotenen Service noch vorhanden sind. Es ist sehr schwierig, diese zu finden und zu eliminieren, denn die Service Provider werden nicht benachrichtigt, wenn ein User seine Heimorganisation verlässt.

Genauere Informationen zum Problem und ein Lösungsansatz sind in der Präsentation "AAI Account Checking" zu finden, welche im Rahmen des AAI OpCom Meeting im September 2009 gehalten wurde.¹⁰

Hier wäre wünschenswert, dass die Integrationsprodukte eine Möglichkeit haben, die Userdatenbank zu durchsuchen und potenzielle Zombies zu identifizieren und zu löschen. Leider bietet keines der getesteten Produkte eine solche Möglichkeit.

4.2 Vergleich der Produkte

4.2.1 Installation

Das Vorgehen für die Installation ist für beide Integrationsprodukte ausgehend von einer Grundinstallation (laufender, domain-integrierter MOSS 2007 Server) in etwa gleich:

- Shibboleth Service Provider Software installieren und für die Shibboleth-Federation (in unserem Fall Switch AAI) konfigurieren
- Sharepoint Webapplication mit einer Extranet-Zone erweitern und die Zone für das entsprechende Integrationsprodukt konfigurieren. Dies erzeugt eine neue Site im IIS Manager
- Die neue Site in IIS Manager konfigurieren: Host-Headers, Ports, SSL, Zertifikate, Shibboleth-Erweiterungen

⁹ Informationen und Download: <http://www.switch.ch/aai/support/tools/gmt.html>

¹⁰ Download unter: <https://www.switch.ch/aai/support/presentations/opcom-200909/>

- Shibboleth SP für die neue IIS-Site konfigurieren
- Produkt-Binaries und Konfiguration ins Webroot kopieren
- Produkt konfigurieren

Beim Aufwand für die Grundkonfiguration unterscheiden sich die Produkt deutlich: Die nötigen Anpassungen an den Konfigurationsdateien sind bei ActiveShareFS klar dokumentiert und einfach umzusetzen, während sie bei shib4moss ziemlich umfangreich sind. Zudem sind die Informationen bei shib4moss über die Dokumentation verteilt, und einige Einstellungen, die offenbar zum Funktionieren nötig sind, gar nicht dokumentiert. (Diese Einstellungen wurden erst spät im Projekt beim Vergleich der Konfigurationsdateien unseres Testservers und einer durch Jean Marie Thia, den Projektleiter von shib4moss, zur Verfügung gestellten Test-VM gefunden und eingepflegt.)

Andererseits ist die Konfiguration von shib4moss mit den Anpassungen an den Konfigurationsdateien abgeschlossen. Bei ASFS sind anschliessend noch einige Schritte zu erledigen:¹¹

- Erstellen einer Datenbank auf dem SQL Server, welche die Konfiguration und Zugriffsregeln von ASFS enthält
- Datenbankzugriff mittels "ASFS Database Manager" konfigurieren
- Die eigentlichen Zugriffsregeln¹² mit dem "ASFS Manager" erstellen.

Dabei ist anzumerken, dass die Bedienung der "ASFS Manager"-Oberfläche einem eher eigenwilligen Muster folgt welches nur wenig mit anderen Windows-Programmen gemeinsam hat, was die Anwendung der Konfigurationsoberfläche zusätzlich erschwert. Allerdings steht einem bei Problemen mit der Konfiguration der 9Star Research Support, wenn nötig via Webex (Desktop-Sharing) und Telefon zur Seite.

Letztendlich wurden für ASFS 27 Arbeitsstunden aufgewendet bis zum ersten Shibboleth-Login auf Sharepoint, bei shib4moss waren es deren 37. Bei beiden Produkten wurde Hilfe vom Lieferanten in Anspruch genommen. Im Fall von ASFS waren das mehrere Mails und zwei Webex-Sessions mit dem 9Star Research Support, bei shib4moss Mails mit dem Projektleiter und die Installation einer vom Projektleiter zur Verfügung gestellten Test-VM.

4.2.2 Gruppenverwaltung

Wie in Abschnitt 4.1.3 erklärt, ist die Gruppenverwaltung eine Königsdisziplin für die Integrationsprodukte. Erstaunlicherweise verfolgen die beiden getesteten Produkte sehr unterschiedliche Strategien.

¹¹Die neue Version von ASFS wird komplett in einer zentralen XML-Datei konfiguriert, daher entfallen diese Schritte

¹²Identity-Provider der Partner-Institutionen, erfragte Attribute, Mapping von Shibboleth-Attributen auf Sharepoint-Attribute, Buchen in Gruppen etc.

Shib4moss auf der einen Seite hat ein sehr einfaches Konzept. Der Administrator definiert in den Konfigurationsdateien, aus welchen Attributen Werte entnommen werden sollen, um Rollen zu bilden. Hier bieten sich z.B. die Affiliation (Student, Dozent etc.) oder die Heimatorganisation (bfh.ch, unil.ch etc.) an. Ebenso definiert er die für ihn relevanten Werte dieser Attribute, welche dann gleichzeitig die verfügbaren Rollen darstellen.

So wird z.B. aus dem Wert *student* im Attribut *affiliation* die Rolle *shibbolethroleprovider:student*, welche mit dem Sharepoint People Picker gefunden und berechtigt werden kann. Leider ist es mit dieser einfachen Strategie unmöglich Rollen zu erstellen, welche mehrere Attribute bedingen, um Mitglied dieser Rolle zu werden. Ein Beispiel wäre die Rolle "BFH-Studenten", welche Affiliation "Student" und Heimatorganisation "bfh.ch" verlangt.

ActiveShareFS verfolgt einen wesentlich flexibleren, aber auch komplexeren Ansatz. Der Administrator definiert über eine beliebig grosse Menge Regeln, welche User überhaupt Zugriff zum Server erhalten, in welche Gruppen diese gebucht werden sowie welche Shibboleth-Attribute in welche Profildfelder übertragen werden. Eine Gruppe wie "BFH-Studenten" lässt sich also problemlos realisieren.

Diese Stärke ist aber gleichzeitig die Schwäche von ASFS. Ein solches Regelset enthält immer alle Bereiche der Konfiguration. Also Herkunfts-Identity-Provider, Attribut-Mapping auf Sharepoint-Profildfelder sowie die Gruppen, in welche User mit dieser Regel gebucht werden. Daher wird der Grossteil einer solchen Regel immer wieder kopiert und ist dann redundant vorhanden, was zu einem unnötig hohen Pflegeaufwand führt. Zudem werden die User beim Login aus allen Sharepoint-Gruppen, in welche sie gemäss Regelset nicht mehr gehören, entfernt. Daher können Shibboleth-User mit ASFS zwar von Hand in Gruppen gebucht werden, verlieren diese Zugehörigkeit beim nächsten Login aber wieder. Dies kann umgangen werden indem diese User direkt und nicht über Gruppen berechtigt werden.

Gemäss Information von 9Star Research soll die neue Version ASFS in diesem Bereich wesentliche Verbesserungen bringen. So soll z.B. der "Group Usecase", also das regelbasierte Buchen von Usern in Gruppen, wesentlich komfortabler möglich sein.

Beide Produkte haben also Unzulänglichkeiten bei der Gruppenverwaltung, welche die effiziente Erstellung und Verwaltung von Gruppen, die die Site-Betreiber dann zur Berechtigung nutzen können, unmöglich machen. Daher werden bei beiden Produkten die Site-Betreiber fast gezwungen, ihre Gruppen selber zu verwalten mit allen Problemen, die dieser Umstand nach sich zieht (siehe Abschnitte [4.1.2](#) sowie [4.1.3](#)).

4.2.3 Funktionsumfang

Beide Produkte bieten die grundsätzliche Möglichkeit, mit Shibboleth-Accounts auf einen Sharepoint-Server zuzugreifen.

Shib4moss bietet darüber hinaus nur die auf Shibboleth-Attributen basierenden Rollen, welche die Site-Betreiber zur Berechtigung nutzen können.

ActiveShareFS bietet die wesentlich grössere Funktionalität. Einerseits die gegenüber shib4moss fast frei konfigurierbare, regelbasierte Gruppenzugehörigkeit, aber auch das Übertragen von Shibboleth-Attributen in die Sharepoint-Profilfelder ist sehr nützlich. So werden Personen anhand ihres Namens einfacher gefunden, und die dem Sharepoint-Server bekannte Mailadresse ermöglicht das Abonnieren von Mail-Benachrichtigungen sowie Massenversände an alle Nutzer der Site. Zudem unterstützt ASFS fast alle "Client Integration" Features wie Dokumente direkt ab Sharepoint öffnen und speichern, Listen in Outlook abonnieren, WebDAV-Folders etc. sofern die Aktion vom Internet Explorer ausgehend gestartet wird. Dies ist für den Benutzer wesentlich bequemer gegenüber shib4moss, welches überhaupt keine Client-Integration bietet.

In Sachen Funktionsumfang liegt ActiveShareFS also klar vorn. Es unterstützt fast alle Funktionen, welche mit Domain Login vorhanden sind.

4.2.4 Support durch den Lieferanten

Für shib4moss gibt es keinen offiziellen Support. Jean Marie Thia, der Projektverantwortliche der Universität Pierre et Marie Curie, gab aber per E-Mail bereitwillig Auskunft und Unterstützung.

Bei ASFS 2007 gibt es offiziellen Support durch die Herstellerfirma 9Star Research. Der Support von 9Star Research erwies sich während der Installation als äusserst hilfreich und kompetent. Auch die Reaktionszeit bei Mail-Anfragen war gut, wurde aber durch die Zeitverschiebung ausgebremst: Die gestellten Anfragen wurden jeweils "über Nacht" beantwortet.

4.2.5 Preis

Shib4moss steht wie bereits in Abschnitt 2.3.2 erwähnt unter der Open Source Lizenz CeCILL. Es ist daher kostenlos erhältlich und darf für beliebige Zwecke eingesetzt sowie nach Belieben angepasst und erweitert werden. ActiveShareFS als kommerzielles Produkt muss hingegen eingekauft werden und verursacht jährliche Kosten für Wartung und Support.¹³ Demgegenüber bietet ActiveShareFS ein wesentlich ausgereifteres Produkt, welches sich sofort einsetzen lässt. Es hat einen für den User fast kompletten Funktionsumfang und die Schule hat die Möglichkeit, bei Problemen auf den kompetenten Support von 9Star Research zurückgreifen zu können.

¹³Preise sind Teil der Offerte von 9Star Research, Inc. an die BFH und unterliegen der Vertraulichkeit.

5 Empfehlung

5.1 Produktwahl

Ist eine Lösung gefordert, die sofort verfügbar ist und viele Features bietet, so empfiehlt sich trotz der Investition und laufenden Kosten ActiveShareFS. Die Lösung von 9Star Research ist stabil, gut dokumentiert, der Hersteller gibt Support und entwickelt das Produkt mit Blick auf Sharepoint 2010 weiter.

Aus Sicht der Community wäre shib4moss als Open Source Produkt sicher die günstigere und unabhängigere Lösung. Im aktuellen Zustand ist shib4moss aber nur ein Starterkit, ein Proof-Of-Concept. Bevor shib4moss produktiv eingesetzt werden kann, ist noch viel Entwicklungsarbeit nötig. Ist man in der Lage und gewillt, diese zu leisten, bietet shib4moss sicher eine gute Grundlage. Jedoch hat man bei shib4moss die Möglichkeit, Anpassungen vorzunehmen sowie weitere Funktionen hinzuzufügen wie z.B. Shibboleth-Portalfunktionen.

5.2 Weiteres Vorgehen

Wie in Kapitel 4.1 beschrieben sind für den Einsatz von Shibboleth-Logins für Sharepoint, unabhängig vom Produkt, einige konzeptionelle Probleme zu lösen. Der Aufwand zur Lösung dieser Probleme sowie für die Installation und Wartung der Integration wird hoch eingeschätzt. Beide getesteten Produkte bedienen grundsätzlich verschiedene Einsatzgebiete. Daher muss vor dem Einleiten weiterer Schritte eine klare Beschreibung des Use Case für die Shibboleth-Logins auf Sharepoint gemacht werden. Bei dieser Beschreibung ist auf folgende Punkte besonders zu achten:

Nutzen Welchen Mehrwert generiert die Möglichkeit der Shibboleth-Logins für die Benutzer und die Institution genau?

Gewünschte Funktionen Welche Sharepoint-Funktionen sollen mit den Shibboleth-Logins genau genutzt werden? Müssen Shibboleth-User nur einloggen und primär Inhalte herunterladen können? Oder sind sie vollwertige Mitglieder, welche auch die Kollaborationsfunktionen nutzen? Ist eine über die reine Login-Möglichkeit hinausgehende Verwendung von Shibboleth im Sharepoint-Umfeld geplant, wie z.B. die Verwendung von Sharepoint als Portal für andere shibboleth-geschützte Ressourcen?

Eigene Kapazitäten Inwiefern wird die Lösung durch Eigenleistungen der einsetzenden Institution unterstützt und gefördert? Sind eigene Entwickler vorhanden, die ggf. eine Weiterentwicklung oder Anpassungen vornehmen können? Wird Support vom Lieferanten benötigt?

Zeithorizont Bis wann soll die Lösung einsatzbereit sein? Auf welcher Version Sharepoint Services wird aufgesetzt?

Im weiteren sind produktabhängig vorbereitend die folgenden Punkte zu klären:

Deployment-Szenario Wo wird das Shibboleth-Login eingesetzt? Wird ein spezieller Sharepoint-Server dafür installiert, oder soll eine bestehende Sharepoint-Farm um Shibboleth-Logins erweitert werden?

Nutzungskonzept Wie greifen die verschiedenen User auf die Inhalte zu? Sollen alle User ihre Shibboleth-Identität nutzen, oder verwenden die User der Heimat-Organisation ihre Domain-Logins?

Verwaltung der Berechtigungen Welche Gruppen für Berechtigungen werden vom Systemadministrator zur Verfügung gestellt? Wie werden Benutzer effektiv auf den Seiten berechtigt? Wie werden Berechtigungen wieder entzogen?
Besonders wichtig ist hier, dass die gewählte Vorgehensweise darauf ausgelegt ist, die Verwaltung der User delegieren zu können. Ebenso ist auf die nötigen Sicherheitsrichtlinien zu achten.

Schulung Site-Admins/User Je nach Nutzungs- und Berechtigungskonzept müssen die Site-Admins und ggf. auch die Sharepoint-Nutzer geschult oder entsprechende Dokumentationen erstellt werden. Inhalte der Schulung und Dokumentation umfassen unter anderem das gewählte Berechtigungskonzept und die zur Verfügung stehenden Funktionen. Die Nutzung der verschiedenen Accounts (Domain und Shibboleth) werden idealerweise erklärt.

Die Site-Admins müssen auf das Problem des nicht vorhandenen Benutzerverzeichnisses (siehe Abschnitt 4.1.2) aufmerksam gemacht werden. Es ist mit ihnen eine Lösung dafür auszuarbeiten.

6 Ausblick Phase 2: Sharepoint-Moodle Integration

Für die im Gesamtkontext angestrebte Integration von Moodle-Inhalten in Sharepoint bieten sich zwei mögliche Strategien an.

Shibboleth Portal In der Variante Portal werden die mit Shibboleth 2.0 eingeführten Funktionen zur Unterstützung von Portalen genutzt. Der Sharepoint-Server würde also als Shibboleth-Portal dienen, um auf die Moodle-Inhalte zuzugreifen. Diese Variante würde eine Weiterentwicklung der Integrationsprodukte bedingen, so dass diese die Shibboleth-Portalfunktionen nutzen können.

Moodle-API Bei dieser Variante werden entsprechende Sharepoint-WebParts programmiert, die direkt auf eine Moodle-API oder, sollte eine solche nicht zur Verfügung stehen, auf die Moodle-Datenbank und -Dateien zugreifen. Shibboleth wäre an diesen Verbindungen also nicht beteiligt.

Hierzu muss den Webparts allerdings die Identifikation der User auf Moodle bekannt gemacht werden. Bei der BFH-Moodle-Installation ist dies die *SwissEduPerson-UniqueID*. Dazu würde sich ActiveShareFS anbieten, da damit die *SwissEduPerson-UniqueID* ins Profil des Benutzers auf Sharepoint übertragen werden kann. Shib4moss müsste dafür zuerst erweitert werden.

Wie diese Analyse gezeigt hat, sind mehrere Produkte auf dem Markt vorhanden, welche je nach genauem Bedarf für eine Integration von Sharepoint in Shibboleth und später von Moodle in Sharepoint geprüft werden können. Eine grundlegende Eigenentwicklung ist also nicht erforderlich. Insbesondere da mit shib4moss bereits eine Grundlage als Open Source Software zur Verfügung steht.

Folgende Schwierigkeiten behindern den Start der Phase 2:

- Die nötigen personellen Ressourcen sind nicht vorhanden
- Der Nutzen ist zu wenig konkret: Ein paar Klicks weniger für die e-Learning-User beim Zugriff auf Moodle rechtfertigen den hohen Aufwand nicht, und eine weitergehende Nutzung ist nicht konkret absehbar.
- Die BFH plant, in der Zukunft auf Sharepoint 2010 zu wechseln. Dafür sind aber noch keine Zeitpläne vorhanden. Ebenso müssten Teile der vorliegenden Analyse mit Sharepoint 2010 wiederholt werden.

Aus diesen Gründen verzichtet die Berner Fachhochschule darauf, die Phase 2 zu beantragen und zu starten.