Benutzerzentrierte Lokalisierung für den Einsatz in Shibboleth-basierten Föderationen

Sebastian Rieger

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG)
Am Fassberg
37075 Göttingen
sebastian.rieger@gwdg.de

Abstract: Benutzer müssen durch die stetig wachsende Anzahl an Web-Anwendungen (nicht zuletzt durch deren gesteigerte Funktionalität, vgl. „Web 2.0“) zunehmend unterschiedliche Benutzernamen und Passwörter verwalten. In der Vergangenheit haben sich für die Vereinheitlichung der dezentralen Authentifizierung und Autorisierung an Web-Anwendungen Föderationen (basierend auf SAML) und benutzer-zentrierte Verfahren (z.B. OpenID) etabliert. Während letztere für Betreiber und Benutzer einfacher zu verwenden sind, haben SAML-basierte Verfahren eine deutlich höhere Verbreitung insbesondere im wissenschaftlichen Umfeld. Das vorliegende Paper beschreibt eine Erweiterung der SAML-basierten Shibboleth Lösung um eine benutzer-zentrierte Lokalisierung in heterogenen IT-Strukturen über mehrere Föderationen hinweg.

1 Dezentrales Identity Management für heterogene IT-Strukturen

Getrieben durch Entwicklungen wie Asynchronous JavaScript and XML (kurz: AJAX) bzw. „Web 2.0“ sind in den letzten Jahren Web-Anwendungen entstanden, die durch die Verschmelzung von Client- und Server-seitiger Dynamik eine weitaus höhere Interaktivität erlauben [Gar05]. Anwendungsbereiche, die zuvor Desktop-Applikationen vorbehalten waren, können nun dezentral über das World Wide Web zur Verfügung gestellt werden. Durch diesen Trend hat sich auch die Anzahl der verfügbaren Web-Anwendungen erhöht. Web-Anwendungen erlauben ein hohes Maß an Dezentralität z.B. für den gemeinsamen Zugriff auf Inhalte über weltweit verteilte Nutzergruppen hinweg. Um die im Web verarbeiteten Daten zu schützen, erfordern die Anwendungen eine erfolgreiche Authentifizierung und Autorisierung der Anwender z.B. über Benutzernamen und Passwörter. Sichere Single Sign-On Lösungen, die dem Benutzer nach einmaliger Anmeldung Zugang zu unterschiedlichen Web-Anwendungen ermöglichen, können durch unterschiedliche Verfahren realisiert werden. Neben spezialisierten Lösungen, die direkt HTTP-Mechanismen wie z.B. Cookies verwenden, existieren in Föderations-basierten (federated identity) und benutzerzentrierten Verfahren (user-centric) offene Standards (vgl. [RiHi08]). Beide erlauben eine dezentrale Authentifizierung und Autorisierung bzw. eine dezentrale Verwaltung und Speicherung der Identitäten.

Benutzerzentrierte Verfahren wie z.B. OpenID erlauben es den Benutzern, selbst zu entscheiden, für welche Web-Anwendungen sie ihre Identität verwenden. Außerdem ermöglichen sie den Benutzern, im Gegensatz zu föderationsbasierten Verfahren, weltweit eindeutige einheitliche Benutzernamen (z.B. E-Mail Adressen oder URLs). Obwohl benutzerzentrierte Verfahren einige weitere Vorteile gegenüber föderativer Authentifizierung bieten, haben letztere u.a. aufgrund des Security Assertion Markup Language (SAML) Standards insbesondere im wissenschaftlichen Umfeld eine größere Verbreitung. Beispielsweise existiert mit der DFN-AAI des DFN-Vereins eine Föderation für deutsche Forschungseinrichtungen, die das SAML-basierte Verfahren Shibboleth einsetzt [DFAAI].

Dieses Paper beschreibt eine Erweiterung für Shibboleth Identity Provider (IdP), die Vorteile von benutzerzentrierten Verfahren für die föderations-übergreifende Authentifizierung verwendet. Die Implementierung erfolgte für die Integration der Föderation der Max-Planck-Gesellschaft (MPG-AAI) in der Föderation des DFN-Vereins (DFN-AAI). Da die 80 Institute der Max-Planck-Gesellschaft (MPG) ihre IT eigenständig verwalten, unterstützt die Erweiterung neben Shibboleth auch andere Authentifizierungsverfahren für den Zugriff auf die Ressourcen in unterschiedlichen Föderationen. Die Mehrzahl der Institute verwendet LDAP-basierte Verzeichnisse für die Verwaltung ihrer Benutzer. Einzelne Institute verwenden Kerberos oder Datenbanken. Einige Institute betreiben bereits eigene Shibboleth Identity Provider für die Authentifizierung und Autorisierung. Auf der anderen Seite gibt es auch kleinere Institute, die keine eigene Benutzerverwaltung durchführen, bzw. die Verwaltung an externe Dienstleister auslagern.

Aufgrund der Funktion als Vermittler zwischen mehreren Föderationen und verschiedenen Authentifizierungsverfahren wird die in diesem Papier vorgestellte Erweiterung als „IdP Proxy“ bezeichnet. Der IdP Proxy ermöglicht es die Eigenständigkeit der Max-Planck-Institute hinsichtlich des Identity Managements aufrecht zu erhalten, ohne alle 80 Institute separat in externe Föderationen (z.B. der DFN-AAI) integrieren zu müssen.

1.1 Föderatives Identity Management in wissenschaftlichen IT-Strukturen

Um die Interoperabilität von Web-basierten Single Sign-On Verfahren unterschiedlicher Hersteller zu gewährleisten, wurde von der OASIS die Security Assertion Markup Language (SAML) als einheitlicher Standard verabschiedet [SAML]. SAML liegt aktuell in der Version 2.0 vor. Bei der Authentifizierung und Autorisierung wird in SAML zwischen dem Service Provider (SP), der die zugriffsbeschränkte Ressource vorhält, und dem Identity Provider (IdP), der berechtigte Identitäten (Benutzernamen, Passwort) bereitstellt, unterschieden. Ein Service Provider kann beispielsweise bei einem Verlag bzw. einem externen Dienstleister implementiert werden. Identity Provider werden dezentral in den Instituten (als „Heimat-Organisationen“) realisiert und ermöglichen die Authentifizierung und Autorisierung der Instituts-Benutzer in SAML-basierten Föderationen. Eine Föderation umfasst mehrere SPs und IdPs, die sich untereinander vertrauen. Dies ermöglicht des über die IdPs angebundenen Benutzern ein Single Sign-On an den von den SPs zur Verfügung gestellten Ressourcen.

Hierfür stellt der IdP nach einer erfolgreichen Authentifizierung ein digital signiertes Token (Assertion) für den Benutzer aus, dessen Signatur durch die SPs überprüft wird. Die Vertrauensstellung wird dabei über X.509 Zertifikate gewährleistet, wie sie z.B. die DFN-PKI [DFPKI] anbietet. Zertifikate und Dienstzugriffspunkte werden in den sog. Metadaten verwaltet, die die Föderation definieren. Für die Autorisierung werden Attribute verwendet, die der IdP zusätzlich zur Assertion bereitstellt und die von den SPs verwendet werden.

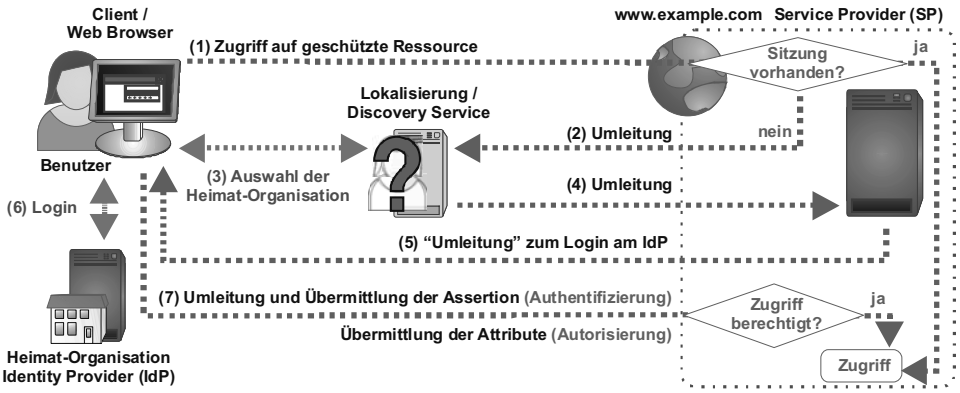

Abbildung 1: Föderatives Identity Management am Beispiel von Shibboleth 2.0.

In wissenschaftlichen IT-Strukturen hat sich das SAML-basierte Shibboleth Verfahren etabliert, das auch bei der DFN-AAI verwendet wird. Abbildung 1 zeigt den Ablauf einer Authentifizierung und Autorisierung bei Shibboleth in der Version 2.0. Für die Lokalisierung des für den Benutzer zuständigen IdPs verwendet Shibboleth einen sog. Discovery Service (DS). Der Benutzer wählt hier die Heimat-Organisation, der er angehört, aus. Ab Shibboleth 2.0 wird auch eine passive Auswahl des zuständigen IdP durch den SP unterstützt. Hierbei erfolgt die Lokalisierung passiv auf Basis der IP Adresse des Clients. Nach dem erfolgreichen Login am IdP übermittelt der Benutzer die von dem IdP ausgestellte Assertion an den SP, der diese prüft und anhand der übermittelten Attribute die Autorisierung durchführt. Konnte die Authentizität des Benutzers erfolgreich geprüft werden und ist dieser anhand der Autorisierung berechtigt, wird der Zugriff auf die Ressource gewährt. Eine Referenz auf die Assertion wird als Cookie für den IdP im Web-Browser gespeichert, so dass ein nachfolgender Zugriff auf eine Ressource eines anderen SPs innerhalb der Föderation keine erneute Anmeldung erfordert. Zusammen mit den am SP aufgebauten Sitzungen (HTTP sessions) wird so ein Single Sign-On innerhalb der Föderation erzielt.

Föderative Authentifizierungsverfahren (insbesondere Shibboleth) sind derzeit sowohl in wissenschaftlichen als auch in wirtschaftlichen IT-Strukturen weit verbreitet. Durch die Interoperabilität des SAML Standards bieten auch viele Software-Hersteller Lösungen für föderative Authentifizierung an (z.B. Microsoft ADFS, Sun OpenSSO oder Novell Access Manager). Andererseits sind die konkreten Implementierungen (z.B. Shibboleth) häufig vergleichsweise komplex zu administrieren.

Für den Benutzer wird zusätzlich die Verwendung komplex, sofern er Ressourcen unterschiedlicher Föderationen verwenden kann. Für jede Föderation muss der Benutzer seine Zugangsdaten verwalten, sowie seinen IdP bzw. seine Heimat-Organisation und zugehörige Föderationen kennen. Die Lokalisierung wird dabei für den Benutzer zusätzlich erschwert, wenn mehrere Föderationen zu einer Konföderation zusammengefasst werden (vgl. eduGAIN [EGAIN]). Er muss in diesem Fall zwei DS Instanzen durchlaufen, und zunächst seine Heimat-Föderation und dann seine Heimat-Organisation auswählen. Neben dem Mehraufwand durch die zusätzliche Auswahl bedingt dies, dass der Benutzer seine Zugehörigkeit zu einer Heimat-Föderation (z.B. DFN-AAI, SWITCH-AAI) überhaupt kennt bzw. namentlich zuordnen kann.

1.2 Benutzerzentrierte Ansätze für das Identity Management

Während die Lokalisierung bei föderativen Authentifizierungsverfahren auf einem zentralen DS basiert, erfolgt sie bei benutzerzentrierten Verfahren dezentral anhand eines vom Benutzer ausgewählten eindeutigen Identifikationsmerkmals. Der Benutzer wählt beispielsweise eine Karte (I-Card), die seine Zugehörigkeit zu einem Provider, der eine ähnliche Funktion wie der Identity Provider in Föderationen realisiert, angibt. Zusätzlich hat er die Möglichkeit auszuwählen, welche Informationen er an den Consumer, der eine ähnliche Funktion wie der Service Provider in Föderationen aufweist, übermitteln möchte. Dies erhöht neben der Usability hinsichtlich der Lokalisierung auch den Datenschutz. Nicht zuletzt durch die vereinfachte Lokalisierung sind Implementierungen benutzerzentrieter Authentifizierungsverfahren in der Regel weniger komplex als Föderationsbasierte. I-Cards werden jedoch noch nicht von allen Web-Browsern für die Authentifizierung an Web-Anwendungen unterstützt. Eine häufig verwendete Alternative für benutzerzentrierte Verfahren bilden daher URLs oder E-Mail-Adressen als Identifizierungsmerkmal der Benutzer. URLs und E-Mail-Adressen werden beispielsweise von OpenID verwendet, das nicht zuletzt aufgrund der Unterstützung durch Google und Yahoo immer mehr an Bedeutung gewinnt.

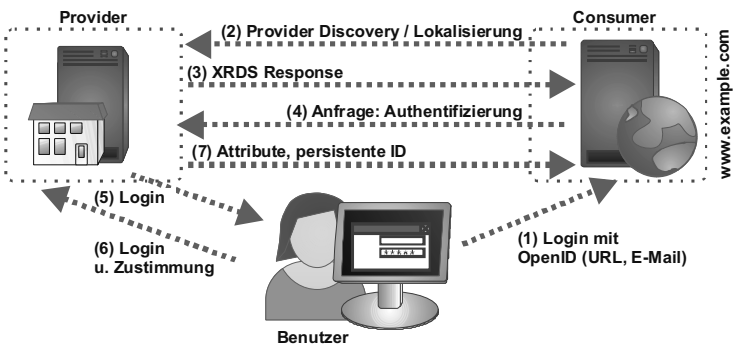

Abbildung 2: Benutzerzentriertes Identity Management mit OpenID.

Alternativen zu OpenID bilden z.B. Microsoft CardSpace oder Higgins. Andere benutzerzentrierte Authentifizierungsverfahren integrieren OpenID (z.B. sxip, OAuth). Zum aktuellen OpenID Standard [OID] in der Version 2.0 existieren einige Erweiterungen, die beispielsweise neben dem Single Sign-On auch die Übertragung von Attributen für die Autorisierung, analog zu den föderativen Authentifizierungsverfahren, erlauben. Ein Beispiel für eine Authentifizierung und Autorisierung mittels OpenID zeigt die Abbildung 2. Der Benutzer meldet sich am Consumer mit seiner OpenID an. Anhand der E-Mail Adresse oder einem Zugriff auf die URL ermittelt der Consumer den zuständigen Provider, an den er anschließend eine Authentifizierungsanfrage richtet. Die eigentliche Authentifizierung erfolgt vom Benutzer über das Login am Provider. Ist die Authentifizierung erfolgreich, so leitet der Provider den Benutzer wieder an den Consumer. Hierbei kann er auch Attribute für die Autorisierung des Benutzers am Consumer übermitteln. Die Autorisierung erfolgt durch die Überprüfung der erforderlichen Attribute am Consumer. Durch die Realisierung einer Sitzung (Cookie) am Provider wird ein Single Sign-On über unterschiedliche Consumer realisiert.

Benutzerzentrierte Verfahren wie z.B. OpenID sind vergleichsweise neu und weisen daher noch einige Sicherheitslücken auf. Beispielsweise wurden einige typische Angriffe auf Web-Anwendungen wie Phishing, Replay Attacken und Implementierungsfehler (z.B. Cross-Site Scripting und Cross-Site Request Forgeries) in [Tsyr07] vorgestellt.

Obwohl für benutzerzentrierte Verfahren kein einheitlicher Standard existiert, hat das OpenID Verfahren seit 2008 eine große Verbreitung erlangt. Dies resultiert vor allem aus der Unterstützung von OpenID durch Google und Yahoo. Allerdings betreiben diese bislang nur OpenID Provider und keine Consumer für ihre eigenen Dienste. Sie vergeben somit lediglich OpenIDs für ihre Benutzer. Benutzer mit einer OpenID (z.B. von Yahoo) können jedoch nicht auf die Dienste von Google oder Yahoo zugreifen. Auf diese Weise sind Benutzer gezwungen nach wie vor separate Accounts bei Google und Yahoo zu registieren. OpenID Consumer werden momentan eher von kleineren Anbietern betrieben, die sich dadurch eine Steigerung der Anzahl ihrer Benutzer erhoffen. Solange große Unternehmen ausschließlich OpenID Provider anbieten, werden auch zukünftig unterschiedliche Benutzernamen bzw. OpenIDs auf der Seite der Benutzer erforderlich sein. Google verwendet zusätzlich Erweiterungen für den OpenID Standard, um z.B. die Anmeldung mittels E-Mail-Adresse zu ermöglichen. Während dies die Usability erhöht, könnte diese Abweichung vom Standard (in der Regel verwenden OpenID Provider URLs) zukünftig auch der Interoperabilität von OpenID schaden und so die Bindung der Kunden an die von Google unterstützten Dienste erhöhen.

Die Bindung der Benutzer an ihren OpenID Provider ist mitunter ein allgemeiner Nachteil von OpenID. Hat ein Benutzer seine OpenID für unterschiedliche Dienste registriert, so ist er abhängig von der Verfügbarkeit der OpenID durch seinen Provider. Fällt der Dienst des OpenID Providers aus oder ändert dieser seine Geschäftsbedingungen, und der Benutzer wechselt den Anbieter, so sind unter Umständen auch die Consumer und dort hinterlegte Daten, für die er seine OpenID verwendet hat, nicht mehr zugänglich.

2 Benutzerzentrierte Lokalisierung mit Shibboleth

Obwohl benutzerzentriertes Identity Management, wie im vorherigen Abschnitt geschildert Vorteile in Bezug auf die geringere Komplexität, einheitliche Lokalisierung und Usability aufweisen, sind SAML-basierte Föderationen derzeit insbesondere in wissenschaftlichen IT-Strukturen das Standard-Verfahren (vgl. z.B. Shibboleth innerhalb der DFN-AAI [DFAAI] in Deutschland, InCommon [INCO] in den USA oder simpleSAMLphp für die FEIDE [FEIDE] Föderation in Skandinavien) für dezentrales Identity Management.

Darüber hinaus existieren neben freien Implementierungen auch kommerzielle Lösungen z.B. in Microsoft ADFS oder Sun OpenSSO. Der SAML Standard ist weitgehend ausgereift und es liegen derzeit keine Sicherheitslücken, wie für OpenID geschildert, vor. Außerdem können Betreiber ihre IdPs in unterschiedliche Föderationen integrieren und so die Abhängigkeit von einem konkreten Provider, wie im vorherigen Abschnitt beschrieben, vermeiden.

Um einige Vorteile benutzerzentrierter Verfahren für föderatives Identity Management nutzbar zu machen, wurden im Rahmen der Realisierung der Föderation der Max-Planck-Gesellschaft (MPG-AAI [MPAAI]) einige Erweiterungen für Shibboleth realisiert, die in den folgenden Abschnitten beschrieben werden.

2.1 Shibboleth IdP Proxy für heterogene IT-Strukturen

Innerhalb der Max-Planck-Gesellschaft bestand die Anforderung Shibboleth für die Authentifizierung und Autorisierung verteilter Forschungsgruppen einzusetzen. Außerdem sollten die ca. 80 Institute Zugriff auf externe Dienstleister bzw. Verlage erhalten, die ihre Authentifizierung und Autorisierung bereits auf Shibboleth umgestellt haben. Die Mehrheit dieser externen Service Provider ist bereits in der ebenfalls Shibboleth-basierten DFN-AAI Föderation des DFN-Vereins integriert. Um die Dienste innerhalb der DFN-AAI für die Benutzer der Max-Planck Institute nutzbar zu machen, wurde eine Anbindung der MPG-AAI an die DFN-AAI angestrebt.

Eine einfache Lösung für die Integration der eigenständigen Institute in die DFN-AAI bildet die Registrierung separater IdPs für jedes Institut der MPG innerhalb der DFN-AAI. Dies hätte jedoch zur Folge gehabt, dass jedes Institut auch einen IdP installieren und warten muss. Aus Sicht des DFN-Vereins war es außerdem nicht wünschenswert, alle 80 Institute der Max-Planck-Gesellschaft separat zu integrieren, da dies die Verwaltung des DS erschwert hätte. Insbesondere wäre hierbei die Verwendung der DFN-AAI aufgrund der Länge der Liste der Heimat-Organisationen (Universitäten, Forschungseinrichtungen) durch die zusätzlichen MPG Institute schwieriger geworden. Benutzer anderer Einrichtungen hätten bei der Auswahl ihrer Heimat-Organisation am DS der DFN-AAI jeweils die 80 Institute der MPG durchgehen müssen. Die MPG-AAI sollte zusätzlich offen für die Integration weiterer Föderationen, z.B. von internationalen Forschungsgruppen oder -netzen, konzipiert werden. Dies schließt auch die eigenständige Integration einzelner Institute in weitere Föderationen mit ein.

Als Alternative zur Registrierung separater IdPs für die Institute wurde daher ein einzelner IdP entwickelt, der als Proxy die gesamte MPG in der DFN-AAI repräsentiert. Dieser „IdP Proxy“ ist dabei sowohl in der DFN-AAI als auch in der MPG-AAI registriert, wie in Abbildung 3 illustriert. Verwenden Benutzer eines Instituts der MPG einen Dienst innerhalb der DFN-AAI, so wählen sie im DS des DFN-Vereins „Max-Planck-Gesellschaft“ aus, und werden zum Login an dem IdP Proxy weitergeleitet. An diesem können sich die Benutzer mit dem Account ihres lokalen Instituts anmelden.

Um die heterogene Struktur der Benutzerverwaltung an den Instituten abzubilden, können Institute bezüglich der Anbindung an den IdP Proxy zwischen drei Optionen wählen, die in Abbildung 3 gezeigt werden.

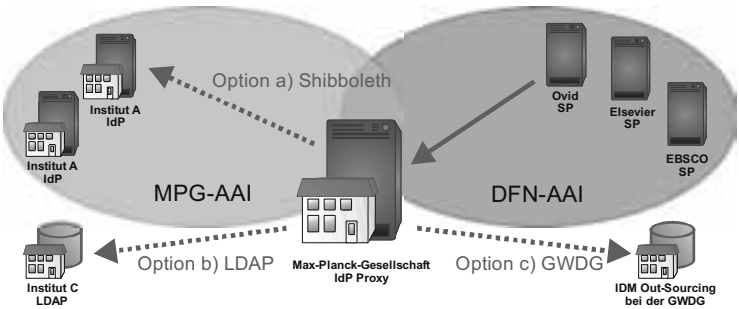

Abbildung 3: Shibboleth IdP Proxy als Bindeglied zwischen heterogenen IT-Strukturen.

Bei dem in Option a) gezeigten Betriebsmodell betreibt das Institut selbst einen Shibboleth IdP innerhalb der MPG-AAI, der dann vom IdP Proxy für die Authentifizierung und Autorisierung verwendet wird. Besitzt das Institut keine eigenen Kapazitäten für den Betrieb eines Shibboleth IdP, so kann auch eine andere bestehende Benutzerverwaltung angebunden werden. Beispielsweise könnte der IdP Proxy gemäß Option b) eine Datenbank, ein Kerberos KDC oder, wie in der MPG am häufigsten verwendet, einen LDAP Server des Instituts abfragen. Innerhalb der MPG existieren darüber hinaus kleinere Institute, die keine eigene Benutzerverwaltung durchführen bzw. diese an externe Dienstleister auslagern. Die Option c) in Abbildung 3 zeigt diese Auslagerung des Identity Mangements an die Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG) als externen Dienstleister. Der IdP Proxy kann zusätzlich zur in Abbildung 3 gezeigten MPG-AAI und DFN-AAI auch in weitere Föderationen aufgenommen werden. Beispielsweise können Föderationen anderer Länder oder Forschungsgruppen am IdP Proxy angebunden werden. Dies unterstützt auch die Fluktuation von Personen und Projekten (z.B. temporäre Aufnahme von Gastforschern etc.). Der IdP Proxy bildet somit eine zentrale Instanz, um dezentrale Authentifizierung und Vertrauensstellungen zu realisieren.

Abbildung 4 zeigt die Implementierung des IdP Proxy als Erweiterung für einen Shibboleth 2.0 IdP. Der Shibboleth IdP ist eine Web-Anwendung die in der Regel in einem Apache Tomcat Application Server läuft. Kern des IdP Proxy ist das Shib Proxy Servlet, das als Login Handler (Auth Engine) in dem Shibboleth IdP konfiguriert wird.

Sofern für Benutzer, die durch einen DS an den IdP Proxy weitergeleitet werden, noch keine Sitzung (basierend auf einem vom Web Browser übermittelten Cookie) am Proxy existiert, wird eine Login-Seite angezeigt. Andernfalls wird vom SSO Profile Modul direkt eine Assertion erstellt, signiert und an den SP übermittelt. Die Login-Seite ist eine Java Server Page, die den Benutzernamen (E-Mail Adresse) und das Passwort an das Shib Proxy Servlet übermittelt. Anhand der Domain der E-Mail Adresse (bzw. dem Realm) ermittelt der IdP Proxy den zuständigen IdP. Die Zuordnung zu den entsprechenden Instituten wird in der Konfiguration des IdP Proxy definiert.

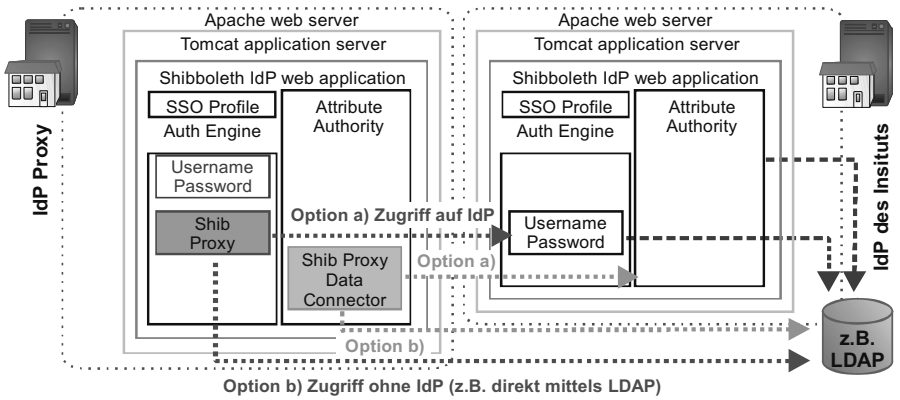

Abbildung 4: Implementierung des IdP Proxy als Erweiterung für den Shibboleth IdP

In Abbildung 4 werden zwei Optionen für die Anbindung eines Instituts an den IdP Proxy beschrieben, die auch in Abbildung 3 gezeigt wurden. Option a) zeigt den Fall, in dem das externe Institut einen eigenen Shibboleth IdP betreibt. In diesem Fall wird die Authentifizierung und Autorisierung direkt an den IdP des Instituts weitergeleitet. Hierbei werden vom Proxy unterschiedliche, von Shibboleth angebotene, Login Verfahren unterstützt (z.B. HTTP- oder Formular-basierte Authentifizierung jeweils für Shibboleth 1.3 und 2.0). Bei der Formular-basierten Authentifizierung fügt der IdP Proxy die auf seiner Login-Seite eingegebene Kennung (der Realm am Benutzernamen kann optional zuvor gefiltert werden) im Formular des IdPs am Institut ein und schickt dieses ab.

Sendet der IdP des Instituts daraufhin eine Assertion (SAML Response) zurück, so wird die enthaltene digitale Signatur anhand der X.509 Zertifikate in den Metadaten der Föderation bzw. der Konfiguration des IdP Proxy überprüft. Sofern die Überprüfung und damit die Authentifizierung erfolgreich war, erstellt der IdP Proxy seinerseits eine Assertion, die er dann z.B. an den externen SP in einer anderen Föderation sendet. Überprüfung und Erzeugung der Assertion im IdP Proxy verwenden analog zum Shibboleth IdP OpenSAML [OSAM]. Der Name Identifier der Shibboleth Sitzung, wird aus der SAML Response extrahiert und im Proxy zwischengespeichert. Dies ermöglicht es, nachfolgende Autorisierungs- bzw. Attributanfragen (wie bei Shibboleth 1.3 verwendet), dem Benutzer zuzuordnen, für den die Assertion erstellt wurde. Dadurch kann das Institut bzw. der IdP ermittelt werden, von dem die Attribute für den Benutzer abgerufen werden müssen. Um die Attribute des Benutzers zu ermitteln, wurde zusätzlich zum Shib Proxy Servlet ein Custom Data Connector für den Shibboleth IdP implementiert.

Scoped Attribute (z.B. „mmuster@institut-a.mpg.de“) werden „prescoped“ verwendet, um die in den Instituten vergeben Scopes im Proxy beibehalten zu können. SAML Attribute Statements an Shibboleth 2.0 IdPs werden digital signiert und geprüft. Verfügt das Institut dem der Benutzer angehört über keinen eigenen IdP, so kann analog zu Option b) und c) aus Abbildung 3, die Authentifizierung gegen ein separates System (z.B. Datenbank, Verzeichnisdienst) erfolgen. Abbildung 4 zeigt hierfür die Option b).

Das Shib Proxy Servlet sowie der zugehörige Data Connector können z.B. JNDI verwenden, um mittels LDAP(S) die Authentifizierung durchzuführen und Attribute des Benutzers zu ermitteln. Alternativ können Datenbanken (über JDBC) oder separate Authentifizierungssysteme (z.B. Kerberos) über JAAS angebunden werden.

Unabhängig von dem durch das Institut gewählten Betriebsmodell können die für den Benutzer ermittelten Attribute vor der Übermittlung an den SP gefiltert oder modifiziert werden. Beispielsweise können Scopes auf „@mpg.de“ geändert oder Attribute, deren Inhalt nur innerhalb der MPG übertragen werden darf, gefiltert werden. Dadurch wird der Datenschutz bei der Übermittlung von Attributen zwischen unterschiedlichen Föderationen gewährleistet. Um den Benutzern vergleichbar mit den benutzerzentrierten Verfahren, wie in Abschnitt 1.2 beschrieben, die Möglichkeit zu geben, die übermittelten Attribute selbst zu kontrollieren, wurde auf dem IdP Proxy der in der Schweiz für die SWITCH-AAI entwickelte ArpViewer [ArpVie] installiert. Der ArpViewer zeigt dem Benutzer alle ermittelten Attribute an und erfordert dessen explizite Zustimmung vor der Übermittlung.

2.2 Integration mehrerer Föderationen ohne zusätzlichen Lokalisierungsdienst

Wie im vorherigen Abschnitt beschrieben, erlaubt der IdP Proxy den Benutzern der MPG Institute Zugriff auf Ressourcen in unterschiedlichen Föderationen zu nehmen. Um hierbei die Vorteile der Lokalisierung anhand globaler Benutzernamen, wie im Abschnitt 1.2 für benutzerzentrierte Verfahren beschrieben, zu nutzen, verwenden die Benutzer für die Anmeldung am IdP Proxy ihre E-Mail Adresse. Anhand der Domain der E-Mail Adresse kann der Proxy das für den Benutzer zuständige Institut sowie das gewünschte Authentifizierungs- und Autorisierungsverfahren ermitteln. Die Benutzer müssen sich daher nur ihre E-Mail Adresse, nicht die Zugehörigkeit zu Institutionen oder unterschiedlichen Föderationen, merken. Anders als bei alternativen Verfahren wie z.B. eduGAIN [EGAIN], die ebenfalls mehrere Föderationen miteinander verbinden, erfolgt für den Benutzer nur eine Lokalisierung. Er muss nur die Max-Planck-Gesellschaft und nicht anschließend in einem weiteren DS das zuständige Institut auswählen. Außerdem kann in den externen Föderationen ein einziger IdP für die gesamte MPG angegeben werden und so die Übersichtlichkeit des DS für den Benutzer gewährleistet werden. E-Mail Adressen werden nur für das Login am IdP Proxy verwendet. Sie werden nicht an die Service Provider übermittelt. Dem SP ist nur eine Shibboleth Sitzung bzw. deren Name Identifier bekannt, über den er z.B. Attribute für den Benutzer anfordern kann. Zusätzlich können übermittelte Attribute auch, wie im vorherigen Abschnitt beschrieben, gefiltert werden.

3 Fazit und Ausblick

Föderative Verfahren für die dezentrale Authentifizierung und Autorisierung an Web-Anwendungen sind insbesondere in wissenschaftlichen IT-Strukturen nach wie vor der Standard. Eine Integration mehrerer Föderationen stellt Herausforderungen für die Usability und den Datenschutz bezüglich der übermittelten Attribute dar.

Der in diesem Paper vorgestellte IdP Proxy adressiert diese Anforderungen für die Institute der MPG. Dabei werden Eigenschaften von benutzerzentrierten Verfahren (z.B. globaler Benutzername in unterschiedlichen Föderationen, einfache Lokalisierung und benutzerzentrierter Datenschutz) in der skizzierten Shibboleth Erweiterung implementiert. Eine Kaskadierung der DS bei der Verbindung mehrerer Föderationen wird hierdurch vermieden. Die Integration mehrerer Föderationen wird auch von anderen Lösungen wie eduGAIN [EGAIN] sowie benutzerzentrierten Verfahren adressiert. Zukünftig sind darauf basierende Erweiterungen für den IdP Proxy realisierbar.

Aktuell befindet sich eine Integration von OpenID im IdP Proxy in der Entwicklung. Benutzer der MPG erhalten dabei eine OpenID (z.B. nach dem Muster https://shib-idp.mpg.de/id/mmuster@inst-a.mpg.de) am IdP Proxy. Auch eine Anmeldung über OpenID auf der Login-Seite des IdP Proxy wäre möglich. Dies würde allerdings eine Konvertierung der übermittelten Attribute erfordern. Momentan bieten die innerhalb der MPG verwendeten Web-Dienstleister noch keine OpenID Consumer an, so dass die Unterstützung von OpenID keine explizite Anforderung darstellt.

Literaturverzeichnis

[ArpVie] SWITCH: uApprove ArpViewer, http://www.switch.ch/aai/support/tools/arpviewer.html, abgerufen am: 12.1.2009.

[DFAAI] DFN: DFN-AAI Einfacher Zugang zu geschützten Ressourcen, http://www.dfn.de/index.php?L=0&id=75522, abgerufen am: 18.1.2008.

[DFPKI] DFN: DFN-PKI Überblick, http://www.pki.dfn.de/, abgerufen am: 18.1.2008.

[EGAIN] eduGAIN: http://www.edugain.org, abgerufen am: 12.1.2009.

[FEIDE] UNINETT: Feide, http://feide.no, abgerufen am: 12.1.2009.

[Gar05] Garret, J. J.: Ajax: A New Approach to Web Applications, http://www.adaptivepath.com/ideas/essays/archives/000385.php, abgerufen am: 12.1.2009.

[INCO] Internet2: InCommon, http://www.incommonfederation.org, abgerufen am: 12.1.2009.

[MPAAI] MPG: MPG-AAI, https://aai.mpg.de, abgerufen am: 12.1.2009.

[OID] OpenID: Specifications, http://openid.net/developers/specs, abgerufen am: 12.1.2009.

[OSAM] Internet2: OpenSAML, www.opensaml.org, abgerufen am: 12.1.2009.

[RiHi08] Rieger S.; Hindermann T.: Dezentrales Identity Management für Web- und Desktop-Anwendungen. In (Müller, P.; Neumair, B.; Dreo Rodosek, G., Hrsg.): Proc. 1. DFN-Forum Kommunikationstechnologien, Kaiserslautern 2008. Gesellschaft für Informatik , Bonn, 2008; S. 107-116.

[SAML] OASIS: Security Services (SAML) TC, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security, abgerufen am: 12.1.2009.

[Tsyr07] E. Tsyrklevich. V. Tsyrklevich: OpenID - Single Sign-On for the Internet (Blackhat USA, 2007), https://www.blackhat.com/presentations/bh-usa-07/Tsyrklevich/Whitepaper/bh-usa-07-tsyrklevich-WP.pdf, abgerufen am: 12.1.2009.