Shibboleth an der Universität Konstanz

Markus Grandpre
Herr Grandpre ist Mitarbeiter des Rechenzentrums der Universität Konstanz

Der Name Shibboleth wurde am Anfang des letzten Jahrzehnts erstmals einem größeren Publikum bekannt, da diese von der Internet2-Middleware-Initiative entwickelte Software die Realisierung eines robusten Single-Sign-On-Verfahren für große Organisationen versprach. Tatsächlich ist der Single-Sign-On-Mechanismus nur ein Nebeneffekt der freien Software, stellt diese doch in erster Linie ein komplexes System zur verteilten Authentisierung und Autorisierung für Webinhalte und Webanwendungen zur Verfügung, welches auf dem freien Standard des zugrunde liegenden SAML-Protokolls (Security Assertion Markup Language) beruht, der ebenfalls von den Entwicklern der Internet2-Middleware-Initiative entworfen und implementiert wurde. Es dauerte nicht lange, bis einige große Verlage die Vorteile dieses verteilten Systems für sich entdeckten, um ihre im Internet veröffentlichten Inhalte mit Hilfe der Shibboleth-Software vor nichtberechtigten Zugriffen zu schützen. Den Verlagen folgten die Bibliotheken, denn Verlage und Bibliotheken sahen in der Anwendung der Shibboleth-Software eine tragfähige Alternative, die bisherige Praxis der statischen Zuweisung von Zugriffsrechten über die Internetadressen einzelner Rechner aus dem Adressbereich einer Organisation langfristig abzulösen und um die Möglichkeit einer variablen und dezentralen Autorisierung zu erweitern, die zudem versprach, die oftmals komplizierten, bilateralen Lizenzregelungen abzubilden zu können. So fanden Verlage und Bibliotheken in Europa mit Shibboleth sehr schnell zueinander und organisierten sich in sog. Shibboleth-Föderationen, um ihren Kunden einen einfachen und sicheren Zugang zur Literaturrecherche im Internet anbieten zu können.

Die Grundidee der Shibboleth-Software ist die verteilte Authentisierung und Autorisierung innerhalb einer Shibboleth-Föderation. Anbieter von Webinhalten, sog. Service-Provider, sind mit Hilfe von Shibboleth in der Lage eigene Autorisierungsregeln zu formulieren, um den Zugriff auf ihre Webseiten, Webanwendungen und die dahinter liegenden Datenbanken zu steuern und zu kontrollieren. Dabei vertrauen sie dem Identity-Management-System der einzelnen Heimateinrichtungen in einer Föderation, den sog. Identity-Providern, dass anfragende Kunden auch tatsächlich Mitglieder der betreffenden Heimateinrichtung sind, denen sie eine unbeschränkte Einsicht in Dokumente und das kostenlose Herunterladen von Dokumenten erlauben können, sofern lizenzrechtliche Bestimmungen zur jeweiligen Heimateinrichtung vorhanden sind und auf das jeweilige Dokument zutreffen.

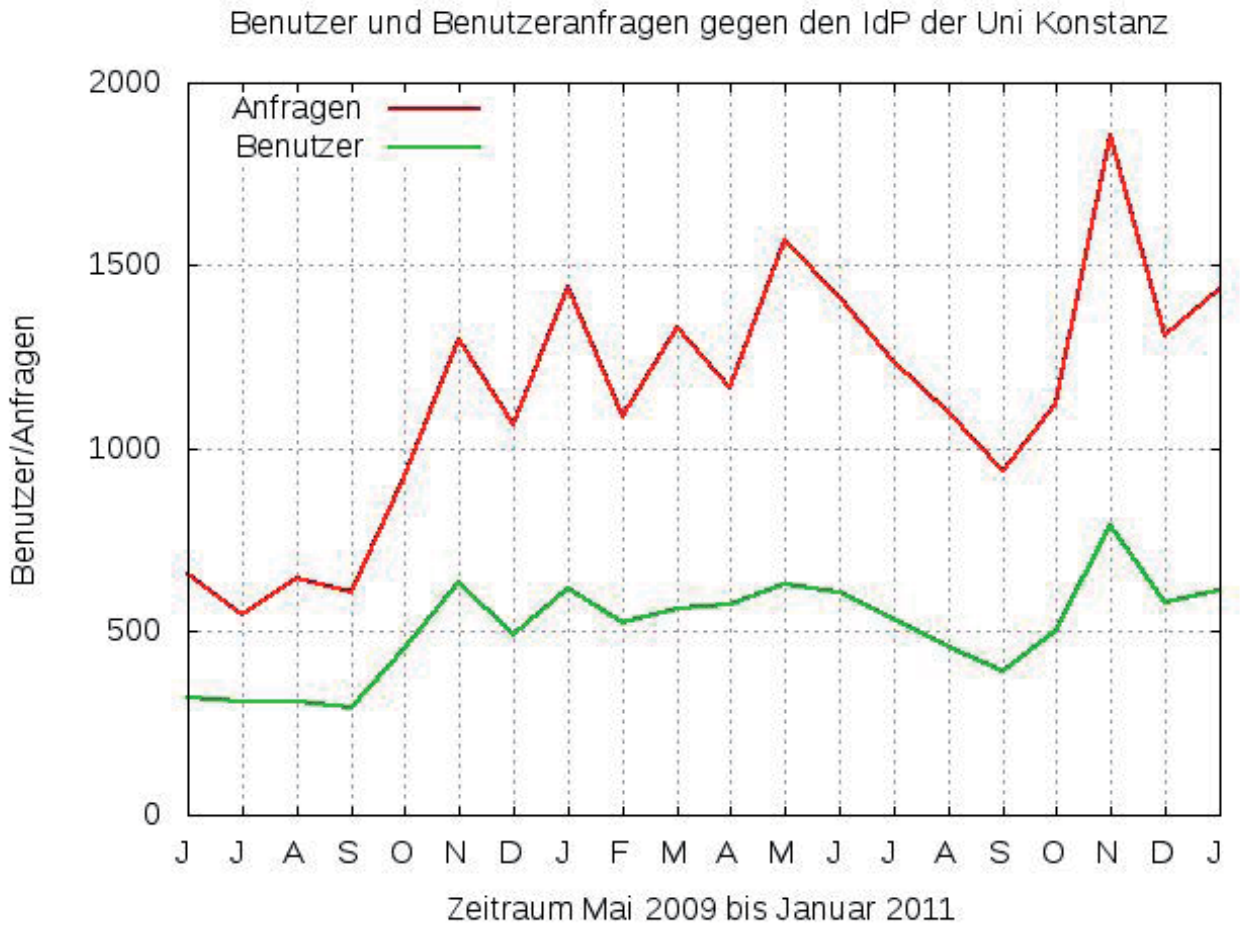
Die Grundidee der Shibboleth-Software ist die verteilte Authentisierung und Autorisierung innerhalb einer Shibboleth-Föderation

Der typische Ablauf einer Literaturrecherche im Internet mit Shibboleth sieht in etwa so aus: Ein Mitglied unserer Universität recherchiert auf den Internetseiten eines Verlags und findet ein Dokument, welches zum Download angeboten wird. Nachdem das Dokument zum Download ausgewählt wurde, wird diese Anfrage an den Identity-Provider der Universität weitergeleitet und das Mitglied muss anhand seiner eindeutigen Benutzerkennung und seines Passworts beweisen, dass es entweder ein Student oder ein Angestellter unserer Hochschule ist. Erst dann wird die Anfrage wieder an den Service-Provider zurückgeschickt, der dann anhand der mitgelieferten Autorisierungsdaten entscheidet, ob der Download freigegeben werden kann. Die bewusst vage Formulierung „in etwa“ weist schon darauf hin, dass der soeben beschriebene Ablauf nicht immer zutrifft. Auch sollte man an dieser Stelle annehmen dürfen, dass das von den Shibboleth-Entwicklern implementierte Single-Sign-On-Verfahren dazu führen sollte, dass das Mitglied sich nur ein einziges mal beim Identity-Provider anmelden muss, um für die Dauer seiner gültigen Shibboleth-Sitzung ohne weiteres andere Dokumente herunterladen zu können. Jedoch ist alle Theorie bekanntlich grau, und dass es in einer Shibboleth-Föderation recht bunt zugehen kann, soll im Laufe dieses Artikels noch zur Sprache kommen.

Seit Dezember 2007 betreibt die Bibliothek und das Rechenzentrum der Universität Konstanz gemeinsam im Rahmen des Serviceverbunds Kommunikation-Information-Medien (KIM) einen Shibboleth Iden-

tity-Provider, der in die Shibboleth-Föderation der Authentifikations- und Autorisierungsinfrastruktur des Deutschen Forschungsnetz (DFN-AAI) integriert ist. Die DFN-AAI verwaltet die Föderation, nimmt aber keinen Einfluss auf die bilateralen Lizenzbestimmungen zwischen den einzelnen Anbietern und Bibliotheken, sie regelt lediglich die technische Realisierung des Datenaustausch von Benutzerdaten, indem sie Verträge mit den einzelnen Anbietern und Heimateinrichtungen abschließt, deren Service- und Identity-Provider in die Föderation integriert und die Mindestanforderungen festlegt, welche Benutzerdaten zur Autorisierung verwendet werden sollen. Sondervereinbarungen, die den Datenaustausch von zusätzlichen Benutzerdaten zwischen Service- und Identity-Providern betreffen und die über die festgelegten Mindestanforderungen hinausgehen, müssen jedoch mit der DFN-AAI abgesprochen werden. In dieser Föderation findet man namhafte nationale und internationale Verlage und Recherchedienste, Hochschulen und Firmen wie de Gruyter, EBSCO, GBI, IEEE, Mircosoft, S. Karger, uva. Im Zeitraum von Anfang Juni 2009 bis Ende Januar 2011 haben 3927 Mitglieder unserer Universität 22769 mal über den Identity-Provider der Universität auf das Angebot der DFN-AAI-Föderation zugegriffen. Dabei fällt auf, dass die Zugriffszahlen nach Schließung der Bibliothek im November 2010 sprunghaft anstiegen, was man vielleicht auf eine Art von Panikreaktion in Form von „Hamster-Recherchen“ zurückzuführen könnte. Zum Jahresende 2010 ist die Anzahl der Anfragen und der anfragenden Benutzer wieder zurückgegangen. So stellte ein Mitglied unserer Universität in der Zeit von Juni 2009 bis Januar 2011 im Durchschnitt zwei bis drei Anfragen im Monat. In diesem Zeitraum wurden die Service-Provider von ScienceDirect (Elsevier) mit 2173 Anfragen, Metapress mit 5147 Anfragen und ReDI (Regionale Datenbank-Information Baden-Württemberg) mit 14223 Anfragen am häufigsten aufgerufen. Auffällig ist auch, dass vier mal so viele Benutzer von zu hause oder von unterwegs Shibboleth zur Literaturrecherche im Internet verwenden als von einem Arbeitsplatz an der Universität. Das Benutzerverhalten deutet also darauf hin, dass das Angebot des KIM-Serviceverbunds, Shibboleth zur Literaturrecherche zu verwenden, neben der Zuweisung der Zugriffsrechte über feste Internetadressen aus dem Campusnetz und der Einwahl ins Campusnetz über das Virtual Private Network, bei den Mitgliedern unserer Universität angekommen ist. Mit Shibboleth ist lediglich ein herkömmlicher Internetbrowser nötig, um weltweit von jedem Rechner im Internet auf das Angebot der DFN-AAI-Föderation zugreifen zu können.

Trotz des hohen Installations- und Konfigurationsaufwands zeichnet sich der Betrieb der Shibboleth-Software durch ihre Robustheit aus. Seitdem der Identity-Provider der Uni Konstanz in Betrieb genommen wurde, treten nur sehr selten technische Fehler auf, die schnell behoben werden können. Supportanfragen, welche die Benutzerberatung von Bibliothek und Rechenzentrum erreichen, enthalten in der Hauptsache lizenzrechtliche Fragen oder betreffen die schlechte Konfiguration einzelner Service-Provider, die nicht nur die Benutzer sondern auch die Benutzerberater bei der Reproduktion des aufgetretenen Fehlers immer wieder ratlos zurück lässt. Verstöße gegen lizenzrechtliche Bestimmungen oder gegen einzelne Autorisierungsregeln werden von manchen Service-Providern sehr deutlich angezeigt, andere Service-Provider verweisen in ihren Fehlermeldungen lediglich auf die eigene Kundenberatung oder die Benutzerberatung der Heimateinrichtung und wieder andere zeigen keinerlei Fehlermeldungen an und schicken auf diese Weise Benutzer und Berater ins Ungewisse. Aufgrund der für Shibboleth charakteristischen Verteilung der Aufgaben von Authentisierung und Autorisierung innerhalb einer Föderation können Benutzer nur schwer nachvollziehen, warum und vor allem an welcher Stelle beim Zugriff auf geschützte Inhalte ein Fehler aufgetreten ist. Zudem bleibt Shibboleth für den Benutzer bis auf die Anmeldung am Identity-Provider unsichtbar. Daher ist es schon vorgekommen, dass Benutzer ihre Supportanfragen an die Kundenberatung des ausgewählten Service-Provider gestellt haben, anstatt sich vor Ort an die Benutzerberatung ihrer Heimateinrichtung zu wenden. Es ist auch für die Benutzerberater nicht immer ersichtlich, an welche Instanz innerhalb der Föderation sie sich wenden sollten, um einen aufgetretenen Fehler zu melden. Hier erweist sich das Team der DFN-AAI-Hotline als zuverlässiger Ansprechpartner, welches zum einen Orientierung verschaffen und in manchen Fällen die Kommunikation mit einzelnen Service-Providern auch moderieren kann. Die Kommunikation mit einigen Anbietern in der DFN-AAI-Föderation kann manchmal recht langwierig sein, sodass es auch bei leicht zu lösenden Problemen für die Berater und somit für die Benutzer zu langen Wartezeiten kommt, bis das Problem endlich gelöst ist. In der Praxis hat sich gezeigt, dass es von Vorteil ist, die in manchen Fehlermeldungen enthaltene Empfehlung, zuerst die Kundenberatung der Anbieter zu kontaktieren, einfach zu ignorieren und stattdessen die administrativen und technischen Verantwortlichen des betreffenden Service-Provider direkt anzuschreiben. Die passenden E-Mail-Adressen sind in den Metadaten der DFN-AAI-Föderation enthalten und sollten den Beratern von Bibliothek und Rechenzentrum zugänglich sein.



Da Shibboleth im Verborgenen arbeitet, ist einem Mitglied einer Hochschule nicht bewusst, welche Daten über das Mitglied vom Identity-Provider seiner Heimateinrichtung an die verschiedenen Service-Provider in der Föderation versendet werden. Die von der schweizer Organisation SWITCH-AAI für Shibboleth entwickelte Software „uApprove“, die den Benutzer auffordert das Versenden seiner Daten zu bestätigen, kann diesem Missstand ein Ende bereiten. Diese Zusatzsoftware wird aber von der Universität Konstanz nicht angewendet, stattdessen beschränkt sich der KIM-Verbund auf die von der DFN-AAI festgelegten Mindestanforderungen, was das Versenden von benutzerbezogenen Attributen anbelangt. So werden zur Autorisierung bei Service-Providern von jedem Mitglied der Universität Konstanz, welches entweder Student oder Angestellter der Uni ist, lediglich die Attributwerte „member@uni-konstanz.de“ und „common-lib-terms“ innerhalb der Föderation versendet, die das Mitglied seiner Heimateinrichtung zuordnen und es darüber hinaus berechtigen, kostenlos auf geschützte Inhalte einiger Anbieter zuzugreifen. Diese Vorgehensweise entspricht natürlich nicht dem bereits genannten Anspruch an die Shibboleth-Software, die komplizierten, bilateralen Lizenzbestimmungen zwischen der Universitätsbibliothek und den verschiedenen Verlagen vollständig abzubilden, sodass während der Literaturrecherche im Internet nicht immer ersichtlich ist, welches Dokument von welchem Service-Provider nun eingesehen und heruntergeladen werden darf. Zudem gibt es Service-Provider, welche die Mindestanforderungen der DFN-AAI zwar einhalten, aber dennoch um eigene Spielregeln erweitern. Ein Beispiel ist der kostenlose Download der Produkte eines prominenten Softwareherstellers, der neben der Zugehörigkeit zu einer deutschen Hochschule ebenfalls den Erwerb einer sog. „Live ID“ erforderlich macht. Es gab in der Vergangenheit auch schon den Fall, dass ein Service-Provider die persönliche E-Mail-Adresse eines Mitglieds unserer Universität zur Erfüllung seiner Autorisierungsregeln eingefordert hat. Selbstverständlich wurde diese Anforderung vom Identity-Provider nicht umgesetzt, was allerdings zur Folge hatte, dass das Rechercheangebot dieses Anbieters für die Mitglieder unser Universität nicht zur Verfügung stand.

In einer Föderation führen viele Wege zu einem erfolgreichen Download geschützter Inhalte. Manche Mitglieder unserer Universität finden ihren Weg über die Portalseiten der Universitätsbibliothek, manche rufen die Webinhalte direkt auf den Seiten der Anbieter auf, um dann zum Identity-Provider ihrer Heimateinrichtung weitergeleitet zu werden.

Manche beginnen erst mit ihrer Recherche, um dann nach erfolgreicher Anmeldung bei ihrer Heimateinrichtung die gefundenen Dokumente herunterzuladen. Manche Benutzer melden sich zuerst bei Ihrer Heimateinrichtung an, um dann mit ihrer Recherche zu beginnen. Der oben bereits vorgestellte „typische“ Ablauf einer Authentisierung und Autorisierung mit Shibboleth ist somit nur eine Möglichkeit von vielen. Diese Vielfalt an Zugriffsmöglichkeiten ist zum einem den Vorlieben der Benutzer bei ihrer Literaturrecherche im Internet geschuldet, zum anderen kann man feststellen, dass jeder Service-Provider einen eigenen Weg vorgibt, an geschützte Dokumente zu gelangen, wobei es manchmal den Anschein hat, dass einige Anbieter den Zugang zu ihren geschützten Inhalten mit Shibboleth eher stiefmütterlich behandeln und nicht nur ihre eigene Kundenanmeldung in den Vordergrund stellen, sondern den Zugang für die berechtigten Mitglieder einer Hochschule auch noch verstecken oder ungenügend warten. Beim Zugang zu den geschützten Inhalten mit Shibboleth spielt die Auswahl der Heimateinrichtung eine wichtige Rolle, welche von vielen Service-Providern selbst implementiert wird, anstatt die zentrale Auswahl der Heimateinrichtung zu verwenden, welche von der DFN-AAI bereitgestellt wird. Um den Identity-Provider der Universität Konstanz auf den Seiten der Anbieter zu finden, müssen dem anfragenden Benutzer unterschiedliche Auswahloptionen wie z.B. „Athens /institution login“ oder „German Higher Education & Research (DFN-AAI)“ bekannt sein. Um den Zugang zu den geschützten Inhalten der DFN-AAI-Föderation für die Benutzer und die Benutzerberatung von Bibliothek und Rechenzentrum nachvollziehbar und übersichtlich zu gestalten, kam im Herbst letzten Jahres die Idee auf, sich das Single-Sign-On-Verfahren zu Nutze zu machen und eine eigene mit Shibboleth geschützte Seite zum Einstieg in die Föderation anzubieten. Die Mitglieder unsere Universität würden dann nach Aufruf eines eigenen, von der Universität Konstanz betriebenen Service-Provider, auf dessen Seiten sie zudem detaillierte Informationen über das Angebot der DFN-AAI-Föderation finden sollten, sofort auf die zentrale Anmeldeseite des Identity-Providers der Universität gelangen und wären nach erfolgreicher Authentisierung für die anderen Service-Provider der Föderation automatisch freigeschaltet, sofern die jeweiligen Anbieter Lizenzregelungen mit der Universitätsbibliothek unterhalten und sich an die Mindestanforderungen der DFN-AAI halten. Leider konnte diese Idee nicht umgesetzt werden, da bei einem Wechsel zu einem anderen Service-Provider die Information verloren geht, dass es bei dem anfragenden Benutzer um ein Mitglied der Universität Konstanz handelt. Der Einsatz eines eigenen Service-Providers hätte somit zur Folge, dass einem Mitglied unserer Universität eine weitere Anmeldung beim Identity-Provider der Uni zwar erspart bleiben würde, dass der Benutzer sich aber nach wie vor bei jedem Service-Provider dennoch bis zur Auswahl seiner Heimateinrichtung durchklicken müsste, da der Attributwert „member@uni-konstanz.de“ erst nach der Auswahl des Identity-Providers wieder an den Service-Provider versendet wird.

Wie schön wäre es doch, wenn man zu Beginn seiner Arbeit sich nur ein einziges Mal am Identity-Provider unserer Hochschule anmelden müsste, um dann den Tag über bis zur Abmeldung nicht nur die Dienste zur Literaturrecherche, sondern auch alle anderen auf dem Campus angebotenen Dienste von Bibliothek, Rechenzentrum, Verwaltung und den einzelnen Fachbereichen und Abteilungen nutzen zu können, ohne ständig auf verschiedenen Anmeldeseiten unterschiedliche Benutzerkennungen und Passwörter eingeben zu müssen. Es wäre doch ebenfalls wünschenswert, dass verschiedene Hochschulen, Firmen und andere Organisationen sich in regionalen, nationalen und internationalen Shibboleth-Föderationen zusammenschließen, um den Zugang zu ihren Diensten für die Zusammenarbeit ihrer Mitglieder mit Shibboleth einfach, effizient und sicher zu gestalten. Doch trotz aller Hoffnungen, die im letzten Jahrzehnt in das von den Shibboleth-Entwicklern implementierte Single-Sign-On-Verfahren gesetzt wurden, liegt die Anwendung dieses Verfahrens zu Beginn des neuen Jahrzehnts noch sehr im Argen. Die Gründe dafür sind schnell genannt. Shibboleth dient in erster Linie dem Schutz von Webinhalten und Webanwendungen, obwohl es bis heute Bestrebungen gibt, das Single-Sign-On-Verfahren auch für andere Anwendungen, z.B. das Grid-Computing, verfügbar zu machen. Dennoch liefern viele Anbieter kommerzieller und freier Software ihre Software ohne Shibboleth-Unterstützung aus, so bleibt die Anpassung von Standardsoftware an Shibboleth oftmals proprietär, undokumentiert und unveröffentlicht, ist somit sehr aufwendig und nur dann zu realisieren, wenn der Quelltext der Software offenliegt. Leider sind auch die Entwickler der Shibboleth-Software bis heute noch nicht so weit, zum bereits implementierten Single-Sign-On-Verfahren ein ebenso robustes Single-Logout-Verfahren anbieten zu können. Und so verführerisch die Möglichkeiten einer campusweiten und campusübergreifenden Anwendung von Shibboleth auch klingen mögen, der Betrieb der Shibboleth-Software an der Universität Konstanz bleibt bis auf weiteres auf die Literaturrecherche im Internet beschränkt.