Dezentrales Identity Management für Web- und Desktop-Anwendungen

Sebastian Rieger, Thorsten Hindermann

Arbeitsgruppe IT-Infrastruktur
Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen (GWDG)
Am Fassberg
37075 Göttingen
sebastian.rieger@gwdg.de, thorsten.hindermann@gwdg.de

Abstract: Identity Management Lösungen werden auch in wissenschaftlichen IT-Strukturen seit einigen Jahren für die Vereinheitlichung der Authentifizierung und Autorisierung eingesetzt. Die erzielte Vereinheitlichung ist jedoch in der Regel auf einen Standort begrenzt. Für externe, fluktuierende Benutzer (z.B. standortübergreifende Forschungsgruppen) müssen häufig nach wie vor in verschiedenen Anwendungen separate Benutzerkonten angelegt werden. In Bezug auf Desktop-Anwendungen umfasst dies beispielsweise die Anmeldung an lokalen Rechnern in CIP-Pools kooperierender Universitäten, den Zugriff auf IT-Dienste oder den Funk-LAN Zugang für Gast-Wissenschaftler. Lösungen für dezentrale, föderationsbasierte (z.B. Shibboleth) Authentifizierung, die diese Probleme adressieren, sind derzeit auf Web-Anwendungen beschränkt. Gegenstand dieses Papers ist die Implementierung von Erweiterungen für die Verwendung föderationsbasierter Authentifizierungsverfahren an Desktop-Anwendungen. Es werden Ansatzpunkte für ein plattform- und anwendungsübergreifendes Identity Management unter Verwendung bestehender Standards aufgezeigt.

1 Benutzerverwaltung in wissenschaftlichen IT-Strukturen

In den folgenden Abschnitten werden die charakteristischen Anforderungen an die Benutzerverwaltung in wissenschaftlichen Rechenzentren erläutert. Abschnitt 1.1 beschreibt anhand der Heterogenität wissenschaftlicher IT-Strukturen die Notwendigkeit zur Automatisierung der Benutzerverwaltung mithilfe eines geeigneten Identity Managements. Dezentrale Zugriffe von externen Benutzern auf die von den Rechenzentren angebotenen IT-Dienste bilden die Grundlage für den Bedarf an dezentraler Authentifizierung und dezentralem Identity Management.

1.1 Heterogenität der IT-Strukturen und Identity Management

Benutzer wissenschaftlicher IT-Strukturen verwenden in der Regel IT-Dienste, die auf unterschiedlichen Plattformen (z.B. Microsoft Windows, Linux) bereitgestellt werden. Die Heterogenität der Plattformen, und damit der IT-Strukturen, kann neben Präferenzen der Benutzer, z.B. bedingt durch spezielle Funktionen und erforderliche Eigenschaften der Plattformen, auch aus deren historischer Entwicklung resultieren. Reine Windows- oder reine Unix-Umgebungen lassen sich an Rechenzentren nur selten etablieren. Teilweise ist die Heterogenität sogar erwünscht, um die negativen Auswirkungen einer Monokultur z.B. bei Implementierungsfehlern oder Sicherheitslücken zu reduzieren [Rie07].

Für die Benutzer und Betreiber der IT-Strukturen bedeutet dies, dass separate Benutzerkonten (z.B. mit separaten Passwörtern) für die einzelnen Anwendungen verwaltet werden müssen. So verwenden beispielsweise Windows (in der Regel NTLM) und Unix (z.B. crypt, (S)MD5, (S)SHA1) unterschiedliche Verfahren für die Passwortspeicherung. Benutzer sehen sich dadurch mit unterschiedlichen, separat zu verwaltenden Passwörtern z.B. für die Anmeldung an ihrem Desktop, ihrem E-Mail-Programm, geschützten Web-Seiten etc. konfrontiert. Da die Passwörter in den einzelnen Anwendungen als Hash-Werte bzw. irreversibel verschlüsselt gespeichert werden, entstehen neben dem erhöhten Verwaltungsaufwand für die Betreiber durch die Diversität der Passwörter zusätzlich Einschränkungen bei der Skalierung der IT-Struktur. Diese behindern die Integration neuer Anwendungen, die bis dahin nicht abgedeckte Hash- bzw. Authentifizierungsverfahren verwenden.

Aufgrund der beschriebenen Heterogenität wissenschaftlicher IT-Strukturen können, insbesondere in Kombination mit hohen Komplexitätsanforderungen an die verwendeten Passwörter, neben dem erhöhten Aufwand bei deren Verwaltung und Verwendung auch Sicherheitsrisiken die Folge sein. Diese können aus der Reaktion der Benutzer auf die Komplexität entstehen, die die Passwörter für Dritte leicht zugänglich am Arbeitsplatz aufschreiben oder direkt in der Anwendung ohne weitere Schutzmaßnahmen speichern.

Für die Betreiber entsteht durch die im vorherigen Abschnitt skizzierte Heterogenität ein hoher Aufwand für die Verwaltung der unterschiedlichen Authentifizierungsmerkmale und -verfahren. Aus der Heterogenität können unter Umständen auch seitens der Betreiber Sicherheitsrisiken entstehen, wenn die Administration der Sicherheitsmaßnahmen zu komplex wird. Die Komplexität kann zudem durch zu viele zu berücksichtigende Ausnahmen (z.B. Zugriff für Gäste, Externe etc.) erhöht werden [Rie07].

Um die Verwaltung für Benutzer und Betreiber zu vereinfachen und über die Plattformen hinweg zu vereinheitlichen wurden in den vergangenen Jahren Lösungen für das Identity Management realisiert. Eine Übersicht über diese Entwicklung wird in [Win05] gegeben. Die Lösungen erlauben eine Reduktion des Aufwands für die Benutzer und Betreiber durch eine Vereinheitlichung der Authentifizierungsmerkmale sowie Authentifizierungs- und Autorisierungsverfahren. Adressiert werden somit Sicherheitsmechanismen für die Authentifizierung, Autorisierung und Abrechung (Authentication, Authorization, Accounting kurz: AAA).

AAA-Lösungen lassen sich dabei in die in der nachfolgenden Abbildung gezeigten Kategorien einteilen. Die Teilmenge der Lösungen, die eine vereinheitlichte Verwaltung dezentraler Benutzerkonten bzw. Identitäten wird dabei dem Identity Management zugeordnet.

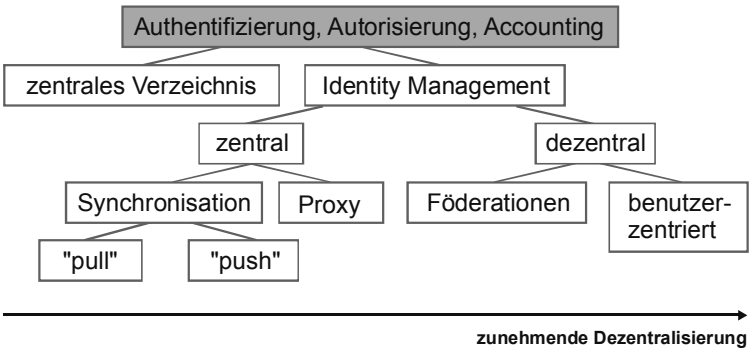

Abbildung 1: Dezentralisierung der Verwaltung von Identitäten.

Zunächst wurden AAA-Lösungen als zentrale Komponenten für die Integration der Benutzerkonten unterschiedlicher Systeme und Anwendungen entwickelt (z.B. NIS, LDAP-Verzeichnisse). Mit zunehmender Anzahl dieser zentralen Lösungen wurde deren eigene Integration erforderlich, die aufgrund der fehlenden Kompatibilität der Systeme anwendungs- und plattformübergreifende Identity Management Lösungen notwendig machte. Identity Management wurde in den letzten Jahren überwiegend zentral an einem Standort betrieben (z.B. Synchronisation über Meta-Directories oder Integration in Virtual Directories als Proxy). Um eine standortübergreifende Verwaltung von Identitäten zu erlauben, werden aktuell Föderationen bzw. ein föderiertes Identity Management realisiert (vgl. DFN-AAI [DFNA]). Basis dafür bilden in der Regel Authentifizierungsverfahren, die auf der Security Assertion Markup Language (kurz: SAML) basieren oder diesen Standard verwenden. Beispiele für Implementierungen sind Shibboleth [Shib], Active Directory Federations Services (kurz: ADFS) [ADFS] sowie das Liberty Project [Lib]. Ein Treiber für das dezentrale Identity Management sind die Probleme zentraler Identitätsverzeichnisse, wie z.B. die Einhaltung des Datenschutzes. An der Spitze dieser Entwicklung stehen die benutzerzentrierten Verfahren, bei denen der Benutzer die Verwaltung seiner Identitäten selbst bestimmt und z.B. in Form von sog. Karten verwaltet. Beispiele hierfür sind sxip [sxip], Ping [Ping] und Microsoft CardSpace [CS].

Ausgehend von der zentralisierten Verwaltung der Identitäten lässt sich aus der Abbildung ein Trend zum dezentralen Identity Management erkennen, der durch die ubiquitäre und standortübergreifende Bereitstellung von IT-Diensten für unterschiedliche Benutzergruppen zusätzlich verstärkt wird.

1.2 Dezentraler Zugriff und externe Benutzer

Aufgrund der weltweiten Vernetzung der IT-Strukturen sehen sich die Betreiber wissenschaftlicher Rechenzentren hinsichtlich ihrer Benutzerverwaltung mit einer zunehmenden Menge externer Benutzer konfrontiert. Diese können beispielsweise aus Kooperationen in der Forschung über verschiedene Standorte hinweg oder durch die Fluktuation von Gast-Wissenschaftlern usw. entstehen. Häufig müssen Forschungsgruppen, beispielsweise im e-Science bzw. Grid-Umfeld, weltweit Zugriff auf die von ihnen verwendeten Ressourcen erhalten. Aber auch Studierende kooperierender Hochschulen sollen beispielsweise dezentral Ressourcen (z.B. Lehr- und Lernmanagementsysteme) verwenden können. Dies umfasst nicht nur Web-Anwendungen, sondern auch den Zugang zu Rechnern (z.B. in CIP-Pools), Netzwerken (z.B. Funk-LAN) und File-Servern sowie Peripheriegeräten (z.B. Drucker). Zusätzliche Benutzerkonten, Passwörter für die externen Benutzer und die jeweilige Anwendung (vgl. Abschnitt 1.1) sind die Folge und erhöhen erneut die Heterogenität der Sicherheitsmaßnahmen innerhalb der IT-Struktur. Dies stellt auch für die Vergabe von X.509 Zertifikaten an dezentrale Benutzergruppen innerhalb von Public-Key-Infrastrukturen ein Problem dar [Rie06].

Darüber hinaus können erneut Sicherheitsrisiken bei der sicheren Übermittlung der neu vergebenen Zugangsdaten an die dezentralen, und den Betreibern der IT-Struktur unbekannten bzw. fluktuierenden, Benutzer entstehen. Ein weiteres Sicherheitsproblem bildet die gezielte Einschränkung resp. Autorisierung der Benutzer. Sollen diese ausschließlich Zugriff auf die z.B. gemeinsam im Forschungsprojekt verwendeten Ressourcen, aber keine anderen Dienste innerhalb der IT-Struktur erhalten, so werden in der Regel separate Benutzerkonten eingerichtet, die erneut die Heterogenität erhöhen. Im einfachsten Fall kann dies zur Folge haben, dass Benutzerkonten und Berechtigungen auch lange Zeit nach dem Austritt des Benutzers aus dem Projekt bzw. der Forschungsgruppe an verschiedenen Standorten weiter existieren.

2 Dezentrales Identity Management

Um den dezentralen Zugriff durch externe Benutzer auf Dienste innerhalb wissenschaftlicher IT-Strukturen zu erlauben, und die im Abschnitt 1.2 genannten Probleme zu adressieren, ist ein dezentrales Identity Management, wie es in Abbildung 1 erläutert wurde, erforderlich. Durch dezentrales Identity Management können Benutzerverwaltungen unterschiedlicher Standorte integriert werden, und so übergreifende Kooperationen und Projekte unterstützen. Für Web-Anwendungen haben sich in diesem Zusammenhang bereits Lösungen anhand einer föderationsbasierten Authentifizierung und Autorisierung etabliert (vgl. Federated Identity in [Win05]). Diese werden in den folgenden beiden Abschnitten erläutert. Abschnitt 2.2 zeigt basierend auf den hierbei herausgearbeiteten Problemen und Anforderungen Möglichkeiten für ein dezentrales Identity Management bzw. eine dezentrale Authentifizierung über die Grenzen von Web-Anwendungen hinweg. Es werden Implementierungen beschrieben, die die Verwendung der bestehenden Lösungen für die Authentifizierung an Desktop-Anwendungen erlauben.

2.1 Web-basierte Föderationen und benutzerzentriertes Identity Management

Die im Abschnitt 1.1 beschriebene Vereinheitlichung und Vereinfachung der Verwaltung heterogener AAA-Systeme lösen die im Abschnitt 1.2 genannten Probleme durch zunehmend dezentrale Zugriffe externer Benutzer auf wissenschaftliche IT-Strukturen nur bedingt. Im Rahmen des Identity Managements können beispielsweise spezielle Rollen für die externen Benutzer definiert werden. Diese ermöglichen es, den Zugriff für Externe gezielt zu autorisieren bzw. den Zugriff auf die übrigen Dienste der IT-Struktur zu verweigern. Entsprechend rollenbasierte Lösungen (vgl. RBAC [San00]) führen jedoch zu einer erhöhten Komplexität in Bezug auf die Administration der IT-Struktur. Proxy-Systeme können die Authentifizierung und Autorisierung der Benutzer an verteilte Standorte weiterleiten. Sie müssen jedoch erneut als separate Authentifizierungssysteme verwaltet werden, und erhöhen somit ebenfalls die Komplexität der Administration.

Eine akzeptable Lösung stellen dezentrale Authentifizierungsverfahren dar, die z.B. Föderationen über unterschiedliche Betreiber hinweg realisieren. Häufig werden diese unter dem Begriff Authentication and Authorization Infrastructure (kurz: AAI) zusammengefasst. Man spricht in diesem Zusammenhang in Bezug auf die verwalteten Identitäten auch von „federated identity“ [Win05]. Als Standard für die Interoperabilität dieser Föderationen existiert SAML [SAML], auf der z.B. das in wissenschaftlichen IT-Strukturen häufig verwendete Authentifizierungsverfahren Shibboleth [Shib] basiert. Alternativen dazu bieten beispielsweise der Central Authentication Service (kurz: CAS) [CAS], Liberty [Lib] oder Microsoft ADFS [ADFS], die sich ebenfalls auf den SAML Standard ausgerichtet haben. Um eine dezentrale Authentifizierung zu erlauben, werden bei den föderationsbasierten Verfahren Service (kurz: SP) und Identity Provider (kurz: IdP) unterschieden. Die Föderationen beinhalten jeweils eine definierte Menge von Service und Identity Providern.

Um die Problematik des Datenschutzes über unterschiedliche Service und Identity Provider der Föderation hinweg zu adressieren, wurde unter Anderem die Pseudonomisierung von Benutzernamen (vgl. eduPersonTargetedId) in Richtung der Service Provider eingeführt [I2eP03]. Außerdem existieren Erweiterungen, die dem Benutzer eine Verwaltung der den individuellen Service Providern zur Verfügung gestellten Daten erlauben (vgl. Shibboleth Erweiterungen ShARPE und Autograph [Li08]).

Der Trend geht in Bezug auf die Verbesserung des Datenschutzes in Richtung benutzerzentrierter Authentifizierungsverfahren. Diese erlauben es dem Benutzer seine Identitäten lokal zu verwalten und können als Nachfolger der föderationsbasierten Lösungen angesehen werden [Har07] [Cam07]. Lösungen für ein benutzerzentriertes (user-centric) Identity Management sind beispielsweise Ping Identity [Ping], sxip [sxip], Microsoft CardSpace [CS] oder OpenID [OpID].

Sowohl Föderationen, als auch benutzerzentrierte Authentifizierungsverfahren erlauben ein dezentrales Identity Management. Während innerhalb von Föderationen an jedem beteiligten Identity Provider ein Identity Management am jeweiligen Standort erfolgt, können beim benutzerzentrierten Ansatz die Anwender selbst das Management ihrer Identitäten übernehmen. Es zeichnet sich somit in der Entwicklung der Authentifizierungsverfahren ein Trend hinsichtlich der zunehmenden Dezentralisierung ab (vgl. Abbildung 1).

Aktuelle Implementierungen bzw. Verfahren, die auf SAML aufsetzen, um eine dezentrale, standardisierte Authentifizierung zu erlauben, fokussieren derzeit Web-Anwendungen. Eine Anmeldung an Rechnern bzw. eine Authentifizierung für Desktop-Anwendungen ist derzeit nicht möglich. Für einige föderationsbasierte Authentifizierungsverfahren wurde für zukünftige Versionen (z.B. für Shibboleth 2.0 [Shib2]) eine Integration von Desktop-Anwendungen angedacht, jedoch nicht implementiert. Darüber hinaus existieren aktuell z.B. im Hinblick auf das Accounting der dezentralen Zugriffe, sowie der föderationsübergreifenden Authentifizierung noch einige Herausforderungen für SAML-basierte Lösungen.

2.2 Dezentrale Authentifizierung für Desktop-Anwendungen

Im vorherigen Abschnitt wurden Verfahren beschrieben, die derzeit für die dezentrale Authentifizierung an Web-Anwendungen verwendet werden. In den Roadmaps dieser Verfahren wird zum Teil auch die Integration von Desktop-Anwendungen außerhalb des World Wide Web genannt. Insbesondere für das dezentrale Authentifizierungsverfahren Shibboleth, das in wissenschaftlichen IT-Strukturen, unterstützt durch die DFN-AAI [DFNA], eine große Verbreitung aufweist, existiert derzeit keine Implementierung, die beispielsweise eine dezentrale Authentifizierung bei der Anmeldung am Desktop oder Netzwerk (z.B. Funk-LAN) erlaubt.

Dieser Abschnitt erläutert eine prototypische Verwendung von Shibboleth für die Authentifizierung an Desktop-Anwendungen. Dadurch lassen sich die in Abschnitt 1.1 skizzierten Anforderungen z.B. der Zugang zum Funk-LAN und die Anmeldung in CIP-Pools für externe Benutzer mit einer dezentralen Authentifizierung realisieren. Das Identity Management kann daher, wie in den vorherigen Abschnitten beschrieben, auch für Desktop-Anwendungen dezentral abgewickelt werden.

Aufgrund der Verbreitung von Microsoft Windows in den im Rahmen der Test-Umgebung betrachteten CIP-Räumen der Georg-August Universität Göttingen, wurde dieses Betriebssystem als Plattform gewählt. Windows bietet für das Login bzw. die Authentifizierung der Benutzer die standardisierte Schnittstelle „Graphical Identification aNd Authentication“ (kurz: GINA) [GINA]. Da diese Schnittstelle modulare Erweiterungen nur über die proprietäre Windows-API zulässt, wurde das Open-Source-Projekt „pluggable GINA“ (kurz: pGINA) [pGINA] als Ausgangsbasis ausgewählt. Innerhalb der pGINA können Plug-Ins für unterschiedliche Authentifizierungssysteme (z.B. LDAP, RADIUS, SSH) neben der lokalen Anmeldung (Local Security Authority, kurz: LSA) und der Domänenanmeldung von Windows verwendet werden.

Das realisierte Shibboleth Plug-In für die pGINA führt eine Authentifizierung gegen reguläre Shibboleth 1.3 IdP durch. Um den jeweilig zuständigen IdP des Benutzers zu ermitteln, wird bei Shibboleth 1.3 regulär ein sog. „Where are you from?“ (kurz: WAYF) Server eingesetzt, auf dem der Benutzer seine Heimatorganisation auswählen kann. Für die web-basierte Authentifizierung erfolgt hierfür ein Redirect vom SP an den WAYF. Um die Anmeldung für die Benutzer und die Implementierung zu vereinfachen, wurde für das pGINA Shibboleth Plug-In auf die Funktion des WAYF zu Gunsten einer IdP Ermittlung über DNS verzichtet. Zukünftig ließe sich hier ggf. eine Integration mit dem für Shibboleth 2.0 geplanten Discovery Service realisieren, der ebenfalls eine Unterstützung für mehrere Föderationen erlaubt. Die Auflösung des zuständigen IdP erfolgt anhand des vom Benutzer angegebenen Realms. Verwendet der Benutzer beispielsweise „mmuster@gwdg.de“ für die Anmeldung, so führt das realisierte Plug-In eine SRV Query am DNS nach dem Record „_shibboleth._tcp.gwdg.de“ durch. Im Anschluss erfolgt eine Authentifizierung an der aus dem SRV Record ermittelten Adresse. In der Test-Umgebung wurde für die Authentifizierung ein separater SP, dessen Adresse im SRV Record hinterlegt ist, verwendet und gemeinsam mit dem IdP in die Föderation (bzw. metadata.xml) integriert. Zukünftig soll das Shibboleth Plug-In selbst als SP fungieren und direkt über SAML mit dem IdP kommunizieren. Hierbei erfolgt auch die IdP Discovery direkt im Plug-In der pGINA. Im Rahmen eines Proof-of-Concept wurde die Implementierung jedoch zunächst durch die Authentifizierung über HTTP (sowohl HTTP Authentication [HTTPA] als auch formular-basiert) vereinfacht. Server-Zertifikat und Entität des IdP werden jedoch nach der Weiterleitung durch den SP vom Plug-In anhand einer lokalen metadata.xml geprüft. Abbildung 2 zeigt eine vereinfachte Darstellung des Ablaufs einer Anmeldung mittels pGINA über das realisierte Shibboleth Plug-In.

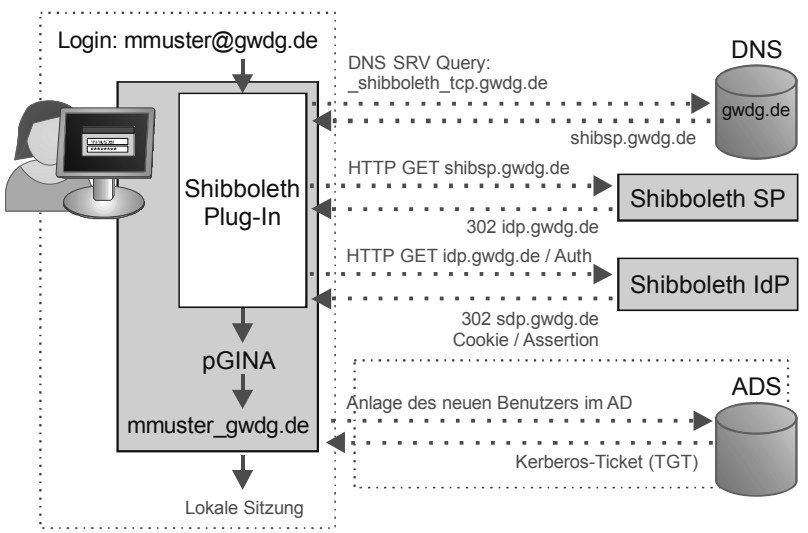

Abbildung 2: Übersicht einer Desktop-Anmeldung mittels pGINA Shibboleth Plug-In.

Nach der erfolgreichen Anmeldung erzeugt die pGINA im einfachsten Fall, sofern keine Domänenanmeldung realisiert wird, für den Benutzer ein lokales Profil, das nach der Abmeldung wieder entfernt wird. Da der hierfür verwendete Benutzername (SAM-AccountName) in Windows kein „@"-Zeichen enthalten darf, wurde dieses Zeichen nach der Authentifizierung durch einen Unterstrich ersetzt. Aufgrund der maximalen Länge des SAMAccountName von 20 Zeichen wurde ebenfalls eine evtl. Kürzung der Eingabe vorgenommen. Diese entfällt, wenn die pGINA für eine Integration in einer bestehenden Windows- bzw. Active Directory Domäne konfiguriert wird, wie in Abbildung 2 dargestellt. Hierbei wird nach der Anmeldung ein neuer Benutzer gemäß des angegebenen Benutzernamens in der Domäne erzeugt. Der hierbei verwendete User-PrincipalName (kurz: UPN) besitzt im Active Directory keine Längenbeschränkungen.

Vorteil der Domänen-Integration bildet das damit innerhalb der angebundenen Active Directory Forests realisierte Single Sign-On. Die Gast-Benutzer die gegenüber einem IdP innerhalb der Föderation authentifiziert wurden, erhalten nach der automatisierten Anlage innerhalb der Domäne (in einer separaten Organizational Unit) ein Kerberos-Ticket (Ticket Granting Ticket) vom Key Distribution Center (kurz: KDC), das für die Verwendung von Diensten innerhalb der Active Directory Umgebung genutzt werden kann. Auf diese Weise wird eine umfassende Reduzierung der erforderlichen Anmeldungen in Richtung eines Reduced Sign-On ermöglicht. Um dies zusätzlich zu erweitern, wurde die Speicherung des im Rahmen der Shibboleth-Authentifizierung an das Plug-In übermittelten Cookies im Default-Profil des Firefox Web-Browsers getestet.

Für die Authentifizierung von Studierenden mit eigenem Notebook wurde für den Zugang zum Funk-LAN in der Test-Umgebung eine Web-Seite mit zugehörigem SP realisiert, auf die Benutzer bei erstmaliger Verwendung eines Web-Browsers umgeleitet werden. Im Proof-of-concept wurde das Discovery des zuständigen IdP analog zum pGINA Shibboleth Plug-In durch die Web-Anwendung bzw. das Funk-LAN Portal mittels DNS SRV Query und anschließender Weiterleitung implementiert. Zukünftig ist hier ebenfalls die Erweiterung des SP um eine eigenständige Ermittlung des IdP, wie sie auch für Shibboleth 2.0 geplant ist, möglich. Ein Reduced Sign-On für Desktop-Anwendungen z.B. Windows File-Services etc. ist anhand der skizzierten Authentifizierung im Funk-LAN über die Grenzen des Web-Browsers hinweg jedoch derzeit nicht möglich.

3 Fazit und Ausblick

Die skizzierten Ansätze und Erweiterungen zeigen, dass eine universelle Verwendung web-basierter Verfahren für eine dezentrale bzw. föderierte Authentifizierung möglich ist. Ihr Potential liegt in der Verwendung offener Web-Standards (z.B. HTTP, SAML) die sich, wie aufgezeigt, auch für Desktop-Anwendungen verteilter Benutzergruppen und Föderationen einsetzen lassen. Durch Erweiterungen, wie die Abfrage zusätzlicher Attribute und die konsequente Trennung zwischen Dienste- (SP) und Identitätsprovider (IdP) wird eine plattform- und anwendungsübergreifende Authentifizierung ermöglicht, wie sie auch von bestehenden Authentifizierungsverfahren wie Kerberos und RADIUS adressiert wurde. Im Vergleich zu diesen bestehenden Verfahren sind die web-basierten Lösungen jedoch leichter zu implementieren und zudem erweiterbar. Zusätzlich skalieren föderationsbasierte Verfahren besser, da das Vertrauen anhand von X.509 Zertifikaten ohne zentrale Komponenten und somit dezentral realisiert werden kann.

Die im Abschnitt 2.2 beschriebene Integration mit DNS erlaubt weit verteilte wissenschaftliche IT-Strukturen. Neben der Anmeldung an Windows Desktop-Rechnern kann dies auch für Terminal Service Lösungen verwendet werden. Die Lösung ist auch für Web-Anwendungen einsetzbar, um auf die Funktion des WAYF Servers zu verzichten. Durch zunehmende Interaktivität von Web-Anwendungen und die Verschmelzung von client- und serverseitiger Dynamik von Web-Anwendungen, die unter Technologien wie AJAX [Gar05] bzw. dem Sammelbegriff „Web 2.0“ zusammengefasst werden, ist die Relevanz von Desktop-Anwendungen zukünftig jedoch unklar. Insbesondere verteilte wissenschaftliche Benutzergruppen werden zukünftig immer weniger reine Desktop-Anwendungen als viel mehr reine Web-Anwendungen für die verteilte Kollaboration verwenden. Nicht zuletzt die Bestrebungen bestehende Verfahren um die Integration mit Desktop-Anwendungen zu erweitern zeigen jedoch, dass vorläufig noch einige Anwendungsfälle hinsichtlich einer dezentralen Authentifizierung für Desktop-Anwendungen existieren. Ansätze gibt es hierbei bereits für CAS [CASA] und Ping Identity [PingA].

Für Windows plant auch Microsoft selbst die Erweiterung der Anmeldung bzw. GINA durch ADFS und CardSpace. Für Unix-Anwendungen wäre eine Implementierung eines PAM-Moduls (z.B. als pam_shib) [XSSO] analog zum Ansatz in Abschnitt 2.2 realisierbar. Diese würde eine dezentrale Authentifizierung für Dienste wie z.B. SSH, E-Mail etc. erlauben. Allerdings erfordert die Abbildung auf Rechte etc. eine Integration mit bestehenden Name Service Switch (kurz: NSS) Lösungen (z.B. nss_ldap). Entscheidend für eine dezentrale Authentifizierung und ein Reduced Sign-On über Web-Anwendungen hinaus ist somit die Integration in die Betriebssysteme. Ideale Voraussetzung hierfür bieten, wie gezeigt, modulare bzw. „pluggable“ Clientlösungen wie pGINA oder PAM, die eine Integration unterschiedlicher Authentifizierungsverfahren und -systeme erlauben.

Literaturverzeichnis

[ADFS] Microsoft: Introduction to ADFS, http://technet2.microsoft.com/WindowsServer/en/library/c67c9b41-1017-420d-a50e-092696f40c171033.mspx, abgerufen am: 18.1.2008.

[Cam07] Cameron, K.: The Laws of Identity, http://www.identityblog.com/stories/2004/12/09/thelaws.html, abgerufen am: 18.1.2008.
[CAS] JA-SIG: Central Authentication Service, http://www.ja-sig.org/products/cas/index.html, abgerufen am: 18.1.2008.
[CASA] JA-SIG: Yale PAM client distribution, http://www.ja-sig.org/wiki/display/CASC/PAM+Module, abgerufen am : 18.1.2008.
[CS] Microsoft: CardSpace, http://netfx3.com/content/WindowsCardspaceHome.aspx, abgerufen am: 18.1.2008.
[DFNA] DFN: DFN-AAI Einfacher Zugang zu geschützten Ressourcen, http://www.dfn.de/index.php?L=0&id=75522, abgerufen am: 18.1.2008.
[Gar05] Garret, J. J.: Ajax: A New Approach to Web Applications, http://www.adaptivepath.com/ideas/essays/archives/000385.php, abgerufen am: 18.1.2008.
[GINA] Microsoft: Customizing GINA, http://msdn.microsoft.com/msdnmag/issues/05/05/SecurityBriefs/, abgerufen am: 18.1.2008.
[Har07] Hardt, D. C.: Identity 2.0, http://www.identity20.com/, abgerufen am: 18.1.2008.
[I2eP03] Internet2: EduPerson Specification (200312), http://www.nmi-edit.org/eduPerson/internet2-mace-dir-eduperson-200312.html, abgerufen am: 18.1.2008.
[HTTPA] IETF: RFC 2617 - HTTP Authentication: Basic and Digest Access Authentication, http://www.ietf.org/rfc/rfc2617.txt, abgerufen am: 18.1.2008.
[Li08] Liong, B.: Shibboleth Attribute Release Policy Editor (ShARPE), http://www.federation.org.au/twiki/bin/view/Federation/ShARPE, abgerufen am: 18.1.2008.
[Lib] Liberty Alliance Communications: Liberty Alliance Project, http://www.projectliberty.org, abgerufen am: 18.1.2008.
[OpID] OpenID Foundation: OpenID, http://openid.net/, abgerufen am: 18.1.2008.
[pGINA] pGINA: http://www.pgina.org/, abgerufen am: 18.1.2008.
[Ping] Ping Identity Corporation: Ping Identity http://www.pingidentity.com/, abgerufen am: 18.1.2008.
[PingA] Ping Identity Corporation: Windows IWA Integration Kit, http://www.pingidentity.com/products/windows-iwa.cfm, abgerufen am: 18.1.2008.
[Rie06] Rieger, S. et.al.: Self-Service PKI-Lösungen für eScience. (Paulsen, C. Hrsg.) In Sicherheit in vernetzten Systemen. 13. DFN-CERT Workshopband, Hamburg, 2006.
[Rie07] Rieger, S.: Einheitliche Authentifizierung in heterogenen IT-Strukturen für ein sicheres e-Science Umfeld, Cuvillier, E, 2007.
[SAML] OASIS: Security Services (SAML) TC, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security, abgerufen am: 18.1.2008.
[San00] Sandhu, R. et. al.: The NIST Model for Role Based Access Control: Towards a Unified Standard. In *Proceedings, 5th ACM Workshop on Role Based Access Control*, July 26-27, 2000.
[Shib] Internet2: Shibboleth Project - Internet2 Middleware, http://shibboleth.internet2.edu/, abgerufen am: 18.1.2008.
[Shib2] Internet2: Shibboleth 2 Roadmap, http://spaces.internet2.edu/display/SHIB/ShibTwoRoadmap, abgerufen am: 18.1.2008.
[sxip] sxip Identity Corporation: sxip identity, http://www.sxip.com/, abgerufen am: 18.1.2008.
[Win05] Windley, P. J.: Digital Identity, O'Reilly Media, 2005.
[XSSO] X/Open: X/Open Single Sign-on Service (XSSO) - Pluggable Authentication Modules, http://www.opengroup.org/onlinepubs/008329799/toc.htm, abgerufen am: 18.1.2008.