AAI in Aktion: Web Single Sign-On an der Uni Wien

Was ist AAI?

AAI steht für *Authentifizierungs- und Autorisierungs-Infrastruktur*:

- **Authentifizierung** ist die Überprüfung elektronischer Identitäten (UserIDs), basierend auf physiologischen Eigenheiten (Fingerabdruck, Stimmmuster), Gegenständen, über die verfügt wird (Mobiltelefon, Chipkarte), Geheimnissen (PIN-Code, Passwort) oder beliebigen Kombinationen dieser Faktoren. Am häufigsten ist immer noch die Authentifizierung mittels UserID und Passwort. Mit der Wahl eines entsprechenden Passworts (siehe `www.univie.ac.at/ZID/passwort#sicher`) ist diese Methode auch für die meisten elektronischen Vorgänge ausreichend sicher – und im Gegensatz zu Methoden, die den Besitz von bestimmten Gegenständen voraussetzen, nicht durch teure Anschaffung und Verwaltung bzw. Probleme bei Verlust dieser Gegenstände belastet.
- **Autorisierung** bezeichnet das Überprüfen der Zugriffsberechtigungen von bereits authentifizierten Identitäten in Bezug auf bestimmte Ressourcen bzw. Dienste, meist anhand der Zugehörigkeit der Identität zu einer berechtigten Gruppe oder Rolle. Dabei könnten z.B. auch zeitliche (Labornutzung „wochentags bis 18 Uhr") oder quantitative (Bestellungen „bis 10 000 €") Einschränkungen berücksichtigt werden.
- **Infrastruktur** verweist auf den grundlegenden, zentralen Charakter, den eine AAI in der elektronisch vermittelten Welt zunehmend spielt.

Die wesentlichen Elemente einer Authentifizierungs- und Autorisierungs-Infrastruktur sind in der Regel

- **Identity Management**, also die Vergabe und Verwaltung von UserIDs, deren verschiedenen Zuständen und Wandlungen im universitären Universum, bis zu ihrem Ablauf,
- **Verzeichnisdienste** (z.B. LDAP, siehe `http://comment.univie.ac.at/06-3/29/`) und
- **zentralisierte Authentifizierungs- und Autorisierungs-Services.**

Dieser Kernbereich einer AAI wird auch als *Core Middleware* bezeichnet, da die Bestandteile selbst in der Regel für die BenutzerInnen nicht sichtbar sind: Middleware sitzt sozusagen zwischen dem Netzwerk und den Anwendungen und *„hilft Organisationen, Personen mit Ressourcen zu verbinden"* (JISC, `www.jisc.ac.uk`).

„Improving security and usability at the same time. How often do you get a chance to do that?" [1]

Wie bereits in der *Comment*-Ausgabe vom Oktober 2006[2] angedeutet, ist der ZID seit einiger Zeit damit beschäftigt, seine Authentifizierungs- und Autorisierungs-Infrastruktur (AAI, siehe nebenstehender Kasten) dahingehend auszubauen, dass sie auch von anderen Organisationseinheiten der Universität Wien verwendet werden kann. Als erstes „sichtbares" Ergebnis dieser Arbeiten wird voraussichtlich noch heuer ein *Web Single Sign-On* (WebSSO)-System in Betrieb genommen werden.

Dabei handelt es sich um eine zentrale Komponente, die allen teilnehmenden Webanwendungen die nötige Authentifizierung bei Zugriffen auf geschützte Ressourcen abnimmt: Personen, die sich bereits an einem bestimmten System authentifiziert haben, werden als solche erkannt und bis zum Ablauf einer definierten Zeitspanne (z.B. acht Stunden) nicht wieder zur Authentifizierung aufgefordert.[3] Dabei kommt es zur oben erwähnten, sich nur selten ergebenden Gelegenheit, einerseits die Sicherheit der beteiligten Systeme zu erhöhen und gleichzeitig die Benutzerfreundlichkeit zu verbessern – eine Gelegenheit, die wir natürlich nicht auslassen wollen.

Der Nutzen eines WebSSO-Systems beginnt bereits bei der zweiten teilnehmenden Anwendung und steigt mit jeder weiteren. Es ist nicht nötig, sofort alle Webanwendungen im „Einzugsbereich" des WebSSO-Systems umzustellen, was den Einstieg in diese Technologie und den sukzessiven Aufbau eines solchen Systems massiv erleichtert. Neben allen interessierten BenutzerInnen von Webapplikationen (also Anwendungen, die lediglich einen Standard-Webbrowser benötigen – Online-Datenbanken, Wikis, Diskussionsforen usw.) wendet sich dieser Artikel daher vor allem an die BetreiberInnen von Webapplikationen in allen Bereichen der Universität Wien.

---

1) Charlie Catlett, Teragrid Director (siehe `http://teragrid.blogspot.com/2006/09/improving-security-and-usability.html`)

2) siehe Artikel *Wie sag ich's meinem LDAP-Server?* in *Comment 06/3*, Seite 33 (`http://comment.univie.ac.at/06-3/33/`), Abschnitt *LDAP und Authentifizierung*

3) Solche Systeme werden heute auch oft als WebISO-Systeme (*Initial Sign-On*) bezeichnet, um die *initiale* Authentifizierung zu betonen und nicht auf dem *Single* Sign-On zu beharren, das in der Praxis nur selten erreicht wird.

Mehr Sicherheit

Da UserID und Passwort bei einem WebSSO-System – unabhängig von der Anzahl der benutzten Anwendungen – nur einmal an den zentralen Authentifizierungsserver übertragen werden, reduziert sich die Zahl der im Netzwerk übertragenen Passwörter insgesamt. Wenn Passwörter gar nicht erst elektronisch übertragen werden, können sie auch nicht abgehört, aufgezeichnet oder manipuliert werden. Etwaige Fehler in anderen sicherheitsrelevanten Komponenten (von der Firewall bis zum SSL-gesicherten Webbrowser) verlieren also einen Teil ihrer potentiellen Auswirkungen. Ein wichtiger Faktor, denn einmal „ausgekommene" – d.h. in fremde Hände geratene – Passwörter sind nur schwer wieder „einzufangen": Die missbräuchliche Verwendung wird oft nicht sofort entdeckt und kann als Ausgangspunkt für weitere unautorisierte Zu- oder Angriffe auf andere Systeme dienen.

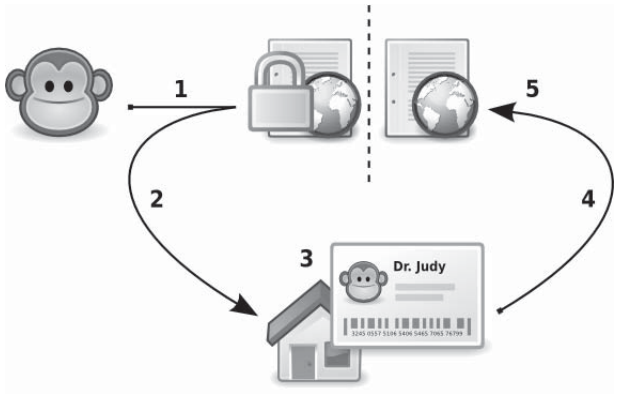
Neben der Anzahl der durchs Netz geisternden Passwörter reduziert ein WebSSO-System auch die Anzahl der Komponenten, die direkt mit dem Passwort in Berührung kommen müssen: Nicht jede Webapplikation, nicht jeder Webserver muss künftig das Passwort zur Überprüfung entgegennehmen, daher sind unautorisierte Zugriffe auf diese Komponenten meist weniger gravierend. Das verringert die sicherheitstechnischen Anforderungen an die teilnehmenden Systeme und auch die Folgen ihrer etwaigen Sicherheitslücken für alle anderen Systeme.

Mehr Benutzerfreundlichkeit

Durch die Integration möglichst vieler Webanwendungen in ein zentrales WebSSO-System wird es für die BenutzerInnen dieser Anwendungen möglich, sich nur einmal an einer gesicherten Website anzumelden und dann für eine gewisse Zeit direkten Zugriff auf alle teilnehmenden Anwendungen zu haben (siehe **Abb. 1**). Dies erleichtert den Arbeitsalltag, erübrigt das praktische, aber deutlich weniger sichere Speichern von UserID/Passwort im Webbrowser[4)] und fördert die Verwendung komplexerer Passwörter, da diese im Idealfall nur einmal pro Tag eingegeben werden müssen.

Wie weiter unten näher beschrieben wird, ist eine weitere Verbesserung der Benutzerfreundlichkeit vor allem auch im vergrößerten Anwendungsbereich der u:net- und Mailbox-Accounts zu sehen, ohne jedoch den BetreiberInnen von

4) Das Speichern von UserID und Passwort im Webbrowser erlaubt auch nicht berechtigten Personen Zugriff auf Ihre Daten/Anwendungen, z.B. unbemerkt während einer Kaffeepause oder am Weg zur Toilette. Der Einsatz eines passwortgeschützten Bildschirmschoners kann dieses Risiko etwas verringern; dieser wird aber in der Regel erst nach einiger Zeit der Inaktivität wirksam und kann unter Umständen auch selbst fehlerhaft sein (und damit umgangen werden) oder durch andere Schadsoftware beeinträchtigt werden. Darüber hinaus wurde bereits demonstriert, dass Unberechtigte unter gewissen Umständen Zugriff auf die im Browser gespeicherten UserIDs und Passwörter bekommen können.

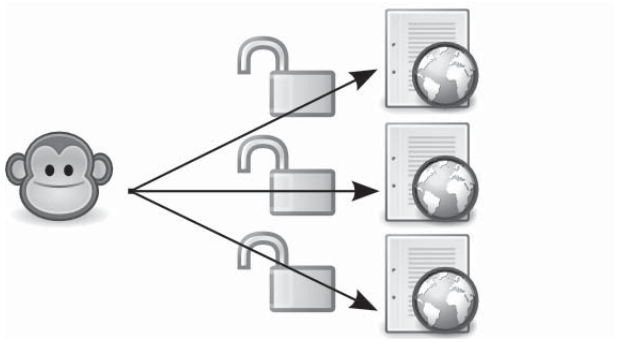


Judy versucht auf eine geschützte Webseite zuzugreifen (1).

Da Judy dem System noch nicht bekannt ist, wird ihr Webbrowser automatisch umgeleitet (2), und zwar zum zentralen Weblogin-Server ihrer Heimateinrichtung (3).

Hier bestätigt sie ihre elektronische Identität (z.B. mittels UserID und Passwort) und wird anschließend automatisch zur ursprünglich aufgerufenen Webseite weitergeleitet (4).

Dort wird Judy als bereits authentifiziert erkannt und bekommt sofort Zugriff auf das gewünschte Dokument (5).



Weitere Zugriffe – auch auf andere teilnehmende Webanwendungen – können nun ohne Umweg und ohne weitere Authentifizierungsaufforderungen stattfinden.

Eine detailliertere Erläuterung der Funktionsweise einer Authentifizierungs- und Autorisierungs-Infrastruktur bietet die **AAI Demo** des Schweizer Wissenschaftsnetzes SWITCH, die unter **www.switch.ch/aai/demo/** in drei Schwierigkeitsstufen (Easy, Medium, Expert) verfügbar ist.

Abb. 1: Vereinfachte schematische Darstellung der Nutzung eines WebSSO-Systems

Webapplikationen irgendwelche Freiheiten zu nehmen oder neue Sicherheitsrisiken zu schaffen. Verwirrungen mit verschiedenen Accounts und Passwörtern für die verschiedenen Systeme werden dabei deutlich reduziert. Der Helpdesk des ZID ist folglich in der Lage, bei Passwort-Problemen auch dann zu helfen, wenn die betroffenen Anwendungen nicht vom ZID betrieben werden – sofern sie das Angebot der zentralen Authentifizierung nutzen.

Einbindung von Institutsanwendungen

Auch wenn wir am ZID überzeugt sind, viele Services besser zentral anbieten zu können[5], ist klar, dass die diversen Organisationseinheiten der Universität Wien eine Vielzahl von unterschiedlichen Programmen und Werkzeugen benötigen, die der Zentrale Informatikdienst nicht ähnlich effizient für *alle* Mitglieder der Universität zentral betreiben und auf Jahre hinaus professionell unterstützen kann. In der Folge betreiben also viele Institute ihre eigenen Webanwendungen, entweder auf PCs unter einem Schreibtisch[6], auf „richtiger" Hardware im Rahmen des ZID-Serverhousing oder auch direkt auf den zentralen Webservern des ZID. Nur auf den Servern des ZID ist in der Regel auch eine Authentifizierung mit Hilfe der zentral vergebenen UserIDs möglich, da der ZID nicht für die Sicherheit von externen Systemen sorgen kann – was die Verwendung von u:net- und Mailbox-Accounts für solche Systeme bisher unmöglich machte.

Mit einem zentralen WebSSO-System lassen sich nun prinzipiell[7] auch Applikationen, die nicht vom ZID betrieben werden, in die zentrale Authentifizierung integrieren. Die aktuellen Implementierungen solcher WebSSO-Systeme funktionieren auf der Ebene des Webservers, der dazu eine Erweiterung laden muss. Sie verlagern die Überprüfung der zugreifenden Identitäten also von der Webapplikation auf den Webserver, der mit dem WebSSO-System Rücksprache hält, ob die zugreifende UserID bereits bekannt ist.

Wenn weder die Applikation noch der Webserver, auf dem sie läuft, in Berührung mit dem Passwort kommt (das nur dem zentralen Authentifizierungsserver zur Überprüfung anvertraut wird), besteht auch keine Missbrauchs- und Fehlermöglichkeit am institutseigenen Webserver. Das wiederum senkt die Sicherheitsanforderungen an die teilnehmenden Systeme ganz wesentlich – eine einzelne, „außer Kontrolle" geratene Maschine kann die Sicherheit des gesamten SSO-Systems nicht gefährden. Die Integration eines Moduls in den Webserver hat außerdem den Vorteil, dass das SSO-System damit unabhängig von der in der jeweiliger Webanwendung eingesetzten Programmiersprache (Perl, Python, PHP, Java etc.) funktioniert. Auch muss die Erweiterung, die die Teilnahme am WebSSO-System ermöglicht, nur einmal pro Webserver konfiguriert werden – es können auf diesem Server aber beliebig viele Applikationen, Seiten oder Verzeichnisse mittels Passwort geschützt (oder auch selektiv von diesem Schutz ausgenommen) werden.

Ein weiterer Grund, Webanwendungen mit einer eigenen, lokalen Benutzerdatenbank zu verknüpfen[8], ist die Anforderung, auch externen Personen ohne u:net- bzw. Mailbox-Account Zugriff auf eigene Ressourcen zu gewähren. Das zentrale Authentifizierungs-System kann klarerweise nur zentral vergebene UserIDs überprüfen; an der Universität werden jedoch zunehmend auch elektronische Identitäten von Personen verwaltet, die traditionell keinen Account erhalten haben (externe DienstleisterInnen, KollegInnen aus anderen Forschungseinrichtungen etc.). Die Verbindungen dieser Personen zur Uni Wien sind ebenso unterschiedlich wie die Berechtigungen, die sie innerhalb der Universität benötigen, um erfolgreich kooperieren zu können. Daher sind die standardisierten und mit vielen Privilegien – von Zugriffen auf geschützte Ressourcen der Universitätsbibliothek bis hin zu Speicherplatz am zentralen Storage-System – ausgestatteten u:net- und Mailbox-Accounts für die Authentifizierung dieser BenutzerInnen ungeeignet. Mit dem vor kurzem etablierten Konzept der Mailbox Light-Accounts (siehe Seite 2) kann jedoch auch für diese „neuen" Benutzergruppen eine zentrale Authentifizierung eingerichtet werden, ohne zu viele Privilegien zu verleihen. Über den „Umweg" der zentral verwalteten Light-IDs können also lokale Webanwendungen auf die zentrale Authentifizierung umgestellt werden und gleichzeitig wie bisher auch externen Personen Zugriff gewähren.

Wie bereits erwähnt, ermöglicht es die Integration in ein zentrales WebSSO-System den BenutzerInnen von dezentralen Webanwendungen, ihr Passwort jederzeit über die gewohnten Webmasken des ZID zu ändern und im Problemfall (Passwort vergessen, Passwort „funktioniert" nicht etc.) beim Helpdesk des ZID schnelle und unbürokratische Unterstützung zu bekommen. Für die BetreiberInnen dieser dezentralen Anwendungen entfällt vor allem auch der Support für das Vergeben oder Neusetzen von Passwörtern, die nur für dieses eine System gelten und allein schon deshalb

---

5) Vor allem durch professionelle Betreuung in Bezug auf Klimatechnik, Stromversorgung, Hard- und Software, Security und Incident Handling, Helpdesk und Beratung u.v.m.

6) siehe Artikel *Artgerechte Server-Haltung: Serverhousing am ZID* in *Comment 06/1*, Seite 6 (`http://comment.univie.ac.at/06-1/6/`)

7) Je nachdem, wie eine bestimmte Webapplikation die Authentifizierung und Autorisierung derzeit durchführt, können eventuell Änderungen an der Software nötig werden, um die Integration in das WebSSO-System zu ermöglichen. Oft kann die Software aber konfiguriert werden, die Authentifizierung dem Webserver zu überlassen. Sollten Änderungen an der Software notwendig sein, kann man diese entweder selbst durchführen bzw. jemanden damit beauftragen (einer der vielen Vorteile der Nutzung von Freier und Open Source-Software) oder sich an den Hersteller wenden und diesen um die Software-Unterstützung von *HTTP Basic Auth* ersuchen. Der ZID steht in jedem Fall gern beratend zur Seite.

8) D.h. neben der Tatsache, dass immer noch viele Anwendungen von Haus aus eine eigene Benutzerverwaltung mitbringen und manchmal nur mit Mühe dazu gebracht werden können, Daten von BenutzerInnen aus einer zentralen Quelle (wie dem LDAP-Verzeichnisdienst) zu beziehen.

entweder häufiger vergessen (und daher eventuell aufgeschrieben) oder niemals geändert werden, was beides für die Sicherheit der betroffenen Systeme nicht förderlich ist.

Attributbasierte Autorisierung

Aus dem Umstand, dass zunehmend auch neue Benutzerkreise ihre individuell limitierten Zugangsberechtigungen am ZID erhalten können, folgt schließlich, dass eine Zugriffskontrolle über korrekte Authentifizierung allein möglicherweise in manchen Fällen nicht mehr ausreichend ist. Ein zentrales Authentifizierungs-Service sollte deshalb auch Möglichkeiten bieten, den Zugriff auf ein Service aufgrund weiterer Eigenschaften (oder Attribute) der anfragenden Identität zu erlauben oder zu verweigern.

Auf den zentralen Webservern des ZID ist es schon lange möglich, nur Studierenden oder/und Uni-MitarbeiterInnen Zugriff zu gewähren bzw. diese Beschränkung mit Hilfe so genannter „Authentifizierungsklassen" (basierend auf Abfragen in der Personaldatenbank, siehe `www.univie.ac.at/ZID/www-htaccess/#institut`) noch weiter einzugrenzen – z.B. auf Angehörige einer Fakultät oder eines Instituts. Aus technischen Gründen kann der direkte Datenbankzugriff aber nur für die zentralen Webserver des ZID zur Verfügung gestellt werden, was die Einsatzmöglichkeiten dieser attributbasierten Autorisierung stark reduziert. Um auch allen TeilnehmerInnen am künftigen Authentifizierungs-System eine detailliertere Selektion der Zugriffsberechtigten zu erlauben, soll dieses System daher um ein zentrales Autorisierungs-Service ergänzt werden. Dazu ist es notwendig, Standards zum Austausch solcher Daten zu definieren und umzusetzen. An der Entwicklung dieser Standards wird bereits gearbeitet; die entsprechenden Details werden – ebenso wie alle Einzelheiten zum kommenden Authentifizierungs-System – rechtzeitig im *Comment* und auf den Webseiten des ZID bekannt gegeben werden.

Zukunftsmusik: Organisationsübergreifendes Single Sign-On

Da die zentralen Fragen des Themenkreises AAI nicht spezifisch für die Uni Wien sind, haben sich schon einige andere Institutionen der höheren Bildung[9)] damit befasst und auch bereits Konzepte und Anwendungen vorgestellt. Im lokalen und internationalen Diskurs von Forschungseinrichtungen und Universitäten wurden Standards entwickelt, die zur Zeit weltweit umgesetzt werden. Dazu gehören Schemata zur Verwaltung und zum Austausch von Attributen, die bisher folgende Punkte abdecken:

- Organisationen und Organisationseinheiten,
- Personen und ihre Organisationszugehörigkeit,
- Gruppen (als Zusammensetzung von Personen oder wiederum Gruppen),
- Berechtigungsinformationen bezüglich Personen und Ressourcen,
- Kennzeichnung von Lehrveranstaltungen.

Um die gemeinsam entwickelten Konzepte für die weltweite wissenschaftliche Gemeinschaft praktisch nutzbar zu machen, wurden wesentliche Komponenten vom Internet2-Konsortium als Freie bzw. Open Source-Software entwickelt: *Grouper* zur Gruppenverwaltung innerhalb einer Organisation, *Signet* zur gruppenbasierten Verwaltung von Berechtigungen sowie *Shibboleth* zum sicheren Austausch dieser Informationen innerhalb einer Organisation, aber auch zwischen kooperierenden Universitäten und Forschungseinrichtungen. Einerseits werden damit *best practices* etabliert und vermittelt, die Interessierte für die Verwaltung ihres lokalen Campus übernehmen können, andererseits ergeben sich damit neue Möglichkeiten in der elektronisch vermittelten Zusammenarbeit und Lehre, die über die jeweilige Heimatinstitution hinausreichen.

Dies gilt insbesondere für das Shibboleth-Projekt (`http://shibboleth.internet2.edu/`), welches das Campus-interne Single Sign-On-Prinzip (Authentifizierung für verschiedene Ressourcen einer Institution an einem einzigen gesicherten Ort) um inter-institutionelles Single Sign-On erweitert: Die Authentifizierung findet hierbei ebenso am SSO-System der jeweils eigenen Heimateinrichtung statt, ermöglicht aber durch Austausch von standardisierten Attributen auch die Verwendung von Ressourcen anderer teilnehmender Institutionen. Beispielsweise kann die Universität Wien, sofern gewünscht und vereinbart, damit auch Angehörigen anderer Universitäten (ohne gültigen Account an der Universität Wien) Ressourcen zur Verfügung stellen (und umgekehrt) und sich gleichzeitig darauf verlassen, dass nur Personen darauf zugreifen können, die sich an einer Partner-Einrichtung bereits erfolgreich authentifiziert haben und nach gemeinsam beschlossenen Kriterien autorisiert wurden.

Die notwendige Zugriffsbeschränkung für gewisse (z.B. lizenzpflichtige) Ressourcen auf bestimmte Benutzergruppen wird dabei mittels eines vertraglich und technisch zwischen den Kooperationspartnern geregelten Attribut-Austausches realisiert, bei gleichzeitiger voller Wahrung des Datenschutzes und der Privacy: „Anbieter" von Identitäten (hier die Universitäten als Verwalter der UserIDs) und Anbieter von Ressourcen (das können auch externe Content Provider sein) schließen sich zu einem Verbund (einer so genannten *Federation*) zusammen und vereinbaren, welche Daten un-

9) Die wichtigsten dieser Einrichtungen sind *Internet2* (`www.internet2.edu/about/`), *Educause* (`http://educause.edu/`), das *Enterprise and Desktop Integration Technologies Consortium* der *National Science Foundation Middleware Initiative* (NMI-EDIT, `www.nmi-edit.org`) sowie *TERENA*, die *Trans-European Research and Education Networking Association* (`www.terena.org`).

10) Für die Verwendung innerhalb der Universität Wien werden die Bestimmungen in der Regel weniger streng sein, sodass UserID, Name oder eMail-Adresse einer zugreifenden Person (also Daten, die über die Suche im Online-Personalverzeichnis ohnehin öffentlich zugänglich sind) an interne Applikationen weitergereicht werden können, um das Anlegen und Einrichten von Accounts für BenutzerInnen zu erleichtern oder gar zu erübrigen.

ter welchen Bedingungen innerhalb dieses Verbundes ausgetauscht werden sollen.

Dieses Konzept ermöglicht es beispielsweise auch, einem bestimmten Anbieter nur mitzuteilen, dass die Person, die soeben eine seiner geschützten Ressourcen aufgerufen hat, sich zuvor erfolgreich z.B. an der Universität Wien authentifiziert hat und dort den Status *Studierende* besitzt, ohne aber ihren Namen oder ihre eMail-Adresse preiszugeben.[10)] Dem Anbieter kann auch eine automatisch generierte pseudonyme Identität für die zugreifende Person übermittelt werden: Das ermöglicht ihm bei Bedarf eine Wiedererkennung (was sinnvoll ist, wenn BenutzerInnen Daten oder Profile beim Anbieter speichern können sollen) bzw. kann umgekehrt auch – durch Generieren einer neuen pseudonymen Identität bei jedem Zugriff – das Erstellen von Datenbanken über Benutzerverhalten wirksam verhindern. Dazu kommt noch die Funktion, vor der Weitergabe von persönlichen Informationen die explizite Zustimmung der betroffenen Person einzuholen. Die neuen Kooperationsmöglichkeiten werden also keineswegs mit einem Verzicht auf Privacy oder Datenschutz erkauft – aufgrund der potentiellen anonymen oder pseudonymen Nutzung gilt sogar eher das Gegenteil: Ein solches System ermöglicht verbesserten Datenschutz, erhöhte Sicherheit, weniger Aufwand für BenutzerInnen und ApplikationsbetreiberInnen sowie neue Kooperationen durch den interoperablen Zusammenschluss von lokalen Authentifizierungs- und Autorisierungsstrukturen an Universitäten und anderen Forschungs- und Bildungseinrichtungen.

So utopisch das alles klingen mag, so sehr haben sich die ersten Umsetzungen dieser Konzepte bereits international bewährt. Nicht zuletzt die KollegInnen vom Schweizer Wissenschaftsnetz SWITCH haben gezeigt, wie eine gemeinsame Nutzung von im ganzen Land verstreuten eLearning-Systemen mit jeweils lokalen Benutzerdatenbanken erfolgreich möglich ist (siehe `www.switch.ch/aai/`), und sind damit Vorreiter zahlreicher existierender und geplanter Federations weltweit. Neben der Schweiz betreiben oder entwickeln zur Zeit auch Australien, Dänemark, Deutschland, Finnland, Frankreich, Norwegen, Schweden und Großbritannien Shibboleth-basierte nationale Federations. Damit nicht genug, sind bereits erste Zusammenschlüsse solcher nationalen Federations – so genannte *Confederations* – im Entstehen, etwa für den Bereich des Grid-Computing.

Der ZID der Universität Wien wird daher im Zuge seiner lokalen Aktivitäten um eine verbesserte AAI auch mit den anderen Teilnehmern am österreichischen Wissenschaftsnetz ACOnet zusammenarbeiten, um die vielfältigen Anwendungsmöglichkeiten solcher Systeme im Laufe der Zeit so weit wie möglich auszuschöpfen.

Peter Schober