

# WEBLOGIN MIT SHIBBOLETH

## Neues Login-System für Web-Applikationen der Universität Wien

Im Sommer ist ein neues Single Sign-On-System<sup>1)</sup> für Web-Applikationen auf Basis von Shibboleth in Betrieb gegangen. Derzeit sind erst einige Anwendungen auf das neue System umgestellt, aber die Vision ist verlockend: Einmal UserID und Passwort eingeben und automatisch zu allen webbasierten Anwendungen der Universität Wien angemeldet sein.

### Gestatten, Weblogin ist mein Name

Der Name des neuen Single Sign-On-Systems ist Weblogin. Es ist über <https://weblogin.univie.ac.at/> erreichbar. Idealerweise speichern Sie diese Seite in Ihren Bookmarks und rufen sie von dort aus zu Arbeitsbeginn auf. Achten Sie auf das „s“ in https und darauf, dass das Schloss-Symbol im Browser geschlossen ist (**Abb. 1**). Klicken Sie auf den blauen Button „Login“<sup>3)</sup>. Danach erscheint ein Formular, in dem Sie UserID und Passwort eingeben und klicken schließlich auf „Ok“.

Die in Weblogin eingebundenen Services – z.B. sind das bereits das *Computer Telephone Interface* (CTI) und die E-Learning-Plattform Fronter – können Sie von nun an nutzen, ohne nochmals nach UserID oder Passwort gefragt zu werden. Das Angebot bietet zur Zeit noch Raum für Erweiterungen, jedoch werden bestehende Web-Anwendungen des ZID nach und nach auf das neue System umgestellt.

### Eine langfristige Strategie

In der IT-Security spielt die Benutzerauthentifizierung im wahrsten Sinne des Wortes eine Schlüsselrolle: Der Nachweis

der Identität öffnet den Zugriff auf verschiedenste Services und Daten. Mit dem neuen System werden gleichzeitig der Komfort, die Sicherheit und die Flexibilität der Benutzerauthentifizierung verbessert. Vordergründig scheint es, als beschränkten sich die Vorzüge von Weblogin darauf, dass es hier und da das Eintippen von UserID und Passwort überflüssig macht. Dahinter steckt jedoch ein ausgetüfteltes Konzept und seine Umsetzung ist ein nachhaltig angelegter strategischer Schritt mit weitreichenden Konsequenzen. Auf die nicht so offensichtlichen, aber umso bedeutenderen Vorteile, die das System mit sich bringt, wird im Folgenden eingegangen.

### Legitimieren Sie sich Ihnen!

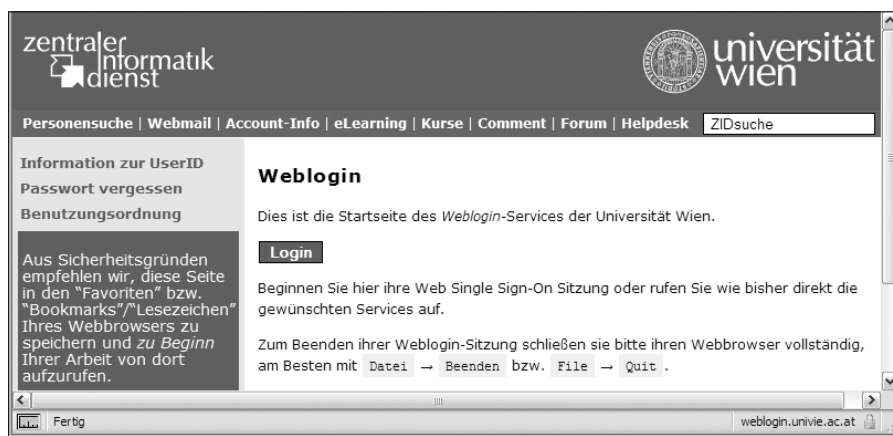
Die Aufforderung „*Legitimieren Sie sich!*“ hat etwas Magisches: Sie verleiht dem Fragenden eine – vielleicht angemähte – Autorität. Doch wer hakt schon nach: „Wer fragt mich das und mit welchem Recht?“ Pflichtbewusst kramt man stattdessen in der Tasche, um das verlangte Papier vorzuweisen.

Nicht anders in der digitalen Welt: Kaum fragt eine Webmaske oder ein Popup-Fenster nach UserID und Passwort, tippt man auch schon seine geheimen Zugangsdaten ein – mit etwas Pech jedoch in die Webmaske von Betrügern, die die soeben erhaltene UserID und das Passwort dazu verwenden, um sich an anderer Stelle als ihr Opfer auszuweisen. Dieses Vorgehen wird als *Phishing*<sup>4)</sup> bezeichnet und ist eine der verbreitetsten Formen der Internetkriminalität.

Verantwortungsbewusste User, die sichergehen wollen, dass sie nur in „gute“ Webmasken ihre u:net- oder Mailbox-Passwörter eingeben, haben es aber an Universitäten sehr schwer: Es ist bei der Fülle an Services schier unmöglich, den Überblick über die zur Passwortabfrage berechtigten Seiten zu behalten. Bei einem Single Sign-On-System besteht dieses Problem nicht: Idealerweise gibt es – sind einmal alle Anwendungen darauf umgestellt – nur mehr eine einzige Anmeldemaske. Alles andere wird damit klar als Fälschung erkennbar.

### Auth, Auto und mehr

Wenn bisher von Authentifizierung die Rede war, so war das etwas ungenau: Shibboleth und somit Weblogin trennt streng zwischen zwei Dingen:



**Abb. 1:** Die Weblogin-Einstiegsseite ist über den Link <https://weblogin.univie.ac.at/> erreichbar. Sie sollte idealerweise als Bookmark gespeichert und von dort aus zu Arbeitsbeginn aufgerufen werden.

- **Authentifizierung:** Wer ist jemand?
- **Autorisierung:** Darf jemand ein bestimmtes Service nutzen?

Die Authentifizierung erfolgt an der Universität Wien bei der bereits beschriebenen Webseite – im Shibboleth-Jargon nennt man das den *Identity Provider* (IdP). Die Autorisierung hingegen, und das ist in dieser klaren Trennung neu, liegt in der Hoheit der Anwendung, im Jargon *Service Provider* (SP) genannt.

Um beurteilen zu können, ob bzw. welche Rechte ein/e User/-in hat, benötigt die Anwendung gewisse Informationen – sogenannte Attribute –, etwa „ist Mitarbeiter/-in“, „studiert Schwedisch im 2. Abschnitt“ etc. Diese liefert Weblogin der Anwendung, und diese entscheidet dann anhand ihrer Richtlinien. Damit können auch ohne Spezialkonstruktionen Zugriffsberechtigungen wesentlich gezielter als je zuvor erteilt werden.

Wenn es die Anwendung benötigt, werden auch weitere Attribute übermittelt – etwa UserID, Name, E-Mail-Adresse, die sonst bei der erstmaligen Benützung mühsam in Formulare eingetippt werden müssten. Weblogin ist aber kein Plappermaul: Welche Attribute welche Anwendung erhalten darf, wird vorab vom ZID genau geprüft und in der Konfiguration von Weblogin festgelegt.

## Wider den Passwortklau

Die Kombination von UserID und Passwort als Mittel zum Nachweis der Identität einer Userin bzw. eines Users hat sich über Jahrzehnte bewährt. Das Verfahren ist einfach: Es braucht keine technische Expertise, um einzusehen, dass das Sicherheitskonzept mit der Geheimhaltung des Passworts steht und fällt. Es ist daher leicht zu verstehen, warum die Weitergabe des Passworts verboten ist<sup>5)</sup> und dass, sollte das Passwort aus irgendeinem Grund doch einmal einer anderen Person als dem/der Account-Inhaber/-in bekannt werden, die Misere durch Änderung des Passworts leicht (aber unverzüglich!) zu beheben ist.

Shibboleth selbst macht keine Vorgaben betreffend das Authentisierungsverfahren. Man könnte es auch zusammen mit Chipkarten oder Token einsetzen<sup>6)</sup>. Da mit Weblogin die Authentifizierung für alle Services über ein- und dieselbe Webseite erfolgt, könnten in ferner Zukunft, wenn einmal alle webbasierten Services in Weblogin eingebunden sind, quasi durch Austausch einer Login-Seite alle webbasierten Services mit einem Schlag umgestellt werden. Das ist eine wertvolle längerfristige Option, bis auf weiteres bleibt aber auf Seite der Anwender/-innen jedoch alles beim Alten.

Auch kurzfristig bringt die Einbindung eines Services in Weblogin einen ganz entscheidenden Sicherheitsgewinn: Selbst wenn z.B. Hacker in das Service einbrechen, können sie keine Passwörter mehr erschnüffeln. Diese gelangen

nämlich nur mehr zur (einzigen) Login-Seite, aber nicht mehr zu den Anwendungen selbst. Mit dem konventionellen System hingegen braucht ein Bösewicht nur in ein einziges der vielen passwortgeschützten Services einzubrechen, um auch zu allen anderen Zugang zu erlangen. Damit verringert sich die Angriffsfläche für Identitätsdiebstähle dramatisch. Darüber hinaus kann sich die Absicherung und Überwachung auf ein System konzentrieren, was wiederum ein Beitrag zur Gesamtsicherheit ist.

## Wider den Account-Wildwuchs

Jeder kennt das leidige Problem: Tausende Stellen, vom Astronomieportal bis zum Zentralen Informatikdienst, geben einem für ihre Dienste einen Account, man muss sich also eine UserID und ein Passwort merken. Das Passwort sollte möglichst kompliziert sein, darf aber niemals aufgeschrieben werden. Wehe dem, der kein photographisches Gedächtnis hat. Der Einfachheit halber überall das selbe Passwort zu verwenden, ist ebenso verlockend wie fahrlässig: Würde nur bei einem Betreiber eingebrochen, wären damit auch alle anderen Accounts betroffen, mit allen möglichen Konsequenzen.

Sogar innerhalb der Universität Wien gibt es zahlreiche Accountsysteme, die nicht miteinander bzw. dem des ZID-Passwörtern verbunden sind. Das liegt nicht etwa am Eigensinn der Institute oder an der Selbstherrlichkeit des ZID, sondern genau am soeben geschilderten Problem: Die ZID-Accounts sind nur so stark wie das schwächste Glied und es wäre nicht verantwortbar, zuzulassen, dass Server, die nicht unter der Kontrolle und regelmäßigen Wartung des ZID stehen, zum schwächsten Glied werden.

Mit Weblogin hat sich das schlagartig geändert: Da keine Passwörter zu den Services gelangen, können nun auch Institute und Dienstleistungseinrichtungen für webbasierte Services die vom ZID zentral verwalteten Accounts verwenden.

1) siehe Artikel *AAI in Aktion – Web Single Sign-On an der Uni Wien* in comment 07/2, Seite 21 (<http://comment.univie.ac.at/07-2/21/>)

2) <http://shibboleth.internet2.edu/>

3) Allerdings ist es hierbei unbedingt notwendig, dass der Browser Cookies akzeptiert.

4) siehe hierzu auch Artikel *Phishing – Bitte nicht anbeißen!* in comment 06/2, (<http://comment.univie.ac.at/06-2/37/>)

5) siehe Punkt 3 zu Verpflichtungen des Benutzers/der Benutzerin in der *Benutzungsordnung für UserIDs* des Zentralen Informatikdienstes abrufbar unter [www.univie.ac.at/ZID/benutzungsordnung/#verpflichtungen](http://www.univie.ac.at/ZID/benutzungsordnung/#verpflichtungen)

6) Chipkarten ergeben im Anwendungsbereich der allgemeinen ZID-Services aus Security-Sicht wenig Sinn, hingegen sind Einmalpasswörter bzw. Token durchaus überlegenswert.

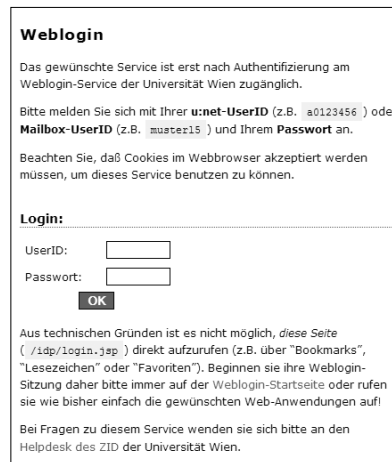
Für die Anwender/-innen bedeutet das, dass sie keinerlei Registrierung, UserID oder Passwort für alle diese Services mehr benötigen, sondern diese völlig beruhigt mit ihrem ZID-Account nutzen können. Für die Sicherheit bedeutet das, dass der Druck, Passwörter mehrfach zu verwenden oder gar auf Post-Its zu schreiben und unter die Tastatur zu kleben, sinkt.

## Mehr als die Summe aller Teilnehmer

Shibboleth, eine SAML V2 Implementierung<sup>7)</sup> – vereinfacht gesagt, die Technologie hinter Weblogin –, ermöglicht die Bildung sogenannter *Federations*. Dazu wird ein organisatorischer und technischer Rahmen aufgebaut, der mehrere Identity Provider (also Institutionen wie z.B. Universitäten, die User/-innen authentifizieren und Attribute liefern können) sowie Service Provider (also webbasierte Anwendungen) zusammenfasst.

Im Rahmen des ACONet wird eine derartige Federation für österreichische Wissenschafts- und Bildungseinrichtungen aufgebaut, sie heißt *ACONet-AAI Federation* (AAI steht für Authentifizierungs- und Autorisierungs-Infrastruktur, siehe [www.aco.net/aai.html&L=0](http://www.aco.net/aai.html&L=0)). Dass hier eine einheitliche

7) *Security Assertion Markup Language* (kurz SAML) ist eine XML-basierte Auszeichnungssprache für Sicherheitsbestätigungen. Sie stellt Funktionen bereit, um sicherheitsbezogene Informationen zu beschreiben und zu übertragen.



**Abb. 2: Die Login-Maske kann aus technischen Gründen nicht direkt aufgerufen werden. Nach der Anmeldung für ein in Weblogin eingebundenes Service, z.B. CTI, können auch alle anderen eingeschlossenen Services ohne erneute Anmeldung genutzt werden.**

Schnittstelle geschaffen wird, macht es möglich, mit der UserID und dem Passwort einer Universität auch Services an anderen Universitäten oder sonstigen Institutionen sowie teilnehmenden externen Dienstleistern in Anspruch zu nehmen.

Die Möglichkeit des interuniversitären Sign-On wurde bereits bei u:book intensiv genutzt: Die Berechtigungskontrolle für die u:book-Shops sowie das u:book-Forum erfolgte bei der letzten u:book-Aktion (siehe Artikel Seite 14) bereits für Angehörige aller elf teilnehmenden Universitäten über SAML V2.

## Und das Single Logout?

Bedenken Sie, dass Ihr Browser durch das Single Sign-On nach dem Weblogin für alle Services angemeldet ist. Vergessen Sie also nicht, den Browser zu schließen, wenn Sie Ihre Arbeit beenden bzw. Ihren Arbeitsplatz zu schützen, wenn Sie diesen kurz verlassen.

## Fazit

Es wird mit Sicherheit noch einige Zeit brauchen, bis das neue Single Sign-On-System einigermaßen flächendeckend bei den webbasierten Anwendungen der Universität Wien im Einsatz ist. Mit dessen Inbetriebnahme ist jedenfalls ein wichtiger Schritt in diese Richtung gelungen.

Alexander Talos-Zens ■