Auth/Aut/Sig, IDM, LDAP und Shibboleth

Ein KIM-Projekt

Markus Grandpre
Iris Kustermann
Michael Längle
Bernd Schmid-Ruhe

Wer aufgrund des Titels meint, es handle sich hier um einen Artikel über ein in KIM betriebenes Krypto- oder Dechiffrierungsprojekt liegt falsch. Vielmehr verbergen sich dahinter Technologien und Prozesse, die für die Universität von großer Bedeutung sind. Um was es geht, soll im Folgenden erklärt werden. Um es vorweg zu nehmen: Es handelt sich - ganz verallgemeinernd gesagt - um die Beantwortung der Frage, wer im Netz was darf. Eine solche Fragestellung ist im Zeitalter elektronischer Dienste essentiell; personalisierte Dienste, sei es in der Verwaltung, im Rechenzentrum oder der Bibliothek, prägen die Online-Arbeit und finden immer weiter Verbreitung.

Durch die gewachsenen Strukturen und die große Autonomie der einzelnen Einrichtungen und Fachbereiche haben sich in den letzten Jahren viele unterschiedliche Verfahren zur Authentifizierung („Auth" - hier lösen wir also das erste Abkürzungsrätsel des Titels) herausgebildet. Bisher hatten die Benutzer unterschiedliche Kennungen für die unterschiedlichen Dienste. Eine pop-Nummer, eine Matrikel-Nr., Vorname.Nachname oder andere Kennungen - je nach System. Ein Ziel des Projekts ist es, die große Zahl an Login-Kennungen zu vereinheitlichen. Nur ein kleiner Test: Kennen Sie ihre mdm-Nummer auswendig? Nein? Sie wissen nicht einmal, was das ist? Es gibt also viel zu tun...

Eine Vereinheitlichung macht es aber nicht nur dem Benutzer leichter, schließlich muss er sich nicht mehr viele Kennungen und Passwörter merken, sondern konsolidiert in erheblichen Maß die dahinter liegenden IT-Prozesse. Die Einführung universitätsweiter Dienste, wie z.B. bei den Druckern und Kopierern, zeigte nämlich recht schnell, dass die vielen unterschiedlichen Verfahren zu Problemen führen können.

Auf lange Sicht ist aber wesentlich mehr geplant als nur die Vereinheitlichung von Login-Daten. Es geht auch darum, für derzeit in der Planung befindliche automatisierte Verfahren eine Basis zu schaffen, die es erlaubt, Routinetätigkeiten und Verwaltungsaufgaben elektronisch erledigen zu lassen. Dabei soll vor allem für Transparenz der Vorgänge, Abläufe und Fortschritte eines Vorgangs gesorgt werden, um den Service zu verbessern. Beschaffungsvorgänge sollen so nachvollziehbar gemacht werden und Reisekostenanträge können dann in Zukunft als Formular im Netz zur Verfügung gestellt und dort ausgefüllt und elektronisch bearbeitet werden. Dafür ist allerdings die Einführung einer elektronischen Signatur notwendig, um z.B. die Identität eines Antragstellers prüfen zu können. Hierfür ist ein konsistentes Identity Management („IDM") notwendig, das die Infrastruktur für alle weiteren elektronischen Verfahren zur Authentifizierung zur Verfügung stellt. Davon ausgehend können dann z.B. mit anderen technischen Lösungen automatisch persönliche Signaturen erstellt und diese auf maschinenlesbare Medien gebracht werden.

Bis dahin ist es aber noch ein weiter Weg. Jetzt müssen zunächst die bisherigen Verfahren zur Anmeldung von Benutzern auf Vereinheitlichung geprüft werden, neue Datenbanken müssen dafür aufgebaut und alte Datenbanken angepasst werden. Vor allem aber müssen die bestehenden Datenstrukturen überprüft und neue Benutzergruppen modelliert werden. Zudem müssen die neuen Arbeitsprozesse aufgeschrieben, überprüft und standardisiert werden, damit sie sich nahtlos in die bestehenden Systeme und Prozesse einpassen. Das Projekt ist mit seiner Komplexität wegweisend für die Zukunft aller digitalen Dienste im Serviceverbund KIM, da es nicht nur zentral für den Aufbau neuer Dienste ist, sondern ein Fundament für alle Aufgaben im Bereich der Authentifizierung darstellt.

Ein weiterer immens wichtiger Bereich der Authentifizierungsverfahren, vor allem, wenn es um die Anmeldung für bestimmte Bibliotheksdienstleistungen (z.B. ReDi) geht, ist unter dem Schlagwort Shibboleth benannt. Vielleicht verwendeten die Gileaditer vor 3000 Jahren das erste Authentifizierungsverfahren, denn sie verlangten bei Personenkontrollen dass das Wort "Schiboleth" ausgesprochen wurde; erklang danach nur ein gelispeltes "Siboleth" erkannten sie ihren Feind und erschlugen ihn.

So heisst es im Buch Richter 12, 5-6:

„Und die Gileaditer nahmen ein die Furten des Jordans vor Ephraim. Wenn nun die Flüchtigen Ephraims sprachen: Laß mich hinübergehen! so sprachen die Männer von Gilead zu Ihm: Bist du ein Ephraimiter? Wenn er dann antwortete: Nein! hießen sie ihn sprechen: Schiboleth; so sprach er Siboleth und konnte es nicht recht reden; alsdann griffen sie ihn, schlugen ihn an den Furten des Jordans, daß zu der Zeit von Ephraim fielen zweiundvierzigtausend."

Die Folgen eines nicht erfolgreichen Authentifizierungsvorgangs sind heute nicht mehr ganz so drastisch. Statt Totschlags haben die Benutzer heute nur mit einer Meldung zu rechnen, dass entweder Benutzername oder Passwort unbekannt bzw. falsch waren.

Wenn wir also obiges Verfahren in unsere Zeit übernehmen würden, könnten wir mit Hilfe der richtigen Aussprache zwar mit "Chuchikäschtli"" den Schweizer, mit "Nebeprisikiškiakopūsteliaudavome" einen Litauer und mit

吃葡萄不吐葡萄皮，不吃葡萄倒吐葡萄皮

(= Pinyin: chi pu tao bu tu pu tao pi, bu chi pu tao dao tu pu tao pi.) eine Chinesin identifizieren.
aber mit dieser Methode lässt sich nur schwer ein sinnvoller elektronischer Authentifizierungs- und Autorisierungsdienst für den Campus aufbauen. Ziel von Shibboleth ist es nämlich, Studierenden und Forschern geschützte Ressourcen weltweit zugänglich zu machen. Die Anmeldung geschieht jeweils am Authentifizierungsdienst der Heimatuniversität der nach außen keine vertraulichen Daten preisgibt und nur Daten übermittelt, die für das Einloggen in diesen einen bestimmten Dienst notwendig sind.

Vielleicht ist es noch zu früh um zu prophezeien, dass zukünftig Studenten unserer Partneruniversität Tongji vom fernen Shanghai aus Online-Seminare der Universität Konstanz besuchen, elektronisch Prüfungen ablegen und in ihrer Heimat diese Leistungen anrechnen lassen können. Jedoch die organisatorischen und technischen Vorbereitungen für eine internationale Authentifizierungs- und Autorisierungsinfrastruktur sind bereits in vollem Gange.

Glossar:

Authentisierung/Authentifizierung
Man versteht darunter die Vorgänge und Verfahren, sich gegenüber einem Verzeichnisdienst "auszuweisen" bzw. von diesem als die Person anerkannt zu werden, die man vorgibt zu sein. In der Regel passiert das heute mit einem Benutzernamen und einem Passwort, kann in anderen Bereichen auch über einen Fingerabdruck- oder Retinalscan erfolgen.

Autorisierung
Dabei handelt sich um den Vorgang, der direkt auf die Authentisierung folgt. Weiss man erst einmal, um wen es sich handelt, der sich da anmeldet, muss das System bei der Autorisierung nun entscheiden, was die Person im System tun darf. Die so genannte Rechtevergabe ist Kernstück der Autorisierung.

Signatur
Man versteht unter elektronischen Signaturen die Übertragung der händischen Unterschrift in die digitale Welt. Mit diesen Signaturen soll gewährleistet werden, dass sich niemand für eine andere Person ausgeben kann und somit rechtsgültige Vorgänge autorisiert werden können.

IDM
Das Identity Management (IDM) beschreibt verschiedene Prozesse und Techniken, um Authentifizierungsdaten mit den einzelnen Diensten in Verbindung zu bringen bzw. um Daten zwischen den einzelnen Diensten abzugleichen. Das ist zum Beispiel notwendig, wenn ein Benutzer sein Passwort ändern will oder sich andere persönliche Daten ändern und die angeschlossenen Systeme davon in Kenntnis gesetzt werden müssen.

LDAP
LDAP steht für "Lightweight Directory Access Protocol" und beschreibt, wie Authentifizierung und Authentisierung gegen einen Authentifizierungsdienst abzulaufen haben. Oftmals wird das Kürzel auch synonym für den zentralen Authentifizierungsdienst verwendet.

Shibboleth
Shibboleth ist der Name für ein verteiltes Authentifierungsverfahren im Internet, das es erlaubt, die Autentisierungsdaten dezentral vorzuhalten, aber dennoch für viele unterschiedliche Dienste und Institutionen zu nutzen. So müssen Benutzerdaten nicht vielfach für jeden Dienst gepflegt werden und Benutzer müssen sich nur einmal einloggen, um viele Dienste parallel nutzen zu können ("single sign on").