

Konzept

für eine elektronische Akademische Gemeinschaft in der Schweiz

und den Aufbau einer gemeinsamen Authentifizierungs- und Autorisierungsinfrastruktur (AAI) für das Schweizerische Hochschulsystem

Ausgearbeitet von einer interuniversitären Arbeitsgruppe ¹

Version 2.4, 8.10.2001

Vision

Unsere Vision: Wir wollen eine hochschulübergreifende virtuelle Gemeinschaft, in welcher alle Angehörigen des Schweizer Hochschulsystems Zugang zu den elektronischen Hochschulressourcen erhalten, unabhängig vom physischen Ort, wo sie akkreditiert sind und unabhängig vom Ort, wo sie gerade arbeiten. Unsere Besorgnis: Wir finden heute Papierbasierte Anmeldeverfahren pro Hochschule, der Einsatz inkompatibler Zugangskontrollsysteme und die Notwendigkeit mehrfacher elektronischer Identitäten. So darf die Zukunft der Hochschullandschaft nicht aussehen. Deshalb unser Aufruf: Bauen wir e-Academia, lasst uns die Grundlage legen in Form einer gemeinsamen Authentifizierungs- und Autorisierungsinfrastruktur (AAI) für das Schweizerische Hochschulsystem!

e-Trust

Es gibt eine lange und fruchtbare Tradition der Zusammenarbeit unter unseren Hochschulinstituten in der Schweiz. Die Ergebnisse dieser Bemühungen sind eine einheitliche Zugangspolitik (Matura), ein System für die finanzielle Abrechnung von Ausbildungskosten unter den Kantonen oder eine gemeinsame nationale Computer-Netzinfrastuktur. Neben den Vorteilen für den Einzelnen hat diese Zusammenarbeit auch eine solide Beziehung des Vertrauens geschaffen: Akademische Grade anderer Institutionen werden voll anerkannt, die Mitgliedschaft in einer Partnerinstitution ist die erforderliche und ausreichende Voraussetzung für den Zugang zu lokalen Ressourcen wie Bibliotheken und Kursangeboten. Gegenstand des vorliegenden Konzeptes ist die Ausdehnung dieser Vertrauensbeziehung in das Computer-Zeitalter. Zu diesem Zweck schlagen wir vorbereitende Studien für die Entwicklung einer Schweizerischen Authentifizierungs- und Autorisierungsinfrastruktur (AAI) für das Hochschulwesen vor.

¹ Mitglieder: Dr. Serge Droz (PSI), Christoph Graf (SWITCH), Gerhard Hassenstein (Fachhochschule Bern), Christian Heim (Universität Bern), Thomas Lenggenhager (SWITCH), David Meier (Universität Zürich), Dr. Jacques Monnard (Universität Fribourg/Swiss Virtual Campus), Dr. Alexandre Roy (Universität Lausanne), Hansueli Sonderegger (Universität Zurich), Prof. Dr. Christian Tschudin (Universität Basel)

e-Mobility

In naher Zukunft wird alles, was von Hochschulinstituten hervorgebracht wird, über das Netz verfügbar sein: Online-Immatrikulationsformulare, Lehrmaterial (z.B. Swiss Virtual Campus), Stundenpläne, Kursbeurteilungen und sogar Prüfungsergebnisse! Im Hintergrund stehen die Standardisierung akademischer Lehrpläne und die Einführung von Bonuspunktesystemen als Grundlage der Personenmobilität. Mobilität bedeutet in vielen Fällen, dass Personen an einem anderen Ort erneut ein komplettes Immatrikulations- oder Anmeldeverfahren durchlaufen müssen, wobei die Vertrauensbeziehung und das oben erwähnte Prinzip der Delegation ganz einfach ignoriert werden. Gleiches gilt im elektronischen Raum, wo der Zugang zu Ressourcen nur den Benutzern an einem spezifischen Standort oder innerhalb eines Netzwerkes offen steht. Dadurch wird der Nutzen vorhandener oder zukünftiger Möglichkeiten des Fernzugriffs stark eingeschränkt. Fernzugriff sowie Personenmobilität erfordern die Mobilität und die elektronische Transitivität von Vertrauen!

e-Administration

Wir haben das Vertrauen der Hochschulen untereinander und die Mobilitätsprobleme einzelner Mitglieder der Hochschulgemeinschaft angesprochen. Neben den individuellen Erleichterungen, die eine Lösung dieser Probleme mit sich bringen würde, ist eine AAI auch für die administrativen Prozesse von Wichtigkeit: Zu oft gibt es parallele Immatrikulationsverfahren und inkompatible Zugangskontrollsysteme; Die Medienkette wird stets unterbrochen, wenn es um interuniversitären Datenaustausch geht. Wir haben die Pflicht, das Potenzial der Informationstechnologien zugunsten der Hochschulen auszuschöpfen. Dazu braucht es eine landesweiten AAI, auf welche interne administrative Prozesse aufsetzen können.

e-Academia

Unsere Vision ist e-Academia: eine Gemeinschaft von Studenten, Forschenden und Lehrenden, welche den freien Fluss der Ideen, den Austausch über Entdeckungen und die wissenschaftliche Debatte in den neuen digitalen Raum trägt. Eine AAI stellt einen kleinen aber wichtigen Schritt in diese Richtung dar.

AAI-Profil und Nutzen

Eine Authentifizierungs- und Autorisierungsinfrastruktur erfüllt mehrere Zwecke:

- Bereitstellen von vollständig computergestützten Verfahren, um über das Netz zu ermitteln, ob eine Person tatsächlich Mitglied einer akademischen Institution der Schweiz ist (**Authentifizierung**).
- Der Zugang zu Ressourcen kann auf der Grundlage von Mitgliedsinformationen gewährt werden (**Autorisierung**). Viele Zugangskontrollsysteme beruhen auf derartigen Mechanismen, z.B. Nutzung von Bibliotheken, Zutritt zu Gebäuden, elektronische Dienste oder Fernimmatrikulation für Kurse.
- Digitale Signaturen in elektronischen Dokumenten können auf ihre **Authentizität** und Dokumente auf ihre **Integrität** geprüft werden. Dies ist eine Grundvoraussetzung, um unterzeichnete Dokumente durch elektronische Formulare zu ersetzen und wird auch für die gesicherte E-Mail-Übertragung verwendet.

- Daten können gegen unberechtigtes Einsehen geschützt werden, indem eine Verschlüsselung verwendet wird, die für ein bestimmtes Mitglied codiert ist. Die **Vertraulichkeit** von Daten gewinnt für Einzelpersonen und für gemeinschaftliche F&E-Projekte von Hochschulen und Industrie zunehmend an Bedeutung.

Das Endergebnis dieser Fähigkeiten ist, dass Interaktionen zwischen Einzelpersonen und mit administrativen Instanzen kryptographisch gesichert werden und sich elektronisch überprüfen lassen. Diese Eigenschaften sind auch erforderlich, um die Ergebnisse und den Ruf einer akademischen Institution in der entstehenden Cyber-Welt zu schützen. Für die physische Mobilität von Austauschstudenten oder den Standortwechsel von Forschern stellt eine AAI die grundlegenden Mechanismen für ihre nahtlose Integration in vorhandene Zugangskontrollsysteme bereit.

Unter wirtschaftlichen Gesichtspunkten sind die Vorteile unmittelbar mit der Möglichkeit verknüpft, noch mehr administrative Prozesse zu automatisieren: Das einheitliche Identifizierungsschema (d.h. die Authentifizierung) ermöglicht die Straffung und das Zusammenlegen von parallel existierenden Autorisierungssystemen, die heute oft manuell überbrückt werden müssen. Durch die gemeinsamen Bemühungen um den Betrieb einer bundesweiten AAI profitieren akademische Institute von Mengenrabatten. Darüber hinaus werden die einer AAI zugrunde liegenden gemeinsamen Richtlinien zu einer Harmonisierung der Akkreditierungs- und Immatrikulationsverfahren führen.

Eine AAI kann auf unterschiedliche Arten implementiert werden. So könnten zum Beispiel Studentenausweise oder auf einer Festplatte gespeicherte Zertifikate Bestandteil einer AAI sein, ergänzt durch Biometriesensoren im Bedarfsfall. Unabhängig davon können unterschiedliche Niveaus der Entscheidungsdelegation angestrebt werden, auch Mischformen sind denkbar: von reiner Authentifikation („uns interessiert nur die Identität der Benutzer und wir gewähren Zugangsrechte aufgrund lokaler Tabellen“), über allgemeine Regeln („Netzwerkzugang soll allen Angehörigen einer Organisation des Schweizer Hochschulsystems gewährt werden“), bis zu expliziter Delegation („Jeder an der ETH in einem IT-Kurs eingeschriebene Student soll Bibliothekszugang erhalten“). Die Wahl hängt ab von den Wünschen der Organisationen, sowie von den technischen, ökonomischen und juristischen Rahmenbedingungen. Diese Rahmenbedingungen aufzudecken ist ein erster Schritt zu einer AAI.

Mandat für eine vorbereitende AAI-Studie

Angesichts der oben beschriebenen Umstände ist eine vorbereitende Studie erforderlich, um Form und Umfang einer AAI zu definieren. Wir zeigen vier Bereiche im Zusammenhang mit einer AAI auf, die behandelt werden müssen:

1. **Rechtliche Aspekte** Datenschutzaspekte, Haftung und Verantwortung der beteiligten Institutionen und der Benutzer einer AAI. Ausarbeiten von Richtlinien für eine AAI.
2. **Organisatorische Aspekte** Welche Prozesse innerhalb von Institutionen müssen eingerichtet oder verändert werden?
3. **Technische Aspekte** Was ist technisch machbar, welche Technologien stehen für die Implementierung zur Verfügung? Ermitteln, welche Standards und Profile zu verwenden sind.
4. **Finanzielle Aspekte** Schätzungen für einmalige und laufende Kosten pro Institution und pro Benutzer. Untersuchung von Finanzierungsmodellen für gemeinsam genutzte Infrastruktur und Verfahren.

Diese Studie sollte in enger Zusammenarbeit und Absprache mit allen beteiligten Parteien durchgeführt werden und muss die dezentralisierte Struktur des Hochschulsystems der Schweiz berücksichtigen. Entwicklungen auf internationaler Ebene sind ebenfalls zu berücksichtigen.

Wir empfehlen den Prozess der Schaffung einer gemeinsamen AAI einzuleiten. Wir schlagen vor, dass die "Rektorenkonferenz der Schweizer Universitäten" (CRUS) die Studie in den oben genannten vier Bereichen bei SWITCH, Universitäten, Fachhochschulen oder Privatunternehmen in Auftrag gibt und koordiniert. Die CRUS sollte den Fortschritt überwachen und einen Abschlussbericht mit Empfehlungen ausarbeiten.

Der Weg zu einer AAI

Die oben beschriebene vorbereitende Studie wird als ein erster Schritt in Richtung einer Authentifizierungs- und Autorisierungsinfrastruktur für das Hochschulwesen in der Schweiz betrachtet. Wenngleich nur die erste Studienphase in den Themenbereich dieses Konzeptes fällt, zeigen wir mögliche Etappen und einen Zeitplan für den gesamten Weg in Richtung einer betriebsfähigen AAI auf:

- **Vorbereitende Studie:** (Oktober 2001 – April 2002)
Erreichen eines gemeinsamen Verständnisses und einer gemeinsamen Sichtweise dessen, was erforderlich ist, und wie man zu einer AAI für das schweizerische Hochschulwesen gelangen kann. Ergebnis sind ein Bericht und Empfehlungen.
- **Entscheidung:** (Juni 2002)
Die Ergebnisse werden geprüft, einzelne Institutionen entscheiden, ob sie ein AAI-Konsortium bilden oder ein Mandat vergeben.
- **Pilotprojekt:** (August 2002 - Juni 2003)
Auf der Grundlage der vorbereitenden Studie wird ein Pilotprojekt gestartet. Ziel ist es, praktische Erfahrungen zu sammeln und noch fehlende Komponenten zu ermitteln.
- **Entscheidung:** (Juni 2003)
Die Mitglieder des Konsortiums entscheiden, die AAI in Betrieb zu nehmen.
- **Implementierung:** (August 2003 - August 2005)
Das Pilotprojekt wird allmählich zu einer AAI in grossem Massstab entwickelt. Die vollständige Implementierung und Abdeckung wird für den Herbst 2005 ins Auge gefasst.

Zusammenfassung

Nicht alle Institutionen werden die gleichen Ziele verfolgen und die vorgeschlagene Authentifizierungs- und Autorisierungsinfrastruktur (AAI) in gleicher Weise nutzen. Die Autoren sind jedoch der Überzeugung, dass in Zukunft jedes Mitglied des schweizerischen Hochschulwesens eine bundesweite AAI brauchen und hiervon profitieren wird.

Wir glauben, dass eine gemeinsame AAI ein entscheidendes Element ist, wenn es darum geht, die organisatorischen Herausforderungen und Chancen der Informationstechnologien im akademischen Bereich zu meistern bzw. zu nutzen. Den beteiligten Organisationen steht es frei, sich für eine eigene AAI-Lösung zu entscheiden oder Allianzen mit anderen Institutionen zu bilden. Um ein Interworking zwischen verschiedenen AAI-Lösungen zu gewährleisten, ist die Einhaltung einer Reihe von AAI-Mindeststandards, der Betrieb einer grundlegenden Infrastruktur und die Einhaltung gemeinsamer Richtlinien von entscheidender Bedeutung. Um ihre Schaffung zu unterstützen, wird die CRUS aufgefordert, eine vorbereitende Studie über Umfang und Form einer potenziellen AAI in Auftrag zu geben und zu überwachen.