Auf dem Weg zur DFN-AAI: Identity Management

Das Projekt DFN-AAI (Authentifizierungs- und Autorisierungs-Infrastruktur) hat das Ziel, eine Föderation für Einrichtungen im Bereich Forschung und Lehre aufzubauen. Die Föderation schafft einen organisatorischen Rahmen und eine Vertrauensbeziehung zwischen Föderationspartnern (Anbieter von Ressourcen) und Föderationsmitgliedern (Nutzer dieser Ressourcen), die eine gemeinsame Authentifizierungs- und Autorisierungsinfrastruktur nutzen. Als Software wird die im Internet2 entwickelte Open-Source-Software Shibboleth[1] eingesetzt.

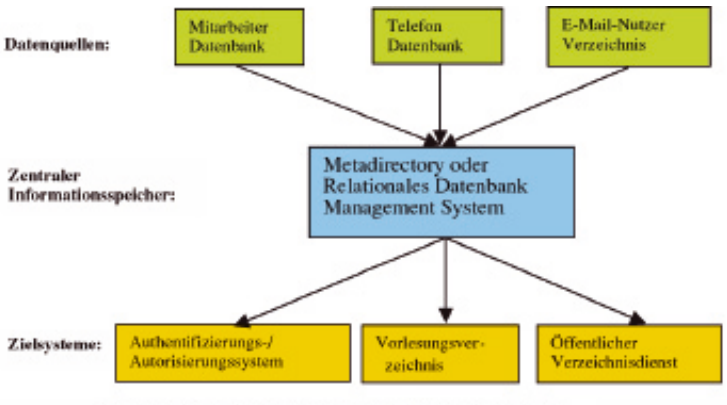
Im Folgenden werden die Voraussetzungen beschrieben, die Föderationsmitglieder in Bezug auf Identity Management einhalten müssen. Die ersten beiden Kapitel dienen zunächst der Einführung in das Thema Identity Management sowie der Beschreibung der Bedeutung des Identity Management in einer Shibboleth-Föderation. Danach werden die Voraussetzungen zur Teilnahme an der DFN-AAI beschrieben, gefolgt von Empfehlungen zur Umsetzung der Voraussetzungen.

Einführung in Identity Management

Motivation

Einrichtungen betreiben zur Nutzerverwaltung verschiedene Datenbanken und Verzeichnisse (z.B. Mitarbeiter- und Studentendatenbank, Telefondatenbank, E-Mail-Nutzerverzeichnis), die teilweise sich überschneidende Personendaten enthalten. Diese Vielzahl der Datenbestände führt häufig zu Redundanzen und Inkonsistenzen bei der Datenhaltung einer Einrichtung. Durch verschiedene Zuständigkeiten bei der Administration der Datenbestände fehlt zudem eine übergeordnete Sicht, welchem Nutzer welche Rechte gegeben wurden. Auch die Nutzer wissen nicht immer, in welcher Datenbank sie unter welchem Benutzeraccount eingetragen sind. Unter diesen Voraussetzungen ist z.B. nicht gewährleistet, dass Nutzern, die die Einrichtung verlassen, auch tatsächlich der Zugriff auf alle damit verbundenen Dienste entzogen wird.

Solche Probleme werden durch Identity Management gelöst. Mit Identity Management Systemen kann die Vielzahl der Accounts, die ein Nutzer für den Zugriff auf verschiedene Datenbanken und Anwendungen benötigt, in einer einzigen digitalen Identität zusammengefasst werden. Es ist abzusehen, dass Identity Management Systeme zukünftig zu einem grundlegenden Bestandteil der Infrastruktur einer Einrichtung werden.



Beispiel für Komponenten eines Identity Management Systems

Digitale Identität

Eine digitale Identität ist ein eindeutiger Name, eine Nummer oder Login-ID, mit der ein Computersystem eine Person identifiziert. Eine digitale Identität (ID) kann auch weitere, mit der ID verbundene Merkmale (auch Attribute genannt) besitzen, z.B. eine E-Mail-Adresse, Vor- und Nachname, Pseudonyme, akademischer Titel, Telefonnummer. Weitere Merkmale zu der ID können Gruppenzugehörigkeiten wie Mitgliedschaften in Mail-Listen oder **Rollen** sein, d.h. Funktionen, die die Person innerhalb der Einrichtung ausübt.

Komponenten

Als Identity Management (IdM) wird die Verwendung neuerer Technologien bezeichnet, die Identitätsinformationen zentral verwalten, sowie den Zugriff identifizierbarer Personen auf Ressourcen kontrollieren. Dadurch werden zwei wesentliche Ziele erreicht:

1. Identity Management erhöht das Sicherheitsniveau einer Einrichtung, indem die Datenbestände zur Nutzerverwaltung konsistent gehalten werden.
2. Identity Management senkt die Kosten für die Verwaltung von Identitätsinformationen.

Identity Management Systeme arbeiten mit automatisierten Prozessen, die die Aktualität der Daten in allen Systemen gewährleisten. Sie bestehen hauptsächlich aus folgenden Architekturbausteinen:

- **Datenquellen**, in denen Personendaten eingetragen und gepflegt werden. Dies können z.B. Mitarbeiterdatenbanken, Telefondatenbanken oder E-Mail-Nutzerverzeichnisse sein.
- **zentraler Informationsspeicher**, der aus den Datenquellen gespeist wird. Dieser kann als LDAP-Server implementiert sein (z.B. Metadirectory) oder als Relationales Datenbank Management System (RDBMS) vorliegen.
- **Zielsysteme** und Anwendungen, die ihre Daten aus dem zentralen Informationsspeicher beziehen. Ein mögliches Zielsystem kann ein **Authentifizierungs- und Autorisierungssystem** sein.
- automatisierte **Prozesse**, die einen Abgleich der Daten zwischen Datenquellen und zentralem Informationsspeicher bzw. zentralem Informationsspeicher und Zielsystemen vornehmen.

Die Einführung eines Identity Management Systems in einer Einrichtung stellt neben den technischen Aspekten auch eine **organisatorische Herausforderung** dar, da viele verschiedene Abteilungen (Rechenzentrum, Verwaltung, Pressestelle, Personalrat, Datenschutzbeauftragter etc.) mit einbezogen werden müssen. Um eine Zusammenarbeit der Abteilungen zu ermöglichen, ist es notwendig, dass die (Hochschul-)Leitung die Einführung eines IdM aktiv unterstützt.

Vorteile von Identity Management

Der erhebliche technische und organisatorische Aufwand zur Einführung von Identity Management wird durch eine Reihe von Vorteilen aufgewogen. Dies sind insbesondere:

- dauerhafte Kosteneinsparungen in der Administration
- Vereinfachung der Datenhaltung
- Konsistenz und Aktualität der Datenbestände
- höhere Sicherheit
- bessere Kontrolle über die Ressourcen
- Erleichterung bei der Einführung von neuen Diensten und Methoden (Single Sign On)
- optimale Unterstützung von internationalen Projekten, insbesondere im Bereich Gridcomputing

Bedeutung von Identity Management im Rahmen einer Shibboleth-Föderation

Innerhalb einer Shibboleth-Föderation vertraut man darauf, dass die teilnehmenden Föderationspartner und -mitglieder bei der Erbringung der folgenden Funktionen einen gemeinsamen Sicherheitsstandard einhalten:

- Authentifizierung und Autorisierung von Nutzern,
- Zugriffskontrolle auf Ressourcen,
- organisatorische und technische Prozesse, die durchlaufen werden, wenn eine Person in die Einrichtung aufgenommen wird, innerhalb der Einrichtung die Rolle ändert oder die Einrichtung verlässt.

Anbieter von Ressourcen wie z.B. einer kommerziellen Datenbank werden in Shibboleth als „Service Provider" bezeichnet. Service Provider vertrauen darauf, dass die verabredete Lizenzvereinbarung eingehalten wird. Steht eine bestimmte Datenbank z.B. nur Studenten zur Verfügung, ist es wichtig, dass eine Person nach der Exmatrikulation nicht mehr auf diese Datenbank zugreifen darf. Besagt die Lizenzvereinbarung, dass nur Studenten einer bestimmten Fachrichtung auf die Ressource zugreifen dürfen, sind auch diese Attribute (hier: Studienfach) aktuell zu halten und bei Fächerwechsel zeitnah zu ändern.

Einrichtungen, deren Angehörige Ressourcen nutzen wollen, treten als „Identity Provider" in einer Shibboleth-Föderation auf und sind für Authentifizierung und Attributierung zuständig. Für Identity Provider wird der Betrieb eines Identity Management Systems, mindestens aber einer vertrauenswürdigen Benutzerverwaltung mit konsistentem und aktuellem Datenbestand vorausgesetzt. Ein Identity Management System muss nicht als kommerzielles Produkt vorliegen, Systeme mit automatisierten Prozessen, die z.B. in Open Source Software implementiert sind, werden als gleichwertig angesehen. Zum Austausch der Attribute muss es ein gemeinsames Datenschema geben. Die obligatorisch und optional zu verwendenden Attribute werden in einem eigenen Dokument [2] spezifiziert.

Peter Gietz
DAASI International GmbH
peter.gietz@daasi.de

Dr. Jürgen Rauschenbach
DFN-Verein
jrau@dfn.de

Prof. Dr. Christian Grimm
RRZN Hannover
grimm@rvs.uni-hannover.de

Renate Schroeder
DFN-Verein
schroeder@dfn.de

Dr. Hans Pfeiffenberger
Alfred Wegener Institut
hpfeiffenberger@awi-bremer

Shibboleth ermöglicht nicht nur den Zugriff auf Ressourcen von Partnern, sondern kann auch für Anwendungen in der eigenen Einrichtung genutzt werden. Wird die in Shibboleth implementierte Single-Sign-On-Lösung auch innerhalb der eigenen Einrichtung eingesetzt, steht nach einmaliger Authentifizierung dem Nutzer jede an Shibboleth angepasste Anwendung – innerhalb und außerhalb der Einrichtung- ohne weiteren Login-Prozess zur Verfügung.

Voraussetzungen zur Teilnahme an der DFN-AAI

Vorausgesetzt wird der Betrieb eines **Identity Management Systems** oder mindestens einer **vertrauenswürdigen Benutzerverwaltung**, in denen Identitäten folgendermaßen verwaltet werden:

- Personen, die in einer Einrichtung aufgenommen werden, erhalten eine digitale Identität.
- Identitäten erhalten Attribute, die der Rolle der Person entsprechen.
- Werden Rolle oder Berechtigungen einer Person geändert, werden die Identitätsinformationen spätestens nach zwei Wochen angepasst.
- Für Personen, die die Einrichtung verlassen, wird die Identität mit allen in der Föderation relevanten Rechten und Rollen spätestens nach zwei Wochen gelöscht bzw. geändert (z.B. Student -> Alumni).
- Das Attributschema der DFN-AAI muss unterstützt werden (s. Dokument in [2]).
- Der Ressourcengeber kann sich darauf verlassen, dass alle Änderungen spätestens nach zwei Wochen ausgeführt sind.
- Die Prozesse müssen soweit schriftlich dokumentiert werden, dass das Sicherheitsniveau aus der Dokumentation ableitbar ist.

Empfehlungen zur Umsetzung der Voraussetzungen

Im Folgenden werden organisatorische und technische Maßnahmen zur Umsetzung der Voraussetzungen beschrieben. Auch unabhängig von der Föderation nutzen diese Maßnahmen bei der Integration der IT-Systeme.

Organisatorisch

- Es müssen definierte Prozesse für die Aufnahme einer Person in die Einrichtung bzw. das Ausscheiden einer Person aus der Einrichtung vorhanden sein.
- Die Identität der aufgenommenen Person muss verifiziert werden, mindestens über die postalische Adresse (durch Senden des Eingangspassworts an die gemeldete postalische Adresse), besser durch Vorlage eines Personalausweises oder eines entsprechenden Dokuments bei der registrierenden Stelle.
- Identitäten und Berechtigungen müssen spätestens zwei Wochen nach Aufnahme in die Einrichtung eingetragen und aktiv sein und ebenfalls spätestens zwei Wochen nach Ausscheiden wieder gelöscht sein.
- Diese Prozesse müssen von allen maßgeblichen Abteilungen der Einrichtung im laufenden Betrieb unterstützt werden.
- Diese Prozesse müssen im Einklang mit der Datenschutzgesetzgebung stehen.
- Diese Prozesse müssen dokumentiert sein, die Dokumentation sollte enthalten
  - in welchen Systemen welche Daten vorgehalten werden,
  - welche Daten von welchen Systemen auf welche Systeme übertragen werden,
  - welcher Art die Zustimmung der Betroffenen zu diesen Datenübertragungen ist,
  - wie die Daten vor unberechtigtem Zugriff geschützt werden,
  - die Maximaldauer, nach der die Daten eingetragen, geändert bzw. gelöscht werden,
  - in welchen Abständen ein Abgleich der Daten vorgenommen wird.

Technisch

- Es muss ein Identity Management System oder ein aus der Benutzerverwaltung gespeistes Authentifizierungs-/Autorisierungssystem existieren,
- das Authentifizierungsvorgänge ermöglicht,
- das Standardattribute für die Nutzer vorhält, die für Autorisierungsentscheidungen maßgeblich sind,
- dessen Daten über wohldefinierte, zumindest teilautomatisierte Prozesse von den Quellsystemen empfangen werden,
- das an den Identity Provider eines Shibboleth-Systems angeschlossen werden kann,
- das über einen Backup so gesichert ist, dass bei Ausfall eines Systems zeitnah ein neues System aufgesetzt werden kann.

Diese verkürzte Beschreibung eines Identity Managements soll den Einstieg der DFN Einrichtungen in dieses Thema unterstützen. Der hier beschriebene vorläufige, minimalistische Ansatz einer vertrauenswürdigen Benutzerverwaltung anstelle eines aufwändigeren Identity Management Systems soll den Einrichtungen im DFN die Möglichkeit geben, schon sehr bald – vielleicht sogar schon zum Start der DFN-AAI in 2007 - in diese viel versprechende Technologie einzusteigen.

Links

1 http://shibboleth.internet2.edu/
2 http://wiki.aai.dfn.de

Begriffe:

Attributierung
Attributierung heißt, die Identität mit Attributen versehen, wie zum Beispiel „Art der Zugehörigkeit: Mitarbeiter“ (oder: „Student“, „Alumni“,...). Dieses und andere Attribute können als Grundlage für Autorisierungsentscheidungen herangezogen werden (s. Autorisierung).

Authentifizierung
Beim Vorgang der Authentifizierung wird eine Überprüfung der Identität durchgeführt. Der Nutzer gibt an, die mit der ID verbundene Person zu sein. Das System führt Tests durch, um diese Behauptung zu beweisen bzw. zu widerlegen. Der einfachste und heute immer noch gebräuchliche Test ist die Abfrage eines Passworts. Hat der Nutzer das der ID zugewiesene Passwort angegeben, wird die Identität bestätigt.

Autorisierung
Nach erfolgter Authentifizierung des Nutzers kann das System aufgrund vordefinierter Zugriffsregeln (auch Access Control bzw. in ihrer Gesamtheit Policy genannt) entscheiden, welche Ressourcen dem Nutzer zugänglich gemacht werden.

Pseudonym
Fingierter Name, der anstelle eines realen Personennamen angegeben werden kann. um aus Datenschutzgründen eine gewisse Anonymität zu erreichen. In Shibboleth kann ein persistentes Pseudonym verwendet werden, das nur im Missbrauchsfall aufgelöst wird.

Single Sign On (SSO)
Eine auf Unified Login aufbauende Funktionalität, bei der sich ein Nutzer nur einmal am zentralen Authentifizierungsserver anmelden muss und danach für eine festgelegte Dauer für verschiedene Rechner und Anwendungen authentifiziert ist. SSO kann durch Nutzung und Implementierung von Shibboleth unterstützt werden.

Unified Login
Möglichkeit, auf verschiedene Rechner und Anwendungen über einen zentral gespeicherten Account, d.h. über ein einziges Passwort zugreifen zu können. Dies wird durch einen zentralen Authentifizierungsserver erreicht.