Integriertes Management von Identitäten im fakultativen und universitätsweiten Kontext

[I]Klaus Scheibenberger, [II]Horst Wenske, [II]Hannes Hartenstein, [I]Olaf Hopp

[I] Abteilung Technische Infrastruktur, Fakultät für Informatik,
[II] Rechenzentrum
Universität Karlsruhe (TH),
Kaiserstraße 12, 76131 Karlsruhe
klaus.scheibenberger | olaf.hopp @atis.uni-karlsruhe.de
horst.wenske | hannes.hartenstein @rz.uni-karlsruhe.de

Abstract: Die effiziente Verwaltung und Bereitstellung von Identitätsdaten in heterogenen Systemumgebungen ist nach wie vor eine intensiv diskutierte Thematik. Verschärft wird die Diskussion durch den Einsatz von IuK-Diensten[1] die institutionsübergreifend agieren und somit eine institutionsübergreifende Authentisierung und Autorisierung benötigen. Bisherige Umsetzungen im fakultativen, d.h. lokalen Kontext der ATIS (Abteilung Technische Infrastruktur), als Betreiber der Dienste für die Fakultät für Informatik, und Arbeiten im KIM-Projekt (**K**arlsruher Integriertes **I**nformations**M**anagement, [KIM]) haben ergeben, dass man diesbezüglich drei evolutionäre Phasen im lokalen Kontext eines einzelnen Betreibers und zwei in Bezug auf den universitätsweiten Kontext identifizieren kann. Diese Phasen werden vorgestellt und die Motivation für diese Phasen diskutiert.

1 Einleitung

Die Überprüfung der Identität eines Nutzers der einen IT-Dienst nutzen möchte, d.h. einen Dienst basierend auf einer Anwendung oder sonstigen IT-Systemen, wird als Authentisierung bezeichnet. Damit die technischen Systeme, die den IT-Dienst realisieren, eine Identitätsprüfung vornehmen können, muss dem Nutzer in irgendeiner Form eine Kennzeichnung zugeordnet sein. In vielen Fällen ist dies eine Kombination aus einer Benutzerkennung und einem Passwort. Außer seiner Benutzerkennung und dem Passwort zur Authentisierung sind dem Nutzer aber noch weitere, systemspezifische Attribute zuzuordnen, über welche die Nutzung des angebotenen IT-Dienstes gesteuert wird ([Sp03]). Dies kann beispielsweise der Pfad für das Heimatverzeichnis auf dem Fileserver sein, auf dem der Nutzer seine Daten ablegt. Ein weitere Klasse von Attributen sind die Informationen, in welcher Rolle der Nutzer von einem System oder eine Anwendung zugelassen werden, z.B. als Administrator, Mitarbeiter oder als eingeschränktes Mitglied. An derartige Rolleninformationen sind dann die entsprechenden Nutzungsrechte für eine Anwendung gebunden.

---

[1] *IuK-Dienst = Informations- und Kommunikations-Dienst.*
Wird im folgenden abkürzend als Dienst bezeichnet.

Der Vorgang, anhand solcher Informationen die Nutzung von IT-Diensten zu steuern, wird als Autorisierung (des Nutzers) bezeichnet. Im folgenden werden unter der allgemeinen Bezeichnung „Identitätsdaten“ sowohl Authentisierungs-, als auch Autorisierungsdaten zusammengefasst. Die Benutzerkennung, das Passwort und die weiteren zugeordneten Attribute u.a. Rolleninformationen, bilden eine Menge von Identitätsdaten – eine Identität. Im einfachsten Fall hat der Nutzer für alle Systeme bzw. Applikationen, die er beansprucht, voneinander unabhängige Identitäten. Bei einer Zahl von n Nutzern und m Diensten ergäben sich somit jedoch theoretisch nxm solcher Identitäten, die unabhängig voneinander anzulegen und zu pflegen sind, was in größeren Umgebungen bereits aus rein betrieblicher Sicht kein realistisches Vorgehen ist.

Die vorliegende Arbeit präsentiert im ersten Teil drei Entwicklungsschritte (Phasen) hin zu einer dienstorientierten Identitätenbasis im fakultativen (d.h. lokalen) Kontext eines Betreibers als Grundlage für das Management von Identitäten. Als Identitätenbasis wird hier eine Menge von einheitlich strukturierten Identitäten bezeichnet. Der lokale Kontext eines Betreibers umfasst die Dienste, die er selbst bereitstellt und betreibt. Die Phasen werden motiviert, indem die Defizite der einzelnen Schritte aus dem Blickwinkel des Betriebs sowie aus der Sicht des Nutzers analysiert werden. Im zweiten Teil (Kapitel 4) werden zwei weitere Phasen vorgestellt, die den lokalen Kontext erweitern. Universitätsweite Prozesse, wie beispielsweise das Lehrveranstaltungs- und das Prüfungsmanagement können in Bezug auf die darin eingebundenen Dienste betreiberübergreifend sein, berücksichtigt man ein kooperatives Versorgungssystem für IuK-Dienste mit mehreren Betreibern. Pflegen diese für ihre lokalen Dienste eine jeweils eigenständige Identitätenbasis, ist ein Konzept für die Verknüpfung dieser dezentral organisierten und damit in der Regel unterschiedlich strukturierten Identitätenbasen erforderlich, um eine eindeutige Nutzeridentität herzustellen (Phase 4). Da die, in die universitätsweiten Prozessen eingebundenen Dienste gemäß einer service-orientierte Architektur (SOA), unter Einsatz der Webservice-Technologie (WS-Technologie) realisiert werden sollen, ergeben sich zusätzliche Randbedingungen ([Ar04]). Diese resultieren aus der Berücksichtigung der, im Kontext einer SOA, aktuell verfolgte föderative Ansätze ([WS-F], [LiAl]) für die Handhabung von Identitäten und führen schließlich zu einem Gesamtkonzept (Phase 5).

2 Typisches Szenario - Verteilung von Identitätsdaten (Phase 1)

Eine heterogene Systemlandschaft ist gegeben, wenn mehrere, technologisch unterschiedliche Systemumgebungen parallel existieren. Ein Beispiel für verschiedene Teilumgebungen im universitären Umfeld sind Arbeitsplätze im Rechnerpool der Fakultät für Studierende, die sowohl Windows als auch Linux als Betriebssystem bereitstellen. Die im Laufe der Zeit entstandenen, Teilansätze zur Pflege und Bereitstellung von Identitätsdaten wie der *Network Information Service* (NIS(+), Fa. Sun, [NIS]), der *Active Directory Service* (ADS, Fa. Microsoft) oder der *Remote Authentication Dial-In User Service* (RADIUS, [RAD]), berücksichtigen jedoch jeweils nur spezifische Systemumgebungen. Für die Versorgung der einzelnen Teilumgebungen mit den erforderlichen, systemspezifischen Identitätsdaten werden diese in einem solchen Szenario meist zentral in einer Datenbank vorgehalten. Dort werden die Identitätsdaten je Nutzer gepflegt und dann, beispielsweise skriptgesteuert, in die einzelnen Systemumgebungen verteilt.

2.1 Defizite

Die Verteilung der Identitätsdaten hat sowohl sicherheitsrelevante Nachteile (Datensicherheit), sowie Nachteile aus betrieblicher Sicht und aus der Sicht des Nutzers.

a) Sicherheitsrelevante Defizite

- In der zentralen Nutzerdatenbank werden typischerweise unverschlüsselte Passwörter gespeichert. Das ist notwendig, um beim Zeitpunkt der Verteilung die Passwörter evtl. mit unterschiedlichen Kryptografieverfahren zu verschlüsseln, um sie an die speziellen Randbedingungen der heterogenen Systemumgebungen anzupassen. Das Datenbanksystem mit den grundlegenden Nutzerkonten muss dementsprechend gut abgesichert sein, da bei einem erfolgreichen Einbruch in ein derartiges System die Passwörter unmittelbar zugänglich wären.
- Die Verteilung der erforderlichen spezifischen Identitätsdaten in die jeweiligen Systemumgebungen und die damit verbundene Vervielfältigung sind weitere Probleme. Die Anzahl an Systemen, auf denen Identitätsinformationen vorgehalten werden ist hoch, dadurch steigt gleichzeitig das Potential, um Identitätsinformationen zu entwenden. Mit entsprechend verfügbaren „brute force“ Methoden könnten diese dann entschlüsselt werden. Z.B. liegen bei älteren RADIUS-Varianten die Nutzerdaten zum Teil sogar unverschlüsselt vor, wodurch potentiell ein direkter Zugriff auf die Passwörter möglich wird.

b) Betriebliche Defizite

- Für die Generierung der systembezogenen Identitätsdaten müssen speziell angepasste Verfahren, z.B. Skriptlösungen, entwickelt werden. Bei Änderungen, beispielsweise durch Aktualisierung des Betriebssystems an einem System für die Einwahl in das Datennetz, müssen diese evtl. ebenfalls angepasst werden. Damit entsteht wiederum ein hoher betrieblicher Aufwand, um den Verteilungsmechanismus aktuell zu halten.
- Ein weiteres Problem liegt in den betrieblichen Abläufen selbst, die potentiell Dateninkonsistenzen verursachen können. Muss beispielsweise ein Attributwert eines Nutzers für eine der Systemumgebungen angepasst werden, besteht die Gefahr, dass dies von einem Administrator lokal in der Systemumgebung, unabhängig von der Benutzerverwaltung, vorgenommen wird und damit Inkonsistenzen auftreten. Um dies automatisiert auszugleichen, wären aufwendige Synchronisationsmechanismen erforderlich.

c) Defizite aus Nutzersicht

- Gerade in größeren Umgebungen stehen Änderungen erst nach der oft zyklisch gesteuerten Verteilung aus der zentralen Datenbank zur Verfügung. Das hat für den Nutzer zur Folge, dass Änderungen evtl. nicht zeitnah verfügbar sind.

3 Teil I - Lokaler Kontext

3.1 Universeller Verzeichnisdienst

Unter einem universellen Verzeichnisdienst versteht man einen Dienst, der Daten, hier Identitätsdaten, über ein standardisiertes Zugriffsprotokoll bereitstellt. Dabei wird in der Regel von überwiegend statischen Daten ausgegangen, d. h., es werden wesentlich mehr Lesezugriffe als Schreiboperationen (Hinzufügen, Ändern oder Löschen von Daten) erwartet. Ein solcher (universeller) Verzeichnisdienst lässt sich beispielsweise als LDAP-Verzeichnis, d.h. als ein Verzeichnis, auf das unter Verwendung des *Lightweight Directory Access Protocol* (LDAP) zugegriffen werden kann, implementieren [Ca03]. Prinzipiell können die bereitgestellten Daten aber auch aus einem völlig anderen Kontext sein, z.B. die Bereitstellung von Regeln (Policies) im Rahmen eines Policy-basierten Managements. In [RFC2753] wird beispielsweise in diesem Kontext LDAP als Möglichkeit für die Realisierung eines Policy-Verzeichnisses vorgesehen. Verzeichnisdienste nach LDAP-Standard werden derzeit sowohl von der Sun als auch von der Microsoft als Nachfolger für die älteren Dienste NIS(+) und LAN Manager verwendet. Das LDAP-Protokoll wurde 1993 an der University of Michigan entwickelt, ursprünglich mit dem Ziel, basierend auf diesem Protokoll, eine Schnittstelle zwischen den existierenden X.500-Servern auf OSI-Basis und TCP/IP-basierten Clienten entwickeln zu können ([KV04]). Verglichen mit dem X.500 Directory Access Protocol (DAP) war das resultierende TCP/IP-basierte Protokoll deutlich einfacher (weniger Operationen, eine vereinfachte Codierung, etc.), woraus sich die Bezeichnung Lightweight DAP bzw. LDAP ergeben hat. Zur Organisation der gespeicherten Daten in einem Verzeichnisdienst werden vergleichsweise einfache Strukturen verwendet. Beispielsweise werden bei LDAP die Daten in einer Baumstruktur der so genannten DIT (Directory Information Tree) organisiert. Um die Zuverlässigkeit und die Zugriffsgeschwindigkeit zu erhöhen, werden in der Regel mehrere Verzeichnis-Server eingesetzt und die Änderungen ihrer Datenbestände durch Nutzung von Replikationsmechanismen abgeglichen. LDAP stellt entsprechende Mechanismen standardmäßig zur Verfügung. Inzwischen hat sich LDAP als ein de facto Standard für Verzeichnisdienste etabliert, und viele Anwendungen erlauben es inzwischen, Nutzerattribute u.a. zur Authentisierung, gegenüber einem LDAP-Verzeichnis zu verifizieren. Eine Speicherung der nutzerspezifischen Attribute in den Anwendungen selbst kann dann entfallen.

3.2 Reduzierung der Verteilung von Identitätsdaten (Phase 2)

Die zentrale Nutzerverwaltung an der Fakultät für Informatik der Universität Karlsruhe enthält aktuell etwa 4000 Nutzerkonten der Mitarbeiter der Fakultät und der Informatikstudierenden. Diese werden in einer SQL-Datenbank gehalten und umfassen die für die Nutzung verschiedener zentraler Dienste erforderlichen Identitätsdaten, z.B. für den Maildienst oder den Systemzugang im öffentlichen Poolbereich für die Studierenden. Die Nutzerverwaltung der Fakultät wird als zentraler Dienst durch die Betreiberorganisation für zentrale IT-Dienste der Fakultät, die Abteilung Technische Infrastruktur (ATIS), bereitgestellt. Aus dem SQL-Datenbestand wurden bislang im

wesentlichen die für das zentrale Mailsystem der Fakultät erforderlichen Identitätsattribute generiert. Dazu gehören u.a. Mailadressen, Mailalias-Adressen und Mailroutinginformationen. In der aktuellen Architektur werden für die zentralen IT-Dienste der Fakultät aber Identitätsdaten auch bereits über LDAP bereitgestellt. Die Mailadresse kann in einem zentralen LDAP-Adressbuch veröffentlicht werden – dies wird auch über ein LDAP-Attribut gesteuert. Außerdem wird aus dem SQL-Datenbestand das LDAP-Verzeichnis für den Studentenpool generiert, einem Bereich mit ca. 70 freien Arbeitsplätzen für Informatikstudierende und etwa 2000 Nutzerkonten. Die Authentisierung an diesen Arbeitsplätze unter dem Betriebssystem Linux erfolgt direkt gegenüber diesem LDAP-Verzeichnis, die notwendigen Identitätsdaten für die Anmeldung unter Windows werden daraus generiert und mit dem ADS des Pools synchronisiert. Die Pflege der Nutzerkonten wurde dezentralisiert, um eine hohe betriebliche Effizienz sicherzustellen; d.h. Neueinträge, Veränderungen oder Löschungen können von den zuständigen technischen Administratoren in den Einrichtungen selbstständig vorgenommen werden. Dazu erhalten sie über eine Weboberfläche Zugriff auf den ihnen jeweils zugeordneten Nutzerkontenbestand in der Datenbank.

3.2.1 Defizite

Gegenüber dem Szenario aus Phase 1 hat diese Lösung bereits den Vorteil, dass Identitätsdaten für einige Dienste nicht mehr verteilt und damit vervielfacht werden. Aber auch diese Struktur weist noch Mängel auf, die im Folgenden dargestellt werden:

a) Sicherheitsrelevante Defizite

- Es existieren noch mehrere voneinander unabhängige Datenbestände von Nutzerkonten (LDAP-Verzeichnisse und Datenbank). Dies ist eine unnötige Redundanz der Datenbestände.

b) Betriebliche Defizite

- Die LDAP-Verzeichnisse sind intern unterschiedlich strukturiert, da sie an den spezifischen, systemtechnischen Erfordernissen und Gegebenheiten der Systeme bzw. Applikationen ausgerichtet wurden. So wurden beispielsweise für die Dienste „Studentenpool“ und „Dial-In“ das LDAP-Verzeichnis zur Speicherung der verschlüsselten Passwörter verwendet. Im LDAP des Mailsystems dagegen wurden keine Passwörter hinterlegt, da diese über einen anderen Mechanismus im Mailsystem gehalten werden.
- Ist ein neuer Dienst einzubinden,
  - sind aufgrund der bestehenden Mischstruktur Anpassungen sowohl hinsichtlich der LDAP-Verzeichnisstrukturen, als auch der Verteilungsmechanismen aus der SQL-Datenbank in die LDAP-Verzeichnisse neu zu entwickeln oder anzupassen.
  - ist unter Umständen die Datenbankstruktur anzupassen , wenn beispielsweise bestehende Relationen verändert werden müssen.

  Dies hat unter Umständen wiederum Auswirkung auf die Weboberfläche zur Pflege des Nutzerkontenbestands. Dadurch ist insgesamt der Anpassungsaufwand bei der Einbindung neuer Dienste erhöht.

c) Defizite aus Nutzersicht

- Der Nutzer hat in der aktuellen Situation im Regelfall für die verschiedenen Dienste unterschiedliche, voneinander unabhängige Authentisierungsdaten (Benutzerkennung, Passwort). Häufig verwenden Nutzer deshalb für mehrere Dienste das gleiche Passwort, womit diese Information aber in verschiedenen Systemen unabhängig voneinander gespeichert wird. Daher muss sich der Nutzer zur Änderung seines Passworts auf verschiedene Systeme verbinden, wenn er die „Einheitlichkeit" seines Passworts nicht verlieren möchte, was sehr aufwändig ist. Eine automatische Verteilung des geänderten Passworts über die Dienste hinweg wäre zwar wünschenswert, würde aber in der aktuellen Situation einen hohen Aufwand für die Synchronisation erfordern. Außerdem wäre zu berücksichtigen, wie Fehler in dieser Synchronisation abzufangen wären.

3.3 Eliminierung der Verteilung von Identitätsdaten (Phase 3)

Die Ziele einer Weiterentwicklung bezogen auf die aktuelle Situation sind demzufolge, entsprechend den vorher aufgelisteten Defiziten:

- Reduktion der Anzahl von redundanten Datenbeständen für Nutzerkonten und hohe Verfügbarkeit.
- Vereinheitlichung von bereits bestehenden LDAP-Verzeichnissen und Orientierung am Nutzer und den Diensten, nicht an systemtechnischen Erfordernissen oder Gegebenheiten.
- Vereinfachung der Einbindung neuer Dienste.
- Vereinheitlichung der Authentisierung.
- Geringer Entwicklungsaufwand durch modulare, dienstbezogene Werkzeuge zur Pflege der Nutzerkonten.

3.3.1 Zielarchitektur

Die Architektur der zukünftigen Lösung wurde ausgehend von der bestehenden Architektur und den oben genannten Zielen entsprechend abgeleitet (Abbildung 1).

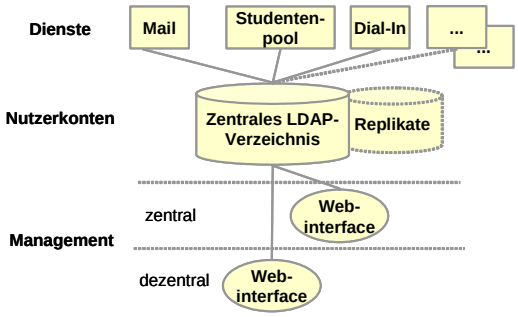

Abbildung 1: Architektur der zukünftigen Lösung

Auf die detaillierte, interne Struktur des zentralen LDAP-Verzeichnisses wird nachfolgend eingegangen. Diese Architektur bietet schließlich mittelfristig die Möglichkeit, die noch bestehenden Nutzerverwaltungen für lokale Nutzerkonten

innerhalb der Einrichtungen der Fakultät (z.B. NIS) abzulösen, und hierfür in Zukunft das zentrale LDAP-Verzeichnis zu nutzen (siehe auch 3.4).
Die folgende Abbildung 2 zeigt die interne, dienstorientierte Struktur des zentralen LDAP-Verzeichnisses.

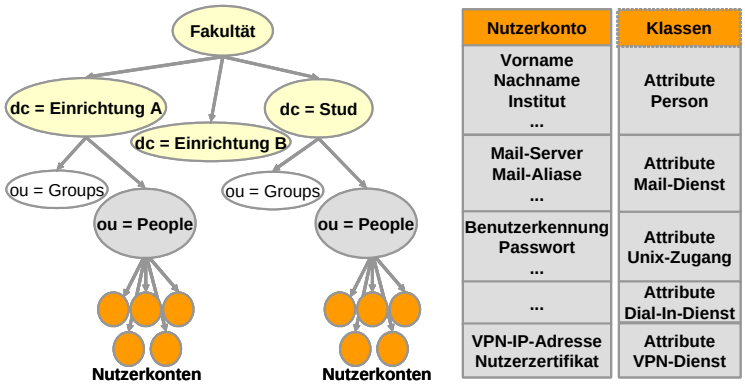

Abbildung 2: Dienstorientierte LDAP-Struktur der Nutzerdaten

Gruppen (ou=groups) bieten die Möglichkeit, Personen (ou=People) zusammenzufassen und ihnen kollektiv spezielle Anwendungen bereitzustellen.

3.3.2 Einbindung neuer Dienste

Bei dem in der Abbildung 2 dargestellten Dienst VPN (Virtual Private Network, [VPN]) handelt es sich um einen Zugangsdienst in das Datennetzwerk, der in der ATIS unter Verwendung von X.509-Zertifikaten [KV04] realisiert wurde. Für den VPN-Dienst sind für jeden Nutzer eine nutzerspezifische VPN-IP-Adresse sowie ein Nutzer-Zertifikat nach X.509-Standard zur Authentisierung zu verwalten. Für die Einbindung des VPN Dienstes wurden die VPN-spezifische Attribute in einer eigenen Klasse zusammengestellt und diese dem LDAP-Verzeichnis hinzugefügt. Damit stehen sie sofort als mögliche Attribute für alle Nutzerkonten zur Verfügung.

3.3.3 Managementwerkzeuge

Neben der einfachen Einbindung neuer Dienste ist aber ebenso die Frage nach der Pflege der Daten und der entsprechenden Werkzeuge wesentlich, da hier Routineaufgaben im täglichen Betrieb betroffen sind. Zwei Managementwerkzeuge wurden bereits (exemplarisch) für den Dial-In-Dienst und VPN-Dienst entwickelt (Dial-In-Adm, VPNadm) und werden produktiv eingesetzt. Beide Werkzeuge sind Webapplikationen, die direkt auf dem LDAP-Verzeichnis operieren, wie es in Abbildung 1 bereits angedeutet war. Da von den einzelnen Werkzeugen ausschließlich die dienstspezifischen LDAP-Attribute manipuliert werden, können analog dazu die erforderlichen Managementwerkzeuge für andere Dienste implementiert werden. Somit entstehen für unterschiedliche Dienste modulare, einheitlich strukturierte Werkzeuge. Die Pflege der Daten, ob intern durch die ATIS oder dezentral durch die Forschungsbereiche, bleibt erhalten, wird aber dadurch vereinfacht.

Die Abbildung der zur Zeit realisierten Zugriffsmodalitäten für die dezentrale Administration wird kein Problem darstellen.

3.3.4 Authentisierung

Ein vorteilhafter Effekt der Struktur in Abbildung 2 ist, dass sich eine einheitliche Kombination {Benutzerkennung, Passwort} für alle Dienste eines Nutzers ergibt. Will man aber die Möglichkeit, etwa aus Sicherheitsgründen, nicht für alle Dienste eines Nutzers haben, dann besteht die Möglichkeit, dass er einen zweiten, im LDAP gelisteten Account erhält, dem dann „andere“ Dienste zugeordnet sind. Die hier dargestellte vereinheitlichte Authentisierung ist ein erster Schritt zur Unterstützung der Integration von Anwendungen. Dies bedeutet gegenüber der Anwendung die Auslagerung der Authentisierung an LDAP. Man gewinnt hierdurch unmittelbar den bereits diskutierten Vorteil, dass Benutzerkennungen und Passwörter nicht auf einem lokalen System abgelegt sind. Die Einheitlichkeit von Benutzerkennung und Passwort über die Dienste hinweg ist ein Teilaspekt des sog. Single-Sign-On ([ZZ04],[HG05]). Eine Single-Sign-On-Lösung verfolgt jedoch darüber hinaus das Ziel, dass sich der Nutzer nur einmal anmelden muss und damit alle weiteren von ihm beanspruchten Dienste ohne erneute Authentisierung nutzen kann. Dieser Aspekt kann mit dem LDAP-Verzeichnis allein nicht realisiert werden, dazu müsste die Architektur um weitere Systeme ergänzt werden (z.B. Kerberos, [KER]).

3.3.5 Autorisierung

Neben der Authentisierungsmöglichkeit ist die Autorisierung die eigentliche Kernaufgabe eines Verzeichnisdienstes. Basierend auf den Daten im Verzeichnisdienst können Autorisierungsentscheidungen getroffen werden, mit welchen Rechten ein Nutzer auf ein System bzw. Applikation zugreifen darf. Im vergangenen Semester wurde dies im Kontext eines Vorlesungsportals verifiziert, das in dem Forschungsbereich Cooperation&Management aufgesetzt wurde ([Ha04]). Für einen Nutzer wurde dabei, über ein Registrierungsmodul, automatisiert ein LDAP-Verzeichniseintrag erstellt. Aufgrund von Zusatzinformationen, die bei der Registrierung abgefragt und als Attribute im LDAP-Verzeichnis gespeichert wurden, wurden den Teilnehmern unterschiedliche Rechte im Zugriff auf das System zugeordnet (z.B. das Erstellen von Beiträgen im Diskussionsforum des Portals). Dazu wurde eine eigene LDAP-Objektklasse erzeugt, in der entsprechende Zusatzattribute definiert und auf das im Portal vorhandene Rollenschema abgebildet wurden.

3.4 LDAP und Active Directory

Im Studentenpool wird den Nutzern über einen Dualboot-Modus sowohl Linux als auch Microsoft Windows als Betriebssystem angeboten. Nutzer an Windows-Clients, die in die Windows-Domäne des Studentenpools eingebunden sind, authentisieren sich bislang über den Active Directory Service (ADS) des Studentenpools. Die Nutzer von Linux-Clienten dagegen am LDAP-Verzeichnis. Die Passworteintragungen und -änderungen werden im LDAP-Verzeichnis vorgenommen und mit dem ADS synchronisiert, wofür das Werkzeug Services for Unix (SFU) eingesetzt wird. Ziel war es, unabhängig vom Betriebssystem immer das LDAP-Verzeichnis für die Authentisierung zu nutzen. Die oben dargestellte Verkettung war jedoch aufgrund von Inkompatibilitäten zwischen dem

LDAP-Verzeichnis und dem Active Directory erforderlich, beispielsweise in Bezug auf die Verschlüsselungsalgorithmen für Passwörter. Die Verkettung kann durch den Einsatz eines Samba-Servers (www.samba.org, [SAM]) aufgelöst werden, der als Windows-Domaincontroller einer eigenen Windows-Domäne eingesetzt wird. Zwischen der Windows-Domäne für die PCs des Studentenpools und dieser „Samba-Domäne“ wird eine Vertrauensstellung (*trusted relationship*) eingerichtet, und Windows-Anmeldungen werden über diesen Samba-Server schließlich an das LDAP-Verzeichnis weitergeleitet. Auch die Handhabung von sog. Grouppolicies ist in dieser Konstellation möglich.

4 Teil II - Universitärer Kontext

4.1 Verteilte Identitätenbasen

Innerhalb der Universität gibt es mehrere Betreiber von IuK-Systemen und Diensten, die bisher bereits eigenständig die Verwaltung und Bereitstellung von Identitäten, jeweils in einer eigenen Identitätenbasis, für ihre lokalen Dienste durchführen. Diese Betreiber, die in Bezug auf die gesamte IuK-Infrastruktur ein kooperatives Versorgungssystem bilden, werden im Folgenden als Satelliten bezeichnet und werden durch ihre Identitätenbasis repräsentiert. Ein solcher Satellit ist beispielsweise die ATIS (s. Kapitel 3); die Identitätenbasis bildet das zentrale LDAP-Verzeichnis für die Fakultät. Ein Nutzer hat evtl. in den verschiedenen Satelliten unterschiedliche, bisher von einander unabhängige Identitäten.

4.2 Anwendungsdienste – KIM-LPS

Im Rahmen des KIM-Projekts (**K**arlsruher integriertes **I**nformations**M**anagement [KIM]) der Universität Karlsruhe (TH) werden universitätsweite Prozesse untersucht. Im Teilprojekt KIM-LPS stehen zunächst Prozesse für das Lehrveranstaltungs-, das Prüfungsmanagement, sowie für die Studienassistenz im Vordergrund, und es werden Anwendungsdienste zur Unterstützung dieser Prozesse entwickelt. Diese Dienste werden in einer service-orientierten Architektur (SOA, [Ar04]) unter Einsatz der Webservice-Technologie (WS-Technologie) realisiert und nach Anwendungs- und Basisdiensten unterschieden. Die Basisdienste stellen Grundfunktionalitäten über Webservice-Schnittstellen zur Verfügung, die zu Anwendungsdiensten aggregiert werden. Die Anwendungsdienste werden unabhängig von dem Kontext, dem die Nutzer angehören, also institutionsübergreifend bereitgestellt. D.h. die Nutzer sind nicht mehr nur einem spezifischen Satelliten zugeordnet. Der Zugriff der Nutzer auf die Anwendungsdienste soll über ein Portal erfolgen. Da ein Anwendungsdienst in der Regel auf mehreren Basisdiensten beruht, werden Identitätsinformationen des Nutzers, die zur Anmeldung am Portal erforderlich sind, im Rahmen des Anwendungsdienstes von Basisdienst zu Basisdienst weitergegeben. Aus den initialen Identitätsinformationen, werden hierbei die weiteren, für die Basisdienste, notwendigen abgeleitet und beispielsweise in Form eines Identitätstokens zusammengefasst. Für die Weitergabe und Akzeptanz des Token ist die Einrichtung von Vertrauensstellungen zwischen den Bereichen (sog. *Realms*), die die Dienste bereitstellen, erforderlich. Damit kann ein Single-Sign-On ([ZZ04], [HG05]) realisiert werden, d.h. der Nutzer muss sich für die weiterführenden Basisdienste nicht erneut identifizieren. Gemäß einer service-orientierten Architektur wurde, für die

Anwendungs- und Basisdienste in KIM-LPS, zunächst ein in die SOA eingebettetes Konzept für die Authentifizierung und Autorisierung ausgearbeitet. Hierbei wurde auf Spezifikationen aus dem Bereich der Föderation zurückgegriffen (z.B. WS-Federation [WS-F]). Die Weitergabe der Identitätsinformationen über die Basisdienste hinweg erfordert natürlich auch ein entsprechendes Sicherheitskonzept. Dies ist aber eine Problemstellung im Rahmen der SOA und wird hier nicht weiter betrachtet.

4.3 Integration verteilter Identitätenbasen (Phase 4)

Unter dem Aspekt universitätsweiter Prozesse ist es erforderlich die existierenden Identitätenbasen zu integrieren. Die Beibehaltung der Eigenständigkeit der verschiedenen Satelliten ist dabei eine grundlegende Prämisse für den im folgenden diskutierten Ansatz. Motiviert wird dieser dadurch, dass ein Datenschema für eine zentrale Identitätenbasis in der Handhabung als zu wenig flexibel angesehen wird. Betrachtet man die heutige Identität eines Nutzers in einem der Satelliten als Teil einer Gesamtidentität dieses Nutzers, ist, als Folge der obigen Prämisse, eine effiziente Verknüpfung der Identitäten erforderlich.

Definitionen:

- Gesamtidentität: Zusammenfassung aller, in den Satelliten, einem Nutzer zugeordneten Identitäten.
- Identität: Menge der Identitätsattribute die einen Nutzer in einem Satelliten eindeutig definieren.
- Teilidentität: Teilmenge einer Identität.

Folgende Anforderungen wurden identifiziert:

- Es müssen unterschiedliche Satelliten mit unterschiedlichen Anforderungen in Bezug auf Identitäten berücksichtigt werden (Heterogenität).
- Die Satelliten sollen weiterhin flexibel die sie betreffenden Identitäten selbst verwalten können (Selbstverwaltung).
- Die Möglichkeit dezentraler Verzeichnisse für Identitäten (Identitätsbasen) soll weiterhin gegeben sein (Autonomie).
- Die Identitäten eines Nutzers in verschiedenen Einrichtungen müssen eindeutig aufeinander abzubilden sein (Eindeutigkeit).
- Identitätsattribute müssen zur Synchronisation und Sicherstellung der Konsistenz im gesamten Verbund austauschbar sein (Datenharmonisierung).
- Nur die für den jeweiligen Satelliten notwendigen Informationen sollen übernommen werden (Datenminimalität, Datenschutz).

Um einen eindeutigen Zusammenhang der Identitäten in den Satelliten zu gewährleisten, wird eine so genannte Kernidentität für einen Nutzer eingeführt. Die nach Rollen gegliederten Kernidentitäten umfassen die grundlegenden Identitätsinformationen zu Personen. Die Informationen für eine Kernidentität sollen aus dem Bereich der zentralen Verwaltung bereitgestellt werden, um eine hohe Qualität der Personendaten zu erreichen. Ordnet man einer solchen Kernidentität eine eindeutige Global User ID zu (GUID, RFC4122), können die Identitäten eines Nutzers in den dezentralen Bereichen über die GUID seiner Kernidentität verknüpft werden, wodurch eine universitätsweit eindeutige

Gesamtidentität einer Person hergestellt wird. Die Architektur für die Verknüpfung der Identitätenbasen besteht demnach aus einem zentralen Verzeichnis für die Kernidentitäten und mehreren unabhängigen Satelliten. Auf die Kernidentitäten soll von den Satelliten bei Bedarf, unter Kontrolle eines Rechtemanagements, zugegriffen werden, wobei aber die Verzeichnisse für die lokalen Identitäten (die Identitätsbasen) in den Satelliten technologisch unterschiedlich ausgeprägt sein können. Die Informationen einer Kernidentität sollen von einem Satelliten als Grundlage einer lokale Identität benutzt und durch zusätzliche Informationen, bezogen seine lokalen Dienste, angereichert werden. Minimal ist dabei die GUID einer Kernidentität zu übernehmen. Beispielsweise kann der ATIS-Satellit für einen Studierenden dessen Kernidentität beziehen und diese zu einer lokalen Identität erweiteren, die aus der lokalen Objektklasse „ATIS-Student“ abgeleitet wird. Diese kann dann weitere, für die Dienste der ATIS erforderliche, spezifische Attribute beinhalten, z.B. sein Druckguthaben im Studentenpool der Fakultät. Dieses Attribut ist ausschließlich im Bereich der ATIS relevant. Die Satelliten können damit weiterhin voneinander unabhängig „ihre“ Nutzer und deren „lokale“ Identitäten verwalten und die Identitätsinformationen an den Diensten ausrichten, die lokal bereitgestellt werden. Damit bleibt die Autonomie und Selbstverwaltung im lokalen Kontext eines Satelliten erhalten. Die Identitäten von Nutzern, die nur in einem der Satelliten lokal auftreten, müssen nicht in das Verzeichnis der Kernidentitäten aufgenommen werden, sondern werden rein lokal verwaltet. Damit wird die Änderungshäufigkeit im Verzeichnis der Kernidentitäten reduziert und somit auch der Aspekt der Datenminimalität berücksichtigt. Die unterschiedlichen Identitäten eines Nutzers in den Bereichen lassen sich aber über das Konzept der Kernidentität in einen eindeutigen Zusammenhang – die Gesamtidentität des Nutzers – stellen.

4.4 Gesamtszenario (Phase 5)

Die Zielstellung des Gesamtprojekts KIM ist es, die bisher erörterten Aspekte des lokalen Kontexts und universitätsweiter Prozesse miteinander in Einklang zu bringen. In Bezug auf das Identitätsmanagement sind unter Berücksichtigung der Struktur nach 4.1 und den dort erörterten Randbedingungen folgende Punkte zu beachten:

- Anwendungs- und Basisdienste sollen (evtl.) auch von Organisationseinheiten bereitgestellt und betrieben werden, die nicht notwendigerweise mit den Satelliten übereinstimmen.
- Anwendungsdienste können aus Basisdiensten, die von den Satelliten oder von weiteren Organisationseinheiten bereitgestellt werden, aggregiert sein. Sie sind also in diesem Sinne betreiberübergreifend.
- Die bereichsübergreifende Nutzung der Anwendungsdienste im KIM-Kontext erweitert den bislang in Kapitel 3 diskutierten lokalen Kontext eines Betreibers. Hier war die Gruppe der Nutzer eines Dienstes jeweils dessen lokaler Identitätenbasis zugeordnet. Dies galt auch noch in 4.1.

Die konzeptionelle Gesamtarchitektur zeigt Abbildung 3. Die initiale Authentisierung und Autorisierung eines Nutzers für einen Anwendungsdienst erfolgt hier nicht mehr wie in 4.2 innerhalb der SOA, sondern wird an eine der Identitätenbasen nach Kapitel 4.1 delegiert. Welcher Satellit, bzw. welche Identitätenbasis für den speziellen Nutzer zuständig ist, kann beispielsweise bei der Anmeldung am Portal anhand seiner

Nutzerkennung entschieden werden. Damit lassen sich Organisationseinheiten, die Anwendungs- oder Basisdienste bereitstellen, aber keine Satelliten sind, völlig von den Satelliten, die evtl. ebenfalls Anwendungs- oder Basisdienste bereitstellen, entkoppeln. Diese Organisationseinheiten können die bestehenden Identitätenbasen nutzen, ohne selbst Eigene aufzubauen.

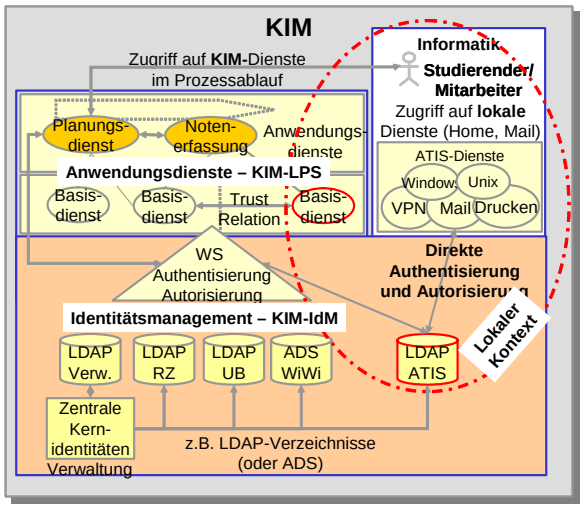

Abbildung 3: Gesamtszenario

Voraussetzung für diese Gesamtarchitektur ist eine Webservice-Schnittstelle, die das Identitätsmanagement bereitstellen muss. Die von einem einzelnen Betreiber bereitgestellten Dienste nutzen hingegen, wie bisher, die lokale Identitätenbasis (lokaler Kontext). Als notwendige Voraussetzung für ein konsistentes Identitätsmanagement über Betreibergrenzen hinweg ist diese lokale Identitätenbasis in die Struktur nach 4.1. eingebunden. Der Aufbau des Identitätsmanagements ist das Ziel des KIM-Teilprojekts KIM-IdM.

5 Zusammenfassung und Ausblick

Anhand der vorgestellten Entwicklungsschritte wurde eine Struktur für die dezentrale Organisation von Identitätenbasen entwickelt. Diese genügt hinsichtlich ihrer Flexibilität (Dienstorientierung, mehrere Betreiber) der Anpassungsfähigkeit sowohl an neue Technologien (SOA) als auch an neue Nutzungsszenarien. Die dezentrale Verwaltung und Bearbeitung, im lokalen Kontext mit einfachen Werkzeugen (3.3.6), bleibt erhalten, dennoch wird eine Gesamtidentität eines Nutzers geschaffen. Ein entsprechendes Gesamtkonzept wurde vorgestellt.

5.1 Ausblick

Im nächsten Schritt sind, auf der hier vorgeschlagenen Struktur zur Verknüpfung von Identitätsbasen, die Managementprozesse für Identitäten zu modellieren. Hierfür sind ein entsprechendes Rollen- und Zugriffskonzept zu entwickeln, sowie Regeln, die eine Automatisierung dieser Prozesse unterstützen.

Literatur

[Ar04] Ph.D. A. Arsanjani,: Service-oriented modeling and architecture; SOA and Web services Center of Excellence, IBM, Nov 2004

[Ca03] Carter G.: LDAP System Administration; O'Reilly, First Edition March 2003 ISBN: 1-56592-491-6

[Ha04] v.d.Hagen P.: Vereinheitlichter Zugang zu IT-Diensten am Beispiel des Informatik-I-Portals; Diplomarbeit, 2004, Cooperation&Management, Prof. Abeck,

[HG05] Hillenbrand, M.; Gotze, J.; Muller, J.; Muller, P.: A single sign-on framework for web-services-based distributed applications; Telecommunications, 2005; ConTEL 2005. Proceedings of the 8th International Conference on Volume 1, June 15-17, 2005 Page(s):273 – 279

[KIM] www.kim.uni-karlsruhe.de, www.kim.uni-karlsruhe.de/288.php

[KER] Kerberos, www.dfn-cert.de/infoserv/dib/dib-2002-02-Kerberos5

[KV04] Koutsonikola, V. Vakali, A.: LDAP: framework, practices, and trends , Aristotelian Univ. of Thessaloniki, Greece Internet Computing, IEEE Publication Date: Sept.-Oct. 2004 Volume: 8 , Issue: 5, page(s): 66 - 72

[LiAl] Liberty Alliance; www.projectliberty.org

[NIS] NIS, www.protocols.com/pbook/sun.htm

[RAD] RADIUS, http://de.wikipedia.org/wiki/RADIUS (Kurzbeschreibung und weiterführende Links)

[RFC2753] RFC 2753, www.faqs.org/rfcs/rfc2753.html

[SAM] Samba, J. Ts, R. Eckstein, D. Collier-Brown: Using Samba; O'Reilly & Associates; 2nd Edition February 2003, ISBN: 0-596-00256-4

[Sp03] Spencer C. L.: An Introduction to Identity Management; SANS Security Essentials Certification Practical Assignment version 1.4b option 1, March 11, 2003

[VPN] VPN, Yuan R., StrayerW. T.: Virtual Private Networks: Technologies and Solutions; Addison-Wesley Professional; 1st edition April 2001, ISBN: 0201702096

[WS-F] WS-Federation; www.ibm.com/developerworks/library/specification/ws-fed

[ZZ04] Zhao G., Zheng D., Chen K.: Design of single sign-on; IEEE International Conference on 2004 Page(s):253 – 256, Digital Object Identifier 10.1109/CEC-EAST.2004.34