Von der Accountverwaltung zum erweiterten Identity Management

Die Einbindung von Services am Beispiel der Integration einer Schließanlage

Tarik Gasmi, Gerhard Schneider, Dirk von Suchodoletz

{tarik.gasmi,gerhard.schneider,dirk.von.suchodoletz}@rz.uni-freiburg.de
Rechenzentrum / Lehrstuhl für Kommunikationssysteme

Abstract: Das Identity Management (IDM) an Hochschulen ist in der Praxis angekommen und muss sich in der Realität bewähren. Hierzu zählt einerseits die Integration von Datenbeständen unterschiedlicher organisatorischer und administrativer Einheiten und andererseits die Offenheit für neue Herausforderungen. Die Universität Freiburg verfolgt ein evolutionäres Modell ihres IDM, welches inzwischen die zentralen Einrichtungen der Universitätsverwaltung, die Bibliothek und das Rechenzentrum umfasst und darüber hinaus Schnittstellen zu weiteren Einrichtungen bietet. Die erarbeiteten Organisationsmodelle und Datenflüsse koordinieren die Aufgaben in den gekoppelten Systemen. Dieser Ansatz erweist sich als robust, um zügig auf neue Anforderungen, wie die Integration einer Schließanlage oder die Anbindung von Shibboleth reagieren zu können. Gerade die in Eigenregie implementierte erweiterbare Self-Service-Komponente macht eine der Stärken des Systems aus. Neue Dienste, wie nun die Zuteilung von Öffnungsberechtigungen, finden die Mitglieder der Hochschule genau an der Stelle, wo sie bereits ihre anderen Daten zu ihrer Person und abonnierten Diensten bearbeiten können.

1 Einleitung

Die Zeiten karteikartenbasierter Studentenverwaltung, papierner Leihscheine und der Dominanz des klassischen Schlüssels sind vorbei. Nach einer Phase paralleler elektronischer Infrastrukturen in Verwaltung, Rechenzentrum und Bibliothek wurde mit der zunehmenden Vernetzung der administrativen Einheiten ein Identity Management (IDM) eingeführt. Dabei lassen sich verschiedene Perioden identifizieren: Ausgang nahm die Entwicklung oft von der Idee der Vereinheitlichung der diversen Systeme und Dienste eines Rechenzentrums. Die Accountverwaltung sollte vereinheitlicht und für den Benutzer transparent werden. Zügig tauchten auf diesem Feld eine Reihe kommerzieller Anbieter auf, die ein umfassend integriertes Identitätsmanagement versprachen. Hinzu kamen etliche, auch öffentlich geförderte Forschungsprojekte, die einige Aufmerksamkeit erregten. Sie reichten von ganzen Verbünden nicht nur administrativer Einheiten einer Hochschule, sondern über verschiedene Einrichtungen hinweg. [vKHJ05], [GB07]

Die anfängliche Euphorie hat sich gelegt, der Pragmatismus kehrte in dem Maße ein, wie der Produktionsbetrieb von IDMs durch die steigende Zahl elektronischer Dienste und

Verwaltungsabläufe zwingender wurde. Vielfach haben sich die evolutionären Schritte[1] gegenüber den revolutionären Sprüngen als durchaus erfolgreiches Modell etabliert. Auch nach sechseinhalb Jahren Produktivbetrieb werden regelmäßig neue Herausforderungen bewältigt. Hierzu zählt die Einbindung der Campus-Online Lernplattform oder die Verwaltung der Abonnements von Mailinglisten.

Dieser Beitrag legt den produktiven Einsatz des Freiburger Universitäts-IDMs dar und zeigt, wie es aufgrund seines Designs durchaus geeignet ist, auch zukünftige Anforderungen ohne große zeitliche Verzögerungen zu erfüllen. Als Beispiel steht deshalb im zweiten Teil die Integration der elektronischen Schließanlage mittels eines sogenannten Konnektors im Mittelpunkt, um typische Herausforderungen zu illustrieren.

2 Identity Management aus Rechenzentrumssicht

Das Rechenzentrum der Universität (RZ) begann 2002 mit der Hilfe externer Consultants den Aufbau eines IDM umzusetzen, welches die vorher vier inkompatiblen Benutzerverwaltungen ablösen sollte. An die hierarchische, replizierte Datenbank, realisiert mit OpenLDAP am RZ, klinken sich die verschiedenen Authentifizierungsdienste und die Benutzerselbstverwaltung ein ([BPvS06]). Das Grundgerüst wuchs im Laufe der Zeit und

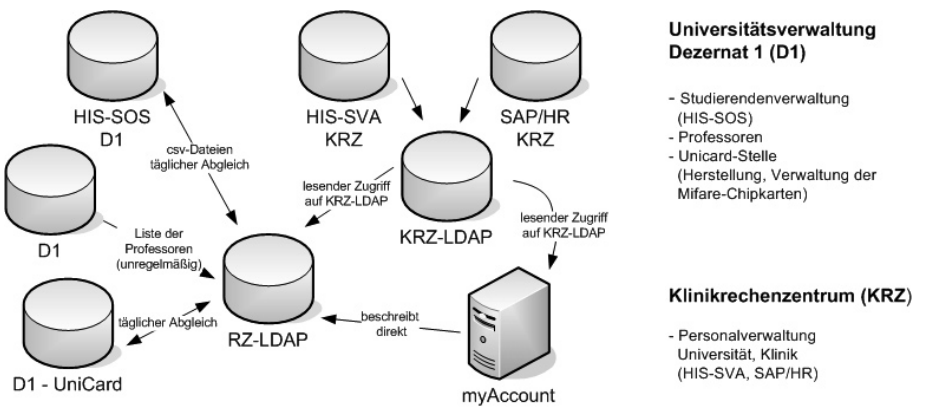

Abbildung 1: Organisatorische Zusammenhänge des IDM an der Universität Freiburg

integrierte bedarfsorientiert weitere Module. Der Start erfolgte mit der campus-weiten Benutzerverwaltung, welche die Mitglieder der Hochschule (im folgenden Uni-Mitglieder), Studierende, Professoren, Mitarbeiter, externe Studierende und Lehrbeauftragte sowie Gast-

[1] Im Gegensatz zu vielen Großprojekten, die nach einer Planungsphase ein möglichst umfassendes IDM typischerweise eines kommerziellen Anbieters einführt, setzt die Universität Freiburg auf eine stufenweise Eigenentwicklung mit offener Standardsoftware, wie OpenLDAP: Zu Beginn wurde lediglich die Account-Verwaltung des Rechenzentrums vereinheitlicht aus den HIS-Daten erzeugt, sukzessive dann weitere Einheiten angebunden. Das erlaubte die Verkürzung der Planung bei sehr schnellem Start in einen Produktivbetrieb.

hörer in ihren verschiedenen Rollen als zentrale Accounts im Benutzerverzeichnis zur Verfügung stellt.

Datenflüsse und Konnektoren Die Daten der Benutzerverwaltung werden nach abgestimmten Prinzipien aus den Quellen des Studierendensekretariats (HIS-SOS) und den Daten des Klinikrechenzentrums, welches die HIS-SVA und SAP/HR Datenbanken verwaltet, bezogen (Abb. 1). Die Datenflüsse erfolgen gerichtet von den genannten Datenquellen der Spitze an darunterliegende Hierarchien. Exporte erfolgen immer nur gefiltert, um Datenschutzbelangen Rechnung zu tragen. Personen lassen sich daher nur in den führenden Datenbanken anlegen oder löschen. Jede Stufe in dieser Hierarchie importiert lediglich die für sie notwendigen Daten. Sie darf aber keine neuen Datensätze erzeugen, die äquivalent zu den importierten sind, jedoch eigene betriebs- und systemwichtige Daten hinzufügen. Organisatorisch wurde so die wichtige Zentralisierung erreicht. Ferner bildet ein Konnektor die Nahtstelle zwischen Benutzer- und Zutrittsverwaltung, in dem er Verwaltungsprozesse beider Einheiten integriert und die notwendigen Mechanismen in einem Modul implementiert. Dieses Modul ließe sich zu einer eigenständigen Administrationsanwendung ausbauen oder von der vorhandenen offenen Plattform *myAccount* verwenden.

Dienste und Benutzerselbstverwaltung Ein wichtiges Moment der Akzeptanz und Effizienzsteigerung ist das Self Service Modul *myAccount*. Es erlaubt die umfassende Account-Verwaltung seitens der Administratoren. Benutzer können selbst Dienste abonnieren, die Organisation ihrer Mailadressen sowie Mailinglisten vornehmen und einen nicht unerheblichen Teil ihrer persönlichen Daten aktualisieren.

Das IDM versorgt die zentralen Dienste des RZ: Mail, WLAN-Zugang, Benutzung der RZ- und etlicher Fakultätsrechnerpools, Nutzung des zentralen Fileservers mit öffentlichem WWW-Bereich, das zentrale CMS und die e-Learning-Plattform. Weiterhin bildet der LDAP die Grundlage für Authentifizierungsprozesse der Universitätsbibliothek wie REDI oder stellt die zentrale ID-Quelle für Shibboleth bereit. Daneben erfolgte die Kopplung mit dem System zur Anmeldung für Lehrveranstaltungen (LSF). Ebenfalls realisieren die meisten Web-Server den authentifizierten Zutritt zu geschützten Bereichen mittels des IDM. In jüngerer Zeit kamen neue Funktionen wie die Abwicklung des Zahlungsverkehrs für die Druckerkonten hinzu, womit die Grundlagen für weitere Dienste wie Shop-Funktionen oder das Inkasso der Semestergebühren geschaffen wurden.

3 IDM Integration der zentralen Zutrittskontrolle

Vor einigen Jahren wurde an der Universität Freiburg ein elektronisches Schließsystem mit dem Ziel der Erweiterung der klassischen Zutrittsmechanismen und der Ablösung der bisher üblichen händischen Schlüsselvergabe eingeführt. Dazu lassen sich die verschiedenen Rollen im IDM perfekt nutzen. Gerade im Zuge der Umsetzung einer 24-Stunden-Universität, welche Mitgliedern auch außerhalb der regulären Öffnungszeiten Zutritt zu Gebäuden und Räumen, wie Fakultätsbibliotheken, Rechnerpools oder Laboren sichern

soll, gewinnt ein funktionierendes IDM zunehmende Bedeutung.

Das campusweit eingesetzte, proprietäre elektronisches Zutrittskontrollsystem beruht auf der kontaktlosen Chipkartentechnik Mifare.[2] Alle registrierten Uni-Mitglieder erhalten mit der *Unicard* als elektronischem Identitätsausweis eine Mifare-Chipkarte mit eindeutiger Kartennummer. Sie wird von einer eigens eingerichteten Abteilung der zentralen Universitätsverwaltung ausgegeben. Die Karte dient einerseits als Studenten- oder Mitarbeiter- sowie als Bibliotheksausweis, wird aber auch als bargeldloses Zahlungsmittel in Mensen und Cafeterien des Studentenwerks, sowie bei Pool-Druckern und Kopiergeräten der Universität eingesetzt.

Alle Türen der Schließanlage verfügen über ein Kartenlesegerät und sind in der Datenbank des zentralen Servers des Zutrittssystems gespeichert. Einzelne Türen lassen sich hier zu Schließgruppen kombinieren und mit Zeitprofilen versehen, die dann bestimmten Kartennummern als Zutrittsprofile zugeordnet werden können. Auf diese Weise erhalten definierte Personen individuelle Zutrittsberechtigungen. Die Kartenlesegeräte fungieren als Clients, die dem Server die eingelesene Kartennummer übermitteln, der auf zugeordnete Profile prüft und bei Erfolg Zutritt gewährt.

Die Verwaltung der Zutrittsberechtigungen, durch das technische Gebäudemanagement der Universität, erfolgte bislang ausschließlich händisch mittels der Administrationssoftware des Systems. Bei einer Zahl von mehr als 30.000 potentiell zu verwaltenden Identitäten mit verschiedensten Zutrittsprofilen ist dies mit einem erheblichem Verwaltungsaufwand verbunden und stellt bei begrenzten Haushaltsmitteln für Personal die Administration vor gewisse Herausforderungen. Zum einen ist der Überblick über alle erteilten Schließberechtigungen zu bewahren. Daneben kommt es, von Fehlern einmal abgesehen, zu zeitlichen Verzögerungen bei Vergabe und Entzug der Zutrittsrechte. Während längere Wartezeiten bis zum Erhalt der beantragten Zugangsrechte sich "nur" auf Nutzerzufriedenheit und die Akzeptanz des Systems auswirken, sind Verzögerungen beim Entzug von Berechtigungen etwa nach Verlust der Karte oder bei Austritt aus der Universität als äußerst sicherheitskritisch einzustufen.

4 Anbindung an das zentrale Benutzerverzeichnis

Für Abhilfe sorgt die Anbindung an das vom RZ betriebene LDAP, da hier alle relevanten Benutzerinformationen zusammenfließen und tagesaktuell vorliegen. Diese werden dazu herangezogen, Vergabe und Entzug von Zutrittsberechtigungen zu automatisieren. Durch direkte Kopplung der Berechtigungen einer Person an Gültigkeit und Status ihres Benutzeraccounts – der eventuell zusätzlich definierte Kriterien erfüllen muss – lassen sich im RZ-LDAP erfolgte Änderungen zeitnah an das Schließsystem weitergeben.

Zu diesem Zweck wurden die LDAP-Benutzer-Accounts um die Datenbestände Karten-

[2] Die Mifare-Technologie, Akronym für Mikron Fare System, wurde 1990 von der Mikron GmbH entwickelt, die seit 1995 Teil von Philips (heute NXP) Semiconductors ist. Standardkarten verfügen über einen Speicher von 1024 Byte und arbeiten heute mittels RFID bei einer Frequenz von 13,56 MHz und einer maximalen Distanz von ca. 10 cm. Das verwendete, geheimgehaltene Sicherheitsmodell erwies sich als nicht sehr robust (*ct 08/08*).

nummer und einer zugehörigen Sperrinformation erweitert. Durch tägliche Synchronisation fließen die entsprechenden aktuellen Daten aus den führenden Datenbanken (Abb. 1). Um Zutrittsberechtigungen automatisiert in das proprietäre Schließsystem (dessen Lizenz-

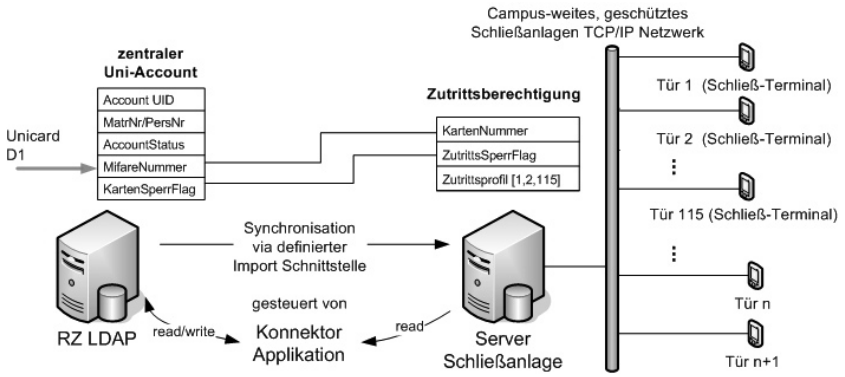

Abbildung 2: Anbindung RZ-LDAP und Schließsystem

bestimmungen den Datenbankzugriff erheblich einschränken) einpflegen zu können, wurde beim Hersteller eine zertifizierte, Batch-basierte Importschnittstelle in Auftrag gegeben. Sie stellt Befehle für folgende Schreiboperationen auf einzelne Zutrittsberechtigungen im Schließsystem bereit:

Initialisierung, *Sperrung*, *Löschen* einer Kartennummer

Zuweisung, *Entzug* von Zutrittsprofilen einer angelegten Kartennummer

Die Steuerung des Imports übernimmt eine eigens implementierte Konnektorapplikation, die geeignete Administrations-Tools bereitstellt. Eine ihrer Aufgaben besteht darin, als LDAP-Client definierte und für die Zutrittskontrolle relevante Änderungen im LDAP zu registrieren. Dies geschieht anhand von Informationen wie Benutzer- oder Kartenstatus. Diese Änderungen setzt sie dann in die jeweils entsprechenden Batch-Befehle um, übergibt sie in Form einer Import-Datei an die Schließanlage und initialisiert den Import.

Integrierte und automatisierte Prozesse In einem ersten Schritt werden vom Konnektor Funktionen bereitgestellt, die eine sofortige, kontrollierte und automatisierte Umsetzung grundlegender IDM Prozesse in die Schließanlage ermöglichen:

- Initialisierung der Kartennummern im Schließsystem neuer Uni-Mitglieder, die beim täglichen Import im LDAP als neue Benutzer-Accounts angelegt werden.
- Umgehende Sperrung im Schließsystem aller Zutrittsberechtigungen von Benutzern, deren Accounts beim täglichen Abgleich nach Exmatrikulation bzw. Vertragsende gesperrt wurden (Account Status: disabled).
- Löschen aller Kartennummern aus dem Zutrittssystem, deren zugeordnete Accounts im LDAP gelöscht werden.

Im nächsten Schritt konnten durch Integration in *myAccount* Teile der Zutrittsverwaltung für einen größeren definierten Personenkreis geöffnet werden. So kann der Benutzer, etwa nach einem Verlust der Unicard, die Sperrung seiner Karte und damit aller Zutrittsberechtigungen selbstständig vornehmen. Desweiteren ist es möglich Benutzern eine Reihe von Standard-Zutrittsprofilen nach dem Prinzip der Freiwilligkeit zur Selbstfreischaltung anzubieten. Die Auswahl an verfügbaren Profilen erfolgt benutzerspezifisch und ist anhand bestimmter im LDAP vorliegender Kriterien festzulegen, wie ID-Rolle (Student, Mitarbeiter, Professor), Zugehörigkeit zu einer bestimmten Einrichtung, Fakultät oder Fachsemester. Beispielsweise kann so allen Studenten einer Fakultät ab einem bestimmten Semester angeboten werden, den 24h-Zutritt zur Fakultätsbibliothek selbst freizuschalten.

Zudem kann über diese Plattform die Verwaltung von Schließberechtigungen an Untereinheiten, Sekretariate einzelner Einrichtungen, delegiert werden, so dass berechtigte Personen zuvor spezifizierte Zutrittsprofile einer definierten Personengruppe verwalten, etwa den Mitgliedern dieser Einrichtung.

5 Fazit

Die firmenunabhängige Implementierung der zentralen Elemente des Freibunger IDMs hat bisher für eine kontinuierliche Entwicklung auf das Ziel einer integrierten Lösung gesorgt. Dieses vereint in sich durchaus sehr verschiedene administrative Einheiten, wie Rektorat mit Dezernaten, Rechenzentrum und Universitätsbibliothek und nahestehende Institutionen, wie das Studentenwerk. Die nicht zu enge Koppelung der Dienste erlaubt zeitnahe Reaktionen auf neue Bedürfnisse, da sie nicht einem Maximalanspruch genügen muss und zumindest die zentralen Komponenten in den Händen der beteiligten Institutionen liegen. Darüber hinaus erleichtert die Benutzerselbstverwaltung die Akzeptanz des Systems, beschleunigt und reduziert personalaufwändige Vorgänge.

Das IDM führt eine ganze Reihe von Verwaltungsvorgängen zusammen. Die Integration der Zugriffskontrolle erleichtert deren Nutzung und entlastet wesentlich von händischen Vorgängen. Die gefundenen Realisierungen sind sicherlich immer noch von den typischen Werbeaussagen kommerzieller IDM-Anbieter entfernt, erweisen sich jedoch als flexibel und robust: Die frisch nachgewiesene Unsicherheit der verwendeten Mifare-Karte bringt das System nicht aus dem Konzept. Da die Kontrolle über die zentralen Module besteht und keine zu enge Verheiratung mit einem Hersteller eingegangen wurde, kann bei Bedarf ein Austausch erfolgen, ohne das restliche System zu gefährden. Dieses gilt ebenso für die Zugriffskontrolle, die nicht zwingend auf die Benutzerverwaltung angewiesen ist, sondern im Bedarfsfall ebenso händisch verwaltet werden kann (nicht Mission-Critical). Aktualisierungen im Gesamtsystem beschränken sich vielfach auf die Adaption der betroffenen Konnektoren.

Kommerzielle, proprietäre Softwarelösungen neigen dazu, auch nach ihrer Beschaffung noch viel Geld zu kosten. So verursachte die Anbindung der e-Learning-Plattform clix und der Siemens Schließanlage nicht unerhebliche Folgekosten für die Erstellung ihrer Konnektoren. Die Zukunft wird zeigen, wie nachhaltig diese investierten Gelder wirken.

Literatur

[BPvS06] B. Buhardt, S. Pioch und D. v. Suchodoletz. Identity Management an der Universität Freiburg in einer Realisierung des Rechenzentrums. *Praxis der Informationsverarbeitung und Kommunikation*, 5(1):54–59, 2006.

[GB07] M. Gaedke und R. Borgeest. Quo vadis Universität 2.0? In *Integriertes Informationsmanagement an Hochschulen*. Universitätsverlag Karlsruhe, 2007.

[vKHJ05] Jan van Knop, Wilhem Haverkamp und Eike Jessen. 19. DFN-Arbeitstagung über Kommunikationsnetze, Düsseldorf. In *Heute schon das Morgen sehen*. Gesellschaft für Informatik, 2005.