

Identity Management – Best Practice

Boris Rohrbacher, Michael L. Schrei

Zentraler Informatikdienst – Abteilung Informationsmanagement
Technische Universität Graz
Steyrergasse 30/I, A-8010 Graz
boris.rohrbacher@TUGraz.at, michael.schrei@TUGraz.at

Zusammenfassung: Mit dem als Informationsmanagement und Identity Management fungierenden System TUGonline steht der Technischen Universität Graz seit Längerem ein mächtiges Werkzeug zur Verfügung, an das bis dato alle bediensteten- und studienrelevanten Systeme angebunden worden sind. Mittlerweile wird TUGonline mit der Produktbezeichnung CAMPUSonline an mehreren Universitäten in Österreich produktiv eingesetzt. Wie im Einzelnen Fremdsysteme vom Identity Management System profitieren und eingebunden wurden, wird in diesem Bericht erörtert.

1 Einführung zu TUGonline

1.1 Informationsmanagementsystem

Mitte der Neunziger Jahre war die Situation des Informationsmanagements in vielen Firmen und Institutionen die von mehreren relativ kleinen Datenbanken, die jeweils Teile des Informationsbedarfes des Unternehmens abdeckten. Die einzelnen Systeme, meist PC-basiert, erfüllten die Anforderungen, waren aber untereinander kaum vernetzt. Dies bedeutete, dass Grunddaten, wie Personen, Organisationen, etc. in jedem System neu erfasst oder für jedes System eigens abgeglichen werden mussten. Ein aufwändiger und fehleranfälliger Prozess. Mit dem Internet wurde in diesen Jahren zudem die Möglichkeit geschaffen, die Daten für viel mehr Anwender als bisher zur Verfügung zu stellen. Auch die TU Graz befand sich in einer solchen Situation. Um die Möglichkeiten des Internets zu nutzen und gleichzeitig Verwaltungsvereinfachung zu erzielen wurde in dieser Situation der Entschluss gefasst, ein neues Gesamtsystem zu erstellen. Es wurde die Vision eines Systems mit folgenden Zielen erstellt:

- Es sollte die Integration aller Daten in einer zentralen Datenbank erfolgen. Dadurch ist kein aufwändiger Abgleich zwischen Datenbanken mehr notwendig.
- Jedes Datenelement sollte nur einmal existieren, keine Duplikate, keine Transfers von Daten. Dies bedingt, dass alle Daten in ein zentrales Datenmodell integriert werden. Die Daten sollen an der verantwortlichen Stelle (Quelle) elektronisch erfasst werden.
- Der Zugang zu den Daten sollte abhängig von den Rechten einzelner Person erfolgen. Damit wird eine Identifizierung bzw. eine Funktionszuordnung ad personam notwendig.
- Die Datenhaltung soll zentral erfolgen, die Datenpflege jedoch soweit möglich dezentral.

Mit dem System sollte der Universität ein Medium zur Verfügung gestellt werden, das auch den Vorgaben im Bereich B2C (Business-to-Consumer) entspricht. B2C definiert unter anderem die Art der Kommunikation zwischen einem Unternehmen und seinen Angehörigen (Mitarbeitern und Kunden). Darunter sind folgende Punkte zu nennen, die im System berücksichtigt werden:

Jede/r Angehörige erhält eine persönliche, aktuelle Sicht auf das Unternehmen bzw. auf seine/ihre Daten

- durch persönliche Identifizierung
- mittels „Single Sign-on“, d. h. der Zugang zu allen Diensten erfolgt durch EINmalige Identifizierung
- zu jeder Zeit
- von jedem Ort (im Web)

1.2 Entwicklung

Mit diesen Vorstellungen wurde das System 1997 beginnend entwickelt und Anfang 1998 in einer ersten Version mit wenig Funktionalität erstmals online gestellt. Die Funktionalitäten wurden rasch erweitert und umfassen heute alle informationsrelevanten Vorgänge der Universität bis auf jene, die durch das SAP System der Module FI/CO und HR abgedeckt werden.

Die nachfolgende Liste gibt einen Überblick über den derzeit bestehenden Funktionsumfang in TUGonline:

- Übersicht über das Lehrveranstaltungsangebot
- Durchführung der Erhebung der Lehre
- Beschreibung laut ECTS
- Terminverwaltung
- Teilnehmerverwaltung
- Prüfungsverwaltung
- Übersicht über Prüfungstermine
- ECTS-Management
- Studienplan-Management
- Kostenberechnung von Studienplänen
- Forschungsaktivitäten und Veröffentlichungen
- Veranstaltungen
- Raumverwaltung
- Inventarverwaltung / Inventarbestandsrechnung
- Personalverwaltung (auch für Drittmittelpersonal, . . .)
- Telefondaten
- Funktionen
- Verteilerlisten (per E-Mail / Postadresse)

- Studienführervorschau/-druck
- Lehrzulage / Kollegiengeld-Abrechnung
- Prüfungstaxenabrechnung
- Bestätigung von Anerkennungsanträgen und von Nachträgen zu Zeugnissen der TUG
- Kommunikation mit an LV teilnehmenden Studierenden (E-Mail, Diskussionsforum)
- Evaluierung: Erstellung von Fragebögen, Durchführung, Freigabe der Ergebnisse
- Nutzung eines persönlichen Terminkalenders, in dem die Termine eigener Lehrveranstaltungen automatisch aufscheinen und durch weitere Termine ergänzt werden können
- Suche nach freien Unterrichtsräumen
- Zugang zur Terminverwaltung von Räumen
- Dokumentation von Forschungsaktivitäten und Veröffentlichungen
- Verwaltung von Diplomarbeiten und Dissertationen
- Verwaltung interner Weiterbildungskurse
- Einsicht in Prüfungsergebnisse
 - vorab am Institut / bestätigt durch Studienabteilung
 - Wahl der automatischen Zustellung per E-Mail
- Diskussionsforum für Lehrveranstaltungen für Lehrende und Studierende
- Nachtrag von Anerkennungen bzw. nicht erfassten Zeugnissen der TUG
- Vorab-Ausdruck eines Studienerfolgsnachweises laut ECTS
- Erstellung eines Studienvertrages (im Rahmen von Erasmus)
- Bearbeitung von Studien- bzw. Heimatadresse
- Ausdruck von Studienbestätigungen
- Erstellung von Studienverlaufsanalysen mittels Datawarehouse

Für die Bereiche Personal, Inventar und Räume stehen außerdem SAP-Schnittstellen zur Verfügung.

TUGonline ist zum datenführenden System für alle Subsysteme geworden. Bereits 1998 wurden Anfragen von anderen Universitäten für die Übernahme des Systems gestellt. 2001 wurde TUGonline von CSC Plönzke im Rahmen einer Ausschreibung für Universitätsinformationssysteme für Kunstuniversitäten evaluiert und auf Platz eins gereiht. In der Folge wurde 2002 eine Reviewphase begonnen mit dem Ziel das Produkt CAMPUSonline zu erstellen. Dieses wurde bis Ostern 2004 erstellt und ist aktuell an fünf österreichischen Universitäten im produktiven Einsatz.

1.3 Technologie

TUGonline basiert auf einer Datenbank der Firma ORACLE. Um den Web-Zugang zu ermöglichen, wird – neben dem Datenbankrechner – ein Webserver eingesetzt, der die Schnittstelle zwischen den Web-Anwendern und der Datenbank darstellt. Weiter wird für die Ausführung von FORM- bzw. REPORT-Programmen ein eigener FORMS/REPORT-Server verwendet.

In TUGonline gibt es grundsätzlich drei Arten von Anwendungen, die abhängig vom Zugang der Anwender zum System sind:

- WEB-Anwendungen

Diese Programme sind für den Web-Zugang gebaut und verwenden folgende Programmiertechnologien:

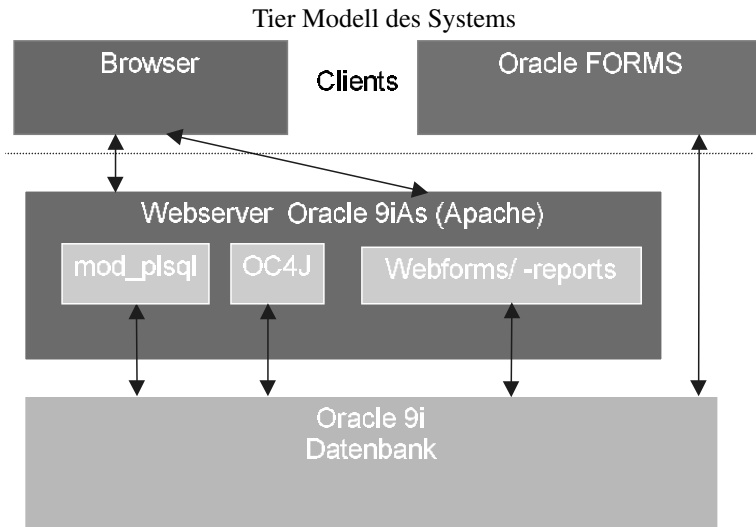
- die Programmiersprache PL/SQL als Schnittstelle zur Datenbank
- HTML und JavaScript als Schnittstelle zur Anwenderin

- FORMS-Anwendungen

Diese Programme werden primär für Fachabteilungen der zentralen Verwaltung erstellt und erlauben eine komplexere Programmlogik, sowie den direkten Zugang zur Datenbank. Die FORMS-Technologie hat den weiteren Vorteil, dass auch die Programmierung effizienter erfolgen kann als mit Web-Werkzeugen (PL/SQL, HTML bzw. JavaScript). Programme in FORMS-Technologie können – wenn sie an vielen Stellen verwendet werden – unter Verwendung eines speziellen Zusatzprogrammes (PlugIn) auch in einem Webbrowser ausgeführt werden (z. B. die Prüfungsverwaltung an den Instituten).

- REPORT-Anwendungen

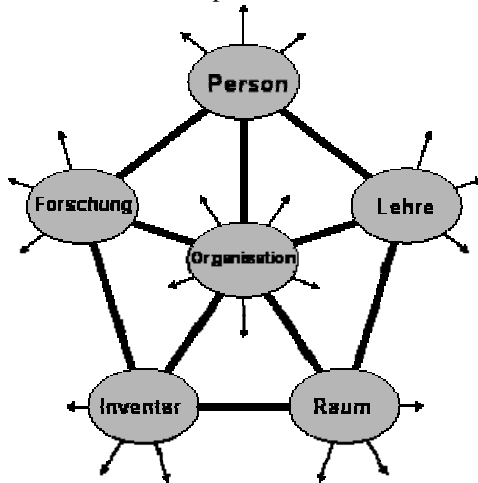
Diese Anwendungen erlauben die Erstellung von Listen oder Formularen, die als druckbare PDF-Files dem Anwender zur Verfügung gestellt werden. Ein typisches Beispiel ist die Erstellung von Beauftragungs- bzw. Betrauungsschreiben für Vortragende. REPORT-Programme werden sowohl von WEB- als auch von FORMS-Anwendungen aufgerufen.



1.4 Datenmodell

Das Datenmodell wurde im Rahmen der Entwicklung von TUGonline völlig neu erstellt. Es besteht grundsätzlich aus sechs Teilmodellen, welche die Daten zu den Basisressourcen der Universität beinhalten, sowie den Verbindungen zwischen diesen (siehe nachfolgende Grafik).

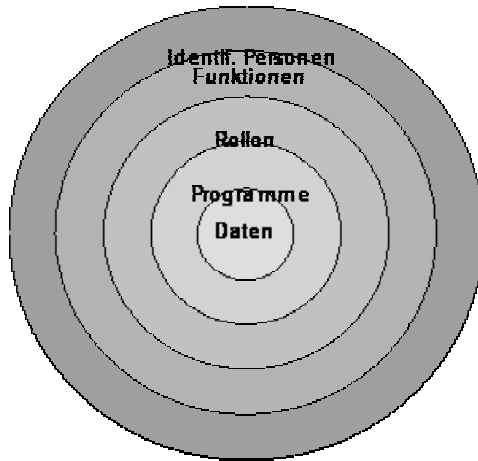
Das Modell beinhaltet derzeit etwa 600 Tabellen und wird nach Bedarf erweitert. Das Wissen über das Modell eröffnet die Möglichkeit, sehr flexibel und rasch auf neue Anforderungen oder Änderungswünsche zu reagieren. Die Abbildung stellt die wichtigsten Entitäten des Datenmodell symbolisch dar, die kleinen Pfeile verdeutlichen die Lookups und vielen Hilfstabellen, die um eine Hauptentität herum notwendig sind.



1.5 1.5 Funktionsmodell

Das Funktionsmodell besteht auf fünf ineinander geschachtelten Bereichen (siehe nachfolgende Grafik)

- Daten bezeichnen alle Tabellen und Relationen zwischen diesen.
- Programme sind Anwendungen, diese erlauben den Zugriff auf die Daten.
- Rollen geben an, unter welchen Bedingungen ein Programm benutzt werden kann (z. B. nur lesend, schreibend, . . .). Jedes Programm besitzt seine eigenen Rollen.
- Funktionen stellen die Schnittstelle zwischen den Rollen eines Programms und einer identifizierten Person dar. Die Relationen zwischen Funktionen und Rollen bzw. Funktionen und Personen sind vom Typ M:N (viele zu viele). Dies erlaubt ein Maximum an Flexibilität in der Festlegung sowie Zuordnung von Funktionen. Funktionen werden immer bezüglich einer bestimmten Einrichtung der Universität vergeben und wirken damit implizit (Funktion → Rolle → Programm → Daten) auf die Daten dieser Einrichtung
- Identifizierte Personen sind physische Personen, die dem System durch Identifizierung mit Benutzername/Kennwort bekannt sind. Grundsätzlich hat jede/r Angehörige/r der TU Graz (Studierende und Bedienstete) das Recht auf den Zugang.



Zwei Aktivitäten erfordern im laufenden Betrieb einen besonderen Aufwand und wurden daher im Sinne der Verantwortlichkeit und der operativen Durchführung auf die einzelnen Einrichtungen ausgelagert:

- Die Vergabe von PIN-Codes
PIN-Codes sind einmal verwendbare „Tickets“, die einer Person erlauben, sich für TUGonline einen Benutzernamen bzw. ein Kennwort zu wählen. PIN-Codes werden in der Regel an neue Personen einer Einrichtung vergeben, um ihnen den Zugang zu TUGonline zu erlauben, oder an Person, die ihr Kennwort vergessen haben.
- Die Zuordnung von Funktionen zu Personen

Verantwortlich für beide Aktionen ist in jedem Fall der Leiter/die Leiterin der jeweiligen Einrichtung. Die operative Durchführung beider Aktionen ist jenen Personen vorbehalten, die eine spezielle Funktion (TUGonline-Beauftragte/r) bezüglich der Einrichtung besitzen.

2 Überblick über die Systemlandschaft

An der TU Graz sind derzeit etwa 9.000 Studierende aktiv gemeldet. Die Zahl der Bediensteten beläuft sich auf zirka 2.000. Diese Zahl an Personen entspricht in Österreich einem mittelständischen bis größeren Betrieb. Für die Betreuung der gesamten IT-Landschaft der TU Graz zeichnet der Zentrale Informatikdienst (ZID) verantwortlich – dieser entspricht in Deutschland dem „Rechenzentrum“.

Das an der TU Graz eingesetzte Produkt CAMPUSonline (die für die TU Graz angepasste Instanz wird TUGonline genannt) wird als zentrales Informationsmanagement- und Identity Management System eingesetzt. Es sollte jedoch angemerkt werden, dass ab dem nächsten Kalenderjahr die Personaldaten (nur Bedienstete) aus einem SAP HR System stammen und SAP somit personaldatenführendes System wird!

Die Systemlandschaft an der TU Graz – siehe dazu Abbildung 1 – umschreibt folgende Dienste (es werden nur die für den allgemeinen Betrieb relevanten Dienste angeführt, da das Aufzählen und Beschreiben ansonsten den Rahmen sprengen würde). In einem späteren Kapitel wird genauer auf die Integration im Identity Management System eingegangen.

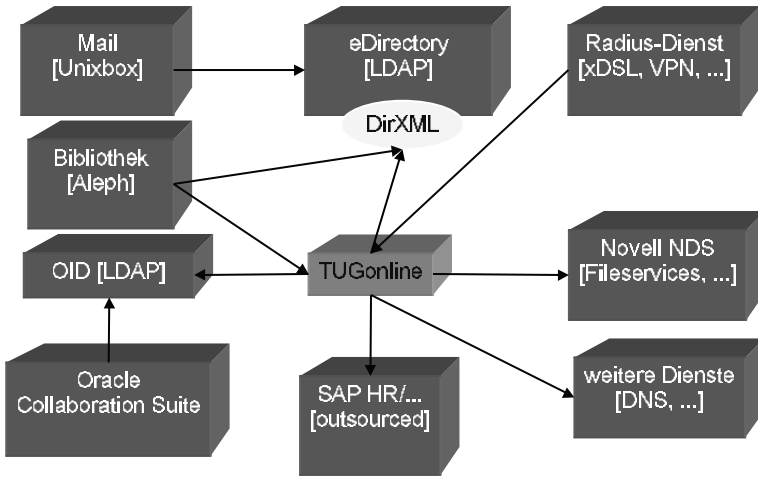


Abbildung 1: Die Systemlandschaft an der TU Graz

2.1 eDirectory

Das aus dem Hause Novell stammende Metaverzeichnis ist LDAP v3 konform und wird im Loadbalancing Betrieb mittels Content-Switch betrieben (insgesamt drei Replicas). Aus Sicherheitsgründen steht dieser Dienst nur im TU Graz internen Netzwerk zur Verfügung. Der etwa 21.000 Benutzerobjekte enthaltende Verzeichnisdienst erhält die Daten vom TUGonline per one-way-propagation. In unserem Fall setzen wir auf das Produkt DirXML, das eine asynchrone Übertragung mit Fehlerbehandlung zulässt.

2.2 Mail

An der TU Graz kommt ein auf OpenSource basierendes Unix-Mailsystem zum Einsatz, das ebenso per Web erreichbar ist. Die Webmail Komponente ist im TUGonline direkt per Link aufrufbar, d. h. per Single Sign-on angebunden (in der persönlichen Visitenkarte einer Person). Das Mailsystem unterstützt Black- und Greylisting und der SMTP Server ist von außerhalb des TU Graz Netzes nur authentisiert verwendbar.

2.3 Bibliothek

Als Bibliothekssoftware kommt Aleph von der israelischen Firma ExLibris zum Einsatz, wobei zusätzlich rund 4.000 registrierte externe Personen im Metaverzeichnis (eDirectory) gespeichert werden. Dies geschieht derzeit indirekt über einen Datenbanklink im TUGonline, da die Aleph Datenbank in dieser Version (Oracle 8) noch mit keiner LDAP Unterstützung aufwarten kann.

2.4 Groupware

An der TU Graz wird als Groupware/Collaborationssoftware die Oracle Collaboration Suite (kurz OCS) eingesetzt, wobei die Kalender Applikation allen Bediensteten zur Verfügung

steht. Es besteht auch die Möglichkeit, die Termine mit dem persönlichen Terminkalender vom TUGonline mittels Webservices abzugleichen, i. e. Prüfungs-, Lehrveranstaltungs- und Veranstaltungstermine.

2.5 Novell Netware

Als zentrale und teils auch dezentrale File- und Druckservices (Studierende und Bedienstete) kommt die Novell Netware in verschiedenen Versionen zum Einsatz. Es bestehen zur Zeit rund 50 Bereichsserver, d. h. eigene Novell Server an den Instituten, ergo sind auch unterschiedliche Versionen aktiv. Der Studierendenabgleich erfolgt mittels selbst entwickeltem JANUS (Java Acquired Novell USer) zwischen NDS (so wird das Metaverzeichnis der Novell Netware bezeichnet) und TUGonline – in Zukunft soll dies durch DirXML abgelöst werden. Es besteht kein Bedienstetenabgleich, die Begründung ist darin zu finden, dass die an den Instituten verteilten Server großteils eigene Strukturen besitzen und somit einen einheitlichen Abgleich quasi unmöglich machen!

2.6 Radius

Dieser Dienst greift direkt auf die Datenbank vom TUGonline zu und authentisiert resp. autorisiert folgende Dienste:

- VPN Zugang (verschiedene Berechtigungsgruppen)
- xDSL Zugang für Angehörige der TU Graz (Studierende und Bedienstete), wobei dies per PPPoE und CHAP erfolgt
- VC Graz (Virtueller Campus Graz); dieser besitzt eine eigene Benutzerverwaltung, einfach aus dem Grund, da mehrere Universitäten involviert sind!
- Transparentes PPPoE für die EDV-Lernzentren
- WLAN Zugriff (VPN)

Zudem steht – im TUGonline pro Dienst definierbar – ein Quotamanagement mit Hard- und Softlimits zur Verfügung. Somit ist der Radius ein AAA Dienst, der aber nicht lokal, sondern im TUGonline die Daten ablegt bzw. abfragt.

2.7 Webservices

Webservices werden an der TU Graz derzeit zur einfachen Datenbereitstellung für weitere Dienste verwendet, die entweder nicht direkt auf die Datenbank zugreifen können oder kein LDAP Protokoll verstehen. Für die Telefonanlage werden die Displaybezeichnung und zugehörige Nebenstelle(n) an den Verwaltungsrechner der Telefonanlage übertragen. Dynamische Mailinglisten, die zwar im TUGonline zur Verfügung stehen, aber nicht ohne Interaktion abrufbar sind, werden ebenfalls per Webservice angeboten. Ein weiterer kleiner Dienst ist das TUGtoday – das auf den Informationsterminals im Campusbereich läuft und u. a. aktuelle Veranstaltungen bewirbt. In der Betaphase befindet sich gerade der schon erwähnte Kalenderdatenabgleich mit der Groupware (Oracle Collaboration Suite), wobei hier die Performance noch ein Problem darstellt.

2.8 Weitere Dienste

In diese Kategorie fallen Dienste wie das Internetportal mit integriertem Content Management System (CMS), das die Benutzerdaten ebenfalls aus dem TUGonline bezieht – zusätzlich auch Rollen und Funktionen, die im TUGonline abgebildet werden. Als webbasiertes Datawarehouse Tool wird in Zukunft der Oracle Discoverer zum Einsatz kommen, der ebenso wie das Internetportal auf ein bestehendes Benutzermanagement zurückgreift – hierfür wird die selbe Infrastruktur wie im Internetportal verwendet werden.

Erwähnenswert sind noch die diversen SAP Schnittstellen zum Bundesrechenzentrum. Dort werden fast österreichweit die SAP Instanzen für Universitäten gehostet.

An der TU Graz wird seit geraumer Zeit darauf geachtet, sich möglichst an (Protokoll)-Standards zu halten und keine proprietären Schnittstellen zu schaffen. Aus historischen Gründen, d. h. applikatorisch bedingter Einsatz von älterer – zu neuen Standards inkompatibler – Software, ist es nicht einfach und manchmal unumgänglich, eigene Schnittstellen zu schaffen. Der Schritt, das an der TU Graz entwickelte System TUGonline als Produkt CAMPUSonline auch an andere Universitäten zu verkaufen, hat immens geholfen, dieses Vorhaben möglichst effizient umzusetzen!

3 Identity Management an der TU Graz

Im vorhergehenden Kapitel ist die Systemlandschaft im Allgemeinen etwas näher erläutert worden. Detaillierter wird dies im Folgenden geschehen, wobei besonderes Augenmerk nicht auf die technische Umsetzung, sondern etwaige Probleme und Hintergründe gelegt wird!

3.1 TUGonline

Das Informationsmanagement- und Identity Management System bildet den kompletten Identity Lifecycle ab, beginnend vom Accountanmeldeverfahren bis hin zum Accountbeendigungsverfahren! Darüber hinaus besteht die Möglichkeit, zentral Benutzer umbenennen (z. B. nach Heirat), die dann auch in den angebundenen Fremdsystemen automatisch umbenannt werden. Außerdem wird die Organisationsstruktur an der TU Graz abgebildet.

TUGonline bietet einen vollwertigen AAA Dienst und diverse standardisierte Schnittstellen zu anderen Systemen.

3.2 Aufbau des zentralen Metadirectories (Novell eDirectory)

Es wird auf eine möglichst einfache Struktur gebaut, die aus getrennten Containern besteht. Ein Container ist eine Organizational Unit (OU), die Benutzerobjekte beinhaltet, die wiederum Attribute besitzen.

An der TU Graz sind zur Zeit drei solcher Container im Einsatz: einer für alle Angehörigen – sprich Studierende und Bedienstete – der zugleich Fremddiensten zur Authentisierung und Autorisierung dient. Ein weiterer Container beinhaltet nur die Bediensteten

der Universität, wobei dieser ausschließlich für Suchdienste und als Adressbuch verwendet wird, da nur ein Bruchteil der Attribute zu den Benutzerobjekten gespeichert sind! Last but not least existiert ein Container für externe Personen, der derzeit nur für die Bibliothek zum Einsatz kommt und etwa 4.000 externe Personen beherbergt. Das Berechtigungsmodell sieht generelle Zugangsberechtigungen pro Container vor, denn die Benutzerberechtigungen werden in den zugehörigen Attributen abgelegt. Wie im Überblick schon kurz erwähnt ist der LDAP Dienst nur im internen Netz der TU Graz erreichbar. Das hauptsächlich aus sicherheitstechnischen Überlegungen. Wenn der Bedarf besteht, von zuhause aus das Metaverzeichnis als Adressbuch zu verwenden, stellt dies trotz dessen kein Problem dar, da die Möglichkeit besteht, per VPN Zugang eine interne Adresse aus dem Adresspool der TU Graz zugewiesen zu bekommen.

Um die Frage zu beantworten, wieso sich die TU Graz gerade für das Novell eDirectory als Metaverzeichnis entschieden hat: Das war eine rein historische Entscheidung (kurzer Exkurs: Zum Zeitpunkt des Aufbaus des zentralen LDAP Verzeichnisses war die Überlegung da, SAP lokal auf der TU Graz zu hosten, damit wäre ein für SAP zertifizierter Verzeichnisdienst notwendig gewesen – und zu dieser Zeit war das eDirectory der einzige für uns in Frage kommende, der zudem zertifiziert war!)

Wie werden die Daten zwischen dem zentralen Identity Management System TUGonline und dem eDirectory ausgetauscht? Um eine gewisse Unabhängigkeit der beiden Systeme zu gewährleisten, haben wir uns für eine asynchrone Schnittstelle entschieden, wobei von Seiten Novells ein fertiges Produkt existiert: DirXML (hat mittlerweile eine Namensänderung erfahren. . .). DirXML greift per JDBC Schnittstelle direkt auf eine vordefinierte Eventlog-Tabelle auf der Datenbank zu, in der zeilenweise Einträge abgearbeitet werden.

Welche Abhängigkeiten ergeben sich nun, wenn einer der beiden Dienste nicht verfügbar sein sollte?

Wenn das Metaverzeichnis offline gehen sollte, wird das Eventlog (die Tabelle) weiterhin befüllt, denn Änderungen den Benutzer entsprechend (Kennwort, Telefonnummer, Mailadresse etc.) können nur am datenführenden System – ergo im TUGonline vollzogen werden! Was passiert aber, falls das eDirectory „crashen“ sollte, i. e. ein vollständiges Versagen der Maschine? Zunächst ist dies äußerst unwahrscheinlich, da der Verzeichnisdienst aus mehreren unabhängigen Replicas besteht, die über einen Content-Switch (entspricht einem „intelligenten“ Loadbalancer) erreicht werden. Aber falls dieser Fall doch eintreten sollte, kann, von einer leeren Struktur am Metaverzeichnis ausgehend, das eDirectory jederzeit wieder befüllt werden, da sich alle aktuellen Daten jederzeit im TUGonline befinden. An dieser Stelle sei noch erwähnt, dass die Zeitspanne, alle Daten wiederherzustellen recht lange dauern kann! Auf der anderen Seite muss abgeklärt werden, welche Folgeerscheinungen auftreten, wenn das datenführende System TUGonline nicht erreichbar sein sollte. In diesem Fall können keine Benutzerdaten modifiziert werden, somit sind auch keine Daten zu propagieren. Im Falle eines Desasters am Datenbankrechner vom TUGonline, könnten Daten im schlimmsten Falle verloren gehen, wenn erstens die Eventlog-Tabelle nicht mehr hergestellt werden könnte und zweitens sich darin überhaupt Datensätze befunden haben. Diese Tabelle ist quasi immer leer, da die Änderungen im Normalfall unverzüglich ins eDirectory übernommen werden (getriggert!). Abhilfen für diesen Fall könnten natürlich auch über eine Standby Datenbank führen.

Kurz möchte ich noch die Vor- bzw. Nachteile vom eDirectory beschreiben: Mit DirXML steht ein mächtiges Tool zur Verfügung, das auch diverseste Schnittstellen für kommerzielle Anwendungen wie zum Beispiel SAP zur Verfügung stellt. eDirectory ist auf so gut wie allen Plattformen erhältlich und einfach zu administrieren (Reparieren, Backup und Replicas gehen einfach von der Hand). Einen Nachteil, den man sich mit dem Einsatz von DirXML erkaufte ist die Abhängigkeit zum eDirectory, was ja nicht unbedingt ein Nachteil sein muss, wenn da nicht die Sache mit dem ‚userpassword‘ wäre. Bis dato (Version 8.7.3.x) ist dieses Attribut case-insensitiv, wird aber ab der nächsten Version implementiert sein (in Version 8.8 als Security Feature angekündigt). Diese „kleine“ Unannehmlichkeit hat bewirkt, dass wir unsere Password-Policy umstellen mussten – mehr dazu noch später.

3.3 Ein weiteres Metadirectory

Wenn Sie nun die Überschrift lesen, werden Sie sich zweifelsohne fragen, wozu denn parallel zum zentralen eDirectory noch ein weiteres benötigt wird. Eine durchaus berechtigte Frage, deren Beantwortung aber trivial erscheint! Resultierend aus den Abhängigkeiten der verwendeten Produkte konnte die Groupwarelösung von der Firma Oracle (Oracle Collaboration Suite) in der damals installierten Version (9.0.4.1) nicht ausreichend mit dem eDirectory zusammenspielen. Mittlerweile bieten die meisten Hersteller Adapter resp. Schnittstellen an, um bidirektionalen Datenaustausch zwischen LDAP-Verzeichnissen zu gewährleisten. Somit war es notwendig, den eigens von Oracle mitgelieferten LDAP-Dienst „Oracle Internet Directory“ (OID) zu verwenden. Es sei auch erwähnt, dass selbst heute noch ein OID mandatory ist, von diesem können dann zwar Daten auf weitere Third-Party LDAP-Verzeichnisse propagiert werden – auch nicht immer bidirektional – aber um den OID kommt man nicht herum (ich bezeichne dies gerne als Produktbindung, was wohl vielen größeren Softwareherstellern gemein ist).

Das weitere Metadirectory ist ein Oracle Internet Directory (OID), das ebenfalls LDAP v3 konform ist und einen für uns gewichtigen Vorteil mit sich bringt, nämlich die Unterstützung aller Oracle-Applikationen. Auch das Single Sign-on, das bei vielen Oracle Produkten standardmäßig dabei ist, baut darauf auf!

Die Erfahrung, die wir zu Metadirectories in der Praxis erlangt haben, zeigt, dass Berechtigungsprobleme auftauchen können, wenn mehrere Dienste auf eine Struktur zugreifen (außer bei read-only, wie bei uns umgesetzt). Des Weiteren werden Attribute von verschiedenen Applikationen oft unterschiedlich gedeutet (e. g. cn, displayName, uid). Das kann zu einem Problem führen, wenn kein anwendungsspezifisches Mapping der Attribute möglich ist. Hier sei beispielhalber Mozilla erwähnt, bei dem cn=displayName ist, d. h. anstatt den Namen (displayName) anzuzeigen wird der Username (cn) angezeigt! Um dem Schlamassel, entstanden durch inflexible Applikationen, zu entfliehen, kommt man um Redundanzen nicht umhin. Die selben Benutzerdaten werden nochmals mit anderen Attributbezeichnungen am Metadirectory abgelegt.

Was haben wir daraus gelernt? LDAP ist gleich LDAP, aber Applikationen setzen teilweise andere Strukturen voraus. Während am Oracle Internet Directory das Gruppenprinzip für das Berechtigungsmodell zum Einsatz kommt (für Oracle Applikationen), wird im eDirectory die Autorisierung von uns per Attributzuweisung geregelt. Es ist nicht einfach,

mehrere LDAP-Verzeichnisse zu konsolidieren, vor allem nicht, ohne Daten redundant zu halten!

Ein weiterer Punkt ist die Entscheidung, ob man Profiles oder Accounts einsetzt. Eine Person kann derzeit im Besitz mehrerer Accounts sein (Studierende und Bedienstete, in Zukunft auch Alumni), was natürlich dazu führt, dass sich diese Person mehrere Benutzernamen und Kennwörter merken muss. Abhilfe schafft hier das „Profile“, das eine Person nach außen hin mit nur einem Account aufscheinen lässt. Ganz unproblematisch ist dies natürlich nicht, denn wie geht man mit Applikationen um, die nur Benutzername und Kennwort abfragen, ergo keine Trennung zwischen Profilen ermöglichen. Ist man dann als Studierender oder Bediensteter autorisiert?

3.4 Mailing

Der Mailingdienst fragt auf das eDirectory ab und führt nicht nur eine Authentisierung, sondern auch Autorisierung durch. Dafür gibt es Benutzerobjekt-Attribute, die definieren, ob die Person überhaupt den Dienst verwenden darf. Weiter wird unterschieden, ob ein Studierender oder Bediensteter den Dienst verwenden möchte, denn dementsprechend gibt es weitere benutzertypspezifische Attribute. E. g. ist der Alias-Name bei Studierenden bereits aus dem ‚username‘ ersichtlich, wobei dieser bei Bediensteten erst aus einem eigenen Attribut ausgelesen werden muss!

An manchen Instituten sind so genannte Bereichsserver im Einsatz. Die auf diesen Servern verwendeten Mail-Adressen müssen im TUGonline erfasst werden, damit die betroffenen Personen überhaupt E-Mails empfangen können (Posteingang für die Domäne der TU Graz ist nämlich ein zentrales Mailgate, das überprüft, ob eine eingehende E-Mail überhaupt zugestellt werden kann oder soll). Dadurch wird sichergestellt, dass nur E-Mails mit gültiger Adresse auf die Institutsmailserver und den zentralen Mailserver weitergeleitet werden und diese nicht selbst noch filtern müssen. . .

3.5 Radius

Über den Radius Dienst laufen sämtliche Netzwerkverbindungen, die einerseits von außen kommen aber auch interne, die z. B. eine VPN Verbindung in ein sicheres Netzwerksegment aufbauen wollen.

Dieser Dienst greift nicht auf das zentrale Metadirectory sondern direkt auf die Datenbank vom TUGonline zu! Per SQL Statement wird authentisiert, autorisiert (Gruppenzuordnung) und auch das Accounting (Quotadaten pro Session und Dienst) abgewickelt. Wieso erfolgt der Zugriff nicht auf das Metadirectory? Hinter den Accounting-Informationen stecken Berechnungen (Quota pro Dienst), die im eDirectory nicht durchführbar sind. In einer Oracle Datenbank besitzt man wesentlich bessere Hilfsmittel, um die Sessiondaten, die vom Radius kommen, pro Monat für jeden Dienst einzeln zu berechnen. Zudem geschieht eine Limitierung per Soft- und Hardlimit, die derzeit pro Dienst im TUGonline definierbar ist. Ein weiterer wichtiger Grund ist die Einhaltung unserer Strategie, die darauf aufgebaut ist, Dienste auf das eDirectory nur lesend zugreifen zu lassen. Das datenführende System ist TUGonline! Andernfalls würden wir uns mit Abhängigkeiten auseinandersetzen

müssen, die das einfache, aber sichere Konzept zu Fall bringen würden (Stichwort: Bidirektionaler Abgleich mit dem eDirectory).

3.6 Novell Netware

Die Benutzerdaten unserer File- und Druckservices werden nur teilweise mit TUGonline abgeglichen – im speziellen nur von Studierenden. Die Anbindung an das TUGonline erfolgt mittels selbst entwickeltem JANUS (Java Acquired Novell User), soll aber zukünftig von DirXML abgelöst werden.

Bedienstetendaten werden nicht synchronisiert, weil wie eingangs erwähnt erstens die Daten auf viele Bereichsserver verteilt sind und zweitens die Organisationsstruktur nicht der vom TUGonline entspricht. Ergo würde daraus eine komplizierte Mappingstruktur resultieren.

3.7 Bibliothek

Die Bibliothek setzt Aleph ein, derzeit noch in einer etwas älteren Version und gleicht die Daten indirekt über das eDirectory ab. Indirekt deshalb, weil zwar das DirXML seitens des Metaverzeichnisses direkt auf die Eventlog-Tabelle der Bibliotheksdatenbank zugreift – hier kommt dasselbe Verfahren wie im TUGonline zur Anwendung, aber andererseits kennt die auf Oracle 8 basierende Version von Aleph keine LDAP-Unterstützung. So waren wir gezwungen, indirekt über eine Verbindung zwischen Bibliotheksdatenbank und TUGonline auf die Benutzerdaten im Metaverzeichnis zuzugreifen. Da es nicht nur Bediensteten und Studierenden gestattet ist, den Bibliotheksdienst zu nutzen, gibt es einen Container eigens für die Bibliothek am eDirectory, der zur Zeit an die 4.000 externe Benutzer beherbergt. Sobald die neue Version von Aleph ab Sommer im Einsatz ist, kann diese etwas komplizierte Verfahrensweise vereinfacht werden und LDAP-Aufrufe direkt von der Bibliotheksdatenbank abgesetzt werden.

3.8 SAP

Bis dato werden die Personaldaten im TUGonline erfasst. Ab dem nächsten Kalenderjahr wird sich diesbezüglich jedoch einiges ändern, da dann die Personendaten im uni.pers (SAP HR Instanz) von der Personalabteilung eingepflegt werden. Insbesondere umfasst dies die Stammdatenerfassung und Organisationszuordnung. Derzeit läuft das parallel zur Datenpflege im TUGonline, da wir in unserem System eine tiefere Organisationsstruktur abbilden, die natürlich nicht hundertprozentig der vom SAP entspricht. Um später die exakten Unterordnungen (i. e. Unterabteilungen) auch noch im TUGonline zu sehen, müssen diese manuell nachgebessert werden. Hinzu kommt noch, dass Beamte nicht Bestandteil vom uni.pers, sondern einer eigenen SAP HR Instanz, namens PM SAP, sind. Bis dato werden Beamte im PIS (Personalinformationssystem) gewartet und kommen ab 2006 in vorher erwähntes PM SAP, das der Vollständigkeit halber erwähnt alle Bundesbeamten Österreichs beherbergt. Somit ergibt sich ab 2006 dieses Szenario: Es existieren zwei SAP HR Systeme, zudem mit unterschiedlichen Mandanten, wobei vom PM SAP täglich die Beamtendaten in das uni.pers exportiert werden. Vom uni.pers ausgehend werden dann

die kumulierten Personaldaten der TU Graz in das TUGonline importiert. Eine recht komplizierte Angelegenheit.

Kleiner Exkurs: Die Bedienstetendaten werden von der Personalabteilung eingepflegt, aber woher stammen die Studierendendaten?

Bei der Ersteinschreibung, auch Immatrikulation genannt, können Studierende sich per Web zunächst voranmelden, was der Stammdatenerfassung entspricht. Im Laufe des Studiums erfolgt die Weitermeldung (Inskription) per Zahlschein. Sobald bestätigt worden ist, dass der Studienbeitrag mittels Zahlschein termingerecht eingezahlt worden ist, erfolgt automatisch die Accountverlängerung, d. h. sämtliche Dienste stehen dem Studierenden weiterhin zur Verfügung. Im Falle einer Beendigung des Studiums oder falls nicht termingerecht eingezahlt wurde, wird zu einem Stichtag der Status des Accounts entsprechend gesetzt (es gibt sehr wohl eine Übergangsfrist).

3.9 Weitere Dienste

Noch erwähnenswert ist die Anbindung etwas kleinerer aber keineswegs unbedeutender Dienste an das Identity Management vom TUGonline. Die Telefonanlage wird im TUGonline gewartet und die Daten – Displaytext und Nebenstelle(n) – werden per Webservice auf den Verwaltungsrechner der Telefonanlage propagiert. Im TUGonline werden IP Adressen, Mac-Adressen, Hostnamen und Aliases eingetragen und an den/die Nameserver als „Plaintextfile“ übertragen. Dies wird in naher Zukunft auf Webservices umgestellt. Das gerade im Aufbau begriffene Internetportal <http://www.tugraz.at/> wird ebenso baldigst auf ein Content Management System umgestellt, das die Benutzerdaten, Funktionen und Rollen zwar aus einem Oracle Internet Directory (OID) bezieht, diese stammen aber aus dem TUGonline. Projektiert ist ebenso die Verwendung des Produktes Oracle Discoverer, das ein Datawarehouse Tool darstellt und dem ebenso benutzerspezifische Berechtigungen zugrunde liegen – wie im Internetportal.

3.10 Allgemeines

Ein funktionierender Identity Lifecycle bedingt auch die Reservierung von Benutzernamen und Accounts. Dies kommt dann zum Tragen, wenn sich Studierende beurlauben lassen. Dabei wird nur der Account inaktiv gesetzt. Nach Beendigung eines Accounts bleibt für eine definierte Zeitspanne der Benutzername ebenso reserviert. Das hat unter anderem den Grund, damit ein potentieller Account-Nachfolger – sprich jemand mit dem selben Benutzernamen – nicht die E-Mails die für seinen Vorgänger bestimmt waren zugestellt bekommt. Des weiteren ist es notwendig, für spezielle Dienste Benutzernamen sperren zu lassen, e. g. webmaster, ldap, admin, root. Dies geschieht prophylaktisch aus dem Grund, damit nicht jemand reservierte Accounts verwenden kann. Zu bedenken bleibt die Verwendung von unterschiedlichen Benutzernamen pro Benutzer-Typ. Im Speziellen kann jemand Studierender, Bediensteter oder Alumni sein, was bei einer großen Anzahl an Benutzern schnell zu einer Ressourcenknappheit führen kann.

Bei einem Identity Management System spielt eine übergeordnete Password Policy eine große Rolle. Wichtig ist, dass Kennwörter nur im TUGonline geändert werden dürfen,

da hier die Regeln vorgegeben werden. Bedingung dafür ist natürlich die vollständige Unterstützung der Policy in den anderen Systemen (eDirectory, Mail, . . .). Denn es bringt nicht viel, wenn ein System gewisse Sonderzeichen nicht erlaubt, die im zentralen Rule-Container zulässig sind!

In diesem Zusammenhang soll auf ein unlängst aufgetauchtes Problem aufmerksam gemacht werden: Seit der Einführung eines transparenten PPPoE in den EDV-Lernzentren meldet sich eine Person per Novell Login-Dialog nicht nur beim Novell Netware Dienst an, sondern wird im Hintergrund per PPPoE über RADIUS beim Internetprovider (in diesem Fall die TU Graz) eingeloggt. Da der Novell Verzeichnisdienst (sowohl NDS als auch eDirectory) case-insensitiv ist, funktioniert unter Umständen das Login zwar am Novell Netware Server, aber nicht im Internet (RADIUS: geht direkt auf die case-sensitive TUG-online Datenbank). Der nicht zu umgehende Workaround, bis eDirectory und NDS case-sensitiv sind (wie bereits erwähnt wird dies ab der kommenden Version 8.8 der Fall sein) schaut so aus, dass der Rule-Container im TUGonline keine upper-case Character beinhaltet.

Single Sign-on (SSO) spielt in Identity Management Systemen eine große Rolle, sobald mehrere auf unterschiedlichen Systemen situierte Applikationen darauf zugreifen. Realisiert ist dies bis dato im Webmail – hier steht in der persönlichen Visitenkarte im TUG-online dem Benutzer ein Link zum Webmail zur Verfügung. Außerdem ist der Bibliotheksdienst per SSO angebunden und ebenfalls per Weblink in der Visitenkarte erreichbar. Geplant ist eine Erweiterung auf einen zentralen SSO Server (allerdings für Webapplikationen und nicht für Serverdienste, die Kerberos oder Ähnliches voraussetzen würden), der nicht nur dem Zentralen Informatikdienst sondern auch den Instituten für eigene Applikationen zur Verfügung steht. Vorteil dieser Lösung gegenüber einer „einfachen“ LDAP Authentisierung ist die Sicherheit, dass keine Man-in-the-Middle Attacke möglich ist. Als Anstoß gebe ich noch zu bedenken, ob SSO und Security wirklich Hand in Hand gehen oder ob dies nicht ein Widerspruch ist. SSO bedingt einen Benutzernamen und ein Kennwort, mit dem man auf alle Applikationen zugreifen kann. Wenn diese Daten in die falschen Hände geraten ist wesentlich mehr verloren als in Einzellösungen. Allerdings ist die Wahrscheinlichkeit größer, dass ein besseres Kennwort gewählt wird, wenn es nur eines zu merken gilt. Zudem ist es in der Praxis so, dass bei unterschiedlichen Diensten erst wieder dasselbe Kennwort zum Einsatz kommt. . .

Welche Challenges haben sich während der Implementierung unseres Identity Management Systems ergeben? Abgesehen davon, dass an Universitäten eine besonders heterogene Systemlandschaft besteht, ist die Koordination schwierig, sobald etwaige unterschiedliche Verantwortliche, die teils aus anderen Abteilungen oder Institutionen stammen, involviert sind. Es ist auch nicht immer einfach abzuschätzen wer bei Umstellungen nun tatsächlich davon betroffen ist – Schuld daran sind wohl großteils fehlende Dokumentationen. Eine mögliche Abhilfe dafür stellt die Umsetzung von ITIL (IT Infrastructure Library) dar. Damit kennt man die Abhängigkeiten der Dienste ebenso wie die Verantwortlichen!

4 Ausblick

Der Lerneffekt im Zuge der Einführung unseres Informationsmanagement und Identity Management Systems TUGonline war enorm. Im Endeffekt hat sich herauskristallisiert, dass unsere Lösung, obwohl wir kein anderes System explizit zum Vorbild genommen haben, anderen kommerziellen Identity Management Systemen sehr ähnelt. Dies hatte uns darin bestätigt, dass wir auf dem richtigen Weg waren. Was hat die TU Graz noch daraus gelernt? Redundanzen sind unvermeidlich, so gerne auch der Wunsch von CEOs gehegt wird, möglichst alles zu konsolidieren. . .

Es ist einfacher, auf der „grünen Wiese“ anzufangen als nachträglich Dienste und Daten zusammenzufassen! Meist bedeutet Konsolidierung mehr Aufwand als dass Nutzen daraus gezogen werden kann.

Als weiterer Lerneffekt hat sich herausgestellt, dass beinahe immer irgendeine Abhängigkeit bei Umstellungen vergessen oder nicht ausreichend berücksichtigt wird, sofern die Systemlandschaft komplex strukturiert ist! Abhilfe kann hier eine ausführliche Dokumentation schaffen, wie schon im vorigen Kapitel erwähnt – Stichwort: ITIL.

Vorgenommenes Ziel der TU Graz ist es in Zukunft keine weiteren LDAP-Verzeichnisdienste aufbauen zu müssen, egal welche Applikationen auch hinzukommen mögen. Angestrebt wird ebenso statt Accounting auf Profiles zu setzen, hinlänglich bekannt ist dabei ja die Hürde mit den Applikationen, die da nicht mitspielen können.

Das ganze Projekt TUGonline wäre aber nicht möglich gewesen, hätten nicht die Entscheidungsträger den Mut zum Risiko gehabt und dem Zentralen Informatikdienst freie Hand beim Entwickeln dieses Systems gelassen. Das Ergebnis gibt diesen Personen aber Recht, und sollte andere dazu motivieren, eigenständige Lösungen umzusetzen.