Dienstorientiertes Identitätsmanagement für eine *Pervasive University*

T. Höllrigl, A. Maurer, F. Schell, H. Wenske,.H. Hartenstein

KIM / Rechenzentrum
Universität Karlsruhe (TH)
Zirkel 2
76128 Karlsruhe
[hoellrigl | maurer | schell | wenske | hartenstein]@kim.uni-karlsruhe.de

Abstract: IT-gestützte Prozesse und Dienste in Lehre, Forschung und Weiterbildung durchdringen zunehmend die Universität im Inneren und verbinden sie mit der Außenwelt. Als Basis für einrichtungsübergreifende Geschäftsprozesse einer solchen *Pervasive University* wird ein flexibles Identitätsmanagement benötigt, welches eine lebendige Dienstevielfalt unterstützt. Hierfür schlagen wir eine dienstorientierte Identitätsmanagementarchitektur vor. Fundament der vorgestellten Architektur ist die Betrachtung der Universität als föderativer Verbund ihrer organisatorischen Einheiten. Die Architektur unterstützt universitätsweite Prozesse bei einer losen Kopplung von weiterhin autarken Organisationseinheiten, deren lokalen Geschäftsprozesse auch durch die Integration in einen föderativen Verbund weitgehend erhalten bleiben. Wir beschreiben die Entwurfsprinzipien und die Architektur des bereits prototypisch umgesetzten Systems.

Einleitung und Motivation

Aktuelle Entwicklungen erfordern von Universitäten den autorisierten Zugriff auf personenbezogene und kontextsensitive Dienste überall und jederzeit. Zudem muss sich eine moderne Universität durch die Fähigkeit auszeichnen, dem stetigen Wandel, getrieben durch strategische und politische Vorgaben, neue Kooperationen im nationalen und internationalen Umfeld sowie durch wissenschaftliche Weiterentwicklungen, gewachsen zu sein. Ein Ansatz sich dieser Herausforderung zu stellen, ist ein integriertes, dienstorientiertes Informationsmanagement, das ein Fundament für eine *Pervasive University* darstellt und damit eine Durchdringung sowohl nach außen über Universitätsgrenzen hinaus als auch nach innen innerhalb der Universität erzielt [Ju03]. Um dies zu erreichen, ist es notwendig, durchgängige Geschäftsprozesse auf heterogenen Organisations- und IT-Infrastrukturen zu realisieren. Dabei gilt es, bereits bestehende Dienstleistungen, die sich unabhängig voneinander entwickelt haben und in der Regel zueinander inkompatibel sind, zusammenzuführen. Da integrierte Geschäftsprozesse über verschiedene Dienstanbieter und deren Zugriffskontrolle hinwegreichen, ist es notwendig, ein sich über Organisationsstrukturen erstreckendes Identitätsmanagement mit entsprechender Benutzer- und Rechteverwaltung zur Verfügung zu stellen.

In diesem Beitrag skizzieren wir die wesentlichen Entwurfsprinzipien für ein flexibles und erfolgreiches Identitätsmanagement an einer Universität. Hierbei dienen uns die Dienstorientierung und das Prinzip der Föderation als Leitgedanken: notwendige Abhängigkeiten müssen einfach und nachvollziehbar implementiert werden können, künstliche und meist blockierende Abhängigkeiten innerhalb „klassischer" Identitätsmanagementsysteme müssen aufgebrochen beziehungsweise vermieden werden.

Dienstorientiertes Identitätsmanagement: Grundzüge

Ein weit verbreiteter Ansatz, welcher von einer Vielzahl von Universitäten zur Bereitstellung einrichtungsübergreifender, personenbezogener Dienste verfolgt wird, ist der Einsatz eines Meta Directories, auf dessen Basis ein Identitätsmanagement-System entwickelt wird [JS04, Kl05, Pa05]. Mit Hilfe eines Meta Directorys werden personenbezogene Identitätsinformationen aus einer Menge von Datenquellen aggregiert, in einem zentralen Repository gehalten und über eine Datenschnittstelle für universitätsweite Applikationen zur Verfügung gestellt. Darüber hinaus werden Änderungen sowohl im zentralen Repository, als auch in den angeschlossenen Datenquellen anhand vordefinierter Regeln abgeglichen, wodurch die Synchronität der Daten erreicht wird [Or05].

Während bei einem Meta Directory basierten System eine universitätsweite Anwendung die benötigten Daten aus dem zentralen Meta Directory bezieht, wird im Gegensatz dazu bei einer dienstorientierten Identitätsmanagement-Architektur diese Information von Identitätsmanagement-Diensten bereitgestellt. Als Baustein für die personalisierte Nutzung durch integrierte Geschäftsprozesse dient uns die Authentifizierung und Autorisation über ein föderatives Protokoll. Vorraussetzung hierfür ist die mögliche Abbildung der verschiedenen Identitäten einer Person bei den kooperierenden Organisationseinheiten (Satellit) aufeinander. Diese erfordert stabile Schnittstellen bei gleichzeitig flexibler Funktionalität, wie sie derzeit nur durch eine dienstorientierten Architektur ermöglicht wird. Bezogen auf ein Identitätsmanagement bedeutet die Dienstorientierung insbesondere Wiederverwendbarkeit der angebotenen Dienste, auch wenn sich deren Kontext im Laufe der Zeit ändert. So kann beispielsweise ein Dienst zur Erreichbarkeit der Mitglieder im Falle einer befristeten Kooperation kurzfristig durch Nutzung der Dienstschnittstelle des Kooperationspartners verändert werden, ohne bestehende Verzeichnisstrukturen modifizieren zu müssen. Darüber hinaus stellt das vorgeschlagene dienstorientierte Identitätsmanagement einen allgemeinen Dienst zur Synchronisation kongruenter, personenbezogener Daten zwischen den verschiedenen autark operierenden Einrichtungen zur Verfügung. Zudem wird eine übergreifende Single Sign-On (SSO) Funktionalität angeboten, welche die Nutzung von Diensten unterschiedlicher Organisationseinheiten ohne erneute explizite Nutzerauthentifizierung ermöglicht. Im Zuge der Selbstbestimmung wird den Benutzern ermöglicht, organisatorischen Einheiten – respektive deren Dienste – festzulegen, für die Synchronisations- und SSO-Mechanismen verwendet werden sollen. Dadurch ergibt sich für den Benutzer eine klare Nachvollziehbarkeit bezüglich der Datenflüsse zwischen den organisatorischen Einheiten und des Zugriffs auf lokale Dienste aus integrierten Geschäftsprozessen.

Identitätsmanagement-Architektur

Grundlage der vorgestellten Architektur ist die Betrachtung der Universität als föderativer Verbund ihrer organisatorischen Einheiten (Satelliten). Ein wesentlicher Punkt dieses Ansatzes ist, dass auf der einen Seite die Autarkie der Satelliten erhalten bleibt, auf der anderen Seite flexibel auf organisatorische Veränderungen reagiert werden kann, ohne das Gesamtsystem grundsätzlich ändern zu müssen. Dies wird erreicht, indem keine zentrale Datenbasis existiert, sondern die lokalen Prozesse sich so koordinieren, dass eine Gesamtsicht auf die erbrachten Dienste im Sinne von föderativen Prozessen entsteht. Die Koordination der lokalen Prozesse zu übergreifenden Diensten findet über eine Synchronisationsebene statt, die in der Lage ist, anhand der konkreten Informationsflüsse ereignisgesteuert lokale Prozesse auszulösen. Somit ergibt sich ein Modell, das auf drei verschiedenen Typen von Prozessen basiert. Zum einen Intra-Satellitenprozesse, die originär die Aufgaben der organisatorischen Einheit unterstützen, zum anderen Inter-Satellitenprozesse, die die konkrete Behandlung der personenbezogenen Daten über Satelliten hinweg übernehmen und letztlich satellitenübergreifende, integrierte Geschäftsprozesse, welche die Dienste des Identitätsmanagement-Systems nutzen (s. Abb1).

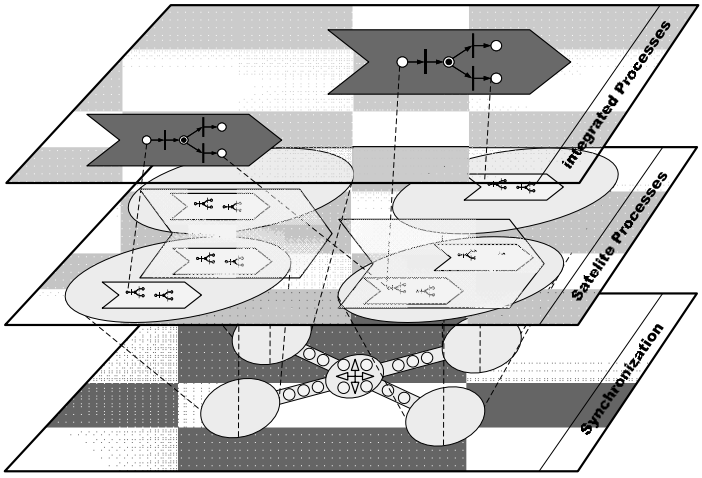

Abbildung 1 – Overlay Model

Die auf der obersten Ebene befindlichen integrierten Geschäftsprozesse nutzen die Dienste des Identitätsmanagements ohne Kenntnis dessen innerer Struktur. Die Bereitstellung von Diensten über Schnittstellen zu den vorhanden Systemen ermöglicht es, durch eine Orchestrierung dieser Dienste, flexibel auf neue Dienstanforderungen zu reagieren. So ist es beispielsweise möglich, ein Erreichbarkeitsdienst auf der Basis dieser Dienste zu konstruieren, bei dem die Gruppe der zu erreichenden Personen dynamisch mit Hilfe von Informationen aus verschiedenen Satelliten zusammengestellt werden kann. Als konkretes Beispiel kann eine Email an alle Studierende eines Studiengangs geschickt werden, wobei die Studiengangsdaten möglicherweise bei der zentralen Universitätsverwaltung und die Email-Adresse am Rechenzentrum vorliegen könnten.

Inter-Satellitenprozesse setzen sich aus Sequenzen von Intra-Satellitenprozessen, Ereignisse und Datenflüssen zusammen. Die grundlegenden Inter-Satellitenprozesse sind das einrichtungsübergreifende Anlegen, Ändern und Löschen von Identitäten. Das Zusammenspiel der Intra-Satellitenprozesse zu einem föderativen Inter-Satellitenprozess findet dadurch statt, dass lokale Datenänderungen über eine Synchronisations-Schicht transportiert werden und bei anderen Satelliten wiederum entsprechende Intra-Satellitenprozesse ereignisgesteuert auslösen. Diese konsequente Aufteilung der übergreifenden Geschäftslogik in die Prozesse der Satelliten und die damit verbundene Abspaltung der Datenflüsse von den Prozessen führt zu einer Reduktion der Komplexität bei gleichzeitiger Nachvollziehbarkeit der Datenflüsse. Da die bestehenden Intra-Satellitenprozesse weitgehend erhalten bleiben, wird eine breite Akzeptanz bei gleichzeitig geringem Integrationsaufwand erreicht. Lediglich die zu Grunde liegenden Systeme müssen mit dienstorientierten Schnittstellen ausgestattet werden. Inter-Satellitenprozesse basieren immer auch auf Vereinbarungen zwischen den organisatorischen Einheiten, in denen sowohl die Berechtigung als auch der Zugriff auf ausgetauschte Daten geregelt werden. Auf Grund der erhaltenen Autonomie der Satelliten bezüglich ihrer Daten und Prozesse liegt die Verantwortung für den Schutz personenbezogener Daten auch im gesamtuniversitären Umfeld grundsätzlich bei den Satelliten. Somit beruht ein zentrales Berechtigungsmanagement auf den Vereinbarungen zwischen den Satelliten, sofern keine universitätsweite Regelung vorliegt. Änderungen dieser Regelungen erfordern somit lediglich Eingriffe in den Datenfluss und die Abbildung in lokale Prozesse. Dadurch kann eine deutlich höhere Dynamisierung solcher Regelungen erreicht werden.

Der Synchronisationsdienst sichert die Konsistenz der Daten und nutzt hierzu einen Mechanismus, der es ermöglicht, über eine ereignisgetriebene Dienstschnittstelle zu jedem zu synchronisierenden Datensatz Intra-Satellitenprozesse auszulösen. Dadurch entsteht ein Datenaustauschsystem das zum einen die notwendige Nachvollziehbarkeit der Informationsflüsse gewährleistet, zum anderen die Flexibilität bei Änderung der Geschäftsprozesse erhält. Darüber hinaus wird hierdurch sowohl eine Provisionierung als auch eine Deprovisionierung personenbezogener Informationen unterstützt. Auf dieser Ebene werden die Satelliten sternförmig mit dem zentralen Synchronisations-System verbunden. Im Gegensatz zu einem klassischen Meta Directory sind personenbezogene Informationen ausschließlich über die Satelliten zugänglich und werden nach außen über Dienste zur Verfügung gestellt. Für jedes Synchronisationselement, das auch ein Attribut zu einem Datensatz sein kann, stellt genau ein Satellit die autoritative Quelle dar, während die Zugriffsberechtigung durch einen anderen Satelliten geregelt werden kann. Das Synchronisations-System hält die Daten lediglich zur Steigerung der Performanz, zur Dokumentation und Nachvollziehbarkeit sowie zur Gewährleistung der Konsistenz. Den Satelliten werden die Daten erst zur Verfügung gestellt, nachdem zwischen autoritativer Quelle, Berechtigungssteuerung und zugreifendem Satelliten entsprechende Vereinbarungen getroffen wurden. Auf Grund der Restriktion, dass keine Dienste direkt auf die Datenbasis des Synchronisations-Systems zugreifen können, sind diese Datenzugriffsvereinbarungen jederzeit dynamisch änderbar und müssen nicht wie bei einem Meta Directory bereits beim Anlegen der zentralen Datenbasis festgelegt werden. Ein weiterer Vorteil liegt in der nicht notwendigen Replikation der Satelliten-Zugriffsberechtigung in ein zentrales Repository.

Der Einsatz eines konfigurierbaren Web Service als Schnittstelle zwischen Synchronisations-System und Satellit erlaubt die Integration neuer Satelliten ohne aufwändige Programmierung. Durch diese Synchronisations-Schnittstelle eines Satelliten wird das Anstoßen lokaler, interner Prozesse, welche die Synchronisation der lokalen Identitätsbasen zur Folge haben, ermöglicht. Die Harmonisierung der Daten, d.h. die Umsetzung des zu Grunde liegenden Informationsmodells, findet nicht auf Ebene der Satelliten, sondern im Synchronisationssystem bzw. in der Schnittstelle zu dem jeweiligen Satelliten statt. Diese Architektur bietet neben der Nachvollziehbarkeit der Datenflüsse den Vorteil, dass das Zentralsystem nicht die Abbildung und Koordination der satellitenübergreifenden Geschäftsprozesse vornehmen muss.

Zusammenfassung und Ausblick

In diesem Beitrag wurde eine föderierte Architektur für ein dienstorientiertes Identitätsmanagement-System vorgestellt. Diese Architektur ermöglicht eine lose Kopplung von weiterhin autarken Organisationseinheiten, deren lokale Geschäftsprozesse auch durch die Integration in einen föderativen Verbund weitgehend erhalten bleiben. Gleichzeitig können über Organisationseinheiten hinwegreichende Prozesse etabliert werden. Kerngedanke der Architektur ist die Einführung von Inter-Satellitenprozessen, die durch konsequente Trennung des Datenflusses und der übergreifenden Geschäftslogik erhebliche Vorteile in Flexibilität und Datenschutz bietet. Die vorgestellte Architektur wurde bereits exemplarisch mit den in der zentralen Universitätsverwaltung eingesetzten Produkten der HIS GmbH, Hannover, als Satellit umgesetzt. Dabei wurde eine dienstbasierte Synchronisationsebene geschaffen, die in der Lage ist, ereignisgetrieben Synchronisationsprozesse auf vorhandenen Systemen auszulösen. Zur Gewährleistung der Selbstbestimmung der personenbezogenen Daten der Nutzer wird ein zentraler Authentifizierungsserver mit Selbstbedienungsfunktionalität aufgesetzt. Gleichzeitig ist dieser „Zentralsatellit“ auch Identity Provider für verschiedenste Föderationsprotokolle wie beispielsweise Shibboleth oder WS-Federation [DD05].

Literaturverzeichnis

[DD05] Djordjevic, I, Dimitrakos, T.: A note on the anatomy of federation. In: BT Technology Journal, Vol 23 No 4, Oktober 2005, S. 89-106.

[Kl05] Klasen, F.: IntegraTUM Aufbau einer durchgängigen integrierten Infrastruktur für die Technische Universität München, Vortrag von A. Bode. In: ceck Werkstattgespräche, Hagen: Centrum für eCompetence, Dezember 2005; S 12-13.

[Ju03] Juling, W.: Zukunftspläne - Integrierte Infrastruktur einer eUniversity. In: Forschung & Lehre - Bonn: Dt. Hochschulverband, 2003, S. 301-303.

[JS04] Jahn, G., Stamms, R.: Identity Management und Zentraler Verzeichnisdienstdienst. In: Workshop - Campus Web, Portale für Forschung & Lehre – TU München, März 2004

[Or05] Oracle: Directories, Directory Synchronization and Virtual Directories, http://www.oracle.com/technology/products/id_mgmt/ovds/pdf/oraclevirtualdirectory_whitepaper_10gr2.pdf, 2005.

[Pa05] Parthier, U.: Our Digital Identity, www.uspmarcom.de/de/presse/documents/BulletinIdM2005_web_3.pdf, 2005.