Seminar
„Smarte Objekte und smarte Umgebungen “
SS05

Identitätsmanagement: Industrielle Systeme

Marcel Beer
marcel.beer@student.ethz.ch

30. Mai 2005

Betreuer: Harald Vogt
Prof. Friedemann Mattern

1 Abstract

Mit der zunehmenden Informatisierung des Arbeitsalltags hat die Verwaltung von personenbezogenen Daten und Zugriffsrechten in vielen meisten Firmen stark an Bedeutung gewonnen. Mit Hilfe von Identitätsmanagement (IM) soll die Administration dieser Daten einfacher, effizienter und sicherer erledigt werden als bis anhin. Auf diese und weitere Ziele von IM werden ich in Kapitel 2 genauer definieren. Nachdem im Jahre 2002 die ersten IM Lösungen auf den Markt kamen, bieten heute alle grossen Softwarehersteller eigene Lösungen an. Die Grundfunktionen solcher Systeme werde ich in Kapitel 3 anhand von Microsofts „Identity and Access Management“ vorstellen, und den besonders interessanten Aspekt des „Federated Identity Management“ anhand von Oracles Lösung. Dabei gehe ich auch auf die „Liberty Alliance“ ein, die globale Standards für „Federated IM“ entwickelt und zu deren Mitglieder zahlreiche Grossfirmen aus diversen Branchen zählen. In Kapitel 4 werde ich die Industriellen Systeme mit den Identitätsmanagement-Systemen aus der Forschung vergleichen, wo der Endbenutzer und dessen Privatsphäre im Mittelpunkt stehen. Der Markt für IM Lösungen weist schon heute hohe zweistellige Wachstumsraten auf, und es wird erwartet, dass er in den nächsten Jahren explodieren wird. Vor allem dem Federated IM wird eine grosse Bedeutung beigemessen, und ein paar Jahre später wird auch IM für Smarte Objekte ein grosses Thema werden.

2 Einleitung

Während der letzten Jahren hat die Verwendung von Informatikmitteln in der Wirtschaft stark zugenommen. Firmenintern wurde dadurch die Administration vereinfacht und die Effizienz der Mitarbeiter erhöht. Gleichzeitig werden dem Kunden immer mehr Dienstleistungen auf dem elektronischen Weg angeboten. Die Verwaltung der personenbezogenen Daten und Zugriffsrechte erwies sich jedoch als schwierig. Seit einigen Jahren gibt es dafür zwar so genannte „Verzeichnisdienste“ , welche die Verwaltung dieser Daten vereinfachen, doch das Zusammenspiel verschiedener Verzeichnisse und proprietärer Systeme war bisher eher schwerfällig. In den meisten Firmen sind die personenbezogenen Daten daher auf verschiedene „Identity Stores“ verteilt und die meisten Anwendungen haben eine eigene Benutzerverwaltung. Das beeinträchtigt sowohl die Produktivität als auch die Sicherheit und bringt einen grossen administrativen Aufwand mit sich. Die Mitarbeiter müssen sich zahlreiche Passwörter merken, und verbringen gemäss Statistiken (3) bis zu 15 Minuten pro Tag damit, sich bei verschiedenen Anwendungen anzumelden. Es existieren auch selten einheitliche Sicherheitsrichtlinien und viele Angestellte notieren sich die Passwörter, so dass sie für andere einfach zu beschaffen sind. Auch der Austausch von Daten zwischen verschiedenen Abteilungen oder mit anderen Firmen gestaltet sich schwierig, und ist mit viel manueller Arbeit verbunden. Durch ein Zu-

sammenfassen der Verwaltung dieser Daten kann die Administration automatisiert, die Sicherheit und die Produktivität der Mitarbeiter erhöht und der Firmenübergreifende Informationsaustausch vereinfacht werden.

3 Der Begriff Identitätsmanagement (IM)

„Identity management is the process by which the complete security lifecycle for end-users and network entities is managed for an organization“ (4)
„Identity and access management combines processes, technologies, and policies to manage digital identities and specify how they are used to access resources“ (3)

Die Hersteller von IM Lösungen definieren IM als Zusammenfassung der Verwaltung von allen personenbezogenen Daten und Zugriffsrechten. Die Administration soll von der Erstellung über die Wartung bis zur Löschung solcher Daten vereinfacht und weitgehend automatisiert werden.

4 Die Ziele von Identitätsmanagement

4.1 Produktivität

Mit Single Sign On soll die Login-Zeit für die Mitarbeiter wesentlich verkürzt werden. Ein Login-Vorgang pro Tag bzw. Systemstart soll ausreichen - die Anmeldung für die verschiedenen Applikationen soll im Hintergrund ohne Benutzerinteraktion ablaufen. Das führt dazu, dass viel seltener Passwörter vergessen werden oder geändert werden müssen. Dadurch, und durch die automatisierte Erstellung, Wartung und Löschung von Benutzerkonten kann im internen Helpdesk ebenfalls viel Arbeitszeit eingespart werden.

4.2 Sicherheitsgewinn

Durch das Zusammenfassen der Verwaltung kann eine einheitliche, und sicherere Authentisierung der Benutzer erfolgen, z.B. mit Smart Cards oder biometrischen Merkmalen. Eine transparente Verwaltung der Benutzerrechte soll möglich werden, ebenso wie bessere Passwort-Richtlinien. Wichtig ist auch die zuverlässigere Löschung von nicht mehr benötigten Benutzerkonten. Untersuchungen haben nämlich gezeigt, dass in vielen Firmen zahlreiche Benutzerkonten von ehemaligen Mitarbeitern versehentlich nicht gelöscht werden.

4.3 Flexibilität

Die firmeninterne Softwareentwicklung wird vereinfacht, weil neue Anwendungen keine eigene Benutzerverwaltung mehr brauchen, sondern auf das Identitätsmanagement-

System zurückgreifen können. Die Kunden und Geschäftspartner können mit der mächtigeren Daten- und Rechteverwaltung einfacher angebunden werden. Zudem können die Datenbestände bei Firmenübernahmen oder Fusionen viel einfacher zusammengeführt werden.

4.4 Gesetzliche

Bestimmungen Die Umsetzung von neuen Richtlinien, z.B. in den Bereichen Datenschutz, Archivierung oder Auskunftspflicht, soll vereinfacht werden. Dies gestaltet sich ohne IM oft als sehr schwierig, und häufig werden deshalb die Bestimmungen nur teilweise erfüllt.

4.5 Kostensenkung

Durch die Konsolidierung der „Identity Stores“ und die Automatisierung der Administration können nennenswerte Wartungskosten eingespart werden. Auch die Zeitersparnis für die Angestellten und der stark reduzierte Helpdesk-Aufwand führt zu grösseren Einsparungen.

5 Industrielle Systeme

5.1 Marktüberblick

Die ersten Identitätsmanagement Lösungen kamen 2002/03 auf den Markt. Heute bieten alle grossen Softwarehersteller IM Lösungen an, u.a. IBM, HP, Microsoft, Novell, SAP und Sun Microsystems. Alle genannten Firmen haben ausserdem zwischen 1999 und 2005 mindestens je eine kleinere auf IM spezialisierte Firma aufgekauft; das unterstreicht, dass in IM ein enormes Markpotential steckt. Auch Analysten und Marktbeobachter versprechen hohe zweistellige Wachstumsraten, IDC schätzt, dass bereits 2007 ein Volumen von vier Milliarden Dollar erreicht wird - gegenüber etwa 600 Millionen Dollar im Jahr 2002.

5.2 Microsoft Identity Management Framework: „Identity and Access Management“

Microsoft unterteilt ihre „Identity and Access Mangement“ Lösung in 3 Hauptbestandteile: Directory Services, Identity Lifecycle Management und Access Management.

Directory Services (Verzeichnisdienste)

Microsofts „Active Directory“ speichert alle identitätsrelevanten Daten. Benutzerprofile mit allen Attributen, aber auch Zugriffsrechte, Passwörter und digitale Zertifikate. Ein Identitätsmangement-System kann aber durchaus aus mehreren Verzeichnissen bestehen, die alle das - herstellerunabhängige - Protokoll LDAP (Lightweight Directory Access Protocol) beherrschen müssen.

Identity Lifecycle Management: Identity Aggregation and Synchronization

Identity Lifecycle Management umfasst die Verwaltung der Daten über die ganze Lebensdauer - von der Eingabe bis zur Löschung. Dazu gehört neben dem Erstellen und Löschen von Accounts das Zusammenfassen der Daten von verschiedenen Verzeichnissen, das Setzen von Passwörtern, das Synchronisieren von mehrfach vorhandenen Daten und die Migration von Daten zwischen verschiedenen Verzeichnissen.

Access Management

Grundsätzlich werden zwei Arten von Zugriffen auf das System unterschieden: solche aus dem Firmennetz (Intranet-Zugriff) und solche von ausserhalb, z.B. über das Web mit einem Browser (Extranet-Zugriff). Beim Intranet-Zugriff ist „Single Sign On“ für die Angestellten möglich. Das heisst, der Benutzer meldet sich an, wenn er das erste mal am Tag einen Dienst benutzt, der Authentisierung/Autorisierung verlangt, und das System erledigt dann spätere Anmeldungen zum selben Dienst oder zu anderen Diensten im Hintergrund ohne Zutun des Benutzers. Für externe Mitarbeiter wie z.B. Vertreter oder auch Filialen gibt es die Möglichkeit, sich über VPN mit dem Firmennetz zu verbinden. Im Gegensatz dazu ist der Extranet-Zugriff besser geeignet, um Dienste für Kunden oder Geschäftspartner anzubieten. Der Zugriff erfolgt in der Regel mit einem Browser über eine Webseite. Auch hier gibt es die Möglichkeit, Single Sign On zu ermöglichen, also dem Benutzer nach einmaligem einloggen (pro Browser-session) automatisch Zugriff auf andere Dienste derselben Firma oder sogar auf Dienste von Partner-Unternehmen Zugriff zu gewähren. Die Möglichkeiten zur Authentisierung des Benutzers sind vielfältig. Sie reichen von einfachen Benutzername/Kennwort Paaren über Digitale Zertifikate und SmartCards bis hin zu biometrischen Merkmalen und Kerberos Systemen. Auch die Autorisierung, also das Erteilen von Zugriffsrechten ist auf verschiedene Arten möglich. Die traditionelle Rechteverwaltung mit „Access Control Lists“ (ACL) und Gruppenrichtlinien ist genauso möglich, wie die flexiblere, rollenbasierte Rechtevergabe, die dynamische, zur Laufzeit berechnete Rechte ermöglicht.

5.3 Oracle Federated Identity Mangement: Secure Federation Services

Auch Oracle bietet eine komplette Identitätsmanagement-Lösung an. In den oben beschriebenen Funktionen ist sie der Microsoft Lösung sehr ähnlich, darum konzentriere ich mich auf einen Aspekt, auf den Oracle speziell Wert legt: das „Federated Identity Management“ : Die Kernidee des Federated IM ist es, eingeschränkten Informationszugriff über die Grenzen von Organisationseinheiten hinweg zu vereinfachen. Zum Einen wird dadurch der Informationsaustausch zwischen funktional oder örtlich getrennten Geschäftsbereichen oder Abteilungen möglich, und bleibt gleichzeitig auf das nötigste beschränkt - z.B. die Quartalsergebnisse oder die Angestelltendatenbank. Zum Anderen werden auch firmenübergreifende, sichere Handelsbeziehungen ermöglicht. Geschäftspartner, Zulieferer, Geschäftskunden oder Outsourcingpartner erhalten eingeschränkten Zugriff auf interne Informationen und Ressourcen und umgekehrt. Zwei oder mehr Unternehmen bilden dann zusammen eine „Föderation“ . Um die dabei Sicherheit für beide Seiten zu wahren benötigt es aber vertraglich abgesicherte Vertrauensverhältnisse, die beidseitig kündbar sein müssen. Insbesondere braucht es in den Föderationen die Möglichkeit, selbst auszutreten, oder gewisse Mitglieder auszuschliessen. Die dazu nötigen technischen Massnahmen wie die Sperrung von Accounts, der Rückruf von Credentials (Passwörter, Digitale Zertifikate, usw.) und die Anpassung der Zugriffsrechte können grösstenteils automatisch erledigt werden. Die Anwendungsmöglichkeiten von Federated IM sind vielfältig. Interessante Möglichkeiten eröffnet Federated IM unter anderem in den folgenden vier Gebieten:

E-Government

Durch einfachen und sicheren Datenaustausch zwischen Behörden kann der Aufwand für die Verwaltung und den Bürger drastisch reduziert werden.

Gesundheitswesen

Federated IM ermöglicht den Austausch von Patientendaten zwischen Krankenhäusern, Arztpraxen und Apotheken unter Wahrung der Privatsphäre des Patienten -

Bildungswesen

Zugriff der Professoren und Studenten auf Departements- und Universitätsübergreifende Ressourcen und Dienste sind einfacher realisierbar.

Telekommunikation

Ortsabhängige Dienste werden realisierbar, wobei der Benutzer trotzdem anonym bleiben kann, und somit seine Privatsphäre wahrt.

5.4 Liberty Alliance

Das Ziel der Liberty Alliance ist es, globale, offene Standards für Federated IM und Federated Services zu entwickeln und zu etablieren. Gegründet wurde die Allianz im Jahre 2001 von 33 grossen Unternehmen aus verschiedenen Branchen - Sun Microsystems, American Airlines, IBM, Philips, Nokia, General Motors, Bank of America - um einige zu nennen. Ursprünglich als Alternative zu Microsoft's „Passport" System ins Leben gerufen, entwickelte sich die Allianz zum Quasi-Standard und zählt mittlerweile 160 Mitglieder, darunter auch Oracle und Intel. Von den " Grossen" fehlt einzig Microsoft, wobei aber eine gewisse bilaterale Zusammenarbeit gepflegt wird. Die Liberty Alliance definiert also die Standards des Federated IMs, prüft industrielle Produkte und vergibt Zertifikate für standardkonforme, interoperable Produkte. (Die Lösung von Oracle erfüllt z.B. die meisten Liberty Standards). Zu den weiteren bisherigen Resultaten der Liberty Allianz gehören:

- Spezifikation, die einfaches Single Sign On (SSO) innerhalb von Föderationen ermöglicht.
- Interface spezifikationen, Privatsphären- und Sicherheits-Richtlinien für Identitätsbasierte WebServices. Dazu gehört u.a. die dafür entwickelte XML-basierte Sprache SAML (Security Assertion Markup Language).
- Richtlinien für Federated IM mit mobilen Geräten

6 Vergleich Industrie vs. Forschung

Die Industriellen IM-Lösungen unterscheiden sich stark von den Forschungssystemen, die an Universitäten entwickelt und in (1) vorgestellt werden. Auf den ersten Blick wird schon der Begriff des IM grundverschieden definiert. Die Forscher stellen den Endbenutzer und dessen Privatsphäre in den Mittelpunkt. Er soll für verschiedene private oder geschäftliche Kontakte unter verschiedenen Pseudonymen auftreten können. Die ausgetauschten Informationen über den Benutzer werden dabei möglichst gering gehalten und der Benutzer kann für jeden Kontakt selbst bestimmen, was er von sich preisgibt. Im Gegensatz dazu geht es bei den Industriellen Lösungen vor allem darum, IM-Prozesse im Unternehmen effizienter, flexibler und sicherer zu gestalten. Die informationelle Selbstbestimmung des Angestellten gegenüber der Firma hat wenig Bedeutung. Beim Federated IM hingegen, sind erstaunlich viel Parallelen zu den Forschungssystemen zu erkennen. Die Firma nimmt dabei die Rolle des Endbenutzers an, und hat ähnliche Bedürfnisse wie der private Nutzer: Die Firma will beim Informationsaustausch mit Geschäftspartnern selbst bestimmen, welche Informationen welchen Partnern zur Verfügung stehen. Dabei sollen gleichzeitig sensitive Daten gegen unberechtigte Zugriffe geschützt werden.

7 Diskussion

Schwierigkeiten

Die Hauptschwierigkeit von IM Lösungen liegt in deren Komplexität, wie ein Zitat von Microsoft aus (3) treffend beschreibt: “ Identity and access management initiatives tend to be more complex than the majority of IT projects [. . .] because of the diversity of identity stores and protocols, encryption mechanisms, policies need to work together “ . Und trotz Datenaustausch und Zusammenarbeit müssen sensitive Daten und Ressourcen zuverlässig geschützt werden.

Heute

Drei Jahre nach dem ersten Erscheinen von kompletten IM Lösungen läuft die Entwicklung immer noch auf Hochtouren. Die Einführung von IM in Unternehmen ist erst am Anlaufen, jedoch weisen die Absatzzahlen für IM Lösungen hohe zweistellige Wachstumsraten auf.

Morgen

Mit der zunehmenden Verbreitung von IM Lösungen in den nächsten Jahren werden vor allem Federated IM Anwendungen interessanter. Ein weiterer grosser Sprung ist zu erwarten, wenn IM nicht mehr nur für die Verwaltung von Personendaten eingesetzt wird, sondern auch in Verbindung mit Sachen angewandt wird. Bisherige Anwendungsbeispiele, die in diese Richtung gehen sind die Paketverfolgung und die automatische Lagerverwaltung mit RFID-Tags. Später soll auch die Kommunikation und Informationsaustausch zwischen verschiedenen „Smarten Objekten“ ermöglicht werden und mit IM kontrolliert werden.

Literatur

[1] *Identitätsmanagement: Einführung und die ideale Sicht – Systeme aus der Forschung*, Bettina Polasek

[2] *Liberty Alliance Project*
http://www.projectliberty.org/ [Stand: 1.5.2005]

[3] *Microsoft Identity and Access Management Series*
http://www.microsoft.com/technet/security/topics/
identitymanagement/idmanage/default.mspx/ [Stand: 1.5.2005]

[4] *Oracle Identity Management Components*
http://www.oracle.com/technology/products/id_mgmt/ [Stand: 1.5.2005]

[5] *Proof of ID Required? Getting Identity Management Right*, Malcolm Crompton, Federal Privacy Commissioner von Australien
http://www.vs.inf.ethz.ch/edu/SS2005/DS/papers/
identity/crompton_proof_of_id.pdf [Stand: 1.5.2005]

[6] *Sun wagt neuen Vorstoss in Richtung Identity Management*
Interview mit Frank Issing, Product Marketing Manage bei Sun Microsystems
http://www.zdnet.de/itmanager/unternehmen/0,39023441,39123000,00.htm
[Stand: 1.5.2005]

[7] *The road to identity management: How to know who's who and what's what*
Opinion by Sara Gates, Sun Microsystems Inc.
http://www.computerworld.com/printthis/2005/0,4814,99749,00.html
[Stand: 1.5.2005]