

# *manage it*

[[ IT - S t r a t e g i e n u n d L ö s u n g e n ]]

## **Identity Management**

Strategische IT-Komponente

## **Server-konsolidierung**

IT-Kosten sparen

## **Enterprise Application Integration**

Auf dem Prüfstand

## **Rundumschutz**

# **IT-Sicherheit**

Nutzen Sie unser Angebot für  
Sonderdrucke oder E-Publishing-Dateien  
von Artikeln dieser Ausgabe

Tel.: +49 8092 87543

 **D·A·CH Security**

Universität Basel | 30. und 31. März 2004

Directory-Technologie als strategische IT-Komponente im Siemens-Konzern

# Identity Management macht komfortable Portale möglich

Sicherheit und wirtschaftlicher IT-Einsatz in größeren Unternehmen beruhen heute entscheidend

auf einem effizienten Identity Management: »Wer darf was wann womit«?

Die geschäftlichen Abläufe fließen bei großen Unternehmen und Organisationen heute oft über mehrere Zeitzonen und tangieren Tausende von Mitarbeitern, Kunden und Lieferanten. Die Zusammensetzung von Arbeitsgruppen wechselt sehr oft, in manchen Organisationen sind virtuelle Teams eher die Regel als die Ausnahme, und immer mehr Unternehmen wickeln einen Großteil ihrer geschäftlichen Transaktionen digital über ein Netzwerk beziehungsweise das Internet ab.

Sicherheit und Rentabilität von Organisationen dieser Größenordnung, Reichweite und Struktur beruhen ganz entscheidend auf einer effizienten Verwaltung der Identitäten. »Wer darf was wann womit tun«, ist die eine wichtige Frage dieses Identitätsmanagements, die gewöhnlich unter dem Begriff »Autorisierung« subsumiert wird. Der andere Knack-Punkt ist die Authentifizierung, also die zweifelsfreie Feststellung, ob ein Mitarbeiter auch tatsächlich derjenige ist, als der er sich ausgibt. Die Authentifizierung ist gerade in einem Kontext des E-Business mit unzähligen Prozessen, bei denen nur noch zwei Maschinen miteinander verknüpft sind beziehungsweise rein digitale Identitäten vorliegen, besonders schwierig.

Gerade für Unternehmen, die sich konsequent in Richtung E-Business orientieren, ist deshalb ein Meta-Verzeichnis für die Verwaltung der Identitäten unabdingbar. Der Aufbau und

die Handhabung eines solchen zentralen Speichers von Identitäten ist freilich keine reine IT-Angelegenheit, sondern greift tief in die Organisationsstruktur eines Unternehmens ein, zumindest dann, wenn eine Infrastruktur entstehen soll, die leistungsfähig, sicher und flexibel ist. Die zuletzt genannten Parameter werden nur durch ein rollenbasiertes Modell voll erfüllt, bei dem eine Verknüpfung zwischen einer digitalen Identität, sprich einer Person, die im Netzwerk arbeitet, und einem be-

aufwand genaue Kostenzuordnungen machen«, sagen in diesem Zusammenhang Harald Kopper und Andreas Wolff vom Unternehmensbereich Information and Communication Networks (ICN) der Siemens AG.

Kopper und Wolff wissen wovon sie reden, haben die beiden doch maßgeblichen Anteil an der Verwirklichung der »Directory Infrastructure for a Global Organization« (DINGO), wie sie in den letzten vier Jahren zunächst in der Netzwerksparte von Siemens (ICN) und jetzt zunehmend auch in anderen Unternehmensbereichen des Konzerns wie Mobilfunk (ICM), Medizintechnik (MED) und IT-Dienstleistung (SBS) verwirklicht wird. DINGO basiere zwar auf der Directory- beziehungsweise Meta-Directory-Technologie von Siemens, erläutern Kopper und Wolff, gleichwohl sei diese Anwendung aber viel mehr als nur ein Stück zusätzliche Software. Sie stelle vielmehr heute den Rahmen dar für das organisatorische Gesamtkonzept des Gesamtkonzerns. So werde die Directory-Infrastruktur, die DINGO repräsentiere, mittlerweile auch vom zentralen CIO des Konzerns gepusht, freuen sich die beiden DINGO-Architekten der ersten Stunde. Die Konzernzentrale betreibe in Zukunft praktisch, so Kopper und Wolff, einen »DINGO-Klon«, in dem die Identitäten der Bereiche aggregiert und konsolidiert seien.

**IBAC versus RBAC: Eine Grundsatzfrage.** Die Directory-Infrastruktur bei Siemens ICN ist die technische

Nutzen Sie unser  
Angebot für  
Sonderdrucke oder  
E-Publishing-Dateien  
von Artikeln aus

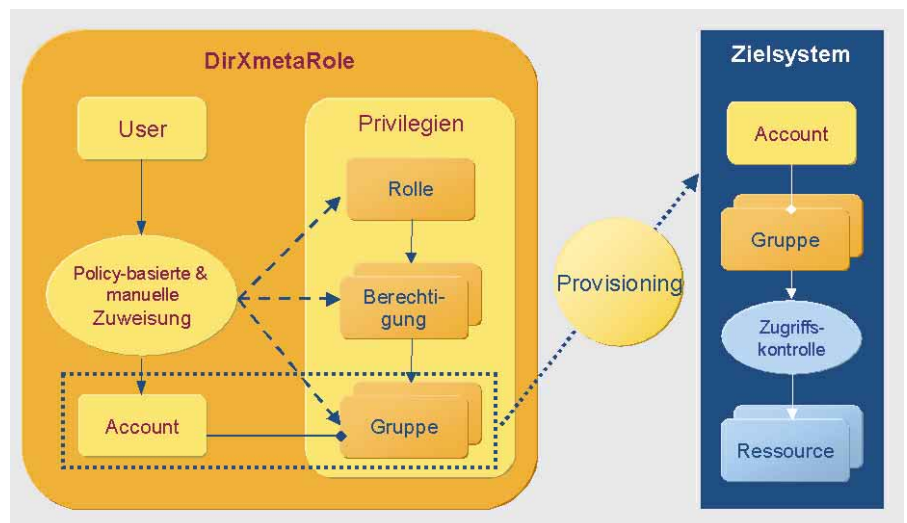
**manage it**  
[IT-STRATEGIEN UND LÖSUNGEN]

Tel.: +49 8092 87543

stimmten Prozess, sprich einer oder mehrerer IT-Applikationen, über eine Stellenbeschreibung oder Rolle vermittelt werden. »Nur wenn Sie Authentifizierung und Autorisierung auf einem rollenbasierten Konzept aufsetzen, können Sie auf innerbetriebliche Änderungen, Fusionen oder die Bildung von virtuellen Arbeitsgruppen ausreichend flexibel im zentralen Directory reagieren, können diesen schnell aktualisieren und ohne größeren Zusatz-

Grundlage für die so genannte Entitlement-Architektur, eine Middleware-Schicht, in der die digitalen Identitäten verwaltet werden. Im Wesentlichen geht es dabei um Objekte wie »Benutzer«, »Rolle« und »Zugriffs-Recht« sowie klassifizierende Attribute für diese Objekte. Aus der Sicht der Informationstechnik stellen diese Objekte Informationen über Menschen, Applikationen und Ressourcen dar, die irgendwo im Unternehmen in Verzeichnissen, Datenbanken und Benutzerprofilen gespeichert sind. Die Speicher der Entitlement-Schicht verteilen die Informationen über Zugangsrechte an die verschiedenen dezentralen Speicher in den Unternehmensbereichen, Landesgesellschaften, Minderheitenbeteiligungen oder auch Lieferanten und Kunden. Während Rechte und Benutzerprofile in der Entitlement-Schicht zentral gehalten werden, ist die Vergabe der Rollen und der Rechte dezentral. Mit anderen Worten: wer was wann womit darf, spricht: die Datenflüsse und die Geschäftsprozesse, all dies wird in den einzelnen Bereichen, Landesgesellschaften, bei den Kunden oder Lieferanten festgelegt. Auch die Steuerung erfolgt dezentral von diesen Einheiten aus. Die Sicht im Directory ist aber »total«: »Wenn beispielsweise so verschiedene Bereiche wie »Mobilfunktechnik« und »Kraftwerksbau« den selben Kunden haben sollten, dann ist der nur einmal im Directory gespeichert, erhält aber für die unterschiedlichen Bereiche unterschiedliche Attribute mit vermutlich unterschiedlichen Rechten«, erklärt Harald Kopper.

Die Entitlement-Architektur ist quasi die informationstechnische Ausprägung des rollenbasierten Organisationsmodells, das Siemens verwirklicht. Standardisiert wird dieses Organisationsmodell, das weit über reine IT-Strukturen hinausweist, in den Festlegungen der »Role based Access Control« (RBAC) des amerikanischen »National Institute of Standards and Technology« (NIST). Siemens arbeitet eng mit dem NIST, dem NAC (Network Applications Consortium) und der EEMA (The European Forum für Electronic Business) an der Standardisie-



rung von RBAC mit. In Europa wird der RBAC-Standard von der EEMA vorangetrieben. Dort engagieren sich neben Siemens Firmen wie IBM, Guardionic, Volvo sowie Institutionen wie die Europäische Kommission.

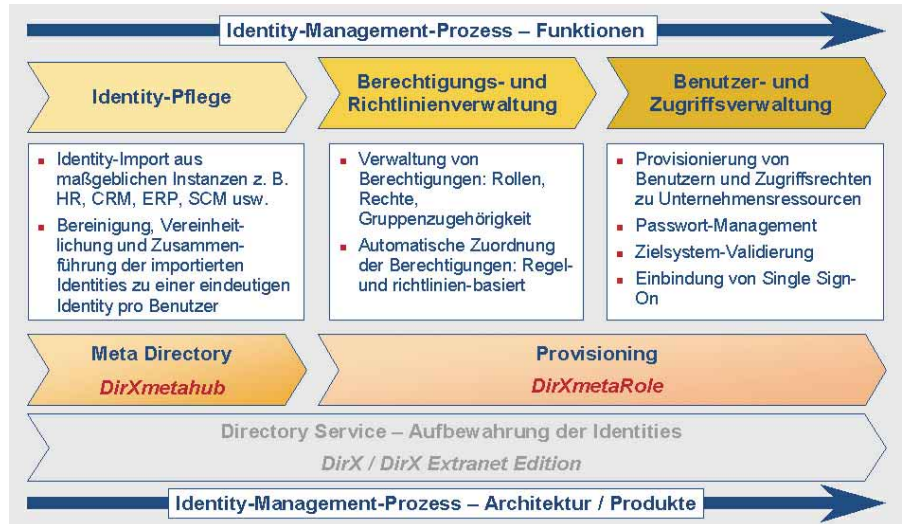
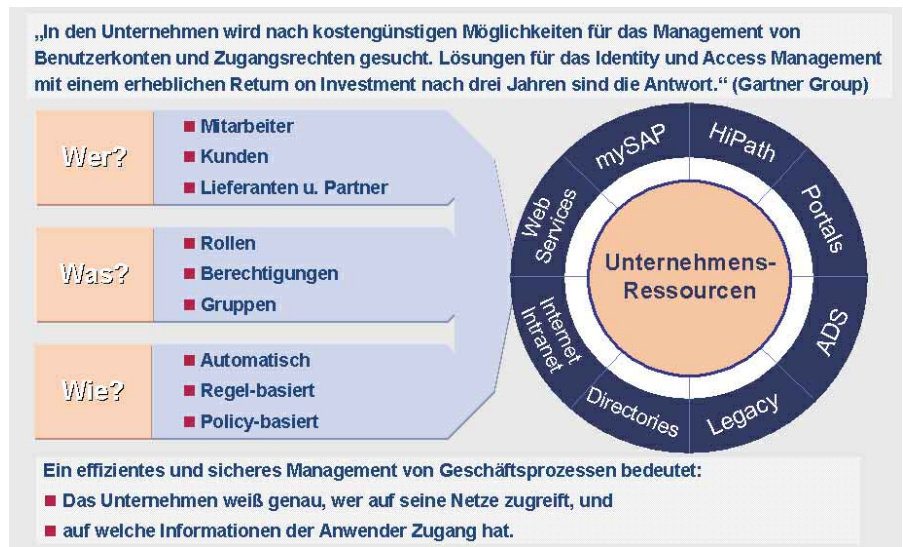
Das rollenbasierte Modell ist nicht zuletzt für die Abrechnung weit effizienter als die »Identity Based Access Control« (IBAC), die heute von fast allen Unternehmen mehr oder weniger angewandt wird, falls die Unternehmen überhaupt ein halbwegs funktionierendes Identitäts- und Zugangsmanagement betreiben. »Sie müssen bei rollenbasiertem Zugang zum Beispiel nicht für jeden Mitarbeiter, Kunden oder Lieferanten die benutzten Applikatio-

nen für die Kostenberechnung einzeln addieren, die Anzahl der zugangsberechtigten Anwendungen ist vielmehr schon in der Rolle selbst konsolidiert«, erläutert Andreas Wolff einen der Vorteile. Trotz der klaren Überlegenheit des rollenbasierten Modells haben viele Unternehmen organisatorische Probleme mit der Einführung. Harald Kopper weiß auch, warum: »Wenn Sie eine rollenbasierte Organisation schaffen, müssen Sie notwendigerweise individuelle Erbhöfe beseitigen und Statussymbole attackieren, das ist nicht einfach«. Und Andreas Wolff ergänzt: »In vielen Unternehmen ist es halt immer noch so, dass einer nach einem bestimmten Zugangsrecht schreit und

dann bekommen er oder sie es meist auch, ganz gleich, ob das von der Unternehmensorganisation notwendig und von der Sicherheitsstruktur her sinnvoll ist.«

Ohne Interesse und Engagement der obersten Führungsebene lässt sich nach Meinung von Kopper und Wolff eine rollenbasierte Organisationsstruktur nicht schaffen. Bei Siemens ist dieses Engagement »von oben« schon länger vorhanden, deshalb werde der Konzern auch weiterhin eine Vorreiterrolle in Sachen »Directory Enabled Organization« spielen, darin sind sich die beiden DINGO-Protagonisten sicher. Bei der Überzeugungsarbeit für eine rollenbasierte Organisationsstruktur hat nicht zuletzt die enge Zusammenarbeit der DINGO-Anwender mit den Identity Management Entwicklungs- und Marketingteams von Siemens ICN entscheidenden Anteil. Dieser engen Zusammenarbeit ist es zu verdanken, dass Siemens der erste Anbieter war, der seine Meta-Directory-Lösung um eine darauf aufbauende RBAC-Provisioning-Lösung erweitert und damit die integrierte Provisioning-Komponente auf eine neue Ebene gehoben hat.

**DINGO und die Philosophie der Portale.** Durch die Entitlement-Middleware muss nur noch die jeweilige Rolle in der Middleware-Schicht »provisioniert«, sprich: mit den aktuellen Informationen versorgt werden, und nicht mehr die Rolle in den einzelnen Anwendungen. Mit dieser Reduzierung der Provisionierungsarbeit auf die Identitäts-Management-Middleware fällt das letzte Element der harten Verdrahtung zwischen den Applikationen und dem Meta-Directory weg. Denn ursprünglich – das heißt im Jahr 1998 – gingen auch die Entwickler und die Anwender der Meta-Directory-Technologie bei Siemens von einer durchgängigen »harten Verdrahtung« von Identitätsmanagement und Zielapplikation aus. Man begann, jede Applikation über einen eigenen Agenten direkt an das Directory anzudocken. Wenn sich eine Änderung im Verzeichnis ergab, wurde diese sofort über die zuständige Agen-



tensoftware an die jeweilige Applikation überspielt. Auch die Provisionierungskomponente arbeitete in ihrer ersten Version auf diese Art: Vergabe und Änderung von Rechten für bestimmte Rollen wurden getrennt für jede einzel-

ne Anwendung geregelt.

Eine derartige enge Kopplung wird mit zunehmender Komplexität nicht nur immer schwerer beherrschbar, sondern sie kann überhaupt nur dann funktionieren, wenn die einzelnen Applikationen als Code-Elemente für den Verwalter auch wirklich zur Verfügung stehen. Das ist aber seit einigen Jahren immer weniger der Fall. Für die meisten Unternehmen gehört Informationstechnik nicht zum Kerngeschäft, zumindest aber nimmt man IT-Funktionen nicht mehr als Applikationen wahr, sondern sieht sie als Dienstleistung, die in konfektionierter Form zugeliefert werden sollte. Je nach Qualitätsstufe oder »Service Level« wird mehr oder weniger für diese Dienstleistung bezahlt. Festgelegt wird die Qua-

Nutzen Sie unser Angebot für Sonderdrucke oder E-Publishing-Dateien von Artikeln aus

**manage it**  
[IT-Strategien und Lösungen]

Tel.: +49 8092 87543

litätsstufe durch so genannte Service Level Agreements«, also Verträge über den Funktionsumfang und die Qualität der zu liefernden IT-Services.

Die Welt der IT-Services basiert auf einer losen Kopplung zwischen Dienstleister und Abnehmer, zwischen denen neben dem Service Level lediglich bestimmte Schnittstellen abgesprochen werden müssen. Die Entitlement-Architektur von DINGO passt genau zu dieser Vorstellung der Informationstechnik als einem konfektionierten Dienstleistungsprodukt. Und sie korrespondiert auch mit der Welt der Portale, die bei Siemens die herkömmlichen Applikationen immer mehr ablösen. Portale sind Anwendungen ohne eigene Nutzerverwaltung, die bestimmte Funktionen für diejenigen zur Verfügung stellen, die auf diese Funktionen ein Zugangsrecht haben. Die Nutzerverwaltung wird dabei durch das Identitätsmanagement des DINGO-Systems übernommen. Die Directory-Technologie und damit DINGO sind zu einem der wichtigsten »Enterprise Portal Services« geworden, freuen sich Harald Kopper und Andreas Wolff. Die beiden DINGO-Architekten machen im Kontext der Portaltechnologie noch einmal die zentrale Bedeutung der Rollenorientierung deutlich: »Bei Portalen müssen ein- und dieselben Daten aus vielen verschiedenen Sichten dargestellt werden können. Bei der daten-

technischen Realisierung dieser Separierung hilft uns das Rollenkonzept enorm.« Das Portal selbst ist nicht auf die einzelnen Sichten fixiert, sondern verwaltet Rollen, über die wiederum bestimmte Personen Services abonnieren können.

**Entitlement-Architektur reduziert SLA-Kosten.** Natürlich gibt es bei Siemens auch noch jede Menge eng gekoppelter Applikationen, beispielsweise den Verzeichnisdienst »Active Directory«, der die Microsoft-Applikationen steuert oder auch die Betriebswirtschaftssoftware von SAP (SAP /R3): »Wir werden eng angebundene Services nicht um des bloßen Prinzips willen entkoppeln, das rechnete sich nicht«, sagt Wolff. »Aber alle neuen Anwendungen und Dienste laufen über die Directory-Middleware.« Die Entitlement-Architektur und das darunter liegende Organisationskonzept der Rolle erleichtert nicht nur die Zusammenarbeit mit den diversen Service Providern, die IT-Dienstleistung an Siemens liefern, sondern sie spart auch ganz unmittelbar Geld. »Wenn wir einem unserer IT-Service-Provider die Entitlement-Architektur zur Verfügung stellen und damit Verwaltungsaufwand abnehmen beziehungsweise ihm leichter bedienbare Schnittstellen breit stellen, dann muss sich das natürlich auch in finanziell günstigeren Service-Level-

Verträgen widerspiegeln«, schildern Kopper und Wolff das Wechselspiel zwischen Directory-Technologie und Outsourcing-Verträgen.

Heute werden bei Siemens ICN und ICM etwa 180 Verfahren beziehungsweise Applikationen und rund 60000 Benutzer durch das Identitätsmanagement von DINGO verwaltet. Tendenziell wird das Zentralregister die Identitäten, Rollen und Rechte weltweit im Konzern speichern. »Wir haben durch das Konzept der rollenbasierten Organisation und des directory-basierten Identitätsmanagements die Zahl der Schnittstellen enorm verringert. Die Zahl der Stellschrauben ist viel übersichtlicher geworden und das Drehen an einer dieser Schrauben hat klar definierte Effekte, so dass wir letzten Ende viel Geld dadurch sparen«, resümieren Harald Kopper und Andreas Wolff die bisherige Entwicklung und meinen: »Siemens hat erkannt, dass man mit einer Directory-Infrastruktur klare Wettbewerbsvorteile erreichen kann.«

*Jürgen Höfling*

[jhoefling@t-online.de](mailto:jhoefling@t-online.de)

Links:

<http://csrc.nist.gov/rbac/>  
<https://www.eema.org/home1.asp>  
<http://www.netapps.org/>  
<http://www.siemens.de/directory>



3 Monate lang

# Einblick

# Durchblick

# Ausblick

f ü r d r e i z e h n f ü n f z i g !

[ ] **Ja**, ich bestelle » *manage it* « für drei Monate zum Preis von Euro 4,50 pro Ausgabe. Dieses Probeabonnement verlängert sich nicht automatisch.

Schicken Sie diesen Coupon an:

**ap verlag GmbH**  
**Postfach 1380**  
**85554 Ebersberg**

oder faxen Sie die Seite einfach an die Nummer

**+49 8092 87544**

Titel: \_\_\_\_\_

Vorname: \_\_\_\_\_

Nachname: \_\_\_\_\_

Position: \_\_\_\_\_

Firma: \_\_\_\_\_

Straße: \_\_\_\_\_

PLZ: \_\_\_\_\_ Ort: \_\_\_\_\_

E-Mail: \_\_\_\_\_

Telefon: \_\_\_\_\_

Fax: \_\_\_\_\_