Identity und Access Management

ZKI Arbeitstreffen, Köln, 04./05.Oktober 2005

Jens Bußjäger, Principal Security

Jens.bussjaeger@siemens.com

SIEMENS

Vision der „Hochschule 2010“

... die Konkurrenzfähigkeit einer Gesellschaft wesentlich von dem aus Wissenschaft und Forschung resultierenden Innovationsgrad der auf den Märkten angebotenen Produkte und Verfahren abhängt.

(Zitat aus Hochschulpakt, 09.02.2004)

Multimedia

- eLearning Plattform
- Verwaltung Digitaler Identitäten
- Medienintegration über das Internet abrufbar

Mobilität

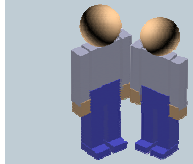
- Funk-basiertes Campus-Netz
- Internationale Teilnahme an Hochschul-Veranstaltungen
- Desk Sharing
- Geschützte Zutrittsbereiche

Sicherheit

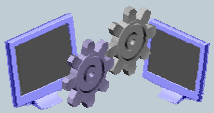
- Schutz Hochschul-interner Ressourcen
- Sichere elektronische Prozesse
- Sichere Digitale Identitäten (Digitaler Ausweis)

DirXidentity Management

Identity und Access Management



- Mitarbeiter
- Lehrbeauftragte
- Student
- Partner



Identity Management

Wer benötigt Zugriff worauf?

- Identitäten
- Organisationen
- Applikationen
- IT-Systeme
- Ressourcen
- ...

Metadirectory

Wer benötigt welche Rechte?

- Benutzerprofile
- Rollen & Berechtigungen
- Geschäftsprozesse

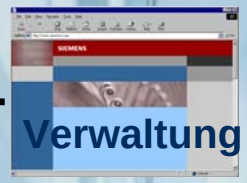
Provisioning

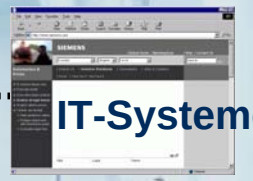
Access Management

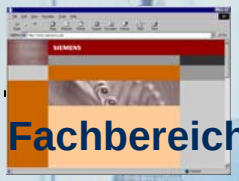
Wer erhält welche Zugriffrechte?

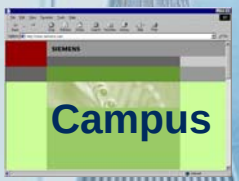
- Regeln
- Vorschriften
- Bedingungen

Access Management

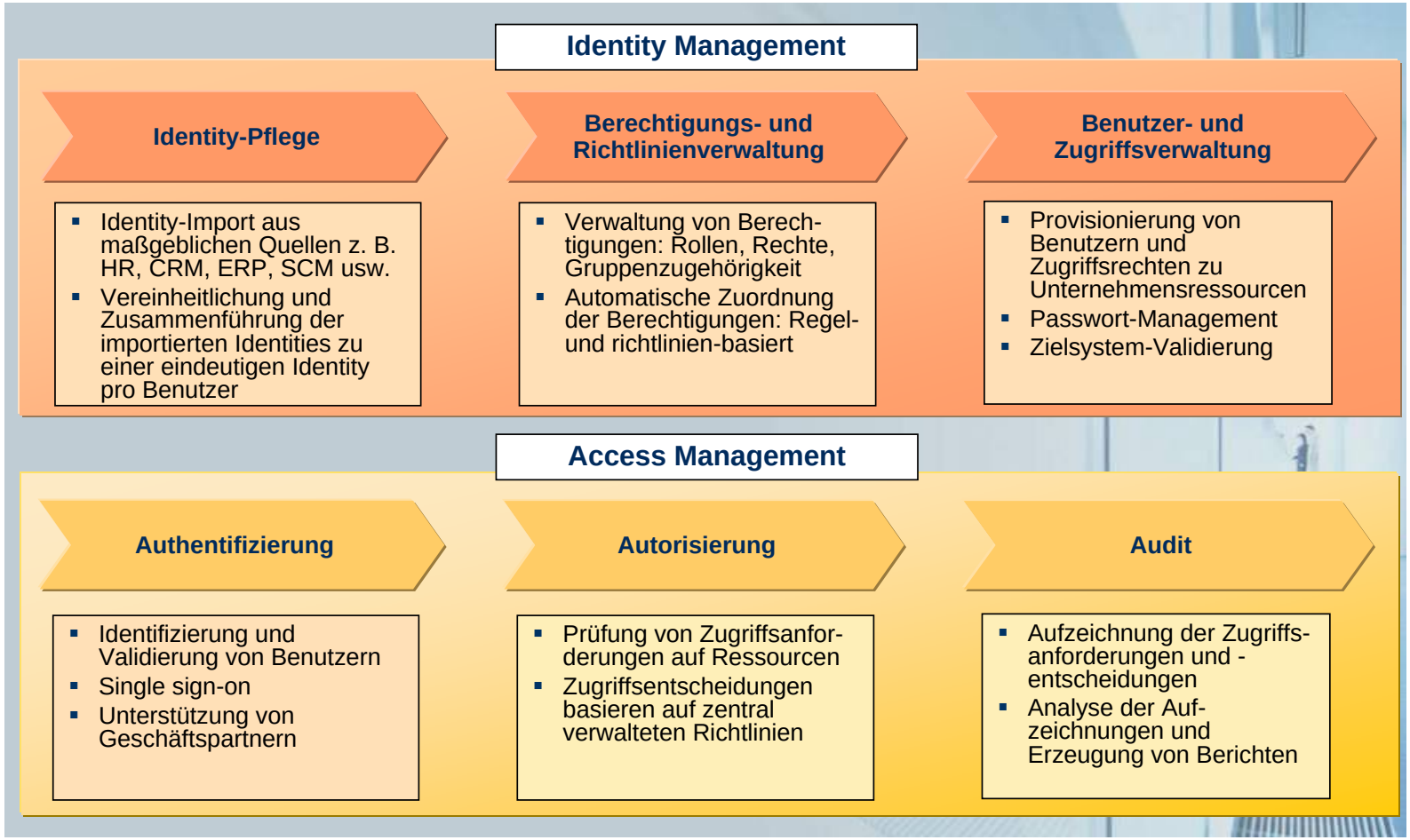








Funktionen des Identity und Access Managements



DirX
Integrierte Produktfamilie für Identity und Access Management

Funktionalität

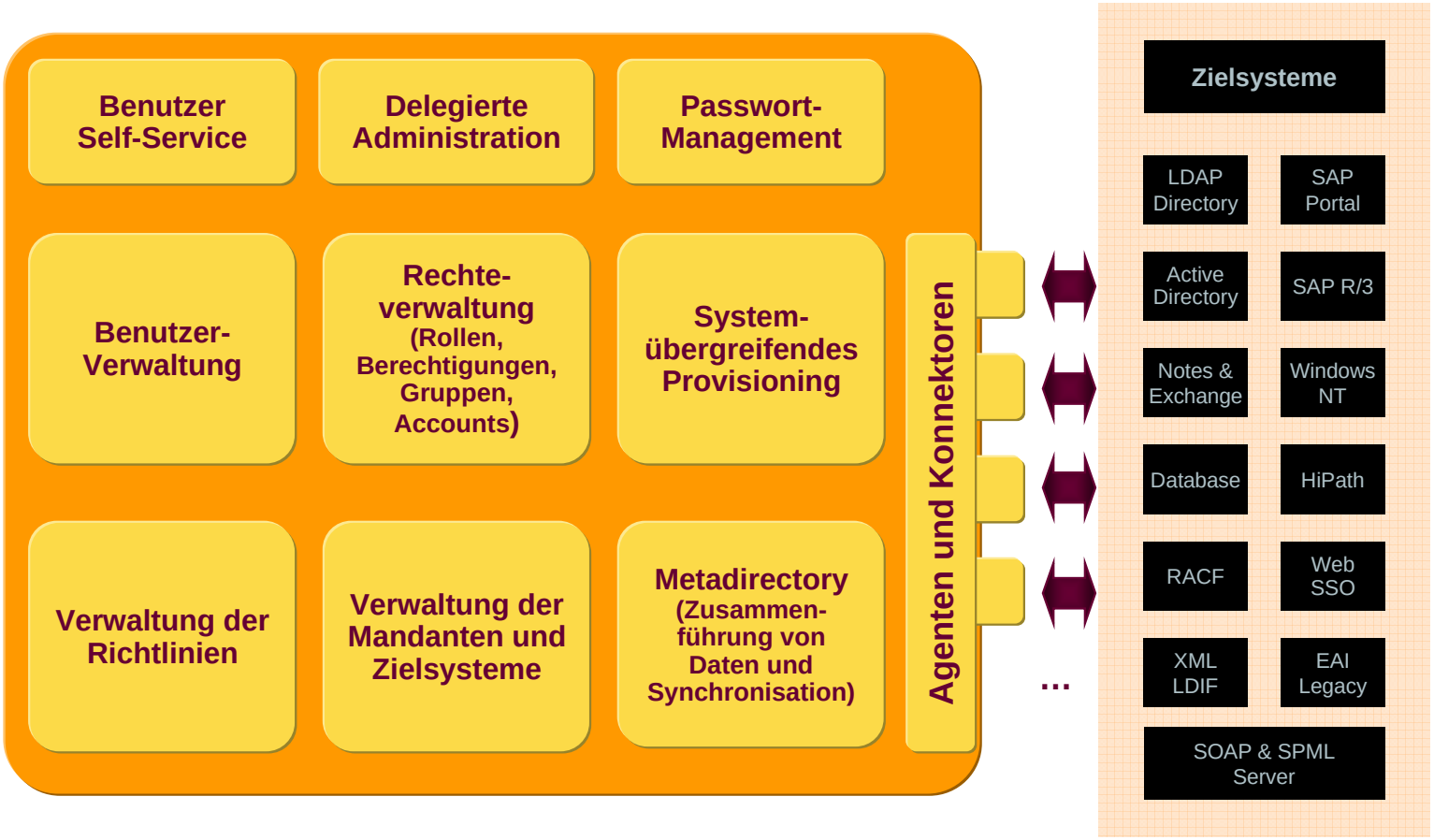
Produkte

Identity Management
DirXidentity
DirXmetaRole
DirXmetahub

Directory Server
DirX
DirX Extranet Edition

Access Management
DirX Access

DirX Identity
Funktionen



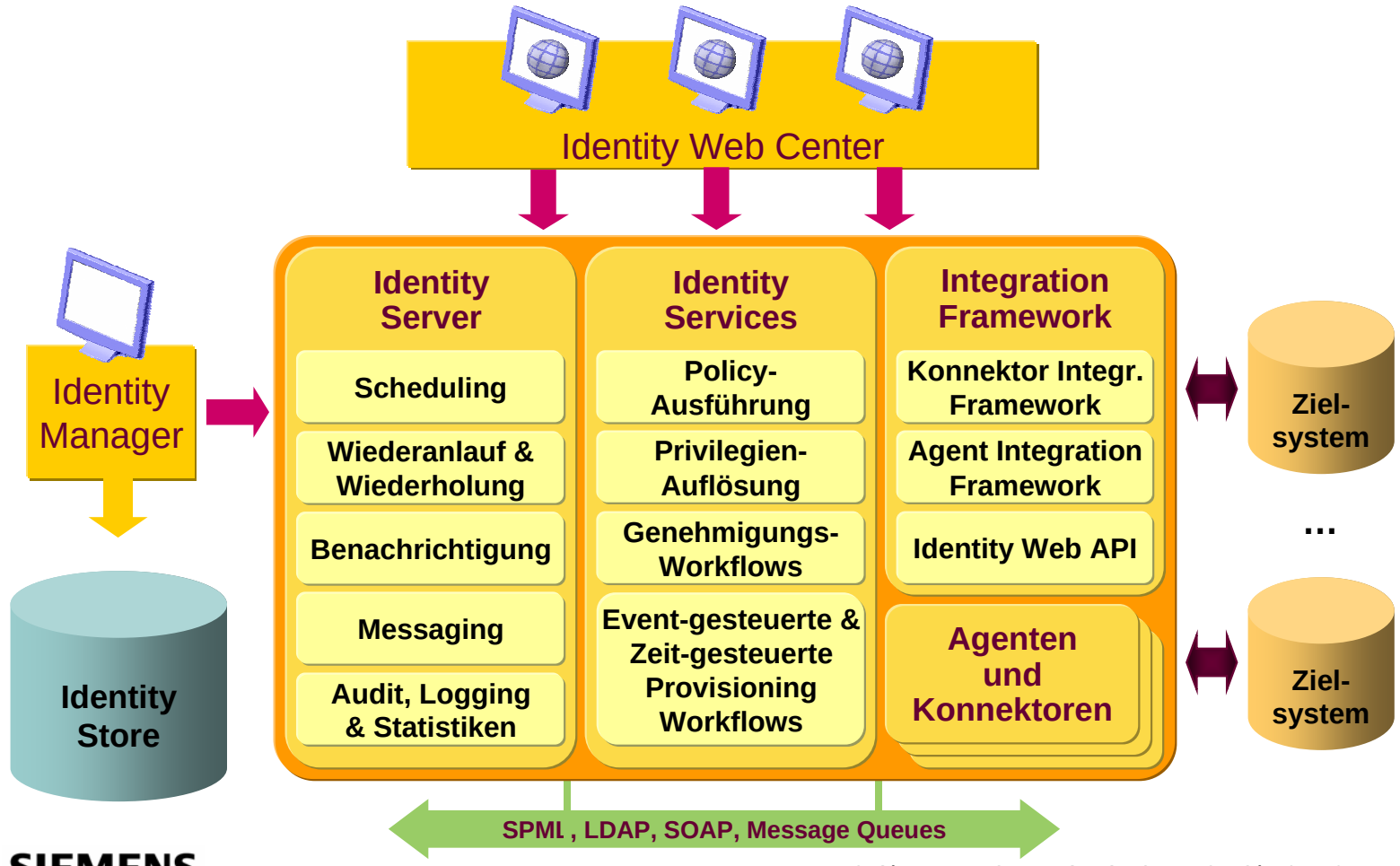
DirX Identity
Funktionen und Aufgaben

Benutzer Self-Service	**Benutzer pflegen eigene Daten und Passwörter, beantragen Rechte, überwachen den Antragsstatus und delegieren Zugriffsrechte an Stellvertreter**
Delegierte Administration	**Ausgewählte delegierte Administratoren verwalten bestimmte Gruppen von Benutzern / Unterstützung von Delegation über mehrere Ebenen**
Passwort-Management	**Administratoren pflegen zentrale Passwortrichtlinien und setzen Passwörter zurück / Benutzer verwenden ein einziges Passwort für alle Anwendungen**
Benutzer-verwaltung	**Pflegen eines zentralen Benutzerverzeichnisses mit aktuellen und konsistenten Daten und Zuweisen von Rechten an Benutzer**
Rechte-verwaltung	**Aufbau eines zentralen und systemübergreifenden Modelles für die Verwaltung von Zugriffsrechten**

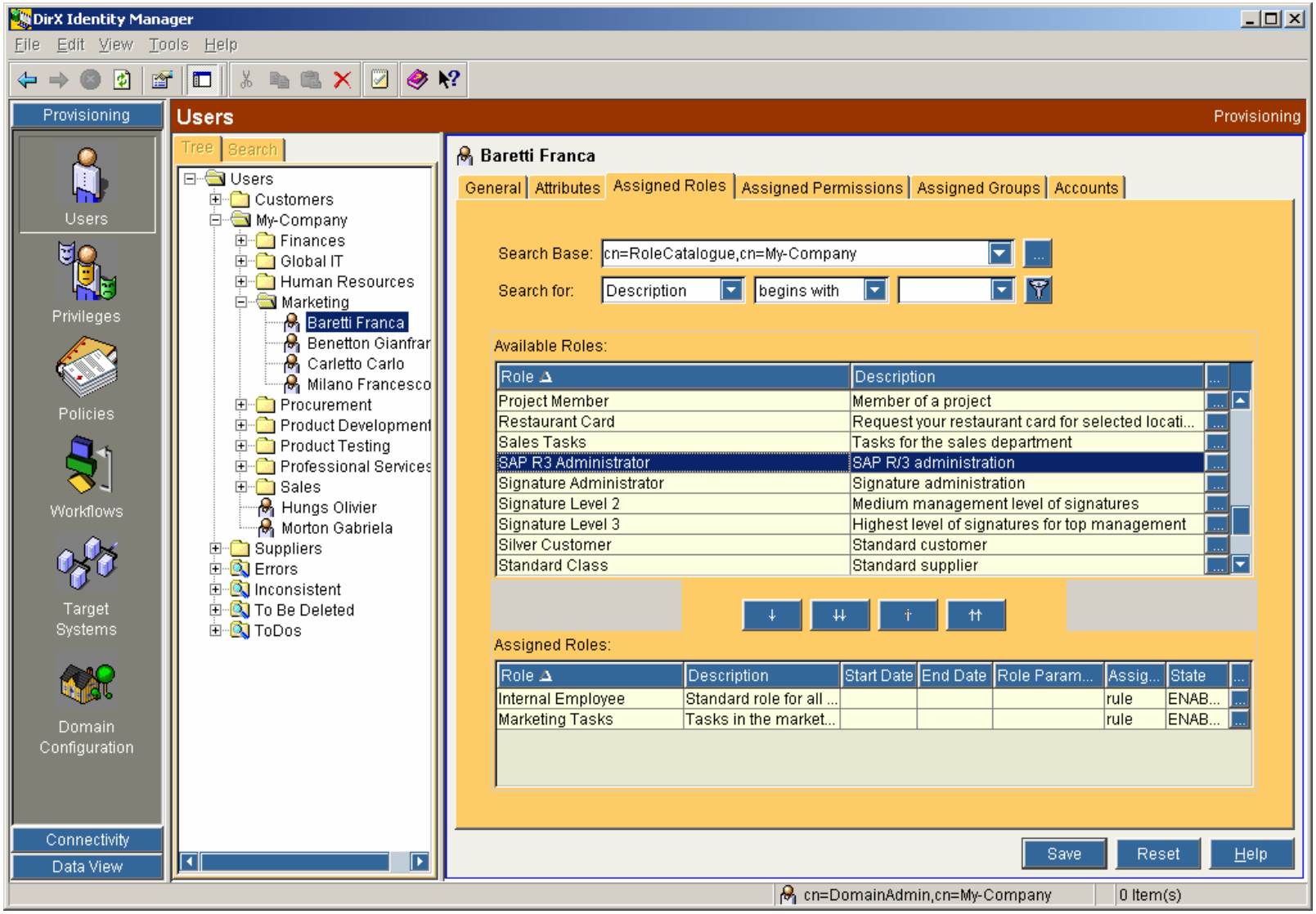
DirX Identity
Funktionen und Aufgaben

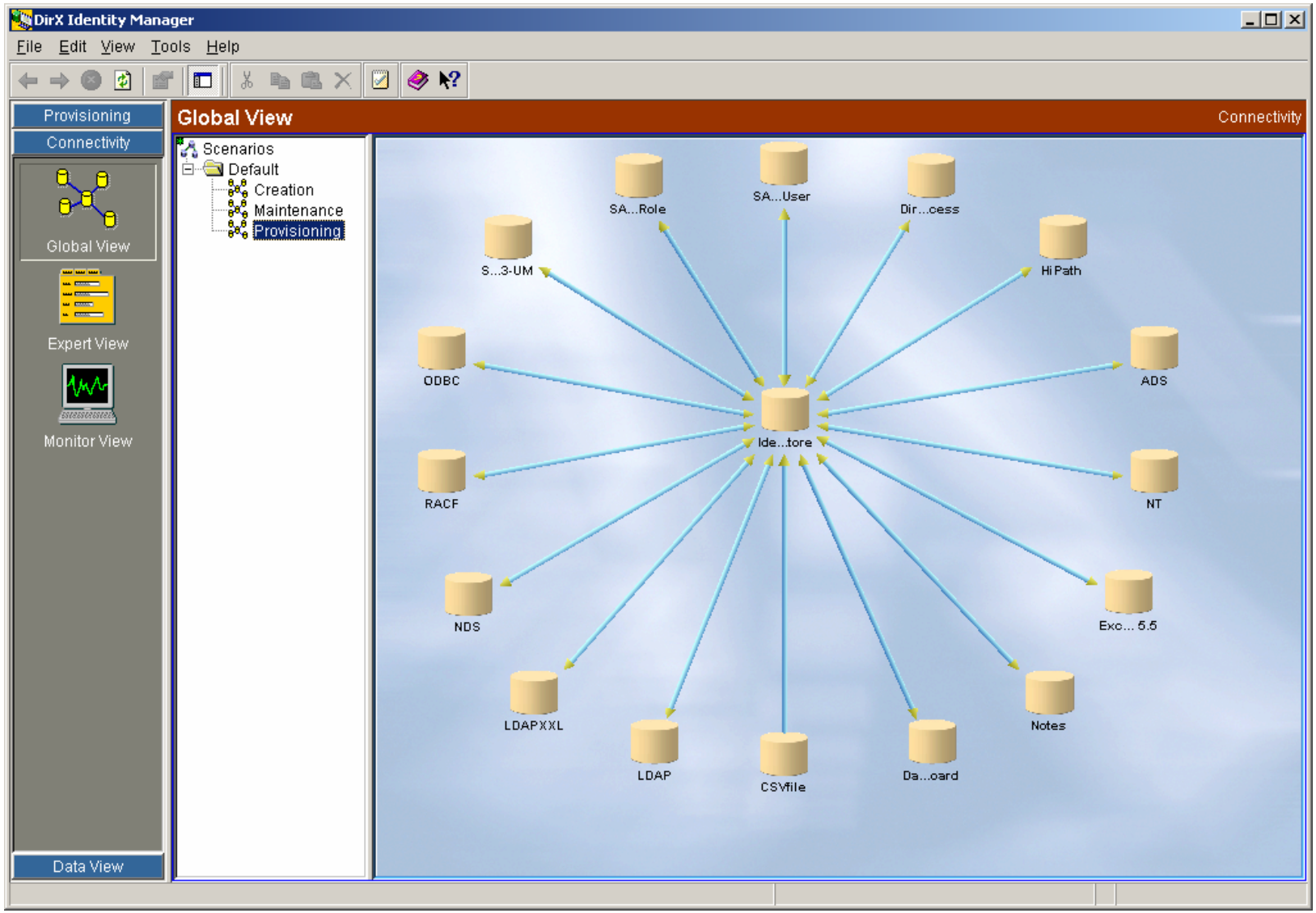
Verwaltung der Richtlinien	**Pflegen von Sicherheits- und administrativen Richtlinien, z.B. Provisioning-Richtlinien für die automatische Vergabe oder den Entzug von Rechten**
Provisioning	**Auflösen von Rechtezuweisungen in systemspezifische Zugriffsrechte und Versorgen der Anwendungen mit Benutzerdaten und Zugriffsberechtigungen**
Metadirectory	**Konsolidierte und konsistente Daten aufbauen durch Integrieren und Synchronisieren von Directories, Benutzerdatenbanken und anderen Datenbeständen**
Audit & Berichte	**Aufzeichnen aller administrativen Änderungen und Erzeugen von Berichten über Benutzer und ihre Zugriffsrechte**
Verwaltung der Mandanten	**Pflege von Mandanten und spezifische Anpassung**

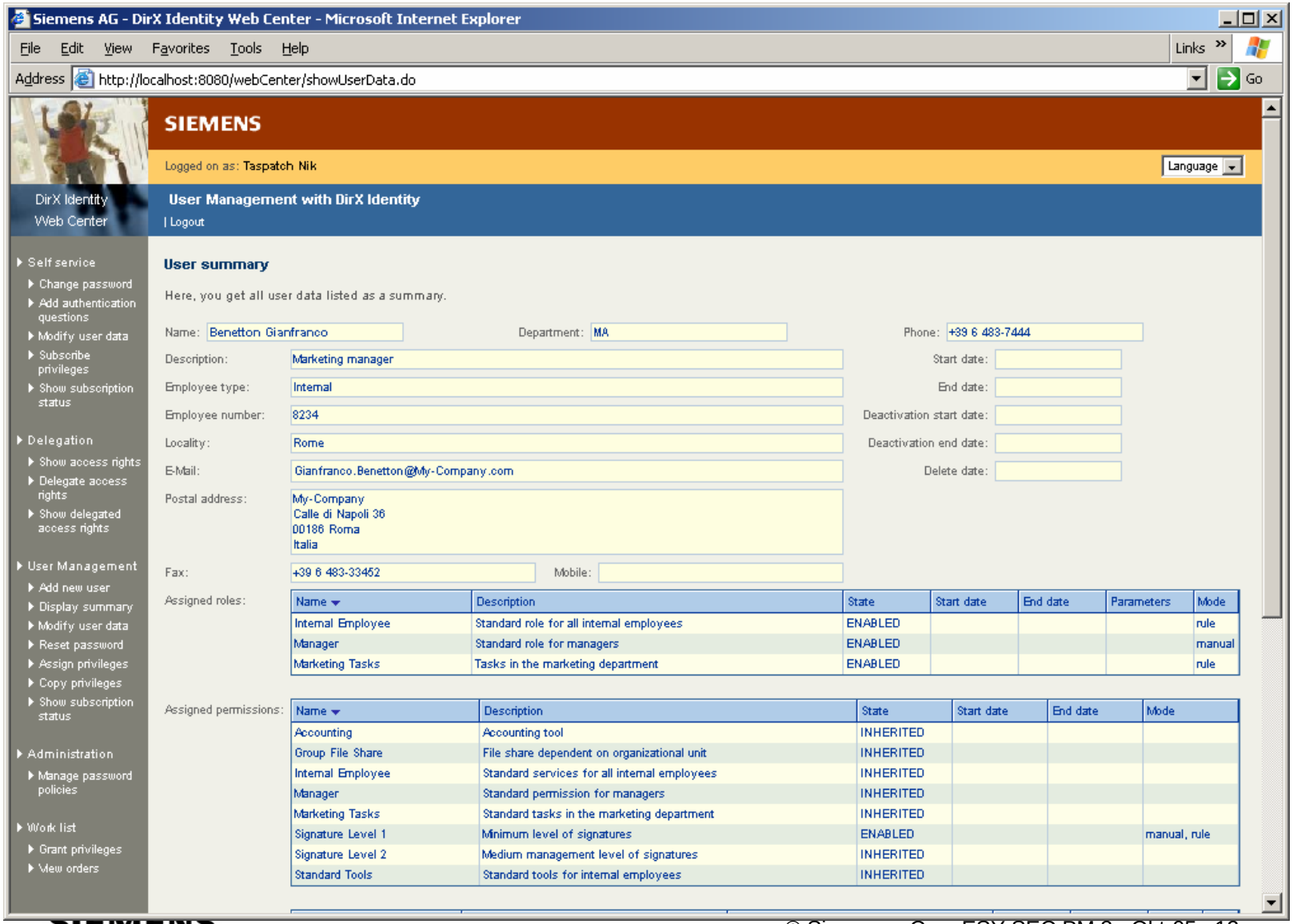
DirX Identity Architektur

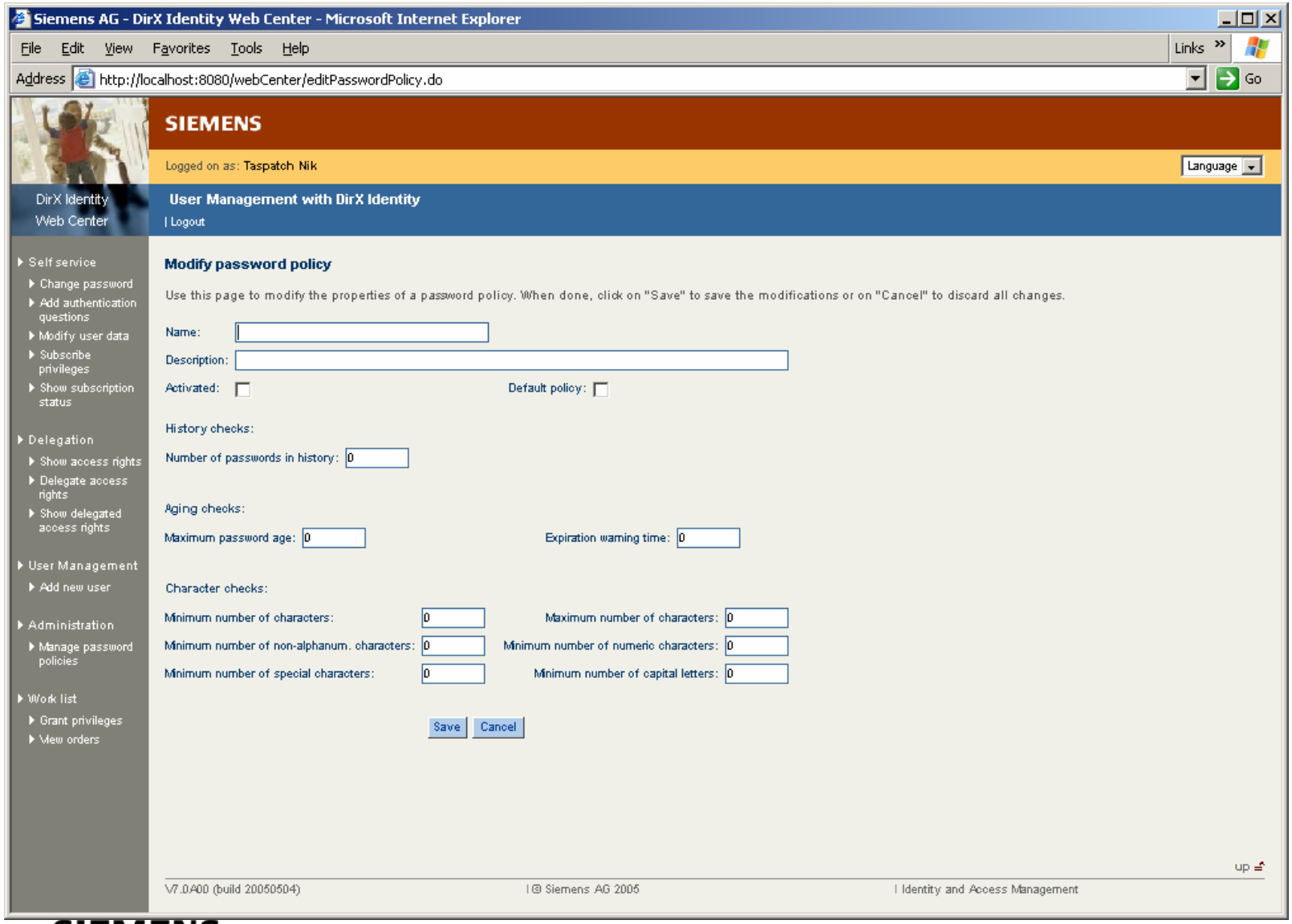


SIEMENS

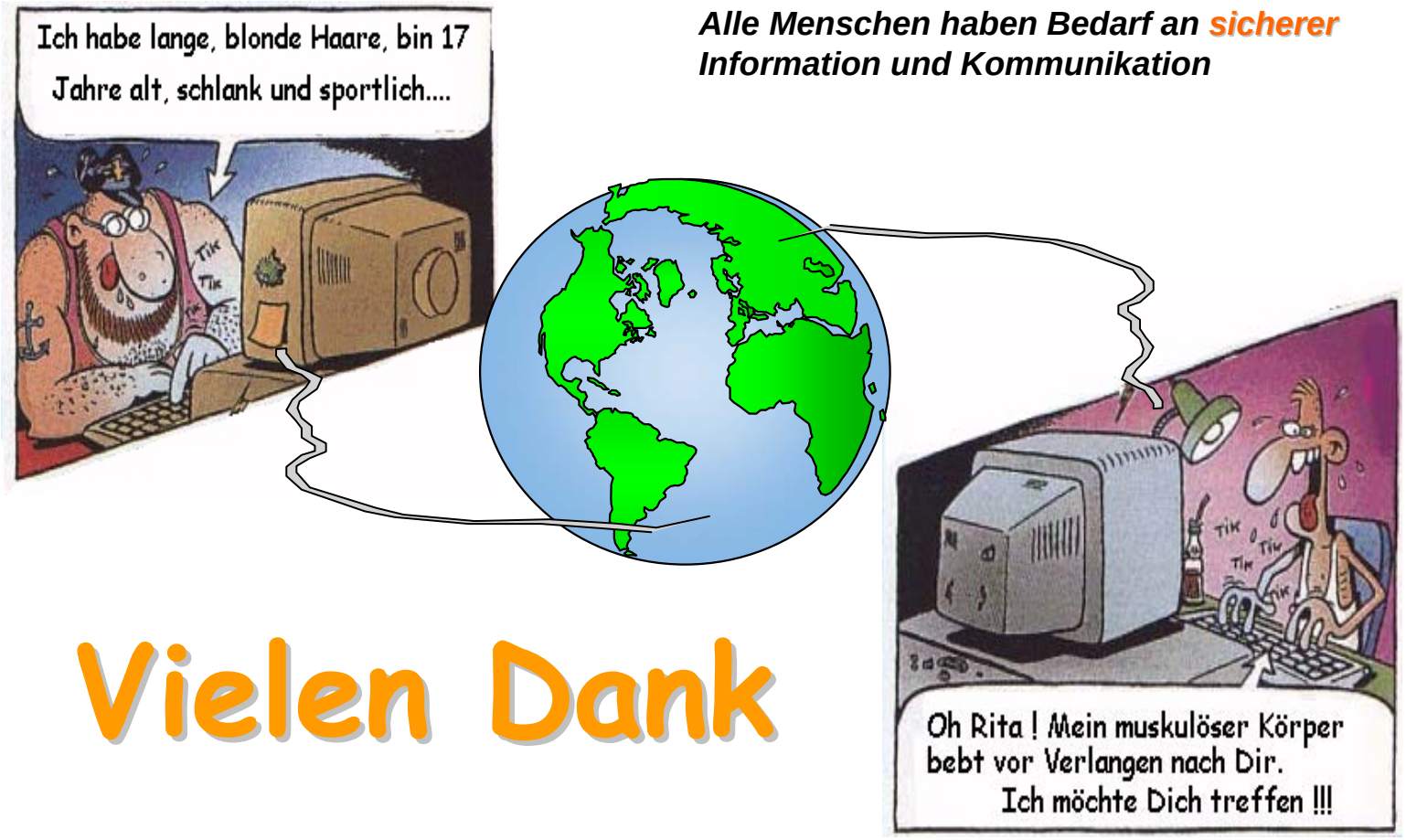

DirX Identity Manager
File Edit View Tools Help
Provisioning
Users
Privileges
Policies
Workflows
Target Systems
Domain Configuration
Connectivity
Data View
Users
Provisioning
Tree Search
Users
Customers
My-Company
Finances
Global IT
Human Resources
Marketing
Baretti Franca
Benetton Gianfrar
Carletto Carlo
Milano Francesco
Procurement
Product Development
Product Testing
Professional Services
Sales
Hungs Olivier
Morton Gabriela
Suppliers
Errors
Inconsistent
To Be Deleted
ToDos
Baretti Franca
General Attributes Assigned Roles Assigned Permissions Assigned Groups Accounts
Search Base: cn=RoleCatalogue,cn=My-Company
Search for: Description begins with
Available Roles:
Role Description
Project Member Member of a project
Restaurant Card Request your restaurant card for selected locati...
Sales Tasks Tasks for the sales department
SAP R3 Administrator SAP R/3 administration
Signature Administrator Signature administration
Signature Level 2 Medium management level of signatures
Signature Level 3 Highest level of signatures for top management
Silver Customer Standard customer
Standard Class Standard supplier
Assigned Roles:
Role Description Start Date End Date Role Param... Assig... State
Internal Employee Standard role for all ... rule ENAB...
Marketing Tasks Tasks in the market... rule ENAB...
Save Reset Help
cn=DomainAdmin,cn=My-Company
0 Item(s)


DirX Identity Manager
File Edit View Tools Help
Provisioning
Connectivity
Global View
Expert View
Monitor View
Data View
Global View
Connectivity
Scenarios
Default
Creation
Maintenance
Provisioning
SA...Role
SA...User
Dir...cess
S...3-UM
HiPath
ODBC
ADS
Ide...tore
RACF
NT
NDS
Exc... 5.5
LDAPXXL
Notes
LDAP
CSVfile
Da...oard


Siemens AG - DirX Identity Web Center - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links
Address http://localhost:8080/webCenter/showUserData.do
Go
SIEMENS
Logged on as: Taspatch Nik
Language
DirX Identity
Web Center
User Management with DirX Identity
| Logout
Self service
Change password
Add authentication questions
Modify user data
Subscribe privileges
Show subscription status
Delegation
Show access rights
Delegate access rights
Show delegated access rights
User Management
Add new user
Display summary
Modify user data
Reset password
Assign privileges
Copy privileges
Show subscription status
Administration
Manage password policies
Work list
Grant privileges
View orders
User summary
Here, you get all user data listed as a summary.
Name: Benetton Gianfranco
Department: MA
Phone: +39 6 483-7444
Description: Marketing manager
Start date:
Employee type: Internal
End date:
Employee number: 8234
Deactivation start date:
Locality: Rome
Deactivation end date:
E-Mail: Gianfranco.Benetton@My-Company.com
Delete date:
Postal address: My-Company
Calle di Napoli 36
00186 Roma
Italia
Fax: +39 6 483-33452
Mobile:
Assigned roles:
Name | Description | State | Start date | End date | Parameters | Mode
Internal Employee | Standard role for all internal employees | ENABLED | rule
Manager | Standard role for managers | ENABLED | manual
Marketing Tasks | Tasks in the marketing department | ENABLED | rule
Assigned permissions:
Name | Description | State | Start date | End date | Mode
Accounting | Accounting tool | INHERITED
Group File Share | File share dependent on organizational unit | INHERITED
Internal Employee | Standard services for all internal employees | INHERITED
Manager | Standard permission for managers | INHERITED
Marketing Tasks | Standard tasks in the marketing department | INHERITED
Signature Level 1 | Minimum level of signatures | ENABLED | manual, rule
Signature Level 2 | Medium management level of signatures | INHERITED
Standard Tools | Standard tools for internal employees | INHERITED


Siemens AG - DirX Identity Web Center - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links
Address http://localhost:8080/webCenter/editPasswordPolicy.do
Go
SIEMENS
Logged on as: Taspatch Nik
Language
DirX Identity Web Center
User Management with DirX Identity
| Logout
Self service
Change password
Add authentication questions
Modify user data
Subscribe privileges
Show subscription status
Delegation
Show access rights
Delegate access rights
Show delegated access rights
User Management
Add new user
Administration
Manage password policies
Work list
Grant privileges
View orders
Modify password policy
Use this page to modify the properties of a password policy. When done, click on "Save" to save the modifications or on "Cancel" to discard all changes.
Name:
Description:
Activated:
Default policy:
History checks:
Number of passwords in history: 0
Aging checks:
Maximum password age: 0
Expiration warning time: 0
Character checks:
Minimum number of characters: 0
Maximum number of characters: 0
Minimum number of non-alphanum. characters: 0
Minimum number of numeric characters: 0
Minimum number of special characters: 0
Minimum number of capital letters: 0
Save
Cancel
up
V7.0A00 (build 20050504)
| © Siemens AG 2005
| Identity and Access Management

Alle Menschen haben Bedarf an sicherer Information und Kommunikation



Vielen Dank

DirX Identity
Features

DirX Identity stellt eine umfassende Identity Management Lösung für Unternehmen und Organisationen zur Verfügung. DirX Identity enthält

- Web-basierte Benutzer-Self-Service-Funktionen und delegierte Administration
- Passwort-Management and -Synchronisation
- Benutzerverwaltung
- Privilegienverwaltung mit Rollen, Berechtigungen und Gruppen
  - Basieren auf dem NIST RBAC Modell mit Rollenhierarchien
  - Rollen- und Berechtigungsparameter
- Manuelle oder automatische, Regel-basierte Zuweisung von Privilegien an Benutzer
- Genehmigungs-Workflows für Zuweisungen von Privilegien
- System-übergreifendes Provisioning von Benutzer/Accounts, Gruppen, und Benutzer-Gruppen-Beziehungen
  - Initiales Laden, Zeit-gesteuerte Synchronisation, Validierung und Abgleich
- Zielsystemverwaltung
- Mandantenfähigkeit
- Funktionen zur Überwachung des Systems, für Audit-Zwecke und Report-Erstellung
- Metadirectory
- Umfangreiche grafische Administrations- und Benutzer-Schnittstellen

DirX Identity
Passwort-Management

DirX Identity Passwort-Management stellt eine konsistente und einfache Anmeldung für die unterstützten Zielsysteme bereit:

- Identische Passwörter in allen Zielsystemen durch sofortige Passwort-Synchronisation
- Web Center unterstützt
  - Benutzer-Self-Service zum Ändern und Rücksetzen von Passwörtern
  - Administratives Zurücksetzen von Passwörtern
- Benachrichtigung über bevorstehende erforderliche Passwort-Änderungen auf Grund von Passwort-Policies
- Password Listener für Windows zum Erkennen von Passwort-Änderungen, die über den Windows Desktop durchgeführt werden
- Sichere Speicherung und sicherer Transport von Passwörtern
- Verwaltung von Passwort-Policies

DirX Identity
Metadirectory

- **Integration von heterogenen Verzeichnissen und Datenbanken in ein LDAP Verzeichnis, z.B. DirX**
  - Einstufige, skriptfähige Join Engine mit dedizierten und generischen Agenten
  - Basiert auf dem Datenintegrations-Paradigma „Extract, Transform, Move, Load“ (ETML)
  - Asynchrone Verarbeitung im Hintergrund
  - Steuerung durch Metadaten, Verwaltung über grafische Oberfläche
  - Bi-direktionale Synchronisation mit vielen, unterschiedlichen Quellen und/oder strukturierten Dateien (XML, LDIF, CSV)

- **Anwendungsnutzen**
  - Konsistenz und Datenintegrität
  - Konsolidierte Directory-Daten
  - Infrastruktur für Provisioning und Identity Management

- **Wird seit vielen Jahren erfolgreich in Projekten eingesetzt**

DirX Identity Server
Highlights

- Skalierbares, Multi-Thread Framework als Komponenten-Container; gemeinsames Framework für Server und Agenten
- Ermöglicht verteilte Installation von Komponenten und Agenten
- Zeit- und Event-gesteuerte Ausführung von Synchronisations- und Provisioning-Workflows
- Status-Tracking, Ausnahmebehandlung und Wiederanlauf
- Steuert den Meta Controller (Script-fähige Join Engine)
- Optionale Verschlüsselung von Attributen (z.B. Passwörter)
- Läuft mit DirX und Sun LDAP Servern
- Plattform-unabhängig: Windows 2000/2003/XP, Solaris (Sparc), Linux (Red Hat / SuSE)
- Identity Integration Framework für Java und C
- Unterstützt Hochverfügbarkeit (Supervisor, Hardware-Cluster Unterstützung)

DirX Identity Manager
Features

- Einfach zu bedienende Administrationsschnittstellen mit mehreren Views zur
  - Verwaltung der Identitäten und Privilegien (Provisioning)
  - Verwaltung der Synchronisations- und Provisioning-Workflows (Konnektivität)
  - Anzeige des Objektmodells im Identity Store (Data View)
- Graphische Repräsentation und Konfiguration der Objekte und Prozeduren
- „State of the art“ Java Technologie, Plattform-unabhängig
- LDAP-basierte zentrale Datenhaltung für Konfigurations- und Meta-Daten für die GUI und den Administrationsprozess
- Überwachung (Monitoring) der Synchronisations- und Provisioning-Jobs, Audit und Trace
- Kontext-sensitive Online-Hilfe
- Graphische Modellierung der Synchronisations- und Provisioning-Workflows
- Schema-Erkennung von angeschlossenen Directories

DirX Identity V7.0A00
Neue Funktionen

- Zusammenführung von DirXmetahub und DirXmetaRole mit einer optimierten Produktstruktur
- Verfügbarkeit auf zusätzlichen Plattformen: Linux (Red Hat, SuSE)
- Unterstützung von Sun LDAP-Servern als Datenhaltung für DirX Identity
- Passwort-Management
- Event-basierter Identity Server
- Identity Integration Framework für Java und C++
- Neue Konnektivität:
  - System im Gesundheitswesen (Health Enterprise Dashboard)
  - Zugangskontrollsysteme (SiPass)
  - Rollen-basiertes Provisioning für IBM Lotus Notes
- Verbesserte Integration zwischen DirX Access und DirX Identity

DirX Identity V7.0
Business und Pro Suites

Funktionen	Pro	Business	Pro Up.
Regelbasiertes Provisioning (Benutzer und Gruppen)	X	X	
Metadirectory / Synchronisation	X	X	
Web Center mit Benutzerselbstverwaltung	X	X	
Grafische Administration (Identity Manager)	X	X	
Identity integration framework für Java und C++	X	X	
Passwort-Synchronisation	X	X	
Rollenbasiertes Provisioning (RBAC, Rollenhierarchie, Parameter)	X		X
Antrags- und Genehmigungsworkflow	X		X
Delegierte Administration	X		X
Passwort-Management / Richtlinien / Self-Service	X		X
Rechteverwaltung (Rollen und Berechtigungen)	X		X
Audit / Historie	X	Basis	X

DirX Identity V7.0
Connectivity Packages

- **Standard**
  LDAP, HiPath SIcurity DirX Access, Files, XML
- **Microsoft**
  ADS, NT, Exchange, Windows Password Listener
- **Datenbanken**
  Relationale Datenbanken über ODBC, JDBC
- **HiPath**
  HiPath 4000 Manager, Hicom DMS
- **Medizinische Informationssysteme**
  Health Enterprise Dashboard
- **Gebäudezugang**
  SiPass
- **SAP**
  R/3 und mySAP ERP HR, OM, UM/CUA, NetWeaver/Enterprise Portal 6
- **IBM**
  RACF, Lotus Notes