

SAP NetWeaver Identity Management

Dr. Peter Gergen

Presales Specialist Identity Management
Platform Solutions

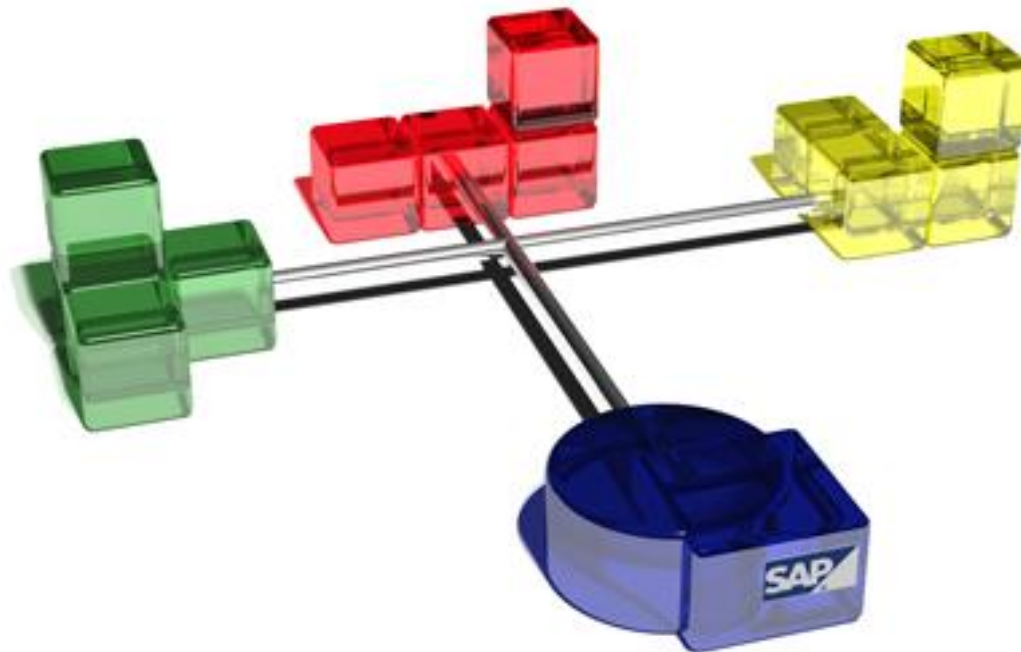
SAP Deutschland

THE BEST-RUN BUSINESSES RUN SAP™



1. Überblick

2. Features, Funktionen, Architektur
3. Typische Szenarien
4. Demo



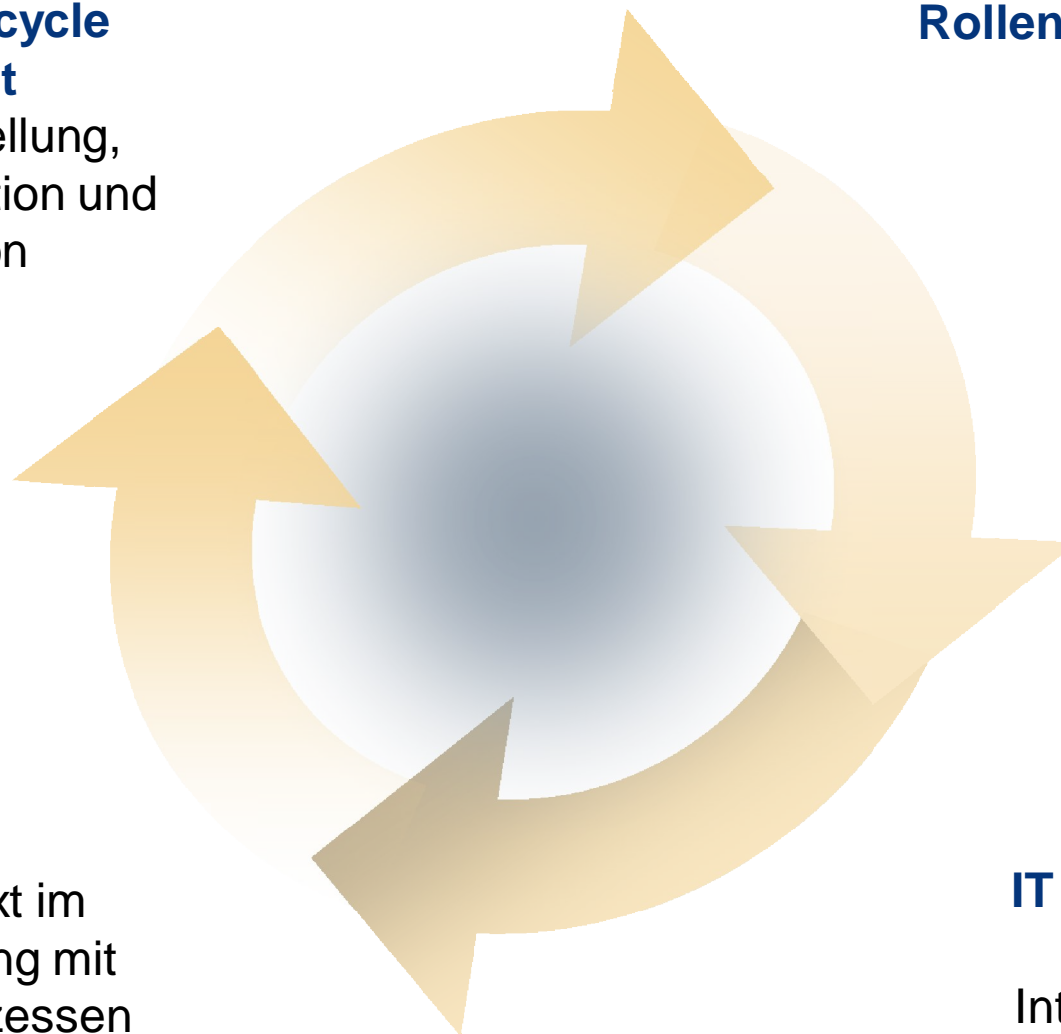


Identity Lifecycle Management

Identity-Erstellung,
Synchronisation und
Administration

Rollen & Regel-basiertes Provisioning

Wem ist wann was
gestattet?



eSOA

Identity Kontext im
Zusammenhang mit
Geschäftsprozessen

Compliance & IT Risk Management

Audit & Reporting,
Interfacing mit Risiko-
Analyse

Lebenszyklus einer Identität im Unternehmen



Einstellungsdatum:

Erster Arbeitstag von Tim Krüger

Verfügbar:

temp. E-Mail-Account



3 Wochen später:

Tim Krüger arbeitet bei der Lohnbuchhaltung

Verfügbar:

Portal, E-Mail, Internet, Gehaltsliste



1 Jahr später:

Tim Krüger wechselt in den Vertrieb

Manuelle Anträge auf Berechtigungen durch neuen Manager

Verfügbar:

Portal, E-Mail, Internet, Siebel, Gehaltsliste, Marketing (west)

7 Jahre später:

Tim Krüger wird neuer Vice President Sales.

Er fordert neue Berechtigungen an:

Verfügbar:

Portal, E-Mail, Internet, Gehaltsliste, Siebel, Marketing (global)



8 Jahre später:

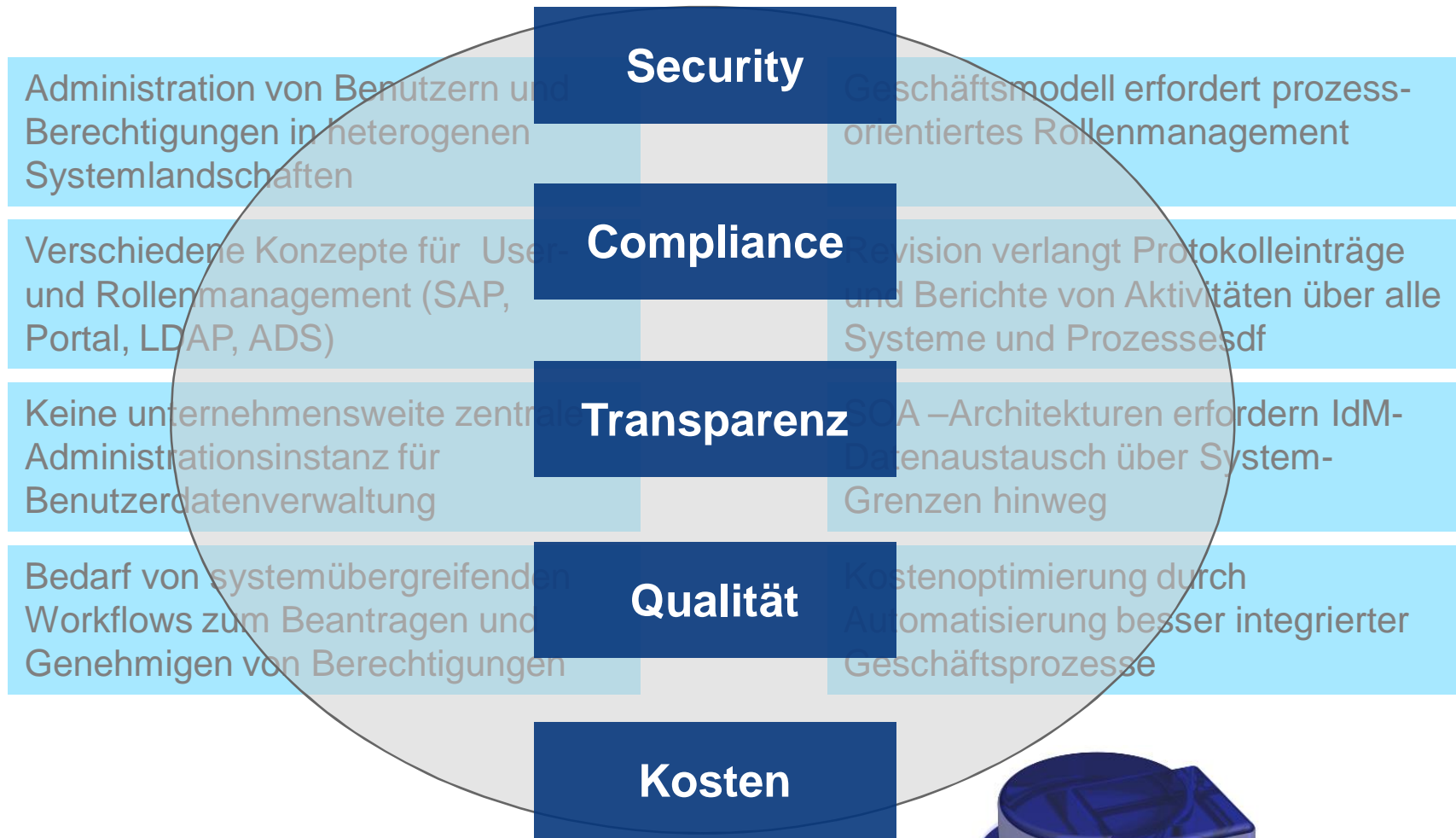
Tim Krüger verläßt das Unternehmen



10 Jahre später :

Revision entdeckt: **TKRUEGER**
Hatte wiederholten Zugriff auf
Sales-Information innerhalb der
Letzten 2 Jahre

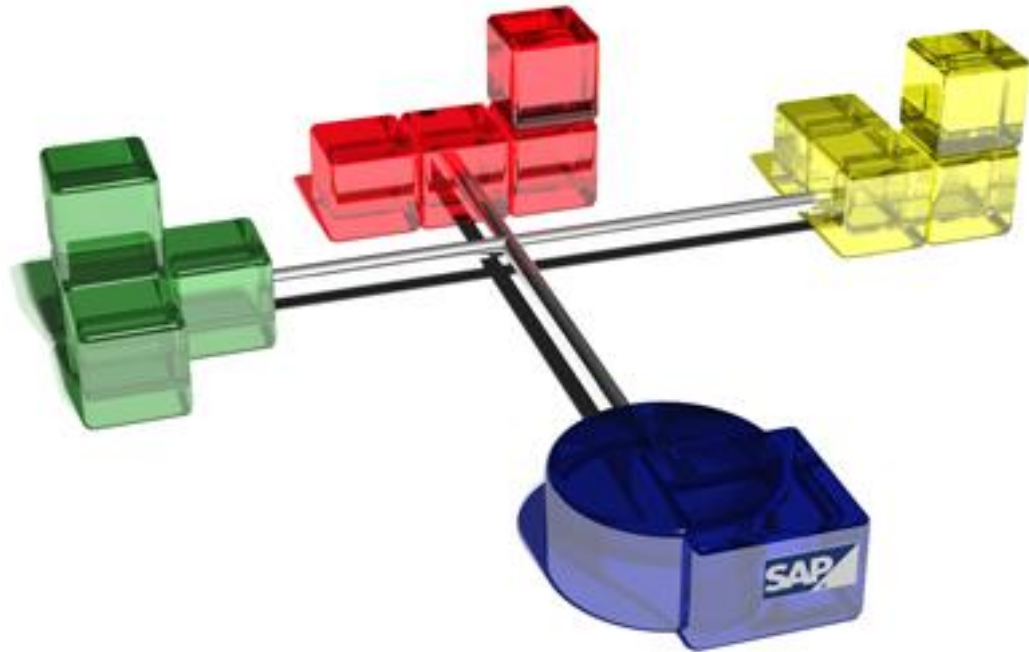




SAP Netweaver
Identity Management



1. Überblick
2. **Features, Funktionen, Architektur**
3. Typische Szenarien
4. Demo



SAP NetWeaver Identity Management:

Integraler Bestandteil der SAP NetWeaver Technology-Plattform

- Management personenbezogener Daten
- SAP Welt + heterogene Systemlandschaften
- integriert in NetWeaver Plattform und in Business Applikationen
- Ergänzt SAP NetWeaver Security Frameworks



SAP NetWeaver Identity Management Komponenten



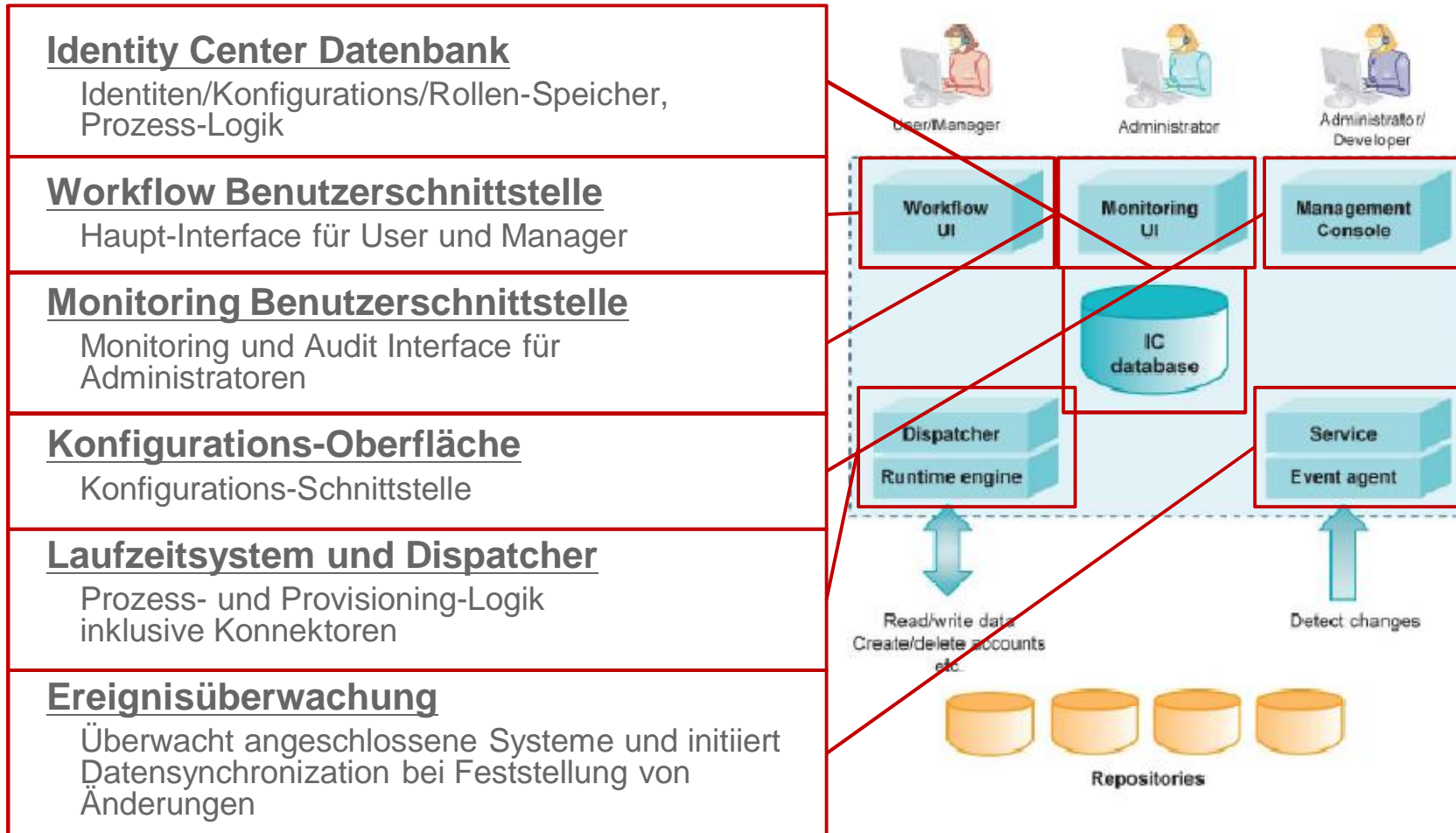
SAP NetWeaver Identity Management:

Komponenten:

1. **Identity Center**
2. Virtual Directory Server



Identity Center: Architektur

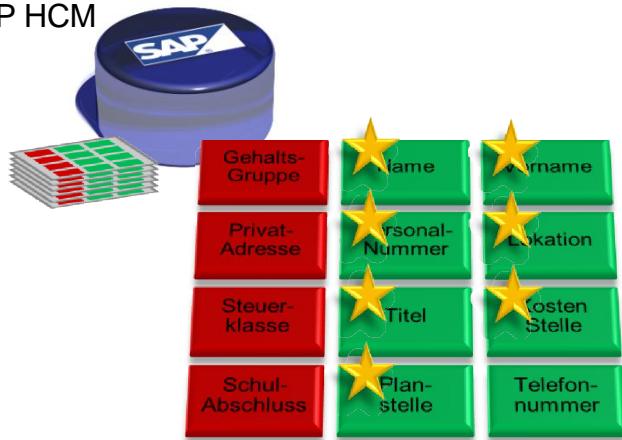


Datensynchronisation



Private und "shared" Attribute, Datenhoheit

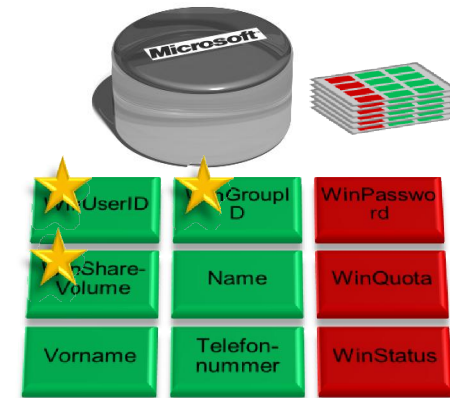
SAP HCM



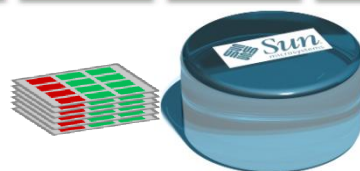
SAP Netweaver Identity Management



MS Active Directory



Corporate Directory



Lagerbestands-DB



Manuelle Interaktion durch Browser

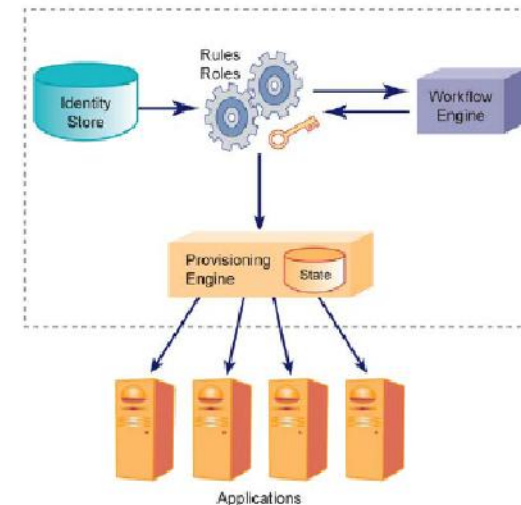
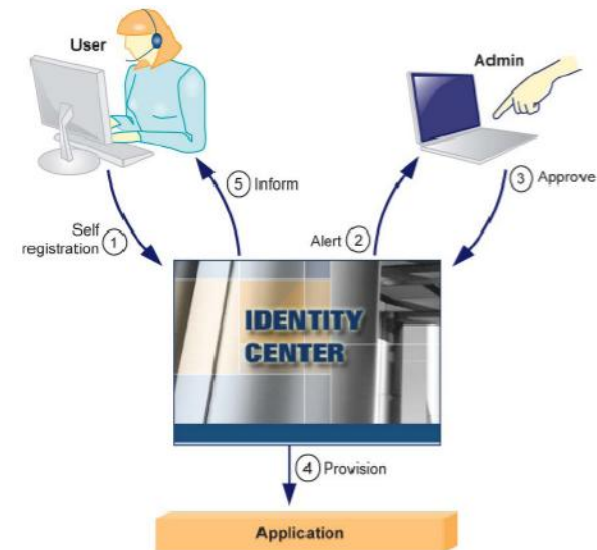
- Starte Provisionierungsaufgaben
- Genehmige Berechtigungszuweisungen
- Statuskontrolle

Workflows startbar über

- Webschnittstelle (Browser)
- Ereignissteuerung im IdM
- Änderung von Berechtigungszuweisungen

Prozesslogik

- Sequenziell
- Parallel
- Konditional
- Genehmigungsschritte



Rollendefinition und Berechtigungsprovisionierung

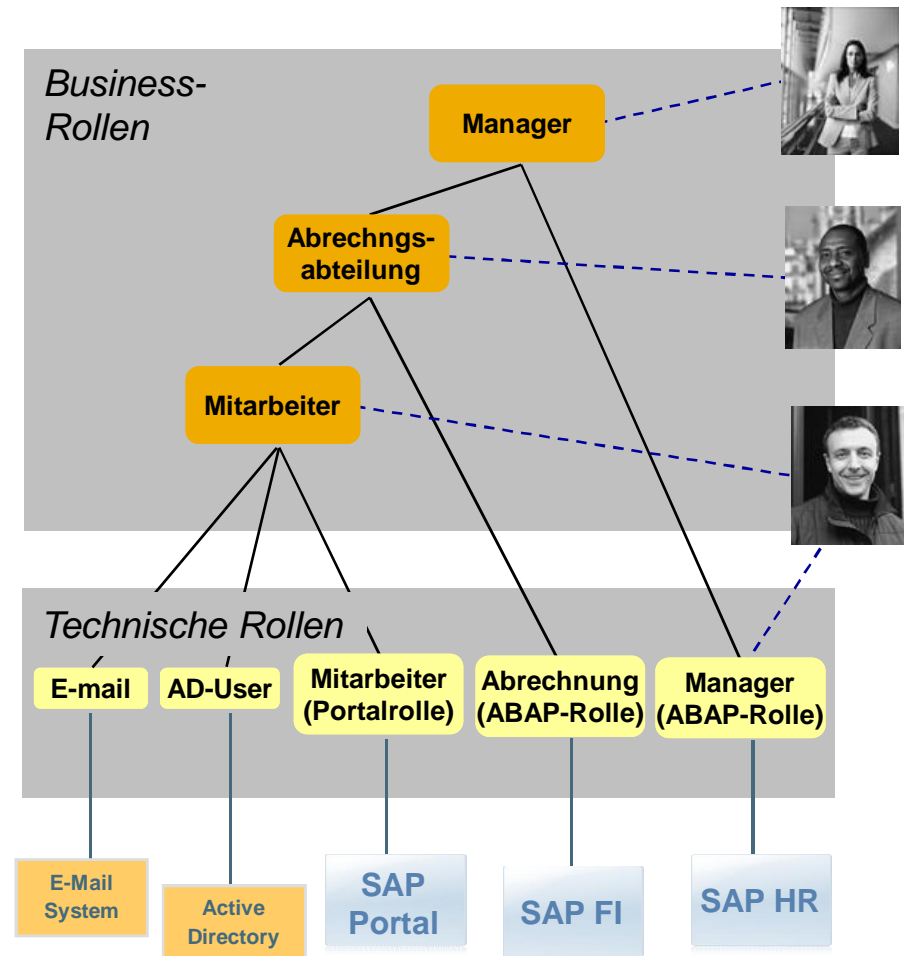


Businessrollen

- Werden im Identity Center definiert
- Repräsentieren die Aufgaben eines Mitarbeiters
- Werden oft im Rahmen eines Organisationsprozesses beschrieben
- Können hierarchisch strukturiert sein
- Sind eine Kombination von technische Rollen und/oder untergeordneten Businessrollen
- Werden Benutzern zugewiesen

Technische Rollen

- Repräsentieren die Rollen aus dem Zielsystem (bzw. Technische Berechtigungen)
- Werden von den Zielsystemen importiert
- Sind systemspezifisch



Protokollierung und Auditing



Bezogen auf Applikationen/Privilegien

- Wer hat Zugriff auf welches System?

Bezogen auf Nutzer

- Welche Berechtigungen/Rollen hat ein Nutzer?

Berichte können regelmäßig oder auf Anfrage generiert werden

Stammdatenstand und -änderungen

- Derzeitiger Stand, früherer Stand, Änderungshistorie, Prüfkennzeichen

Genehmigungsdaten

- Wer hat wann was genehmigt?

Prozess/Aufgabenaufzeichnungen

- Welcher IdM-Prozess wurde wann durch welchen Benutzer aufgerufen?

Allgemeine Aufzeichnungsdaten zu IdM-Prozessen

Access control history
User: 3020 Christopher Wright
Date: 11.03.2005

3020 Christopher Wright
Period: 2004-12-01 2005-02-28
1092 Accounting system

Access	Period	Approval data	Approver
Reporting	2004-12-01 - 2004-12-31	2004-06-01	3031 Sarah Davies
Full access	2005-01-01 - 2005-02-28	2005-01-01	3031 Sarah Davies

1093 E-mail account

Access	Period	Approval data	Approver
Normal e-mail account	2004-12-01 - 2005-02-28	2004-01-01	3026 Daniel Brown

Access control history
System: 1092 Accounting system
Date: 11.03.2005

1092 Accounting system
Period: 2005-01-01 2005-02-28

Full access

The following persons have full access to the accounting system.

EmployeeID	Name	Period
3005	Allison Clarke	2005-01-01 - 2005-01-31
3020	Christopher Wright	2005-01-01 - 2005-02-28

Reporting

The following persons can produce reports from the accounting system.

EmployeeID	Name	Period
3001	Lisa Andersson	2005-01-01 - 2005-01-31
3008	David Kelly	2005-01-01 - 2005-02-28
3010	Betsy Rogers	2005-01-01 - 2005-02-28
3013	Elizabeth Burns	2005-01-01 - 2005-02-28
3025	Daniel Brown	2005-01-01 - 2005-02-28
3026	Hannah Green	2005-02-01 - 2005-02-28
3048	Brittany Jackson	2005-01-01 - 2005-02-28

Microsoft Active Directory
Microsoft ADAM
IBM Tivoli Directory
Novell eDirectory
SunONE Java Directory
Oracle Internet Directory
Siemens DirX
OpenLDAP

CA eTrust Directory
SAP NetWeaver Virtual Directory Server
Any LDAP v3 compliant Directory

Microsoft Exchange
Lotus Domino

SAP (ABAP, Java including Portal)

RSA Cleartrust
RSA SecureID

Microsoft Access
Microsoft SQL Server
Sybase
IBM UDB (DB2)
MySQL
Oracle Database
Any JDBC-enabled database

Microsoft Windows NT
Microsoft MIIS
Unix/Linux

SPML (Services Provisioning Markup
Language)
DSML (Directory Services Markup
Language)
CSV files
LDIF files
XML files
Shell execute
Custom Java Connector API

SAP NW Identity Management:

Komponenten:

1. Identity Center
2. **Virtual Directory Server**



Virtual Directory Server

Der Virtual Directory Server (VDS) bietet

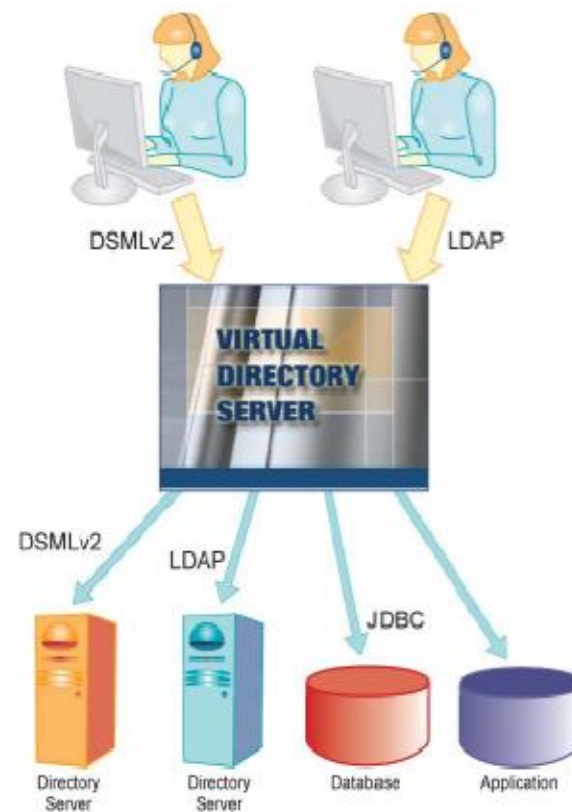
- Eine konsistente Sicht auf viele, verteilte Identitätsdatenquellen
- Nutzerinformation als „Dienst“ für Applikationen mittels Standardprotokollen (LDAP, DSMLv2)
- Abstraktionsschicht

Anwender sieht nur Standardschnittstelle (LDAP)

- Transformiere einkommende LDAP-Anfragen und leite diese direkt an die richtigen Datenquellen weiter
 - Datensätze verbleiben in Quellsystemen (anders als IC)
 - Effizientes Caching

Eigenschaften

- Echtzeitzugriff auf Nutzerdaten (anders als IC)
- Datenquellen bleiben separiert, keine Konsolidierung notwendig
- Kein extra Datenspeicher/Datenbank
 - Schnelle Integration über LDAP
 - Einfache Wartung
- Attributmanipulation
- Namensraumänderungen



SAP NW IdM – vorläufige Roadmap



Business Process Integration

Management of identities and roles concerning business aspects of identity

- Provisioning to applications based on NW AS ABAP and NW AS Java
- SAP integration framework (templates)
- HCM integration (batch)

- GRC integration scenarios
- Improved HCM integration

- Event-driven HCM import
- Extended GRC integration
- Application and industry specific identity aspects
- SAP integration framework extensions

Business process driven identity & business role management

- Standard service interface support (LDAP)

- Additional standard services (DSML, SPML)

- Extended identity services API

Identity enterprise services

Heterogeneous landscape support

Integration with non-SAP systems and applications

- Out-of-the-box connectors and extension framework for non-SAP systems
- Open interface for non-SAP business applications

- Extension via additional standard support, partner eco-system or customer projects

- SSO infrastructure integration
- Portal UI integration

- CUA connectivity

- Workflow NetWeaver UI
- Additional
 - NetWeaver Admin
 - Universal Work List
 - Further to be finalized

Extend NetWeaver integration

This presentation and SAP's strategy and possible future developments are subject to change and may be changed by SAP at any time for any reason without notice

NW IDM 7.0 SP1

Q4/2007

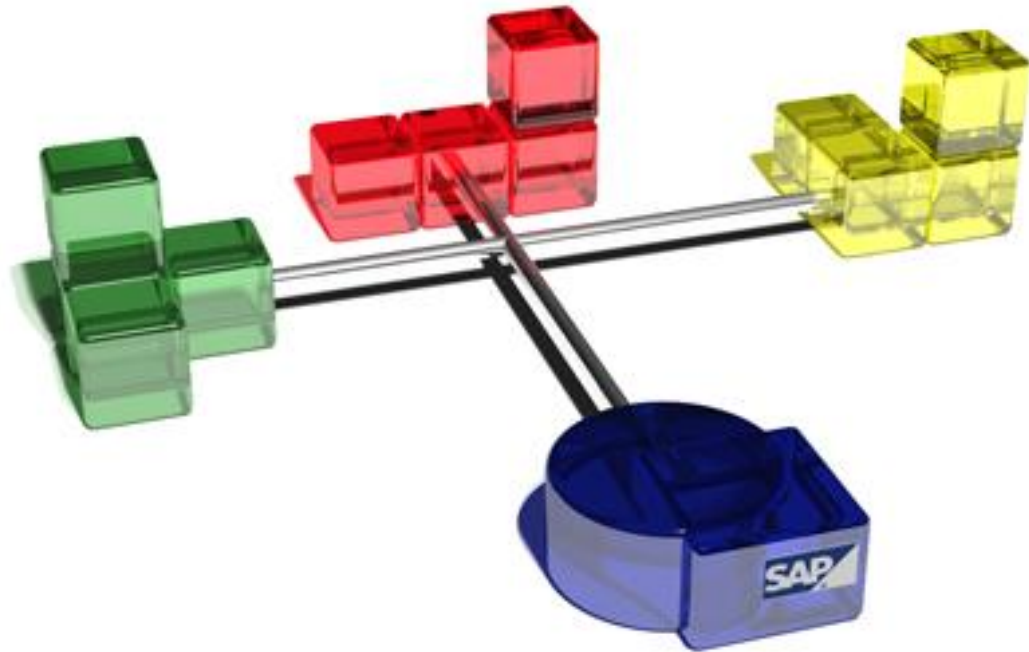
H1/2008

2008

2009



1. Überblick
2. Features, Funktionen, Architektur
- 3. Typische Szenarien**
4. Demo



Identity Management (IdM)

- bisher

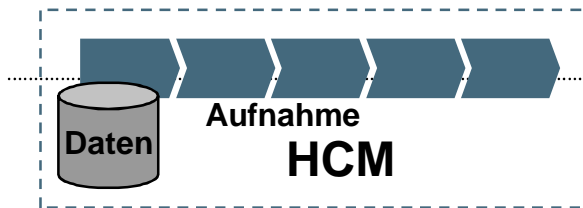


IDM sollte durch beteiligte Organisationsprozesse gesteuert werden



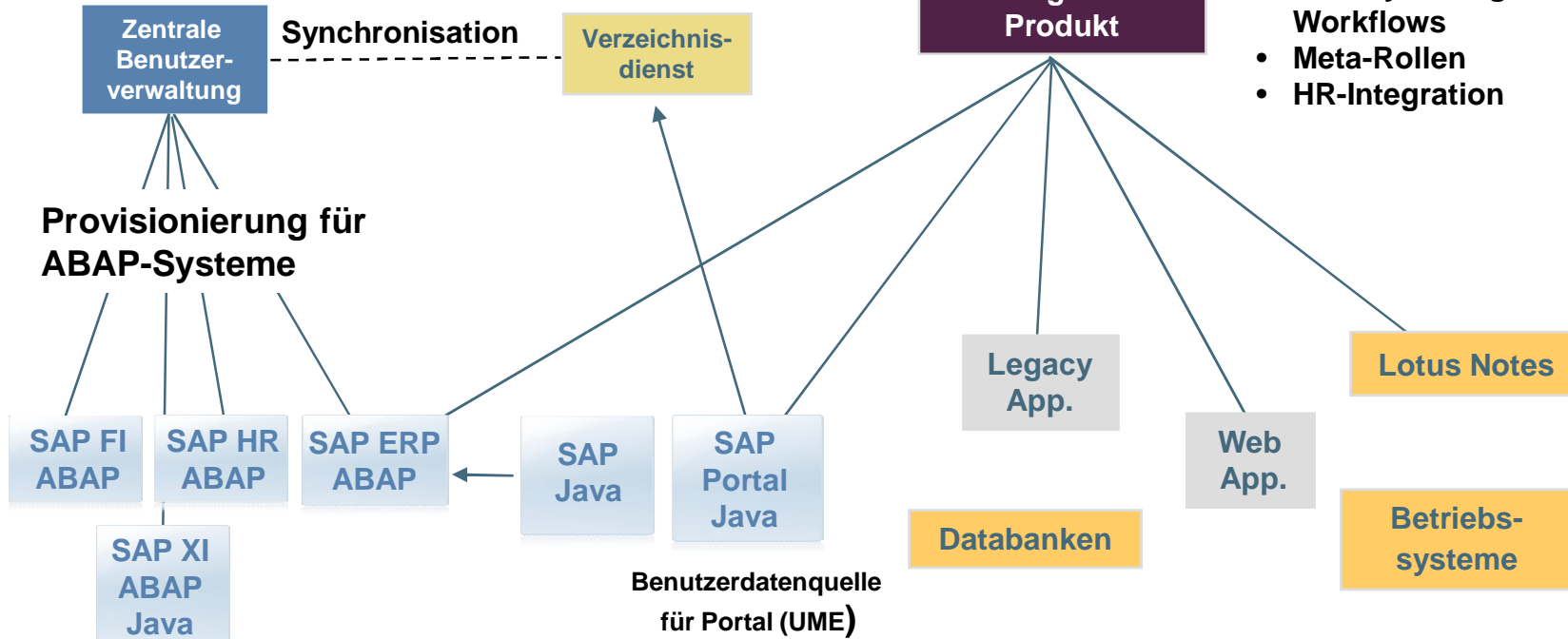
z.B. Personaladministration

Prozesse und Tätigkeiten benötigen korrekte Benutzer- und Rechte- zuweisungen für Systeme



Separates Identity Management Produkt

- Identitätsprovisionierung für SAP and nicht-SAP-Systeme
- Identity-Management-Workflows
- Meta-Rollen
- HR-Integration



SAP NetWeaver Identity Management 7.0

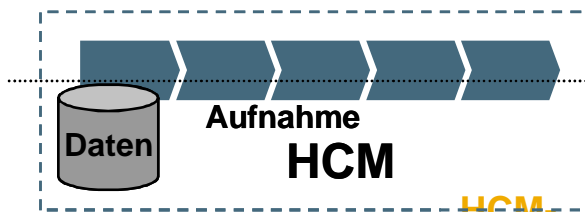


IDM sollte durch beteiligte Organisationsprozesse gesteuert werden



z.B. Personaladministration

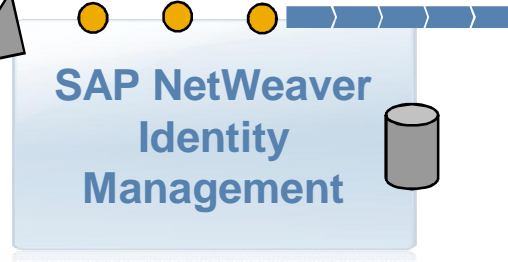
Prozesse und Tätigkeiten benötigen korrekte Benutzer- und Rechte-zuweisungen für Systeme



HCM-Integration

Identitätsvirtualisierung und Identitätsdienste mittels Standardschnittstellen

Genehmigungsprozesse



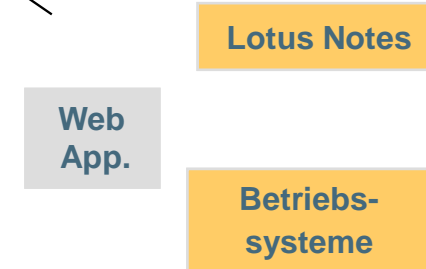
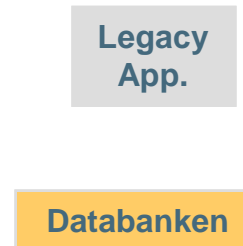
Zentraler Identitätsspeicher

Definition und regelgesteuerte Zuweisung von „Business-Roles“

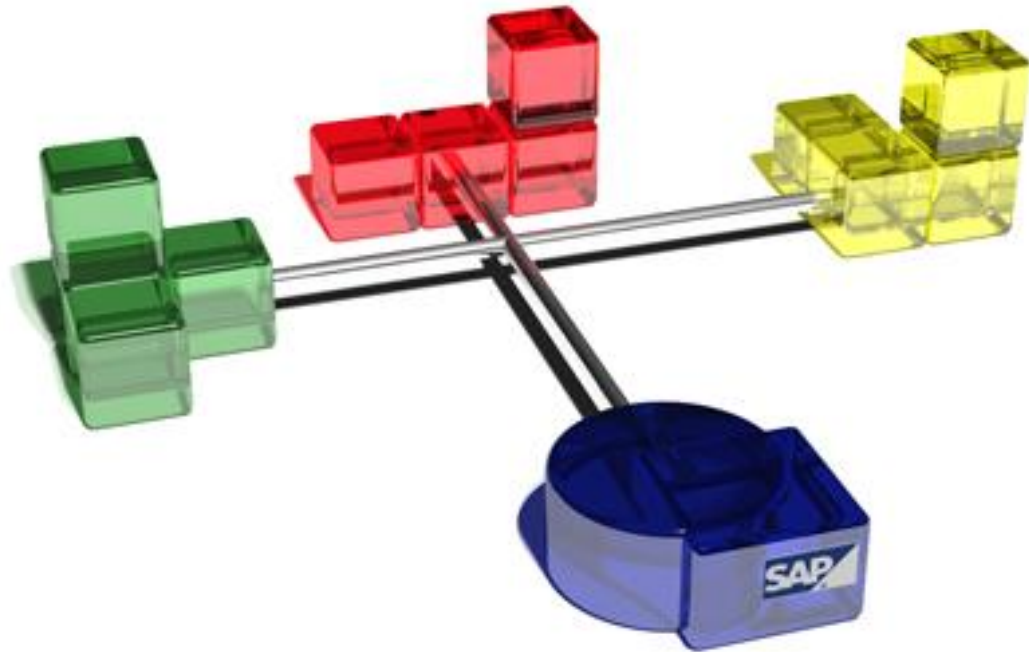
Monitoring & Audit

Passwort-Verwaltung

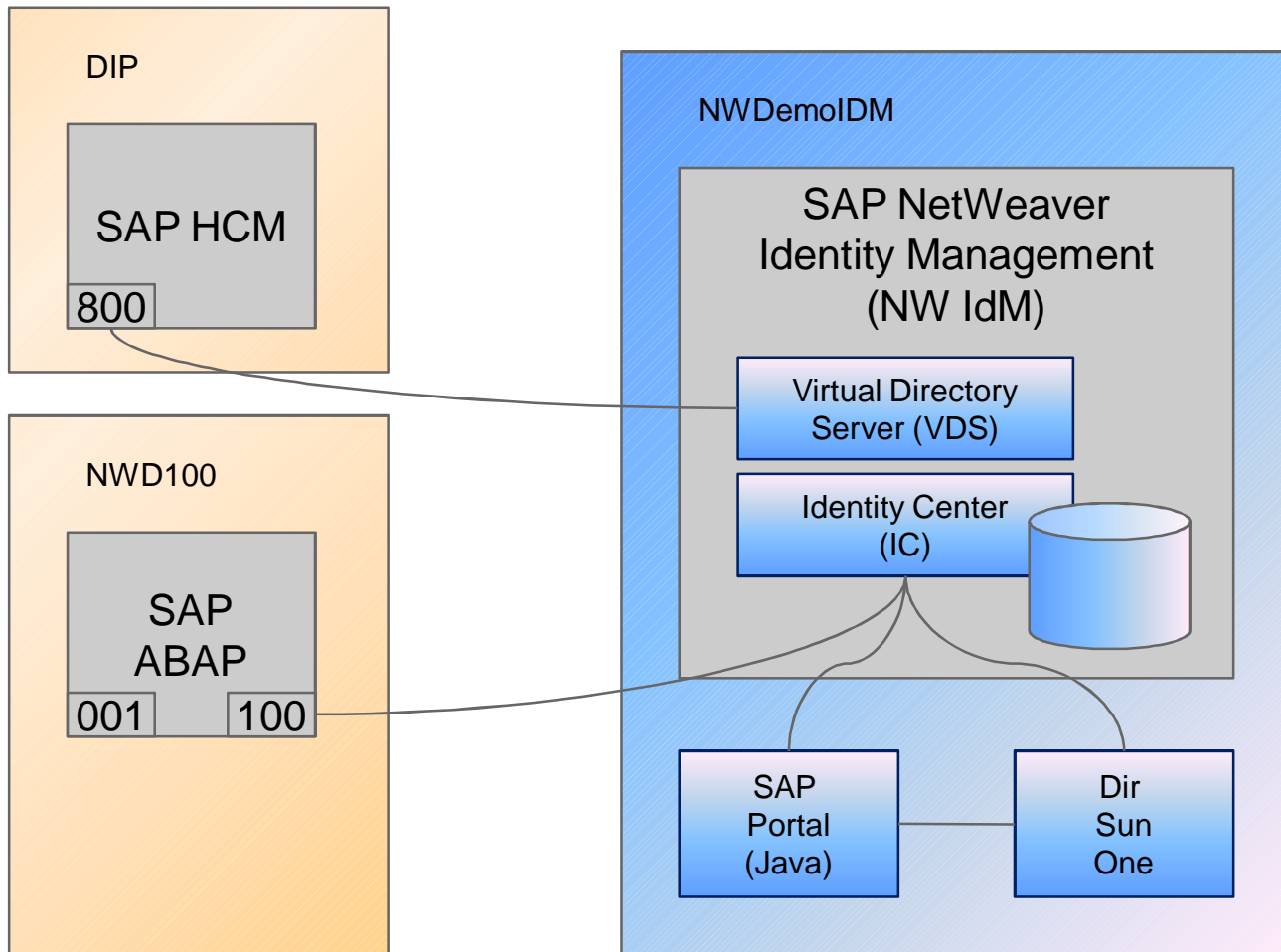
Verteilung von NutzerIds und Rollen-/ Rechtezuweisungen für SAP und Nicht-SAP-Systeme



1. Überblick
2. Features, Funktionen, Architektur
3. Typische Szenarien
4. **Demo**



Demo Setup



Links zum SAP NetWeaver Identity Management



Informationen auf <http://www.SAP.com>

- Plattform
- SAP NetWeaver
- Component & Tools
- SAP NetWeaver Identity Management

Detailliertere Informationen auf <http://sdn.SAP.com/> → Security

- Identity und Access Management
 - SAP NetWeaver Identity Management 7.0
 - High level Übersichtsdokumente
 - Whitepapers
- SAP NetWeaver Identity Management FAQ
 - Wiki-like FAQ

Vielen Dank



Name

Dr. Peter Gergen
Presales Specialist SAP NW IdM
NW Platform Solutions

SAP Deutschland
Zeppelinstrasse 2
85399 Hallbergmoos, Germany

T +49 6227 7-70544
E peter.gergen@sap.com
W www.sap.com



Copyright 2007 SAP AG

All rights reserved



No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, Duet, Business ByDesign, ByDesign, PartnerEdge and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries all over the world. All other product and service names mentioned and associated logos displayed are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

The information in this document is proprietary to SAP. This document is a preliminary version and not subject to your license agreement or any other agreement with SAP. This document contains only intended strategies, developments, and functionalities of the SAP® product and is not intended to be binding upon SAP to any particular course of business, product strategy, and/or development. SAP assumes no responsibility for errors or omissions in this document. SAP does not warrant the accuracy or completeness of the information, text, graphics, links, or other items contained within this material. This document is provided without a warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

SAP shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials. This limitation shall not apply in cases of intent or gross negligence.

The statutory liability for personal injury and defective products is not affected. SAP has no control over the information that you may access through the use of hot links contained in these materials and does not endorse your use of third-party Web pages nor provide any warranty whatsoever relating to third-party Web pages

Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch SAP AG nicht gestattet. In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden.

Einige von der SAP AG und deren Vertriebspartnern vertriebene Softwareprodukte können Softwarekomponenten umfassen, die Eigentum anderer Softwarehersteller sind.

SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, Duet, Business ByDesign, ByDesign, PartnerEdge und andere in diesem Dokument erwähnte SAP-Produkte und Services sowie die dazugehörigen Logos sind Marken oder eingetragene Marken der SAP AG in Deutschland und in mehreren anderen Ländern weltweit. Alle anderen in diesem Dokument erwähnten Namen von Produkten und Services sowie die damit verbundenen Firmenlogos sind Marken der jeweiligen Unternehmen. Die Angaben im Text sind unverbindlich und dienen lediglich zu Informationszwecken. Produkte können länderspezifische Unterschiede aufweisen.

Die in diesem Dokument enthaltenen Informationen sind Eigentum von SAP. Dieses Dokument ist eine Vorabversion und unterliegt nicht Ihrer Lizenzvereinbarung oder einer anderen Vereinbarung mit SAP. Dieses Dokument enthält nur vorgesehene Strategien, Entwicklungen und Funktionen des SAP®-Produkts und ist für SAP nicht bindend, einen bestimmten Geschäftsweg, eine Produktstrategie bzw. -entwicklung einzuschlagen. SAP übernimmt keine Verantwortung für Fehler oder Auslassungen in diesen Materialien. SAP garantiert nicht die Richtigkeit oder Vollständigkeit der Informationen, Texte, Grafiken, Links oder anderer in diesen Materialien enthaltenen Elemente. Diese Publikation wird ohne jegliche Gewähr, weder ausdrücklich noch stillschweigend, bereitgestellt. Dies gilt u. a., aber nicht ausschließlich, hinsichtlich der Gewährleistung der Marktgängigkeit und der Eignung für einen bestimmten Zweck sowie für die Gewährleistung der Nichtverletzung geltenden Rechts.

SAP übernimmt keine Haftung für Schäden jeglicher Art, einschließlich und ohne Einschränkung für direkte, spezielle, indirekte oder Folgeschäden im Zusammenhang mit der Verwendung dieser Unterlagen. Diese Einschränkung gilt nicht bei Vorsatz oder grober Fahrlässigkeit.

Die gesetzliche Haftung bei Personenschäden oder die Produkthaftung bleibt unberührt. Die Informationen, auf die Sie möglicherweise über die in diesem Material enthaltenen Hotlinks zugreifen, unterliegen nicht dem Einfluss von SAP, und SAP unterstützt nicht die Nutzung von Internetseiten Dritter durch Sie und gibt keinerlei Gewährleistungen oder Zusagen über Internetseiten Dritter ab.

Alle Rechte vorbehalten.