SAP NetWeaver Identity Management

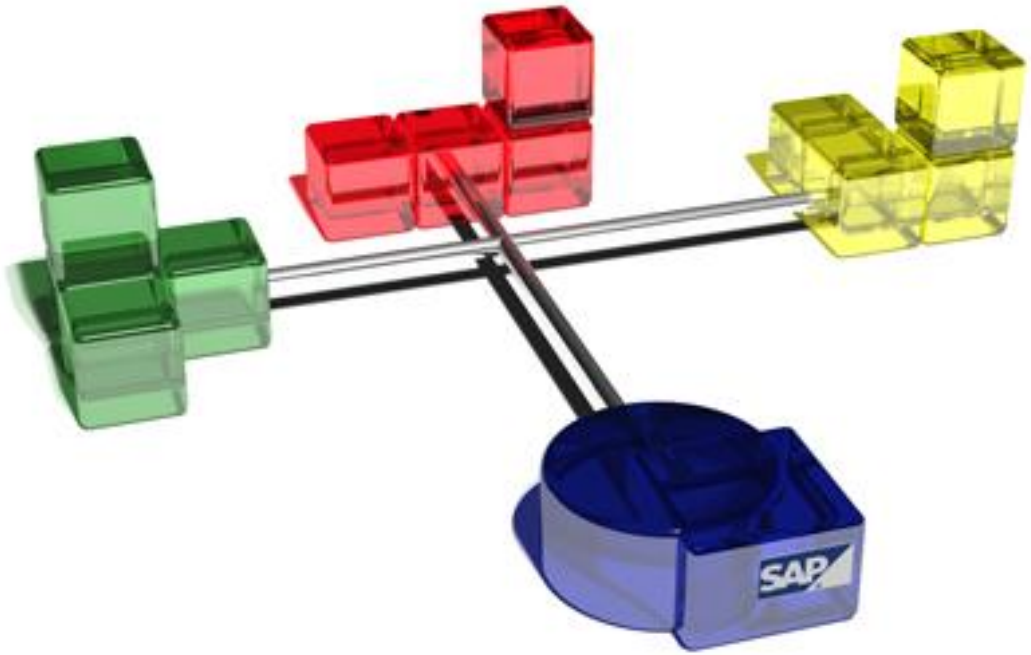
Dr. Peter Gergen

Presales Specialist Identity Management
Platform Solutions

SAP Deutschland

Agenda

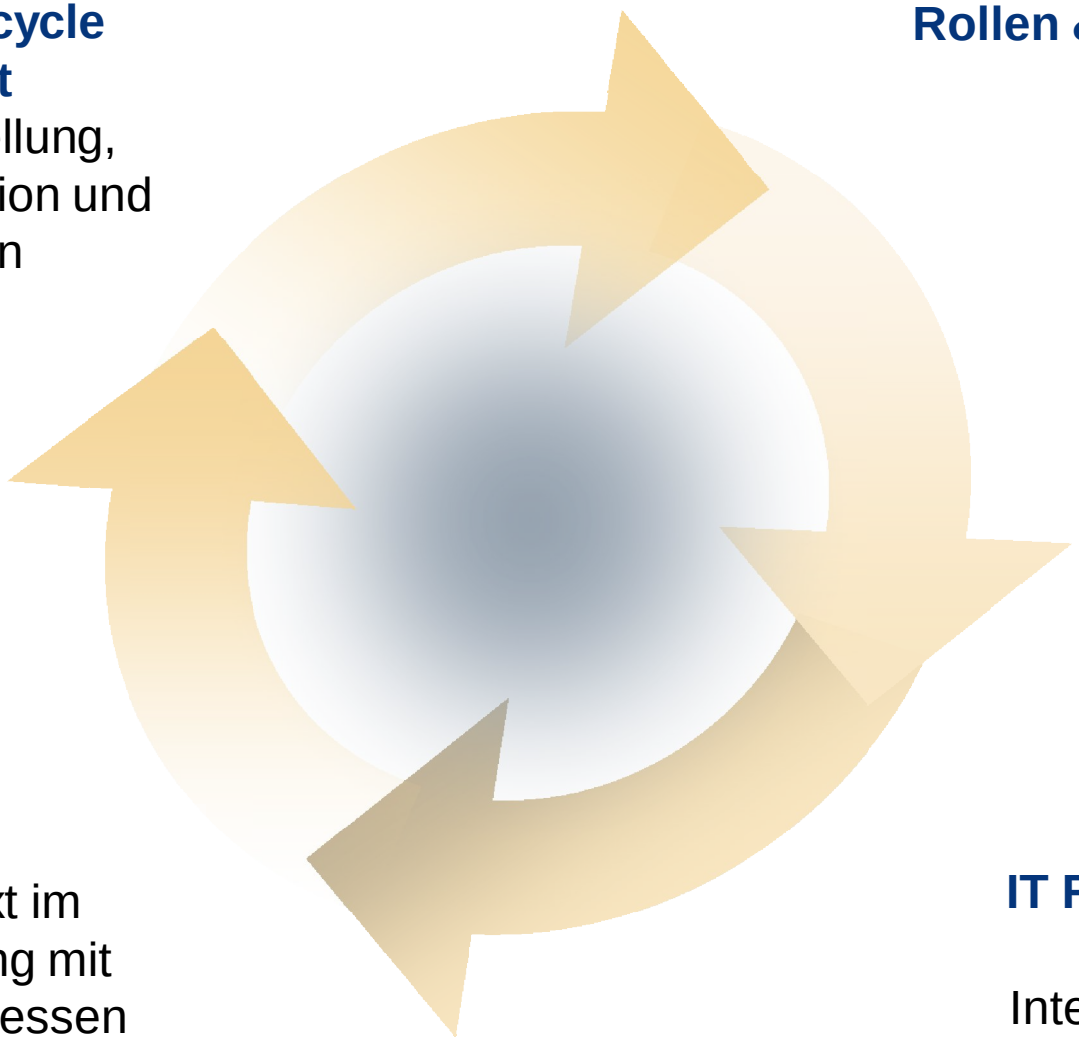
1. **Überblick**
2. Features, Funktionen, Architektur
3. Typische Szenarien
4. Demo



Identity Management – Key benefits

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
Verügfbar:
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

Herausforderungen

Security

Administration von Benutzern und Berechtigungen in heterogenen Systemlandschaften

Geschäftsmodell erfordert prozess-orientiertes Rollenmanagement

Compliance

Verschiedene Konzepte für User- und Rollenmanagement (SAP, Portal, LDAP, ADS)

Revision verlangt Protokolleinträge und Berichte von Aktivitäten über alle Systeme und Prozessesdf

Transparenz

Keine unternehmensweite zentrale Administrationsinstanz für Benutzerdatenverwaltung

SOA –Architekturen erfordern IdM-Datenaustausch über System-Grenzen hinweg

Qualität

Bedarf von systemübergreifenden Workflows zum Beantragen und Genehmigen von Berechtigungen

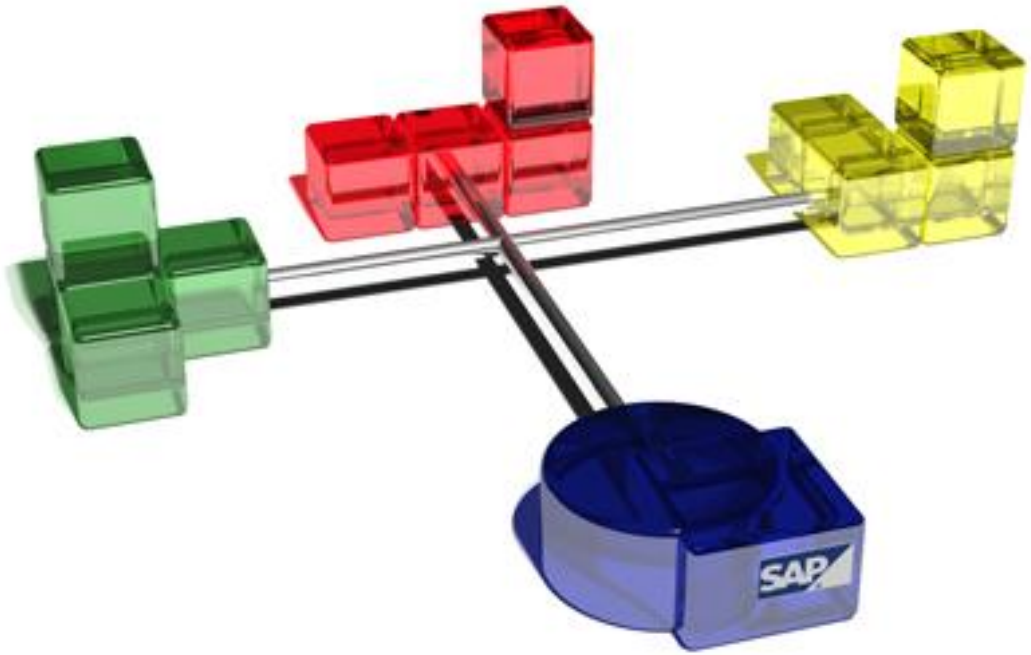
Kostenoptimierung durch Automatisierung besser integrierter Geschäftsprozesse

Kosten

SAP Netweaver
Identity Management

Agenda

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



Positionierung in SAP NetWeaver

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

Identity Center Datenbank
Identiten/Konfigurations/Rollen-Speicher, Prozess-Logik

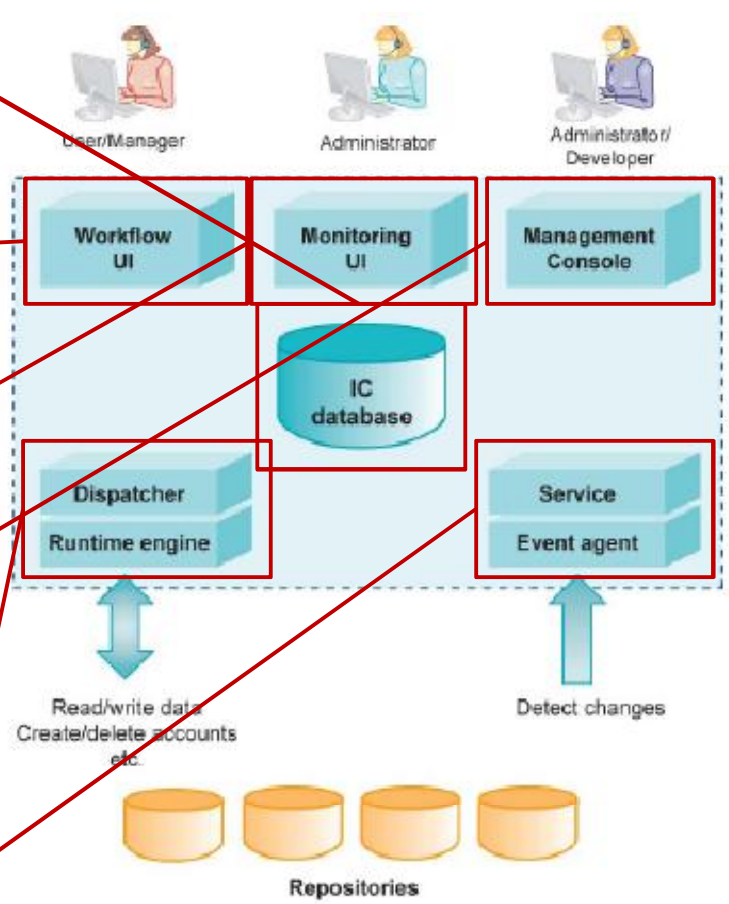
Workflow Benutzerschnittstelle
Haupt-Interface für User und Manager

Monitoring Benutzerschnittstelle
Monitoring und Audit Interface für Administratoren

Konfigurations-Oberfläche
Konfigurations-Schnittstelle

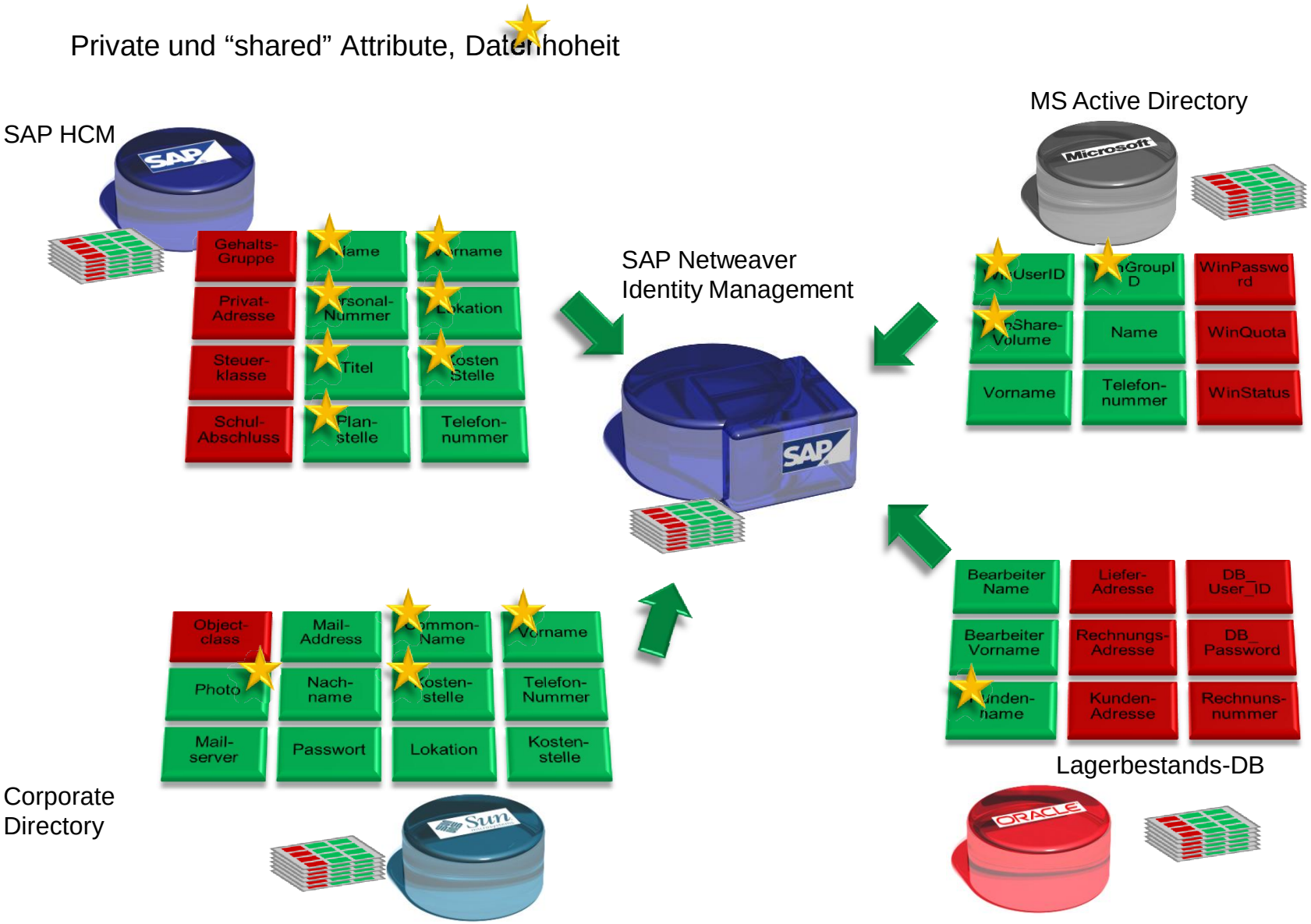
Laufzeitsystem und Dispatcher
Prozess- und Provisioning-Logik inklusive Konnektoren

Ereignisüberwachung
Überwacht angeschlossene Systeme und initiiert Datensynchronization bei Feststellung von Änderungen



Datensynchronisation

Private und “shared” Attribute, Datenhoheit



Workflows in der IdM-Architektur

Manuelle Interaktion durch Browser

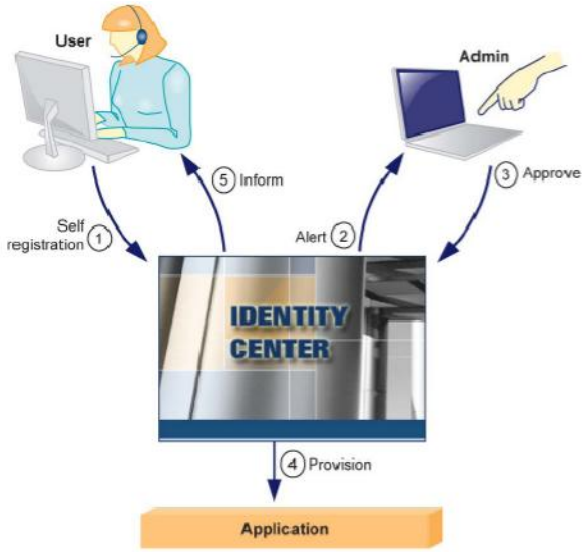
- Starte Provisionierungsaufgaben
- Genehmige Berechtigungszuweisungen
- Statuskontrolle

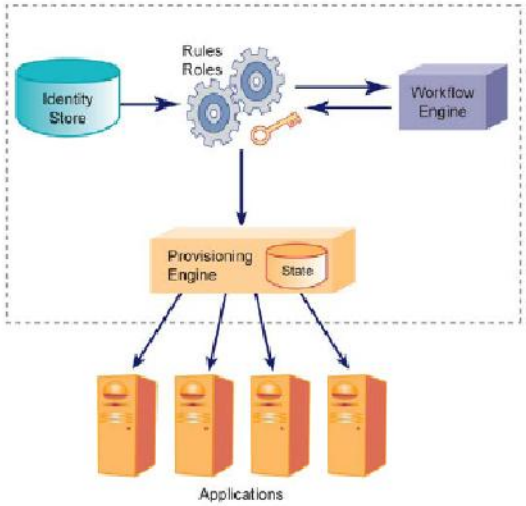
Workflows startbar über

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

Prozesslogik

- Sequenziell
- Parallel
- Konditional
- Genehmigungsschritte





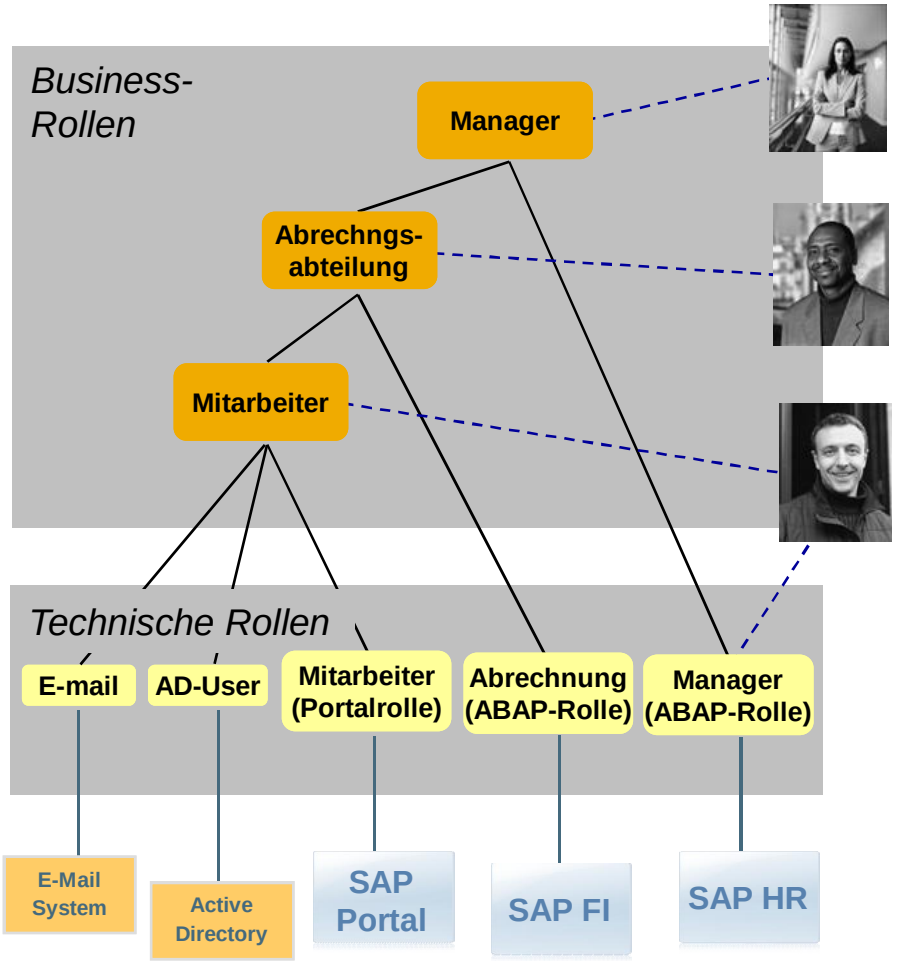
Rollendefinition und Berechtigungsprovisionierung

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/Aufgabenaufzeichnnugen

- 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	3025 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	Elisabeth 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

Konnektoren

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

Connectors as of November 2007

SAP NW IdM Komponenten

SAP NW Identity Management:

Komponenten:

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

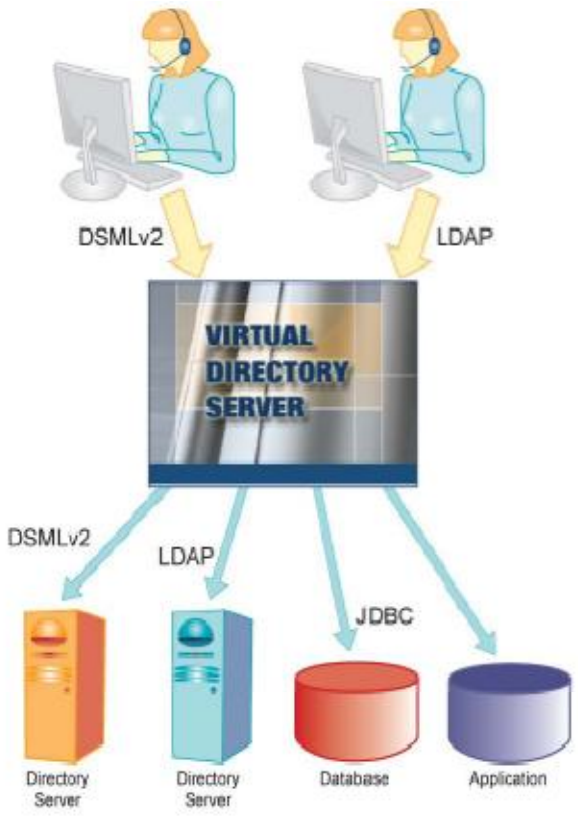
Virtual Directory Server

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)

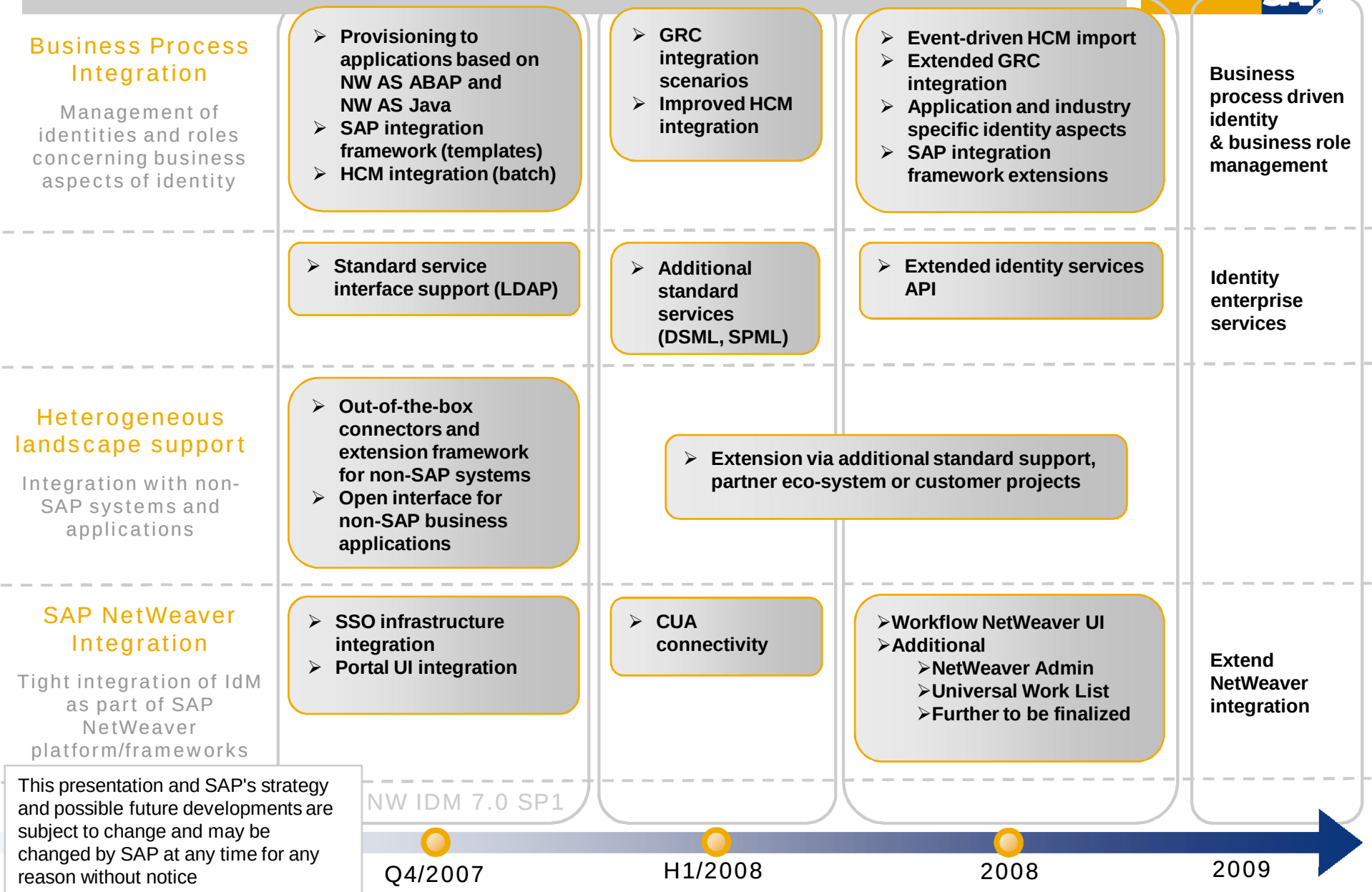
- Transformiere einkommende LDAP-Anfragen und leite diese direkt an die richtigen Datenquellen weiter
  - Datensätze verbleiben in Quellsystemen (anders als IC)
  - Effizientes Caching



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

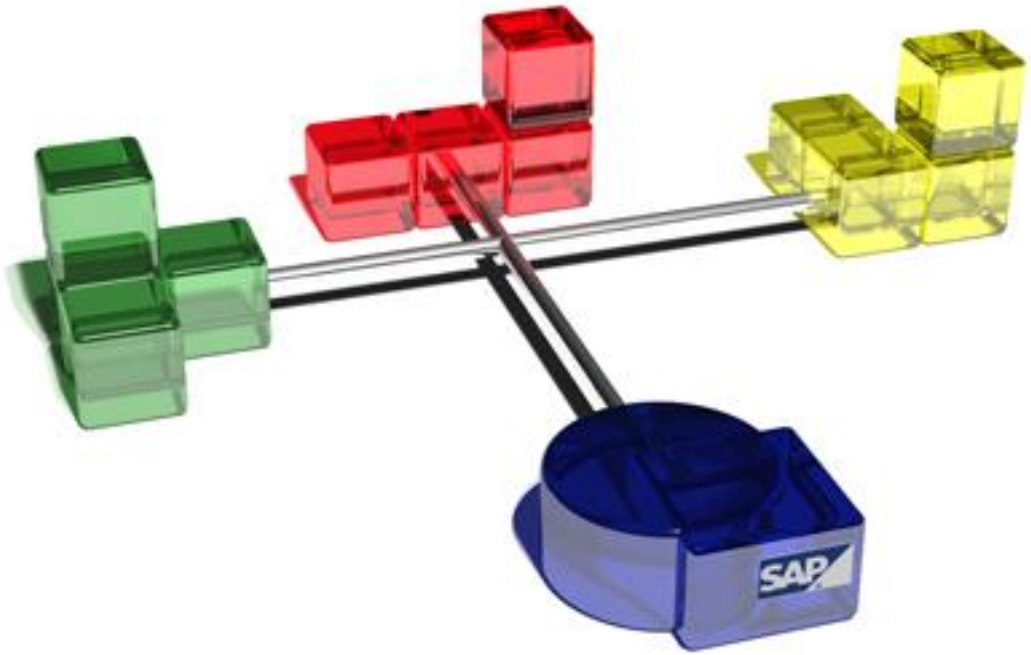
SAP NW IdM – vorläufige Roadmap



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

Agenda

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

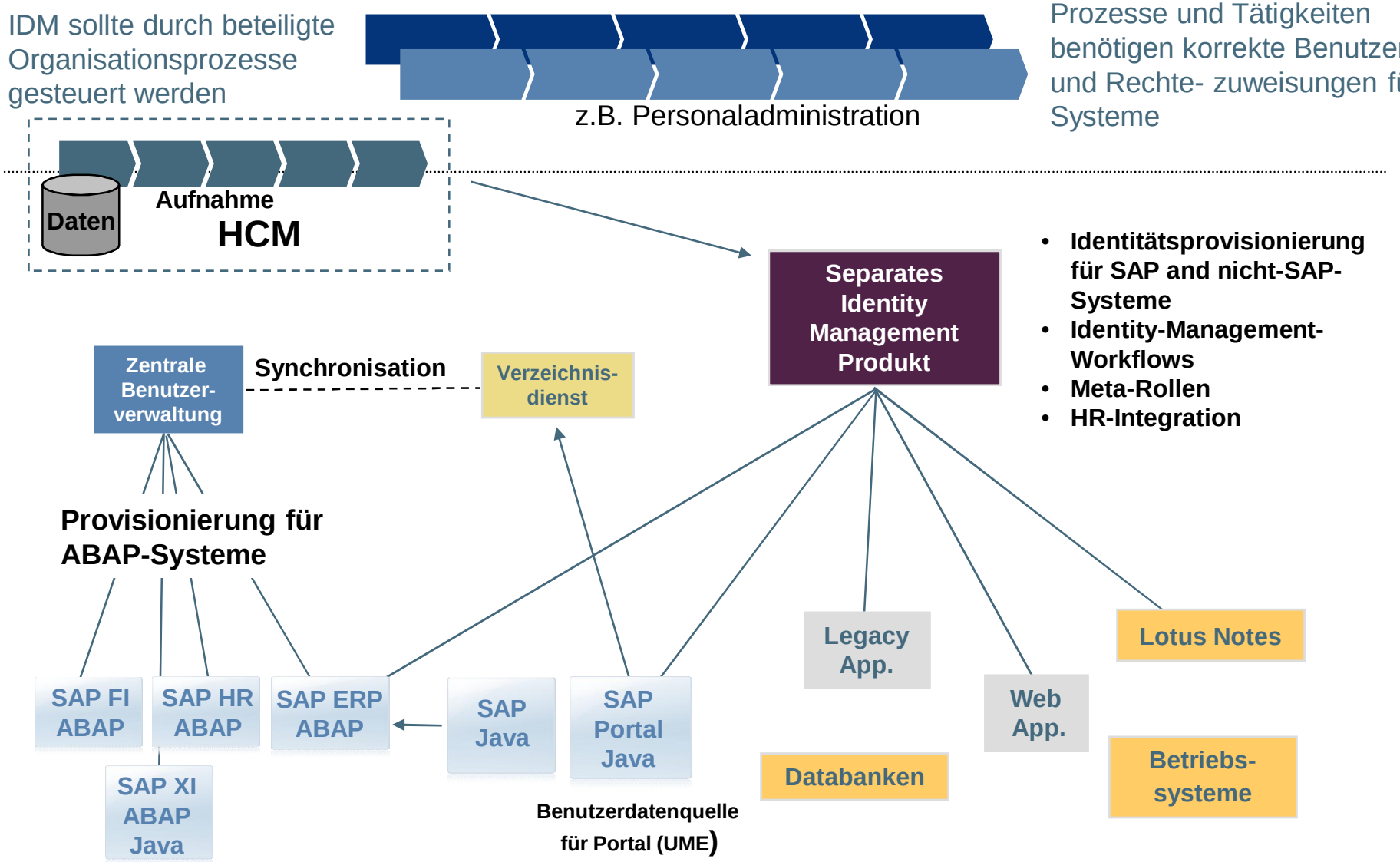


Identity Management (IdM) – bisher

IDM sollte durch beteiligte Organisationsprozesse gesteuert werden

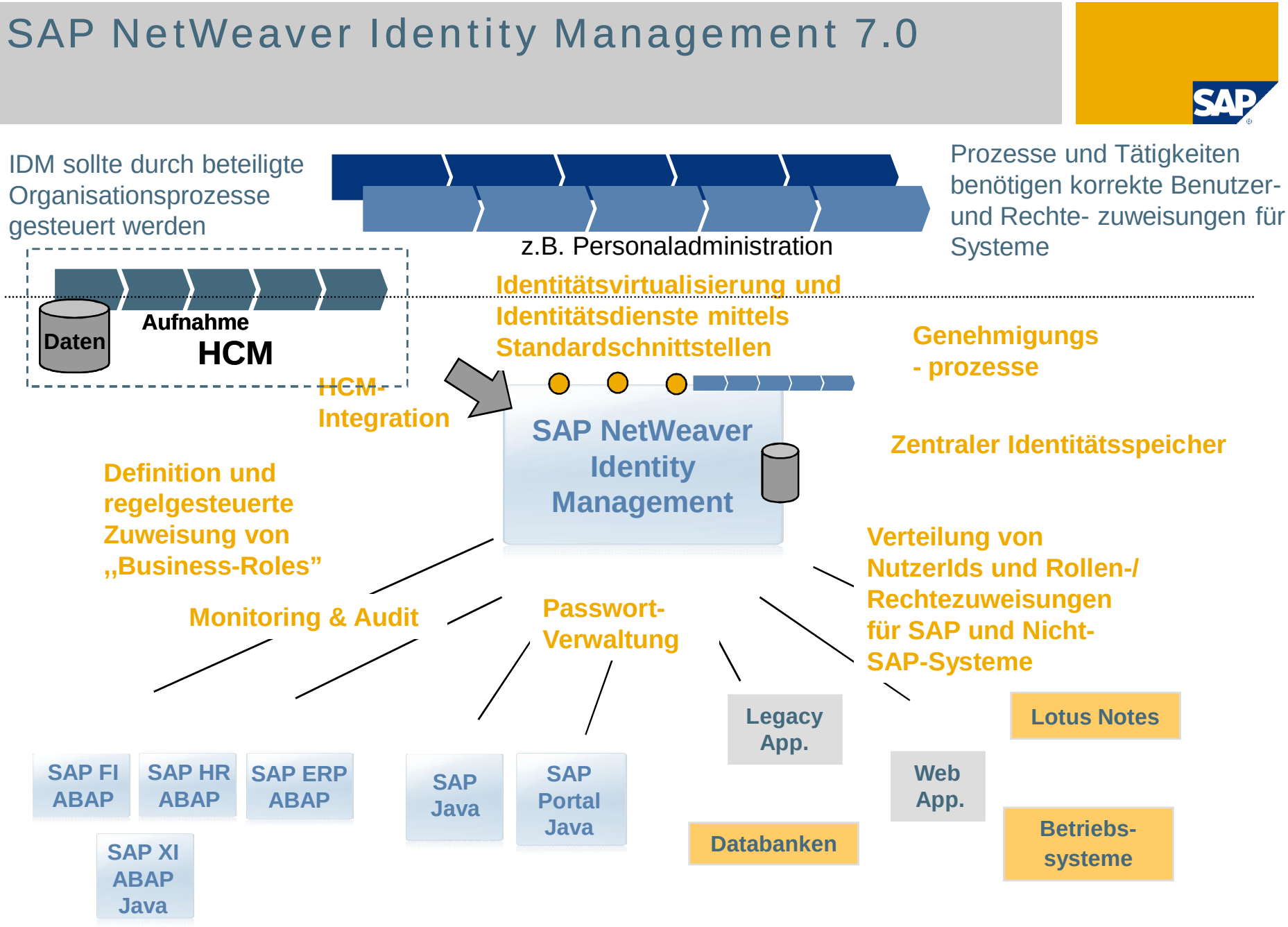
z.B. Personaladministration

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



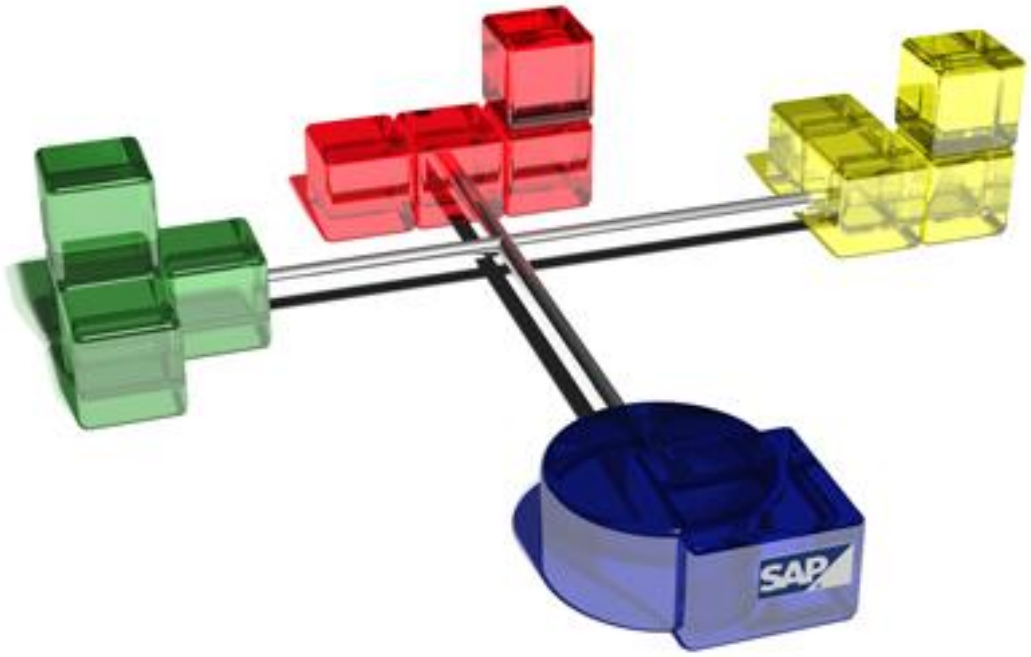
- **Identitätsprovisionierung für SAP and nicht-SAP-Systeme**
- **Identity-Management-Workflows**
- **Meta-Rollen**
- **HR-Integration**

SAP NetWeaver Identity Management 7.0

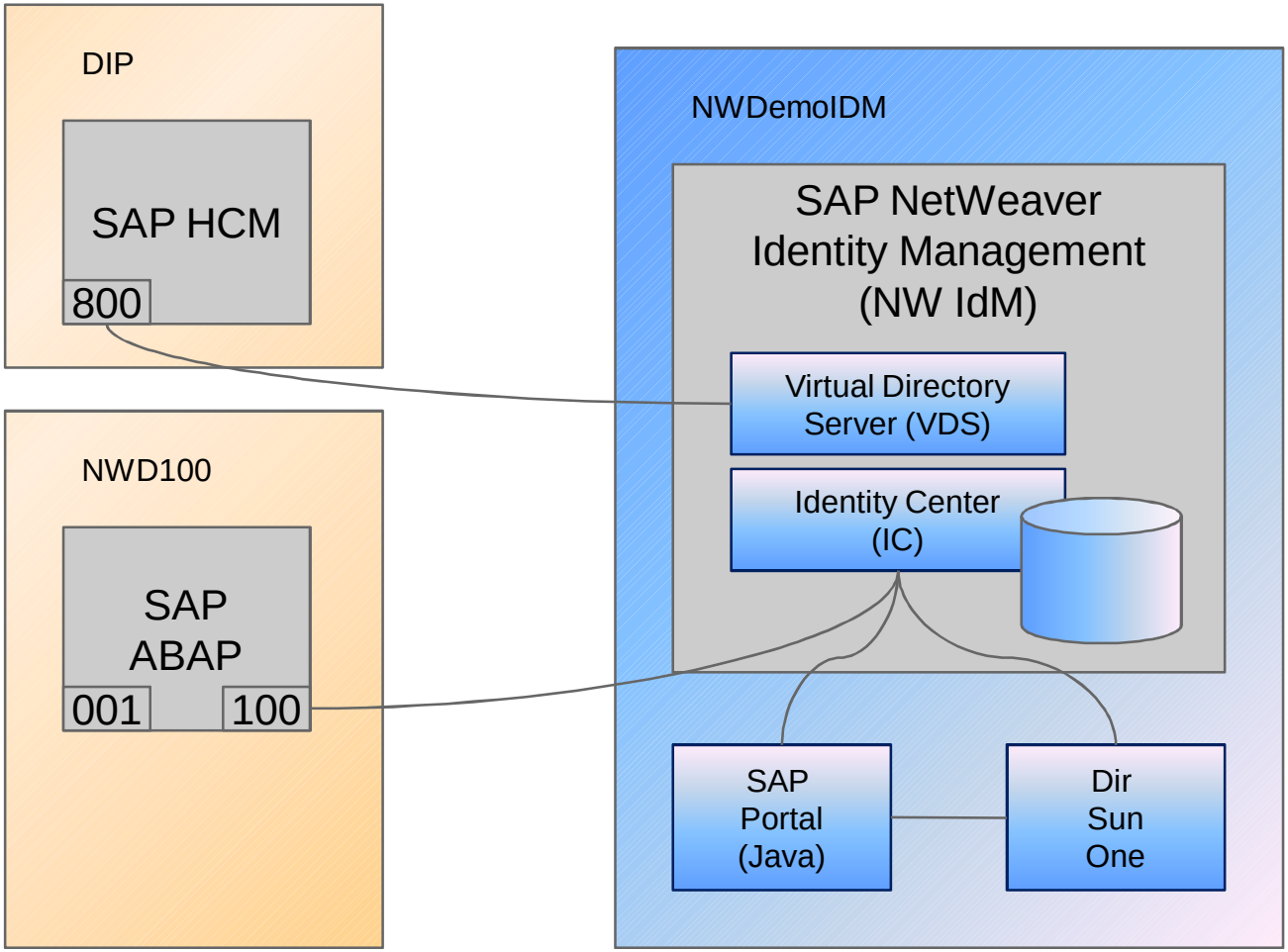


Agenda

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



Demo Setup


DIP
SAP HCM
800
NWD100
SAP
ABAP
001
100
NWDemoIDM
SAP NetWeaver
Identity Management
(NW IdM)
Virtual Directory
Server (VDS)
Identity Center
(IC)
SAP
Portal
(Java)
Dir
Sun
One

Links zum SAP NetWeaver Identity Management

Informationen auf http://www.SAP.com

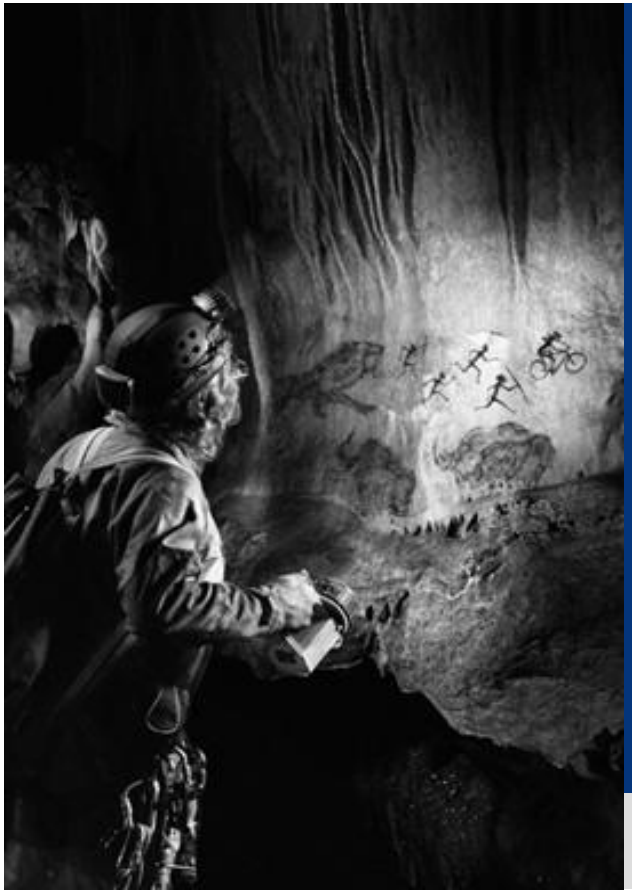
- **Plattform**
- **SAP NetWeaver**
- **Component & Tools**
- **SAP NetWeaver Identity Management**

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

Kontakt SAP Presales Identity Management



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