



# Role & User Repositories in SAP NetWeaver / SAP Application Environments

NetWeaver RIG Expert Call  
16 December 2004

Hartmut K. Goetze, SAP



**Hartmut Karl Goetze**

**Senior RIG Consultant,  
SAP NetWeaver Regional Implementation Group  
Asia Pacific & Japan**

## **Identity Management with SAP**

- n Central User Administration**
- n Directory Integration**
- n Portal User Management Engine**

## **Role Management with SAP**

- n ABAP Authorization Roles**
- n J2EE / UME Authorization Roles**
- n Portal Roles**
- n Role Integration Example**

## **SAP's strategy for Identity Management**

## **Summary**

**As a result of this workshop, you will understand the concepts behind:**

- n User Management with SAP including the Central User Administration**
- n Directory Integration**
- n Portal User Management Engine**
- n Portal Roles**
- n Role Management in ABAP and Java based systems**

## **Role Management with SAP**

- n ABAP Authorization Roles**
- n J2EE / UME Authorization Roles**
- n Portal Roles**
- n Role Integration Example**

## **SAP's strategy for Identity Management**

## **Summary**

## Central Identity Management

Manage the Individual's **profile** and **relationships** in **heterogeneous and federated landscapes**

**Provide Services and Delegated Administration Features for**

nAuthentication (policy-based)

nSingle Sign-On

nAuthorization (policy-based)

nProfile Management

nProvisioning for Legacy Systems

**IM done through one centralized component**

SAP R/3



Network  
OS



Ext. access



HR



Other apps.



# Decentralized User Maintenance

**Each SAP System has its own user data store**

**à Decentralized user maintenance**

**à Inconsistencies can occur between address data**



**SAP R/3  
Enterprise**



**SAP  
EBP**



**SAP  
BW**



**SAP  
APO**



**SAP  
...**

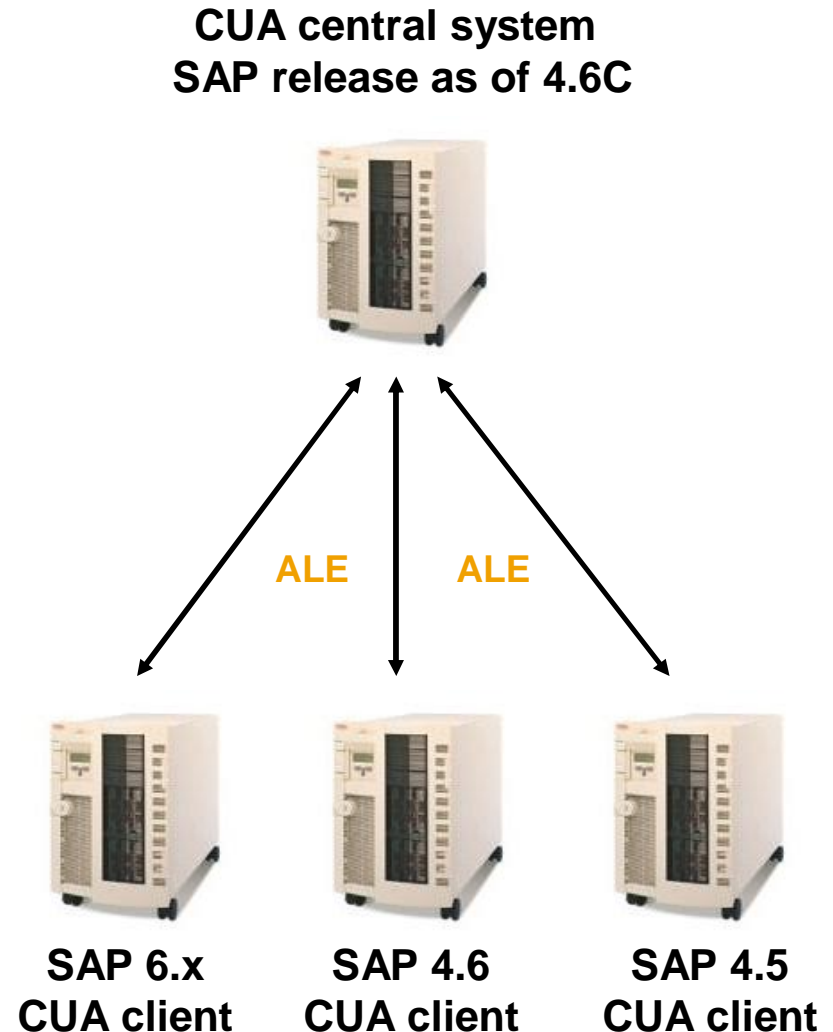
**Users can be administrated in central SAP system**

**Automatic distribution to client SAP systems**

**Local administration still possible (back distribution)**

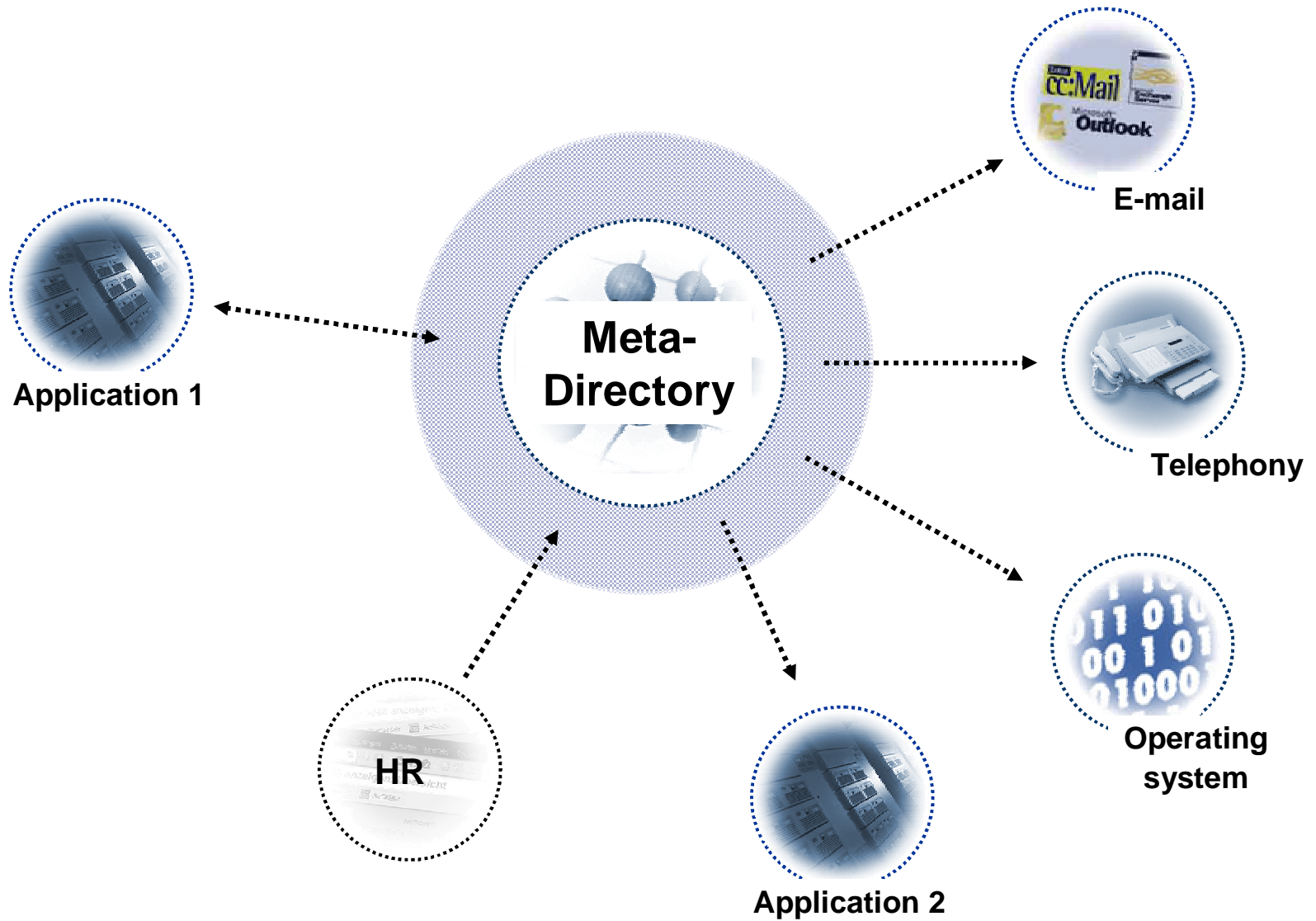
**No inconsistencies**

**Central locks possible**





# User Management – Directory Integration



**Directories serve as central repository for master data, which is used by several different applications.**

**Modifications on this data can be done by every authorized application.**

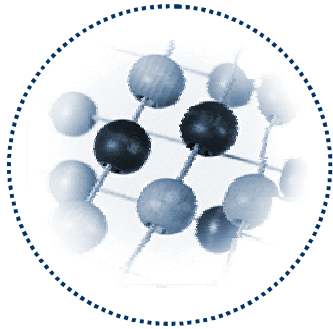
**Access to this data is provided using the standardized Lightweight Directory Access Protocol (LDAP).**

**Hundreds of other application and hardware suppliers support this protocol.**

**SAP systems can be connected to such a directory to share parts of their user data or database content (e.g. HR data) with other applications.**

# LDAP Synchronization

Directory



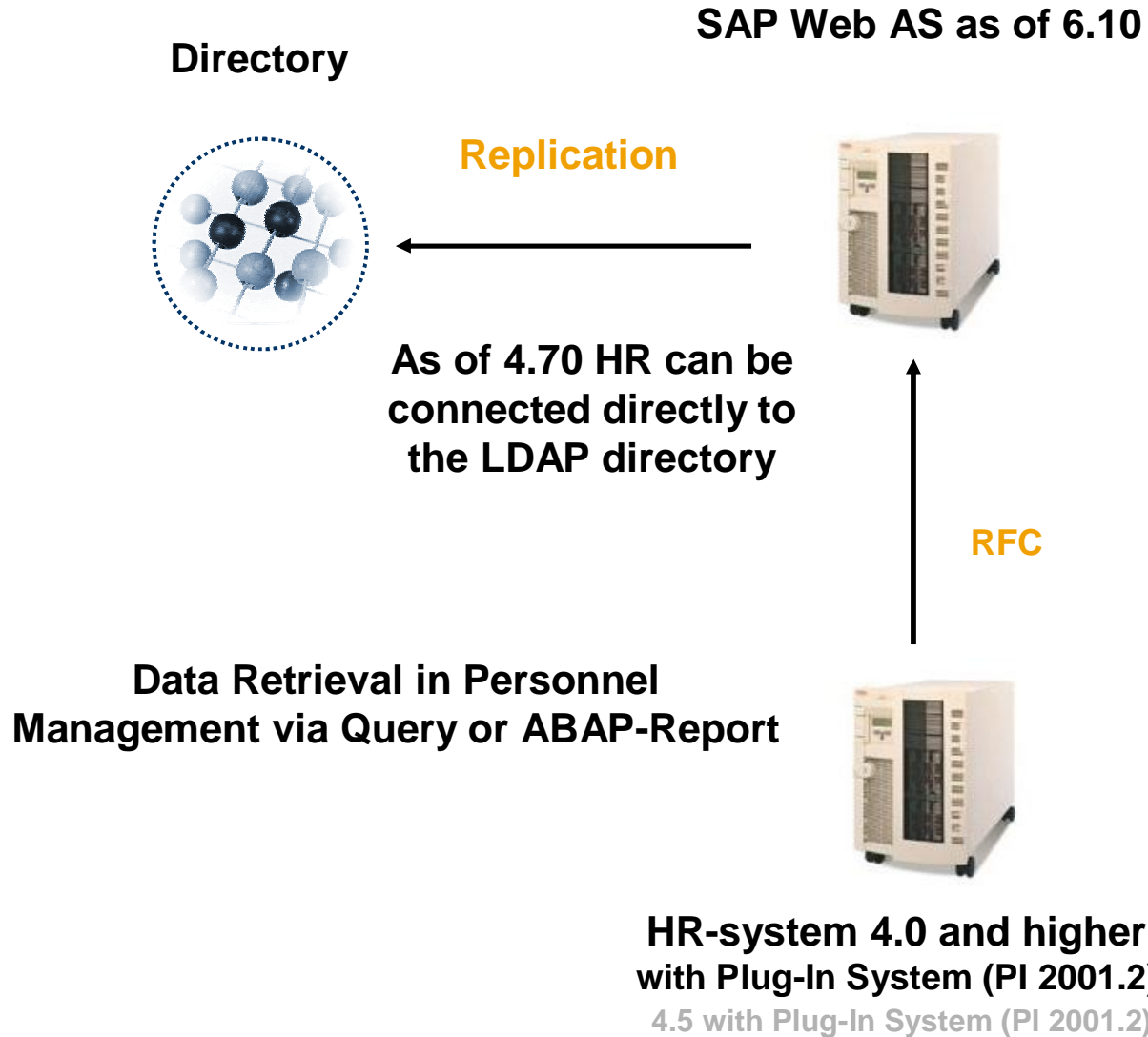
LDAP  
synchronization



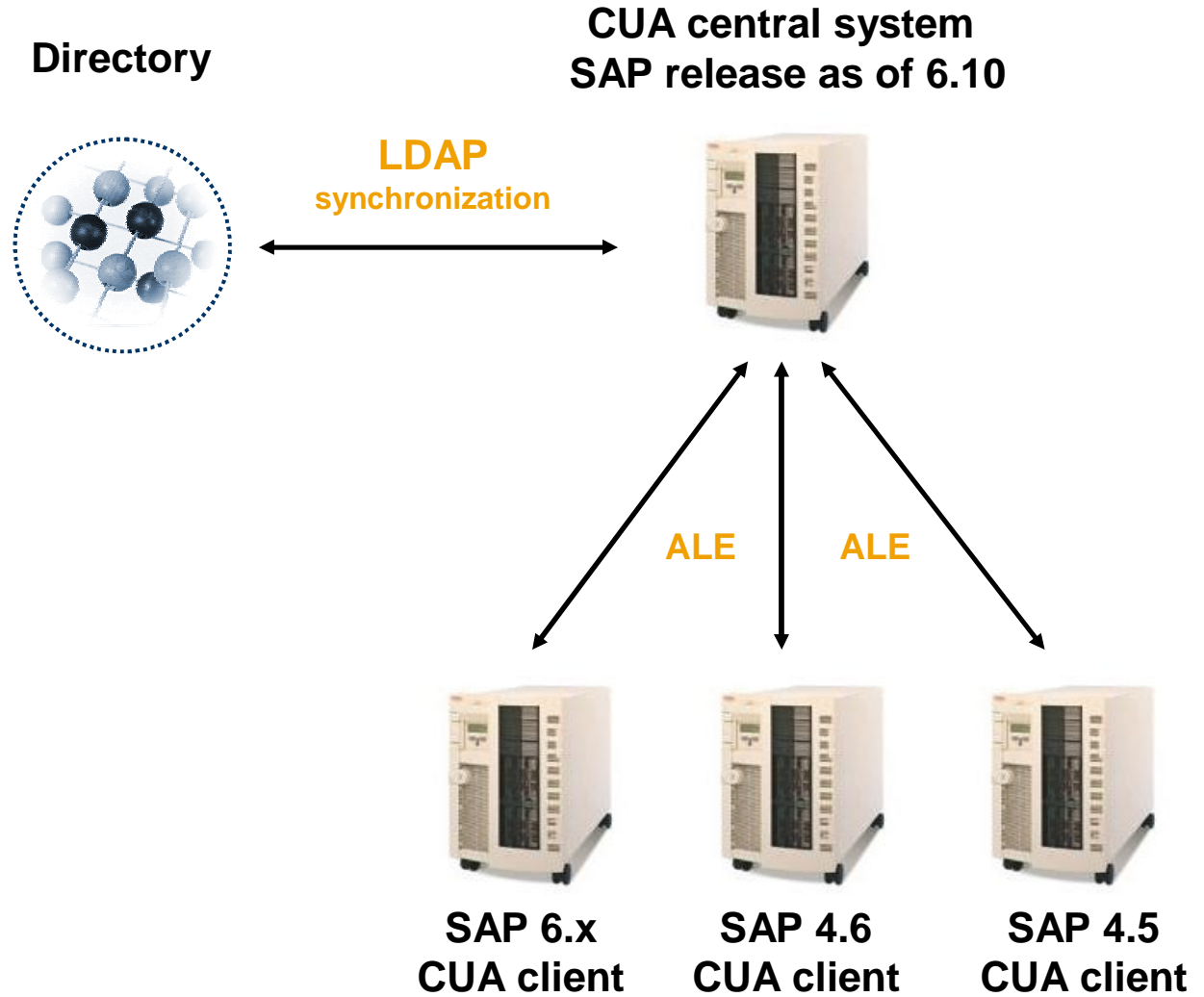
SAP ABAP System  
release as of 6.10



# HR Data Replication from SAP in an LDAP Enabled Directory Service



# Central User Administration & LDAP Synchronization

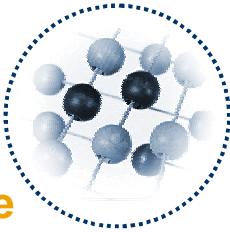


# CUA & LDAP Synchronization & Enterprise Portal

**Enterprise Portal  
with User Management  
Engine (UME)**

**Directory**

**CUA central system  
SAP release as of 6.10**



**Persistence  
store**

**LDAP  
synchronization**

**ALE**

**ALE**



**SAP 6.x  
CUA client**

**SAP 4.6  
CUA client**

**SAP 4.5  
CUA client**

# Architecture Overview - User Management Engine

Applications  
Accessing User  
Management

SAP  
Enterprise  
Portal

... other  
J2EE  
Application

User Management  
Core Layer

User  
API

User  
Account  
API

Group  
API

Role  
API

Persistence Manager

Replication  
Manager

Persistence  
Adapters

User Persistence  
Store

Database

LDAP  
Directory

SAP  
System

External  
System

## Identity Management with SAP

- n Central User Administration
- n Directory Integration
- n Portal User Management Engine

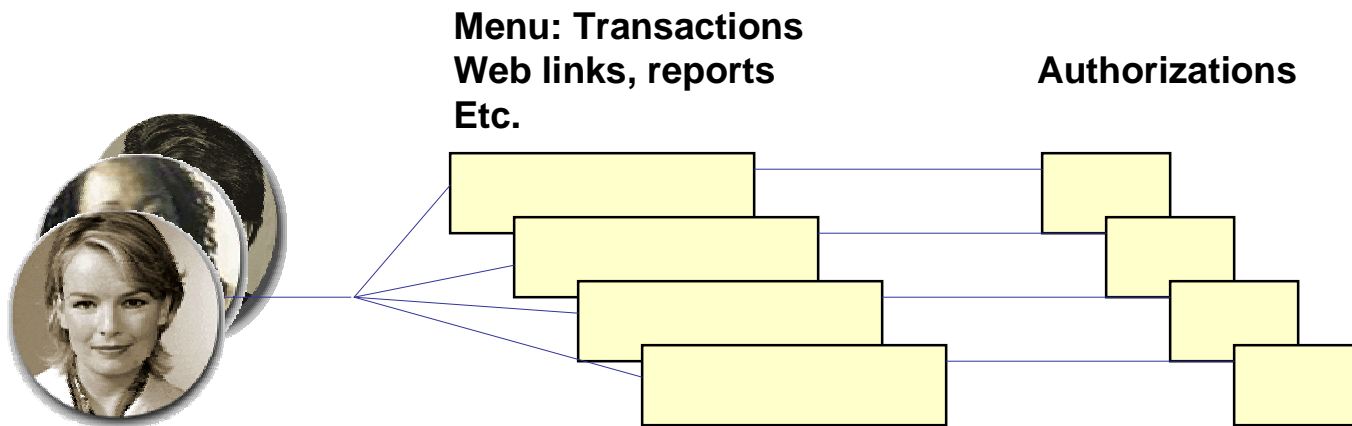


**SAP's strategy for Identity Management**

**Summary**

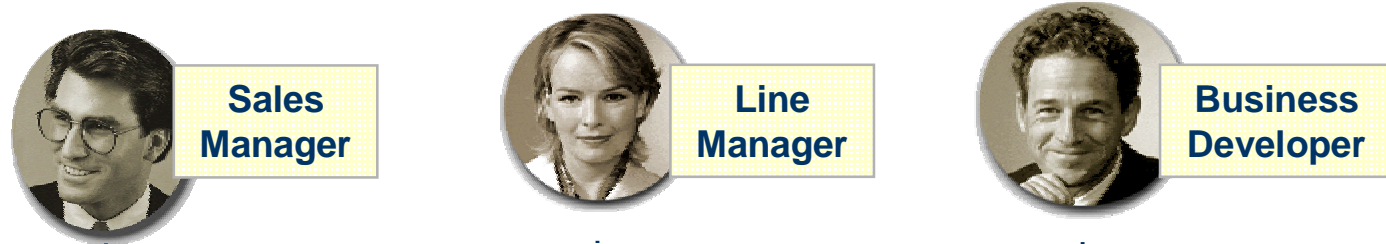


User **m:n** ABAP Role **1:n** Authorization Data



# SAP NetWeaver Portal Introduction

*Role-based, ...*



*...secure...*

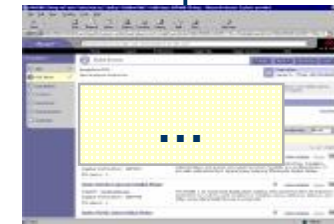
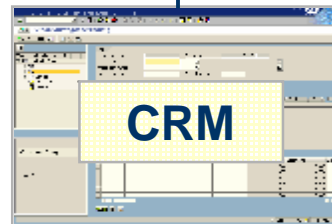
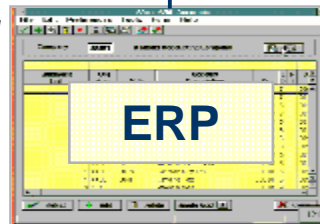
Authentication

*...and Web based...*



*...access to any kind of applications, information and services*

Single Sign On



\*covered by KM

# SAP NetWeaver powers mySAP Solutions

## Role-specific, Easy Access to All Systems

Welcome Tom Bender

Collaboration | Search

Home Corporate Services Business Area **My Staff** My Budget BI Analyst BI Consumer

Overview Attendance **Employee Review** Personnel Change Request Recruitment Reporting Compensation Quota Planning

... Quarterly Comparison > Cost Center Monitor > Asset Monitor > Overview > Employee Profile | Back

**Detailed Navigation**

- Employee Profile
- Compensation Information
- Personnel Development
- Employee Documents
- Appraisal Overview
- Edit Appraisals
- Objective Setting and Appraisals

**General Data**


**Julia Grimm (00001444)**

**Contract Data**

Work Contract Comm. employee  
 Hiring Date 1/1/2001  
 Cap. Util. Level 100.00

**Organizational Assignment** [More...](#)

**Photo**



**Team Viewer**

All Employees

**Employee**

<a href="#">Julia Grimm</a>	
<a href="#">Andreas Klein</a>	
<a href="#">Felicitas Bauer</a>	00001451
<a href="#">Ellen Rilke</a>	00001441
<a href="#">Axel Janosch</a>	00001443
<a href="#">Maika Thoma</a>	00001445

**Organizational History**

**Position** Secretary Sales PC Group 1 From 1/1/2001

**Center** Secretary

**Organizational Unit** Sales PC Group 1

**Manager Self Service Role (SAP ERP)**

Welcome, George Harvey

MySAP MyBudget **Employee Self-Service**

Overview Administration Working Time Travel Life and Work Events Personal Information Benefits and Payment Career

**Employee Self-Service**

Welcome to Employee Self-Service. This site is an overview of all available services and provides easy access to each of them.

**Administration**  
 Manage your daily work activities such as report PC problems by using service internal service requests. Book rooms for meetings. Monitor and maintain your assets.

**Travel**  
 Create your travel requests and plan travel service for your business trip, such as booking flights, hotels, car rental and train tickets. Record your travel expenses.

**Benefits and Payment**  
 Display the plans in which you are currently enrolled, enroll in new benefits and download an enrollment form. Display your salary.

**Working Time**  
 Request leave and other types of absence. Display calendar and time balances, and cancel leave requests.

**Life and Work Events**  
 Guides you through a number of Life and Work Events from a birth of a child to beginning work at a new company.

**Personal Information**  
 Administrate addresses, bank information, and information on your family members and dependents.

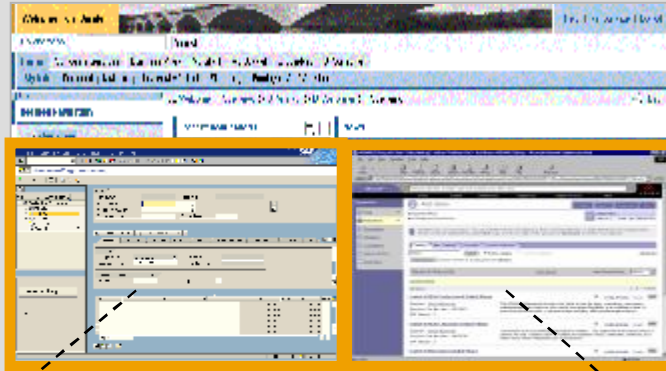
**Career**  
 Monitor and approve your objectives and appraisals. View and change your own skills profile.

**Employee Self Service Role (SAP ERP)**

# Overview SAP Roles

## Portal Roles

... define, what is displayed in the Portal



## ABAP Roles

... define, what Authorizations the user has in the Backend System

**ABAP**

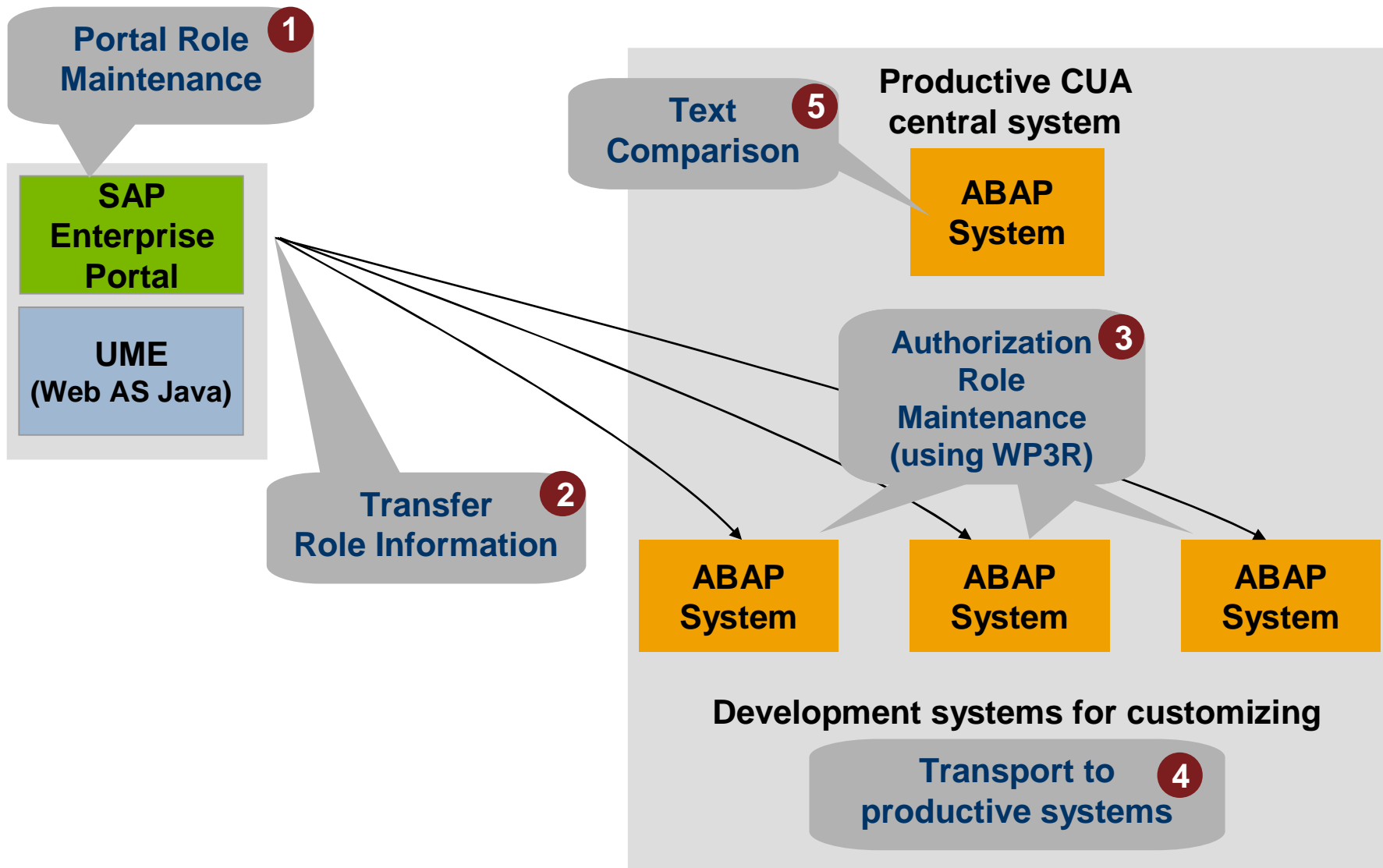
## UME Roles or J2EE Security Roles

**J2EE**

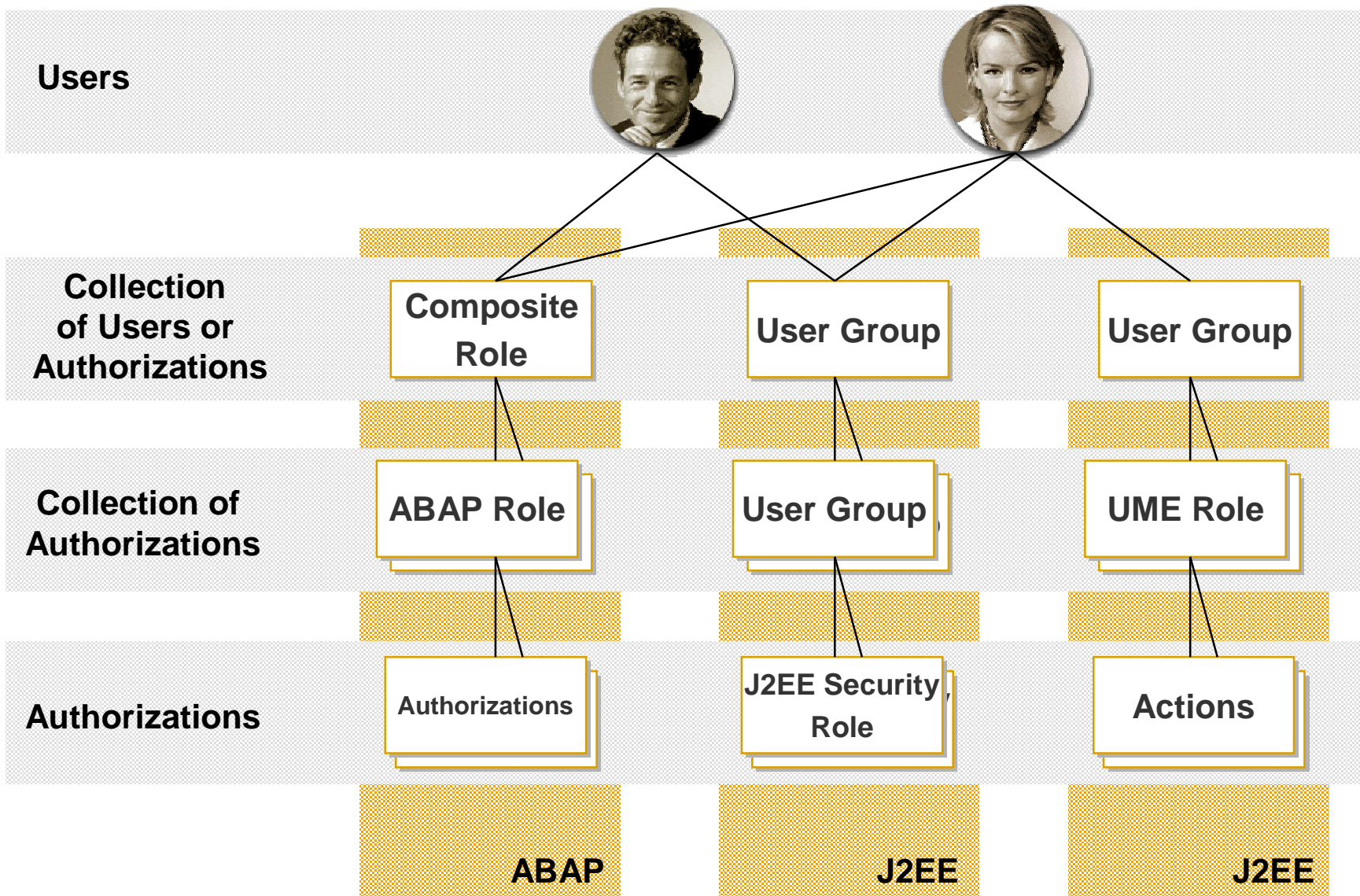
# ABAP Roles and Portal Roles: A Comparison

<b>ABAP-Roles</b>	<b>Portal Roles</b>
<p><b>Roles (single roles) carry authorization information.</b></p> <p><b>The Profile Generator is part of the role administration in transaction PFCG.</b></p> <p><b>The content of Authorization Roles can be generated using the definition of Portal Roles</b></p>	<p><b>Portal Roles carry the user interface information but (almost) no authorization information.</b></p> <p><b>Portal roles cannot be used in the Portal environment to create authorizations for the backend systems.</b></p> <p><b>Authorizations must still be maintained in the backend system.</b></p>

# Portal Role and ABAP Role Integration (Example)



# Comparison of Authorization related Objects



## Identity Management with SAP

- n Central User Administration
- n Directory Integration
- n Portal User Management Engine

## Role Management with SAP

- n ABAP Authorization Roles
- n J2EE / UME Authorization Roles
- n Portal Roles
- n Role Integration Example

## Summary



# Players: Identity and Access Management

## Identity Management:

Managing attributes of identities for a complex landscape, incl. those needed for security

User Lifecycle Mgmt  
Business Partner Integration  
Attribute Federation  
Administration Workflow  
Organizational Structure  
*Provisioning of User Info*

## Access management:

Centralized access control decision, to be enforced in all components

Authentication  
Single Sign-On  
Access Control  
Policy Definition  
Policy Enforcement  
*Provisioning of Authorization Info*

*“Legacy“ Integration Option*

SAP  
Applications

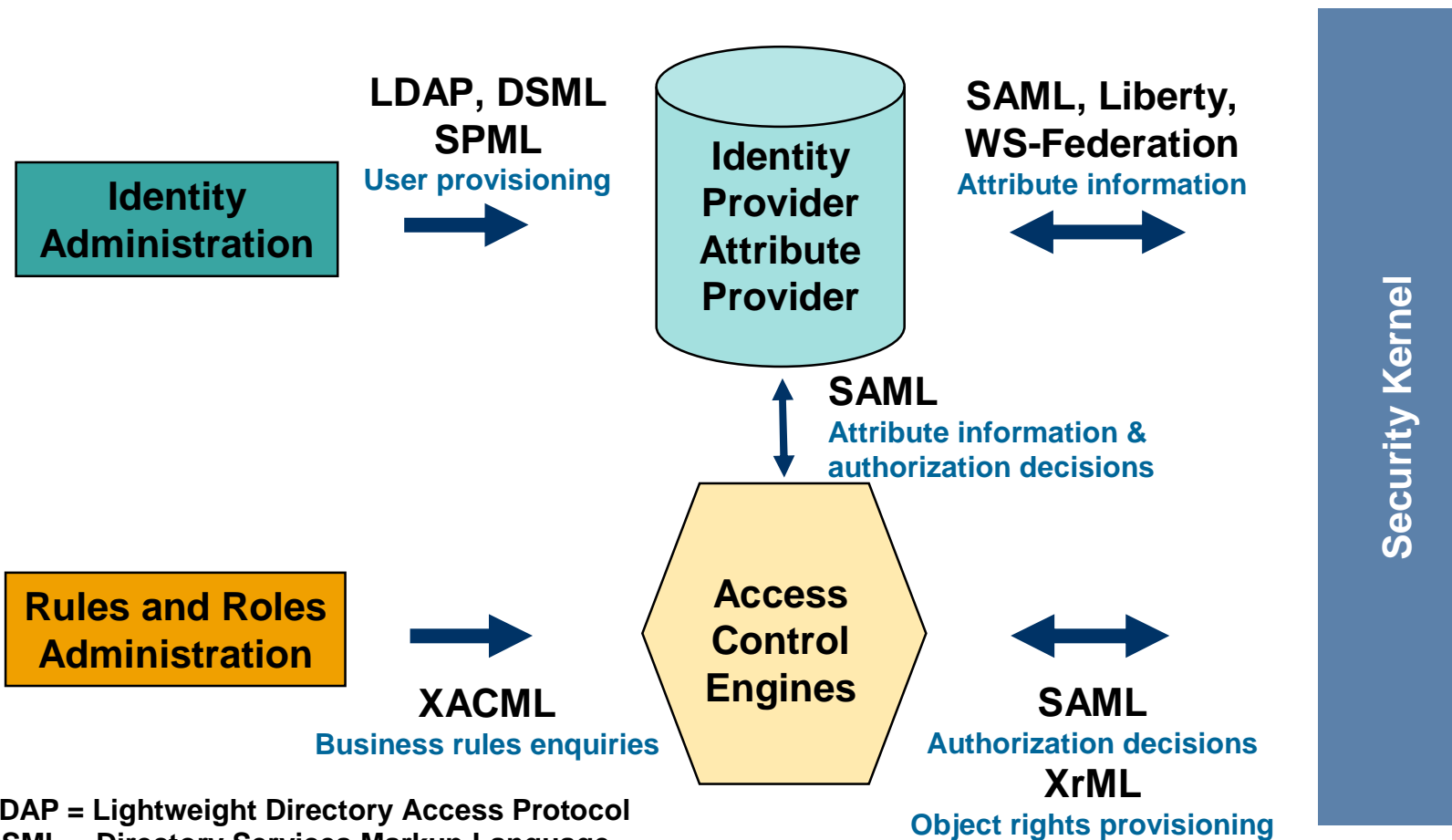
Application  
Infrastructure

Business Process  
Information

Web Services  
Choreography

Non-SAP  
Applications

# Standards: Identity and Access Management



LDAP = Lightweight Directory Access Protocol  
 DSML = Directory Services Markup Language  
 SPML = Service Provisioning Markup Language  
 SAML = Security Assertion Markup Language  
 XACML = eXtensible Access Control Markup Language  
 XrML = eXtensible rights Markup Language

## Identity Management with SAP

- n Central User Administration
- n Directory Integration
- n Portal User Management Engine

## Role Management with SAP

- n ABAP Authorization Roles
- n J2EE / UME Authorization Roles
- n Portal Roles
- n Role Integration Example

## SAP's strategy for Identity Management

- n **SAP leverages various user persistence store options**
- n **SAP allows for roles and authorizations with appropriate strength**
- n **SAP further enhances its Identity Management features and functions**
- n ***SAP will develop its own solution for the external user account provisioning application (for SAP and non-SAP applications) based on NetWeaver.***
- n ***The existing applications (Portal User Management Engine / Central User Administration / Directory Integration) will be an integral part of the new solution.***
- n ***Customers who use these applications follow exactly the recommendation of SAP***

# Q&A

 [security@sap.com](mailto:security@sap.com)

URL: <http://service.sap.com/security>



# *Appendix*

## J2EE supports two different Security Models

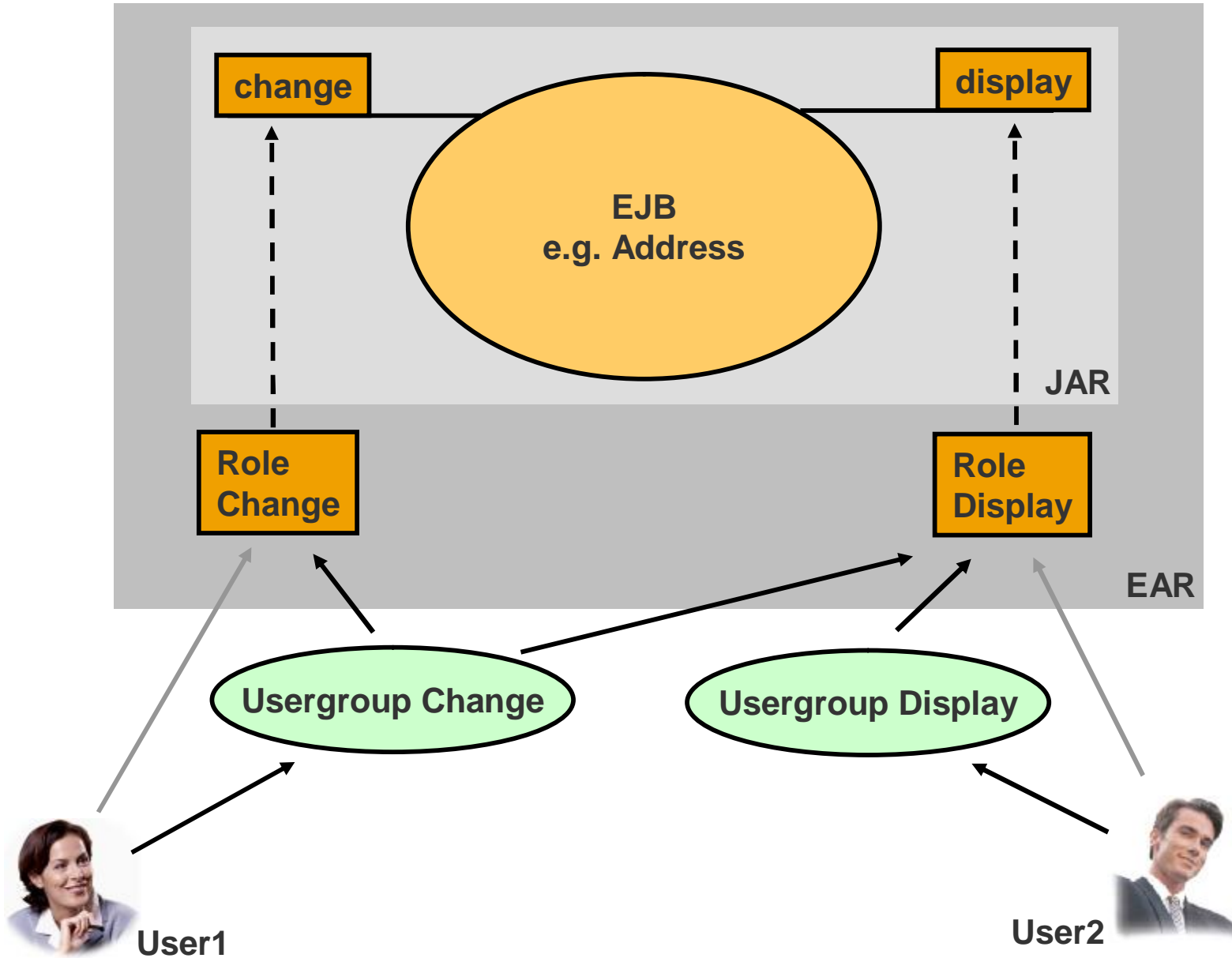
### n Declarative Security

- u Access control linked to the resource
- u Decouples Access Control from application logic
- u Easy to implement and maintain

### n Programmatic Security

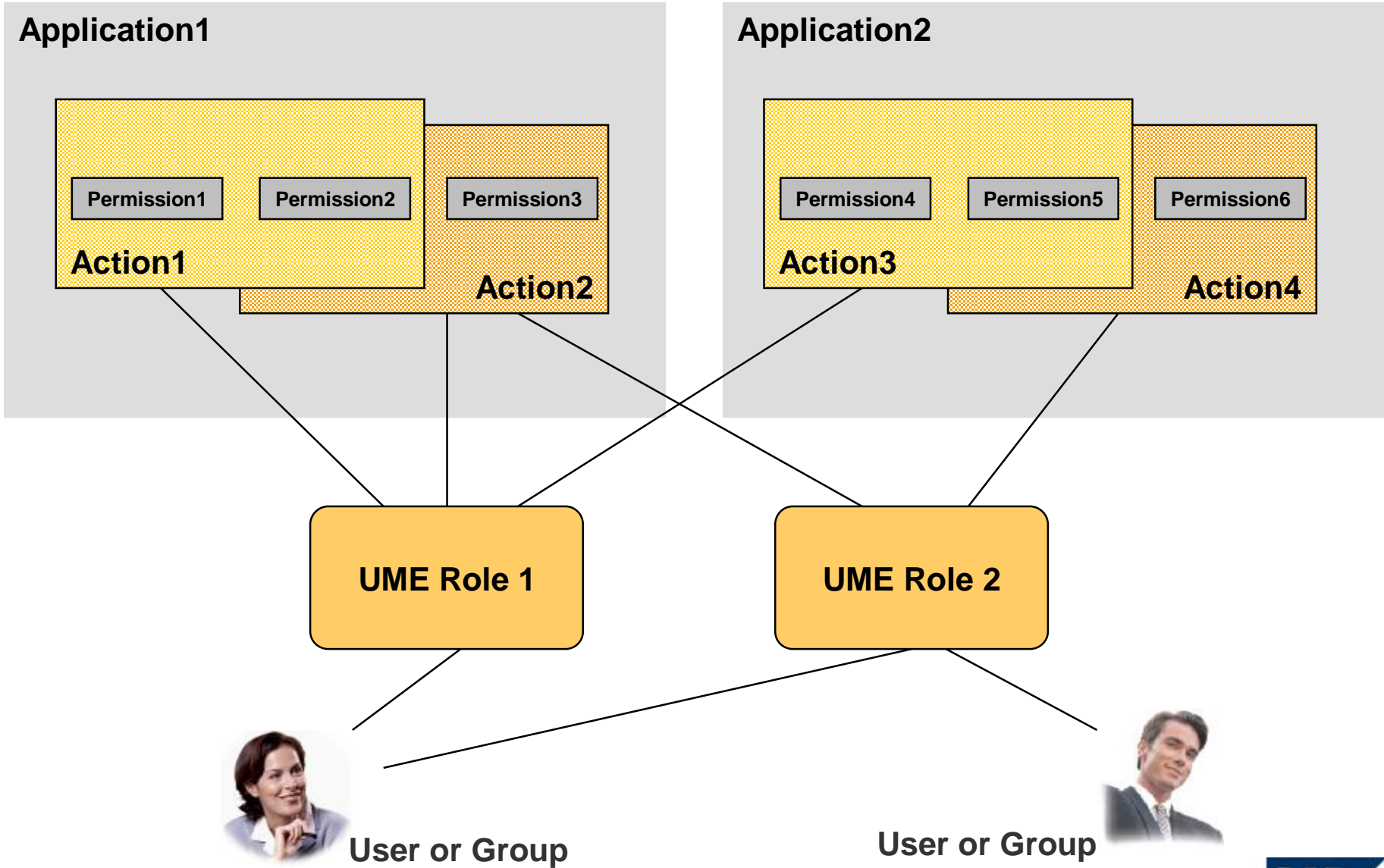
- u Access control within Java code
- u More flexible but linked to application logic
- u More work to implement

# J2EE Role Concept (Example) - Declarative Security





# UME Role Concept – Programmatic Security



- n 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.
- n Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.
- n Microsoft, Windows, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.
- n IBM, DB2, DB2 Universal Database, OS/2, Parallel Sysplex, MVS/ESA, AIX, S/390, AS/400, OS/390, OS/400, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere, Netfinity, Tivoli, and Informix are trademarks or registered trademarks of IBM Corporation in the United States and/or other countries.
- n Oracle is a registered trademark of Oracle Corporation.
- n UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.
- n Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.
- n HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.
- n Java is a registered trademark of Sun Microsystems, Inc.
- n JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.
- n MaxDB is a trademark of MySQL AB, Sweden.
- n SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver 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 are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.
- n These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.