Role & User Repositories in SAP NetWeaver / SAP Application Environments

NetWeaver RIG Expert Call

16 December 2004

Hartmut K. Goetze, SAP

Speaker

Hartmut Karl Goetze

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

Agenda

Identity Management with SAP

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

Role Management with SAP

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

SAP’s strategy for Identity Management

Summary

Learning Objectives

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

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

Agenda

Role Management with SAP

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

SAP's strategy for Identity Management

Summary

Identity Management: Customers' Vision

Central Identity Management

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

Provide Services and Delegated Administration Features for

- Authentication (policy-based)
- Single Sign-On
- Authorization (policy-based)
- Profile Management
- Provisioning 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 …

Central User Administration

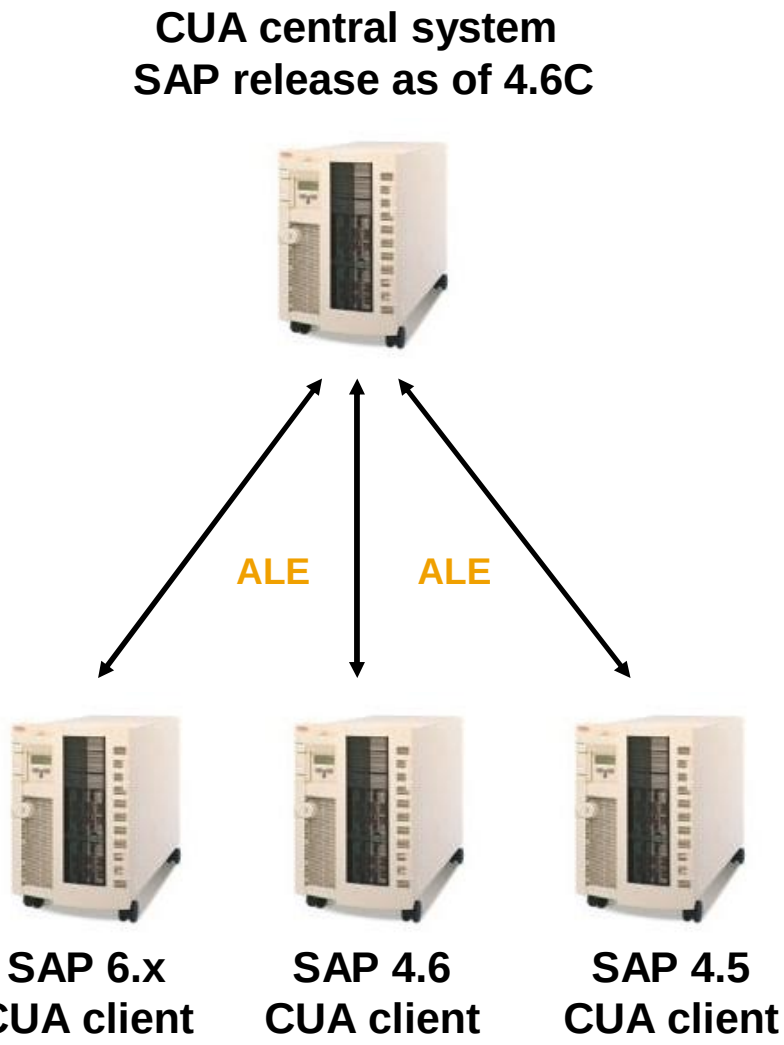
Users can be administrated in central SAP system

Automatic distribution to client SAP systems

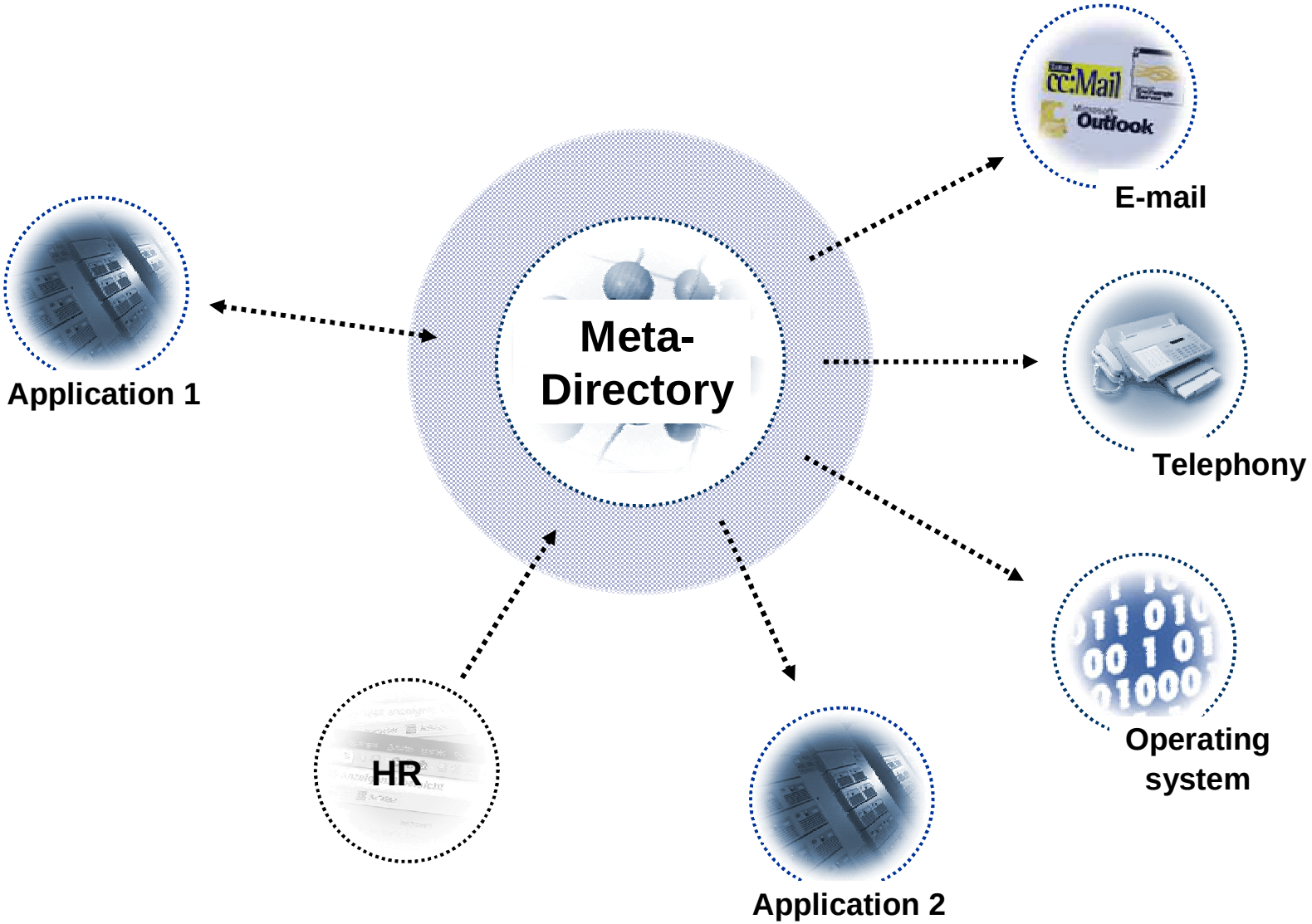
Local administration still possible (back distribution)

No inconsistencies

Central locks possible



User Management – Directory Integration



Directory Benefits

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.

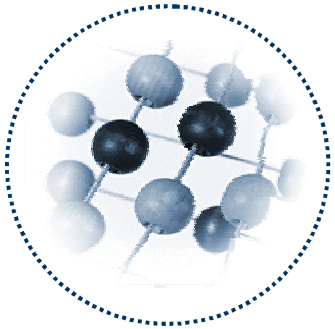
Access to this data is provided using the standardized Lightweight Directory Access Protocol (LDAP).

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



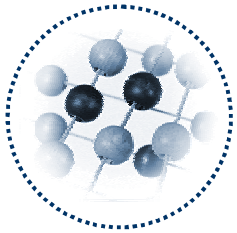
LDAP
synchronization

SAP ABAP System
release as of 6.10

HR Data Replication from SAP in an LDAP Enabled Directory Service

SAP Web AS as of 6.10

Directory



Replication

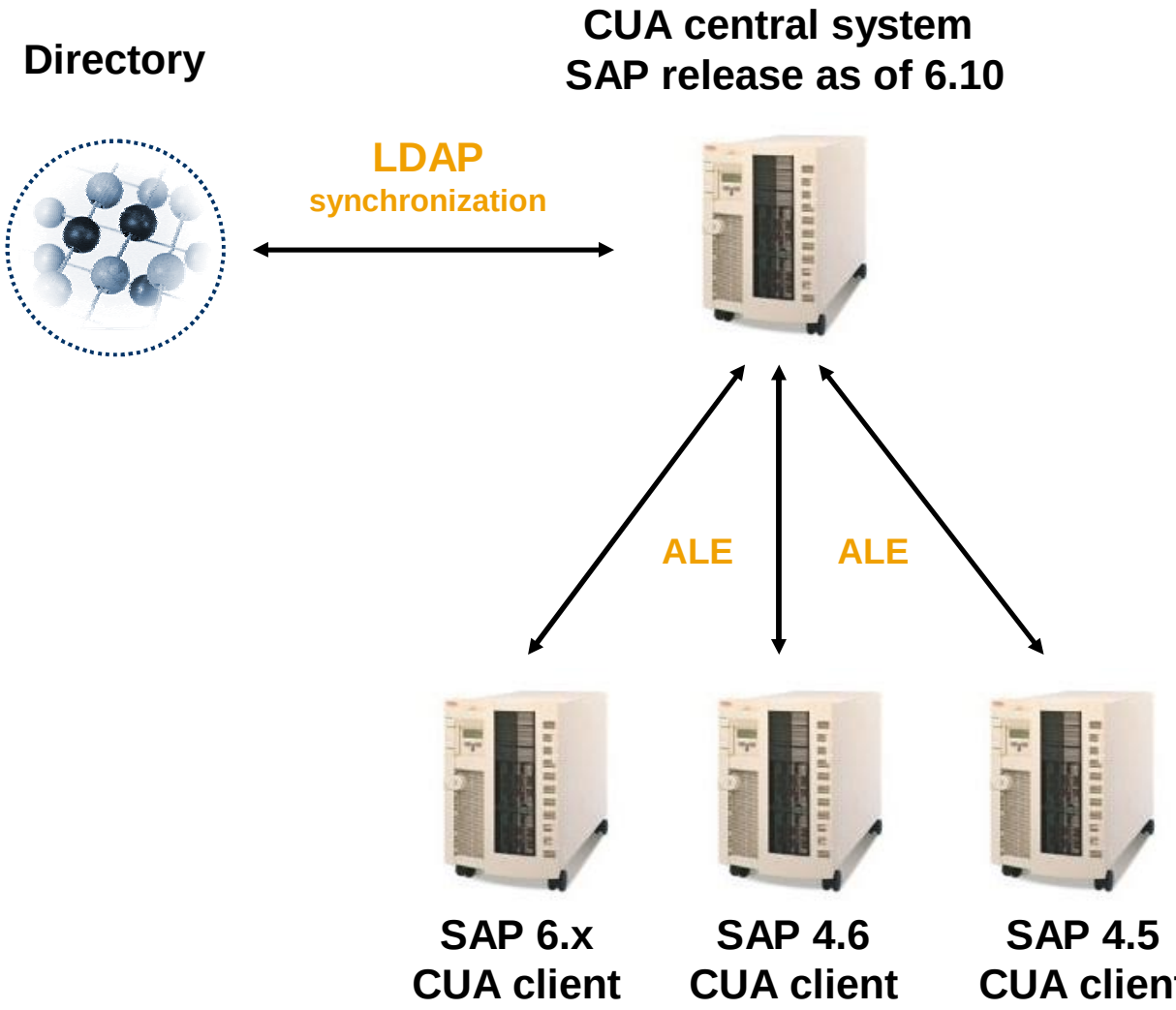
As of 4.70 HR can be connected directly to the LDAP directory

RFC

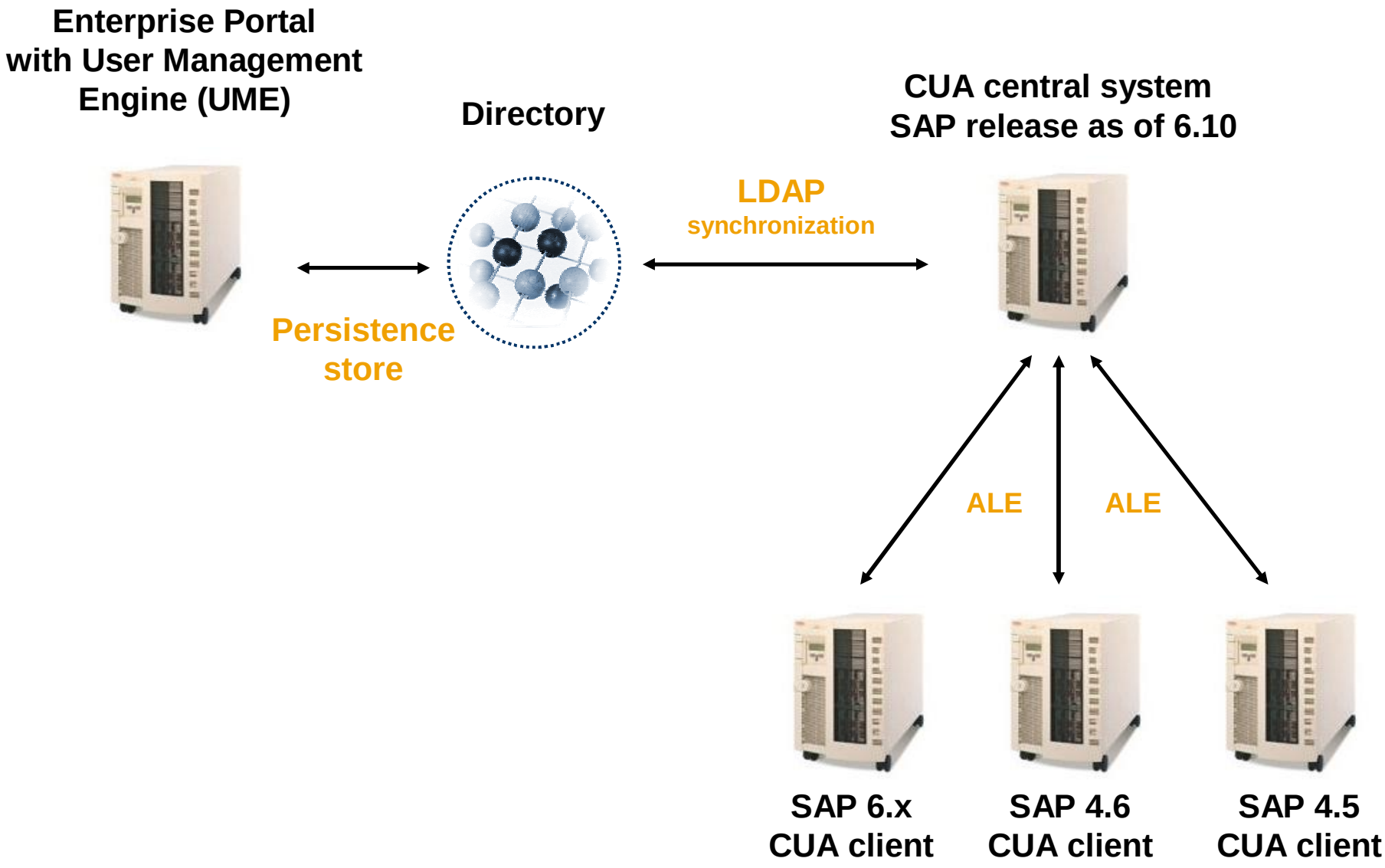
Data Retrieval in Personnel Management via Query or ABAP-Report

HR-system 4.0 and higher
with Plug-In System (PI 2001.2)
4.5 with Plug-In System (PI 2001.2)

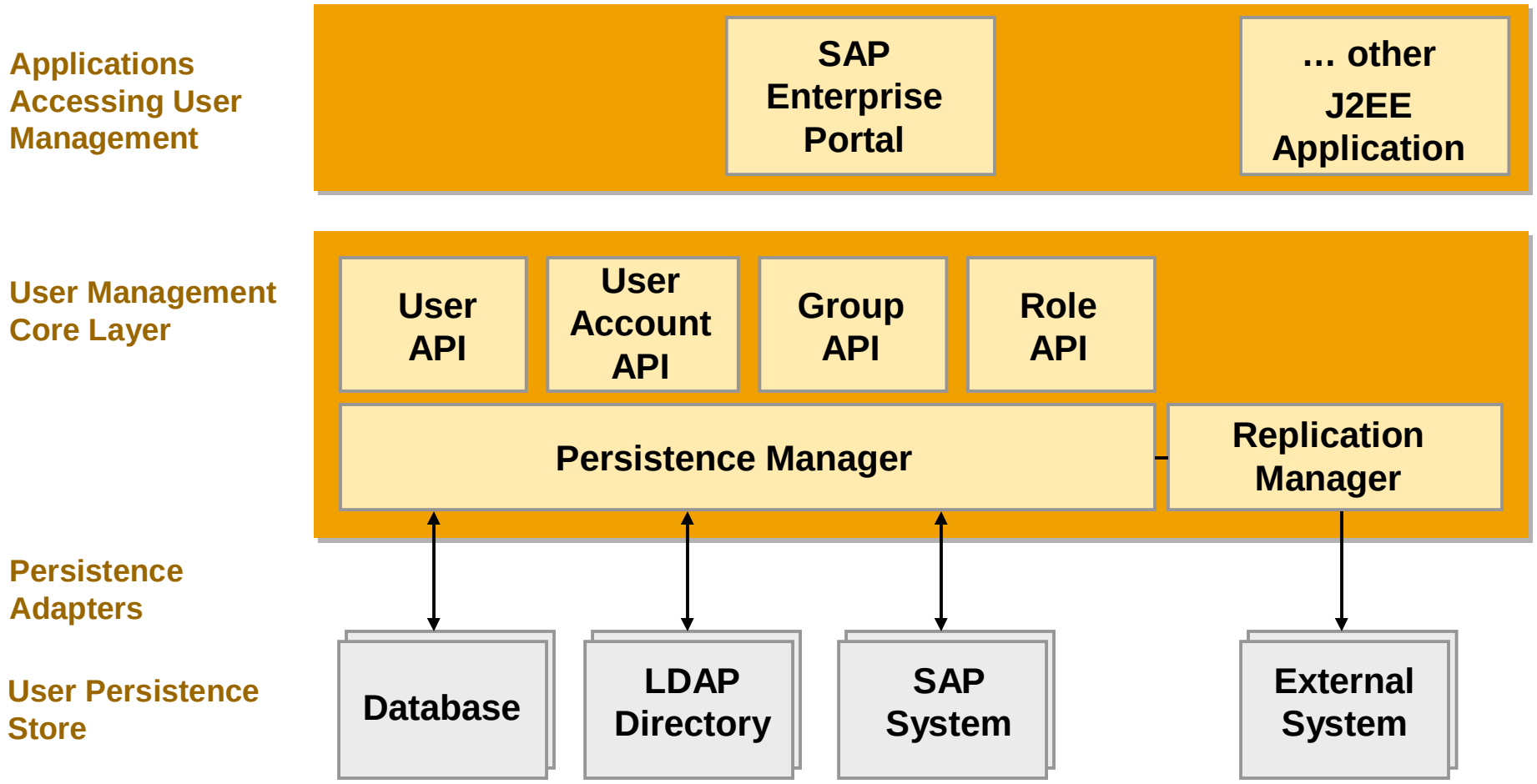
Central User Administration & LDAP Synchronization



CUA & LDAP Synchronization & Enterprise Portal



Architecture Overview – User Management Engine



Agenda

Identity Management with SAP

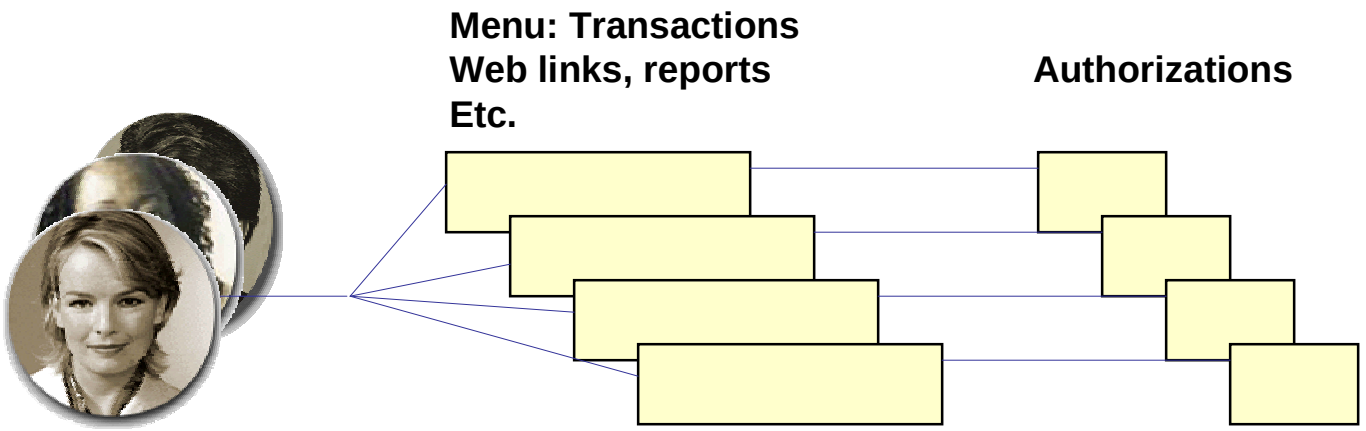
- Central User Administration
- Directory Integration
- Portal User Management Engine

SAP's strategy for Identity Management

Summary

ABAP Roles

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



SAP NetWeaver Portal Introduction

Role-based, …

Sales Manager

Line Manager

Business Developer

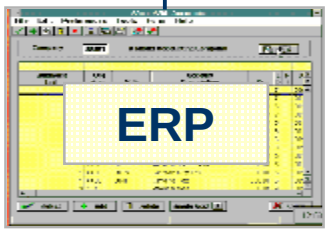
…secure…

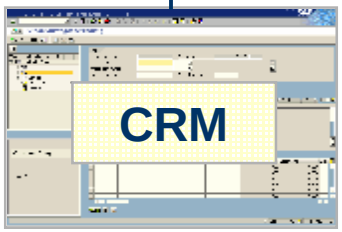
Authentication

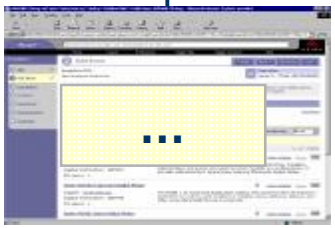
…and Web based…

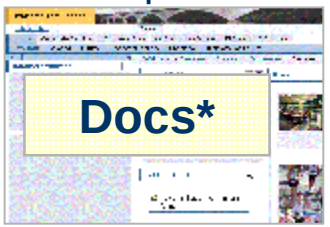
Single Sign On

…access to any kind of applications, information and services



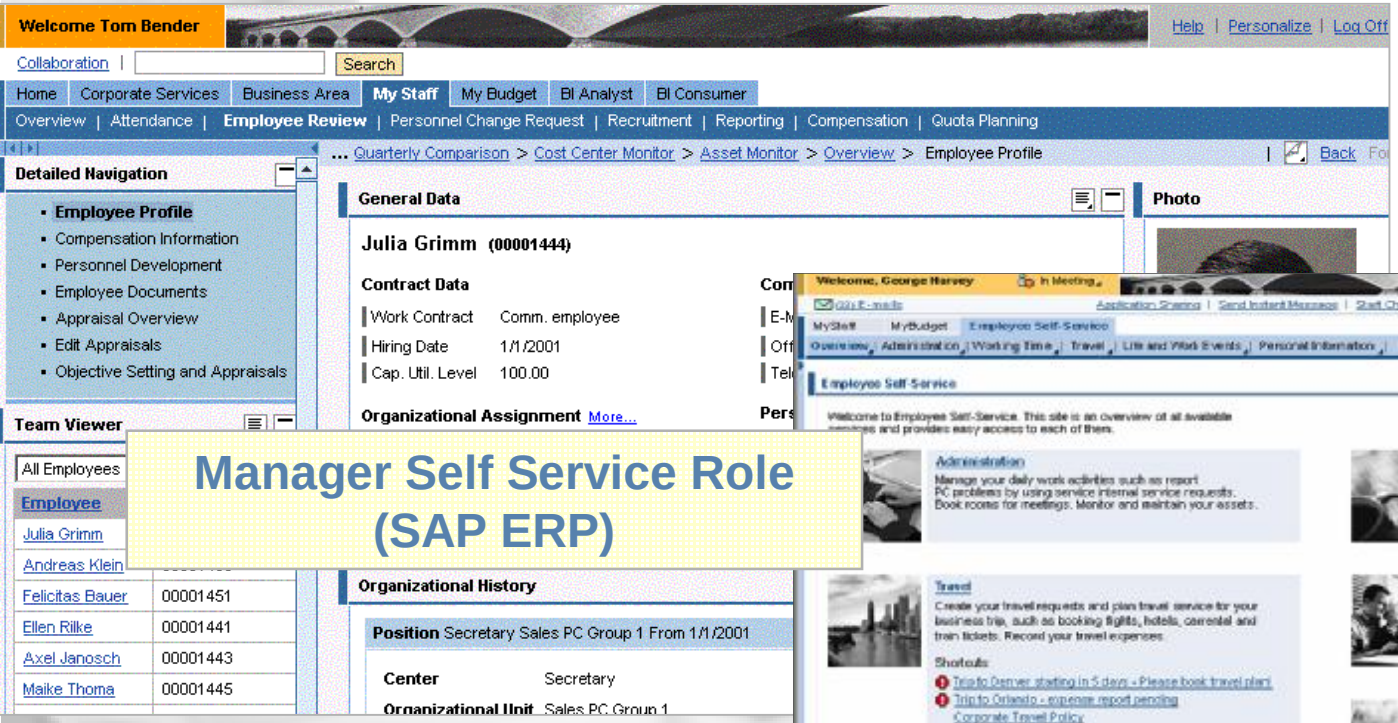




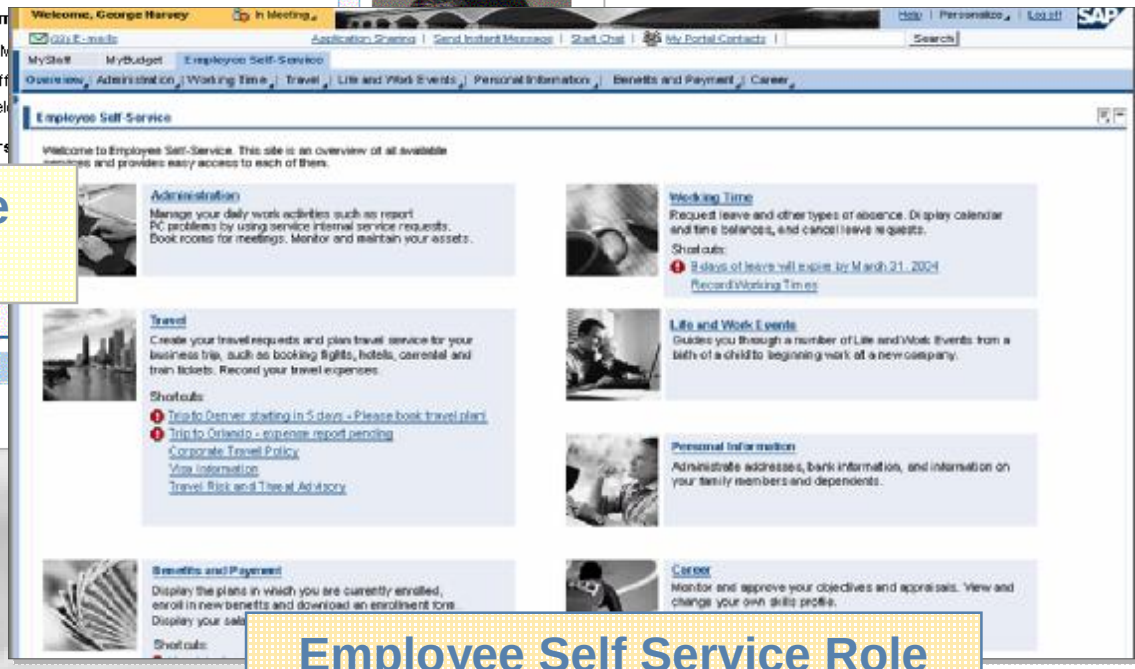


***covered by KM**

SAP NetWeaver powers mySAP Solutions
Role-specific, Easy Access to All Systems



Manager Self Service Role (SAP ERP)

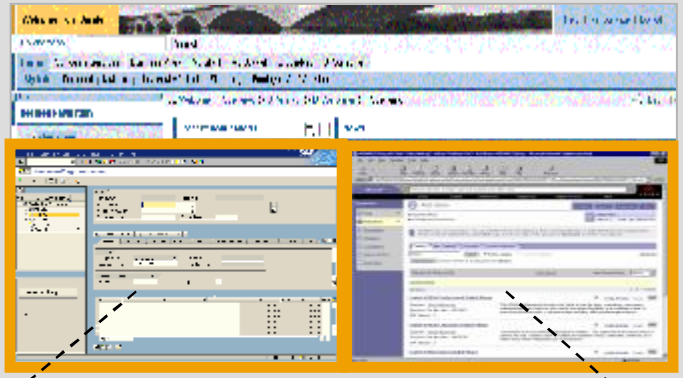


Employee Self Service Role (SAP ERP)

Overview SAP Roles

Portal Roles

… define, what is displayed in the Portal



ABAP Roles

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

UME Roles

or

J2EE Security Roles

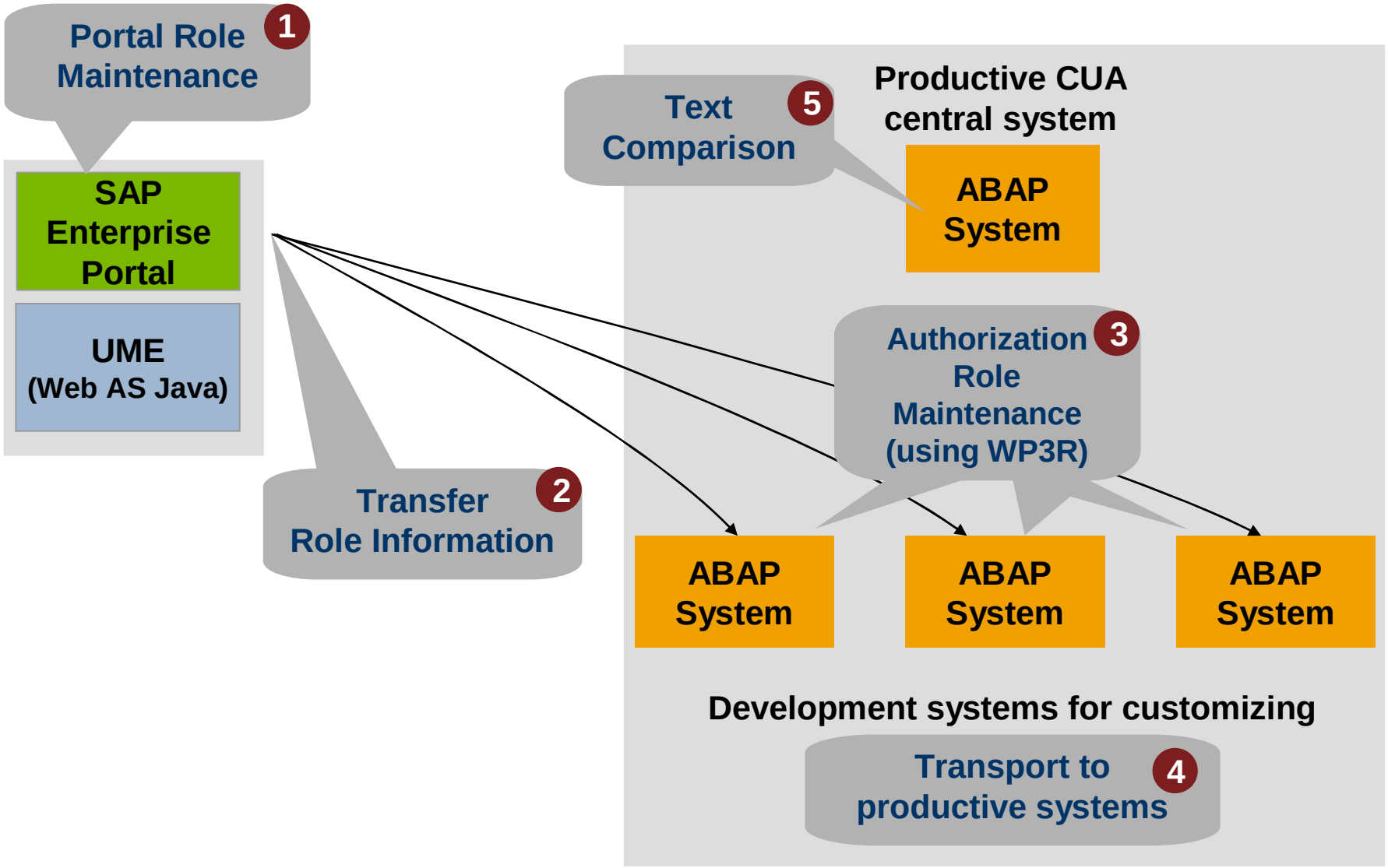
ABAP

J2EE

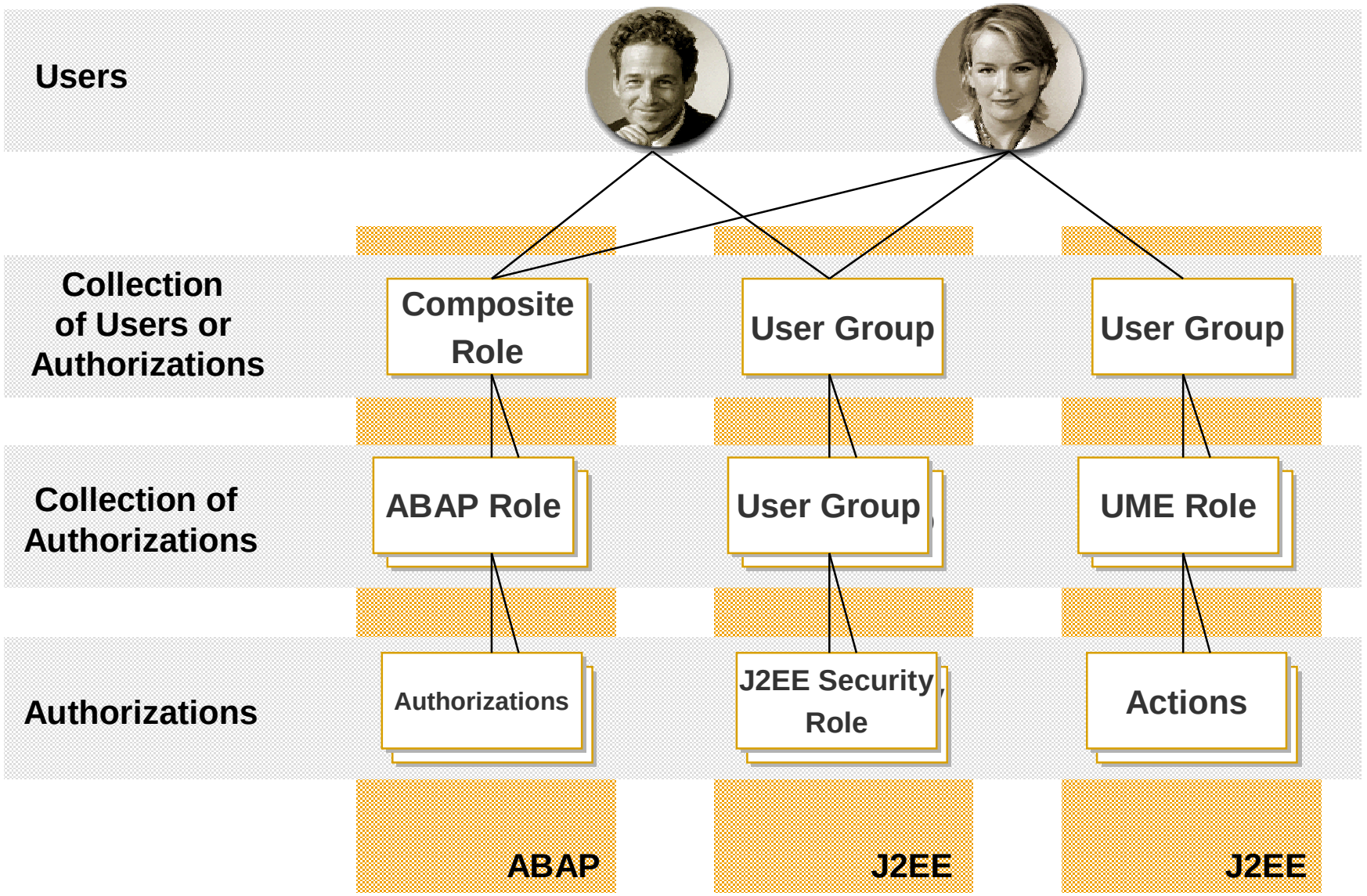
ABAP Roles and Portal Roles: A Comparison

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

Portal Role and ABAP Role Integration (Example)



Comparison of Authorization related Objects



Agenda

Identity Management with SAP

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

Role Management with SAP

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

Summary

Players: Identity and Access Management

Identity Management:

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

Access management:

Centralized access control decision, to be enforced in all components

"Legacy" Integration Option

User Lifecycle Mgmt

Business Partner Integration

Attribute Federation

Administration Workflow

Organizational Structure

Provisioning of User Info

Authentication

Single Sign-On

Access Control

Policy Definition

Policy Enforcement

Provisioning of Authorization Info

SAP Applications

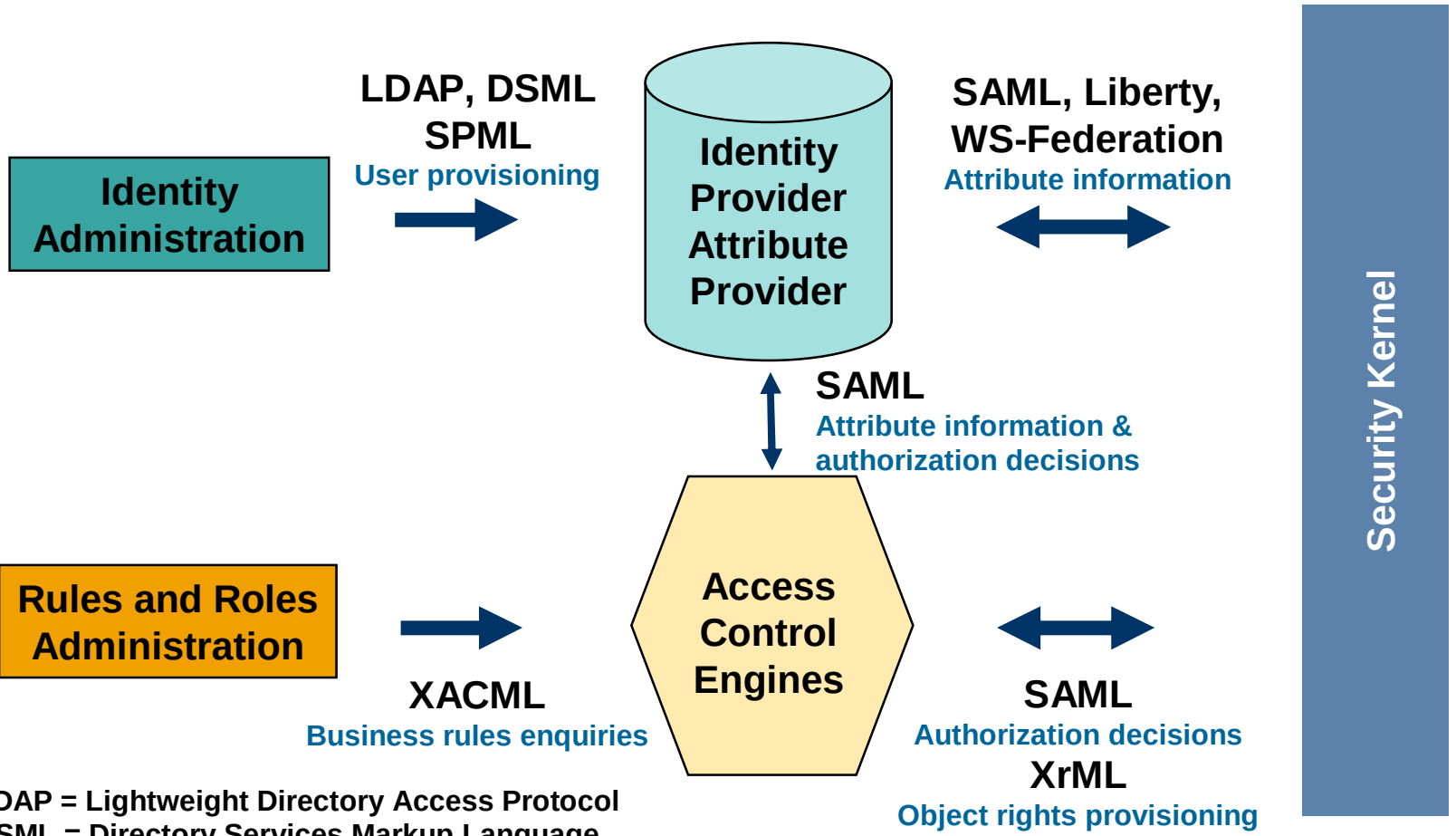
Application Infrastructure

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

Agenda

Identity Management with SAP

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

Role Management with SAP

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

SAP's strategy for Identity Management

Summary

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

Questions?

Q&A

security@sap.com

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

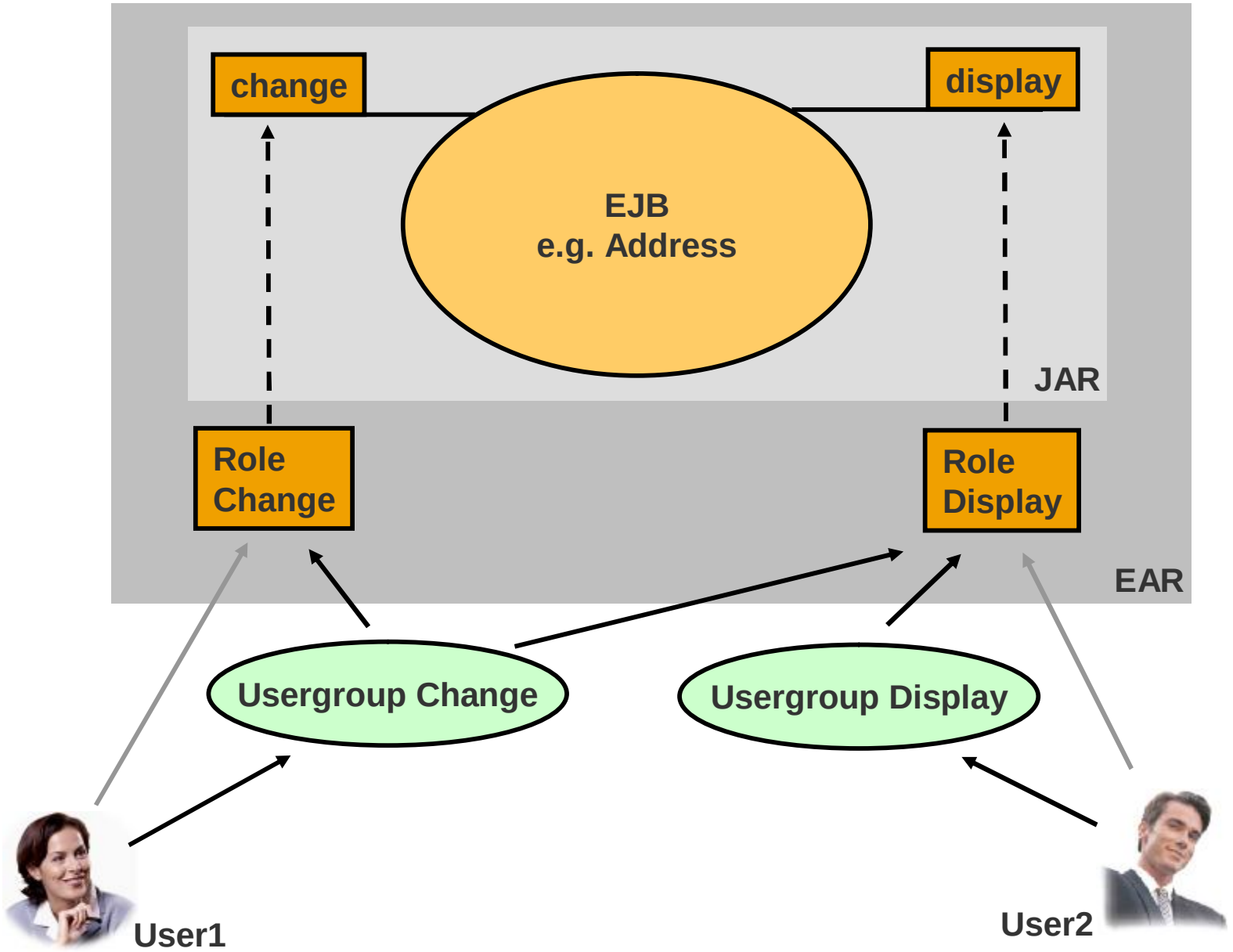
Appendix

J2EE Security Security Models

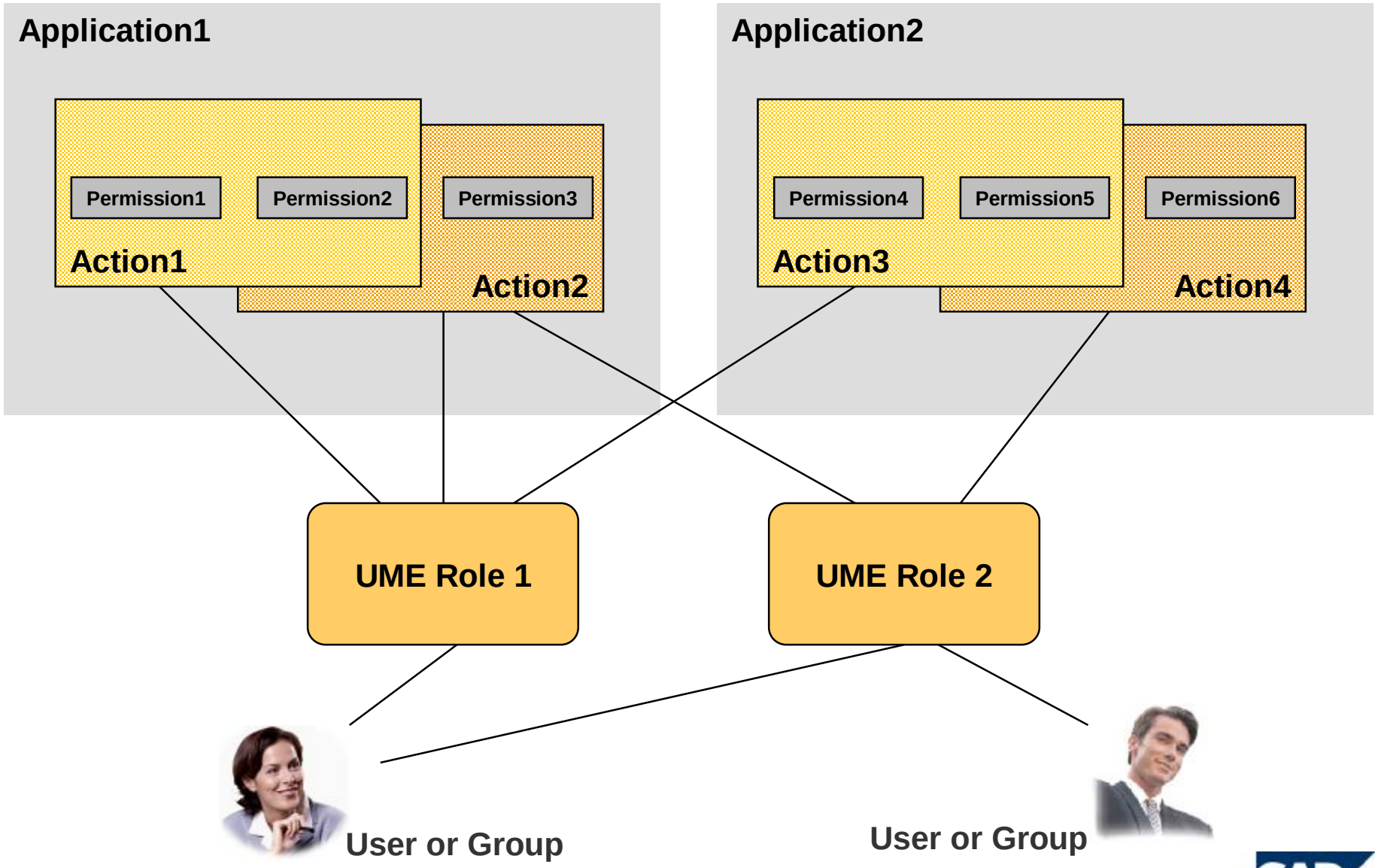
J2EE supports two different Security Models

- **Declarative Security**
  - Access control linked to the resource
  - Decouples Access Control from application logic
  - Easy to implement and maintain
- **Programmatic Security**
  - Access control within Java code
  - More flexible but linked to application logic
  - More work to implement

J2EE Role Concept (Example) - Declarative Security



UME Role Concept – Programmatic Security



Copyright 2004 SAP AG. All Rights Reserved