Session ID: SCUR102
User Management and Authorizations Overview
Contributing Speakers

TechEd San Diego:

Larry Justice
Security Consultant, SAP America

Jens Koster
Security Product Manager, SAP AG

Gerlinde Zibulski
Security Product Manager, SAP Labs LLC

TechEd Munich:

Frank Buchholz
Security Product Manager, SAP AG

Jens Koster
Security Product Manager, SAP AG

Oliver Nocon
Portal RIG Consultant, SAP AG
Agenda

Identity and Role Management with SAP
- Central User Administration
- Directory Integration
- Portal User Management Engine

User and Role Management for J2EE Web Applications
- User Management Engine
- J2EE Security Roles
- UME Roles

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 Central User Administration
- Directory integration
- User Management Engine
- Portal roles
- Role management in ABAP and Java-based systems
Agenda

Identity and Role Management with SAP
- Central User Administration
- Directory Integration
- Portal User Management Engine

User and Role Management for J2EE Web Applications
- User Management Engine
- J2EE Security Roles
- UME Roles

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
- Authentication (policy-based)
- Single sign-on
- Authorization (policy-based)
- Profile management
- Provisioning for legacy systems

IM done through one centralized component
Decentralized User Maintenance

Each SAP System has its own user data store

→ Decentralized user maintenance

→ Inconsistencies can occur between address data
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

CUA central system
SAP release as of 4.6C
ABAP Roles

Single roles (and the corresponding authorization profiles) are created in the CUA client systems.

Composite roles can be used either in the CUA client systems or in the CUA central system.
Portal Roles

- A portal role is a container for applications and information that can be assigned to a particular group of users.
- The content of a role enables users to perform the tasks belonging to their job description.
- The content of a portal role is based on the company structure and on the information needs of the portal users in the company.
- The portal navigation structure is defined by the sum of the roles assigned to the user.
- Technically, a role is a hierarchy of folders containing other portal content objects.
- Roles can be assigned to users or groups of users, i.e. the portal role connects users (or groups of users) to the portal content.
- Introduction of Worksets as a new layer in a role hierarchy.
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.
HR Data Replication from SAP
in an LDAP-Enabled Directory Service

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

Data Retrieval in Personnel Management via Query or ABAP-Report

SAP Web AS as of 6.10

Directory

Replication

RFC

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

Directory

CUA central system
SAP release as of 6.10

LDAP synchronization

ALE

SAP 6.x
CUA client

SAP 4.6
CUA client

SAP 4.5
CUA client
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

SAP 6.x CUA client

SAP 4.6 CUA client

SAP 4.5 CUA client

© SAP AG 2004, SAP TechEd / SCUR102 / 15
SAPNetWeaver Portal Infrastructure

Role-based, ...

...secure...

...and Web-based...

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

Authentication

SAP Enterprise Portal 6.0

Single Sign On

ERP

CRM

Docs*

*covered by KM

Sales Manager

Line Manager

Business Developer

© SAP AG 2004, SAP TechEd / SCUR102 / 16
SAP NetWeaver Powers mySAP Solutions
Role-Specific, Easy Access to All Systems

Manager Self Service Role (SAP ERP)

Employee Self Service Role (SAP ERP)
Architecture Overview – User Management Engine

Applications
Accessing User Management

User Management
Core Layer

Persistence
Adapters

User Persistence
Store

SAP Enterprise Portal

User API
User Account API
Group API
Role API

Persistence Manager

Replication Manager

Database
LDAP Directory
SAP System
External System
Main Role Concepts in SAP NetWeaver

SAP Enterprise Portal

Generate Authorization Roles in ABAP from User Interface Roles in the Portal

Roles in ABAP-based systems (roles in transaction PFCG)

Portal roles

Single and composite roles in ABAP-based systems
## ABAP Roles and Portal Roles: A Comparison

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

Identity and Role Management with SAP
- Central User Administration
- Directory Integration
- Portal User Management Engine

User and Role Management for J2EE Web Applications
- User Management Engine
- J2EE Security Roles
- UME Roles

SAP’s Strategy for Identity Management

Summary
Usage of UME by applications in SAP J2EE 6.40

- SAP J2EE Engine
- UME
- Database
- LDAP Directory
- ABAP Stack
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

- EJB e.g. Address
- Role Change
- Role Display
- Usergroup Change
- Usergroup Display
- User1
- User2

JAR
EAR
UME Role Concept – Programmatic Security

Application 1

- Permission 1
- Permission 2
- Permission 3

Action 1

- Action 1
- Action 2

Permission 4

Permission 5

Permission 6

Application 2

Action 3

Action 4

UME Role 1

UME Role 2

User or Group

User or Group

© SAP AG 2004, SAP TechEd / SCUR102 / 25
Agenda

Identity and Role Management with SAP
- Central User Administration
- Directory Integration
- Portal User Management Engine

User and Role Management for J2EE Web Applications
- User Management Engine
- J2EE Security Roles
- UME Roles

SAP’s strategy for Identity Management

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

SAP Applications
Application Infrastructure
Business Process Information
Web Services Choreography

Non-SAP Applications

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
Standards: Identity and Access Management

Identity Administration
- LDAP, DSML
- SPML
- User provisioning

Access Control Engines
- XACML
- Business rules enquiries

Identity Provider Attribute Provider
- SAML
- Attribute information & authorization decisions

Rules and Roles Administration
- SAML, Liberty, WS-Federation
- Attribute information

Security Kernel
- XrML
- Object rights provisioning

Standards: Identity and Access Management
Agenda

Identity and Role Management with SAP
- Central User Administration
- Directory Integration
- Portal User Management Engine

User and Role Management for J2EE Web Applications
- User Management Engine
- J2EE Security Roles
- UME Roles

SAP’s strategy for Identity Management

Summary
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 plans to 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
Further Information (San Diego)

Public Web:

www.sap.com
SAP Developer Network: www.sdn.sap.com ➔ SAP NetWeaver Platform ➔ Security
SAP Customer Services Network: www.sap.com/services/

Related SAP Education Training Opportunities

http://www.sap.com/usa/education/ ADM940-960

Related Workshops/Lectures at SAP TechEd 2004

SCUR351, User Management and Authorizations : The Details
Wed, 2:00 PM - 6:00 PM, 31A
Fri, 8:00 AM - 12:00 PM, 30D

SCUR101, Security Basics
Tue, 1:30 PM - 2:30 PM, 2
Wed, 4:00 PM - 5:00 PM, 4

SCUR251, Single Sign-On in Heterogeneous Landscapes
Wed, 10:30 AM - 12:30 PM, 30C
Thu, 1:45 PM - 3:45 PM, 30A

SCUR202, Security Optimization Service
Wed, 9:15 AM - 10:15 AM, 6C
Thu, 9:15 AM - 10:15 AM, 9

PRTL152, Portal Roles – Roles vs. Authorizations
Wed, 1:45 PM - 3:45 PM, 30A
Thu, 8:00 AM - 10:00 AM, 30B
Further Information (Munich)

Public Web:

www.sap.com
SAP Developer Network: www.sdn.sap.com ➔ SAP Netweaver Platform ➔ Security
SAP Customer Services Network: www.sap.com/services/

Related SAP Education Training Opportunities

http://www.sap.com/education/ ADM940-960

Related Workshops/Lectures at SAP TechEd 2004

SCUR351, User Management and Authorizations: The Details
Thu, 9:00 AM - 1:00 PM, HO01

SCUR202, Security Optimization Service
Wed, 5:00 PM - 6:00 PM, L1
Look for SAP TechEd ’04 presentations and videos on the SAP Developer Network.

Coming in December.

http://www.sdn.sap.com/
Feedback

Please complete your session evaluation.

Be courteous — deposit your trash, and do not take the handouts for the following session.

Thank You!