Contributing Speakers

TechEd Vienna

Frank Buchholz  
Security Product Manager, SAP AG

Jens Koster  
Security Product Manager, SAP AG

TechEd Boston

Gerlinde Zibulski  
Security Product Manager, SAP Labs LLC
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

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
Decentralized User Maintenance

Each SAP System has its own user data store

→ Decentralized user maintenance

→ Inconsistencies can occur between address data

SAP R/3 Enterprise
SAP EBP
SAP BW
SAP APO
SAP...

© SAP AG 2005, SAP TechEd '05 / AGS101 / 6
Central User Administration

- Users can be administrated in central SAP system
- Automatic distribution to client SAP systems
- Local administration still possible (redistribution)
- No inconsistencies
- Central locks possible

CUA central system
SAP release as of 4.6C

ALE

ALE

SAP 6.x
CUA client

SAP 4.6
CUA client

SAP 4.5
CUA client
User Management – Directory Integration

- Application 1
- Meta-Directory
- Application 2
- E-mail
- Telephony
- Operating system
- HR
LDAP Synchronization

Directory

SAP ABAP System release as of 6.10

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

Directory

SAP Web AS as of 6.10

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

LDAP synchronization

Directory

CUA central system
SAP release as of 6.10

LDAP synchronization

ALE

ALE

SAP 6.x
CUA client

SAP 4.6
CUA client

SAP 4.5
CUA client

© SAP AG 2005, SAP TechEd '05 / AGS101 / 11
CUA & Enterprise Portal (no Directory)

Enterprise Portal with User Management Engine (UME)

CUA central system
SAP release as of 6.10

SAP J2EE Engine
Persistence store

SAP CUA client

SAP ABAP + J2EE Engine

SAP NetWeaver CUA client

SAP 4.6 CUA client

SAP 4.5 CUA client

ALE

ALE

ALE
SAP Identity Management and Siemens Identity Management

Enterprise Portal with User Management Engine (UME)

Central User Administration

SAP HR

Provisioning incl. SPML integration*

Provisioning

HiPath Security DirX Identity Management

DirX Identity DirX Directory

Password Management
Self-service
Metadirectory
Audit

Provisioning and Synchronization
Account and group management, validation and reconciliation

E-mail

Telephony

Operating system

Non-SAP applications

*SPML integration available as of SAP NetWeaver NW 2004s SPS5 und NW 2004 SPS14
Siemens HiPath S1curity DirX and DirX Identity complement SAP NetWeaver with Identity Management for heterogeneous landscapes.

The solution provides uniform identity provisioning for the SAP Enterprise Portal and all SAP applications as well as non-SAP applications.

SAP ships Siemens HiPath S1curity DirX and HiPath S1curity DirX Identity demo license starting with NetWeaver 2004s ramp-up phase.

Customer Benefits:
- Secure and centralized management of user identities and their access rights for all enterprise applications.
- Regulatory compliance.
- Increased operational efficiency and end user productivity.
- Reduced administration and help-desk costs.
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 NetWeaver Enterprise Portal

Role-based, ...

...secure...

...and Web based...

SAP Enterprise Portal 6.0

Authentication

Single Sign On

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

ERP

CRM

Docs*

*covered by KM
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

Java
# ABAP Roles and Portal Roles: A Comparison

<table>
<thead>
<tr>
<th>ABAP Authorization 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 the role administration in transaction PFCG.</td>
<td>Authorization must still be maintained in the backend system.</td>
</tr>
<tr>
<td>The content of Authorization Roles can be generated using the definition of Portal Roles.</td>
<td></td>
</tr>
</tbody>
</table>
Scenarios for Role Integration

When using different SAP components, different scenarios for managing identities are possible.

The following slides describe an example with the following components:

- SAP Enterprise Portal
- ABAP based SAP Systems
- Directory Server

Scenario A:
- The administrators uses the UME to maintain users and portal role assignments
- Portal roles and related ABAP authorization roles are linked together
- The system ensures that necessary ABAP authorization roles are assigned, too

Scenario B:
- The administrators uses the CUA to maintain users and role assignments
- Portal roles and related ABAP roles are linked together
- The system ensures that necessary Portal roles are assigned, too
Scenario A: Role Maintenance

1. Portal Role Maintenance

2. Transfer Role Information

3. Authorization Role Maintenance (using WP3R)

4. Transport to productive systems

5. Transfer Role Information to CUA

Development systems for customizing

SAP ABAP + J2EE Engine

CUA
Scenario A: User Management based on a Directory

1. User Maintenance
2. Portal Role Assignment
3. Synchronize User Data
4. Publish Role Assignment
5. Authorization Role Assignment using transaction WP3R
6. Users get roles in backend systems

Enterprise Portal
Directory
SAP ABAP + J2EE Engine
CUA
LDAP synchronization
ALE
ALE
Synchronize User Data
Portal Role Assignment
User Maintenance
Scenario B: Role Maintenance

1. Portal Role Maintenance

2. Maintain auth. role templates for the Portal

3. Authorization Role Maintenance (using PFCG)

4. Transport to productive systems

5. Role - Group Assignment

SAP backend Authorization Role EQUALS Group in the Enterprise Portal!

Enterprise Portal

Persistence store

Development systems for customizing

SAP ABAP + J2EE Engine

© SAP AG 2005, SAP TechEd '05 / AGS101 / 23
Scenario B: User Management based on the CUA

SAP backend Authorization Role EQUALS Group in the Enterprise Portal!

Persistence store

User Maintenance

Role Assignment

ALE ALE

Users get groups and indirect roles in the Portal

Users get authorization roles in the backend systems

SAP ABAP + J2EE Engine
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
Central Person (ABAP)

Terms of Employment
- Employee
- Holder
  - Central Attributes
    - Name
    - Identification
    - Addresses
  - ... (Add. Attributes)

Personnel Administration
- Personnel Administration
  - Terms of Employment
  - Organization Management

R/3 User Account
- R/3 User Account
  - ... (Add. Attributes)

Portal User Account
- Portal User Account
  - ... (Add. Attributes)

User Management

Organizational Management
- Organization Management
  - Position 1
  - Position 2
  - Position 3
  - Unit A / Faculty A
  - Unit B / Faculty B

Customer Data Sets
- Customer Data Sets
  - ... (Add. Attributes)

CRM
Identity Provisioning – Big Picture

Data Sources for Identities

Central Identity Management

Provisioning

Identity Model

Inbound

Outbound

Provisioning Interface (SPML)

SAP HR

SAP CRM

J2EE Engine

ABAP System

SAP Web AS ABAP+Java

LDAP Directory

Target Systems for Provisioning

Non-SAP System

Partner Provisioning System

ABAP System

J2EE Engine

Non-SAP System
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
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 (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.
Further Information (Boston)

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 2005

AGS351, User Management and Authorizations – The Details
AGS103, Identity Management – Streamlining the User Provisioning Process
Between HR, LDAP, and CUA
AGS104, SAP MIC Tool – SAP NetWeaver in Support of Sarbanes-Oxley
Requirements
AGS105, Security Primer
AGS201, Sarbanes-Oxley Compliance – Challenges and Benefits
CD261, Using Authorizations in Java Application Development
Further Information (Vienna)

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 2005

- AGS104 SAP MIC Tool – SAP NetWeaver in Support of Sarbanes-Oxley Requirements
  Fri, 9:15 a.m. – 10:15 a.m., L3
- AGS106 Virus Scanning of Documents in SAP Applications
  Thu, 6:00 p.m. – 7:00 p.m., L3
- AGS200 Increasing Infrastructure Security by using Application Gateways
  Fri, 10:45 a.m. – 12:45 p.m., L4
- AGS202, Security in SAP Internet Transaction Server (ITS) Landscapes
  Fri, 11:45 a.m. – 12:45 p.m., L3
- AGS350, Configuring J2EE & SAP NetWeaver Portal UME Authentication
  Thu, 2:15 p.m. – 4:15 p.m., H2
SAP Developer Network

SAP NetWeaver Security

SAP Security Newsletter, July Edition
28 July 2005

Now available on SDN, the July issue of the SAP Security Newsletter highlights recent news and product information pertaining to SAP NetWeaver and SAP security.

What is Identity Management?
30 Jun 2005

"Identity management" is a phrase buzzing around in the emerging area of Enterprise Security Management. SAP Security Product Manager GerHilde Thirkill explains the significance and benefits of identity management, what to consider in a project involving identity management, and how SAP helps you support identity management within your system landscape.

Popular Documents
Updated 28 Jul 2005

- How to Set Up SSO Between SAP BusinessObjects and SAP NetWeaver Portal (PDF 72 KB)
- SAP Security Newsletter – May 2005 (PDF 36 KB)
- SAP Security Newsletter – June 2005 (PDF 50 KB)
- How to Set Up Single Sign-On Between an IBM

Germany Hosts "Survival for Programmers" Event
21 Jul 2005

"Survival for Programmers," an event presented by Germany’s "Secure it! Ask [sic]" program, targets students, professors, and anyone else interested in secure programming and running applications safely. SAP and Microsoft experts lead emerging initiatives and workshops demonstrating key issues on application security. Get event details and register now. Participation is free, but space is limited.

Creating a .NET Client for an SAP Java Web Service
2 June 2005

Based on an interoperability scenario between Microsoft and SAP, a .NET application client is created using KeyStore and X.509 certificate management, and the application is then deployed to a production environment. A small .NET client is created that can send secure messages to the Java Web Service using Microsoft WS-Addressing and Java JSR-111.

Featured Weblog

Security Considerations for ISDN Communication with SAP XI

http://www.sdn.sap.com/
Q&A

security@sap.com

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

Please complete your session evaluation.

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

Thank You!
Appendix
Comparison of Authorization related Objects

- **Users**
  - Composite Role
  - User Group
  - User Group

- **Collection of Users or Authorizations**
  - ABAP Role
  - User Group
  - UME Role

- **Collection of Authorizations**
  - Authorizations
  - J2EE Security Role
  - Actions

- **Authorizations**
  - ABAP
  - J2EE
  - J2EE
J2EE supports two different security models

- **Declarative security (Standard J2EE Security Roles)**
  - Access control linked to the resource (executables)
  - Decouples access control from application logic
  - Easy to implement and maintain

- **Programmatic security**
  (SAP specific Permission, Action, UME Role)
  - Access control within Java code
  - More flexible but linked to application logic
  - More work to implement

**SAP adds its well known role concept to J2EE applications**

- Java programs reuse business services in ABAP and inherit the ABAP authorization concept
J2EE Role Concept (Example) – Declarative Security

Method: change

EJB
e.g. Java program to display / maintain something

Method: display

J2EE Security Role: Change

J2EE Security Role: Display

User Group: CHANGE

User Group: DISPLAY

User1

User2
UME Role Concept – Programmatic Security

Application1

- Permission1
- Permission2
- Permission3

Action1

Action2

Application2

- Permission4
- Permission5
- Permission6

Action3

Action4

UME Role 1

UME Role 2

User or Group

User or Group
ABAP and Java together

Program flow with authorization checks in both ABAP and Java

Connectivity between ABAP and Java

Business relevant authority check based on ABAP roles

Business relevant authority check based on UME roles