Agenda

Introduction to Identity Management

SAP NetWeaver Identity Management Solution in Detail

- Role Management and Workflows
- Business-Driven Identity Management
- Compliance, Reporting, and Auditing
- Password Management
- Identity Virtualization
- Connectivity and Services
- Identity Federation and Web-Based Single Sign-On
- Database support

SAP NetWeaver Identity Management Architecture

Summary and Additional Information Sources
Introduction to Identity Management
Identity Management Definition

Enables the efficient, secure and compliant execution of business processes

By ensuring that the right users have the right access to the right systems at the right time

Consistent with their roles across all systems and applications
Challenges of a Typical Employee Lifecycle

- Long time to become productive
- Enormous costs and efforts
- Security leaks if employee leaves

Hire Date
Chuck Brown joins company
Available:
- Temporary accounts

3 Weeks Later
Chuck Brown is able to work in accounting
Available:
- E-Mail
- Portal
- Internet
- Accounting

1 Year Later
Chuck Brown transfers to sales
Available:
- E-Mail
- Portal
- Internet
- Accounting

7 Years Later
Chuck Brown is promoted: Vice President Sales
Available:
- E-Mail
- Portal
- Internet
- Accounting
- CRM (west)
- Marketing data (west)

8 Years Later
Chuck Brown resigns
All known accounts of Chuck Brown are deactivated
Available:
- Accounting
- CRM (global)
- Marketing data (west)

10 Years Later
Chuck Brown still has access to the system
Available:
- Accounting
- Marketing data (global)
Business Drivers for Identity Management

**Increasing Operational Costs**
- Maintenance of multiple sources of identity data
- Manual user provisioning by help desk delays on/off-boarding and change in positions
- Labor-intensive, paper-based approval systems
- Users dependent on help desk response times

**Changing Business Processes**
- Multi-enterprise fulfillment transactions with increasing partner process participation
- Industry-specific user provisioning requirements
- Inconsistent and informal processes proliferate

**Compliance Requirements**
- No record of who has access to which IT resources
- Inability to de-provision user access rights upon termination
- Identify and manage business & IT controls
- Provide auditors with complete audit trail
- Prevention of unauthorized access in multi-enterprise environments
SAP NetWeaver Identity Management Value Proposition

**Efficiency**
- Central management of user identities
- Lower cost of administration

**Insight**
- Regulatory compliance
- Governance model for policy management

**Flexibility**
- Business-driven identity management
- Responsive to business changes

- Standards-based technology platform
- Leverage SAP NetWeaver management and administration capabilities
- Rule-driven workflow / approval process

- Extensive audit trail, logging and reporting capabilities
- Integration with SAP Business Suite and SAP BusinessObjects Access Control (GRC) for end-to-end, compliant, role-based control

- Standards-based integration with SAP Business Suite
- Identity services enable tightly aligned, loosely coupled integration
SAP offers a complete suite of compliance, governance, identity and single sign-on solutions.
Identity Management Yesterday
Localized User Administration

ABAP: Transaction SU01 for local user mgmt
Java: User Management Engine (UME) for local user mgmt
Local user mgmt
Identity Management Yesterday
Partial Centralization

- CUA
- Provisioning for ABAP-based systems
- LDAP Directory
- 3rd Party Identity Management Product
- Synchronization
- UME data source
- e.g. on-boarding

© 2011 SAP AG. All rights reserved.
SAP NetWeaver Identity Management
Holistic Approach

- SAP Business Suite Integration
- Identity virtualization and identity as service
- Approval workflows
- Central Identity Store
- Provisioning to SAP and non-SAP systems
- Web-based Single Sign-On & Identity Federation

- Compliance checks
- Reporting
- Password management
- Rule-based assignment of business roles
- SAP BusinessObjects Access Control (GRC)

- e.g. on-boarding

- SAP NetWeaver Identity Management

- SAP Business Suite Integration
- Identity virtualization and identity as service
- SAP NetWeaver Identity Management

- Central Identity Store
- Provisioning to SAP and non-SAP systems
- Web-based Single Sign-On & Identity Federation

© 2011 SAP AG. All rights reserved.
Identity management is an integral part of the SAP NetWeaver technology platform:
It enables efficient and secure management of identity information.
It supports both SAP-only and heterogeneous system landscapes.
It integrates with the SAP NetWeaver platform and business applications.
It complements integrated SAP NetWeaver security frameworks.
Agenda

Introduction to Identity Management

SAP NetWeaver Identity Management Solution in Detail
- **Role Management and Workflows**
- Business-Driven Identity Management
- Compliance, Reporting, and Auditing
- Password Management
- Identity Virtualization
- Connectivity and Services
- Identity Federation and Web-Based Single Sign-On
- Database support

SAP NetWeaver Identity Management Architecture

Summary and Additional Information Sources
Solution in Detail: Role Management and Workflows
Role Definition and Provisioning

Role Definition (design, one-time task)
Read system access information (roles, groups, authorizations, etc.) from target systems
Define a business role hierarchy
Assign technical roles to business roles
Develop rules for role assignments

Provisioning (regularly)
Assign or remove roles to/from people
- Through request/approval workflow
- Manually (administrator)
- Automatically, e.g. HR-driven

Automatic adjustment of master data and assignments of technical authorizations in target systems
Role Management Based on Business Processes

Create order in SAP CRM

Check pricing in SAP IPC

Check availability in SAP SCM

1. Create “Create Sales Order” business role

2. Assign authorization needed for business process

3. Create rule to automatically link business role to employees with position sales clerk

Design Time

Execution Time

SAP ERP HCM

SAP NetWeaver Identity Management
Context-Based Role Assignment  
Available as of Release 7.2

As of Release 7.2, SAP NetWeaver ID Mgmt allows for the assignment between
A person / a role or privilege
And an optional context
Context types are defined by the customer; examples include factory, store, project, location, etc.

Use case:
A person has a specific role in a given factory. Using context-based role assignment, there is no need to duplicate these roles for each factory.

Example:
- 20 roles, 1000 factories
  - IDM 7.1: 20,000 entries (roles)
  - IDM 7.2: 1,020 entries (roles + contexts)

Benefit: Assigning a context reduces the number of roles (and privileges).
Workflows in SAP NetWeaver Identity Management

**Operates on entries in the identity store**
- Manual interactions through Web interface
  - Start provisioning tasks
  - Approve requests
  - Monitor status

**Workflows can be started from:**
- Web interface
- Event tasks
- Change of privilege assignments
- Meta directory operations

**Processing logic includes:**
- Sequential operation
- Parallel operation
- Conditional operation
- Approval operation
Agenda

Introduction to Identity Management

SAP NetWeaver Identity Management Solution in Detail

- Role Management and Workflows
- **Business-Driven Identity Management**
- Compliance, Reporting, and Auditing
- Password Management
- Identity Virtualization
- Connectivity and Services
- Identity Federation and Web-Based Single Sign-On
- Database support

SAP NetWeaver Identity Management Architecture

Summary and Additional Information Sources
Solution in Detail:
Business-Driven Identity Management
SAP NetWeaver ID Mgmt and SAP Business Suite: Increasing User Management Efficiency

Automated User Account Maintenance for SAP Business Suite Applications

Example: SAP CRM

- Sales representative Tom Peck needs access to SAP CRM.
- Creating a user account and role for Tom is not sufficient; you also have to create a Business Partner in CRM and assign the user account to this Business Partner.

SAP NetWeaver ID Mgmt automates the Business Partner assignment in SAP CRM, eliminating the need for manual administration steps.
SAP NetWeaver ID Mgmt and SAP HCM: Synchronization of Organizational Information

Organizational Information upload from SAP HCM to Identity Center

- Pre-requisite: SAP Organizational Management (OM) is used together with SAP HCM
- HCM stores Information from OM in Infotype 0001
- All information that is stored in HCM-Infotypes can be synchronized with Identity Center (highly configurable):
  - Last name, first name, address, start-date,…
  - Organizational information like Org.-Unit and Org.-Key
- No direct connection from HCM-OM with Identity Center is necessary
SAP Business Suite Integration
Business-Driven Identity Management

Key Benefits
- Automated creation of Business Partner in SAP CRM, SAP SCM
- Link from Business Partner to user

SAP NetWeaver Identity Management

- SAP Supplier Relationship Management
- SAP Human Capital Management
- SAP ERP Financials
- SAP Transportation Management
- SAP Extended Warehouse Management
- SAP Service Parts Planning
- SAP Supply Network Collaboration
- SAP Customer Relationship Management
- SAP Portfolio and Product Management
- SAP Product Lifecycle Management
- SAP Customer Relationship Management
Kim Perkins joins the company as a marketing professional. From the first day with her new company, she is able to log on to all relevant systems, including access to the employee self-services, and access to SAP CRM to track the marketing activities she is responsible for.

Pre-hire phase

1. HR ensures that all necessary employee data for Kim is available, such as position and entry date.

2. Event-based extraction of Personnel data

3. Based on the position in HCM the business role “Marketing Professional” is being assigned automatically.

4. Kim’s manager approves the assignment.

First day at work

User created “Employee”

Business Partner created User created “Marketing Professional”

User created Access to SAP ESS

Access to SAP CRM

SAP NetWeaver Identity Management
Organizational Change: Line Manager Promotion

After two years as a marketing professional, Kim Perkins is promoted to take over personnel and budget responsibility for her marketing team.

On the first day in her new role, she has access to the manager self-services. In her new position, she is responsible for budget approvals for all marketing campaigns - this requires immediate access to SAP ERP to view the marketing costs.

1. HR ensures that all necessary employee data for Kim are available, such as position and entry date.

2. Event-based extraction of Personnel data.

3. SAP NetWeaver Identity Management recognizes the line manager information for Kim and automatically assigns the business role “Marketing Manager.”

Day of change:

- User updated “Employee” “Line Manager”
- User created “Marketing Controller”
- User updated “Marketing Controller”
- User updated Access to SAP ESS
- Access to SAP MSS
- Access to SAP CRM
After eight years, Kim Perkins leaves the company. On her last day, she finishes her tasks in the systems she used to work on. The day after her official assignment with the company ends, she is no longer able to access these systems.

1. HR ensures that all termination relevant data for Kim are available, such as last day with the company.

2. Event-based extraction of Personnel data

3. SAP NetWeaver Identity Management recognizes the last day information for Kim and automatically un-assigns all access rights and disables her accounts.

Day after termination date
- SAP HCM: User disabled
- SAP ERP: User disabled
- SAP CRM: User disabled
- Portal: User disabled
Agenda

Introduction to Identity Management

SAP NetWeaver Identity Management Solution in Detail
- Role Management and Workflows
- Business-Driven Identity Management
- Compliance, Reporting, and Auditing
- Password Management
- Identity Virtualization
- Connectivity and Services
- Identity Federation and Web-Based Single Sign-On
- Database support

SAP NetWeaver Identity Management Architecture

Summary and Additional Information Sources
Solution in Detail:
Compliance, Reporting, and Auditing
Reporting Options in SAP NetWeaver Identity Mgmt

Basic Reporting, Reporting with Jasper Reports / Crystal Reports

- Focus: Static, printable reports
- Report creation on database level

Extended Reporting with SAP Business Warehouse (SAP BW)*

- Focus: Dynamic reports, offering more, highly detailed, and customizable reporting options
- Report creation on semantic BW InfoProviders
- Data is extracted from SAP NetWeaver Identity Management on a regular basis (as per defined job)
- Predefined report templates available
- Custom reports can be freely defined based on individual customer requirements
- SAP BW features include filtering, sorting, export to MS Excel, CSV, PDF, send via e-mail, publishing in Portal, etc.

*SAP BW is not part of the SAP NetWeaver ID Mgmt license
SAP NetWeaver Identity Management
Basic Reporting Functionality

- **Application/Privilege-Centric**
  Determination of system access

- **User-Centric**
  Determination of user privileges

- **Entry data**
  Current data, historical data, time stamps, modified by, audit flags

- **Approval data**
  Who approved what when?

- **Who had what privilege at what time?**
  Segregation of duties, Attestation

- **Task audit log**
  Determination of tasks run on user / by user

- **General logs**

- **Off-the-shelf reporting tools can be used**
SAP NetWeaver ID Mgmt Extended Reporting Capabilities: Integration with SAP BW

- SAP BW report templates delivered with persons, privileges, roles and their assignments over time and for specific dates
- Advanced filtering and sorting options
- Access control: Roles for Reporting User (Administrator, Manager, Owner)
- Flexibility (BEX reports are used)

Implementation Guide:

BI Content Documentation:
SAP NetWeaver Identity Management
Extended Reporting With SAP BW

✓ Object types (can be extended)
    Person, privilege (aggregated by system), role

✓ Report types
    Content-based reporting (person-attributes or role memberships)
    Time-based reporting (state on given date or changes in period)

✓ Aggregations
    Number of assignments between object types

✓ Navigation between reports ("report-report interface")
    Person to assigned manager, role, etc.

✓ Basic auditing data: Who changed what

✓ Authorization concept with three roles
    Administrator, HR Manager, Object Owner

✓ Flexibility
    Use of BEx reports
Reporting with SAP BW: Input Help

List of attributes can be extended/modified
Reporting With SAP BW: Person Details at a Given Date

<table>
<thead>
<tr>
<th>Person</th>
<th>Person Display Name</th>
<th>E-Mail Address</th>
<th>Attribute Name</th>
<th>Attribute Value</th>
<th>Referenced Entry Type</th>
<th>Referenced Entry</th>
<th>Changed By</th>
<th>Change Information</th>
<th>Change Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>u1</td>
<td>Jackie Rees</td>
<td><a href="mailto:u1@demo.com">u1@demo.com</a></td>
<td>DISPLAY_NAME</td>
<td>Jackie Rees</td>
<td>#</td>
<td>#</td>
<td>0</td>
<td>Identity Center - Job</td>
<td>09.10.2009 00:59:23</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MSKEYVALUE</td>
<td>u1</td>
<td>#</td>
<td>#</td>
<td>0</td>
<td>Identity Center - Job</td>
<td>09.10.2009 00:59:23</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MXREF_MX_ROLE</td>
<td>31147</td>
<td>MX_ROLE</td>
<td>Manager user</td>
<td>0</td>
<td>Identity Center - Job</td>
<td>09.10.2009 01:05:04</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MX_ADDRESS_COUNTRY</td>
<td>Norway</td>
<td>#</td>
<td>#</td>
<td>0</td>
<td>Identity Center - Job</td>
<td>09.10.2009 00:59:23</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MX_AUTOPRIV</td>
<td>31148</td>
<td>MX_PRIVILEGE</td>
<td>MX_PRIV_WD:TAD_HISTORY</td>
<td>0</td>
<td>Identity Center - Job</td>
<td>09.10.2009 01:05:04</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>31150</td>
<td>MX_PRIVILEGE</td>
<td>MX_PRIV_WD:TAD_TODDO</td>
<td>0</td>
<td>Identity Center - Job</td>
<td>09.10.2009 01:05:05</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>31151</td>
<td>MX_PRIVILEGE</td>
<td>MX_PRIV_WD:TAD_MANAGE</td>
<td>0</td>
<td>Identity Center - Job</td>
<td>09.10.2009 01:05:05</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>31152</td>
<td>MX_PRIVILEGE</td>
<td>MX_PRIV_WD:TAD_REPORT</td>
<td>0</td>
<td>Identity Center - Job</td>
<td>09.10.2009 01:05:05</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>31154</td>
<td>MX_PRIVILEGE</td>
<td>User</td>
<td>0</td>
<td>Identity Center - Job</td>
<td>09.10.2009 01:05:05</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>31158</td>
<td>MX_PRIVILEGE</td>
<td>VDS</td>
<td>0</td>
<td>Identity Center - Job</td>
<td>09.10.2009 01:05:05</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MX_AUTOROLE</td>
<td>31147</td>
<td>MX_ROLE</td>
<td>Manager user</td>
<td>0</td>
<td>Identity Center - Job</td>
<td>09.10.2009 01:05:04</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MX_ENTRYTYPE</td>
<td>MX_PERSON</td>
<td>#</td>
<td>#</td>
<td>0</td>
<td>Identity Center - Job</td>
<td>09.10.2009 00:59:23</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MX_FIRSTNAME</td>
<td>Jackie</td>
<td>#</td>
<td>#</td>
<td>0</td>
<td>Identity Center - Job</td>
<td>09.10.2009 00:59:23</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MX_KEYWORDS</td>
<td>Jackie Rees Norway CEO</td>
<td>#</td>
<td>#</td>
<td>0</td>
<td>Identity Center - Job</td>
<td>09.10.2009 00:59:23</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MX_LASTNAME</td>
<td>Rees</td>
<td>#</td>
<td>#</td>
<td>0</td>
<td>Identity Center - Job</td>
<td>09.10.2009 00:59:23</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MX_MAIL_PRIMARY</td>
<td><a href="mailto:u1@demo.com">u1@demo.com</a></td>
<td>#</td>
<td>#</td>
<td>0</td>
<td>Identity Center - Job</td>
<td>09.10.2009 00:59:23</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MX_PHONE_PRIMARY</td>
<td>74568843</td>
<td>#</td>
<td>#</td>
<td>0</td>
<td>Identity Center - Job</td>
<td>09.10.2009 00:59:23</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MX_TITLE</td>
<td>CEO</td>
<td>#</td>
<td>#</td>
<td>0</td>
<td>Identity Center - Job</td>
<td>09.10.2009 00:59:23</td>
</tr>
</tbody>
</table>

Reference attributes: Show referenced entry’s type and MSKEYVALUE
Reporting With SAP BW: Person History

### Person Details (History)

<table>
<thead>
<tr>
<th>Person</th>
<th>Person Display Name</th>
<th>E-Mail Address</th>
<th>Valid from</th>
<th>Valid to</th>
<th>Attribute Name</th>
<th>Attribute Value</th>
<th>Referenced Entry Type</th>
<th>Referenced Entry</th>
<th>Previous Value</th>
<th>Changed By</th>
<th>Change Information</th>
<th>Change Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>u10000</td>
<td>Sarah Bell</td>
<td><a href="mailto:u10000@demo.com">u10000@demo.com</a></td>
<td>08.10.2009</td>
<td>31.12.2009</td>
<td>DISPLAYNAME</td>
<td>Sarah Bell</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Historic values

- **Valid from**: 08.10.2009, **Valid to**: 31.12.2009
- **Attribute Name**: DISPLAYNAME, **Attribute Value**: Sarah Bell
- **Attribute Name**: MSKEYVALUE, **Attribute Value**: u10000
- **Attribute Name**: MX_ADDRESS_COUNTRY, **Attribute Value**: Arizona
- **Attribute Name**: MX_ENTRYTYPE, **Attribute Value**: MX_PERSON
- **Attribute Name**: MX_AUTOROLE, **Attribute Value**: 31148
### Systems with Their Privileges and Assigned Persons (State)

#### Number of assignments per privilege

<table>
<thead>
<tr>
<th>System</th>
<th>Privilege Display Name</th>
<th>Person Display Name</th>
<th>E-Mail Address</th>
<th>Display Name</th>
<th>Changed By</th>
<th>Change Information</th>
<th>Change Time</th>
<th>Number of Assignments</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSSQL</td>
<td></td>
<td>GP Admin. Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>PORTAL</td>
<td></td>
<td>GP Developer Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>42</td>
</tr>
<tr>
<td>SUNONE</td>
<td></td>
<td>GP Admin. Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>PRV GROUP:SUNONE</td>
<td>GP Admin. Group</td>
<td>GP Admin. Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>PRV GROUP:SUNONE</td>
<td>GP Developer Group</td>
<td>GP Developer Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>PRV GROUP:SUNONE</td>
<td>TWI Employee Group</td>
<td>TWI Employee Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>PRV GROUP:SUNONE</td>
<td>VC Group</td>
<td>VC Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Demo</td>
<td></td>
<td>DeeDemo</td>
<td><a href="mailto:Dee.Demo@tdddemol.asap.de">Dee.Demo@tdddemol.asap.de</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>LerchA</td>
<td></td>
<td>#</td>
<td><a href="mailto:Anna.Lerch@as1wdfvin2070.asap">Anna.Lerch@as1wdfvin2070.asap</a></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
<tr>
<td>WD</td>
<td></td>
<td>#</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>
Compliant Identity Management: The Vision

- Provides compliant identity management across SAP and heterogeneous landscapes in one integrated solution
- Standards-based integration creates tightly aligned, loosely coupled solution from complementary components
- Gives a consistent view on current and historic access rights, approvals and policy violations

CIO
SAP NetWeaver Identity Management

- Provides the reduced TCO and increased security required by the CIO

CFO
GRC (SAP BusinessObjects Access Control)

- Meets the requirements of the CFO to ensure that IT business application controls are compliant
SAP BusinessObjects Access Control (GRC) and SAP NetWeaver Identity Mgmt: Integration Scenario

**SAP NetWeaver Identity Management**
- Heterogeneous connectivity
- SAP Business Suite integration
- Powerful business role mapping
- Password management

**SAP BusinessObjects Access Control (GRC)**
- Compliance checks
- Business risk controls and mitigation

**Combined**

Compliant identity management for the entire system landscape!
Compliant, Business-Driven Identity Management

**Requirement:**
Provide automated, position-based role management while ensuring compliance

Reduce TCO by simplifying assignment of roles and privileges to users, triggered by HCM events
Reduce risk through compliance checks and remediation
Automate manual processes through integration with SAP Business Suite

New Hire

Calculate entitlements based on position

Compliance check
Remediation

Approve assignments

Yes

No

Create User
Assign roles
Create User
Assign privileges

Create user
Assign roles

HCM
SAP NetWeaver Identity Management
SAP BusinessObjects Access Control
Line Manager
Landscape

Requirement:
Provide automated, position-based role management while ensuring compliance
Minimal Time-to-Compliance
- Quick, effective, and comprehensive access risk identification
- Elimination of existing access and authorization risks is key

Continuous Access Management
- Improve productivity of end users
- Reduce cost of role maintenance
- Avoid business obstructions with faster emergency response
- Ease compliance and avoid authorization risk

Effective Management Oversight
- Capabilities for management oversight
- Capabilities for internal audit

Identity management
Periodic access review and audit

Risk analysis and remediation
Compliant user provisioning
Enterprise role management
Superuser privilege management

Cross-enterprise library of best practice segregation of duties rules

Regulations
Rules
Corporate Policies
Best Practices

FIN
SCM
SRM
MFG
HR

IT Infrastructure
Compliant Identity Management
Process Flow

1. Request Role Assignment
2. Manager approval
3. Forward request for risk analysis
4. Risk analysis
5. Risk mitigation
6. Risk status
7. Provisioning to target systems
8. Notification to user / manager

SAP BusinessObjects Access Control (GRC)
SAP NetWeaver Identity Management
Compliant Identity Management
Component Usage

Usage of SAP NetWeaver Identity Management components:

Virtual Directory Server
- Accepts requests from Identity Center.
- Handles all connection to/from SBOP Access Control through the Web service API exposed by SBOP Access Control.

Identity Center
- Contains the workflow tasks and necessary jobs that drive the provisioning to SBOP Access Control based on the Provisioning Framework for SAP Systems.
- Communicates with the Virtual Directory Server using the LDAP protocol.

Usage of SAP BusinessObjects Access Control components:

Compliant User Provisioning (CUP)
- Provides Web services for compliance checks, status checks, etc.
- Includes workflow for risk analysis and mitigating controls

Risk Analysis and Remediation (RAR)
- Provides risk analysis services to detect SOD violations and critical permissions
- Handles CUP-RAR communication via internal Web services
Compliant Identity Management
Central User Provisioning

Create role assignment request in Identity Management (Identity Center)
Automatic (using rules, e.g. department assignment)  Manual (per user request)

Pre-process request in Identity Management (Identity Center)
Assignments require compliance check  Assignments do not require compliance check

Request processing & risk analysis in Compliant User Provisioning
Risk violations found  No risk violations found

Request rerouted to manual workflow
Declined  Approved

Identity Management reads request status
No provisioning  Identity Management starts provisioning
Agenda

Introduction to Identity Management

SAP NetWeaver Identity Management Solution in Detail
- Role Management and Workflows
- Business-Driven Identity Management
- Compliance, Reporting, and Auditing
- **Password Management**
- Identity Virtualization
- Connectivity and Services
- Identity Federation and Web-Based Single Sign-On
- Database support

SAP NetWeaver Identity Management Architecture

Summary and Additional Information Sources
Solution in Detail:
Password Management
Password Management

**Requirement:** Centralized password management

Reduce calls to help desk for password resets
Enable password provisioning across heterogeneous landscape

User

- Reset password
- Recover lost password

Help Desk

- Set new password

SAP NetWeaver Identity Management

Landscape
Introduction to Identity Management

SAP NetWeaver Identity Management Solution in Detail
- Role Management and Workflows
- Business-Driven Identity Management
- Compliance, Reporting, and Auditing
- Password Management
- **Identity Virtualization**
- Connectivity and Services
- Identity Federation and Web-Based Single Sign-On
- Database support

SAP NetWeaver Identity Management Architecture

Summary and Additional Information Sources
Solution in Detail: Identity Virtualization
Identity Virtualization

Virtual Directory Server (VDS) provides

- Single consistent view and entry point for multiple distributed identity data sources
- Identity information as a service for applications through standard protocols (LDAP, SPML)
- Abstraction layer for underlying data stores

Consumer only sees one standard interface

- Transform incoming LDAP requests, and connect directly to the existing data repositories
  - Data stays within original data source
  - Efficient caching

Properties

- Real-time access to data
- No need to consolidate data sources
- No extra data store
  - Quick LDAP deployment
  - Easier and cheaper maintenance
- Attribute manipulation
- Name space modifications
- Complex operations on-the-fly

SPML

LDAP

Virtual Directory Server

Directory Server

Directory Server

Database

Application

© 2011 SAP AG. All rights reserved.
Agenda

Introduction to Identity Management

SAP NetWeaver Identity Management Solution in Detail

- Role Management and Workflows
- Business-Driven Identity Management
- Compliance, Reporting, and Auditing
- Password Management
- Identity Virtualization
- Connectivity and Services
  - Identity Federation and Web-Based Single Sign-On
  - Database support

SAP NetWeaver Identity Management Architecture

Summary and Additional Information Sources
Solution in Detail:
Connectivity and Services
What is the relationship between SAP NetWeaver Identity Management and the Central User Administration (CUA)?

- SAP NetWeaver Identity Management is the strategic solution for managing identities in SAP and non-SAP environments.
- SAP recommends replacement of the CUA by SAP NetWeaver ID Mgmt. This is a valuable strategic move, as it yields significant benefits and functional enhancements.
- SAP will continue to support SAP CUA in its current functionality according to SAP maintenance rules; however, the solution will no longer be enhanced with new functionality.
- Systems connected to CUA can be smoothly migrated to a SAP NetWeaver ID Mgmt solution without loss of functionality.
- Main benefits of SAP NetWeaver ID Mgmt compared to CUA include:
  - Connectivity for a heterogeneous system landscape
  - Automatic cross-system rule-based access management
  - Workflow support
## Comparing SAP CUA and SAP NetWeaver Identity Management

<table>
<thead>
<tr>
<th>Functionality</th>
<th>Central User Administration (CUA)</th>
<th>SAP NetWeaver Identity Management (ID Mgmt)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Systems</td>
<td>ABAP only</td>
<td>SAP and non-SAP</td>
</tr>
<tr>
<td>Workflow Support</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Rule based access management</td>
<td>almost no (except the rarely used HR Org rule engine)</td>
<td>Yes</td>
</tr>
<tr>
<td>Modeling of role hierarchy</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Cross system role assignments</td>
<td>Manual</td>
<td>Full support</td>
</tr>
<tr>
<td>LDAP directory integration</td>
<td>LDAP synchronization</td>
<td>Full support</td>
</tr>
<tr>
<td>Support of all user attributes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Password management</td>
<td>Management and distribution of initial passwords</td>
<td>Yes; including user interface and workflow support</td>
</tr>
</tbody>
</table>
Central User Administration: Gradual Migration to SAP NetWeaver ID Mgmt

Requirement:
Extend identity management to non-SAP environments and increase level of functionality

- Supports SAP and heterogeneous environments
- Self-service and delegated administration
- Workflows and approvals
- Business role management

Manage CUA from SAP NetWeaver ID Mgmt
Migrate ABAP systems from CUA to ID Mgmt
Shut down CUA when all systems are migrated
SAP NetWeaver Identity Management Connectivity Overview

Other
- SAP Application Server
- Microsoft Windows NT
- Unix/Linux
- Shell execute
- Custom Java connector API
- Script-based connector API

Applications
- SAP Business Suite
- SAP BusinessObjects
- Access Control (GRC)
- Lotus Domino / Notes
- Microsoft Exchange
- RSA ClearTrust
- RSA SecurID

Databases
- Microsoft SQL Server
- Microsoft Access
- Oracle database
- IBM UDB (DB2)
- MySQL
- Sybase

Directory Servers
- Microsoft Active Directory
- IBM Tivoli Directory
- Novell eDirectory
- SunONE Java Directory
- Oracle Internet Directory
- Microsoft Active Directory Application Mode (ADAM)
- Siemens DirX
- OpenLDAP
- eB2Bcom View500 Directory Server
- CA eTrust Directory
- SAP NetWeaver IDM Virtual Directory Server
- Any LDAP v3 compliant directory srv

Technical
- SPML
- LDAP
- ODBC / JDBC / OLE-DB
- RFC
- LDIF files
- XML files
- CSV files
Connector Framework: Purpose and Components

**Purpose**
To provide a development toolkit and guidelines for third party vendors to create an SAP NetWeaver Identity Management connector for non-SAP applications.

**Components**

Identity Center
Main functionality used here: Identity provisioning

Virtual Directory Server
Single access point for data updates in multiple repositories
Connector Framework: Two Integration Steps

Identity Center Integration
The connector tasks integrate into the existing (common) provisioning framework in the Identity Center
- A set of tasks has to be customized to work together with the target application utilizing VDS.

Virtual Directory Server Integration
The generic VDS core functionality has to be extended
- A code has to be created which will be used by VDS to connect to the target application.

Two parts that build the connector; to be created by 3rd party vendor
Typically exists within 3rd party application
Connectivity Architecture

**Provisioning Framework**
- Independent of repositories and back-ends
- Hooks into the partner’s set of IC connector tasks

**IC Tasks (Set From Partner)**
- Hooked into the provisioning framework

**Virtual Directory Server (VDS)**

**Connectors from Partners**
- Multiple connectors in a virtual tree

**Back-Ends (Third-Party Applications)**
The SAP Integration and Certification Center (ICC) offers a certification for the integration scenario NW-IDM-CON.

SAP partners as well as potential partners and independent software vendors (ISVs) are invited to use the Connector Development Kit (CDK) to create an SAP NetWeaver Identity Management connector for their application, and to integrate the application into the identity management landscape. This connector can then be certified by the SAP ICC.

For general information about third party certifications with SAP products, please refer to http://www.sdn.sap.com/irj/sdn/interface-certifications, or contact the SAP Integration and Certification Center (ICC) directly at icc@sap.com
Identity Services: SOA-Based Identity Management

Requirements:
- Create a tight integration with SAP applications
- Integrate third-party applications

Identity services as a standards-based single access point for querying and managing identity information in the complete system landscape

'Tightly aligned, loosely coupled' integration with SAP and heterogeneous applications based on industry standards

Requirements:
- Create a tight integration with SAP applications
- Integrate third-party applications

Identity services as a standards-based single access point for querying and managing identity information in the complete system landscape

'Tightly aligned, loosely coupled' integration with SAP and heterogeneous applications based on industry standards
Connectivity – SAP Hana connector

SAP Hana – SAP NetWeaver Identity Management connector

- Available as of SAP Identity Management 7.2 Service Pack 3
- Connection via the SQL interface
- User provisioning into SAP Hana:
  - Create/drop users
  - Create/drop roles
  - Assign roles to users
  - Revoke roles from users
  - Change passwords
- Enables synchronization of users in complex landscapes
Agenda

Introduction to Identity Management

SAP NetWeaver Identity Management Solution in Detail
  • Role Management and Workflows
  • Business-Driven Identity Management
  • Compliance, Reporting, and Auditing
  • Password Management
  • Identity Virtualization
  • Connectivity and Services
  • Identity Federation and Web-Based Single Sign-On
  • Database support

SAP NetWeaver Identity Management Architecture

Summary and Additional Information Sources
Solution in Detail: Identity Federation and Web-Based Single Sign-On
What is Identity Federation?

Identity Federation

- Describes the technologies, standards and use-cases which serve to **enable the portability of identity information across otherwise autonomous security domains.**

- Enables users of one domain to securely access data or systems of another domain seamlessly, and **without the need for completely redundant user administration.**

- **Comes in many flavors**, including "user-controlled" or "user-centric" scenarios, as well as enterprise controlled or B2B scenarios.

- Could involve **user-to-user, user-to-application as well as application-to-application use-case scenarios at both the browser tier as well as the web services tier.**
Identity Federation in SAP NetWeaver Identity Management 7.2

- Identity federation provides the means to share identity information across company boundaries.
- User must be unambiguous and clearly identifiable, even though different user identifiers may exist across the landscape.
- The name identifier (name ID) is the means to establish a common identifier.
- Once the name ID has been established, the user is said to have a federated identity.
- Identity federation enables SSO for web browser based access (user-centric) and web services (system centric) across domains.
- SAP’s solution relies on standards for interoperability between SAP and non SAP systems
- For Web browser-based access, identity federation uses an identity provider that supports SAML 2.0.
- For Web services, identity federation uses a security token service (STS) that supports WS-Trust 1.3, supporting X.509, SAML 1.1, and SAML 2.0 tokens.
The Security Assertion Markup Language (SAML) version 2.0 is a standard for the communication of assertions about principals, typically users.

The assertion can include the means by which a subject was authenticated, attributes associated with the subject, and an authorization decision for a given resource.

The main benefits of SAML 2.0 are:

- **SSO with SAML 2.0**
  - SAML provides a standard for cross-domain Single Sign-On (SSO)
  - SAML 2.0 supports identity-provider-initiated SSO as in SAML 1.x
  - SAML 2.0 also supports service-provider-initiated SSO

- **SLO with SAML 2.0**
  - Single Log-Out (SLO) enables users to cleanly close all their sessions in a SAML landscape, even across domains.

- **Identity federation**
  - Identity federation provides the means to share identity information between partners.
Identity Federation Web Browser-Based Access

- For Web browser-based access, identity federation uses an identity provider that supports SAML 2.0.
- SAML 2.0 also enables Single Log-Out (SLO).
- Identity federation can also be used to transport profile attributes to create or update temporary or permanent users between systems.
- Authorization attributes can be transported enabling to change user authorizations in target systems.
For Web services, identity federation uses a security token service (STS) that supports WS-Trust 1.3.

STS supports a number of authentication methods from a Web service consumer. It can convert these tokens into a security token that a Web service provider can use.

STS supports X.509, SAML 1.1, and SAML 2.0 tokens.

Like SAML 2.0 for Web-based access, the SAML 2.0 assertion can transport profile and authorization attributes to the target Web service provider.
Solution in Detail:
Database support
Enhanced database support

Database options for SAP NetWeaver Identity Management

IBM DB2 supported as of SAP NetWeaver Identity Management 7.2 SP 6

SAP NetWeaver Identity Management

- Microsoft SQL Server
- IBM DB2 database
- Oracle database
Introduction to Identity Management

SAP NetWeaver Identity Management Solution in Detail
- Role Management and Workflows
- Business-Driven Identity Management
- Compliance, Reporting, and Auditing
- Password Management
- Identity Virtualization
- Connectivity and Services
- Identity Federation and Web-Based Single Sign-On
- Database support

SAP NetWeaver Identity Management Architecture

Summary and Additional Information Sources
SAP NetWeaver Identity Management Architecture
SAP NetWeaver Identity Management Architecture

Identity Center Database
- Identity store
- Configuration
- Processing logic

Workflow User Interface
- Main interface for users and managers

Monitoring User Interface
- Monitoring and audit interface for administrators

Management Console
- Visual development and configuration UI

Runtime Engine and Dispatcher
- Processing and provisioning logic including connectors

Event Agent
- Monitors connected systems and initiates synchronization

Virtual Directory Server
- Virtualization layer
SAP NetWeaver Identity Management: Communication Paths

- Transfer employee data to IDM (LDAP)
- Update employee record with communication details (RFC)
- Provision identity to target system (Protocol dependant on target system)
- Forward request for risk analysis & poll status (Web Service Call)

Diagram:

- SAP ERP HCM System
- SAP NetWeaver Identity Management
  - Virtual Directory Server (VDS)
  - Identity Center (IC)
- SAP BusinessObjects Access Control (GRC)
- SAP NetWeaver: SCM, ERP, Legacy, WebApp, DB, Email

© 2011 SAP AG. All rights reserved.
Central Identity Store

Central Hub for All Identity Center Components

- Provisioning is based on identity data from the store
- Business roles and privileges are stored here
- Workflow processing is based on this data
- Meta directory operations keep the information up-to-date

Identity Store Properties

- Keep historical data and full audit to support compliance
- Temporary attributes for tracking time-critical values
- Roles and privileges – validity periods can be defined
- Events on attributes trigger workflow tasks
- Virtual attributes reference data in external sources
- Roll-back of identity data
Virtual Directory Server Architecture

- Multiple Inbound Protocols
  - LDAP
  - Extensible Transformation Framework

- In-Memory Cache

- Connector Framework
  - Protocol Connectors
    - LDAP
    - DB
    - API
  - Web Services Connectors
    - SPML
    - DSML
  - Application Connectors
    - SAP
    - Sales Force

- Java GUI
- Configuration management and version control
- Log
- Statistics
- Audit
- Performance
Sizing SAP NetWeaver Identity Management

Sizing SAP NetWeaver Identity Management

- Sizing means determining the hardware requirements of an SAP application, such as the network bandwidth, physical memory, CPU processing power, and I/O capacity.
- The size of the hardware and database is influenced by both business aspects and technological aspects.
- The number of users using the various application components and the data load they put on the server must be taken into account.
- Usage patterns influences how to size SAP NetWeaver ID Mgmt. The main factors are: Number of entries (amount of data), number of lookups (searches), number of changes, number of simultaneous users.

The SAP NetWeaver Identity Management 7.1 Sizing Guide

- The Sizing Guide provides initial sizing information for the SAP NetWeaver Identity Management.
- Precise recommendations for each customer will be determined on a case-by-case basis for each customer's specific requirements.

Custom User Interfaces for SAP NetWeaver ID Mgmt With Open API (RESTful Web Services)

**Architecture**
- REST (Representational State Transfer)
- JSON (Java Script Object Notation)

**Schema**
- Retrieve schema information

**Entries**
- Search for entries
- Retrieve entries and attributes
- Change attribute values
- Resetting of passwords

**Approvals**
- Retrieving open approvals
- Processing of approvals
Custom Role Request User Interface Based on REST API
Custom User Display Based on REST API
Introduction to Identity Management

SAP NetWeaver Identity Management Solution in Detail
  - Role Management and Workflows
  - Business-Driven Identity Management
  - Compliance, Reporting, and Auditing
  - Password Management
  - Identity Virtualization
  - Connectivity and Services
  - Identity Federation and Web-Based Single Sign-On
  - Database support

SAP NetWeaver Identity Management Architecture

Summary and Additional Information Sources
Summary and Additional Information Sources
## Highlights of SAP NetWeaver Identity Management 7.1

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Event-Driven SAP ERP HCM Integration</strong></td>
<td>In this release, the integration with SAP ERP HCM is extended to be event-based.</td>
</tr>
<tr>
<td><strong>Further Integration With SAP Business Suite</strong></td>
<td>A new framework enables product-specific extensions to be executed when identity provisioning operations are performed. This enables a deep integration with various applications in SAP Business Suite, including operations like updating employee master data or linking users to business partners.</td>
</tr>
<tr>
<td><strong>Extended Integration With SAP’s GRC Solution (SAP BusinessObjects Access Control)</strong></td>
<td>The integration with SAP’s GRC solution has been extended and covers current BusinessObjects Access Control releases.</td>
</tr>
</tbody>
</table>
| **WebDynpro-Based UIs**                                                | The PHP-based Web interfaces for workflow used by end users and managers for self-service, delegated administration, approval tasks, and monitoring are replaced by a WebDynpro-based user interface deployed on SAP NetWeaver AS Java 7.0 or 7.1.  
You can run the user interface as a stand-alone application or integrate it into the portal. 
New features are added for improving the task layout in the user interface, such as tabs and multiple columns. |
| **Extended Platform Support**                                          | Extended support of operating systems (Windows, Unix, Linux, …)                                                                                                                                              |
| **Extended Identity Services**                                         | Simplify management of deployed services and connectors  
  - Support for connector framework to enable partners to develop third-party connectors  
  - Improved deployment on SAP NetWeaver including logging |
Highlights of SAP NetWeaver Identity Management 7.2

- **Identity Federation**
  Use of Identity Provider (IdP) and Security Token Service (STS) for Web- and browser-based single sign-on scenarios.

- **Reporting with SAP Business Warehouse**
  Leverage SAP BW for dynamic, flexible reporting.

- **Context-Based Role Assignments**
  Use of context-based assignment to reduce the number of roles and privileges in the enterprise.

- **Custom User Interfaces with Open API**
  Use of a REST-based open API to develop custom user interfaces (for example for mobile devices) and/or extend the existing UIs.

- **Continuous Improvement in Various Areas**
  Examples include: Assignment improvements, context towards back-end systems, accessing assignment information from run time, guided tasks, approvals, configuration transport, request-complete task, dispatcher system tuning, extension framework, provisioning framework, etc.
Rapid Deployment Solution (RDS)

IDM RDS available as of SAP NetWeaver Identity Management 7.2 SP04 patch 1. Implementation via SAP Security Consulting (recommended) or own custom implementation project

Content (available to all SAP NetWeaver Identity Management customers):
- Connection between 2 SAP systems: SAP NetWeaver ABAP/Java, SAP ERP Human Capital Management (SAP ERP 6.0 EhP 4 or SP37) and an LDAP directory
- Templates for mass user maintenance, copy user, delete user, multi step approval workflows, reset password system dependently, rule engine
- Templates and functionality for CUA replacement
- Pre-defined HTML based reporting

Solution today
Why SAP NetWeaver Identity Management

- Offers close alignment with business processes
- Provides best value for business sponsors
- Re-uses SAP deployment experience and intellectual property
- Integrates with existing identity management infrastructure
- Combines tight SAP integration with heterogeneous IT
- Integrates roadmap and “blueprint” with SAP BusinessObjects Access Control (GRC)
- Provides the lowest-risk solution for SAP connectivity
More Information

Visit the SAP Community Network (SCN) for comprehensive information on SAP NetWeaver Identity Management, such as

- Product information, documentation, training, and support information
- Articles, blogs, WIKI, FAQs, forum, and newsletters
- Downloads

http://scn.sap.com/community/netweaver-idm
Thank You!
Change History Master Slide Deck
SAP NetWeaver Identity Management

- Nov 19 2012: (by Gerlinde)
  - Changes:
    - New slides: database support, RDS and Hana connector

- Nov. 2011:
  - New slide: added slide about “IDM-HR Integration – Organizational Information”

- May 2011 (by Kristian):
  - Changes: repair of animation in some slides, and other visual changes

- March 2011 (by Regine):
  - Changes: Transferred contents to new SAP template

- December 2010 (by Regine)
  - Changes:
    - Total rework – IDM to ID Mgmt.; news about 7.2 etc.
    - New slides:
      BW reporting, federation, context-based role management, partner certification, a slide about what’s new with 7.2, and many other adjustments
June/July 2010:
- Changes:
- Agenda: Changed topic 2.3 into Compliance, Reporting, and Auditing
- Added topic 2.7: Identity Federation and Web-Based Single Sign-On
- Slide 12: Added Identity Federation and Web SSO functionality
- New slides: 26, 28, 29, 30 (BW Reporting) 50, (Identity Federation and Web SSO)

April/May 2010:
- Changes: N/A
- New slides: Slide 51 (Sizing + link to sizing guide)

March 2010:
- Changes:
- Slide 9: Deleted “Vision of a” in the headline
- New slides:
  - Slides 30 - 33 including new notes (integration GRC and IDM)
  - Slide 48 (SAP NetWeaver IDM: Communication Paths)