First-hand Information about the Enhanced Functionality and Integration Options Within SAP NetWeaver Identity Management 7.2

SAP Product Management, SAP NetWeaver Identity Management & Security
Kristian Lehment, May 2011 – ASUG-Conference – Session ID 0709
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

SAP NetWeaver Identity Management Architecture

Summary and Additional Information Sources
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

Chuck Brown

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
- CRM (west)
- Marketing data (west)

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

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

10 Years Later
Chuck Brown still has access to the system
Available:
- Accounting
- Marketing data (global)
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
- SAP BusinessObjects Access Control (GRC)
- Compliance checks
- Reporting
- Rule-based assignment of business roles
- Password management
- Web-based Single Sign-On & Identity Federation
- SAP NetWeaver Identity Management
- e.g. on-boarding

© 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

SAP NetWeaver Identity Management Architecture

Summary and Additional Information Sources
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
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 and 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

SAP NetWeaver Identity Management Architecture

Summary and Additional Information Sources
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 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 Supplier Relationship Management
- SAP Human Capital Management
- SAP Customer Relationship Management
- SAP NetWeaver Identity Management
- SAP Portfolio and Product Management
- SAP Product Lifecycle Management
- SAP ERP Financials
- SAP Transportation Management
- SAP Extended Warehouse Management
- SAP Service Parts Planning
- SAP Supply Network Collaboration
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

SAP NetWeaver Identity Management Architecture

Summary and Additional Information Sources
Reporting Options in SAP NetWeaver Identity Mgmt

**Basic Reporting, Reporting with Jasper Reports or 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
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

- SAP CRM
  - Create user
    - Assign roles
- SAP ERP
  - Create User
    - Assign roles
- Portal
  - Create User
  - Assign privileges
- 3rd Party
  - Create User
  - Assign privileges

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

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
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
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

SAP NetWeaver Identity Management Architecture

Summary and Additional Information Sources
Password Management

Requirement:
Centralized password management

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

SAP NetWeaver Identity Management

User

Help Desk

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

SAP NetWeaver Identity Management Architecture

Summary and Additional Information Sources
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
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

SAP NetWeaver Identity Management Architecture

Summary and Additional Information Sources
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

© 2011 SAP AG. All rights reserved.
SAP NetWeaver Identity Management Connectivity

Overview

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

Technical
- SPML
- LDAP
- ODBC / JDBC / OLE-DB
- RFC
- LDIF files
- XML files
- CSV files

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

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

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

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

Technical
- SPML
- LDAP
- ODBC / JDBC / OLE-DB
- RFC
- LDIF files
- XML files
- CSV files

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

Databases
- Microsoft SQL Server
- Microsoft Access
- Oracle database
- IBM UDB (DB2)
- MySQL
- Sybase
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](http://www.sdn.sap.com/irj/sdn/interface-certifications), or contact the SAP Integration and Certification Center (ICC) directly at [icc@sap.com](mailto: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
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**

SAP NetWeaver Identity Management Architecture

Summary and Additional Information Sources
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.
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.
Identity Federation Web Services-Based Access

- 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.
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

SAP NetWeaver Identity Management Architecture

Summary and Additional Information Sources
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)

SAP ERP HCM System

Identity Center (IC)
Virtual Directory Server (VDS)

SAP NetWeaver Identity Management

SAP BusinessObjects Access Control (GRC)
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

**WEB browser**

**Client-side UI library**

**Mobile device**

**RESTful web services**

**AS Java**
IdMREST
Web Dynpro UI

**Identity Store**

**WEB browser**

**Client-side UI library**

**Mobile device**

**RESTful web services**

**AS Java**
IdMREST
Web Dynpro UI

**Identity Store**
Custom Role Request User Interface Based on REST API
Custom User Display Based on REST API
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

SAP NetWeaver Identity Management Architecture

Summary and Additional Information Sources
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.
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 Developer Network (SDN) 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://sdn.sap.com

→ SAP NetWeaver Product
→ Complementary Offerings
→ SAP NetWeaver Identity Management

http://www.sdn.sap.com/irj/sdn/nw-identitymanagement
Thank You!