

SAP NetWeaver Identity Management

Technical Overview Presentation



SAP AG
Walldorf, April 2009

THE BEST-RUN BUSINESSES RUN SAP™ 



This presentation outlines our general product direction and should not be relied on in making a purchase decision. This presentation is not subject to your license agreement or any other agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or to develop or release any functionality mentioned in this presentation. This presentation and SAP's strategy and possible future developments are subject to change and may be changed by SAP at any time for any reason without notice. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. SAP assumes no responsibility for errors or omissions in this document, except if such damages were caused by SAP intentionally or grossly negligent.

Agenda



- 1. Introduction to Identity Management**
2. SAP NetWeaver Identity Management Solution in Detail
 - 2.1 Role Management and Workflows
 - 2.2 Business-Driven Identity Management
 - 2.3 Compliance and Auditing
 - 2.4 Password Management
 - 2.5 Identity Virtualization
 - 2.6 Connectivity and Services
3. SAP NetWeaver Identity Management Architecture
4. Summary & Additional Information Sources



SAP NetWeaver Identity Management



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

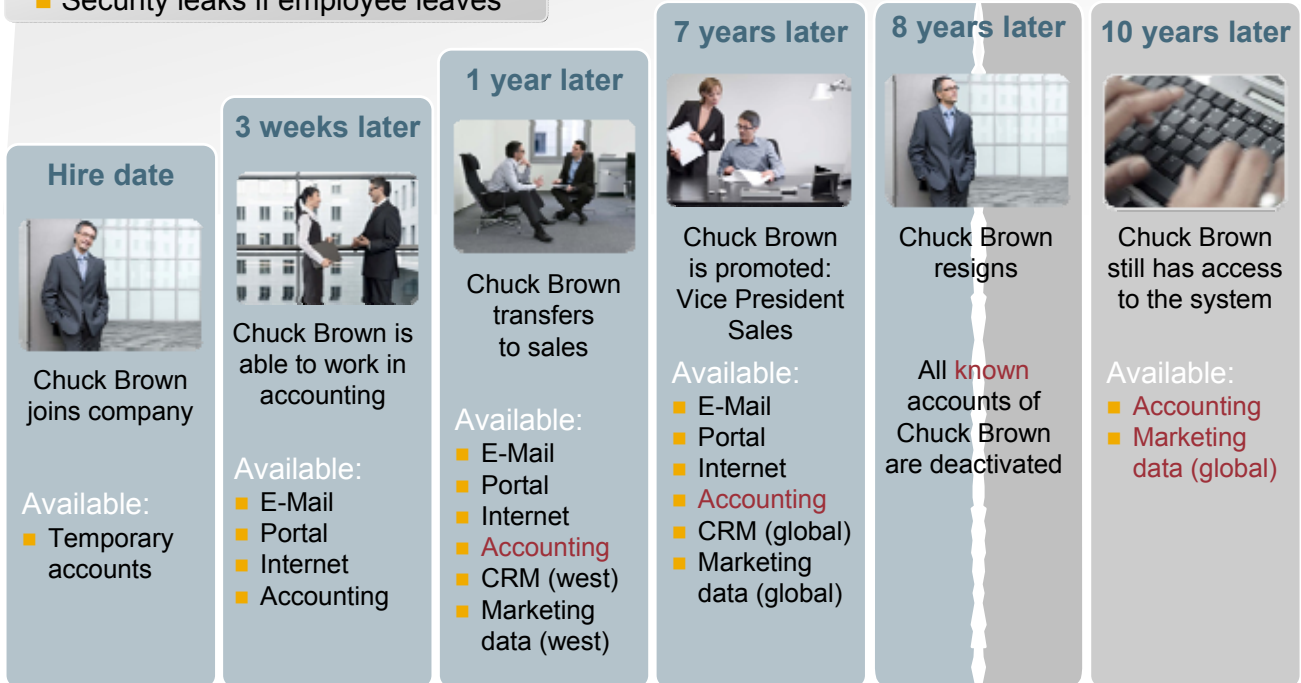
Consistent with their roles across all systems and applications

Typical User Lifecycle



Challenges:

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



© SAP AG 2009. All rights reserved. / Page 5

Employee Life-Cycle

This slide shows how an identity develops throughout its lifecycle and demonstrates the potential risks associated with the ineffective management of identities.

As Chuck Brown progresses through the company, his permissions and access set increases; it is no longer aligned with his job role and function. Even when he resigns, his permissions are still in effect.

Issues in this scenario:

- Long time to become productive
- Manual steps required to get access
- No de-provisioning of authorizations

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

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

Insight

- Regulatory compliance
- Governance model for policy management

- 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

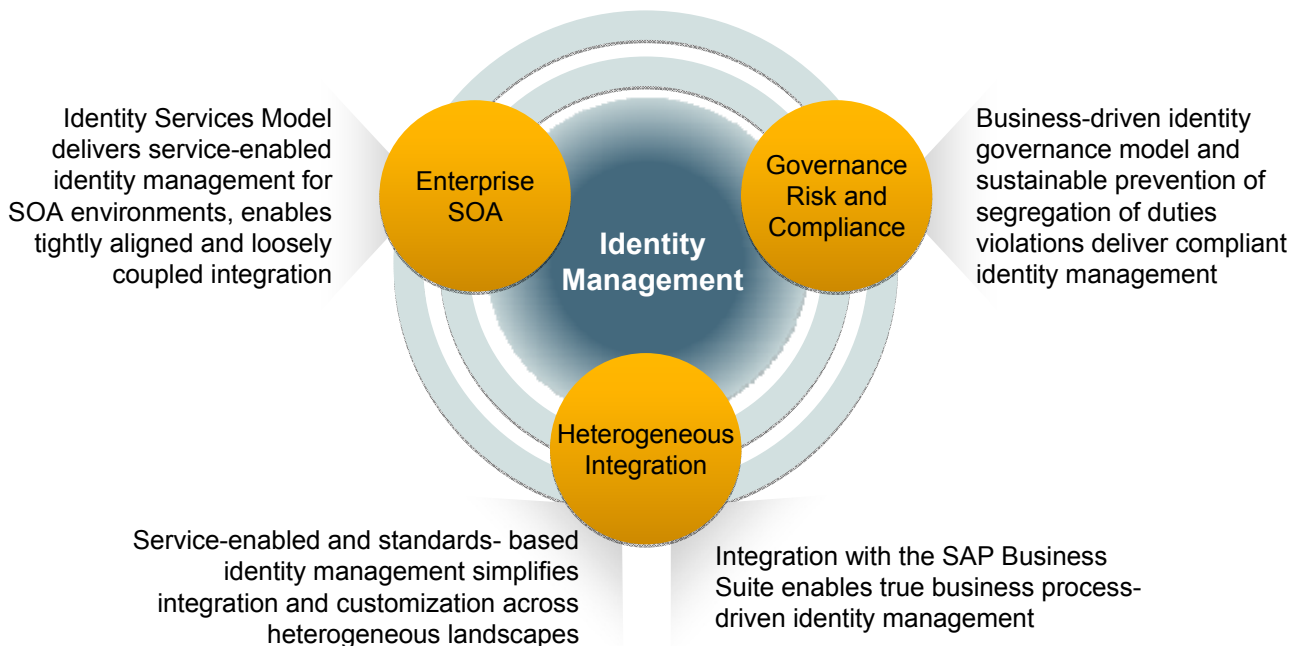
Flexibility

- Business-driven identity management
- Responsive to business changes

- Standards-based integration with SAP Business Suite
- Identity services enable tightly aligned, loosely coupled integration

Note: SAP GRC Access Control was renamed to SAP BusinessObjects Access Control (Jan. 2009)

Business-Driven, Compliant Identity Management



Vision

To provide an integrated, business-driven, and compliant* identity management solution on a standards-based technology platform

*Provided by SAP BusinessObjects Access Control (GRC)

© SAP AG 2009. All rights reserved. / Page 8

Taking it to the Next Level

The SAP NetWeaver Identity Management solution is based on the IDM product of MaXware, a Norwegian company SAP acquired in 2007.

SAP NetWeaver IDM provides innovative functions that can help companies reduce TCO, increase security, and empower users.

The solution includes account provisioning, synchronization, as well as workflow that support self-services and delegated administration. It also includes functions for password management and advanced role management.

In addition to general identity management features, SAP takes identity administration to the next level by tying it into the Business Process Platform to help enable Business Network Transformation.

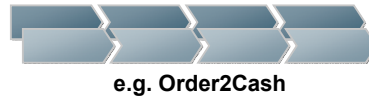
- An important part of SAP's Business Process Platform is the possibility to orchestrate services or Enterprise SOA into composite applications using Business Process Management. These composite applications require efficient management of access rights across the SAP Business Suite and heterogeneous environments. SAP NetWeaver Identity Management focuses on making these processes as seamless as possible.
- Managing authorizations for business transactions requires the sustainable prevention of segregation of duties violations. SAP NetWeaver Identity Management is integrated with the SAP BusinessObjects Governance, Risk and Compliance solution. This gives customers the possibility to "Get Clean, Stay Clean and Stay in Control" across SAP Business Suite and heterogeneous applications.
- Integrating external applications with the applications that form the core of your business can be a scary thought. SAP NetWeaver Identity Management delivers the lowest-risk integration with SAP Business Suite. Our goal is to deliver predefined content and wizards based on best practices.
- SAP is currently setting up a certification program for partners to develop connectors for SAP NetWeaver Identity Management. This will create an ecosystem focused on delivering added value. In addition, the IDM infrastructure will be enabled for Web Services. This offers third parties, such as other IDM vendors, an opportunity to integrate with the solution and re-use the existing infrastructure.

Identity Management Yesterday

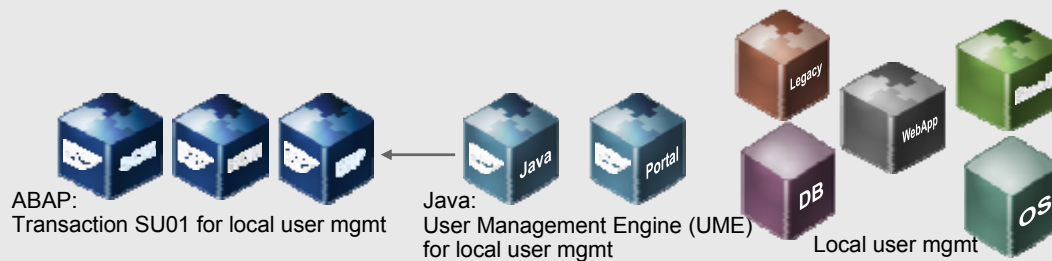
Localized User Administration



IDM triggered by identity business processes and data



Business process relies on appropriate user and role assignments in systems



© SAP AG 2009. All rights reserved. / Page 9

Localized User Administration

Enterprises usually operate a variety of different SAP and non-SAP systems. Every one of those systems has its own separate user management. This creates a lot of manual effort for the user administrator, who has to manage user information and role assignments in each system.

On the other hand, employees need to perform different tasks within a business process. These tasks require certain authorizations/roles in the system landscape.

Furthermore, the source of employee information is usually the HCM (Human Capital Management) system. Actions such as on-boarding, change of position, location, or name are triggered by HCM. These changes also need to be reflected in the system landscape.

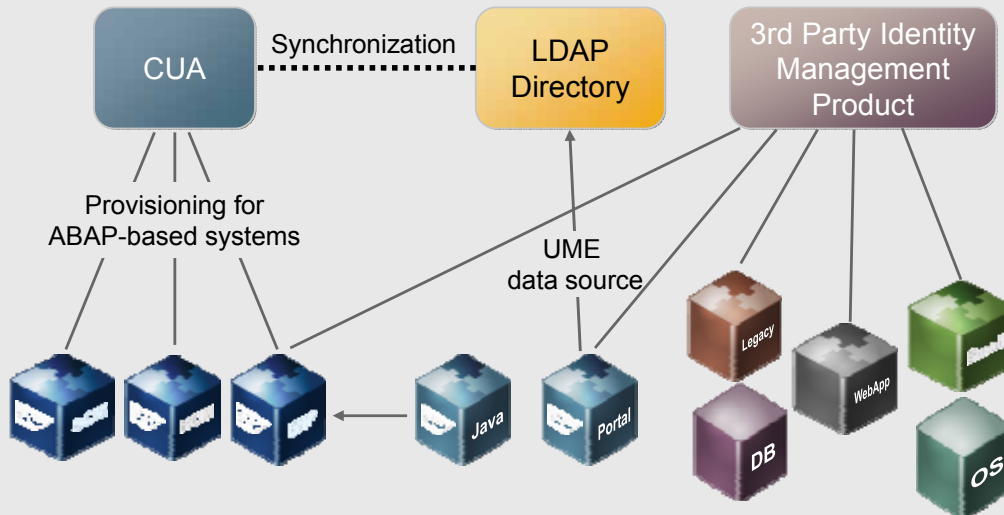
Identity Management Yesterday Partial Centralization



IDM triggered by identity business processes and data



Business process relies on appropriate user and role assignments in systems



© SAP AG 2009. All rights reserved. / Page 10

Partial User Management Centralization

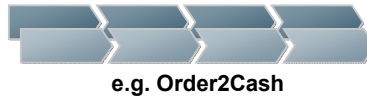
Before SAP offered SAP NetWeaver Identity Management, companies used the Central User Administration (CUA) for centralizing their user management processes. However, CUA is only supported for ABAP-based systems. For interoperability with Java systems that use an LDAP directory as user store, and for the integration with non-SAP applications, users can be synchronized with an LDAP directory using the ABAP LDAP connector.

For the central management of a heterogeneous system landscape, companies still needed a third-party identity management product.

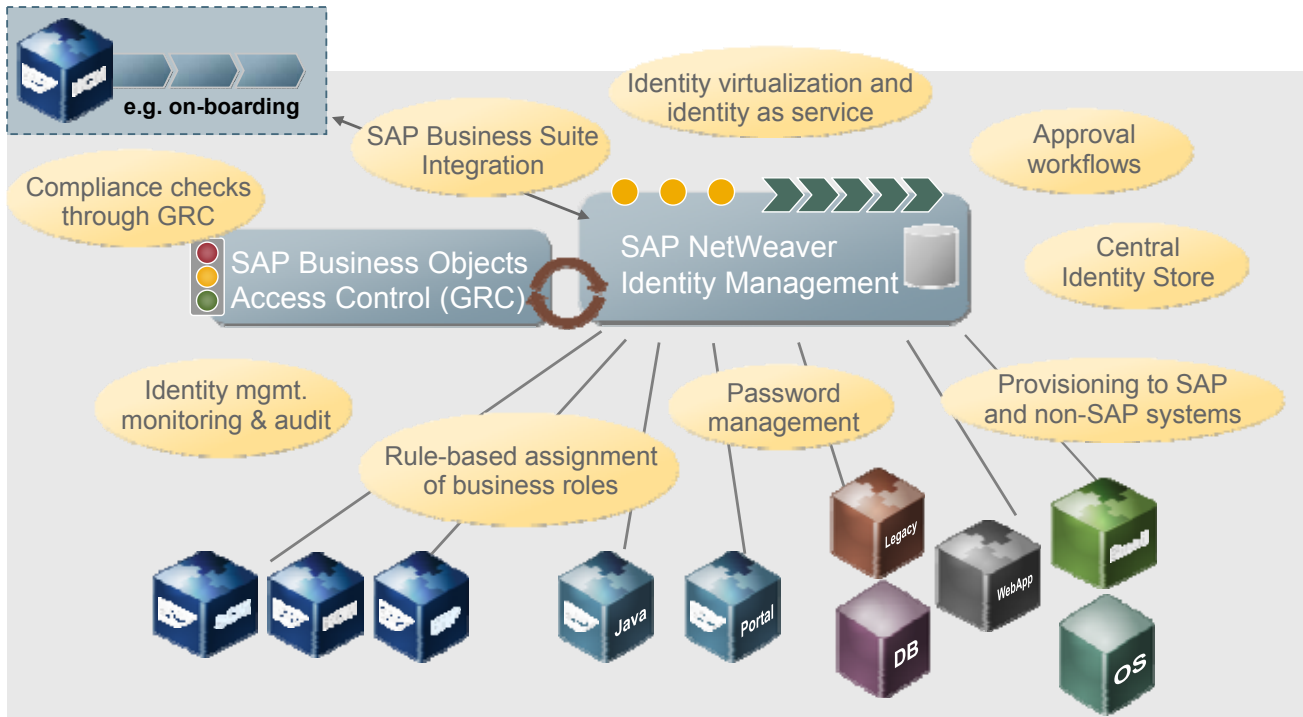
SAP NetWeaver Identity Management Holistic Approach



IDM triggered by identity business processes and data



Business process relies on appropriate user and role assignments in systems



© SAP AG 2009. All rights reserved. / Page 11

Holistic Identity Management Approach

With SAP NetWeaver Identity Management, SAP offers integrated identity management capabilities for a heterogeneous system landscapes (SAP and non-SAP software), driven by business processes.

- **Central Identity Store:** The central store consolidates identity data from different source systems (example: SAP HCM) and then distributes this information to the target systems.
- **Approval Workflows:** Workflows distribute the responsibility for authorization assignments to the different business process owners and managers.
- **Identity Virtualization / Identity as a service:** The data within SAP NetWeaver Identity Management can be accessed using services and standard protocols such as LDAP.
- **SAP Business Suite Integration:** The integration of HCM as one of the possible source systems for identity information is a key functionality for enabling business-driven identity management.
- **Compliance Checks / GRC:** The integration with SAP BusinessObjects Access Enforcer offers extensive functions for assuring compliance and segregation of duties in the role and authorization assignment process.
- **Definition and Rule-Based Assignment of Business Roles:** You can define different rule sets for the assignment of roles to users. This means that the assignment can be performed automatically based on attributes of the identity.
- **Monitoring and Audit:** Provides auditors with one central place to check employees' authorizations in all systems. This information is also available for the past.
- **Password Management:** A centralized password management reduces calls to the help desk for password resets, and enables password provisioning across heterogeneous landscape.
- **Distribution of Users and Role Assignments:** Handles user accounts and role assignments of SAP and non-SAP applications.

SAP NetWeaver Identity Management Within the Technology Platform



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.



Compliance	Regulatory Compliance	Auditing	SAP Solutions for Governance, Risk and Compliance	Security Targets	
Secure Collaboration	Web Services Security	Content Security	Security Interoperability		
Identity and Access Management	Identity Management	Authorization Concepts and Management	Authentication and Single Sign-On		
Infrastructure Security	Network and Communications Security	Operating System and Database Security	Front-End Security		
Software Lifecycle Security	Secure Product Development	Secure Delivery	Secure Configuration	Secure Change Management	Security Governance

© SAP AG 2009. All rights reserved. / Page 12

Identity Management - an Integral Part of the SAP NetWeaver Technology Platform:

- It enables the 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



1. Introduction to Identity Management
- 2. SAP NetWeaver Identity Management Solution in Detail**
 - 2.1 Role Management and Workflows**
 - 2.2 Business-Driven Identity Management
 - 2.3 Compliance and Auditing
 - 2.4 Password Management
 - 2.5 Identity Virtualization
 - 2.6 Connectivity and Services
3. SAP NetWeaver Identity Management Architecture
4. Summary & Additional Information Sources

Business Roles and Technical Roles

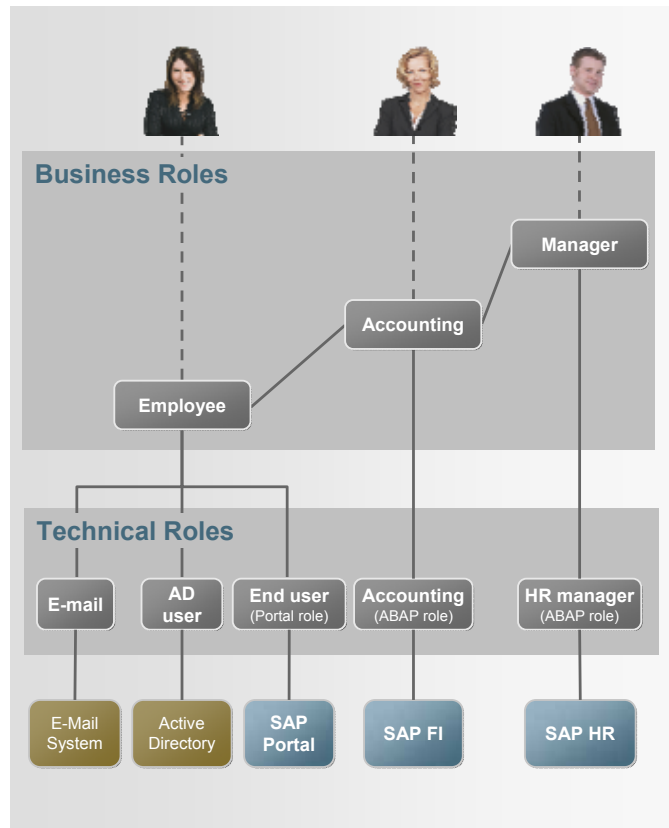


Business Roles

- Are defined in the Identity Center
- Represent the business tasks of an employee
- Are usually defined as part of a business process
- Can be set up in hierarchies
- Are a combination of technical roles and/or other business roles
- Are usually assigned to end users

Technical Roles

- Represent access information or technical authorizations (e.g. ABAP authorization roles, UME roles, Portal roles, AD groups, ...)
- Are usually uploaded from the target system
- Are system-specific
- Are usually represented as “privileges” in the Identity Center



© SAP AG 2009. All rights reserved. / Page 14

Business Roles and Technical Roles

The Identity Center uses the concept of **business roles** and **technical roles**.

Technical roles in the Identity Center represent the access information or technical authorizations from the various target systems.

- ABAP authorization roles are uploaded from ABAP-based SAP systems.
- Portal roles, UME roles, and UME groups are uploaded from Java-based SAP systems.
- Other access information is uploaded from non-SAP systems.
- You can define technical roles for the Identity Center itself as well.
- All technical roles are maintained in the target systems and are uploaded/refreshed in the Identity Center regularly. Technical roles in the Identity Center are called “privileges”.

Business roles represent the business tasks of an employee. You can define business roles in the Identity Center; these roles help manage and structure the assignment of technical roles in the target systems.

- By assigning a business role to a user, all technical roles of that business role and any role below that business role in the hierarchy will be assigned to the user.
- Workflow and provisioning will also be triggered.

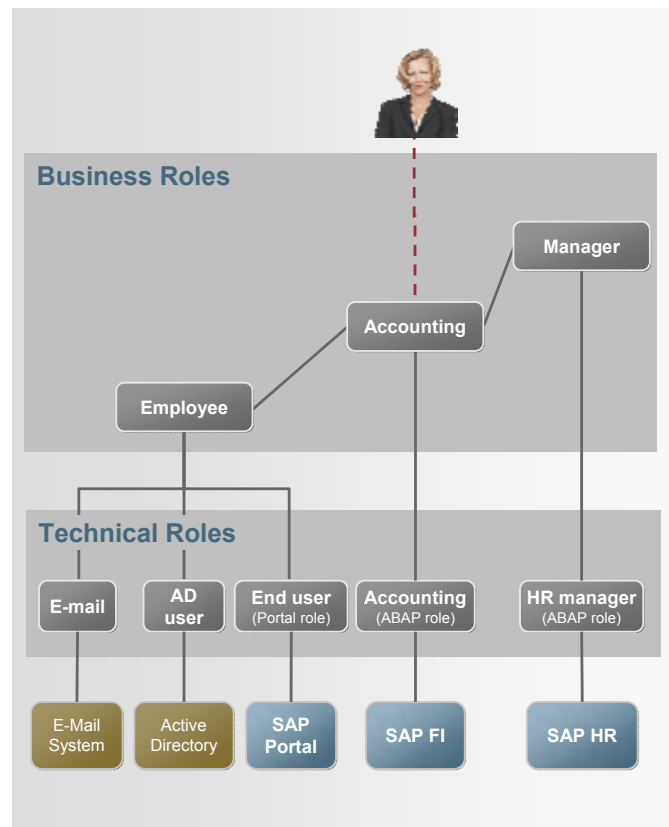


Role Definition (design, one-time task)

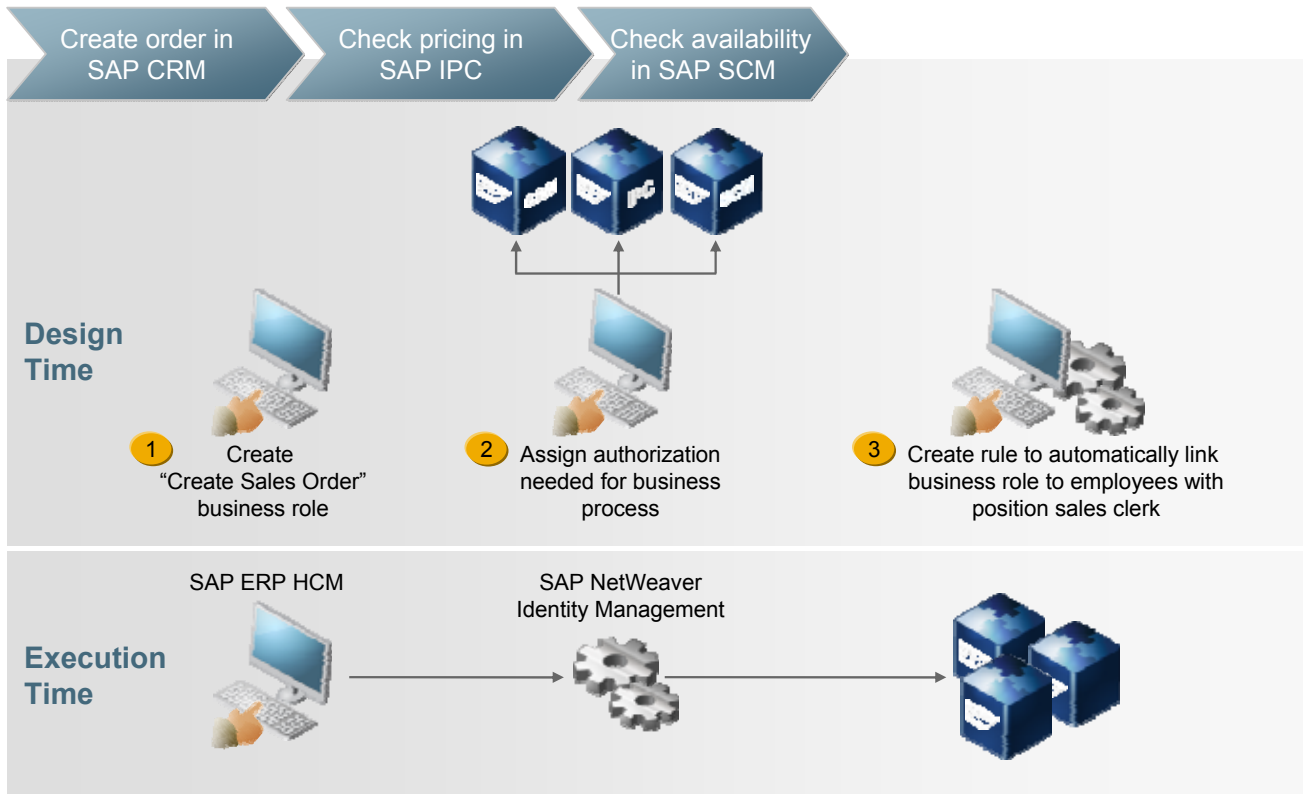
- Read system access information (roles, groups, authorizations, ...) from target systems
- Define a business role hierarchy
- Assign technical roles to business roles
- Develop rules for role assignments

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



© SAP AG 2009. All rights reserved. / Page 16

Role Management

Managing authorizations by assigning one authorization to one person at the time is not only a time-consuming process; it also makes it difficult to control and manage access in general.

Role management provides the solution: It starts out with the analysis of an employee's tasks, then maps these tasks to the appropriate access rights and tools.



Operates on entries in the identity store

Manual interactions through Web interface

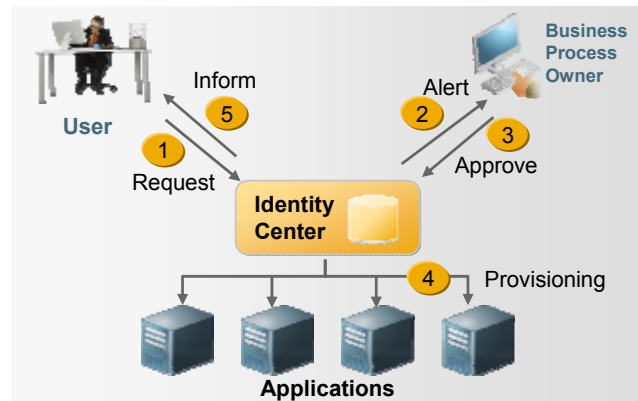
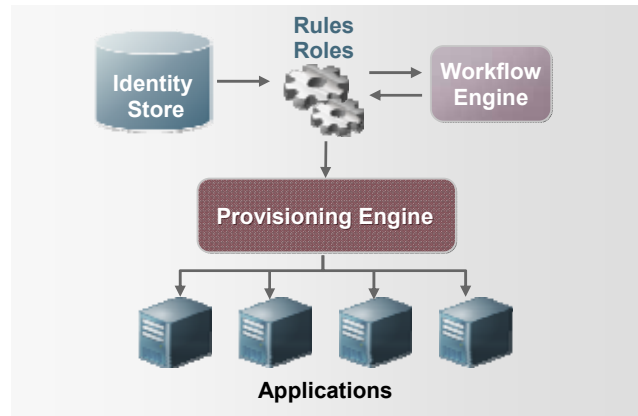
- Start provisioning tasks
- Approve requests
- Monitor status

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



Workflows

Workflow support for identity management operations is an important feature of the Identity Center. Employees, their managers, and the IT team can use workflows to delegate certain tasks to the responsible people.

You can create Web-based tasks for interactive identity management operations (request, approve, ...), but rule definitions that have no interaction are also defined in the workflow.

The workflows can either be triggered by a Web interface task or by an “event task” that recognizes changes.

The definition of the rule logic is highly flexible. This includes sequential, parallel, conditional, and approval operations.

Agenda



1. Introduction to Identity Management
- 2. SAP NetWeaver Identity Management Solution in Detail**
 - 2.1 Role Management and Workflows
 - 2.2 Business-Driven Identity Management**
 - 2.3 Compliance and Auditing
 - 2.4 Password Management
 - 2.5 Identity Virtualization
 - 2.6 Connectivity and Services
3. SAP NetWeaver Identity Management Architecture
4. Summary & Additional Information Sources

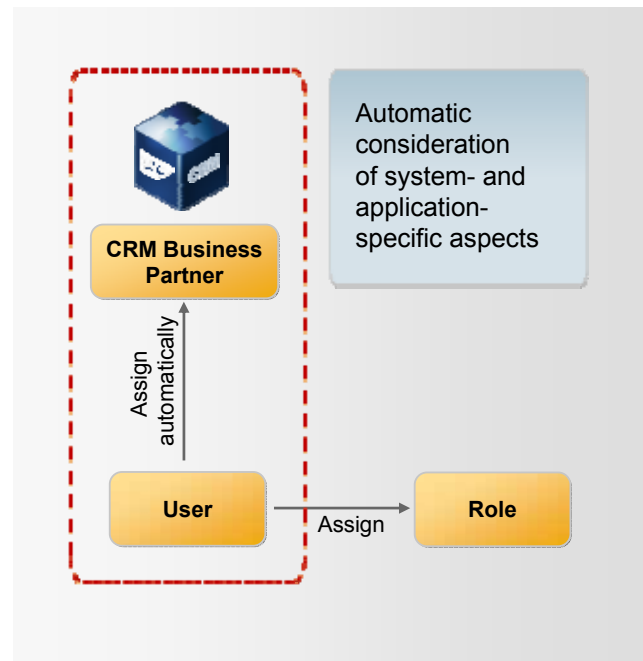
SAP NetWeaver IDM and SAP Business Suite: Increasing User Management Efficiency



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.



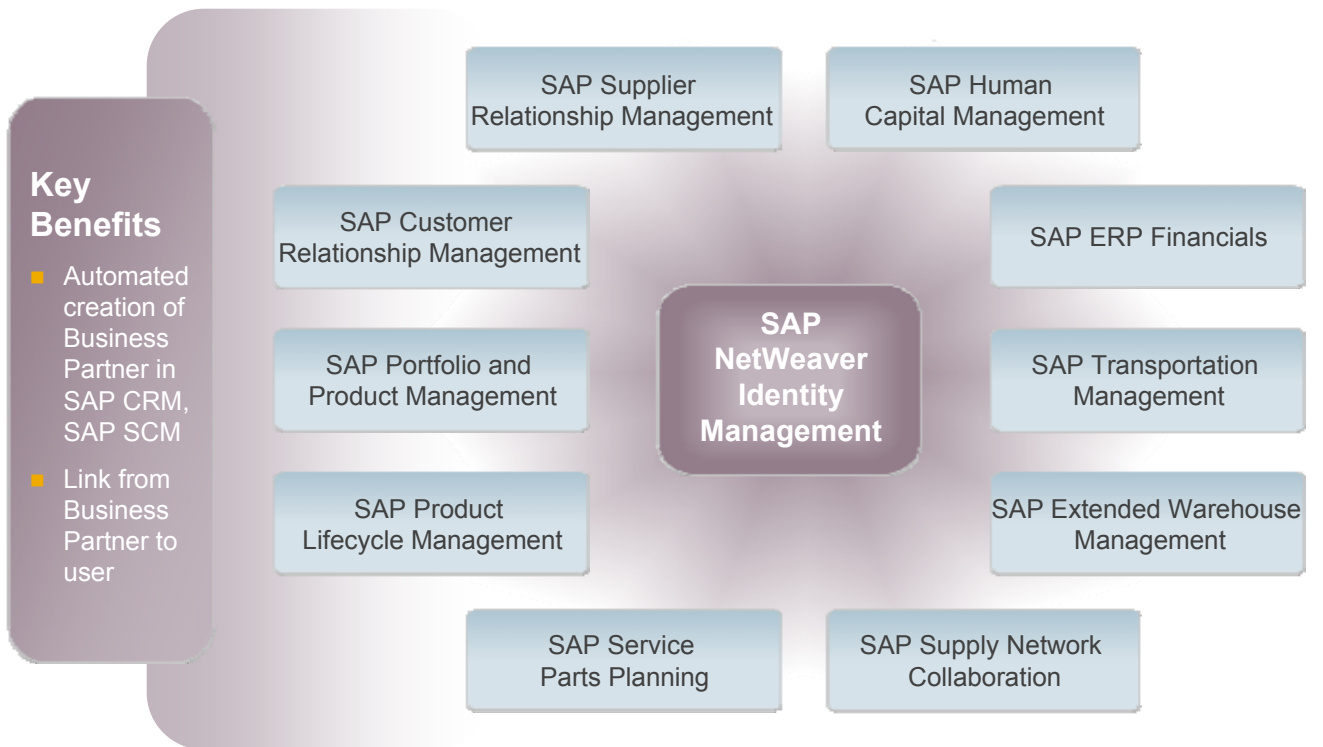
SAP NetWeaver IDM automates the Business Partner assignment in SAP CRM, eliminating the need for manual administration steps.

© SAP AG 2009. All rights reserved. / Page 19

SAP Business Suite Integration

User accounts are often maintained manually in each system, increasing the workload for system administrators. What is more, the different systems that require user account maintenance often have their own set of prerequisites - such as the creation of a "Business Partner" in SAP CRM or SAP SCM. Features like these add to the complexity of managing users in heterogeneous system landscapes.

SAP Business Suite Integration Business-Driven Identity Management



© SAP AG 2009. All rights reserved. / Page 20

SAP Business Suite

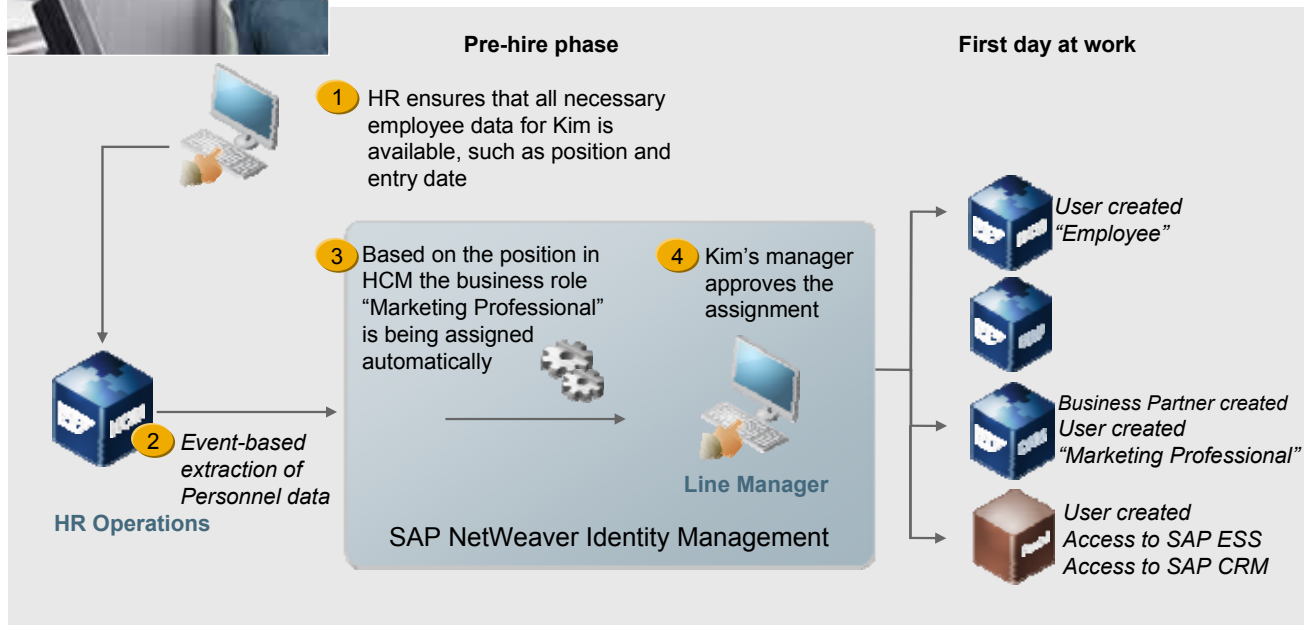
SAP NetWeaver IDM offers more than identity provisioning in heterogeneous landscapes. With Release 7.1, it is capable of integrating seamlessly into the business processes of SAP Business Suite, simplifying tasks such as linking to employee data and creating or assigning users to Business Partners. In SAP NetWeaver Identity Management 7.1, all use cases involving employees are supported.

Business Process Driven Identity Management On-Boarding



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.



© SAP AG 2009. All rights reserved. / Page 21

On-Boarding Process

By integrating SAP NetWeaver Identity Management with the SAP Business Suite, SAP supports user administration and distribution in alignment with business events that require user-centric activities, such as:

- On-boarding process of new hires**
 Your company expects a new hire. The SAP NetWeaver Identity Management integration with SAP ERP allows you to generate the user before the new employee even joins the company. On their first day of work, new hires already have access to the systems that correspond to their new job roles. This speeds up the time to productivity.
- Organizational changes**
 When employees change jobs within your company, this often requires a re-assignment of system access rights. For example, an employee could be promoted to the position of line manager, or transfer to a different department. Employees might also be assigned to mid- or long-term projects that require access to a new set of systems. The integration of SAP NetWeaver Identity Management with your SAP Business Suite enables you to automate system access control.
- Termination of employment**
 When employees leave the company, their access rights and authorizations for your IT landscape need to be revoked at once. This ensures that former employees cannot tamper with company information.

Let's take a closer look at the on-boarding process on this slide. You just hired Kim Perkins as a marketing professional. On her first day of work, she can already access all relevant systems and perform her job. Which steps were necessary to achieve such a quick start for Kim? During the pre-hire phase, once Kim had accepted the job offer and a start date was set, your SAP ERP HCM system handed over the relevant data for Kim to SAP NetWeaver Identity Management.

Based on this extraction of Kim's personnel data, SAP NetWeaver IDM created a user for Kim, assigned the role of marketing professional to this newly generated identity, and, based on her manager's approval, also generated the users in the systems Kim will need to access (such as CRM, e-mail, etc.). In our example, Kim needed access to the following systems:

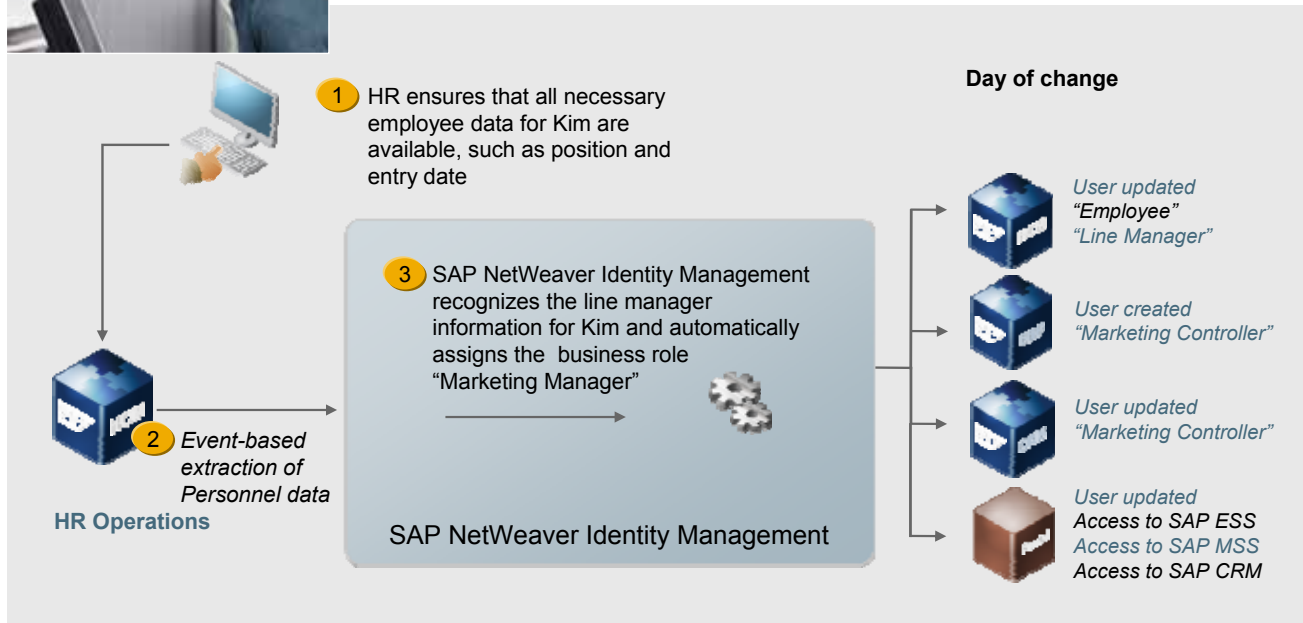
- SAP ERP HCM:** All employees have access to the SAP Employee Self-Service functions to maintain their own personal data. The system automatically generates and assigns this user.
- SAP CRM:** The system automatically receives Kim's user and creates the corresponding business partner. She is able to execute all business tasks necessary for her marketing job in the SAP CRM system.
- SAP Enterprise Portal:** Kim will access some applications through the Enterprise Portal; the necessary users are also available in these systems from the first day.

All users in the receiving systems were created and active in time because the marketing professional role was assigned to Kim in SAP NetWeaver Identity Management. Based on the business role information, Kim has access to all business processes she needs as a new employee in the company.

Business Process Driven 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.



© SAP AG 2009. All rights reserved. / Page 22

Organizational Change

The second example shows how the combination of SAP NetWeaver Identity Management and SAP Business Suite handles relevant user information updates and their distribution. This update is triggered by a business event, in our case an organizational change.

Kim Perkins takes over additional responsibility after two years with the company. She is promoted to take over the role of line manager, and she is now responsible for a team and a marketing budget. Based on the HR data available in the system (e.g. the new line manager assignment) and the data extraction from SAP ERP HCM to SAP NetWeaver Identity Management, the system automatically recognizes the new line manager responsibility for Kim.

By assigning the new business role "marketing manager", the system automatically adjusts the user information and system access rights to match her new responsibilities.

In the SAP HCM system, Kim's user information is updated to reflect her new role as line manager. This includes the appropriate authorization profile assignment.

To view the marketing budget, she gets a new user in the SAP ERP system and now has access to all budget-relevant transactions in this system.

In SAP CRM, her user information is updated as well. Under her new role assignment as a marketing controller, she can access all relevant business tasks in SAP CRM.

In her company's enterprise portal, she is now able to access the SAP Manager Self-Service application.

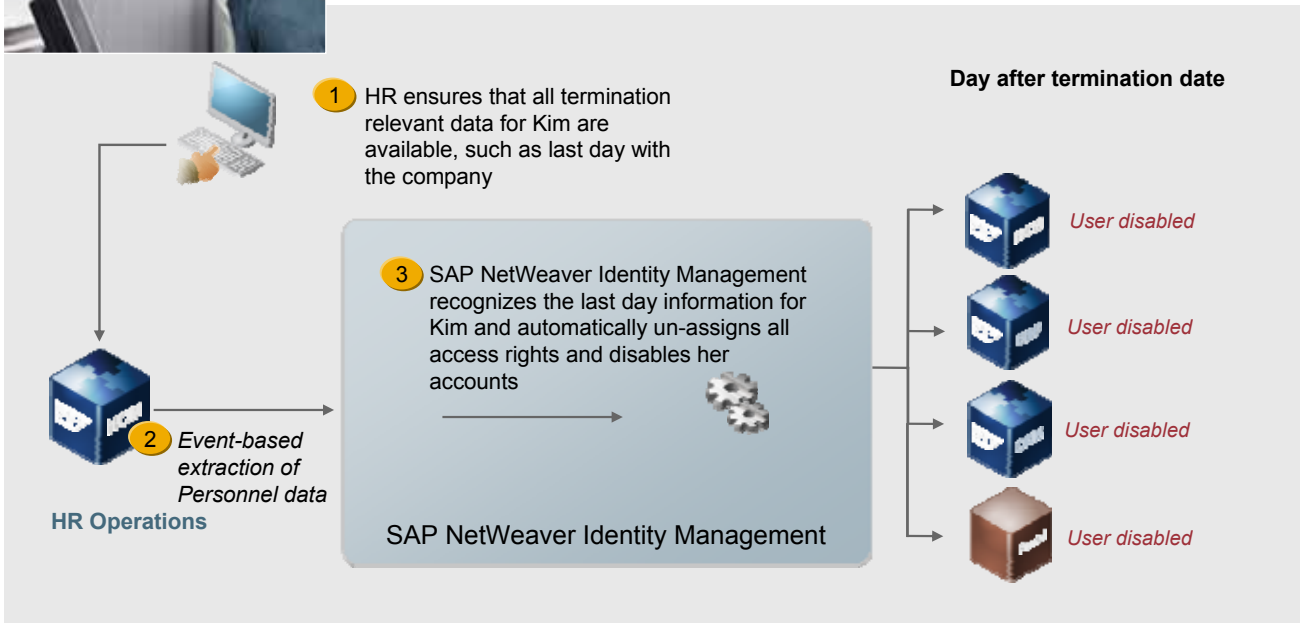
Kim's users in receiving systems were created or updated and are active. Based on the business role information, Kim has access to all the new business processes she needs right from the day the organizational change becomes effective.

Note: Her line manager's approval is not required for the user administration and distribution process. All necessary actions are automated and considered authorized based on the fact that her promotion was already approved. The integration of an additional workflow to approve the new role / authorization assignments is possible, but not mandatory.

Business Process Driven Identity Management Termination



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.



© SAP AG 2009. All rights reserved. / Page 23

Termination of Employment

If an employee leaves the company, a reverse chain of actions is triggered in SAP NetWeaver IDM.

After eight years, Kim Perkins decides to move on to a new company. Her most current HR data is extracted from SAP HCM to SAP NetWeaver IDM. The identity management system automatically un-assigns or deletes all access rights and disables Kim's accounts. Based on the last day information, Kim no longer has access to any company system the day after she leaves. As the termination of Kim's employment was approved beforehand, the implementation of an approval step in the user administration and distribution procedure is again optional.

Agenda



1. Introduction to Identity Management
- 2. SAP NetWeaver Identity Management Solution in Detail**
 - 2.1 Role Management and Workflows
 - 2.2 Business-Driven Identity Management
 - 2.3 Compliance and Auditing**
 - 2.4 Password Management
 - 2.5 Identity Virtualization
 - 2.6 Connectivity and Services
3. SAP NetWeaver Identity Management Architecture
4. Summary & Additional Information Sources

SAP NetWeaver Identity Management Auditing and Monitoring



- **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**

Access control history
User: 3020 Christopher Wright
Date: 11/07/2007

3020 Christopher Wright
Period: 2004-12-01 2005-02-28

1092 Accounting system

Access	Period	Approval Date	Approval
Full access	2004-12-01 2005-02-28	2005-01-01	1092 System Admin

1093 E-mail account

Access	Period	Approval Date	Approval
Full access	2004-12-01 2005-02-28	2005-01-01	1092 System Admin

Access control history
System: 1092 Accounting system
Date: 11/07/2007

1092 Accounting system
Period: 2005-01-01 2005-02-28

Full access
The following persons have full access to the accounting system:

Employee ID	Name	Period
1092	John Doe	2005-01-01 2005-02-28
1092	Christopher Wright	2005-01-01 2005-02-28

Reporting
The following persons can produce reports from the accounting system:

Employee ID	Name	Period
1092	John Doe	2005-01-01 2005-02-28
1092	Christopher Wright	2005-01-01 2005-02-28
1092	John Doe	2005-01-01 2005-02-28
1092	Christopher Wright	2005-01-01 2005-02-28
1092	John Doe	2005-01-01 2005-02-28
1092	Christopher Wright	2005-01-01 2005-02-28

© SAP AG 2009. All rights reserved. / Page 25

Auditing and Monitoring

The auditing and monitoring functionality of the Identity Center provides a central mechanism to show which user has or had which access rights to which system. You can create reports and schedule them to run on a regular basis (or upon request). SAP delivers a set of pre-defined reports; you can easily extend these reports to match your individual requirements.



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

Compliant Identity Management

- 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

Compliant Identity Management

Combining the strengths of SAP BusinessObjects Access Control (GRC) and SAP NetWeaver Identity Management creates the perfect solution to ensure that IT business application controls are compliant across SAP and heterogeneous environments while ensuring increased security and reduced TCO.

Deploying SAP NetWeaver Identity Management together with SAP BusinessObjects Access Control enhances the solution in two ways:

- It enables SAP BusinessObjects Access Control to extend its reach beyond ERP.
- It enables the solution to cover the whole picture from the compliance need of the CFO to the cost reduction and security requirements of the CIO.

SAP BusinessObjects Access Control (GRC) & SAP NetWeaver IDM – Integration



SAP NetWeaver Identity Management

SAP NetWeaver Identity Management

- Heterogeneous connectivity
- SAP Business Suite integration
- Powerful business role mapping
- Password management

SAP BusinessObjects Access Control (GRC)

SAP BusinessObjects Access Control (GRC)

- Compliance checks
- Business risk controls and mitigation

Combined

SAP NetWeaver Identity Management

SAP BusinessObjects Access Control (GRC)

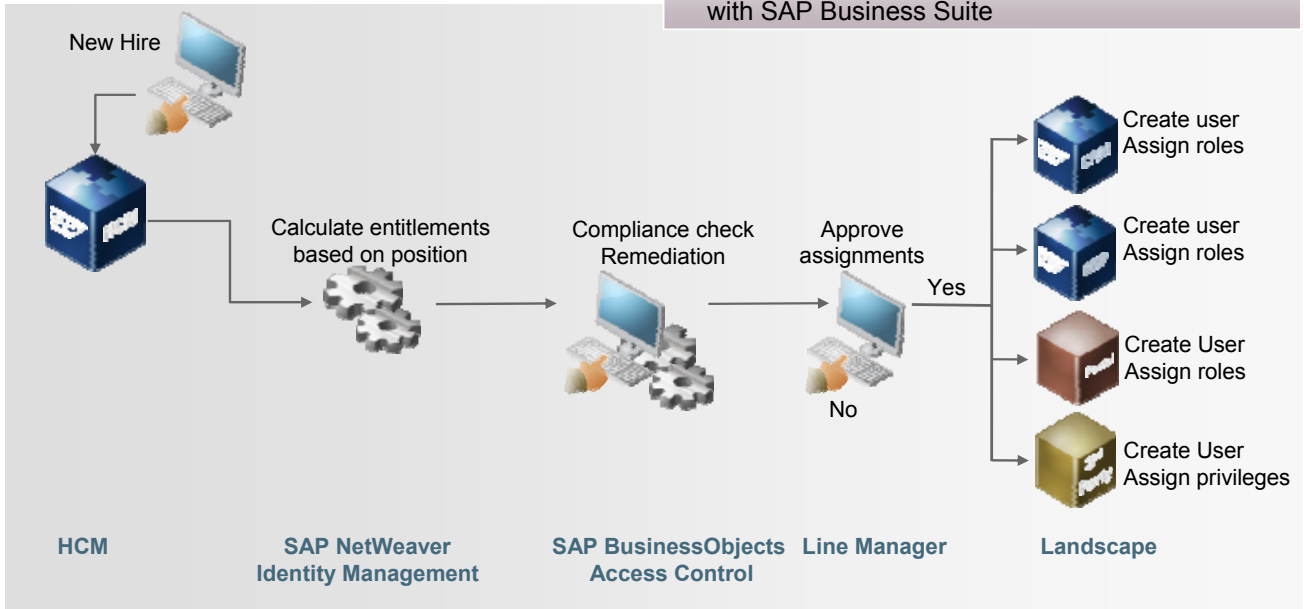
Compliant identity management for the entire system landscape!

Business Process Driven, Compliant 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



Agenda



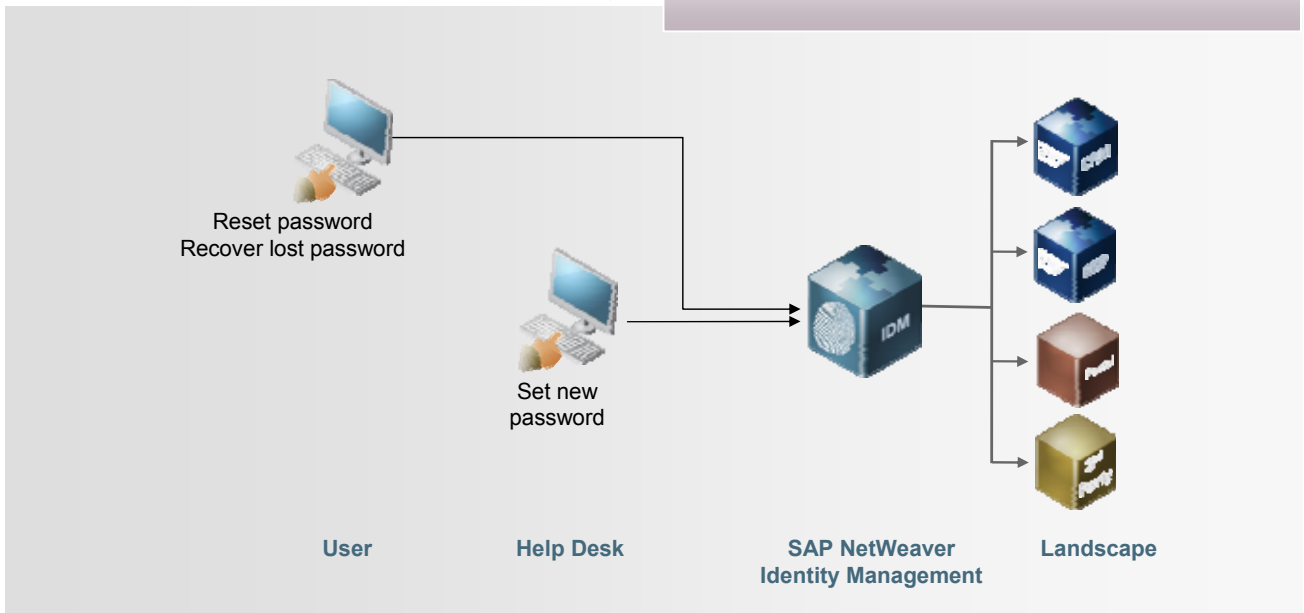
1. Introduction to Identity Management
- 2. SAP NetWeaver Identity Management Solution in Detail**
 - 2.1 Role Management and Workflows
 - 2.2 Business-Driven Identity Management
 - 2.3 Compliance and Auditing
 - 2.4 Password Management**
 - 2.5 Identity Virtualization
 - 2.6 Connectivity and Services
3. SAP NetWeaver Identity Management Architecture
4. Summary & Additional Information Sources

Password Management



Requirement:
Centralized password management

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



© SAP AG 2009. All rights reserved. / Page 30

Password Management

SAP NetWeaver Identity Management supports self-service password reset and password synchronization across all connected target systems. This function reduces the cost incurred by the help desk for password resets.

Agenda



1. Introduction to Identity Management
- 2. SAP NetWeaver Identity Management Solution in Detail**
 - 2.1 Role Management and Workflows
 - 2.2 Business-Driven Identity Management
 - 2.3 Compliance and Auditing
 - 2.4 Password Management
 - 2.5 Identity Virtualization**
 - 2.6 Connectivity and Services
3. SAP NetWeaver Identity Management Architecture
4. Summary & Additional Information Sources

Identity Virtualization



Virtual Directory Server (VDS) provides

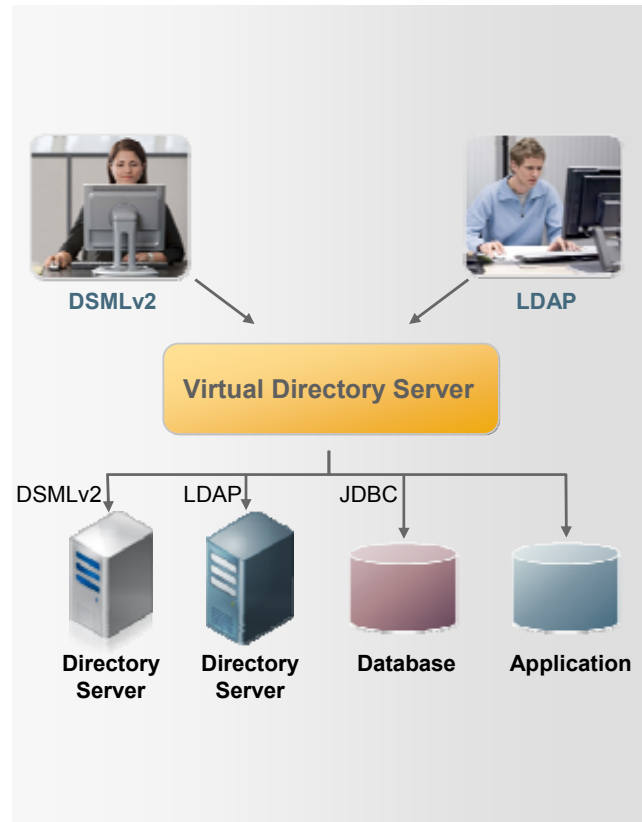
- Single consistent view and entry point for multiple distributed identity data sources
- Identity information as a service for applications through standard protocols (LDAP, DSMLv2)
- Abstraction layer for underlying data stores

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



© SAP AG 2009. All rights reserved. / Page 32

Identity Virtualization

SAP NetWeaver Identity Management consists of two main components: The Identity Center and the Virtual Directory Server (VDS). The VDS provides a single and consistent view and entry point to multiple distributed identity data sources. The data can be accessed using standard protocols such as LDAP. The data is not copied, but loaded online upon request. Since the data is not copied, the Virtual Directory Server uses caching mechanisms for best performance.

The Virtual Directory Server grants real-time access to data in multiple data stores.

Agenda



1. Introduction to Identity Management
- 2. SAP NetWeaver Identity Management Solution in Detail**
 - 2.1 Role Management and Workflows
 - 2.2 Business-Driven Identity Management
 - 2.3 Compliance and Auditing
 - 2.4 Password Management
 - 2.5 Identity Virtualization
 - 2.6 Connectivity and Services**
3. SAP NetWeaver Identity Management Architecture
4. Summary & Additional Information Sources

CUA & SAP NetWeaver Identity Management Frequently Asked Questions



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 will continue to support CUA in its current functionality according to SAP maintenance rules.
- SAP NetWeaver IDM can be connected and used in combination with an existing CUA.

Should I install a new CUA?

- It depends on the scope of your project and your current stage:
You can quickly and easily connect ABAP-based systems to a new CUA. This enables you to manage several thousand users and their individual role assignments.
- However, if you require automatic cross-system rule-based access management, workflow support, or connectivity for a heterogeneous system landscape, you should consider using SAP NetWeaver Identity Management.

© SAP AG 2009. All rights reserved. / Page 34

Feature Comparison CUA and SAP NetWeaver IDM:

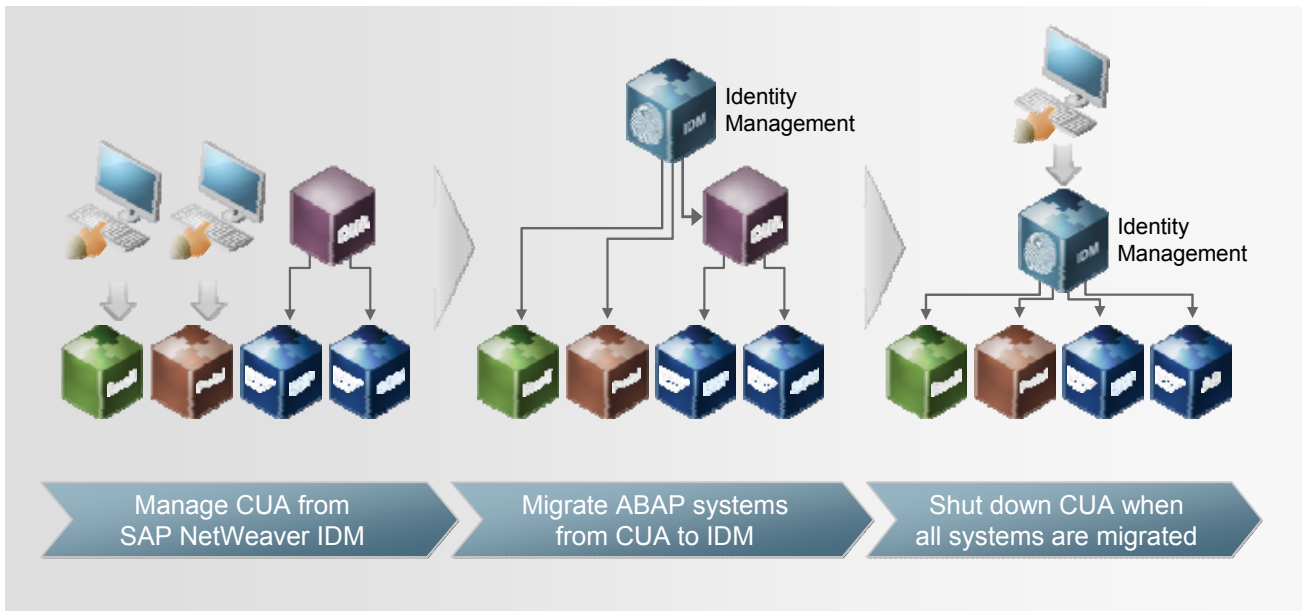
Functionality	CUA	SAP NetWeaver Identity Management 7.0
Target systems	ABAP only	SAP and non-SAP
Workflow support	no	yes
Rule-based access mgmt	almost no (exc. rarely used HR Org. rule engine)	yes
Modeling of role hierarchy	no	yes
Cross-system role assignm	manual	full support
LDAP directory integration	LDAP synchronization	full support
Support of all user attributes	yes	Partial (->full in 7.1)
Password management	Initial passwords	yes incl. workflow support

Central User Administration (CUA) Migration



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

- Supports SAP and heterogeneous environments
- Self-service and delegated admin
- Workflow and approvals
- Business role management



© SAP AG 2009. All rights reserved. / Page 35

Central User Administration (CUA)

In the past, Central User Administration (CUA) was SAP's solution for managing users and roles in a typical large ABAP system landscape. The solution has significantly reduced the complexity of managing such landscapes compared to separate user administration in each system. However, CUA has several limitations:

- CUA only supports ABAP systems. This means that neither Java-based nor 3rd party applications can be managed consistently.
- Role management is limited to assigning users to roles and creating composite roles within one ABAP system. There is no support for managing business roles across multiple ABAP systems, Java-based and 3rd party applications
- CUA offers no support for self-service, delegated administration or approvals.

Due to these limitations, SAP recommends the migration from CUA to SAP NetWeaver Identity Management.

The benefits of a CUA – IDM migration:

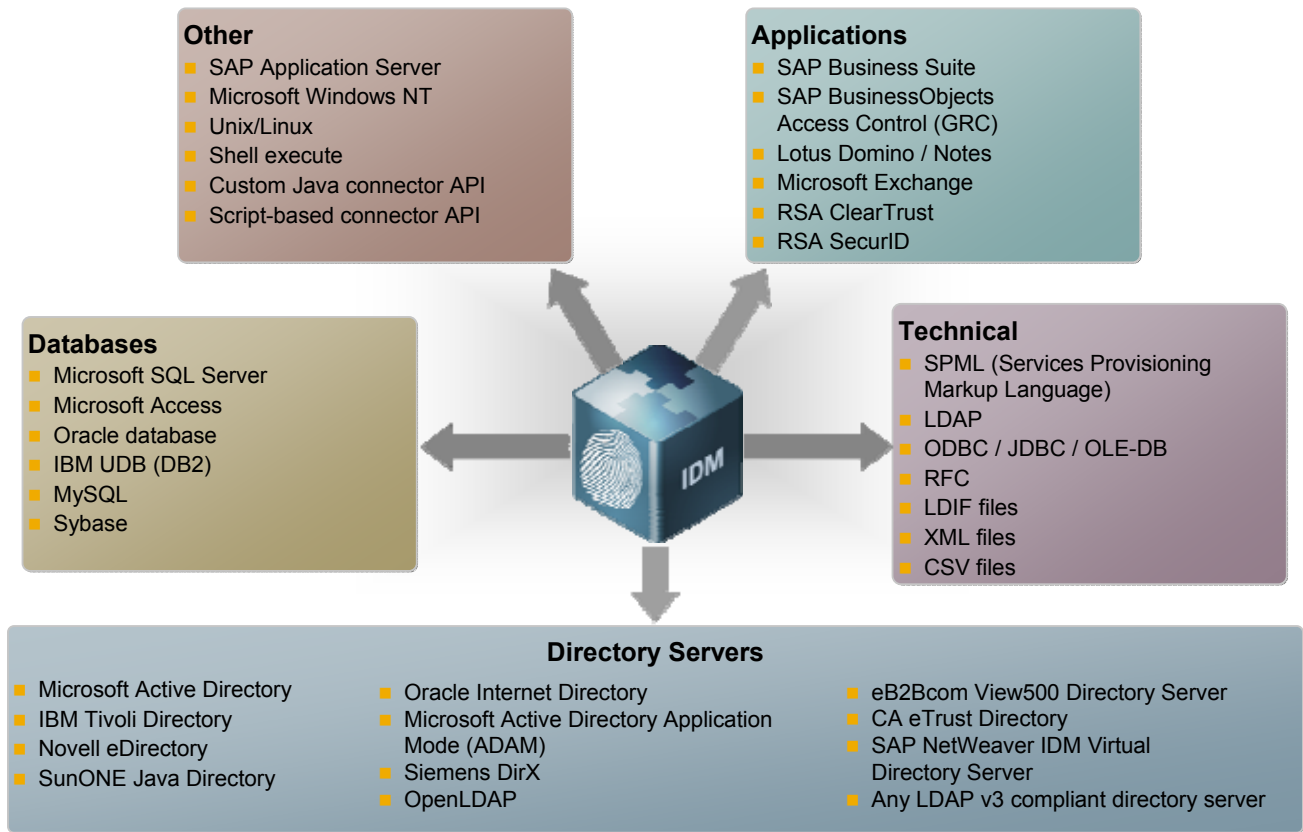
- Support is not limited to ABAP systems, but extends to Java-based systems and 3rd party applications in a heterogeneous environment.
- More flexible role management that enables the creation of business roles across ABAP, Java and heterogeneous environments. The advanced role management enables you to manage the life cycle or business roles, including creation, assignment of authorizations and request management including approval flows.
- SAP NetWeaver Identity Management offers powerful and flexible workflow mechanisms for supporting self-service, delegated administration and approval flows.

For the migration, SAP recommends to install SAP NetWeaver Identity Management on top of your CUA. This way you can introduce the benefits of SAP NetWeaver IDM without disrupting your current landscape.

Then, you can start connecting the ABAP systems to SAP NetWeaver Identity Management, and disconnect them from CUA.

When the last system is disconnected from CUA, the CUA can be shut down and you have completed a successful migration.

SAP NetWeaver Identity Management Connectivity – Overview



© SAP AG 2009. All rights reserved. / Page 36

Connectivity

The connectors shown on this slide are offered out-of-the-box with SAP NetWeaver IDM.

Note that there are certain limitations.

Example:

Version limitations for the MS-Exchange connector: We currently support Microsoft Exchange 5.5, Microsoft Exchange 2000 and Microsoft Exchange 2003. For Microsoft Exchange 2007 as well as for the RSA ClearTrust and SecurID connectors, you need to open a CSS-ticket in BC-IDM in order to receive more detailed information (status Q1/2009).



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






Identity Center Integration

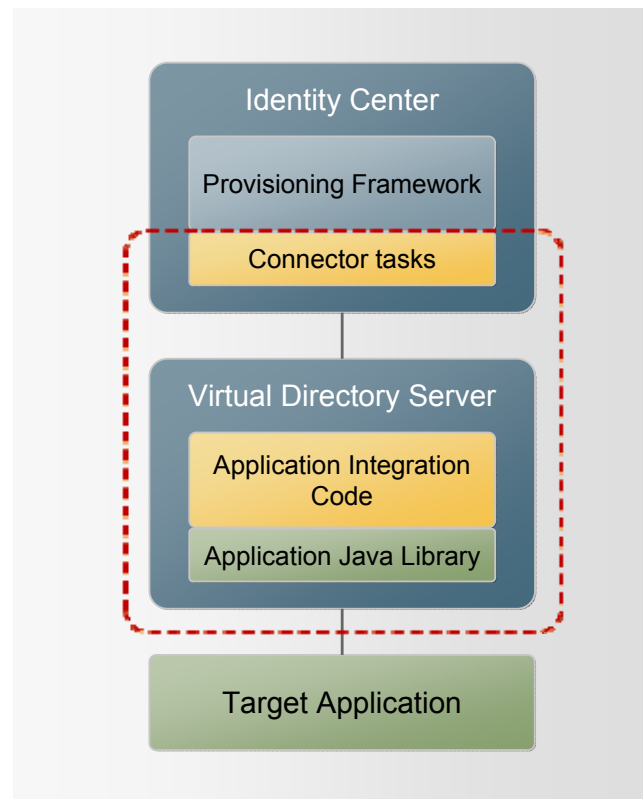
- The connector tasks integrate into the existing (common) provisioning framework in the Identity Center
 - A set of tasks has to be customized to work together with the target application utilizing VDS.

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)

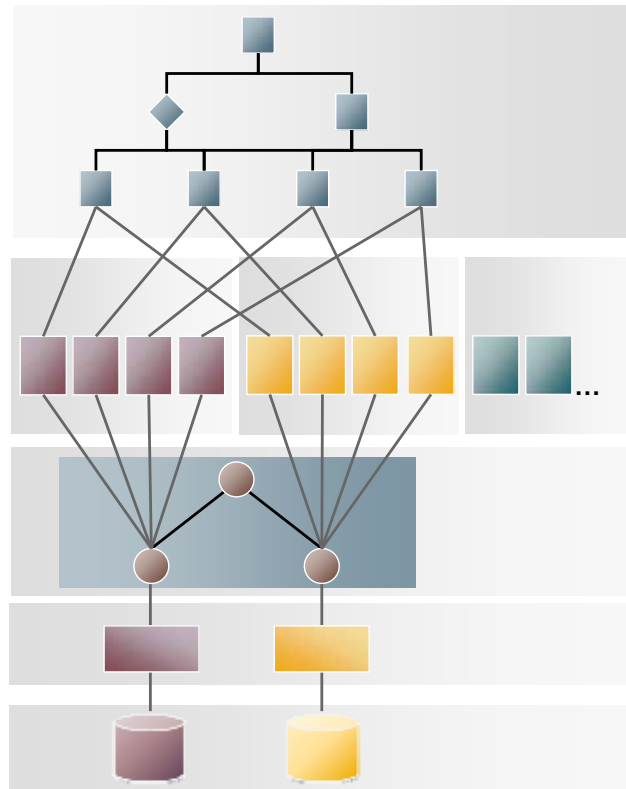
- Hooked into the provisioning framework

Virtual Directory Server (VDS)

Connectors from Partners

- Multiple connectors in a virtual tree

Back-Ends (Third-Party Applications)



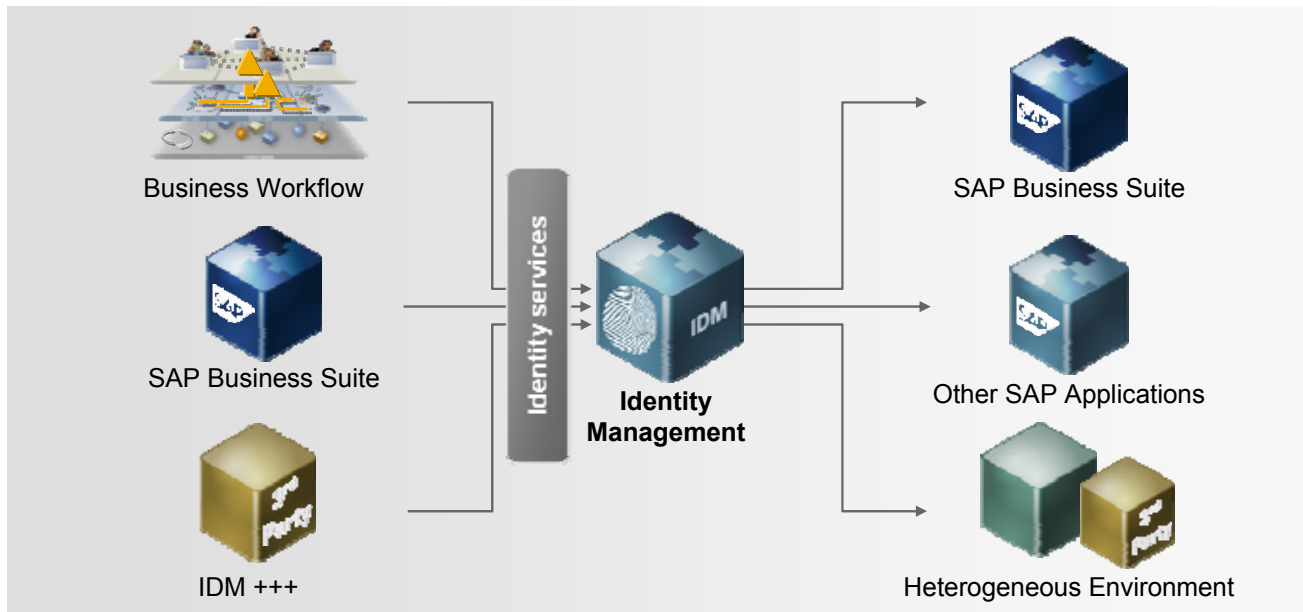
Identity Services SOA-Based Identity Management



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



© SAP AG 2009. All rights reserved. / Page 40

SOA-Based Identity Management

Most applications offer the possibility of assigning authorizations and access rights directly to users. Since this is not a very efficient way of managing access, most applications offer a role or group concept. Depending on the application, access rights are assigned to the role (as in SAP Business Suite applications) or applications give access rights to groups (as in MS Active Directory). These roles and groups normally grant rights for functions in the application, but they are unable to cover complex business processes that include multiple functions across different applications.

The most efficient way of streamlining the process of managing individual users, their access rights, and membership to these IT roles, is Business Role Management.

How organizations model their business roles depends on two factors:

- The set-up of the IT infrastructure
- How authorizations can be mapped to business processes and job functions or positions

With SAP NetWeaver Identity Management, you can manage business roles based on your specific organizational requirements.

It enables you to group authorizations and access rights into "process roles" that correspond to business processes. These process roles can then be grouped again according to position/job functions. Users can be given this position, which then will automatically assign the correct authorization and access rights.

A next step planned for the future will be to link these "position roles" to the position the user has according to the Organizational Management feature in SAP ERP HCM.

Since not all of the role management functionality can be automated, self-service and delegated administration is also available. This enables users to request membership for roles; managers can approve these requests or directly assign the required roles.

Agenda



1. Introduction to Identity Management
2. SAP NetWeaver Identity Management Solution in Detail
 - 2.1 Role Management and Workflows
 - 2.2 Business-Driven Identity Management
 - 2.3 Compliance and Auditing
 - 2.4 Password Management
 - 2.5 Identity Virtualization
 - 2.6 Connectivity and Services
- 3. SAP NetWeaver Identity Management Architecture**
4. Summary & Additional Information Sources

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

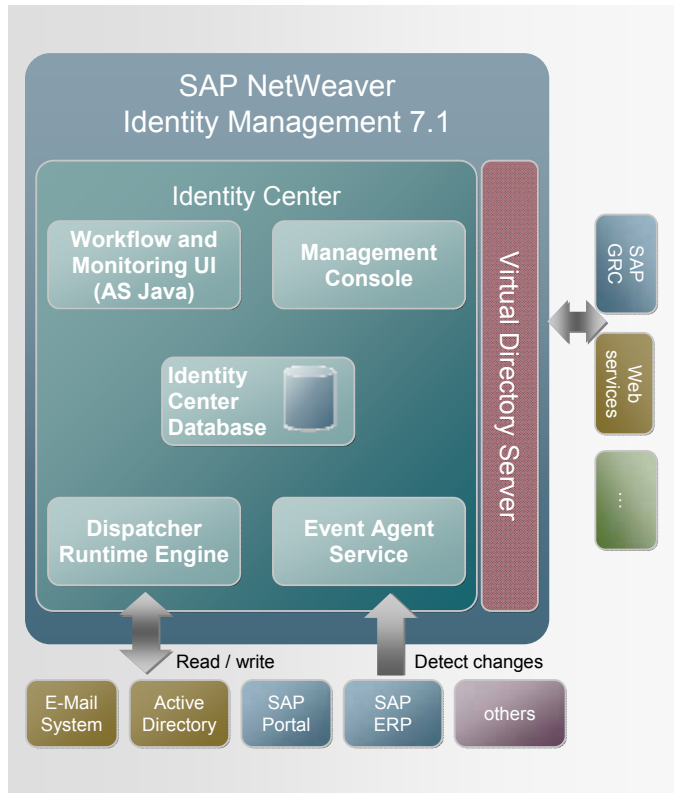
- Processing and provisioning logic including connectors

Event Agent

- Monitors connected systems and initiates synchronization

Virtual Directory Server

- Virtualization layer



© SAP AG 2009. All rights reserved. / Page 42

Architectural Overview

The Identity Center uses a database to store information about identities as well as configuration information. Currently, it supports MS SQL server and Oracle databases. The configuration and the processing logic are defined within the data base.

The Workflow UI is based on WebDynpro Java*; it provided access to end users access for tasks such as requests or approvals.

The Monitoring UI is based on the same technology as the Workflow UI; it enables administrators to access audit and monitoring functionality as well as the status of the provisioning tasks.

The Management Console is a snap-in for the MS Management Console. It is used to configure the processing logic of the Identity Center (i.e. connect target systems, definition of workflow processes, ...).

The Dispatcher is based on the runtime engine. The runtime engine is responsible for provisioning.

The Event Agent detects changes in repositories that are not able to actively report changes to the Identity Center.

*) In SAP NetWeaver Identity Management 7.0, the user interface is generated with PHP and uses a Web Server (either MS IIS or Apache)

Central Identity Store

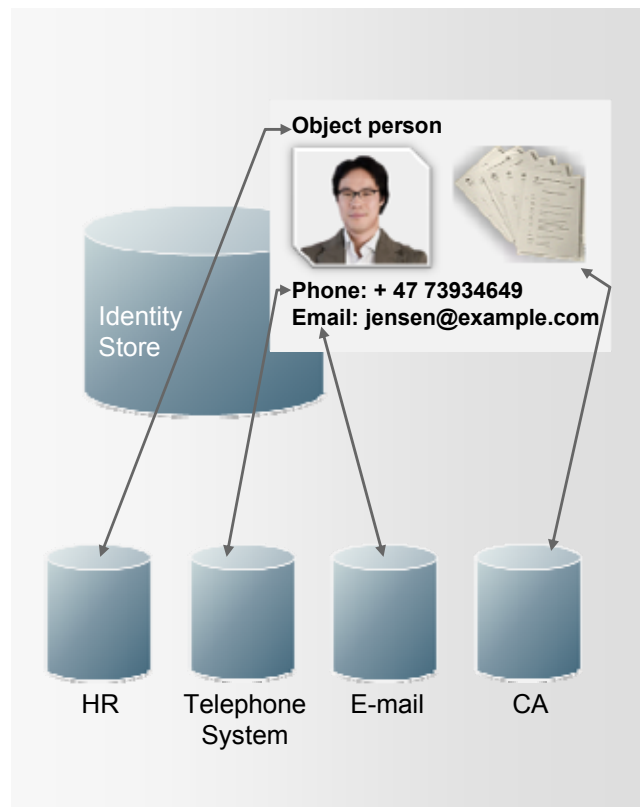


Central Hub for All Identity Center Components

- 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



© SAP AG 2009. All rights reserved. / Page 43

Central Identity Store

The Identity Store is the central hub that reads data from different source systems and later provisions the data back to the target systems.

Business roles and technical roles (privileges) are stored here. The workflow capability allows you to create a process of different request and approval steps for different persons.

The Identity Store contains a complete audit trail which reports on historical data as well.

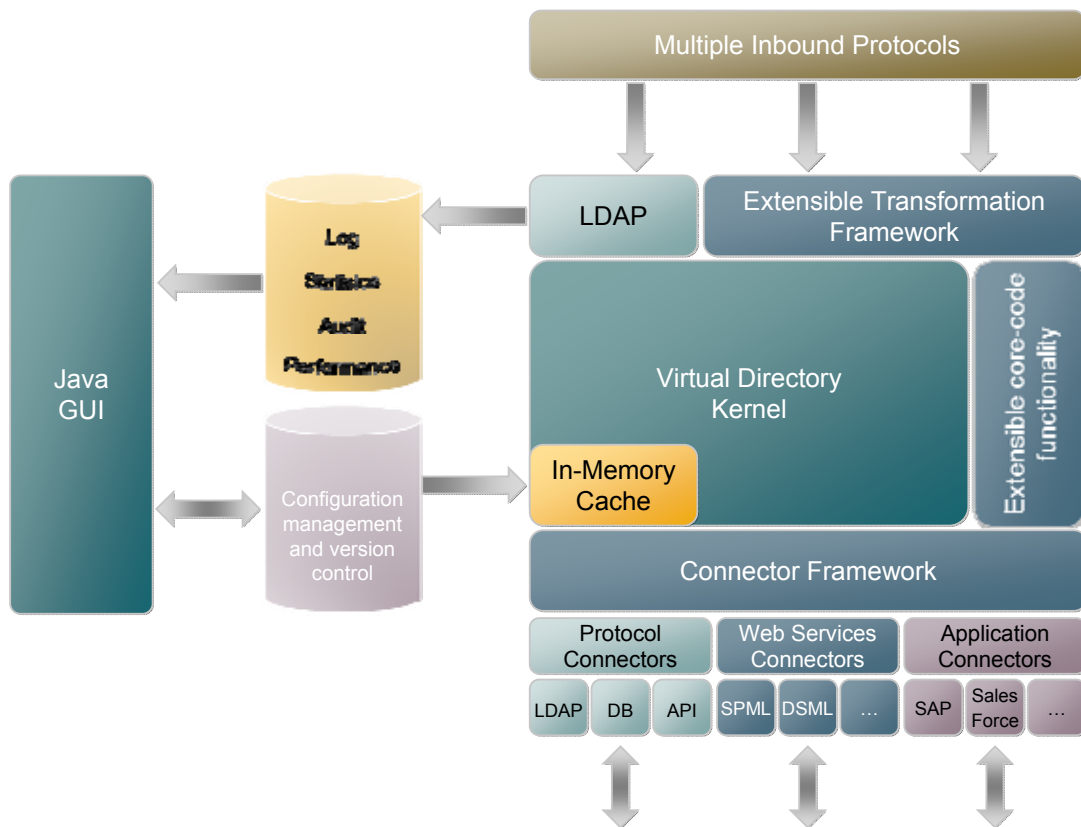
Temporary attributes can be assigned to identities to make sure that these attributes are removed after the configured time period is over. The same concept applies to the assignment of roles and privileges. For every attribute in the identity store, events can be configured to trigger workflow tasks as soon as this attribute is changed.

For attributes that only live in the target system (can be used for real-time access of data), virtual attributes can be used in the identity store.

It is also possible to roll back identity data.

The Identity Center can use multiple identity stores to manage identity data in the system environment.

Virtual Directory Server Architecture



© SAP AG 2009. All rights reserved. / Page 44

Virtual Directory Server

The Virtual Directory Server has a highly flexible architecture. It can be extended by customers to include new connectors to target systems. In the lower part of the graphic, you can see the various connectors for standard protocols. With the Connector Framework, you can easily create new connectors in Java. The cache mechanism is used to optimize performance.

Agenda



1. Introduction to Identity Management
2. SAP NetWeaver Identity Management Solution in Detail
 - 2.1 Role Management and Workflows
 - 2.2 Business-Driven Identity Management
 - 2.3 Compliance and Auditing
 - 2.4 Password Management
 - 2.5 Identity Virtualization
 - 2.6 Connectivity and Services
3. SAP NetWeaver Identity Management Architecture
- 4. Summary & Additional Information Sources**

Highlights of SAP NetWeaver IDM 7.1



■ Event-Driven SAP ERP HCM Integration

In this release, the integration with SAP ERP HCM is extended to be event-based.

■ Further Integration With SAP Business Suite

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.

■ Extended Integration With SAP's GRC Solution (SAP BusinessObjects Access Control)

The integration with SAP's GRC solution has been extended and covers current BusinessObjects Access Control releases.

■ 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

© SAP AG 2009. All rights reserved. / Page 46

Release 7.1 – New Features and Functions:

- The way tasks are executed in the SAP NetWeaver Identity Management user interface was changed to align with best practices and SAP NetWeaver.
Up to version 7.0, the user first selected a task, and then searched for the entry/entries to perform the task on.
- From version 7.1, the user sees a generic search dialog to search for an entry. Then the user can select one of the entries in the search result, and get a list of available tasks which can be performed on that entry.
- If the Virtual Directory Server configuration is deployed on SAP NetWeaver AS Java, the SAP Logging Framework is used for logging tasks.
- The Identity Store access control was enhanced by using relations between the subject (the user performing the operation) and object (the entry being changed). By using the relations, complex SQL statements for checking access can be avoided, and performance improves.

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



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 Offering
- SAP NetWeaver Identity Management

<https://www.sdn.sap.com/irj/sdn/nw-identitymanagement>





Questions?

SAP NetWeaver
Identity Management



No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP AG. The information contained herein may be changed without prior notice.

Some software products marketed by SAP AG and its distributors contain proprietary software components of other software vendors.

Microsoft, Windows, Excel, Outlook, and PowerPoint are registered trademarks of Microsoft Corporation.

IBM, DB2, DB2 Universal Database, System i, System i5, System p, System p5, System x, System z, System z10, System z9, z10, z9, iSeries, pSeries, xSeries, zSeries, eServer, z/VM, z/OS, i5/OS, S/390, OS/390, OS/400, AS/400, S/390 Parallel Enterprise Server, PowerVM, Power Architecture, POWER6+, POWER6, POWER5+, POWER5, POWER, OpenPower, PowerPC, BatchPipes, BladeCenter, System Storage, GPFS, HACMP, RETAIN, DB2 Connect, RACF, Redbooks, OS/2, Parallel Sysplex, MVS/ESA, AIX, Intelligent Miner, WebSphere, Netfinity, Tivoli and Informix are trademarks or registered trademarks of IBM Corporation.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Adobe, the Adobe logo, Acrobat, PostScript, and Reader are either trademarks or registered trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Oracle is a registered trademark of Oracle Corporation.

UNIX, X/Open, OSF/1, and Motif are registered trademarks of the Open Group.

Citrix, ICA, Program Neighborhood, MetaFrame, WinFrame, VideoFrame, and MultiWin are trademarks or registered trademarks of Citrix Systems, Inc.

HTML, XML, XHTML and W3C are trademarks or registered trademarks of W3C®, World Wide Web Consortium, Massachusetts Institute of Technology.

Java is a registered trademark of Sun Microsystems, Inc.

JavaScript is a registered trademark of Sun Microsystems, Inc., used under license for technology invented and implemented by Netscape.

SAP, R/3, SAP NetWeaver, Duet, PartnerEdge, ByDesign, SAP Business ByDesign, and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP AG in Germany and other countries.

Business Objects and the Business Objects logo, BusinessObjects, Crystal Reports, Crystal Decisions, Web Intelligence, Xcelsius, and other Business Objects products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of Business Objects S.A. in the United States and in other countries. Business Objects is an SAP company.

All other product and service names mentioned are the trademarks of their respective companies. Data contained in this document serves informational purposes only. National product specifications may vary.

These materials are subject to change without notice. These materials are provided by SAP AG and its affiliated companies ("SAP Group") for informational purposes only, without representation or warranty of any kind, and SAP Group shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP Group products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warrant.