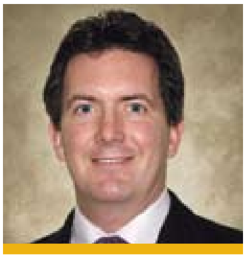
SAPinsider This article appeared in the Apr ▪ May ▪ Jun 2008 issue of *SAP Insider* and appears here with permission from the publisher, Wellesley Information Services (WIS), **www.WISpubs.com.** WIS Wellesley Information Services

Getting Started with Identity Management

A Roadmap for Automated, Regulated User Access to IT Resources



Keith Grayson (keith.grayson@sap.com) is the Business Development Manager for SAP NetWeaver Identity Management in EMEA. As such, he is the EMEA point of contact for sales and partner queries about this new SAP solution. Having joined SAP with the acquisition of MaXware, he has been involved with identity management projects for over 10 years, working with clients to help develop business plans, as well as scope and deploy identity management solutions.

Think about how your organization handles identity management, the process by which individuals gain access to IT resources (and, moreover, how those access rights are handled throughout the lifetime of individuals' association with your organization). For many, identity management processes are excessively manual, inefficient, and difficult to trace.

For many organizations, identity management processes are excessively manual, inefficient, and difficult to trace.

Consider your current process for requesting user accounts for desktop logins and other applications. Likely, it's done by paper forms that are sent through intra-company mail to personal contacts within the IT department. Staff looking for access to a new application must first find out who owns the application before they can even apply for access rights. They then have to fill out another paper application — countersigned by an authorizing manager — and submit it to multiple groups for approval.

In other words? It's a time-consuming, inefficient, and potentially insecure process. But that's not all:

- Since different groups grant and manage application access, there may be no central record of all the application access rights that a person has; so when an employee leaves or changes positions, this leads to a large number of orphan accounts that cause IT security audit failures, create unnecessary maintenance costs, and form a back door for potentially malicious or even criminal activity.
- As organizations attempt to prove IT governance for regulatory purposes, they're finding that, because of the ad hoc nature of granting access rights (it often involves a quick, undocumented phone call to the help desk, followed by impromptu installation of programs or rights), it's difficult to know just *who* has access to *what*.
- Organizations have had no choice but to dedicate key staff to compliance and process issues, thereby increasing costs and the pressures on IT teams tasked to provide a high level of service to users.

In light of these and other challenges (see sidebar), think about your organization's ideal identity management state. It would likely be marked by automated and well-regulated standards for granting user access to IT environments and applications. Application access rights would be automatically determined by reference to an employee's role within the organization, as every job role would have a standard definition of appropriate rights. You'd have an identity management platform that enabled the IT environment to rapidly reflect business and organizational change. And individual managers and administrators would have full accountability for any changes made.

The ideal, in other words, is a set of standardized and centralized processes associated with requesting user accounts across the various IT services that the office of the CIO provides. The question, then, is how do you get there?

What's Driving Increased Interest in Identity Management?

Identity management is rising on the list of IT hot topics for a host of reasons:

- Constant pressure to reduce help-desk and IT operating costs
- Growing emphasis on meeting regulatory and compliance demands for IT access
- IT users' growing service-level demands
- Increasingly distributed computer systems
- Scarce technical resources that are too often occupied with trivial IT operations, such as password resets and user account management

Closing the Gap Between the Real and the Ideal

The call to action for IT organizations that want to automate their manual identity management operations is to apply repeatable processes and tools. That's why SAP has developed and released a new solution – SAP NetWeaver Identity Management – generally available since mid-July 2007.

The SAP NetWeaver Identity Management solution serves as the authoritative source of information about anybody who has access to your IT resources. It manages and keeps permission and password information synchronized across your entire IT landscape, including SAP, partner, customer, and legacy systems (see **Figure 1**).

Embarking on a Successful Identity Management Project

Even the most robust identity management tools, though, can be rendered useless if an organization doesn't develop a well-planned and carefully executed identity management project. Companies getting started with an identity management initiative need to consider some basic steps to ensure project success.

Step #1: Prepare Your Organization for Change

Before you implement SAP NetWeaver Identity Management (or any identity management solution, for that matter), you first need to agree – on both a political and technical level – how to distinctly represent users of all IT resources across the enterprise. This upfront planning is critical to achieving project success.

On a political level, I'm referring to the many stakeholders that are vested in employee information, from HR to IT operations to application owners. And to be frank – getting them all on the same page about ownership of user identity data isn't easy. The key is to ensure that all stakeholders clearly understand the business benefits they'll enjoy from this coordinated and automated identity management with a central point of control. This means creating a personalized set of benefits for each of them. With this approach, the business case will fall into place.

On the technical side, the first goal is to associate multiple user accounts across multiple systems with a single individual. To do this, you need to assign every individual with a unique identifier. Keep in mind that because of security standards, you may need to mandate that certain users have difficult-to-guess unique identifiers.

Step #2: Cleanse Your User Data

The next step to any identity management project is data cleansing – the process of associating user accounts on different systems across the IT landscape with a single individual in the identity management system (see **Figure 2**). Only then can you begin to manage all user accounts from a central point of control.

To achieve this, SAP NetWeaver Identity Management becomes the foundation of a reliable identity data platform for the entire enterprise IT environment. It includes powerful data synchronization functionality (see **Figure 3** on the next page), which reads information from multiple data sources, associates it with an individual's record, and populates this record in an

SAP NetWeaver Identity Management is designed to alleviate the stress on IT in your organization and to help address your IT security audit issues.

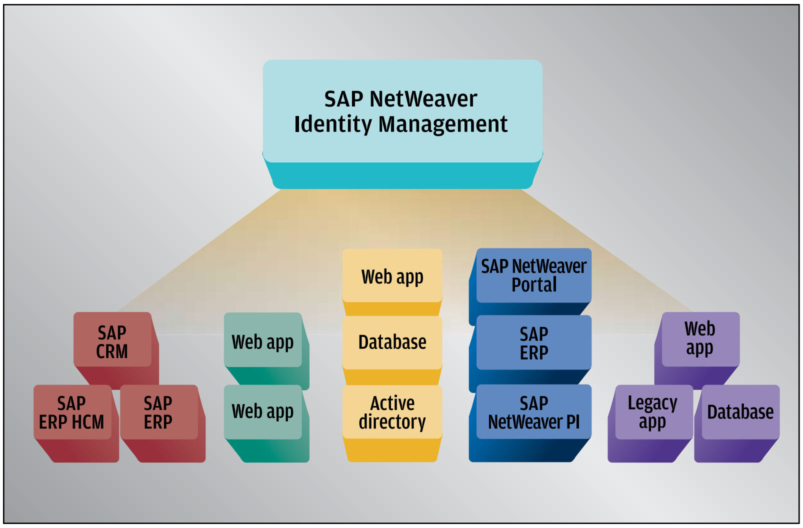


FIGURE 1 ▲ SAP NetWeaver Identity Management synchronizes user identity and access rights information across your heterogeneous system landscape

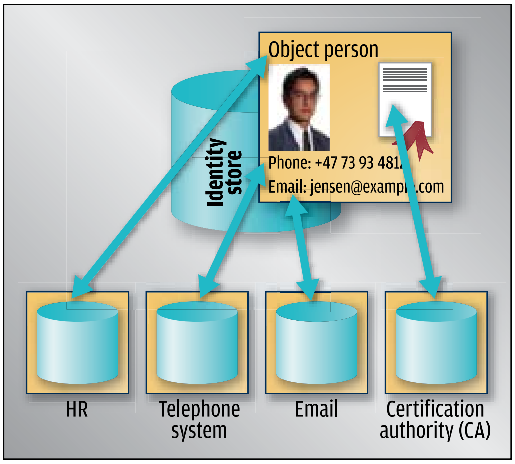


FIGURE 2 ▲ SAP NetWeaver Identity Management brings together "cleansed" identity data about an individual from multiple sources to create a central authoritative source of user data

"identity store." This identity store then forms the single source of user information, and target identity data sources can now all be synchronized with this authoritative data.

Following these two basic steps, you'll achieve the critical milestones for an identity management project:

1. The application of a unique global identifier for all users
2. A delivered identity data platform, which creates — through a data-cleansing process — a single point of authoritative identity data for the organization across a defined set of IT systems

Where in Your Landscape Is the Best Starting Point?

I'd strongly recommend using your organization's HR system as an intuitive place to start your identity management project; it is presumably the hub of employee records, as well as their maintenance and management. It's for this reason that SAP ERP Human Capital Management (SAP ERP HCM) is a key integration scenario for SAP NetWeaver Identity Management (see **Figure 4**).

In this scenario, SAP NetWeaver Identity Management can take authoritative information from the SAP ERP HCM system and then monitor the environment for any life circumstance changes — change of marital status, name, or home address, for example — or organizational status changes, including a change of role, title, base location, or employment status.

As these life and organizational changes occur, SAP NetWeaver Identity Management will automatically grant and remove individuals' IT account names and IT resource access rights, depending on the entitlements attached to their job role. In addition, any personal information change will be reflected across all of the systems where that information is stored.

Taking authoritative information from your HR system may sound like a simple concept. But don't forget a few important realities:

FIGURE 3 ▼ The technical components of SAP NetWeaver Identity Management

SAP NetWeaver Identity Management functionality	Functionality includes...	Benefits
Identity provisioning functionality	Central point of user IT access rights management; password synchronization and management; user business and technical role management; manager workflow approvals for access rights assignment and changes; central point of audit	▪ Provides an authoritative, single source of user information with data taken from various trustworthy data sources; target identity data sources can now be synchronized with this data ▪ Enables self-service management of user information and passwords, providing increased accuracy and minimizing help-desk calls ▪ Provides a central point of control for auditing and reporting on users' access rights across the IT landscape
Data synchronization functionality	Extensible connectivity to a broad range of IT environments: operating systems, databases, directories, enterprise applications, Web services, and flat files; powerful data transformation and meta-directory facilities including data joins and selection through SQL queries; multiple pass synchronization between authoritative and target data sources	▪ Reads information from multiple data sources and associates it with a single individual's record; this information then populates the individual's record in an identity store ▪ Maintains consistent data about individuals across all the systems that they have access to
Identity virtualization functionality	Standards-based connectivity to multiple system types, including directories, databases, SAP environments, third-party applications; a key part of a directory services architecture	▪ Provides a single access point to all information in real-time and can also be used to control access to identity data ▪ Provides a technical solution for issues of user data ownership and management

- Real life is rarely that simple, so the system that manages employees' personal and organizational changes needs to hide a considerable amount of complexity from the end users, line managers, application owners, and administrators that use the system on a day-to-day basis
- Any design must factor in users not covered in this approach, such as contractors and project workers; these are important additional considerations to equate throughout the course of your project

Beyond the Basics: Advanced Identity Management Capabilities

Once you have a basic framework for establishing a consistent identity data platform, think ahead to the more advanced areas you'll be able to tackle. For example, you can:

- Define approval workflows for additional user access rights requests
- Define a process for self-service password resets
- Automate the process of assigning user privileges based on job role information
- Create high-level, business-focused roles – such as EMEA sales management, accounts payable, or pensions administrator – and map them to specific application accounts and privileges
- Generate reports to meet demanding IT security auditors' requirements
- Create an enterprise-wide identity platform in support of a broader service-oriented architecture (SOA) approach

The possibilities and potential efficiency improvements within your IT organization are endless.

Summary

Only by tackling an identity management project can an organization overcome the clumsy, inefficient, and manual processes by which user access rights and information are likely managed in your company today. Armed with a straightforward, well-planned project approach, you can ease IT's taxing user access management workload and make key strides in decreasing the costs of maintaining compliance.

To ensure your project's success, it's important to first get the basics right: Make sure key stakeholders are on board, start with clean and synchronized data, and consider taking authoritative information from your HR system first. SAP NetWeaver Identity Management provides an excellent set of tools to manage this entire process.

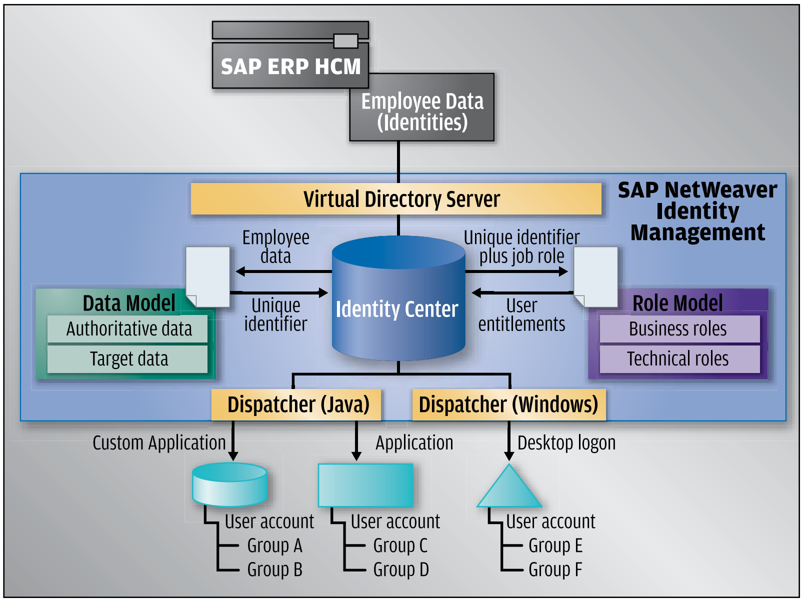


FIGURE 4 ▲ Managing and protecting access to employee records: A look at SAP NetWeaver Identity Management's architecture and how SAP ERP HCM is a logical integration point

For more information, please visit **https://www.sdn.sap.com/irj/sdn/security.**

The call to action for IT organizations that want to automate their manual identity management operations is to apply repeatable processes and tools.

Additional Resources...

...from SAPinsider

- *SAP Security and Authorizations – Risk Management and Compliance with Legal Regulations in the SAP Environment* by Mario Linkies and Frank Off (SAP PRESS, **www.sap-press.com**)
- "Special Report: SAP Extends Functionality for Identity Management – A Harmonized Approach to Managing a Heterogeneous Landscape" (*SAP NetWeaver Magazine*, Spring 2008, **www.NetWeaverMagazine.com**)
- "The Three C's of SAP Identity Management – Centralization, Certified Partners, and Compliance," a Security Strategies column by Frank Buchholz, Jens Koster, and Gerlinde Zibulski (*SAP Insider*, October-December 2006, **www.SAPinsideronline.com**)