TECHNICAL COLUMN | **Take Note!**

SAPinsider

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

WIS

SAP NetWeaver Identity Management: How Can You Leverage Its Benefits Now?

Dr. Franz-Josef Fritz (franz-josef.fritz@sap.com) has a Ph.D. in mathematics and 30 years of experience in all areas of IT. Workflow and business process management have been particular areas of interest for much of his life. He has worked at SAP since 1993 as Program Director and Vice President with responsibility for the Business Process Technology and Internet-Business Framework departments. Since 2003, he has been responsible for several areas within SAP NetWeaver Product Management.

Torgeir Pedersen (torgeir.pedersen@sap.com) is Product Manager for SAP NetWeaver Identity Management. Previously Torgeir was a senior architect at MaXware, which was acquired by SAP. He has more than 10 years of experience designing identity management products and working directly with customers. Before joining MaXware, Torgeir worked for the Norwegian Army as an IT manager running IT and telco networks. He earned an engineering degree from the Norwegian Army School of Technology.

In the article "Getting Started with Identity Management" — which appeared in the Security Strategies column of the April-June 2008 issue of SAP Insider — Keith Grayson introduced SAP NetWeaver Identity Management, its benefits, and some key ways to start preparing your organization for an identity management project.

In this article, we will go one step further and introduce some practical examples of how you can leverage SAP NetWeaver Identity Management in an SAP environment. This column also covers integration with your wider infrastructure and application landscape, including interoperability with LDAP-based directory servers and other third-party identity management components.

SAP customers have traditionally been able to control user access to back-end SAP systems with tools that protected specific solutions within — but no further than — the boundaries of the SAP system landscape.

As IT landscapes expand, however, companies' identity management needs are becoming more complex and must cover more ground. Applications increasingly rely on services that bring additional functionality from external sources, including partners and other third-party systems. This resulting flexibility also creates a challenge for security, governance, and compliance concerns: How do you ensure that the right users are accessing the right solutions?

If you're an SAP customer, this particular confluence of business forces — the need for greater security, accountability, and risk management at a time when architectures are becoming increasingly open — is the reason to look at SAP NetWeaver Identity Management now (see **Figure 1**).

The SAP NetWeaver Identity Management solution manages assignments of privileges and complex authorizations across both SAP Business Suite and heterogeneous environments. It allows companies to link business processes to the right people with the right level of access to help ensure accountability and risk management. This is key to keeping your system secure and compliant while still remaining flexible enough to accommodate an ever-changing set of employees, business needs, and technology. Before we look at the implications for broader identity management in your company's solution landscape, let's first look at how SAP NetWeaver Identity Management affects your SAP system.

Broaden Identity Management Within the SAP Landscape

SAP NetWeaver Identity Management is tightly integrated with SAP Business Suite and is able to

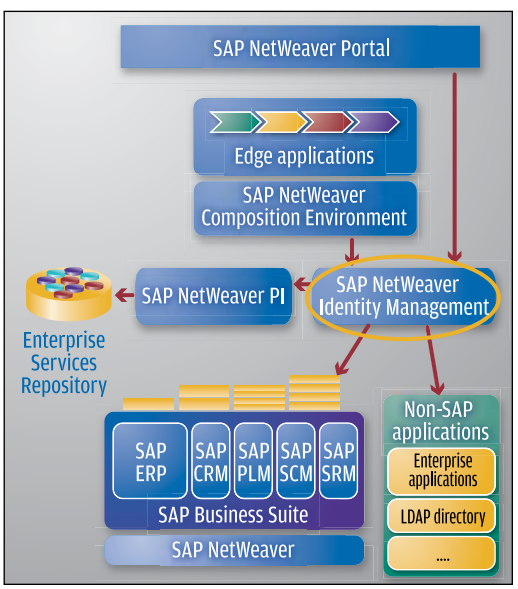


FIGURE 1 ▲ SAP NetWeaver Identity Management in the heterogeneous landscape

✔ **NOTE!**
The most recent version of SAP NetWeaver Identity Management was released in May 2008.

manage all applications and support all use cases that involve employee identities: onboarding, change of role, assignment of responsibilities for additional applications, termination of employment, and more.

SAP NetWeaver Identity Management is also integrated with SAP NetWeaver Portal and SAP NetWeaver Composition Environment via the Java-based User Management Engine. This means that information regarding identities in SAP NetWeaver Portal, SAP NetWeaver Composition Environment, and all back-end systems can be kept up to date without manual work. This supports smooth execution of processes while greatly reducing administration cost and effort.

For those SAP customers who have been using Central User Administration (CUA) to manage users and roles in the large landscape of ABAP systems, it's now time to evaluate what a broader approach can offer you. While CUA does significantly reduce the complexity of managing such landscapes compared to separate user administration in each system, it also has several limitations:

- CUA only supports ABAP systems. This means that neither Java-based nor third-party applications can be managed consistently.
- Role management is limited to assigning users to roles and creating composite roles within one ABAP system. CUA has no support for managing business roles across multiple ABAP systems or Java-based and third-party applications.
- CUA has no support for some user-friendly features such as self-service requests (that allow a user to reset a password, for example), requests for new authorizations, or support for delegation and approvals.

For these reasons, SAP is recommending that customers migrate from CUA to SAP NetWeaver Identity Management – a relatively painless process due to the support for CUA within SAP NetWeaver Identity Management. See the sidebar to the left for an overview of the three basic steps for migrating to SAP NetWeaver Identity Management.

Moving from CUA, you gain flexible mechanisms for self service, delegated administration, and approval workflows. And because of SAP NetWeaver Identity Management's ability to manage access rights across various systems, SAP customers will find they can better handle user access scenarios: Your company can now manage user access for business roles that cross ABAP, Java, and heterogeneous environments.

SAP NetWeaver Identity Management also supports heterogeneous environments like LDAP directories and databases. This dramatic change from CUA enables SAP customers to take a holistic approach to identity management and ensure that access rights are consistently managed across their SOA landscape and into back-end applications (see **Figure 2**).

Extend Identity Management Beyond Your SAP System Landscape

Consider, for example, a business-to-business (B2B) purchasing system that uses an SAP Customer Relationship Management (SAP CRM) order entry

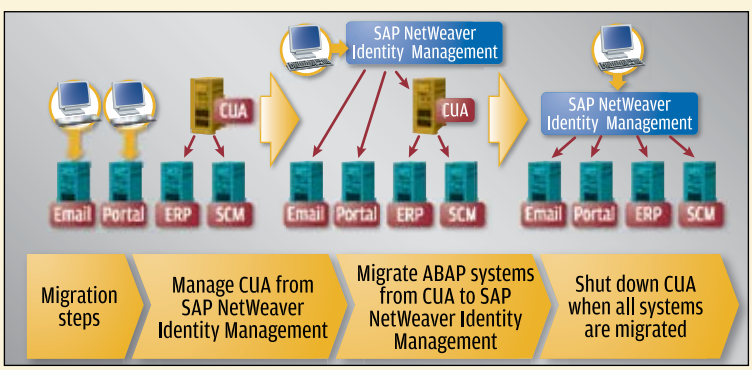
More Technical Details on SAP NetWeaver Identity Management

For more details about how SAP NetWeaver Identity Management integrates with SAP Business Suite, see the configuration guide at **www.sdn.sap.com/irj/sdn/go/portal/prtroot/docs/library/uuid/706065c4-3564-2a10-2382-a52fcbd7eefb**.

Step-by-Step Migration from ABAP-Only User Administration

Because SAP NetWeaver Identity Management is designed to work with CUA, moving to the new solution is relatively straightforward. For the migration from CUA to SAP NetWeaver Identity Management, we recommend the following approach (see figure below):

1. Install SAP NetWeaver Identity Management on top of CUA. This way you can introduce the benefits of SAP NetWeaver Identity Management without disrupting your well-functioning landscape.
2. Start connecting the ABAP systems to SAP NetWeaver Identity Management and disconnecting them from CUA.
3. When you have disconnected the last ABAP system from CUA, you can then shut down CUA to complete a successful migration.



▲ CUA and SAP NetWeaver Identity Management: A nondisruptive migration to a broader solution

service and a homegrown pricing system. Both are accessible for portal authentication and authorization through SAP NetWeaver Identity Management. Within a broader environment, SAP NetWeaver Identity Management has two important integration points for a heterogeneous environment:

- **Identity Services** is the standards-based single access point for every system that queries and manages identity information across your landscape. Internal applications use this access point for integration with SAP NetWeaver Identity Management, but a third-party application, such as another identity management solution, could also use this interface.
- A certifiable **connector framework** from SAP supports integration with third-party applications. Connectors built using this framework could be reused across the identity management solution for role management, self service, and delegated administration in the identity management solution or using Identity Services (see sidebar below).

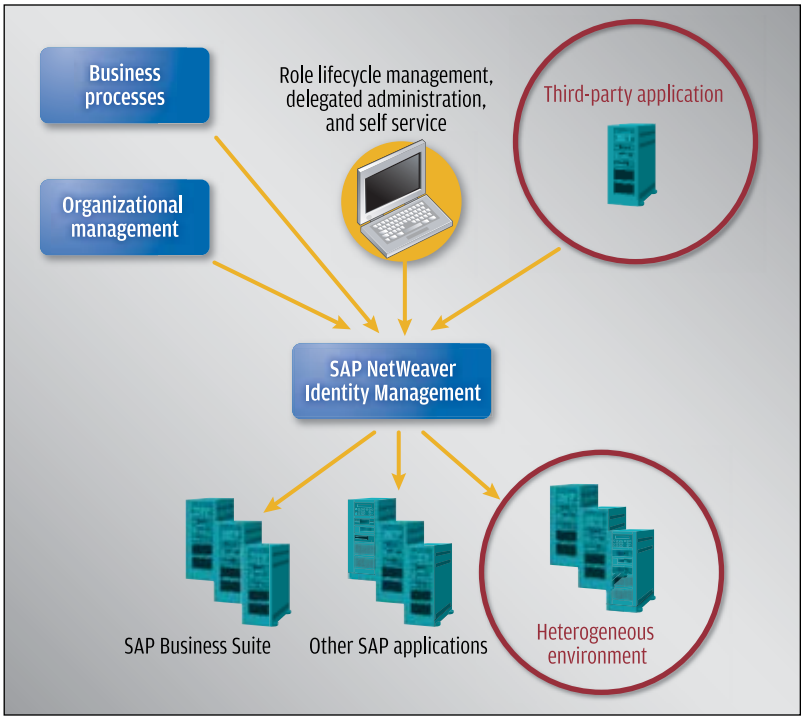


FIGURE 2 ▲ SAP NetWeaver Identity Management integrates with the broader IT environment

Overview: The Latest SAP NetWeaver Identity Management Features

One of the most prominent new offerings of SAP NetWeaver Identity Management is **Identity Services**, which provides Web services (via the SPML open standard) with access to identity information.

This separates other identity services clients from the identity information itself, enabling a consistent, reusable way to support access and management, and reducing the complexity of integration for the system. Other new features include:

1. Identity Center extensions, available with the latest version of SAP NetWeaver Identity Management Identity Center release 7.0, support package 2 include:

- **Time-limited attributes.** Administrators can set time constraints for attributes such as role assignments. This means they can set a future start date or assign an end date for a role assignment.
- **Automatic approvals with role assignments.** A role can be set for automatic approval each time a new user is assigned to that role.
- **Full-text search support for Microsoft SQL Server 2005 as your database system.** This enables Google-like search capabilities, supporting better-matched search results and making it easier for administrators to locate roles or to identify privileges in self-service requests.

2. Provisioning framework for SAP systems, which supports:

- **Central User Administration (CUA).** This makes replacing CUA with SAP NetWeaver Identity Management a relatively simple process (see previous sidebar on migration).
- **Dual-stack SAP system.** This enables support for dual-stack components – such as SAP NetWeaver Process Integration – which support both Java and ABAP.
- **Time-dependent assignments for ABAP roles.** Time dependencies on ABAP role assignments are now kept in tact when the role assignment is read into the Identity Center. The role or privilege assignments are then provisioned to the appropriate target systems. This means that you'll no longer see a time-dependent role assignment in the ABAP system.

3. A **password hook**, which synchronizes user passwords in the Microsoft domain with other applications. The hook distributes any passwords to other applications using the Identity Center, keeping all applications in sync.

4. Integration with SAP GRC Access Control; SAP NetWeaver Identity Management can execute compliant provisioning to multiple target systems that are managed by SAP GRC Access Control. SAP NetWeaver Identity Management's integration with SAP GRC Access Control also extends the solution's reach in regards to compliant identity management processes.

It is with the connector framework that SAP NetWeaver Identity Management supports generic data sources, such as JDBC databases and LDAP directories, and applications like Microsoft Active Directory, Microsoft Exchange, or Lotus Notes.

Business Pain Points – and How Identity Management Can Help

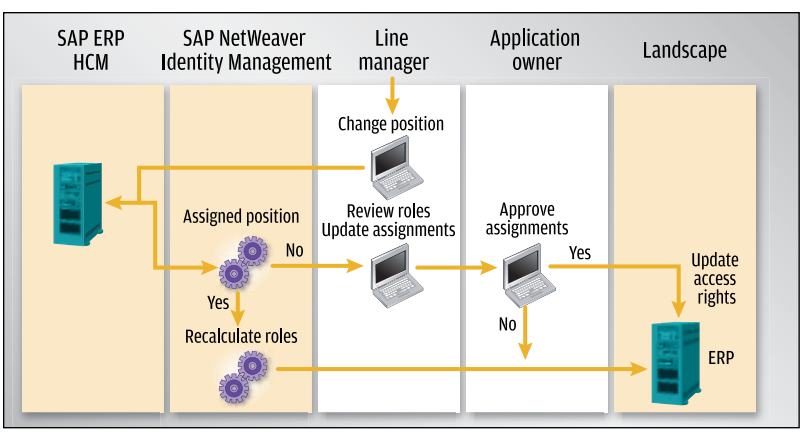
The basic function of SAP NetWeaver Identity Management is to ensure that the right users get access to the right solutions and data – but there are other business processes it can support as well.

Streamline User Access from Hire Date and Beyond

IT teams often struggle with access administration in hire/fire scenarios. Many are relying on inefficient manual processes that lead to:

- Delays in employee assignments
- A backlog of user authorizations and deprovisioning for inactive employees
- The inability to track who has access to what throughout the entire organization

FIGURE 3 ▼ SAP NetWeaver Identity Management works with your HR processes to handle authorizations whenever an employee is assigned a new position in the company



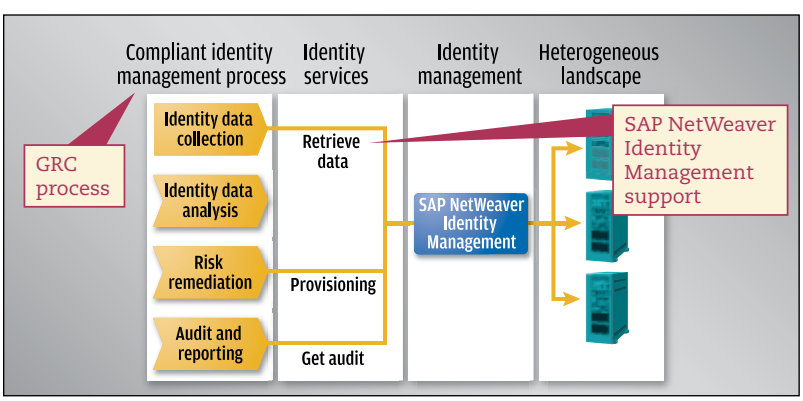


FIGURE 4 ▲ Achieving compliant identity management

And the challenges are not limited to the beginning or end of employment. Tracking changes in positions and responsibilities and keeping the corresponding roles and authorizations in sync is even more important since such changes occur multiple times over the course of a user's employment (see **Figure 3**).

SAP NetWeaver Identity Management allows administrators to tie identity management with HR processes, enabling companies to automate the core of the authorization process. Linking IT resource allocation to the human capital management (HCM) business process helps to reduce TCO.

Positions-based role management sets authorizations based on roles that are tied in to the user's position in the company. This reduces risk by enforcing strict access controls and improves operational efficiency by reusing business processes.

Support Governance Efforts with Compliant User Provisioning

User access to corporate resources has a profound impact on both security and corporate governance, as well as on how you mitigate risk and stay compliant. When it comes to risk management and compliance, SAP NetWeaver Identity Management can also help expedite regulatory audits, make user access more transparent, and ensure that your access rights remain compliant.

To enable organizations to successfully manage identity *and* compliance, SAP has designed SAP GRC Access Control to fully integrate with SAP NetWeaver Identity Management (see **Figure 4**).

Identity management processes that are started in SAP NetWeaver Identity Management will be sent to SAP GRC Access Control when compliance checks are needed – for adding mitigation controls, for example. Likewise, a workflow can begin in SAP GRC Access Control (in versions 5.3 onward) and continue in SAP NetWeaver Identity Management as soon as compliance checks have been completed. With this built-in integration, SAP:

- **Extends** the reach of SAP GRC Access Control into non-SAP and heterogeneous environments. With SAP GRC Access Control 5.3 and SAP NetWeaver Identity Management 7.0, support package 2, SAP GRC Access Control is capable of sending provisioning requests to SAP NetWeaver Identity Management using the identity service it exposes.

- **Enables** SAP NetWeaver Identity Management to ensure that user access to SAP ERP is compliant using Web services that SAP GRC Access Control exposes.

Outlook: Features Planned for SAP NetWeaver Identity Management 7.1

SAP plans to make release 7.1 of SAP NetWeaver Identity Management available by the end of 2008. This release will have features such as:

- **Event-driven SAP ERP Human Capital Management (SAP ERP HCM) integration.** In this release, the integration of SAP ERP HCM extends to include time-dependent values and enables customers to react more quickly to changes in employee status.
- **Extended GRC integration.** This is accompanied by an improved audit mechanism, simpler deployment, and password management capabilities.
- **Further integration with SAP Business Suite.** This includes a framework that enables product-specific extensions to be executed when identity provisioning operations are done. This allows a deeper integration with the applications in SAP Business Suite — for operations like linking users to business partners, for example. SAP NetWeaver Identity Management 7.1 supports all use cases involving employees, including managing employee data in SAP ERP HCM, creating an accounting clerk role in SAP ERP Financials, and enabling a user to access the Financial Customer Care and Collection Management solution.
- **Extended identity services.** These services support the connector framework, enabling partners to develop third-party connectors; they also improve deployment on SAP NetWeaver, including enhanced logging capabilities.
- **Web Dynpro-based UIs.** The UI that end users work in for self services, delegated administration, and approval tasks is ported to Web Dynpro. This gives SAP customers a user interface that could both run as a standalone application and be integrated with their portal.

Conclusion

SAP NetWeaver Identity Management can help you reduce the overall cost of identity administration and integrate identity information from SAP and non-SAP stores. There are various ways to get started with SAP NetWeaver Identity Management, and you can leverage its benefits in steps. For instance, you could look to SAP NetWeaver Identity Management to bolster your key business processes in areas such as compliance and human resources. Or you could start to replace the limited CUA capabilites with SAP NetWeaver Identity Management. Or you could connect to other existing — typically LDAP-based — identity stores.

SAP also plans to expand the breadth and depth of SAP NetWeaver Identity Management's integration with SAP Business Suite. With planned expansions for the connector framework, customers can also look for opportunities to extend the reach of their SAP NetWeaver Identity Management capabilities to encompass third-party solutions.

For more information, see "Identity Management for SAP System Landscapes: Architectural Overview" and the Compatibility Matrix at **www.sdn.sap.com**. ■

Want to Test the GRC and Identity Management Integration?

A demo environment showcasing the integrated solution for the GRC scenarios noted in this article is available. See **www.sdn.sap.com/irj/sdn/go/portal/prtroot/docs/library/uuid/e08e21ba-dffa-2a10-5da7-c9c1d46d80bd** or visit **www.sdn.sap.com/irj/sdn/go/portal/prtroot/docs/library/uuid/e08e21ba-dffa-2a10-5da7-c9c1d46d80bd**).

SAP NetWeaver Identity Management can help you reduce the overall cost of identity administration and integrate identity information from SAP and non-SAP stores.

Additional Resources... ...from SAP insider

- "Getting Started with Identity Management," a Security Strategies column by Keith Grayson (*SAP Insider*, April-June 2008, **www.SAPinsideronline.com**)
- The **GRC 2009** conference in Las Vegas, March 17-20, 2009, for tips and tricks on how to identify and reduce risk across your enterprise (**www.sapgrc2009.com**)
- The Governance, Risk, and Compliance special feature on page 31 of this October-December issue of *SAP Insider* for more information on SAP solutions for GRC, including SAP GRC Access Control (**www.SAPinsideronline.com**)