



**SAP White Paper
SAP NetWeaver**

STREAMLINING THE TRANSITION TO SERVICES-BASED IT SECURITY

**Via SAP NetWeaver®, Companies Can Move Safely and Gradually
Toward a More Flexible Systems Architecture**

© Copyright 2006 SAP AG. All rights reserved.

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

IBM, DB2, DB2 Universal Database, OS/2, Parallel Sysplex, MVS/ESA, AIX, S/390, AS/400, OS/390, OS/400, iSeries, pSeries, xSeries, zSeries, z/OS, AFP, Intelligent Miner, WebSphere, Netfinity, Tivoli, and Informix are trademarks or registered trademarks of IBM Corporation.

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.

MaxDB is a trademark of MySQL AB, Sweden.

SAP, R/3, mySAP, mySAP.com, xApps, xApp, SAP NetWeaver, 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 in several other countries all over the world. 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 warranty.

CONTENTS

- Overview 5
 - Project Goal 5
 - Challenges 5
 - Resolution 5
 - Benefits 5

- Project Goal: Develop a Security Road Map 6

- Challenges for IT: Optimize Security Without Impeding Productivity 7

- Resolution: Optimize Security Step-by-Step 8
 - Step One: Consolidate User Management 9
 - Step Two: Unify and Integrate User Authentication 10
 - Step Three: Implement Message Security 10
 - Step Four: Add Controls for Modular Business Processes 10

- Benefits: Protects Information Assets, Optimizes IT Efficiency 11
 - Moving Toward an Enterprise Services Architecture 11

This paper describes how the SAP NetWeaver® platform and its components help IT organizations align with their enterprise business requirements in the area of security. It demonstrates how the platform enables companies to leverage their existing assets to maintain an appropriate level of security in the face of the growing challenges posed by more open and flexible

systems. This level of security can be achieved via an incremental rollout strategy based on user- and process-oriented security components and capabilities. The result: a secure, service-oriented architecture that lets the enterprise adapt to continuous change while at the same time containing costs.

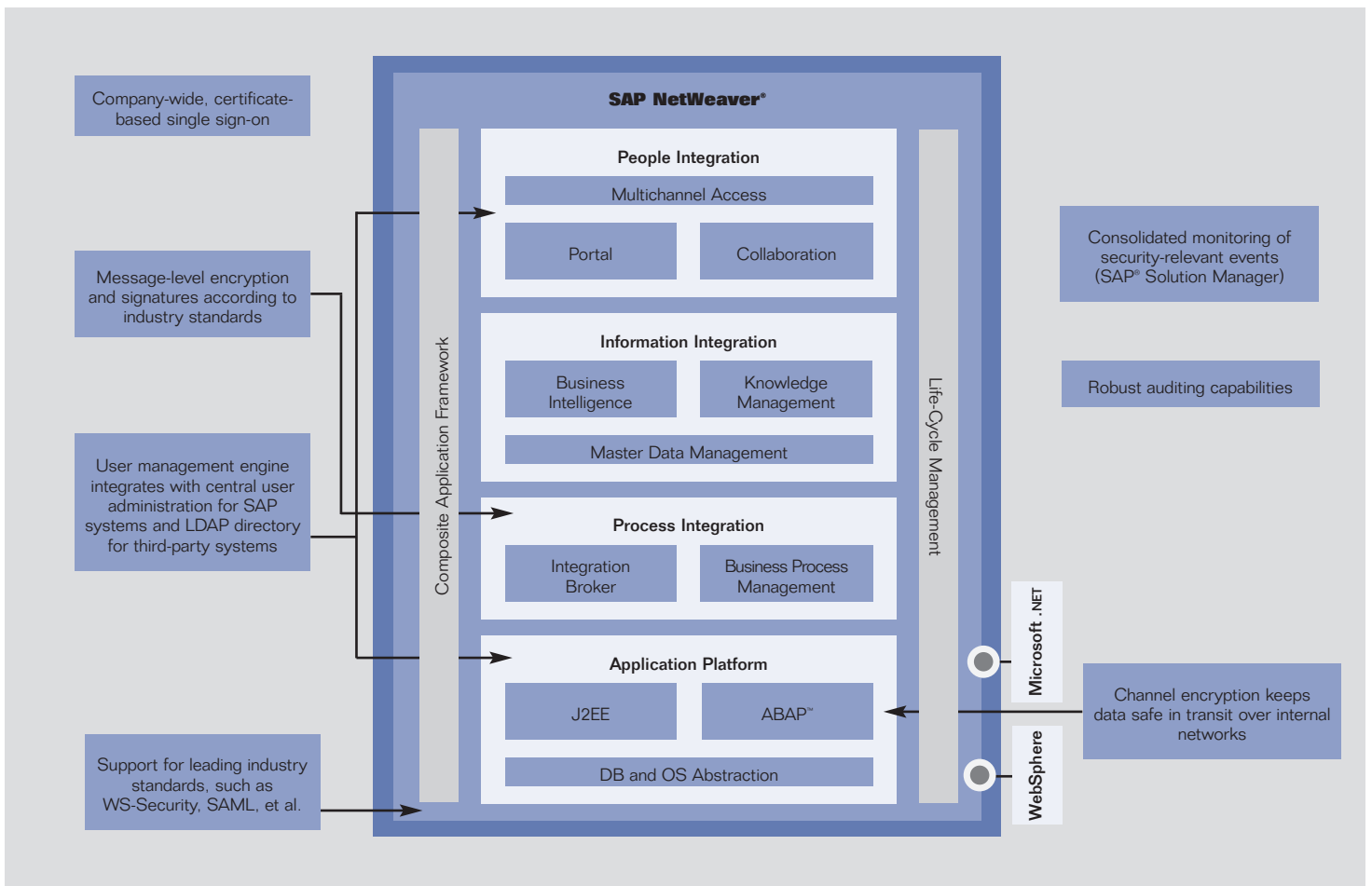


Figure 1: Security with SAP NetWeaver

OVERVIEW

Project Goal

Develop a road map for preparing enterprise IT security for a services-based future

Challenges

Optimize user and process security without impeding productivity

Resolution

Enable success through a four-step implementation method supported by SAP NetWeaver technology. The implementation includes:

- Consolidating user management
- Unifying and integrating user authentication
- Implementing message security
- Adding controls for modular business processes

Benefits

Protect a company's information assets while optimizing the efficiency of its IT infrastructure

PROJECT GOAL: DEVELOP A SECURITY ROAD MAP

Today more than ever before, corporate executives are aware of the critical need to provide effective security for their IT assets and intellectual property. For the IT managers charged with protecting these assets, security issues present a familiar challenge: How do you optimize security without seriously impeding user productivity? This challenge is complicated on one hand by IT systems that are more complex, more varied, and more far-flung than ever before and on the other hand by an increasing potential for security breaches resulting from the move toward service-based architecture.

The high demand for IT security has produced a high level of development energy from companies such as SAP. At SAP, whose customers include the world's largest corporations, security has always been an important element of all product development, planning, and quality-assurance life cycles. To learn more about SAP's general approach to IT security and mature and emerging security standards, visit www.sap.com/solutions/netweaver/brochures.

This paper shows how components of the SAP NetWeaver open-technology platform can help IT organizations put in place an incremental approach to security that prepares the enterprise infrastructure for a services-oriented future, where users and business processes grow in numbers and in diversity. This approach optimizes protection with minimal impact on productivity – even for the demanding collaborative and modular business processes companies will face in the future.

CHALLENGES FOR IT: OPTIMIZE SECURITY WITHOUT IMPEDING PRODUCTIVITY

Companies today know all too well that one of their most important responsibilities is to protect their intellectual property and information assets. Failure to do so can cause financial loss and serious damage to corporate image and competitive standing.

Yet at the same time, companies strive for agility. They want to be flexible enough to take advantage of sudden market opportunities or rapid changes in customer demand. They want to evolve to a world of Web services and automated business processes.

These needs – for safety and agility – are not mutually exclusive, but they come close. Typically, the IT department is expected to perform the necessary behind-the-scenes balancing necessary to deliver both benefits to the enterprise simultaneously. This balancing act presents a variety of real-world challenges. For instance, users don't want to have to remember five different passwords, and if asked to do so are likely to paste the passwords to their monitors. Users also want to be able to collaborate with their peers and business partners without involving their entire division or work group.

RESOLUTION: OPTIMIZE SECURITY STEP-BY-STEP

Most companies today have general security controls either in place or underway – for software development, for instance, and for basic hardware/software infrastructure.

But user security – and, by extension, process security – is a fast-moving target. Not only are company resources (people as well as processes) expanding exponentially in number and type, company employees are increasingly mobile and their application needs increasingly diverse. Rather than saddle busy users and administrators with outdated authentication and authorization procedures, the IT organization needs to develop a simpler, evolved approach to gaining control over the company’s increasingly diverse resources, a method that doesn’t get in the way of productivity and doesn’t require total system changeover.

SAP recommends an incremental approach to building this kind of security architecture. The four-step method outlined here (see Figure 2) represents just one of many different approaches companies can take for implementing SAP NetWeaver solutions. It includes the following steps:

- 1. Consolidate user management.** By consolidating and streamlining its processes, companies will be in a better position to keep track of user management and minimize mistakes.
- 2. Unify and integrate user authentication.** This step is achieved by implementing a company-wide single-sign-on process. (Note: Either Step One or Step Two can be used as “starting points” for the implementation process.)

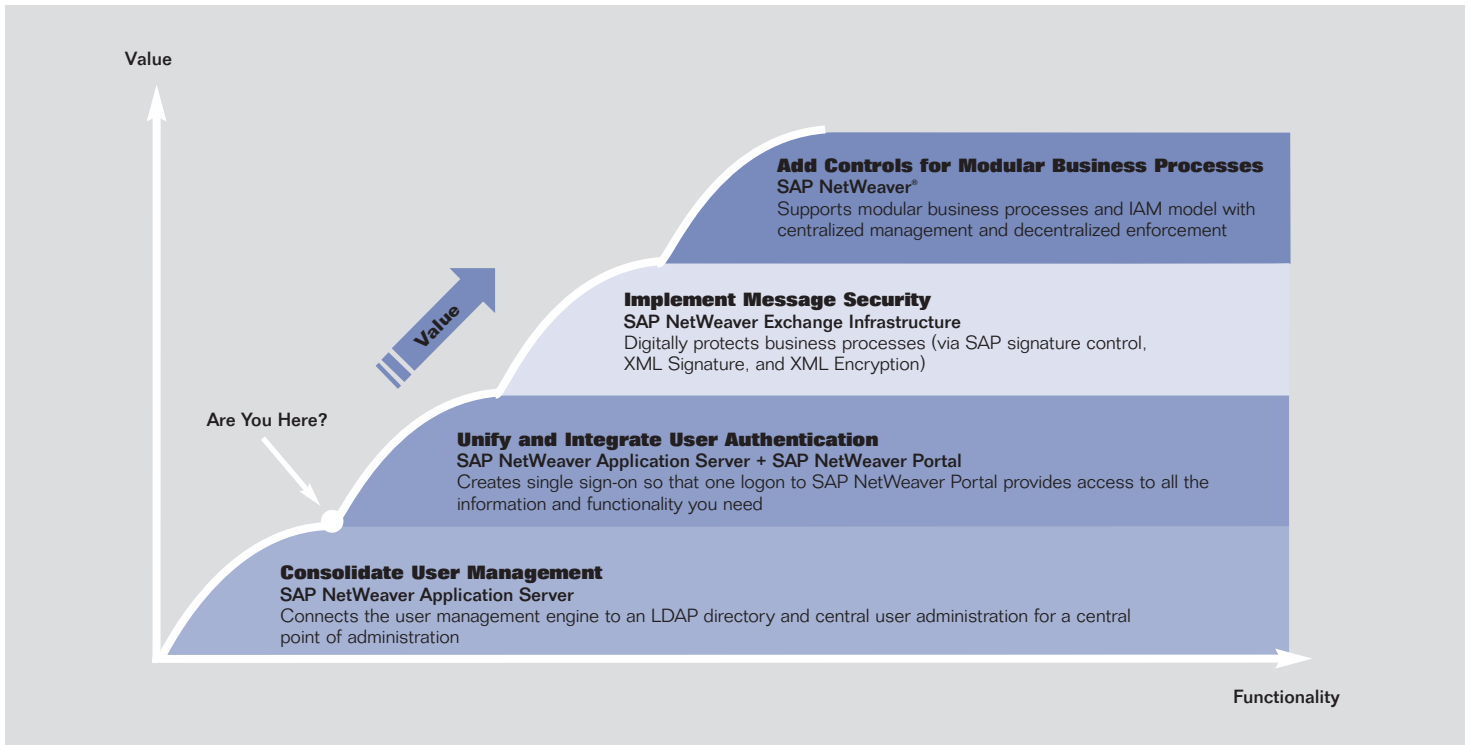


Figure 2: Road Map to Enterprise Security

3. **Implement message security.** Message-level protection is key to business-process security because it allows IT teams to leverage potentially insecure channels, such as the Internet, without unnecessary exposure to risk.
4. **Add controls for modular business processes.** Although these controls are still being developed by SAP and other companies, they will, in the future, form the basis of a full-scale identity and access management model.

The SAP NetWeaver open-technology platform plays a vital role in providing or distributing the security mechanisms required to implement this plan (see Figure 2) via a comprehensive set of components and tools, including:

- SAP NetWeaver Application Server (SAP NetWeaver AS) component
- SAP NetWeaver Portal component
- SAP NetWeaver Exchange Infrastructure (SAP NetWeaver XI) component

Step One: Consolidate User Management

At the most fundamental level, the IT team needs to create a centralized user administration facility to consolidate the user management technology already in place. Through its central user-administration and user-management-engine functionality, SAP NetWeaver AS can provide a single point of user administration for SAP landscapes, which can be synchronized with an external directory server via the industry-standard Lightweight Directory Access Protocol (LDAP).

Step Two: Unify and Integrate User Authentication

Once user management is centralized, the IT team can take the next step – implementing single-sign-on functionality. In pure SAP landscapes, this is made possible via a logon ticket solution. In certain environments, SAP NetWeaver AS can issue a logon ticket after the user has signed on via Microsoft Windows NT LAN Manager or another external mechanism. The ticket lets the user access all other authorized SAP systems.

For a more comfortable user experience, the IT team can employ SAP NetWeaver Portal as the company's single-sign-on portal. SAP NetWeaver Portal is used by many companies worldwide as the point of access to all SAP and non-SAP applications. It gives users a single-sign-on mechanism for working with multiple applications.

Step Three: Implement Message Security

This step focuses on protecting high-level activities such as user collaboration and business processes. To achieve this protection, the IT team employs SAP NetWeaver XI to comply with emerging XML Signature and XML Encryption standards. SAP NetWeaver XI enables business processes to exchange information across a diverse landscape with full security. In situations where users need to sign individual messages electronically on the front end, the IT team relies on SAP NetWeaver signature control, available to all applications via SAP NetWeaver AS.

Step Four: Add Controls for Modular Business Processes

Once the first three steps are in place, the IT team will be prepared to move to the next level, where support for modular business processes plus identity and access management (IAM) combine to take advantage of centralized management with decentralized enforcement. To achieve this level of security, SAP NetWeaver will further develop its use of standards such as the Security Assertion Markup Language (SAML) and Web Services Security (WS-Security) to attach formatted authentication information to each piece of data that moves across the company's services infrastructure.

SAP NetWeaver supports many mature and emerging security standards. Although many of these standards are not yet ready for deployment, IT organizations who take the steps described here will be ready to move when more elements of Step Four become available.

BENEFITS: PROTECTS INFORMATION ASSETS, OPTIMIZES IT EFFICIENCY

An incremental, holistic approach to effective user- and process-based security, such as the one just described, benefits companies in a number of ways. For example:

- It bolsters security, yet places controls in ways that are least obtrusive to users and business processes. This is a valuable benefit for companies trying to accommodate the needs of users; it helps them remain as mobile and as productive as ever throughout a change process.
- It enables the enterprise itself to become more agile and potentially more responsive to changing business conditions. By applying advanced security techniques to users and business processes, the enterprise can work more closely with its suppliers, customers, and other partners while maintaining appropriate security.
- By combining these measures with other SAP security techniques and technologies – and with those of SAP’s certified security partners – it enables companies to protect their information assets even in today’s dynamic business environment.

Moving Toward an Enterprise Services Architecture

Ultimately, a step-by-step approach to enterprise security serves another purpose: It prepares companies to take advantage of a service-oriented architecture that SAP calls enterprise services architecture. This architecture is a blueprint for structuring Web services in such a way that they create a flexible foundation for transforming existing applications into services-based business processes.

Enterprise services architecture defines two layers of Web services – application services and enterprise services – and assigns each a clearly defined role within the IT infrastructure. It shows IT organizations how to package existing applications for reuse as application services. Once packaged, these applications can be combined into enterprise services that can be quickly reconfigured to meet changing business conditions.

In the blueprint laid out by enterprise services architecture, application services provide the detail while enterprise services put everything together. The result: an architecture that enables the composition of flexible business processes that span multiple systems and organizations.

www.sap.com/contactsap