

**Integration von SAP Netweaver mit
Identity und Access Management**



Integration von SAP Netweaver mit Identity und Access Management

Unternehmenslösungen für sicheres und skalierbares Identity und Access Management, basierend auf einer standardisierten Integrationsplattform

White Paper

**Dr. Elmar Paul Selbach, Lovekesh Chandra
HCL Technologies GmbH**

Zusammenfassung

Identity Management ist ein wesentlicher Teil der Aufgaben eines firmenweiten System-Managements, mit erheblichen Auswirkungen auf die Sicherheit und Risikostrategie eines Unternehmens. Damit führt Identity Management nicht nur zu einer technologischen Diskussion, sondern hat vielmehr Einfluss auf Geschäftsprozesse und darüberhinaus organisatorische Auswirkungen.

Die Rolle der „Rollen und Aufgaben“ ist für Unternehmen lebenswichtig: Das heißt: wie greifen Menschen, Systeme und Applikationen auf Informationen zu, seien es andere Anwendungen, Datenbanken, Maschinen, oder andere vitale Informationsbestände? Welchen Mitarbeitern, Kunden, Partnern etc. erlaube ich unter welchen Bedingungen Zugriff auf mein Intranet?

Das zu organisieren, Sicherheitsrichtlinien zu erarbeiten und Konsequenzen einer Implementierung hinsichtlich der Geschäftsziele zu berücksichtigen, ist eine zentrale und strategische Aufgabe der IT Organisation.

Der erste Schritt ist oft zu überlegen, wieviel Identity Management überhaupt möglich ist, ohne in vitale Geschäftsprozesse überregulierend einzugreifen. Bei heterogenen IT-Landschaften sind Kostenaspekte darüberhinaus ein wesentlicher weiterer Gesichtspunkt. Sicherheit versus Integration, diese Diskussion kann aber in Zukunft nicht mehr das Wesen einer Entscheidung bei der Planung von Identity Management Strategien spielen.

Ohne eine effektive Identity Management Strategie laufen die meisten Unternehmen Gefahr, nicht mehr auf strategische Anforderungen reagieren zu können, seien dies Compliance Regeln (z.B. Sarbanes Oxley, Basel II), Schutz wichtiger Firmendaten, Audit-feste Anforderungen, Schutz der Privatsphäre (Datenschutzgesetze) und weitere. Dies ist beileibe nicht als taktische Vorgehensweise zu betrachten. Fakt ist, dass ein einheitliches und vor allem effizientes Management zu auditierender Daten (wer greift wann auf was unter welchen Berechtigungen zu – seien es Mitarbeiter, Partner, Kunden,...) und Informationen der Schlüssel für die Reduzierung von Risiken, Kosten und auch z.B. Klarheit von Finanzdaten ist (Compliance Management).

Kaum ein Unternehmen kann heute darauf verzichten, vertrauliche Daten in einer weltweiten Umgebung im Intranet zur Verfügung zu stellen. Wo das der Fall ist und wo Sicherheit bereits einen hohen Stellenwert hat, ist meistens der Weg zu einer horizontalen Integration der Zugriffsrechte noch nicht begehbar. Dieses Dilemma zu lösen, ist ein Ziel, das sich HCL mit dem hier beschriebenen Identity Management und Access Management Framework gesetzt hat: Sicherheit und Kommunikation gleichermaßen zu berücksichtigen, Risiken zu reduzieren und auf Basis der als Standard geltenden SAP Netweaver Technologie über Anwendungsgrenzen hinweg eine kostengünstige Integration und Administration zu ermöglichen.

Überblick über die Lösung

Mit der SAP Netweaver Technologie hat SAP eine offene und umfassende Integrationsplattform für Anwendungen, Systeme, Geschäftsprozesse und Daten geschaffen. Als Basis von mySAP ERP/mySAP Business Suite sowie der SAP x-Apps Anwendungen lassen sich über Netweaver sowohl Enterprise Integration Services bedienen, als auch standardisierte Strukturen in der IT aufbauen.

Ein Bereich, in dem sich mit SAP Netweaver erhebliche Kostenreduzierungen und Sicherheitsgewinne erzielen lassen, ist die Integration und das Management gegebener oder neuer Identity- und Access-Management Lösungen.

In diesem kurzen Artikel wird eine Zusatzanwendung zu SAP Netweaver vorgestellt, die es ermöglicht, Identity und Access Management Lösungen in heterogenen Umgebungen zu integrieren.

Diese Lösung basiert auf standardisierter JAVA/J2EE Technologie und erlaubt es, Identity Management bezogene Aufgaben in Unternehmen mit einer Multi-Plattform Umgebung zu administrieren.

Auf Grundlage der SAP NetWeaver Plattform entwickelt, erledigt dieses Framework Routineaufgaben, die mit dem Lebenszyklus des Identity Managements in der komplexen Umgebung der Unternehmensanwendungen verbunden sind.

Die zugehörige Benutzeroberfläche führt Anwender wie Administratoren mit Hilfe selbsterklärender Prozesse durch die administrativen Aufgaben.

Als Web-basierte Applikation kann diese Lösung durch das Netweaver Portal adressiert werden.

Sie erleichtert darüberhinaus, die Einhaltung der Richtlinien firmenweiter Benutzer- und Zugangsidentitäten des Unternehmens zu organisieren und durchzusetzen und ihre Übereinstimmung mit Compliance Regeln zu überprüfen.

Verwaltung der Identität der Benutzer und ihrer korrespondierenden Zugangsrechte in heterogenen Anwendungsumgebungen wird hierdurch ermöglicht. Dazu gehören auch alle Anwendungen, die auf Basis von Technologien wie J2EE, .Net, RDBMS,

SAP R/3 und SAP NetWeaver Enterprise Portal in einem Unternehmen existieren. Dies kann auch Domain Netzwerk und E-Mail Benutzer einschließen.

Als Framework lässt sich diese Identity und Access Management Lösung an beliebige Umgebungen anpassen.

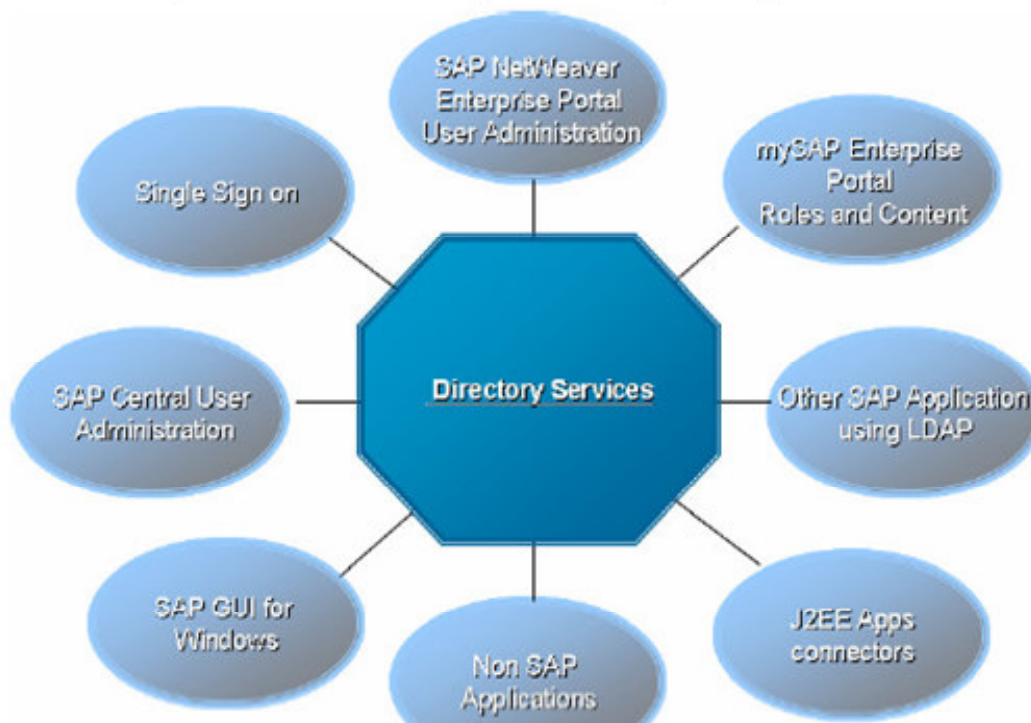


Bild: Schematische Darstellung der Integrationsplattform für Directory Services

Dabei dienen Active Directory Services als zentrales Repository für alle individuellen Managementaufgaben für Systembenutzer. Die Integration mit Domain Network Directory Services macht den Austausch der Daten der Benutzer unternehmensweit möglich.

Damit integriert dieser Ansatz zentrale Directory-Service Systeme und Anwendungen, seien sie von SAP oder anderen Herstellern. Die Integration von SAP-Anwendungen mit Directory-Services ermöglicht es nun Unternehmen, die Vorteile des Identity Managements auszunutzen. Gleichzeitig kann man Lösungen von anderen Herstellern mit den Applikationen von SAP über Directory Services ansprechen.

Für bereits vorhandene Directories kann man deren Vorteile unternehmensweit so konsolidieren, dass ein Identity Management über einen „Single Point Access“ möglich wird, was erhebliche Verbesserungen in der Wartung und Sicherheit erlaubt.

Details der Lösung:

SSO:

Auf alle Web basierten Applikationen, die unter der IAM Lösung integriert sind, lässt sich per Single Sign On zugreifen. Zugangspunkt ist üblicherweise das bestehende Firmenportal

Skalierbarkeit: Es gibt keine Begrenzung der Zahl der Benutzer und Zugriffe sowie der Systeminstanzen. Ein spezielles Framework erlaubt die Konfiguration nahezu aller Enterprise Anwendungen mit relativ geringem Aufwand.

User Self Service:

Die Lösung enthält eine Self Service Schnittstelle, über die die diversen Zugriffsrechte über die Plattformgrenzen hinweg betrachtet werden können. Die Benutzer können ihre Passwörter selbst ändern und haben einen Überblick über Anfragen, die an die Administratoren gestellt wurden.

Für Administratoren steht eine einheitliche Schnittstelle zur Verfügung, über die Benutzeranfragen bearbeitet werden können.

Auditing Compliance / Einhaltung von Firmenrichtlinien:

Das Enterprise Identity Management System konsolidiert alle Zugriffsrechte, wenn gewünscht, und lässt sich hinsichtlich bestehender Richtlinien konfigurieren. Darüberhinaus erhält man einen einheitlichen Zugriff auf die diversen System Activity Logs und allgemeinen Zugriffsdaten, die mit der Identity Management Lösung entstehen.

Single Install / Single Tool:

Das Identity und Access Framework wird auf Basis von Web Application Services (WAS) integriert und die Benutzerschnittstelle im bestehenden Enterprise Portal implementiert (Single Install). Die Enterprise Identity Management Lösung ist sowohl für einen Portal-Zugriff als auch als alleinstehende J2EE Applikation einsetzbar.

Provisioning Services:

Mit dieser Eigenschaft können Administratoren Zugriffsrechte kontrollieren. Die Lösung ist außerdem mit einem Mail-basierten "Notification Service" und einem „Request Fulfillment Module“ für die Erfüllung von Benutzeranfragen ausgestattet.

Flexible Administration:

Als Web-Applikation kann man auf die Enterprise Identity Management Lösung über jeden beliebigen Standard Browser von jedem System im Intranet zugreifen. Dies erleichtert vor allem Administratoren die Kontrolle der Benutzerdaten, bringt aber auch für Anwender erhebliche Vorteile.

Funktionen für Administratoren:

Die jetzige Lösung bietet eine zentrale und selbsterklärende Kontrollschnittstelle, um die täglichen Aufgaben des Identity Managements ausführen zu können. Im Betrieb kann jeder Systemadministrator über diese Schnittstelle auf alle

Applikationen in der IT-Umgebung zugreifen. Bisherige Tests zeigen, dass sich der administrative Aufwand durch das IAM Framework um mindestens 30% reduzieren lässt.

Secure Remote Access:

Dies ist eine Browser basierte Applikation, die die SAP NetWeaver Plattform und das Enterprise Portal benutzt. Für sicheren Zugriff kann SSL auf dem SAP NetWeaver Enterprise Portal konfiguriert werden. Die Benutzerinformationen von verschiedenen angebotenen Applikationen lassen sich sicher durch JCA kompatible Anschlüsse managen.

Directory Integration Services (Heterogene Umgebungen):

Dieses Feature ist auf allen Ebenen verfügbar und gibt einer Organisation einen konsolidierten Überblick über alle Directories und deren Benutzer.

In zukünftigen Versionen der IAM Lösung finden sich weiterhin folgende Eigenschaften:

- Federation Services Supports
- Adressbuch
- Directory Security Services
- PKI

Copyright:/Contact:

HCL Technologies GmbH

Netweaver Team

Am Söldnermoos 17

D 85399 München-Hallbergmoos

Tel.: +49-89-607-68671

Fax.: +49-89-607-68679

c/o: Dr. Elmar Paul Selbach elmar.selbach@hclt.de