

Oracle Identity Management for SAP in Heterogeneous IT Environments

An Oracle White Paper

December 2008

Oracle Identity Management for SAP in Heterogeneous IT Environments

Executive Overview.....	3
Introduction	3
Oracle Identity Management Approach	5
Provisioning in Heterogeneous Environments.....	6
Access Management in Heterogeneous Environments.....	7
Oracle Access Manager Integrations with Various Platforms.....	7
Authentication.....	7
Authorization.....	9
Auditing.....	9
Attestation in Heterogeneous Environments	9
Conclusion.....	11

Oracle Identity Management for SAP in Heterogeneous IT Environments

Oracle's solution enables efficiency and compliance in managing enterprise-wide user accounts, SSO and security policies across SAP and other systems in a heterogeneous environment.

EXECUTIVE OVERVIEW

In today's fast paced business environment, companies are increasingly turning to automating business operations – using a range of enterprise applications including CRM, ERP, HR, corporate directories, etc. While these applications help to streamline businesses processes, if not properly managed, they can also create an environment where user information is fragmented and difficult to manage centrally. Further compounding the problem is the business driven need to make internal applications available to partners and customers, while assuring the security of critical corporate resources. This paper describes how the Oracle Identity and Access Management solution, enables organizations to meet these challenges in the heterogeneous Enterprise using SAP.

INTRODUCTION

Most enterprises, including those with SAP installations suffer from fragmented user management. User identity information is typically dispersed among multiple applications, and organizations often do not have a centralized enterprise directory that is the authoritative source for their user data.

This results in a number of business issues:

1. Increased cost

Defining new users and keeping their entitlements/access rights up to date across multiple discrete data stores costs time, and therefore money. Independent analysts estimate this cost to be at least €/ \$150 per user annually. These costs can be substantially reduced by putting an identity and access management infrastructure and processes in place to reduce the number of instances of user data and access policies that must be managed.

2. Increased security risks

Without an identity and access management infrastructure, security of key corporate data is easily compromised. When users change roles within an organization, it is often the case that they have the wrong accounts and access

rights in applications and systems due to inadequate user maintenance. Frequently users who have left an organization weeks or months earlier still have accounts and access to applications and systems. Finally, users authenticate to applications using different strength passwords with different password rules (e.g. frequency of password change).

Security can be increased by deploying an identity and access management infrastructure, which provides mechanisms for centralized management of key corporate resources.

3. Business agility

Organizations must derive as much value as possible from their existing IT investments while at the same time compete more effectively by adding new business functionality quickly and at reasonable cost. One way of doing this is to modularize pieces of business functionality by creating (web) services. A major obstacle to achieving this modularization/re-factoring is that user information is spread across applications and application components.

New services can be introduced more quickly and more securely if user authentication and service access do not need to be considered by the service developer. This can be accomplished by centralizing user management external to the services, and putting directory, authentication and access controls in place.

4. Governance and compliance

Many organizations are subject to independent audits of their IT systems as part of a wider 'governance' imperative. These audits can be internally imposed, for example in the government sector, or externally imposed, for example Basel II, Sarbanes Oxley, EU Privacy Directives, etc. At a minimum, such audits expect an organization to be able to demonstrate that only the appropriate people have access to specific resources (applications, information, services). By centralizing identity management and access control, it is possible to automatically produce accurate reports documenting which users have access to which systems, and who accessed what at what time. It is also possible to determine who had access to which systems at some point in the past, using historic audit data.

5. Usability

Finally, user productivity and satisfaction can be greatly enhanced by putting an Identity and Access Management solution in place. This is achieved through features such as single-sign-on, self-service, personalization and ensuring that authorized users always have access to the right resources instantly.

These issues are relevant regardless of whether organizations run eBusiness suite, Oracle-PeopleSoft, SAP or Oracle-Siebel alongside their other enterprise applications.

ORACLE IDENTITY MANAGEMENT APPROACH

Oracle's Identity Manager is a standards-based solution that supports all major IT systems, including leading portals, application servers, enterprise applications, directories and operating systems.

Oracle has a unique approach – it provides an enterprise-wide Identity Management system to support the heterogeneous IT environments prevalent in most organizations. Oracle's Identity Manager is a standards-based solution that supports all major IT systems, including leading portals, application servers, enterprise applications, directories and operating systems. Whether you are using Microsoft Active Directory for directory services, or IBM WebSphere application servers, or SAP for ERP applications, Oracle Identity Manager provides the most functional and scalable solution. Oracle is committed to supporting these heterogeneous environments on an ongoing basis and delivering an end-to-end solution focused on addressing cost reduction, increased security, improved user productivity and regulatory compliance. Figure 1 shows the overall Oracle Enterprise Applications Security logical architecture.

Enterprise Applications Security Architecture

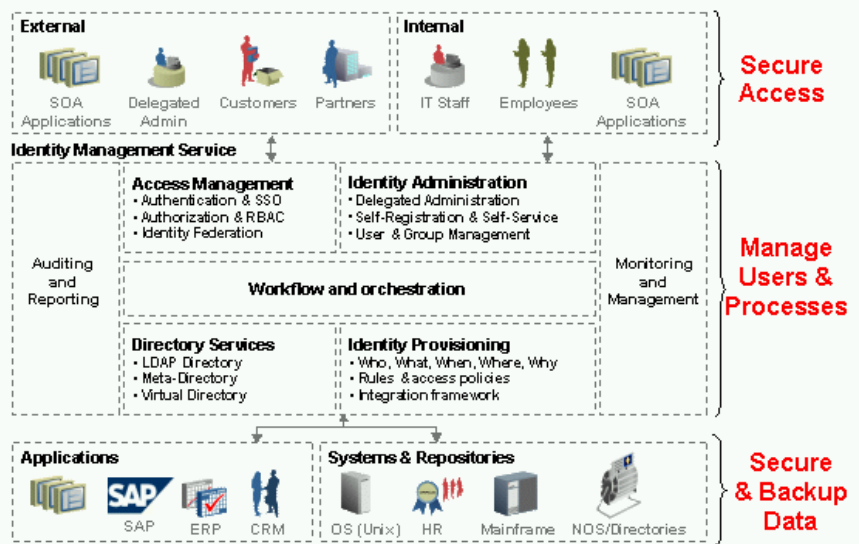


Figure 1: Oracle Enterprise Applications Security Logical Architecture

The Oracle Identity Management Solution provides Web Access Management, Enterprise Single Sign-on, Identity Provisioning, Directory Services, Identity Federation, User Administration, all in a complete suite that:

- complements and augments security in all infrastructure layers
- supports existing heterogeneous infrastructure – Hot-Pluggable
- is implemented centrally for all applications, or selectively for a subset of applications according to customer requirements

Oracle's solution ensures efficiency and compliance in managing enterprise-wide user account creation, modification, deactivation and security policies across SAP and other systems.

PROVISIONING IN HETEROGENEOUS ENVIRONMENTS

Oracle Identity Manager is a robust provisioning solution that works with SAP, and heterogeneous 3rd party systems, and provides the management activities, business processes and technologies governing the creation, modification and deletion of user access rights and privileges across an organization's IT systems. By automating these activities, companies gain better control over user access rights, enforce organizational security policies and ensure adherence to regulatory standards.

Oracle Identity Manager is a cross-enterprise, heterogeneous solution that offers an extensive and rapidly expanding library of pre-configured connectors, which are used to automate the provisioning and de-provisioning of user privileges across a wide array of applications. Each connector supports a wide range of identity management functions and uses the most appropriate and supportable integration technology recommended for the target resource, whether it's proprietary or based on open standards. These connectors enable out-of-the-box integration, but can be further modified using an 'Adapter Factory' integration generator to suit each enterprise's unique integration requirements. Agentless connectors are used wherever possible, reducing support and maintenance costs by avoiding installation of software on target systems.

The SAP Enterprise Applications Connectors (Figure 2), which are part of the Oracle Identity Manager solution, provide comprehensive out-of-the-box user provisioning, role and profile management, both to and from SAP Enterprise Applications, User Reconciliation across all managed SAP solutions, and comprehensive audit, reporting and attestation on accounts and entitlements across the mySAP Business Suite, thus meeting regulatory compliance requirements in a cost-effective manner.

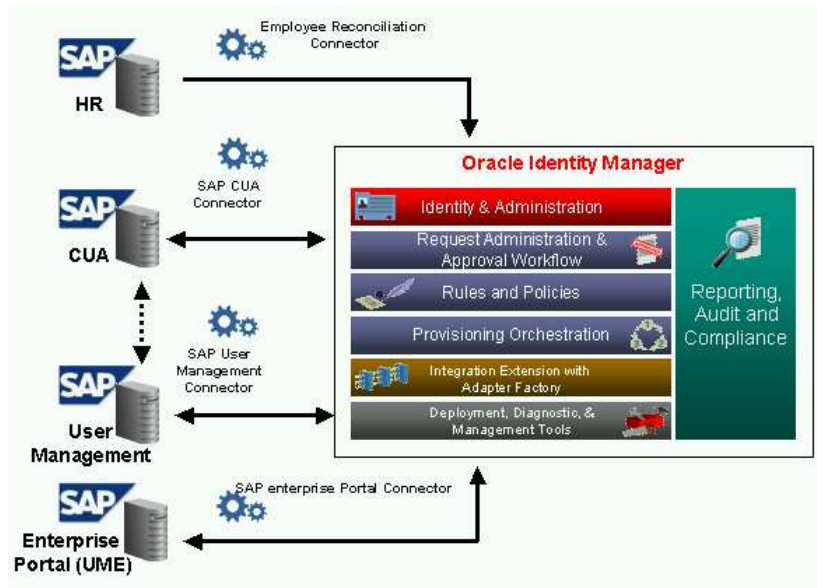


Figure 2: Oracle SAP Enterprise Applications Connectors for Oracle Identity Manager

Oracle's solution offers Single Sign-On for employees and business partners for SAP and heterogeneous environments, across company borders using advanced technologies such as federation.

ACCESS MANAGEMENT IN HETEROGENEOUS ENVIRONMENTS

Today companies must manage user access not only for SAP or other applications, but also to collaboration environments, such as portals.

To provide secure and auditable user access across these heterogeneous infrastructures, Oracle offers a comprehensive suite to manage user accounts and entitlements, authorize or lock out users according to roles, and protect resources via strong authentication methods such as smart cards and security tokens. Oracle's solution offers a centralized policy and identity administration service across enterprise platforms from SAP, IBM, and Microsoft, as well as custom-built applications. It enables organizations to meet compliance and governance requirements while keeping costs under control. Strong partnerships with market leaders such as Entrust grid cards and Gieseke & Devrient smartcards allow Oracle to provide off-the-shelf solutions for enterprise environments with the level of support that large organizations demand.

ORACLE ACCESS MANAGER INTEGRATIONS WITH VARIOUS PLATFORMS

Oracle Access Manager today offers authentication, auditing, authorization and single-sign-on for leading application server platforms and portals such as BEA WebLogic, IBM WebSphere, SAP NetWeaver and Microsoft SharePoint, as well as to business applications like Oracle-Siebel, Oracle-PeopleSoft and SAP.

It is capable of providing multiple levels of authentication as well as integrated authorization, and works seamlessly with the standard mechanisms of these systems.

Authentication

Using agents on a variety of web platforms such as web-servers and reverse proxy-servers, Oracle Access Manager can control all access requests and, based on centrally stored and managed policies, challenge the end user for authentication according to the required security level. Microsoft Active Directory domain logon via Kerberos tickets and impersonation is also supported such that Oracle Access Manager can actually trust a session initiated in the user's Windows desktop. Delegated administrators can easily maintain enterprise security policies by making use of pre-configured authentication types such as form-based login, smart cards, SecurID tokens, one-time-passwords or biometrics to protect the resources at the appropriate level. Based on Oracle Access Manager policies, tokens and cookies can be created such as SAP logon tickets, IBM WebSphere LTPA tokens and others. This provides a seamless user experience for single sign-on.

Figure 3 describes the Oracle Access Manager integration with SAP Portal (as an example).

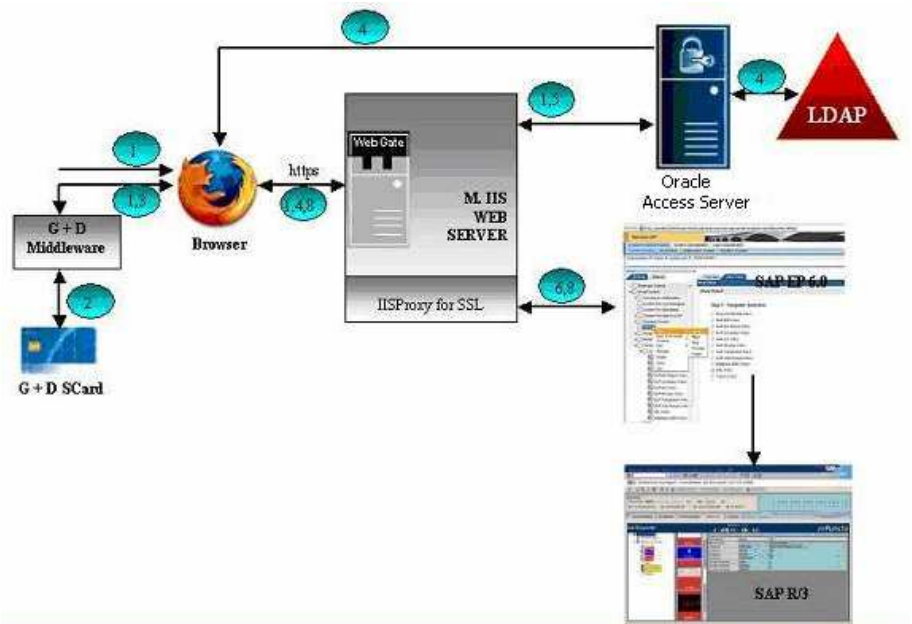


Figure 3: Oracle Access Manager Integration with SAP

1. User requests SAP EP logon page `https://<host>:<port>/irj` for HR application. Oracle Access Manager intercepts this request and redirects the authentication (regarding the defined policies in the Access Server) to the Smart Card Middleware.
2. User logs in through Smart Card and PIN.
3. Smart Card Middleware forwards Certificate from the card to the browser.
4. If the credentials are successfully validated, Oracle Access Manager authenticates the user and sets an encrypted SSO session cookie in the user's browser.
5. Following authentication, the Oracle Access Manager authorization rules are applied based on the security policy. If the user is authorized, access to the requested content (SAP Portal Login) is allowed.
6. Oracle Access Manager Access Server sets the authenticated user-id in the defined HTTP header variable. The proxy web-server then redirects the request to SAP EP internal web-server containing the HTTP header variables.
7. SAP EP uses this HTTP header variable value to check mapping of this user-id against the configured backend. (E.g. SAP R/3, DB). It is required that both Oracle Access Manager and SAP EP backend contain the same user-id value.
8. On successful mapping, SAP EP allows resource access to the user. It sends a response back to the proxy and the proxy redirects to the client browser.

The whole communication to the SAP EP server happens through the proxy web server.

Authorization

Oracle Access Manager also provides a central policy store for authorization of users to applications, protecting HTTP, J2EE and other resource types. The authorization policies are enforced by standard agents as well as modules integrated with application servers, such as the Oracle Access Manager connector for IBM WebSphere or the ready realm or security provider SSPI for BEA WebLogic. Using Oracle Access Manager, developers of applications use a standard interface to request information about authorization in their familiar environments, eliminating the need for proprietary custom policy enforcement code. These generic authorization policies are centrally stored, and easily configured through the Access Manager administration web interface. For fine-grained entitlement and application specific permissions, Oracle Identity Manager can be used to provide role and profile information to the SAP modules and components, so that SAP is able to enforce the right application access once the Oracle Access Manager has established the session and completed the initial user authorization.

Auditing

Oracle Access Manager provides master audit rules for identity administration, policy management, and access events. The auditable events include authentication success/failure, and authorization success/failure; and each audit trail entry can be configured to capture various details about the event, such as user profile information, the network where the request originated, on which web server, at what authentication level, etc. In addition to master audit rules, individual audit rules can be enforced to capture additional information as required by each protected application. Thus, all roles, permissions and access events can be audited for SAP applications and portals and for all other applications managed by the Oracle Identity Management solution. Audit trail information is typically sent to a central audit database.

Organizations can use Oracle's framework for temporary auditing and attestation to provide data snapshots on current data as well as identity history, by leveraging centralized identity reporting to ensure sustainable and cost efficient compliance.

ATTESTATION IN HETEROGENIOUS ENVIRONMENTS

Oracle provides a common framework for attestation across the entire Identity and Access Management infrastructure. Attestation is a process for reviewers to verify the provisioned resources that certain users have. Attestations may be scheduled or manually initiated. Responsibility to perform regular reviews and attestation of employee privileges within SAP components and other enterprise applications can be assigned to individuals or groups of participants. User-centric or application-centric reviews may be conducted. All events are recorded and are reportable, allowing attestation processes (Figure 4) to be automated and compliance measured. Oracle Identity Manager automates attestation scheduling, notification, supply of data to be audited, execution, auditing and reporting for all integrated applications or external entities. Oracle Identity Manager controls attestation of SAP user profiles and accounts, and any other enterprise applications, in addition to other attestation

requirements, which may not relate to any specific IT systems, such as physical resources varying from business cards, securID tokens, mobile phones, etc.

Reviewer + Data to Attest + Schedule = Attestation Process

Attestation Process Framework

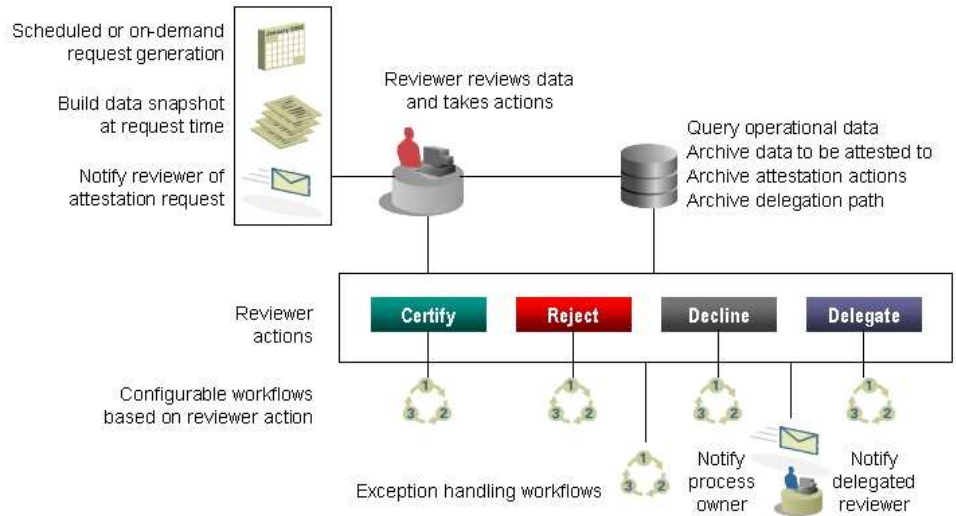


Figure 4: Attestation Process Framework

Comprehensive identity management is mandatory for handling business processes securely in a modular service oriented transaction environment.

CONCLUSION

Oracle leads the industry with the most complete Identity and Access Management solution. Built on an open-standards architecture, Oracle Identity and Access Management supports heterogeneous environments ensuring interoperability with multiple IT systems, a key requirement for today's leading companies.

Oracle Identity and Access Management is architected for Service Oriented Application environments allowing applications to utilize Identity and Access Management shared services via standards-based interfaces so that more and more applications can be deployed as loosely coupled reusable security services. This approach saves enterprise organizations significant integration costs.

Oracle Identity and Access Management Suite integrates out-of-the-box with your business applications, automating the business processes your organization relies on today.

This application centric Identity and Access Management approach is an integral component of a wider application development and deployment framework that integrates seamlessly, and allows you to bring new secure applications on-line to meet urgent business requirements.



Oracle Identity Management for SAP in heterogeneous IT environments

Dec 2008

Author: EMEA Technology Solutions

Contact: Christine Wever-Diehl

Contributing Authors: Frank Villavicencio

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:

Phone: +1.650.506.7000

Fax: +1.650.506.7200

oracle.com

Copyright © 2007, Oracle. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice.

This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission. Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.