

Introduction to Oracle Identity Management

*An Oracle White Paper
September 2005*

Introduction to Oracle Identity Management

Fundamental and important business drivers are compelling worldwide organizations to implement Identity Management solutions.

OVERVIEW

At a high level, five fundamental market drivers are leading worldwide enterprises, government, and educational entities to implement secure identity management solutions:

Extending the Enterprise: An enterprise must broaden its reach to grow its business, create new revenue streams, and enable productivity from anywhere. This entails extending business resources, systems, and services to customers, partners, and employees wherever they are.

Providing Regulatory Compliance: Nearly every organization around the world – publicly traded corporations, hospitals, schools, government entities – is subject to multiple regulations that mandate different aspects of privacy or accountability (e.g., Sarbanes-Oxley, HIPAA, Graham-Leach-Bliley, Data Protection Directive, etc.). The common challenge is to ensure that the right people have appropriate access to the right resources at the right time—and to be able to prove it.

Providing Security: Organizations must be confident in the security and integrity of business resources, systems, and services. In essence, organizations need to open the doors to the world while ensuring that the whole world doesn't walk through them. It is important to securely manage appropriate access to business resources for employees, customers, partners and suppliers.

Reducing Costs and Increasing Productivity: In short, this means doing business more efficiently. Within IT organizations, this includes looking at the drivers behind system administration and help desk costs. It also includes a tighter, correlated relationship between employees and the business resources they support in order to work productively.

Increasing Customer Loyalty through Higher Service Levels: More stringent service level agreements and rising customer expectations are important metrics to ensure customer retention and increased customer loyalty, which in turn lead to higher revenues. To provide this level of service, organizations must eliminate identity silos, bring customer data together, and provide comprehensive information from which to make informed business decisions. Also, when customers are empowered to manage their personal information, they will appreciate the convenience and resulting improved service. To meet these business

challenges, organizations need to orchestrate an ever-growing set of resources and allow an increasing and diverse set of people to interact with them—all in a personalized and secure way. The thing to understand is that identity is the common thread in these challenges.

So, how does one leverage identity to solve these challenges? First, one must eliminate the unintentional identity silos that separate business resources today. Next, the enterprise must know who someone is, what their role or relationship is with the organization, and what resources and information they should have access to. And finally, one must be able to control access based on business policies while gauging regulatory compliance.

Proper and secure management of employee, partner and customer identity is a common thread in improving organizational efficiency.

To do all of this, it is imperative that organizations implement a secure identity management solution that leverages a common identity foundation across the entire infrastructure. This solution must include and integrate all critical components: policy-based identity management, access control, and auditing. This type of comprehensive, secure identity management solution will address critical business drivers and put the enterprise in a position to compete effectively now and in the future.

Identity Management is a strategic imperative.

Identity Management spans organizational, technological, political, and social issues. As stated above, Identity Management has become a strategic imperative for the enterprise. In short, Identity is the foundation for security functions within the loosely couple web services architecture. A non-centralized security infrastructure creates additional administration overhead, user frustration and reduced productivity. Security vulnerabilities can expose a company to legal and financial liabilities for failing to meet the data privacy compliance requirements of HIPAA, Gramm-Leach-Bliley, Sarbanes-Oxley, California’s Security Breach Information Act (SB 1386) and European Union’s Data Protection Policy. Oracle’s Identity Management solution helps organizations strengthen security, comply with requirements for privacy and reduce costs, even as they increase access to applications across their enterprise.

Identity Management solutions must be complete, well integrated, and open.

SOLUTION CRITERIA

Oracle has recognized the need for a comprehensive approach to Identity Management and is providing our customers with a set of products that meet the following key criteria:

Complete Identity Solution

The market requirements for Identity Management solutions dictate that solutions encompass the full range of identity Management functionality – from initial identity provisioning to long-term management, from highly secure access to cross-organization deployment, from fine-grained authorization to federated trading relationships, all of which are built on a robust and well-proven security infrastructure. Customers need to be able to deploy at whatever level of complexity that the business requires. That may mean to “start small” and “grow large” along

with the needs of the business. Or it may mean to provide specialized and compartmentalized access for some business functions while providing more broad-based access for other functions as the business needs dictate. An Identity Management solution must provide this level of functional completeness and discrete flexibility.

Integrated

Customers look to large solution providers to tightly integrate Identity Management technologies within business applications. This is where the most leverage comes to businesses. It is not enough to simply provide identity and access management tools. Customers need those functions to closely support the business functions of the enterprise. Oracle is uniquely positioned to deliver this critical requirement through integration with Oracle's business applications like PeopleSoft, JD Edwards and other eBusiness applications. Moreover, Oracle's Fusion Middleware has rapidly proven its value to worldwide enterprises as a robust, flexible, and value-rich solution to organizations that require a world-class middle-tier solutions platform. Finally, Oracle's strong reputation and proven strengths in secure, reliable data management is unquestioned today. The collection of such comprehensive technologies is a unique strength of Oracle. The integration of Identity Management with these technologies provides our customers with high value solutions to business needs.

Heterogeneous & Open

While Oracle provides unique and strong value through the integration of Identity Management technologies with its business applications, Application Server and database products, we understand that customers need solutions to perform well in heterogeneous technology infrastructures. Oracle Identity Management solutions are designed to work with the leading directories, Web Servers, Application Servers, and business applications because of their state-of-the-art design, architecture, and adherence to relevant industry standards for system design, development tools, security, identity management, communication and data management. It is because of this conformance to industry standards that Oracle is able to offer our customers solutions that work well within existing information technology infrastructures, deploy quickly and economically to enable new business relationships with an enterprise's customers, partners and suppliers.

PRODUCT OVERVIEW

Oracle Identity Management leverages Oracle's secure technology stack. As a result, it provides a high degree of reliability, scalability, security and performance, as well as an infrastructure for privacy.

Oracle Identity Management streamlines the identification of users across the extended enterprise and controls their access to applications and information for improved security and regulatory compliance. Oracle Identity Management's integrated management features permit system administrators to manage security

Identity Management solutions must conform to established standards in order to preserve and protect customers' investments.

from a central coordinated service to include access to Oracle and non-Oracle applications.

Built on Oracle 10g database and Fusion Middleware technologies, Oracle's Identity Management solution is a security framework that is foundationally based on an LDAPv3 compliant directory, Oracle Internet Directory, for storing identity information. Oracle Identity Management leverages LDAP services to manage user identities and access control privileges, while providing Web single sign-on capabilities, provisioning of network resources, web-based delegated administration to allow users and non-IT managers assume certain administrative responsibilities and a built-in authority for issuing and deploying PKI certificates for intranet (non-public-facing) services. The Oracle Identity Management solution framework includes APIs for integrating with other authorization sources and authentication services from third parties providing interoperability with leading directory, access management and user provisioning solutions. This allows the organization to leverage their existing identity management infrastructure point solutions and speed implementation while standardizing on Oracle technology.

Oracle Identity Management provides the essential controls for regulatory compliance and privacy management.

The Oracle Identity Management infrastructure aids an organization's compliance efforts by providing privacy controls and security manageability features that protect consumer confidential information. This infrastructure centralizes management of security across the enterprise, simplifying management and reducing administrative overhead. This increases security while reducing administrative costs.

Centralization afforded by this approach is the key to tracking and managing user's authorizations and preferences across the enterprise. Centralization allows you to manage privacy preferences and exert central control over who is authorized to access personally identifiable information (PII).

The identity management infrastructure is an integral part of building an infrastructure for privacy. It is far easier to ensure that privacy preferences are enforced if there is a common notion of the user. If the privacy policy changes, you can manage access rights centrally; thereby you can easily change rights as privacy policy evolves. Additionally, you gain the cost savings inherent in self-service and consolidated administration.

The Oracle Identity Management solution framework is based on industry standards and the following core functions:

- LDAP directory services to store and manage user identities and access control privileges
- Web Single Sign-on services to provide users with single sign-on to access applications
- Directory integration services to integrate Oracle EIM with an organization's existing security and directory infrastructure

Identity Management saves money, improves organizational efficiency, and protects individual and corporate information.

- User provisioning services for Oracle products and other software vendor's applications
- Delegated administration services to enable users to modify security privileges.

Identity management is important to customers because it reduces administrative costs associated with application deployments and user management, while at the same time improving security. For example, Oracle's Identity Management solution:

- Centralizes and automates many user administration tasks, thereby reducing administration costs while improving accuracy and security.
- Provides IT management efficiency and help desk cost avoidance by simplifying end user and administrative processes.
- Improves productivity as a result of consolidating and automating IT administrative responsibilities, enabling staff to work more efficiently and address revenue-enhancing initiatives.
- An effective identity management strategy allows better end-user experience for greater employee productivity and increased customer and partner satisfaction.
- Improves business agility by shortens application development lifecycles via a “build once, leverage always” model, enabling faster time to market.
- Enables secure and cost-effective interaction with customers, partners and suppliers.
- Improves application security by providing centralized management of passwords and security credentials. This reduces the insecure practice of users leaving IDs and passwords exposed.
- Improves security by providing timely and restrictive access to corporate information from legitimate users versus intruders.
- Assists an organization in complying with corporate governance and regulations.

PRODUCT HIGHLIGHTS

Oracle Identity Management is an integrated infrastructure that Oracle products rely on for securing users and applications across the enterprise. The Oracle Identity Management infrastructure includes the following components:

Oracle Access and Identity Management

Access and identity are the means for administering users and their privileges and controlling their access to enterprise resources. Oracle Identity Management delivers access control and identity management through Oracle Identity Management, Oracle Fusion Middleware and Oracle Delegated Administration

Services. These components work together to provide centralized, fine-grained access management for heterogeneous application environments, as well as out-of-the-box integration with Oracle products such as Oracle Portal, Oracle Collaboration Suite, and Oracle business application. In many organizations, user profile management is the shared responsibility of centralized administrators, delegated administrators, and the users themselves. Oracle Access and Identity supports all of these usage models. In addition, Oracle Identity Management enables customers to build composite identity profiles consisting of attributes from both RDBMS and LDAP user stores for use in both access control and identity administration. Oracle Access and Identity Management also provides flexible and detailed reporting about who has access and to which corporate applications, which is critical for Sarbanes-Oxley, HIPAA and Gramm-Leach-Bliley compliance. Oracle Access and Identity improve application security, ease regulatory compliance concerns, and improve the end user experience. Key features and benefits of Access and Identity are:

**Oracle Identity and Access Management
provide many similar and powerful
benefits.**

- Self-service and password administration to allow system users to self-manage appropriate account profile, preferences and password information thereby saving significant help desk overhead costs.
- Delegated administration that provides line managers with control over appropriate identity privileges and access providing increased business agility and faster implementation of organization and responsibility changes.
- Workflow engine to automate business policies and procedures to ensure that organizations comply with regulatory requirements thereby easing the cost of regulatory compliance and audits.
- Web Services interfaces to provide more identity infrastructure and controls that more easily adapt to changing business requirements and installed information technology infrastructure thereby decreasing costs, providing higher security controls and increasing competitive advantage.
- Heterogeneous environment support to ensure that Identity Management is more widely adopted within the enterprise thereby preventing identity silos that are not integrated within the corporate guidelines and are subject to security risks.
- Policy based access management to ensure that the right people have access to the right information and applications thereby providing increased organizational efficiency, security and regulatory compliance
- Multi-level, multi-factor authentication management to provide for the typical organization's complex authentication policies, easing administrative burden, duplicate systems, consistent implementation of security policies, and saving deployment costs.

- Open & heterogeneous provides for economical integration with legacy systems and provides a flexible framework for future business technology requirements.
- Broad platform, directory, database and applications support to allow customers to deploy within existing information technology infrastructures without requiring expensive “rip and replace” alternatives.
- Proven to scale to multi-million user deployments to provide the assurance and cost savings of virtually unlimited organizational growth.
- Improved and more consistent user experience to improve productivity, morale and save training costs.

Oracle Provisioning

Provisioning automates the creation and management of large numbers of users in heterogeneous enterprise environments. Oracle Provisioning combines the rich delegated administration, self-service and workflow capabilities of Access and Identity with the synchronization and identity provisioning capabilities of Oracle's Directory Integration and Provisioning platform. Working with Oracle Internet Directory, Oracle Provisioning allows automated provisioning and de-provisioning of user identities in applications, databases, identity repositories and other systems, thereby enabling huge time-and-cost savings within heterogeneous IT environments of all sizes. Key features and benefits of Oracle Provisioning are:

- **Complete workflow for approvals** to ensure that appropriate resources are accessed quickly, consistently, easily and in compliance with corporate policies.
- **Broad range of connectors** for operating systems, databases, directories, groupware, applications, and devices, to ensure access across diverse installed infrastructure.
- **Direct connectivity** to Human Resources applications and data so that employees are granted access to all of the corporate applications and data necessary to do their jobs, thereby improving productivity, morale, and administrative costs.
- **Compliance reporting** to provide fast response to regulators and auditors for minimal business interruption.

Oracle Secure Federation Server

As more companies move their business processes to the web, many organizations have a greater need to extend the boundaries of their enterprise to include partner applications. Federating identity data allows each company to operate independently and cooperate for business purposes. Oracle Secure Federation Server is an identity federation server that provides cross-domain single sign-on and helps large corporations securely link their business partners into the corporate

portal or extranet while also increasing their compliance with privacy and security regulations. Oracle Secure Federation Server enables customers to manage multiple partners and choose from industry standard federated identity solutions from within one self-contained software product that companies can easily distribute to their partners. Key features and benefits of Oracle Secure Federation Server are:

Oracle Secure Federation provides multi-protocol support in flexible deployment configurations.

- Multi-protocol gateway – including SAML, Liberty, WS-Federation – providing both Service Provider and/or Identity Provider functionality to ensure that business partners are able to inter-operate with appropriate business applications regardless of their installed systems.
- Flexible deployment configurations – from tightly integrated to standalone – to ensure that diverse business requirements can be easily satisfied without extensive and expensive customization.
- Improved end user experience to simplify cross-domain single sign-on access, improve business relationships cost-effectively, strengthen security and compete more effectively.

Oracle Web Services Manager

Oracle Web Services Manager is a comprehensive solution for adding policy-driven best practices to existing or new Web services and provides the key security and management capabilities necessary to deploy Service-Oriented Architectures across line-of-business applications. Oracle Web Services Manager allows IT management to centrally define policies that govern Web services operations (such as access policy, logging policy, and load balancing), and then wrap these policies around Web services without requiring modification to those services. In addition, Oracle Web Services Manager collects monitoring statistics to ensure quality of service, uptime, and security threats and displays them in a Web dashboard. As a result, Oracle Web Services Manager brings better control and visibility over Web services. With Oracle Web Services Manager, compliance risk and time to market are greatly reduced. Key features and benefits of Oracle Web Services Manager are:

- Web Services access control and single sign-on to ensure secure yet flexible availability of key business applications within a modern, cost-effective web-service-oriented architecture.
- Centralized security policy management with localized enforcement to provide maximum policy control with maximum system performance.
- Unified Monitoring of Cross-Organization Web Services for improved security, simplified administration, and more agile business responsiveness.

Oracle Internet Directory

Directory services are central to an identity management strategy. Oracle Internet Directory is an LDAPv3 directory that leverages the scalability, high availability and security features of the Oracle Database. Oracle Internet Directory serves as the

central user repository for Oracle Identity Management, simplifying user administration in the Oracle environment and providing a standards-based application directory for the heterogeneous enterprise. Additionally, Oracle Directory Synchronization allows Oracle Identity Management to seamlessly integrate with other directories and enterprise user repositories, allowing users to leverage identity information wherever it resides. Key features and benefits of Oracle Internet Directory are:

Oracle Internet Directory is a massively scalable identity store.

- Full feature LDAP server with a RDBMS data-store to provide simplified and cost-effective management of identity repositories
- Highly scalable to many millions of users for long-term system stability and low cost of ownership
- Strong Oracle platform integration – including Oracle GRID support – to maximize customers' investments

HETEROGENEOUS AND OPEN

While Oracle solutions work well within an Oracle environment, we recognize that customers have a very diverse information technology infrastructure within which any new technology must cleanly interoperate. Oracle Identity Management products have been designed to work with a wide array of directories, web servers, application servers, SSO servers, portal servers, database and business applications.

To achieve this, Oracle is committed to conform to relevant industry standards for identity and web service development, including: WSDL, WSRP, JSR, JCP, SOAP, Oracle Jdeveloper, Oracle BPEL Designer, Oracle TopLink and ADF, SAML, Liberty, SPML, WS-Security, WS-Federation, LDAPv3, XACML.

In addition, Oracle conforms to a number of security-specific standards, such as: XKMS, WSS, PKI, XML-SIG, XML-ENC, SSL, PKCS, TLS, S/MIME, LDAP, and Kerberos.

Oracle Identity Management Partners

Oracle provides a robust and comprehensive Identity Management infrastructure for our customers. In addition, a number of market-leading companies have created specific solutions for business needs, such as: smart cards, bio-metrics, and other specialized devices and software functions.

Additionally, Oracle has partnered with many of the leading global systems integrators so that customers have a ready source of deployment expertise and assistance as their business requirements dictate.

SUMMARY AND CONCLUSION

Scalable, Robust and Integrated Infrastructure

As enterprise identity management and security services become centralized, the scalability and reliability of the infrastructure are key concerns. Oracle Identity

Management is an integrated enterprise infrastructure that is built on Oracle's "unbreakable" technology stack, providing the traditional Oracle technology strengths of scalability, reliability and security.

Oracle Identity Management brings high value to Oracle Customers.

Out-of-the-Box Deployment Support for Oracle Products

All Oracle products (Oracle Database, Fusion Middleware, and Oracle Business Applications) are engineered to leverage Oracle Identity Management out of the box. Each of these product sets relies on Oracle Identity Management as the primary infrastructure to manage web services and administer user provisioning, authentication and authorization. The result is an overall lower cost of deployment and cost of ownership for these products in the enterprise.

Single Point of Integration

Many Oracle customers run several instances of various Oracle products in their environments. Without the Oracle Identity Management infrastructure, customers and vendors would have to worry about integrating their various third-party directories, web single sign-on solutions, and provisioning systems with each individual Oracle product, creating an integration and maintenance nightmare. Oracle Identity Management eliminates the need for customers to build and maintain these integration points. Oracle Identity Management serves as a single point of integration between the Oracle environment and other identity management solutions. Integration of third-party identity management solutions with Oracle Identity Management gives them instant compatibility with the customer's Oracle environment.

Open, Standards-Based Infrastructure

Oracle Identity Management is an open, extensible, and standards-based infrastructure, which can accommodate a wide variety of deployments and partner solutions and customer environments. For example, partner products may leverage Oracle Identity Management to provide ready integration with Oracle application environments. To this end, Oracle works with partners to help them ensure that customers will be able to take advantage of the Oracle Identity Management infrastructures right out of the box.

Oracle Identity Management provides superior return on investment.

Oracle is committed to providing comprehensive and robust Identity Management solutions to our customers. Above all, Oracle is committed to provide well-integrated and open solutions that afford our customers superior return on their investment in Oracle technology

ORACLE FUSION MIDDLEWARE

Introduction to Oracle Identity Management
September 2005

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 © 2005, 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, and PeopleSoft, are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.