

# Otecia Implementation of Oracle Access Manager (OAM) and Oracle Virtual Directory (OVD)

*An Oracle White Paper  
September 2007*

# Otecia Implementation of Oracle Access Manager (OAM) and Oracle Virtual Directory (OVD)

Otecia's areas of expertise include cross-vendor Identity Management (IdM), Federation, and Web Access Management (WAM) integrations, Directory Services (LDAP) design, integrations with application servers, legacy systems, and portal.

## EXECUTIVE OVERVIEW

Identity Management has become a central business issue across all industries and geographies. Although organizations see the immediate value, they often struggle with the implementation. The key to a successful implementation is selecting a System Integrator with a successful project management track record, who can address your specific business requirements and technical architecture. This paper introduces one such System Integrator – Otecia – and one of the significant identity management implementations they drove using Oracle's products. Otecia consultants have extensive experience in Web Access Management and Directory Services to help organizations successfully implement Identity Management solutions quickly and efficiently. They have implemented such solutions across various verticals such as Education, Financials, Government, Healthcare, Pharmaceutical and Telecommunications, in locations such as Africa, Europe and North America. This white paper will discuss Otecia's implementation of Oracle Access Manager and Oracle Virtual Directory for a leading market research firm.

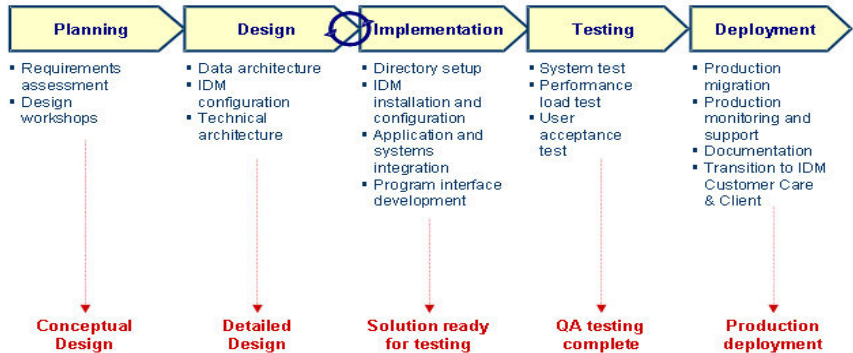
## OTECIA METHODOLOGY

The Otecia Methodology breaks down each project into one or more threads. Once, the project threads are defined the consultants can execute the plan.

Otecia's objective is to provide the customer with a successful deployment within 90 days or less, and does so by collaborating with the customer starting on day one. Oblix consultants, who founded the company, realized Identity Management projects affect the entire enterprise. Project success rates increase if customers properly prepare their underlying infrastructure for Identity Management. The Otecia methodology is based on multiple project phases as outlined in figure 1.

## Project Phases

The methodology we have successfully used in previous deployments breaks down each project into one or more threads. With the project threads defined, the methodology next suggests a path to take the project from kickoff to production deployment.



**Figure 1: Otecia Methodology**

The customer can also include the following mitigation activities:

- **Product Training:** This occurs prior to the implementation.
- **Architecture Review:** A third party validates the design before implementation.
- **Product Readiness Assessment:** Senior architects validate the deployment before production.

## BUSINESS REQUIREMENTS

The customer, a leading market research firm, needed to rebuild their custom Identity Management solution to increase security, reduce costs, achieve compliance and improve end-user experience. The previous enterprise infrastructure required individuals to authenticate multiple times, so that users needed to remember multiple IDs and passwords, a potential security risk to the organization. On the technology side, the custom-built security framework had to accommodate numerous platforms, making it expensive to maintain and upgrade. Additionally, user data was scattered across multiple repositories, which made it nearly impossible to maintain a single snapshot of the customer.

Otecia replaced this custom solution by implementing Oracle Access Manager and Oracle Virtual Directory at the customer site to:

- Provide an industry-standard identity management solution in compliance with best practices
- Create a supportable and upgradeable solution to integrate with other applications
- Centralize, manage and automate user accounts

**Oracle Access Manager** delivers critical functionality for access control, single sign-on, and user profile management in the heterogeneous application environment.

**Oracle Virtual Directory** provides Internet and industry standard LDAP and XML views of existing enterprise identity information, without synchronizing or moving data from its native locations.

- Enable managers and auditors to effectively audit employee's access and transactions
- Reduce the cost of maintaining a custom-built solution

Otecia's customer wanted to roll out the technology in two phases. The initial phase included authentication and SSO for Web sites and the portal. The enterprise needed to design an access management system to integrate with several custom applications and to provide backward compatibility, as well as audit & logging capabilities. The Oracle Virtual Directory provided a real-time view of identity data stored in repositories such as directories and databases, which provided a common and consistent format for applications. By utilizing Oracle Virtual Directory, Otecia eliminated the need for a new directory, neutralizing the associated political questions - What data should a new directory include? Who will manage it? And more importantly, who will fund it?

The following user scenarios were prioritized for the first phase.

- Registration on Web site
- User Signs onto Web site
  - The customer has various types of users: Paid vs. Unpaid Users, Enterprise Users vs. Non-Enterprise Users, Employee vs. Non-Employee and Site Admin vs. Regular User
- Kiosk Users
  - Needed for conferences, events, and seminars
- Detect Concurrent User Logins
  - Prevents the sharing of login IDs
- Enterprise Access (via custom plug-in)
  - Enterprise registration is automatic and the employees of an entire company have access to the client's applications
- Scalability and response time
  - Tested 500 concurrent users
  - Required a response time of 5 **seconds**. Otecia delivered a response time of 1.5 seconds.

The second phase involved the following:

- Custom OAM Plug-in to prevent sharing of IDs
  - System provides a 10 minutes grace period for users who log into the system with the same ID
- Custom OAM Plug-in for persistent logins

- Use of persisted session token cookies to allow transparent login to web-based applications
- Integration with legacy system applications

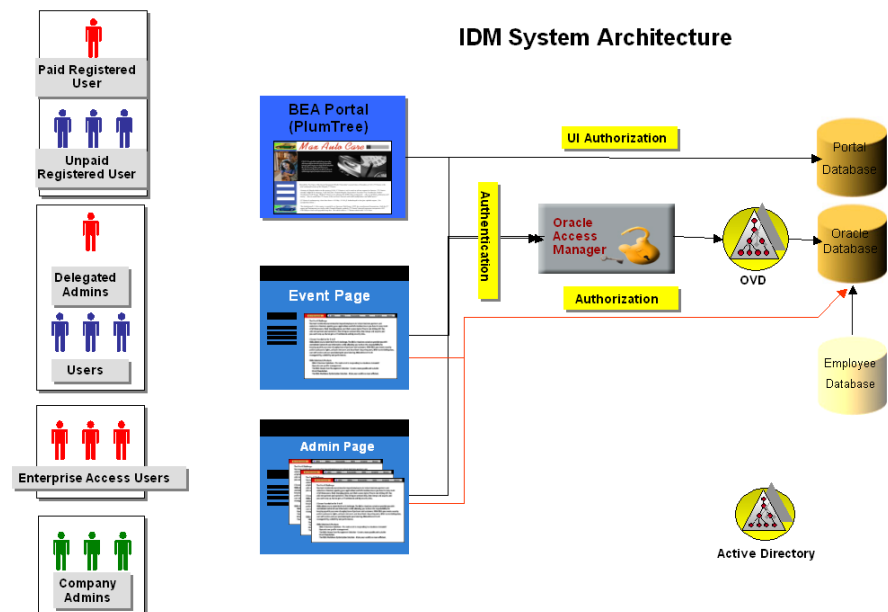
## IDENTITY MANAGEMENT ARCHITECTURE

The design phase was an opportunity to map the new technologies, i.e. Oracle Access Manager and Oracle Virtual Directory, into the current environment and identify/resolve issues before implementation.

Oracle Access Manager enabled the customer to create a security framework to manage and automate their identities and provide users with secure, fine-grained access to enterprise resources. Even though the business requirements for Oracle Access Manager were complex, customization only amounted to 10% of the solution. The new system was designed to detect persistent logins, concurrent users, several user types and entry points, as well as honor legacy credentials for authentication and authorization. OAM reduced costs, improved security, and provided end-users with self-service and delegated identity administration capabilities, as well as approval workflows for user creation and management.

Oracle Virtual Directory is a flexible and secure service for connecting applications to existing data repositories, such as databases and directories, without requiring changes to either the infrastructure or applications. The customer's back-end system remains unchanged, since the credentials are already stored in a database.

Otecia mapped Oracle Virtual Directory into the custom database and created a custom plug-in to transparently handle old legacy-format passwords that Oracle Access Manager could validate. See Figure 2 for additional details on the architecture.



**Figure 2: Customer Identity Management Architecture**

## **IMPLEMENTATION**

Otecia rolled out the Identity Management implementation in two phases. The first phase involved clarifying business requirements, mapping data elements, data manipulation, installation, and the configuration of Oracle Access Manager and Oracle Virtual Directory. The second phase included development of custom plug-ins, additional access policy configuration, extended authentication and authorization schemes, as well as integration of the legacy system and BEA Applications with Oracle Access Manager and Oracle Virtual Directory.

Otecia addressed performance and scalability requirements during the implementation process. They configured and fine-tuned the Oracle Database, Oracle Access Manager and Oracle Virtual Directory systems for fail over and load balancing to maximize performance and improve reliability.

Once the infrastructure was set in place, Otecia reviewed and configured Oracle Access Manager to comply with federal regulations and meet industry auditing and security standards.

Policy domains were configured to provide authentication and authorization for all Single-Sign-On applications. Custom authentication and authorization plug-ins were developed to provide the following features:

- Backward compatibility with legacy applications including a custom federation solution
- Persistent login
- Concurrent login detection and enforcement

Configuration and initial testing were performed in a development environment. Otecia developed a well-documented migration plan to move the solution across QA, staging, and production environments. All tests were performed using production-like data as follows:

- 1- Performance testing for up to 500 concurrent users
- 2- Simulation of hardware failure to exercise failover, and load balancing.
- 3- Load test simulating three times the anticipated load
- 4- Functional testing
- 5- Login/Logout testing for 500 concurrent users

Otecia implemented phase one in three months and phase two in two months. The customer went live within 45 days after the Otecia implementation without experiencing any disruptions to the business. During each user's first login, his authentication credentials were transparently migrated to the new, secure Single Sign-On solution.

## LESSONS LEARNED

Otecia ensures success by strictly following four guidelines:

- **Meet key parties early.** Otecia met with the business and technology groups early on in the process to determine the best strategy and set expectations.
- **Re-evaluate existing corporate processes.** For example, the customer had attached security to an IP address, which meant users needed to re-login if they switched from wireless to wireline connections. Otecia removed this constraint to facilitate SSO and improve security.
- **Over-deliver on expectations.** By reducing response time from 5 seconds to 1.5 seconds, Otecia nearly tripled the customer's Internet traffic. This proved to be beneficial, since the customer had underestimated the demand.
- **Plan for the future.** Otecia designed flexible security architecture to accommodate the customer's growth for the next 5 years.

## CONCLUSION

The solution not only met expectations, but also enabled the customer to identify and correct previously undetectable deficiencies with their homegrown solution. The new secure system prevents customers from cracking cookies, which means additional revenue. It also allows them to add new products to their web site with minimal cost and time. The project was accomplished within the customer's budget, and allowed the executive team to plan for future growth.



Otecia Implementation of Oracle Access Manager (OAM) and Oracle Virtual Directory (OVD)  
September 2007

Authors: Amanda West and Tim Arafat  
Contributing Authors: Alex Hristov

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](http://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 is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.