

# Oracle Extended Identity Management Ecosystem

## Reference Architecture

*An Oracle White Paper  
June 2006*

# Oracle Extended Identity Management Ecosystem – Reference Architecture

The Need For an Extended Identity Management Ecosystem .....	3
Business Benefits .....	4
Enhanced Compliance .....	4
Reduced Costs .....	4
Improved Security .....	4
Seamless User Experience .....	5
Reduced Risk .....	5
Components .....	5
Core Identity Management (IdM) Infrastructure .....	5
Strong Authentication .....	6
Enterprise Single Sign-on (ESSO) .....	6
Physical Access Control Systems .....	6
SSL VPN Solutions (Network Security) .....	7
Reference Architecture .....	7
Use Cases .....	9
Use Case 1 – User Management .....	9
Use Case 2 – End-to-end Access Control .....	11
Use Case 3 – One-Touch / No-Touch De-provisioning .....	12
Conclusion .....	13

# Oracle Extended Identity Management Ecosystem – Reference Architecture

**The boundaries of an identity management infrastructure can span a wide range of technologies and components including authentication, directory, access management and physical security systems. Enterprises are seeking integrated approaches to manage these disparate systems in a more efficient and holistic manner.**

**—Gerry Gebel  
Service Director, Burton Group**

## **THE NEED FOR AN EXTENDED IDENTITY MANAGEMENT ECOSYSTEM**

The advent of directory services almost 15 years ago gave rise to the broad spectrum of technologies that we today collectively refer to as “Identity Management”. Over that period, this multi-faceted market has gone through waves of stratification, as innovative new solutions have been conceptualized and progressed through the technology maturation lifecycle. As a result of this natural evolution, many of the more mature technology components have been consolidated into Identity Management (IdM) “suites”. Such suites are typically comprised of those services and elements that are broadly applicable to the vast number of constituents (employees, customers, suppliers and partners) for most small, medium, and large enterprises. Inclusive of elements such as User Provisioning and Access Management solutions, these suites serve as the core IdM infrastructure platforms for these enterprises. To date, many enterprises have deployed these IdM platforms, or significant subsets of, to realize benefits in the areas of regulatory compliance, reduction of IT operational costs and improved IT security.

In addition, vendors also continue to innovate in areas that are complementary, but adjacent to these “core” IdM services, spanning areas as diverse as strong authentication, enterprise single sign-on (eSSO) and physical access control. However, many of these peripheral technology solutions are not considered holistically with Identity Management from the perspectives of design, implementation, and ongoing operational management. While some suite vendors have indeed invested in making their individual products well-integrated, attention has not yet been paid to the interoperability and “inter-deployability” of those suites with the types of adjacent technologies mentioned above. This has resulted in a fragmented solution model for enterprises that aim to benefit from the joint deployment of “classic” IdM infrastructure in conjunction with other security technologies.

Oracle views the amalgam of IdM infrastructure and surrounding technologies as a single organic ecosystem with multiple touch points and inter-dependencies between the constituent components. The co-deployment of various elements of the ecosystem can yield multiplicative resulting benefits above and beyond those typically cited for core IdM suite solutions. Oracle is providing the underpinning

for this ecosystem through a combination of pre-packaged connectors, certification testing, and rigorous support for the relevant industry standards.

## **BUSINESS BENEFITS**

**The Oracle Extended Identity Management Ecosystem enhances the core IdM benefits of improved compliance, reduced costs, and enhanced security, while also introducing the new benefits of risk reduction and improved user experience.**

The value proposition for Identity Management has been built around three key areas: improved compliance, reduced costs and enhanced security. As described below, these same benefits can be further enhanced by expanding the scope of management for the IdM platform to include the other components of the ecosystem. In addition, the ecosystem also delivers added benefits by reducing the overall integration risk of co-deploying the various components as well as providing a more seamless user experience.

### **Enhanced Compliance**

IdM platforms provide a comprehensive framework for various compliance activities including access monitoring, point-in-time and historical reporting, and the periodic attestation (sometimes referred to as “re-certification”) of users’ credentials and entitlements. The value of this capability is further enhanced by the ecosystem due to the fact that the central IdM infrastructure is now providing an end-to-end view of all physical and logical access each user has, including the issuance and management of any strong authentication credentials issued to users for access to high-value and/or high-sensitivity applications and resources.

### **Reduced Costs**

IT cost reduction via IdM is primarily realized through the consolidation and automation of user management operations. In addition, consolidating access points through an Access Control solution reduces the number of places in the enterprise where each user’s identity has to be managed. User Provisioning further reduces costs by automating those touch points. The ecosystem builds on this benefit in multiple ways. Enterprise SSO solutions help to further consolidate the number of channels via which a user accesses enterprise systems and applications. Furthermore, when properly integrated, user provisioning solutions can greatly reduce the cost of deploying strong authentication to a consumer population.

### **Improved Security**

The ecosystem also augments the third key benefit of IdM solutions – by further enhancing an enterprise’s security profile. Strong authentication is an instrumental pre-requisite for exposing sensitive or high-value applications and is now a legal mandate for industry segments such as consumer banking. Integrating physical access systems into the IdM infrastructure extends the identity lifecycle umbrella to the point where a user enters a facility, long before even approaching the vicinity of accessing a secure system. In addition, it also enables more consistent enforcement of security policies across both physical & logical domains.

## Seamless User Experience

Through integration of perimeter security (physical and logical) with ESSO and the cored IdM infrastructure, the ecosystem reduces costs and improves security. Unifying the user experience from the perimeter to the desktop and into the business application infrastructure improves security by centralizing and automating user management and also reduces help desk costs by providing significantly more convenience to the end-user.

## Reduced Risk

Finally, the ecosystem reduces the overall risk of an enterprise IdM deployment. While many integration touch-points within the components of the ecosystem are based on standard interfaces such as LDAP and SPML, the reality is that most technology components need, at a minimum, to be configured in accordance with customer-specific requirements and pre-requisites, in order to interoperate properly. Schemas need to be adjusted or enhanced, vendor-specific settings need to be incorporated, and other site-specific considerations such as network settings need to be taken into consideration. The ecosystem mitigates this interoperability and deployment risk by testing, certifying, and supporting the interoperability of the various components. This translates into a smoother deployment and reduced ongoing operational risks and costs.

## COMPONENTS

The ecosystem is comprised of an enterprise's core Identity Management infrastructure as well as various surrounding technologies in the security arena. Taken as an aggregate, this overall extended IdM system provides end-to-end security services for the enterprise.

### Core Identity Management (IdM) Infrastructure

At the heart of a sound Identity Management deployment is the "classic" IdM platform comprised of a number of well understood components. These are technologies that have matured over several years and are now generally regarded as being baseline requirements for any enterprise. These areas are listed below and are expanded upon in detail in other white papers previously published by Oracle.

- Access Management
- Enterprise Single Sign-on (ESSO)
- User Provisioning
- Federation
- Directory Services
- Virtual Directory Services

**The Oracle Extended Identity Management Ecosystem is comprised of core Identity Management infrastructure components augmented by Strong Authentication, Physical Access Control Systems, and Network Security.**

## **Strong Authentication**

Strong authentication refers to any mechanism that verifies the identity of a user in a manner that is more reliable than using passwords. While this was traditionally used to refer to PKI-based authentication technologies, this segment of the industry has expanded in recent years to include other mechanisms such as low complexity two-factor mechanisms (e.g. pre-printed grids), biometrics, and one-time password (OTP) tokens.

The strong authentication transaction is seamlessly integrated with Oracle Access Manager (formerly COREid Access), resulting in the issuance of standards-based credentials upon the successful completion of the transaction. From that point forward, the user has the convenience of single sign-on (SSO) access to all the protected resources to which she has been entitled.

One of the historical drawbacks of strong authentication mechanisms was that it was logistically challenging to manage the process of getting the authenticator (the device or token housing the user's credentials) into the hands of the end user. Today, tight integration with User Provisioning solutions can assist with this, allowing an enterprise to extract the value, without incurring the costly administrative overhead.

## **Enterprise Single Sign-on (ESSO)**

Even with the ever progressing migration of applications to a web-based architecture, thick clients remain ubiquitous in most enterprises today. These applications contribute to increased management cost and security exposure within those organizations. ESSO solutions mitigate these factors by delivering increased convenience to the end user by further reducing the number of authentication challenges that they need to navigate over the course of a day. In turn, this results in diminished costs by drastically reducing helpdesk calls as well as the amount of administrative overhead involved in managing user identities.

ESSO tools are integrated into the ecosystem in two ways. From an administrative perspective, they are tied into user provisioning solutions via SPML interfaces such that when a user is provisioned with a resource, those credentials are also immediately propagated to the ESSO credential store via a secure channel. From a runtime perspective, when a user successfully authenticates to the ESSO solution, that authentication is also communicated to the Access Management tool, resulting in a smoother experience for the user during transitions from thick client applications to web-based applications, and vice versa.

## **Physical Access Control Systems**

Physical Access Control Systems (PACS) secure access to office buildings, data centers, and other corporate sites. Through interoperability with other technology components in the ecosystem, they can authenticate users via mechanisms such as smartcards and bio-metrics prior to granting them access to various facilities. Their

strength lies in the ability to control physical access in a very fine-grained fashion using parameters such as room, floor, location and time of day.

The key touch point for PACS into the ecosystem is User Provisioning. Many of the same criteria that businesses use to justify managing IT systems and applications through a centralized provisioning solution also apply to PACS. Indeed, it makes logical sense that when a user is initially onboarded into an enterprise, their physical access credentials be issued at the same time as their system accounts. More critically, when a user's relationship with the business is terminated it is vital to ensure that facilities access be terminated just as quickly and efficiently as logical system access. Robust integration with the provisioning solution also yields a compliance benefit by bringing physical access within the scope of compliance reporting and the attestation of internal controls.

### **SSL VPN Solutions (Network Security)**

With business travel and telecommuting on the rise, it has become imperative for enterprises to offer their employees remote connectivity in order to access corporate systems. SSL VPN solutions help manage the costs associated with delivering this capability in a secure and effective manner. By delivering the required client-side functionality over a browser SSL connection, SSL VPN solutions eliminated the need to have a dedicated VPN client on each desktop. When dealing with workforces that number in the thousands or tens of thousands, this reduction in desktop footprint can translate into significant cost savings from both initial desktop provisioning and ongoing management perspectives.

SSL VPN solutions are integrated into the ecosystem via directory services. They use standard LDAP connectivity to perform authentication and authorization transactions against pre-existing user objects within a directory. By leveraging pre-existing provisioning mechanisms that automatically enroll a user into a corporate directory, they can truly provide a zero-touch solution for providing enterprise connectivity to remote users.

### **REFERENCE ARCHITECTURE**

The reference architecture presented below illustrates the interaction model between the various components of the ecosystem. Since “classic” IdM components are generally well understood, they have been abstracted into a single logical entity. That entity is made up of numerous services including Access Management, User Provisioning, Directory Services and so forth. The context provided in the explanatory text following the diagram clarifies which specific service in the IdM “container” is being referenced.

One point that merits mention is that the ESSO infrastructure described is typically delivered as two components – a provisioning integration service and an optional strong authentication interface, with the latter typically integrated into the ESSO desktop client itself. The diagram has logically consolidated those as an external

## ORACLE IDENTITY MANAGEMENT COMPONENTS

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

**Oracle Enterprise Single Sign-On Suite** provides end-users with unrivaled convenience and uncompromised security through true SSO capabilities from network login through to application access

**Oracle Identity Manager** is a powerful and flexible enterprise identity provisioning and compliance monitoring solution that automates the creation, updating, and removal of users from enterprise systems such as directories, email, databases, and ERP.

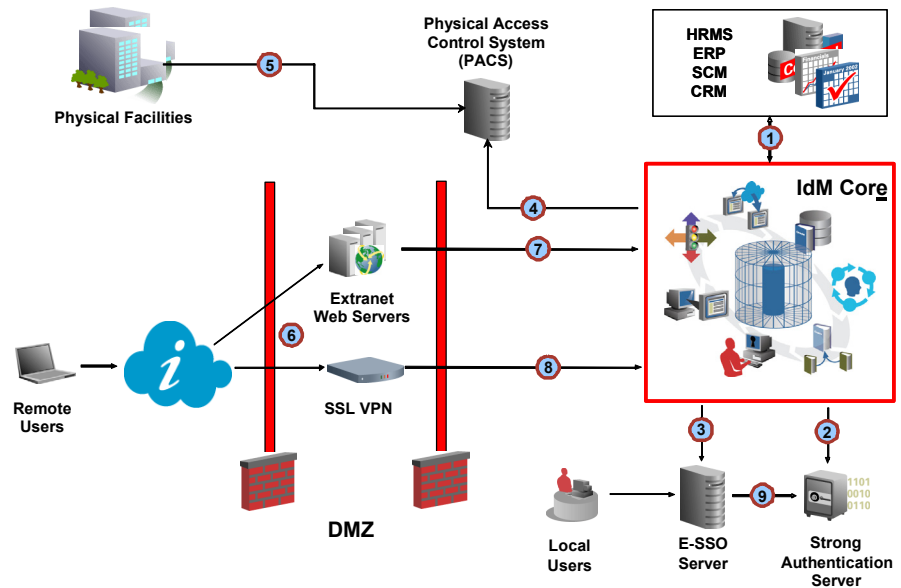
**Oracle Identity Federation** enables cross-domain single sign-on with the industry's only identity federation server that is completely self-contained and ready to run out-of-the box.

**Oracle Internet Directory** is a robust and scalable LDAP V3-compliant directory service that leverages the high availability capabilities of the Oracle 10g Database platform.

**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.

entity to the user desktop in order to better illustrate the functionality and connectivity that those components provide.

Finally, it is also important to note that the diagram illustrates the back-end wiring for the various components rather than the transaction flow from an end user's perspective. The latter is covered in more detail further on in this document in the section entitled "Use Cases".



**Figure 1 – Oracle Extended Identity Management Ecosystem Reference Architecture**

- 1) The IdM Core services interface with an enterprise's business infrastructure using a combination of proprietary APIs as well as standards such as LDAP and SPML. This channel is typically used to accept inbound messages regarding user lifecycle changes and also to manage the resulting user administration events back into the infrastructure.
- 2) This connection is invoked in two different scenarios. When a user is attempting to access resources requiring strong authentication, the Access Management server provides step-up authentication and interfaces with the Strong Authentication server to validate the user's credentials (biometrics, token-based certificates, grid authentication, etc.). In addition, it is also used by the User Provisioning system to manage each user's identity in the Strong Authentication system. The specific protocol depends on the underlying strong authentication vendor, but these interfaces are typically exposed via SOAP over HTTPS, with a vendor-specific schema embedded in the SOAP message.

- 3) The User Provisioning server communicates with the ESSO infrastructure using SPML to inform it of any changes in user access rights as they relate to logical system access.
- 4) The User Provisioning server communicates with the PACS infrastructure using vendor-specific APIs to inform it of any changes in user access rights as they relate to physical security.
- 5) When a user is attempting to access a secured facility, the card reader (or comparable technology) interfaces with the PACS infrastructure to validate the user's identity and access privileges prior to granting the desired access. This connection is typically proprietary to the provider of the PACS system.
- 6) All inbound connectivity from remote users is limited to HTTP and HTTPS. Remote access connections are typically forced to use HTTPS and connectivity for extranet-based applications can be HTTP or HTTPS based on the sensitivity of the content being served.
- 7) The connections from the web servers back into the Access Management infrastructure are normally proprietary to the Access Management vendor. In some cases they are invoked as web services (SOAP over HTTP) but are also implemented as proprietary calls via RPC in some instances.
- 8) When processing inbound requests for network access, SSL VPN devices, sometimes referred to as controllers, connect back to the directory service using LDAP. This channel is typically used at the beginning of the session to authenticate and authorize the end-user prior to granting her a network access session.
- 9) When the ESSO system has been configured to use strong authentication, this channel is used to validate the user's credentials. As with (2), this connection can be established in a variety of ways, but is typically exposed via SOAP over HTTPS.

## **USE CASES**

Many of the benefits of the ecosystem become more immediately apparent when articulated as use cases. While there are numerous combinations of use cases that are possible with the various components of the ecosystem, three representative cases are given below.

### **Use Case 1 – User Management**

One key area in which the ecosystem drives cost benefits in an enterprise is the user management process. By automating the mechanical tasks involved in user account provisioning, the ecosystem provides seamless user management while reducing the workload of the IT administrative staff. This is particularly true in the areas of strong authentication and physical access, which have traditionally not been integrated into the overall IdM process due to the complexity of the provisioning

process involved and due to the lack of robust provisioning connectors for those systems.

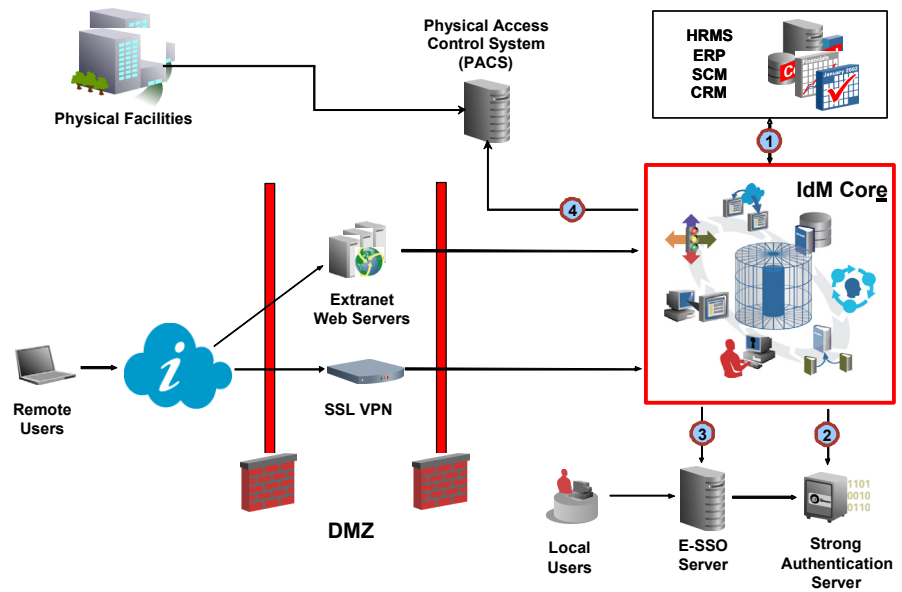


Figure 2 – Use Case 1

- 1) A user change event (creation, update, etc.) occurs in a source system, typically an HRMS, CRM, or SCM system depending on the user type in question. This change is propagated to the Oracle Identity Management infrastructure via SPML or some other mechanism depending on the vendor of the source system.
- 2) The user is provisioned with an account in the strong authentication infrastructure. This could be a token server, PKI, or any strong authentication mechanism. Depending on the mechanism(s) in question, the provisioning process can contain human interactions such as physical delivery of a token. If end-user interaction is required, for instance to support initial registration and enrollment scenarios in the case of biometrics or PKI based credentials, these can also be automatically initiated and completed without manual intervention on the part of an administrator.
- 3) The user's logical access profile is also propagated to the ESSO infrastructure via SPML. The profile is calculated based on provisioning rules pre-defined in the IdM core infrastructure.
- 4) Finally, the user is also granted access to all necessary physical facilities including offices, data centers, lab environments, etc. This can be done in a very-fine grained manner by limiting access to specific floors and rooms, as well as based on environmental parameters such as day of week and time of day. If necessary, the provisioning workflow can accommodate

human interaction steps such as hand delivery or shipment of a magnetic card or smart card for physical access.

At the end of this use case, the end user has immediately and automatically being provisioned with all appropriate elements of physical and logical access. No interaction from the part of a security administrator is mandated, although such can certainly be accommodated if required due to policy or procedural needs.

### Use Case 2 – End-to-end Access Control

The second use case revolves around delivering a seamless access experience for the end user. While many organizations consider this a benefit unto itself, delivering this level of convenience for the user population also results in enhanced security through reduction of credentials as well as lowered costs due to a reduction in help desk calls.

This use case assumes that an end user has already been appropriately provisioned as described in Use Case 1.

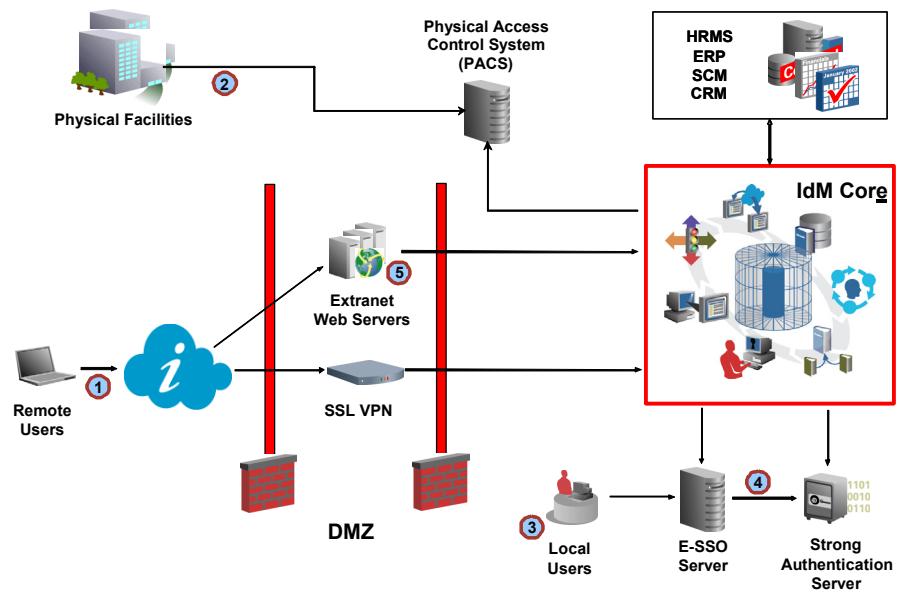


Figure 3 – Use Case 2

- 1) The end user is at a remote location and signs in locally to the ESSO client resident on her laptop. Once authenticated, she attempts to access the corporate network. The request is terminated at an SSL VPN device, which transparently authenticates the user against credentials already provisioned in the enterprise directory. After successful authentication, the user is permitted to remotely access her desktop.

Note: If necessary, a step-up request for stronger authentication can take place at this time.

- 2) Alternately, the user attempts to physically access her desktop by walking into the office at the start of a work-day. In this case, she is asked to “badge” into the location using one of a number of mechanisms. Potentially, this authentication can be via the same PKI/smartcard based that she uses to access other corporate resources.
- 3) The user is now at her desktop. If she had not previously authenticated to the ESSO client (i.e. her entry point was step (2) above), she is prompted to authenticate. If this was already done in step (1), no additional authentication is mandated to access her desktop. She now has access to her desktop-based applications.
- 4) Depending on her profile, she can optionally be prompted for stronger authentication. This can be accomplished in a variety of ways including smartcards, grid authentication, and biometrics.
- 5) Finally, if the user attempts to access web-based extranet or intranet resources, the ESSO client transparently brokers an authentication with the Access Management solution in the IdM core infrastructure.

At this point, the user has been asked to authenticate only once and optionally been requested for step-up authentication depending on her profile. With this one transaction, she has been granted access to the network, her desktop, and any thick or web-based applications to which she has been provisioned. This level of convenience significantly reduces the chances that she will make errors thus lowering the amount of support that she will require over time from the corporate help desk.

### **Use Case 3 – One-Touch / No-Touch De-provisioning**

While the final use case certainly has cost reduction benefits, it most clearly illustrates how the ecosystem helps tighten security and compliance. It involves the de-provisioning of a user upon the severance of the user’s relationship with the enterprise. Because the use case is most commonly initiated and concluded based on an administrative activity or a trigger from a business source system, it is commonly referred to as “one-touch” or “no-touch” de-provisioning.

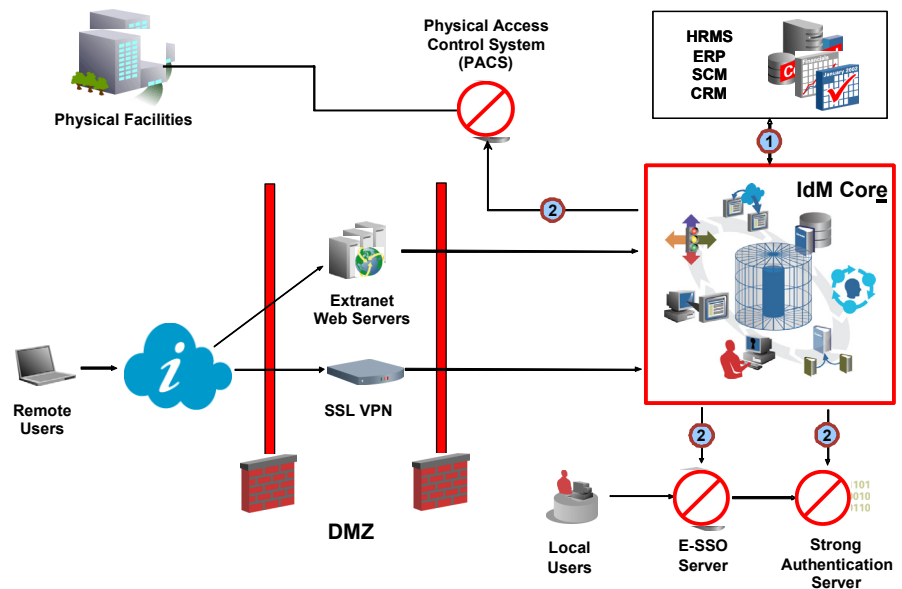


Figure 4 – Use Case 3

- 1) A user revocation event occurs in a source system, typically an HRMS, CRM, or SCM system depending on the user type in question. This change is propagated to the Oracle Identity Management infrastructure via SPML or some other mechanism depending on the vendor of the source system.
- 2) The user is automatically and instantly revoked from the entire security infrastructure including strong authentication systems and physical access control systems.

The cost reduction benefits are certainly obvious. Based on a single business event, the user has been instantly revoked from all access to business applications and security infrastructure without any manual intervention. However, the security ramifications are even more important. Even if a user is “in-session” with access to sensitive applications or data, he is immediately cut off from that access at the time when he may be most motivated to attempt malicious activity. Perhaps most crucially, all of this is centrally captured to ensure that at any time in the future, auditors can be given full visibility into when a user’s access was revoked and when it took effect.

## CONCLUSION

Many organizations of all sizes have already begun to realize the benefits of their cored Identity Management deployments consisting of directory services, Access Management, and User Provisioning. However, silos of security infrastructure comprised of elements such as strong authentication, physical access, and network security continue to be deployed and managed outside of the management framework of the core IdM infrastructure. These silos represent cracks in the

armor of benefits that IdM delivers and lead to cost leakage and lower levels of compliance and security.

The Oracle Extended Identity Management Ecosystem helps close these gaps by delivering testing, certification, and support of the interoperability points between those technology areas and the core Oracle Identity Management infrastructure. This results in enhanced benefit levels for the core value proposition for the Identity Management deployment. In addition, the ecosystem yields added benefits in the areas of risk reduction and improved user convenience by providing supported integrations and seamless user experience from the corporate perimeter all the way through to the use of business applications.

The end result for Oracle clients is a smooth Identity Management deployment that spans their entire business and security infrastructure leading to a more complete realization of the full potential of their IdM deployment.

## **ORACLE FUSION MIDDLEWARE**

Oracle Extended Identity Management Ecosystem Reference Architecture

July 2006

Author: Ranjeet Vidwans

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 © 2006, 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 Retek are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.