

# Customer Priorities in a Competitive Identity and Access Management Marketplace

---

Present and future enterprise needs in an  
increasingly identity-driven world

**Written by:** Alan Rodger

Published November 2006  
© Butler Direct Limited

All rights reserved. This publication, or any part of it, may not be reproduced or adapted, by any method whatsoever, without prior written Butler Direct Limited consent.

---

## ► INTRODUCTION

### Objectives of this White Paper

---

The purpose of this White Paper is to detail the range of customer functional requirements that may need to be addressed by the organisation's choice of Identity and Access Management (I&AM) solution, highlighting those of greatest importance and business benefit, along with other ownership considerations that Butler Group believes customers should assess. It discusses how Oracle is placed to meet these needs, in the context of today's fast-changing and competitive I&AM market place, and (where solutions are particularly differentiated) compares the capabilities in the Oracle solution with those of other key identity management vendors in the market place, and with the functionality available from the open source software sector.

### The growing extent of requirements for identity-based access

---

In recent times, the management of application access has grown in importance for most organisations. While this capability has long been a fundamental need, in the modern business and IT landscape it has become a key enabler for strategic considerations such as integration (within organisational boundaries, and outside them), increased efficiency, structural flexibility (without the addition of associated cost), and security.

Organisations face a proliferation of application access needs, and at the same time a greater imperative than ever to ensure that such access is only available on a controlled basis of proven user identity. Web delivery of applications, allowing remote access to users within and outside the organisation, greatly multiplies the number of users whose identities have to be managed, and also adds a need to manage those non-corporate identities in different ways. As organisations generally increasingly realise value to a greater extent from outside partnerships of all kinds, their ability to manage relationships via identity is a key capability that must be efficiently operated.

The greater range of requirements that need to be addresses has led to Identity and Access Management (I&AM) solutions being significantly extended in scope in recent years. Many market leaders have extended or acquired functionality in order to offer a suite-based approach to customers. The scale of investment and commitment to adopt these solutions have been a challenge to prospective customers in some cases, but ultimately these factors also determine how value can be driven from I&AM into their organisation.

In technical terms, challenges in considering an integrated I&AM approach arise from infrastructure heterogeneity, and the range of asset types (such as applications) with which I&AM solutions are required to integrate. Primary business requirements, meanwhile, can vary from centralised control (for efficiency), to delegated control (for flexibility); commonly include automated control to avoid management costs; and in many cases include 'future-proofing' to cover off the need to cater for Web services, and the plethora of 'trusted identity' arrangements.

## ► CUSTOMER FUNCTIONAL REQUIREMENTS

The move to Internet based business processes and an increasingly collaborative framework means that it is not a question of if, but when enterprises must implement security solutions that are based on the principles of identity and trust. This drive will affect all organisations both large and small, but the enormous diversity in the levels of maturity, scale, and degree of legacy IT involved will offer them different priorities and challenges, and will make some solutions more appropriate than others.

Regulatory compliance will be a major driver for many, but the efficiencies that can be gained from better management of identities (and their corresponding access rights) can constitute a significant financial benefit, and simply improving ease of access to a large number of available services and applications can also have time-saving benefits.

This section looks at requirements in the major functional areas of end-to-end I&AM solutions, some of which are illustrated by Figure 1, in the context of the many actors and business operations around I&AM.

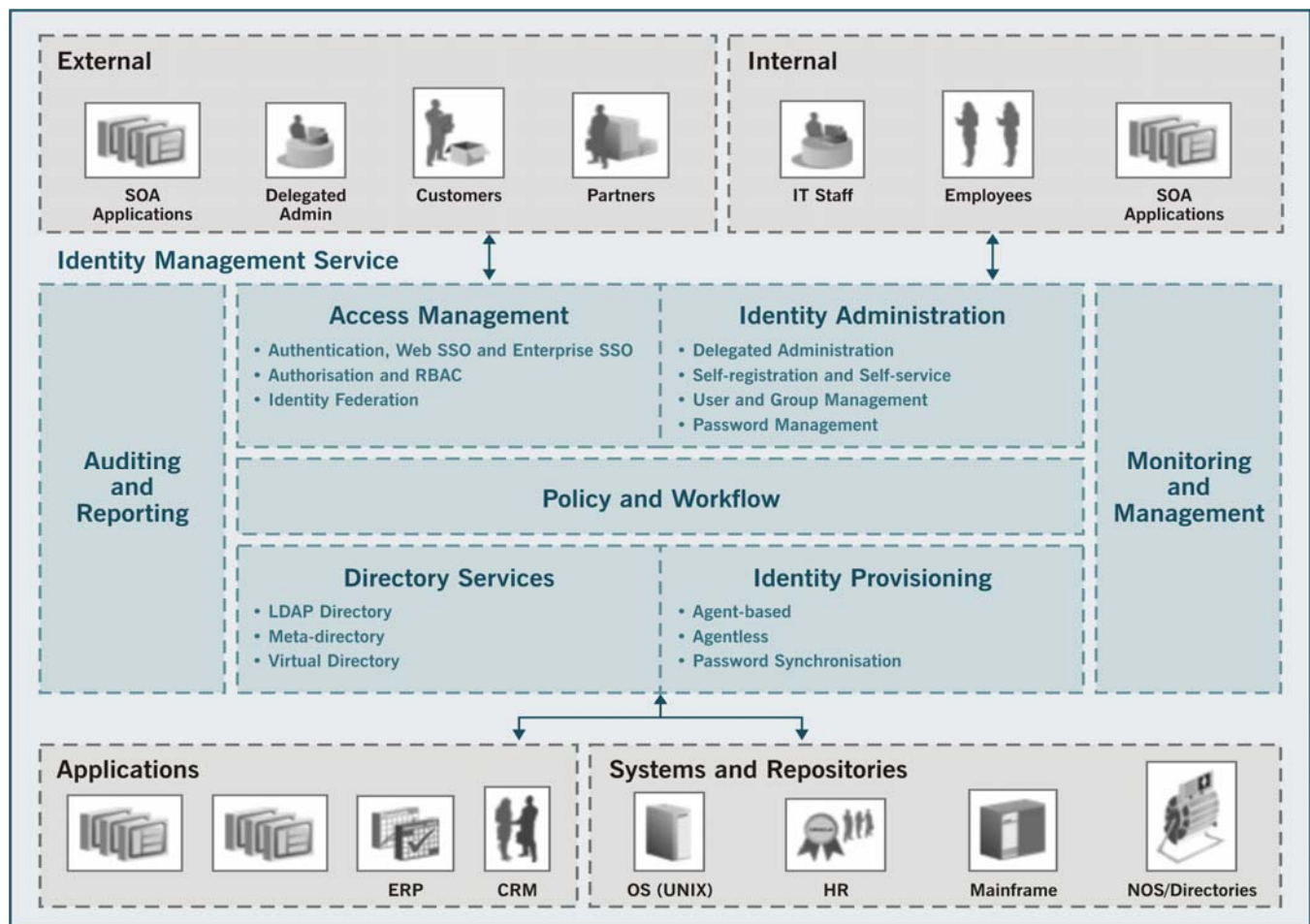


Figure 1: I&AM in the Enterprise Context

## Identity Management

The primary purpose of identity management functionality is to provide facilities and processes to store and manage the identities of valid users who are allowed access to information held within organisational systems and networks, but at a high level it fulfils a dual role as both an enabler and guardian of business and information.

Organisations cannot operate effectively without having the ability to control who and what is able to access their network infrastructures and business systems, and many now have to be able to report on this information on a current and historic basis for compliance purposes. While organisations must be able to demonstrate (and indeed prove) that their identity management controls meet both the access needs of authorised users and the protection requirements of the information stores that they are trusted to protect, at the same time enabling real-time, cross-enterprise access for valid users is critical in order to support business operability. The ideal for identity management is to deliver that balance between the needs of authorised users for open information access and enterprise information privacy.

Identity stores must offer security for protection of the information, and flexibility and scalability to accommodate change. For many organisations, the evolution of systems and applications has seen identity stores established in disparate locations, and quite likely underpinned by different technologies – often, part of the identity management challenge is to integrate identity stores so that they can be used as one resource. As well as technical integration to enable communication across technologies, this can involve data integration, for example to define how duplicated data should be resolved (e.g. which of two applications' databases holding 'address' should be viewed as the definitive source).

Within many organisations the range of platforms, systems, and networks is itself a challenge to simple technical integration, let alone that of complex data like identities. The use of directories that use Lightweight Directory Access Protocol (LDAP) protocol can solve all such problems jointly. Functionally, LDAP involves the use of standard protocols that enable any entity to be easily located within the directory hierarchical structure, for example the location of individuals, groups, departments, and organisations, etc., plus other resources such as files and devices in a network, irrespective of where such resources are located on the public Internet or corporate Intranets. I&AM systems should be able to integrate identities and resources held in multiple LDAP instances, and control access to a range of infrastructure element types such as databases, operating systems, application platforms, and Web servers. 'Virtual' directories can provide particular flexibility in addressing this requirement to integrate information from individual LDAP instances, achieving aggregation without moving or restructuring the base data. They can also provide additional abstraction between application and directory layers, an important feature underlying many of the most up-to-date enterprise applications.

Additionally, solutions need to provide, or enable to be established, a strong set of processes to manage identity data, including complex elements such as groups, and organisational role structures, that allow particular value to be gained from I&AM functions.

## Password Management

---

Passwords are the most well-established and best-understood solution to the problem of how a user can prove his claim to an identity when presenting credentials to a system or application, via the combination of username and password. However, the variations in password formats within enterprise systems, and the number of passwords that users have to remember, are the root cause of one of the biggest headaches (and financial pressures) that organisations currently face around identity – that is, users forgetting or mislaying their passwords.

When the mostly common approach adopted to this problem by users themselves is to write these passwords down where they are easily accessible, the strength of security provided plummets due to the password (and therefore the consequential access rights arising from the user's identity) being freely available. The security industry's most common illustrative tale is of consultants hired to look into security issues walking into offices where users' computer screens are festooned with Post-it® notes inscribed with all their passwords. However familiar this is, it demonstrates how easily compromised passwords can be, and therefore what a weak link they are in the chain of protection.

Many organisational users have access rights to a number of systems, and commonly each might require the user to present a password. If the user could choose one password, and only had to remember that each time he had to log-in to a system, the problem of forgetting passwords could probably be overcome (although the difficulty would be that individual systems force password expiry in different cycles, and changing one would involve the user changing all to maintain consistency). In any case, password systems have evolved in various ways throughout the history of software development, and many different password formats are mandated throughout organisational IT estates, so it is hard to envisage the option of choosing a single password being available.

The variations in password formats, which combine to form a password policy, can include:

- Passwords of different lengths, and also restrictions on variable or fixed length.
- Different limitations on format, such as repeating groups, and adjacent duplicate, or consecutive characters.
- Numeric or alphabetic character positions and sequence.
- Character case (lower, upper, or if mixed perhaps with fixed positions).

Despite strong passwords being intended to deliver strong security, those that are too strong (i.e. complex) can become very difficult to remember and then have to be written down, critically weakening security. Conversely, passwords that are too weak can easily be guessed, with the same result as for over-strong ones. Although the apocryphal Post-it note is an extreme example of its effect on security, any degree of personal information management becomes an overhead (and is increased by multiple passwords), and can to some degree compromise security.

## Provisioning and De-Provisioning

In broad terms, provisioning is really the point at which identity management and access management meet, and commonly involves any processes that organisations require in order to pre-determine the availability of access rights. Many organisations see provisioning as very much part of business processes, and an increasingly popular requirement is for it to deliver responsibility for the distribution and control of access rights into the hands of responsible end-users. Efficiency and timeliness were early factors motivating this shift away from IT departments or help desks controlling access rights, and recent estimates still quote waiting times of up to three weeks for new accounts to be activated within some organisations that haven't implemented an automated I&AM solution. However, for many organisations these drivers have been surpassed in importance by regulatory compliance. For example, the US Sarbanes-Oxley legislation requires organisations to be able to demonstrate strong management of the appropriateness of users' automated access rights to applications and assets, and as this requires business management insight into employees' roles (and awareness of how those roles, and organisational structural, change periodically) it is likely to be less effectively and accurately handled if managed by anyone other than the person(s) directly responsible within the business.

Provisioning is a means of implementing an identity lifecycle for users, and an important stage of that lifecycle is when a user leaves an organisation, when de-provisioning of the user's access rights needs to be undertaken. Even short-term employees or associates may have been granted login access to numerous systems or applications, and over a number of years many organisations grant access rights that are never revoked in a timely manner when users' roles change. In any event, there is a significant risk in allowing access rights to remain valid after users are no longer employed, as there may be circumstances involved in the discontinuation of their employment that lead to ill-feeling being held against the organisation, when those access rights might present an opportunity for individuals to harm the organisation's interests or assets. Butler Group recognises as valuable one estimate that between 30% and 60% of user accounts in many organisations exist without justification, applying to users whose roles no longer require the relevant access, or who are no longer employed.

In the area of provisioning there is a particular requirement for workflow, so that automated processes can be integrated with other systems to meet end-to-end business needs. Often, for example, an HR department's processes could be the initiator of an event relating to provisioning needs. Many organisations extend the value of identity by combining individuals into groups representing organisational structure, which often correspond to the need for similar access rights. Most enterprise-strength I&AM solutions allow roles also to be used as a basis for assigning rights, and in some cases to validate that users' access rights are in line with the needs of their position (a requirement that the Sarbanes-Oxley legislation brands as 'segregation of duties').

---

## Authentication

---

Although passwords have long provided an easy means of establishing the identity of a user, they suffer from being a weakness in security systems, as they are easily compromised by the foibles of human choice (of passwords that can easily be guessed) and behaviour (e.g. due to being written down accessibly). They can form part of a more secure system if used as only one of multiple means of authentication, an approach known as multi-factor authentication. There are basically three types of authentication: something you know (a password being an example), something you have, and something that you are. The second of these manifests in the form of something that a system can verify and that can be registered as associated with a particular user – an example is an electronic token, or a uniquely identifiable smart card. The third is normally an electronic record of a personal biometric, against which a user can present himself as the credential that matches the registered biometric.

There are numerous factors to take into account when choosing which methods of strong authentication is suitable for a user population, of which the relative costs, and the appropriateness of authentication methods to environmental and human user conditions, are primary considerations. Organisations determining their approach to I&AM should bear in mind the value of the greater strength of multi-factor authentication, and ensure some readiness to adopt this in future – this is particularly important if the popular SSO approach is likely to be implemented, as in this framework a user has only to authenticate successfully once to gain access to all resources available to his identity.

A variety of authentication technologies have important roles to play in extra validation of users' login or access attempts, in addition to passwords, against the recorded identities of *bona fide* users. These include hardware tokens, smartcards, biometrics, Public Key Infrastructure (PKI) digital certificates, and Virtual Private Networks (VPNs). Organisations should be aware of the need to maintain flexibility to adapt or change the authentication methods in use as circumstances and technology change, and avoid tie-in to particular technologies. Additionally, the convergence of authentication being leveraged jointly to enable physical access to premises, as well as 'logical' access to IT resources, is likely to provide opportunities for many organisations to increase security and reduce risk.

---

## Access Management

---

Access management is the real-time enforcement of application security using identity-based controls, and provisioned access rights. As such, the assurance of performance in delivering these services becomes important, and the ability to provide access across a wide range of resource types is a key capability. To achieve this across disparate platforms, solutions adopt a variety of approaches such as deploying agents on target technologies, or using standards-based authorisation via Security Assertion Markup Language (SAML). For the normal range of business applications, application access via Web browser, portals, or client screens on different desktop platforms must be catered for, and also the various interface types that legacy applications allow. Organisations should also assess their requirements for access to Web services functionality, in order to ensure that potential needs are fulfilled by an I&AM solution of choice.

---

## Enterprise Single Sign-On

---

Enterprise SSO enables the user to be removed from the role of remembering and managing passwords to multiple enterprise systems, abstracting this instead to an automated system of password management. Users only have to remember their primary password, so because passwords for back-end systems do not have to be used by people when users have SSO, the passwords to those back-end systems can be as strong, complex, and unintelligible as necessary to maintain strong security without causing any overhead. Effectively, passwords to back-end systems ('secondary' passwords, in the parlance of SSO) can become 'zero-touch' passwords, automatically generated within the password management system but never seen by any user, and forming a very strong solution from a security standpoint.

The Enterprise SSO system has to automate several functions in place of the user's involvement:

- Remember the password that is relevant to each application.
- Know the account in each application that is relevant to the user.
- Recognise when the password is requested, and present it to the application seamlessly without user involvement.
- Cater for events in the password lifecycle (see Figure 2).
- Handle passwords for each application as appropriate to the policy, throughout the lifecycle particular to that application.

SSO must be integrated with password management to enable the storage and retrieval of passwords. Often this is centralised, with a directory as the platform, with its on-board facilities for resilience, scalability, and security, but some solutions base password information in local storage (under strong encryption, to ensure its integrity) that is synchronised with a central repository.

Legacy back-end systems with group log-ins (e.g. 'Financedept'), rather than individual user names, must be eliminated when undertaking formal password management. Such log-ins would render synchronisation of passwords impossible as multiple single-user identity definitions in the central system could not be mapped to such a group credential. In any case, organisations in the many industries in which increased legislative and regulatory pressures are brought to bear on operations would be aware of the compliance implications of allowing access rights to be inaccurate (and therefore unaccountable) identities.

In contrast to the considerable variety of password formats that occur, the lifecycle of password information is normally straightforward (see Figure 2). Systems allowing registration of users would enable a password to be generated (or validate the entry of a user choice), and later repeat this stage upon the password's expiry. Enterprise SSO solutions must be able to handle these processes and events arising from multiple back-end systems and applications.

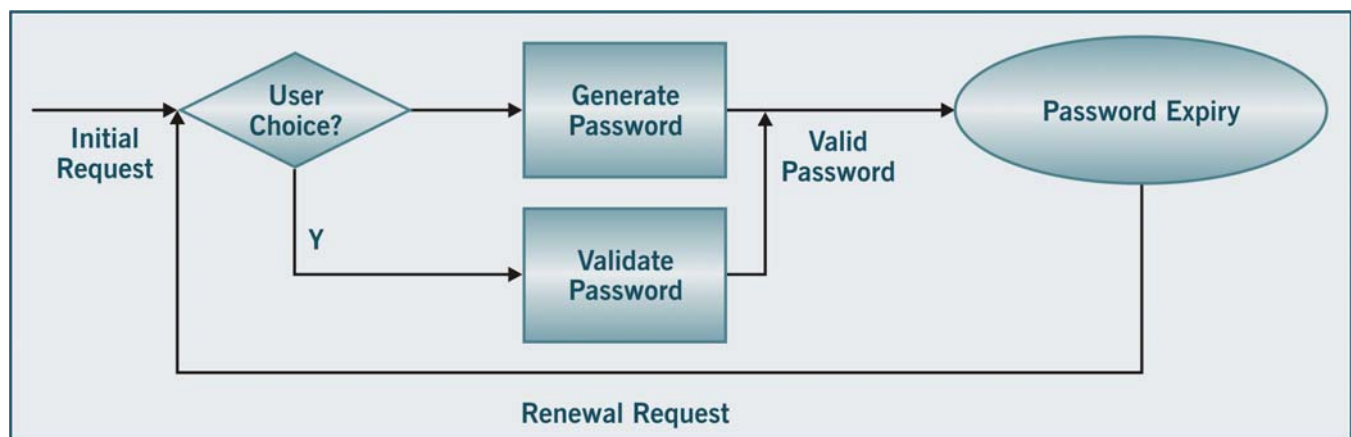


Figure 2 – The Password Lifecycle

## Web Single Sign-On

Enterprise SSO commonly caters for users whose identities are defined within the organisation, but while totally unknown users might be justifiably treated completely differently to those within the organisation, sometimes the boundary is blurred by the need to provide identity-based facilities to users from partner organisations (such as suppliers), or to personal consumer customers. This may bring a requirement to extend SSO to these users, this often being achieved via an external enterprise network (e.g. using a portal, hence the term Web SSO). External users' identities are usually stored separately to those of users defined within the enterprise, this being particularly appropriate due to the differing access requirements to the respective identity sets – the identities of individual external users are often maintained by the users themselves, while those of internal users are subject to management control (partly for purposes such as regulatory and legal compliance).

It is increasingly common for organisations working together in partnership, or linked by a relationship such as that of supplier-customer, to use Web-based access to allow users to leverage the partner company's applications. This can be achieved using Web SSO, although in theory greater efficiency is available via a federated approach, as it enables duplicated identities and associated maintenance to be avoided.

## Federated Identity

---

Identity federation allows a user's identity in one domain to be used to gain access to resources in another domain without the need for separate authentication. Usually a particular close business relationship, or basis of trust, would be involved as the foundation for providing access across network boundaries between distinct organisations, although consumer-facing e-commerce is also an appropriate application for federation. Using federated identity, users can present a single set of identity and authentication information to access applications and services across multiple technical domains, organisational boundaries, and distributed, heterogeneous networks. In theory savings can be made via a federated approach, as it enables duplicated identities and associated maintenance to be avoided – however, many organisations would not yet be at a stage of managing their identity information with sufficient maturity, which should be considered a prerequisite.

## ► SOLUTION OWNERSHIP REQUIREMENTS

Not all factors in assessing solution options can be assessed by comparison against potential customer organisations' business, and this section outlines a number of examples. Butler Group believes that organisations must apply judgement rather than entirely empirical reasoning in making conclusions from consideration of such factors. Nevertheless, any of these factors can be as important as the fit with individual business or technical requirements in affecting the overall customer ownership experience resulting from a buying decision.

In order to consider the information appropriate to these factors, prospective customers should seek to understand the vendor's overall portfolio strategy, the product development strategy as an element of the portfolio strategy, and the degree of commitment to extending and supporting the solution within the vendor's overall portfolio. Additionally, the maturity of solutions' product elements, and any architectural restrictions inherent within products should be investigated.

Butler Group believes that the following considerations relating to prospective ownership of I&AM solutions are amongst the most important for all types of organisation.

### **Range and comprehensiveness of functional requirements coverage**

Adoption of I&AM solutions is increasingly being seen as a strategic decision, and Butler Group believes that most organisations will extend the scope of their initial implementations. In assessing their long-term approach to I&AM, organisations should take account of the likelihood that the availability of end-to-end functionality from one vendor, across the range of functional requirements, could well reduce the total time and cost spent on integrating parts of a deployed solution, as compared to adopting products from multiple vendors. All the major vendors can deliver a broad range of capabilities that meet the end-to-end needs of many organisations, but the emphasis and background is somewhat different in each case.

### **Strategy relating to I&AM**

Oracle and its major competitors have all acquired functionality extensively in the last few years to broaden their coverage of the range of customer I&AM requirements. Customers need to be satisfied that solution elements are well-integrated, and from the point of view of assurance of further product development that the vendor they choose sees I&AM as central to its strategy, rather than a product area that might be neglected in times to come.

### **Supplier channel strategy and execution**

While this is not an area where vendors can satisfy requirements directly, we feel that customers must be aware of how suppliers approach the market, and be satisfied that they are not disadvantaged by any lack of focus on their own market area.

## ► PROFILE OF ORACLE IDM SUITE

### Products and Capabilities

---

Oracle IdM Suite is comprised of the following components:

- **Oracle Access Manager**, which provides a wide range of identity management and security functions, including: Web single sign-on (SSO); user self-service and self-registration; reporting and auditing; policy management; dynamic groups; and delegated administration.
- **Oracle Identity Federation**, a standards-based solution that enables authenticated users' sessions to be allowed access across business domains.
- **Oracle Identity Manager**, a functionally rich user lifecycle, password management, and compliance automation solution that supports out-of-the-box integration with a variety of heterogeneous resource types.
- **Oracle Virtual Directory**, which enables an integrated view of disparate identity stores.
- **Oracle Internet Directory**, a highly scalable identity store that combines Oracle's relational database solution with a Lightweight Directory Access Protocol (LDAP) server, and also incorporates meta-directory capability.

Complementing IdM Suite, and completing its provision of end-to-end functionality across the entire range of I&AM requirements, is the leading Enterprise SSO solution, v-GO Single Sign-on Platform (from Passlogix). After a prolonged period in which its customised integration with Oracle I&AM products has matured, this is now offered as an OEM'd product by Oracle, known as **Oracle Enterprise Single Sign-On**.

Oracle Access Manager provides an extensive range of features including: policy management that can cover authentication, authorisation, and auditing; management of multi-level, multi-factor authentication; password administration, including self-service facilities; delegated administration; a workflow engine; and Web services interfaces. The product's identity management functionality allows structured and delegated management of identity, including group, roles, and organisation elements, which can be managed by the individuals that are responsible for individuals' rights, rather than a centralised authority. With this release, password management functionality has been enhanced to provide improved challenge-response features around password reset, better checks on password quality, and tracking of the user's last login time stamp.

For Web SSO, the product provides a WebGate module that is installed on the Web server. This directs a user's access request to an Access Server, which checks the user's log-in credentials against the attributes held in the directory. When application credentials are granted they are passed as a 'session-only' cookie to the user's client, and this allows the user to pass through the WebGate subsequently to the application server and onto the underlying applications.

Oracle Identity Federation is a standards-compliant means of achieving SSO and identity sharing between partner organisations. It can deal with identity claims based on all of the prevalent standards – Security Assertion Markup Language (SAML), WS-Federation, and Liberty Identity Federation Framework (ID-FF), and is available in packages that support the service provider, or identity provider, roles within the standards' frameworks. Its deployment options can facilitate a system that is either integrated with the rest of IdM Suite, or is usable stand-alone, and additionally comes with a development toolkit to allow custom integration with applications, as well as a utility that helpfully sets up account linking in bulk as preparation for federated identity sharing between partner organisations.

Oracle Identity Manager enables user accounts, user profiles, and corporate policies to be managed via user self-service (where appropriate), or by administrators, with authorisation to functions depending on dynamically controlled access rights. It allows management of access to technologies and resources from across the heterogeneous IT environment, and includes features to extend this range from its extensive out-of-the-box range of target environments by enabling customer definition of integration with additional systems.

To build these features into meaningful business processes, the product provides workflow management features that enable definition and deployment of manual (e.g. approval), or automated (e.g. execution of an Add User adapter), identity administration tasks. It can control synchronisation of passwords across systems, including bi-directionally, and password policies relating to resources under management can be defined to, and enforced by, the product. Recent enhancements include scheduled or event-driven logging of the information defining users' identity, and access rights, with configurable data capture and reporting options, as well as an attestation framework that supports compliance requirements by enabling periodic automated review of access rights by responsible parties such as organisational management.

Oracle's Virtual Directory provides standards-compliant LDAP and XML views of existing enterprise identity information without the need to synchronise or move data from its native locations. The product is based on Java and Web services technology, and offers a means of achieving real-time directory integration within identity and access management (I&AM) systems, and reducing development costs as compared with more complex solutions. Recent development has seen its reporting and auditing features enhanced, and new Wizard-based definition of management for Active Directory environments.

Oracle Internet Directory is underpinned by the company's relational database solution to store data relating to identity and access, while implementing a LDAP view to facilitate integration with non-Oracle I&AM solutions, and indeed the rest of the IdM Suite. The product's heritage is as the identity repository for Oracle application products, but its development is ongoing and most recently has seen the addition of a Java extensibility framework to further facilitate integration.

The suite also includes a reporting engine, which incorporates definitions of a number of standard reports as well as facilities for customers and other third parties (e.g. services partners) to define customised reporting requirements. Standard reports include current and historic access mapping to identity, extending to role-based analysis, and compliance exceptions. The suite overall can optionally be configured to support audit and reporting requirements in a separate database to operational data, which in Butler Group's opinion is a well thought-out aid to performance improvement. The current release supports localisation of a customer's I&AM deployment in 28 languages.

Each of the products can be deployed independently, and do not depend on other Oracle products. IdM Suite is certified on the following platforms, in multiple combinations such as:

- Application Server – Oracle Fusion Middleware, BEA WebLogic, IBM WebSphere, and JBoss.
- Operating System – Windows Server, Red Hat Linux, Sun Solaris, IBM AIX, and HP-UX.
- Database – Oracle, Microsoft SQL Server, IBM DB2 UDB.
- LDAP – any LDAPv3-compliant server e.g. Microsoft AD, Novell eDirectory.

Legacy platform integration is provided for provisioning and access control, within both the Oracle Access Manager, and Oracle Identity Manager products. The latter ships with out-of-the-box connectors to myriad mainframe security systems, including RACF, ACF2, and Top Secret. These connectors leverage a Java Host API to perform remote invocation of commands to these targets, which are then locally executed via terminal emulation. Identity Manager also supports Advance Mainframe Connectors, which are agent-based and provide much more richly functional and fine-grained integrations to those environments.

## Analysis

---

Oracle positions IdM Suite's elements more as capabilities than as products, suitable for the wide range of customer scenarios that arises with respect to I&AM. Intense acquisition activity (mostly during 2005) brought most of these anew into the Oracle fold. Oracle Access Manager, and Oracle Identity Federation were acquired with Oblix (although capability from the previous acquisition of Phaos also features in the Federation product); Identity Manager with the acquisition of Thor Technologies; and Oracle Virtual Directory from OctetString. The constituent products have particularly notable heritages of features supporting Web services, which Butler Group views as a differentiating strength: Oracle's recent developments and roadmap indicate that it will continue to leverage and extend these.

In Butler Group's opinion, all the acquired technology was considered to be of market-leading standard, hence the foundation of the suite is one of exceptionally high-quality and well-featured products. Together, they address the entire gamut of I&AM business and technical requirements that we believe organisations should be considering, for deployments currently and in the foreseeable future, and do so in a manner that enables identity-based security to be driven into the heart of applications and their environments, rather than by adding an external layer.

We have identified particular strengths throughout the suite with respect to capabilities that readily facilitate integration with an extremely wide range of applications and other IT resources in heterogeneous environments. The range of target environments provided is a potential cost saving in the increasingly common circumstances where organisations have to cater for new integrations arising from restructures, mergers and acquisitions, or business partnership opportunities – the integrations are characterised by Oracle as 'hot-pluggable', emphasising their ready availability. Significant added value is provided by the depth of functionality that Oracle includes – rather than merely ironing out the technical difficulties, the integrations incorporate added business value by providing links out-of-the-box into detailed functionality within a wide range of leading applications.

## ► COMPARISON OF HOW SOLUTIONS ADDRESS FUNCTIONAL AND OWNERSHIP REQUIREMENTS

### Introduction

The purpose of this section is to provide a detailed comparison of the features of Oracle IdM with those provided by the competing solutions from CA, IBM, and Sun, and within the open source market place. Each set of features is grouped by the category of requirements that it addresses, as detailed in the earlier Customer Functional Requirements section.

Similarly, a comparison of those vendors is included from the point of view of the Solution Ownership Requirements that were outlined in a separate earlier section.

### Identity Management

To store data relating to identity and access, Oracle offers Oracle Internet Directory. Underpinned by the company's relational database solution, it implements an LDAP view to facilitate integration with non-Oracle I&AM solutions, and also incorporates meta-directory capabilities. The Oracle Identity Manager product provides a best-in-class range of support for identity management use cases. Additionally, Oracle Virtual Directory provides standards-compliant LDAP and XML views of existing enterprise identity information, without the need to synchronise or move data from its native locations. This product, acquired from OctetString an acknowledged leader in its area, is based on Java and Web services technology, and offers a means of achieving real-time directory integration within identity and access management (I&AM) systems, and reducing development costs as compared with more complex solutions.

Oracle's directory products provide compatibility with an extensive range of identity stores, database platforms, and heterogeneous environments. They also demonstrate extremely impressive, proven scalability credentials. For example, a major telecommunications company chose Oracle Internet Directory as the platform for over 60 million users' identities, in instances distributed over six locations, supporting complex operations that include each user's authentication performing six write operations to the identity store. Further demands on this implementation include replication of each directory instance's changes within the group, providing resilience. Another example is that of an on-line gaming company that uses a clustered deployment of Oracle Internet Directory against a deployment of Oracle databases, supported by Real Application Cluster, not only to ensure maximum availability, but to support the peak demands of up to 1.1 million users, a population which forecast to grow to 10 million. In both these customers' cases, Oracle's solution was chosen over that of Sun.

---

## Password Management

---

Oracle Identity Manager offers advanced password administration facilities, including self-service password reset facilities (with customisable challenge-response features), strong checks on password quality, and tracking of the user's last login time stamp. The product can synchronise or map passwords across managed resources and enforce differences in password policies among these resources. Additionally, complexities such as Microsoft Windows' desktop-based password reset feature are dealt with, as Oracle Identity Manager's Active Directory (AD) Connector can intercept password changes at the AD server and subsequently propagate it to other managed resources in accordance with policies. Similar bi-directional password synchronisation capability is available in Oracle Identity Manager Connectors for most directory servers and mainframes. One Oracle consulting services customer has attested to cost savings of US\$750,000 per year via increased efficiencies from using Oracle's password management solutions. Another major financial services customer, having selected Oracle over both CA, and a niche supplier, for its password management needs, has attested to savings of US\$8.4 million annually, reducing the number of password resets by more than 35,000 per month on average.

Additionally, while both IBM's and Oracle's I&AM solution sets include v-GO, the market-leading Enterprise SSO product from Passlogix, as an OEM'd element that incorporates extensive password management features, only Oracle has completed extensive integration, incorporating this as Oracle eSSO Suite, and offers its full range of features for a very competitive per-user price.

---

## Provisioning and De-Provisioning

---

Oracle Identity Manager enables user accounts, user profiles, and corporate policies to be managed, as well as access to technologies and resources from across the heterogeneous IT environment. It includes features to extend the support of over 100 target environments from its out-of-the-box range, by enabling customer definition of integration with additional systems. To build these features into meaningful business processes, the product provides workflow management features that enable definition and deployment of manual (e.g. approval), or automated (e.g. execution of an Add User adapter), identity administration tasks. It can control synchronisation of passwords across systems, including bi-directionally, and password policies relating to resources under management can be defined to, and enforced by, the product. Oracle has added particularly differentiating features in that its provisioning platform offers auditing features, which address compliance requirements very strongly. Additionally, Oracle's partnerships around converging physical and logical access solutions will enable efficiencies to be driven through the integration of provisioning the access rights to the two types of systems.

Oracle Identity Manager ships with out-of-the-box connectors to myriad mainframe security systems, including RACF, ACF2, and Top Secret. These connectors leverage a Java Host API to perform remote invocation of commands to these targets, which are then locally executed via terminal emulation. Identity Manager also supports Advance Mainframe Connectors, which are agent-based and provide much more richly functional, and fine-grained, integrations to those environments. A top-tier global financial institution chose Oracle solutions because of their ability to provision over 800 applications in a highly complex, heterogeneous environment – this is believed to have a greater number of applications under management than any other known I&AM implementation. Oracle's major competitors also aim to address the same functional goals, but amongst them only IBM has as strong a focus as Oracle on providing ready integration for provisioning operations with a wide range of heterogeneous environments. The capabilities within Sun's and CA's solutions do not compare favourably, and there are no viable open source solutions in this functional area.

---

## Authentication

---

IdM Suite is positioned as a pillar of Oracle's Fusion middleware, and the suite will also leverage some advantages of being part of that wider family; for example, support for strong authentication, and Public Key Infrastructure (PKI) – including the option to set up a Certificate Authority – is already built into Oracle Application Server. Oracle has established what it calls an Extended Identity Management Ecosystem, which widely extends the value available from strong authentication, and within which Oracle has partnerships with leading suppliers of both physical access and network control solutions, with specific integrations being available in both areas. Oracle Access Manager offers strong, policy-based management of multi-level, multi-factor authentication, and can enable self-service management and delegated administration, where organisations consider this appropriate.

IBM provides support for strong authentication methods within its two separate access management offerings for enterprise, and external, users. CA mirrors this capability in its SSO, and SiteMinder offerings. Sun resells a third-party solution that extends the support (from that within Sun's own software) for authentication. Two-factor authentication is supported by a few open source offerings, but these do not support other I&AM requirements, or offer integration with products that do so.

## Access Management and Web Single Sign-On

---

Oracle Access Manager is a policy based access management solution that enables Web SSO to be achieved very elegantly, via a Web server-based module that initially deals with a user's credential presentations, and after authentication subsequently passes through requests straight to applications. It also extends its value to protecting access to Web services, as it provides a Web service interface which allows the business logic governing the identity administration to be integrated with applications in a service-oriented architecture (SOA) environment. Oracle has demonstrated the advantages of its Extended Identity Management Ecosystem (see above section on Authentication) in an implementation for a major international airlines, in which its Web SSO solution is augmented by multi-factor authentication, provided by RSA SecurID token devices. This customer selected Oracle over IBM Tivoli Access Manager and attested that it saves \$1.2 million per month by providing SSO to employees.

## Enterprise Single Sign-On

---

Oracle IdM Suite includes Oracle Enterprise Single Sign-On, which is an OEM'ed version of v-GO, the market-leading Enterprise SSO product from Passlogix. In common with Oracle's other I&AM products, Oracle Enterprise Single Sign-On is a best-of-breed solution that offers an optimal end-user experience of SSO. Oracle has added to the value delivered by providing Oracle Enterprise Single Sign-On Provisioning Gateway, which integrates Enterprise SSO directly with the user provisioning process, enabling organisations to automatically provision diverse accounts through a single identity administration process.

IBM also OEMs the Passlogix product, and Sun resells it, but neither company has integrated it with their provisioning systems. Sun also resells the SSO solution from Actividentity, but again does not highlight any value-adding integration with the SSO solution. CA has its own offering, called SSO, which is not judged to be of market-leading quality. There are no open source alternatives in this functional area.

## Federated Identity

---

Oracle Identity Federation is a standards-compliant means of achieving SSO and identity sharing between partner organisations. It can deal with identity claims based on all of the prevalent standards – Security Assertion Markup Language (SAML), WS-Federation, and Liberty Identity Federation Framework (ID-FF), and is available in packages that support the service provider, or identity provider, roles within the standards' frameworks. Its deployment options can facilitate a system that is either integrated with the rest of IdM Suite, or is usable stand-alone, and additionally comes with a development toolkit to allow custom integration with applications, as well as a utility that helpfully sets up account linking in bulk as preparation for federated identity sharing between partner organisations. A leading US financial organisation had outsourced applications supporting several HR business functions, but required employees to be able to use self-service to access them using the company's own Intranet. Using Oracle Identity Federation, this company has attributed savings of US\$400,000 annually to the 14 applications that employees can access directly via leveraging internally-defined identities.

CA sees federated identity as a development opportunity rather than a current capability. IBM's federated identity framework provides implementations of each of the major standards, but customers must use its Tivoli Directory Server, and Tivoli Access Manager, products in order to glean its benefits. Sun has a number of fairly mature federation capabilities, but does not support a wider range of protocols such as WS-Federation.

---

## Range and comprehensiveness of functional requirements coverage

---

Not surprisingly IBM has an enormous range and breadth of offerings, although these are very mature and sometimes duplicate or overlap in functionality. Some of the solutions are rather large-grained functionally, forcing customers to buy modules of Tivoli with functionality that may not actually be required.

With Sun, on the other hand, some of the products are strong functionally in their discrete areas, and are also very open and interoperate well, while other functional areas are supported via offerings from niche players in order to broaden the range of functionality sufficiently. To some extent the emphasis is on selling licences rather than taking responsibility for the total implementation.

CA also has an extensive solution set held together by a good workflow engine that extends into other service management solutions. The I&AM solution's particular strength in providing integration with heterogeneous environments is consistent with the company's history of support for mainframes and a wide range of other legacy environments.

With its excellently-architected, modern set of solutions Oracle provides a well engineered and integrated solution set that benefits particularly from being able to leverage the company's Fusion Middleware, and which has an application-centric approach that will be particularly impressive to new customers.

---

## Strategy relating to I&AM

---

CA started a series of component acquisitions as long ago as 1999, and is certainly still integrating the more recent of these, i.e., Netegrity – indeed the challenge is for CA to overcome a perception in the market place that it still has much integration work to complete.

IBM has recently established a range of discretely-branded Express offerings, aimed at the I&AM requirements of SMEs, and offering easier and quicker deployment while maintaining the power of its larger-scale solutions' integration capability, and coverage of heterogeneous environments and asset types. IBM positions its I&AM solutions in the context of overall security management, with a focus on customers' compliance and risk needs.

Sun now has a comprehensive suite of I&AM functionality, which is aligned with strategy and vision in this area, although for a long time it was judged to have weaknesses in the Access Management area – however, the company may not yet have made its improvements well-known, and overall we feel the focus is on integration with technology, rather than applications or business needs.

Oracle's recent acquisitions, and now combination, of a clutch of the best I&AM technology that was still in independent hands has catapulted the company towards the market-leading bracket. The critical, value-adding parts of IdM Suite are advanced and functionally rich, and in Butler Group's opinion provide the basis for excellent solutions both in the present, and with an eye on forward-looking requirements such as federation, and Web services. Additionally, Oracle's coverage of the customer requirements that we have detailed is complete in its breadth. We feel that Oracle considers I&AM a critical strategic capability in the context of the company's portfolio of application and middleware offerings, and that correspondingly customers can expect to benefit from Oracle's strong investment and focus on this area. The foundation of a completely standards-based set of solutions provides customers with investment protection, and prospectively better integration qualities, which collectively Oracle characterises as 'hot-pluggable'.

---

## Supplier channel strategy and execution

---

CA's I&AM products are primarily sold direct, although the channel currently plays a more prominent role in Europe, the Middle East, and Africa and Asia-Pacific, than in North America, and hence CA will need to develop its channel more widely.

IBM's customer implementations rely on a mix of home-grown expertise, and services resources from either SI partners or IBM's services arm.

Sun's route to market is through both direct sales and via partners. Sun works with a number of large SIs including EDS, Cap Gemini, Accenture, LogicaCMG, PWC, and CSC. However, we feel that some of these partners might see Sun's acquisition of Neogent, itself an SI, as damaging to the partnership relationship.

Oracle has worldwide partnerships with major SIs including Deloitte, Accenture, and CSC, as well as a network of SIs that operate at regional and country level. Oracle's consulting arm is always available in support of the SIs, providing the capacity to underwrite an implementation. In extending its channel strategy by establishing a number of relationships with mid-market SI partners, and some SIs that specialize in particular vertical sectors, Oracle has also shown innovation that will could well provide added value to significant numbers of potential customers.

## ► ORACLE CUSTOMERS' EXPERIENCES

In assessing any software solution, great value can be gleaned from actual experience of customer use. Factors such as quality and usability can only be truly proven in the field, and customers can evidence the proof (or otherwise) of vendor claims, and comment on how their own organisation has created value. During production of this White Paper, Butler Group has been given access to a number of Oracle customers (whose names we undertook not to publish) that use its I&AM solutions. We have held in-depth discussions covering those organisations' experiences as customers of Oracle I&AM solutions, which revealed many factors that we believe are useful to consider for other organisations. This section is a brief summary of those factors.

### **Complex Identity Integration in Heterogeneous Environments**

One organisation uses its Oracle I&AM solution to administrate identity centrally, dealing with identity data held in three different non-Oracle directories, and providing self-service features including group maintenance (and cross-platform synchronisation) for internal users, and registration for external users. The Oracle solution's capability to manage identity structures across other vendors' platforms, without difficulty, contrasted with competitor solutions and was a major factor in its choice as the strategic I&AM solution going forward.

### **Breadth and Depth of Solution Capability**

Oracle's ability to address the entire range of customers' end-to-end I&AM requirements was highlighted as a differentiating strength by customers, but additionally the underlying products' depth was also complimented. One customer organisation had an essential requirement to deal with role management, and found alternative suppliers less able than Oracle to provide flexibility in managing roles.

### **Value Delivery and Flexibility**

One organisation was very pleased with the way that the Oracle solution provides significant value out-of-the-box, whilst also readily facilitating customisation, and enabling a service-oriented approach via a Web service API. Its decision to invest in the Oracle I&AM solution has delivered greater value than was originally estimated as its use has been extended to manage a wider range of identity infrastructure – indeed, it admitted that with hindsight Oracle would have been the best choice as a central identity repository.

Another organisation complimented the Oracle solution's capability to support a complex, delegated administration hierarchy that affords flexibility to manage identity without unwanted functional restrictions.

### **Quality, Performance, and Scalability**

Oracle's solution was described by one customer as advanced, well-documented and –supported, and having features that work as well as Oracle claims. Another commented that the organisation has experienced no down-time in over two years of using its Oracle I&AM solution, which handles business worth over US\$3 billion annually.

### **Customers' Relationships with Oracle**

Butler Group was impressed by customers' feelings that not only were they well supported by Oracle, but are able to understand and even influence its product development strategy via participation structures such as its customer advisory board. Customers' comments relating to the acquisition of their original suppliers (Thor Technologies, and Oblix) by Oracle, were universally positive, and included satisfaction that not only had their original suppliers' expertise been retained, but that Oracle's experience in vertical markets had enhanced the value delivered from the vendor relationship.

## ► CONCLUSION

Oracle is, in Butler Group's opinion, a leading I&AM vendor, and is extremely well placed in relation to other competitors in this market place. There are numerous factors that mitigate for Oracle to be considered very strongly by organisations, in the context of their end-to-end I&AM requirements:

- I&AM is a focal point of development within Oracle's product range, at the hub of the company's middleware and application product strategy. Customers will benefit from Oracle's strong investment and innovation in the area of I&AM.
- Oracle's coverage of the broad scope of customers' I&AM requirements is extremely comprehensive.
- The products comprising Oracle's offerings are of best-of-breed quality.
- Oracle is committed to standards-based product development, a prerequisite that Butler Group believes customers must make a high priority in their choice of I&AM solution in order to protect their investment and avoid unnecessary integration costs.
- Oracle's I&AM solution has particular strengths in dealing with heterogeneous infrastructures, and a wide range of applications and asset types, providing customer organisations with the flexibility to cater for all likely integration needs while providing reduced implementation timescales compared with some competitors.

Given the benefits of risk reduction, greater efficiency, and potential cost savings, Butler Group firmly believes that organisations of all sizes should consider whether their strategy on I&AM maximises their opportunities, and whether any alternative suppliers could match their requirements as well as Oracle, as we believe Oracle to be an extremely strong solution provider candidate when compared with other competitors in this market.

## ► QUESTIONS TO ASK VENDORS

The following is a 'top 10' list of questions that customers should pose to vendors when they are considering candidates to meet their I&AM needs.

1. Can you demonstrate that I&AM has a strategic position within your range of offerings?
2. Can you provide products that meet my entire range of I&AM needs, and are they all well-integrated?
3. Does your set of I&AM capabilities allow a phased adoption approach, or do many or most of the products have to be implemented at the same time?
4. Can your I&AM products interoperate with those that I'm already using from other vendors?
5. Do your I&AM products support all the prevalent standards, throughout the range of I&AM functionality? As a company, can you demonstrate leadership in terms of driving new standards in the industry?
6. Are the individual components in your I&AM offering considered amongst the best-of-breed? If not, why should I consider adopting them?
7. Can you offer capabilities that allow customers to readily and inexpensively integrate access to applications, and other IT resources, in all types of heterogeneous IT environments? Does your solution include integration connectors to specific identity management and provisioning functions within common enterprise applications, and usability features to facilitate these integrations?
8. Can the apparent value from your proof-of-concept implementations be delivered across the wider scope of an actual delivery to a customer?

9. Can your I&AM capabilities support identity-based access to Web services, and the management of identity around SOA?
10. Can you demonstrate that your solutions support extremely high numbers of applications and users, and volumes of I&AM traffic such as provisioning and access requests, using a wide range of integrations via connectors to different types of application and environment?

## Contact Details

---

### World Headquarters

Oracle Corporation  
500 Oracle Parkway  
Redwood Shores, CA 94065  
USA

Tel: +1 650.506.7000

[www.oracle.com](http://www.oracle.com)

---



WP000073IAMa

---

**Headquarters:**

Europa House,  
184 Ferensway,  
Hull, East Yorkshire,  
HU1 3UT, UK

Tel: +44 (0)1482 586149  
Fax: +44 (0)1482 323577

**Australian Sales Office:**

Butler Direct Pty Ltd.,  
Level 46, Citigroup Building,  
2 Park Street, Sydney,  
NSW, 2000, Australia

Tel: + 61 (02) 8705 6960  
Fax: + 61 (02) 8705 6961

**End-user Sales Office (USA):**

Butler Group,  
245 Fifth Avenue, 4th Floor,  
New York, NY 10016,  
USA

Tel: +1 212 652 5302  
Fax: +1 212 202 4684

**Important Notice**

This report contains data and information up-to-date and correct to the best of our knowledge at the time of preparation. The data and information comes from a variety of sources outside our direct control, therefore Butler Direct Limited cannot give any guarantees relating to the content of this report. Ultimate responsibility for all interpretations of, and use of, data, information and commentary in this report remains with you. Butler Direct Limited will not be liable for any interpretations or decisions made by you.

For more information on Butler Group's Subscription Services please contact one of the local offices above.