An Oracle White Paper
July 2010

Oracle Identity Management 11g

ORACLE

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Introduction to Oracle Fusion Middleware 11g

Oracle Fusion Middleware (OFM) 11g provides a unified, standards-based infrastructure allowing customers to develop, deploy, and manage enterprise applications. OFM 11g extends Oracle's vision of delivering a complete, integrated, hot-pluggable, and best-of-breed middleware suite based on Oracle WebLogic Server, the industry's leading application server.

Figure 1: Oracle Fusion Middleware 11g Components

OFM 11g enables a new level of agility and adaptability in enterprise applications by delivering on the promise of service-oriented architectures (SOA). OFM 11g provides developers and business users with a declarative toolset to design and roll out enterprise

applications; a business process platform to orchestrate and monitor applications at runtime; and an enterprise portal allowing easy user interaction and secure access to corporate and business partners' resources. In addition, OFM 11g enhances middleware services in terms of enterprise performance management, business intelligence, content management, and identity management (the subject of this document).

OFM 11g greatly increases the efficiency of modern data centers by extending the capabilities of application grids. OFM 11g leverages the benefits of new hardware technologies such as 64-bit architectures, multi-core processors, and resource virtualization to provide high-performance, pooled Internet services (commonly known as "cloud computing") that are easier to deploy, integrate, and manage.

Finally, OFM 11g relies on Oracle Enterprise Manager to provide a complete management solution in a single console. Oracle Enterprise Manager automatically discovers all OFM components and their interdependencies and provides industry best practices built into dashboards for systems, services, and compliance.

Purpose and Scope

This document focuses on Oracle Identity Management 11g.

As part of Oracle Fusion Middleware, Oracle Identity Management provides a unified, integrated security platform designed to manage user identities, provision resources to users, secure access to corporate resources, enable trusted online business partnerships, and support governance and compliance across the enterprise.

Oracle Identity Management ensures the integrity of large application grids by enabling new levels of security and completeness to address the protection of enterprise resources and the management of the processes acting on those resources.

Oracle Identity Management provides enhanced efficiency through a higher level of integration, consolidation, and automation, and increased effectiveness in terms of application-centric security, risk management, and governance. Oracle Identity Management supports the full life cycle of enterprise applications, from development to deployment to full-blown production.

This document is mainly intended for a line-of-business and Information Technology (IT) audience, including application developers and application development managers, security architects, and systems and security administrators.

This document covers all the aspects of the identity services provided by Oracle Identity Management: directory services, identity administration, access control, platform and web services security, identity and access governance, operational manageability, and service integration within the identity management suite and with other Oracle and non-Oracle environments.

"Oracle has established itself as the IAM [Identity and Access Management] market leader due to its solid technology base across the IAM landscape and its compelling, aggressive strategy around what it refers to as application-centric identity."

Andras Cser, Forrester Research, Inc.

Oracle Identity Management Overview

In just a few years Oracle has established itself as the foremost identity and access management (IAM) vendor by providing an integrated, application-centric product portfolio unmatched by its competitors. Oracle's ability to anticipate and meet customer demand through a savvy combination of key acquisitions and organic growth has turned the company's identity and access management offering into the IAM market leader.

Oracle Identity Management Business Benefits

Oracle Identity Management allows enterprises to manage the end-to-end life cycle of user identities across enterprise resources both within and beyond the firewall, independently from enterprise applications. In other words, Oracle Identity Management's application-centric approach allows customers to clearly separate business logic from security and resource management, thus promoting development agility and lowering maintenance costs.

Oracle's strategy for identity and access management provides the following key benefits:

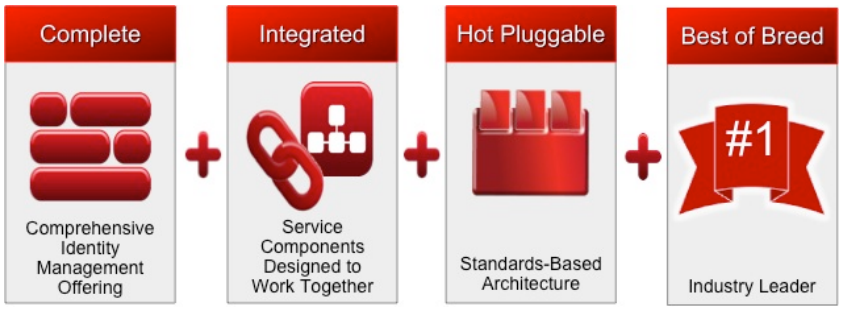

Figure 2: Oracle Identity Management Benefits

Complete: Oracle Identity Management provides a comprehensive set of market-leading services including identity administration and role management; user provisioning and compliance; web applications and web services access control; single sign-on and federated identities; fraud detection; strong, multifactor authentication and risk management; role governance and identity

analytics, audit and reports. All Oracle Identity Management components leverage the product suite's best-in-class, highly scalable directory and identity virtualization services to maximize operational efficiency and ensure the highest levels of performance and availability.

Integrated: Oracle Identity Management components can be deployed separately or together as an integrated suite of identity services. The various components making up Oracle Identity Management are designed to work together to satisfy each identity management and access control requirement met throughout a business transaction. Oracle Identity Management components integrate seamlessly with Oracle applications such as human capital management (Oracle's PeopleSoft), performance management (Oracle's Hyperion), customer relationship management (Oracle's Siebel), as well as other Oracle Fusion Middleware components such as Oracle SOA, Oracle WebCenter, and Oracle Business Intelligence. Oracle Identity Management integrates with Oracle's Governance, Risk, and Compliance platform to provide an enterprise-wide governance solution. Oracle Identity Management leverages and integrates with Oracle Database through its own directory and identity virtualization services, thus providing extreme scalability and lower cost of ownership. Finally, Oracle Identity Management provides extensions to Oracle Information Rights Management, closing the gap between identity management and content management.

Hot-Pluggable: Oracle Identity Management's standards-based suite of products is designed to support heterogeneous, multiple-vendor development and runtime environments, including operating systems, web servers, application servers, directory servers, and database management systems. For example, XML standards for federation (e.g., Security Services Markup Language – SAML and WS-Federation) allow Oracle Identity Management components to support both in-house, mission-critical applications (e.g., Java-based service providers) and third-party packaged applications (e.g., Microsoft .NET-based accounting or project management systems), thus optimizing past and future IT investments.

Best-Of-Breed: In addition to Oracle Identity Management's level of completeness, integration, and hot-pluggability, the components of the suite deliver functional depth and sophistication that, taken individually, makes them market-leading, best-of-breed products. Customers, especially those looking for advanced capabilities to support their application grid, can choose the best-in-class Oracle Identity Management component to meet their specific requirements and integrate that component with the rest of their existing identity management portfolio, or they can deploy the best-of-breed Oracle Identity Management suite to take advantage of its enhanced integration.

Oracle Identity Management is an integral part of Oracle Fusion Middleware. It leverages Oracle Fusion Middleware's services such as Business Intelligence, Enterprise Management, and SOA and Process Management, and it provides security services to multiple Oracle Fusion Middleware components and Oracle Fusion Applications.

Introducing Oracle Identity Management 11g

Oracle Identity Management 11g is characterized by the following:

- Establishment of Oracle Identity Management as a security development platform (see the *Oracle Platform Security Services* and *Identity Governance Framework* sections later in this document).
- Oracle Identity Management becomes Oracle Fusion Applications' *de facto* security infrastructure.
- Enhanced integration between Oracle Identity Management's components and other Oracle Fusion Middleware components, Oracle Applications, and third-party security providers.
- Enhanced functionality allowing easier environment deployments (e.g., wizards to guide users through rapid deployment tasks, multi-level actionable dashboards for business users to analyze compliance and risk indicators, and take remediation actions).
- Streamlined release synchronization and technology uptake between the various products making up Oracle Identity Management.

Service-Oriented Security

Key to Oracle Identity Management 11g is the concept of Service-Oriented Security (SOS). SOS provides a set of security services leveraged by Oracle Fusion Middleware components, as shown in the figure below.

Figure 3: Service-Oriented Security

Oracle's SOS applies Service-Oriented Architecture (SOA) principles to security in order to promote better design (industry-standard security "components"), deployment (appropriate level of security applied where necessary), and management (through a single point of administration). SOS is built upon Oracle Platform Security Services (OPSS), a security development framework described later in this document.

Oracle Identity Management leverages SOS to provide "identity as a service." Identity services take the functionality of an identity management solution that would otherwise be bolted onto applications and make the set of identity services available in a SOA environment. Applications following SOA guidelines are able to leverage these services without any concern about how these services are provided. Shared identity services enable enterprises to make identity a reusable, standard, transparent, and ubiquitous part of their applications.

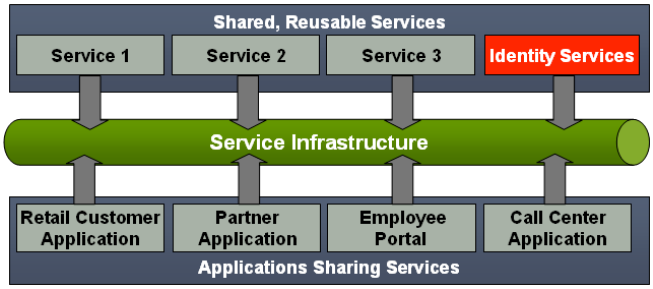

Figure 4: SOA-Based Shared, Reusable Services

Oracle Identity Management's Key Services

Oracle Identity Management 11g provides a comprehensive set of services as shown in Figure 5: Identity administration; access management; directory services; identity and access governance; platform security; operational manageability.

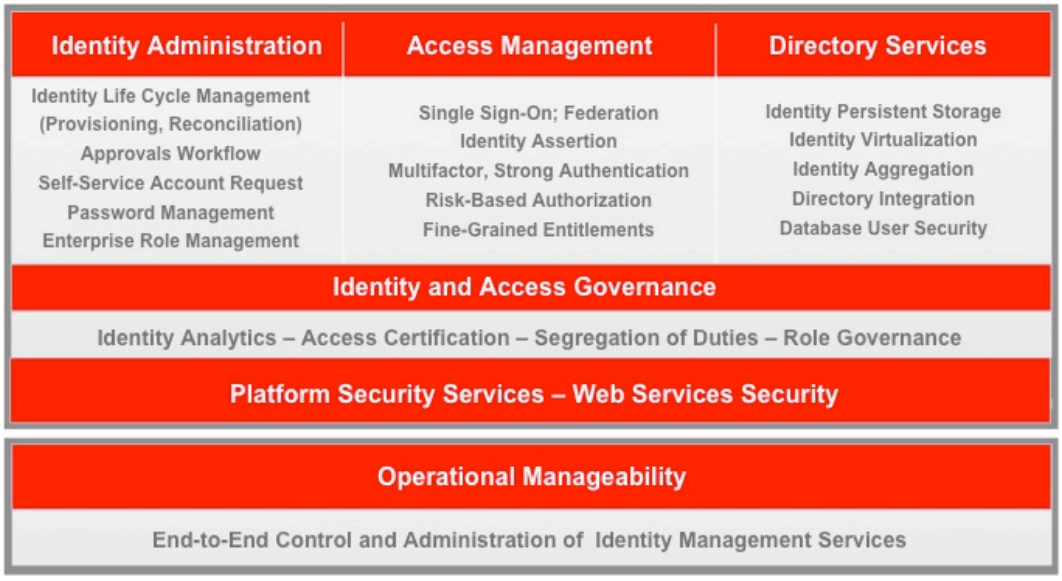

Figure 5: Oracle Identity Management 11g Services

Instead of cobbling together a heterogeneous environment from diverse, separate products, each service (for example user on-boarding) works with other identity services through standard interfaces to provide a complete, homogeneous environment.

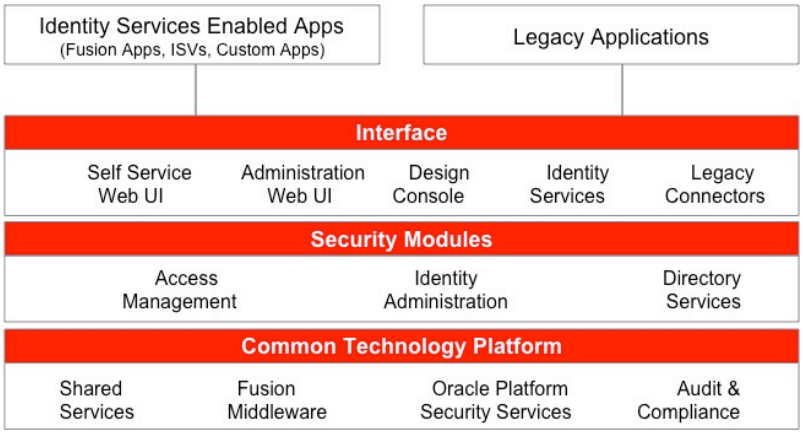

Figure 6: Oracle Identity Management Architecture

An SOA architecture allows each service to leverage the environment within and outside identity management. For example, the workflow engine used in user provisioning approvals is the same, standards-based workflow engine used by Oracle SOA Suite. Likewise, the same standard cryptographic libraries are used throughout the identity management environment and other Oracle Fusion Middleware components.

The following tables summarize Oracle's identity services and products by category.

Platform Security Services

COMPONENTS	DESCRIPTION	COMMENTS
Oracle Platform Security Services (OPSS)	Standards-based, enterprise-grade framework exposing security services through pluggable abstraction layers. OPSS provides the "service-oriented security" approach for Oracle Identity Management.	Security foundation for Oracle Fusion Middleware: all Oracle Fusion Middleware components and Oracle Fusion Applications "consume" the OPSS framework's services.
Oracle Authorization Policy Manager (OAPM)	OAPM is a graphical user interface console for administering OPSS-based authorization policies.	OAPM is intended for customers relying on Oracle Fusion Middleware products based on OPSS, custom or in-house applications built with Oracle ADF, and next-generation Oracle Fusion Applications.

Identity Governance Framework (IGF)	Oracle's IGF is designed to help enterprises control how identity-related information (e.g., attributes and entitlements) is used, stored, and propagated between applications.	Originally started by Oracle, IGF is an open-source project hosted by The Liberty Alliance.
Authorization API (OpenAz)	Oracle's Authorization API provides a standard interface between an application and a general authorization service. It also provides an effective way to enable authorization providers to plug in client-side authorization functionality.	Authorization API is a public project started by Oracle. As part of OPSS, it will become the sole authorization API for Oracle Fusion Middleware.
Oracle Web Services Manager (OWSM)	OWSM secures standards-compliant web services (Java EE, Microsoft .NET, PL/SQL, etc.), service-oriented architecture (SOA) composites, and Oracle WebCenter's remote portlets.	Standards-based, policy-centric security lynchpin for Oracle Fusion Middleware web services.

Directory Services

COMPONENTS	DESCRIPTION	COMMENTS
Oracle Internet Directory (OID)	Enterprise Lightweight Directory Access Protocol (LDAP) directory server and directory integration platform implemented on top of Oracle Database technology providing unsurpassed level of scalability, high-availability, and information security. OID includes Oracle Directory Services Manager (ODSM), a web-based administration user interface for server configuration.	Highly scalable LDAP directory integrated with Oracle Fusion Middleware and Oracle Fusion Applications.
Oracle Directory Server Enterprise Edition (ODSEE)	Enterprise identity services including the LDAP Directory Server, Directory Proxy, Directory Synchronization, web-based management user interface and deployment tools. ODSEE is the industry's leading, carrier-grade directory.	Small-footprint, best-of-breed LDAP directory, recommended for heterogeneous application deployments. Will be integrated with ODSM and Data Integration Platform (DIP).
Oracle Virtual Directory (OVD)	Java-based environment designed to provide real-time identity aggregation and transformation without data copying or data synchronization. OVD includes two primary components: the OVD Server to which applications connect, and ODSM (described above).	OVD provides a single standard interface to access identity data no matter where it resides while hiding the complexity of the underlying data infrastructure (OVD does not store information, this role is left to the persistence systems used for that purpose, such as OID and ODSEE).

Access Management

COMPONENTS	DESCRIPTION	COMMENTS
Oracle Access Manager (OAM)	OAM provides centralized, policy driven services for web applications authentication, web single sign-on (SSO), and identity assertion.	OAM integrates with a broad array of authentication mechanisms, third-party web servers and application servers, and standards-based federated SSO solutions to ensure maximum flexibility and a well-integrated, comprehensive web access control solution.
Oracle Identity Federation (OIF)	OIF is a self-contained solution enabling browser-based, cross-domain single sign-on using industry standards (SAML, Liberty ID-FF, WS-Federation, Microsoft Windows CardSpace).	OIF seamlessly integrates with third-party identity and access management solutions. OIF is specifically designed for identity providers.
Oracle OpenSSO Fedlet	A lightweight federation extension allowing a service provider to immediately federate with an identity provider without requiring a full-blown federation solution in place.	Oracle's Fedlet is specifically designed for service providers and fully integrated with OIF.
Oracle OpenSSO Security Token Service (STS)	Oracle's STS establishes a trust relationship between online partners through web services. STS provides both standard and proprietary security token issuance, validation, and exchange.	STS is currently available with the Oracle Access Management Suite Plus. Going forward, Oracle's STS will be integrated with OAM.
Oracle Enterprise Single Sign-On (eSSO)	Oracle eSSO is a Microsoft Windows desktop-based set of components providing unified authentication and single sign-on to both thick- and thin-client applications with no modification required to existing applications.	Using Oracle eSSO, enterprise users benefit from single sign-on to all of their applications, whether users are connected to the corporate network, traveling away from the office, roaming between computers, or working at a shared workstation.
Oracle Entitlements Server (OES)	OES is a fine-grained authorization engine that externalizes, unifies, and simplifies the management of complex entitlement policies.	OES provides a centralized administration point for complex entitlement policies across a diverse range of business and IT systems.
Oracle Adaptive Access Manager (OAAM)	OAAM provides resource protection through real-time fraud prevention, software-based multifactor authentication, and unique authentication strengthening.	OAAM consists of components that create one of the most powerful and flexible weapons in the war against fraud.

Identity Management, Identity and Access Governance

COMPONENTS	DESCRIPTION	COMMENTS
Oracle Identity Manager (OIM)	OIM typically answers the question "*Who* has access to *What*, *When*, *How*, and *Why*?". OIM is designed to administer both intranet and extranet user access privileges across a company's resources throughout the entire identity management life cycle, from initial on-boarding to final de-provisioning of an identity.	In extranet environments, OIM's superior scalability allows enterprises to support millions of customers accessing the company's resources using traditional clients (e.g., browsers) or smart phones.
Oracle Identity Analytics (OIA)	OIA helps enterprises address regulatory mandates, automate processes, and quickly make compliance a repeatable and sustainable part of business. OIA provides a comprehensive solution for attestation (access certification), role governance, and enterprise-level segregation-of-duties enforcement.	Integrates with OIM for role administration and role-based provisioning automation as part of Oracle remediation.

Operational Manageability

COMPONENTS	DESCRIPTION	COMMENTS
Oracle Identity Navigator (OIN)	OIN is an SSO-enabled launch pad for all of Oracle Identity Management services' administrative consoles.	OIN acts as a user experience consolidation point for Oracle Identity Management.
Oracle Management Pack for Identity Management	Oracle Management Pack for Identity Management leverages Oracle Enterprise Manager's broad set of capabilities to control end-to-end identity management components.	Support for service-level configuration, dashboard-based user interaction, environment monitoring, performance automation, and patch management.

Each Oracle Identity Management functional area is described in detail in the following sections of this document.

Oracle Identity Management Components

Oracle Identity Management's areas of functionality presented in the previous section are implemented by the multiple products described in this document. Details for each product are provided in dedicated technical white papers (please visit oracle.com/technology/products/id_mgmt/ to download Oracle Identity Management's components information).

Platform Security Services

Platform security services include the Oracle Platform Security Services (OPSS) framework, Identity Governance Framework (IGF), Authorization API, and Oracle Web Services Manager (OWSM).

Oracle Platform Security Services

One of the key benefits and differentiators of Oracle Identity Management 11g is enhanced support for application development, provided by *Oracle Platform Security Services* (described in this section) and the *Identity Governance Framework and ArisID* (described in the next section).

Companies understand the necessity of including security as part of the development process, but they face challenges in implementing security in the various layers of multi-tiered web applications.

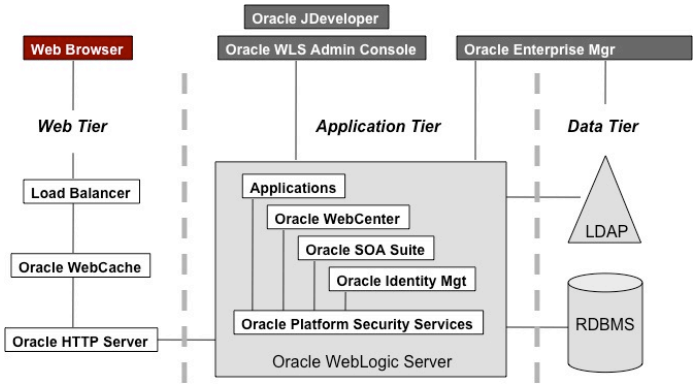

Figure 7: Oracle Platform Security Services

Oracle Platform Security Services (OPSS) provides enterprise product development teams, systems integrators, and independent software vendors with a standards-based, portable, integrated, enterprise-grade security framework for Java Platform, Standard Edition (Java SE) and Java Platform, Enterprise Edition (Java EE) applications.

OPSS insulates developers from the intricacies of tasks not directly related to application development by providing an abstraction layer in the form of standards-based application programming interfaces (API). Thanks to OPSS, in-house-developed applications, third-party applications, and integrated applications benefit from the same, uniform security, identity management, and audit services across the enterprise.

OPSS is the security foundation for Oracle Fusion Middleware: all Oracle Fusion Middleware components and Oracle Fusion Applications "consume" the OPSS framework's services.

OPSS is a self-contained, portable environment that runs on Oracle WebLogic Server. At development time, OPSS services can be directly invoked from the development environment (Oracle JDeveloper) through wizards. When the application is deployed to the runtime environment, systems and security administrators can access OPSS services for configuration purposes through Oracle Enterprise Manager Fusion Middleware Control or command line tools.

OPSS complies with the following standards: role-based-access-control (RBAC); Java Platform, Enterprise Edition (Java EE), Java Authorization and Authentication Services (JAAS), and Java Authorization Contract for Containers (JACC).

OPSS includes Oracle WebLogic Server's internal security services used by BEA-heritage products such as Oracle Entitlements Server; these services are consumed by Security Services Provider Interface (SSPI), which becomes part of OPSS as well. In addition, OPSS includes Oracle Fusion Middleware's security framework (formerly referred to as Java Platform Security (JPS) or JAZN).

- SSPI provides Java EE container security in permission-based (JACC) mode and in resource-based (non-JACC) mode. It also provides resource-based authorization for the environment, thus allowing customers to choose their security model. SSPI is a set of APIs designed to implement pluggable security providers in order to support multiple types of security services, such as custom authentication or a particular role mapping.
- JPS was first released with Oracle Application Server 9.0.4 as a JAAS-compatible authentication and authorization service working with XML-based and Oracle Internet Directory providers. In 11g, JPS has been expanded to include the following services (described later in this section): Credential Store Framework (CSF), User and Role API, Oracle Fusion Middleware Audit Framework, and JDeveloper/ADF integration (application security life cycle support).

OPSS also includes Oracle Security Developer Tools (OSDT), a set of Java-based cryptographic libraries supporting XML signature, XML encryption, XML Key Management Specification (XKMS), SAML, WS-Security, and other non-XML standards such as Secure / Multipurpose Internet Mail Extensions (S/MIME) and Online Certificate Status Protocol (OCSP).

OSDT is used in many Oracle products including Oracle applications and Oracle Fusion Middleware components. OPSS leverages OSDT for SSL configuration and Oracle Wallet (used by Oracle Identity Management products, Oracle EM, and Oracle Database).

OPSS provides out-of-the-box support for (1) applications using WebLogic Server's internal security and SSPI, such as Oracle Entitlements Server and Oracle Access Manager, and (2) applications using JPS, such as Oracle ADF, Oracle WebCenter, Oracle SOA, and Oracle Web Services Manager.

Developers can use OPSS APIs to build security features for all types of applications and integrate them with other security artifacts, such as LDAP servers, database systems, and custom security components. Administrators can use OPSS to deploy large enterprise applications with a small, uniform set of tools and administer all security in them. OPSS simplifies the maintenance of application security because it allows the modification of security configuration without changing the application code.

Figure 8: Oracle Platform Security Services Architecture

OPSS's functional layers include:

Authentication: OPSS uses WebLogic Server authentication providers, components that validate user credentials or system processes based on a user name-password combination or a digital certificate. Authentication providers include the Default Authenticator, external LDAP stores, and database systems to host data for enterprise applications.

Identity Assertion: The WebLogic Identity Assertion providers support certificate authentication using X.509 certificates, SPNEGO tokens, SAML assertions, and CORBA Common Secure Interoperability version 2 (CSIv2) identity assertion.

Single sign-on (SSO): Authentication providers can use different types of systems to store security data. The Authentication provider that WebLogic Server installs uses an embedded LDAP server. Oracle Fusion Middleware 11g also supports perimeter authentication and SSO through Oracle Access Manager (OAM). For small environments that don't need to be integrated with an enterprise SSO solution such as OAM, lightweight SSO is provided by a SAML-based solution using WebLogic Server's SAML Credential Mapping Provider.

Authorization: OPSS provides a Java policy provider that supports code-based and *subject*-based authorization.

Note: A *subject* is a grouping of related security information that includes a collection of *principals* such as a name ("John Doe"), an email address ("jd@oracle.com"), together with (optional) security-related attributes (credentials) such as passwords or cryptographic keys. The Java class `javax.security.auth.Subject` represents a *subject* and an instance of this class is created and populated with *principals* when authentication succeeds. OPSS authentication providers enable identity propagation across multiple components in a domain through *subjects*.

OPSS supports application roles (logical roles specific to an application). Unlike Java EE's logical roles, OPSS supports role hierarchy. OPSS also provides an advanced policy model that includes elements such as resource types (e.g., an ADF task flow) and entitlement sets (authorized actions on a given resource instance) allowing complex authorization policies to be conveniently defined and managed. Using Oracle EM Fusion Middleware Control or WebLogic Scripting Tool (WLST), the administrator can manage an application's authorization policies, including mapping application roles to enterprise groups and users, or editing the permissions granted to an application role. OPSS also provides a policy management API allowing programmatic control over authorization policies.

User and role: OPSS's User and Role API framework allows applications to access identity information (users and roles) in a uniform and portable manner regardless of the particular underlying identity repository. The User and Role API frees the application developer from the intricacies of particular identity sources.

Role mapping: OPSS supports the mapping of application roles to enterprise groups in the domain Policy Store, no matter the kind of domain policy repository employed (file-based or LDAP-based). This mechanism allows users in enterprise groups to access application resources as specified by application roles.

Security stores: The Identity Store is the repository of enterprise users and groups. The Policy Store is the repository of application and system policies. The Credential Store is the repository of domain credentials. Credentials are used during authentication when *principals* are populated in *subjects*, and during authorization when determining what actions the *subject* can perform. OPSS provides the Credential Store Framework (CSF), a set of APIs that applications can use to create, read, update, and manage credentials securely. OPSS uses one logical store to keep both policies and credentials. OPSS's security stores are virtualized through Oracle Virtual Directory (OVD).

Audit: OPSS provides a common audit framework for Oracle Fusion Middleware products. Customers using OPSS automatically get the benefit of audit without writing a single line of audit-related code. The Oracle Fusion Middleware audit framework provides out-of-the-box customizable analytical reporting capabilities within Oracle Business Intelligence Publisher; data can be analyzed on multiple dimensions (e.g., Execution Context Identifier (ECID) or user ID) across multiple components.

Application life cycle support: OPSS provides support for all the phases of an application's life cycle. OPSS is integrated with Oracle JDeveloper, which allows an application designer to model security into the application when building Oracle ADF task flows. Oracle JDeveloper also provides an authorization editor that allows developers to create authorization policies for ADF taskflows and pages without writing a single line of code. Typically a developer deploys her application to a WebLogic Server domain embedded in JDeveloper. The developer can then deploy the application to a remote WebLogic Server domain using Oracle Enterprise Manager Fusion Middleware Control (FMWControl). OPSS is integrated with FMWControl to allow application security policies and credentials migration to be configured during application deployment. Post deployment, an administrator uses FMWControl to manage the application's security policies, e.g., edit authorization policies, or change audit policies. All such changes are transparent to the application and do not require any application code change. In any non-trivial application scenario, an application normally goes from development to a staging (or test) environment before being put in full-blown production. OPSS supports this model by providing migration tools that move security policies from a test domain into a production domain. For example, audit policies configured in a test domain can be exported into the target production domain.

Oracle Authorization Policy Manager

Oracle Authorization Policy Manager (OAPM) is graphical user-interface console for managing OPSS-based authorization policies. OAPM is designed for customers relying on Oracle Fusion Middleware products consuming OPSS services, Oracle ADF or OPSS used by in-house custom applications, and Oracle's next generation Fusion Applications.

OAPM is a standards-based environment (JAAS permissions and enterprise RBAC) that supports delegated administration, advanced life cycle management, and identity store access through IGF / ArisID (IGF and ArisID are described later in this document).

OAPM is licensed through the Oracle Identity Management suite and available through the Oracle Identity Management 11g installer.

As shown in Figure 9, both Oracle Identity Manager and Oracle Access Manager leverage OAPM (and OPSS) services for administering authorization policies.

OAPM-Administered Artifacts

OAPM administers both *global* and *application-specific* artifacts. Global artifacts include users, external roles, and system policies.

Global artifacts apply to all application *stripes* (an application stripe is a logical subset of the domain policy store where the application policies are kept).

Application-specific artifacts include the resource catalog, application policies, application roles, and role categories. Application-specific artifacts apply to a single application stripe.

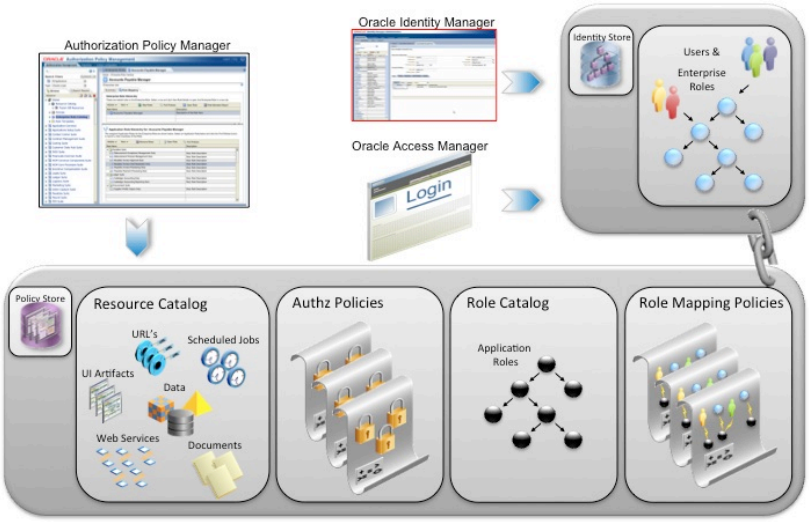

Figure 9: Managing Authorization Policies Leveraged by OIM and OAM

OPSS Authorization Policy Model Concepts

Resource Type: A template of secured artifacts is represented as a Resource Type. An Oracle ADF task flow is a good example of a Resource Type.

Resource Instance: Each secured resource of a given type is represented as a Resource Instance (e.g., `orderEntryTaskflow`) and points to a physical resource.

Entitlement: Aggregates resources and allowable actions, and encapsulates privileges sufficient for a task (e.g., `CreatePOTaskFlow`).

External Role: A collection of users and other groups, synonymous with *enterprise role* or *enterprise group*, typically implemented as an LDAP group in the Identity Store.

Application Role: A logical and hierarchical role that exists in the Policy Store. An Application Role is tagged via the Role Catalog.

Application Policy: A collection of entitlement and resource permissions granted to a principal (an Application Role or an External Role are examples of principals).

System Policy: A global policy that grants an application access to OPSS APIs.

Role Mapping: Role mapping allows users to access protected application resources. Application Roles are mapped to External Roles.

Identity Governance Framework and ArisID

As mentioned earlier, OPSS leverages its User and Role API to provide developers with relatively simple methods to manage identities. However, developers will still be inclined to map the User and Role API to business objects. To simplify this development process, Oracle has created the Identity Governance Framework (IGF) project, now hosted by the Liberty Alliance (www.projectliberty.org).

IGF is designed to help enterprises control how identity-related information (e.g., attributes and entitlements) is used, stored, and propagated between applications.

IGF allows application developers to build applications that access identity-related data from a wide range of sources, and administrators and deployers to define, enforce, and audit policies concerning the use of identity-related data.

IGF's functional layers include:

- *Client Attributes Markup Language (CARML)*: A specification built by the developer during the development process. CARML indicates the required and optional attributes, operations, and indexes the application will use when deployed (CARML is to an application what WSDL is to a web service). The application developer uses the CARML API to both declare the attribute data needed for the application and the operations needed to support the application (the CARML API uses SAML and SOAP-based protocols to communicate with attribute services).
- *Attribute Authority Policy Markup Language (AAPML)*: An Extensible Access Control Markup Language (XACML) profile designed to allow attribute authorities to specify conditions under which information under management may be used (and possibly modified) by other applications.
- *Attribute service*: a web service that reads the CARML file in order to configure "views" of one or more attribute authorities that meet the requested data requirements of the application specified in the CARML document.

In 11g, the first incarnation of the IGF project is ArisID Identity Beans. ArisID is designed for developers to access identity information using a single API. ArisID enables access and management of identity information stored in different types of repositories accessed using different protocols. ArisID implements the IGF specification and in particular it enables

developers to create their own virtual identity database while retaining the ability to interconnect with enterprise identity services.

ArisID uses a declarative, multi-function API that depends on providers to do the work of data mapping, protocol transformation, and connectivity. The Oracle Virtual Directory (OVD) Provider for ArisID is an example of an ArisID provider. The OVD Provider for ArisID is a library that enables OVD to provide identity services to an application using the ArisID API. In this way, OVD plus the OVD Provider library for ArisID and the ArisID API library comprise a complete set of libraries that can be used by applications to access identity services. Please visit www.oracle.com/technology/tech/standards/idm/igf/arisid/index.html to download a developer preview of ArisID.

Authorization API

Oracle's Authorization API framework is an ongoing public project known as "OpenAZ" (http://lists.openliberty.org/mailman/listinfo/openaz_lists.openliberty.org), originally started by Oracle.

Enterprises need to control authorization for services and devices in a systematic way. The market has been growing with offerings from several vendors, but none of these offerings has become an industry standard.

An authorization framework must allow the use of information about users, resources, application context, and network in an extensible fashion. Authorization is in essence a matter of evaluating a set of attributes. Application programming interfaces (APIs) and service provider interfaces (SPIs) only need to pass these attributes.

While the Extensible Access Control Markup Language (XACML 2.0) provides a good foundation for authorization services and XACML's representation of attributes is general enough to map to and from existing APIs and SPIs, the initial focus of XACML is on an interoperable policy language. What is missing is an API for requesting an authorization decision, a way to describe a service's authorization requirements and information about required attributes.

Oracle's Authorization API provides a thin interface between an application and a general, primarily XACML-based, authorization service. The Authorization API will ultimately include multiple language bindings. Originally co-authored by Oracle and Cisco, the Java XACML Authorization API draft has been submitted to the OASIS XACML Technical Committee in July 2009 (http://lists.oasis-open.org/archives/xacml/200907/msg00020.html).

Oracle's Authorization API provides an effective way to enable authorization providers to plug in client-side authorization functionality (Policy Enforcement Point (PEP)). Also, the Authorization API is needed for calls to a local Policy Decision Point (PDP) as it is inefficient to serialize data to and from XML.

The Authorization API supports standard API calls for remote requests and common code to build request messages.

The typical use cases for Oracle's Authorization API are:

- Policy Enforcement Points (PEP): Build PEPs within a container to issue authorization requests for the container or for an application.
- Policy Information Points (PIP): Obtain attributes from an attribute authority.
- Policy Decision Points (PDP): Enhance the functionality of existing authorization providers.

Over time, the Authorization API framework will become the sole authorization API for Oracle Fusion Middleware delivered as part of the OPSS framework.

Oracle Web Services Manager

Oracle Web Services Manager (OWSM) is designed to protect access to multiple types of resources:

- General purpose, standards-compliant web services (Java EE, Microsoft .NET, PL/SQL, etc.).
- Oracle ADF Data Control (DC) clients, Oracle ADF Business Component (BC) web services, JAX-WS web services, and Oracle ADF JAX-WS proxy dynamically invoking services of different endpoints.
- Service-oriented architecture (SOA) composite components including Business Process Execution Language (BPEL) and enterprise service bus (ESB) processes.
- Oracle WebCenter's remote portlets.

OWSM 11g is installed as part of Oracle SOA 11g and Oracle WebCenter 11g. In addition, OWSM 11g is the runtime policy governance component for the Oracle SOA Governance solution. In this case, it provides production assurance for deployed SOA artifacts through policy-based security and participates at various stages of the closed-loop life cycle control.

OWSM 11g includes a policy manager (an active / active component) and interceptors or enforcement points (also known as agents). Both policy manager and agents run on Oracle WebLogic Server. Agents can be on the service requester side (client) and/or the service provider side (endpoint server). Typically, a request made to a web service is intercepted by an OWSM agent that enforces security policies defined in the OWSM policy manager. OWSM's policy model is the security lynchpin for Oracle Fusion Middleware's web-services-based components.

In Oracle Fusion Middleware 11g, you can provide security and management policy enforcement of WebLogic Server (WLS) web services based on the Java API for XML Web Services (JAX-WS) using either OWSM or WLS web services policy types. WLS policies are provided by WLS and a subset of WLS web services policies interoperate with OWSM policies.

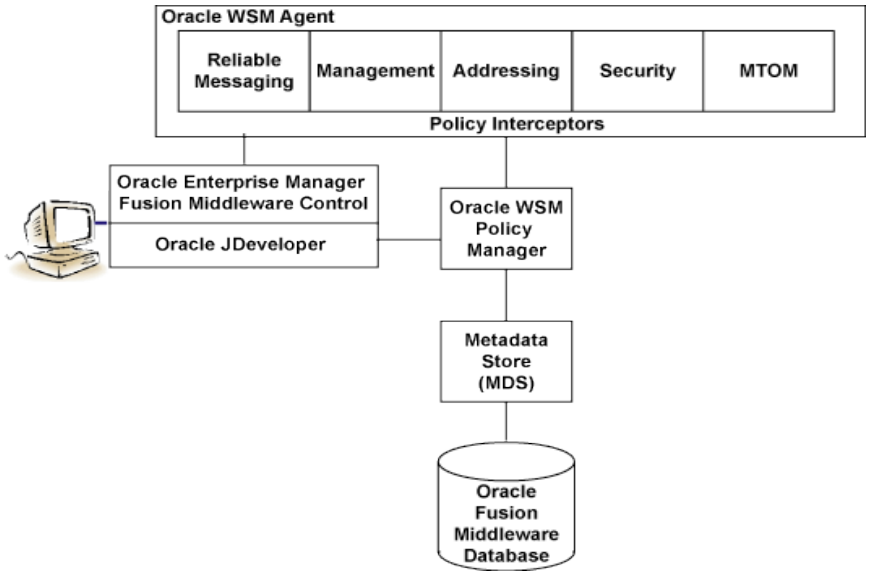

Figure 10: Oracle Web Services Manager

OWSM's functional layers include:

Industry-standards-compliant policy management: OWSM 11g's policy manager is based on web services security industry standards, in particular WS-Security (SOAP security extensions that provide message-level confidentiality, data integrity, and profiles that specify how to insert different types of binary and XML security tokens (e.g., X.509 certificates) in WS-Security headers for authentication and authorization purposes), WS-Policy (an XML framework that describes the capabilities and constraints of a web service, e.g., required security tokens, encryption algorithms, etc.), and WS-SecurityPolicy (which defines a set of security policy assertions used in the context of the WS-Policy framework). OWSM's strict compliance with industry standards allows the publication of security requirements in the Web Service Definition Language (WSDL) file that describes each web service. In addition to security policies, OWSM 11g supports Message Transmission Optimization Mechanism (MTOM), reliable messaging (RM), and management policies (see Figure 10).

Oracle Enterprise Manager (EM) Fusion Middleware Control for monitoring: OWSM 11g benefits from the advantages of using the runtime monitoring and integration capabilities of Oracle EM. As a result, web services monitoring is now part of the larger monitoring of a whole enterprise application (OWSM agents provide Oracle EM with the monitoring information it requires). In addition, OWSM 11g is integrated with Oracle JDeveloper to provide declarative policy attachment at development time (see Figure 10).

Authentication: OWSM 11g leverages Oracle Platform Security Services (OPSS) log-in module infrastructure for authentication and makes it possible to plug in custom log-in modules. You

need to configure the right Oracle WebLogic Server "authenticator" to get credentials authenticated (WLS comes with a generic LDAP authenticator that you can use for this purpose, WLS also comes with an Oracle Access Manager authenticator that performs authentication directly against the Oracle Access Manager server). Following successful authentication, OWSM sets a Fusion security context for consumption by Fusion applications. OWSM also leverages OPSS for identity propagation (ability to read and set `javax.security.auth.Subject`), credentials store, key store and certificate management, and auditing. (See more detail on Java *subject* in the OPSS section earlier in this document.)

Authorization: Authorization can be role-based (OWSM policies allow one to check if the authenticated user belongs to one of the allowed roles configured in a policy), permission-based (OWSM policies allow one to check if the authenticated user has the required Java permission (in OPSS's `jazn-data` file), and entitlement-based (using a custom integration, OWSM integrates with Oracle Entitlements Server to provide content- (XPath) and context- (HTTP header, client IP, etc.) based authorization.

Tight integration with Oracle Service Bus (OSB): Using OSB 11g in conjunction with OWSM 11g provides a scalable, standards-based, centrally managed approach to securing your SOA environment with WS-Security policies while leveraging your existing security providers. You create policies, attach them to services in OSB, and enforce those policies at various points in the messaging life cycle with OWSM agents.

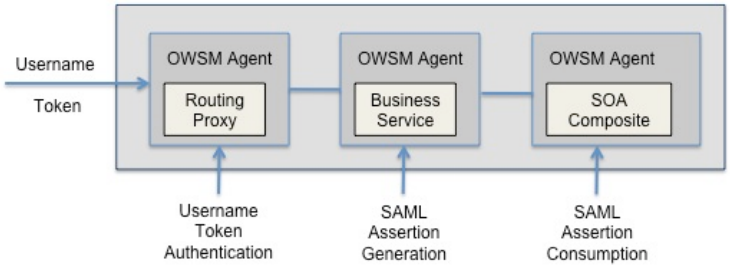

Figure 11: Securing OSB Processes With OWSM Agents

OWSM can override OSB's security out of the box (OSB ships with the OWSM extension). OWSM support is enabled by selecting the "Oracle Service Bus OWSM Extension" template when you create or extend an OSB domain. In future releases of OSB, OWSM policies will replace and enhance the functionality of Oracle WebLogic Server 9.2 security policies.

Perimeter security: OWSM 11g tightly integrates with market-leading appliances such as Vordel's XML Gateway to provide perimeter security and intrusion detection.

Directory Services

Oracle Directory Services (ODS) include Oracle Internet Directory (OID) and Oracle Directory Server Enterprise Edition (ODSEE) to handle data storage and directory synchronization services, and Oracle Virtual Directory (OVD) to provide identity aggregation and transformation without data copying.

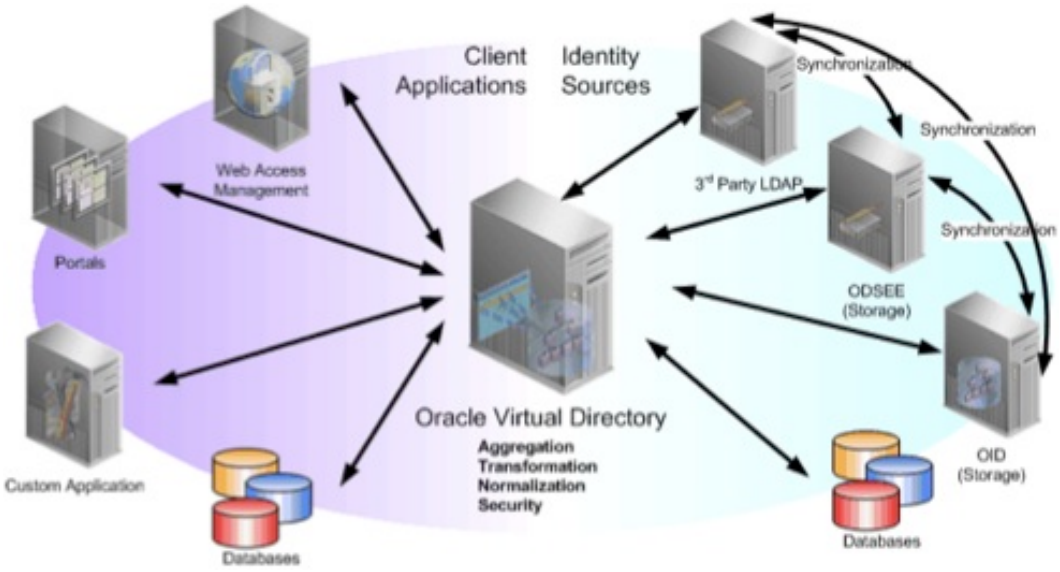

Figure 12: Oracle Directory Services

OID and ODSEE have different strengths for different customer requirements. OID is application-driven and focuses on Oracle environments, in particular Oracle Fusion Middleware components and Oracle Fusion Applications. ODSEE, on the other hand, is architecture-driven and addresses more heterogeneous, multiple-vendor environments. ODSEE's smaller footprint (e.g., embedded database) allows for faster enterprise deployments.

OVD supports ODSEE as a target data source and provides a unified environment to access ODSEE, OID, Microsoft Active Directory (AD), and other third-party directories. OVD also provides unified access to multiple ODSEE environments. OID co-exists and synchronizes with ODSEE through OID's directory integration platform (DIP), described later in this document.

The following sections describe in detail each component of Oracle Directory Services.

Oracle Internet Directory

Oracle Internet Directory (OID) provides Oracle Fusion Middleware components, Oracle Fusion Applications and in-house enterprise applications with a standard mechanism for storing and accessing identity data such as user credentials (for authentication), access privileges (for authorization), and profile information. OID is predicated on the Lightweight Directory Access Protocol (LDAP), an Internet standard designed to organize directory information and to allow communication of client applications with directories for look-up, search, and retrieval operations.

OID is implemented on top of Oracle Database technology, thus providing LDAP directory services with an unsurpassed level of scalability, high-availability, and information security. The OID plus Oracle Database combination allows customers to run Oracle's applications in a highly scalable and high-performance manner.

OID's functional layers include:

Scalability: The LDAP servers running on an OID server node are multithreaded to use database connection pooling in order to prevent running into resource limitations as the number of simultaneous LDAP client connections increases. In addition, the ability to run multiple LDAP server processes on a single OID server node provides vertical scalability by increasing the number of server process per hardware node, and horizontal scalability by distributing server processes over clustered hardware nodes.

High availability: OID is designed to enable continuous service availability at the OID server process level and at the data storage level. Multi-master replication between OID servers ensures that if any of the servers in the replicated environment goes down, any other server can act as the "master." Based on robust and field-proven Oracle Database replication technology, this ensures full availability even in the event of hardware failure. LDAP-based multi-master replication with any number of nodes is an additional option with OID 11g. LDAP replication provides more flexible deployment topologies with very little overhead, and very granular filtering and partitioning options.

Information security: OID administrators can define their directory service environment in order to provide different levels of access to the directory information based on how a given user was authenticated (both password and certificate-based authentication are natively supported). In addition, OID 11g offers attribute-level encryption. OID supports two unique database security features: Oracle Database Vault (enforcing separation of duties for database administrators) and Oracle Transparent Encryption (automatically encrypts data when it is written to disk and decrypts it when it is read back to the authorized user).

Enhanced usability and diagnostics: OID 11g delivers superior usability with Oracle Directory Services Manager (ODSM). Based on Oracle's Application Development Framework (ADF), ODSM provides OID (and OVD) administrators with an easy-to-use administration tool including deployment accelerators for creating new users, sizing and tuning OID, and setting up

and configuring LDAP replication. Enhanced diagnostics (now built into all of Oracle Fusion Middleware components) make use of execution context identifiers (ECID) attached to directory operations. This allows an administrator to trace an operation such as a failed user log-in through the entire environment starting with the web server all the way down to OID and finally the database.

Integrated management and monitoring: OID 11g administration and monitoring have been streamlined around two complementary components: Oracle Enterprise Manager (EM) 11g Fusion Middleware Control and Oracle Directory Services Manager (ODSM, mentioned above). Oracle EM provides management and monitoring of OID distributed processes and their performance including host characteristics as well as end-to-end network layer security (SSL) configuration, and audit management. ODSM supports administrative tasks such as LDAP data browsing, schema creation and modification, and management of directory data security. Oracle Business Intelligence Publisher is used for audit report generation, with a wide variety of out-of-the-box and customizable reports.

Directory integration platform: OID includes a directory integration platform (DIP), a set of services enabling customers to synchronize data between various third-party data sources and OID targets. In addition, DIP enables OID to be interoperable with third-party meta-directory solutions. DIP includes connectors for out-of-the-box synchronization with Oracle E-Business Human Resources, Oracle Database, as well as connectors for synchronizing information with third-party LDAP servers, such as Microsoft AD and Active Directory Lightweight Directory Services (LDS), Novell eDirectory, OpenLDAP, and IBM Tivoli. DIP is managed and monitored using Oracle EM. Wizards guide users through the process of profile creation and graphical attribute-mapping between third-party directories and OID.

External authentication: OID's external authentication functionality enables seamless authentication against third-party directories, such as Microsoft AD, Novell eDirectory, and OpenLDAP. In many cases, this can completely remove the need to synchronize sensitive password information into OID.

Extensibility and client-side development: Oracle provides the Oracle Internet Directory SDK intended for application developers using Java, C, C++, and PL/SQL for client integration with OID's functionality.

Support for Database Enterprise User Security (EUS): The combination of EUS (as part of Database Advanced Security) and OID (or OVD) forms the centerpiece of the Oracle Database enterprise user security strategy. For more information on this, please see the *Oracle Identity Management and Oracle Database* section later in this document)

Authentication services for operating systems: This functionality leverages OID to enable enterprises to centralize Unix and Linux authentication, user accounts, `sudo` authorization policies, and enforce enterprise-wide strong passwords across server platforms. In addition to OID, the authentication services for operating systems functionality uses Pluggable Authentication Modules (PAM) which

are standard operating system modules available on most Unix and Linux distributions designed to support externalized authentication, and automation tools that configure both PAM and OID components, simplify user migration, and ensure strong default security between network endpoints.

Oracle Directory Server Enterprise Edition

Oracle Directory Server Enterprise Edition (ODSEE) provides a core directory service, directory proxy, virtual directory, synchronization with Microsoft AD, and a single web console to manage the entire environment. ODSEE includes a number of key, small-footprint components that together provide complete directory services ideal for deployment of heterogeneous applications across the enterprise.

ODSEE functional layers include:

Centralized repository for identity, application, and network resource information: ODSEE provides a highly scalable, secure, and flexible means of storing and managing identity data from entry-level to large-scale enterprise deployments. ODSEE's centralized repository enhances security, reduces IT complexity and cost by reducing the number of directories you have to manage.

Directory proxy services: ODSEE's proxy services prevent denial-of-service (DoS) attacks, control access based on specific criteria, and intercept unauthorized operations. In addition, proxy services enable failover operations allowing the directory service to continue operating when a server is offline. Load balancing protects the directory environment from load-related failures and delivers horizontal scalability on reads and searches.

Throttle control: ODSEE limits operation rates on the directory proxy server to ensure uptime and load partitioning across the entire authentication infrastructure.

Consolidated identity view: ODSEE allows multiple directory servers with different schemas to act together to service clients, which reduces complexity for administrators and developers by providing a single view of an identity and its attributes.

Virtual directory: ODSEE aggregates identity data from multiple sources to provide a virtual view accessed through LDAP thus avoiding data ownership issues associated with accessing data from different applications or business units.

Access control: Used by the directory server to evaluate what rights are granted or denied when it receives an LDAP request from a client. ODSEE uses access control lists to create rules at the attribute level to control data access.

Multiple password policies: ODSEE defines password policies based on time, group, and role to meet application and security requirements. Security requirements are enforced by giving developers and administrators the tools to create the right password policy for each application.

Security protocol support: ODSEE uses industry-standard protocols to encrypt identity attributes and allow customers to adapt to complex security environments and changing requirements with an open plug-in architecture.

Replication: ODSEE allows one to create a high-availability environment for the company's authentication architecture, which enables development teams to access real data while maintaining control over the enterprise data and authentication schema.

Oracle Virtual Directory

One of the identity management challenges enterprises are facing is the lack of a single source for identity data and the proliferation of identity stores including directories and databases. Enterprises have employee information in various repositories such as human resources databases and/or Microsoft AD, customer and partner data in customer relationship management systems, and additional LDAP directories.

Oracle Virtual Directory (OVD) is designed to provide real-time identity aggregation and transformation without data copying or data synchronization.

OVD provides a single standard interface to access identity data no matter where it resides while hiding the complexity of the underlying data infrastructure (OVD does not store information, this role is left to the persistence systems used for that purpose, such as OID).

Since OVD enables applications to access existing authoritative identity data sources without copying, it reduces the need for application-specific user stores and data synchronization, thus simplifying user and resource provisioning and accelerating application deployment.

OVD includes two primary components: the OVD Server to which applications connect, and the Oracle Directory Services Manager (ODSM), a web-based administration user interface for server configuration (also used by OID, as described in the previous section).

OVD's functional layers include:

Single interface for identity: OVD provides a join adapter allowing support for split profiles. A split profile is one where the user identity data is divided between two or more sources. For example, a user's identity information is stored in a database, an LDAP server, and a web service but applications want to treat it as a single entry. The join adapter uses a join rule (similar to a SQL join condition) to virtually link the data together into a "super-entry."

LDAP interface for non-LDAP data: Many applications including the various Oracle Identity Management services described in this document as well as Oracle Database use LDAP to access identity information. As a result, to leverage data in a database or a web service, the data must be made accessible via an LDAP interface. OVD contains adapters that allow LDAP-enabled applications to leverage database or web-service data directly without the need to copy the data into another LDAP server. For example, OVD can expose Oracle's PeopleSoft or Oracle's Siebel Universal Customer Master (UCM) data as LDAP for applications to access.

Data transformation and application-specific views: OVD not only virtually unifies data, it can also transform data (for example change ORCL to Oracle) and provide application-specific views. Many of these transformations are possible with configuration. In addition, customers can do their own business-logic-driven transformations using OVD's Java plug-in API. Because OVD is stateless and supports data transformations, it is able to create application-specific views of data. This means that different applications (all accessing the same OVD server) can appear to be accessing completely different data schemas, structures, attribute names and values.

Enhanced usability: As mentioned in the previous section, OVD 11g leverages Oracle Directory Services Manager (ODSM) which provides enhanced usability for administrators.

Enterprise scalability, availability and manageability: OVD can route requests to different sources based on name or user ID ranges. OVD can also leverage additional Oracle technology such as Oracle TimesTen or Oracle Coherence to further reduce latency and improve scalability. OVD can be deployed either centrally or geographically dispersed depending upon application requirements. The simplest way to make OVD highly available is to add multiple nodes and then use round-robin DNS or load-balancers to route requests properly.

Database account and role management centralization: Oracle Database supports centralizing accounts and roles in an enterprise directory. The database can use OVD to allow this data to be stored in a third-party LDAP directory. This reduces the number of passwords that a person needs to remember and can eliminate the need to have a provisioning product update individual databases. This maximizes the benefits of database and account security while eliminating the potential problems caused by trying to copy existing identity data into multiple repositories.

Access Management

Access management components are grouped in the Oracle Access Management Suite Plus, including Oracle Access Manager, Oracle Identity Federation and Oracle OpenSSO Fedlet, Oracle Entitlements Server, Oracle Adaptive Access Manager, Oracle OpenSSO Security Token Service, and Oracle Information Rights Management. Each component can be licensed separately except the Oracle OpenSSO services, which are only available through the Oracle Access Management Suite Plus.

Figure 13: Oracle Access Management Suite Plus

Oracle Access Management Suite Plus services are tightly integrated. The following table shows the benefits of the addition of new features enhancing cross-product integration and security.

KEY FEATURES	DESCRIPTION	BENEFITS
Next-generation architecture	• Java EE-based Oracle Access Manager server • Consolidated SSO architecture • Out-of-the-box Oracle Access Manager and Oracle Identity Manager integration	• Simplified deployment • Backward compatibility across OAM and Oracle SSO • Integrated identity and access management
Out-of-the-box, suite-wide security	• Oracle Access Manager secures Oracle Identity Manager out of the box • Policy simulation	• Pre-integrated platform • Secure access by default

Risk-based challenges	• Augment Oracle Access Manager with adaptive authentication schemes synchronization	• Deliver one-time-password (OTP) to any device
Malware and phishing protection	• Virtual devices and personalization to defend against identity hijacking	• Consumer-grade identity protection for the entire enterprise
eCo Grid	• Persist session data for authenticated users in an embedded Oracle Coherence grid	• High performance access to distributed session data • Enforce session constraints
Centralized agent management	• Manage agent creation, management, and diagnostics from a central administration console	• Centralize application protection • Simplify ongoing administration
Integrated diagnostics framework	• Centralize diagnostics information for servers and connected agents	• Simpler troubleshooting for security administrators
Simplified security administration	• Oracle ADF-based administration console with streamlined, task-based flows	• Simplify creation and management of complex fraud policies
OTP Anywhere	• Register delivery options and generate one-time passwords (OTP) for advanced / secondary user challenges	• Add sophisticated security to basic flows in a few easy steps
AppSecure Control Center	• Manage agent creation and diagnostics from a central administration console	• Centralize application protection • Simplify ongoing administration
SSO Security Zones	• •Scope agent-to-server security to application enforcement zones	• •Prevent unauthorized access from spreading to multiple applications
Universal Risk Snapshot	• Create security data snapshots for policies, rules, challenge questions	• Easily and simply restore security configuration to a known state
AnswerLogic	• Pre-integration of Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager for forgotten password flows and secure login	• Add needed security to “unprotected” password reset pages

Oracle Access Manager

Oracle Access Manager (OAM) provides centralized, policy driven services for authentication, single sign-on (SSO), and identity assertion. OAM integrates with a broad array of authentication mechanisms, third-party web servers and application servers, and standards-based federated SSO solutions to ensure maximum flexibility and a well-integrated, comprehensive web access control solution.

OAM provides authentication and SSO services in the web tier and integrates with applications and data providers by asserting authenticated identities to application access control systems.

OAM complements its own coarse-grained authorization and attribute assertion capabilities by integrating with Oracle Entitlements Server to provide fine-grained authorization and entitlements to applications, portals, databases, and web services (for more detail on this, please see the *OAM and OES Integration* section later in this document).

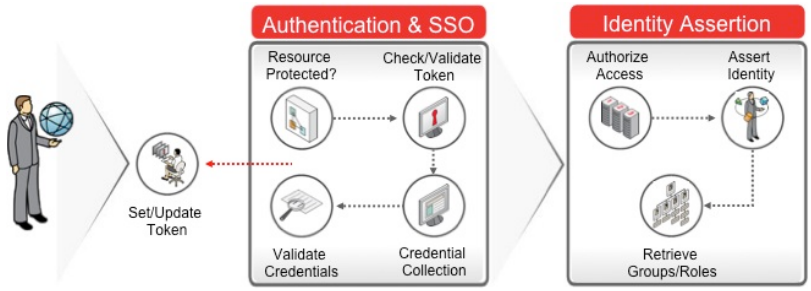

Figure 14: Oracle Access Manager's Functionality

OAM leverages Oracle Directory Services including Oracle Internet Directory (OID) for the persistence and management of user information, and Oracle Directory Integration Platform (DIP) for user synchronization (OID and DIP are described earlier in this document). OAM can also leverage any other type of third-party user directory platform.

OAM's functional layers include:

Authentication: OAM's Access Server, Policy Manager, and out-of-the-box web server plug-ins called WebGates (or AccessGates for integration with application servers, packaged applications, and other enterprise resources) work together to intercept access requests to resources, check for a pre-existing authentication, validate credentials, and authenticate users.

Single Sign-On: Typically, when a browser user attempts to access an application, OAM first checks whether the application is protected. If it is, OAM (through a WebGate or AccessGate) challenges the user for credentials (e.g., simple username / password, X.509 certificates, smart cards, etc.). Based on these credentials, OAM enforces its security policies to authenticate the user against a user store and creates a session ticket (in the form of an HTTP (browser) cookie) enabling single sign-on or repeated access to the same application without re-logging.

Access control: OAM allows coarse-grained authorization to resources based on user roles and access policies. Typically, following successful authentication, OAM provides access to a specific resource (e.g., a web page) based on the authenticated user's role. For example, a basic user and an administrator authorized to the same web application may have access to different levels of functionality through a personalized web page based on their role's attributes.

Support for enterprise applications: OAM integrates with existing e-business infrastructures (such as SAP, Oracle's Siebel, Oracle's PeopleSoft, and Oracle E-Business Suite). It provides pre-built agents to protect, access, and manage all popular third-party web servers, application servers, portals, user directories, email systems, and relational databases.

Support for Windows Native Authentication: OAM enables Microsoft Internet Explorer users to automatically authenticate to their web applications using their desktop credentials. This is known as Windows Native Authentication (WNA). Cross-platform authentication is achieved by emulating the negotiate behavior of native Windows-to-Windows authentication services that use the Kerberos protocol. In order for cross-platform authentication to work, non-Windows servers (in this case, OAM) must parse SPNEGO tokens in order to extract Kerberos tokens subsequently used for authentication. With OAM single sign-on combined with WNA, a Kerberos session ticket is generated that contains the user's log-in credentials (this Kerberos session ticket is not visible to the user). With WNA implemented, the user can click on a web application without another challenge for credentials; the Kerberos session ticket including the user's credentials is passed through the browser to OAM. OAM validates the credentials by checking them against the Key Distribution Center (KDC) server on the Windows domain server.

Compliance Reporting: OAM includes unified and centralized audit reporting for all OAM components, with all operations stored and correlated in a secure database for analysis. OAM comes with pre-built reports and the ability to create custom reports through Oracle Business Intelligence Publisher in order to provide greater visibility and reporting on common events such as user access attempts, successful or failed authentications, and single sign-on events. These features improve an organization's ability to meet common governmental and industry regulations.

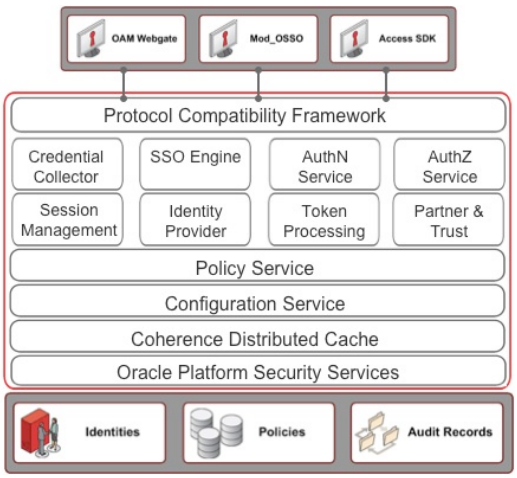

Figure 15: Oracle Access Manager's Architecture

In Oracle Identity Management 11g, OAM becomes the web access and single sign-on solution of choice for Oracle Fusion Middleware components and Oracle Fusion Applications.

OAM 11gR1 is designed to replace Oracle SSO over time (as shown in Figure 15, the Mod_OSSO agent now communicates directly with OAM's policy server thus allowing Oracle SSO customers to leverage OAM's functionality). Likewise, Oracle OpenSSO will converge with OAM. OAM 11g's new policy model provides an easy migration of OAM 10g, Oracle SSO, and Oracle OpenSSO to OAM 11g.

Thanks to its tight integration with Oracle Platform Security Services (OPSS), OAM is able to make calls to container-managed applications in order to invoke authentication events that are enforced by OAM. In this case, the application makes the decision to authenticate by calling OPSS for log-in. This is just one example of OAM's integration with OPSS. Please refer to the Oracle Access Manager technical white paper for more examples.

Oracle Identity Federation

Identity federation is required when there is a need for single sign-on beyond a single Internet domain (the single Internet domain requirement is met by Oracle Access Manager, described above).

Oracle Identity Federation (OIF) is a standalone federation server that bundles all the required components necessary for deployment, including a Java EE container (Oracle WebLogic Server) and a web server (Oracle HTTP Server (OHS)).

OIF is designed to support mission-critical applications through load balancing and failover. OIF allows customers to set up a system with shared database instances (to store session data), which multiple servers can access. OIF servers can be also configured to support specific load-distribution algorithms and remove configured servers from service if particular machines go down.

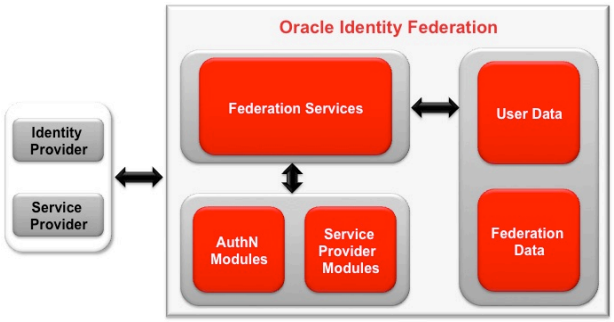

Figure 16: Oracle Identity Federation

The most widely accepted industry standard for identity federation is the Security Assertion Markup Language (SAML). SAML is an open framework for sharing security information on the Internet through XML documents. SAML was designed to address the following:

Limitations of web browser cookies to a single domain: SAML provides a standard way to transfer cookie information across multiple Internet domains.

Proprietary web single sign-on (SSO): SAML provides a standard way to implement SSO within a single domain or across multiple domains.

Federation: SAML facilitates identity management (e.g., account linking when a single user is known to multiple web sites under different identities).

Web services security: SAML provides a standard security token (a SAML assertion) that can be used with standard web services security frameworks (e.g., WS-Security, mentioned earlier in this document). This use of SAML is particularly relevant to web services security, fully supported by Oracle Web Services Manager.

Identity propagation: SAML provides a standard way to represent a security token that can be passed across the multiple steps of a business process or transaction, from browser to portal to networks of web services.

OIF's functional layers include:

Multiple Federation Protocols Support: OIF participated in vendor-neutral conformance events and has achieved Liberty Alliance certification for Liberty ID-FF and SAML 2.0. OIF supports the following protocols: SAML 1.0, 1.1, and 2.0; Liberty Alliance ID-FF 1.1 and 1.2; WS-Federation (WS-Federation enables brokering of trust and security token exchange, support for privacy by hiding identity and attribute information, and federated sign-out.). OIF provides support for Microsoft Windows CardSpace (CardSpace provides a user's digital identity in information "cards"; for example, an OIF identity provider can challenge a user for login via the CardSpace protocol and then return a SAML assertion based on the CardSpace authentication and claims).

Support for heterogeneous architectures: OIF seamlessly integrates with third-party identity and access management solutions. Acting as an identity provider, OIF can authenticate users against a user directory or a database. If a supported authentication or authorization system is already deployed, OIF can leverage it to authenticate users and create authentication (SAML) assertions to be passed on to partner applications. Acting as a service provider, OIF communicates with a supported authentication or authorization system to determine the access privileges of authenticated users by locating the attributes of the user from the data repository. In addition, OIF provides simplified programmatic interfaces to allow customers to directly integrate with specific applications or homegrown solutions, thus requiring no additional operational footprint.

Bulk account set up and provisioning: OIF includes a tool that enables administrators to bulk load user federation records. As a federation represents account linking between a user and two providers

(the identity provider and the service provider), the two providers agree to identify an individual using the data contained in the federation contract.

Certificate validation support: OIF provides a certificate validation store to support X.509 certificates for digital signatures and encryption. It enables you to manage trusted certificate authorities (CA) and certificate revocation lists (CRL) in an easy-to-use administration console. Administrators can sign and encrypt outgoing SAML assertions as well as validate and authenticate messages received from trusted providers.

Audit, logging, monitoring: Audit (integration with Oracle Platform Security Services' common audit framework and Oracle Business Intelligence Publisher); monitoring (Oracle EM); and logging integrated with Oracle Fusion Middleware and Oracle Identity Management.

Oracle OpenSSO Fedlet: Oracle OpenSSO Fedlet is a small web archive (WAR) including Java Archives (JARs), properties, and metadata. Oracle's Fedlet is designed to be embedded into a service provider's Java EE web application to allow for SSO between an identity provider instance of Oracle OpenSSO Enterprise or Oracle Identity Federation and the service provider's application without the need for installing Oracle OpenSSO Enterprise or Oracle Identity Federation on the service provider's side. Oracle's Fedlet is ideal for an identity provider that needs to enable a service provider with no federation solution in place. The service provider simply downloads the Fedlet, modifies their application to include the Fedlet JARs, and re-archives and redeploys the modified application. The service provider is now able to accept an HTTP POST (that contains a SAML 2.0 assertion) from the identity provider and retrieve included user attributes to accomplish SSO. Oracle's Fedlet can communicate with multiple identity providers, using a discovery service to find the preferred identity provider.

Oracle OpenSSO Security Token Service

Oracle OpenSSO Security Token Service (STS) implements the Web Services Trust Language (WS-Trust). In a message exchange using the WS-Security standard only, it is assumed that both parties involved in the exchange have a prior agreement on which type of security tokens they must use for sharing security information. However, there are cases where these parties don't have such an agreement, as a result trust must be established before exchanging messages. Trust between two parties exchanging SOAP / WS-Security-based messages is established by implementing the WS-Trust specification. In this context, establishing trust between partners means that the web service provider must trust the security information submitted by the requesting party (web service client). This trust must be brokered when both parties don't use the same security tokens (i.e., the incompatibility of the security token formats must be resolved). WS-Trust addresses these issues by

- defining a request / response protocol where a client (or a gateway on its behalf) sends a `RequestSecurityToken` (RST) met with a `RequestSecurityTokenResponse` (RSTR),

- providing a Security Token Service (STS) which enables security token exchange, token issuance, and token validation.

Because of the extensive use of tokens in web services security, there is a need for a centralized token service; Oracle's Security Token Service serves this purpose. Oracle's Security Token Service is hosted as a servlet endpoint and coordinates security-based interactions between a web service client and a web service provider.

Oracle's Security Token Service is a standalone service that any third party client can use without implementing web services security. It provides the following functionality:

- Issue, renew, cancel, and validate security tokens.
- Allow customers to write their own plug-ins for different token implementations and for different token validations.
- Provide a WS-Trust-based API for client and application access.
- Provide security tokens including Kerberos, Web Services-Interoperability Basic Service Profile (WS-I BSP), and Resource Access Control Facility (RACF).

When a web service client makes a call to the web service provider, it first connects with the Security Token Service to determine the security mechanism required and optionally obtain the security tokens expected by the web service provider.

When an authenticated web service client requests a token for access to a web service provider, the Security Token Service verifies the credentials and, in response, issues a security token that provides proof that the web service client has been authenticated. The web service client presents the security token to the web service provider which verifies that the token was issued by a trusted Security Token Service.

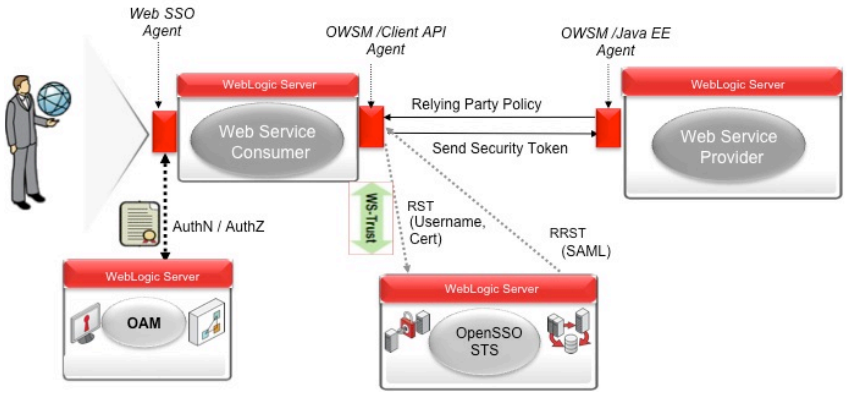

Figure 17: Oracle OpenSSO STS Use Cases

Oracle OpenSSO STS works in conjunction with Oracle Access Manager and Oracle Web Services Manager to support identity propagation and security token exchange, as shown in Figure 17.

Oracle's Security Token Service supports the following tokens.

- Tokens that can be authenticated with the Security Token Service: UserName, X.509, SAML 1.1 and 2.0, Kerberos.
- Tokens that can be issued with the Security Token Service: UserName, X.509, SAML 1.1 and 2.0.
- End user tokens that can be converted or validated out of the box: Oracle OpenSSO Enterprise `SSOToken` to SAML 1.1 or SAML 2.0 token; SAML 1.1 or SAML 2.0 token to Oracle OpenSSO Enterprise `SSOToken`.

Oracle Enterprise Single Sign-On

Oracle Enterprise Single Sign-On (eSSO) is a desktop-based suite of products providing unified authentication and single sign-on to thick- and thin-client applications with no modification required to existing applications. With Oracle eSSO, users don't have to remember and manage multiple passwords thus saving helpdesk time in responding to user requests for resetting forgotten passwords.

Oracle eSSO's functional layers include:

Logon Manager: Strengthens security and improves user productivity by enabling end users to securely use a single log-in credential to all web-based, client-server, and legacy applications.

Password reset: Reduces helpdesk costs and improves user experience by enabling strong password management for Microsoft Windows through secure, flexible, self-service interfaces.

Authentication Manager: Enforces security policies and ensures regulatory compliance by allowing organizations to use a combination of tokens, smart cards, biometrics, and passwords for strong authentication throughout the enterprise.

Provisioning Gateway: Improves operational efficiencies by enabling organizations to directly distribute single log-in credentials to the Logon Manager based on provisioning instructions from Oracle Identity Manager.

Kiosk Manager: Enhances user productivity and strengthens enterprise security by allowing users to securely access enterprise applications even at multi-user kiosks and distributed workstations.

eSSO Anywhere: Simplifies deployment to very large numbers of client desktops and automates updates.

Oracle Entitlements Server

Oracle Entitlements Server (OES) is a Java EE-based, fine-grained authorization engine that externalizes, unifies, and simplifies the management of complex entitlement policies. OES secures access to application resources and software components (such as URLs, Enterprise JavaBeans, and Java Server Pages) as well as arbitrary business objects (such as customer accounts or patient records in a database).

OES provides a centralized administration point for complex entitlement policies across a diverse range of business and IT systems. OES offers a sophisticated delegated administration model that allows multiple organizations and application stakeholders to create, modify, and report on the entitlement policies that affect them.

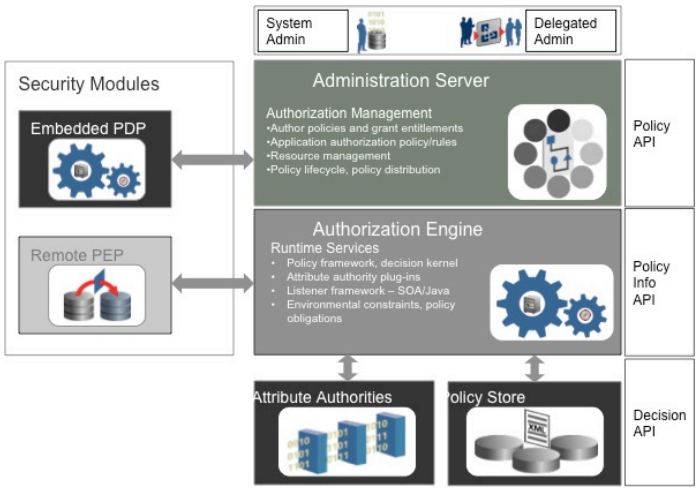

Figure 18: Oracle Entitlements Server

OES is made up of two major components, the Administration Server and Security Modules. The Administration Server acts as the policy administration point (PAP) and is used to manage configurations, organizations, applications, policies, and roles. OES enforces authorization at runtime through one or more Security Modules. Security Modules evaluate fine-grained access control policies at the policy decision point (PDP) and enforce them at the policy enforcement point (PEP). OES's unique architecture allows Security Modules to be combined as a single policy decision point and policy enforcement point that runs in process with an application to vastly increase the performance and reduce latency of runtime authorization decisions. The Security Modules are also the integration point for user identities and access to external attributes that may be incorporated into policies. Security Modules include attribute retrievers to return information dynamically during policy evaluations from policy information points (PIP). These

information sources can be relational databases, identity directories, web services, or any other source of data.

OES policies specify which users, groups, and/or roles can access application resources, allowing those roles to be dynamically resolved at runtime. A typical OES policy could be as follows: "Grant the 'Get' action for 'AccountReports' to anyone who is in the user group 'BankManagers'." Through a unique, flexible architecture, OES can also evaluate specialized attributes to make further, more granular access control decisions.

OES's functional layers include:

Policy administration: Support for massive policy stores with thousands of resources and policies; partitioning features for large numbers of organizations and applications; fully delegated administration with flexible role mapping of users; web-based interface that runs on popular Java EE containers; fully programmable administrative interface for custom administrative needs. OES's administration model is protected by OES itself.

Policy distribution: OES's Administration Server handles the task of publishing policies to the individual Security Modules protecting applications and services. This distribution provides a transactional mechanism to ensure each Security Module has just the policy it needs. Features of policy distribution include: ability to update policies in Security Modules without interrupting applications; intelligent push technology that only pushes the policies needed by a Security Module; sophisticated protocol which handles interrupted distribution scenarios; simple architectural requirements for policy distribution without forsaking security and integrity of policies in-flight; Security Modules operate in a disconnected mode with no runtime dependency on OES.

Support for multiple platforms: OES runs on many popular Java EE containers such as Oracle WebLogic Server, Tomcat, and IBM WebSphere. Policy repositories can be managed against Oracle Database, Sybase, Microsoft SQL Server, and IBM DB2.

Policy reporting: OES provides an ad-hoc query facility to help policy administrators understand how users and roles map to permissions and entitlements. Policy reports can be generated for specific application resources (e.g. database columns, Enterprise JavaBeans), identities (users, groups, roles) and even permissions. Reports are available as simple text files for consumption by downstream business intelligence or reporting tools.

Oracle Adaptive Access Manager

Oracle Adaptive Access Manager (OAAM) provides protection for businesses and their customers through real-time fraud prevention, multifactor authentication, and unique authentication strengthening.

Conceptually, OAAM consists of two primary components that together create one of the most powerful and flexible weapons in the war against fraud. Adaptive Strong Authenticator (ASA)

provides multifactor authentication and protection mechanisms for sensitive information such as passwords, personal identification numbers (PIN), tokens, security questions, account numbers and other credentials. Adaptive Risk Manager (ARM) provides real-time and offline risk analysis, and proactive actions to prevent fraud at critical log-in and transaction checkpoints.

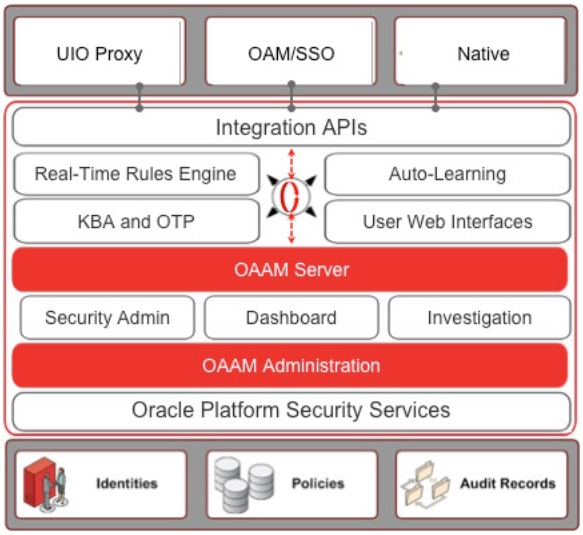

Figure 19: Oracle Adaptive Access Manager

OAAM's functional layers include:

Authentication security: ASA provides a solution for strengthening any authentication scheme, including web SSO forms, one-time passwords, knowledge-based authentication, biometrics, smartcards, X.509 certificates, and user directory and database authentication. ASA includes a server component and a suite of web-based virtual authentication devices that secure sensitive user authentication information and protect against malware attacks such as key loggers and mouse-click loggers as well as man-in-the-middle attacks.

Risk analysis: ARM evaluates risk by analyzing contextual data from a variety of sources, including user profiles, device fingerprints, transactional data, Internet Protocol (IP) addresses, geo-location, and third-party data feeds. By looking at various risk factors simultaneously, ARM can store the relative risk level at any time and take steps to proactively prevent fraud and alert investigators.

Behavior profiling: ARM dynamically identifies high-risk situations by learning, refreshing, and maintaining what a normal behavior is for users and devices. In this way, fraud prevention can adapt to the changing behavior of users without manual intervention.

Fraud investigation and forensics: ARM provides real time and offline risk analysis tools to simplify investigation and auditing. Reporting can be done using Oracle Business Intelligence Publisher.

Fraud intelligence: Security policies need to be able to adjust to new requirements without needing to bring down a production system. OAAM gives security administrators the ability to experiment with different security policies, assess their usefulness at preventing fraud, test-run specific rules, and track the difference in system behavior as a result of policy change before fraud occurs.

Universal Risk Snapshot: The following can be saved in a snapshot: Policies, rules, conditions, groups, patterns, trigger combinations, actions and score overrides; Actions, alerts, configuration actions; Transactions, entities; Knowledge-based authentication (KBA) questions, validations, registration and answer logic; Database-based properties.

Challenge processor framework: Allows integrators the ability to write custom processor classes to trigger on OAAM rule actions. Also, this functionality provides server-generated one-time passwords (OTP), e.g., email, SMS, voice.

OTP Anywhere: One-time password (OTP) adds sophisticated security to basic flows in a few easy steps.

AnswerLogic: Provides needed security to "unprotected" password reset pages.

Oracle Information Rights Management

Oracle Identity Management is an application-centric platform primarily operating on application containers (web portals, web servers, application servers), and file and database systems. Typically, user directories, such as Oracle Internet Directory, are the central "engine room" of identity management. For example you store "John Doe" as a member of "Sales" once, not multiple times for each application; you can then define what applications John Doe may access based on his role (salesperson) and entitlements (what actions he can perform on a specific application).

In addition, in the course of his work, John Doe will create, read, or modify documents such as spreadsheets, presentations, etc. Copies of these documents will be stored in one or multiple places, and will possibly be distributed to many people within and outside the enterprise firewall.

As a result, in addition to securing access to applications, an identity and access management solution needs to be able to secure the contents produced by the employees, partners, and possibly customers of a company. In other words, in addition to being application-centric, an identity and access management solution also needs to be information-centric. The latter requirement is met by Oracle Information Rights Management (IRM).

As shown in Figure 20, Oracle IRM extends the perimeter security provided by Oracle Identity Management.

Documents and emails may "live" in access-controlled repositories such as file system folders, email inboxes, content management systems, and collaborative workspaces but copies of these documents go out to "work" every day on thousands of desktops, laptops, and mobile devices. The simplest action of clicking on a file obtained online causes a copy of that file to be downloaded to your desktop from where it can be easily and untraceably redistributed anywhere.

Oracle IRM safeguards information directly. It uses encryption to shrink the access control perimeter down to the actual units of digital information, e.g., documents, emails, and web pages. Oracle refers to the process of protecting digital documents as "sealing", which includes:

- wrapping the file within industry-standard encryption, e.g., AES 256,
- digitally signing the file to detect and prevent tampering,
- including indelible URL hyperlinks into each sealed file that point back to the customer-operated Oracle IRM Server on which the decryption keys and access rights are stored.

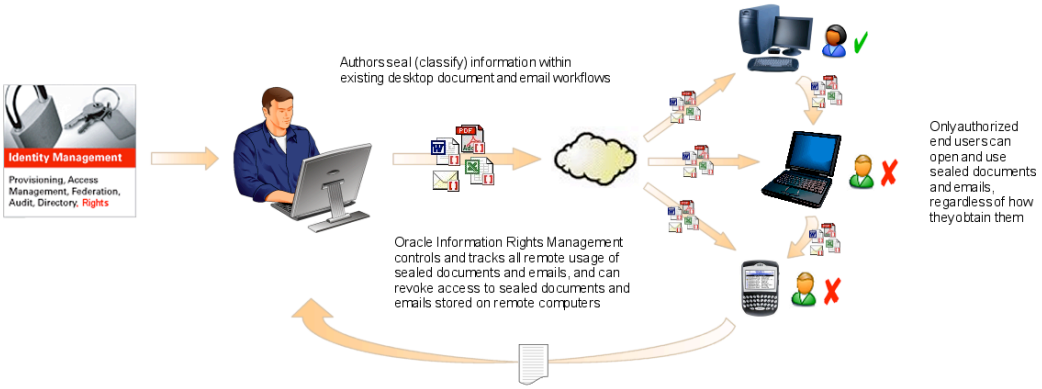

Figure 20: Oracle Information Rights Management Process

Typically, the Oracle IRM process goes as follows:

- An author creates a document or an email on her desktop or laptop.
- Using tools integrated into the Windows desktop or supported applications, the author seals the document.
- The author shares the sealed document through email, file transfer, instant messaging, etc.
- The receiver clicks on the document sent by the author. Because the file is sealed, all the user sees is cipher text with a plain text header informing her that she must install the Oracle IRM Desktop to access this file. If she already has the Oracle IRM Desktop (the most common scenario), the document is unsealed and ready to be used (i.e., read or modified, based on the receiver's entitlements).

Oracle IRM leverages the following Oracle Identity Management components:

- Oracle Identity Manager (OIM) to centrally provision IRM users and entitlements.
- Oracle Virtual Directory (OVD) to synchronize IRM users and groups from existing enterprise LDAP and non-LDAP directories.
- Oracle Enterprise Single Sign-On (eSSO) for desktop single sign-on and additional support for strong authentication.

Complementing Oracle Identity Management's application-centric focus with the information-centric approach of Oracle Information Rights Management is unique to Oracle's offering and a major competitive differentiator.

Identity Management, Identity Access and Governance

Oracle's identity management and identity access and governance services have been fully consolidated in Oracle Identity Management 11g. Likewise, Oracle Identity Management ensures that the customer's experience is consistent throughout Oracle's identity management components (all components' user interfaces are based on Oracle Application Development Framework (ADF)).

When a user clicks on the "forgotten password" link from the log-in page rendered by Oracle Access Manager, the associated forgotten password flow is invoked by Oracle Identity Manager. Similarly Oracle Identity Manager and Oracle Adaptive Access Manager are integrated for risk-based password authentication.

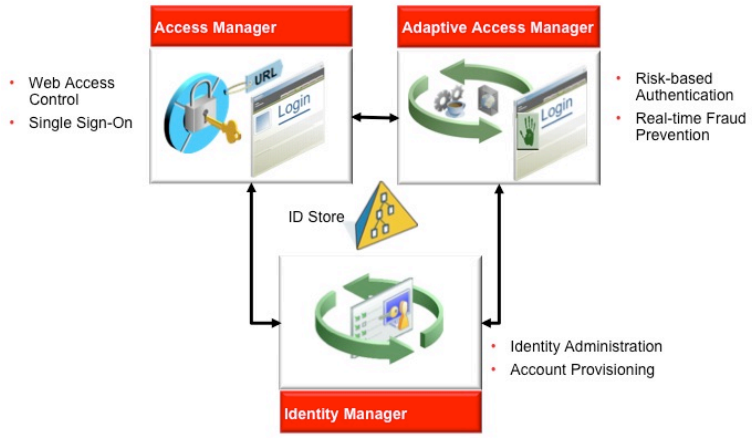

Figure 21: Oracle Identity Management Services Consolidation

Oracle identity management is provided by Oracle Identity Manager. Identity access and governance is provided by Oracle Identity Analytics.

Oracle Identity Manager

Oracle Identity Manager (OIM) typically answers the question "*Who* has access to *What*, *When*, *How*, and *Why*?". OIM is designed to administer user access privileges across a company's resources throughout the entire identity management life cycle, from initial on-boarding to final de-provisioning of an identity. OIM is a fully integrated platform for identity provisioning and administration as well as identity audit and compliance.

OIM is used both in enterprise-user-centric (intranet) environments, and customer- and partner-centric (extranet) environments.

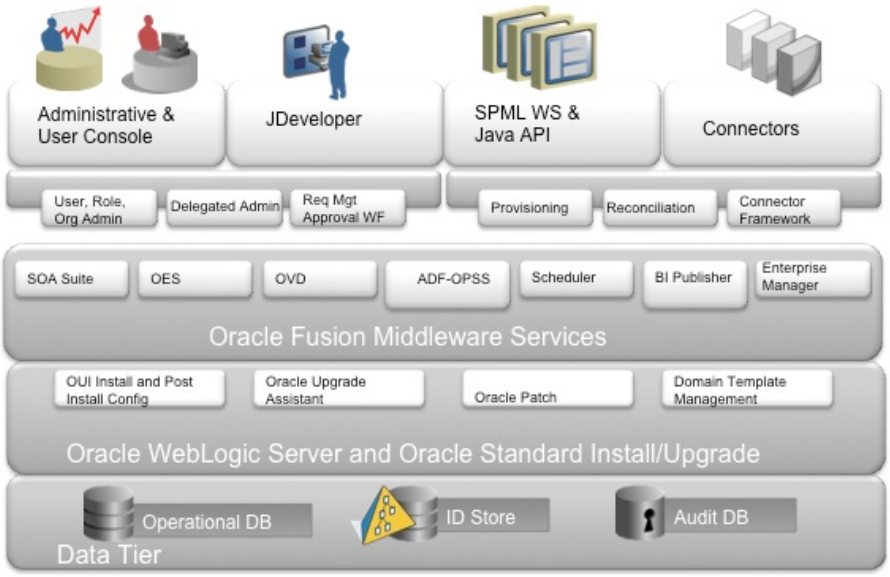

Figure 22: Oracle Identity Manager Architecture

In extranet environments, OIM's superior scalability allows enterprises to support millions of customers / partners accessing the company's resources using traditional clients (e.g., browsers) or smart phones. In this case, OIM provides centralized on-boarding and a combined self-registration interface to multiple enterprise applications, for example Oracle's PeopleSoft Enterprise Customer Relationship Management, Oracle E-Business iSupplier or Oracle E-Business iRecruitment, thus improving a company's ability to address increasing compliance and privacy regulations through centralized management of external users and partners.

OIM is a Java Platform, Enterprise Edition (Java EE) application that can be deployed in single- or multiple-server instances.

OIM's functional layers include:

New metadata model: All configurations in various components of OIM are stored centrally in an XML store (Metadata Store –MDS) common to the various services provided by Oracle Fusion Middleware (Oracle SOA, WebCenter, etc.). This new medatada model allows you to run multiple jobs performing different types of reconciliation against the same target.

User provisioning: Provisioning provides outward flow of user information from OIM to a target system (e.g., a business application). Provisioning is the process by which an action to create, modify, or delete user information in a resource is started from OIM and passed into the resource. The provisioning system communicates with the resource and specifies changes to be made to the account.

User administration: User administration includes self-service profile management (users can view and edit their own profile), administrative profile management (one can view and manage the profiles of other users subject to access permissions), request management (enables users to create provisioning requests for resources with fine-grained entitlements, profile management requests, and role membership requests – approvers use the same user interface to process requests), delegated administration (by moving administration points as close to the user as possible, an organization can achieve tighter control and better security).

Policy Management: OIM enables policy-based automated provisioning of resources with fine-grained entitlements. For any set of users, administrators can specify access levels for each resource to be provisioned, granting each user only the exact level of access required to complete the job. These policies can be driven by user roles or attributes, enabling implementation of role-based access control (RBAC) as well as attribute-based access control (ABAC).

Workflow Management: OIM supports the separation of approval and provisioning workflows. An *approval workflow* enables an organization to model its preferred approval processes for managing resource access requests. A *provisioning workflow* enables an organization to automate IT tasks for provisioning resources with the most complex of provisioning procedures. OIM provides the *Workflow Visualizer* that allows business users, administrators, and auditors to visualize task sequences and dependencies to understand process flow and the *Workflow Designer* to edit and manage the process flow. OIM's workflow leverages Oracle SOA's BPEL engine and Oracle JDeveloper at design time (see Figure 22).

Password management: Password management includes self-service (users can reset their own passwords), advanced password policies (password length, alphanumeric and special characters usage, etc.), password synchronization (OIM can synchronize or map passwords across managed resources and enforce differences in password policies among these resources). OIM is tightly integrated with Oracle Access Manager to support password management (detailed later in this document).

Audit and compliance management: Audit and compliance management includes identity reconciliation (OIM tracks the creation, update, and deletion of account across all managed resources – reconciliation is performed by the reconciliation engine described in the following paragraph), rogue and orphan account management (A *rogue account* is an account created "out of process" or beyond the control of the provisioning system; an *orphan account* is an operational account without a valid owner), attestation (also referred to as recertification, attestation is mandated by the Sarbanes-Oxley Act -- OIM offers an attestation feature that can be deployed quickly to enable an organization-wide attestation process that provides automated report generation, delivery, and notification).

Reconciliation: The reconciliation process involves generation of events to be applied to OIM. These events reflect atomic changes in the target system, and contain the data that has changed, the type of change, along with other information. The reconciliation events that are generated as a result of changes occurring in the target system must be managed in such a way that they meet various business requirements. OIM's event management APIs, the reconciliation APIs, and the UI to manage reconciliation events are protected by using authorization policies controlled by Oracle Entitlements Server.

Segregation of Duties: The concept of Segregation of Duties (SoD) is aimed at applying checks and balances on business processes. Each stage of a business process may require the involvement of more than one individual. An organization can convert this possibility into a requirement for all IT-enabled business processes by implementing SoD as part of its user provisioning solution. The overall benefit of SoD is the mitigation of risk arising from intentional or accidental misuse of an organization's resources. In the OIM implementation of SoD, IT privilege (entitlement) requests submitted by a user are checked and approved by an SoD engine and other users. Multiple levels of system and human checks can be introduced to ensure that even changes to the original request are vetted before the request is cleared. This preventive simulation approach helps identify and correct potentially conflicting assignment of entitlements to a user, before the requested entitlements are granted to the user.

Approval and request management: With OIM, account request and approval processes can be automated to meet your organization's needs. In intranet and extranet deployments, administrators, peers, or users themselves can initiate requests for access to resources and track the status of their requests through web applications and email notifications. OIM 11g features a new request model based on Oracle SOA's (BPEL) approval workflow (design and orchestration). Approval workflows are highly configurable to accommodate multiple approval processes and stakeholders. OIM 11g provides *Request Templates* for persona-specific request catalogs.

Policy-based entitlement management: OIM's policy engine controls fine-grained, attribute-level entitlements across managed applications through Oracle Entitlements Server-based authorization policies, automating IT processes and enforcing security and compliance requirements such as segregation of duties. Policy-based management of entitlements allows

multiple request and approval processes to be implemented and refined over time in parallel, reducing the total cost of implementation. *Universal Delegated Administration* is provided through the embedded Oracle Entitlements Server.

Integration and Adapter Factory: OIM integrates with any application or resource through highly configurable, agentless interface technology. Oracle provides a growing library of pre-configured connectors to popular applications and user repositories. Each connector supports a wide range of identity management functions and uses the most appropriate method of integration recommended for the target resource, whether it's proprietary or based on open standards. Connecting to proprietary systems might be difficult. OIM's *Adapter Factory* eliminates the complexity associated with creating and maintaining these connections. The *Adapter Factory* provided by OIM is a code-generation tool that enables you to create Java classes.

Oracle Identity Analytics

Compliance has become an integral part of the business requirements for identity and access management customers. To this effect, Oracle Identity Management 11g introduces a common Oracle Fusion Middleware audit framework as part of Oracle Platform Security Services. In addition, Oracle Identity Management 11g leverages Oracle Business Intelligence extensively for publishing reports on audited data.

Oracle Identity Analytics (OIA) offers additional functionality allowing administrators to analyze identity services in a holistic manner using business intelligence technologies and leveraging the wealth of information controlled by Oracle Fusion Middleware components.

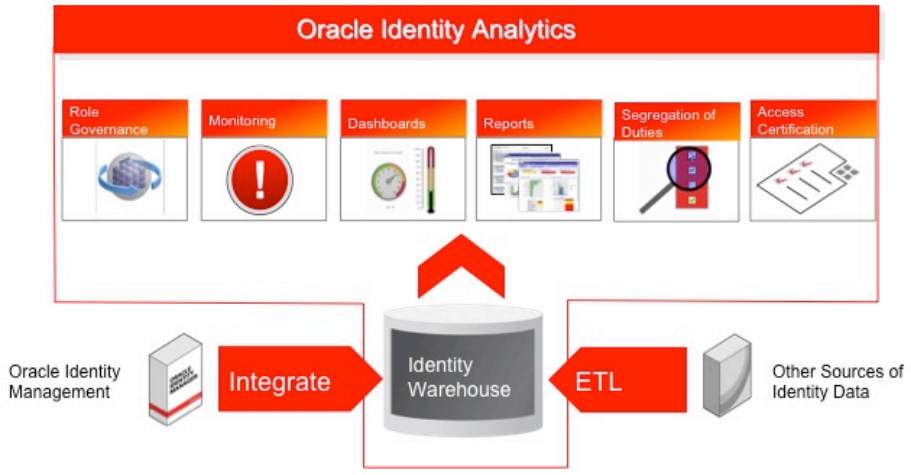

Figure 23: Oracle Identity Analytics

OIA's functional layers include:

Identity Warehouse: At the heart of OIA is the *Identity Warehouse*, which consolidates and correlates identities, resources, and entitlement information, thus providing a complete view of access-related data including the user's access; the "who, why, and where" of that access; whether the access violates defined segregation-of-duties policies; and activity associated with the access process.

Access Certification: OIA supports a variety of access certification features. Role certification allows for ongoing role certification by business unit managers or role owners. Entitlement and account level certification provides business managers and application owners with an efficient way to periodically review user access to various applications and business functions. OIA supports event-based access certification where access certification can be kicked off following a change in the user attribute. This is especially useful in monitoring access during a job change or a departmental change of an employee in order to ensure appropriate access. OIA provides an entitlement glossary allowing business friendly glossary names to either be imported or assigned to entitlements for display during certification. This aids in the review process by ensuring that the reviewers understand entitlements within the context of defined business processes.

Segregation of Duties: Segregation of Duties (SoD) policies can be defined in OIA at the role and policy level to prevent toxic combinations of entitlements assigned to any individual user. OIA supports both inter- and intra-application SoD policy enforcements and provides a complete life cycle management for policy violations. OIA joins forces with Oracle Identity Manager to support SoD, as shown in Figure 24.

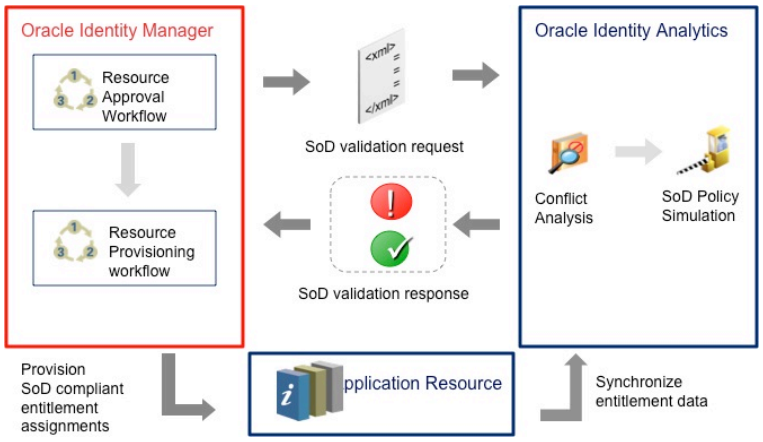

Figure 24: SoD Support With OIA and OIM

Compliance Reports and Dashboard: OIA provides a number of analysis and reporting capabilities within the various modules. Detailed history of every object as well as changes made to the

object and who made the change is captured and stored and may be analyzed to provide change management reporting. This includes a time-related capability, which can be leveraged for forensic analysis. Additionally, over 50 standard Business Unit, System, and Audit reports are provided out of the box, which can be further refined and customized. A graphical dashboard is available for providing executive style reporting via charts and graphs. The dashboard also provides a mechanism for historical and trend analysis.

Flexible Deployment: OIA can be deployed as a standalone product or in conjunction with a provisioning solution such as Oracle Identity Manager. A combined OIA-OIM solution provides an end-to-end identity administration solution providing support for role-base provisioning, access certification, compliant provisioning, automated remediation and analytics for all the targets integrated with OIM. Alternatively, OIA also provides a quick and easy way to import users and their associated entitlement data into its Identity Warehouse, allowing enterprises to get quickly enabled to perform access certifications. Not only does this provide a quick return on investment and immediate security surrounding user access, it also lays the foundation for provisioning thanks to the cleanup of inaccurate user access information.

Role Governance: OIA's role life cycle management and role governance supports information regarding change management (role change approvals, role versioning and offline copies, rollbacks, and role change impact analysis); role audit (role and entitlement mapping history, role membership history, approvals history, role ownership history); governance (role definition attestation, role membership attestation, role consolidation).

Cert360: Provides a 360-degree granular view of user access for educated decision-making, including a business glossary, audit exceptions, account status, historical data, approval data, attestation dashboards for compliance, closed-loop remediation with OIM integration.

Operational Manageability

Operational manageability includes the Management Pack for Identity Management and the new Oracle Identity Navigator.

Management Pack for Identity Management

Oracle Management Pack for Identity Management leverages Oracle Enterprise Manager's broad set of capabilities to administer end-to-end identity management components along with the rest of Oracle Fusion Middleware and Oracle Fusion Applications. Key capabilities include configuration and patch management, diagnostics and tuning, and monitoring with service-level agreement (SLA) management.

Oracle Identity Navigator

Oracle Identity Navigator (OIN) is a unified, single sign-on launch pad for all of Oracle Identity Management components. OIN can be used by administrators to see high-level performance and

operational metrics from the various Oracle Identity Management components. Likewise, end-users can perform self-services actions, and approvers can view various types of tasks assigned to them from a single console.

OIN is available (free of charge) to all Oracle Identity Management customers that license any Oracle Identity Management component.

OIN's functional layers include:

Navigator Administration Tab: A system administration-only tab used for product registration and Navigator configuration.

Personalization: Used to personalize OIN's portlets to show on the Dashboard and open the Resource Catalog for portlet selection.

Administration Console Launcher Portlet: A centralized portlet for launching all of the products included in Oracle Identity Management suite with support for single sign-on and access control (each product's administration console opens in its own browser window).

"My Report" Portlet: Supports user-selected reports with access control as well as real-time reports from Oracle BI Publisher.

News And Announcements Portlet: Provides RSS feed default from Oracle Metalink and supports configurable syndication feeds.

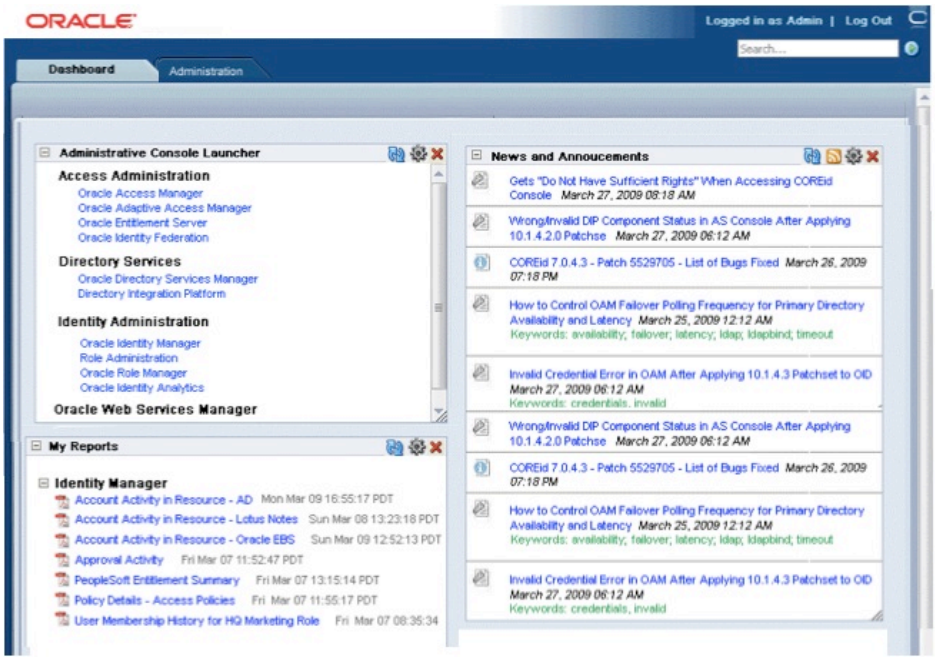

Figure 25: Oracle Identity Navigator's User Interface

Identity-As-A-Service

As mentioned previously, Oracle Identity Management leverages Oracle's Service-Oriented Security (SOS) platform to provide shared identity services delivered by the various components described in this document. In turn, Oracle's identity services are leveraged by the various Oracle Identity Management components as well as other Oracle Fusion Middleware components and Oracle Fusion Applications.

This section focuses on how Oracle Identity Management's various components work together (as well as with third-party environments) to provide integrated security across web transactions.

Details of how the various Oracle Identity Management services are integrated are provided in the *Oracle Fusion Middleware – Integration Overview for Oracle Identity Management Suite 11g Release* documentation manual.

OIM and Third-Party Environments Integration

OIM provides a wealth of provisioning connectors to target applications. In addition, OIM implements the industry-standard Service Provisioning Markup Language (SPML) to help organizations provide user access to resources without custom connectors, thus enabling rapid integration across heterogeneous environments.

Essentially, SPML defines interoperable management of provisioning services objects (PSO). A PSO represents information on a target resource, for example a provider would represent as an object each account that the provider manages.

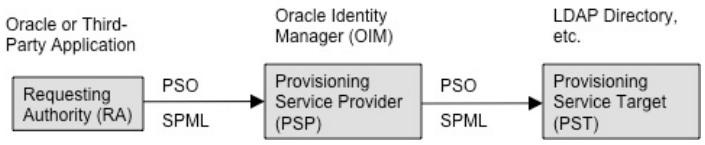

Figure 26: OIM Support for SPML

As shown in Figure 26, a requesting authority (RA) issues an SPML request (e.g., create user, assign role, etc.) to a provisioning service provider (PSP) such as OIM, which listens for SPML requests and processes them. The provisioning service target (PST) consumes the SPML requests it receives from the PSP.

Authentication, Identity Assertion, Authorization Integration

Figure 27 shows how Oracle Identity Federation, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Entitlements Server work together across the web, application, and data tiers.

Identity assertion directly relies on the integration of Oracle Access Manager with WebLogic Server (the identity asserter is provided by the latter).

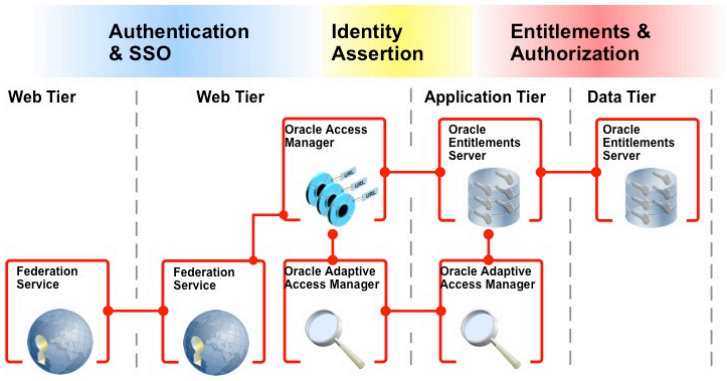

Figure 27: Authentication, Identity Assertion, Authorization Integration

OAM and OIF Integration

1. A user requests access to a protected resource. OIF intercepts the request and redirects it to OAM for authentication.
2. OAM challenges the user for credentials.
3. Upon successful authentication, OAM sets an SSO cookie and asserts the authenticated identity to the federation service (OIF).
4. OIF generates an authentication ticket (a SAML assertion) based on the information provided by OAM, and sends the (signed and encrypted) SAML assertion to a service provider.
5. At the service provider, OIF (or any other SAML-compliant security system) consumes the SAML assertion produced in step 4, locally authenticates the user and redirects the user to the target resource.

OAM and OWSM Integration

1. A user requests access to a protected portal resource. OAM intercepts the request and challenges the user for credentials.
2. Upon successful authentication, OAM sets an SSO cookie and asserts the authenticated identity to the portal application.
3. The portal application sends a web service request (SOAP) to a remote web service on the original requester's behalf.

4. An OWSM client agent intercepts the request before it leaves the portal. The OWSM client agent inserts the necessary security information in the SOAP message header (for example a signed SAML assertion or a simple username / password token), based on the asserted identity information provided by OAM.
5. The OWSM client agent sends the SOAP request to the remote web service.
6. At the remote web service site, either an OWSM server agent or a web-services-standards-compliant security system intercepts the incoming message and consumes the standards-based security information provided in the SOAP message header to enable authorized access to the remote web service.

OAM and OES Integration

1. A user accesses a protected web resource. OAM intercepts the request and challenges the user for credentials.
2. Upon successful authentication of the user, OAM sets a session cookie and authorizes the user to access the requested resource.
3. OAM asserts the authenticated user's identity and passes an authorization request to OES.
4. OES retrieves information about the trusted subject, resource request, and security context, and executes a dynamic role evaluation.
5. OES check the application authorization policy against the subject and role, and enforces the fine-grained resource access.

OES and OWSM Integration

OES provides support for fine-grained entitlements to OWSM. A web service may be selectively entitled to certain types of users based upon the contents of the messages being sent to the service itself. For example, consider an expense approval service. A rogue employee may attempt to hijack the service to get a bogus expense report approved by invoking the back-end services. Entitlements within the service gateway can detect this by looking inside the message structure and using contextual information to deny access. For instance, the policy may define that the approval service should be denied to the user if the expense report identity is contained in a list of pending reports for the user.

OWSM can delegate a service access decision to OES by passing down the identity of the user and contextual parameters that tell OES how to unpack data from the message itself when making an entitlement decision. OES can then take the message information and its own policies into account and provide a *grant* or *deny* response back to OWSM. OWSM can then enforce that decision.

Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager

In the Oracle Identity Management 11*g* release, OAM does not provide its own identity service. Instead, it consumes identity services provided by OIM, LDAP directories, and other sources, and it integrates with OIM and OAAM to deliver a range of secure password collection and challenge-related functionality to OAM-protected applications.

Integrating OAM, OAAM, and OIM provides the following functionality:

- Password entry protection through personalized virtual authenticators.
- Knowledge-based authentication (KBA) challenge questions for secondary log-in authentication based on risk.
- One-time password (OTP) challenge for secondary log-in authentication based on risk.
- Registration flows to support password protection and KBA and OTP challenge functionality.
- User-preference flows to support password protection and KBA and OTP challenge functionality.

OAAM is responsible for executing fraud rules before and after authentication, and navigating the user through OAAM flows based on the outcome of fraud rules. OIM is responsible for provisioning users (add/modify, delete users), and managing passwords (reset/change password). OAM is responsible for authenticating and authorizing users, and providing statuses such as Reset Password, Password Expired, User Locked, etc.

In this type of deployment, OAM redirects users to OAAM when a trigger condition for password management is in effect. The "trigger condition" is the authentication scheme used in OAM. OAAM interacts with the user based on lifecycle policies retrieved from OAAM, and when the condition is resolved, notifies OAM so that the user is redirected to the protected resource. OIM provides password policy enforcement (OIM's password management includes password policy support and self-service administration for password reset and password change). OIM provides centralized password management for other Oracle Identity Management components where password management is needed.

Oracle Identity Management and Other Oracle Technologies

Oracle Identity Management is at the intersection of several complementary Oracle technologies. The following sections describe how Oracle Identity Management integrates with Oracle's Governance, Risk, and Compliance (GRC) platform, and Oracle Database.

Oracle Identity Management and Enterprise Governance

Oracle's Governance, Risk, and Compliance (GRC) platform integrates business intelligence, process management, and automated controls enforcement to enable sustainable risk and compliance management.

Oracle Identity Manager and Oracle Access Manager are part of the multiple products making up Oracle GRC's infrastructure controls.

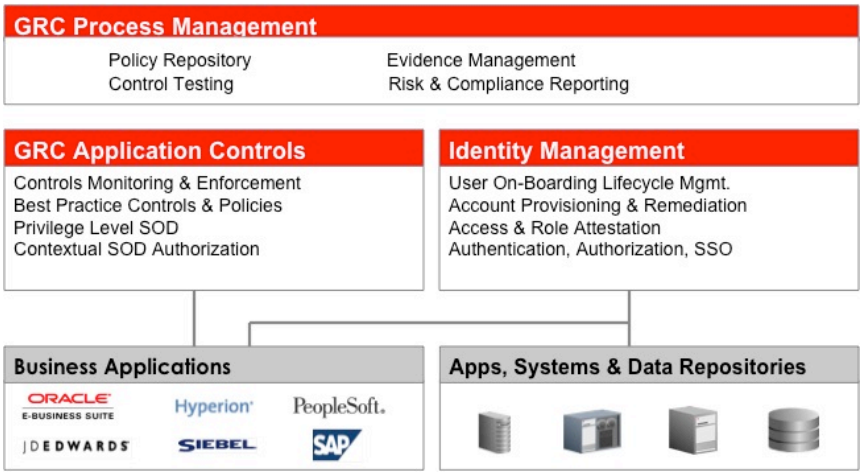

Figure 28: Oracle GRC and Oracle Identity Management Synergy

Segregation of duties (SoD) is a key principle of internal control and often the most difficult and costly to achieve, especially within critical business applications such as enterprise resource planning, customer relationship management, and supply chain management systems. Oracle Application Access Controls Governor, a key product in the Oracle GRC platform, allows customers to manage, remediate, and enforce enterprise resource planning SoD policies.

Enterprise resource planning roles and responsibilities are effectively segregated, thus minimizing the risk of fraud and ensuring regulatory compliance. Oracle Application Access Controls Governor also provides a comprehensive library of real-world, best-practice SoD controls for Oracle E-Business Suite and Oracle's PeopleSoft applications and is easily extensible to support

other platforms including Oracle's JD Edwards, Oracle's Siebel, and Oracle's Hyperion, as well as non-Oracle enterprise resource planning environments.

Oracle Identity Manager integrates with Oracle Application Access Controls Governor by performing real-time SoD validation prior to provisioning Oracle E-Business Suite roles and responsibilities to Oracle E-Business.

Oracle Identity Management and Oracle Database

One of the key differentiators of Oracle's identity management offering is its ability to provide customers greater flexibility and choice by integrating *Enterprise User Security* (EUS), a feature of Oracle Database, with Oracle Virtual Directory (OVD), enabling organizations to centrally manage database-user identities through their existing corporate directories such as Oracle Internet Directory, Microsoft Active Directory and Sun Java System Directory Server.

Thanks to the integration of OVD with EUS, organizations can now use virtualization capabilities to manage database-user identities and their privileged roles across diverse identity stores without having to migrate or synchronize the data.

Many organizations have dozens if not hundreds of Oracle databases. Users may access these databases for administrative functions. There are still many cases (in particular for reporting and custom applications built with Oracle Application Express) where local database accounts are used for access. Because of compliance challenges, local database accounts are harder to manage, which often results in expensive help desk calls when users forget their login credentials.

Oracle Identity Management provides a competitively distinctive solution leveraging Oracle Database's EUS feature. EUS allows the database to map both database usernames to LDAP users and database roles to LDAP groups. Additionally EUS can use LDAP passwords if client applications are using username/password authentication.

Typically, with Oracle Database, Oracle Virtual Directory can use its unique identity virtualization capabilities so that Microsoft Active Directory can be used to store the required database EUS metadata and user/role mappings. This allows customers to use their existing provisioning workflow to create the proper accounts and role-based privileges for users who need to access the database.

Additionally, customers can use Oracle Identity Manager to manage access to the database by building provisioning workflows to the enterprise directory to control access to the database.

Leveraging EUS simplifies compliance because there are fewer accounts to audit. It improves security because there are fewer systems to update when people change status. Finally, end-users benefit because they have fewer passwords to remember.

Please see *Oracle Directory Services and DB Enterprise User Security Deployment Options* on the Oracle Technology Network web site for more information.

In addition, as mentioned previously in this document, Oracle Internet Directory supports two unique database security features: *Oracle Database Vault* (enforcing separation of duty for database administrators) and *Oracle Transparent Encryption*.

Oracle Database Vault provides a unique capability for directory storage. It prevents identity data from being accessed or manipulated outside of the OID protocol listener(s). Products that use flat-file directory storage can often be modified by simply updating the proper file with a text editor. This can be a potential back door for either changing passwords or unauthorized access to sensitive data. Only OID with *Oracle Database Vault* can prevent this type of access.

Transparent Data Encryption is the Oracle Database feature that encrypts the data within the database. Even if someone gets unauthorized access to the database, they can't read the data. Encrypting data is a very simple way to prevent identity theft because the data can only be accessed through approved accounts.

Oracle Database Vault and *Oracle Transparent Data Encryption* allow Oracle to provide the only directory services with complete security from storage to the client.

Conclusion

With the introduction of Oracle Fusion Middleware 11g, Oracle fulfills its vision of delivering a complete, integrated, hot-pluggable, and best-of-breed middleware suite based on Oracle WebLogic Server, the industry's leading application server. As part of Oracle Fusion Middleware 11g, Oracle provides the latest enhancements to Oracle Identity Management.

Oracle Identity Management 11g ensures the integrity of large application grids by enabling new levels of security and completeness to address the protection of enterprise resources and the management of processes (both human and automated) acting on those resources.

Oracle Identity Management 11g provides enhanced efficiency through a higher level of integration, consolidation, and automation, and increased effectiveness in terms of application-centric security, risk management, and governance.

Oracle Identity Management 11g supports the full life cycle of an application, from development to deployment to full-blown production.

Oracle Identity Management 11g
July 2010
Author: Marc Chanliau

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

Oracle is committed to developing practices and products that help protect the environment

0109