Information Rights Management –
Managing information everywhere
it is stored and used

An Oracle White Paper
October 2009
Introduction........................................................................................................3
The problem.......................................................................................................4
  Limitations of current information security ..............................................4
  Limitations of repository-based information management ....................4
The solution........................................................................................................5
  Information-centric security ........................................................................6
  Managing information “beyond the repository” ......................................6
How information rights management works.................................................7
  Key architectural differentiators .................................................................9
Successfully deploying information rights management..............................9
Security..........................................................................................................10  
  Persistent control....................................................................................10
  Authentication.........................................................................................10
  Cryptography...........................................................................................11
  Tamper-proofing ....................................................................................11
  Breach response......................................................................................12
Usability ........................................................................................................12
  Support for heterogeneous enterprise environments........................12
  Easy integration into existing workflows ............................................12
  “Hands free” offline working ...............................................................13
Internationalization ................................................................................13
Manageability ...............................................................................................14
  Classification-based rights management .............................................14
  Standard rights model............................................................................15
  Role-based control of application functionality.....................................16
  Role-based administrative model .........................................................16
  Audit.......................................................................................................16
  Integration with enterprise infrastructure ............................................16
  Performance/Scalability .......................................................................17
Technology characteristics and specifications.............................................17
  Typical Oracle IRM deployment topology............................................17
  Integrating Oracle IRM .........................................................................18
  IRM component specifications ............................................................19
INTRODUCTION

Oracle Information Rights Management (IRM)\(^1\) is a new form of information security technology that secures and tracks sensitive digital information everywhere it is stored and used. Conventional information management products only manage documents, emails and web pages while they remain stored within server-side repositories. Oracle Information Rights Management uses encryption to extend the management of information beyond the repository – to every copy of an organization’s most sensitive information, everywhere it is stored and used – on end user desktops, laptops and mobile wireless devices, in other repositories, inside and outside the firewall.

Oracle Information Rights Management is information-centric security, in that it secures information directly, rather than as a side-effect of placing (some) copies of that information within access-controlled repositories. Oracle Information Rights Management is a Fusion Middleware service with profound and immediate synergies throughout the entire Oracle solution stack – particularly with Content Management, Records Management, Identity and Access Management.

Oracle Information Rights Management introduces some new elements into information workflows, such as encrypting (“sealing”) and classifying documents, emails and web pages, and the requirement to install Oracle IRM Desktop agent software on every end user device on which sealed information is created or used. The benefits of information-centric security are so considerable, and changes to existing workflows so minimal, that Oracle Information Rights Management is now routinely being adopted by enterprises and government agencies worldwide to secure their most confidential information\(^2\).

This technical whitepaper provides more detail on Oracle’s Information Rights Management solution – the problems it solves; how it works; the key features required for successful, large scale enterprise deployment; deployment topologies, SDKs and component specifications.

\(^1\) Oracle Information Rights Management was formerly SealedMedia E-DRM.

\(^2\) Oracle recently announced a key milestone: the millionth independent end user download of its Oracle IRM Desktop agent (a figure which excludes all the IRM Desktops centrally deployed by IT administrators).
THE PROBLEM

The problem that Oracle Information Rights Management solves is that the tools currently available to organizations to manage their digital information actually only apply to the small fraction of that information stored within managed repositories. The bulk of the information remains loosely managed, or not managed at all, as it circulates in the normal course of business to servers, desktops, laptops and mobile wireless devices, inside and outside the firewall.

Limitations of current information security

Information security today is really perimeter security – securing the perimeters within which information is stored, rather than securing information directly. Documents and emails are somewhat secure while they remain within access-controlled perimeters, such as file system folders, email inboxes, content management or collaborative repositories, etc. But these documents and emails are also routinely used and stored on thousands of desktops, laptops and mobile wireless devices – inside and outside the corporate firewall – from where they can be easily and untraceably opened, copied and forwarded … anywhere.

Perimeter security only secures information as a side effect of where it is stored or how it is transmitted. This results in several fundamental limitations:

- Conventional perimeter security stops dead at the firewall, even though sensitive information does not - because all modern enterprises and government agencies must share sensitive information externally, with partners, customers, suppliers and citizens.
- Copies of the same information end up stored within different perimeters, with different access controls (for example a price list copied from a sales folder to a marketing folder) or no access control at all.
- In practice there are too many perimeters to manage consistently, even if the information stayed in one place.
- Trying to further nest perimeters to share and segregate information between partners, suppliers and customers just makes matters worse.

Despite all the current investment in information security it is a remarkable fact that once information is shared today, no one knows who will be accessing it tomorrow.

Limitations of repository-based information management

Organizations invest millions of dollars in information management solutions that manage information in terms of security, auditing, search, records retention and disposition, version control, etc. These information management solutions are predominantly repository-based. To manage their information organizations store
their information in managed repositories, ranging from databases (for structured information) to enterprises content management systems and collaborative workspaces (for unstructured information).

The problem is that in the normal course of business many copies of this managed information are inevitably stored and used outside the repository, where they are no longer managed. The lack of security and auditing beyond the repository has already been discussed in the previous section, but version control and records management also provide excellent illustrations of the shortcomings of repository-based information management:

- Records management systems enforce record retention and disposition policies, for example ensuring that critical business records are retained for (say) seven years, during which they cannot be modified, and after which they are deleted so that they are no longer subject to the risk of legal discovery during a potential litigation. But again, deleting records from a records management repository will still leave hundreds of copies scattered around internal and external servers and desktops, from where they can be easily discovered using modern enterprise search tools.

- Content management systems provide powerful support for managing versioned documents, and ensuring that users can easily obtain the latest versions. But many users will still use out-of-date versions they have stored locally, outside the repository, for example from on their desktop or in their email inbox. This can result in costly errors, wasted work and failure to comply with current regulations and operating procedures.

The fact that repository-based information management solutions only manage a subset of an organization’s information can undermine the solution benefits – for example in regulatory compliance applications where ideally all the copies of the information should remain managed, regardless of where they are stored and used.

**THE SOLUTION**

Oracle Information Rights Management uses encryption (“sealing”) to shrink the access control perimeter down to the actual units of digital information – documents, emails and web pages – and this access control perimeter stays with the information everywhere it goes.

Figure 1: “Sealed” information remains managed – everywhere it goes
Oracle refers to the encryption process as “sealing”, which really encompasses three things:

- Wrapping the information within a layer of encryption, so that regardless how many copies are made, or where they are stored, they are of no use without the associated decryption keys.
- Embedding an indelible set of URL links into the sealed information, so that every copy points back to the Oracle IRM Server to which they are sealed.
- Digitally signing the information so that any tampering can be detected and prevented.

**Information-centric security**

The rights governing which users can access sealed information are stored separately from the information itself, on network-hosted Oracle IRM Servers owned and operated by the organization that owns the information. This brings several revolutionary benefits – that wherever sealed information is stored, transmitted or used:

- Unauthorized users cannot access it (this is the most important benefit).
- Only authorized users can open and/or modify it, in accordance with their assigned rights (for example, whether they can print especially sensitive information).
- All actual and attempted access to sealed information can be centrally audited and reported.
- Access to remotely stored information can be centrally revoked, for example when employees or contractors leave, or partner relationships end, even after remote copies have been made to DVDs, USB, etc.

Perhaps the most unique feature of Oracle Information Rights Management, compared to any other information security products is that it continues to manage information outside the firewall, even when that information is stored deep within the networks of other organizations, or at home. This is extremely important, because most modern business processes involve external parties, such as partners, suppliers, outsourcing/offshore, advisers, home workers, etc.

**Managing information “beyond the repository”**

Oracle Information Rights Management does more than just extend security and auditing beyond access-controlled repositories. It also extends other aspects of information management beyond the repository – such as records management and version management – extending associated solution benefits to every copy of an organization’s information, everywhere it is stored and used – on end user desktops, laptops and mobile wireless devices, in other repositories, inside and outside the firewall.
For example:

- If documents and emails that will be business records are sealed then not only can they be protected from tampering (by not assigning anyone rights to edit them) but, when the time comes for records disposition, every copy of those records can effectively be deleted by deleting the associated decryption keys from the Oracle IRM Server. This is a natural extension to Oracle’s Universal Records Management solution, which manages records stored across multi-vendor repositories, extending it still further, to apply to every copy of an organization’s records.

- If versioned documents are sealed within a content management repository (such as Oracle Universal Content Management) then Oracle Information Rights Management can be configured to automatically revoke access to old versions of documents when new versions are checked in to the content management repository. If users have stored the old version locally, outside the repository, then not only will they be denied access when they try to open the old version but, because of the URL links embedded into sealed files, they can be automatically routed back to the new version in the content management system. Ensuring that employees use up-to-date information can result in considerable cost savings for enterprises and government agencies, and ensure more complete compliance with regulations.

**HOW INFORMATION RIGHTS MANAGEMENT WORKS**

Oracle Information Rights Management has a patented architecture that distributes rights management between centralized IRM Servers and IRM Desktop agents, which must be installed on every user device on which users intend to create or use sealed information.

![Oracle Information Rights Management architecture](image)

**Figure 2: Oracle Information Rights Management architecture**
Figure 2 provides a step-by-step illustration of how the Oracle Information Rights Management architecture operates (omitting some components for clarity, for example the integrations between the Oracle IRM Server and enterprise authentication and directory infrastructure).

1. Authors continue to create documents and emails in their existing document and email applications such as Microsoft Office, Microsoft Outlook, Adobe Reader, Lotus Notes, etc.

2. Oracle Information Rights Management enables documents or emails to be automatically or manually sealed at any stage in their lifecycle, using sealing tools integrated into the Windows desktop, authoring applications, email clients and content management and collaborative repositories. Sealing wraps documents and emails within a layer of strong encryption and digital signatures, together with indelible links back to network-hosted Oracle IRM Servers (operated by the organization to which the information belongs) which store the decryption keys and associated access rights.

3. Sealed documents and emails can be distributed by any existing means, such as email, web, file share, etc.

4. The rights governing end user access to sealed documents or emails can be assigned at the time of sealing, or separately, the latter being much more typical in enterprise deployments (where end users do not want to make complex rights management decisions every time they author a new document or email). Rights are stored separately from sealed documents and emails on Oracle IRM Servers, which is what enables them to be assigned, updated or unassigned at any time.

5. To create and use sealed documents and emails within their existing desktop applications end users must download and install a single, universal agent called the Oracle IRM Desktop. The Oracle IRM Desktop is small, easy-to-install and is responsible for authenticating the user, transparently requesting rights from the Oracle IRM Server and protecting and tracking sealed documents and emails while "in use" within native desktop applications.

   Note: Oracle's patented distributed architecture automatically synchronizes user rights and audit records between the Oracle IRM Desktop and Oracle IRM Server, ensuring completely transparent offline working without sacrificing revocability or requiring end users to remember to synchronize.

6. The Oracle IRM Desktop and Oracle IRM Server together audit all attempted and actual end user access (online and offline) to sealed documents or emails, and all administrative operations such as assigning or revoking rights. The level of auditing is configurable and audit records can be stored in the Oracle IRM Server database, sent to message queues for use by external monitoring applications, or exported to log files for import by standard reporting tools.
7. The Oracle IRM Management Console and Oracle IRM Web Service SDK provide query-based audit reporting, with useful pre-defined reports such as "End User Activity" or "Item Activity" and user-defined reports. Oracle IRM auditing opens an unprecedented window onto the use (or abuse) of enterprise information on end user desktops, and this value-add feature alone often justifies investment in Oracle Information Rights Management, aside from its security benefits.

Key architectural differentiators

Two aspects of the Oracle Information Rights Management architecture are particularly important, and differentiate Oracle’s solution from other vendors in terms of its enterprise deployability:

- Oracle’s classification-based rights model (see later) results in users being assigned rights to related sets of information, rather than to individual files. This results in orders of magnitude fewer rights “under the hood”. Far fewer rights make it possible to periodically and automatically synchronize rights and audit records between the IRM Desktop and the IRM Server.

- Automated synchronization enables completely transparent mobile (offline) working sealed information, while retaining rapid centralized revocation and updating of rights.

Competing information rights management products manage rights on a per-file basis. For enterprise document and email volumes, this means that there are too many rights to allow automated synchronization to the desktop. Administrators of competing solutions are forced to choose between caching rights in perpetuity on desktops, to enable offline working (limited by requiring an initial online request) while sacrificing revocation, or retaining revocation by configuring short per-file offline periods but sacrificing offline working. Competing information rights management solutions cannot provide both offline working AND revocability.

SUCCESSFULLY DEPLOYING INFORMATION RIGHTS MANAGEMENT

For Information Rights Management solution to be successfully deployed and used throughout the heterogeneous desktop and server environments of a modern extended enterprise (and its partners, customers and outsourced or offshore suppliers) the solution must be secure, usable and manageable at enterprise scale (by end users, business process owners and administrators).

Note: While Information Rights Management may initially be purchased for specific applications, with limited numbers of internal-only users, the buyer should consider the broader applicability of Information Rights Management throughout their organization and avoid solutions that can only support specific application or operating system versions, or cannot support external users.
Security

While there can never be 100% security against determined attack by skilled or professional hackers Oracle Information Rights Management provides effective multi-layered security using several industry-standard and industry-leading security technologies. The result is a solution that is easy to use by authorized users, but difficult to use in unauthorized ways or to compromise. The elements of the layered security model include persistent control, authentication, cryptography, tamper-proofing and breach response mechanisms.

Persistent control

Oracle Information Rights Management can control every aspect of sealed document and email usage on end user desktops:

- **Who**: control who can and cannot open sealed documents.
- **What**: control access to sets (classifications) of documents, or to single documents.
- **When**: control when access begins and ends, and can revoke access at any time.
- **Where**: prevent sensitive documents from being accessed outside your network.
- **How**: control how users interact with documents on their desktops: with fine-grained control over opening, annotating, editing, change tracking, copying, printing, interacting with form fields or cells, viewing spreadsheet formulas, etc.

In all cases, this control persists for the lifetime of the sealed documents or emails, regardless of where they are stored and used.

Authentication

Oracle Information Rights Management currently supports three authentication mechanisms:

- Windows authentication (for single-sign-on, SSO)
- Username/password (for external users)
- Web-based authentication

Windows authentication transparently uses the existing Windows login sessions on end user computers. Username/password authentication is built into the Oracle IRM Server to support external users without requiring access to Windows authentication domains. Web-based authentication provides a means to login to an Oracle IRM Desktop based on an authenticated web browser session, using any authentication scheme supported by the web server and web browser. Web-based authentication requires some server-side web development, but can be used to
integrate the Oracle IRM Desktop with any web-based authentication system, such as RSA SecurID, PKI certificates, etc.

**Cryptography**

Oracle Information Rights Management uses industry-standard cryptographic algorithms throughout the system, for example:

- To encrypt and digitally sign documents and emails (referred to as “sealing”). This typically increases file size by less than 1%.
- To protect network communications between the Oracle IRM Desktop and other client-side components and the Oracle IRM Server.
- To protect rights cached by the Oracle IRM Desktop.
- To assist in tamper-proofing Oracle IRM software components.

The cryptographic algorithms used include:

- AES 128 bit encryption for bulk encryption.
- RSA 1024 bit encryption for key exchange and digital signatures.
- Tiger Hash message digest.

In addition, Oracle Information Rights Management uses several secondary algorithms, for example for software obfuscation.

**Tamper-proofing**

Cryptography does not prevent someone from grabbing images from a PC screen, or from attempting to tamper with the software. Oracle Information Rights Management therefore invests substantial effort in measures that prevent people from tampering with sealed information or the software, including:

- Low-level 'policing' of certain loopholes in applications or the underlying operating system, such as the ability to access virtual or video memory for memory- or screen-grabbing.
- Code-signing techniques such as used by Microsoft Authenticode.
- Layered code and interface obfuscation.
- Maintaining a trusted clock, rather than relying on the local PC clock.
- Preventing writing unsealed information to disk.

Oracle Information Rights Management is unable to fully protect against misuse by users who have rights to open sealed content. Examples of such misuse are:

- Use of a camera to take images of sealed information.
- Certain third-party screen-capture applications.
- Viruses and other malicious programs.
Breach response

In the event that security is breached, a robust system must have the capability to repair the breach. A fundamental feature of the Oracle Information Rights Management architecture is that the Oracle IRM Desktop routinely communicates with centralized Oracle IRM Servers. The product includes the ability to provide optional triggers within the Oracle IRM Server that can force the end-user to download and install security updates as required. Information owners may mandate a security update level for specific items of information. If the end user does not accept the update then they are not permitted further access to the sealed information.

Usability

Support for heterogeneous enterprise environments

Broad and deep support for current and legacy application and operating system versions is essential when sharing sensitive information across the heterogeneous end user environments of real-world enterprises and government agencies, where global subsidiaries, citizens, customers, partners or suppliers may be slow to upgrade to the latest application or operating system version. Oracle therefore supports the broadest and deepest range of current and legacy Microsoft and non-Microsoft application versions:

- Microsoft Office 2000-2007 (Word, Excel and PowerPoint)
- Adobe Acrobat or Reader 6.0+
- Email: Microsoft Outlook 2000-2007 and Lotus Notes 6.5-7.0
- Email: BlackBerry for Exchange and Domino, BES 4.1.6
- HTML and XML (Internet Explorer 6.0+)
- .TXT and .RTF documents
- GIF, JPEG and PNG images

Easy integration into existing workflows

While the value of managing sensitive documents and emails on end user desktops may be obvious to business process owners, it will be resented by end users if it impacts existing workflows. Oracle Information Rights Management includes several key usability features that ease the insertion of sealing into existing end user document and email desktop workflows:

- Single, small Oracle IRM Desktop installer requiring minimal administrative privileges.
- End users can create, open and use sealed documents from within their existing desktop applications.
Oracle Information Rights Management provides out-of-the-box support for full-text indexing and search of sealed files, using native Windows search capabilities.

Oracle IRM Desktop “trusted search” enables Windows Search to full-text index and search sealed files. Access to search is controlled just like any application functionality, enabling IRM administrators to control which users can search for which files.

“Hands free” offline working

A significant proportion of enterprise workforces are mobile, and must be able to use sealed documents and emails while offline. Oracle Information Rights Management is the only solution to offer “hands free” offline working, while retaining the ability to revoke access to sealed documents or emails.

The Oracle IRM Desktop automatically synchronizes end user rights to their desktop, without end user intervention (such as impractical schemes requiring identification and “leasing” of specific documents or emails prior to going offline). Oracle IRM “roles” have configurable offline periods, set to represent a balance between usability for mobile workers and security (rapid revocation for more sensitive content). Sealed documents and emails can be created and used while offline, and operations such as opening and printing are logged into a secure offline cache for later transmission to the Oracle IRM Server, resulting in a complete chronological record of offline end user access to sealed documents and emails on remote desktops.

Internationalization

The Oracle IRM Desktop is available in English, French, German, Spanish, Italian, Dutch and Brazilian Portuguese variants, providing localized integration of Oracle Information Rights Management functionality into applications including Windows Explorer, Office, Outlook, Notes and GroupWise. For example, options to seal documents and email are presented by localized toolbars and menu options.

The Oracle IRM Desktop can use all localized Office variants to display sealed Office documents, and provides comprehensive control of localized Office menus, toolbars, and dialogs for English, French, German, Italian, Spanish, Danish, Dutch, Norwegian, Portuguese, and Swedish Office variants. For other language variants the Oracle IRM Desktop provides broad control with some limitations.

- Compose sealed emails within standard email clients, then automatic “seal on send”.
- Right-click sealing, resealing and creation of sealed documents from within Windows Explorer.
- Single-sign-on to NT domains, and “login automatically” for non-NT authentication.
- Error and exception handling (such as “No Rights”) via integrated self-service web application.
- Out-of-the-box support for full-text indexing and search of sealed files.

Few things better illustrate the superior usability of the Oracle Information Rights Management solution than its “hands free” support for mobile (offline) working.

Safely share sensitive information with your international partners, knowing that it remains protected and tracked, and that the Oracle IRM Desktop supports sealed information in almost all languages.
The Oracle IRM Standard Rights Model web application is available in English, French, German, Spanish, Italian, Dutch and Brazilian Portuguese variants, providing localized variants of web pages, new user notification emails and administrative and document roles.

### Manageability

**Classification-based rights management**

Oracle’s unique classification-based approach to rights management enables organizations to easily manage access to large volumes of sensitive information in terms of existing business processes or information classifications (such as “Board Communications” or “Top Secret”), existing employee roles (such as “Reviewer”), and existing users and groups defined in enterprise directories (such as “Sales”).

The above diagram illustrates the simplicity and power of classification-based rights management. Eight files have been sealed to two pre-defined classifications (“Executive Communications” and “Company Announcements”). The CFO and HR Director users and the All Employees group have each been assigned appropriate roles for each of the classifications, resulting in four rights assignments for a total of eight documents. Much of the scalability and manageability of the Oracle Information Rights Management solution comes from the fact that as the number of sealed documents grows from eight to eighty thousand over a period of time, there could still only be four rights assignments, because rights are managed at the level of classifications rather than individual files. With orders of magnitude fewer rights to manage, transmit and store than competing IRM solutions (which are based on per-file rights management) Oracle offers unparalleled consistency and scalability even when running on relatively modest server hardware.

Oracle Information Rights Management supports the inevitable real-world exceptions to classification-based policy by enabling administrators to easily...
configure per-user or per-file exceptions, which is far more effective than attempting to implement enterprise policies based on millions of individual per-user and/or per-file rights. Once classifications and roles have been defined, and users assigned roles, the only ongoing decisions made by authors are to which classification to seal their latest sensitive document or email. Most end users do not even need to make those decisions, since they will be reading, reviewing or updating pre-sealed documents or emails. This last point is critical to effective use at enterprise scale.

**Standard rights model**

Correct configuration is important to get the best out of most IT products, but it is especially important for Information Rights Management. No organization wants to lose control of encrypted information, or to place unnecessary authentication and authorization barriers between authorized users and the information they need to do their jobs.

Oracle Information Rights Management is the only IRM solution to have built over five years of best-practice consulting and successful deployment experience directly into the product – as a feature called the Oracle IRM Standard Rights Model – an easy to use web application which includes pre-defined end user and administrative roles, template classifications, automated user provisioning and email notifications, online self-help and end user and administrative tutorials.

![Figure 4: Standard rights model](image)

Oracle Information Rights Management is the only IRM solution to have built over five years of best-practice consulting and successful deployment experience directly into the product – as a feature called the Oracle IRM Standard Rights Model – an easy to use web application which includes pre-defined end user and administrative roles, template classifications, automated user provisioning and email notifications, online self-help and end user and administrative tutorials.

The intuitive end user and administrative Oracle IRM Standard Rights Model is a key ingredient in enabling customers to adopt Information Rights Management quickly and successfully from the outset, with a proven rights model that can immediately scale out across and beyond the organization – from 100 to 50,000+ users.
Role-based control of application functionality

Oracle Information Rights Management's close integration with desktop applications provides enterprises with fine-grained control and tracking of the use of sensitive documents and emails on remote desktops. Oracle enables business process owners to distinguish between viewing, annotation and editing; to enforce change tracking; and to control printing, copying and interaction with form fields or cells, hide sensitive formulas, etc. All application controls are assigned to end users via reusable roles (such as “Contributor”, “Reviewer” or “Reader) which map directly onto actual roles within existing business processes.

Role-based administrative model

Oracle Information Rights Management differs from other IRM solutions in that it has a role- and classification-based administrative rights model that is every bit as fine-grained as its end user rights model. Administrative operations such as creating security classifications, defining roles and assigning per-classification or per-item rights can all be segregated or delegated to different users or groups. Business process owners and their assistants can now easily manage the security of their most sensitive information, without imposing undue load on IT administrators (or granting them blanket access via coarse-grained and inflexible “superuser” accounts).

Audit

Oracle Information Rights Management audits all online and offline end user access to sealed documents or emails, and all administrative operations such as assigning or revoking rights. The level of auditing is configurable and audit records can be stored in the Oracle IRM Server database, sent to message queues for use by external monitoring applications, or exported to log files for import by standard reporting tools.

The Oracle IRM Management Console and Oracle IRM Web Service SDK provide query-based audit reporting, with useful pre-defined reports such as "End User Activity" or "Item Activity" and user-defined reports. Oracle IRM auditing opens an unprecedented window onto the use (or abuse) of enterprise information on end user desktops, and this value-add feature alone often justifies investment in Oracle Information Rights Management, aside from its other security benefits.

Integration with enterprise infrastructure

The Oracle IRM Directory Gateway integrates with enterprise LDAP directories such as Microsoft Active Directory, Oracle Virtual Directory and Sun ONE Directory Server to synchronize the Oracle IRM Server with centralized user and group definitions. The Oracle IRM Directory Gateway also supports script and plugin extensions for synchronizing users and groups from enterprise databases, Windows domains or other sources. Oracle Information Rights Management also includes comprehensive and easy-to-use Oracle IRM Web Service SDK for custom
integration with additional enterprise infrastructure such as web applications, content management and collaboration systems, content filtering scanners, etc.

**Performance/Scalability**

The extensive caching inherent in Oracle’s patented “distributed” IRM architecture, combined with a rights model that assigns users rights on a per-classification basis as opposed to a per-file basis, results in massively less network traffic and load on the Oracle IRM Server than other IRM products, and therefore achieves exceptional scalability and resilience at modest hardware cost. With normal enterprise settings a single Oracle IRM Server, running on relatively modest server hardware, has shown in testing and real-world deployments that it can support over 50,000 users.

**TECHNOLOGY CHARACTERISTICS AND SPECIFICATIONS**

Oracle Information Rights Management has four key components:

- **Oracle IRM Server** – stores the decryption keys and rights governing end user access to sealed documents and emails.
- **Oracle IRM Desktop** – enables authorized users to create and use sealed information, subject to rights obtained from the Oracle IRM Server.
- **Oracle IRM Management Console** – enables administrators to manage every aspect of the Oracle Information Rights Management solution.
- **Oracle IRM Standard Rights Model** – web application enabling business and IT administrators to create new users, assign roles, etc.

**Typical Oracle IRM deployment topology**

The figure below illustrates a typical deployment of Oracle Information Rights Management.

![Figure 5: Typical Oracle IRM deployment topology](image-url)
A single server, typically hosted in the DMZ, runs the Oracle IRM Server and the Oracle IRM Standard Rights Model web application. The Oracle IRM Server uses a high-availability database cluster hosted in the organization’s private network. All end users need the Oracle IRM Desktop, and some users with administrative roles may also need the Oracle IRM Management Console. Encrypted client-server communications are tunneled through HTTP and by default use port 80 (highly recommended).

This is a simple but representative deployment topology, capable of scaling to large user and information volumes. More sophisticated topologies may include hosting a second Oracle IRM Server in the private network (providing a double assurance that external users cannot access internal-only information). The Oracle IRM Server stores all its internal state in the database, and caching can be disabled, so secondary Oracle IRM Servers can be deployed in failover configurations.

**Integrating Oracle IRM**

Although Oracle Information Rights Management can meet the needs of many organizations out-of-the-box, it is also designed for easy integration with third party products and infrastructure.

The Oracle IRM Web Services SDK provides documentation and samples for a comprehensive set of SOAP/WSDL web services (implemented by the Oracle IRM Server) which provide developers with access to sealing and administration services. Typical applications for the Oracle IRM Web Services SDK include:

- Dynamically sealing files as they enter or leave a repository, for example file shares, content management systems, collaborative repositories, etc.
- Temporarily unsealing files so that they can be indexed (for full-text search), transformed to other formats (e.g. Word to PDF), or scanned for malware.
- Sealing or resealing files as part of automated business process workflows.
- Integrating Oracle IRM with user provisioning systems, for example adding/removing users, assigning/unassigning roles, etc.

All these web services are subject to the same user and administrative rights model as other Oracle IRM components.
**IRM component specifications**

### Oracle IRM Server

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Standard server hardware (for example, HP Proliant DL300 series) with minimum 256 MB RAM. Fast disks and network cards are recommended.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>Oracle 10g or 11g; or Microsoft SQL Server 2000 or 2005. If the database is remote the Oracle IRM Server system needs the relevant database client software. Database disk space of 2GB recommended to allow for audit records.</td>
</tr>
<tr>
<td>Network</td>
<td>One IP address with a public address allocation.</td>
</tr>
<tr>
<td>Firewall rules</td>
<td>HTTP-based connections to server – ideally on port 80. ODBC connections from server to database (if remote).</td>
</tr>
</tbody>
</table>

### Oracle IRM Desktop

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Standard desktop PC, 10 MB free disk space.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Microsoft Windows 2000, Windows XP or Windows Vista</td>
</tr>
<tr>
<td>Formats/applications</td>
<td>See previous section on “Support for heterogeneous enterprise environments”.</td>
</tr>
<tr>
<td>Browser</td>
<td>Requires Internet Explorer 6.0+ to be installed (does not need to be default browser).</td>
</tr>
<tr>
<td>Install</td>
<td>8MB MSI installer, requires administrator or elevated install privileges. Support for silent/managed installations.</td>
</tr>
</tbody>
</table>

### Oracle IRM Management Console

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Standard desktop PC, 20 MB free disk space.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating system</td>
<td>Microsoft Windows 2000, Windows XP or Windows Vista.</td>
</tr>
<tr>
<td>Browser</td>
<td>Requires Internet Explorer 6.0+ to be installed (does not need to be default browser).</td>
</tr>
<tr>
<td>Install</td>
<td>5MB MSI installer, requires administrator install privileges. Support for silent/managed installations.</td>
</tr>
</tbody>
</table>
### Oracle IRM Standard Rights Model

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Standard server hardware with minimum 256 MB RAM.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web server</td>
<td>Microsoft IIS 6.0</td>
</tr>
<tr>
<td>Network</td>
<td>One IP address with a public address allocation.</td>
</tr>
<tr>
<td>Firewall rules</td>
<td>HTTP-based connections to server – ideally on port 80. Email routing – either allowing access to a remote SMTP pickup folder, or allowing a local SMTP server to send email.</td>
</tr>
</tbody>
</table>

### Oracle IRM Directory Gateway

<table>
<thead>
<tr>
<th>Hardware</th>
<th>Standard server hardware with minimum 256 MB RAM.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directories</td>
<td>Syncs users/groups from Microsoft Active Directory, Oracle Virtual Directory, Sun ONE Directory Server (and other LDAP directories, subject to validation).</td>
</tr>
</tbody>
</table>