Oracle Information Rights Management 11g – Managing information everywhere it is stored and used

An Oracle White Paper
March 2010

ORACLE

Oracle Information Rights Management 11g - Managing information everywhere it is stored and used

Oracle Information Rights Management 11g - Managing information everywhere it is stored and used

INTRODUCTION

Oracle Information Rights Management extends information management beyond the repository and beyond the firewall – managing sensitive information regardless of how many copies are made, or where they are stored and used – inside and outside the firewall.

Oracle Information Rights Management (Oracle IRM) extends security, control, and tracking of sensitive information beyond repositories and beyond enterprise perimeters – protecting every copy of an organization's most sensitive information, everywhere it is stored and used – on end user desktops, laptops and in disparate repositories, inside and outside the firewall. Most information management solutions only control documents, emails, web pages, and media files while they remain stored within server-side repositories – or, at best, while they remain within the enterprise perimeter.

Oracle IRM provides **information-centric security** - meaning that it applies directly to information assets, rather than relying on the security settings of the various locations in which the assets are stored.

SECURITY INSIDE OUT

Oracle Information Rights Management is a Fusion Middleware service that complements database and application security by extending protection and tracking to all copies of information that might be downloaded and distributed.

Oracle IRM is a Fusion Middleware service that forms part of Oracle's comprehensive information security and compliance portfolio. Oracle security solutions enable Oracle customers to protect information in the database, to protect mission-critical enterprise applications by managing user identities, authentication, authorization, roles, and entitlements, and to extend that protection to information that might be downloaded or distributed from applications, or created and managed on end-user desktops and laptops.

This technical whitepaper provides an overview of Oracle Information Rights Management – the problems it solves; how it works; the key features required for successful, large scale enterprise deployment; deployment topologies, SDKs and component specifications.

THE PROBLEM

Most information security technologies do not really secure information; they secure the locations where information is stored, and the perimeters across which information might be distributed.

Most efforts to protect sensitive information focus on one or two factors:

- Guarding the **locations** or **repositories** where information is stored and managed – for example, by applying access controls to folders, and authentication and authorization frameworks to collaborative environments and business applications.
- Guarding the **perimeters** across which information might be distributed – for example, by blocking or quarantining information, or encrypting it before allowing it to proceed.

Solutions based on file location typically do not cater for the fact that authorized users routinely check-out or download copies of information, and that many applications distribute copies of information, for example, by email. Each location – each shared folder, each application repository, each collaboration system, each local or removable drive - offers different security settings and models, such that information receives inconsistent protection – or none.

Meanwhile, blocking information at perimeters can frustrate perfectly legitimate business requirements to share information. In some cases, information may be encrypted prior to release beyond the perimeter, but encryption alone provides no control or tracking of subsequent usage of the decrypted information. Control and tracking stops dead at the firewall.

And there are just so many locations and so many perimeters to guard - with each having the potential to enforce a different security model, or be controlled and perhaps bypassed by a different set of administrators. And many of these locations and perimeters may be beyond your direct control, as your information is handled and stored by partners, regulators, and suppliers.

Because of the limitations of location and perimeter security, Oracle IRM applies directly to the information assets – the sensitive documents, emails, web pages, and media files. For sure, the assets are encrypted, so they can be distributed beyond your perimeter, but the solution continues to control and audit even after delivery and authorized decryption – and access rights can be changed or revoked at will.

Of course, this is not to say that repository and perimeter security have no value. Indeed, IRM is often at its most powerful when used in conjunction with those modes of security enforcement, such that policies defined by applications and perimeters continue to apply even after information is distributed beyond them.

The following sections describe the IRM solution, and how it can extend and enhance both repository and perimeter security.

THE SOLUTION

Oracle IRM uses encryption to place information into a"virtual" managed repository – but one that stays with the information, regardless of how many copies are made, or where the information is stored and used.

Oracle Information Rights Management shrinks the access control perimeter right down to the actual units of digital information – documents, emails, images, web pages – regardless of location. Oracle refers to this as **sealing**. No matter where a sealed asset goes, or how many copies are created, Oracle IRM retains control and visibility according to policy defined on an Oracle IRM Server.

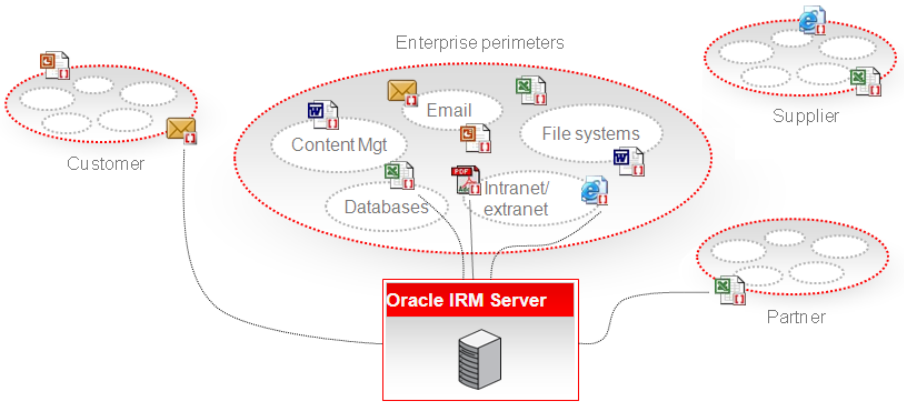

Figure 1: "Sealed" information remains managed everywhere it goes

Sealing encompasses three things:

- Encrypting the information so that no matter how many copies are made, or where they are stored, they are useless without the relevant decryption keys.
- Embedding metadata - including URL links to the Oracle IRM Server that manages policy and auditing for the information.
- Digitally signing the information to guard against tampering.

Once sealed, the information is only accessible to authenticated, authorized users and applications and, unlike ordinary encryption solutions, IRM guards against the creation of copies of the decrypted content. This means that information can continue to be protected and tracked for its entire lifecycle – not just until an authorized user decrypts it for use – and information owners retain the option to change or revoke access even after distribution.

The Separation of Rights from Content

Wherever "sealed" information is stored, transmitted or used – unauthorized users cannot access it, all actual or attempted access is centrally audited, and authorized access can be revoked at any time – even after copies made to DVD, USB, etc.

The rights governing who 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 powerful benefits – that wherever sealed information is stored, transmitted or used:

- Unauthorized users cannot access it (this is the most important benefit).
- All actual and attempted access to sealed information can be centrally audited and reported.
- Usage may be constrained in accordance with policy. Most obviously, for example, printing or editing can be restricted. More significantly, the creation of unsealed copies can be prevented – the user can decrypt the information so that they can work on it, but they cannot save a decrypted copy.
- Different users and groups can be given different roles for the same information. For example, some may be defined as Readers for a specific time period, whereas others may be Contributors with longer term access.
- Policy for particular documents, or for entire classifications of content, can be modified at any time. For example, some users may be stripped of access rights while others are added. Since the documents themselves do not contain a statement of policy, there is no danger of obsolete policies continuing to apply to content that has already been distributed.
- Access to all copies 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 powerful 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 copied to home systems. This is extremely important, because most modern business processes involve external parties, such as partners, suppliers, outsourcing/offshore, advisers, home workers, etc.

Oracle IRM provides superior scalability and governance by means of a unique classification-based policy model that enables very large numbers of information assets to be protecting by a very small, manageable policy set.

Classification-Based Rights Management

A significant challenge created by protecting individual documents, emails, and so on is that this can very easily lead to an unmanageable number of policies and tie business workflows into knots. Potentially, each business user and application could define unique rules for each document, creating great inconsistency and an overwhelming administrative burden. From a governance and compliance standpoint, it can rapidly become difficult to ensure or demonstrate that information really is being protected as required.

Oracle IRM addresses this challenge with a unique classification-based rights model that enables a very large number of documents to be protected by a very small, manageable number of policies. Each policy has clearly defined business ownership and, in most deployments, the solution guards against the creation of ad hoc policy at the whim of individual business users. Indeed, the management of IRM policies may simply be a facet of a broader security infrastructure that manages roles and rights for a range of business data and applications.

In practical terms, what this means is that users and applications are invited to pick the most appropriate classification for their documents – rather than being invited to make up policy for themselves.

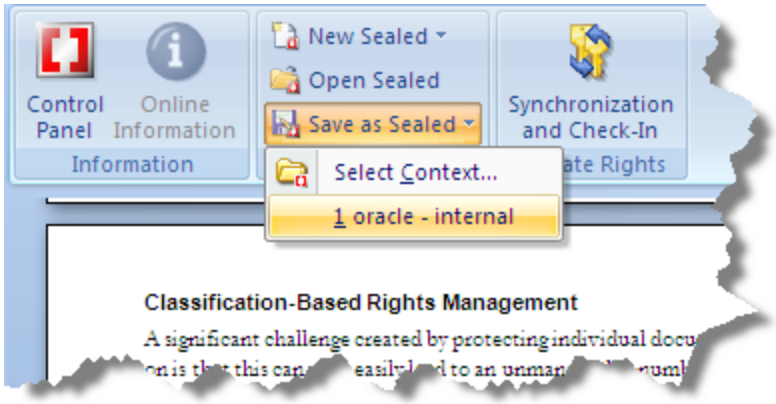

Figure 2: Sealing Involves Simply Selecting an Appropriate Classification

All documents in a particular classification are subject to the same policy by default (exceptions may be made if required) and any policy changes apply consistently to the entire classification.

By contrast, other solutions usually allow users to define their own policies, or to pick something that appears to be a classification, but is actually a static copy of a policy as it stood at the time of protection. If the policy changes, existing documents may not be subject to the new rules – creating security and compliance issues for potentially thousands of documents.

Extending Repository Security With Oracle IRM

Managing information by placing it within repositories only ever manages a small subset of an organization's information. Use or misuse of the thousands of unmanaged copies of information - which have been shared with other organizations, or stored on end user devices – can result in significant costs and liabilities.

Oracle IRM has a significant role to play in extending the information management capabilities of content management and collaboration systems – not just in terms of security, but also in terms of records and retention management, version control, and auditing.

For each of these capabilities, control only really applies to the "master copies" that are stored in the repository. For example:

- Records and retention policy may state that you can dispose of a set of documents after, say, seven years – but copies are typically going to survive outside the repository long after the disposal date, on local drives, on USB keys, in the hands of third parties, and so on.
- Version control policy may state that only the latest versions of a standard operating procedure, design document, or legal contract are to be used – but the repository has no way to prevent users from reading, modifying, and circulating older versions.
- The same policy may also state that a document can only be revised by particular users, but in practice a repository can only control who can successfully upload new versions – it cannot control whether users are changing and circulating local copies.

In truth, repositories only manage a subset of an enterprise's information – and the inability to control and track all copies in circulation can expose the enterprise to significant security and compliance risks.

Oracle IRM enhances information management in a number of ways:

- Sealing business records can not only make them tamper-proof (by not assigning anyone rights to edit them) but also enables the enterprise to make all copies permanently inaccessible when the disposal date arrives.
- IRM policy can ensure that rights for old versions of documents are reduced or revoked when new versions are published, and can automatically provide users with links to the latest version.
- IRM policy ensures that edit rights are only available to the subset of users who are currently supposed to be revising documents. Other users of the documents will have read-only access.
- IRM auditing provides an insight into the distribution and usage of documents. Information owners can see where their documents are being used, and verify that users are being denied access to obsolete documents and using new versions instead.

Extending Perimeter Security With Oracle IRM

Data Loss Prevention systems can use Oracle IRM web services to seal information that is identified as being too sensitive to circulate otherwise. Where DLP monitoring and tracking ordinarily stops at the perimeter, Oracle IRM allows it to continue in remote networks.

Oracle IRM can also add significantly to security initiatives that focus on the flows of information across perimeters ranging from USB ports through to the corporate firewall, and through critical systems, such as the email system, that can act as vectors for data loss – initiatives that fall under the broad definition of data loss prevention (DLP).

Such solutions aim to recognize sensitive information using a range of mechanisms from simple pattern matching through to more complex, contextual forms of analysis. Once identified, policy determines whether information is allowed to continue on its journey or be subject to a range of remedial actions such as blocking and quarantining.

The challenges faced by these solutions is that there are so many and varied perimeters to worry about, and that once information is allowed beyond your perimeters there is no way to claw it back.

Nor is it plausible for such solutions to continue monitoring any information on third party networks – no organization is likely to allow its own information flows to be exhaustively monitored to satisfy the security needs of a third party.

The closest such solutions get to persistent protection of information is to apply encryption – but tracking stops at the perimeter, and protection stops once the information is decrypted by the recipients.

This obliges organizations to make a choice – block and frustrate business communications, or allow communications, raise alerts, and accept the risks. There is a growing recognition that moving from passive monitoring to active intervention is a big step, as so much depends on the quality of the content analysis algorithms.

Oracle IRM works in powerful alliance with DLP simply by sealing information according to policy before allowing it to continue on its way – the DLP system calls Oracle IRM web services to seal as required. This provides business-friendly encryption, but also persistent protection, revocability, and tracking. Oracle IRM acts as a safety net that continues to apply DLP policy, even if that policy changes, for the lifetime of the information.

HOW INFORMATION RIGHTS MANAGEMENT WORKS

Oracle IRM has a unique, distributed architecture that enables completely transparent mobile (offline) working – without sacrificing centralized revocation, or requiring users to remember to synchronize rights.

Oracle IRM 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.

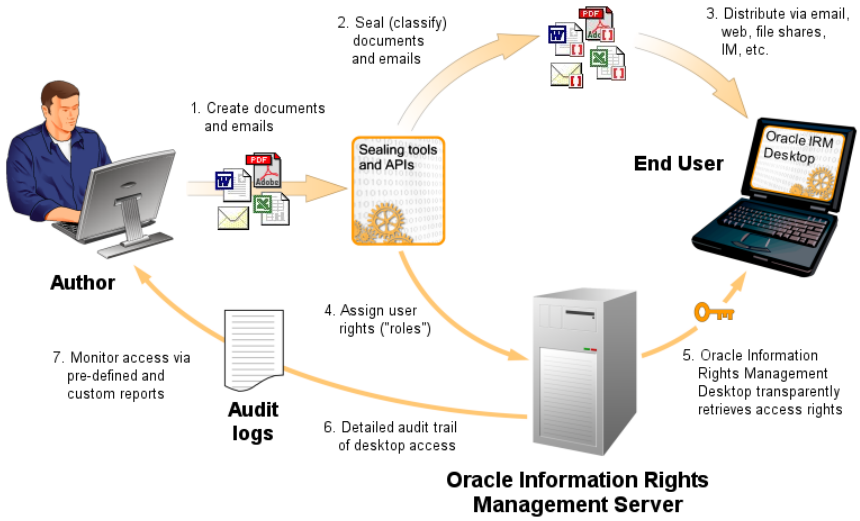

Figure 3: Oracle Information Rights Management Architecture

Figure 3 provides a high-level illustration of how Oracle IRM operates.

1. Authors continue to create documents and emails with familiar tools - Microsoft Office, Microsoft Outlook, Adobe Reader, Lotus Notes, etc.
2. Documents are sealed automatically or manually at the appropriate point in their lifecycle – during document creation, or during up to a folder or repository, or at a particular milestone in a workflow.
3. Sealed documents are distributed in the usual ways - email, web, file share, USB memory sticks, and so on.
4. The details of the policies that govern access and usage are stored on Oracle IRM Servers and can be assigned, modified, or revoked at any time.
5. The Oracle IRM Desktop agent provides secure and transparent management and synchronization of rights and keys, and controls rendering applications in accordance with user rights.
6. The Oracle IRM Desktop regularly uploads audit data to the server.
7. Audit data is available via web services and the IRM console so that all usage and attempted usage, online and offline, can be tracked. (In some cases, auditing is sufficient justification in itself for an IRM deployment.)

Key Differentiators

By managing per-classification rights, as opposed to per-file rights, Oracle IRM generates orders of magnitude fewer rights "under the hood". This enables regular synchronization of rights - even at enterprise scale. The rights model also provides clarity of information ownership, rather than relying on the best efforts of thousands of authors.

Oracle IRM has numerous significant differentiators that set it apart from rival solutions – especially when deploying at enterprise scale:

- Oracle IRM's classification-based rights model results in orders of magnitude fewer rights "under the hood". This slim-line model enables IRM to serve users with ALL of their rights pro-actively rather than on request.

  Rival solutions typically require a client-server communication at the point of use for most document accesses - resulting in frustration for offline users. Users often need to take manual steps to be confident of offline access.

- The same slim-line rights model enables regular (typically daily) synching of ALL rights for ALL users.

  Rival solutions require desktop agents to communicate with the server explicitly for each and every document. At any scale, an attempt to synchronize all rights results in unacceptable amounts of traffic.

- Regular and complete synching means that policy changes propagate rapidly – typically over the course of a single business day.

  Rival solutions typically allow users to benefit from cached rights for a defined period without any re-evaluation of those rights. If the offline period is two weeks, you can expect a policy change to take two weeks to propagate – if indeed the policy change can affect pre-existing documents at all.

- Another feature of the classification-based model is that information ownership is well defined – and need not rest with document authors.

  Rival solutions typically treat the originating author of each document to be the "owner" of that document – with preferential rights to use it and with ongoing responsibility for managing the rights for it. So, a thousand authors equals a thousand rights administrators. If an author leaves the enterprise or changes role within the enterprise, transfer of ownership can be a significant challenge.

- The classification model has other practical benefits when it comes to operations that affect multiple documents. For example, policy may allow some users to copy information between documents that are in the same classification or related classifications, or to search thousands of documents without needing to request thousands of rights.

  File-by-file models make it impractical to define and maintain the rules matrix needed to control pasting, and would generate significant network traffic in the event of a search. For most solutions, clipboard is limited to ON or OFF, and searching simply isn't an option unless handled by a server-side application with carte blanche to decrypt everything programmatically.

SUCCESSFULLY DEPLOYING INFORMATION RIGHTS MANAGEMENT

Information Rights Management solutions must be secure, usable and manageable.

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 offer the right balance of **security**, **usability**, and **manageability** – even at enterprise scale.

Security

Oracle Information Rights Management provides effective, multi-layered security for enterprise information. Security layers include persistent (post-delivery) control, authentication, industry-standard cryptography, tamper-proofing and breach response mechanisms.

While no solution can guarantee 100% security, Oracle Information Rights Management provides effective multi-layered security using several industry-standard and industry-leading security technologies, and is a key component of Oracle's overall security portfolio for protecting and tracking information in storage, in applications, and on desktops.

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 IRM continues to protect information even after it is decrypted for use by authorized users, giving control over:

- **Who** can and cannot open sealed documents.
- **What** documents or classifications of document can be accessed.
- **When** rights are effective, and how often the desktop agent needs to communicate with the server to check for possible revocation of rights.
- **Where** documents can used – for example, enforcing internal use only.
- **How** documents can be used, with fine-grained control over opening, searching, annotating, editing, change tracking, copying, printing, interacting with form fields or cells, viewing spreadsheet formulas, using accessibility features and so on.

In all cases, this control persists for the lifetime of the sealed documents or emails, regardless of where they are stored and used, because the solution guards against the creation of unsealed, decrypted copies of the information.

Authentication

Oracle Information Rights Management currently supports the following authentication mechanisms:

- Windows authentication (for single-sign-on using Kerberos)
- Oracle Access Manager (using basic authentication over SSL)
- Username/password (using basic authentication over SSL to LDAP)

Windows authentication transparently uses the existing Windows login sessions on end user computers. Oracle Access Manager and username/password authentication enables Oracle IRM Server to support users without requiring access to Windows authentication domains. Basic authentication enables users to authenticate with the credentials from their corporate directory user account - removing the need to manage and remember a separate IRM password.

Cryptography and FIPS 140-2 Certification

Oracle Information Rights Management is based on industry-standard encryption and can be run in modes using FIPS 140-2 certified cryptographic modules.

Oracle Information Rights Management uses industry-standard encryption technologies widely to protect documents, keys, and client-server communications. Only recognized third-party cryptographic modules are used to provide the required functions, including all encryption, hash computation, key generation and random number generation. In order to provide a range of levels of security and optionally offer Federal Information Processing Standard (FIPS) 140-2 validated modes, the system can be configured to use various different modules, algorithms and key sizes. For full details of the available cryptographic modes, please see the table below.

Oracle IRM Cryptographic modes					
Mode	**FIPS 140-2**	**Content Encryption**	**Content Signing**	**Key Encryption**	**Client Module**
AES128		AES 128	HMAC-SHA256 w/ 128-bit key	RSA 1024, RSA 2048, AES 128	Wei Dei Crypto++
AES256		AES 256	HMAC-SHA256 w/ 256-bit key	RSA 1024, RSA 2048, AES 128	Wei Dei Crypto++
AES128-FIPS	✓	AES 128	HMAC-SHA1 w/ 128-bit key	RSA 512, RSA 1024, AES 128	Microsoft Crypto API
AES256-FIPS	✓	AES 256	HMAC-SHA256 w/ 256-bit key	RSA 512, RSA 1024, AES 128	Microsoft Crypto API
DES3-FIPS	✓	Triple-DES 168	HMAC-SHA1 w/ 128-bit key	RSA 512, RSA 1024, AES 128	Microsoft Crypto API
Server Module	Sun JCE Security Providers: sun.security.rsa.SunRsaSign com.sun.crypto.provider.SunJCE				

Oracle IRM desktop utilizes a FIPS validated library operating in validated mode to perform its cryptographic functions and so meets the requirement of a validated solution.

Oracle IRM desktop utilizes a FIPS validated library operating in validated mode to perform its cryptographic functions and so meets the requirement of a validated

solution. Oracle IRM Server sealing will use a validated 3rd party cryptographic module when configured to do so.

Files protected by Oracle IRM are encrypted and signed. The encryption uses a combination of a per-document key which is generated at the time of sealing and stored encrypted in the resultant file, and a classification-wide key which applies to all documents in the same IRM classification. Signing utilizes a classification-wide key only. The Oracle IRM Desktop synchronization agent silently downloads the encryption and signing keys for all classifications in which a user has rights on a regular basis; typically daily. This then enables users to open all sealed documents to which they have rights while offline, even if they have never opened those documents before. At the same time, the use of per-document keys reduces the risks that would be associated with using only a single key to encrypt all the files within a classification.

On the server, classification keys are stored encrypted in the database. The master key is held in a software key store of the administrator's choice. The encryption algorithm used to wrap the classification keys, and the size of the master key to use, are specified at the time of installation. The three available encryption algorithms are the JCE Standard implementations of AESWrap, DESedeWrap and RSA/ECB/OAEPWithSHA-256AndMGF1Padding. The recommended sizes for the master key are 256 for AES, 168 for DES, and 2048 for RSA.

On the client, classification keys are stored in an embedded instance of the lightweight Oracle Berkeley DB Database. They are heavily encrypted using symmetric and asymmetric encryption algorithms with a combination of fixed and one-time-only keys. Some of the keys are partially derived from hardware specific information so as to lock the database to the client machine. This prevents users from sharing their offline database with others, in order to give them access to their sealed files.

During transmission from the server to the client the classification keys are heavily encrypted using symmetric and asymmetric algorithms with a combination of fixed and session keys. The communication is additionally sent over SSL. This unique key exchange process defends effectively against both man-in-the-middle attacks, and attempts by a valid end-user to directly access the encryption keys as they are downloaded onto their machine.

Overall, Oracle's carefully designed encryption and key management scheme provides a unique balance of usability and security which enables users to work with sealed content in much the same way they work with unprotected content, while at the same time giving organizations the assurance they need that their classification keys are safe from both external and internal attacks.

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 for evaluating rights expiry times, 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.

Usability

Usability is essential for information rights management solutions (because unusable security products achieve nothing).

Over a million end users of Oracle Information Rights Management attest to the fact that it is the most usable solution in the market today. This is because it can be easily used within existing online and offline workflows, without requiring users to upgrade existing desktop environments.

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. For the current range of supported applications, formats and versions see the Certification Matrix at http://www.oracle.com/goto/irm, these include:

- Microsoft Office (Word, Excel and PowerPoint)
- PDF (Adobe Reader)
- Email: Microsoft Outlook and Lotus Notes
- HTML and XML (Internet Explorer)
- .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.
- 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[1].

Oracle Information Rights Management provides out-of-the-box support for full-text indexing and search of sealed files, using native Windows search capabilities.

"Hands free" offline working

Few things better illustrate the superior usability of the Oracle Information Rights Management solution than its "hands free" support for mobile (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.

[1] 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.

Internationalization

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.

Oracle IRM Desktop is available in 27 language variants, providing localized integration of Oracle Information Rights Management functionality into applications including Windows Explorer, Office, Outlook, Notes and Adobe Reader. For example, options to seal documents and email are presented by localized toolbars and menu options.

Oracle IRM Server Administration Console is a browser-based web application and is also available in 27 language variants. For the full list of all supported languages see the Certification Matrix at http://www.oracle.com/goto/irm.

Manageability

Classification-based rights management

Oracle Information Rights Management's classification-based rights model is superior to the per-file policy templates of competing products.

Classification-based rights management is a key Oracle differentiator for enterprise deployability, because it enables organizations to manage rights directly in terms of existing business processes and employee roles – ensuring that Oracle Information Rights Management remains easily manageable at enterprise scale.

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 "Executive Communications" or "Top Secret"), existing employee roles (such as "Reviewer"), and existing users and groups defined in enterprise directories (such as "Sales").

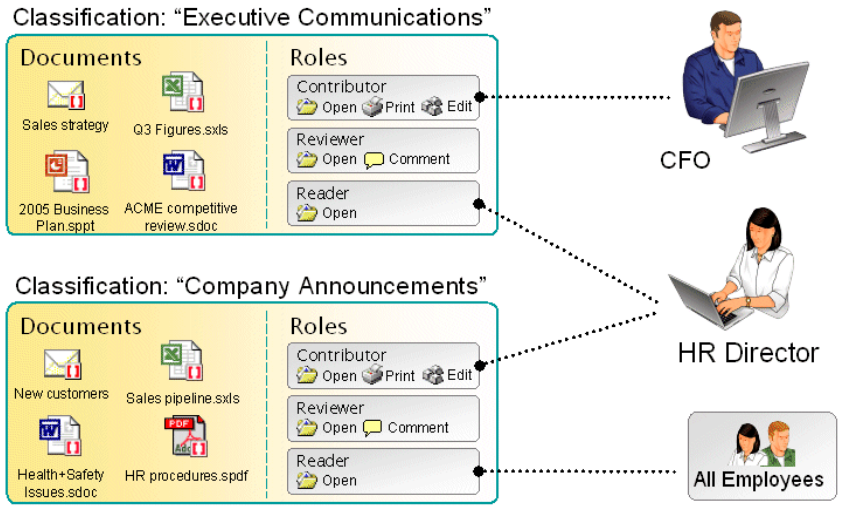

Figure 4: Classification-based rights management

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.

Best practice standard rights model

Oracle IRM is the only IRM solution to have built over nearly ten years of best-practice consulting and successful deployment experience directly into the product – the Oracle IRM 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.

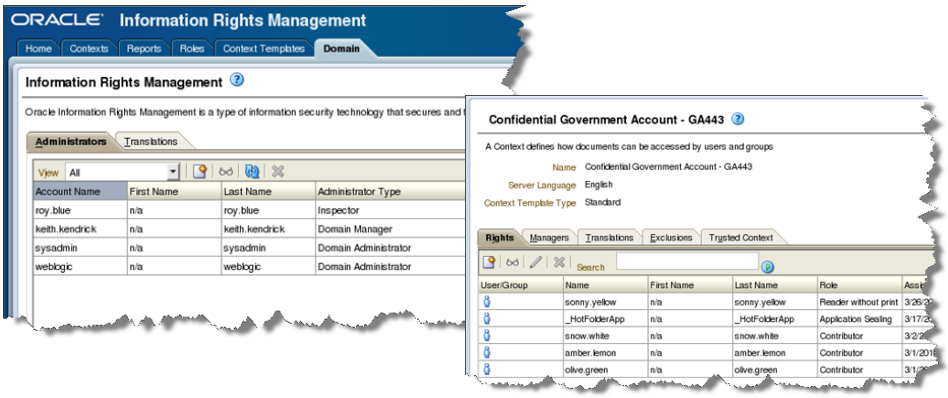

Figure 5: Administration and document roles in the standard rights model

Oracle Information Rights Management is the only IRM solution to have built nearly ten years of best-practice consulting and successful deployment experience directly into the product; including pre-defined end user and administrative roles, templates and online self-help.

The intuitive end user status pages and administrative Management Console are key ingredients 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's role-based administrative model enables delegation and partitioning of information rights management administration between business and IT without granting IT blanket "superuser" access to particularly sensitive information.

Oracle Information Rights Management differs from other IRM solutions in that it has a role- and classification-based administrative rights model. 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). Policy administrators can ensure that consistent roles are available and used across an organization, without them being able to access content or assign rights.

Audit

By auditing all actual and attempted access to sealed information Oracle Information Rights Management opens an unprecedented window onto the use (or misuse) of an organization's information – inside and outside the firewall – a feature that can itself justify investment in Oracle Information Rights Management, aside from its other security benefits.

Oracle Information Rights Management audits all online and offline end user access to sealed documents or emails. 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. Oracle IRM auditing opens an unprecedented window onto the use (or attempted misuse) 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.

Integration with enterprise infrastructure

Oracle IRM connects to different LDAP directories via Oracle Platform Security Services. Unlike the Oracle IRM 10g server, the 11g server does not synchronize with a directory but instead connects directly. This allows the support of different authentication mechanisms such as Windows Authentication (via Kerberos) or basic authentication, using users' LDAP usernames and passwords. 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 4,000 users.

TECHNOLOGY CHARACTERISTICS AND SPECIFICATIONS

The technological profile of Oracle Information Rights Management is an Oracle IRM Desktop agent, installed on every end user device on which sealed information is created and used, and a centralized Oracle IRM Server, which stores and serves the rights governing access to sealed information. Some business and IT administrators also use an Oracle IRM Management Console web application to create new users, assign roles, etc.

Oracle Information Rights Management has two key components:

- Oracle IRM Server – stores the decryption keys and rights governing end user access to sealed documents and emails. Its Management Console enables administrators to manage every aspect of the solution.
- Oracle IRM Desktop – enables authorized users to create and use sealed information, subject to rights obtained from the Oracle IRM Server.

Typical Oracle IRM deployment topology

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

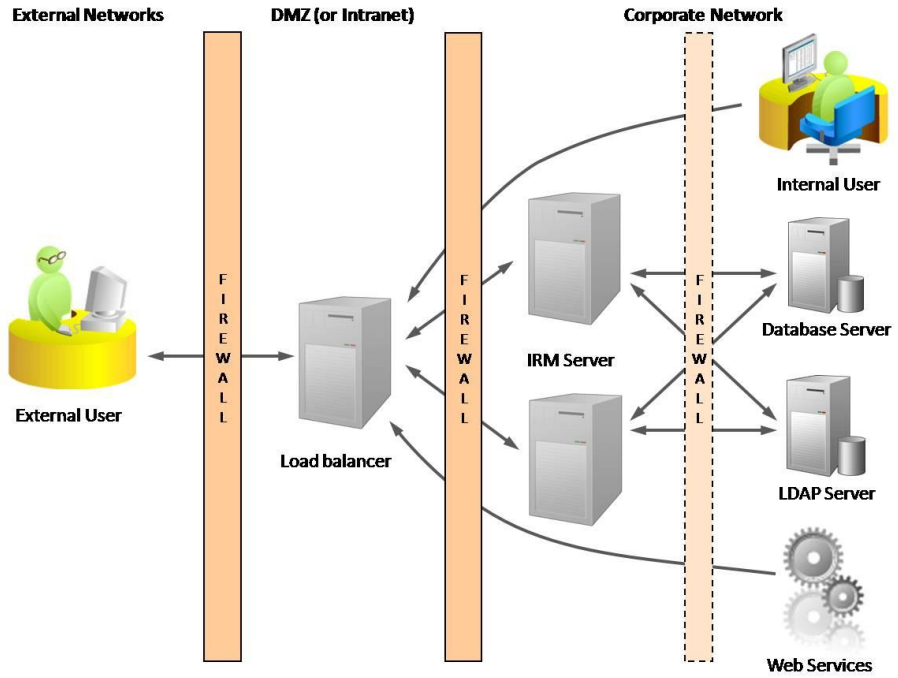

Figure 4: Typical Oracle IRM deployment topology

A single load balancer, typically hosted in the DMZ, sits in front of an Oracle IRM Server cluster. The internal firewall is configured to enable the load balancer to communitcate with the IRM Servers over a specified port. The Oracle IRM Server cluster uses a high-availability database cluster and user directory hosted in the organization's private network. All end users need the Oracle IRM Desktop. Encrypted client-server communications are typically transmitted using HTTPS and by default use port 443.

Oracle IRM Server stores all its internal state in the database, so high availability can largely be provided via load balancing across multiple servers without the need for server clustering to cache state.

Integrating Oracle IRM

It is easy to integrate Oracle Information Rights Management with third party products and infrastructure. The Oracle IRM Web Services SDK provide comprehensive sealing and administrative services via industry-standard SOAP/WSDL web services, enabling easy integration with content management and collaborative repositories, automated workflows, content filters and full-text search indexers and search engines.

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 role management systems, for example 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

For all supported specifications see the certification matrix at http://www.oracle.com/goto/irm.

Oracle IRM Server	
Hardware	Standard server hardware with minimum 2 GB RAM. Fast disks and network cards are recommended.
Operating system	Linux, Windows, Solaris, HP-UX and AIX.
Database	Oracle and SQL Server. Database disk space of 100GB recommended to allow for audit records for 1000 users.
Network	One IP address with a public address allocation.
Firewall rules	HTTPS-based connections to server. Connections from server to database.
Directories	Connect via OPSS to users/groups in Oracle Internet Directory, Oracle Virtual Directory, Active Directory, Sun Java System Directory Service, Novell eDirectory and OpenLDAP.

Oracle IRM Desktop	
Hardware	Standard desktop PC, 15 MB free disk space.
Operating system	Microsoft Windows XP, Windows Vista or Windows 7
Formats/ applications	See previous section on "Support for heterogeneous enterprise environments" and the certification matrix.
Browser	Requires Internet Explorer to be installed (does not need to be default browser).
Install	10MB MSI installer, requires administrator or elevated install privileges. Support for silent/managed installations.

Information Rights Management 11g – Managing information everywhere it is stored and used
March 2010
Authors: Martin Lambert and Andy Peet

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