IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

DRM VECTORS, LLC, **Plaintiff,** **v.** **ORACLE CORPORATION,** **Defendant.**	**CIVIL ACTION NO.** **JURY TRIAL DEMANDED**

PLAINTIFF'S ORIGINAL COMPLAINT

Plaintiff DRM Vectors, LLC ("Plaintiff"), by and through its undersigned counsel, files this Original Complaint against Defendant Oracle Corporation ("Defendant") as follows:

NATURE OF THE ACTION

1. This is a patent infringement action to stop Defendant's infringement of United States Patent No. 9,305,143 ("the '143 patent") entitled "Broadcasting of Electronic Documents Preserving Copyright and Permitting Private Copying". A true and correct copy of the '143 patent is attached hereto as Exhibit A. Plaintiff is the owner by assignment of the '143 patent. Plaintiff seeks monetary damages and injunctive relief.

PARTIES

2. Plaintiff is a limited liability company having a principal place of business located at 717 North Union St. Wilmington, DE 19805.

3. Upon information and belief, Defendant is a corporation organized and existing under the laws of the State of Delaware with a principal place of business located at 500 Oracle Parkway, Redwood Shores, California 94065. Defendant can be served with process by serving the Corporation Service Company, 251 Little Falls Dr. Wilmington, Delaware 19808.

JURISDICTION AND VENUE

4. This action arises under the Patent Laws of the United States, 35 U.S.C. § 1 *et seq.*, including 35 U.S.C. §§ 271, 281, 283, 284, and 285.

5. This Court has subject matter jurisdiction over this case for patent infringement under 28 U.S.C. §§ 1331 and 1338(a).

6. The Court has personal jurisdiction over Defendant because Defendant is present within or has minimum contacts within the State of Delaware and the District of Delaware; Defendant has purposefully availed itself of the privileges of conducting business in the State of Delaware and in the District of Delaware; Defendant has sought protection and benefit from the laws of the State of Delaware; Defendant regularly conducts business within the State of Delaware and within the District of Delaware; and Plaintiff's cause of action arises directly from Defendant's business contacts and other activities in the State of Delaware and in the District of Delaware. Further, this Court has personal jurisdiction over Defendant because it is incorporated in Delaware and has purposely availed itself of the privileges and benefits of the laws of the State of Delaware.

7. More specifically, Defendant, directly and/or through intermediaries, ships, distributes, uses, provides, offers for sale, sells, and/or advertises products and services in the United States, the State of Delaware, and the District of Delaware including but not limited to the Accused Instrumentalities as detailed below. Upon information and belief, Defendant has committed patent infringement in the State of Delaware and in the District of Delaware. Defendant solicits and has solicited customers in the State of Delaware and in the District of Delaware. Defendant has paying customers who are residents of the State of Delaware and the

District of Delaware and who each use and have used the Defendant's products and services in the State of Delaware and in the District of Delaware.

8. Venue is proper in the District of Delaware pursuant to 28 U.S.C. §§ 1400(b). On information and belief, Defendant is incorporated in this district, or has a regular and established business presence in this district and has transacted business in this district, and has directly and/or indirectly committed acts of patent infringement in this district.

COUNT I – PATENT INFRINGEMENT

9. Plaintiff refers to and incorporates herein the allegations of Paragraphs 1-8 above.

10. The '143 patent was duly and legally issued by the United States Patent and Trademark Office on April 5, 2016 after full and fair examination. Plaintiff is the owner by assignment of the '143 patent and possesses all rights of recovery under the '143 patent, including the exclusive right to sue for infringement and recover past damages and obtain injunctive relief.

11. Defendant owns, uses, operates, advertises, controls, sells, and otherwise provides systems, methods and apparatus that infringe the '143 patent. The '143 patent provides, among other things, "a method of broadcasting electronic documents allowing the protection of copyright and private copying including a network accessible control server taking customer orders, network accessible delivery and control servers, and equipment supporting a display for consulting the document."

Defendant has been and is now infringing the '143 patent in the State of Delaware, in this judicial district, and elsewhere in the United States, by, among other things, directly or through intermediaries, making, using, importing, testing, providing, supplying, distributing, selling, and/or offering for sale, methods (including, without limitation, the Defendant's products including Oracle Information Rights Management platform, content and its copyright protection functionality identified herein as the "Accused Instrumentality") that provide methods for accessing an order server containing models of documents to distribute, an item database, a customer database with the emails of customers, an order database containing references of the works ordered, and digital rights associated with the works ordered, said digital rights comprising controlled consultation rights as constraints, and permanently acquired digital rights, the order server configured for handling an order received from the customer on the network accessing a delivery server via the network, the delivery server configured for generating a specific copy of a document ordered by a customer from the model of the document ordered, the order server sending order information to the delivery server, the order information comprising, at least the reference to the work, customer contact information, the controllable consultation rights,and other digital rights ordered, the delivery server creating a delivery record of the work ordered containing the unique identifier to control the said work ordered, the order server responding to the customer's order by sending the customer a URL link towards the delivery server, the URL link comprising, as a parameter, at least the unique identifier of the copy ordered; responsive to an activation of the URL link by the customer, the delivery server generating a specific copy of the work ordered, by a library used for creation of documents on the fly containing the unique identifier, a supervision agent for the document, and the other permanently acquired digital rights relating to the document, the supervision agent designed to verify the controlled digital rights of each copy of the ordered work; accessing a control server via the network, the control server configured to verify digital rights acquired by the customer using the unique identifier of the ordered document copy; when delivering the ordered document copy to the customer, the delivery server sending to the control server the controlled information containing at least the unique identifier of the ordered document copy and the set of digital rights controlled; and operating a customer computing device, supporting a viewer, to allow the customer, via the viewer, to consult the ordered document, previously downloaded from the delivery server, said viewer designed to allow the customer to consult the ordered document; and a verification step comprising the sub-steps of when opening the specific copy on the customer computing device, the supervision agent of the specific copy causing the customer computing device to connect to the control server, and the supervision agent of the specific copy sending a query containing at least the unique identifier of the specific copy, in response to receiving the query, the control server returning a response comprised of one of i) an authorization to consult the specific copy, and ii) a consultation refusal, according to the specific copy's controlled digital rights as stored by the control server, and when the customer computing device receives the response from the control server, the supervision agent of the specific copy allowing the consultation of the specific copy when the response comprises the authorization to consult the specific copy and prohibiting the consultation of the specific copy when the response comprises the consultation refusal covered by at least claim 1 of the ‘143 patent to the injury of DRM Vectors, LLC. Defendant is directly infringing, literally infringing, and/or infringing the ‘143 patent under the doctrine of equivalents. Defendant is thus liable for infringement of the ‘143 patent pursuant to 35 U.S.C. § 271.

15. Defendant has induced and continues to induce infringement of the ‘143 patent by intending that others use, offer for sale, or sell in the United States, products and/or methods covered by one or more claims of the ‘143 patent, including, but not limited to, methods, and products comprising methods that broadcast electronic documents which preserve copyrights and premite private copying that infringe one or more claims of the ‘143 patent.

16. Defendant indirectly infringes the ‘143 patent by inducing infringement by others, such as resellers, customers and end-use consumers, in accordance with 35 U.S.C. § 271(b) in this District and elsewhere in the United States. Direct infringement is a result of the activities performed by the resellers, customers and end-use consumers of the broadcasting of electronic documents which preserve copyrights and permit private copying, including methods, and products comprising methods for broadcasting electronic documents which preserve copyrights and permit private copying.

17. Defendant received notice of the ‘143 patent at least as of the date this lawsuit was filed.

18. Defendant's affirmative acts of providing and/or selling the methods, and products comprising methods for broadcasting electronic documents which preserve copyrights and permit private copying, including manufacturing and distributing, and providing instructions for using the methods, and products comprising methods for broadcasting electronic documents which preserve copyrights and permit private copying in their normal and customary way to infringe one or more claims of the ‘143 patent. Defendant performs the acts that constitute induced infringement, and induce actual infringement, with the knowledge of the ‘143 patent and with the knowledge or willful blindness that the induced acts constitute infringement.

19. Defendant specifically intends for others, such as resellers, customers and end-use consumers, to directly infringe one or more claims of the ‘143 patent, or, alternatively, has been willfully blind to the possibility that its inducing acts would cause infringement. By way of example, and not as limitation, Defendant induces such infringement by its affirmative action by, among other things: (a) providing advertising on the benefits of using the Accused

Instrumentalities' functionality; (b) providing information regarding how to use the Accused Instrumentalities' functionality; (c) providing instruction on how to use the Accused Instrumentalities' functionality; and (d) providing hardware and/or software components required to infringe the claims of the '143 patent.

20. Accordingly, a reasonable inference is that Defendant specifically intends for others, such as resellers, customers and end-use consumers, to directly infringe one or more claims of the '143 patent in the United States because Defendant has knowledge of the '143 patent at least as of the date this lawsuit was filed and Defendant actually induces others, such as resellers, customers and end-use consumers, to directly infringe the '143 patent by using, selling, and/or distributing, within the United States, methods, and products comprising methods for broadcasting electronic documents which preserve copyrights and permit private copying.

21. As a result of Defendant's acts of infringement, Plaintiff has suffered and will continue to suffer damages in an amount to be proved at trial.

22. Defendant continues advising, encouraging, or otherwise inducing others to use the methods, and products comprising the methods claimed by the '143 patent to the injury of Plaintiff. Since at least the filing date of the Original Complaint, Defendant has had knowledge of the '143 patent, and by continuing the actions described above, has specific intent to induce infringement of the '143 patent pursuant to 35 U.S.C. § 271(b), and has further contributed to said infringement of the '143 patent by their customers by providing them with the Accused Instrumentalities so that their customers could directly infringe the '143 patent.

23. Claim 1 of the '143 patent, claims:

24. An electronic document creation method protecting copyrights and allowing private copying, comprising the steps of:

accessing an order server containing models of documents
to distribute, an item database, a customer database with the emails of customers, an order database containing references of the works ordered, and digital rights associated with the works ordered, said digital rights comprising controlled consultation rights as constraints, and permanently acquired digital rights, the order server configured for handling an order received from the customer on the network;

accessing a delivery server via the network, the delivery server configured for generating a specific copy of a document ordered by a customer from the model of the document ordered, the order server sending order information to the delivery server, the order information comprising, at least the reference to the work, customer contact information, the controllable consultation rights,and other digital rights ordered;

the delivery server creating a delivery record of the work ordered containing the unique identifier to control the said work ordered;

the order server responding to the customer's order by sending the customer a URL link towards the delivery server, the URL link comprising, as a parameter, at least the unique identifier of the copy ordered;

responsive to an activation of the URL link by the customer, the delivery server generating a specific copy of the work ordered, by a library used for creation of documents on the fly containing the unique identifier, a supervision agent for the document, and the other permanently acquired digital rights relating to the document, the supervision agent designed to verify the controlled digital rights of each copy of the ordered work;

accessing a control server via the network, the control server configured to verify digital rights acquired by the customer using the unique identifier of the ordered document copy;

when delivering the ordered document copy to the customer, the delivery server sending to the control server the controlled information containing at least the unique identifier of the ordered document copy and the set of digital rights controlled; and

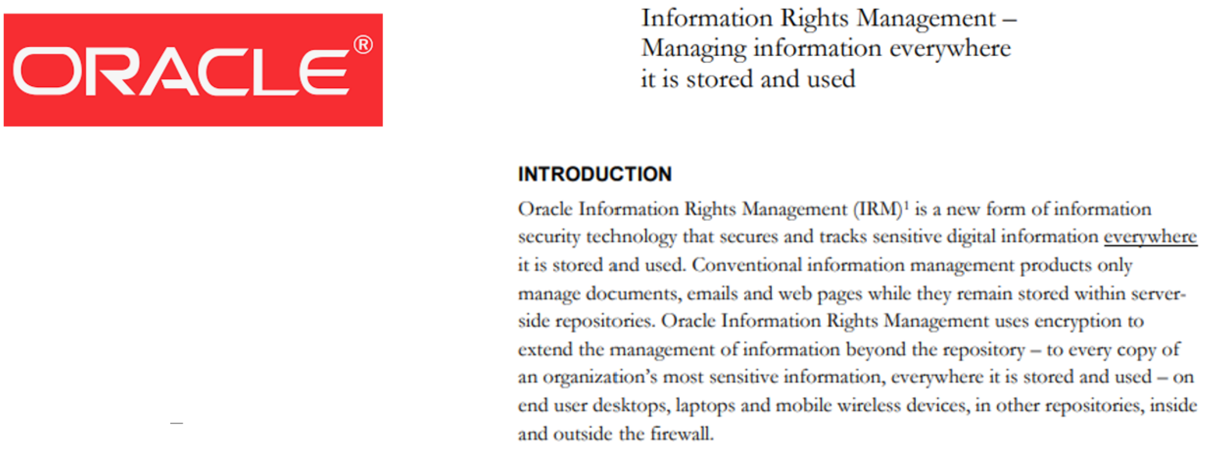
operating a customer computing device, supporting a viewer, to allow the customer, via the viewer, to consult the ordered document, previously downloaded from the delivery server, said viewer designed to allow the customer to consult the ordered document; and

a verification step comprising the sub-steps of

when opening the specific copy on the customer computing device, the supervision agent of the specific copy causing the customer computing device to connect to the control server, and the supervision agent of the specific copy sending a query containing at least the unique identifier of the specific copy;

in response to receiving the query, the control server returning a response comprised of one of i) an authorization to consult the specific copy, and ii) a consultation refusal, according to the specific copy's controlled digital rights as stored by the control server, and when the customer computing device receives the response from the control server, the supervision agent of the specific copy allowing the consultation of the specific copy when the response comprises the authorization to consult the specific copy and prohibiting the consultation of the specific copy when the response comprises the consultation refusal.

25. An electronic document creation method protecting copyrights and allowing private copying, comprising the steps of:



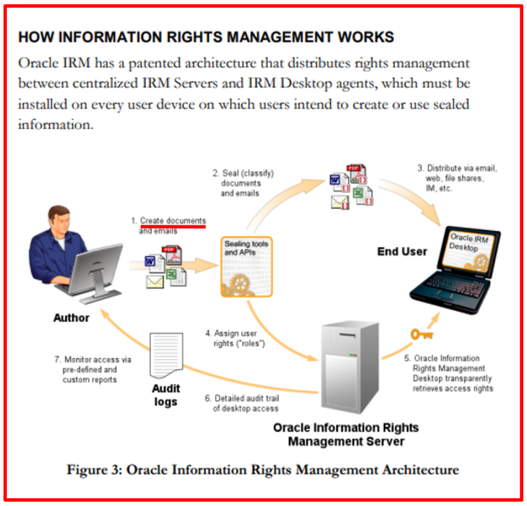
ORACLE®

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

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.

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-10g-technical-whitepaper-129901.pdf



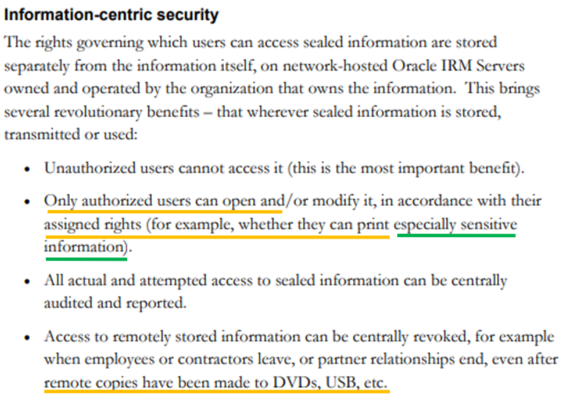
HOW INFORMATION RIGHTS MANAGEMENT WORKS

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.

1. Create documents and emails
2. Seal (classify) documents and emails
3. Distribute via email, web, file shares, IM, etc.
Sealing tools and APIs
End User
Oracle IRM Desktop
Author
4. Assign user rights ("roles")
5. Oracle Information Rights Management Desktop transparently retrieves access rights
6. Detailed audit trail of desktop access
7. Monitor access via pre-defined and custom reports
Audit logs
Oracle Information Rights Management Server

Figure 3: Oracle Information Rights Management Architecture

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-technical-whitepaper-134345.pdf



Information-centric security

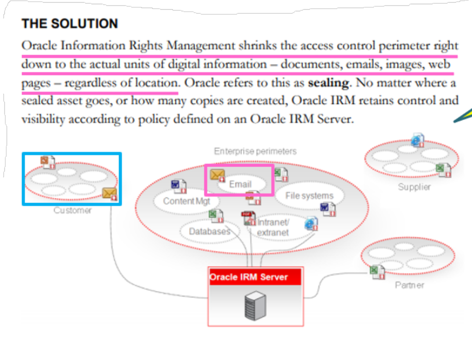
The rights governing which users can access sealed information are stored separately from the information itself, on network-hosted Oracle IRM Servers owned and operated by the organization that owns the information. This brings several revolutionary benefits – that wherever sealed information is stored,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

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-10g-technical-whitepaper-129901.pdf

accessing an order server containing models of documents to distribute, an item database, a customer database with the emails of customers, an order database containing references of the works ordered, and digital rights associated with the works ordered, said digital rights comprising

controlled consultation rights as constraints, and permanently acquired digital rights, the order server configured for handling an order received from the customer on the network;

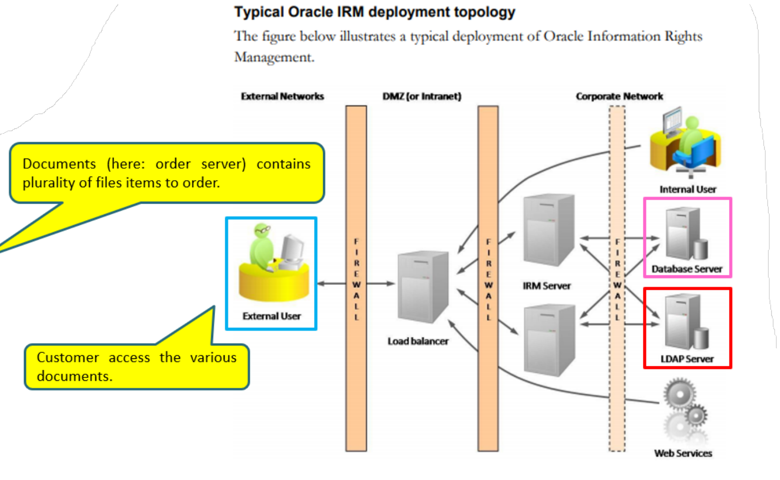


THE SOLUTION

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

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-technical-whitepaper-134345.pdf



Typical Oracle IRM deployment topology

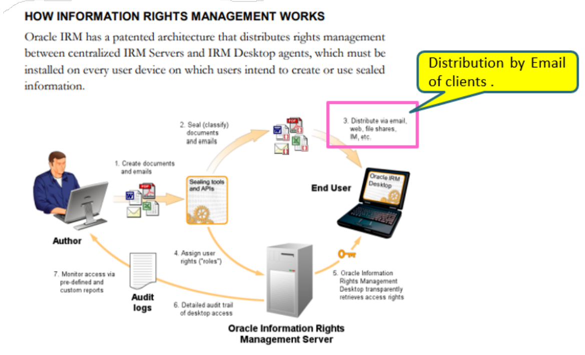
The figure below illustrates a typical deployment of Oracle Information Rights Management.

Documents (here: order server) contains plurality of files items to order.

Customer access the various documents.

Figure 4: Typical Oracle IRM deployment topology

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-technical-whitepaper-134345.pd



HOW INFORMATION RIGHTS MANAGEMENT WORKS

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.

Distribution by Email of clients .

1. Create documents and emails
2. Seal (classify) documents and emails
3. Distribute via email, web, file shares, IM, etc.
Sealing tools and APIs
End User
Oracle IRM Desktop
Author
4. Assign user rights ("roles")
5. Oracle Information Rights Management Desktop transparently retrieves access rights
6. Detailed audit trail of desktop access
7. Monitor access via pre-defined and custom reports
Audit logs
Oracle Information Rights Management Server

Figure 3: Oracle Information Rights Management Architecture

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-technical-whitepaper-134345.pdf

Persistent control

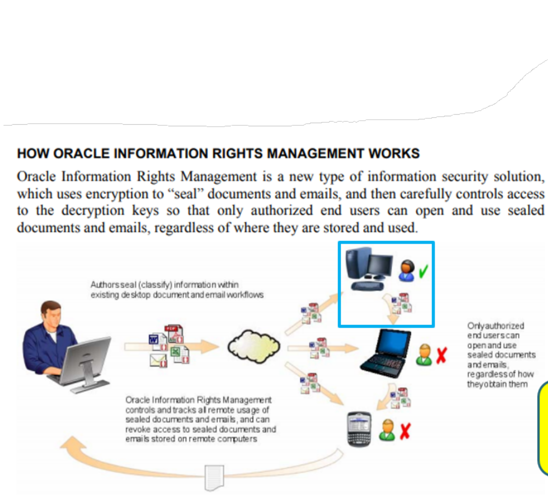
Oracle Information Rights Management can control every aspect of sealed document and email usage on end user desktops:

- **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.

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-10g-technical-whitepaper-129901.pdf

accessing a delivery server via the network, the delivery server configured for generating a specific copy of a document ordered by a customer from the model of the document ordered, the order server sending order information to the delivery server, the order information comprising, at least the reference to the work, customer contact information, the controllable consultation rights,and other digital rights ordered;

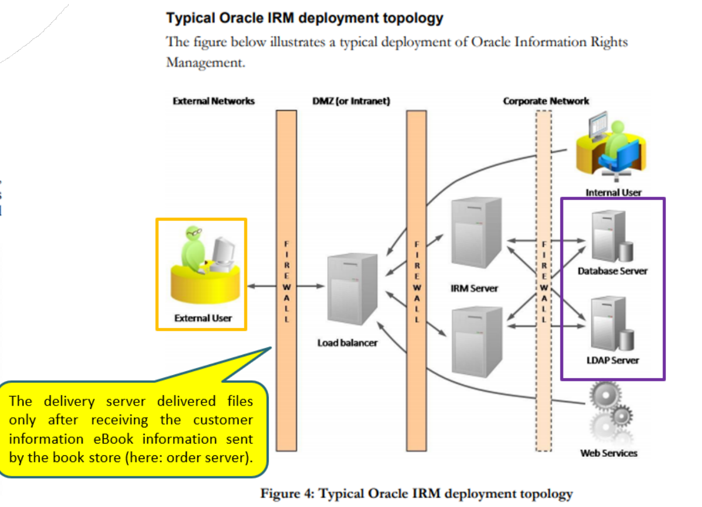


HOW ORACLE INFORMATION RIGHTS MANAGEMENT WORKS

Oracle Information Rights Management is a new type of information security solution, which uses encryption to "seal" documents and emails, and then carefully controls access to the decryption keys so that only authorized end users can open and use sealed documents and emails, regardless of where they are stored and used.

Authors seal (classify) information within existing desktop document and email workflows
Only authorized end users can open and use sealed documents and emails, regardless of how they obtain them
Oracle Information Rights Management controls and tracks all remote usage of sealed documents and emails, and can revoke access to sealed documents and emails stored on remote computers

SOURCE: https://www.Oracle Corporation.com/technetwork/testcontent/irmquickevalguide-131714.pdf



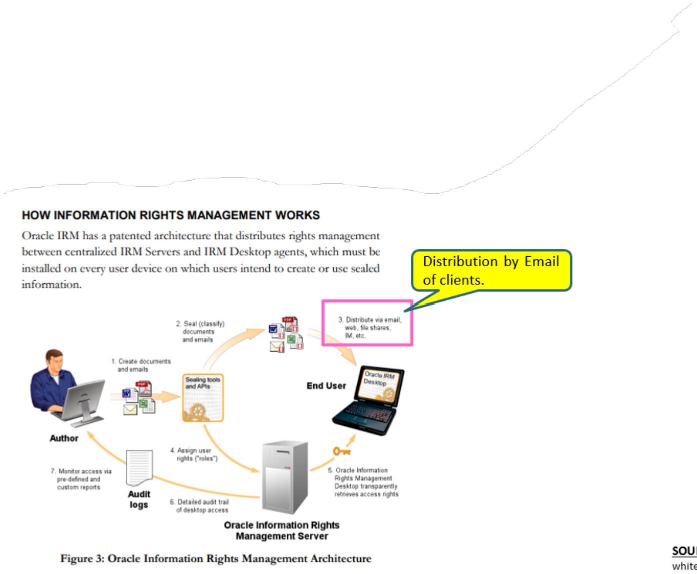
Typical Oracle IRM deployment topology

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

The delivery server delivered files only after receiving the customer information eBook information sent by the book store (here: order server).

Figure 4: Typical Oracle IRM deployment topology

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-technical-whitepaper-134345.pdf



HOW INFORMATION RIGHTS MANAGEMENT WORKS

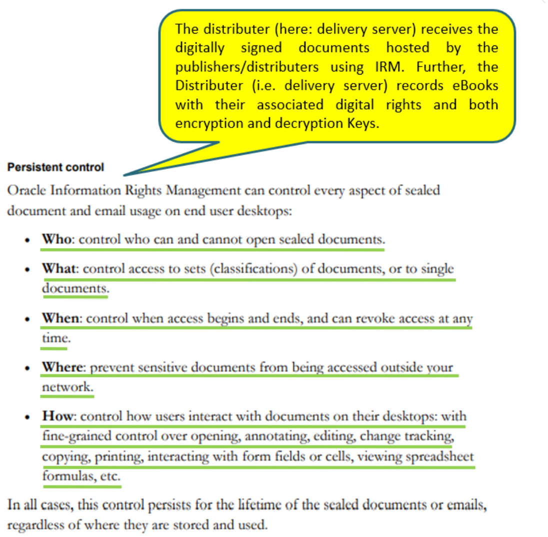
Oracle IRM has a patented architecture that distributes rights management between centralized IRM Servers and IRM Desktop agents, which must be installed on every user device on which users intend to create or use sealed information.

Distribution by Email of clients.

2. Seal (classify) documents and emails
3. Distribute via email, web, file shares, IM, etc.
1. Create documents and emails
Sealing tools and APIs
End User
Oracle IRM Desktop
Author
4. Assign user rights ("roles")
7. Monitor access via pre-defined and custom reports
Audit logs
6. Detailed audit trail of desktop access
5. Oracle Information Rights Management Desktop transparently retrieves access rights
Oracle Information Rights Management Server

Figure 3: Oracle Information Rights Management Architecture

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-technical-whitepaper-134345.pdf



The distributer (here: delivery server) receives the digitally signed documents hosted by the publishers/distributers using IRM. Further, the Distributer (i.e. delivery server) records eBooks with their associated digital rights and both encryption and decryption Keys.

Persistent control

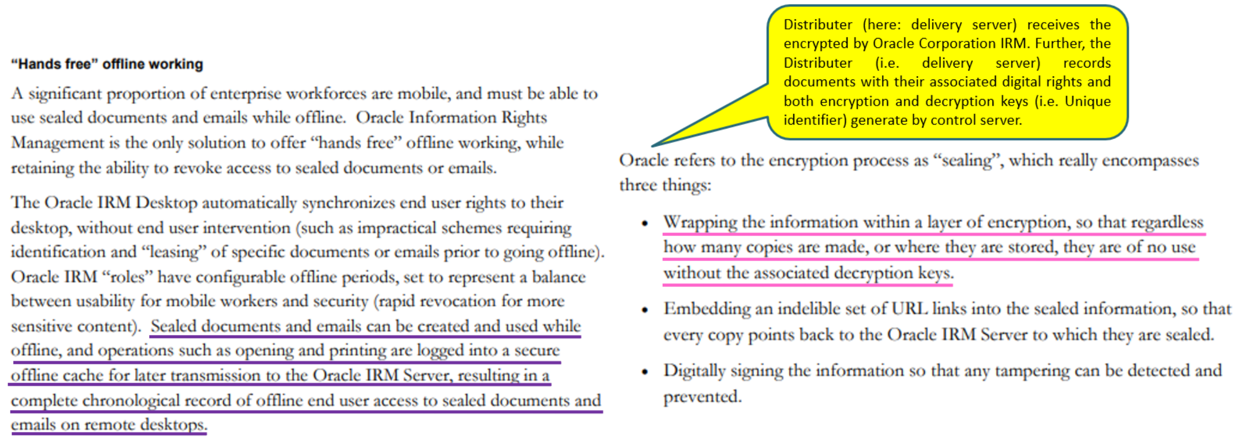
Oracle Information Rights Management can control every aspect of sealed document and email usage on end user desktops:

- **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.

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-10g-technical-whitepaper-129901.pdf

the delivery server creating a delivery record of the work ordered containing the unique identifier to control the said work ordered;



"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.

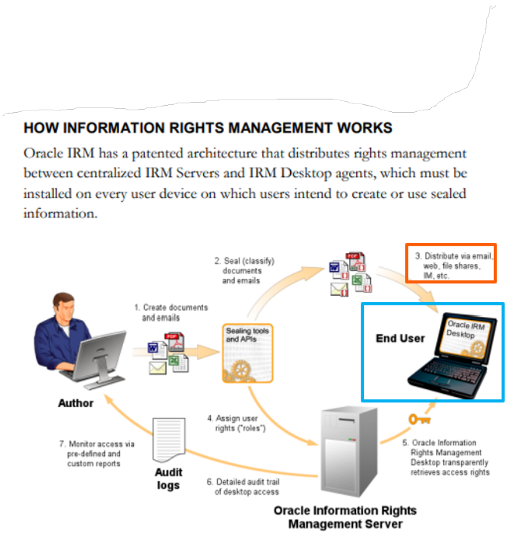
Distributer (here: delivery server) receives the encrypted by Oracle Corporation IRM. Further, the Distributer (i.e. delivery server) records documents with their associated digital rights and both encryption and decryption keys (i.e. Unique identifier) generate by control server.

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.

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-10g-technical-whitepaper-129901.pdf

the order server responding to the customer's order by sending the customer a URL link towards the delivery server, the URL link comprising, as a parameter, at least the unique identifier of the copy ordered;



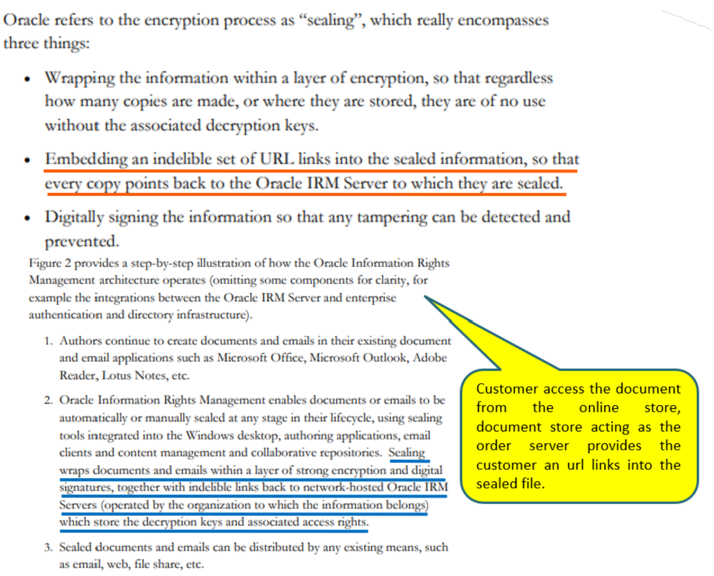
HOW INFORMATION RIGHTS MANAGEMENT WORKS

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.

2. Seal (classify) documents and emails
3. Distribute via email, web, file shares, IM, etc.
1. Create documents and emails
Sealing tools and APIs
End User
Oracle IRM Desktop
Author
4. Assign user rights ("roles")
7. Monitor access via pre-defined and custom reports
5. Oracle Information Rights Management Desktop transparently retrieves access rights
Audit logs
6. Detailed audit trail of desktop access
Oracle Information Rights Management Server

Figure 3: Oracle Information Rights Management Architecture

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-technical-whitepaper-134345.pdf



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.

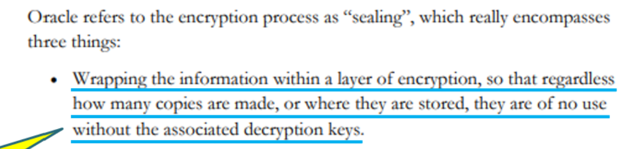
Figure 2 provides a step-by-step illustration of how the Oracle Information Rights Management architecture operates (omitting some components for clarity, for example the integrations between the Oracle IRM Server and enterprise authentication and directory infrastructure).

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.

Customer access the document from the online store, document store acting as the order server provides the customer an url links into the sealed file.

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-10g-technical-whitepaper-129901.pdf

responsive to an activation of the URL link by the customer, the delivery server generating a specific copy of the work ordered, by a library used for creation of documents on the fly containing the unique identifier, a supervision agent for the document, and the other permanently acquired digital rights relating to the document, the supervision agent designed to verify the controlled digital rights of each copy of the ordered work;

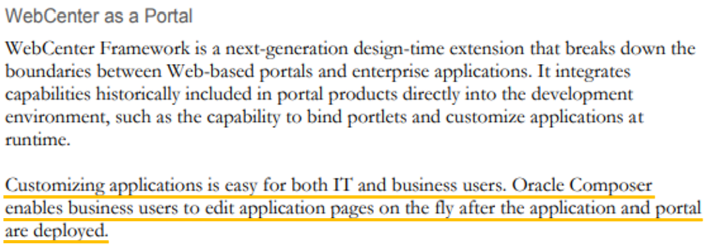


Oracle refers to the encryption process as "sealing", which really encompasses three things:

- 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.

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-10g-technical-whitepaper-129901.pdf

Unique identifier (keys)

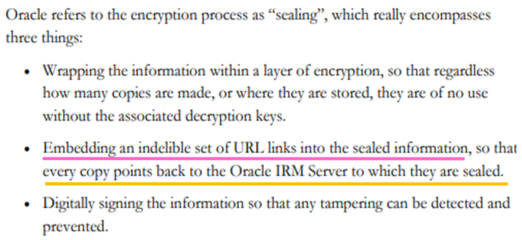


WebCenter as a Portal

WebCenter Framework is a next-generation design-time extension that breaks down the boundaries between Web-based portals and enterprise applications. It integrates capabilities historically included in portal products directly into the development environment, such as the capability to bind portlets and customize applications at runtime.

Customizing applications is easy for both IT and business users. Oracle Composer enables business users to edit application pages on the fly after the application and portal are deployed.

SOURCE: http://www.Oracle Corporation.com/us/products/applications/peoplesoft-enterprise/Oracle Corporation-fusion-middleware-wp-068327.pdf

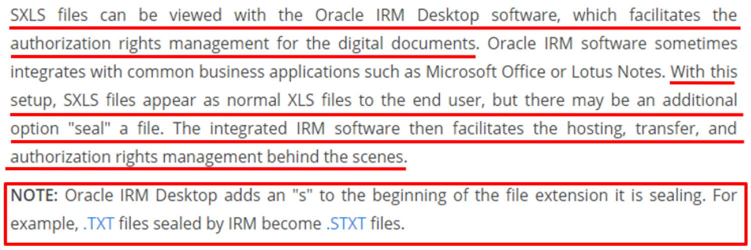


Oracle refers to the encryption process as "sealing", which really encompasses three things:

- 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.

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-10g-technical-whitepaper-129901.pdf

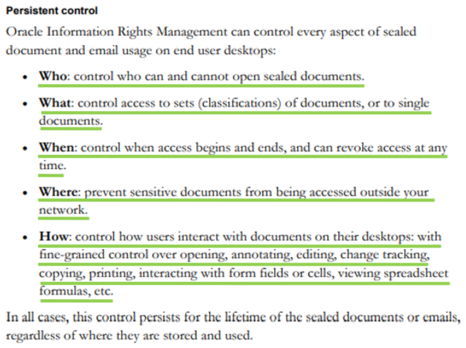
User is redirected towards the delivery server, the server generates a specific copy as per user requirement and send it in the form of "seal" file which contains the encrypted key.



SXLS files can be viewed with the Oracle IRM Desktop software, which facilitates the authorization rights management for the digital documents. Oracle IRM software sometimes integrates with common business applications such as Microsoft Office or Lotus Notes. With this setup, SXLS files appear as normal XLS files to the end user, but there may be an additional option "seal" a file. The integrated IRM software then facilitates the hosting, transfer, and authorization rights management behind the scenes.

NOTE: Oracle IRM Desktop adds an "s" to the beginning of the file extension it is sealing. For example, .TXT files sealed by IRM become .STXT files.

SOURCE: https://fileinfo.com/extension/sxls



Persistent control

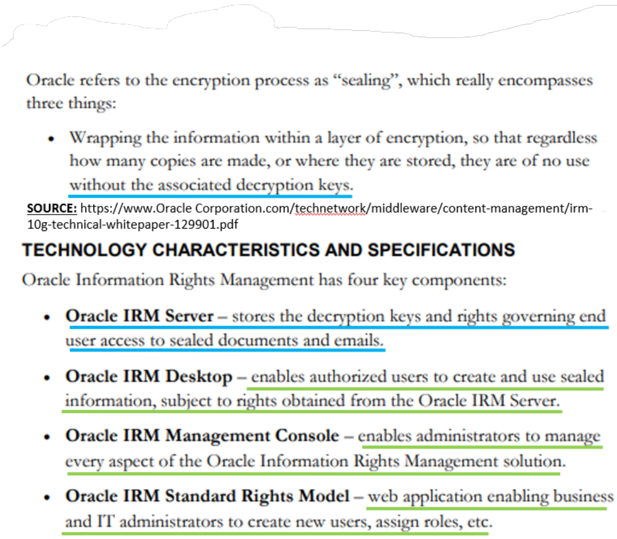
Oracle Information Rights Management can control every aspect of sealed document and email usage on end user desktops:

- **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.

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-10g-technical-whitepaper-129901.pdf

accessing a control server via the network, the control server configured to verify digital rights acquired by the customer using the unique identifier of the ordered document copy;



Oracle refers to the encryption process as "sealing", which really encompasses three things:

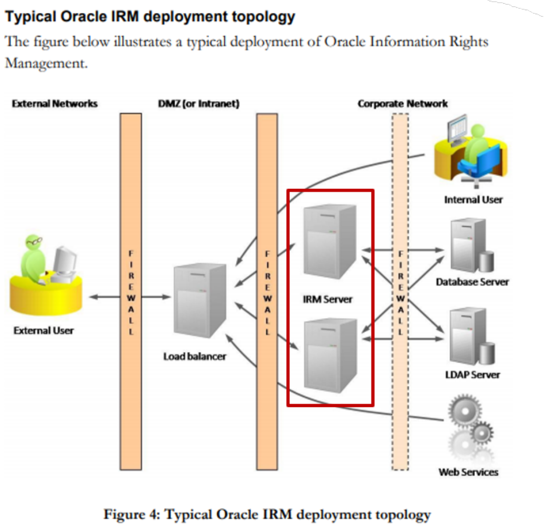
- Wrapping the information within a layer of encryption, so that regardless how many copies are made, or where they are stored, they are of no use without the associated decryption keys.

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-10g-technical-whitepaper-129901.pdf

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

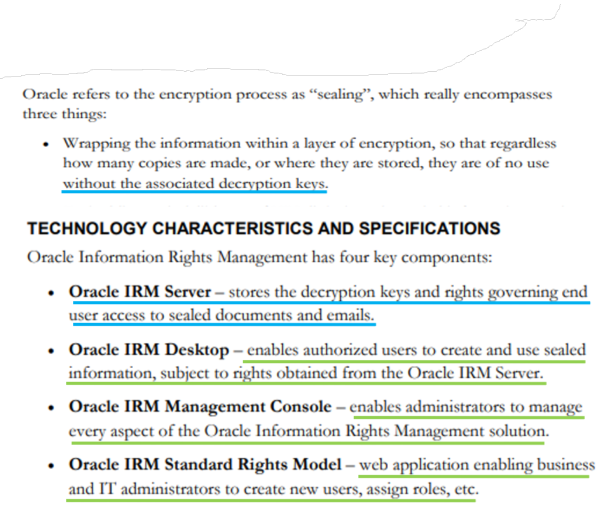
The figure below illustrates a typical deployment of Oracle Information Rights Management.

Figure 4: Typical Oracle IRM deployment topology

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-10g-technical-whitepaper-129901.pdf

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-technical-whitepaper-134345.pdf

when delivering the ordered document copy to the customer, the delivery server sending to the control server the controlled information containing at least the unique identifier of the ordered document copy and the set of digital rights controlled; and



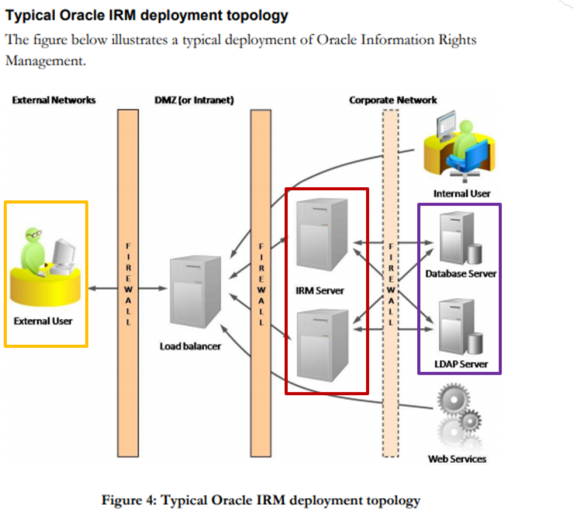
Oracle refers to the encryption process as "sealing", which really encompasses three things:

- 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.

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

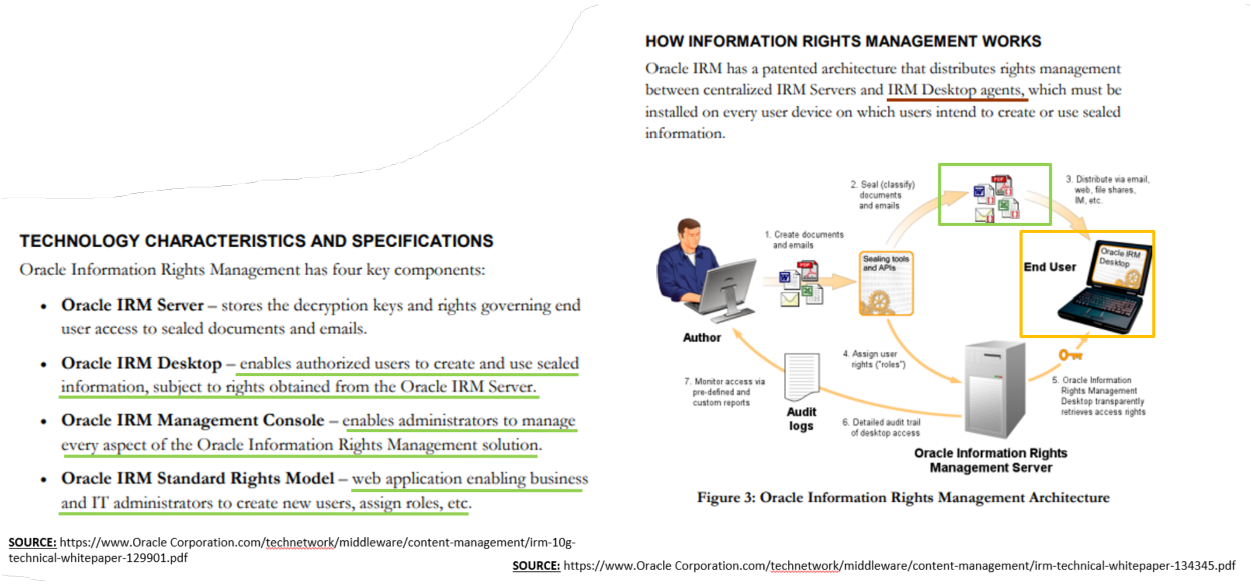
The figure below illustrates a typical deployment of Oracle Information Rights Management.

Figure 4: Typical Oracle IRM deployment topology

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-10g-technical-whitepaper-129901.pdf

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-technical-whitepaper-134345.pdf

operating a customer computing device, supporting a viewer, to allow the customer, via the viewer, to consult the ordered document, previously downloaded from the delivery server, said viewer designed to allow the customer to consult the ordered document; and



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.

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-10g-technical-whitepaper-129901.pdf

HOW INFORMATION RIGHTS MANAGEMENT WORKS

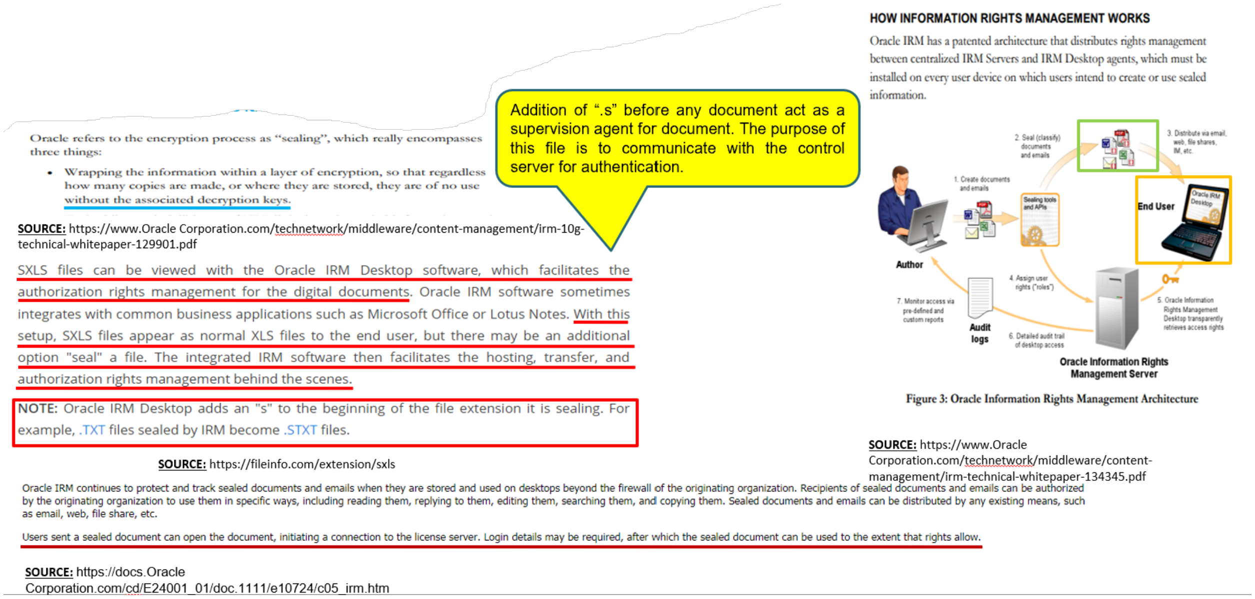
Oracle IRM has a patented architecture that distributes rights management between centralized IRM Servers and IRM Desktop agents, which must be installed on every user device on which users intend to create or use sealed information.

1. Create documents and emails
2. Seal (classify) documents and emails
3. Distribute via email, web, file shares, IM, etc.
Sealing tools and APIs
End User
Oracle IRM Desktop
Author
4. Assign user rights ("roles")
5. Oracle Information Rights Management Desktop transparently retrieves access rights
6. Detailed audit trail of desktop access
7. Monitor access via pre-defined and custom reports
Audit logs
Oracle Information Rights Management Server

Figure 3: Oracle Information Rights Management Architecture

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-technical-whitepaper-134345.pdf

a verification step comprising the sub-steps of when opening the specific copy on the customer computing device, the supervision agent of the specific copy causing the customer computing device to connect to the control server, and the supervision agent of the specific copy sending a query containing at least the unique identifier of the specific copy;



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.

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-10g-technical-whitepaper-129901.pdf

Addition of ".s" before any document act as a supervision agent for document. The purpose of this file is to communicate with the control server for authentication.

SXLS files can be viewed with the Oracle IRM Desktop software, which facilitates the authorization rights management for the digital documents. Oracle IRM software sometimes integrates with common business applications such as Microsoft Office or Lotus Notes. With this setup, SXLS files appear as normal XLS files to the end user, but there may be an additional option "seal" a file. The integrated IRM software then facilitates the hosting, transfer, and authorization rights management behind the scenes.

NOTE: Oracle IRM Desktop adds an "s" to the beginning of the file extension it is sealing. For example, .TXT files sealed by IRM become .STXT files.

SOURCE: https://fileinfo.com/extension/sxls

HOW INFORMATION RIGHTS MANAGEMENT WORKS

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.

1. Create documents and emails
2. Seal (classify) documents and emails
3. Distribute via email, web, file shares, IM, etc.
Sealing tools and APIs
End User
Oracle IRM Desktop
Author
4. Assign user rights ("roles")
5. Oracle Information Rights Management Desktop transparently retrieves access rights
6. Detailed audit trail of desktop access
7. Monitor access via pre-defined and custom reports
Audit logs
Oracle Information Rights Management Server

Figure 3: Oracle Information Rights Management Architecture

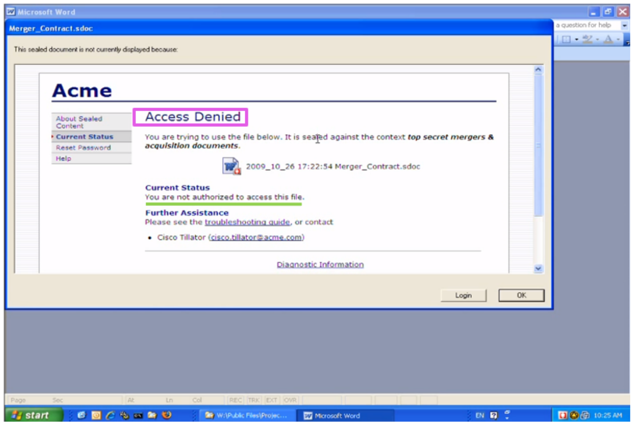
SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-technical-whitepaper-134345.pdf

Oracle IRM continues to protect and track sealed documents and emails when they are stored and used on desktops beyond the firewall of the originating organization. Recipients of sealed documents and emails can be authorized by the originating organization to use them in specific ways, including reading them, replying to them, editing them, searching them, and copying them. Sealed documents and emails can be distributed by any existing means, such as email, web, file share, etc.

Users sent a sealed document can open the document, initiating a connection to the license server. Login details may be required, after which the sealed document can be used to the extent that rights allow.

SOURCE: https://docs.Oracle Corporation.com/cd/E24001_01/doc.1111/e10724/c05_irm.htm

in response to receiving the query, the control server returning a response comprised of one of i) an authorization to consult the specific copy, and ii) a consultation refusal, according to the specific copy's controlled digital rights as stored by the control server, and



This sealed document is not currently displayed because:

Access Denied

You are trying to use the file below. It is sealed against the context ***top secret mergers & acquisition documents***.

2009_10_26 17:22:54 Merger_Contract.sdoc

Current Status
You are not authorized to access this file.

Further Assistance
Please see the troubleshooting guide, or contact

- Cisco Tillator (cisco.tillator@acme.com)

Diagnostic Information

SOURCE: https://www.youtube.com/watch?v=HVXrzpo8jxs

Typical Oracle IRM deployment topology

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

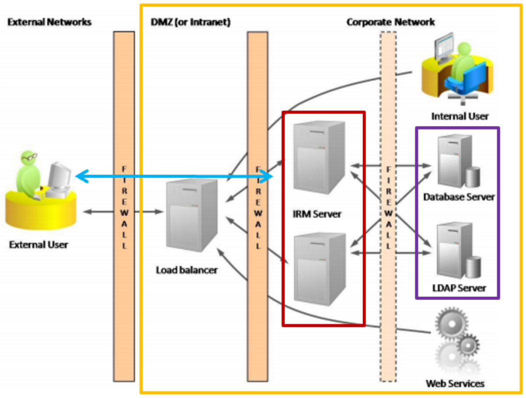


Figure 4: Typical Oracle IRM deployment topology

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-technical-whitepaper-134345.pdf

when the customer computing device receives the response from the control server, the supervision agent of the specific copy allowing the consultation of the specific copy when the response comprises the authorization to consult the specific copy and prohibiting the consultation of the specific copy when the response comprises the consultation refusal.

IRM Desktop receives the authorization response from the control server using sealed file. Reader software can allow the customer to consult the document if the authorization completes, and it can refuse the customer to consult the document if the authorization fails from the control server.

SXLS files can be viewed with the Oracle IRM Desktop software, which facilitates the authorization rights management for the digital documents. Oracle IRM software sometimes integrates with common business applications such as Microsoft Office or Lotus Notes. With this setup, SXLS files appear as normal XLS files to the end user, but there may be an additional option "seal" a file. The integrated IRM software then facilitates the hosting, transfer, and authorization rights management behind the scenes.

NOTE: Oracle IRM Desktop adds an "s" to the beginning of the file extension it is sealing. For example, .TXT files sealed by IRM become .STXT files.

SOURCE: https://fileinfo.com/extension/sxls

Typical Oracle IRM deployment topology

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

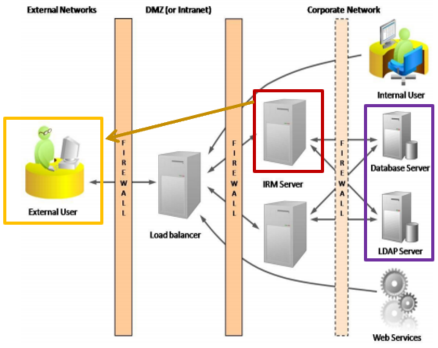
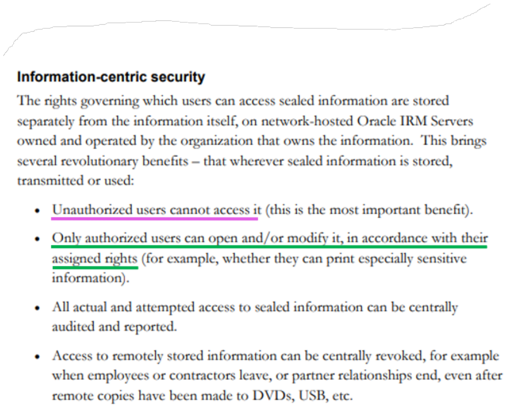


Figure 4: Typical Oracle IRM deployment topology

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-technical-whitepaper-134345.pdf

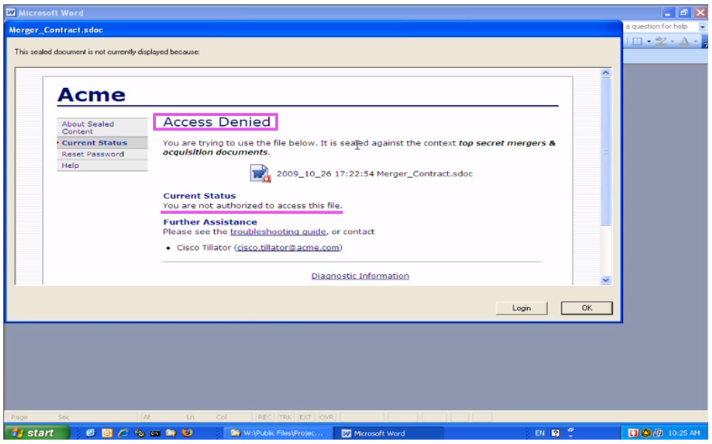


Information-centric security

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.

SOURCE: https://www.Oracle Corporation.com/technetwork/middleware/content-management/irm-10g-technical-whitepaper-129901.pdf



This sealed document is not currently displayed because:

Acme

Access Denied

You are trying to use the file below. It is sealed against the context ***top secret mergers & acquisition documents***.

2009_10_26 17:22:54 Merger_Contract.sdoc

Current Status
You are not authorized to access this file.

Further Assistance
Please see the troubleshooting guide, or contact

- Cisco Tillator (cisco.tillator@acme.com)

Diagnostic Information

SOURCE: https://www.youtube.com/watch?v=HVXrzpo8jxs

26. Defendant's aforesaid activities have been without authority and/or license from Plaintiff.

27. To the extent any marking was required by 35 U.S.C. § 287, Plaintiff and all predecessors in interest to the '143 patent complied with all marking requirements under 35 U.S.C. § 287.

28. Plaintiff is entitled to recover from Defendant the damages sustained by Plaintiff as a result of the Defendant's wrongful acts in an amount subject to proof at trial, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

JURY DEMAND

Plaintiff hereby requests a trial by jury pursuant to Rule 38 of the Federal Rules of Civil Procedure.

PRAYER FOR RELIEF

Plaintiff respectfully requests that the Court find in its favor and against the Defendant, and that the Court grant Plaintiff the following relief:

A. a judgment that Defendant directly and/or indirectly infringes one or more claims of the '143 patent;

B. award Plaintiff damages in an amount adequate to compensate Plaintiff for Defendant's infringing products' infringement of the claims of the '143 patent, but in no event less than a reasonable royalty, and supplemental damages for any continuing post-verdict infringement until entry of the final judgment with an accounting as needed, under 35 U.S.C. § 284;

C. award Plaintiff pre-judgment interest and post-judgment interest on the damages awarded, including pre-judgment interest, pursuant to 35 U.S.C. § 284, from the date of each act of infringement of the '143 patent by Defendant to the day a damages judgment is entered, and an award of post-judgment interest, pursuant to 28 U.S.C. § 1961, continuing until such judgment is paid, at the maximum rate allowed by law; and an accounting of all damages not presented at trial;

D. a judgment and order finding this to be an exceptional case and requiring defendant to pay the costs of this action (including all disbursements) and attorneys' fees, pursuant to 35 U.S.C. § 285;

E. award a compulsory future royalty for the '143 patent; and award such further relief as the Courts deems just and proper.

Dated: April 9, 2019

STAMOULIS & WEINBLATT LLC

/s/ Stamatios Stamoulis
Stamatios Stamoulis (#4606)
Richard C. Weinblatt (#5080)
800 N. West Street, Third Floor
Wilmington, DE 19801
(302) 999-1540
stamoulis@swdelaw.com
weinblatt@swdelaw.com

Austin Hansley (*pro hac vice* application forthcoming)
Texas Bar No.: 24073081
HANSLEY LAW FIRM, PLLC
13355 Noel Rd., STE. 1100
Dallas, Texas 75240
(972) 528-9321 Ext. 1000
ahansley@hansleyfirm.com

Attorneys for Plaintiff
DRM Vectors, LLC