Stopp! Niemals die Kontrolle über unternehmenskritische digitale Daten verlieren

Carsten Mützlitz, ORACLE Deutschland B.V. & Co. KG

Wichtige Dokumente sollten geschützt kontrolliert werden, egal mit welchen Systemen man diese verarbeitet, verwaltet und verteilt. Auch wenn die Dokumente die Unternehmensgrenzen verlassen, will man die Kontrolle über diese Dokumente beziehungsweise Informationen behalten. Lösungen für diese Anforderungen sind in den Konzepten des Digital Rights Managements (DRM) beziehungsweise des Information Rights Managements (IRM) zusammengefasst.

Idealerweise sollte man folgende Aktionen durchführen können:

- Den Zugriffsschutz auf wichtige Dokumente und E-Mails kontrollieren, auch wenn diese sich außerhalb der Unternehmensgrenzen befinden
- Sicherstellen, dass Dokumente und Dateien auf verloren gegangenen Notebooks und anderen Speichermedien (DVD, USB-Sticks) nicht zugreifbar sind
- Ein Zugriffs-Audit einschließlich Reporting auf alle gesicherten Unternehmens-Dokumente sicherstellen
- Den Zugriff auf gesicherte Dokumente jederzeit verbieten, auch wenn diese Dokumente bereits ausgeliefert sind, das heißt sich nicht mehr innerhalb der IT-Infrastruktur befinden
- Für fast jedes beliebige Dokument besondere Aktionen wie Drucken, Kopieren, Copy/Paste und sogar das Erstellen von Screenshots verbieten
- Prüfen, dass die regulatorischen Kontrollen aktiv sind

Noch besser ist es, wenn diese Schutzmöglichkeiten sehr einfach umzusetzen sind, ohne im Unternehmen eine Komplexität implementieren zu müssen. Gesucht ist eine transparente Lösung, die sich sozusagen in die normale und bestehende Arbeitsumgebung einfügt.

Der kontrollierte Zugriff auf unternehmenskritische Informationen ist besonders heute in der Zeit der zusammenwachsenden Unternehmen (Extended Enterprises) wichtig. Nicht gewollte Datenverluste, Mitarbeiter-Kündigungen, Wirtschaftsspionage, Compliance-Anforderungen, Joint-Ventures und auch das Risiko der internen Bedrohungen nehmen drastisch zu. Eine vollständige und sehr effektive Sicherheitslösung muss heute in der Lage sein, den Zugriffsschutz auf beliebige digitale Daten zu kontrollieren, egal wo sich diese Daten oder Kopien der Daten befinden. Antworten auf die Frage „Wer hat Zugriff auf die Unternehmensdaten?“ müssen möglich sein. Denn ohne dieses Wissen ist eine Kontrolle nicht möglich und somit auch das Risiko nicht abschätzbar.

Oracle Information Rights Management (IRM) in der Version 11*g* bietet eine effektive Information-Security-Technologie an, die alle Kopien der unternehmenskritischen digitalen Daten schützt und zwar überall dort, wo diese Daten gespeichert und genutzt werden, auch außerhalb der Unternehmensgrenzen beziehungsweise Firewalls. Oracle IRM nutzt eine transparente Verschlüsselung und erweitert hiermit die Sicherheit für alle sensitiven Dokumente – egal wo sich diese Informationen befinden (siehe Abbildung 1).

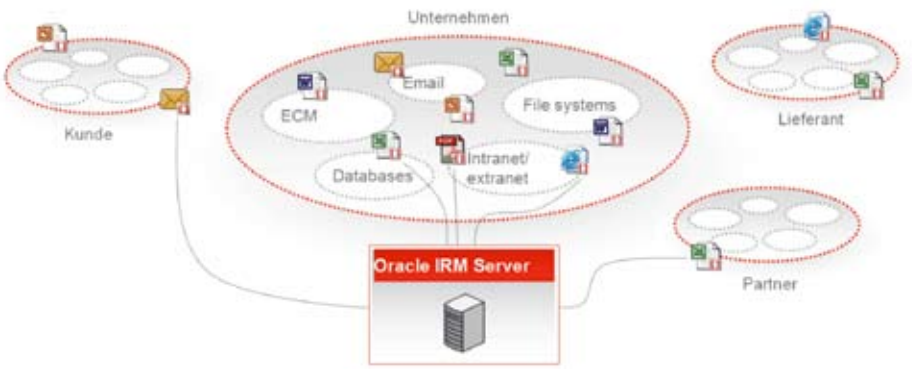

Abbildung 1: Sicherheit und Kontrolle für alle sensitiven Informationen

Erhöhte Sicherheit und Kontrolle ohne Komplexitätssteigerung

Eine Anforderung ist immer gegeben: Sicherheit darf nicht zu erhöhter Komplexität führen. Denn dann ist die Sicherheit nicht praktikabel. Oracle IRM 11*g* schafft es durch seine Anwendungsarchitektur und die Art und Weise, wie die Sicherheit umgesetzt wird, eine effektive und transparente Sicherheit zu implementieren, ohne die Arbeitsweise der Endanwender zu beeinflussen beziehungsweise ohne diesen eine andere Arbeitsweise aufzuzwingen.

Oracle IRM ist eine Policy-basierte Lösung, die in einem zentralen Repository die Policy (Oracle nennt das „Context“) und die anzuwendenden Rollenkonzepte speichert. Der Endanwender bedient mittels eines in der Client-Windows-Umgebung transparenten Oracle-IRM-Desktop-Tools die Policies und setzt diese transparent auf die entsprechenden digitalen Daten um. Der

IRM-Client klinkt sich transparent in die gängigen Windowsanwendungen wie Office, Mail wie Outlook oder Notes, Adobe und andere ein. Mit diesem Konzept sind auf einfache Art und Weise Hunderttausende von digitalen Dateien abgesichert und kontrollierbar (siehe Abbildung 2).

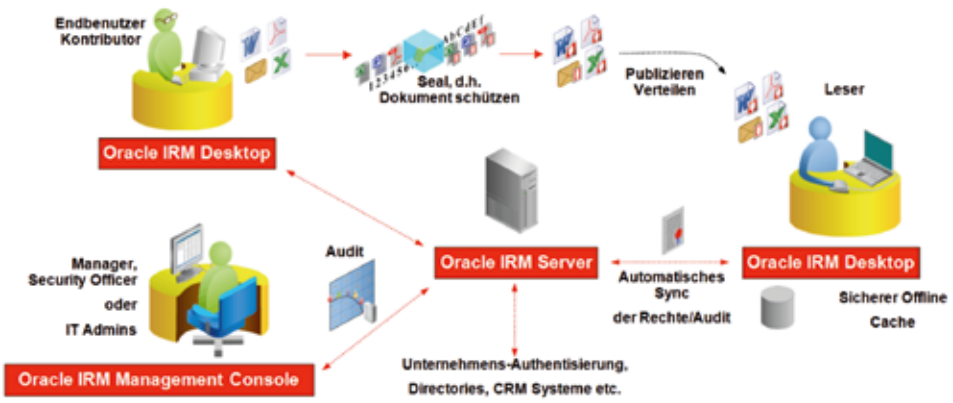

Abbildung 2: Sicherheits-Kreislauf für gesicherte digitale Daten mit Oracle IRM

Standard Rights Model

Oracle IRM nennt sein Klassifizierungssystem „Standard Rights Model“, also ein Modell zur Umsetzung von Sicherheitspolicies. Hier werden Klassifizierungen entsprechend der Sensitivität und Geschäftsbereiche benannt, etwa:

- Top Secret – Vorstandskommunikation
- Beschränkter Zugriff – Projekt A
- Andere

Die Rechte werden basierend auf Rollen vergeben. Projektmitglieder sollten Read/Write-Zugriff auf “Beschränkter Zugriff – Projekt A”, jedoch nicht auf “Top Secret – Vorstandskommunikation” haben. Entsprechend sollten Vorstandsmitglieder Read/Write-Zugriff auf letztgenanntes und eingeschränkten Lese-Zugriff auf “Beschränkter Zugriff – Projekt A” erhalten, um beispielsweise nur ein Monitoring zu ermöglichen, ohne aber selbst am Projekt mitzuarbeiten. Mit diesen geeigneten Rollen und Rechte-Definitionen bleiben bestehende Workflows unberührt, während IRM den Schutzschirm beliebiger digitaler Informationen bietet (siehe Abbildung 3). Der IRM-Client erzwingt die Umsetzung der eingestellten Sicherheits-Policy, und zwar egal wann und wo ein Dokument geöffnet wird:

- Standard-Rollen-Definitionen
- Standard Context (Klassifikation) Templates

Eine Separation von Verantwortlichkeiten ist im Standard und trennt Business und IT:

- System-Management durch die IT-Organisation
- Dokumenten-Kontrolle durch Business-Benutzer

Will der Endanwender ein Dokument schützen, nennt Oracle das Verfahren „Sealing“. Alle „sealed“ Dokumente werden auf Basis einer Sicherheitsklassifizierung durchgeführt. Oracle nennt diese Klassifizierung wie gesagt „Context“ (siehe Abbildung 4). Dieser beschreibt die Beziehung zwischen:

- Einer Gruppe ähnlicher Dokumente, wie Dokumente eines Projekts
- Den Benutzern und Gruppen, die diese Dokumente nutzen, wie das Projektteam
- Den Rollen, die für diese Benutzer und Gruppen erstellt wurden, zum Beispiel Contributor oder Reader und andere

Kontexte werden erstellt, um Informationen zu schützen, und zwar immer im Zusammenhang mit dem entsprechenden Thema oder sensitiven Level. So gibt es verschiedene Kontexte für Vertriebsmaterial, Unternehmensverträge und geheime Projekte.

Sealing – Verschlüsseln und Signieren

Mit definierten Kontexten können die entsprechende Benutzer und/oder Gruppen digitale Daten verschlüsseln („Sealing“). Dieses „Sealing“ umfasst im Wesentlichen drei Dinge:

- Verschlüsselung der Information, so dass es egal ist, wo sich diese befin-

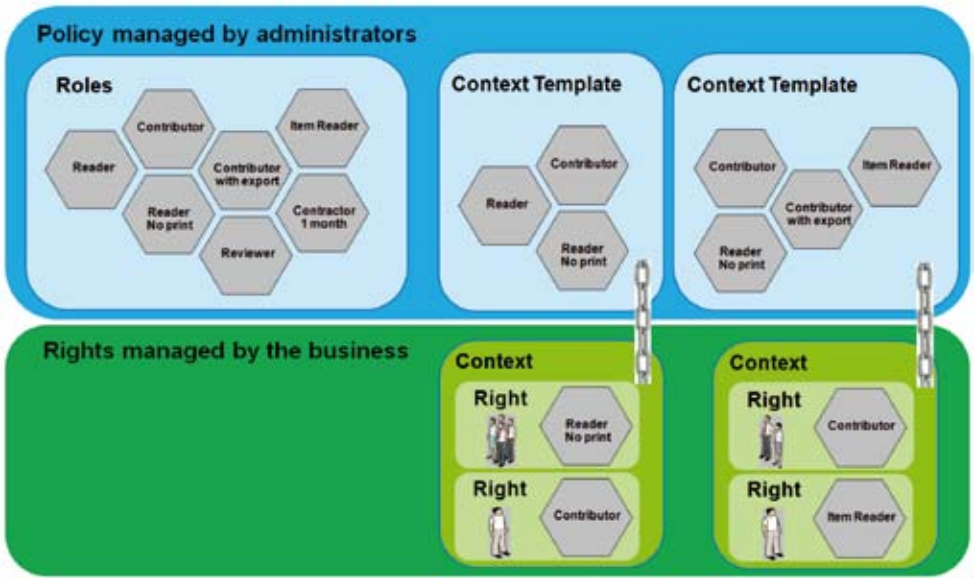

Abbildung 3: Oracle IRM Standard Rights Model

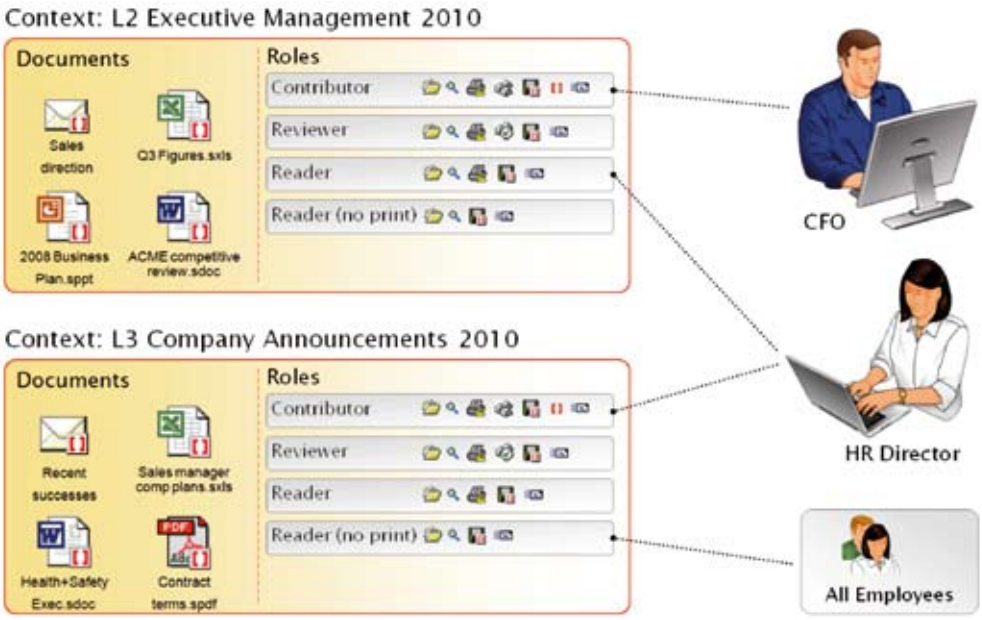

Abbildung 4: Context-, Benutzer- und Rollen-Kombinationen

det. Ohne Entschlüsselungsschlüssel ist die Information dann unbrauchbar. Es stehen verschiedene Verschlüsselungsalgorithmen zur Auswahl

- Einbettung von Metadaten inklusive URL-Links zum IRM-Server, der die Verwaltung des Audits und der Policy für die Information übernimmt
- Digitales Signieren der Information, um diese vor Manipulation zu schützen

Sind die digitalen Daten „sealed", dann ist nur noch ein kontrollierter Zugriff von authentisierten und autorisierten Benutzern und Applikationen möglich. Ein unkontrolliertes Kopieren des entschlüsselten Inhalts funktioniert nicht mehr, das heißt, die Informationen sind für den gesamten Lebenszyklus geschützt.

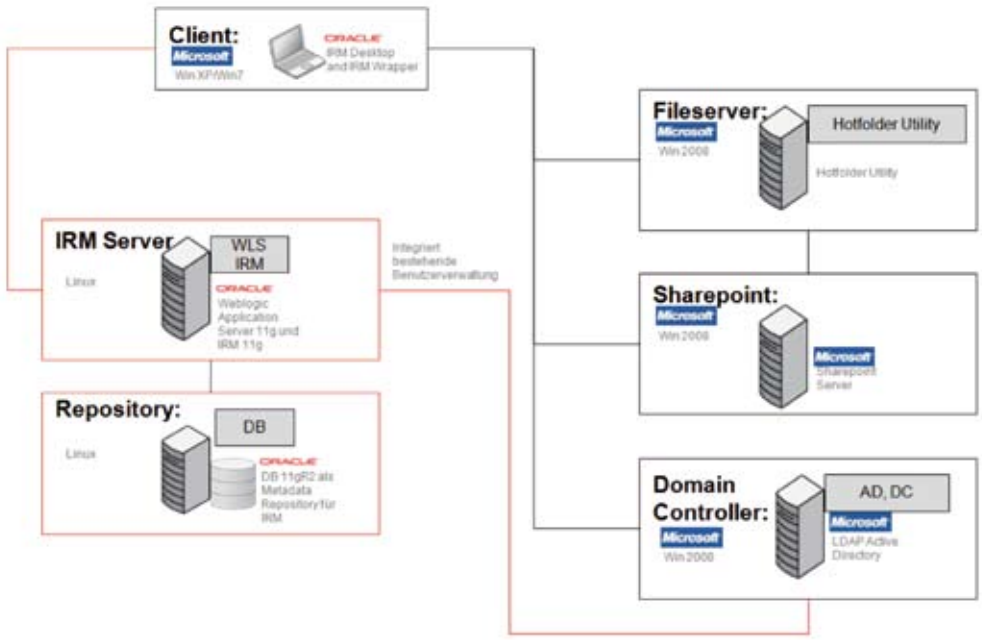

Abbildung 5: Typische Kunden-Umgebung

Aufsetzen einer IRM-Umgebung

Das Aufsetzen einer IRM-Sicherheitslösung ist für fast alle digitalen Dokumente schnell umsetzbar. Eine typische Installation dauert mit einer gegebenen Datenbank in der Regel eine gute Stunde. Abbildung 5 zeigt eine solche typische Kundenumgebung. Hier wird zunächst IRM 11*g* installiert, um eine erhöhte Sicherheit für beliebige Dokumente zu implementieren. Dokumente, die auf einem Fileserver beziehungsweise Sharepoint abgelegt sind, sollen automatisiert verschlüsselt werden. Zudem ist eine bestehende Benutzerverwaltung einzubinden (hier MS Active Directory). Die gute Nachricht ist, dass keine Anpassungen an der Umgebung notwendig sind, das heißt, alle Systeme werden mit Standardmitteln von IRM 11*g* sofort umgesetzt.

Die Installation ist recht einfach, sofern die Datenbank 11*g* R2 bereits installiert ist. Simon Thorpe fasst die Installationsschritte in einem Quick Guide (siehe http://blogs.oracle.com/irm/2010/06/quick_guide_to_oracle_irm_1.html) zusammen:

1. Pre-Installation: Erstellung IRM-Repository-Database-Schema mit Repository Creation Utility 11 (RCU 11*g*) in einer bestehenden Datenbank
2. Pre-Installation: Installation WebLogic Server 11*g*
3. Ausführung des ECM Installers mit einer ECM-Suite-Basis-Installation
4. Erstellung der IRM-Domain mittels Fusion Middleware Configuration Wizard, um dann eine oder mehrere IRM-Service-Anwendungen in einer Oracle WebLogic Server Domain zu erstellen
5. Starten des IRM Admin und Managed Servers

Im Linux-Umfeld wird empfohlen, die Vorbereitungen wie bei der Datenbank-11*g*-Installation durchzuführen, das heißt mit „up2date" alle neuen Libs zu laden, Kernel einzustellen etc. Nach der Installation wurde exakt die

Anwendungsarchitektur von Oracle IRM deployed.

Der nächste Schritt ist die Integration des bestehenden MS Active Directory Servers als Standard-Authentication-Provider. Oracle Weblogic 11*g* erlaubt über die Oracle Platform for Security Service (OPSS) die Einbindung externer Authentication-Provider, siehe http://download.oracle.com/docs/cd/E14571_01/doc.1111/e14495/config.htm#BABGHICG.

Hinweis: Um die Einbindung des MS AD einfacher und beim Aufsetzen schneller zu machen, wird empfohlen, erst nach der AD-Integration auf die IRM-Admin-Konsole zuzugreifen. Somit vermeidet man den Ex- und Import von Benutzern, die bei einem vorherigen Zugriff auf die IRM-Admin-Konsole im internen User Repository angelegt wurden.

Bevor das erste Dokument „gesealt" werden kann, müssen im nächsten Schritt Kontexte erstellt und der IRM-Desktop auf dem Client installiert werden (siehe http://blogs.oracle.com/irm/2010/06/quick_guide_to_oracle_irm_11g_2.html). Der IRM-Desktop integriert sich transparent in den Windows Client. Gibt es im Unternehmen Formate, die nicht out-of-the-box unterstützt sind, kann das IRM Wrapper Tool genutzt werden (siehe https://oracle-irm-wrapper-java.samplecode.oracle.com/). Damit lassen sich beliebige Formate verschlüsseln.

Natürlich ist es möglich, „gesealte" Dokumente auch ohne eine bestehende Verbindung zum IRM-Server zu bearbeiten. Der IRM-Client lässt sich auch im Offline-Modus nutzen. Wie lange der geschützte IRM-Client-Cache ohne Zugriff auf den Server arbeiten kann, wird im IRM-Server eingestellt. Sobald eine Verbindung zum IRM-Server wiederhergestellt wird, synchronisiert sich der IRM-Client mit dem Server.

Letztendlich werden noch der Fileserver und der Sharepoint-Server eingebunden. Hierfür deployed man das Hotfolder-Utility auf den entsprechenden Servern und überwacht damit die freigegebenen Directories des Fileservers und die WebDav-Verzeichnisse der entsprechenden Sharepoint Teamsites. Das Hotfolder Utility besitzt ein „hot.

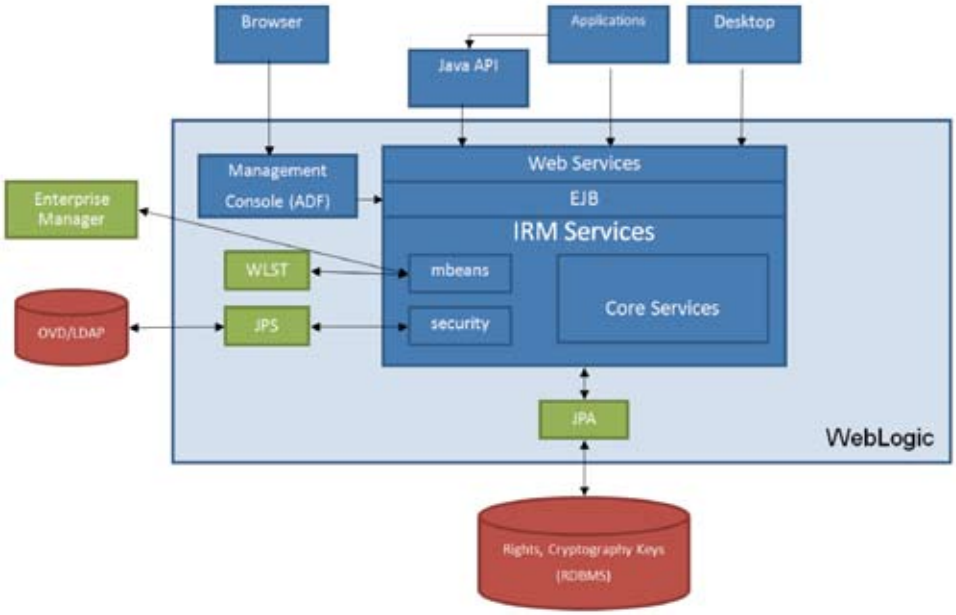

Abbildung 6: Oracle-IRM-Anwendungsarchitektur

properties"-File, in dem die Einstellungen der Folder und die IRM-Sealing-Informationen (Context, Server etc.) einzustellen sind.

Der technische Aufwand, um eine solche typische Umgebung für den Testzweck aufzusetzen, ist äußerst minimal. Bei einer produktiven Umgebung müssen grundlegende Konzepte der Hochverfügbarkeit überdacht werden, die aber mit Standardmitteln der IRM-Infrastruktur (WebLogic Cluster, DB Real Application Cluster) gegeben sind.

Mit der IRM-Infrastruktur sind nun verschiedene Szenarien umsetzbar:

- Klassifizierung, Verschlüsselung und Signierung von digitalen Daten wie Dokumenten
- Automatisierte Überwachung von „Fileshares" und, falls notwendig, automatische Klassifizierung, Verschlüsselung und Signierung von Dokumenten
- Gesicherter E-Mail-Verkehr, das heißt, der unternehmenskritische Informationsaustausch über E-Mail ist nun abgesichert
- Standardanwendungen wie „gesealte" Dokumente erstellen, öffnen oder verändern
- Zugriffsentziehung auf bestimmte digitale Daten
- Der geschützte Content in den Dokumenten kann nicht kopiert werden, auch nicht mittels „Screen-Capture"
- Reporting über das Zugriffsverhalten auf die durch Oracle IRM geschützten Dokumente

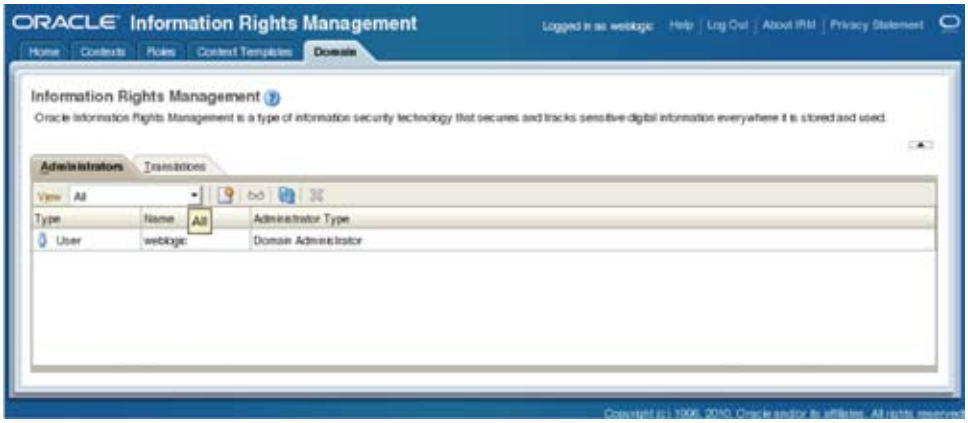

Abbildung 7: Oracle IRM Web-Admin-Console

- Urheber-Informationen in die IRM-Statusmeldung einbauen, so dass zu jeder Zeit sichtbar ist, an wen man sich wenden muss, wenn man Zugriff erhalten will
- Nutzung der geschützten Dokumente auch im Offline-Modus (ohne Zugang zum Internet/Intranet)
- Beliebige Integrationsmöglichkeiten durch die IRM-Webservices

Fazit

Oracle IRM liefert eine Anwendungsarchitektur, die einfach einzuführen ist und die effektiv eine sehr große Anzahl von Dokumenten Policy-basiert schützen kann. Alle Komponenten sowie die Verschlüsselungsalgorithmen der Anwendungsarchitektur sind sicherheitszertifiziert. Die Einfachheit und transparente Anwendung bringt keine zusätzliche Komplexität ins Unternehmen und die meisten Unternehmensanwendungen sowie Formate werden „out-of-the-box“ unterstützt.

Download der Software

- Oracle Weblogic Server 11*g*: http://www.oracle.com/technetwork/middleware/weblogic/downloads/index.html
- Oracle IRM Server 11*g*: http://www.oracle.com/technology/software/products/content-management/index_irm_server.html
- Oracle IRM Desktop: http://www.oracle.com/technology/software/products/content-management/index_irm_desktop.html
- Oracle IRM Repository Creation Utility 11*g*: http://www.oracle.com/technology/software/products/content-management/index_irm_server.html
- Hotfolder Utility: https://oracle-irm-hotfolders-java.samplecode.oracle.com/
- IRM Wrapper: https://oracle-irm-wrapper-java.samplecode.oracle.com/

Weitere Informationen

1. Oracle IRM Whitepaper: http://www.oracle.com/technetwork/middleware/content-management/irm-technical-whitepaper-134345.pdf
2. Oracle IRM Blog: http://blogs.oracle.com/irm/
3. Quick Installation Guide Oracle IRM 11g: http://blogs.oracle.com/irm/2010/06/quick_guide_to_oracle_irm_1.html
4. Oracle IRM Certification Matrix: http://www.oracle.com/technetwork/middleware/content-management/oracle-ecm-11gr1-.xls

Kontakt:
Carsten Muetzlitz
carsten.muetzlitz@oracle.com