

# Wie funktioniert IRM?

## Information Rights Management



© [www.hoffmann-consultingservices.de](http://www.hoffmann-consultingservices.de)

### Das IRM System

Information Rights Management Systeme basieren in der Regel auf einer Architektur, die es ermöglicht, das Rechtemanagement zwischen zentralisierten IRM-Servern und entsprechenden IRM-Desktop Agenten zu verteilen. Die Agenten müssen dazu auf jedem Gerät installiert sein auf dem ein Benutzer vor hat Information zu versiegeln oder versiegelte Informationen zu verwenden. Agenten sind zumeist einfach zu installieren und nehmen nur wenig Speicherplatz in Anspruch. Eine ihrer wichtigsten Aufgaben ist die Authentifizierung der Benutzer, die unter Windows als sogenannte Windows Authentifizierung mittels Single-Sign-On erfolgen kann, das heißt der Benutzer meldet sich einmalig an seinem Windows-Rechner an und hat bereits dadurch Zugriff auf alle Anwendungen und muß sich nicht mehrmals bei unterschiedlichen Clients anmelden. Alternativ kann man sich auch mit dem Usernamen und einem entsprechenden Passwort am IRM-Clients anmelden oder ein zur Verfügung gestelltes Web-basiertes Interface dafür nutzen.

### Verschlüsselung von Dokumente und Verteilungsprozess

IRM Systeme bieten zumeist mehrere Alternativen zum Verschlüsseln und Verteilen von Informationen. Grundsätzlich kann jeder Anwender seine Inhalte schützen und kontrollieren indem er sie an einem IRM Server selbst registriert. Dies kann mithilfe von Standardanwendungen wie Microsoft Office, Microsoft Outlook oder Adobe Acrobat erfolgen. Alternativ kann die Registrierung auch im Hintergrund über die sogenannte Batch-Verarbeitung erfolgen. Unternehmen, die ihren Mitarbeiter diese Entscheidungen nicht individuell überlassen oder sie von dieser Tätigkeit befreien wollen, haben die Möglichkeit durch entsprechende Konfiguration ihrer Systeme Inhalte nach definierten Vorgaben automatisch zu versiegeln. Dies hat den Vorteil, dass Inhalte gemäß unternehmensweiten Sicherheitsrichtlinien geschützt werden können.

Die Initiierung des Registrierungsprozesses bewirkt, dass der IRM-Client eine sichere Verbindung zu einem IRM-Server aufbaut. Der Client authentifiziert sich anschließend am IRM-Server und wählt die gewünschten Sicherheitsparameter aus. Dabei handelt es sich um Zugriffsrechte, Druckrechte, ob Dokumente durch Wasserzeichen geschützt werden sollen, ob ein Ablaufdatum definiert werden soll oder anderes.



Der IRM-Server erzeugt daraufhin einen zufälligen Zugriffsschlüssel für den zu schützenden Inhalt, speichert eine lokale Kopie des Schlüssels mit den dazugehörigen Sicherheitsparametern und sendet den Schlüssel an den Clienten. Der Client verschlüsselt nun den Inhalt mit dem passenden Schlüssel indem er einen symmetrischen Code verwendet und vernichtet den Schlüssel danach.

Nach Abschluss dieses Prozesses besitzt der IRM-Server nur die Policy, also die Vorgehensweise und den Verschlüsselungscode für den Inhalt. Der Client-Computer besitzt nur den verschlüsselten Inhalt. Für den Benutzer ist kein Schlüssel oder gar Klartext verfügbar. Wenn der Inhalt einmal registriert ist, also verschlüsselt, dann kann er sicher im Netz verteilt werden, unabhängig vom verwendeten Mechanismus oder dem benutzten Übertragungsprotokoll. Für die Kommunikation selbst ist es dann nicht mehr entscheidend, ob sie auf sicherem oder unsicherem Weg erfolgt, da der Inhalt an sich geschützt ist.



© [www.hoffmann-consultingservices.de](http://www.hoffmann-consultingservices.de)

Trotzdem gibt es Anwender, die auf eine sichere Kommunikation Wert legen, da sie damit zusätzlich Sicherheit verbinden. Wenn ein Empfänger versucht den geschützten Inhalt zu öffnen, wird der passende IRM-Client automatisch aufgerufen. Der Client baut eine sichere Verbindung zurück zum IRM-Server auf, der die Entschlüsselungscodes besitzt. Der Empfänger wird über diese Verbindung authentifiziert und eine Anfrage nach dem passenden Schlüssel wird abgesetzt um den verschlüsselten Inhalt anschauen zu können. Wenn der IRM-Server akzeptiert, dass der Zugriff autorisiert werden soll, da der Anwender autorisiert ist, die zeitlichen Bedingungen eingehalten werden, die Anfrage von einer gültigen IP-Adresse stammt, etc, dann wird der Schlüssel gemeinsam mit möglichen Anwendungsrestriktionen über die sichere Verbindung versandt. Anwendungsrestriktionen sind Kopiererlaubnis oder Druckerlaubnis, Wasserzeichen oder anderes. Der Client entschlüsselt den Inhalt im Speicher des Rechners und vernichtet dann den Schlüssel. Die Speicherkopie wird gelöscht, wenn der Benutzer die Datei schließt.

Der Besitzer einer Information kann verteilte Rechte für Inhalte jederzeit entziehen oder die Policy ändern. Die Änderungen werden bei der nächsten Anforderung umgesetzt, die bereits dann erfolgen kann, wenn ein Dokument geöffnet, gedruckt oder bei PDF-Dokumenten geblättert wird.



Wenn die Schlüssel auf dem IRM-Server gelöscht werden, entweder manuell durch den Besitzer der Information oder automatisch durch das Überschreiten eines Ablaufdatums, dann werden alle Kopien des Inhalts dauerhaft gesperrt.

Dies wird dadurch erreicht, dass die Clienten niemals lokale Kopien der Schlüssel speichern, außer bei offline-Dokumentenzugriff. Die Kommunikation zwischen Client und Server wird auf dem Server protokolliert. Durch diese Protokolle können Besitzer von Informationen ermitteln, wer auf ihre Inhalte erfolgreich zugegriffen hat, wem der Zugriff verweigert wurde, ob ein Dokument gedruckt wurde und welche IP-Adresse der Client benutzt hat. Damit werden die Möglichkeiten eines Missbrauchs weiter reduziert.

## Kryptographie

IRM-Server verwenden Methoden der Kryptographie um die Sicherheit der elektronischen Informationen zu gewährleisten. Es werden verschiedene Codes mit unterschiedlichen Schlüssellängen verwendet. Ein Code besteht aus einer Gleichung, die auf einfachen Text angewandt wird um codierte Texte zu erzeugen. Zur Entschlüsselung wird der Vorgang umgekehrt um aus dem Code wieder den originalen Text zu erzeugen. Dabei wird ein Schlüssel als Variable der Gleichung verwendet. Die genaue Beschreibung der Kryptographie wird von den Herstellern der IRM-Systeme aus Sicherheitsgründen in der Regel nicht näher erläutert. Ganz allgemein gibt es jedoch zwei grundsätzliche Arten von Verschlüsselung, die symmetrische und die unsymmetrische.

Als Symmetrische Verschlüsselung bezeichnet man eine Methode, die für die Verschlüsselung und die Entschlüsselung jeweils den gleichen Schlüssel verwendet. Bei asymmetrischer Verschlüsselung wird ein Paar von Schlüsseln benutzt, ein Schlüssel zum Verschlüsseln und einer zum Entschlüsseln. IRM Systeme verwenden in der Regel symmetrische Algorithmen.

Damit IRM-Client und IRM-Server sensitive Daten auf sichere Weise austauschen können bedarf es einer sicheren Methode zur Datenübertragung. Ansonsten wäre es möglich die gesendeten Authentifizierungsdaten oder die codierten Schlüssel auf der Leitung abzugreifen.

Die entsprechende Verbindung dazu wird deshalb über ein sogenanntes SSL (Secure Socket Layer) aufgebaut oder über TLS (Transport Layer Security), eine Weiterentwicklung von SSL. SSL und TLS sind hybride Verschlüsselungsprotokolle zur sicheren Datenübertragung im Internet. Dadurch wird sichergestellt, dass ein IRM-Client und ein IRM-Server sicher im Netz miteinander kommunizieren können. Einfache Daten der Benutzer lassen sich aus den LDAP-Verzeichnissen der Unternehmen herauslesen und für die Verwendung mit dem IRM-System einsetzen. Unter LDAP versteht man das sogenannte Lightweight Directory Access Protocol, ein Anwendungsprotokoll für die Abfrage und die Modifikation von Informationen eines Verzeichnisdienstes.



© [www.hoffmann-consultingservices.de](http://www.hoffmann-consultingservices.de)

## Der IRM Server

Der IRM-Server ist ein Software-Service, der Verbindungen von verschiedenen Clienten akzeptiert. Er authentifiziert Benutzer und verwaltet die Autorisierung und den Entzug von Verschlüsselungscodes und Policies für geschützte Inhalte. Dabei stellt das System sicher, dass Einzelne, auch wenn sie autorisierte Benutzer sind, keinen direkten Zugriff auf die verschlüsselten Codes bekommen. Um dies zu erreichen, werden die Verschlüsselungscodes selbst verschlüsselt in der Serverdatenbank abgelegt. Der Schlüssel für diese verschlüsselten sensitiven Informationen wird von der IRM-Serverinstanz generiert, wenn sie selbst erzeugt wird. Sie wird durch ein IRM-Instanz-Passwort geschützt.

IRM-Server verschlüsseln die Codes und die sensitiven Informationen beispielsweise mit dem AES-Algorithmus. Die Schlüsselgröße beträgt 128 Bit und wird im CTR-Modus (counter) verwendet. Andere IRM-Server verwenden dagegen den RC5 Algorithmus, mit ebenfalls 128 Bit, jedoch im CBC Modus (cipher-block chaining).



Neben den Verschlüsselungscodes werden eine Reihe von Konfigurationsinformationen in der Konfigurationsdatei des Servers abgelegt, wobei manche davon ebenfalls sensitiv sind. Zum Beispiel beinhaltet die Datei sowohl den öffentlichen als auch den privaten Schlüssel des Server Zertifikats.

Bevor ein IRM-Server Service gestartet werden kann, muss der Administrator das Server Startup Passwort eingeben. Dieses Passwort wird dafür benutzt den Schlüssel für die Entschlüsselung der sensitiven Informationen der Konfigurationsdatei zu bekommen. Der Server benutzt das Passwort um die Konfigurationsdatei zu entsperren und um die notwendigen Informationen zu extrahieren. Danach wartet der Server auf mögliche Verbindungen der Clienten. Die Konfigurationsdatei selbst wird unter anderem mit dem 3DES (Triple-DES) im CBC-Modus verschlüsselt.

Der Datenbank Verschlüsselungscode wird auch in der Datenbank selbst gespeichert und mit demselben Startup-Passwort geschützt. Damit verhindert man Probleme, die in Situation auftreten können, in denen mehrere IRM-Server dieselbe Datenbank verwenden. Für den Algorithmus, der den Datenbankschlüssel selbst verschlüsselt, wird meist ein DES verwendet (kein 3DES!). Der Schlüssel, der in der Datenbank selbst gespeichert ist, kann durchaus gelöscht werden. Das System läuft trotzdem ordnungsgemäß. Der Schlüssel wird dort nur einmalig bei der Initialisierung der Datenbank erzeugt.



© [www.hoffmann-consultingservices.de](http://www.hoffmann-consultingservices.de)

## IRM-Clienten

Die IRM-Clienten können zumeist Microsoft Office Dokumente, PDF-Dokumente und email-Nachrichten aus MS Outlook oder auch Lotus Notes schützen. Unter Verwendung eines IRM SDK (System Development Kits) können zusätzliche IRM-unterstützte Applikationen entwickelt werden um Inhalte anderer Datenformate zu schützen.

Entscheidend ist, dass die Schlüssel niemals jemandem zugänglich gemacht oder gar auf der Platte eines Klienten gespeichert werden. Ansonsten gäbe es keine Möglichkeit Policy-Änderungen sicherzustellen oder Zugriffsrechte wieder zu verweigern. Deshalb wird große Sorgfalt darauf gelegt die Wahrscheinlichkeit zu minimieren, dass diese sensitiven Information zugreifbar werden. Zum Beispiel werden Verschlüsselungscodes sofort vernichtet, sobald sie nicht mehr benötigt werden.

## Beispiel der Verschlüsselung eines Herstellers

Um Inhalte zu verschlüsseln benutzt der IRM-Server die AES-256 Block-Verschlüsselung im CTR-Modus für Microsoft Office Dokumente. IRM-basierte Applikationen, die mit der Clienten-Integrations APIs erstellt wurden, verwenden die AES-128 Block Verschlüsselung im CTR-Modus. Für PDF-Dokumente wird eine der folgenden Verschlüsselungen verwendet:

- bei Verwendung von seitenweiser Verschlüsselung: AES256 im CBC Modus
- bei Verwendung von dokumentenweiser Verschlüsselung: AES-128 im CBC Modus.  
Dieser wird deshalb genommen, da Acrobat höchstens eine 128 Bit Verschlüsselung im Dokumentlevel erlaubt.

Die Entschlüsselung wird entweder in Acrobat oder im Adobe Reader durchgeführt.

## IRM SDK

Das IRM Server Software Developer's Kit (SDK) ist eine Sammlung von APIs, die für die Automatisierung von Managementfunktionen benutzt werden kann. Damit lassen sich Erweiterungen für die IRM Server Autorisierungsarchitektur schreiben. Es lassen sich auch eigene Applikationen integrieren um Inhalte in verschiedenen Formaten zu schützen.

## Benutzer und Gruppen

Wenn man Authentifizierungsdomains erzeugt hat und individuelle gemeinsam genutzte Accounts eingerichtet wurden, dann kann man Benutzer oder Gruppen hinzufügen unabhängig von der Art der Policy. Dadurch kontrolliert man die Autorisierung. Während eine Authentifizierungsdomain oder gemeinsam genutzte Accounts Benutzern erlauben sich zu authentifizieren, identifiziert eine Gruppe einen oder mehrere Benutzer und legt fest welche Rechte sie haben.



© [www.hoffmann-consultingservices.de](http://www.hoffmann-consultingservices.de)

Jeder Benutzer, der auf einen IRM Server zugreift, muss mindestens einer Gruppe angehören. Man kann auch LDAP Directory Service nach Benutzern und Gruppen fragen oder eine LDAP-Anfrage zu einer Gruppe hinzufügen, sofern eine LDAP Authentifizierungsdomain oder eine Authentifizierungsdomain mit LDAP Fähigkeiten eingerichtet wurde. Es kann festgelegt werden, ob Benutzer oder Gruppen von einem bestimmten Netzwerk aus oder zu einer bestimmten Zeit zugreifen dürfen. Außerdem kann festgelegt werden, ob anzeigen, drucken oder kopieren von geschützten Inhalten erlaubt werden sollen oder ob Gastaccounts zugreifen dürfen, ob Löschen oder automatisches Löschen benutzbar sind oder ob Benutzer offline arbeiten dürfen.

Wenn ein Benutzer in mehr als einer Gruppe ist, dann werden Genehmigungen für das Drucken oder Editieren als logisches "ODER" der Gruppenrechte evaluiert und die Genehmigung gemäß der am wenigsten restriktiven Policy erteilt. Gruppenrechte lassen sich auch vererben.

Ein IRM Server beinhaltet verschiedene Ebenen von Administratorberechtigungen.

## Policies

Policies werden dazu verwendet Zugriffsrechte für ein vorhandenes Dokument zu steuern. Die Policy Optionen beinhalten in der Regel folgendes:

- eine Zugriffsliste, die die Benutzer, Gruppen und die Netzwerkstandorte, die auf das Dokument zugreifen können, beinhaltet
- Rechte: Die Dokumentenrechte beinhalten Drucken, Kopieren und Editieren von Dokumenten
- Verfügbares Datum: Das Datum an dem das Dokument den Nutzern zur Verfügung gestellt wurde
- Ablaufdatum: Datum oder Zeitspanne nachdem niemand mehr in der Lage sein wird auf das Dokument zuzugreifen
- Wasserzeichen: Zuweisung eines Wasserzeichens, wenn das Dokument gedruckt wird

## Offline-Zugriff

Grundvoraussetzung des IRM Ansatzes ist es, dass der Benutzer mit dem Server verbunden sein muss um auf geschützte Informationen zugreifen zu können. Mit der Verwendung von Breitband-Netzwerken und dauerhaften Verbindungen ist dies eine durchaus sinnvolle Forderung. Trotzdem kann es Fälle geben, in denen eine Verbindung nicht machbar ist.



© [www.hoffmann-consultingservices.de](http://www.hoffmann-consultingservices.de)

Für diese Fälle ist das IRM System in der Lage sogenannte Gutscheine (Vouchers) zu vergeben, die auf einem lokalen Clienten liegen. Wie bei anderen Gutscheinsystemen sind die Information verschlüsselt und so optimal wie nur möglich gegen Angriffe geschützt. Mit Hilfe der Dokumentenpolicy können sowohl der Informationsbesitzer auch als der IRM Serveradministrator überprüfen, ob einem Dokument die Erlaubnis für eine offline Benutzung gegeben wird oder nicht.

Der Informationsbesitzer kann bestimmen über welchen Zeitraum die offline-Verarbeitung erlaubt sein soll. Beispielsweise kann eine Erlaubnis für genau zehn Tage gegeben werden. Danach ist das Dokument nicht mehr zugreifbar, solange sich der Nutzer nicht wieder mit dem IRM Server verbindet.

Der offline-Zugriff entspricht dem online-Zugriff. Wenn man sich online authentifizieren muss, dann ist diese Information auch offline erforderlich. Die Genehmigungen für offline entsprechen denen bei online (z.B. editieren, drucken und kopieren).

Aus Sicherheitsgründen sorgen Änderungen an der Systemuhr des Clienten für einen Entzug der offline Rechte.

## Audits, Reports und Benachrichtigungen

Kein Sicherheitssystem der Welt ist vollständig sicher. Trotzdem gibt es eine Fähigkeit, die dabei hilft die Sicherheit eines bestehenden Systems zu maximieren. Hierbei handelt es sich um das Audit. Eine dafür wichtige Notwendigkeit besteht darin, dass der IRM Server in jeden Zugriff auf sensible Informationen eingebunden ist. Damit ergibt sich die Möglichkeit alle Zugriffe zu protokollieren. Es wird nicht nur festgehalten, wer auf welche Information zugegriffen hat, sondern es wird auch protokolliert wem der Zugriff verweigert wurde und von welcher IP-Adresse aus es versucht wurde. Oftmals genügt schon die Warnung vor den Audits vor den Versuchen unberechtigten Zugriffs. Zusätzlich kann man sich als Informationsbesitzer eine Benachrichtigung schicken lassen, wenn die Serverlog-Messages vorher gesetzten Bedingungen entsprechen.

## Datenbank

Der IRM-Server benötigt einen Tablespace in einer relationalen Datenbank. Abhängig von der Betriebssystemplattform auf der der IRM-Server installiert ist, können unterschiedliche Datenbanksysteme verwendet werden. Oft werden Datenbanksysteme von Oracle oder Microsoft verwendet. Die Datenbank wird dafür benutzt Informationen wie verschiedene Schlüssel, einige Konfigurationseinstellungen, Policies und Gruppen zu speichern. Ein einfacher Tablespace kann für mehrere Instanzen eines IRM Servers verwendet werden, die zusammen arbeiten.



© [www.hoffmann-consultingservices.de](http://www.hoffmann-consultingservices.de)

## Ausschalten der Screen Capture Funktionalität

IRM-Systeme beinhalten zumeist eine Funktion, die auch als Advanced Screen Capture Defeat (ASCD) bezeichnet wird. Sie schützt davor, dass Bildschirme mit der MS Windows PrintScreen-Funktion einfach abfotografiert werden oder dass Produkte von Drittanbietern den Bildschirminhalt auslesen. Diese Funktionen werden von Nutzern benutzt, die sich unberechtigter Weise Inhalte speichern wollen. Natürlich kann auch das Abschalten dieser Funktion nicht davor schützen, dass jemand mit einer Digitalkamera den Bildschirm abfotografiert oder einfach auf Papier abschreibt was er gerade liest oder auch den Bildschirm eines Laptops auf einen Kopierer legt.

## Klassifikationsbasierendes Rechtemanagement

Im Gegensatz zur Datei-basierten Verwaltung liefert das Klassifikationsbasierte Rechtemanagement eine Vereinfachung bei der Verwaltung der Benutzer und ihrer Zugriffsrechte. Mit zunehmender Anzahl von Dateien wird es erfahrungsgemäß immer komplexer die richtigen Benutzer oder Gruppen mit den entsprechenden Dateien zu verknüpfen. Ein rollenbasierter Ansatz reduziert die Anzahl der Zuweisungen um ein Vielfaches. Dazu werden die Benutzer entsprechend in verschiedene Rollen klassifiziert und deren Rechte entsprechend gesetzt. Standardmässig existiert bereits ein Reader, ein Reviewer und ein Contributor in einem jeweiligen Kontext.

Für die Administration lässt sich ebenfalls ein rollenbasiertes Rechtemodell einführen. Administrative Aufgaben wie das Erzeugen von Sicherheitskontexten, die Definition von neuen Rollen oder das Zuordnen können verschiedenen Benutzern oder Gruppen zugewiesen oder entzogen werden. Damit kann die Administrationsaufgabe auch von einzelnen Benutzern oder Gruppen übernommen werden, ohne dass ein separater Administrator erforderlich ist.

## Gastzugriff

Den Benutzern kann erlaubt werden eine Policy zu erzeugen, die Gästen Zugriff ermöglicht. Wenn geschützte Inhalte mit Gastzugriff versehen werden, dann kann derjenige, der sich den Inhalt ansehen möchte es ohne Authentifizierung tun. Natürlich muss der Gast einen IRM Client installiert haben und mit dem IRM Server in Verbindung stehen. Der Gastbenutzer wird wie jeder andere auch von den genehmigten oder entzogenen Rechten gesteuert, die in der Policy definiert sind und unterliegt auch den Server Restriktionen. Ebenfalls werden alle seine Aktivitäten protokolliert.

## Netzwerk Deployment und Konfiguration

Wie bereits vorher beschrieben ist der IRM Server ein Service und die Clients sind Plug-ins. In den unterschiedlichen IRM-Systemen gibt es keine Einstellungen, die in Bezug auf ein Loadbalancing oder eine Hochverfügbarkeit stehen. Die Unterstützung mehrerer IRM Server wird vom DNS übernommen, von anderer Hardware oder dem Basis Netzwerk. Der IRM Server nutzt TCP für die Verbindung zwischen dem Server und externen Einheiten, wie SMTP, LDAP oder ODBC. Ein einzelner Host kann mehrere Instanzen eines IRM Servers besitzen.



© [www.hoffmann-consultingservices.de](http://www.hoffmann-consultingservices.de)

Mindestens eines der verschiedenen IRM-Systeme unterstützt vollständig virtualisierte Infrastrukturen. So kann dieser IRM Server auch in einer VMWARE Umgebung eingesetzt werden. Dabei kann das System in einem active-active Netzwerk konfiguriert werden um hochverfügbar über Failover und Loadbalancing gemacht zu werden. Typische IRM Implementierungen beinhalten zwei oder mehr IRM Server, die in einer active/active Konfiguration eingerichtet werden mit einer physisch separierten Datenbank oder einem Cluster.

Genauere technische Dokumentationen und Benutzerhandbücher finden sich auf den Internetseiten der einzelnen Hersteller. Diese sind jedoch größtenteils nur in Englisch verfügbar und besitzen unterschiedliche Umfänge und Detaillierungsgrade.



### KONTAKT

email: [info@hoffmann-consultingservices.de](mailto:info@hoffmann-consultingservices.de)

Tel: +49 (7141) 24 22 473

mobil: +49 (172) 83 22 925