GEA Westfalia Separator Group GmbH

Digitales Rechtemanagement für SAP®-Dokumente

Die GEA Group Aktiengesellschaft ist einer der größten Systemanbieter für die nahrungsmittelverarbeitende Industrie und bietet ein breites Spektrum von Prozessindustrien mit einem Konzernumsatz von rund 4,3 Milliarden Euro in 2013. Der Konzern generiert ca. 70 Prozent seines Umsatzes aus der langfristig wachsenden Nahrungsmittelindustrie. Zentrifugen von GEA Westfalia Separator werden weltweit zum Reinigen und Separieren oder Klären von Flüssigkeiten, sowie zum Abtrennen von Feststoffen eingesetzt.

Mit der Unterstützung und Lösungen der SEAL Systems AG hat die GEA Westfalia Separator Group GmbH ein umfangreiches eDRM-System (Enterprise Digital Rights Management) für alle mit SAP DVS (Dokumentenverwaltungssystem) verwalteten Dokumente eingeführt.

DRM für SAP DVS: Anforderungen und Motivation

Die GEA Group ist ein global aufgestellter Konzern mit vielen internationalen Standorten und Partnern. Operative Arbeitsabläufe mit Kunden und Montagefirmen erfordern den Austausch von Dokumenten, die mit dem SAP DVS verwaltet werden. Gerade bei der Verteilung von Dokumenten an externe Empfänger können Informationssicherheit und Know-How-Schutz jedoch nicht mehr über das Rechtemanagement von SAP gewährleistet werden.
Um durchgängigen Know-How-Schutz zu erzielen wurde ein Projekt zum Thema „Digitales Rechtemanagement“ aufgesetzt. Das Ziel: Alle Dokumente aus dem SAP DVS sollten konsequent von der Ablage bis zum Empfänger geschützt sein, auch wenn sie das Unternehmensnetz verlassen.

„Schlupflöcher“, um Dokumente ungeschützt aus dem SAP DVS in Umlauf zu bringen, sollten geschlossen werden. Dazu müssen alle relevanten SAP-Schnittstellen überwacht werden, die im SAP-System zum Export von Dokumenten genutzt werden können.
Ein eDRM-System von Adobe (LiveCycle Rights Management) wurde als optimal geeignete Lösung identifiziert.

Um die DRM-Funktionalität lückenlos für alle relevanten Dokumente und Geschäftsprozesse bereitstellen zu können wurde die SEAL Systems AG mit der Bereitstellung aller nötigen Softwaremodule, sowie der System- und Prozessintegration beauftragt. SEAL Systems verfügt über umfangreiche Kenntnisse zur Anbindung externer Systeme an SAP DVS und bietet zudem ausgereifte Technologien zur Prozessintegration und Workflowprogrammierung.

System- und Prozessintegration

Das Adobe LiveCycle Rights Management wurde über die Digital Process Factory (DPF, siehe Infobox) von SEAL Systems mit dem SAP-System gekoppelt. Hierbei kamen weitestgehend Standardintegrationen von SEAL Systems zum Einsatz. Der Umsetzungsaufwand dieses Schrittes war daher gering.

Die Digital Process Factory fungiert als intelligente Schnittstelle zwischen der SAP-Welt und dem DRM-Server. Mit der DPF werden nun alle relevanten SAP-Schnittstellen bei GEA überwacht, die von SAP systemseitig für einen Export von Dokumenten genutzt werden können (z.B. Druck, Email, Aufruf im Viewer). Am jeweiligen Userexit wird über einen DPF-Workflow automatisiert geprüft, ob es sich um eine für die DRM-Verschlüsselung relevante SAP-Dokumentenart handelt. Dokumentenarten sind eine Möglichkeit des SAP DVS, Dokumente nach charakteristischen Merkmalen sowie den sich daraus ergebenden organisatorischen Abläufen zu unterteilen.

Digital Process Factory® (DPF)

Digital Process Factory ist eine Entwicklungs- und Laufzeitumgebung für den Entwurf und die Ablaufsteuerung von Prozessen zur Verarbeitung von Informationen, Daten, Dateien und Dokumenten. Für die Gestaltung kundenspezifischer Abläufe und Verfahren ist die DPF hocheffizient, denn Programmieren wird durch das Konfigurieren von Standardverfahren ersetzt.

Das Prinzip: Elementare, standardisierte Verarbeitungsbausteine, die WorkingUnits, werden zu variablen Verarbeitungsabläufen zusammengestellt. Für Zusammenbau und Ablaufsteuerung gibt es interaktive Werkzeuge.

Die Projektgruppe bei GEA Westfalia Separator definierte parallel zur Installation durch SEAL Systems die Regeln und Parameter für den Einsatz des digitalen Rechtemanagements. Diese umfassen z.B. die Anwendergruppen mit den entsprechenden Rechten, sowie Definitionen, bei welchen Aktionen ein Dokument DRM-geschützt und/oder zusätzlich mit SAP-Informationen bestempelt werden muss.

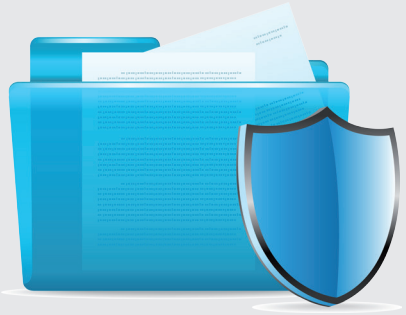
Über eine SAP-Tabelle wurde festgelegt, welche Dokumentenarten der DRM-Verschlüsselung unterliegen sollen und welche keinen DRM-Schutz benötigen. Die in SAP hinterlegten Informationen werden ermittelt und an die DPF von SEAL Systems zur Steuerung der DRM-Verschlüsselung übergeben. Das DRM-Regelwerk wurde anschließend auf dem eDRM-Server umgesetzt. Die zugriffsberechtigten Personen werden im zentralen LDAP gepflegt. Dabei entsteht kein zusätzlicher Verwaltungsaufwand, da dieser Personenkreis ohnehin für jedes Projekt im LDAP zusammen gestellt wird.

Das Ergebnis: Alle möglichen Verteilwege für SAP-verwaltete Dokumente werden von der SEAL Systems DPF überwacht. Möchte ein Anwender Dokumente ausgeben, werden diese automatisiert auf „DRM-Relevanz“ geprüft. Handelt es sich um eine zu verschlüsselnde Dokumentenart, leitet die DPF das Dokument automatisch an den DRM-Server weiter, wo es nach der entsprechenden DRM-Richtlinie (z.B. „read-only“) verschlüsselt wird. Anschließend wird das DRM-geschützte Dokument auf dem normalen Weg ausgegeben/verteilt.

Fazit

Der Know-How-Schutz für die technischen Projektunterlagen ist jetzt gegeben. Alle Dokumente, die an die internationalen Baustellen in digitaler Form verschickt werden, sind jetzt mit dem DRM verschlüsselt.
Das erfolgt über die SEAL Systems Integration automatisch und fehlerfrei. Das Projekt konnte entsprechend des vorgesehen Terminplans und in partnerschaftlicher Zusammenarbeit umgesetzt werden.

eDRM für Business- und Engineering-Dokumente



In der jüngsten Vergangenheit wurde digitales Rechtemanagement intensiv bei der Zuteilung von Nutzungsrechte an Unterhaltungsmedien (Filme, Musik, eBooks etc.) verwendet. Daher denkt man bei DRM zunächst oft an den Schutz von digitalen Unterhaltungsmedien.

Unter Enterprise Digital Rights Management (eDRM) versteht man darüber hinaus Systeme zum Schutz von Unternehmensdaten. Das können wichtige Wirtschaftsdaten sein, aber auch die Vielzahl an Dokumenten, die das Knowhow des Unternehmens beinhalten: technische Zeichnungen, Berechnungen, Spezifikationen, Rezepturen, Angebote [...]. Mit eDRM können Unternehmen vermeiden, dass vertrauliche Daten in die falschen Hände geraten. Dynamische Richtlinien ermöglichen es, wichtige Informationen zu schützen: innerhalb und außerhalb der Firewall und auf Mobilgeräten. Die eDRM-Architektur garantiert dabei den durchgängigen Schutz von Dokumenten, egal ob der Benutzer online oder offline ist.

Eine eDRM-Infrastruktur basiert auf einem zentralen Server, der die Verschlüsselung der Dokumente vornimmt und die Rollen und Rechte der potenziellen Empfänger verwaltet. Bei jedem Öffnen eines vorher verschlüsselten Dokuments muss die jeweilige Clientapplikation (z.B. Adobe Reader) vor der Anzeige beim zentralen eDRM-Server die Rechte des entsprechenden Anwenders abfragen. Die Clientapplikation muss zur Wahrung der Sicherheit dabei die komplette Verarbeitung des Dokuments im Hauptspeicher vornehmen. Entschlüsselndes und darstellendes Programm sind also zwingend dasselbe. Auf diese Weise wird sogar der unauthorisierte Dokumentenzugriff durch Schadsoftware/Manipulationen auf dem Client des Dokumentenempfängers verhindert.

Empfängern von Dokumenten werden auf dem eDRM-Server spezifische Rollen und Rechte zugewiesen. So können z.B. die Möglichkeiten zum Betrachten, Bearbeiten, Drucken oder Versenden des Dokumentes eingeschränkt werden. Nutzerunabhängige, zentrale eDRM-Funktionen umfassen beispielsweise die mögliche Festsetzung von Gültigkeitszeiträumen bei der Verteilung eines Dokumentes. Nach Ablauf der Gültigkeit ist das Dokument automatisch nicht mehr verwendbar. Dokumente können auch nach der Verteilung zurückgezogen/gesperrt werden. Zudem kann über die detaillierten Buchungskontrollverfahren des eDRM-Systems die Verwendung geschützter Dokumente nachvollzogen werden.

Vorteile des Einsatzes von eDRM im Unternehmen:

- Proaktiver Schutz vertraulicher Informationen in PDF-, Microsoft Office- und anderen Dokumenten, sodass sie nicht außerhalb des Unternehmens/des authorisierten Empfängerkreises weitergegeben werden.
- Beschränkung des Zugriffs auf vertrauliche Daten auf einen bestimmten Personenkreis
- Ändern von Zugriffsrechten oder Widerruf des Zugriffs auf Dokumente zu jeder Zeit, auch nach deren Bereitstellung
- Überwachung der Verwendung geschützter Dateien durch detaillierte Buchungskontrollverfahren
- Nachvollziehbarkeit der Informationsverteilung bei Audits
- Versionsverwaltung: veraltete Dokumente können sogar nach Verteilung wieder gesperrt werden

Haben Sie Fragen?

SEAL Systems AG, Dr. Uwe Wächter
uwe.waechter@sealsystems.de