SEALSYSTEMS THE DIGITAL PAPER FACTORY

GEA Westfalia Separator Group GmbH

Digital Rights Management for SAP® Documents

GEA Group is one of the largest suppliers for the food processing industry and offers a wide range of equipment and facilities. In 2013, GEA generated consolidated revenues of 4.3 billion Euro. More than 70 percent of this came from the food sector, which is a long-term growth industry. Centrifuges from Westfalia Separator are used worldwide for cleaning, separating or clearing of liquids or separation of solids from suspensions.

With the knowledge and the solutions from SEAL Systems an extensive eDRM system (Enterprise Digital Rights Management) for all SAP DMS (Document Management System) documents was implemented at GEA Westfalia Separator Group.

DRM for SAP DMS: Requirements and Motivation

GEA Group is a global enterprise with many international locations and partners. Operative workflow processes with customers and assembly companies require the exchange of documents, stored and managed with SAP DMS. But during distribution of documents to external recipients, the information security and knowledge protection cannot be controlled and guaranteed with the rights management of SAP.

To obtain a continuous protection of company intellectual property, a project for “Digital Rights Management” was established. The target: All documents of the SAP DMS should be consequently protected beginning from storage until sending to recipients, even if the documents leave the company‘s environment.

Intolerable “loop holes” for unprotected circulation of documents from the SAP DMS should be closed. For this all relevant SAP interfaces, which are used for document export from the SAP system had to be controlled.

An eDRM system from Adobe (LiveCycle Rights Management) was identified as the optimal solutions for this.

In order to provide a gapless DRM functionality for all relevant documents and business processes SEAL Systems was asked to install all required software modules and to integrate the processes in the system. SEAL Systems has extended knowledge for connection of external systems to the SAP DMS and in addition, offers mature technologies for process integration and workflow programming.

System and Process Integration

The Adobe LiveCycle Rights Management system was connected to the SAP system with Digital Process Factory® (DPF, see info box) from SEAL System. For this, mostly standardized integrations from SEAL Systems were used. Therefore the efforts of substantial implementation were rather low.

The Digital Process Factory works as an intelligent interface between the SAP environment and the DRM server. With DPF, now all relevant SAP interfaces are supervised. They can be used in the SAP system for export of documents, for example, print, email, or viewing. At the respective Userexit a DPF workflow automatically checks, whether it is an SAP document type, which is DRM encrypted. Document types in SAP DMS are used for separation of characteristic document features, which start special organizational workflows.

During installation through SEAL Systems the project group at GEA Westfalia Separator defined the rules and parameters for the use of the digital rights management. These are, for example, the user groups with the corresponding rights. Also definitions were designated for which actions a document will be protected and additionally stamped with SAP information.

With an SAP table, definitions were assigned, which document types should be DRM encrypted and which documents doesn‘t need protection. The information, stored in SAP, are then retrieved and transferred to the DPF for control of the DRM encryption process. The DRM set of rules then was implemented on the eDRM server. The data of the authorized persons are kept in the central LDAP system. This means no additional administrative effort, because this personal data is kept for each project in LDAP anyway.

The result: All possible distribution methods for SAP managed documents are supervised by DPF from SEAL Systems. If a user wants to output documents, an automatic process checks the DRM properties. In case it is an encrypted document type, DPF transfers it to the DRM server. There it is processed according to the specific DRM rule, for example “read-only”. Then the DRM protected document is output or distributed as usual.

Digital Process Factory® (DPF)

Digital Process Factory is a development and runtime environment for design and runtime control of workflows for information, data, file and document processing. For the design of customer-specific workflows and processes DPF provides a highly efficient system, because programming is replaced by configuration of standardized methods.

The principle: Elementary, standardized processing steps, the WorkingUnits, are combined to variable process workflows. There are interactive tools for assembly and runtime control.

Summary

The knowledge protection for technical project documents is ensured now. All documents, which are sent as digital data to international construction sites, are DRM encrypted now. This is automatically done with the SEAL Systems integration in a reliable and error-free method. The project could be implemented within the scheduled time plan with cooperative partnership.

eDRM for Business and Engineering Documents

In the recent past, digital rights management was intensively used for assignment of the use of rights of entertainment media, for example films, Music, eBooks etc. Therefore often DRM is thought of in connection with the protection of digital entertainment media.

Enterprise Digital Rights Management (eDRM) means systems for protection of company knowledge. This can be important economic data, but also a number of documents, which contain the technical knowledge of enterprises: technical drawings, statistical data and calculations, specifications, recipe formulas, proposals [...]. With eDRM, companies can avoid the loss of confidential data. Dynamic guideline standards enable to protect important information: within and outside of firewalls and on mobile devices. The eDRM architecture guarantees the continuous protection of documents, independent of the fact, that the user is online or offline.

An eDRM infrastructure is based on a central server, which does the document encryption and administration of roles and rights of the recipients. At each opening of an encrypted document the respective client application, for example Adobe Reader, asks for the rights of the user at the central eDRM server. To ensure security the client application does the complete document processing in the RAM main storage. The program, which does the decryption, must be the same as the program which does the viewing of the document. This way even the unauthorized document access through malware or manipulation on the client of the document recipient is not possible.

On the eDRM server, recipients of documents are assigned to specific roles and rights. Thus, for example, the possibilities for viewing, editing, printing or sending of documents can be restricted. User independent central eDRM functions can, for instance, define the duration of validity time periods during distribution of documents. After the expiration of the access validity the document is automatically no longer usable. Documents can also be withdrawn or blocked after distribution. In addition, the usage of protected documents can be tracked by cross control methods of the eDRM system.

Advantages of enterprise-wide use of eDRM:

- Protection of confidental information in PDF, Microsoft Office and other documents. This prevents the transfer of company knowledge outside the enterprise and the authorized recipients.
- Access control for confidental data and restriction to a certain group of people.
- Change of access rights or cancellation of access to documents at any time, also after distribution.
- Supervision about usage of protected files through detailled account control methods.
- Traceability of information distribution for evaluation audits.
- Version management: obsolete documents can be locked even after distribution.

Do you have any questions?

SEAL Systems
info@sealsystems.com