SEALSYSTEMS
THE DIGITAL PAPER FACTORY

FACTSHEET

Digital Rights Management

Enterprise Digital Rights Management

What is Digital Rights Management?

With DRM the access regulations of documents are managed by a **central server**. The single rights (read, print, extract, store, etc.) are **centrally managed** and are not stored in the document itself. The usage of DRM is especially important, when documents are not under the **access control** of the own **document management system**, for example if the document have to be provided to suppliers or customers.

After document check-out from the DMS the relevant files are **encrypted** before distribution. A free accessable version of the document remains in the DMS. It is still controlled through the internal DMS user access control. The distributed version can only be used by persons, which apply for an **authorization** on the DRM server.

What can DRM do?

The solutions for DRM guarantee **protection of know-how** during the cooperation with other partners at document level. They allow the **complete control** of the data exchange in every stage of a project – from product development to cooperation with suppliers and the creation of work instructions up to maintenance processes.

Who needs DRM?

Everyone, who has to provide information in any file based kind to recipients outside their own company.

Digital paper offers a number of functions and is an essential part of business processes. If documents are managed with a document management system, then the access is controlled by the DMS. Only authorized users can use the documents released for a special process. These access rights can be changed at any time.

If documents are to be distributed **outside the DMS**, the situation is completely different. During the cooperation with other companies (customers, partners or suppliers) the documents must be provided outside the DMS. For example PDF files can be copied through **authorized** employees from the secure areas of the DMS. Now the user can store these files on a local hard disk and transfer them to any other people. This procedure is necessary for single procurement business processes, but it is to consider that the know-how of an enterprise is in these files. Therefore the access of these data must be **controlled** and **supervised**..

Advantages

- **Complete control of the data exchange**
- **Central management of single rights**
- **Document protection for PDF**
- **Highest security level through ecryption methods**

Enterprise Digital Rights Management

How does DRM work?

The functionality is described exemplary for the Adobe LC ES DRM.

If a user wants to open a DRM protected file, the Adobe Reader will detect the **encrypted content**. The program asks the user for his **user name** and the password. This data is compared with the data on the DRM server. If the DRM server is connected with the internet, this comparison also works outside their own company. The DRM server transfers the allowed functions for this file and for this special user to the Adobe Reader. If a user loses a special right for a certain function in the PDF, this right can be deleted on the DRM server and the PDF cannot be opened any longer. A local copy of the PDF file, which is opened in the Adobe Reader, is worthless, because it is still encrypted.

Adobe does not only offer an effective document protection for PDF. Also plug-ins for the **Microsoft Office Suite** encrypting of native Office documents are included. The Office files are then sent out **encrypted** to the recipient. If the necessary plug-in is available at the recipient's place he can open this file through the Adobe DRM server according to the above described authentification method.

DRM protected documents are encrypted and in contrary to password protected files, can **exclusively** be read under **complete control of the DRM server**.

::: The Components

The complete solution consists of the **DRM software** and the **SEAL Systems interface** to the administration system. Sometimes extensions for the SEAL Systems output management system are necessary in order to process already protected files.

The integration package is available for **DPF based solutions** and for **PLOSSYS**.

The following application methods can be performed:

- **Protection** of PDF files before sending as email or preparation in a **Web portal** (protection of copies outside the DMS)
- **Protection** of PDF files before viewing from **SAP** (prevention of unprotected local copies)
- **Evaluation** of protected PDF files before **check-in** into **SAP** (ensuring internal processing)
- **Cancellation** of protection for output processing (for example for print or conversion)

Enterprise Digital Rights Management

Functions

Personal and document-oriented release:

Protection – Protects a PDF file with predefined profile

The PDF file is encrypted with Adobe Livecycle ES Rights Management. Afterwards this file can only be processed with Adobe products by authorized people.

- Store
- Print
- Copy contents
- Change
- Sign
- Comment
- Offline
- Validity

Evaluation – Checks, whether a PDF is protected with Digital Rights Management

The PDF file is evaluated for finding any protection mechanisms working according Digital Rights Management. Protected files cannot be processed with SEAL Systems products.

Protection cancellation – Removes the protection of a PDF file

The PDF file is decrypted through Adobe Livecycle ES Rights Management and can then be processed with SEAL Systems products, for example print management. The cancellation of the protection is only possible with an Adobe Livecycle ES Rights Management Account, which has the necessary rights.

Enterprise Digital Rights Management

Licensing

The licensing of the Digital Rights Management system is handled by the manufacturer. We help you to find the best fitting licensing techniques.

The licensing of the interface module into your environment is separately charged for each server of the corresponding SEAL Systems software.

Benefit

Enterprise Digital Rights Management with SEAL Systems offers solutions for secure handling of documents also outside the server-based file storage system (DMS).

Flexible design of logging and audits according to legal regulations and instructions.

A version control of the distributed documents for validity period or granting new authorization rights with link to the new version is possible.

The access to documents for persons, who have left the enterprise can be deleted afterwards.

Related products and options

DRM is useful for these distribution methods:

- **PR-WP**
  Document distribution to Web portal
- **PR-EOUT**
  Electronic distribution via email or exchange directory
- **Q-CD**
  PLOSSYS output on CD
- **Q-EP**
  PLOSSYS output to file directory
- **PU-DO**
  Output to CD/DVD structure
- **PU-DROB**
  Output to disc publishing system
- **RM-A2G**
  Record2Go, Offline record from SAP Folders Management

Uwe Wächter and Debra Garls are specialist for your questions concerning:

Conversion and PDF processing

Europe/Asia/Australia
Dr. Uwe Wächter
Tel +49 6154 637 372
uwe.waechter@sealsystems.de

USA/Canada/Americas
Debra Garls
Tel +1 774 200 0933
debra.garls@sealsystems.com

SEALSYSTEMS
THE DIGITAL PAPER FACTORY

E-Mail: info@sealsystems.de
Web: www.sealsystems.de

Convert & Publish
Solutions by SEAL Systems

We would be happy to answer all of your questions around conversion, output and distribution of documents in your company.

Status: January 31, 2019. V516-140911-0-en.