SEALSYSTEMS
THE DIGITAL PAPER FACTORY

Digital Paper: Secure Access

PDF and Security – More important than ever

Digital paper offers a number of functions and is an important part of daily business processes. Therefore the security aspect is an essential part. This article considers this regarding PDF.

The **access** to documents, which are housed within a document management system, is managed by the DMS system itself. Only authorized users can access documents, released for a specific process. Furthermore, these authorization rights can be changed at any time.

For documents outside the DMS, this control is not available. Therefore every company wants to avoid shadow archives. But when working with other companies (customers or suppliers), some documents have to be provided **outside** of the DMS, and these are dangerous cases because viewer-ship cannot be restricted and modifications cannot be controlled. In this case, there is some danger, because nobody knows exactly which ways the documents go.

PDF files can be duplicated via **copy** functions from the secure DMS areas by authorized users. Those users can then copy these files to a local disk and distribute them without any control. While this method is sometimes desirable for sales and procurement business processes, there may be proprietary company information within these files.

Therefore a method is necessary to restrict access to read and process these files to only **authorized recipients**.

Stamps and Signatures

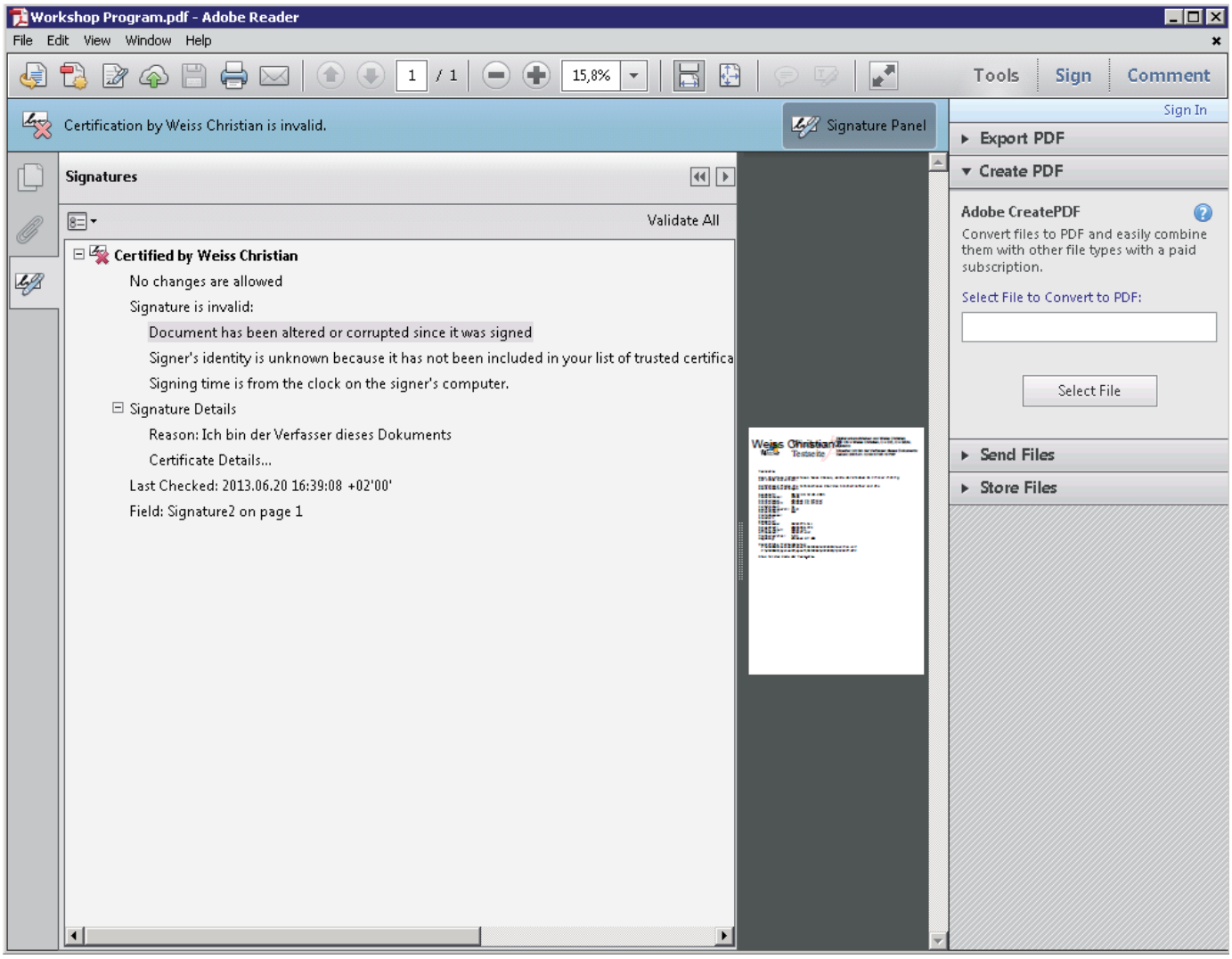
Stamps and signature pages are proven methods for **process control**. A **stamp** characterizes the **status** of the document and the **signature page** shows the actual **process state**. Both methods are called electronic signatures and they have serious disadvantages for security because each can be changed, after the fact, with a PDF editor. As well as the stamp, also the stamped document can be **changed** with a PDF editor. The same applies to the signature page.

These security gaps can be closed with **digital signatures**. In contrast to the electronic signature, the digital signature is a **cryptographic** technique. A digital signature enables the evaluation of the original and the relation to the message can be **checked** by every user. Changes made afterwards can be reliably recognized.

At the transition from digital to analog paper, the result of the evaluation can be printed as **stamp information** on the page.

Digital signatures are PDF/A compatible

SEAL Systems offers products and solutions for signing PDF documents and for evaluation of the signature in connection with **conversion processes**.



Result of evaluation as a warning message realized as a red lined stamp

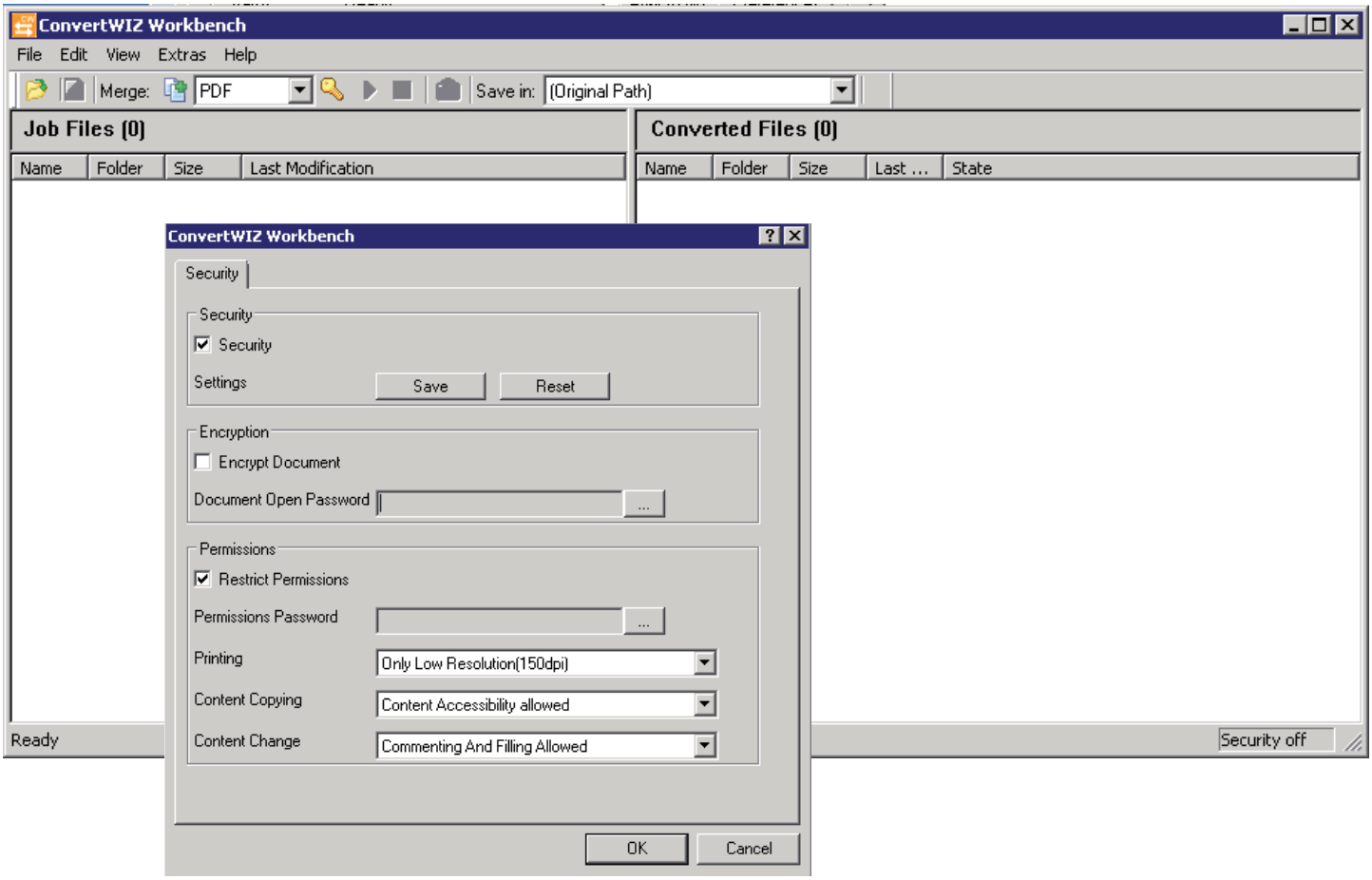
Password Protection – What is allowed?

With password protection, the **allowed functions** for document processing can be set:

- Open
- Print
- Change
- Access to contents

However the password protection is **not safe** with the exception of opening the document. Password protection **cannot be used with PDF/A** files. This means, that a password protected PDF file does not meet the PDF/A requirements.

Password protection functionality is a standard piece of the conversion solution from SEAL Systems.



Configuration of security settings

Digital Rights Management – Who can do what?

The solutions for DRM (Digital Rights Management) offer the required document protection for use in a multi-user environment. These solutions provide **overall control of data exchange** at every stage of a project, from product development in cooperation with suppliers to creation of work orders to maintenance activities.

Within DRM the access control is managed by a **central server**. The single rights (read, print, extract, store, etc.) and the period of validity are centrally managed, not within in the document. The usage of DRM is especially important when an enterprise releases documents out of the control of the company's document management system. If a user wants to read such a file, Acrobat Reader will register encryption and prompt the reader for **user identification** and **password**. The credentials are compared with the DRM server's registration. The DRM server transfers the allowed functions for this reader to Acrobat Reader. Without authentification, a local copy of the PDF file is not usable – it is still **encrypted**.

DRM protected documents are encrypted and can only be read with control of the DRM server, as opposed to documents that are only password-protected. DRM and PDF/A are not compatible.

SEAL Systems offers products and solutions for protection of documents with functions of Adobe LiveCycle Rights Management.

Impose the highest security with Digital Rights Management

Do you have further questions?

SEAL Systems

www.sealsystems.com
info@sealsystems.com

Convert & Publish
Solutions by SEAL Systems