SEALSYSTEMS
THE DIGITAL PAPER FACTORY

Digitales Papier: sicherer Zugriff

PDF und Sicherheit – wichtiger denn je

Digitales Papier bietet eine Vielzahl an Funktionen und ist aus den Geschäftsprozessen nicht mehr wegzudenken. Umso wichtiger ist das Thema Sicherheit. Dieser Artikel betrachtet diesen Aspekt am Beispiel PDF.

Befinden sich Dokumente unter der Verwaltung eines Dokumentenmanagement-Systems, dann wird über das DMS auch der **Zugriff** gesteuert. Nur zulässige Anwender können die für einen Vorgang freigegebenen Dokumente nutzen. Diese Zugriffsrechte können jederzeit geändert werden.

Befinden sich Dokumente außerhalb des DMS, dann sieht die Sache anders aus. Daher werden Firmen Schattenarchive immer vermeiden. In der Zusammenarbeit mit anderen Firmen (Kunden oder Zulieferer) müssen aber Dokumente **außerhalb** des eigenen DMS zur Verfügung gestellt werden. Dazu kommt in diesem Falle noch die Gefahr, dass man nie wissen kann, welche Wege die Dokumente noch gehen.

PDF-Dateien können zum Beispiel durch autorisierte Mitarbeiter aus dem gesicherten Bereich des DMS heraus **kopiert** werden. Jetzt kann der Anwender diese Dateien auf eine lokale Platte speichern und beliebig weiterreichen. Diese Vorgehensweise ist für einzelne Geschäftsprozesse des Einkaufs und Vertriebs so gewollt. Das Knowhow des Unternehmens steckt aber in diesen Dateien.

Gesucht wird also eine Methode, die PDF-Dateien so zu behandeln, dass sie nur vom **gewollten Empfänger** verarbeitet werden kann.

Stempel und Signaturen

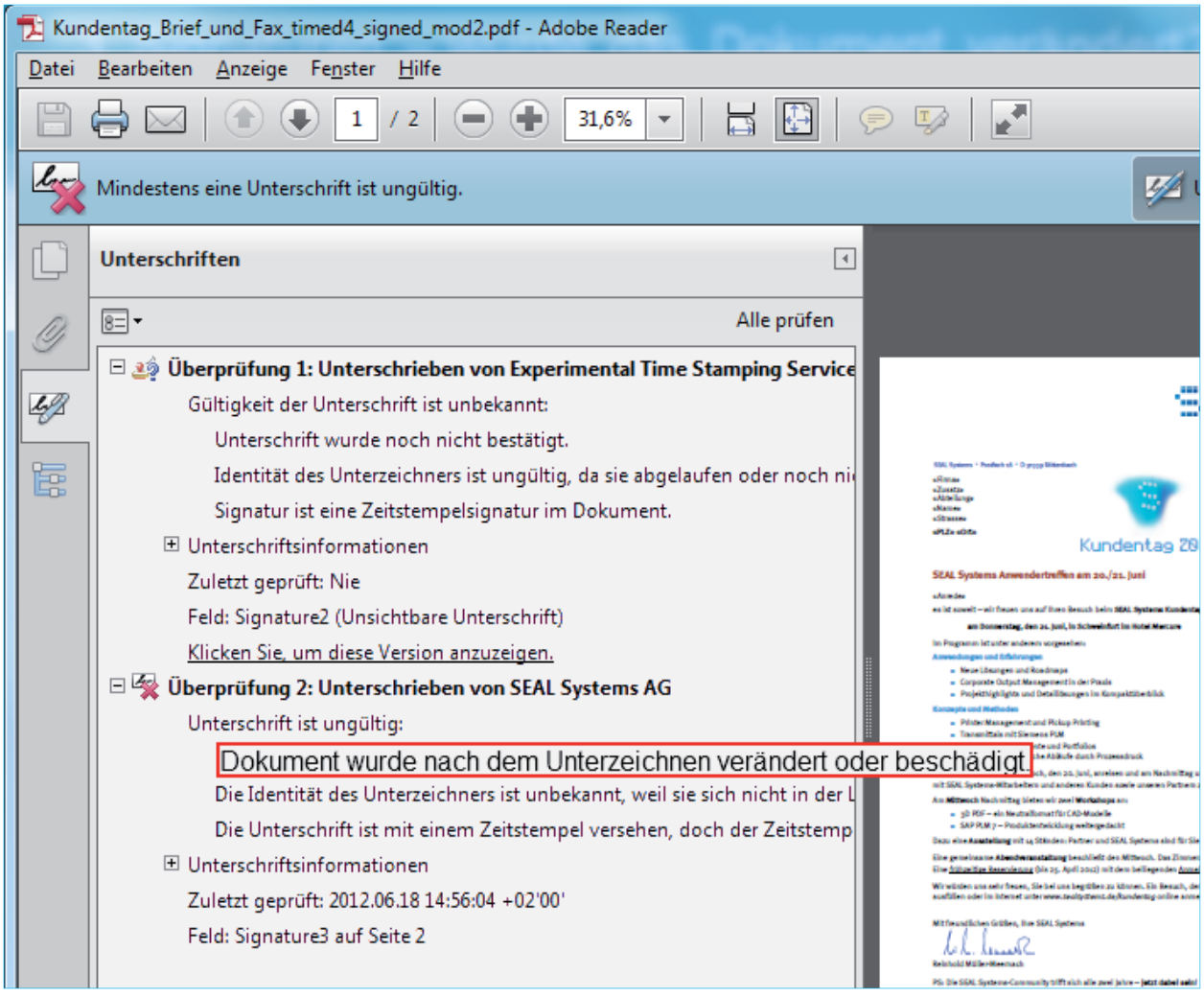
Stempeln und Signaturseiten sind bewährte Verfahren für die **Prozesssteuerung**. Mit dem **Stempel** wird der **Status** der Dokumente gekennzeichnet, die **Signaturseite** zeigt den aktuellen **Bearbeitungsstand**. Beide Verfahren können als elektronische Signaturen bezeichnet werden, haben aber gravierende Sicherheitsnachteile. Sowohl der Stempel als auch das gestempelte Dokument können mit einem PDF Editor **geändert** werden. Das gleiche gilt auch für die Signaturseite.

Diese Sicherheitslücken können mit einer **digitalen Signatur** geschlossen werden. Im Gegensatz zur elektronischen Signatur ist die digitale Signatur ein **kryptografisches** Verfahren. Eine digitale Signatur ermöglicht, dass ihre Urheberschaft und Zugehörigkeit zur Nachricht durch jeden **geprüft** werden kann. Nachträgliche Änderungen können zuverlässig erkannt werden.

Beim Übergang vom digitalen zum analogen Papier, also zum Beispiel beim Drucken, kann dann wieder das Ergebnis der Prüfung als **Stempelinformation** aufgedruckt werden.

Digitale Signaturen sind PDF/A-kompatibel.

SEAL Systems bietet Produkte und Lösungen sowohl für das Signieren von PDF-Dokumenten als auch für die Validierung der Signatur im Rahmen der **Konvertierungsprozesse**.



Prüfungergebnis als Warnmeldung in Form eines Stempels

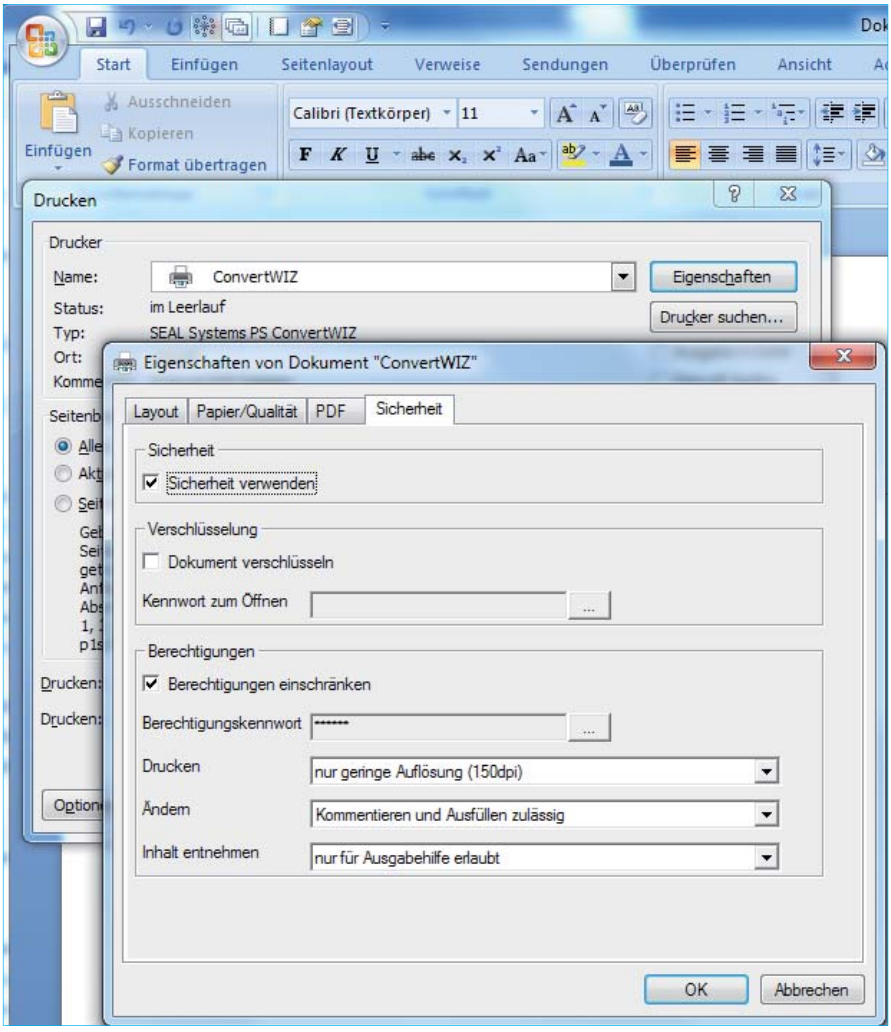
Kennwortschutz – was ist erlaubt?

Mit dem Kennwortschutz können die **erlaubten Funktionen** für die Dokumentenbearbeitung festgelegt werden:

- Öffnen
- Drucken
- Ändern
- Zugriff auf Inhalte

Der Kennwortschutz ist allerdings mit Ausnahme des Schutzes gegen Öffnen **nicht sicher** und kann umgangen werden. Weiterhin schließen sich Kennwortschutz und PDF/A gegenseitig aus, das heißt, ein geschütztes PDF kann **nicht PDF/A-kompatibel** sein.

Die Erstellung eines Kennwortschutzes ist eine Standardfunktionalität der Konvertierungslösungen von SEAL Systems.



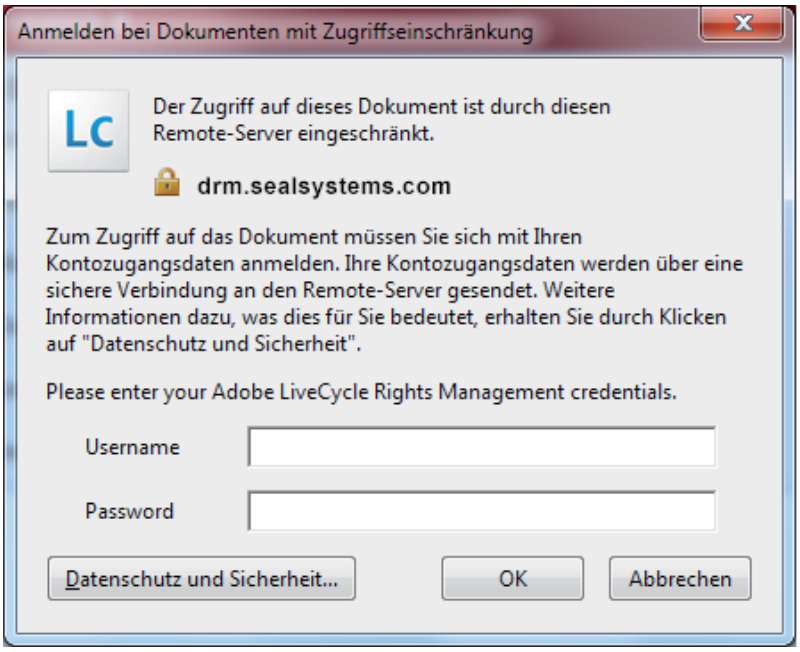
Konfiguration der Sicherheitseinstellungen

Digital Rights Management – wer darf was?

Die Lösungen für DRM (Digital Rights Management; digitale Rechteverwaltung) bieten den für eine Zusammenarbeit notwendigen Schutz. Sie ermöglichen die **umfassende Kontrolle** über den **Datenaustausch** in jeder Phase eines Projekts – von der Produktentwicklung über die Zusammenarbeit mit Zulieferern und die Erstellung von Arbeitsanweisungen bis hin zum Kundendienst.

Beim DRM erfolgt die Zugriffskontrolle durch einen **zentralen Server**. Die einzelnen Rechte (Lesen, Drucken, Extrahieren, Speichern etc.) und der Gültigkeitszeitraum werden zentral gepflegt und sind nicht im Dokument gespeichert. Die Verwendung des DRM ist somit insbesondere dann sinnvoll, wenn ein Unternehmen Dokumente aus der Zugriffskontrolle des eigenen Dokumentenmanagements heraus gibt.

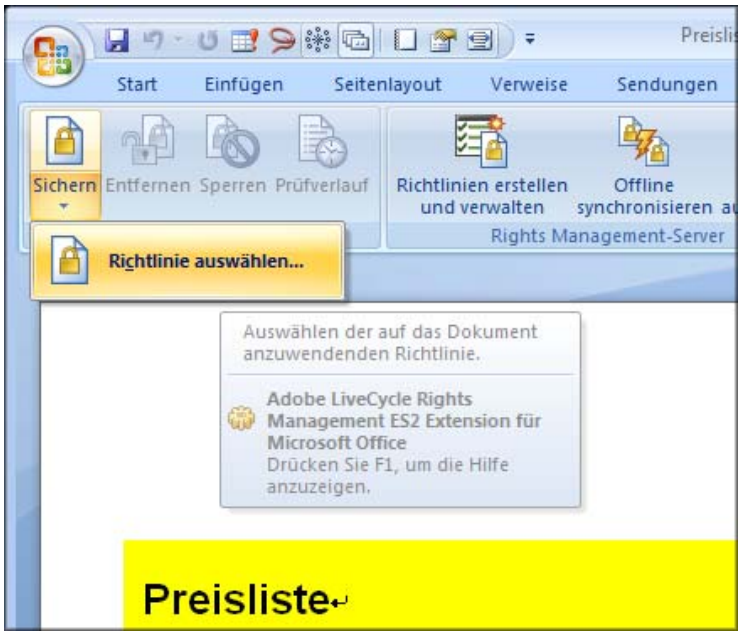
Will ein Anwender jetzt eine solche Datei betrachten, so wird der Acrobat Reader zunächst die Verschlüsselung bemerken. Er fragt den Anwender nach seiner **Userkennung** und **Passwort**. Diese Daten werden mit dem DRM Server abgeglichen. Dieser übermittelt dem Reader die für diese Datei und diesen Anwender erlaubten Funktionen.



Höchste Sicherheit mit Digital Rights Management

Eine lokale Kopie der PDF-Datei ist wertlos - sie ist immer noch **verschlüsselt**.

Adobe bietet aber nicht nur einen wirksamen Dokumentschutz für PDF an. Plugins für die Microsoft Office Suite erlaubt auch die Verschlüsselung von Office Dokumenten. Die so geschützten



Office Dateien werden dann verschlüsselt an den Empfänger verschickt. Ist das notwendige Plugin beim Empfänger vorhanden, so kann dieser die Datei nach beschriebener Authentifi zierung durch den Adobe DRM Server öff nen

DRM-geschützte Dokumente sind verschlüsselt und können im Gegensatz zu Kennwort-geschützten Dokumenten ausschließlich unter Kontrolle des DRM-Servers gelesen werden. DRM und PDF/A schließen sich dadurch gegenseitig aus.

SEAL Systems bietet Produkte und Lösungen zum Schutz von Dokumenten mithilfe des Adobe LiveCycle Rights Management.

Haben Sie Fragen?

SEAL Systems AG

www.sealsystems.de
info@sealsystems.de
+49 - (0)9195 - 9260

Convert & Publish
Solutions by SEAL Systems