Digitale Signatur mit PDF

Wie funktioniert eine Digitale Signatur mit PDF?

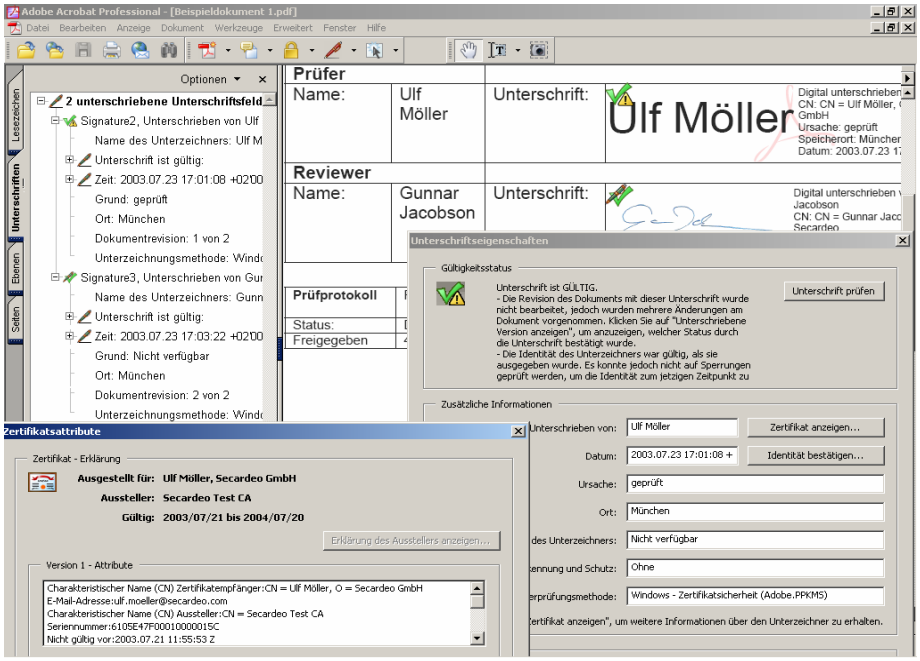
Digitale Signaturen basieren auf asymmetrischen kryptographischen Verfahren und digitalen Zertifikaten, die von einem Trustcenter ausgestellt werden. Damit kann die Unversehrtheit und Echtheit digitaler Dokumente zweifelsfrei geprüft werden und es ist nachvollziehbar, wer ein Dokument unterzeichnet hat.
Mit Adobe Acrobat® ab Version 6 können digitale Signaturen auf Basis Digitaler Zertifikate für ein Dokument in PDF (Portable Document Format) erzeugt und geprüft werden. Einem PDF-Dokument können beliebig viele digitale Signaturen hinzugefügt werden, wobei das Dokument jeweils automatisch als neue Dokumentversion gespeichert wird.

Was sind die Vorteile?

Die Ablösung von unterschriftsrelevanten Papiervorgängen durch elektronische Workflows mit digital signierten PDF-Dokumente wird motiviert durch die damit verbundene Zeiteinsparung, Kostenreduktion, erhöhte Sicherheit sowie in zunehmendem Maße die Erfüllung von Behördenvorgaben.
PDF eignet sich hervorragend für die Verwendung digitaler Signaturen für verbindliche Vorgänge. Die zuverlässige Anzeige des zu signierenden Inhaltes (What You See Is What You Sign), die Eignung als Archivformat, der immensen Verbreitungsgrad und der kostenlos verfügbare Adobe Reader® sind einige der hervorstechenden Merkmale.

Was leistet Adobe Acrobat?

Seit Acrobat® Version 4 ist die Erzeugung und Prüfung digitaler Signaturen mittels so genannter Self-Sign Zertifikate möglich. Acrobat® ab Version 6 unterstützt auch vertrauenswürdige digitale Zertifikate, die beispielsweise von einer Unternehmens-PKI (Public Key Infrastruktur) oder einem öffentlichen Trust-center ausgestellt werden. Über das von Windows bereitgestellte Crypto-API können Soft-Keys, Smartcards oder USB-Tokens für die Signierung genutzt werden. Acrobat bietet dafür unter Windows zwei grundsätzliche Alternativen für die Verwaltung von PKI-Zertifikaten an: Eine interne Zertifikatsliste, die ausschließlich Acrobat verwendet sowie den Windows Zertifikatsspeicher, der auch von anderen Anwendungen genutzt wird.

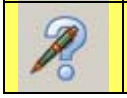


Digitale Signaturen können in

- bereits vorhandenen Signaturfeldern,
- neu anzulegenden Signaturfeldern oder
- unsichtbar platziert werden.

Ein Signaturfeld enthält die durch den Signierenden für das Erscheinungsbild ausgewählten Text- und Grafikelemente sowie das Statussymbol für die dort geleistete gültige Signatur. Durch einfaches Anklicken eines Signaturfeldes öffnet sich der Signaturdialog zur Anbringung einer neuen beziehungsweise Prüfung einer vorhandenen Signatur. Außerdem bietet Acrobat die Möglichkeit, alle im Dokument enthaltenen Unterschriften, also auch die „unsichtbaren Signaturen“ in einer Unterschriften-Palette anzuzeigen.

Bei PDF ist es auch möglich, dass nach dem Signieren Änderungen an einem Dokument gemacht werden. Die bis dann geleisteten Signaturen bleiben in dem Fall gültig und der Benutzer kann sich die signierte Version des Dokuments durch Anklicken eines speziellen Buttons anzeigen lassen. Für die Visualisierung der verschiedenen Prüfzustände einer Signatur werden in Acrobat unterschiedliche Status-symbole verwendet, wobei der grüne Haken für eine gültige und das rote Kreuz für eine ungültige Signatur die wohl wichtigsten sind. Neben den Signaturen der Dokumentanwender bietet Acrobat die Verwendung einer so genannten Zertifizierungs-unterschrift an, die dazu dient, die Authentizität des Ursprungsdokuments zu sichern.

	Dokument als gültig ZERTIFIZIERT.
	Unterschrift ist GÜLTIG. Das Dokument wurde nach dem Unterschreiben nicht mehr geändert.
	Unterschrift ist GÜLTIG. Nach dem Unterschreiben wurden Änderungen am Dokument vorgenommen.
	Gültigkeit der Unterschrift UNBEKANNT. Dokument wurde nach dem Unterschreiben nicht mehr geändert. / Dokument wurde zertifiziert, Gültigkeit UNBEKANNT.
	Gültigkeit der Unterschrift UNBEKANNT. Nach dem Unterschreiben wurden Änderungen am Dokument vorgenommen.
	Unterschrift ist UNGÜLTIG. / Dokumentzertifizierung ist UNGÜLTIG.
	Unterschrift wurde noch nicht geprüft.

Die vollständige Unterstützung von digitalen Signaturen und Zertifizierungsunterschriften ist nur mit Acrobat Standard oder Professional möglich. Der kostenlose Adobe Reader unterstützt von Haus aus die Verifikation digitaler Signaturen. Signiert werden können PDFs mit dem Reader dann, wenn die an das Dokument gebundenen Rechte zur Signaturanbringung durch einen lizenzpflichtigen Adobe LiveCycle Reader Extensions Server frei geschaltet wurden. Dieser Mechanismus basiert ebenfalls auf der Prüfung digitaler Signaturen des Reader Extensions Server durch den Adobe Reader.

Wie können wir Sie unterstützen?

Zur Einführung der Digitalen Signatur sind technische, organisatorische und gegebenenfalls auch rechtliche Fragestellungen zu lösen. SECARDEO hilft Ihnen dabei durch

- Inhouse-Seminare und Workshops,
- Anforderungsanalysen und Lösungskonzepte,
- Produkt- und Serviceauswahl,
- Integration der PDF-Signatur in bestehende Anwendungen und Systeme,
- Management des Signatur-Workflows mittels Signaturverifikationsserver
- Pilotierung und Unterstützung beim Rollout.

Benötigen Sie weitere Informationen?

Wenn Sie weitere Informationen wünschen, wenden Sie sich bitte an

Dr. Gunnar Jacobson, Secardeo GmbH
Betastr. 9a, 85774 Unterföhring
Tel. 089/18935890

Gunnar Jacobson
Muenchen
2005.05.13 10:22:59 +02'00'