

PKI-Infrastrukturen für die Signierung von PDF-Dokumenten

Bei einer elektronischen Signatur handelt es sich um „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentisierung dienen“. So definiert das deutsche Signaturgesetz in seiner Fassung vom 16. Mai 2001 den Begriff „elektronische Signaturen“ (§2 Nr. 1 SigG 2001). Damit kommt zum Ausdruck, dass eine elektronische Signatur den zu signierenden Daten nachträglich hinzugefügt wird und eindeutige Rückschlüsse auf die Identität des Unterzeichnenden liefert. Das Signaturgesetz unterscheidet unterschiedlich starke Signaturen, deren „Stärke“ sich unter Anderem an Hand der Zuverlässigkeit bestimmt, mit der die Signatur einer natürlichen Person zugeordnet und nachträgliche Änderungen eines signierten Dokuments erkannt werden können („einfache“, fortgeschrittene und qualifizierte elektronische Signaturen).

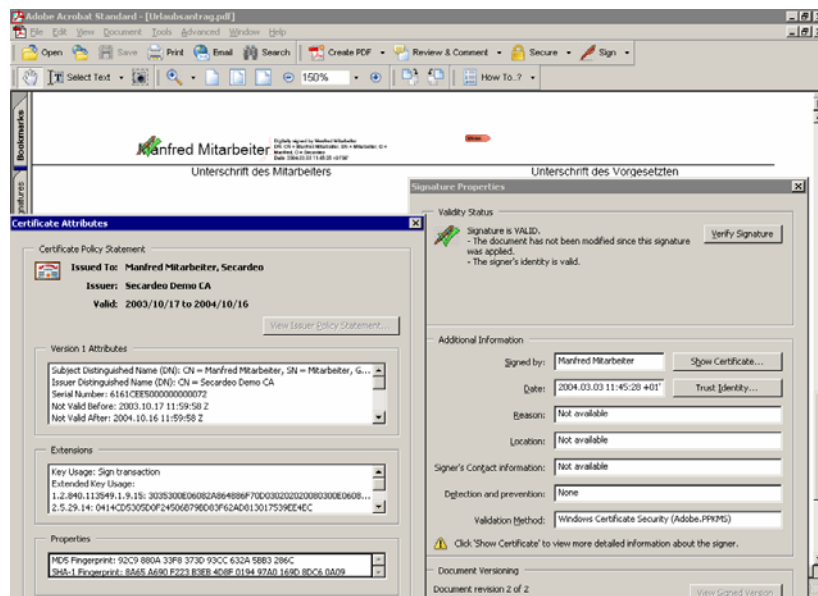


Abbildung 1: PDF-Dokument mit einem ausgefüllten und einem leeren Signaturfeld. Dialog zur Anzeige des Gültigkeitsstatus der Signatur und der Zertifikats-Attribute

Diese Anforderungen des Signaturgesetzes werden durch eine Public Key Infrastruktur (PKI) mit asymmetrischer Verschlüsselung erfüllt. Dabei wird einer Person ein komplementäres Schlüsselpaar zugeteilt. Komplementär bedeutet, dass Daten, die mit jeweils einem der beiden Schlüssel des Schlüsselpaars verschlüsselt wurden, ausschließlich mit dem jeweils anderen Schlüssel entschlüsselt werden können. Einen der beiden Schlüssel

hält der Benutzer geheim („geheimer“ oder „privater“ Schlüssel), der andere wird veröffentlicht („öffentlicher“

Schlüssel). Der private Schlüssel kann auf der Festplatte des Computers abgelegt sein (Softkey), oder man verwendet Signaturhardware wie z.B. eine Smartcard mit Crypto-Chip (Hardkey). Der Schlüssel wird dann auf der Smartcard erzeugt und kann per Software unter keinen Umständen ausgelesen werden. Alle Ver- und Entschlüsselungsvorgänge werden auf der Smartcard ausgeführt, nachdem der Benutzer seine PIN eingegeben hat. Diese Variante ist besonders sicher. Für qualifizierte elektronische Signaturen laut SigG ist der Einsatz von Crypto-Hardware zwingend vorgeschrieben.

Bei der Signierung verschlüsselt der Unterzeichnende einen Auszug aus dem Dokument (Hashwert) mit seinem privaten Schlüssel. Die Prüfung der Signatur geschieht durch Entschlüsselung des Hashwerts mit dem öffentlichen Schlüssel. Die Zuordnung eines öffentlichen Schlüssels zu einer natürlichen Person wird mittels elektronischer Zertifikate nach dem X.509-Standard bestätigt. Elektronische Zertifikate werden personenbezogen nach der Erfassung und Prüfung der Identität einer natürlichen Person durch einen „vertrauenswürdigen Dritten“ (Trustcenter) ausgestellt und durch dessen elektronische Signatur beglaubigt. Die Prüfung der Identität wird durch eine Registrierungsstelle vorgenommen, bei der sich der Benutzer z.B. mit einem Personalausweis oder im Fall einer Firmen-PKI mit seinem Mitarbeiterausweis identifiziert.

Ein Zertifikat ist für einen Zeitraum von einem bis maximal fünf (§14 SigV 2001) Jahren gültig. Für den Fall, dass ein Benutzer seine Smartcard verliert oder sein privater Schlüssel kompromittiert wird, kann sein Zertifikat gesperrt werden. Jedes Trustcenter veröffentlicht

eine Zertifikatssperrliste (CRL). Auf einer CRL werden alle Zertifikate eingetragen, die vor Ablauf ihrer Gültigkeit gesperrt wurden.

Seitens der Signatur-Anwendung darf es nicht möglich sein, Textstellen oder Zahlen so zu formatieren, dass dem Unterzeichnenden andere Daten angezeigt werden, als diejenigen, die er tatsächlich signiert („What You See is What You Sign“). Das Adobe PDF-Format eignet sich hervorragend als Austauschformat für signierte Dokumente und zu deren Archivierung, da PDF-Dokumente genau diese Eigenschaft erfüllen. Ferner kann nahezu jeder Benutzer mit Hilfe des kostenlosen Adobe Reader PDF-Dokumente zwar lesen und seit Version 6 auch signieren. PDF-Dokumente könnte man somit als „elektronisches Papier“ bezeichnen. Aus diesem Grund werden bereits heute in vielen formularbasierten Prozessabläufen PDF-Dokumente verwendet, meistens jedoch ohne elektronische Signatur.

Um ein PDF-Formular zu unterschreiben, klickt der Benutzer auf das dafür vorgesehene Unterschriftsfeld. Er wird dann durch einen Dialog geführt, wo er den Ort und den Grund der Unterschrift eingeben kann. Zudem wird er bei Verwendung einer Smartcard aufgefordert, seine PIN einzugeben. Bei Verwendung eines Softkey muss der Benutzer, abhängig von den Sicherheitseinstellungen, den Zugriff auf den Schlüssel bestätigen oder sein Passwort eingeben. Da für die Erstellung einer Signatur mehrere Schritte erforderlich sind, ist das Unterschreiben eines Dokuments ein bewusster Vorgang und kann nicht ohne Wissen und Zutun des Benutzers erfolgen.

Im Unterschriftsfeld werden nach dem Signieren das Datum, der Name des Unterzeichners und weitere Informationen angezeigt. Eine gültige Signatur ist durch ein grünes Häkchen zu erkennen, bei einer ungültigen wird ein rotes Warnsymbol angezeigt. Um die digitale Signatur auch grafisch sichtbar zu machen, kann zusätzlich eine eingescannte Unterschrift als Bild enthalten sein.

Wenn ein Benutzer ein Dokument unterschreiben will, das noch kein Unterschriftsfeld enthält, kann er

Secardeo GmbH 
Unterföhring



Digital unterschrieben von Gunnar
Jacobson
Speicherort: Unterföhring
Datum: 2004.04.21 15:15:29 +02'00'

an einer geeigneten Stelle ein Unterschriftsfeld einfü-

Abbildung 2: PDF-Signatur mit eingescannter Unterschrift

gen, oder er kann das Dokument „unsichtbar“ signieren. Informationen über unsichtbare Unterschriften kann man im Acrobat über die Karteikarte „Unterschriften“ abrufen. Unsichtbare Signaturen unterscheiden sich von sichtbaren dadurch, dass sie in der Dokumentanzeige nicht zu sehen sind, sie sind aber genauso sicher.

Das Signieren von Dokumenten ist normalerweise nur mit der Acrobat-Vollversion möglich. PDF-Formulare können aber mit kostenpflichtiger Software von Adobe speziell freigeschaltet werden und lassen sich dann auch mit dem Adobe Reader unterschreiben. Zum Prüfen vorhandener Unterschriften reicht der kostenlose Adobe Reader in jedem Fall aus.

Beim Unterschreiben wird eine digitale Signatur nach dem Standard PKCS#7 erzeugt. Dabei wird üblicherweise der als sehr sicher geltende RSA-Algorithmus eingesetzt. Nachträgliche Änderungen an den signierten Daten führen automatisch dazu, dass die digitale Signatur ungültig wird, wodurch Fälschungsversuche entdeckt werden können. Damit dennoch erwünschte Änderungen an einem unterschriebenen Dokument möglich sind, bietet Acrobat die Möglichkeit, eine neue Version des Dokuments anzulegen, die beliebig geändert und auch erneut unterschrieben werden kann. Die ursprüngliche Unterschrift enthält dann den Hinweis, dass das Dokument nach dem Signieren geändert wurde.

Wer Unterschriften prüfen will, muss zuvor entscheiden, welchen Trustcentern er vertrauen möchte und muss deren Zertifikate („Root-Zertifikate“) installieren. Die vertrauenswürdigen Trustcenter können direkt im Acrobat verwaltet werden, es ist aber auch möglich, die Vertrauensstellungen aus dem Windows-Zertifikatsspeicher zu verwenden. Neben der manuellen Prüfung im Acrobat besteht auch die Möglichkeit, PDF-Dokumente serverbasiert zu verifizieren. Dadurch ist es möglich, den Status von Signaturen automatisiert zu überprüfen und beispielsweise zur Steuerung von formularbasierten Prozessen und zur Archivierung zu verwenden. Dies ist mit einem PDF-Verifikationsserver, wie beispielsweise PDFY der Secardeo GmbH, möglich. Dieser Server liest PDF-Dokumente über verschiedene Schnittstellen ein und erzeugt Prüfberichte im XML-Format, die automatisch weiterverarbeitet werden können. Neben der Prüfung auf kryptografische Korrektheit und Vertrauenswürdigkeit der Zertifikatsaussteller kann auch die Autorisierung der Unterzeichner geprüft werden. Für jedes Unterschriftsfeld können Berechtigte und deren Stellvertreter festgelegt werden, wodurch Policies zur Unterschriftsberechtigung serverbasiert umgesetzt werden können. PDFY erkennt auch, ob ein Dokument zwischen zwei Unterschriften geändert wurde, also ob beispielsweise zusätzliche Formularfelder ausgefüllt wurden.

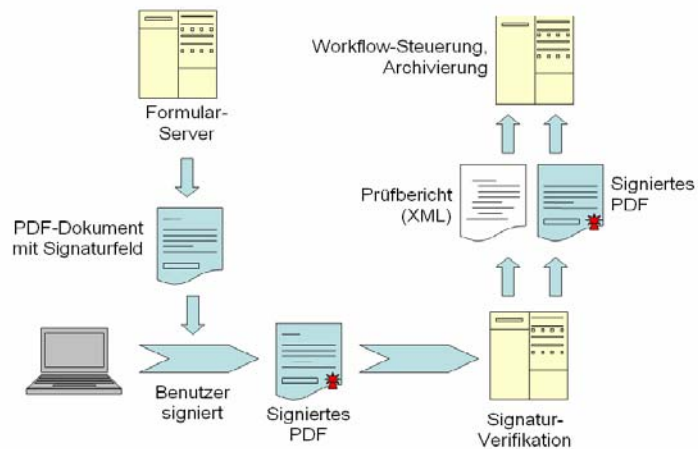


Abbildung 3: Schematische Darstellung eines Signatur-Workflows

und erzeugt Prüfberichte im XML-Format, die automatisch weiterverarbeitet werden können. Neben der Prüfung auf kryptografische Korrektheit und Vertrauenswürdigkeit der Zertifikatsaussteller kann auch die Autorisierung der Unterzeichner geprüft werden. Für jedes Unterschriftsfeld können Berechtigte und deren Stellvertreter festgelegt werden, wodurch Policies zur Unterschriftsberechtigung serverbasiert umgesetzt werden können. PDFY erkennt auch, ob ein Dokument zwischen zwei Unterschriften geändert wurde, also ob beispielsweise zusätzliche Formularfelder ausgefüllt wurden.

Wenn Prozesse aus rechtlichen Gründen eine Unterschrift verlangen, musste bisher immer eine Papierkopie handschriftlich unterzeichnet werden. Mit Hilfe elektronischer Signaturen und durch die Integration einer automatischen Signatur-Verifikation am Server können solche „Signatur-Workflows“ automatisiert und von Medienbrüchen befreit werden. Dadurch werden Prozessabläufe beschleunigt und Kosten eingespart. Durch die Verwendung von verbreiteten Standards wie z.B. PDF erreicht man breite Akzeptanz und hohe Interoperabilität.

Dipl.-Ing. Oliver Klinger, Dipl.-Inform. Ulf Möller