Die elektronische Signatur ist massentauglich

Prozesse mit Dokumenten effizienter gestalten / Rechtsgültige elektronische Signatur im PDF-Dokument möglich / Adobe Reader als Signatur-Client zertifiziert

von Peter Körner,
Senior Strategic Business Development Manager Enterprise, Adobe Systems GmbH

Von A wie Autokauf oder Arbeitsvertrag bis Z wie Zeugnis oder Zulassungspapiere: Wichtige Dokumente werden persönlich und vor allem per Hand unterschrieben. Sitzt der Ansprechpartner nicht direkt am Schreibtisch gegenüber, müssen sie erst ausgedruckt, dann per Post versandt, vom Empfänger unterschrieben, erneut eingetütet, zurückgeschickt und schließlich vom Aussteller bearbeitet und abgeheftet werden. Wie eine Studie von Gartner (2005) festgestellt hat, entfallen 30 bis 40 Prozent der Arbeitszeit in einem Unternehmen auf die manuelle Dokumentenverwaltung. Dabei lassen sich solche Prozesse erheblich verkürzen. Anwender können schnell, einfach und systemübergreifend von ihrem Rechner aus – sei es am Arbeitsplatz oder zu Hause – rechtsgültig unterschreiben. Die elektronische Signatur ist für Jedermann möglich.

Digitale Inhalte haben Konjunktur. Sowohl die Kommunikation mit elektronischen Daten als auch deren Dokumentation und Archivierung sind inzwischen etabliert und bestimmen unseren Alltag. Daraus ist ein Bedarf für eine Lösung entstanden, die diese Form des Austausches vor allen Widrigkeiten schützt. Elektronische Prozesse müssen nicht nur schneller und günstiger ablaufen, sondern auch absolut sicher. Das gilt gerade dann, wenn zusätzlich die elektronische Signatur den digitalen Dokumenten ihre Gültigkeit verleihen soll. Denn mit der Einführung des „elektronischen Fingerabdrucks“ als Massenanwendung treten bei Anwendern Fragen zum Schutz vor Betrug und Identitätsmissbrauch auf. Authentizität und Integrität von elektronischen Dokumenten müssen gewährleistet sein. Außerdem muss die Identität des Signierenden anhand der elektronischen Unterschrift verifizierbar, also überprüfbar sein. Hersteller und Gesetzgeber haben sich mit diesen Voraussetzungen ausführlich auseinandergesetzt und inzwischen den Weg für eine einsatzfähige Plattform geebnet.

Einsatzvarianten bei Behörde, Justiz und zu Hause

Interessant ist die Alternative zur handschriftlichen Unterschrift vor allem bei der Kommunikation mit Behörden, mit der Justiz oder im privaten Bereich. Wie eine Studie von Steria Mummert Consulting (2005) belegt, würden schon jetzt neun von zehn Bürgern gerne alle Behördengänge über das Internet erledigen. Das An- und Ummelden, die Beantragung von

Pass- und Ausweisdokumenten und die elektronische Steuererklärung stehen dabei ganz oben auf der Wunschliste der Bürger. Die Einsatzmöglichkeiten der digitalen Signatur reichen jedoch viel weiter: Angefangen mit der Unterschrift unter ein verbindliches Angebot für eine öffentliche Ausschreibung über eine vom Rechtsanwalt signierte Klage bis hin zu Bankkommunikation und Internetkäufen bei Anbietern wie eBay oder Amazon. Mit der rechtsgültigen elektronischen Signatur können außerdem elektronische Rechnungen empfangen und geprüft sowie weltweit rechtskonforme e-Anträge, Bestellungen und Erklärungen aufgegeben werden. Generell ist diese Form der Unterschrift überall dort angebracht, wo rechtsverbindliche Willenserklärungen sie erfordern.

Elektronische Signatur ist nicht gleich elektronische Signatur

Es gibt für das Unterschreiben in Bits und Bytes zwei verschiedene Ansätze: Die erste Variante lässt sich am Beispiel eines Paketdienstes veranschaulichen: Wer ein Päckchen bekommt, quittiert dem Mitarbeiter des Paketdienstes mit einem Spezialstift den Erhalt auf einem Signatur- bzw. Unterschriftenpad. Dabei werden verschiedene biometrische Merkmale erfasst wie der Druck, der beim Schreiben auf den Bildschirm ausgeübt wird, die Geschwindigkeit, mit der das Autogramm entsteht sowie Schreibpausen und Schreibrichtung. Das ermöglicht es, eine Vielzahl an Merkmalen abzuleiten, die sich auf dem Papier so nicht feststellen lassen. Die andere Möglichkeit hingegen ist wesentlich umfassender, denn es muss sich dabei nicht unbedingt um einen echten Schriftzug des eigenen Autogramms handeln. Auf Basis der technischen Ausstattung auf Empfänger- und Versenderseite lassen sich wichtige Sicherheitsfunktionen einhalten. Dazu gehören Elemente wie Signaturkarten, Chipkartenleser, Anwenderkomponenten, Funktionsbibliotheken, Trust Center und Schlüsselgeneratoren. Der Anwender selbst benötigt neben der entsprechende Karte ein Lesegerät und eine Software, die idealerweise alle Anwendungsgebiete der elektronischen Signatur abdeckt.

Wie funktioniert's?

Die elektronische Signatur basiert in der Regel auf asymmetrischen Kryptosystemen. Dabei werden ein öffentlicher und ein privater Schlüssel vergeben. Der öffentliche Schlüssel (public key) eines Unterzeichners macht es möglich, die Signatur zu überprüfen, die er mit seinem geheimen persönlichen Schlüssel (private key) erstellt hat. Um zu beweisen, dass der öffentliche Schlüssel wirklich dem Unterzeichner gehört, werden verschiedene Verfahren angewendet. Neben dem Standard S/MIME (Secure/Multipurpose Internet Mail Extension), der auf digitalen Zertifikaten von höheren Instanzen basiert, gibt es weitere Lösungen wie das Verfahren nach PGP (Pretty Good Privacy), das einem Netz von Freunden vertraut. In Letzterem werden die Identifikation einer Person und die Zuordnung der Schlüssel durch gegenseitige Beglaubigungen bestätigt – in einem so genannten Web of Trust.

Im Gegensatz dazu wird in zertifikatsbasierten Systemen jedem Benutzer ein digitales Zertifikat zugeordnet, in dem seine Identität und sein öffentlicher Schlüssel festgehalten werden. Dabei sind diese Zertifikate immer von einer ausgebenden Stelle und möglicherweise weiteren hierarchisch höher liegenden Instanzen beglaubigt. In der Praxis sieht das dann so aus: Ist beispielsweise ein wichtiges Dokument fertig gestellt, muss nur noch auf den Befehl „Signieren" geklickt werden. Es folgt die Aufforderung, den Unterschriftenschlüssel – über die SmartCard und den Kartenleser – einzugeben. Alles weitere übernimmt der Computer. Auf Empfängerseite erfolgt die Überprüfung ebenfalls automatisch über die Software des Rechners, der die Echtheit des öffentlichen Schlüssels anhand des Zertifikats überprüft. Generell lassen sich beliebige Dokumententypen signieren, die dann für fünf Jahre gültig sind. Die Signatur kann dabei getrennt von der Datei versandt werden oder eine Containerdatei mit beiden Dateien sein, was etwa für TIFF-Dateien sinnvoll ist. Eine andere Möglichkeit integriert die elektronische Unterschrift etwa bei PDF- oder XML-Formaten direkt in das zu signierende Dokument.

Rechtlicher Hintergrund geschaffen

In Deutschland wurde der elektronischen Signatur mit dem Signaturgesetz (SigG) von 1997 und der nachgeordneten Signaturverordnung (SigV) der Weg geebnet. Hinter den beiden juristischen Begriffen verbergen sich die Voraussetzungen für die rechtsgültige elektronische Signatur. Ein gültiges Zertifikat ist erste Bedingung, hinzu kommt die Forderung nach einer sicheren Signaturerstellungseinheit – also einem Chipkarten-Lesegerät inklusive geeigneter Verschlüsselungssoftware. TrustCenter fungieren dabei als übergeordnete Zertifizierungs-stellen, bei denen die Authentizität nachgefragt werden kann.

Beim Bundesamt für Sicherheit in der Informationstechnik (BSI) wird die Zertifizierung einzelner Komponenten in Auftrag gegeben. Beispiele für auf diesem Weg genehmigte Produkte sind etwa Signaturkarten (Smart Cards) von Telesec, Signtrust und DATEV, die von den Trustcentern verwaltet werden. Chipkartenleser gibt es beispielsweise von CardMan, Cherry oder CyberJack. Anwenderkomponenten hingegen wie eTrust Mail, e-Kurier oder SignTrustMail sind teilweise in anderen Lösungen integriert, haben allerdings meist einen eingeschränkten Funktionsumfang und sind bisher kaum verbreitet. Oftmals sind sie nur regional zertifiziert und daher für den weltweiten Einsatz nach dem übergeordneten Standard Common Criteria ungeeignet. Die Zertifikate selbst werden beim BSI aufbewahrt, während die zugelassenen Kryptoalgorithmen von der Regulierungsbehörde für Telekommunikation und Post (RegTP) genehmigt werden. Hier sind auch die Listen der einzelnen für die rechtsgültige digitale Signatur zugelassenen Produkte erhältlich.

Insellösungen prägten bisher das Bild

Trotz der vielfältigen Einsatzmöglichkeiten hat sich die elektronische Signatur bisher noch nicht durchgesetzt. Hauptgrund ist die fehlende systemübergreifende Hard- bzw. Software, die selten interoperabel, zudem auch nicht zertifiziert und damit für eine rechtsgültige digitale

Signatur ungeeignet ist. Bisher prägen Insellösungen das Bild. Für die sichere Kommunikation über das Internet gibt es bislang noch von jeder Bank oder Versicherung eine spezielle Lösung, die auf dem Rechner installiert werden muss. Damit können auch nur eigens darauf abgestimmte digitale Signaturen in einer Softwaremaske gelesen und bearbeitet werden. Möglicherweise ist zusätzlich die passende Signaturkarte vonnöten, die nur in dem originären Lesegerät eines bestimmten Herstellers funktioniert. Die Bedienung dieser Programme muss dann jedes Mal erst von Neuem erlernt werden und die Umstellung von papierbasierten auf digitale Workflows kann den Prozess der Dokumentenverwaltung zusätzlich verkomplizieren. Am einfachsten wäre es also, so fordern viele Anwender, wenn Papierformular und elektronisches Formular gleich aussehen würden.

Adobe Reader und Acrobat als Königsweg der elektronischen Signatur

Diesen Herausforderungen ist Adobe Systems begegnet und hat beim BSI nach Common Criteria 2.1 den Adobe Reader 7.0 und Adobe Acrobat 7.0 als Komponenten eines elektronischen Signaturprozesses zertifizieren lassen. Das universelle PDF-Format als Basis soll es jedem Nutzer ermöglichen, verlässliche systemunabhängige PDF-Dateien zu generieren, diese zu lesen, zu bearbeiten und natürlich rechtsgültig zu signieren. Um eine nahtlose Integration mit anderen technischen Applikationen zu gewährleisten und die unterschiedlichsten Transaktionen ausführen zu können, werden praktisch alle gängigen Signaturkarten unterstützt, Zeitstempel angefertigt und Attributzertifikate erstellt.

Seit November 2005 ist der Adobe Reader als Komponente elektronischer Signaturprozesse zertifiziert. Damit ist er als erster Standard-Client, der bereits auf nahezu allen Computern verfügbar ist, für rechtsgültige elektronische Signaturen einsetzbar. Allein in den letzten beiden Jahren wurden über eine halbe Milliarde Exemplare des kostenlosen Adobe Reader verteilt und dienen als Grundlage zahlreicher Anwendungen. Darüber hinaus werden nach der ISO-Norm PDF/A gesicherte Dokumente auch den Anforderungen für die Langzeit-Archivierbarkeit digitaler Daten gerecht.

eCard-Strategie der Bundesregierung

Auch die Bundesregierung ist vom Potential der elektronischen Signatur so überzeugt, dass sie diese mit ihrer eCard-Initiative unterstützt. Dabei sollen verschiedene Chipkarten wie die elektronische Gesundheitskarte oder der digitale Personalausweis mit der Option ausgerüstet werden, qualifiziert elektronisch zu unterschreiben. Der neue biometrische Reisepass (ePass) wird seit November 2005 zum Preis von 59 Euro ausgegeben, ein frontal aufgenommenes Digitalbild genügt dafür. Ziel zahlreicher Initiativen des Bundesministeriums für Wirtschaft und Arbeit ist es, Signaturkarten möglichst schnell und aufeinander abgestimmt universell einsetzbar zu machen, ohne dass spezielle Komponenten mit anderen Anwendungen kollidieren. Der Wirtschaft wird dabei die Herstellung der Karten, der Zertifikate und der Zertifizierungsinfrastruktur (u.a. Trust Center) überlassen. Auch Banken haben sich schon in den Prozess eingeklinkt und werden bei der Umstellung von Magnetstreifen-Karten auf Chipkarten die neue Funktion der elektronischen Signatur integrieren.

Einsparungen versus Kosten

Viele Banken übernehmen schon heute die Kosten für Karte, Lesegerät und Software. Zusätzlich wird bald in allen Rechnern serienmäßig ein Kartenlesegerät enthalten sein, während Multifunktionskarten verschiedene Elemente der Chipkarten vereinen. Mit der Zertifizierung des Adobe Reader steht zudem eine kostenlose universelle Software zur Verfügung. Komplettpakete mit personalisierter Smart Card, Zertifikatsgebühren, Software und Kartenlesegerät gibt es im Handel für ca. 150 Euro.

Massenanwendung vor dem Durchbruch

Fasst man die verschiedenen Ansätze für die digitale Signatur zusammen, ist inzwischen bereits ein großes Stück des Weges hin zur Massenanwendung bewältigt: Die gesetzliche Basis ist geschaffen. Die notwendige Technik ist entwickelt, bezahlbar und einsatzfähig. Die zertifizierte Software-Lösung auf der Basis von PDF und Adobe Client-Software ist allgegenwärtig, systemübergreifend und zudem kostenlos für jeden Anwender erhältlich. Flankiert von zielführenden Initiativen von Banken, Behörden und Bundesregierung sollte der rechtsgültigen elektronischen Signatur damit nichts mehr im Wege stehen.

Der Alltag im Umgang mit Dokumenten, insbesondere mit elektronischen, wird sich daher noch stärker verändern und in den Haushalten werden neben einem PC mit Internetzugang und entsprechender Dokumentenverarbeitungssoftware auch Kartenleser, Chipkarten und virtuelle Unterschriften Einzug halten. Zwei objektive Kriterien sind dafür ausschlaggebend: Zum einen lassen sich durch elektronische Workflows erhebliche Kosten einsparen und zum anderen sind eGovernment-Initiativen und gesetzliche Vorgaben bereits fest verankert. Von A wie Antrag bis Z wie Zulassungspapiere, wichtige Dokumente werden schon bald persönlich digital unterzeichnet – und die gesamte Bearbeitung deutlich beschleunigt.

Weitere Informationen: www.adobe.de/signatur