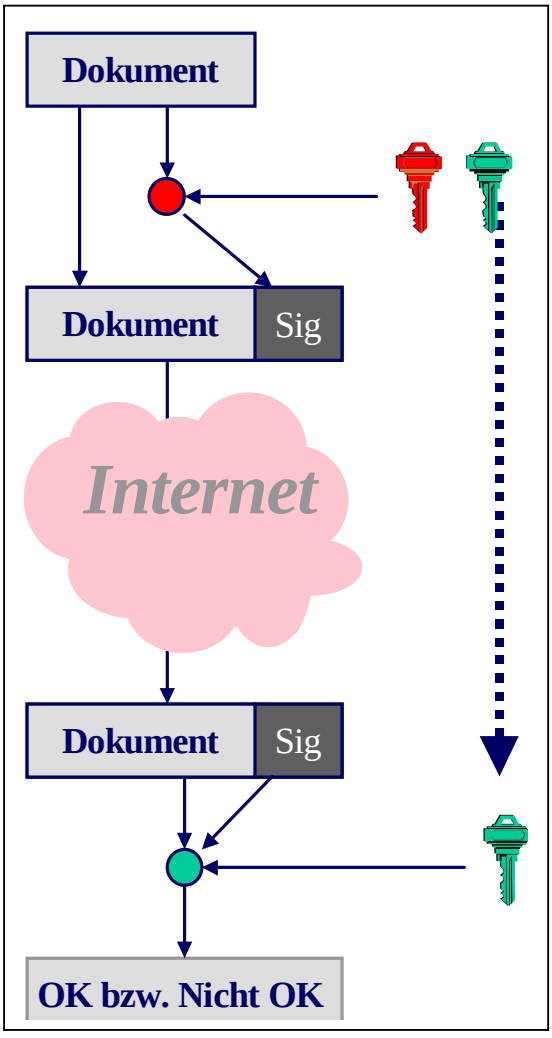
DIE ELEKTRONISCHE SIGNATUR: VOR DEM DURCHBRUCH?

von Ulrich Pordesch

Mit elektronischen Signaturverfahren kann man Daten „unterschreiben“ und deren Unverfälschtheit und Urheberschaft prüfen. Dieser Beitrag führt in die Thematik ein. Ein Folgebeitrag behandelt Chancen und Risiken aus Arbeitnehmersicht.

1 Das unsichere Internet

Elektronische Dokumente haben gegenüber herkömmlichen Papierdokumenten einen entscheidenden Nachteil: Sie können spurenlos verfälscht werden. Besonders groß ist das Fälschungsrisiko im Internet, zu dem der Zugang nicht kontrolliert wird und bei dem Daten im Klartext über Netzknoten privater Betreiber geleitet werden. Der Absenderangabe und dem Inhalt einer E-Mail oder einer Web-Page darf man im Grunde nicht trauen. Vor Gericht lässt sich mit einer Datei oder einem Ausdruck im Ernstfall nichts beweisen. Wenn wir in der Praxis das Internet dennoch häufig bedenkenlos nutzen, dann deshalb, weil wir kaum wirklich wichtige Rechtsgeschäfte vollständig elektronisch erledigen. Ansonsten wird irgendwann eben doch noch ein Stück Papier unterschrieben. Um diesen Zustand zu beseitigen, werden nun verstärkt elektronische Signaturverfahren eingesetzt.



2 Elektronische Signaturverfahren

Elektronische Signaturverfahren basieren auf einer besonderen Form der Datenverschlüsselung, der sogenannten asymmetrischen Verschlüsselung. Asymetrisch deshalb, weil man zum Ver- und Entschlüsseln nicht denselben, sondern verschiedene Schlüssel verwendet. Signaturverfahren sind eine Anwendung dieses Prinzips. Damit man signieren kann, muss zunächst ein persönliches Schlüsselpaar erzeugt werden. Dieses besteht aus einem Signaturschlüssel und einem dazu passenden (Signatur-)Prüfschlüssel. Beim Signieren berechnet ein Signierprogramm aus den Dokumentdaten und dem Signaturschlüssel die Signatur. Dokument und Signatur können dann gemeinsam als signiertes Dokument versendet werden.

Die Signatur kann vom Empfänger verwendet werden, um zu überprüfen, dass das Dokument nicht verändert wurde. Beim Prüfen der Signatur berech-

net das Prüfprogramm aus dem Dokument, der Signatur und dem Prüfschlüssel ein Prüfergebnis. Ein positives Prüfergebnis („Signatur ok“) kommt nur dann zustande, wenn das Dokument unverändert ist. Hingegen führt bereits die kleinste Veränderung des Dokumentes dazu, dass die Signatur nicht mehr zum Dokument passt und als ungültig erkannt wird. Das mathematische Verfahren beansprucht zu garantieren, dass die Signatur nur mit dem zum Prüfschlüssel gehörenden Signaturschlüssel erzeugt werden konnte.

3 Zertifikate

Um das Dokument prüfen zu können, muss man den Prüfschlüssel kennen. Man könnte ihn mitsenden. Allerdings kann der Empfänger dann nicht sichergehen, dass der Prüfschlüssel tatsächlich der im Dokument als Absender angegebenen Person gehört. Theoretisch könnte sich ja irgendjemand ein Schlüsselpaar erzeugt haben und dann einfach fälschlicherweise behaupten, er gehöre der im Dokument angegebenen Person.

Das Mittel, das hier weiterhilft, sind Zertifikate. Ein Zertifikat ist allgemein eine Bestätigung eines Dritten (Zertifizierer bzw. Zertifizierungsstelle), dass ein Schlüssel einer bestimmten Person zugeordnet ist. Zertifikate, die man zum Nachweis des Urhebers einer Signatur verwendet, enthalten den Prüfschlüssel, den Namen des Signierers und den Namen des Zertifizierers und weitere Angaben. Damit es nicht gefälscht werden kann, ist es ebenfalls (vom Zertifizierer) signiert. Das Zertifikat kann der Signatur beifügt werden. Dann kann das Prüfprogramm den Prüfschlüssel daraus ermitteln, um das Dokument zu prüfen, die Echtheit des Zertifikats selbst überprüfen und den Namen des Signierers anzeigen.

Beim Programm PGP kann jeder Nutzer Zertifikate für die Prüfschlüssel anderer Leute erstellen. Das ist praktisch, aber auch unsicher und Bestätigungen von irgendwelchen Privatpersonen haben vor Gericht kaum Beweiskraft. Der Normalfall ist daher die Erstellung von Zertifikaten durch Zertifizierungsdiensteanbieter. Diese überprüfen die Personangaben, etwa anhand eines vorzulegenden Personalausweises, bevor sie ein Zertifikat erstellen und signieren.

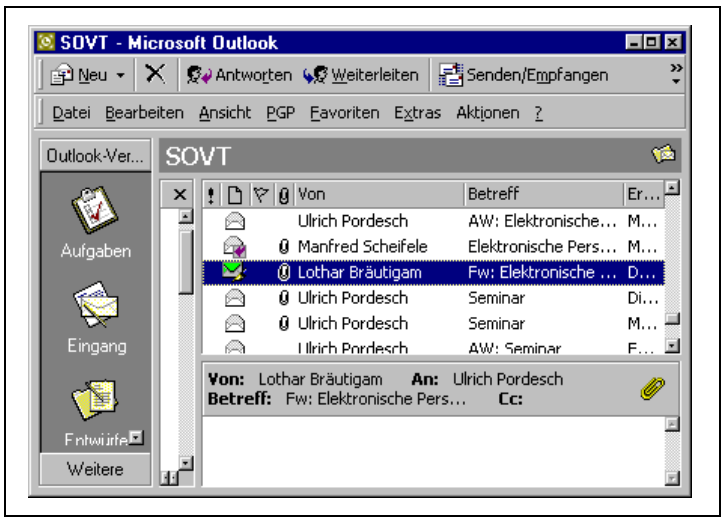
Neben der Erstellung von Zertifikaten können Zertifizierungsdiensteanbieter weitere Aufgaben übernehmen. Sie können Zertifikate vorzeitig sperren, etwa wenn ein Teilnehmer befürchtet, jemand habe seinen Signaturschlüssel kopiert und verwende ihn. Sie können Datenbanken ausgegebener Zertifikate führen, die man abfragen kann und verteilen Listen gesperrter Zertifikate, die man abrufen kann, wenn man eine Signatur prüft. Außerdem können sie den Teilnehmern noch Signier- und Prüfprogramme und Chipkarten als Schlüsselspeicher zur Verfügung stellen und für fehlerhaftes Handeln haften. Die Art der angebotenen Dienstleistungen und die Kosten dafür sind sehr unterschiedlich. Möchte man lediglich ein Zertifikat für den eigenen Prüfschlüssel, so kann man dieses kostenlos über das Internet beantragen und per E-Mail beziehen (z.B. bei WEB.DE http://www.web.de). Möchte man zusätzlich Signaturkarten und Kartenlesegerät, Software und Service, dann muss man bezahlen (z.B. derzeit 159 DM plus monatliche Kosten bei der Telekom http://www.telekom.de).

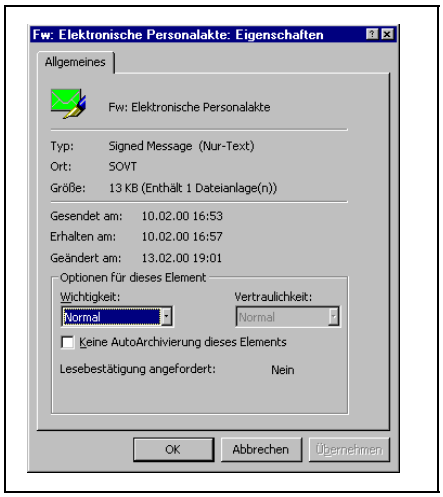
4 Anwendungsmöglichkeiten

Hauptanwendungsbereich von Signaturverfahren ist E-Mail. Betriebssysteme wie Microsoft Windows haben Signier- und Prüfprogramme bereits integriert und bieten in ihren E-Mailprogrammen standardmäßig Signier- und Prüffunktionen an. Hier kann man sich ein Schlüsselpaar erzeugen,

den Prüfschlüssel an eine Zertifizierungsstelle schicken und das per E-Mail erhaltene Zertifikat dann auf seinem PC abspeichern. Erhält man eine signierte E-Mail, dann wird das darin enthaltene Zertifikat auch gleich im elektronischen Adressbuch abgespeichert (es heißt dort digitale ID). Beim Prüfen der Signatur kann man es sich anzeigen lassen, um zu sehen, wer signiert hat. Statt eingebaute Signier- und Prüfprogramme zu nutzen, kann man Signier- und Prüfprogramme aber auch separat installieren und die Programmmenüs des E-Mail-Programms erweitern lassen (sogenannte Plug-Ins). Das oben erwähnt Programm Pretty Good Privacy (PGP) hat z.B. Plug-Ins für verschiedene E-Mailprogramme.

Doch signieren kann man nicht nur E-Mail. Mit Programmen wie PGP kann man Dateien beliebigen Inhalts signieren, also beispielsweise Word-Dokumente, aber auch Tondokumente, Fotos oder Filme. Auch Programme lassen sich signieren und so gegen Veränderung schützen, teilweise geschieht dies bereits. Im Internet steht der breite Einsatz von Signaturverfahren in den nächsten Jahren an, wenn anstatt der HTML-Sprache verstärkt XML eingesetzt wird, für das Signaturstandards derzeit entwickelt werden. Alle wichtigen Web-Seiten könnten künftig mit einer Signatur versehen werden, damit jeder prüfen kann, dass sie unverändert sind und von wem sie erstellt wurden.





Signaturverfahren sind also im Prinzip universell einsetzbar. Derzeit sind die Programm freilich noch zu kompliziert zu bedienen und weisen nur einen eingeschränkten Funktionsumfang auf. Noch gibt es zu verschiedene Datenformate für Signaturen und signierte Dokumente, die miteinander unverträglich sind. Deshalb kann man beispielsweise mit PGP signierte Mail mit den integrierten Signaturprüfprogrammen von MS Outlook prüfen. Hinzu kommen Probleme mit der Handhabung der Prüfschlüssel von Zertifizierungsstellen und den Internet-Adressen von Sperrdiensten. Heute sind diese Probleme nur in geschlossenen Anwendergruppen vernünftig lösbar. Doch es ist zu erwarten, dass sich bestimmte Produkte, Standards und Verfahrensweisen auf dem Markt bald durchsetzen werden.

5 Das Signaturgesetz

Auch wenn der Einsatz von Signaturverfahren gegenüber dem ungesicherten Datenaustausch einen immensen Sicherheitsgewinn bringen kann, so hängt die tatsächliche Sicherheit doch stark davon

ab, wie die Verfahren technisch und organisatorisch ausgestaltet sind. Die Zertifikate einer Zertifizierungsstelle einer Zertifizierungsstelle, die ihre Antragsteller nicht richtig überprüft und die in einem Seminarraum in einem Uni-Rechenzentrum betrieben wird, sind sicher weit weniger vertrauenswürdig als diejenigen eines Diensteanbieters mit einem Hochsicherheitsrechenzentrum. Eine Verfahren, bei dem Signaturschlüssel in einer Datei gespeichert und damit leicht kopiert und von Unbefugten verwendet werden können ist unsicherer als ein Verfahren, bei dem Schlüssel auf einer Chipkarte unsausforschbar gespeichert werden. Eine generelle Gleichstellung von Papierurkunden und Handunterschrift einerseits sowie Daten und elektronischen Signaturverfahren andererseits ist nicht möglich. Deshalb wird der Einsatz von Signaturverfahren und ihre rechtliche Anerkennung durch Gesetze geregelt.

Im zu Beginn des Jahres novellierten Signaturgesetz werden Sicherheitsanforderungen für Signaturen festgeschrieben, die als sicher gelten sollen („qualifizierte elektronische Signatur“). Hauptvoraussetzung ist, dass das dem Signaturschlüssel zugeordnete Zertifikat von einer Zertifizierungsstelle ausgestellt wurde, die gegenüber der zuständigen Regulierungsbehörde nachgewiesen hat, bestimmte Sicherheitsvorkehrungen zu erfüllen. Sie hat unter anderem die Identität der Antragsteller zu überprüfen und eine Schadensversicherung abzuschließen. Sicherzustellen ist auch, dass der Signaturschlüssel nur auf einer Signaturkarte gespeichert ist und nicht etwa in irgendeiner kopierbaren PC-Datei. Zudem ist der Antragsteller darüber zu belehren, zur Signaturerzeugung und –prüfung nur Software einzusetzen, die von zugelassenen Prüfstellen auf ihre Eignung und Sicherheit überprüft wurde.

Nur die qualifizierte elektronische Signatur wird dann der Handunterschrift weitgehend gleichgestellt. Mit im Sommer anstehenden Änderungen im bürgerlichen Gesetzbuch werden mit qualifizierter elektronischer Signatur signierte Dokumente („elektronische Form“) nun nahezu überall zugelassen, wo bisher nur das unterschriebene Stück Papier zulässig war. Hinzu kommt eine wichtige prozessrechtliche Änderung. Ein Dokument mit einer qualifizierten elektronischen Signatur soll vor Gericht den „Anschein der Echtheit“ haben. Der Richter soll davon ausgehen, dass es vom im Zertifikat angegebenen Prüfschlüsselinhaber stammt, unverfälscht ist und willentlich signiert wurde und man soll diesen Anschein nur durch konkrete Tatsachen erschüttern können.

6 Ausblick

Wie gezeigt, werden die rechtlichen und technischen Voraussetzungen für den Durchbruch der elektronischen Signatur derzeit geschaffen. Künftig könnte nahezu überall dort, wo in Betrieben und Verwaltungen heute noch Papierdokumente eingesetzt und unterschrieben werden müssen, Dokumente mit qualifizierter elektronischer Signatur eingesetzt werden. Es ist daher angezeigt, sich mit den Chancen und Risiken dieser Technologie für die Arbeitnehmer zu befassen. Davon wird der Folgebeitrag im nächsten Heft handeln.

Ulrich Pordesch ist Mitarbeiter bei der GMD- Forschungszentrum Darmstadt und arbeitet in Arbeitnehmerfragen mit dem Institut für Sozialverträgliche Technikgestaltung, sovt, in Darmstadt zusammen.