EDV-Gerichtstag – Arbeitskreis "Digitale Signatur"(25.09.2003, 13 Uhr)

Moderation: Ltd. Reg. Dir. Dr. Tauchert
Referenten: Rechtsanwalt Kuck; Herr Bovenschulte (bremen online services)
Berichterstatterin: Ass. jur. Iris Speiser

Auf dem von Herrn Lt.Reg.Dir. Tauchert moderierten Arbeitskreis "Digitale Signatur" haben zwei Referenten zu aktuellen Fragen der digitalen Signatur vorgetragen.

Herr Rechtsanwalt Kuck stellte in seinem Vortrag "Der reale Einsatz der digitalen Signatur im heutigen Rechtsverkehr" zunächst kurz die Funktionsweise der digitalen Signatur dar, um danach auf den praktischen Einsatz einzugehen.

Die derzeit verwendeten Verfahren zur Erzeugung von digitalen Signaturen beruhen auf asymmetrischen Verschlüsselungsverfahren. Das Verfahren ist deswegen asymmetrisch, weil zwei komplementäre Schlüssel verwendet werden, ein privater und eine öffentliche Schlüssel. Der private Schlüssel verbleibt bei den Inhaber. Er wird auf einem sicheren Medium (Chipkarte) gespeichert und durch eine PIN gegen unbefugten Zugriff gesichert. Der öffentliche Schlüssel wird von der zuständigen Zertifizierungsstelle online zur Überprüfung vorgehalten.

Die digitale Signatur selbst wird folgendermaßen erzeugt: Der Sender komprimiert das elektronische Dokument und bildet eine Kurzform (HASH-Wert). Diese Kurzform wird dann mit dem privaten Schlüssel des Senders verschlüsselt. Diese Signatur wird nun an das ursprüngliche Dokumente angehängt und an den Empfänger übermittelt. Der Empfänger entschlüsselt mittels des öffentlichen Schlüssels die Signatur und bildet aus dem Dokument nach den gleichen Verfahren wie der Sender ebenfalls den HASH-Wert. Stimmen beide HASH-Werte überein, steht dadurch fest, was das übermittelnde Dokument mit dem vom Sender verschicktem identisch ist und dass der Sender das ursprüngliche Dokument selbst signiert hat.

Die digitale Signatur wird derzeit hauptsächlich in geschlossenen Benutzergruppen eingesetzt, z.B. in der Rechtspflege bei Rechtsanwälten, Notaren und Ihren Kammern, Gerichten und Behörden, aber auch bei Privaten, wie bei der Kommunikation zwischen Banken und ihren Kunden.

Im Moment laufen bei den Gerichten einige Pilotprojekte zur digitalen Signatur:

- Am Bundesgerichtshof nutzen derzeit vier der 32 zugelassenen Anwälte die Möglichkeit es elektronischen Klageverfahrens mit digitaler Signatur 2003 wurden monatlich bereits zirka 180 Schriftsätze beim BGH elektronisch eingereicht.

- Das Finanzgericht Hamburg bietet seit dem 1. Mai 2002 die Möglichkeit, Klageverfahrens komplett per digital signierter E-Mail abzuwickeln ; ein paralleler Postversand erfolgt nicht mehr. An dem Projekt sind 25 Rechtsanwälte und Steuerberater sowie alle 16 Finanzämter der Stadt beteiligt ; die Einbindung der Hauptzollämter ist bereits geplant. Klageformulare können jetzt im Bildschirmdialog online ausgefüllt werden. Das neue Verfahren bietet zahlreiche Vorteile: Es ist unabhängig vom papiergebundenen gerichtlichen Postverteilungssystem, was Kosten eingespart und die Bearbeitungsdauer verkürzt. Medienbrüche werden vermieden und die Akte ist ständig verfügbar.

- Beim OLG Hamm wurde zum 1. Juli 2003 das elektronische Scheidungsverfahren eingeführt. Derzeit sind sechs Anwaltskanzleien und das Amtsgericht Olpe an dem Pilotversuch beteiligt, einfache Scheidungsverfahren auf elektronischem Wege abzuwickeln. Die Dokumente werden über einen "elektronischem Gerichtsbriefkasten" ausgetauscht ; die Implementierung der digitalen Signatur ist allerdings erst für einen späteren Zeitpunkt geplant. Das OLG erhofft sich von diesem Verfahren reduzierte Erledigungszeiten, eine Straffung des Verfahrens und eine erleichterte Akten Bearbeitung.

Auch für Unternehmen bietet die Verwendung der digitalen Signatur etliche Vorteile, wie z.B. Sicherheit der Kommunikation (sowohl innerhalb des Unternehmens als auch mit Geschäftspartnern), die Möglichkeit des E-Billing, beweissichere Archivierung nach den

Anforderungen des HGB (insbesondere nach den Grundsätzen der ordnungsgemäßen Buchführung), vereinfachte Behördenvorgänge, die Teilnahme an elektronischen Ausschreibungen ("eVergabe"), etc.

Privatleuten dürfte die digitale Signatur vor allem zu vereinfachten Behördenvorgängen verhelfen, z. B. bei der Beantragung von Pässen, Ausweisen und Führerscheinen, der Beantragung von Parkausweisen sowie bei Wahlen.

Der öffentlichen Verwaltung kann die digitale Signatur helfen, interne und externe Verwaltungsabläufe schneller, sicherer und effizienter zu gestalten. Das Ziel ist die vollständig papierlose Verwaltung. In Österreich existiert bereits papierlose Kommunikation zwischen Gerichten und Verfahrensbeteiligten. Dort werden bereits 60 Prozent aller Zivilklagen elektronisch erhoben, mit der Folge, dass sie jährlich eine Million € Portokosten eingespart werden können.

Esslingen fährt derzeit ein Pilotprojekt " Virtuelles Bauamt ", bei dem nach Expertenschätzungen mit Einsparpotential in Höhe von 190 Millionen € pro Jahr zu rechnen ist.

Trotz all dieser Vorteile stehen dem Einsatz der digitalen Signatur auch einige Nachteile gegenüber, die bis jetzt die Verbreitung hemmen. An erster Stelle ist hier der hohe Einführungspreis zu nennen. Es fehlt eine " Killerapplikation ". Auch existieren bisher keine Vermarktungskonzepte für die digitale Signatur. Die Interoperabilität und Kompatibilität der verschiedenen Systeme ist noch immer mangelhaft. Zudem steht die digitale Signatur in dem Ruf, nicht benutzerfreundlich zu sein.

Um Abhilfe zu schaffen, haben sich nun im April 2003 etliche Behörden, Banken und Verbände zu einem Signaturbündnis zusammengeschlossen. Sie haben sich das Ziel gesetzt, bis Ende 2005 einheitliche Standards für die eingesetzten Produkte zu schaffen und multifunktionale Chipkarten zu entwickeln, die für verschiedene Anwendungen genutzt werden können.

Zeitgleich treibt die Bundesverwaltung das Projekt "BundOnline 2005" voran. Mittelfristig soll dies dazu führen, dass Ausweispapiere mit einer digitalen Signatur ausgestattet werden.

Hier könne möglicherweise die Biometrie eine sinnvolle Ergänzung darstellen. In Betracht kommen hierbei mehrere Verfahren, die sich in drei Kategorien einteilen lassen: Physiologische Merkmale, Verhaltensmerkmale sowie kombinierte Verfahren, die mehrere Merkmale prüfen, was die Erkennungssicherheit erhöht.

Derzeit laufen zahlreiche Pilotprojekte zur Biometrie im praktischen Einsatz. Am bekanntesten ist die biometrische Gesichtserkennung auf diversen Flughäfen. Leider hat sich bei diesen Versuchen herausgestellt, dass selbst eine geringe statistische Fehlerquote in Anbetracht der großen Zahl kontrollierter Personen zu einer erheblichen Anzahl von Fehlerkennungen führt, die der vollautomatisierten Kontrolle entgegensteht. So würde eine Fehlerrate von einem Promille auf einem Internationalen Flughafen wie Frankfurt mehr als 100 Fehlalarme täglich auslösen.

In der Folge des 11. September wollen die USA demnächst von Einreisenden nur noch Pässe akzeptieren, die biometrische Merkmale enthalten. Die EU passt sich diesen Vorgaben an und will biometrische Merkmale in Visa einführen.

Biometrische Daten könnten auf der Signaturkarte die PIN als Legitimationsmerkmal ablösen. Dadurch fiele die Gefahr des unbefugten Gebrauchs der Karte durch Erpressung der PIN oder fahrlässigen Umgang mit dieser weg. Es müsste jedoch ein System zum Einsatz kommen, das mit dem geltenden Datenschutzrecht vereinbar ist, da eine zentrale Speicherung der Datensätze die Anfertigung von Bewegungsprofilen ermöglichen würde, was mit dem allgemeinen Persönlichkeitsrecht unvereinbar ist.

Kuck plädiert im Ergebnis für einen Kombination aus biometrischen Daten und elektronischer Signatur. Nur so werde ein breiter Einsatz digitaler Signaturen möglich.

Herr Bovenschulte von bremen online services beleuchtete den elektronischen Rechtsverkehr in der Praxis und zeigte Inkonsistenzen in den Verfahrensvorschriften auf.

Bereits die Eröffnung eines Zugangs für elektronische Kommunikation erfordert einen normsetzenden Akt. So ist für die Einreichung elektronischer Dokumente bei Gericht der Erlass einer Rechtverordnung erforderlich – dies gilt unabhängig davon, ob es sich um signierte oder unsignierte Dokumente handelt. Werden hingegen elektronische Dokumente vom Gericht an die Parteien übermittelt oder zugestellt, so ist dies auch ohne vorherigen Erlass einer Rechtsverordnung zulässig.

Praktische Probleme bereitet die Form elektronischer Dokumente. Nur ein für den Empfänger bearbeitbares Dokument kann Rechtsfolgen auslösen. Diesem Bedürfnis kann durch Rechtverordnung Rechung getragen werden. Es ist jedoch unklar, wie eventuelle Formverstöße rechtlich zu handhaben sind. Denkbar sind folgende Fälle:

- Ein elektronisches Dokument ist zwar verordnungskonform, aber dennoch nicht bearbeitbar. Eine solche materielle Ungeeignetheit geht nach den allgemeinen Zugangsregeln zu Lasten des Absenders.

- Ein elektronisches Dokument ist nicht verordnungskonform, kann aber vom Gericht dennoch bearbeitet werden. Hier kommt es darauf an, ob es sich bei dem Formerfordernis um eine Muss- oder eine Soll- Vorschrift handelt. Handelt es sich um eine Soll-Vorschrift, ist der Verstoß unschädlich. Handelt es sich hingegen um eine Muss-Vorschrift, so würde der Empfänger von der Pflicht zur Bearbeitung entbunden – allerdings nur bis zur Grenze des Willkürverbots.

Die Auslegung des § 130a ZPO ist in diesem Zusammenhang umstritten. Diese Auslegungsprobleme würden noch zunehmen, wenn das Justizkommunikationsgesetz in der vorliegenden Fassung in Kraft treten würde, denn darin werden für unterschiedliche Prozessordnungen unterschiedliche Regelungsmodelle verfolgt:

- Die derzeit geltende ZPO und das ArGG bestimmen für die "Einreichung elektronischer Dokumente bei Gericht", dass eine qualifizierte Signatur eingesetzt werden *soll*, wenn die *Schriftform* angeordnet ist.

- Der ZPO-Entwurf und der ArGG-Entwurf sehen für "elektronische Dokumente des Gerichts" vor, das die qualifizierte Signatur eingesetzt werden *muss*, wenn *Schriftform und handschriftliche Unterzeichnung* angeordnet ist.

- Die Entwürfe für die Neuregelungen in VwGO, SGG und FGG verwenden nur den Begriff "elektronische Dokumente" und verlangen, dass die qualifizierte Signatur eingesetzt werden *muss*, wenn *Schriftform i.S.d. § 126 BGB* angeordnet ist.

- Die Entwürfe zur Neuregelung von StPO und OwiG ordnen an, dass für "elektronische Dokumente" die qualifizierte Signatur eingesetzt werden *muss*, wenn *ausdrücklich Schriftlichkeit oder handschriftliche Unterzeichnung* angeordnet ist.

Zudem schafft der JKommG-E zusätzliche Inkonsistenzen im Hinblick auf die Signaturqualität. Nach derzeitiger Rechtslage genügt durchweg eine "einfache" qualifizierte Signatur. Mit Einführung des JKommG würde sich dies für die VwGO, das SGG und das FGG ändern. Aus europarechtlichen Gründen *darf* den Parteien die Verwendung akkreditierter Signaturen nicht zwingend vorgeschrieben werden. Dagegen *braucht* den Gerichten die Verwendung akkreditierter Signaturen nicht zwingend vorgeschrieben zu werden.

In der Praxis wird der Einsatz qualifizierter Signaturen auf bestimmte Produkte beschränkt. Dies reduziert die technische Komplexität und ist auch sinnvoll, solange es noch keinen etablierten Standard gibt. Eine Rechtsverordnung sollte jedoch neben der Beschränkung eine Öffnungsklausel enthalten, nach der "Produkt X oder ein kompatibles Produkt" einzusetzen ist.

Es ist nicht abschließend geklärt, welche Pflichten das Gericht beim Empfang elektronischer Dokumente hat. Das Gericht ist wohl nicht verpflichtet, die Gültigkeit einer

Signatur zu überprüfen, muss aber bei Dokumenten, die signiert sein müssen feststellen, ob es sich überhaupt um eine qualifizierte Signatur handelt.

Die vom SigG vorgesehenen Pseudonyme sind für den Einsatz bei Gericht ungeeignet. Diese Möglichkeit sollte daher ausgeschlossen werden. Das JKommG sieht einen solchen Ausschluss jedoch nur für einige Verfahrensordnungen vor.

Auch Attribute in Signaturen können zu Problemen führen. In der Regel besteht für Attribute nur dort ein Bedürfnis, wo entsprechende Nachweise erforderlich sind. Werden überflüssige Attribute eingebunden, verstößt dies möglicherweise gegen das Gebot der Datensparsamkeit und kann für den Absender unerwünschte Nebenfolgen haben (z.B. wenn das Gericht hierdurch von einem Rechtverhältnis Kenntnis erlangt und diese bei der Entscheidung zum Nachteil des Absenders berücksichtigt). Zudem sind Attribute nicht standardisiert, was einer automatischen Auswertung entgegensteht.

Beim Austausch elektronischer Dokumente mit den Gerichten sind schließlich noch folgende Aspekte zu beachten:

- Es muss eine technische Infrastruktur geschaffen werden, die es dem Gericht erlaubt, ohne weiteres Zutun des Absenders auf die Dokumente zuzugreifen.

- Gerichte sind grundsätzlich zur Verschlüsselung verpflichtet. Diesen Aspekt hat der Gesetzgeber bisher nicht berücksichtigt. Eine Verschlüsselungspflicht der Parteien besteht dagegen in der Regel nicht (Ausnahme: Übermittlung personenbezogener Daten durch speichernde Stellen i.S.d. Datenschutzgesetze). Eine Verschlüsselungspflicht von Prozessbevollmächtigten ergibt sich möglicherweise aus dem Mandatsverhältnis.

Bovenschulte regt im Ergebnis an, eine einfache Regelung dergestalt zu schaffen, dass bei Dokumenten, die der Schriftlichkeit bedürften eine qualifizierte elektronische Signatur zugelassen wird; für alle übrigen Fälle solle hingegen vom Erfordernis einer Signatur abgesehen werden.