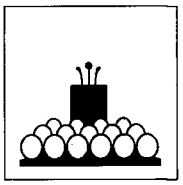
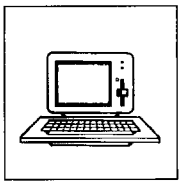



Digitale Signaturverfahren – technische und rechtliche Fragen

(4. Deutscher EDV-Gerichtstag in Saarbrücken – Arbeitskreis "Elektronische Signatur")

Margarethe Bergmann/Siegfried Streitz

Referat Buchmann

Prof. Dr Johannes Buchmann, Leibniz-Preisträger und Professor für Informatik an der Universität des Saarlandes, erläuterte zunächst die Funktionsweise digitaler Verschlüsselungsverfahren. Zur Verschlüsselung werden mathematischen Algorithmen verwendet, bei denen aus zwei Primzahlen (eine Primzahl kann nur durch sich selbst und durch eins geteilt werden) ein Produkt gebildet wird. Die Sicherheit beruht darauf, daß es zwar relativ einfach ist, zwei große Primzahlen miteinander zu multiplizieren, aber äußerst schwierig, eine Zahl in ihre Primfaktoren zu zerlegen. Bei entsprechend langen Produkten läßt sich nur durch aufwendige Rechenverfahren ein Rückschluß auf die Primzahlfaktoren ziehen. Prof. Buchmann wies jedoch darauf hin, daß es keinen mathematischen Beweis für die Komplexität dieses Verfahrens gibt; die Schwierigkeit rührt derzeit nur daher, daß die Forschung keinen einfacheren Weg zur Berechnung der Primfaktoren gefunden hat. Zumindest ist es theoretisch denkbar, daß ein Lösungsverfahren entdeckt wird, das mit erheblich weniger Aufwand die Faktoren berechnet und somit die Sicherheit erheblich reduziert.

Public-Key-Verfahren

Bei den sogenannten *Public-Key-Verfahren* erfolgt die Verschlüsselung mit einem veröffentlichten, die Entschlüsselung mit Hilfe eines privaten Schlüssels. Die Übermittlung von Schlüsseln ist beim Public-Key-Verfahren nicht erforderlich, so daß dieses auch bei vertraulich zu haltenden Nachrichten, also zur Codierung, eingesetzt werden kann. Demgegenüber wird bei der *digitalen Signatur* der zur Verschlüsselung eingesetzte Algorithmus geheimgehalten und zur Entschlüsselung ein veröffentlichter Schlüssel verwendet. Digitale Signaturverfahren sind demnach nicht zur Übermittlung geheimer Nachrichten geeignet, sondern dienen zur Verifikation, d. h. der Überprüfung der Identität des Erklärenden, sowie zur Bestätigung der Authentizität, d.h. der Übereinstimmung mit dem gewollten Erklärungsinhalt.

Rechenverfahren

Es sind somit Rechenverfahren für die Erzeugung der Schlüssel, für die digitale Signatur und für die Verifizierung (Entschlüsselung der Signatur) erforderlich. Dabei wird sichergestellt, daß aus der Kenntnis des öffentlichen Schlüssels der geheime Schlüssel nur mit erheblichem Aufwand berechnet werden kann. Prof. Buchmann erläuterte, daß derzeit Moduln von 512-Bit-Länge verwendet werden. Diese seien nur so lange sicher, als der *Rechenaufwand* zu ihrer Entschlüsselung unverhältnismäßig hoch sei. Nach der Prognose des Referenten wird dies voraussichtlich in fünf Jahren nicht mehr der Fall sein, so daß längere Module (1024 Bit) verwendet werden müssen. Neben der Sicherheit des Schlüssels selbst kommt der sicheren Organisation, der Schlüsselausgabe und -verwahrung besondere Bedeutung zu.

Referat Nilgens

Anhand eines praktischen Beispiels (Apple Mail-Programm) erläuterte anschließend *Dr. Volker Nilgens*, Rechtsanwalt in Düsseldorf, die Vorgehensweise bei der Generierung und Verwendung elektronischer Schlüssel. Die Schlüssel werden von der Herstellerfirma selbst erzeugt und im Klartext übermittelt. Darüber hinaus bedarf es einer Bestätigung, daß dieser Schlüssel einer bestimmten Person zugeordnet wird, damit dieser im Rechtsverkehr verwendet werden kann. Derzeit werden diese Bestätigungen von der Herstellerfirma ausgestellt. Aus dem Teilnehmerkreis wurden Bedenken dahingehend geäußert, ob Bestätigungen ausländischer Notare die gleiche Beweiskraft zukommt wie solchen, die von deutschen Notaren abgegeben werden, da im Ausland teilweise nicht die gleichen strengen Vorschriften hinsichtlich der Notarpflichten bestehen und die Institutionen daher nur begrenzt vergleichbar sind.

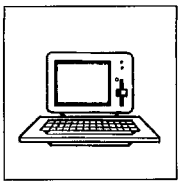
Die Diskussion

In der darauffolgenden, von *Dr. Siegfried Streitz* (öffentlich bestellter und vereidigter EDV-Sachverständiger der IHK Köln) geleiteten Diskussion wurden Nutzen und Risiken digitaler Signaturverfahren eingehend erörtert. Dabei wurde herausgestellt, daß neben der technischen Sicherheit der Schlüssel insbesondere der Sicherheit der Schlüsselvergabe und -verwaltung eine besondere Bedeutung zukommt.

Auf diese Fragen ging im nachfolgenden Referat *Paul Mertes* (LL.M., Produktzentrum Telesec der Telekom, Siegen) ein. Am Beispiel der Firma Telesec erläuterte er den im August 1994 aufgenommen Betrieb eines sog. *Trust-Centers* und legte dar, unter welchen organisatorischen und technischen Sicherheitsvorkehrungen dort Chipkarten erzeugt und den Be-

Margarethe Bergmann ist Richterin am AG Köln, Dr. Siegfried Streitz ist öffentlich bestellter und vereidigter EDV-Sachverständiger der IHK Köln.

JurPC-Archiv: http://www.jurpc.de



nutzern zugeordnet werden. Der praktische Einsatz der Chipkarten wird derzeit bei den Mahngerichten Hagen, Stuttgart und demnächst auch Euskirchen erprobt. Der geheime Schlüssel wird nur auf einer Prozessor-Chipkarte aufgelegt, die zum Signieren von Dokumenten wie z. B. Mahnbescheidsanträgen verwendet werden kann. Erweist sich ein Schlüssel aufgrund technischer Weiterentwicklungen im nachhinein als nicht mehr sicher, so kann auch ein Nachsignieren mit einem sicheren Schlüssel erfolgen. Eine Kaufkarte (ohne Schlüssel-Management, z.B. für einen geschlossenen Benutzerkreis) ist derzeit bereits für 99 DM, eine allgemein verwendbare Mietkarte für 450 DM pro Jahr verfügbar. Derzeit nutzen bereits ca. 2.000 Anwender im Rahmen eines Bürokommunikationssystems der Telekom diese technischen Möglichkeiten.

Referat Sigrun Erber-Faller

In dem abschließenden Referat legte *Sigrun Erber-Faller*, Geschäftsführerin der Bundesnotarkammer in Köln, die rechtlichen Aspekte elektronischer Signaturen dar. Sie erläuterte, in welcher Hinsicht elektronische Dokumente von den bisher verwendeten Papierdokumenten abweichen und welche Funktionen der herkömmlichen Unterschrift zukommen. Die herkömmliche Schriftform gibt Auskunft über die Person des Unterzeichners und beendet den Text räumlich als inhaltlich richtig und vollständig. Daneben hat sie eine Warnfunktion, weil man sich der besonderen Bedeutung der Unterschrift bewußt ist. Darüber hinaus kommt ihr eine Beweisfunktion im Rechtsverkehr und bei bestimmten Dokumenten auch eine Kontroll- und Weitergabefunktion (wie z.B. bei Wertpapieren) zu.

Geeignetheit der digitalen Signatur

Elektronische Signaturverfahren müssen diese Funktionen soweit wie möglich nachbilden, damit sie im Rechtsverkehr in vergleichbarer Weise verwendet werden können. Die digitale Signatur wurde grundsätzlich als hierfür geeignet angesehen, sofern die damit verbundenen technischen und organisatorischen Fragen hinreichend gelöst werden können. In geringerem Maße wurde dies bezüglich der Ausstelleridentität bejaht, da eine Weitergabe der elektronischen Identität durch Übergabe von Chipkarte und *PIN* (Personal Identity Number) schwerer nachweisbar sei als die Fälschung einer handschriftlichen Unterschrift.

Nötig: Adäquate rechtliche Rahmenbedingungen

Die Verwendung elektronischer Chipkarten im Rechtsverkehr bedürfe jedoch adäquater *rechtlicher Rahmenbedingungen*. Der Gesetzgeber müsse regeln, unter welchen Voraussetzungen elektronischen Dokumenten Beweiskraft zukomme. Aufgrund der Verschiebung von Risikopotentialen könnten nämlich mit herkömmlichen Mitteln gefundene Lösungen teilweise nicht mehr befriedigen. So wurde es als schwer hinnehmbar angesehen, daß die bisherige Rechtsprechung beispielsweise sämtliche Risiken der Verwendung elektronischer Chipkarten letztlich dem Kunden auferlegt habe, obwohl insbesondere die Bank durch deren Einsatz erhebliche Vorteile und Erleichterungen im Rechtsverkehr habe. Hier treten rechtliche Interessen- und Beweislastverschiebungen auf, deren Regelung durch den Gesetzgeber gefordert wurde.

Schlußdiskussion

In der abschließenden Diskussion, die von *Rin AG Margarethe Bergmann* (AG Köln) geleitet wurde, wurde die Frage nach dem gesetzgeberischen Handlungsbedarf unterschiedlich beantwortet. Die anwesenden Vertreter des Bundesjustizministeriums erläuterten die bisherigen Arbeiten an einem Rahmenentwurf, der derzeit im Bundesinnenministerium erstellt wird, und den Stand der Überlegungen hierzu im Bundesjustizministerium.

Richtlinienvorschlag über den Abschluß von Verträgen im Fernabsatz

Darüber hinaus wurde auf den Richtlinienvorschlag über den Abschluß von Verträgen im Fernabsatz der Europäischen Kommission und den *EDI-Rahmenvertrag* (Electronic Document Interchange) hingewiesen. Es bestand Einigkeit darüber, daß digitale Signaturverfahren nicht nur bei der Großindustrie, die EDI bereits derzeit im Bestellungswesen einsetzt, eine erhebliche Rolle spielt, sondern daß künftig jeder Verbraucher von diesen Fragen betroffen sein wird. Dabei kommt *Telefax*-Dokumenten eine Sonderstellung zu, da sie neben Willenserklärungen häufig auch Prozeßerklärungen beinhalten, wie die hierzu bereits ergangene umfangreiche Rechtsprechung zeigt.

Weiteres Studium nötig

Im Hinblick auf die Bedeutung und die damit verbundenen Fragestellungen, die nicht nur den einzelnen, sondern die gesamte Volkswirtschaft betreffen, sollte sich der EDV-Gerichtstag auch künftig mit den rechtlichen und technischen Rahmenbedingungen elektronischer Dokumente befassen.

JurPC-Archiv: http://www.jurpc.de