Ein gemeinschaftlicher Rahmen für elektronische Signaturen

Richard Schlechter

Europäische Kommission - Generaldirektion Informationsgesellschaft
Rue de La Loi 200 (BU 24 1/8)
Richard.Schlechter@cec.eu.int

Schlagworte: Elektronische Signatur, Europäische Union, Richtlinie, International, Akkreditierung, Haftung, Zertifikat

Abstract: Ausgehend vom Bedarf an erhöhter Sicherheit im Internet auf Grund der steigenden Bedeutung des Electronic Commerce wird der europäische Regelungsrahmen für die Bereitstellung von Diensten im Zusammenhang mit elektronischen Signaturen vorgestellt. Eingangs werden Ziel und Anwendungsbereich der Richtlinie über elektronische Signaturen behandelt. Danach folgen Erläuterungen zum Modell des freien Marktzuganges für Zertifizierungsdiensteanbieter, zur rechtlichen Anerkennung elektronischer Signaturen und zu den haftungsrechtlichen Bestimmungen auf europäischer Ebene. Durch die Untersuchung des Standardisierungsprozesses für Kryptographieprodukte, der datenschutzrechtlichen Aspekte und der grenzüberschreitenden Anerkennung von Signaturen und Zertifikaten werden alle Regelungsinhalte der Richtlinie besprochen.

Am 19. Januar 2000 trat die Richtlinie der EU über elektronische Signaturen in Kraft. Sie zielt darauf ab, Hindernisse für den Binnenmarkt zu beseitigen. Insbesondere werden die rechtliche Anerkennung elektronischer Signaturen auf Gemeinschaftsebene sowie der freie Verkehr von Diensten und Produkten im Zusammenhang mit elektronischen Signaturen gewährleistet. Schwerpunkt der Richtlinie sind Regelungen zum Marktzugang für Zertifizierungsdiensteanbieter und zur rechtlichen Anerkennung elektronischer Signaturen. Darüber hinaus werden Haftungsregelungen und Regelungen zur rechtlichen Anerkennung von Zertifikaten aus Drittstaaten getroffen.

1. Vorbemerkung

Die Sicherheit des Internets läßt noch viele Wünsche offen: Nachrichten und Dokumente können abgefangen und manipuliert, die Echtheit

von Dokumenten kann bestritten werden. Neue Verfahren zur Verbesserung der Informationssicherheit, wie die elektronische Signatur, können hier Abhilfe schaffen. Produkte und Dienstleistungen in diesem Bereich tragen zu einer sichereren Infrastruktur bei und ermöglichen dadurch nicht nur in umfangreichem Maße kommerzielle Aktivitäten über offene Netze, sondern sie stehen auch für einen vielversprechenden und schnell wachsenden Markt. Allein der Markt für sogenannte „public key infrastructure" (PKI) Dienstleistungen und Produkte soll bis zum Jahr 2001 weltweit etwa 2 Milliarden $ ausmachen. Dieser Markt weist ein durchschnittliches jährliches Wachstum von über 100% auf. 1999 dominierte Nordamerika den Markt noch mit einem Anteil von etwa 80 %. Der Anteil der europäischen Unternehmen soll aber bis zum Jahr 2001 auf 35 % ansteigen[1].

Weltweite elektronische Kommunikation und weltweiter elektronischer Geschäftsverkehr sind auf die schrittweise Anpassung des nationalen und internationalen Rechts an die sich rasch entwickelnde technologische Infrastruktur angewiesen. Obwohl in einigen Fällen Analogien zu bestehenden Regeln zu zufriedenstellenden Lösungen führen können, ist die Kommission der Auffassung, daß aufgrund der neuen Technologien Anpassungen der bestehenden Regeln in bestimmten Bereichen unerläßlich sind.

Auch andere internationale Organisationen beschäftigen sich intensiv mit dem Thema elektronische Signatur. Die UN-Kommission für internationales Handelsrecht (UNCITRAL) hat ein Modellgesetz für den elektronischen Geschäftsverkehr beschlossen und, darauf aufbauend, Arbeiten zur Entwicklung einheitlicher Regeln für elektronische Signaturen aufgenommen[2]. Die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) arbeitet an einer Übersicht über Formvorschriften im Bereich elektronischer Signaturen und führt damit die auf den Leitlinien für die Kryptographiepolitik von 1997[3] basierende Arbeit fort.

Um einen international kompatiblen Rahmen zu schaffen, ist es notwendig, die internationalen Entwicklungen schon frühzeitig in die Arbeit auf europäischer Ebene einzubeziehen. Dies bereitet auch den Weg für spätere Vereinbarungen über die Beseitigung administrativer und rechtli-

---

[1] vgl. http://www.datamonitor.com/dmhtml/tc/tcprodl.htm

[2] vgl. http://www.un.or.at/uncitral/index.htm

[3] vgl. OECD-Leitlinien zur Kryptopolitik („Guidelines on Cryptography Policy") vom 27.3.1997; http://www.oecd.org/dsti/iccp/cryptoe.html

cher Hindernisse sowie zur grenzüberschreitenden Anerkennung elektronischer Signaturen[4].

2. Die Signatur-Richtlinie

Am 13. Mai 1998 legte die Kommission im Rahmen des Mitentscheidungsverfahrens nach Artikel 251 EG Vertrag einen Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über elektronische Signaturen vor[5]. Am 30. November nahm der Europäische Rat die vom Europäischen Parlament in zweiter Lesung verabschiedete Fassung der Richtlinie an. Diese trat mit ihrer Veröffentlichung im Amtsblatt am 19. Januar 2000 in Kraft[6]. Die Mitgliedstaaten haben bis zum 19. Juli 2001 Zeit, die Richtlinie umzusetzen.

Die Richtlinie beschränkt sich auf die Schaffung rechtlicher Rahmenbedingungen für die Bereitstellung von Diensten im Zusammenhang mit elektronischen Signaturen und die zur Erreichung dieses Ziels notwendigen Mindestanforderungen und überläßt die detaillierte Umsetzung den Mitgliedstaaten. Rechtliche Grundlage ist Artikel 47 Absatz 2, 55 und 95 des EG-Vertrages.

2.1 Ziel und Anwendungsbereich der Richtlinie

Ziel der Richtlinie ist es, Hindernisse für den Binnenmarkt zu beseitigen. Insbesondere sollen die rechtliche Anerkennung elektronischer Signaturen auf Gemeinschaftsebene sowie der freie Verkehr von Diensten und Produkten im Zusammenhang mit elektronischen Signaturen gewährleistet werden.

Von der Richtlinie ausgenommen sind solche elektronische Signaturen, die ausschließlich in Systemen verwendet werden, die auf freiwilligen privatrechtlichen Vereinbarungen zwischen einer bestimmten Anzahl von Teilnehmern beruhen. Elektronische Signaturen, die in diesen sog. „geschlossenen Systemen", wie z.B. dem lokalen Netz eines Unternehmens oder einem geschlossenen Banksystem, verwendet werden, sollen

---

[4] vgl. hierzu Mitteilung der Europäischen Kommission: Globalisierung und Informationsgesellschaft – Die Notwendigkeit einer stärkeren internationalen Koordinierung vom 4.2.1998 (KOM(98)50); http://www.ispo.cec.be/eif

[5] Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen (KOM (1998)297endg.); vgl. http://www.ispo.cec.be/eif

[6] Richtlinie 1999/93/EC
http://europa.eu.int/eur-lex/en/oj/2000/l_01320000119en.html

grundsätzlich nicht in den Geltungsbereich der Richtlinie fallen. Damit respektiert die Richtlinie die Vertragsfreiheit der Parteien. Elektronische Signaturen, die in solchen Systemen verwendet werden, können dennoch rechtlich anerkannt werden und sind als Beweismittel in Gerichtsverfahren zulässig.

2.2 Marktzugang

Das Anbieten von Zertifizierungsdiensten über offene Netze darf nicht von einer vorherigen Genehmigung abhängig gemacht werden. Den Mitgliedstaaten steht es aber offen, freiwillige Akkreditierungssysteme für solche Zertifizierungsdiensteanbieter einzuführen, die ein höheres Sicherheitsniveau anstreben. Eine Akkreditierung kann zum Beispiel in Form eines Gütesiegels erteilt werden. Damit kann in transparenter Weise zu mehr Vertrauen und zu einem höheren Maß an rechtlicher Sicherheit bei den Marktteilnehmern beigetragen werden. Einige Mitgliedstaaten streben an, das Akkreditierungssystem unter bloßer staatlicher Aufsicht privatwirtschaftlich zu organisieren.

Ferner dürfen Mitgliedstaaten die Bereitstellung von Zertifizierungsdiensten durch Diensteanbieter aus anderen Mitgliedstaaten in den unter die Richtlinie fallenden Bereichen nicht einschränken. Sie müssen auch dafür Sorge tragen, daß elektronische Signaturprodukte, die den Anforderungen der Richtlinie entsprechen, frei im Binnenmarkt vertrieben werden können.

2.3 Einheitliche Anforderungen

Um die grenzüberschreitende Verwendung und Anerkennung elektronischer Signaturen sicherzustellen, müssen Zertifikate und Produkte in allen Mitgliedstaaten anerkannt werden. Die Richtlinie der Europäischen Union legt hierfür einheitliche Anforderungen an Zertifikate, Zertifizierungsdiensteanbieter und Signaturprodukte fest.

Die Anforderungskataloge sind unabhängig vom konkreten Akkreditierungssystem der Mitgliedstaaten anwendbar. Da die künftige technologische und wirtschaftliche Entwicklung gegebenenfalls Anpassungen erforderlich macht, sind die Anforderungskataloge von Zeit zu Zeit zu überprüfen. Dabei wird die Kommission von einem Ausschuß mit beratender Funktion unterstützt, der sich aus Vertretern der Mitgliedstaaten zusammensetzt. Harmonisierungsmaßnahmen der Gemeinschaft sollen jedoch auf die Festlegung der notwendigen Anforderungen beschränkt bleiben und die technischen Details dem Markt bzw. Normungsgremien

überlassen. Die oben aufgeführten einheitlichen Kriterien für die Tätigkeit von Zertifizierungsdiensteanbietern und für Zertifikate folgen diesem Grundsatz. Zudem bleibt es den Mitgliedstaaten überlassen, wie sie die Einhaltung der Anforderungen konkret sicherstellen wollen, etwa über eine Art Prüfsiegel oder eine Selbstverpflichtung. Auf diese Weise ist ein Nebeneinander von akkreditierten und nicht akkreditierten Zertifizierungsdiensteanbietern möglich.

2.4 Rechtliche Anerkennung

Die entscheidende Frage in der Rechtspraxis ist, ob elektronisch signierte Dokumente gesetzlichen Formvorschriften genügen und ob ein mit einer elektronischen Signatur versehenes Dokument vor Gericht als Beweismittel Anerkennung findet. Da in vielen rechtlichen Bereichen keine spezifische Form notwendig ist, in vielen Mitgliedstaaten besteht beispielsweise für Kaufverträge überwiegend kein Schriftformerfordernis, bliebe es nach der aktuellen Rechtslage im Streitfall den Gerichten überlassen, ob sie im Wege der freien Beweiswürdigung elektronisch signierte Dokumente anerkennen oder nicht. Diese Vorgehensweise wurde bereits bei anderen technischen Neuerungen, etwa bei der Anerkennung von Unterschriften auf Faxen, angewendet. Eine klare rechtliche Regelung ist aber zu bevorzugen, weil sie sich positiv auf die Akzeptanz elektronischer Signaturen durch die Benutzer auswirken würde.

Der pauschalen rechtlichen Gleichstellung von handschriftlicher Unterschrift und elektronischer Signatur werden oft die unterschiedlichen Merkmale und die verschiedene Art und Weise des Zustandekommens entgegengehalten. In der Tat bestehen zwischen beiden Formen der Unterschrift einige Unterschiede: Zum Beispiel ist bei digital unterzeichneten Dokumenten – im Gegensatz zu traditionell unterzeichneten Dokumenten – eine Unterscheidung zwischen Original und Kopie nicht ohne weiteres möglich. Vielmehr können Originale in beliebiger Anzahl hergestellt werden. Ein weiterer Unterschied ist darin zu sehen, daß jede natürliche Person nur eine eigenhändige Unterschrift hat. Aufgrund der spezifischen Art und Weise der Generierung kann aber eine elektronische Signatur jedes Mal anders aussehen. Es geht also nicht um eine ganz bestimmte charakteristische Signatur – wie etwa bei einem eigenhändigen Schriftzug – sondern vielmehr um den Besitz an einer bestimmten Signaturerstellungseinheit (z.B. dem privaten Schlüssel) mit dem die Signatur generiert werden kann. Eine Person kann auch über mehrere solcher Einheiten für elektronische Signaturen verfügen. Andererseits bieten

elektronische Signaturen – verglichen mit eigenhändigen Unterschriften – ein sehr hohes Maß an Fälschungssicherheit.

Diese Unterschiede zwischen traditioneller Unterschrift und elektronischen Signaturen schließen aber nicht aus, daß elektronische Signaturen in bestimmten materiell-rechtlichen bzw. prozessualen Rechtswirkungen traditionellen Unterschriften gleichgesetzt werden können.

Die Richtlinie legt deshalb fest, daß elektronische Signaturen, die bestimmten Mindestanforderungen genügen, die rechtliche Voraussetzung einer eigenhändigen Unterschrift erfüllen. Voraussetzung ist, daß sie auf einem sog. qualifizierten Zertifikat basieren und von einem „sicheren" Produkt erstellt sind. Diese Regelung, die sich auf eine sog. „fortgeschrittene" elektronische Signatur stützt, soll insbesondere in denjenigen Bereichen des nationalen Rechts Anwendung finden, in denen Schriftformerfordernisse bestehen.

Um die allgemeine Akzeptanz elektronischer Signaturen zu fördern, enthält die Richtlinie ein „Diskriminierungsverbot", welches den Mitgliedstaaten unter anderem untersagt, einer Unterschrift die Rechtsgültigkeit allein deshalb abzusprechen, weil sie in elektronischer Form vorliegt.

2.5 Haftung

Klare und europaweit einheitliche Haftungsregelungen sind für die Steigerung der Akzeptanz von Dienstleistungen der Zertifizierungsdiensteanbieter entscheidend und wichtig für die Bildung von Vertrauen bei Verbrauchern und Diensteanbietern. Besondere Bedeutung kommt dabei dem Verhältnis zwischen Zertifizierungsdiensteanbieter und einem Dritten zu, der auf die Gültigkeit und Richtigkeit eines Zertifikates vertraut, z.B. dem Empfänger einer elektronisch unterzeichneten Nachricht. Zwischen diesen beiden Parteien bestehen in der Regel keine vertraglichen Beziehungen. Die Richtlinie legt deshalb fest, daß Zertifizierungsdiensteanbieter, die ein Zertifikat als qualifiziertes Zertifikat öffentlich ausstellen, gegenüber jeder Person, die vernünftigerweise auf das Zertifikat vertraut, insbesondere dafür haften, daß alle Informationen im qualifizierten Zertifikat zum Zeitpunkt seiner Ausstellung richtig sind.

Zertifizierungsdiensteanbieter sollen aber nicht unbeschränkt haften. Sie haben die Möglichkeit, den Anwendungsbereich von Zertifikaten und den Wert der Transaktionen zu begrenzen, für die ein Zertifikat gültig ist. Die Zertifizierungsdiensteanbieter haftet in diesen Fällen nicht für Schäden, die sich aus einer über den Anwendungsbereich oder die Höchstgrenze hinausgehenden Nutzung eines Zertifikats ergeben.

2.6 Verkehr mit Drittstaaten

Kooperative Mechanismen, die die grenzüberschreitende Anerkennung von Signaturen und Zertifikaten im Verkehr mit Drittstaaten fördern, sind für die Entwicklung des internationalen elektronischen Geschäftsverkehrs von zentraler Bedeutung. Zunächst ist Artikel 5 Absatz 2 der Richtlinie anwendbar, das heißt, daß elektronische Unterschriften, die auf einem Zertifikat eines Zertifizierungsdiensteanbieter aus einem Staat außerhalb der EU stammen, rechtlich nicht diskriminiert werden dürfen. Darüber hinaus sieht Artikel 7 für den Bereich der Formvorschriften vor, daß Zertifikate, die von einem Zertifizierungsdiensteanbieter eines Drittstaates ausgestellt werden, den von einer in der Gemeinschaft niedergelassenen Zertifizierungsdiensteanbieter ausgestellten Zertifikaten unter bestimmten Voraussetzungen rechtlich gleichgestellt werden. Die Richtlinie sieht hier drei verschiedene Möglichkeiten vor:

- Der Zertifizierungsdiensteanbieter erfüllt die Anforderungen der Richtlinie und ist im Rahmen eines freiwilligen Akkreditierungssystems eines Mitgliedstaates akkreditiert.
- Ein in der Gemeinschaft niedergelassener Zertifizierungsdiensteanbieter, der die Anforderungen dieser Richtlinie erfüllt, steht für das Zertifikat ein.
- Das Zertifikat oder der Zertifizierungsdiensteanbieter ist im Rahmen einer bilateralen oder multilateralen Vereinbarung zwischen der Gemeinschaft und Drittländern oder internationalen Organisationen anerkannt.

2.7 Standardisierung

Es ist davon auszugehen, daß die Industrie in Zusammenarbeit mit Normungsgremien die Vorreiterrolle bei der Entwicklung international abgestimmter Normen für elektronische Signaturen übernehmen wird. Dabei sollte der Schwerpunkt auf der Schaffung einer offenen Umgebung für interoperable Produkte und Dienste liegen. Die Kommission fördert eine solche Entwicklung[7]. Gemäß Artikel 9 der Richtlinie kann die Kommission Referenznummern für allgemein anerkannte Normen für elektronische Signaturprodukte festlegen und im Amtsblatt der Europäischen Gemeinschaften veröffentlichen. Entspricht ein elektronisches Si-

[7] siehe dazu: European Electronic Signature Standardisation Initiative (EESSI) – http://www.ict.etsi.org/

gnaturprodukt diesen Normen, so ist davon auszugehen, daß deren Anforderungen durch dieses Produkt erfüllt werden.

2.8 Datenschutz

Die Richtlinie legt in Artikel 8 fest, daß Zertifizierungsdiensteanbieter, die öffentlich Zertifikate ausstellen, personenbezogene Daten nur unmittelbar von der betroffenen Person oder mit ausdrücklicher Zustimmung der betroffenen Person einholen können. Dies darf auch nur insoweit geschehen, als dies zur Ausstellung und Aufrechterhaltung des Zertifikats erforderlich ist. Ferner dürfen die Daten ohne ausdrückliche Zustimmung der betroffenen Person nicht für anderweitige Zwecke erfaßt oder verarbeitet werden.

Außerdem steht es nach der Richtlinie Zertifizierungsdiensteanbietern frei, im Zertifikat ein Pseudonym anstelle des Namens des Unterzeichners anzugeben. Damit soll es Benutzern ermöglicht werden, Transaktionen zu tätigen und zu kommunizieren ohne ihre Anonymität aufgeben zu müssen (der Unterzeichner ist nur dem Zertifizierungsdiensteanbieter bekannt) wahrt. Andernfalls könnten elektronische Signaturen als wirksames Instrument mißbraucht werden, um On-Line Benutzungsgewohnheiten und Kommunikation zu verfolgen.

Ein weiterer Belang, der den Schutz der Privatsphäre und Datensicherheit betrifft, rührt von der Notwendigkeit her, daß elektronische Signaturen einzigartig und vertraulich sein müssen, um das Risiko des "Identitätsdiebstahls" und der Fälschung von Daten zu minimieren. Anhang II der Richtlinie verbietet deshalb Zertifizierungsdiensteanbietern, private Schlüssel zu kopieren oder aufzubewahren.