Das Signaturgesetz

Christoph Brenn

Bundesministerium für Justiz
1070 Wien, Museumstraße 7
christoph.brenn@bmj.gv.at

Schlagworte: Elekronische Signatur, Rechtswirkungen, Unterschriftenersatz, Haftung, Zertifikate, Sicherheitsanforderungen, Sicherheitsbescheinigung, Aufsicht, Zertifizierungsdiensteanbieter.

Abstract: Das auf der europarechtlichen Signaturrichtlinie basierende österreichische Signaturgesetz ist am 1.1.2000 in Kraft getreten. Das Signaturgestz legt die technischen Sicherheitsanforderungen für die Erstellung sicherer elektronischer Signaturen fest und statuiert die organisatorischen und personellen Anforderungen an Zertifizierungsdiensteanbieter, die sichere Signaturverfahren bereitstellen. Weiters regelt das Signaturgesetz die Rechtswirkungen elektronischer Signaturen. Es bestimmt, dass die sichere elektronische Signatur in ihren Rechtswirkungen – abgesehen von abschließend genannten Ausnahmen – der eigenhändigen Unterschrift gleichgestellt ist und konkretisiert die Haftung der Zertifizierungsdiensteanbieter. Für einfache Signaturverfahren wird bestimmt, dass sie im Geschäftsverkeht und als Beweismittel zugelassen werden müssen. Zertifizierungsdiensteanbieter werden einem effektiven Aufsichtssystem unterstellt.

1. Grundlagen

Das Signaturgesetz, das auf der gemeinschaftsrechtlichen Signaturrichtlinie (Richtlinie 99/93/EG vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. L 13 vom 19.1.2000, S. 12) basiert, wurde am 14.7.1999 vom Nationalrat einstimmig beschlossen und am 19.8.1999 im Bundesgesetzblatt (BGBl. I Nr. 190/1999) kundgemacht. Österreich hat damit als erster Mitgliedstaat der Europäischen Union die Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen umgesetzt. Das Signaturgesetz ist am 1.1.2000 in Kraft getreten. Am 2.2.2000 wurde die Signaturverordnung kundgemacht (BGBl. II Nr. 30/2000), mit der insbesondere die technischen Sicherheitsanforderungen für sichere elektronische Signaturen sowie die technischen, organisatorischen und personellen Anforderungen an Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, konkretisiert werden.

2. Vertrauen und Sicherheit

Eine unerläßliche Voraussetzung für den Einsatz und den weiteren Erfolg elektronischer Medien im Rechts- und Geschäftsverkehrs *über offene Netzwerke* bildet das *Vertrauen* der beteiligten Akteure, also der Anbieter und Kunden ebenso wie der öffentlichen Hand und ihrer Ansprechpartner, in die elektronischen Informations-, Kommunikations- und Lieferkanäle. Sie müssen die neuen Dienste letztlich auch in rechtlicher Hinsicht – vertrauensvoll in Anspruch nehmen können. Grundlage dieses Vertrauens in die elektronischen Netze und Instrumente ist die Sicherstellung der *Identität* der an den Kommunikationsabläufen bzw den rechtlichen und wirtschaftlichen Transaktionen beteiligten Kommunikations- und Geschäftspartner. Die neuen elektronischen Medien können ihre Vorteile in vielen, zum Teil außerordentlich sensiblen Bereichen erst dann voll entfalten, wenn die Anwender die Möglichkeit haben, sich über die Identität ihres Gegenübers verläßlich und rasch zu informieren. Weiters müssen sie sich darauf verlassen können, daß die elektronischen Daten auf dem Weg von und zu ihnen nicht unerkannt verändert und verfälscht werden.

Das *Signaturgesetz* schafft die notwendige technische und rechtliche Sicherheit für die elektronische Kommunikation und ist somit Voraussetzung für die Entwicklung des elektronischen Rechts- und Geschäftsverkehrs.

3. Wesentlicher Inhalt

3.1 Elektronische Signaturen

Mit dem Signaturgesetz werden die gesetzlichen Grundlagen für die Bereitstellung von Signatur- und Zertifizierungsdiensten sowie die Verwendung elektronischer Signaturverfahren im Internet und in anderen elektronischen Netzwerken geschaffen. Elektronische Signaturen stellen besondere technische Verfahren dar, mit deren Hilfe elektronische Dokumente einem bestimmten Rechtssubjekt zugeordnet werden können. Entsprechend den Vorgaben der Signaturrichtlinie wird für den rechtlichen Rahmen ein *technologieneutraler* Ansatz gewählt. Aus diesem Grund verwendet das Signaturgesetz stets den Begriff „elektronische Signaturen". Dabei handelt es sich um technische Verfahren, mit deren Hilfe festgestellt werden kann, dass eine signierte elektronische Nachricht von einer bestimmten Person stammt und während des Datentransports zum Empfänger nicht verändert wurde. Elektronische Signaturen stellen also *Authentizität* (Echtheit) und *Integrität* (Unverfälschtheit) elektroni-

scher Daten sicher. Die bedeutendste Anwendungsart solcher Technologien ist die digitale Signatur, die auf der asymetrischen Verschlüsselung einer für den Dokumenteninhalt repräsentativen Datenkombination (Hash-wert) beruht.

3.2 Anwendungsbereich

Das Signaturgesetz gilt für *geschlossene Systeme* nur dann, wenn dies von den Teilnehmern des Systems vereinbart wird. Im geschlossenen System gelangt somit die Privatautonomie zum Tragen. Wenn sich ein geschlossenes System den Regelungen des Signaturgesetzes unterwirft, so können auch die besonderen Rechtswirkungen sicherer elektronischer Signaturen (§ 4 SigG) in Anspruch genommen werden. Im *öffentlichen Bereich* (Kommunikationsverkehr mit Gerichten und anderen Behörden) gelangt das Signaturgesetz grundsätzlich (mangels anders lautender gesetzlicher Anordnung) zur Anwendung. Von diesem Gesetzesvorbehalt, der im Einklang mit Art. 3 Abs. 7 der Signaturrichtlinie vorgesehen wurde, soll nach Möglichkeit nicht Gebrauch gemacht werden. In einer Feststellung des Justizausschusses wird dazu zum Ausdruck gebracht, dass auch im öffentlichen Bereich das Signaturgesetz, also keine zusätzlichen Anforderungen, gelten soll.

3.3 Definitionen

Die *Definitionen* werden im Wesentlichen aus der Signaturrichtlinie übernommen. Der berechtigte Inhaber bestimmter Signaturerstellungsdaten (eines bestimmten privaten Signaturschlüssels) wird „Signator" genannt. Im Einklang mit der Signaturrichtlinie kann grundsätzlich nur eine natürliche Person „Signator" sein. Eine Ausnahme besteht nur für die sogenannten „Zertifikate für Zertifizierungsdiensteanbieter" (§ 6 Abs 7 SigG). Diese Zertifikate dürfen nur für die Erbringung von Zertifizierungsdiensten (Signieren der ausgestellten Zertifikate, Signieren der Verzeichnis- und Widerrufsdienste) verwendet werden.

3.4 Rechtswirkungen

3.4.1 Allgemeine Rechtswirkungen

Elektronische Signaturen sind im *Rechts- und Geschäftsverkehr* verwendbar. Voraussetzung ist aber, dass die elektronische Kommunikation an sich (auf Grund einer gesetzlichen Regelung oder einer Vereinbarung

zwischen den Parteien) zulässig ist. Von den Zertifizierungsdiensteanbietern können somit unterschiedliche Sicherheitsstufen und Zertifikatsklassen angeboten werden. Sie müssen die von ihnen bereitgestellten Signaturverfahren allerdings in einem Sicherheits- und Zertifizierungskonzept genau darstellen. Dieses Konzept ist Grundlage für die Durchführung der Aufsicht. Für jedes Signaturverfahren besteht das Gebot zur Nichtdiskriminierung im Sinne des Art. 5 Abs. 2 Signaturrichtlinie.

3.4.2 Besondere Rechtswirkungen

Für sogenannte „sichere elektronische Signaturen" (das sind Signaturen im Sinne des Art. 5 Abs. 1 der Signaturrichtlinie) sind *besondere Rechtswirkungen* vorgesehen. Solche sicheren elektronischen Signaturen sind der eigenhändigen Unterschrift gleichgestellt und können somit die einfache Schriftform und jedes andere Unterschriftserfordernis erfüllen. Ausnahmen bestehen – im Sinne des Art. 9 Abs. 2 des Gemeinsamen Standpunkts im Hinblick auf den Erlass der Richtlinie über den elektronischen Geschäftsverkehr – nur für Bürgschaften von Nichtkaufleuten, Rechtsgeschäfte, die zu ihrer Wirksamkeit oder zu ihrer Eintragung in ein öffentliches Register der Mitwirkung eines Notars oder eines Gerichts bedürfen (sogenannte öffentliche Form) sowie Schriftformerfordernisse im Erb- und Familienrecht. In beweisrechtlicher Hinsicht sind sicher elektronisch signierte Dokumente den eigenhändig unterschriebenen Privaturkunden gleichgestellt. Dies bedeutet, dass für den Inhalt der Erklärung eine qualifizierte Echtheitsvermutung besteht. Weiters besteht eine Sicherheitsvermutung für sichere elektronische Signaturverfahren.

3.5 Sichere elektronische Signatur

Eine sichere elektronische Signatur erfordert neben einem qualifizierten Zertifikat (§ 5 und § 7 SigG) eine Sicherheitsbescheinigung einer Bestätigungsstelle (§ 18 Abs 5 SigG). Die Aufgabe dieser Bestätigungsstellen (siehe auch Art 3 Abs 4 der Signaturrichtlinie) besteht in der Beurteilung, ob die Anforderungen des Anhangs III zur Signaturrichtlinie (§ 18 Abs 1 und 2 SigG) von den technischen Komponenten und Verfahren für die Erstellung sicherer elektronischer Signaturen eingehalten werden. In Konkretisierung des Anhangs III zur Signaturrichtlinie wird in der Signaturverordnung unter anderem angeordnet, dass nur Datenformate verwendet werden dürfen, deren Spezifikation verfügbar ist. Dynamische Veränderungen oder Unsichtbarkeiten müssen ausgeschlossen werden können. Die Autorisierungscodes (zB PIN) müssen so gestaltet sein, dass

ihr unbefugtes Erfahren ausgeschlossen ist. Für unterschiedliche Applikationen müssen unterschiedliche Autorisierungscodes verwendet werden.

3.6 Zertifizierungsdiensteanbieter

Das *Personal* des Zertifizierungsdiensteanbieters muss zuverlässig sein. Dies bedeutet, dass keine Verurteilung von mehr als einem Jahr bzw von mehr als drei Monaten bei Delikten gegen das Vermögen oder gegen Urkunden und Beweiszeichen vorliegen darf. Das Personal muss über einschlägiges Fachwissen verfügen. Die entsprechende Ausbildung muss ein Jahr betragen haben; diese Ausbildung kann durch eine fachlich einschlägige Tätigkeit in der Dauer von drei Jahren ersetzt werden. Das *Mindestkapital* eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt, muss 300.000 Euro betragen. Zudem muss ein solcher Zertifizierungsdiensteanbieter eine obligatorische Haftpflichtversicherung abschließen, wobei die Mindestversicherungssumme eine Million Euro betragen muss.

Für die *Erzeugung und Speicherung* von Signaturerstellungsdaten sowie für die Erstellung und Speicherung von qualifizierten Zertifikaten dürfen nur technische Komponenten und Verfahren eingesetzt werden, die von einer Bestätigungsstelle als geeignet beurteilt werden (§ 7 Abs 2 SigG). Insbesondere muss die Fälschung oder Verfälschung von Signaturen bzw Zertifikaten ausgeschlossen sein.

Im Sinne der Signaturrichtlinie ist eine gesonderte *Genehmigung* für die Aufnahme der Tätigkeit als Zertifizierungsdiensteanbieter nicht erforderlich. Die Aufnahme der Tätigkeit muss allerdings der Aufsichtsstelle angezeigt werden. Dabei ist ein Sicherheits- und Zertifizierungskonzept vorzulegen, in dem die technischen, personellen und finanziellen Mittel darzulegen und die Art der Diensteerbringung beschrieben werden muss. Außerdem müssen der Aufsichtsstelle auch alle sicherheitsrelevanten Veränderungen des Sicherheits- und Zertifizierungskonzepts angezeigt werden.

3.7 Zertifikate

Bei der *Ausstellung* von qualifizierten Zertifikaten muss die Identität des Signators zuverlässig festgestellt werden. Dafür ist die Vorlage eines amtlichen Lichtbildausweises erforderlich. Die Entgegennahme des Antrags sowie die Identitätsprüfung kann auch von einer Registrierungsstelle vorgenommen werden. Die Aufsicht muss auch über derartige Stellen

gesichert sein. Soll eine Vertretungsmacht oder sonstige besondere Eigenschaft des Signators in das Zertifikat aufgenommen werden, so müssen auch diese Umstände zuverlässig nachgewiesen sein. Die Widerrufsdienste müssen während der Geschäftszeiten innerhalb von drei Stunden aktualisiert werden. Außerhalb der Geschäftszeiten (insbesondere in der Nacht) muss zumindest eine jederzeitige automatisierte Sperre der qualifizierten Zertifikate möglich sein.

Die *Widerrufsdienste* müssen zudem rund um die Uhr verfügbar sein, die Verzeichnisdienste während der Geschäftszeiten. Eine Sperre darf höchstens drei Werktage bestehen bleiben. Nach Ablauf dieser Frist ist zu entscheiden, ob die Sperre aufgehoben oder das Zertifikat endgültig widerrufen wird.

3.8 Aufsicht

Aufsichtsstelle ist die Telekom-Control-Kommission. Dabei handelt es sich um eine Kollegialbehörde mit richterlichem Einschlag. Die Aufsichtsstelle hat insbesondere zu prüfen, ob von den Zertifizierungsdiensteanbietern deren Sicherheits- und Zertifizierungskonzepte eingehalten werden. Weiters hat die Aufsichtsstelle Verzeichnisse der gültigen, gesperrten und widerrufenen Zertifikate für Zertifizierungsdiensteanbieter, der im Inland niedergelassenen Zertifizierungsdiensteanbieter, der akkreditierten Zertifizierungsdiensteanbieter sowie der Drittstaatenzertifizierungsdiensteanbieter, für deren Zertifikate ein inländischer Zertifizierungsdiensteanbieter einsteht (§ 24 SigG), zu führen. Die Aufsichtsstelle kann gegen Zertifizierungsdiensteanbieter die unterschiedlichsten Maßnahmen bis hin zur Untersagung ihrer Tätigkeit ergreifen. Wird die Tätigkeit eines Zertifizierungsdiensteanbieters untersagt oder wird die Tätigkeit vom Zertifizierungsdiensteanbieter aus eigener Veranlassung eingestellt, so müssen entweder die Verzeichnis- und Widerrufsdienste von einem anderen Zertifizierungsdiensteanbieter fortgeführt oder die Zertifikate des Zertifizierungsdiensteanbieters sowie aller Signatoren widerrufen werden. Auch im Falle eines solchen Widerrufs der Zertifikate hat die Aufsichtsstelle für die Weiterführung zumindest der Widerrufsdienste Sorge zu tragen.

3.9 Signatoren

Auch die *Pflichten* der Signatoren werden ausdrücklich festgelegt. Diese haben ihre Signaturerstellungsdaten sorgfältig zu verwahren, Zugriffe darauf zu verhindern und deren Weitergabe zu unterlassen. Wenn

den Signatoren die Signaturerstellungsdaten abhanden kommen oder sie Anhaltspunkte für deren Kompromittierung haben, müssen sie unverzüglich den Widerruf des Zertifikats veranlassen.

3.10 Haftung

Im Sinne der Signaturrichtlinie wird für die Haftung von Zertifizierungsdiensteanbietern, die qualifizierte Zertifikate ausstellen, eine Sonderregelung vorgesehen (§ 23 SigG). Bei dieser Haftung handelt es sich um eine Verschuldenshaftung mit Umkehr der Beweislast zu Lasten der Zertifizierungsdiensteanbieter. Diese haben im Wesentlichen dafür einzustehen, dass die Angaben im Zertifikat zum Zeitpunkt der Ausstellung richtig sind. Darüber hinaus haften die Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, für die ordnungsgemäße Führung der Widerrufsdienste sowie für die Einhaltung der Anforderungen des § 7 SigG (Anhang II zur Signaturrichtlinie). Zertifizierungsdiensteanbieter, die sichere elektronische Signaturverfahren bereitstellen, haften auch dafür, dass die von ihnen den Signatoren bereitgestellten oder empfohlenen Signaturprodukte den technischen Anforderungen des § 18 SigG (Anhang III zur Signaturrichtlinie) entsprechen und für diese Signaturprodukte („sichere Signaturerstellungseinheiten") Sicherheitsbescheinigungen einer Bestätigungsstelle vorliegen. Der Zertifizierungsdiensteanbieter trägt die Beweislast dafür, dass ihn und seine Leute an der Herbeiführung des Schadens kein Verschulden trifft. Zudem wird eine Verursachungsvermutung zu Gunsten der Geschädigten normiert. Können Sie eine Pflichtverletzung des Zertifizierungsdiensteanbieters als wahrscheinlich dartun, so wird vermutet, dass diese Pflichtverletzung für den Schadenseintritt kausal war. Der in Anspruch genommene Zertifizierungsdiensteanbieter kann diese Vermutung entkräften.

3.11 Gegenseitige Anerkennung

Schließlich wird eine *Anerkennungsregelung* für ausländische Zertifikate vorgesehen (§ 24 SigG). Zertifikate, die von Zertifizierungsdiensteanbietern aus anderen EU-Staaten ausgestellt werden, entfachen dieselben Rechtswirkungen wie jene der inländischen Zertifizierungsdiensteanbieter. Für qualifizierte Zertifikate, die von Zertifizierungsdiensteanbietern aus Drittstaaten ausgestellt werden, wird im Sinne des Art. 7 der Signaturrichtlinie deren Anerkennung detailliert geregelt. Voraussetzung für die Anerkennung ausländischer Zertifikate ist, dass sie vom Inland aus über-

prüft werden können. Dies bedeutet, dass die Verzeichnis- und Widerrufsdienste vom Inland aus zugänglich sein müssen.

Bei Nichteinhaltung der im Gesetz vorgesehenen, wesentlichen Verhaltenspflichten, insbesondere für Zertifizierungsdiensteanbieter, sind Verwaltungsstrafbestimmungen vorgesehen.

4. Signaturverordnung

Die Verordnung regelt zunächst die Gebühren für die Aufsichtstätigkeiten. Weiters wird in der Verordnung die finanzielle Ausstattung der Zertifizierungsdiensteanbieter konkretisiert. Für die Erstellung und die Verwendung sicherer elektronischer Signaturen müssen sichere Signaturprodukte (Anhang III zur Richtlinie bzw § 18 SigG), also geeignete technische Komponenten und Verfahren, zur Verfügung stehen. Die Verordnung konkretisiert die allgemeinen Sicherheitskriterien des Signaturgesetzes für sichere elektronische Signaturverfahren (§ 7 Abs 2, § 10 und § 18 SigG). Schließlich legt sie die betriebsorganisatorischen Abläufe für die Erbringung sicherer Signatur- und Zertifizierungsdienste sowie für die Ausstellung qualifizierter Zertifikate fest. Die konkrete Ausgestaltung dieser Rahmenbedingungen bleibt dem Sicherheits- und Zertifizierungskonzept der Zertifizierungsdiensteanbieter vorbehalten.

Literatur

Brenn, Signaturgesetz, Manz 1999

Brenn, Das Signaturgesetz, Unterschriftenersatz in elektronischen Netzwerken, ÖJZ 1999

Brenn, Richtlinie über den elektronischen Geschäftsverkehr, ÖJZ 1999