REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES

1014 WIEN, Postfach 100

[illegible]
Bei Beantwortung bitte angeben
5000/2033-IV/11/d/99

Wien, am 2. Juni 1999
Referent: Holubar
Kl.: 2433

Entwurf eines Bundesgesetzes über elektronische Signaturen; Stellungnahme

An das

Präsidium des Nationalrates

Parlament
1017 WIEN

Neue Ref

In der Anlage werden 25 Ausfertigungen der Stellungnahme des Bundesministeriums für Inneres zu dem im Betreff bezeichneten Entwurf übermittelt.

Beilagen

Für den Bundesminister:
Holubar

Für die Richtigkeit
der Ausfertigung:

REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES

1014 WIEN, Postfach 100

DVR: 0000051
Bei Beantwortung bitte angeben
5000/2033-IV/11/d/99

Wien, am 2. Juni 1999
Referent: Holubar
Kl.: 2433

Entwurf eines Bundesgesetzes über
elektronische Signaturen;
Stellungnahme

An das

Bundesministerium für Justiz

Museumstraße 7
1070 W I E N

Zu Zl. 7.051C/50-I.2/1999

Aus der Sicht des Bundesministeriums für Inneres ergeben sich zu dem im Betreff bezeichneten Entwurf folgende Bemerkungen:

I. Allgemeines

Der vorliegende Entwurf unterscheidet - in Übereinstimmung mit dem Text der bezughabenden (provisorischen) EU-Richtlinie - zwischen „sicheren" und „unsicheren" Signaturen sowie zwischen „Zertifikaten" und „qualifizierten Zertifikaten". Dieser Unterscheidung liegt die Intention zugrunde, die derzeit bestehenden - nicht unter die sicheren Signatursysteme zu subsumierenden - elektronischen Signatursysteme nicht verbieten zu müssen. Allerdings wird auf diese Weise ein System geschaffen, das für den Konsumenten Unsicherheiten mit sich bringt und nach Dafürhalten des Innenressorts nicht der Intention der Gewährleistung eines sicheren, elektronischen Geschäftsverkehrs gerecht wird.

Der Entwurfstext ist in vielen Bereichen schwer lesbar und enthält zahlreiche nicht ausreichend determinierte Begriffe. Der Text könnte durch Einfügung entsprechender Verweise klarer und besser lesbar gestaltet werden. Für einen wirtschaftlich hoch entwickelten Staat wie Österreich hat der gute Ruf seines Wirtschaftssystems einen entsprechend hohen volkswirtschaftlichen Stellenwert. Mit der Zulassung nicht qualifizierter Zertifikate (§ 2 Z 8) bzw. „unsicherer Signaturen" (§ 2 Z 1) könnte Rechtsunsicherheit und letztlich ein nicht zu unterschätzender volkswirtschaftlicher Schaden verknüpft sein. Aus diesem Grunde sollte im Gesetzestext vorgesehen werden, daß - nach Ablauf einer mehrjährigen Übergangsfrist - die der Anpassung der bestehenden inkompatiblen Systeme dienen soll - nur noch die Verwendung von sicheren Signaturen und qualifizierten Zertifikaten - zulässig ist.

Parallel hiezu sollte Österreich auf eine den angeführten Gesichtspunkten Rechnung tragende analoge Überarbeitung und Modifizierung des Textes des Richtlinienentwurfes hinwirken. Sollten diese Bemühungen nicht erfolgreich sein, wäre zumindest im Gesetzestext eine für den Konsumenten besser ersichtliche und leichter nachvollziehbare Abgrenzung zwischen sicheren und unsicheren Systemen festzulegen. Insbesonders das Fehlen jeglicher Strafbestimmungen erscheint dem Bundesministerium für Inneres äußerst bedenklich. Es erscheint unbedingt erforderlich, die Nichteinhaltung bestimmter, im Entwurfstext vorgeschriebener, Pflichten unter Strafandrohung zu stellen. Die in §§ 14 Abs 2 und 6 vorgesehenen Sanktionen vermögen den gebotenen Anforderungen in keiner Weise gerecht zu werden. Die Unterlassung der Anzeige- und Widerrufspflicht (vgl. §§ 6 und 9 des Entwurfes), die Nichteinhaltung der Bestimmungen, betreffend die Dokumentation (§ 11) sowie die mißbräuchliche Verwendung einer elektronischen Signatur oder eines Zeitstempels, sollten mit einer Verwaltungsstrafsanktion verknüpft werden. Im Hinblick darauf, daß Firmengründungen im Bereich der organisierten Kriminalität (unter anderem auch) zur Ermöglichung des Anbietens von Signaturverfahren nicht ausgeschlossen werden können, sollte der Strafrahmen entsprechend hoch (etwa in Analogie zu § 104 Abs 3 Telekommunikationsgesetz) bemessen werden und auch eine analog zu § 104 Abs 5 TKG gestaltete Regelung in den Gesetzestext aufgenommen werden.

Unter Bedachtnahme auf den Gesichtspunkt der Generalprävention erschiene auch die Normierung eines gerichtlich strafbaren Tatbestandes für die angeführten mißbräuchlichen Verwendungen durchaus vorteilhaft.

Im übrigen bleibt unklar, inwieweit in Hinkunft elektronisch signierte Dokumente auch als Urkunde im Sinne des § 74 Z 7 StGB anzusehen wären und damit auch der qualifizierte Tatbestand nach § 147 Abs 1 Z 1 StGB verknüpft wäre.

Sofern die angeführten elektronisch signierten Dokumente nicht als Urkunde anzusehen sein, erscheint es jedenfalls dringend erforderlich, das StGB entsprechend zu adaptieren.

II. Zu den einzelnen Bestimmungen des Entwurfes ergeben sich folgende Bemerkungen:

Zu § 2

In der aktuellen Fachliteratur zum Datenrecht wird unter dem Begriff einer elektronischen Signatur ein Mechanismus verstanden, der die Authenzität sowie die Integrität einer elektronischen Nachricht gewährleisten soll. Der Entwurf ordnet dem Begriff einer „elektronischen Signatur" jedoch bloß die Bedeutung einer der Authentifizierung dienenden Technologie zu, während die Integrität erst vom Begriff einer „sicheren elektronischen Signatur" (Z 3d) mitfaßt. Im Interesse einer besseren begrifflichen Unterscheidbarkeit erscheint es vorteilhaft, den Terminus der einfachen (somit nicht sicheren) elektronischen Signatur anders zu nennen.

Im übrigen sollten wohl auch die Begriffe „Zertifikatswerber" (vgl. §§ 5 Abs 1 Z 4 und Abs 2 sowie 20 des Entwurfes), „Zeitstempel" (§ 7 Abs 1 Z 3) „Pseudonym" (§ 22 Abs 2) in den Definitionsstrafkatalog aufgenommen werden.

Zu § 2 Z 3 lit b

Eine „sichere elektronisch Signatur" liegt wohl nur dann vor, wenn der Signator jedenfalls identifiziert wird. Das im Entwurfstext verwendete Wort „kann" könnte zu Mißverständnissen Anlaß geben.

Zu § 2 Z 5 und § 2 Z 7

Es wird angeregt, diese Begriffsdefinition folgendermaßen zu modifizieren: „Eine zur Verarbeitung der Signaturerstellungsdaten konfigurierte Software- oder Hardware-Einheit". Auf diese Weise sollte die Interpretation, wonach eine beliebige Software, sofern sie nur

konfiguriert ist, unter diesen Begriff subsumiert werden kann, somit also auch wenn sie nicht eigens für diesen Zweck bestimmt war, ausgeschlossen werden.

Zu § 2 Z 8

Durch eine „Zertifizierung" soll generell das Vorliegen eines bestimmten Qualitätsstandards, im speziellen Fall eines Sicherheitsstandards, gewährleistet werden. Ein (einfaches, somit nicht qualifiziertes) Zertifikat erweckt durch seine Bezeichnung zwar den Eindruck der Gewährleistung des Vorliegens der entsprechenden Sicherheitsanforderungen, wird diesem Anspruch - tatsächlich - aber nicht gerecht. Es wird daher angeregt, diesen Begriff im Interesse einer deutlichen Abgrenzung umzubenennen.

Zu § 4 Abs 1

Im Zusammenhang mit dieser Bestimmung sollte überdacht werden, ob die im Entwurf vorgesehenen Einschränkungen nicht zu weitgehend gefaßt werden. Derzeit sind auch im Justizbereich intensive Bemühungen in Richtung „elektronischer Akt" im Gange. Der elektronische Rechtsverkehr nimmt - auch aufgrund der Anfang 1998 in Kraft getretenen Bestimmungen - immer umfangreichere Formen an. In nicht allzu ferner Zukunft wird wohl auch die Durchführung des Notariatsaktes in elektronischer Form angestrebt. Der vorliegende Entwurf sollte so gestaltet werden, daß eine Erweiterung im Anwendungsbereich des elektronischen Rechtsaktes keine allzu umfangreichen legistischen Adaptierungen erforderlich macht. So sollte auch für die Anwendung im Verwaltungsverfahren Vorsorge getroffen werden.

Zu § 4 Abs 4

Wenn zwei Vertragspartner (- sofern Schriftlichkeit vereinbart oder diese gesetzlich vorgesehen ist -) unter Zuhilfenahme elektronischer Signaturen einen Vertrag haben, abgeschlossen werden, so wird der Vertrag, sofern die Zertifizierungsstelle ein wesentliches Erfordernis nach dem in Aussicht genommenen Gesetz nicht erfüllt, mangels Schriftlichkeit zur bloßen Naturalobligation.

Eine derartige Konstellation erscheint - ungeachtet allfälliger Schadenersatzansprüche gegenüber der Zertifizierungsstelle für die vertragswillige Partei als unbillig. Somit stellt sich die

Frage, ob diese Bestimmung nicht doch etwas zu restriktiv formuliert wurde und nicht zumindest eine Interessensabwägung zwischen den Interessen der Vertragsparteien und den öffentlichen Interessen (hinsichtlich der Schwere der Verletzung der gegenständlichen Bestimmungen) auch in die Regelung miteinbezogen werden sollte.

Zu § 6 Abs 1 und i.V. mit § 18 Abs 1 und 5

Nach § 6 Abs 1 des Entwurfes bedarf die Aufnahme und Ausübung der Tätigkeiten eines Zertifizierungsdiensteanbieters keiner gesonderten Genehmigung. Diese Bestimmung steht in einem deutlichen Spannungsverhältnis zu § 18 Abs 1 und 5, zumal nach diesen Regelungen nur jene sicheren Signaturen angewendet werden dürfen, hinsichtlich derer die Bestätigungsstelle die Erfüllung der Sicherheitsanforderungen bescheinigt hätte. Aus diesem Grund sollte zumindest in § 6 Abs 2, 2. Satz des Entwurfes festgelegt werden, daß der Anbieter bei seiner Tätigkeitsaufnahme neben der dort bereits angeführten Unterlagen auch die genannte Bestätigung nach § 18 Abs 5 des Entwurfes der Aufsichtsstelle vorzulegen hat. Im übrigen kann dem Entwurf auch nicht entnommen werden, welches Verfahren die Aufsichtsstelle, im Rahmen ihrer Bescheinigungs- und Entgeltsvorschreibungstätigkeit (§§ 18 Abs 5 und 19 Abs 6 des Entwurfes) anzuwenden hätte.

Es erscheint auch durchaus denkbar, daß die Ausstellung einer Bescheinigung (wohl auch mittels Bescheides) zu verweigern wäre, wobei allerdings eine Regelung über allfällige Beschwerdemöglichkeiten gegen eine ablehnende Entscheidung fehlt.

Zu § 6 Abs 2 und 3

Diese Bestimmung unterscheidet zwischen (einfachen) Zertifizierungsdiensteanbietern und solchen, die sichere elektronische Signaturen herstellen. Aus dem Gesamtkonzept des Entwurfes ist ersichtlich, daß die Möglichkeit besteht, Zertifikate mit sehr mangelhaften Sicherheitskriterien anzubieten. Unter Bedachtnahme darauf, daß nach Dafürhalten des Bundesministeriums für Inneres die Vergabe von qualifizierten Zertifikaten zum Mindeststandard des elektronischen Geschäftsverkehrs gehört, sollte die Einrichtung von Zertifizierungsdiensteanbietern, die keine qualifizierten Zertifikate vergeben, überdacht und möglichst aus dem Gesetzestext eliminiert werden. In diesem Zusammenhang wird nochmals auf die unter dem Punkt „Allgemeines" getroffenen Ausführungen hingewiesen.

Zu § 6 Abs 6

Eine Reihe unterschiedlicher Sicherheitsstufen sowie unterschiedlicher Zertifikatsklassen gestaltet den Markt für derartige Technologien unübersichtlich. Eine solche Entwicklung kommt einerseits Großunternehmen im EDV-Bereich zugute, die bereits einen entsprechenden, guten Ruf in der Branche haben, andererseits begünstigt ein unübersichtlicher Markt auch geschickt agierende Kleinunternehmen, die verlockt sein können, mit „Billigangeboten", die eine entsprechend unsichere Technologie aufweisen, auf dem Markt aufzutreten. Die Bestimmung des § 6 Abs 6 steht in der Praxis in einem sehr deutlichen Spannungsverhältnis zu den Interessen des Konsumentenschutzes an einen elektronischen Geschäftsverkehr mit ausreichend hohem Sicherheitsstandard und schadet letztlich auch den in Österreich für diesen Bereich zu etablierenden mittelständischen Unternehmen.

Zu § 7 Abs 1 Z 1 bzw. Abs 2 Z 1

In dieser Bestimmung sollten jene Erfordernisse genau umschrieben werden, die die Voraussetzung für das Vorliegen der Zuverlässigkeit eines Zertifizierungsdiensteanbieters bzw. dessen Personal darstellen. Insbesonders unter Bedachtnahme auf die sehr sensiblen Aufgabenstellungen der genannten Anbieter sollten entsprechend strenge Kriterien festgelegt werden. Soweit eine juristische Person als Zertifizierungsdiensteanbieter tätig wird, sollte festgelegt werden, daß die Anforderungen hinsichtlich der Zuverlässigkeit von der Person des jeweiligen Geschäftsführers erfüllt werden müssen.

Zu § 7 Abs 1 Z 5

Diese Bestimmung enthält nur Regelungen hinsichtlich der fachlichen Qualifikation des Personals. Im Hinblick darauf, daß gerade in diesem Bereich mit hochsensiblen, manipulierbaren Systemen und Daten gearbeitet wird, erscheint die Festlegung strenger Sicherheitskriterien für das in diesem Bereich zum Einsatz gelangende Personal ebenso wie die Normierung einer besonderen (verstärkten) Verantwortung des Zulassungsdiensteanbieters für sein Personal als unabdingbar notwendiges Erfordernis. Nach dem Entwurf wäre als einzige Sanktion bei der Verwendung „unzuverlässiger" Mitarbeiter nach § 14 Abs 2 Z 1 die Untersagung der Ausübung der Tätigkeit des Zertifizierungsdiensteanbieters bzw. die Erteilung von Auflagen (nach § 14

Abs 6) vorgesehen, die derzeit jedoch allein durch die Untersagung der Ausübung durchgesetzt werden könnten. Aus der Sicht des Bundesministeriums für Inneres erscheint die Schaffung einer Überprüfung des Vorliegens der Zuverlässigkeit, für die derzeit im übrigen jegliche inhaltliche Kriterien fehlen, unbedingt erforderlich. Der im Entwurf vorgesehenen Lösung, wonach die Aufsichtsbehörde bzw. ihre Hilfsorgane nur die fachliche Qualifikation, nicht jedoch das Vorliegen der Zuverlässigkeit überprüfen können, kann nicht zugestimmt werden.

Zu § 7 Abs 6

Die in dieser Bestimmung vorgesehene Prüfungspflicht der Zertifikationsdienstanbieter vermag nicht jenem Standard zu entsprechen, den die Sicherheitsbehörden bei der Wahrnehmung ihrer Aufgaben voraussetzen müßten. Es sollte daher eine Regelung geschaffen werden, wonach die Zertifizierungsdiensteanbieter zur Auskunftserteilung und Datenübermittlung gegenüber den Sicherheitsbehörden im Fall einer Gefahrenabwehr oder einer Ermittlungshandlung im Dienst der Strafjustiz verpflichtet werden. Die im Entwurf vorgesehene Bestimmung könnte sogar im Sinne einer Selbstprüfung - die jedoch nach den Erläuterungen nicht intendiert scheint - mißverstanden werden und sollte unbedingt durch eine Mitteilungs- und Offenlegungsverpflichtung ersetzt werden.

Zu § 8 Abs 1

Diese Bestimmung erscheint als zu unbestimmt formuliert und gibt nicht Aufschluß darüber, welche Mindestkriterien anzulegen sind. Im übrigen wird auch darauf hingewiesen, daß in den kommenden Jahren „finger print identification systems" immer größere Bedeutung erlangen werden und daher als zuverlässige Methode zur Identitätsfeststellung einer Person für ein qualifiziertes Zertifikat mitberücksichtigt werden sollten.

Zu § 8 Abs 4

Die Möglichkeit der Verwendung eines Pseudonyms widerspricht in hohem Maße den vom Bundesministerium für Inneres wahrzunehmenden Sicherheitsinteressen und sollte daher unzulässig sein. Es erscheint nicht nachvollziehbar, aus welchen Gründen im redlichen Geschäftsverkehr die Verwendung eines Pseudonyms für die Abwicklung von Rechtsgeschäften zu

rechtfertigen ist. In diesem Sinne sollte auch diesbezüglich auf eine Änderung des Richtlinientextes hingewirkt werden.

Zu § 11

Hinsichtlich der Dauer der Aufbewahrungspflicht erscheint ein Verweis auf die Signaturverordnung im Interesse einer klaren Gestaltung des Gesetzestextes vorteilhaft.

Zu 3 13 Abs 6

Es sollte klargestellt werden, daß auf das AVG in seiner jeweils geltenden Fassung hingewiesen werden.

Zu § 14 Abs 2 Z 1

Auch aus dieser Bestimmung geht nicht ausreichend hervor, welche Kriterien hinsichtlich der Zuverlässigkeit der Zertifizierungsdienstanbieter bzw. seines Personals zur Anwendung gelangen sollen.

Zu § 15 Abs 2 Z 1

Die Telekom Control GmbH kann das Personal auch hinsichtlich seiner fachlichen Qualifikation prüfen, eine Prüfung der Zuverlässigkeit ist nicht vorgesehen. Es stellt sich die Frage, wie nach § 14 Abs 2 Z 1 die Ausübung der Tätigkeit eines Zertifizierungsdiensteanbieters untersagt werden soll, wenn eine präventive Prüfung der Zuverlässigkeit nicht möglich ist. Im übrigen fehlen - wie bereits ausgeführt - jegliche Kriterien für die Durchführung einer Prüfung der Zuverlässigkeit.

Zu § 19

In Analogie zu § 13 sollte vorgesehen werden, daß nur eine Einrichtung als Aufsichtsstelle fungiert. Auf diese Weise könnte verhindert werden, daß sich ein Zertifizierungsdiensteanbieter - im Falle einer ablehnenden Entscheidung nach § 18 Abs 5 des Entwurfes durch eine Auf-

sichtsstelle mit seinem bereits einmal abgewiesenen Begehren an eine andere Aufsichtsstelle wenden.

Zu § 20

Der Zertifizierungsdiensteanbieter sollte zusätzlich verpflichtet werden, zumindest den Vor- und Familiennamen sowie die Anschrift des Zertifikatswerbers verläßlich festzustellen. Insbesonders im Hinblick auf die vorgesehene Zulässigkeit der Verwendung eines Pseudonyms (vgl. § 22 Abs 2) benötigen die Sicherheitsbehörden - bei Erfüllung ihrer sicherheits- und kriminalpolizeilichen Aufgaben - jedenfalls entsprechende Auskünfte über Personen, die - im Zusammenhang mit der Verwendung elektronischer Signaturen - in Verdacht stehen, einen gefährlichen Angriff oder eine gerichtlich strafbare Handlung begangen zu haben.

Im übrigen sollte die Prüfung der Frage, ob ein Dritter ein rechtliches Interesse im Sinne des § 20 Abs 2 hat, nicht durch den Zertifizierungsdiensteanbieter allein erfolgen, sondern auch die Aufsichtsstelle miteinbezogen werden.

Zu § 22

In Absatz 2 erscheint die Frage der Kostentragung für die Übermittlung der Daten nicht geklärt.

Zu der Wahrung der Interessen der Strafverfolgungsbehörden sollte folgender Absatz 3 eingefügt werden:

„Die Auskunfts- und Mitwirkungspflichten des Zertifizierungsdiensteanbieters gegenüber den gesetzlich ermächtigten Überwachungsbehörden im Rahmen der gesetzmäßigen Überwachung des Telekommunikationsverkehrs bleibt unberührt."

Zu § 23 Abs 1

Die vorgesehenen Haftungsbestimmungen gelten nur für den Fall der Ausstellung eines qualifizierten Zertifikates. Offen bleibt, wer den Konsumenten schützt, der auf ein - nicht qualifiziertes - Zertifikat vertraut hat. Wenn ein derartiges (nicht qualifiziertes) Zertifikat nahezu keinen

Schutz bietet, sollte seine Verwendung im Geschäftsleben nicht zulässig sein, zumal es Unsicherheit schafft und keinen hinreichenden Schutz gewährleistet. Auf die Ausführungen unter den Punkt „Allgemeines" wird verwiesen.

Hinsichtlich Höhe und Art der Haftung sollte ein Verweis auf die Verordnung im Interesse der Klarstellung und besseren Lesbarkeit des Textes in diese Bestimmung aufgenommen werden.

Im übrigen erscheint auch die Haftung hinsichtlich „dreipersonaler" Schuldverhältnisse nicht ausreichend geregelt.

Für den Bundesminister:

Holubar

Für die Richtigkeit
der Ausfertigung: