16/SN-389/ME

WIRTSCHAFTSKAMMER
ÖSTERREICH

An das
Bundesministerium für Justiz
Museumstraße 7
1070 Wien

Wiedner Hauptstraße 63
Postfach 191
1045 Wien
Telefon +43(1)50105DW
Telefax +43(1)50206233
Internet: http://www.wk.or.at/vp
E-Mail: salzmans@wkoe.or.at

Ihr Zeichen, Ihre Nachricht vom	Unser Zeichen, Sachbearbeiter	Durchwahl	Datum
GZ 7.051C/50-I.2/99 6. Mai 1999	Vp 26474/46/99/Mag.Rei/Sa Mag. Christoph Reissner	4006	07.6.1999

Entwurf für ein Bundesgesetz über elektronische Signaturen; Begutachtungsverfahren

Die Wirtschaftskammer Österreich bedankt sich für die Übermittlung des Entwurfes für ein Bundesgesetz über elektronische Signaturen (SigG) und nimmt hierzu wie folgt Stellung:

Grundsätzlich entspricht der Aufbau des SigG den Erwartungen der österreichischen Wirtschaft, wobei wir eine baldige Beschlußfassung des Gesetzesentwurfes durch das Parlament begrüßen. Trotz der Tatsache, daß bereits vor mehr als einem Jahr eine diesbezügliche Punktuation in Begutachtung gegangen ist und somit mit dem SigG kurz darauf zu rechnen gewesen wäre, halten wir es für richtig, daß die europäische Entwicklung - in Form des vor kurzem am Telekommunikationsministerrates angenommenen gemeinsamen Standpunktes zur gegenständlichen Richtlinie - abgewartet wurde.

Einleitend sei auch ausdrücklich festgehalten, daß die elektronische Signatur eine der wesentlichen Voraussetzungen für die sichere Abwicklung des elektronischen Geschäftsverkehrs von Unternehmen mit Kunden, Lieferanten und öffentlichen Stellen ist.

Wir möchten jedoch bereits an dieser Stelle darauf hinweisen, daß das SigG hinsichtlich seiner Einordnung in das bestehende Rechtssystem einige Unklarheiten in sich birgt: So ist dessen Verhältnis zum bereits länger bestehenden Akkreditierungsgesetz, das sich ebenfalls mit der Akkreditierung von Zertifizierungsstelle beschäftigt und somit va in terminologischer Hinsicht Verwirrung stiften könnte, ungeklärt.

Auch hinsichtlich der Regelungen der Rechtswirkungen der elektronischen Signatur bestehen Unklarheiten: Grundsätzlich wird die sichere elektronische Signatur der eigenhändigen Unterschrift zwar gleichgestellt, jedoch bleibt die Frage, inwieweit damit auch eine Gleichstellung der „Schrift in elektronischer Form" mit der „Schrift in Papierform" einhergeht, unbehandelt; somit ist auch ungeklärt, ob mit der (sicheren) elektronischen Signatur und der damit verbundenen Identitätsfeststellung die Kriterien einer Privaturkunde respektive einer öffentlich beglaubigten Urkunde erfüllt werden können. Die Erläuterungen auf Seite 50 und 51 sind dazu nur bedingt aufschlußreich und sollten daher um die Behandlung dieses Punktes ergänzt werden. Eine Gleichstellung mit dem Urkundenbegriff hätte darüber hinaus den großen Vorteil, daß die Urkundendelikte des Strafgesetzbuches zur Anwendung kämen und damit sowohl dem Signator und dem Empfänger als auch der Zertifizierungsstelle mehr Rechtssicherheit gegeben wird.

Zu den Bestimmungen im einzelnen:

Zu § 2:

Einleitend ist festzustellen, daß Begriffsdefinitionen des Entwurfes für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Signaturen (RL) so weit als möglich zu übernehmen sind, um va terminologische Ungereimtheiten hintanzuhalten.

Die Abweichung zur RL, nämlich die Ausführungen in Ziffer 1, unter Authentifizierung sei bloß die Feststellung der Identität des Signators zu verstehen, scheint den oben angesprochenen Gedanken betreffend die Verknüpfung von Unterschrift und Schrift in der Weise zu präjudizieren, als mit elektronischen Signaturen keine Gedankenerklärungen authentifiziert werden sollen. Die Wirkung der elektronischen Signatur wäre damit unvollständig, da keine Urkunden - im Sinn des beurkundeten Gedankens - erstellt werden können und die Frage des Mehrwertes der Identitätsfeststellung in Zusammenhang mit der sicheren elektronischen Signatur auftaucht.

Der Ziffer 2 zufolge ist der „Signator" eine natürliche Person, wohingegen die Richtlinie unter dem vergleichbaren Begriff des „Unterzeichners" von einer Person spricht und somit die juristische mitumfaßt. Dieser Umstand stellt in der österreichischen Rechtsordnung nicht unmittelbar ein Problem dar, treten doch juristische Personen immer durch Organe, dh natürliche Personen, nach außen hin auf. Wir weisen jedoch in diesem Zusammenhang darauf hin, daß ausländische Signatoren sehr wohl juristische Personen sein können, sodaß insbesondere in Zusammenhang mit dem grenzüberschreitenden Handel diese Situation in Österreich auftreten kann und unsere Rechtsordnung daher darauf vorbereitet sein sollte.

In Ziffer 3 ist unklar, warum von der RL-Begriffsbestimmung der „fortgeschrittenen elektronischen Signatur" abgegangen wird und ein anderer Begriff, nämlich „sichere elektronische Signatur", eingeführt wird, der der Richtlinie fremd ist. Weiters wird ein zusätzliches Erfordernis für die „sichere elektronische Signatur" eingeführt, das nämlich
e) auf einem qualifizierten Zertifikat beruht und unter Verwendung von technischen Komponenten und Verfahren, die den Sicher-

heitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen entsprechen, erstellt wird. Zwar ist aus den Erläuterungen ersichtlich, daß die österreichische „sichere Signatur" der europäischen „fortgeschrittenen Signatur" unter Einhaltung der Anhänge I, II und III entspricht; die rechtliche Einstufung von anderen europäischen „fortgeschrittenen Signaturen" ohne Einhaltung der Anhänge I, II und III ist aber ungeklärt.

Zu § 3:

Gemäß dem Abs 1 ist die Verwendung elektronischer Signaturen im Rechts- und Geschäftsverkehr zulässig, soweit sich aus gesetzlichen Vorschriften oder vertraglichen Vereinbarungen nicht anderes ergibt, wohingegen die Erläuterungen zu dieser Bestimmung statuieren, daß die Zulässigkeit elektronischer Kommunikation grundsätzlich einer Vereinbarung bedarf und das bloße Einrichten einer e-mail-Adresse hierfür noch nicht ausreicht. Aus Gründen der Rechtssicherheit wird eine Klarstellung va für den Fall des Nichtvorliegens einer diesbezüglichen Vereinbarung empfohlen.

Zu § 4:

Diese Bestimmung stellt zweifelsohne das Kernstück des vorliegenden Entwurfes dar, wird doch grundsätzlich vorgesehen, daß die sichere elektronische Signatur mit der eigenhändigen Unterschrift gleichzustellen ist.

Weiters sind auch Situationen denkbar, in denen die Identität des Signators unstrittig ist, und zwar nicht deshalb, weil der Gebrauch eines qualifizierten Zertifikates vorliegt, sondern weil ein geschlossenes System und somit ein bekannter Benutzerkreis gegeben ist; nach der vorliegenden Textierung - vgl va Seite 45 der Erläuterungen - ist es in zivilrechtlicher Hinsicht zulässig, daß auf Basis einer dementsprechenden Parteienverein-

barung auch das nicht qualifizierte Zertifikat das Schriftlichkeitserfordernis erfüllt; etwaige verwaltungsstrafrechtliche Konsequenzen, welche sich im Zusammenhang mit der Nichteinhaltung der Schriftlichkeit bei Verbraucherkrediten bzw Verbrauchergirokontoverträge ergeben könnten, sollten jedoch durch eine diesbezügliche Regelung ausgeschlossen werden.

Schließlich taucht im diesem Kontext auch die Frage auf, inwieweit das in manchen Gesetzen verankerte Erfordernis der Legitimierung eines Kunden - so wie es zum Beispiel in § 40 BWG vorgesehen ist - durch die „zuverlässige" Identitätsfestellung iS des § 8 Abs 1 SigG bereits durchgeführt wurde und somit beispielsweise im Falle des Abschließens von Kontoverträgen auf elektronischem Wege nicht neuerlich durchzuführen ist. Zum Zeichen der vorgenommenen Legitimierung hätte ein Kreditinstitut dann bloß die Daten des Zertifikates aufzubewahren, um der Verpflichtung zur Identitätsfeststellung nach § 40 BWG zu entsprechen. Vergleichbare Identitätsprüfungspflichten finden sich auch in anderen Bereichen, insbesondere im Versicherungsbereich, wobei die Fragestellung dieselbe ist, weshalb um einen diesbezüglichen expliziten Hinweis in den Erläuterungen ersucht wird.

Sofern jedoch Zweifel an der Qualität der Legitimierung durch einen Zertifizierungsdiensteanbieter bestehen, könnte man diese eventuell dadurch ausräumen, daß man in § 8 Abs. 1 SigG ausdrücklich festhält, daß ein Zertifizierungsdiensteanbieter die Identität von Personen „anhand eines amtlichen Lichtbildausweises" festzustellen hat; diesem Passus wäre im übrigen vor dem Begriff „zuverlässig" der Vorzug einzuräumen.

Im übrigen wird auf die obigen Ausführungen zum Urkundenbegriff verwiesen.

Im Zusammenhang mit dieser Bestimmung sei auch auf die Problematik des „Nachsignierens" kurz eingegangen, welche sich va daraus

ergibt, daß das SigG eine zeitliche Begrenzung für Zertifikate, nicht jedoch für Unterschriften vorsieht. Im Kontext mit gesetzlichen Verpflichtungen bzw im öffentlichen Bereich (finanzrechtliche Vorschriften, Archivierungen von Röntgenbildern udgl.) wird man dieses Problem dadurch lösen können, daß man nach Ablauf und erfolgter Neuausstellung des Zertifikates für eine dementsprechende „Aktualisierung" der jeweiligen Dokumente sorgt. Diese Problematik wird jedoch va im zivilrechtlichen Bereich virulent, man denke nur an die Beweisbarkeit eines elektronisch abgeschlossenen Vertrages nach 20 Jahren. Für derartige Situationen sollten ebenfalls Überlegungen angestellt werden, die ihren Niederschlag im Gesetz finden müßten.

Zu § 5:

Im Zusammenhang mit sog Attributzertifikaten, welche in Abs 1 Z 4 bzw Abs 2 vorgesehen sind, weisen wir darauf hin, daß die Richtigkeit der Attribute mit gleich hoher Sicherheit wie die Richtigkeit der persönlichen Angaben der qualifizierten Zertifikate zu erstellen sind; bei einer allfälligen Streichung des Attributes wäre auch zu klären, ob das Zertifikat als solches weiterbestehen kann.

Die in Abs 1 Z 9 mögliche Beschränkung des Transaktionswertes pro Unterschrift ist zu begrüßen; allerdings sei darauf verwiesen, daß auf elektronischem Wege sehr viele Transaktionen in sehr kurzer Zeit durchgeführt werden können und somit eine Beschränkung pro Unterschrift möglicherweise nicht ausreichend ist.

Die Erkennbarkeit eines qualifizierten Zertifikates ist von der RL vorgegeben und inhaltlich auch sinnvoll. Derzeit fehlen jedoch noch die konkreten Bestimmungen, wie dies technisch umzusetzen ist. Da dies den Aufbau des Zertifikates betrifft und

nicht ohne weiteres nachträglich geändert werden kann, ist eine rasche Klärung notwendig.

Zu § 6:

Ein Zertifizierungsanbieter ordnet grundsätzlich Schlüssel Personen zu. In diesem Kontext taucht immer wieder die Frage auf, inwieweit auch selbst generierte Schlüssel durch eine Zertifizierungsstelle einer Person zugeordnet werden können. Die diesbezüglichen Erläuterungen auf Seite 78 geben nur bedingt Auskunft darüber.

Zu § 7:

Die in Abs 1 Z 5 in Zusammenhang mit den Anforderungen an das Personal verwendeten Begriffe der „Managementfähigkeiten" und der „anerkannten Normen" sind für unser Verständnis doch ein wenig zu allgemein gehalten.

Die Bestimmung in Abs 1 Z 3 hinsichtlich der Zeitstempeldienste scheinen nicht ganz schlüssig zu sein. Die Erläuterungen auf Seite 60 führen dazu unter anderem aus: „Ein **Zeitstempel** (**Z 3**) ist eine elektronisch signierte Bescheinigung eines Zertifizierungsdiensteanbieters, daß (ihm) bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen sind.... Sind in qualifizierten Zertifikaten oder in Zertifikatsverzeichnissen oder Widerrufslisten Zeitangaben enthalten, so müssen diese **qualitätsgesichert** sein, d.h. den Sicherheitsanforderungen des § 18 entsprechen." Die Sicherheitsanforderungen des § 18 sind allerdings für „sichere elektronische Signaturen" ausgelegt, von denen sich die bloß qualifizierten Signaturen dadurch unterscheiden, daß sie eben nicht die Anforderungen des § 18 erfüllen müssen. Unverständlich ist nun, daß der Zertifizierungsdiensteanbieter in nicht sicheren qualifizierten Zertifikaten sichere Zeitstempel verwenden muß. Zur Generierung dieser Zeitstempel

müßte er dann eben doch eine sichere Infrastruktur nach § 18 vorhalten.

Hinsichtlich der in Abs 1 Z 8 genannten Anforderung ist unklar, wie der Zertifizierungsdiensteanbieter für qualifizierte Zertifikate Vorkehrungen dafür treffen kann, daß die Signaturerstellungsdaten der Signatoren nicht von Dritten gespeichert oder kopiert werden können. Wir begrüßen, daß die Signaturerstellungsdaten - außer für die im Zusammenhang mit der Bereitstellung der Signatur- und Zertifizierungsdienste notwendigen Zwecke - weder gespeichert noch kopiert werden dürfen. Wir geben aber zu bedenken, daß es einen absoluten Kopierschutz bezüglich auf Computern gespeicherten Daten nicht gibt. Die Erläuterungen beschränken sich deshalb auch darauf, dem Zertifizierungsdiensteanbieter zu untersagen, Informationen über die Schlüsselerzeugung oder das technische Know-how hierüber bekanntzugeben. Er darf auch in keiner wie immer gearteten Form etwa an der Erzeugung eines Nachschlüssels mitwirken. Diese Formulierung sollte auch im Gesetzestext gewählt werden.

Wenn der Signator von der in Abs 2 niedergeschriebenen Möglichkeit der Verweigerung der Zustimmung betreffend die Veröffentlichung von Zertifikaten Gebrauch macht, stellt sich die Frage, wie man als „Betroffener" dessen Signatur überprüfen kann.

Zu § 8:

Im Zusammenhang mit Pseudonymen ist festzustellen, daß man durchaus auch im Bereich des elektronischen Geschäftsverkehrs die Möglichkeit haben sollte, anonym Geschäfte abzuwickeln. Allerdings sind Situationen vorstellbar, in denen die Verwendung eines solchen Pseudonyms untragbar wäre; beispielsweise sei hier der Behördenkontakt genannt. Ein Kompromiß könnte darin bestehen, daß bei Verwendung eines qualifizierten Zertifikates ein Pseudonym unzulässig ist.

Im Kontext mit dem in Abs 1 genannten Begriff „zuverlässig" stellt sich die Frage, inwieweit dies zwingend die Vorlage eines Lichtbildausweises mitumfaßt; falls dem nicht so ist, wäre eine diesbezügliche Bestimmung in das SigG aufzunehmen.

Zu § 9:

In den Erläuterungen zum Widerruf von Zertifikaten (Seite 66) wird darauf hingewiesen, daß eine „Rückgängigmachung einer Sperre oder eines Widerrufes" unzulässig sein soll. Dies dürfte aber offenbar ein Schreibfehler sein. Da eine Sperre nach dem Wesen des Entwurfes nur vorläufigen Charakter hat, muß auch eine Rückgängigmachung der Sperre zulässig sein. In den Erläuterungen dürfte dagegen vielmehr gemeint sein, daß die Rückwirkung einer Sperre oder eines Widerrufes unzulässig sein soll.

Schließlich sollte die Widerrufsmöglichkeit eines Zertifikates auch bei einer gerichtlichen Verurteilung gegeben sein.

Zu § 13:

Um das Grundprinzip des freien Wettbewerbs der Zertifizierungsdiensteanbieter einerseits und die gewünschten Rechtswirkungen eines qualifizierten Zertifikates andererseits zu ermöglichen, ist grundsätzlich die Telekom-Control-Kommission (TKK) als Aufsichtsstelle vorgesehen. Im Gegensatz zur Rolle der TKK als Marktregulierer im Übergang von einem Monopolmarkt zum Wettbewerb von Netzanbietern und zum Schutz der Telekom-Kunden auf Basis des Telekommunikationsgesetzes (TKG) muß sich die Aufsichtsstelle im SigG vor allem auf die Sicherung und Durchsetzung der Qualitätserfordernisse von Zertifizierungsdiensteanbietern konzentrieren. Dieser Umstand ist bei der Umsetzung zu berücksichtigen.

Inwieweit die Aufsichtsstelle als inländische „Wurzelinstanz" agieren, dh die Ausstellung der Zertifikate für Zertifizierungsstellen durchführen sollte, wäre einer genaueren Betrachtung zuzuführen. Es sollte nämlich in diesem Zusammenhang berücksichtigt werden, daß bei einer Kompromittierung des privaten Schlüssels der Aufsichtsstelle mit einem Schlag das gesamte österreichische System der elektronischen Signatur und damit alle dazugehörigen Zertifikate ungültig gemacht würden. Dieses Risiko ist zwar nicht sehr groß, jedoch existent. Vielmehr sollte überlegt werden, ob nicht auf andere Art und Weise als der Verwendung des „private key" der Aufsichtsstelle derselbe Zweck erreicht werden könnte. Denkbar wäre zB die Veröffentlichung der nötigen Information unter Zuhilfenahme eines anderen, sicheren Kanals, zB der Wiener Zeitung.

Weiters ist sicherzustellen, daß eine eindeutige Trennung der Aufgaben aufgrund des TKG und des SigG in organisatorischer, personeller und finanzieller Hinsicht gewährleistet ist.

Die in Abs 4 verankerte Verordnungsermächtigung sollte dahingehend determiniert werden, daß nur ein für die jeweils erbrachte Leistung angemessenes, kostendeckendes Entgelt vorgeschrieben werden darf.

Schließlich sei noch darauf hingewiesen, daß allfällige Sicherheitsstufen von der Aufsichtsstelle definiert und überwacht gehören.

§ 14:

Diese Bestimmung geht über die Anforderungen des Art 3 Abs 2a der RL hinaus, da dort nur Aufsichtsmaßnahmen für Zertifizierungsstellen vorgesehen sind, die „öffentlich qualifizierte Zertifikate" erteilen, und nicht auch für solche, die nicht qualifizierte Zertifikate anbieten. Diesbezüglich sollte auf den

Richtlinientext zurückgegangen werden, da ansonsten höhere Kosten des Aufsichtssystems und unnötige Belastungen der Zertifizierungsstellen, die keine öffentlich qualifizierten Zertifikate erteilen, zu erwarten sind.

In Abs 1 ist unklar, unter welchen Voraussetzungen die Aufsichtsstelle über die Zertfizierungsdienstanbieter hinweg Zertifikate von Signatoren widerrufen kann. Eine gesetzliche Determinierung dieser Möglichkeit scheint hier angebracht. Unseres Erachtens sollte die Anordnung an die Zertfizierungsdienstanbieter, das Zertifikat von Signatoren zu widerrufen, ausreichen.

Hinsichtlich der Kompetenzen der Aufsichtsstelle wäre eine Determinierung der Begriffe „ungeeignet", „erforderliche Maßnahmen" und „andere geeignete Maßnahmen" wünschenswert, um dem Vorwurf einer Globalermächtigung vorzubeugen.

Zu § 16:

Die in Abs 1 der Aufsichtsstelle vorzulegenden Unterlagen sollten explizit auch den Bereich der elektronisch gespeicherten Aufzeichnungen umfassen.

Zu § 17:

Die von der Richtlinie gebotene Möglichkeit der freiwilligen ex ante Akkreditierung hat im österreichischen Gesetzesentwurf leider nicht die erhofften „Bonus"-Rechtswirkungen erbracht. Das bloße Aufgenommenwerden in eine Liste der Aufsichtsstelle wird als Motivation vermutlich zu wenig sein. Wir regen deshalb an, weitere, vor allem juristische Anreize zu bieten.

Zu § 18:

Einleitend sei hier darauf hingewiesen, daß die in den Erläuterungen genannten „technischen Manipulationen oder Fehler, die dazu führen, daß Daten ungewollt signiert werden....“ mit den derzeit verbreiteten Desktop-Systemen nicht möglich sind.
In diesem Zusammenhang sei erwähnt, daß mit einem nachträglichen Qualitätsverlust jederzeit zu rechnen ist und es daher wichtig erscheint, praktische Mechanismen zu definieren, wie damit umgegangen wird.

Hinsichtlich der in Abs 1 angesprochenen „viewer-Problematik“ (...zuverlässig erkennbar machen..) ist zu sagen, daß diese nach wie vor noch nicht gelöst ist und diese Anforderung daher schwerlich erfüllt werden kann.

In Abs 6 sollte klargestellt werden, daß die Festlegung nicht die Erstellung der Normen beinhaltet, sondern nur die Feststellung, welche der jeweils vorhandenen Normen als geeignet anzusehen sind, um dem Sicherheitsbedürfnis Rechnung zu tragen, wobei die Frage offen bleibt, was in der Zwischenzeit passiert.

Zu § 19:

Wie in den Erläuterungen zu dieser Bestimmung richtig ausgeführt, kommt zur Gewährleistung der Sicherheit elektronischer Signaturverfahren der Vertrauenswürdigkeit und fachlichen Kompetenz der Bestätigungsstelle entscheidende Bedeutung zu. Zumindest die Optik hinsichtlich der Vertrauenswürdigkeit eines Vereines, dessen Mitglieder die beteiligten Ressorts sind, wobei einer der Ressortleiter, nämlich der Bundeskanzler, mittels Verordnung feststellen kann, daß „seine“ Stelle geeignet ist, soll hier nicht weiter diskutiert werden. Es sei jedoch der Hinweis an dieser Stelle erlaubt, daß die RL in Art 3 Abs 2b von „geeig-

neten öffentlichen und privaten Stellen" spricht. Wünschenswert aus Sicht der Wirtschaft wäre es daher, daß unter dem Gesichtspunkt des Subsidiaritätsprinzips eine amtswegige Bestätigungsstelle nur dort einzurichten ist, wo dies tatsächlich erforderlich ist, womit letztendlich eine de-facto-Monopolstellung einer „regierungsnahen" Einrichtung vermieden wird. Bei einem Tätigwerden von privaten Unternehmungen als Bestätigungsstelle wäre auch die Bestimmung zu überdenken, derzufolge die organisatorische Aufsicht über die Bestätigungsstelle der Aufsichtsstelle zukommt.

Der auf Seite 82 der Erläuterungen verankerte Gedanke, demzufolge vorrangig auf „bestehende Infrastrukturen vor allem bei Herstellern" zurückgegriffen werden sollte, ist absolut zu unterstützen. Selbstredend sollte auch vorgesehen sein, daß ein Zertifizierungsdiensteanbieter, der die nötigen Prüfberichte selbst beschafft, sowohl in finanzieller als auch in zeitlicher Hinsicht im Evaluierungsverfahren bei der Bestätigungsstelle bevorzugt zu behandeln ist, sodaß er weniger Unkosten im für ihn kürzeren Verfahren hat.

Abschließend wird noch aus Gründen der Rechtssicherheit eine Mitveröffentlichung der RL und der „anerkannten Normen" empfohlen.

Wunschgemäß werden 25 Exemplare dieser Stellungnahme dem Präsidium des Nationalrates zugeleitet.

Mit freundlichen Grüßen

Leopold Maderthaner
Präsident

Dr. Günter Stummvoll
Generalsekretär