7/SN-389/ME

KAMMER DER
WIRTSCHAFTSTREUHÄNDER

PRÄSIDIUM DES NATIONALRATES

Parlament
Dr.Karl Renner-Ring 3
1017 W i e n

Unser Zeichen: 815/99/Mag.Miller/St
Datum: 31. Mai 1999

Betreff:
Stellungnahme zum Entwurf eines Bundesgesetzes über elektronische Signaturen
(GZ. 7.051C/50-I.2/1999)

Sehr geehrte Damen und Herren,

in der Beilage übersenden wir Ihnen 25 Ausfertigungen unserer Stellungnahme zum Entwurf des Bundesgesetzes über elektronische Signaturen zu Ihrer Kenntnisnahme.

Mit freundlichen Grüßen

Dr. Gerald Klement
(Kammerdirektor)

KAMMER DER WIRTSCHAFTSTREUHÄNDER

Beilagen

Bankverbindungen:
Creditansalt 0049-46000/00
Bank Austria AG 238-109-066/00
Erste Bank 012-03304
Postsparkasse 1838.848

Schönbrunner Straße 222–228/6 (U4 Center), A-1120 Wien
Tel. 01/811 73-0
Fax 01/811 73-100
e-mail: office@kwt.or.at
homepage: http://www.kwt.or.at

DVR 459402

KAMMER DER
WIRTSCHAFTSTREUHÄNDER

BUNDESMINISTERIUM FÜR JUSTIZ

Museumstraße 7
1070 Wien

GZ. 7.051C/50-I.2/1999
Referent: StB Ing.Mag.Dr.Michael Schirmbrand
Unser Zeichen: 815/99/Mag.Miller/St
Datum: 31. Mai 1999

Betreff:
Bundesgesetz über elektronische Signaturen

Sehr geehrte Damen und Herren!

Wir danken für die Einladung zur Begutachung eines Bundesgesetzes über elektronische Signaturen und nehmen dazu wie folgt Stellung:

Einleitung

Durch die ständig steigende Anzahl von Geschäften, welche über Medien wie das Internet abgewickelt werden, erhöht sich auch die Nachfrage nach einem geeigneten Instrumentarium, welches die Anforderungen der Authentizität, Integrität, Vertraulichkeit und Verbindlichkeit erfüllt. Mit der digitalen Signatur hat man ein solches Instrument gefunden, jedoch ist zu bedenken, daß die Art und die Qualität ihres Einsatzes über den Grad der Anwendbarkeit zur Erfüllung der Anforderung entscheidet.

Der Entwurf über das Österreichische Signaturgesetz erfüllt im wesentlichen die Anforderungen (des Entwurfs) der Richtlinie über gemeinsame Rahmenbedingungen für elektronische Signaturen Abl. Nr. C 325 vom 23.10.1998 (Richtlinie).

Dennoch sollten einige Inhalte, welche für Electronic Commerce im Bereich Sicherheit und Vertrauen besonders wichtig erscheinen, näherer Betrachtung unterzogen werden:

- Sicherheit der elektronischen Signatur
- Unterschiedliche Wertigkeit von Zertifikaten
- Haftung der Zertifizierungsstellen

DVR: 459402

Bankverbindungen:
Creditansalt 0049-46000/00
Bank Austria AG 238-109-066/00
Erste Bank 012-03304
Postsparkasse 1838.848

Schönbrunner Straße 222–228/6 (U4 Center), A-1120 Wien
Tel. 01/811 73-0
Fax 01/811 73-100
e-mail: office@kwt.or.at
homepage: http://www.kwt.or.at

Sicherheit der elektronischen Signatur

In weiterer Folge wird von der Technologie der digitalen Signatur ausgegangen, welche auf der Generierung eines Schlüsselpaares (öffentlicher und privater Schlüssel) basiert. Um die Integrität der Daten zu gewährleisten, wird eine Prüfsumme mittels Algorithmus generiert (Hash—Wert). Die Verläßlichkeit der digitalen Signatur hängt einerseits von der Qualität der Verschlüsselung bzw. Hash-Funktion ab, sowie von der zuverlässig bestätigten Identität des benutzten öffentlichen Schlüssels. Letzteres wird unter 3. näher betrachtet.

Der hier vorliegende Entwurf über das Österreichische Signaturgesetz geht auf die Sicherheitsanforderungen der Zertifizierungsstellen für qualifizierte Zertifikate unter §7 Abs (1) bis Abs (3) ein. So muß die Zertifizierungsstelle „vertrauenswürdige Systeme, Produkte und Verfahren, die vor Veränderungen geschützt sind und für die technische und kryptographische Sicherheit sorgen" verwenden. Signaturerstellungsdaten müssen geheim gehalten werden, und dürfen weder vom Zertifizierungsdiensteanbieter noch von Dritten gespeichert und kopiert werden können. Ebenfalls sind die Signaturerstellungsdaten vor unbefugtem Zugriff zu sichern. Die Telecom-Control wird zur Durchführung der Aufsicht herangezogen. Die Aufsicht, welche in §13 bis §17 festgehalten ist, geht nur oberflächlich auf die oben angeführten Sicherheitsanforderungen ein. Wichtig sind in diesem Bereich vor allem ausreichende Zugriffsschutzsysteme (logisch sowie physisch) im Bereich der Signaturerstellungsdaten. Es mangelt an der Definition der Gewährleistung dieser Sicherungssysteme, wie zB ausreichende Dokumentation der Auditing-Tätigkeiten sowie Protokollierung. Dies sollte zur verstärkten Sicherheit in die Obligationen des Zertifizierungsdiensteanbieters aufgenommen werden.

Unterschiedliche Wertigkeit von Zertifikaten

Diese Überlegung ist zu begrüßen, zumal ein und dasselbe Zertifikat nicht für alle Tätigkeiten im Rahmen von Electronic Commerce genügen kann. Wie auch außerhalb des „Cyberspace" gibt es unterschiedliche Anwendungsgebiete, welche nicht den reinen Geschäftsbetrieb umfassen müssen, wie zB Mitgliedschaft in einem Verein, etc. Dieser Trend läßt sich nicht nur international sondern auch national erkennen (zB net.surance im Vergleich zu a-sign).

Eine elektronische Signatur bedeutet einen wesentlichen Eingriff in das private Umfeld des Staatsbürgers. Es ist jedoch festzustellen, daß aufgrund der RL 95/64/EG des Rates sowie im österreichischen DSG 2000 maßgebend die Sicherung von personenbezogenen Daten und betreffend deren Erhebung ausreichen definiert sind. Untrennbar verbunden mit der unterschiedlichen Wertigkeit von Zertifikaten sind die differenzierten Identitätsüberprüfungen der Zertifizierungs-diensteanbieter, welche essentiell für die Verläßlichkeit eines Zertifikates sind. In §22 ist definiert, daß ein Zertifizierungsdiensteanbietern nur jene personenbezogene Daten verwenden darf, welche er zur Durchführung der erbrachten Dienste benötigt. Die Erhebung darf nur unmittelbar beim Betroffenen erfolgen oder mit ausdrücklicher Zustimmung bei einem Dritten selbst. Da die Daten akkurat und fehlerfrei gehalten werden müssen, ist es notwendig, einen Verzeichnis- und Widerrufsdienst zu führen. Vor allem bei Geschäften im Internet ist die Gefahr des Cyberfraud ständig gegeben, was sichere und fehlerfreie Daten unabdingbar macht. In §6(6) wurde dazu

festgelegt, daß Zertifzierungsdiensteanbieter, welche Zertifikate ausstellen, ein Sicherheitskonzept darzulegen haben, ob und gegebenenfalls in welcher Form Verzeichnis- und Widerrufsdienste geführt werden. Zu diskutieren sei hier das „ob", denn ein Verzeichnis- und Widerrufsdienst sollte auf alle Fälle geführt werden, um die Akkuranz und Fehlerfreiheit der Daten zu garantieren. Bei qualifizierten Zertifikaten ist dieser Verzeichnis- und Widerrufsdienst in §7(2) vorgeschrieben.

Zur Identitätsüberprüfung wird in §7(4) festgehalten, daß dies „mit geeigneten Mitteln" für qualifizierte Zertifikate erfolgen soll. Diese Definition sollte diskutiert werden, da es hinsichtlich der Zertifizierungsdiensteanbieter unterschiedliche Auffassungen geben kann, was „geeignete Mittel" sind. Vorzuschlagen wäre eine Aufzählung definitiv nicht zur Identitätsüberprüfung geeigneter Mittel.

Haftung der Zertifizierungsdiensteanbieter

In Anknüpfung zum vorigen Thema haften die Zertifizierungsdiensteanbieter nach §23(1) für die Richtigkeit aller Angaben im qualifizierten Zertifikat im Zeitpunkt seiner Austellung.

Ein wichtiger Punkt ist die Umkehr der Beweislast zu Lasten des Zertifizierungs-diensteanbieters.

Organisatiorisch ist wiederum auf den Widerrufsdienst bei qualifizierten Zertifikaten zu verweisen. Nach §23 (4) muß das Zertifikat unverzüglich widerrufen werden können und die Widerrufsdienste verfügbar sein. Dies erfordert nicht nur einen 24 Stunden - 7 Tage Dienst, sondern auch eine effiziente Infrastruktur zur Abwicklung des Dienstes. Neben der Verfügbarkeit muß der Dienst auch höchstmögliche Sicherheit aufweisen. Das Internet selbst bietet sich aufgrund der Erreichbarkeit und Verfügbarkeit als möglicher Teil dieses Dienstes an. Um das Internet hierfür jedoch nutzen zu können, müssen sicherheitstechnische Applikationen verwendet werden, um den sicheren Widerrufsdienst zu gewährleisten. Dieser Dienst erfordert daher auch genaueste Spezifikation, Dokumentation sowie Auditing und Monitoring während des Betriebes.

Abschließend sollte noch die Rolle der Bestätigungsstelle, welche in §19 festgehalten wird, angesprochen werden. Auf Grundlage der Signaturverordnung, welche auf Basis des Signaturgesetzes erlassen werden soll, werden die Aufgaben der Bestätigungsstelle an geeignete Einrichtungen zugewiesen. Die Bestätigungsstelle muß Zuverlässigkeit aufweisen, qualifiziertes Personal (mit besonderen Kenntnissen) beschäftigen, über ausreichende technische Einrichtungen und Mittel sowie eine ausreichende wirtschaftliche Leistungsfähigkeit verfügen und die erforderliche Unabhängigkeit, Unparteilichkeit und Unbefangenheit sicherstellen. Aufgrund dieser Anforderungen sollten Wirtschaftsprüfungs-organisationen mit entsprechender Größe und Infrastruktur Überlegungen anstellen, sich als Bestätigungsstelle zu bewerben. Vorallem die Argumente der Unabhängigkeit, Unparteilichkeit und Unbefangenheit sowie die Zuverlässigkeit sprechen eindeutig für derartige Überlegungen.

Zusammenfassend sei zu sagen, daß mit diesem Entwurf für ein österreichisches Signaturgesetz im Electronic Commerce ein Schritt in die richtige Richtung zur Erreichung wirtschaftlicher Vorteile getätigt wird. Die Authentizitäts- und Integritätsanforderungen werden durch die elektronische Signatur in Zusammenhang mit der Haftung der Zertifizierungsdiensteanbieter erfüllt. Dies bestätigt die Verläßlichkeit der elektronischen Signatur sowie die Verbindlichkeit von Verträgen, welche mit dieser Signatur „unterschrieben" sind (ausgenommen §4(2)).

Zukünftig sollten vor allem die vorgeschriebenen Technologien, welche Gegenstand der zu erlassenden Signaturverordnung sind, diskutiert werden. Überlegungen bezüglich des Einsatzes von Chipkarten sowie derartige Feldversuche zeigen einen Trend, daß der private Schlüssel über dieses Medium die höchste Sicherheit erfährt. Infrastrukturell sollte die nötige Ausstattung für die Verwendung dieses Mediums allerdings diskutiert werden. Vermieden werden muß, daß Firmen Monopolstellung in diesen Bereichen aufweisen, und somit nicht den für den Konsumenten wichtigen Sicherheitsaspekt durch überteuerte Preise beeinflussen, da dies im krassen Gegensatz zu allen Überlegungen betreffend eines „sicheren und vertrauenswürdigen" Internet für alle Teilnehmer stehen würde.

25 Ausfertigungen dieser Stellungnahme werden gleichzeitig an das Präsidium des Nationalrates zugesandt.

Mit freundlichen Grüßen

Mag.Klaus Hübner e.h.
(Präsident)

KAMMER DER WIRTSCHAFTSTREUHÄNDER

Dr.Gerald Klement
(Kammerdirektor)