An die
Parlamentsdirektion
Begutachtungsverfahren

1010 Wien

Wien, 10. September 2007

Betreff: Zeichen: BKA-410.006/0006-I/11/2007
Stellungnahme der ARGE DATEN zur Änderung des Signaturgesetzes

In der Anlage finden Sie die Stellungnahme der
ARGE DATEN - Österreichische Gesellschaft für Datenschutz
mit dem dringenden Ersuchen um Kenntnisnahme und Berücksichtigung.

Für allfällige Fragen stehen wir gerne zur Verfügung.

Mit vorzüglicher Hochachtung

CN = Mag. Dr. Hans Gerhard ZEGER, Vertretung ARGE DATEN als Obmann, C = AT, L = Wien, S = Wien, O = ARGE DATEN - Oesterreichische Gesellschaft fuer Datenschutz
2007.09.10 11:16:13 +02'00'

Dr. Hans G. Zeger (Obmann)

Charlotte Schönherr (Schriftführerin)

Stellungnahme elektronisch übermittelt

Alle Stellungnahmen werden unter ftp://ftp.freenet.at/ veröffentlicht.

Stellungnahme der ARGE DATEN vom 10. September 2007 zu:
Signaturgesetz, Änderung

1. Allgemeiner Teil

1.1. Einleitung

Grundsätzlich ist es zu begrüßen, dass ein Gesetz, das offensichtlich nicht praktikabel ist und in den letzten Jahren zu enormen Verunsicherungen und bei Unternehmen zu erheblichen Fehlinvestitionen in der Höhe vieler Millionen EURO führte, novelliert wird.

Beunruhigend ist jedoch die Tatsache, dass der bisher eingeschrittene Weg der Überregulierung des Bereiches der "sicheren/qualifizierten Signatur" weiter beschritten werden soll und nicht die gesamte Breite von Signaturanwendungen berücksichtigt wird.

1.2. Grundlagen der elektronischen Sigantur

Seit nunmehr zwanzig Jahren werden in der IT elektronische Vidierungs- und Siegelverfahren erfolgreich eingesetzt, in Österreich werden diese Verfahren seit 2000 unter der Bezeichnung "elektronische Signatur" im Signaturgesetz gesetzlich geregelt. Wie wohl der Begriff, wie weiter unten zu erläutern sein wird, in irreführender Weise einen technischen Vorgang beschreibt, wird die Bezeichnung in Hinblick auf die weite Verbreitung beibehalten.

Die anfänglich euphorischen Erwartungen und übertriebenen Hoffnungen in dieses technische Verfahren haben sich jedoch - erwartungsgemäß - nicht einmal annähernd erfüllt. Die ARGE DATEN beschäftigt sich mit dem Bereich der elektronischen Signatur seit mehr als zehn Jahren, sowohl was die technische Entwicklung, die Praktikabilität, ihre wirtschaftlichen Einsatzmöglichkeiten und die gesellschaftspolitischen und rechtlichen Folgewirkungen betrifft.

Auffällig ist, dass die mit dem Begriff "elektronische Signatur" zusammengefassten Vidierungs- und Siegelverfahren die einzigen informationstechnischen Mittel sind, deren Funktionalität einer ausdrücklichen gesetzlichen Regelung unterworfen wird. Bei allen anderen informationstechnischen Verfahren, wie zum Beispiel Funktionalität von Betriebssystemen, bei der Dokumentenverarbeitung, bei Buchhaltungsprogrammen, bei Datenbanken oder bei eMailprogrammen, fehlen aus guten Gründen derartige gesetzliche Regelungen.

Damit bildet das Signaturgesetz auch einen ungewöhnlichen und letztlich entbehrlichen Ausnahmefall im österreichischen Rechtssystem.

Selbst im hochsensiblen Bereich des Online-Shoppings oder des eCommerce hat es der Gesetzgeber, mit gutem Grund, vermieden gesetzliche Regelungen bei der technischen Umsetzung zu definieren, stattdessen wurde ein formaler Anforderungsrahmen definiert (die sogenannten Informationspflichten des ECG) und es dem Betreiber von eCommerce-Anwendungen freigestellt, wie er diese umsetzt.

Auch hochkritische IT-Infrastrukturen, denken wir an die Buchhaltungssysteme großer Unternehmen, mit Hilfe derer auch viele Milliarden der österreichischen Steuereinnahmen abgewickelt werden oder die Bankensysteme, die ebenfalls täglich viele Milliarden EURO an Transaktionen abwickeln werden ohne gesetzliche Regulierung technischer Standards betrieben.

Diese vernünftige und dem gesamten Rechtssystem entsprechende Vorgangsweise sollte in Zukunft auch bei der "elektronischen Signatur" gewählt werden.

Aus den durchwegs negativen Erfahrungen der letzten Jahre mit der "elektronischen Signatur" wäre es sinnvoll entsprechende Lehren zu ziehen und auch in diesem Bereich auf eine gesetzliche Regelung der technischen Aspekte der elektronischen Signatur gänzlich zu verzichten.

1.3. Umfassende Anpassung des Signaturgesetzes an Markterfordernisse sinnvoll

Einer der wesentlichen Gründe, warum Signaturverfahren keine ausreichende Verbreitung gefunden haben, liegt schon in der irreführenden Bezeichnung "Signatur". Dieser Begriff lässt Assoziationen mit der eigenhändigen Unterschrift aufkommen, die jedoch nicht zutreffend sind.

Wesentliches Merkmal der eigenhändigen Unterschrift ist deren unmittelbare Einsichtigkeit, ihre unbeschränkte Gültigkeit und das Fehlen technischer Vermittlungswerkzeuge. Werden Papier-Dokumente eigenhändig unterschrieben, kann jeder, sofern er Wert darauf legt, diese Willensentscheidung selbst durch Beobachtung überprüfen. Er benötigt keine zusätzliche technische Vermittlung und die Unterschrift ist auch unbegrenzt lang gültig.

Diese Eigenschaften, die den besonderen Beurkundungscharakter der eigenhändigen Unterschrift ausmachen, fehlen der elektronischen Unterschrift. Sie kann weder unmittelbar durchgeführt werden, noch unmittelbar wahrgenommen werden. Die Anfertigung ist von Geräten abhängig, die für den Signator nicht durchschaubar sind, deren wesentliches Merkmal in den Kernfunktionen sogar deren Undurchschaubarkeit ist. "sichere" bzw. nach dem neuen Entwurf "qualifizierte" elektronische Signaturen basieren auf technischen Komponenten, bei denen die Undurchschaubarkeit gegenüber dem Signator bescheinigt ist.

Abhängig von den installierten Geräten und Programmen wird auch die Signaturwahrnehmung beim Empfänger unterschiedlich ausfallen. Auch er ist für die Prüfung der elektronischen Signatur auf bestimmte Geräte und Installationen angewiesen. Mit diesen wird die Gültigkeit mehr oder minder eindeutig bestätigt. Es kann aber auch passieren, dass ein und dieselbe Unterschrift einmal als ungültig, ein anderes mal als gültig angezeigt wird., jeweils abhängig von der verwendeten Computerinstallation.

Der ARGE DATEN sind sogar weit verbreitete und häufig verwendete Programme bekannt, bei denen die Signaturprüfung abhängig vom aufgerufenen Menüpunkt, unterschiedliche Ergebnisse liefert!

Diese mangelhafte Transparenz und somit besonders für den Endverbraucher bestehende Undurchschaubarkeit, ergibt sich daraus, dass auf Grund für Signaturvorgänge eine Vielzahl von Komponenten erforderlich sind: Chipkarte, Signaturschlüssel, Kartenlesegerät, Driver-Software, eigene, betriebssystemabhängige Signaturerstellungs- und Signaturprüfkomponenten), die noch dazu von verschiedenen Lieferanten kommen und nur in wenigen bestimmten Kombinationen einsetzbar sind.

Schon geringfügige Änderungen an Computerkomponenten, die in keinem direkten Zusammenhang mit den Signaturkomponenten stehen, etwa ein Betriebssystemupdate oder die Installation von empfohlener Sicherheitssoftware, wie Virenscanner oder Firewalls führen regelmäßig dazu, dass die Signaturinstallation nicht mehr funktioniert.

Dies ist insbesondere bei rechtsverbindlichen und zeitkritischen Anwendungen problematisch, da sich der Bürger nie sicher sein kann, dass er seine Anträge oder Eingaben rechtsgültig abgeben kann bzw. diese rechtsgültig empfangen werden. Damit ist die "elektronische Signatur" derzeit in der Behörden-Bürger-Kommunikation ungeeignet.

Damit ist dieser Dienst für IT-Endanwender undurchschaubar, intransparent und nicht zumutbar. Gerade dort, wo rechtlich relevante Willensentscheidungen zu treffen sind, das ist die ursprüngliche Idee der elektronischen Signatur gewesen, wäre der Vorgang für den Endanwender nicht nachvollziehbar. Aus diesem Grund ist es auch höchst sinnvoll, dass die elektronische Signatur von der Mehrheit der Bevölkerung abgelehnt wird.

Verwendet man jedoch die elektronische Signatur dort, wo sie ursprünglich ihren Einsatzbereich hat, als elektronisches Siegel, das bloß die Unversehrtheit elektronischer Daten garantiert, dann ist die Mehrzahl der im Signaturgesetz getroffenen Regulierungen überflüssig und entbehrlich.

Für IT-Experten, die es gewohnt sind mit unterschiedlichsten Komponenten einen sicheren IT-Betrieb zu gewährleisten stellen die technischen Regelungen des Signaturgesetzes (bzw. der darauf aufbauenden Signaturverordnung) unzumutbare und sachlich nicht begründete Beschränkungen in der Wahl der verwendeten Verfahren und Mittel dar.

Es wird daher vorgeschlagen keinerlei technische Vorgaben bei der Erstellung von Signaturen zu machen und stattdessen nur den Umfang der Identitätsprüfung (der Qualität der ausgestellten Zertifikate) festzulegen. Die Qualität der Zertifikate, die ein Signaturverfahren an eine bestimmte Person binden, sollte in einem Stufenmodell (sinnvoll sind 3-4 Stufen) geregelt und durch die Aufsichtsbehörde überwacht werden.

1.4. Entwurf erhöht Rechtsunsicherheit

Abgesehen vom Fehlen einer den bisherigen Erfahrungen angemessenen Neukonzeption des Signaturgesetzes enthält der Entwurf auch eine Fülle von Detailproblemen.

Bedenklich und für die Anwender elektronischer Signaturdienste undurchschaubar ist die nunmehr im §2 vorgeschlagene Gleichstellung von Personen und "anderen rechtsfähigen Einrichtungen" als Signatoren.

"Unterschrift leisten" können, nach dem österreichischen Rechtsverständnis, nur Personen, bei rechtsfähigen Einrichtungen und Körperschaften eben nur deren Vertreter und befugten Organe. Die Einrichtungen selbst als Signatoren zu bezeichnen ist ein rechtspolitisches Unikum und erhöht zusätzlich und ohne sachliche Notwendigkeit die Intransparenz der elektronischen Signatur.

1.5. Signaturgesetz verfehlt Regulierungsziel

Begreift man gesetzliche Regelungen als Maßnahmen zur Regulierung von tatsächlich bestehenden oder angebotenen Leistungen, dann verfehlt der vorliegende Entwurf eindeutig das Ziel.

Tatsächlich gibt es eine Reihe von Nischen, in denen Signaturverfahren heute erfolgreich eingesetzt werden, ohne dass es der Benutzer als Signiervorgang im Sinne des Ausstellens einer Unterschrift wahrnimmt.

Es sind dies in der Regel Maschine-Maschine-Kommunikationen, die die Unversehrtheit der Übertragung von Inhalten sichern sollen.

So ist es heute üblich kritische Online-Geschäftsprozesse (eCommerce, Online-Banking, Online-Shopping) durch sogenannte SSL- und TLS-Serverzertifikate abzusichern. Gleiches gilt für eMail-Server. Mit Serverzertifikaten ausgestattet eMail-Server sind die wirksamste Waffe gegen Spam. Diese schon allein deswegen, weil sie Spam nicht beim Empfänger, wo er schon millionenfach verbreitet ist, sondern beim Absender, also an der Wurzel bekämpfen.

Diese Serverzertifikate basieren weltweit technisch auf denselben Routinen und werden mittlerweile von einigen hundert Anbietern angeboten. Die Zertifikate unterscheiden sich nicht technisch untereinander, sondern in der Genauigkeit der Identitätsprüfung. Hier hätte das Gesetz die Chance durch klare Abstufungen in der Identitätsprüfung (bei der Zerifikatsqualität) Rechtssicherheit bei den Benutzern zu schaffen, welche Verfahren wo einzusetzen sind.

Unter anderem werden derartige, der elektronischen Signatur entsprechende Dienste im Gesundheitstelematikgesetz(§§4ff), wiederum abweichend vom Signaturgesetz definiert.

Genau das wurde bisher verabsäumt und wird es auch im neuen Entwurf. Und so verwundert es nicht, dass etwa die österreichischen Banken bei ihren Onlinebanking-Anwendungen in keinem einzigen Fall ein österreichisches oder auch nur von einem EU-Diensteanbieter ausgestelltes Zertifikat benutzen, sondern auf Zertifikate aus den USA oder Südafrika ausweichen, die keinerlei Signaturgesetzgebung kennen.

Aber auch andere Signatur-Bereiche, wie die Dokumentenvidierung oder SingleSignOn-Lösungen werden durchwegs mit Verfahren realisiert, die nicht vom Signaturgesetz erfasst sind.

1.6. Unzureichende Rücksichtnahme auf sonstige einzelgesetzliche Regelungen

Die Entwicklungen der letzten Jahre haben gezeigt, dass es DIE einheitliche elektronische Signatur für alle Zwecke nicht gibt. Die Sicherheitsanforderungen, die Zertifikatsqualität, Zertifikatsinhalte und Umgebung, in der die elektronische Signatur verwendet wird, ergeben höchst unterschiedliche Anforderungen und bedingen zwangsläufig, vergleichbar wie bei jeder anderen edv-technischen Komponente, unterschiedliche elektronische Signaturen und Zertifikate.

So verwenden die österreichischen Gesetze derzeit - ohne Anspruch auf Vollständigkeit - folgende unterschiedlich definierte elektronische Signaturvarianten:

- **Verwaltungssignatur** (§18 Allgemeines Verwaltungsverfahrensgesetz):
  Hier wird nur eine elektronische Signatur ohne weitere besondere Eigenschaften gefordert, eine allgemeine Signatur gem. §2 Z1 SigG.
- **Archivsignatur** (§91c Gerichtsorganisationsgesetz, §1 Urkundenarchivverordnung 2007):
  Hier ist für den Abruf von Dokumenten eine "fortgeschrittene" Signatur vorgesehen.
- **Anwaltsignatur** (§21 Rechtsanwaltsordnung):
  Hier ist eine "qualifizierte" Signatur mit der zwingenden Angabe der Berufsbezeichnung als zusätzliches Attribut im Zertifikat vorgesehen, weiters wird ausdrücklich die Verwendung von Pseudonymen verboten.
- **Ziviltechnikersignatur** (§16 Ziviltechnikergesetz 1993):
  Hier ist eine "qualifizierte" Signatur vorgesehen, bei der ausdrücklich die Verwendung von Pseudonymen verboten ist.
- **Notarsignatur** (§§13f Notariatsordnung):
  Hier ist eine "qualifizierte" Signatur vorgesehen, die nur für die Beurkundung verwendet werden darf.
- Signatur lt. Abschlussprüfungs-Qualitätssicherungsgesetz (Art. 1 §§23f):
  Hier ist eine "fortgeschrittene" Signatur vorgesehen.
- Signatur lt. Verordnung des BMF "**eBilling-Signatur**" (BGBl. II Nr. 583/2003 Art. 1):
  Hier ist eine "fortgeschrittene" Signatur vorgesehen.
- **Bürgerkarten-Signatur** (§2 E-Government-Gesetz):
  Zusätzlich zur Signatur ist eine spezifische Personenbindung erforderlich.
- **Amtssignatur** (§19 E-Government-Gesetz):
  Hier ist eine allgemeine Signatur gem. §2 Z1 SigG, jedoch mit einem Zertifikat vorgesehen das durch ein zusätzliches Attribut auf die signierende Behörde verweist. Die Eigenschaften werden zusätzlich, abweichend vom Signaturgesetz in der Verordnung "Regelung der sicherheitstechnischen und organisationsrelevanten Voraussetzungen für Verwaltungssignaturen (VerwSigV)" geregelt.
- Serverzertifikat (§4 Gesundheitstelematikgesetz):
  Hier ist eine allgemeine Signatur gem. §2 Z1 SigG vorgesehen, jedoch spezifisch für den Maschine-Maschine-Einsatz.
- Signatur lt. Bundesgesetzblattgesetz (§8):
  Hier wird nur eine elektronische Signatur ohne weitere besondere Eigenschaften gefordert, eine allgemeine Signatur gem. §2 Z1 SigG .
- Signatur lt. Bundeshaushaltsgesetz (§68):
  Hier wird nur eine elektronische Signatur ohne weitere besondere Eigenschaften gefordert, eine allgemeine Signatur gem. §2 Z1 SigG.

- Signatur lt. Verordnung zum elektronischen Rechtsverkehr(§1):
  Hier wird nur eine elektronische Signatur ohne weitere besondere Eigenschaften gefordert, eine allgemeine Signatur gem. §2 Z1 SigG.
- Signatur lt. Ergänzungsregisterverordnung (§16):
  Hier ist eine allgemeine Signatur gem. §2 Z1 SigG, jedoch mit einem Zertifikat vorgesehen das durch ein zusätzliches Attribut auf die signierende Behörde verweist (=Amtssignatur).
- Signatur lt. Firmenbuchgesetz (§34):
  Hier wird nur eine elektronische Signatur ohne weitere besondere Eigenschaften gefordert, eine allgemeine Signatur gem. §2 Z1 SigG.
- Signatur lt. Gerichtsorganisationsgesetz (§89b) / Verordnung elektronischer Rechtsverkehr:
  Hier wird nur eine elektronische Signatur ohne weitere besondere Eigenschaften gefordert, eine allgemeine Signatur gem. §2 Z1 SigG.
- Signatur lt. Meldegesetz-Durchführungsverordnung (§15):
  Hier ist eine allgemeine Signatur gem. §2 Z1 SigG, jedoch mit einem Zertifikat vorgesehen das durch ein zusätzliches Attribut auf die signierende Behörde verweist (=Amtssignatur).
- Signatur lt. Zahnärztegesetz (§12):
  Hier wird nur eine elektronische Signatur ohne weitere besondere Eigenschaften gefordert, eine allgemeine Signatur gem. §2 Z1 SigG.

Dieser in der Praxis erforderlichen und sinnvollen Differenzierungen wird jedoch im vorliegenden Entwuf zur Änderung des Signaturgesetzes nicht Rechnung getragen. Hier werden nur "qualifizierte" Signaturen geregelt. Auch die an sich sinnvolle Neudefinition der "fortgeschrittenen" Signatur bleibt mangels klarer Regelungen unzureichend.

Gerade um Rechtssicherheit zu erreichen wäre es notwendig, dass für die verschiedenen Signaturvarianten angemessene Bestätigungs- und Informationspflichten vorgesehen werden, die es den Nutzern dieser Signaturdienste ermöglichen zu überprüfen, welche elektronische Signatur für welche Zwecke geeignet ist.

Diese sinnvolle Aufsichts- und Kontrolltätigkeit wird jedoch, entgegen der jetzigen Situation eingeschränkt, statt erweitert und präzisiert.

1.7. Verlust der Informationssicherheit

Einen Beitrag zur Verunsicherung und damit zum Vertrauensverlust in "elektronische Signaturverfahren" leistet die neu geplante Regelung, indem sie die Zuständigkeit der Aufsichtsbehörde drastisch zu beschneiden.

Bisher hat die Aufsichtsbehörde alle in Österreich öffentlich angebotenen Signatur- und Zertifizierungsdienste einer Prüfung unterzogen und abhängig von den Verfahren sie für bestimmte Eigenschaften als geeignet erklärt. Derzeit werden dazu drei Ebenen verwendet, die die "sichere", die "fortgeschrittene" und die "gewöhnliche" elektronische Signatur.

Dies hat sowohl für Zertifizierungsdienstanbieter und Nutzer Informations- und somit Rechtssicherheit geschaffen. Der Zertifizierungsdienstanbieter konnte auf einfache Weise

auf die Einhaltung der gesetzlichen Bestimmungen verweisen, der Nutzer konnte durch Konsultation dieser Veröffentlichung sicher sein, für die geplante Anwendung das richtige Produkt auszuwählen.

Diese Vorgangsweise wäre auch konform zur EG-Signaturrichtlinie 1999/93/EG.

Tatsächlich ist die bisherige Differenzierung vielfach zu ungenau und zielte statt sinnvollerweise auf die rechtlich wesentliche Zertifikats- bzw. Identitätsprüfung bloß auf das technische Signaturverfahren.

Statt den bisherigen sinnvollen Ansatz durch entsprechende gesetzliche Regelungen zu verbessern, wird diese für die Nutzer wertvolle Informationsquelle vorsätzlich und sachlich unbegründet, reduziert.

Es wird daher vorgeschlagen, die Zuständigkeit der TKK/RTR GmbH als Registrierungs- und Prüfstelle für alle öffentlich angebotenen Signaturverfahren grundsätzlich bei zu behalten, die Anrufung bzw. die Befassung der Stelle durch Zertifizierungsdienstanbieter jedoch auf freiwillige Basis zu stellen.

Gleichzeitig wird vorgeschlagen, dass die Aufsichtsstelle den unterschiedlichen Anforderungen zur elektronischen Signatur (Verwaltungssignatur, Archivsignatur, Anwaltsignatur, Notarsignatur, usw, wie sie mittlerweile in einer Reihe von Gesetzen bestehen) dahingehend Rechnung trägt, dass sie die Eignung bestimmter Angebote für derartige Anwendungen bestätigen kann. Weiters sollte die Qualität des durch den Diensteanbieter ausgestellten Zertifikates (bzw. der Identitätsprüfung) und nicht der technischen Signatur im Vordergrund der Prüfung sein.

Für die Nutzer dieser Dienste wäre damit Rechtssicherheit geschaffen, die Verbreitung von Signaturanwendungen in spezifischen Bereichen wäre damit wesentlich erleichtert.

1.8. Umfang der Gesetzesänderungen

Neben dem Signaturgesetz sollten auch eine Reihe anderer Gesetze angepasst werden. Im wesentlichen sind das das "Gerichtsorganisationsgesetz", das "Bankwesengesetz", die "Rechtsanwaltsordnung", die "Notariatsordnung", das "Ziviltechnikergesetz", das "Versicherungsaufsichtsgesetz", das "Rezeptpflichtgesetz" und die "Gewerbeordnung 1994".

Bedenklich und in geradezu fahrlässiger Weise wird mit der sensitiven Materie elektronische Signatur umgegangen, wenn nicht einmal alle im Begleitschreiben angekündigten Gesetzesänderungen zur Begutachtung verschickt werden. So fehlen die Änderungen zum "Bundesgesetz zur Vergabe von Aufträgen" vollständig.

Die mangelhafte Qualität des Gesetzesvorschlages wird allein dadurch deutlich, dass eine Reihe weiterer gesetzlicher Bestimmungen nicht angepasst werden sollen, sodass in Zukunft in einer Reihe von Gesetzen auf nicht mehr existierende "sichere" Signaturen verwiesen wird oder in anderen Bestimmungen direkt auf die Bestimmungen der EG-Richtlinie oder andere EU-Rechtsbestimmungen.

Dies hätte zur Folge, dass Betroffene (Zertifizierungsdiensteanbieter, Aussteller von elektronischen Signaturen und Empfänger elektronischer Signaturen) eine noch geringere Rechtssicherheit als bisher hätten, ob eine bestimmte Signatur tatsächlich den gesetzlichen Anforderungen entspricht und auf welcher Grundlage sie beruht.

Insgesamt vermitttelt der Entwurf eine konzept- und ziellose Orientierung, getragen vom Wunsch bisher funktionierende Aufsichtseinrichtungen zu reduzieren, ohne jedoch erkennbare Verbesserungen in der Rechtssicherheit herbeizuführen.

Besonderer Teil

Zu § 1 Abs. 3 des Entwurfs:

Die Beschränkung des Anwendungsbereiches des Gesetzes auf qualifizierte Zertifikats- und Zeitstempeldienste und die damit verbundene Beschränkung der Aufsicht- und Informationsrechte der Aufsichtsstellen ist aus Sicht der Rechtssicherheit für Nutzer von Signaturdiensten abzulehnen.

Gerade die Verzeichnis- und Informationsdienste der bisherigen Aufsichtsstelle haben es Nutzern von Signaturdiensten ermöglicht leicht und automatisiert die Gültigkeit und den Geltungsbereich bestimmter Signaturdienste zu prüfen. Für die erleichterte Verbreitung von Signaturdiensten sinnvoller wäre es daher, diese Verzeichnis- und Informationsdienste auf eine fundierte rechtliche Grundlage zu stellen und die Aufsichtsstellen zu ermächtigen, diese Verzeichnisdienste auch gemäß den Erfordernissen des Marktes und der Vielfalt der Signaturformen auszubauen.

Zu § 2 Z2 des Entwurfs:

Die vorgeschlagene Gleichstellung von Personen und "sonstigen rechtsfähigen Einrichtungen" als Signatoren muss als höchst problematisch abgelehnt werden. Sie ist sachlich nicht gerechtfertigt und erhöht zusätzlich die Rechtsunsicherheit.

Nach österreichischem Rechtsverständnis können nur Personen rechtsverbindliche Handlungen setzen und nicht juristische Einrichtungen oder Körperschaften. Bei diesen können nur Organe oder befugte Vertreter rechtsverbindliche Handlungen setzen.

Zu § 2 Z3 des Entwurfs:

Ausdrücklich begrüßt wird die Definition der fortgeschrittenen Signatur . Hier wurde eine längst fällige Klarstellung und Umsetzung der EG-Richtlinie vorgenommen. Leider verabsäumt es jedoch der Entwurf in weiterer Folge ausreichende und für die Nutzer der Signaturdienste nachvollziehbare Rechtsfolgen zu definieren.

Sinnvoll wäre die Festlegung von Aufsichts- und Registrierungspflichten, aber auch Informationspflichten der Diensteanbeiter gewesen. Diese hätten Rechtssicherheit bei den Benutzern derartiger Verfahren geschaffen und wären eine sinnvolle Ergänzung zu einer Reihe von einzelgesetzlichen Regelungen gewesen, in denen auf "fortgeschrittene Signaturverfahren" ausdrücklich Bezug genommen wurde.

Zu § 2 Z3a des Entwurfs:

Die Änderung des Begriffs "sichere Signatur" auf "qualifizierte Signatur" löst nicht das in den Erläuterungen beschriebene Problem, dass als Gegensatzpaar zur sicheren Signatur heute vielfach missverständlicher weise die "unsichere" Signatur angesehen wird.
In Zukunft wird dann stattdessen als Gegensatz zur "qualifizierten" Signatur fälschlicherweise die "unqualifizierte" angesehen werden.

Mit dem bloßen Austausch von Worten wird somit nichts gewonnen, im Gegenteil wird die Begriffsverwirrung und Rechtsunsicherheit bloß erhöht.

Sinnvoll wäre hingegen, so wie im Sicherheits- und Geheimhaltungsbereich weltweit üblich eine Stufenlösung, etwa mit drei bis vier Anforderungsstufen , in denen sowohl die Sicherheits-, als auch die Zertifizierungsanforderungen und die Anforderungen der Identitätsprüfung definiert werden könnten.

Dies würde sowohl die Rechtssicherheit der Nutzer erhöhen, sie könnten leichter erkennen, welche elektronische Signaturverfahren für welche Bereiche anzuwenden sind, gleichzeitig würde es die Gesetzgebung in diesem Bereich erheblich erleichtern, da sich in Zukunft der Gesetzgeber jeweils auf eine der Anforderungsstufen beziehen könnte.

Dieser Stufenlösung angepasst könnten dann die Offenlegungs-, Registrierungs- und Aufsichtspflichten definiert werden.

Zu § 8 Abs.1 des Entwurfs:

Grundsätzlich wird begrüßt dass auch andere Formen des Identitätsnachweises, als die Prüfung eines vorgelegten amtlichen Lichtbildausweises möglich sind. Leider bleibt die verwendete Formulierung "durch einen anderen in seiner Zuverlässigkeit gleichwertigen, dokumentierten oder zu dokumentierenden Nachweis" vage und unbestimmt.

Vorgeschlagen wird, vergleichbar der Regelung im §40 Abs.8 Z1 Bankwesengesetz, der ausdrückliche Verweis auf die Möglichkeit der "Zustellung zu eigenen Handen" (im Sinne §21 Zustellgesetz) als zulässige Variante der Identitätsprüfung aufzunehmen.

Zu § 13 Abs. 3 des Entwurfs:

Die Führung des Verzeichnisdienstes ist widersprüchlich geregelt. Durch die nunmehr geplante Beschränkung der Wirkung des Gesetzes auf qualifizierte Zertifikats- und Zeitstempeldienste gibt es für andere Zertifizierungsdienstanbieter keine Möglichkeit zur Aufnahme in die offiziellen Verzeichnisdienste der Aufsichtsstelle.

Gleichzeitig bleibt jedoch diese Möglichkeit für ausländische Zertifizierungsdienstanbieter (ZDAs) bestehen: "Auf Antrag sind auch andere im Ausland niedergelassene ZDA in dieses Verzeichnis aufzunehmen. In das Verzeichnis der Zertifikate für ZDA sind deren Zertifikate für die Erbringung von Zertifizierungsdiensten einzutragen."

Dies führt zu einer sachlich nicht gerechtfertigten und letztlich EU-widrigen

Ungleichbehandlung inländischer und ausländischer Zertifizierungsdienstanbieter.

Es wird daher vorgeschlagen die Aufnahme sonstiger inländischer Zertifizierungsdienstanbieter in den Verzeichnisdiensten der Aufsichtsstelle ausdrücklich vorzusehen.

Änderung des Bundesvergabegesetzes:

Die im Begleitbrief zum Entwurf angekündigten Änderungen des Bundesvergabegesetzes, die auch bei Änderung des Signaturgesetzes dringend erforderlich wären, fehlen. Ebenso fehlen eine Reihe von weiteren Gesetzesanpassungen, die auf die bisherigen alten, und nach den Vorschlägen nicht mehr in Kraft befindlichen Bestimmungen des Signaturgesetzes Bezug nehmen.

Obwohl grundsätzlich Änderungen des Signaturgesetzes überfällig und zu begrüßen sind, gehen die meisten der vorgeschlagenen Änderungen in eine falsche, am Markt vorbei gehende Richtung. Es wird daher nochmals dringend empfohlen den Entwurf zurückzuziehen und jedenfalls gemeinsam mit den bisherigen Zertifizierungsdienstanbietern und der Aufsichtsbehörde neu zu überarbeiten.