Bundeskanzleramt
z. Hd. Dr. Waltraud Kotschy
Ballhausplatz 1
1014 Wien

ANOR 2/2003-2 Wien, am 25.08.2003
DK/UL

Betreff: Stellungnahme der RTR-GmbH zum Begutachtungsentwurf des e-Government-Gesetzes

Sehr geehrte Frau Dr. Kotschy,

im Folgenden übermittelt die RTR-GmbH ihre Stellungnahme zum Begutachtungsentwurf dieses Gesetzes:

A. Allgemeines

Die RTR-GmbH begrüßt, dass e-Government nun mit einem Gesetz über Erleichterungen des elektronischen Verkehrs mit öffentlichen Stellen gefördert werden soll.

In einigen Punkten (die im Folgenden detaillierter ausgeführt werden) hat die RTR-GmbH aber Bedenken gegen den vorgelegten Gesetzesentwurf:

- **„Verwaltungssignatur“**: Mit einer Übergangsbestimmung (§ 25 e-GovG) soll bis zum 01.01.2010 auf die im Signaturgesetz geregelte sichere elektronische Signatur verzichtet werden können, obwohl diese mittlerweile seit Februar 2002 verfügbar ist und eine Reihe von Unternehmen beträchtliche Investitionen getätigt haben, um sie kommerziell anbieten zu können. Stattdessen führt der Entwurf den Begriff der „Verwaltungssignatur“ ein. Für diese wird ein deutlich niedrigerer Sicherheitsstandard angestrebt als bisher vorgesehen. Insbesondere würde vom bewährten Konzept abgegangen, dass die Sicherheit der Signatur auch darauf beruht, dass sie mit Mitteln erstellt wird, die der Signator unter seiner alleinigen Kontrolle halten kann. Weiters würde das etablierte Aufsichtssystem des SigG für die „Verwaltungssignatur“ umgangen. Im einzelnen würden die Sicherheitsanforderungen laut Entwurf nicht durch das Gesetz oder durch Verordnung geregelt werden, sondern ausschließlich durch Gutachten einer Bestätigungsstelle, also offenbar nur durch Anforderungen an die verwendeten Produkte. Für die Einhaltung der

Anforderungen aus den Gutachten sowie für organisatorische Anforderungen gäbe es kein Aufsichtssystem.

- **Stammzahl und bereichsspezifische Personenkennzeichen**: Der Entwurf sieht aus Datenschutzgründen statt der Verwendung eines einheitlichen Personenkennzeichens (wie der Sozialversicherungsnummer oder der ZMR-Zahl) ein System von verschiedenen Zahlen und Kennzeichen vor, die eine Person bezeichnen. Die RTR-GmbH gibt dazu zu bedenken, dass es sich hierbei um ein sehr kompliziertes und daher fehleranfälliges Konzept handelt und das angestrebte Datenschutzziel nicht erreicht wird, so lange alle Zahlen aus der ZMR-Zahl errechnet werden können und die ZMR-Zahl einfach zugänglich ist.

- **Sicherheitskonzepte und Aufsicht**: Sowohl im Gesetzesentwurf als auch in den bisher veröffentlichten technischen Spezifikationen werden großteils nur Funktionalitäten beschrieben. Es gibt kaum Risikoanalysen, welche Fehler dabei auftreten könnten. Der Entwurf sieht nicht vor, dass die Anbieter von Zertifikaten für „Verwaltungssignaturen“, die Aussteller verschiedenster anderer elektronischer Bestätigungen (wie insbesondere der „Personenbindung“) oder die Betreiber von elektronischen Zustelldiensten ein Sicherheitskonzept haben müssen, das bestimmten Mindestanforderungen genügen müsste, oder dass sie einer Aufsicht unterliegen würden, die der im Signaturgesetz etablierten Aufsicht über Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate oder sichere elektronische Signaturen anbieten, vergleichbar wäre.

- **Rechtssetzungsverfahren für technische Konzepte**: Technische Spezifikationen würden dadurch verbindlich gemacht, dass sie „in geeigneter Form veröffentlicht“ werden. Die RTR-GmbH schlägt vor, technische Spezifikationen stattdessen mittels Verordnung festzulegen. Weiters sollte für die Anwender und die Wirtschaft auch die Sicherheit bestehen, dass einmal beschlossene Spezifikationen auch jeweils für einige Jahre von der Verwaltung unterstützt werden.

- **Datenschutz**: Im Zusammenhang mit den elektronischen Zustelldiensten gibt die RTR-GmbH zu bedenken, dass Datenschutzmaßnahmen bei den Verzeichnissen der Personen, welche die elektronische Zustellung akzeptiert haben, ergriffen werden sollten.

Soweit es uns möglich war, haben wir bei den jeweiligen Punkten auch Alternativen vorgeschlagen. In einigen Punkten sind wir der Ansicht, dass eine vertiefte Diskussion erforderlich wäre. Viele der vorliegenden technischen Konzepte sind sehr innovativ, werfen aber auch noch ungelöste Fragen auf, die auf verschiedene Art und Weise gelöst werden können. Die RTR-GmbH ist gerne bereit, auch an der weiteren Diskussion teilzunehmen und dabei ihr Expertenwissen und ihre Erfahrungen aus der Vollziehung des Signaturgesetzes einzubringen.

A. Allgemeines

A.1 „Verwaltungssignatur“

A.1.1 Strategieänderung im e-Government

Eine Übergangsbestimmung (§ 25 e-GovG) des Entwurfes sieht vor, dass bis zum 01.01.2010 auf die im Signaturgesetz geregelte sichere elektronische Signatur verzichtet werden kann. Dies bedeutet eine grundsätzliche Strategieänderung des e-Government. Bislang wurde – vor allem durch das Signaturgesetz – auf Sicherheit größter Wert gelegt. Die „Verwaltungssignatur“ würde die Sicherheitsanforderungen deutlich senken.

Seit dem 01.01.2000 ist in Österreich das Signaturgesetz in Kraft. In den Erläuterungen zur Regierungsvorlage ging man davon aus, dass die durch das Signaturgesetz geschaffenen Sicherheitsinfrastrukturen auch im öffentlichen Bereich Anwendung finden sollen. Die Regierungsvorlage erwartete positive Auswirkungen auf die Beschäftigung und den Wirtschaftsstandort, insbesondere durch die Beseitigung rechtlicher Unsicherheiten und Ungewissheiten, die sich als Investitionshindernis ausgewirkt hatten. Auf Grund des Gesetzes haben mehrere Unternehmen große Investitionen getätigt, um Zertifizierungsdienste nach dem Signaturgesetz anbieten zu können.

Die Anwendung der elektronischen Signatur in der Praxis war hingegen lange Zeit dadurch gehemmt, dass Anwendungsentwickler im e-Government und e-Business darauf gewartet haben, dass die Zertifizierungsdiensteanbieter qualifizierte Zertifikate und sichere elektronische Signaturen bereitstellen können. In den Jahren 2000 und 2001 war in der Diskussion die Meinung vorherrschend, dass für elektronische Verwaltungsverfahren überwiegend die sichere elektronische Signatur eingesetzt werden sollte.[1] Damals gab es auch Initiativen in der Verwaltung, die sichere elektronische Signatur im großen Stil zu fördern. Es gab etwa Überlegungen, das Personal der Verwaltung flächendeckend mit qualifizierten Zertifikaten auszustatten. Das Bundesrechenzentrum hatte für einen Rahmenvertrag dazu sogar ein Vergabeverfahren durchgeführt und einem Zertifizierungsdiensteanbieter den Zuschlag erteilt, allerdings wurde die Rahmenvereinbarung nie mit Leben gefüllt.

Die vom Signaturgesetz geforderten Sicherheitsinfrastrukturen sind nun alle verfügbar. Am 01.01.2000 hat die Telekom-Control-Kommission ihre Tätigkeit als Aufsichtsstelle für elektronische Signaturen aufgenommen, am 03.02.2000 wurde der Verein A-SIT Bestätigungsstelle nach § 19 SigG. Seit Februar 2002 sind qualifizierte Zertifikate für die sichere elektronische Signatur am Markt erhältlich, wobei inzwischen auch verschiedene Chipkartentypen unterstützt werden. Im September 2002 hat die Telekom-Control-Kommission ihre Public-

[1] Art. 3 Abs. 7 der Signaturrichtlinie 1999/93/EG sieht sogar vor, dass die Mitgliedstaaten den Einsatz elektronischer Signaturen im öffentlichen Bereich *zusätzlichen* Anforderungen unterwerfen können. In den ErläutRV zu § 1 Abs. 2 SigG wurde dazu ausgeführt: „Im Sinn der Bürgernähe (Stichwort ‚multifunktionale Chipkarten’) sollte nach Möglichkeit aber danach getrachtet werden, auch im öffentlichen Bereich mit den sicheren elektronischen Signaturen im Sinn des Signaturgesetzes das Auslangen zu finden.“

Key-Infrastruktur in Betrieb genommen und das sichere Verzeichnis der Zertifizierungsdiensteanbieter realisiert. Eine Reihe österreichischer Hersteller hat Produkte für die sichere elektronische Signatur (Chipkartenleser und Viewer) entwickelt, evaluieren und bescheinigen lassen und auf den Markt gebracht.

Da beim nächsten Rollout der Bankomatkarte im Jahr 2004 eine signaturfähige Karte flächendeckend in Umlauf gebracht wird, wird es spätestens dann auch zu einer entsprechenden Verbreitung von Chipkarten kommen.

Aus Sicht der RTR-GmbH ist nicht verständlich, warum die Verwaltung nun, wo nach beträchtlichen Investitionen aller Beteiligten sämtliche Bausteine für sichere elektronische Signaturen verfügbar sind, umschwenkt und den Einsatz der sicheren elektronischen Signatur in der Verwaltung durch eine Übergangsbestimmung (Entwurf des § 25 e-GovG) bis zum 01.01.2010 (!) aufschieben will.

Statt der sicheren elektronischen Signatur werden von der Stabsstelle IKT-Strategie nunmehr in öffentlichen Veranstaltungen und Musterapplikationen Formen der einfachen elektronischen Signatur gefördert, vor allem das Konzept „Bürgerkarte light“.[2] Bemerkenswert ist dabei, dass dabei vor allem ein Zertifizierungsdienst eines Mobilfunkanbieters präsentiert wird, der von diesem Mobilfunkanbieter noch gar nicht öffentlich angeboten wird, daher auch nicht gemäß § 6 Abs. 2 SigG der Aufsichtsstelle angezeigt wurde und nicht der Aufsicht unterliegt.

A.1.2 Vergleich der verschiedenen Sicherheitsstandards

§ 2 Z 3 SigG sieht als Voraussetzungen für die **sichere elektronische Signatur** die folgenden Anforderungen vor:

a) Die Signatur ist **ausschließlich dem Signator zugeordnet**. Voraussetzung dafür sind einerseits technische Maßnahmen (die Signaturerstellungsdaten dürfen nur einmal vorkommen), andererseits organisatorische Maßnahmen, vor allem Sicherheitsmaßnahmen beim Zertifizierungsdiensteanbieter und eine sichere Identitätsprüfung vor der Ausstellung eines Zertifikates.

b) Die Signatur ermöglicht die **Identifizierung des Signators**. Die zentrale Voraussetzung dafür ist die Identitätsprüfung anhand eines amtlichen Lichtbildausweises.

c) Die Signatur muss mit **Mitteln** erstellt werden, **die der Signator unter seiner alleinigen Kontrolle halten kann**. In diesem Zusammenhang wird immer wieder betont, dass die Signatur durch eine Kombination aus Besitz und Wissen gesichert wird. Der Signator signiert etwa mit einer Chipkarte, die er unter seiner Kontrolle halten kann. Die Chipkarte kann nur mit einem PIN-Code verwendet werden. Dieser dient einerseits als Sicherheit gegen

[2] Als Musterapplikation demonstriert wird z. B. die Applikation Meldebestätigung der Gemeinde Wien (http://www.help.gv.at/cgi-bin/system.pl?label=MeldebestaetigungWien), welche mit der „Bürgerkarte Light“ und mit der sicheren Signatur des Anbieters A-Trust bedient werden kann.

Diebstahl, andererseits ist die PIN-Eingabe aber auch die elektronische Form, mittels der der Signator seinen Willen erklärt.

d) Die Signatur wird mit den Daten, auf die sie sich bezieht, so **verknüpft**, dass jede **nachträgliche Veränderung der Daten festgestellt werden kann**. Dieses Kriterium ist in der Regel bei jedem Signaturverfahren verwirklicht, auch bei solchen, die ansonsten nicht besonders sicher sind.

e) Weiters muss die Signatur auf einem **qualifizierten Zertifikat** beruhen (dies impliziert vor allem eine Reihe von technischen und organisatorischen Anforderungen an den Zertifizierungsdiensteanbieter, der das Zertifikat ausstellt) und es müssen die Anforderungen des Signaturgesetzes und der Signaturverordnung an die verwendeten technischen **Komponenten** erfüllt sein (dazu gehört insbesondere die Evaluierung und Bescheinigung der Komponenten durch eine Bestätigungsstelle).

Die genannten Anforderungen sind durch die Signaturrichtlinie 1999/93/EG europaweit harmonisiert.

Die Anforderungen an die neu eingeführte „Verwaltungssignatur" sind im Gesetzesentwurf nicht spezifiziert. Aus dem, was der RTR-GmbH aus dem Entwurf des § 25 e-GovG, den Erläuterungen dazu und aus einem Schreiben der Stabsstelle IKT-Strategie vom 31.07.2003 bekannt ist, ergibt sich Folgendes:

a) **Ausschließliche Zuordnung an den Signator:** Weder der Gesetzesentwurf noch die Erläuterungen dazu noch das zitierte Schreiben sehen vor, dass es irgendwelche Anforderungen an die Identitätsprüfung gäbe. Die RTR-GmbH geht zwar davon aus, dass eine Identitätsprüfung anhand eines amtlichen Lichtbildausweises stillschweigend vorausgesetzt wird. Festgeschrieben ist dies aber nicht. Auch andere organisatorische Maßnahmen in diesem Zusammenhang fehlen.[3]

b) **Identifizierung des Signators**. An sich ist es ein zentrales Ziel der „Bürgerkartenfunktionalität", die Identifizierung in einem höheren Maße zu gewährleisten als mit einem qualifizierten Zertifikat. In einem qualifizierten Zertifikat muss nämlich nur der Name aufscheinen (das Geburtsdatum oder andere Daten können optional aufgenommen werden), was bei Namensgleichheit zu Verwechslungen führen kann. Im Streitfall kann zwar im Nachhinein problemlos exakt festgestellt werden, wer das Zertifikat verwendet hat, da der Zertifizierungsdiensteanbieter ja über zusätzliche Daten zur Person und vor allem auch über eine Kopie des amtlichen Lichtbildausweises verfügt. Aber damit eine Applikation der Verwaltung in Echtzeit und im vorhinein feststellen kann, um welchen Bürger es sich

[3] Beispielsweise ist auch vor dem Hintergrund des Signaturgesetzes durchaus denkbar, dass es zulässig sein kann, wenn der Zertifizierungsdiensteanbieter die Identität nicht bei der Ausstellung des Zertifikates prüft, sondern auf eine zuvor durchgeführte Identitätsprüfung vertraut. Allerdings sind dann zusätzliche Maßnahmen erforderlich. Beispielsweise kann man aus den von Vertragspartnern der Mobilfunkanbieter bei Vertragsabschluss erstellten Ausweiskopien nicht ohne weiteres schließen, dass der Anschluss Jahre später noch von der selben Person benutzt wird (z. B. Firmenhandys oder familieninterne Weitergabe des Gerätes). Wer sein Mobiltelefon bewusst an ein Familienmitglied weitergibt, geht ein finanzielles Risiko ein, aber er erteilt in der Regel keine Vollmacht, mit dem Gerät in seinem Namen gegenüber Behörden aufzutreten.

handelt, sind Zusatzinformationen erforderlich, die in der „Personenbindung“ nach § 4 Abs. 2 des Entwurfs des e-GovG geregelt sind.

Wie bereits unter a) erwähnt, sieht der Gesetzesentwurf aber keine Anforderungen an die Identitätsprüfung vor. Die Verwaltungssignatur würde daher Personen zwar sehr exakt mit ihrer Stammzahl bezeichnen, aber es könnte leicht vorkommen, dass die falsche Person „eindeutig identifiziert“ wird.

c) **Mittel, die der Signator unter seiner alleinigen Kontrolle halten kann.** Als Musterbeispiel für die „Verwaltungssignatur“ und die „Bürgerkarte light“ wird von der Stabsstelle IKT-Strategie derzeit ein System präsentiert, bei dem die Signatur nicht vom Bürger erstellt wird, sondern (nach Eingabe eines per SMS übersandten Einmalcodes in ein Webformular) stellvertretend für den Signator von seinem Mobiltelefonanbieter. In Diskussion sind hier zwar einige organisatorische Anforderungen (z. B. ein Vier-Augen-Prinzip für Zugriffe auf den entsprechenden Server), aber man kann jedenfalls nicht davon sprechen, dass der Signator seine Signaturerstellungsdaten unter seiner „alleinigen Kontrolle“ halten kann.

   In diesem Zusammenhang sei darauf verwiesen, dass es nach dem Diskussionsstand zur elektronischen Signatur, der dem Signaturgesetz zu Grunde gelegt wurde, als absolut unvertretbar galt, dass ein Signator seine Signaturerstellungsdaten jemand anderem überlässt. Vgl. dazu § 21 SigG, der als Pflicht des Signators (für alle Formen der elektronischen Signatur, nicht bloß für die sichere Signatur) vorschreibt, dass der Signator die Signaturerstellungsdaten sorgfältig verwahrt, soweit zumutbar Zugriffe auf Signaturerstellungsdaten verhindert und deren Weitergabe unterlässt. Diese Bestimmung verpflichtet den Signator auch dazu, den Widerruf des Zertifikates zu verlangen, wenn ihm die Signaturerstellungsdaten abhanden kommen. (Vgl. auch § 26 Abs. 1 SigG.)

   Die RTR-GmbH sieht durchaus, dass das Konzept der delegierten Signatur auch Vorteile hat – vor allem jenen, dass die Technologie der elektronischen Signatur damit leichter eine große Zahl von Anwendern finden könnte. Allerdings bestehen Bedenken, ob das Konzept mit dem § 21 SigG und auch mit dem neuen Gesetzesentwurf[4] in Einklang steht.

d) **Feststellbarkeit nachträglicher Veränderungen der Daten.** Wie erwähnt ist dieses Kriterium in der Regel bei jedem Signaturverfahren verwirklicht, auch bei solchen, die ansonsten nicht besonders sicher sind.

e) **Qualifiziertes Zertifikat, Anforderungen an technische Komponenten.** Das qualifizierte Zertifikat wird bei der „Verwaltungssignatur“ jedenfalls nicht verlangt. Damit fallen fast alle Anforderungen weg, die im Signaturgesetz

[4] Vgl. dazu § 5 Abs. 1 e-GovG, in welchem vorgesehen ist, dass die Stellvertretung dadurch in der elektronischen Welt abgebildet wird, dass der Bürger eine Vollmacht elektronisch signiert. Hier wird vorausgesetzt, dass der Bürger selbst signieren kann. Bei dem zitierten Konzept der delegierten Signatur im Rahmen der „Bürgerkarte light“ hingegen kann der Bürger gar nicht selbst signieren, sondern wird immer vertreten, wobei der Vertreter aber nicht als Vertreter auftritt, sondern so tut, als ob er der Signator wäre. Dies bedarf noch einer vertieften rechtlichen Diskussion und auch einer entsprechenden rechtlichen Verankerung.

und in der Signaturverordnung an den Zertifizierungsdiensteanbieter und an die Aufsicht über den Anbieter gerichtet werden. Es genügt, dass sich der Zertifizierungsdiensteanbieter an sein eigenes Konzept hält; dieses kann ziemlich knapp gehalten sein. Technische Anforderungen an die verwendeten Komponenten sind zwar in Diskussion, würden aber jedenfalls nicht die Evaluierung und Bescheinigung der Signaturerstellungseinheit vorsehen.

Von den fünf gesetzlichen Voraussetzungen an die sichere elektronische Signatur wäre bei der geplanten „Verwaltungssignatur" daher nur ein Kriterium erfüllt, nämlich jenes, das ohnehin bei fast jedem Signaturverfahren verwirklicht ist. Die im Entwurf des § 25 e-GovG enthaltenen Definition der „Verwaltungssignaturen" als „Signaturen, die die Voraussetzungen für sichere Signaturen weitgehend erfüllen" ist daher sehr beschönigend.

A.1.3 „Gutachten" statt Regelung der Anforderungen im Gesetz oder mit Verordnung

Wie erwähnt sieht der Entwurf des § 25 e-GovG keine konkreten Anforderungen an „Verwaltungssignaturen" vor, sondern beschreibt diese im Wesentlichen als Signaturen, die nicht allen Anforderungen an sichere elektronische Signaturen entsprechen.

Der letzte Satz dieser Bestimmung lautet: „Die hinreichende Sicherheit der eingesetzten Verfahren muss nach dem Gutachten einer Bestätigungsstelle gemäß § 19 SigG gegeben sein." Dies bedeutet im Ergebnis eine formalgesetzliche Delegation; die Anforderungen der Bestätigungsstelle für die Erstattung oder Nichterstattung des Gutachtens hätten faktisch die Wirkung einer Verordnung.[5] Geregelt ist weder, wer ein solches Gutachten zu beantragen hätte (der Zertifizierungsdiensteanbieter? der Hersteller einer technischen Komponente? die Behörde, die eine e-Government-Applikation basierend auf dem jeweiligen Signaturverfahren betreiben will?) und welche Rechtswirkungen ein solches Gutachten hätte (ist ein Anbringen von der Behörde gemäß § 13 Abs. 3 AVG zur Verbesserung zurückzustellen, wenn das Gutachten fehlt?). Offensichtlich gibt es auch keinen Rechtsschutz gegen die Verweigerung eines Gutachtens, kein Aufsichtssystem, mit dem die Einhaltung von im Gutachten genannten Bedingungen überprüft werden könnte, und es ist auch keine Möglichkeit vorgesehen, ein einmal erstelltes Gutachten wieder aufzuheben.

Problematisch wäre auch die Kompetenzüberschneidung zwischen der Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen nach dem Signaturgesetz und der Bestätigungsstelle als Normsetzer durch „Gutachten". Es könnte z. B. der Fall eintreten, dass die Bestätigungsstelle in einem Gutachten zum Ergebnis kommt, dass die „hinreichende Sicherheit" nach § 25 e-GovG vorliegt, dass die Aufsichtsstelle aber bei der Aufsicht über den Zertifizierungsdiensteanbieter feststellt, dass es nicht zutrifft, dass „die Voraussetzungen für sichere Signaturen weitgehend erfüllt" sind oder dass die

[5] Das Schreiben der Stabsstelle IKT-Strategie vom 31.07.2003 enthält einen ersten Diskussionsvorschlag für diese Anforderungen, der wie eine Verordnung formuliert und mit „Technisch-organisatorische Vorschriften" überschrieben ist.

gewählte Konstruktion im Hinblick auf eine Bestimmung des SigG sogar unzulässig ist.

A.1.4 Conclusio

Aus all den genannten Gründen regt die RTR-GmbH an, die Übergangsbestimmung gründlich zu überdenken. Die sichere elektronische Signatur ist verfügbar und es wäre wünschenswert, wenn sie in der Verwaltung auch möglichst bald breite Verwendung fände.

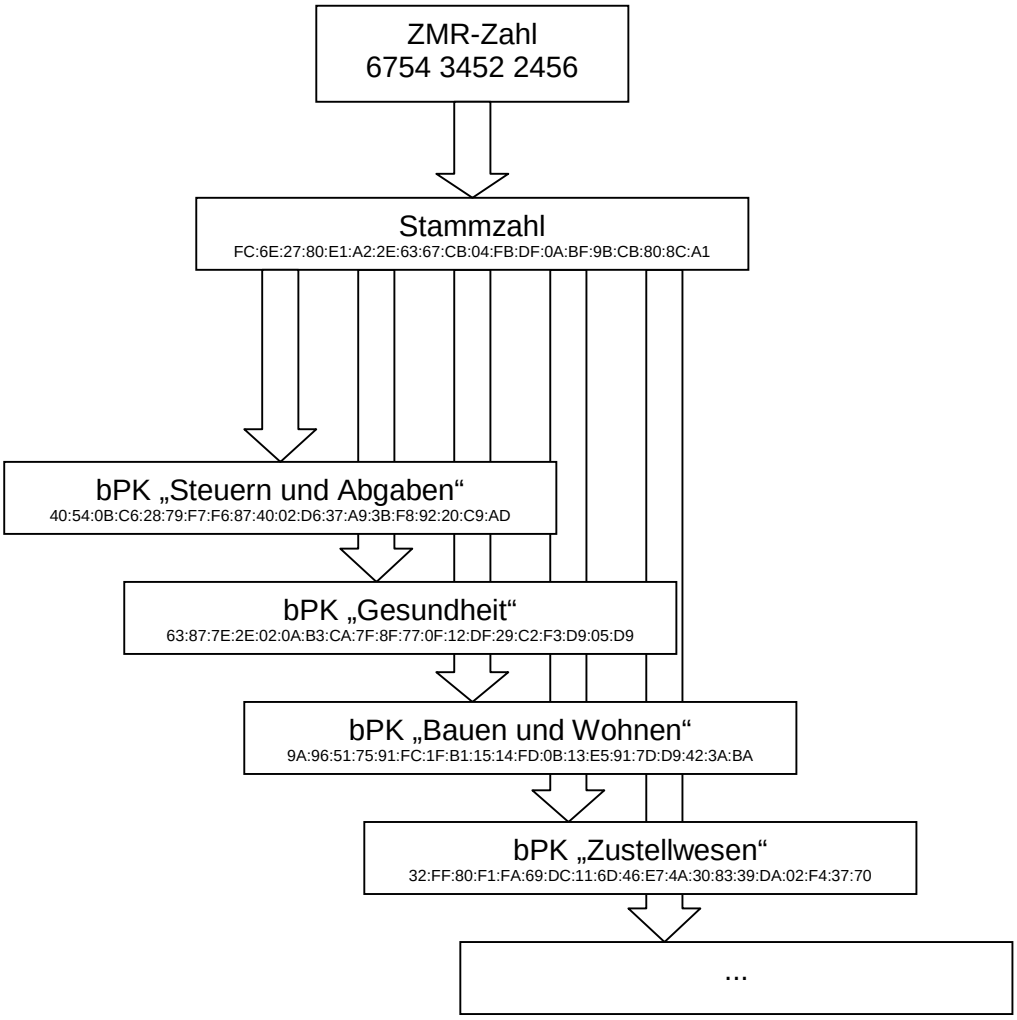
Wenn manche Anforderungen des SigG oder der SigV als für die Praxis zu streng angesehen werden, dann sollten diese Anforderungen im SigG oder der SigV angepasst werden (im Hinblick auf die SigV haben dazu ja auch schon Gespräche mit dem BMJ stattgefunden) anstatt im e-GovG gleich auf einen Großteil der technischen Anforderungen, fast alle organisatorischen Anforderungen und das bewährte Aufsichtssystem zu verzichten.

A.2 Stammzahl und bereichsspezifische Personenkennzeichen

Aus technischer Sicht wäre es für das e-Government natürlich das Einfachste, wenn es ein einheitliches Personenkennzeichen gäbe, das von allen Behörden verwendet wird. Es ist verständlich, dass es dagegen datenschutzrechtliche Bedenken gibt, es würde dadurch der „gläserne Bürger“ entstehen und es wäre für die Behörden leicht, alle Verfahren bei allen Bundes-, Landes- und Gemeindebehörden zu einem einzigen elektronischen Akt zusammenzuführen.

Das von der Stabsstelle IKT-Strategie des Bundes ausgearbeitete Konzept, technische Notwendigkeiten und datenschutzrechtliche Anforderungen zu vereinen, war schon bisher sehr kompliziert und nur für Personen verständlich, die sich im Detail damit befasst haben. Nun wird das Konzept durch den Entwurf neuerlich um eine Stufe komplizierter. An die Stelle der ZMR-Zahl, die bisher eine zentrale Rolle spielte (§ 13 Abs. 4a AVG) tritt die (typischerweise aus der ZMR-Zahl abgeleitete) Stammzahl. Der bislang verwendete Begriff der „verwaltungsbereichsspezifisch unterschiedlichen Personenkennzeichnung“ (VPK) wird nun durch das „bereichsspezifische Personenkennzeichen“ (bPK) ersetzt.

Um Missverständnisse zu vermeiden, führen wir im Folgenden aus, wie wir dieses Konzept verstanden haben. Die folgende Grafik zeigt die verschiedenen Zahlen, die nach dem Konzept eine Person bezeichnen können:



Die Pfeile bezeichnen dabei jeweils die im Entwurf als „Ableitung“ oder „mathematische Verfahren“ bezeichneten Funktionen. In den Erläuterungen zu § 8 e-GovG ist dabei ausgeführt, dass es sich dabei um „kryptographische Einwegableitungen, also nicht-umkehrbare Ableitungen“ handelt.[6] Weiters wird in den Erläuterungen ausgeführt: „Aus einer Stammzahl können zwar alle Ableitungen errechnet werden, nicht aber aus einer Ableitung die Stammzahl und auch nicht aus einer Ableitung die Ableitung für einen anderen Bereich.“

Dieses Konzept ist zwar grundsätzlich geeignet, dem datenschutzrechtlichen Wunsch zu entsprechen, dass Daten aus verschiedenen Verwaltungsbereichen nicht ohne weiteres zusammengeführt werden können.

Übersehen wird dabei aber, dass die Verwendung von kryptographischen Hash-Funktionen keineswegs garantiert, dass die Berechnung unumkehrbar ist. Die Sicherheit dieser Funktionen beruht darauf, dass jemand, der die

[6] In http://reference.e-government.gv.at/uploads/media/VPK-Algorithmus-20020221.pdf wird dafür der SHA-1-Algorithmus verwendet, die abgeleiteten Zahlen sind daher 160 Bit (20 Byte) lang. In der Grafik wurden jeweils 20 Byte in hexadezimaler Darstellung angeführt.

Berechnung umkehren will, keine Information über den Ausgangswert hat und daher eine so große Anzahl von Möglichkeiten durchprobieren müsste, dass dies in absehbarer Zeit auch mit großer Rechnerleistung nicht möglich ist. Die Unumkehrbarkeit ist aber natürlich nicht gegeben, wenn über den Ausgangswert Zusatzinformationen bekannt sind, die den Aufwand des Durchprobierens deutlich reduzieren. Da nach dem vorgeschlagenen Konzept im Regelfall die ZMR-Zahl den Ausgangswert für die Berechnung aller relevanten Zahlen bildet und alle Behörden auf das Zentrale Melderegister zugreifen können[7], kann die Behörde leicht die ZMR-Zahl ermitteln und daraus nach den veröffentlichten[8] mathematischen Verfahren ohne weitere Probleme auch die Stammzahl und alle bereichsspezifischen Personenkennzeichen errechnen.

Der im Entwurf vorgesehene hohe Aufwand zur Geheimhaltung der Stammzahl (§§ 4 bis 16, insbesondere § 10, § 12 und § 15 eGov-G-Entwurf) ist also sinnlos, so lange die Stammzahl und die bereichsspezifischen Personenkennzeichen sich leicht aus der nicht geheim gehaltenen ZMR-Zahl ableiten lassen.

In diesem Zusammenhang sei auch darauf verwiesen, dass im Entwurf für § 29 Abs. 2 ZustellG vorgesehen ist, dass es einen eigenen Verwaltungsbereich „Zustellwesen“ geben soll. Es wird demnach auch jeder Bürger ein eigenes bereichsspezifisches Personenkennzeichen für diesen Bereich haben und alle Behörden, die dem Bürger ein Dokument elektronisch zustellen wollen, müssen dieses bereichsspezifische Personenkennzeichen kennen.[9] Es ist also zu erwarten, dass das „bereichsspezifische“ Personenkennzeichen für den Bereich „Zustellwesen“ sich in der Praxis zu einem Personenkennzeichen entwickeln wird, das in der gesamten Verwaltung zum Einsatz kommen wird. Das datenschutzrechtliche Ziel, ein allgemeines Personenkennzeichen zu vermeiden, wäre damit obsolet.

A.3 Sicherheitskonzepte und Aufsicht

Sowohl im Gesetzesentwurf als auch in den bisher veröffentlichten technischen Spezifikationen werden großteils nur Funktionalitäten beschrieben. Es gibt kaum Risikoanalysen, welche Fehler dabei auftreten könnten.

Die grundsätzliche Vorgangsweise im Bereich der IT-Sicherheit ist die, dass man zuerst eine Risikoanalyse erstellt, welche Gefahren auftreten könnten, und dass auf der Grundlage dessen ein Sicherheitskonzept erstellt wird, das die einzelnen Maßnahmen zur Abwehr dieser Risiken enthält.

---

[7] Nach § 16 Abs. 9 MeldeG **müssen** Behörden, die Bundesgesetze vollziehen und elektronischen Zugriff auf das ZMR haben, sogar in jedem Einzelfall zugreifen, um sich „von der sachlichen Richtigkeit ihrer Wohnsitzanknüpfung zu überzeugen“ – also in allen Fällen, in denen die Zuständigkeit vom Wohnsitz einer Partei des Verfahrens abhängt.

[8] § 6 Abs. 5 und § 8 Abs. 1 eGov-G-Entwurf

[9] In http://www.cio.gv.at/onlineservices/delivery/Zustellung_Prozessbeschreibung_20030506.pdf, Kapitel 4 sind auch andere Formen der Zustellung beschrieben, bei denen der Empfänger nicht durch seine bPK für den Bereich „Zustellwesen“ (dort „VPK-Zustellung“ genannt), sondern durch Name, ZMR-konforme Adresse und Geburtsdatum oder durch Name und Verständigungsadresse bezeichnet wird. Allerdings ist davon auszugehen, dass vor allem die Form der Zustellung mit der bPK angewendet werden wird.

Gerade im Bereich der elektronischen Signatur und der dazu erforderlichen Zertifizierungsdienste ist dies eine bewährte Praxis. Für die Erstellung von Sicherheitskonzepten gibt es international anerkannte Kriterien, deren Einhaltung sicher stellt, dass kein in der internationalen Diskussion erkanntes Risiko übersehen wird. Das Signaturgesetz hat die Anforderung, ein Sicherheits- und Zertifizierungskonzept zu erstellen und zu befolgen, in die österreichische Rechtsordnung übernommen und ein Aufsichtssystem etabliert, durch welches die Einhaltung dieser Anforderung sicher gestellt wird,

Im Bereich des e-Government wird es nun eine Reihe von anderen elektronischen Bescheinigungen geben, von deren inhaltlicher Richtigkeit die Sicherheit des e-Government abhängig ist. Als herausragendes Beispiel ist dabei die sogenannte „Personenbindung“ (§ 4 Abs. 2 e-GovG) zu nennen, durch welche einer Person ihre Stammzahl (siehe oben A.2) zugeordnet wird.

Der RTR-GmbH ist keine Risikoanalyse zu den Risken bei der Ausstellung der Personenbindung (z. B. dass die Identität schlampig geprüft und daher die falsche Stammzahl zugeordnet wird) bekannt und auch kein Sicherheitskonzept, das Maßnahmen zur Abwehr dieser Risken vorsehen würde (z. B. dass der Bund Verträge mit denjenigen schließt, die die Identität prüfen, und diese darin zur Einhaltung gewisser Mindestanforderungen verpflichtet).

Auch der Entwurf des e-GovG enthält keine Sicherheitsanforderungen an die Ausstellung von Personenbindungen. Zu diskutieren wären hier etwa die folgenden Anforderungen:

- die generelle Anforderung, dass die Stammzahlenregisterbehörde für die Ausstellung der Personenbindungen ein Sicherheitskonzept erstellt und dieses im Betrieb einhält,

- dass Personenbindungen nur ausgestellt werden dürfen, nachdem die Identität der Person anhand eines amtlichen Lichtbildausweises überprüft wurde,

- dass die Stammzahlenregisterbehörde, wenn sie die Identität wie geplant nicht selbst prüft, Verträge mit jenen Zertifizierungsdiensteanbietern abschließt, auf deren Identitätsprüfung sie sich verlässt,

- wer für allfällige Fehler bei der Ausstellung der Personenbindung haftet und

- dass es eine Methode gibt, fehlerhaft oder falsch ausgestellte Personenbindungen über einen Widerrufsdienst zu widerrufen.

- Weiters wären alle Anforderungen zu diskutieren, die derzeit an Aussteller qualifizierter Zertifikate gestellt werden (z. B. Ausbildung und Zuverlässigkeit des Personals, Zutritts- und Zugriffsschutz, Verfügbarkeit, Sicherheit der technischen Komponenten, ...).

Die selbe Fragestellung ergibt sich in verstärktem Maße bei der im Entwurf des § 5 Abs. 2 e-GovG vorgesehenen Möglichkeit der elektronischen Bestätigung des Bestehens eines Vollmachtsverhältnisses (gemeint ist wohl nicht die Vollmacht, sondern die organmäßige Vertretung) durch die Stammzahlenregisterbehörde. Die organmäßige Vertretung einer juristischen Person kann sich häufig und rasch ändern. Es besteht hier also jedenfalls der Bedarf, dass die Stammzahlenregisterbehörde in der Lage ist, bei einem Erlöschen der Vertretungsbefugnis die ausgestellte Bestätigung zu widerrufen und dafür einen entsprechend sicheren Widerrufsdienst zu betreiben.

Als Alternative für die Schaffung technisch aufwändiger Sicherheits-infrastrukturen im Bereich der Stammzahlenregisterbehörde könnte auch – im Sinne der Überlegungen bei der Erlassung des Signaturgesetzes – erwogen werden, die Ausstellung solcher elektronischer Bestätigungen nicht zu monopolisieren, sondern dem Markt zu überlassen. Die Personenbindungen und Bestätigungen über das Bestehen einer Vertretungsbefugnis sind ihrem Wesen nach Attributzertifikate (Zusatzinformationen zu einem Zertifikat). Würde der Anwendungsbereich des Signaturgesetzes einfach um Attributzertifikate erweitert, dann könnten die genannten Bestätigungen mit der vorhandenen Sicherheitsinfrastruktur der Zertifizierungsdiensteanbieter ausgestellt werden, wobei bestehende Sicherheits- und Zertifizierungskonzepte und das bestehende Aufsichtssystem ohne viel Zusatzaufwand mitgenutzt werden könnte.

Im Entwurf des § 28 Abs. 2 Zustellgesetz ist eine Reihe von Anforderungen an elektronische Zustelldienste genannt. Es handelt sich dabei ausschließlich um funktionale Anforderungen. Der elektronische Zustelldienst muss die zuzustellenden Dokumente entgegennehmen, Aufzeichnungen über die Abholung der Dokumente führen, den Zustellnachweis an die Behörde übermitteln etc.

Anforderungen an die Datensicherheit hingegen werden nicht gestellt. Zu diskutieren wären hier etwa die folgenden Anforderungen:

- die generelle Anforderung, dass der Betreiber des elektronischen Zustelldienstes ein Sicherheitskonzept erstellt und dieses im Betrieb einhält,

- eine bestimmte Mindestverfügbarkeit über das Jahr gemessen

- bestimmte Maßnahmen, um die Verfügbarkeit sicher zu stellen, z. B. mehrfache physikalische Anbindung an das Internet, Clusterbetrieb des Zustellservers, Bereithaltung eines Ersatzsystems für Wartungsarbeiten und Ausfälle, Betrieb des Zustelldienstes an zwei verschiedenen Standorten, ...

- Anforderungen an das Personal des Betreibers des Zustelldienstes (z. B. im Hinblick auf Ausbildung oder Zuverlässigkeit, vgl. § 10 Abs. 4 und 5 SigV)

- finanzielle Anforderungen (Mindestkapital) und/oder Abschluss einer Haftpflichtversicherung

- Datensicherheitsanforderungen, insbesondere im Hinblick auf den Zugriffsschutz zu dem von den elektronischen Zustelldiensten zu führenden Verzeichnissen der Personen, die sich beim Zustelldienst haben registrieren lassen

Der Entwurf sieht nur die Zulassung zum elektronischen Zustelldienst vor. Ein Aufsichtssystem wird nicht eingerichtet. Ebenso fehlen Regelungen dazu, unter welchen Voraussetzungen eine einmal erteilte Zulassung wieder zu entziehen ist.

A.4 Rechtssetzungsverfahren für technische Konzepte

Maßgebliche Bedeutung für die Funktion des e-Government haben die einzelnen technischen Spezifikationen. Diese technischen Spezifikationen sind für alle Anwendungsentwickler unumgänglich. Wenn die in einem Unternehmen oder von einem Bürger eingesetzte Software sich nicht an die von der Verwaltung vorgegebenen Spezifikationen hält, wird die elektronische Eingabe vom Server der Verwaltung einfach zurückgewiesen werden.[10]

Wer die Spezifikationen vorgibt, setzt also faktisch Recht und entscheidet, in welchem Wege der elektronische Zugang zur Verwaltung möglich ist und in welchem Wege nicht. Vor diesem Hintergrund erscheint es problematisch, dass zentrale Spezifikationen nicht mittels Verordnung kundzumachen wären, sondern nur „in geeigneter Form zu veröffentlichen sind“ (§ 4 Abs. 4, § 6 Abs. 6, § 8 Abs. 1, § 10 Abs. 2 und § 21 e-GovG), wobei an manchen Stellen des Entwurfs nicht einmal vorgesehen ist, wer die Veröffentlichungen vorzunehmen hat. Zahlreiche der bereits erstellten Spezifikationen (etwa die Spezifikationen des Zustellservice) werden im Entwurf nicht einmal angesprochen. Die derzeitige Praxis in diesem Zusammenhang ist unbefriedigend. Spezifikationen werden an unterschiedlichen Stellen[11] veröffentlicht, wobei nicht immer klar ist, welches Gremium die Spezifikation beschlossen und wer die Veröffentlichung vorgenommen hat. Weiters hat die Aufsichtsstelle feststellen müssen, dass manche Bundesbehörden der Rechtsansicht sind, die vom Bund bislang veröffentlichten Spezifikationen seien „unbeachtlich, da sie keine Rechtswirkungen haben“[12].

---

[10] Zu analysieren wäre das Verhältnis dieser technischen Zurückweisung durch eine Fehlermeldung zu der in den Verwaltungsverfahrensgesetzen vorgesehenen Zurückweisung. Gemäß § 13 Abs. 3 AVG (der durch den Entwurf unverändert bleiben soll) berechtigen Mängel schriftlicher Anbringen die Behörde nicht zur Zurückweisung. Stattdessen ist ein Mängelbehebungsauftrag zu erteilen. Für elektronische Anbringen scheint hingegen Lessigs Prinzip „code as code“ zu gelten: wenn das elektronische Anbringen technische Mängel hat, dann wird es – ohne dass ein Organ der Behörde damit befasst würde – vom Server mit einer Fehlermeldung „zurückgewiesen“ und es scheint keine Möglichkeit zu geben, die Rechtmäßigkeit dieser Entscheidung des Servers im Instanzenzug prüfen zu lassen.

[11] Derzeit werden Spezifikationen teilweise auf der Website der Stabsstelle IKT-Strategie (http://www.cio.gv.at/) veröffentlicht, teilweise auf einer Website ohne Impressum (http://reference.e-government.gv.at/ – als Inhaber der Domain e-government.gv.at scheint noch das BMöLS auf, faktisch dürfte die Website von der Länderarbeitsgruppe zum e-Government betreut werden) und teilweise auf der Website http://www.buergerkarte.at/ (laut Impressum vom Verein A-SIT betrieben, die Domain wurde vom IAIK an der TU Graz registriert).

[12] Bundeskanzleramt, GZ 810.200/001-V/3/2003 vom 16.05.2003

Die RTR-GmbH regt daher an, die technischen Spezifikationen mittels Verordnung festzulegen, um die erforderliche Rechtssicherheit zu schaffen.

In diesem Zusammenhang ist zu bedenken, dass die von der Stabsstelle IKT-Strategie erarbeiteten Spezifikationen sich großteils an allerneuesten Entwicklungen orientieren. Signaturen und Verschlüsselung werden generell mit XML realisiert. Die entsprechenden W3C Recommendations wurden am 12.02.2002 (XML-Signatur[13]) bzw. am 10.12.2002 (XML-Verschlüsselung[14]) veröffentlicht. Auch SOAP wird sehr stark eingesetzt. SOAP existiert zwar schon seit mehreren Jahren[15], die Standardisierung durch das W3C wurde aber erst am 24.06.2003 durch die Veröffentlichung von Version 1.2 als herstellerunabhängige W3C Recommendation[16] (Version 1.2) zu einem vorläufigen Abschluss gebracht.[17]

Die RTR-GmbH begrüßt grundsätzlich die Strategie, sich an neuesten Entwicklungen und vor allem an international anerkannten Standardisierungsgremien wie dem W3C zu orientieren. Allerdings ist zu bedenken, dass eine Reihe von Spezifikationen noch nicht stabil sind und dass die Entwickler von Applikationen derzeit noch kaum auf Standardmodule zurückgreifen können und daher fast alles selbst programmieren müssen. Dazu kommt, dass auch die von der Stabsstelle IKT-Strategie selbst entwickelten Spezifikationen keineswegs stabil sind. Als herausragendes Beispiel ist hier das Konzept der Personenbindung zu nennen, das einen zentralen Bestandteil aller Spezifikationen der Stabsstelle IKT-Strategie bildet. Erst im Mai 2003 wurde die letzte Aktualisierung der entsprechenden Spezifikation (Version 1.1[18]) vorgenommen. Aufgrund der nun durch den Gesetzesentwurf vorgenommenen Änderung (die Personenbindung soll gemäß § 4 Abs. 2 e-GovG nicht mehr die ZMR-Zahl, sondern die daraus abgeleitete Stammzahl enthalten) wurde diese Version schon zehn Wochen später wieder obsolet.

Die RTR-GmbH gibt zu bedenken, dass die Entwickler von e-Government-Applikationen und von einschlägiger Anwendersoftware für ihre Investitionsentscheidungen die Sicherheit benötigen, dass einmal für verbindlich erklärte Spezifikationen auch über einen längeren Zeitraum von der Verwaltung unterstützt werden. Längere Produktzyklen sind insbesondere dann erforderlich, wenn Produkte einer Evaluierung und Bescheinigung nach § 9 SigV zu unterziehen sind oder wenn Entwickler – was durchaus begrüßenswert ist – ihre Produkte freiwillig auf ihre Sicherheit evaluieren lassen. Weiters ist zu bedenken, dass beim Upgrade auf neuere Versionen die alten Versionen eine Zeit lang weiterhin unterstützt werden müssen.

Für das Rechtssetzungsverfahren, mit welchem technische Spezifikationen festgelegt werden, regt die RTR-GmbH daher an, dass einerseits breitere

---

13 http://www.w3.org/TR/xmldsig-core/

14 http://www.w3.org/TR/xmlenc-core/

15 SOAP Version 1.0 war eine Entwicklung von Microsoft und UserLand, Version 1.1 wurde im Mai 2000 als W3C Note (als noch nicht standardisierte, herstellerabhängige Version) veröffentlicht.

16 http://www.w3.org/2000/xp/Group/, http://www.w3.org/TR/2003/REC-soap12-part0-20030624/

17 Die Spezifikationen des Zustelldienstes orientieren sich an der W3C Candidate Recommendation von SOAP Version 1.2 aus dem Dezember 2002.

18 http://www.buergerkarte.at/konzept/personenbindung/spezifikation/20030506/

Kreise in den Entscheidungsprozess eingebunden wären (überlegenswert wäre etwa ein verpflichtendes Konsultationsverfahren vor der Erlassung von Verordnungen, vgl. dazu das Konsultationsverfahren des § 128 TKG 2003), dass andererseits aber auch Rechtssicherheit geschaffen wird und einmal beschlossene Spezifikationen auch einige Jahre lang von der Verwaltung unterstützt werden.

A.5 Datenschutz

Die RTR-GmbH weist auf einige mögliche Datenschutzprobleme hin:

A.5.1 Bereichsspezifisches Personenkennzeichen für den Bereich „Zustellwesen“

Siehe oben A.2: Da das bereichsspezifische Personenkennzeichen für den Bereich „Zustellwesen“ für alle Verwaltungsbereiche relevant ist, könnte es sich in der Praxis zu einem alle Verwaltungsbereiche umfassenden Personenkennzeichen entwickeln.

A.5.2 Zentrales Zustellverzeichnis

In der Spezifikation der Nachrichtenstrukturen der elektronischen Zustellung[19] ist vorgesehen, dass die Behörde vor der Zustellung über das LDAP-Protokoll[20] abfragt, ob jemand bei einem Zustelldienst registriert ist. Für diesen Zweck wurde ein eigenes LDAP-Schema definiert.[21] Dort ist vorgesehen, dass ein zentraler Verzeichnisdienst eingerichtet wird, der selbst keine Daten speichert, aber mit allen Verzeichnisdiensten der zugelassenen Zustelldienste in Onlineverbindung steht und die von den Behörden gestellten Anfragen durch Verweise (Referrals[22]) auf die Verzeichnisse der Zustelldienste beantwortet. In der Spezifikation des Schemas wird verlangt[23], dass alle Zustelldienste ein solches Verzeichnis nach dem definierten LDAP-Schema führen müssen. Zu den nach diesem Schema im Verzeichnis gespeicherten Daten gehören unter anderem Vorname, Name und bereichsspezifisches Personenkennzeichen (mandatory), optional werden dazu auch andere Daten wie verschiedene postalische und elektronische Adressen, Telefonnummern und Informationen über Abwesenheiten verwaltet.

Es stellt sich die Frage, ob der zentrale Verzeichnisdienst tatsächlich keine eigenen Daten speichert und auf jede Anfrage hin bloß eine Liste von Verweisen auf alle einzelnen Zustelldienste hin zurückgibt, oder ob der zentrale Verzeichnisdienst doch über eine Kopie der Daten der Zustelldienste verfügt und solcherart in der Lage ist, direkt an die „richtigen“ Zustelldienste zu verweisen. In beiden Fällen ergeben sich potenzielle Datenschutzprobleme:

---

19 http://www.cio.gv.at/onlineservices/delivery/Zustellung_Nachrichtenstrukturen_20030506.pdf

20 Lightweight Directory Access Protocol, ein Protokoll, das z. B. von vielen Mailprogrammen zur Abfrage von Adressbüchern verwendet wird. LDAPv3 wurde spezifiziert in RFC 2251 bis 2256, RFC 2829, RFC 2830 und RFC 3377

21 http://www.cio.gv.at/onlineservices/delivery/Zustellung_Schema_Zustellverzeichnis_20030506.pdf

22 vgl. RFC 2251, Punkt 4.1.11. Ein LDAP-Server, der eine gesuchte Information nicht bereitstellen kann, kann mit einem Referral Error eine Liste von URLs anderer LDAP-Server zurückgeben, wo die Information möglicherweise gefunden werden kann.

23 http://www.cio.gv.at/onlineservices/delivery/Zustellung_Schema_Zustellverzeichnis_20030506.pdf, Zl 24

- Wenn der zentrale Verzeichnisdienst tatsächlich keine eigenen Daten über die Bürger verwaltet, sondern bloß eine Liste der zugelassenen Zustelldienste, dann wird bei jeder einzelnen Zustellung auf Anfrage der zustellenden Behörde die Liste aller zugelassenen Zustelldienste zurückgegeben und die zustellende Behörde fragt daraufhin bei allen zugelassenen Zustelldiensten an, ob der Bürger bei ihnen registriert ist. Abgesehen von der hohen Netzwerkbelastung würde dadurch jeder einzelne Zustelldienst Informationen über alle elektronischen Zustellungen erfahren[24] und hätte die Möglichkeit, diese Daten mitzuprotokollieren und auszuwerten.

- Wenn der zentrale Verzeichnisdienst über Kopien der LDAP-Verzeichnisse der einzelnen Zustelldienste verfügt (was mit den Mitteln der LDAP-Replikation leicht realisierbar wäre), dann könnte der zentrale Verzeichnisdienst immer an die richtigen Zustelldienste verweisen, bei denen sich der Bürger tatsächlich registrieren hat lassen. Andere Zustelldienste würden über den Zustellvorgang nichts erfahren. Allerdings würde dann ein neues zentrales Verzeichnis aller Personen entstehen, die sich bei einem Zustelldienst haben registrieren lassen, was wiederum die Frage nach dem Datenschutz und der Datensicherheit beim Betrieb des zentralen Verzeichnisses aufwirft.

Die RTR-GmbH geht auf Grund der ihr bekannten Konzepte davon aus, dass die erste Variante verwirklicht wird. In beiden Fällen sollte für den zentralen Verzeichnisdienst wohl eine gesetzliche Grundlage geschaffen werden.

In diesem Zusammenhang wird angeregt, datenschutzrechtlich zu prüfen und im Gesetz zu regeln, wie und unter welchen Voraussetzungen auf die Verzeichnisse der einzelnen Zustelldienste bzw. auf das zentrale Verzeichnis zugegriffen werden kann und welche Datensicherheitsmaßnahmen zu ergreifen sind, um Abfragen Unberechtigter zu unterbinden. Insbesondere sollte erörtert werden, ob nur Behörden auf die Verzeichnisse zugreifen dürfen, oder ob dies (gegebenenfalls unter welchen Voraussetzungen) auch für Private möglich sein soll (vgl. dazu den Entwurf von § 29 Abs. 3 ZustellG). Denkbar wäre etwa die Regelung, dass nur Behörden darauf zugreifen dürfen. Abgesichert werden könnte dies technisch mittels Zertifikaten derer, die auf die Verzeichnisse zugreifen können (über LDAP/SSL) und rechtlich mit einer Verankerung der X.509-Zertifikatserweiterungen für die Verwaltung[25], womit die Eigenschaft als Behörde im Zertifikat aufscheint.

A.5.3 Logdateien des Stammzahlenregisters

Es ist anzunehmen, dass die im Entwurf des § 10 e-GovG beschriebene Methode, bereichsspezifische Personenkennzeichen durch das Stammzahlenregister zu ermitteln, starke Verbreitung finden wird (die Methode wird vor allem dann erforderlich sein, wenn die Verwaltung von Amts wegen tätig wird, siehe die Anmerkungen unten zu § 10 e-GovG). Das bedeutet, dass

[24] In http://www.cio.gv.at/onlineservices/delivery/Zustellung_Schema_Zustellverzeichnis_20030506.pdf ist vorgesehen, dass grundsätzlich nach dem bereichsspezifischen Personenkennzeichen für den Bereich „Zustellung“ abgefragt wird. Wenn dieses der anfragenden Behörde aber nicht bekannt ist, dann wird nach Name, Adresse und evtl. auch nach dem Geburtsdatum angefragt.

[25] http://www.cio.gv.at/it-infrastructure/pki/X509ext-20030218.pdf

die Logdateien des Stammzahlenregisters (§ 12 Abs. 3 e-GovG) einen weit reichenden Überblick darüber bilden werden, welcher Bürger mit welcher Behörde zu tun hat. Dies würde eine Zusammenführung von Informationen aus allen Verwaltungsbereichen an einer Stelle bewirken, die durch das komplizierte System der Stammzahlen und der bereichsspezifischen Personenkennzeichen eigentlich vermieden werden sollte (siehe oben A.2).

Die RTR-GmbH regt daher an, für diese Logdateien spezifische Datenschutzmaßnahmen zu ergreifen. Da die Logdateien nur der stichprobenartigen Kontrolle der Zulässigkeit der Zugriffe dienen sollen, wäre weiters denkbar, nur einen gewissen Prozentsatz der Zugriffe mitzuprotokollieren.

A.5.4 Logdateien des Zentralen Melderegisters

Im Entwurf der §§ 14 bis 16 e-GovG ist vorgesehen, die Bürgerkartenfunktion zur eindeutigen Identifikation im Bereich der Privatwirtschaft einzusetzen. Damit diese Funktion für die Privatwirtschaft auch wirklich nutzbar wird, ist eine Abfrage des Zentralen Melderegisters erforderlich. In den Logdateien des Zentralen Melderegisters würden dadurch verstärkt Informationen gesammelt werden, welcher Bürger mit welchem Unternehmen kommuniziert.

Im Entwurf des § 17 e-GovG ist vorgesehen, dass Informationen zu Standarddokumenten zum Personenstand im Zentralen Melderegister gespeichert und von den Verwaltungsbehörden abgerufen werden können. In den Logdateien des Zentralen Melderegisters würden dadurch vermehrt Informationen gespeichert, die Aufschluss darüber geben, zu welchem Bürger bei welcher Behörde welches Verfahren anhängig sein könnte.

Die RTR-GmbH regt an, die bestehenden Datenschutzmaßnahmen des Zentralen Melderegisters im Hinblick auf diese möglicherweise zusätzlich gespeicherten Daten zu überprüfen.

B. Zu einzelnen Bestimmungen

B.1 Zu Art. 1 (e-GovG)

Zu § 4 e-GovG

Zum Begriff der „Bürgerkarte“ wird vorgeschlagen, in das Gesetz eine klare Definition der Bürgerkarte aufzunehmen. Dass die Bürgerkarte nichts mit der Staatsbürgerschaft zu tun hat und dass es sich dabei nicht notwendigerweise um eine Chipkarte handelt, sondern um eine bestimmte Funktionalität, ist für Außenstehende schwer nachvollziehbar.

Auch auf www.buergerkarte.at und auf reference.e-government.gv.at findet sich keine prägnante Definition der „Bürgerkarte“. Auf letzterem Server ist die Bürgerkarte folgendermaßen beschrieben: „Das Konzept der österreichischen Bürgerkarte definiert eine Reihe von grundlegenden Funktionen, welche für eine sichere elektronische Kommunikation zwischen Bürger und Verwaltungsbehörden notwendig sind (sichere elektronische Signatur,

Authentifikation des Bürgers, Datenspeicher)."[26] Weiters wird die Programmierschnittstelle „Security Layer" als zentraler Bestandteil des Konzeptes genannt.

In diesem Zusammenhang sei darauf verwiesen, dass nach dem Wissensstand der RTR-GmbH der Begriff der „Bürgerkarte" immer in Kombination mit dem Begriff der „sicheren elektronischen Signatur" genannt wird. Wo auf letztere verzichtet wird, wird der Begriff der „Bürgerkarte light" verwendet. Diese Terminologie entspricht nicht dem Gesetzesentwurf, in dem ausschließlich den Begriff der „Bürgerkarte" vorkommt, aber offenbar auch im Rahmen der Bürgerkarte bis 2010 auf die sichere elektronische Signatur verzichtet werden kann.

Zu Abs. 2 sei darauf verwiesen, dass eine „eindeutige Identifikation" natürlich nur dann bewirkt werden kann, wenn vor der Ausstellung der Personenbindung, mit welcher die eindeutige Identifikation bewirkt werden soll, auch eine hochqualitative Identitätsprüfung vorgenommen wurde. Dies ist im Entwurf noch nicht erwähnt. Es gibt zwar einen Hinweis auf „einen Zertifizierungsdiensteanbieter", aber keinen Hinweis darauf, welche Rolle er im Zusammenhang mit der Ausstellung der Personenbindung spielt.

Die RTR-GmbH schlägt daher vor, in § 4 die Rolle der Personenbindung und des Zertifizierungsdiensteanbieters klar zu beschreiben, z. B. so: Die Personenbindung stellt eine Zusatzinformation zu dem von einem Zertifizierungsdiensteanbieter ausgestellten Zertifikat dar, in der diesem Zertifikat die Stammzahl des Zertifikatsinhabers zur eindeutigen Identifikation zugeordnet wird. Voraussetzung für die Ausstellung der Personenbindung ist, dass der Person bereits ein (qualifiziertes?) Zertifikat ausgestellt wurde. (Wenn es zulässig sein soll, auch nicht qualifizierte Zertifikate zu verwenden, dann wird man Zusatzanforderungen stellen müssen, um sicher zu stellen, dass die verwendeten Signaturerstellungsdaten nur einer Person zugeordnet werden.) Wenn die Ausstellung der Personenbindung und die Ausstellung des Zertifikates nicht gleichzeitig erfolgt, ist sicher zu stellen, dass die Personenbindung und das Zertifikat der selben Person ausgestellt wird. Vor der Ausstellung der Personenbindung ist eine Identitätsprüfung anhand eines amtlichen Lichtbildausweises durchzuführen und zusätzlich mittels einer Personenbindungsanfrage bei der Stammzahlregisterbehörde zu überprüfen, ob die Person durch die Angaben im amtlichen Lichtbildausweis eindeutig identifiziert werden kann. Reichen diese Angaben nicht aus, sind weitere Merkmale zu erheben, durch welche die Person eindeutig identifiziert werden kann. Die vorgenommenen Erhebungen sind von der Stammzahlregister-behörde zu dokumentieren. Die Stammzahlregisterbehörde kann mit der Erhebung einen oder mehrere Zertifizierungsdiensteanbieter (evtl.: „die qualifizierte Zertifikate ausstellen") im Sinne des SigG beauftragen.

Dieser Vorschlag soll nur einen groben Überblick über einige notwendige und noch nicht geregelte organisatorische Maßnahmen darstellen. Im Wesentlichen werden an die Stammzahlregisterbehörde als Ausstellerin der Personenbindung ähnliche Anforderungen zu stellen sein wie an den Aussteller eines qualifizierten Zertifikates.

[26] http://reference.e-government.gv.at/Das_Konzept_B_rgerkarte.282.0.html

Zu § 5 e-GovG

Diese Bestimmung regelt in Abs. 1 die Bevollmächtigung und in Abs. 2 offenbar (obwohl auch dort vom „Bestehen eines Vollmachtverhältnisses“ gesprochen wird) die organmäßige Vertretung.

Zu Abs. 1 sei darauf verwiesen, dass diese Bestimmung nicht im Einklang mit der von der Stabsstelle IKT-Strategie als Beispiel der „Verwaltungssignatur“ (siehe dazu oben A.1) angesehenen „Bürgerkarte light“ steht. Bei dieser soll auch möglich sein, dass der Signator über die Signaturerstellungsdaten nicht selbst verfügt, sondern die Signaturerstellung etwa an seinen Mobiltelefonanbieter delegiert. Rechtlich wäre dies wohl ein Vollmachtsverhältnis und daher müsste der Signator nach § 5 Abs. 1 die Vollmacht signieren, was er aber eben nicht selbst kann. Die Rechtsfigur der delegierten Signatur sollte daher, wenn man sie tatsächlich einführen will, auch explizit geregelt werden (am besten im Signaturgesetz, wo vor allem § 21 SigG anzupassen wäre).

Zu Abs. 2 sei auf die Ausführungen oben in A.3 verwiesen: da sich die organmäßige Vertretung häufig ändern kann, wird notwendig sein, dass die ausgestellten Bestätigungen über die organmäßige Vertretung auch widerrufen werden können und dass ein zuverlässiger Widerrufsdienst geführt wird. Die Regelungen über den Widerrufsdienst sollten dabei auch mit denen des SigG und der SigV harmonisiert werden. Eine sinnvolle Alternative wäre auch, die Regelungen überhaupt in das SigG aufzunehmen und dessen Anwendungsbereich auf Attributzertifikate zu erweitern.

Zu den §§ 6ff e-GovG

Siehe die Ausführungen oben unter A.2.

Zu § 7 Abs. 2 e-GovG

In dieser Bestimmung wird auf einen „geeigneten Zertifizierungsdiensteanbieter“ verwiesen, ohne dass definiert würde, worin diese Eignung besteht.

Die RTR-GmbH regt an, bereits in § 4 das Zusammenwirken zwischen dem Zertifizierungsdiensteanbieter und der Stammzahlregisterbehörde zu regeln. Wenn das derzeitige Konzept für die Ausstellung von Personenbindungen beibehalten wird, findet die Identitätsprüfung vor der Ausstellung einer Personenbindung ja beim Zertifizierungsdiensteanbieter statt.

Zu § 8 Abs. 2 e-GovG

Die RTR-GmbH gibt zu bedenken, dass die Frage, wie die einzelnen Bereiche der Verwaltung voneinander abgegrenzt werden, wesentliche Auswirkungen darauf hat, welche Datenübermittlungen in der Verwaltung faktisch möglich sein werden und welche nicht. Es ist nicht ganz klar, ob die entsprechende „Festlegung“ der Stammzahlenregisterbehörde (Abs. 1) alle Verwaltungsbehörden (auch Länder und Gemeinden?) binden soll. Daher wird angeregt, in die erläuternden Bemerkungen zur Regierungsvorlage Ausführungen zur

rechtlichen Qualität dieser „Festlegung“ (Erlass? Verordnung?) und die verfassungsrechtliche Zulässigkeit (Bedarfsgesetzgebung für das Verwaltungsverfahren nach Art. 11 Abs. 2 B-VG?) aufzunehmen.

Zu § 9 e-GovG

Aus dem Wortlaut des Gesetzestextes ergibt sich der falsche Eindruck, dass das bereichsspezifische Personenkennzeichen in der Bürgerkarte selbst errechnet werden muss. Weiters enthalten die Erläuterungen zusätzliche Vorschriften für den Vertretungsfall, welche im Gesetzesentwurf nicht enthalten sind.

Die RTR-GmbH regt daher an, den Vorgang verständlicher zu beschreiben, etwa so: „Zur Ermittlung bereichsspezifischer Personenkennzeichen durch Einsatz der Bürgerkarte wird die in der Bürgerkarte eingetragene Personenbindung an die Behörde übermittelt. Die Behörde errechnet aus der in der Personenbindung enthaltenen Stammzahl das bereichsspezifische Personenkennzeichen (§ 8 Abs. 1). Bei elektronischen Anbringen, die in Vertretung einer Person gestellt werden, muss neben der Personenbindung des Vertreters auch die elektronisch signierte Vollmacht gemäß § 5 Abs. 1 oder die Bestätigung gemäß § 5 Abs. 2 an die Behörde übermittelt werden. Die Behörde errechnet das bereichsspezifische Personenkennzeichen dann nicht aus der Stammzahl des Vertreters, sondern aus der Stammzahl des Vertretenen.“

Zu § 10 e-GovG

Es stellt sich die Frage, welches bereichsspezifische Personenkennzeichen eine Behörde zu wählen hat, wenn der Betroffene nicht an die Behörde herangetreten ist (z. B. die Behörde leitet von Amts wegen ein Verwaltungsstrafverfahren ein oder sie will einem mit Name und Adresse namhaft gemachten Zeugen eine Ladung zustellen). Kann die Behörde dann in jedem Fall an die Stammzahlenregisterbehörde herantreten und sich von dieser ein bereichsspezifisches Personenkennzeichen errechnen lassen?

Die RTR-GmbH geht davon aus, dass dies mit § 10 Abs. 1 des Entwurfs gemeint ist. Allerdings ist dann nicht klar, welche Fälle der Halbsatz „... und auf die Fälle der Amtshilfe und der Ausstattung eines Registers ... beschränkt ist“ ausschließen soll.

Zu § 11 e-GovG

Die RTR-GmbH weist darauf hin, dass sowohl die Stammzahl als auch die bereichsspezifischen Personenkennzeichen auf Grund der Verwendung kryptographischer Einwegableitungen wahrscheinlich ziemlich lange Zahlen sein werden (SHA-1 entspricht 20 Byte, also 40 hexadezimalen Stellen). Die Ermittlung eines bereichsspezifischen Personenkennzeichens durch Befragung des Betroffenen dürfte daher sehr fehleranfällig sein – insbesondere wenn nicht (z. B. durch Ergänzung von Prüfziffern) eine Möglichkeit geschaffen wird, Fehler bei der Übermittlung zu erkennen.

Wenn mit der Bestimmung gemeint sein soll, dass es auch zulässig wäre, dass die Behörde den Betroffenen nach seinem Namen und seiner Adresse befragt, dann durch eine Meldeanfrage die ZMR-Zahl ermittelt und daraus die Stammzahl und das bereichsspezifische Personenkennzeichen ermittelt, dann würde sich die Frage stellen, wozu an anderen Stellen ein so großer Aufwand zur Geheimhaltung der Stammzahl betrieben wird (siehe dazu die allgemeinen Ausführungen unter A.2).

Zu § 12 e-GovG

Diese Bestimmung enthält strenge Regelungen zum Schutz der Stammzahl. Vgl. dazu die allgemeinen Ausführungen oben in Kapitel A.2: Da die Stammzahl aus der ZMR-Zahl abgeleitet wird, bringt der Schutz der Stammzahl wenig, so lange man relativ frei auf das ZMR zugreifen kann.

Zu Abs. 1 stellt sich die Frage, ob diese Bestimmung zur Speicherung der Stammzahl auch für die Stammzahlen juristischer Personen gelten soll. Dies scheint im Widerspruch zu den §§ 14 bis 16 zu stehen.

Zu § 13 e-GovG

Vgl. zum Begriff der „nicht-umkehrbaren Ableitung“ in Abs. 1 die Ausführungen in Kapitel A.2. Die Nicht-Umkehrbarkeit gilt nur unter der Annahme, dass die ZMR-Zahl, aus welcher alles abgeleitet wird, nicht auf anderem Wege erfragt werden kann.

Zu Abs. 3 wird darauf verwiesen, dass die Wortfolge „ausschließlich im Rahmen der Leistung von Amtshilfe“ im Widerspruch zu § 11 Abs. 2 des Entwurfs stehen würde. Es sollte wohl „ausschließlich im Rahmen der Leistung von Amtshilfe oder wenn das bereichsfremde Personenkennzeichen gemäß § 11 Abs. 2 vom Betroffenen angeboten wird“ heißen.

Zu den §§ 14 bis 16 e-GovG

Diese Bestimmungen regeln, wie die Bürgerkartenfunktion auch in der Privatwirtschaft eingesetzt werden kann. An die Stelle des bereichsspezifischen Personenkennzeichens tritt dort ein „wirtschaftsbereichsspezifisches Personenkennzeichen“. Der Entwurf regelt nicht ausdrücklich, wie dieses zu berechnen ist; eine Regelung vergleichbar dem § 8 Abs. 1 des Entwurfs fehlt für diesen Bereich, wahrscheinlich soll § 8 Abs. 1 sinngemäß angewendet werden (dies könnte in § 14 Abs. 2 zum besseren Verständnis ausdrücklich angeführt werden).

In den Erläuterungen zu § 16 wird ein Begriff der „Personenbindung“ verwendet, der von der in § 4 Abs. 2 definierten „Personenbindung“ abweicht. Die Personenbindung des § 4 Abs. 2 e-GovG wird vom Stammzahlenregister ausgestellt und enthält als eindeutiges Identifikationsmerkmal die Stammzahl des Bürgers. Die Personenbindung aus den Erläuterungen des § 16 e-GovG enthält statt der Stammzahl das wirtschaftsbereichsspezifische Personenkennzeichen. Wer Aussteller dieser Personenbindung ist, wird nicht beschrieben, wahrscheinlich ist es der Signator selbst.

§ 16 soll eine neue Form der Melderegisterabfrage ermöglichen, die nach den Erläuterungen „bloß mit dem wbPK“ erfolgt. Die RTR-GmbH geht davon aus, dass das wbPK ein Hashwert ist, in welchen die Stammzahl des Bürgers und die Stammzahl des Unternehmens einfließt. Wie es dem Zentralen Melderegister möglich sein soll, das wbPK einer bestimmten Person zuzuordnen, ist für die RTR-GmbH nicht nachvollziehbar. Die einzig praktikable Möglichkeit dürfte darin bestehen, dass das anfragende Unternehmen nicht „bloß das wbPK“, sondern das wbPK, seine eigene Stammzahl und einige Daten des Bürgers (z. B. den Namen) übermittelt. Das ZMR errechnet dann für jeden anhand des Namens in Frage kommenden Bürger aus der ZMR-Zahl dessen Stammzahl (was nach § 12 des Entwurfs unzulässig wäre) und danach aus der so ermittelten Stammzahl des Bürgers und der Stammzahl des Unternehmens das wbPK. Wenn eines der so errechneten wbPKs mit dem übermittelten wbPK übereinstimmt, dann konnte der Bürger identifiziert werden.

Vgl. auch die Anmerkungen in Kapitel A.5.4 und zum Entwurf des § 12 Abs. 1 e-GovG.

Zu § 20 e-GovG

Das Signaturgesetz sieht grundsätzlich vor, dass Signaturen von natürlichen Personen erstellt werden. Signatoren gemäß § 2 Z 2 SigG können nur natürliche Personen (und Zertifizierungsdiensteanbieter) sein.

Von verschiedensten Seiten wurden Wünsche vorgetragen, auch juristischen Personen oder Behörden die Möglichkeit zu schaffen, eine Signatur im eigenen Namen vornehmen zu können. In engem Zusammenhang dazu ist der Wunsch zu sehen, Signaturen nicht bloß als Willenserklärung im Einzelfall oder im Batchbetrieb („ich will dieses Dokument signieren“/„ich will diese 2000 Dokumente signieren“) erstellen zu können, sondern automatisch und in Echtzeit („ich will, dass dieser Server ab jetzt alles signiert, was ihm von der Software XY zur Signatur vorgelegt wird“).

Nach Ansicht der RTR-GmbH sollte eine Erweiterung des Signaturgesetzes in diese Richtung durchaus diskutiert werden. Es werden dabei aber andere Sicherheitskonzepte und daher auch andere rechtliche Anforderungen an die jeweiligen Sicherheitsmaßnahmen zu treffen sein. Das derzeitige Signaturrecht stellt an den Signator relativ wenige Anforderungen – er muss auf seine Signaturerstellungsdaten aufpassen (z. B. die Chipkarte sorgsam verwahren) und er soll sich vor jeder PIN-Eingabe überlegen, ob er auch wirklich unterschreiben will, was ihm angezeigt wird.

Wenn eine juristische Person oder eine Behörde nicht durch ein Organ sondern „selbst“ signiert oder wenn zukünftig automatisch zu erstellende Signaturen im Vorhinein autorisiert werden, dann stellen sich wesentlich höhere Anforderungen an den Signator.

Die RTR-GmbH ist daher der Ansicht, dass solche neuen Möglichkeiten zwar diskutiert werden sollen, aber nur durch eine Änderung des Signaturgesetzes realisiert werden könnten.

Die Bestimmung im Entwurf des § 20 e-GovG wird von der RTR-GmbH daher so verstanden, dass durch die Verordnungsermächtigung keine Möglichkeit geschaffen wird, vom Grundsatz abzugehen, dass elektronische Signaturen von natürlichen Personen (im Bereich der Verwaltung daher von Organwaltern) zu erstellen sind und dass die Möglichkeit bestehen muss, dass die zu signierenden Daten dem Signator vor der Auslösung des Signaturvorgangs dargestellt werden (§ 18 Abs. 2 SigG).

Die Verordnungsermächtigung beschränkt sich daher nach Ansicht der RTR-GmbH darauf, Details dazu festzulegen, wie eine elektronische Signatur als „Amtssiegel" erkennbar ist, also aus welchen Informationen im Signaturformat, im Zertifikat oder in einem Attributzertifikat ableitbar ist, dass eine bestimmte elektronische Signatur als „Amtssiegel" gilt.

Die RTR-GmbH regt an, nicht bloß in den ErläutRV, sondern im Gesetzestext ausdrücklich anzuführen, dass es sich bei einem Amtssiegel um eine elektronische Signatur handelt. Auf Grund der besonderen Bedeutung der Amtssiegel sollte es sich dabei jedenfalls um eine sichere elektronische Signatur iSd § 2 Z 3 SigG handeln.

B.2 Zu Art. 2 (Änderungen des AVG 1991)

Zu § 18a AVG

Durch den vorgeschlagenen § 18a AVG würde stärker als bisher zwischen der behördeninternen Erledigung und der Mitteilung des Erledigungsinhaltes an die Parteien des Verfahrens unterschieden werden. Dabei entsteht für die RTR-GmbH aus der gewählten Formulierung der Eindruck, dass mit der Neuregelung angestrebt wird, von förmlichen Zustellungen mit Zustellnachweis verstärkt abzugehen („Mitteilungen ... sind ... in jener Form vorzunehmen, die für die Behörde und den Adressaten den insgesamt geringsten Aufwand verursacht", Entwurf des § 18a Abs. 1 AVG). Ob zuzustellen oder bloß „zuzusenden" ist, wird in das Ermessen der Behörde gestellt („wenn infolge der Wichtigkeit der Mitteilung aus Sicht der Behörde ..." (Entwurf des § 18a Abs. 1 AVG), „die Auswahl der situationsangepasst ‚richtigen' Kommunikationsform ... ist kein subjektives Recht des Adressaten ..." (Erläuterungen dazu)).

Gerade im Hinblick auf die neue Möglichkeit der elektronischen Zustellung wäre es aber doch sinnvoll, behördliche Mitteilungen in verstärktem Maße förmlich (elektronisch) zuzustellen und nicht bloß informell „zuzusenden", um insgesamt mehr Rechtssicherheit zu gewährleisten.

B.3 Zu Art. 3 (Änderungen des Zustellgesetzes)

Zu § 2 Z 6 und 7 ZustellG

Die Definition der „Adresse" bzw. der „Zustelladresse" ist sehr allgemein gehalten („die für die Erreichbarkeit des Empfängers in einer bestimmten Kommunikationsform notwendigen Angaben"). In den Erläuterungen bleibt unklar, was unter der elektronischen Adresse bzw. elektronischen Zustelladresse zu verstehen ist. Da die Zustelladresse ja in der

Zustellverfügung anzuführen ist (Entwurf des § 5 Z 2 ZustellG) und ihr in diesem Zusammenhang große rechtliche Bedeutung (z. B. bei Zustellung an die falsche Person oder Zustellung an die Nichtpartei) zukommt, sollte dies klarer gefasst werden.

In der Prozessbeschreibung der elektronischen Zustellung[27] wird unterschieden zwischen der Abfrage des Verzeichnisdienstes und dem Versenden des Zustellstückes. Bei der Abfrage des Verzeichnisdienstes sucht die Behörde entweder nach dem bereichsspezifischen Personenkennzeichen des Verwaltungsbereichs „Zustellwesen“[28], oder nach Name, ZMR-konformer Adresse und (optional) Geburtsdatum oder aber nach Name und „Verständigungsadresse“ (das kann eine elektronische oder eine postalische Adresse sein). Für das Versenden des Zustellstückes wird auf eine XML-Spezifikation der Zustellungsdatenstrukturen[29] verwiesen. In diesem werden einerseits verschiedene Möglichkeiten beschrieben, eine Person zu bezeichnen (als Beispiele sind die Matrikelnummer und die Firmenbuchnummer angeführt), andererseits wird darauf verwiesen, dass die Adressierungselemente überhaupt in einem anderen Dokument spezifiziert wären.[30] Dort wiederum werden als Identifikation der Person wiederum verschiedenste Möglichkeiten genannt[31] und die Spezifikation soll in diesem Punkt offenbar bewusst offen gehalten werden.

Angesichts dieser Unbestimmtheit der Spezifikationen sollte im Gesetz klarer definiert werden, was die Zustelladresse ist. Insbesondere sollte dadurch auch die Trennung der Verantwortung zwischen dem elektronischen Zustelldienst und der Behörde klar werden. Als Beispiel sei genannt, dass die Behörde zunächst aufgrund von Name und ZMR-konformer Adresse in den Verzeichnissen der Zustelldienste anfragt und die Partei danach in dem an den Zustelldienst übergebenen Dokument anhand der Matrikelnummer identifiziert. Wie ist es rechtlich zu beurteilen, wenn die Matrikelnummer falsch erfasst war und das Dokument daher der falschen Person übermittelt wurde?

Zu § 2 Z 9 ZustellG

In § 2 Z 9 ist die Post definiert als „die PTA (§ 2 Z 2 des Postgesetzes 1997 ...) bzw. deren Gesamtrechtsnachfolgerin (§ 12 des ÖIAG-Gesetzes, ...)“. Die PTA existiert seit der durch das ÖIAG-Gesetz (rückwirkend mit 01.01.2000) erfolgten Verschmelzung mit der ÖIAG und der PTBG nicht mehr. Schon im Jahr vor dieser Verschmelzung wurde am 03.03.1999 die Österreichische Post AG gegründet und die Unternehmensbereiche Gelbe Post und Postauto wurden aus der Post und Telekom Austria AG mit bilanzieller Rückwirkung zum 01.01.1999 im Wege der Gesamtrechtsnachfolge an die Österreichische Post AG übertragen. Die ÖIAG als Gesamtrechtsnachfolgerin der PTA war also zu keinem Zeitpunkt mit Aufgaben der Briefzustellung befasst, sondern

[27] http://www.cio.gv.at/onlineservices/delivery/Zustellung_Prozessbeschreibung_20030506.pdf, Kapitel 4.1
[28] dort als „VPK-Zustellung“ bezeichnet
[29] http://www.cio.gv.at/onlineservices/delivery/DeliveryData_20030506.zip
[30] In Zeile 92ff wird auf [OLAPPMSG] verwiesen, dieses Dokument wurde unter http://www.cio.gv.at/onlineservices/delivery/Container_20030506.zip veröffentlicht.
[31] Auf S. 8ff wird zunächst der PersonDataType definiert, der beliebig viele Elemente „Identification“ enthalten kann, diese Element kann wiederum verschiedenste Identifikationsmerkmale enthalten, als Beispiel sind das bereichsspezifische Personenkennzeichen, die Firmenbuchnummer, die FON-Nummer und die Matrikelnummer genannt (S. 12).

fungiert in diesem Zusammenhang nur als Eigentümerin der Aktien der Österreichischen Post AG. In § 2 Z 9 sollte daher die Österreichische Post AG genannt werden.

Zu § 4 ZustellG

Das Konzept über die elektronische Zustellung sieht vor, dass es mehrere verschiedene elektronische Zustelldienste gibt und dass eine Person bei mehreren verschiedenen elektronischen Zustelldiensten angemeldet sein kann.

Daher stellt sich die Frage, über welchen elektronischen Zustelldienst zugestellt werden soll, wenn eine Person bei mehreren Diensten angemeldet ist. Dies geht aus den Regeln im Entwurf für § 4 Abs. 2 ZustellG nicht eindeutig hervor. Die Prozessbeschreibung der elektronischen Zustellung[32] geht davon aus, dass die absendende Behörde aus mehreren Zustelldiensten, bei welchen der Empfänger registriert ist, frei wählen kann.

Zu den schwierigsten Problemen im Zustellrecht gehört die Abwesenheit des Empfängers. Zu diesem Punkt ist in § 4 Abs. 2 Z 2 und in der zitierten Prozessbeschreibung bloß ausgeführt, dass ein Zustelldienst, bei dem der Empfänger seine Unerreichbarkeit gemeldet hat, nicht ausgewählt werden darf. Offenbar ist es nach diesem Konzept aber möglich, dass der Empfänger bei einem Zustelldienst als abwesend gemeldet ist und bei einem anderen nicht und dass dann an den anderen Zustelldienst zugestellt werden kann.

Als § 4 Abs. 4 ZustellG wurde nun eine neue Bestimmung zur Abwesenheit des Empfängers vorgeschlagen. Unklar ist, ob diese Bestimmung für die postalische oder die elektronische Zustellung gelten soll. Nach dem Wortlaut des § 4 Abs. 4 erster Satz ZustellG gilt sie für „Abgabestellen"; also gemäß der Definition in § 2 Z 9 für örtlich bestimmte Zustelladressen und nicht für elektronische Adressen. Allerdings passt die neue Bestimmung nicht zu den bestehenden (und durch den Entwurf nicht geänderten) Regelungen in § 17, § 8 und § 16 Abs. 5 ZustellG. Nach § 8 hat die Partei, die während des Verfahrens die Abgabestelle ändert, die Behörde zu verständigen. Nach dem neuen § 4 Abs. 4 ZustellG soll es genügen, die Post oder einen sonstigen Zustelldienst (einen elektronischen Zustelldienst?) von der Abwesenheit zu verständigen und die Behörde soll dies – „außer in offensichtlichen Missbrauchsfällen" – von Amts wegen beachten. Im neuen § 4 Abs. 2 Z 2 ist eine ähnliche Regelung enthalten – hier aber ohne die Ausnahme des Missbrauchs.

Die RTR-GmbH regt an, dass die Frage der Auswahl zwischen verschiedenen Zustelladressen und die Frage der Abwesenheit grundsätzlich neu strukturiert wird. Dabei sollte vor allem auch erörtert werden, was eigentlich die Abwesenheit oder Unerreichbarkeit bei der elektronischen Zustellung ausmacht. Die elektronische Zustellung hat ja grundsätzlich den Vorteil, dass es der Empfänger unter seiner Adresse an jedem beliebigen Ort Nachrichten empfangen kann, so lange er nur über einen entsprechenden Internet-Zugang

[32] http://www.cio.gv.at/onlineservices/delivery/Zustellung_Prozessbeschreibung_20030506.pdf, Kapitel 4.1, Schritt 2; Kapitel 8

verfügt. Allerdings können sich verschiedene andere Probleme ergeben, die erörtert und geregelt werden sollten:

- Es ist möglich, dass der Empfänger gar nicht ortsabwesend ist, aber auf elektronischem Weg nicht erreicht werden kann, weil es ein technisches Problem gibt. Beispiele: Der Computer des Empfängers ist defekt; die Verbindung zum Internet ist defekt, gesperrt oder gekündigt; der Empfänger kann die Nachricht nicht entschlüsseln, weil er seine Chipkarte verloren hat, ... In diesen Fällen kann der Empfänger seinen Zustelldienst auch nicht im dafür vorgesehen Weg über die Unerreichbarkeit informieren. Unter Umständen sind in der Zeit, die bis zur Verständigung des Zustelldienstes vergeht, bereits Dokumente zugestellt worden, auf die der Empfänger nicht zugreifen kann.

- Es ist möglich, dass der Empfänger zwar ortsabwesend ist, aber Zugang zum Internet hat und diesen auch benutzt. Beispiel: Der Empfänger macht Urlaub und liest auch im Urlaub seine privaten E-Mails. Allerdings will der Empfänger im Urlaub keine behördlichen Schriftstücke zugestellt erhalten, weil er sich durch den mit Zustellung beginnenden Fristenlauf und die allenfalls notwendigen Schritte, ein Rechtsmittel einzubringen, den Urlaub nicht verderben lassen will. Der Entwurf sieht vor, dass der Empfänger seine länger dauernde Unerreichbarkeit dem Zustelldienst bekannt geben kann und diese Zustelladresse dann nicht verwendet werden darf. Allerdings wird im Entwurf auch der Fall des „offensichtlichen Missbrauchs“ angesprochen. Auch nach geltendem Recht kommt es nicht auf die Meldung der Abwesenheit an, sondern darauf, ob man tatsächlich abwesend ist oder nicht. Wenn jemand seine Abwesenheit nur vortäuscht, dann kann durch Hinterlegung rechtswirksam zugestellt werden. Es wäre zu erörtern, ob dieser Grundsatz in die elektronische Welt übertragen werden sollte (dann wären objektive Regelungen erforderlich, nach denen zu prüfen wäre, ob der Empfänger erreichbar ist oder nicht) oder ob es dem Empfänger frei stehen soll, sich bei einem elektronischen Zustelldienst beliebig lange als unerreichbar eintragen zu lassen, woraufhin eben postalisch zuzustellen ist. Nach dem Entwurf scheint letzteres zu gelten, allerdings ist der vorgeschlagene § 4 Abs. 4 Satz 2 ZustellG in diesem Zusammenhang etwas verwirrend.

- Ist der Fall denkbar, dass der Empfänger bei einem elektronischen Zustelldienst unerreichbar ist und bei einem anderen nicht? Wenn der Entwurf so zu verstehen ist, sollte es in den Erläuterungen deutlich angesprochen werden.

Zu § 28 ZustellG

Siehe die allgemeinen Anmerkungen in Punkt A.3.

Zu § 29 ZustellG

Nach dieser Bestimmung muss jeder Zustelldienst eine Liste der bei ihm Angemeldeten zu führen. Die Liste der Angemeldeten hat jeweils Vor- und Zuname, das bereichsspezifische Personenkennzeichen für den Bereich

„Zustellwesen“ und die ihm benannten Zustelladressen sowie „die vom Betroffenen gegenüber dem Zustelldienst gemachten Angaben für eine inhaltlich verschlüsselte Speicherung und Übermittlung von zuzustellenden Dokumenten“ zu enthalten.

Zunächst sei darauf verwiesen, dass diese Formulierung nur auf natürliche Personen Bezug nimmt und nicht auf juristische Personen.

Die unter http://www.cio.gv.at/onlineservices/delivery/ veröffentlichten Konzepte gehen von einer bestimmten technischen Realisierung der Liste der elektronischen Zustelladressen, nämlich als LDAP-Verzeichnis nach einem bestimmten LDAP-Schema[33] aus. Wenn diese Realisierung verpflichtend sein soll, dann sollte dies auch im Gesetz festgeschrieben werden (§ 28 Abs. 1 letzter Satz scheint als Rechtsgrundlage dafür nicht auszureichen.)

Nicht nachvollziehbar ist für die RTR-GmbH, wieso im Entwurf für § 29 Abs. 3 ZustellG vorgesehen ist, dass die Liste der elektronischen Zustelladressen nicht bloß für „die Behörden“, sondern auch für „die übrigen elektronischen Zustelldienste“ zugänglich sein muss.

Mit freundlichen Grüßen

RTR-GmbH
Rundfunk und Telekom
Regulierungs-GmbH

Dr. Georg Serentschy
Geschäftsführer Fachbereich Telekommunikation

[33] http://www.cio.gv.at/onlineservices/delivery/Zustellung_Schema_Zustellverzeichnis_20030506.pdf

Nachtrag zur Stellungnahme der RTR-GmbH zum e-Government-Gesetz, 27.08.2003

Kurz nach dem Versenden der Stellungnahme der RTR-GmbH zum Entwurf des e-Government-Gesetzes wurden wir darauf hingewiesen, dass die Berechnung der Stammzahl anders geplant ist, als wir dies aus dem Gesetzesentwurf, den Erläuterungen und den bislang veröffentlichten Dokumenten dazu verstanden haben.

Die Grafik in Kapitel A.2 der Stellungnahme der RTR-GmbH ist grundsätzlich immer noch richtig; allerdings sollen nach den nun vorliegenden Informationen zwei verschiedene Ableitungen zur Anwendung kommen. Die Ableitung der Stammzahl aus der ZMR-Zahl (§ 6 des e-GovG-Entwurfs) soll eine 3DES-Verschlüsselung mit einem nur der Stammzahlregisterbehörde bekannten geheimen Schlüssel umfassen. Für die Ableitungen der bereichsspezifischen Personenkennzeichen aus der Stammzahl (§ 8 des e-GovG-Entwurfs) sollen weiterhin Hashfunktionen verwendet werden.

Die Ableitung der Stammzahl aus der ZMR-Zahl wäre nach diesem neuen Konzept tatsächlich nur der Stammzahlregisterbehörde möglich. Bei entsprechender Ausgestaltung (vor allem: entsprechender Länge) der Stammzahl wäre es auch tatsächlich nicht möglich, aus einem bPK die dazugehörige Stammzahl oder ein anderes bPK zu errechnen, wodurch das angestrebte Datenschutzziel wesentlich besser erreicht werden könnte.

Unverändert bliebe, dass jemand, der Zugang zur Stammzahl hat, daraus alle bPK errechnen kann. Insbesondere wäre die Stammzahlregisterbehörde in der Lage, alle Verfahren zusammenzuführen. Unverändert bliebe auch, dass das bPK für den Verwaltungsbereich „Zustellwesen“ sich in der Praxis zu einem Personenkennzeichen entwickeln kann, das in der gesamten Verwaltung zum Einsatz kommen wird (vgl. dazu den letzten Absatz aus Kapitel A.2 der Stellungnahme).[34]

Aus Sicht der RTR-GmbH ergeben sich zum neuen Konzept die folgenden Anmerkungen:

- Festzuhalten ist, dass es sich dabei um eine deutliche Änderung gegenüber den bisher bekannten Konzepten handelt und dass bislang in keinem veröffentlichten Dokument diesbezügliche Ausführungen enthalten sind. In den Erläuterungen zu § 6 e-GovG-Entwurf ist zur Berechnung der Stammzahl gar nichts ausgeführt, bezüglich der an Personen ohne Melde- und Steuerpflicht ausgestellte Ersatz-Stammzahl ist jedenfalls von einer „Einwegfunktion“ die Rede, also von einer Hashfunktion und nicht von einer symmetrischen Verschlüsselung.

[34] In http://www.cio.gv.at/onlineservices/delivery/Zustellung_Modell_20030506.pdf, „Modell der elektronischen Zustellung“, wird in Kapitel 3.2.2 „allgemein empfohlen, elektronische Zustellungen unter der Verwendung der VPK vorzunehmen“ und ein Modul beschrieben, das aus dem Namen und der VPK (nun: dem bPK) des jeweiligen Verwaltungsbereiches die VPK (nun: das bPK) für den Verwaltungsbereich „Zustellung“ errechnet. Mit diesem Modul könnten also zwei Verwaltungsbehörden aus verschiedenen Verwaltungsbereichen jeweils aus ihren bereichsspezifischen Personenkennzeichen das Personenkennzeichen für die Zustellung ausrechnen und dann unter Umgehung der Stammzahlenregisterbehörde Daten zusammenführen.

Die RTR-GmbH regt an, dass solch grundsätzliche konzeptuellen Fragen durch das Gesetz oder eine Verordnung determiniert werden, dass also durch das beschlossene Gesetz geregelt wird, wo Verschlüsselung eingesetzt wird und wo Hashfunktionen verwendet werden.

In diesem Zusammenhang wird weiters auf die erforderliche Planungssicherheit für Unternehmen hingewiesen, die bereits jetzt Anwendungen auf der Grundlage der veröffentlichten Spezifikationen entwickeln (vgl. Kapitel A.4 unserer Stellungnahme).

- Das neue Konzept bedeutet jedenfalls, dass die Sicherheitsinfrastruktur der Stammzahlregisterbehörde wesentlich kritischer einzustufen sein wird und dass dem Sicherheitskonzept der Stammzahlregisterbehörde dadurch noch größere Bedeutung zukommt (vgl. dazu die Ausführungen in Kapitel A.3 der Stellungnahme der RTR-GmbH). Man muss sich dazu vor Augen führen, dass die Stammzahlregisterbehörde einen geheimen Schlüssel verwahren wird, der in die Berechnung sämtlicher im e-Government verwendeten Personenkennzeichen – aller Stammzahlen und aller bereichsspezifischen Personenkennzeichen – einfließt sowie nach den §§ 14 bis 16 e-GovG-Entwurf auch für den privaten Bereich relevant sein wird.

  Wird der geheime Schlüssel der Stammzahlregisterbehörde kompromittiert, dann wird der durch das komplexe System angestrebte Datenschutz nicht erzielt und jeder, der den geheimen Schlüssel erfahren hat, kann aus den ZMR-Zahlen alle Stammzahlen und bPKs ausrechnen. Verliert die Stammzahlregisterbehörde den geheimen Schlüssel, dann ist es unmöglich, den Zusammenhang zwischen ZMR-Zahl und Stammzahl nachzurechnen.

  In das Sicherheitskonzept der Stammzahlregisterbehörde müssten daher zusätzliche Überlegungen zum Schutz des geheimen Schlüssels vor unbefugtem Zugriff (nach den der RTR-GmbH vorliegenden Informationen ist die Speicherung in einem Hardware Security Module geplant, über organisatorische Sicherheitsmaßnahmen liegen der RTR-GmbH keine Informationen vor) und zum Schutz des geheimen Schlüssels vor Verlust (Backupkonzept) aufgenommen werden.

  Weiters sollten Szenarien erstellt werden, wie man vorgeht, wenn der geheime Schlüssel trotz der Sicherheitsmaßnahmen verloren geht oder wenn man später einmal auf eine andere Technologie umsteigen will: Erhalten dann alle Bürger neue Stammzahlen und bPKs (was ein Umstiegsszenario in den Verwaltungsapplikationen bedingen würde) oder gibt es einen Mischbetrieb aus nach „alter“ und nach „neuer“ Methode berechneten Stammzahlen und bPKs?

- In diesem Zusammenhang regt die RTR-GmbH an, zu erwägen, dass statt symmetrischer Verschlüsselung ein Signaturverfahren (also asymmetrische Verschlüsselung) eingesetzt wird. Dies hätte für das Sicherheitskonzept den Vorteil, dass für den Fall des Verlusts des privaten Schlüssels, mit dem die Stammzahlen errechnet werden, immerhin noch im nachhinein mit dem

öffentlichen Schlüssel die richtige Zuordnung zwischen ZMR-Zahl und Stammzahl nachgeprüft werden könnte. Man könnte dann im Sicherheitskonzept Abstufungen zwischen der Geheimhaltung des privaten Schlüssels und der Geheimhaltung des zugehörigen öffentlichen Schlüssels vornehmen.

Mit freundlichen Grüßen

RTR-GmbH
Rundfunk und Telekom
Regulierungs-GmbH

Dr. Georg Serentschy
Geschäftsführer Fachbereich Telekommunikation