Bundeskanzleramt
z. Hd. Dr. Waltraut Kotschy
Ballhausplatz 1
1010 Wien

ANOR 3/2001-30 Wien, am 17.08.2004
DK/UL

Betreff: Stellungnahme der RTR-GmbH zum Begutachtungsentwurf der Novelle der Signaturverordnung, GZ 810.200/0001-V/3/2004

Sehr geehrte Frau Dr. Kotschy,

die Rundfunk und Telekom Regulierungs-GmbH dankt für die Zusendung des Begutachtungsentwurfs der Novelle der Signaturverordnung und nimmt dazu wie folgt Stellung.

Allgemeines

1. Änderungen gegenüber dem Entwurf des BMJ

Das Bundesministerium für Justiz hat Vertreter der RTR-GmbH und der Bestätigungsstelle A-SIT zu einer Reihe von Besprechungen eingeladen, um die Erfahrungen aus der Vollziehung der Signaturverordnung zu berücksichtigen. Am 26.09.2003 hat das Bundesministerium für Justiz einen Entwurf an das Bundeskanzleramt übersandt, der mit RTR-GmbH und A-SIT akkordiert war.

Wir sind nun überrascht, dass der in Begutachtung übersandte Entwurf vom akkordierten Text (den wir in der Folge als „BMJ-Entwurf“ zitieren werden) doch in vielen Punkten abweicht. In den meisten Punkten handelt es sich dabei zwar nur um sprachliche Neuformulierungen und Umgliederungen, teilweise sind durch die Überarbeitung aber auch offenkundige Fehler entstanden.

Bei einer Reihe von Bestimmungen (siehe dazu im Einzelnen unten) schlagen wir daher vor, die zuletzt vorgenommenen Änderungen wieder rückgängig zu machen und zur Formulierung des BMJ-Entwurfs zurückzukehren.

2. Umfang der Pflicht zur Prüfung und Bescheinigung

Eine für die Praxis entscheidende Frage ist die der Reichweite des § 9 SigV. Um eine sichere elektronische Signatur zu erstellen, benötigt der Signator nicht nur die Signaturerstellungseinheit im engeren Sinn (in der Praxis derzeit immer eine Chipkarte), sondern auch weitere Software und Hardware (in der Praxis derzeit in der Regel ein „Secure Viewer“ zur Anzeige des zu signierenden Dokumentes und ein – meist mit eigenem Pinpad ausgestattetes – Chipkarten-Lesegerät).

Nach der geltenden Signaturverordnung bedürfen alle „technischen Komponenten und Verfahren“ zur Erstellung sicherer elektronischer Signaturen einer Prüfung und Bescheinigung. Daher müssen insbesondere auch Viewer-Programme geprüft und bescheinigt werden. Die Aufsichtsstelle hat diesbezüglich zwar in ihren Akkreditierungsbescheiden als zulässig angesehen, dass die Bescheinigung nicht sofort, sondern binnen 12 Monaten ab Einsatz des Viewer-Programmes vorgelegt wird, dies ändert aber nichts an der materiellen Verpflichtung. Aufgrund der geltenden Rechtslage wurden von mehreren österreichischen Unternehmen Produkte entwickelt.

In den letzten Jahren wurde von Seiten des Bundeskanzleramtes immer wieder angekündigt, mit der Novelle der Signaturverordnung werde die Bescheinigungspflicht für Viewer-Programme fallen. Eine Abschaffung dieser Pflicht würde auch einen möglichen Verstoß gegen das Europarecht beseitigen, da man Österreich evtl. vorwerfen könnte, Anhang 3 der Signaturrichtlinie 1999/93/EG zu rigoros auszulegen. Fast alle anderen Mitgliedsstaaten (ausgenommen Deutschland) interpretieren Art. 3 Abs. 4 und den Anhang 3 der Richtlinie so, dass die dort vorgesehene Bescheinigung von Produkten ausschließlich für sichere Signaturerstellungseinheiten erforderlich ist.

Aus Sicht der RTR-GmbH ist für den Vollzug der SigV vor allem wichtig, dass sich aus der SigV eindeutig ableiten lässt, welche Produkte der Prüfung und Bescheinigung bedürfen und welche nicht. Dies ist im Begutachtungsentwurf leider nicht der Fall. § 3 Abs. 1 nennt „sämtliche technische Komponenten und Verfahren“, was auf eine Fortführung der Bescheinigungspflicht von Viewer-Programmen hindeutet, allerdings verwendet die Bestimmung auch die unklare Formulierung „... müssen im Hinblick auf das Erfordernis ihrer Überprüfbarkeit den Anforderungen des § 9 SigV entsprechen“ – so als ob die Produkte nicht überprüft werden müssten, sondern nur „überprüfbar“ sein müssten. Außerdem stellt die Bestimmung Anforderungen an Produkte zur „Speicherung sicherer elektronischer Signaturen“ – offensichtlich werden hier Signaturen und Signaturerstellungsdaten verwechselt.

Die RTR-GmbH gibt in diesem Zusammenhang auch zu bedenken, dass der Entwurf des neuen § 9 anders als im bisherigen Text (und z. B. auch in der deutschen Signaturverordnung) nicht mehr die Prüfstufe (also den Detaillierungsgrad der Prüfung, z. B. „EAL 4“ bei den Common Criteria oder „E 3“ bei ITSEC) und auch nicht die Mechanismenstärke (also z. B. „hoch“ = Mechanismen, die nur von Angreifern überwunden werden können, die über

sehr gute Fachkenntnisse, Gelegenheiten und Betriebsmittel verfügen, wobei ein erfolgreicher Angriff als normalerweise nicht durchführbar beurteilt wird) regelt. Soweit § 9 nur auf die von der Europäischen Kommission veröffentlichten Referenznummern verweist (die insbesondere für die Prüfung von Chipkarten und Hardware-Sicherheitsmodulen relevant sind) ist die Festlegung der Prüfstufe und Mechanismenstärke in der Verordnung entbehrlich, da sich diese aus den von der Kommission referenzierten Schutzprofilen selbst ergibt. Sofern jedoch auch andere Produkte wie z. B. Viewer-Programme zu evaluieren und zu bescheinigen wären (wobei wahrscheinlich eine niedrigere Prüfstufe wie EAL 3 zur Anwendung kommen müsste) wäre dies wohl in der Verordnung näher zu determinieren.

Die RTR-GmbH regt daher an, dass auf Grund der Ergebnisse des Begutachtungsverfahrens eine klare Definition in die Signaturverordnung aufgenommen wird, aus der sich eindeutig ableiten lässt, welche technischen Komponenten (insbesondere Chipkarten, Chipkarten-Lesegeräte und Viewer-Programme auf der Seite des Signators, Hardware-Sicherheitsmodule, Zeitstempelgeräte, Software zum Ausstellen der Zertifikate und Widerrufslisten auf der Seite des Zertifizierungsdiensteanbieters) evaluiert und/oder bescheinigt werden müssen und welche nicht. Dabei sollte nach Ansicht der RTR-GmbH jedenfalls eine deutliche Trennung danach vorgenommen werden, ob eine Prüfpflicht aus der Signaturrichtlinie (insbesondere Art. 3 Abs. 4 und 5) ableitbar ist oder nicht. Demnach sollte für vertrauenswürdige Systeme nach Anh. II lit. f der Richtlinie und sichere Signaturerstellungseinheiten nach Anh. III der Richtlinie jedenfalls die Evaluierung nach einer allgemein anerkannten Norm oder die Begutachtung durch eine Bestätigungsstelle verpflichtend sein, für sichere Signaturerstellungseinheiten wäre darüber hinaus auch die Bescheinigung durch eine Bestätigungsstelle erforderlich. Die bloße „Überprüfbarkeit“ reicht in diesen Fällen jedenfalls nicht aus. Wenn auch für andere Komponenten (Chipkarten-Lesegeräte, Viewer-Programme, Software der Zertifizierungsdiensteanbieter) eine Prüfpflicht vorgeschrieben werden sollte, sollte die Verordnung jedenfalls für Evaluierungen nach Common Criteria auch Vertrauenswürdigkeitsstufe und Stärke der Funktionen, für Evaluierungen nach ITSEC Evaluationsstufe und Stärke der Mechanismen regeln.

3. Algorithmen/Anhang

In den vom Bundesministerium für Justiz geleiteten Gesprächen zur Vorbereitung der Novelle bestand Einigkeit darüber, dass Österreich sich in der Algorithmenfrage den auf europäischer Ebene beschlossenen Regelungen anschließen solle und dass das von einer Arbeitsgruppe der European Electronic Signature Standardisation Initiative (EESSI) erarbeitete „Algorithmenpapier“ den aktuellen Diskussionsstand auf europäischer Ebene am besten wiedergibt. Diskutiert wurde, ob die Verordnung auf das Algorithmenpapier verweisen solle oder ob es als Anhang zur Verordnung abgedruckt werden solle. Letztlich wurde eine Übersetzung des maßgeblichen Kapitels 4 aus dem Algorithmenpapier erstellt, um eine möglichst wörtliche Übernahme in den österreichischen Rechtsbestand zu gewährleisten.

Das „Algorithmenpapier“ lag lange nur in einer nicht zitierbaren Version vor. Im März 2003 wurde es als ETSI Special Report veröffentlicht (ETSI SR 002 176 V1.1.1). Allerdings werden die Algorithmen darin nur bis Ende 2005 geregelt, und ein Special Report wird von ETSI nicht aktualisiert.

Derzeit gibt es auf europäischer Ebene eine Aktivität von ETSI, einen regelmäßig zu aktualisierenden Technical Standard (ETSI TS 102 176) zu erarbeiten. ETSI TS 102 176 soll planmäßig im November 2004 beschlossen und im Dezember 2004 veröffentlicht werden. ETSI arbeitet diesbezüglich auch mit dem von der Europäischen Kommission geförderten Forschungsprojekt ECRYPT zusammen.

Es ist bedauerlich, dass sich derzeit noch nicht deutlich abzeichnet, welche Algorithmen ab 01.01.2006 gelten sollen und dass die Europäische Kommission derzeit wenig Interesse zeigt, die Algorithmen überhaupt nach dem Verfahren des Art. 3 Abs. 5 der Signaturrichtlinie zu veröffentlichen und diese Frage somit europaweit einheitlich zu entscheiden. Andererseits wird in jeder der gemäß Art. 3 Abs. 5 der Richtlinie allgemein anerkannten Normen (CWA 14167-1, CWA 14167-2 und CWA 14169) auf „Algorithms and parameters for algorithms, list of algorithms and parameters eligible for electronic signatures, procedures as defined in the directive 1999/93/EC, article 9 on the ‘Electronic Signature Committee’ in the Directive“ verwiesen (in CWA 14167-1 sogar als normative Referenz). Insofern bildet dieses Dokument ein unverzichtbares Fundament für die genannten Normen.

Jedenfalls geht die RTR-GmbH davon aus, dass das Algorithmenpapier in der Fassung von ETSI SR 002 176 am besten den europäischen Diskussionsstand wiedergibt und zur Anwendung kommen sollte, bis ein Nachfolgestandard wie ETSI TS 102 176 beschlossen wird. Für die RTR-GmbH ist nicht verständlich, wieso der Begutachtungsentwurf nicht die vorliegende Übersetzung des ETSI SR 002 176, die mit den Experten von RTR-GmbH und A-SIT abgestimmt wurde, als Anhang enthält, sondern eine Kurzfassung, die zahlreiche Fehler, Ungenauigkeiten und Unvollständigkeiten enthält (siehe dazu im Einzelnen die Anmerkungen unten).

Aus Sicht der RTR-GmbH gibt es legistisch zwei sinnvolle Möglichkeiten:

- Eine Möglichkeit bestünde darin, die Verordnung ohne Anhang zu erlassen und stattdessen an den entsprechenden Stellen des Verordnungstextes auf ETSI SR 002 176 zu verweisen. Diese Variante hätte insbesondere den Vorteil, dass auf einen Nachfolgestandard wie ETSI TS 102 176 durch eine sehr kurze Novelle verwiesen werden könnte, ohne dass eine Übersetzung notwendig wäre. Die ETSI-Dokumente sind im Internet als PDF-Datei kostenfrei verfügbar, sind also ebenso zugänglich wie das Bundesgesetzblatt. Das einzige Argument gegen diese Variante ist, dass die ETSI-Dokumente in englischer Sprache, also nicht in der Amtssprache verfasst sind. Allerdings entfalten die Verweise in der SigV nur für ein beschränktes Fachpublikum von Herstellern, Zertifizierungsdienste-anbietern, Bestätigungsstellen und die Aufsichtsstelle normative Wirkung;

die Signatoren müssen die Algorithmen nicht beachten, sondern nur die Empfehlungen ihres Zertifizierungsdiensteanbieters.

- Die andere Möglichkeit besteht darin, eine Übersetzung der entsprechenden Dokumente als Anhang zum Verordnungstext wiederzugeben. Wählt man diese Variante, dann würde die RTR-GmbH jedenfalls die möglichst wörtliche Wiedergabe bevorzugen. Im zur Begutachtung versandten Anhang gingen durch die radikalen Kürzungen zahlreiche wesentliche Inhalte völlig verloren, weiters enthält der Anhang auch Fehler und Ungenauigkeiten (siehe dazu im Einzelnen unten). Es sollte daher, wenn die Verordnung mit Anhang erlassen werden soll, unbedingt die vorliegende Übersetzung des ETSI SR 002 176 verwendet werden.

4. Finanzierung der Aufsichtsstelle

Die bislang in § 1 Abs. 2 vorgesehene Gebühr von 2 Euro pro qualifiziertem Zertifikat und Jahr wurde im Begutachtungsentwurf gestrichen. Diese Gebühr war bei der Erlassung der SigV im Jahr 2000 als wesentlichster Beitrag zur Finanzierung der Aufsichtsstelle gedacht. Obwohl die Kosten der Aufsichtsstelle bislang aufgrund der geringen Anzahl qualifizierter Zertifikate aus dieser Gebühr keineswegs gedeckt werden konnten, wäre doch zu erwarten, dass die Gebühr in der Zukunft einen nennenswerten Beitrag dazu leisten könnte. Die RTR-GmbH begrüßt die Bereitschaft des Bundeskanzleramtes, die Kosten der Aufsichtsstelle in Zukunft aus dem Budget zu bedecken, weist aber – auch im Hinblick auf die Aussage im Vorblatt zum Begutachtungsentwurf, das Vorhaben werde „zu keiner Kostenbelastung der öffentlichen Haushalte führen“ – darauf hin, dass die diesbezüglichen Verhandlungen – wenngleich in weiten Bereichen bereits Übereinstimmung erzielt werden konnte – noch nicht abgeschlossen sind. Die Gebühr kann aus Sicht der RTR-GmbH jedenfalls nur dann abgeschafft werden, wenn die Finanzierung der Aufgaben der Aufsichtsstelle aus anderen Mitteln sichergestellt ist.

Zu den einzelnen Bestimmungen

§ 1 – Gebühren für Leistungen der Aufsichtsstelle

Der BMJ-Entwurf hätte in § 1 nur die Bezeichnung „Telekom-Control GmbH“ durch die seit 01.04.2001 richtige Bezeichnung „Rundfunk und Telekom Regulierungs-GmbH“ ersetzt und klargestellt, dass die hohen Gebührenansätze in § 1 Abs. 1 Z 5 lediglich für Anbieter qualifizierter Zertifikate zum Tragen kommen sollen.

Der Begutachtungsentwurf formuliert § 1 nun völlig neu. Zur wesentlichsten Änderung – der Streichung der Gebühr von 2 Euro pro qualifiziertem Zertifikat und Jahr – wurde bereits oben im allgemeinen Teil Stellung genommen.

Nicht nachvollziehbar ist für die RTR-GmbH, weshalb bei der Neuformulierung des § 1 nur mehr die Leistungen der Aufsichtsstelle (das ist die Telekom-

Control-Kommission), aber nicht mehr die Leistungen der RTR-GmbH genannt sind. Wir verweisen darauf, dass die Signaturverordnung gemäß § 25 Z 1 SigG „die Festsetzung pauschaler kostendeckender Gebühren für die Leistungen der Aufsichtsstelle und der RTR-GmbH“ zu enthalten hat, dass manche der genannten Leistungen ausschließlich von der RTR-GmbH erbracht werden (insbesondere die Führung der Verzeichnisse, § 15 Abs. 2 Z 3 SigG) und dass auch in jenen Bereichen, wo die Kompetenz bei der Telekom-Control-Kommission liegt, ein Großteil der Kosten für die Tätigkeit der RTR-GmbH als Geschäftsapparat der Telekom-Control-Kommission anfällt. Zudem ist darauf hinzuweisen, dass mit der Streichung der RTR-GmbH aus dem neuen § 1 Abs. 2 (im geltenden § 1 Abs. 3 noch „Telekom-Control GmbH“) auch der Kostenersatz für den Fall, dass sich die RTR-GmbH einer Bestätigungsstelle bedient, ungeregelt wäre.

Im Begutachtungsentwurf wurden die Gebührenansätze nun neu gegliedert. Die RTR-GmbH weist auf folgende Änderungen hin:

- Die bei der Aufnahme der Tätigkeit eines Anbieters qualifizierter Zertifikate oder sicherer Signaturen anfallenden Gebühren erhöhen sich von bislang 6.000 Euro (§ 1 Abs. 1 Z 1 lit. b der geltenden SigV) auf 6.100 Euro (§ 1 Abs. 1 Z 1 und 2 des Entwurfs).

- Für Anbieter, die keine qualifizierten Zertifikate und keine sicheren Signaturen anbieten, entfällt die Gebühr von 50 Euro für Änderungsanzeigen (§ 1 Abs. 2 lit. a der geltenden SigV).

- In § 1 Abs. 1 Z 2 und 3 des Entwurfs ist nun nur mehr die „Überprüfung des Sicherheits- und Zertifizierungskonzepts“ erwähnt, obwohl die Aufsichtsstelle ja nicht bloß das Konzept (sondern nach § 13 Abs. 2 SigG vor allem dessen Umsetzung) zu überprüfen hat und auch die Gebühren nach § 1 Abs. 1 Z 5 im Falle einer Anzeige wohl nicht vorgeschrieben werden können. Die bisherige Formulierung „Überprüfung eines Zertifizierungsdiensteanbieters“ beschreibt die Leistungen der Aufsichtsstelle und der RTR-GmbH daher korrekter und entspricht daher auch besser dem Prinzip der Kostenwahrheit.

- § 1 Abs. 1 Z 5 des Entwurfs sieht eine relativ hohe Gebühr von 6.000 Euro für jede „anlassbezogene Prüfung, die zu Aufsichtsmaßnahmen geführt hat“ vor. Dieser hohe Gebührensatz war in § 1 Abs. 1 Z 5 lit. b und c der geltenden SigV einem „nicht nur unerheblichen Verstoß“ gegen SigG und SigV bzw. der Unterlassung der Anzeige sicherheitsrelevanter Veränderungen vorbehalten. Bei bescheidmäßig erteilten Auflagen aufgrund sicherheitsrelevanter Mängel ist nach § 1 Abs. 1 Z 6 der geltenden SigV eine Gebühr von 1 000 Euro vorzuschreiben. Der Begutachtungsentwurf sieht in diesem Fall nur nach einer vorangegangenen Überprüfung des Zertifizierungsdiensteanbieters eine Gebühr vor (selbst dann, wenn ein Sicherheitsmangel auch ohne umfassende Überprüfung vor Ort festgestellt werden kann oder wenn eine Aufsichtsmaßnahme schon vor Abschluss einer umfassenden Überprüfung erforderlich ist). Die RTR-GmbH schlägt daher vor, die Gebühren für die

bescheidmäßige Erteilung von Auflagen sowie für die bescheidmäßige Untersagung der Tätigkeit eines Zertifizierungsdiensteanbieters entsprechend der geltenden SigV zu regeln.

§§ 3 bis 7

Die §§ 3 bis 7 wurden gegenüber dem BMJ-Entwurf völlig neu gegliedert und in vielen Punkten neu formuliert. Für die RTR-GmbH ist nicht nachvollziehbar, wieso diese Änderungen vorgenommen wurden, zumal der Begutachtungsentwurf nun einige offensichtliche Fehler aufweist:

- Fast alle Verweise auf den die Algorithmen regelnden Anhang wurden gestrichen. Ginge es nach dem Begutachtungsentwurf, dann würden Kriterien bezüglich der Algorithmen und deren Parameter nur für die „Erzeugung der Signaturerstellungsdaten für sichere elektronische Signaturen“ (§ 3 Abs. 2) gelten, für die Signaturerstellungsdaten der Zertifizierungsdiensteanbieter (§ 5 Abs. 1) würde der Anhang nicht gelten, obwohl auch im europäischen Umfeld Kriterien für die vom Zertifizierungsdiensteanbieter eingesetzten Algorithmen und Parameter vorgesehen sind (so wird beispielsweise in der für vertrauenswürdige Systeme beim Zertifizierungsdiensteanbieter maßgeblichen allgemein anerkannten Norm CWA 14167-1 eine Liste der in Frage kommenden Algorithmen und Parameter als normative Referenz zitiert). Für die Hashverfahren findet sich nur im Anhang selbst eine Bestimmung, nicht mehr im eigentlichen Verordnungstext. Die RTR-GmbH schlägt daher vor, § 5 Abs. 1 durch folgenden Satz zu ergänzen: „Signaturerstellungsdaten für Signaturen in qualifizierten Zertifikaten gemäß § 5 Abs. 3 SigG müssen die Anforderungen des Anhangs erfüllen.“

- Nach § 3 Abs. 1 des Entwurfs müssten „sämtliche“ technischen Komponenten und Verfahren nach § 9 bescheinigt werden, auch solche, die bei der „Erstellung und Speicherung sicherer elektronischer Signaturen zum Einsatz kommen“. Offensichtlich wurde hier die (sicherheitstechnisch unproblematische) Speicherung von Signaturen mit der (wegen der Gefahr des Ausspähens heiklen) Speicherung von Signaturerstellungsdaten verwechselt. Offenbar sollen in § 3 Abs. 1 und 2 des Begutachtungsentwurfs die Inhalte von § 3 Abs. 1 und § 7 Abs. 1 des BMJ-Entwurfs kombiniert werden. Unter diesem Aspekt würde die RTR-GmbH folgende Formulierung vorschlagen: „Signaturerstellungseinheiten für sichere elektronische Signaturen sowie technische Komponenten und Verfahren, die bei der Erzeugung von Signaturerstellungsdaten für sichere elektronische Signaturen eingesetzt werden, müssen den Anforderungen des § 9 entsprechen. Die dabei eingesetzten Algorithmen und deren Parameter müssen die Anforderungen des Anhangs erfüllen.“

- Der unbestimmte Verweis auf den „Stand der Technik“ in § 3 Abs. 2 Satz 2 ist legistisch unsauber. Offensichtlich wird damit beabsichtigt, die aus dem Anhang gestrichenen Teile des ETSI SR 002 176 auf diesen Umweg doch wieder verbindlich zu machen. Korrekter wäre es, entweder direkt auf das ETSI-Dokument zu verweisen, oder – wie im BMJ-Entwurf vorgesehen –

eine Übersetzung dieses Dokumentes als Anhang anzufügen. Vor allem dann, wenn das (nur bis Ende 2005 gültige) Dokument ETSI SR 002 176 durch einen technischen Standard (ETSI TS 102 176) ersetzt wird, wäre die Auslegung des Begriffs „Stand der Technik“ problematisch.

- Bei § 5 des Entwurfs passt die Überschrift offensichtlich nicht zum Inhalt – insbesondere nicht zu Abs. 2 –, in den Erläuterungen werden Signaturprüfung und Hashverfahren verwechselt. Da für Signaturerstellungseinheiten, die von Zertifizierungsdiensteanbietern bei der Ausstellung qualifizierter Zertifikate verwendet werden, nach Art. 3 der Signaturrichtlinie keine Bescheinigung einer Bestätigungsstelle erforderlich ist und da auch der Eindruck einer Bescheinigungspflicht vermutlich nicht beabsichtigt war, sollte in § 5 Abs. 1 nicht auf § 9 insgesamt, sondern lediglich auf § 9 Abs. 1 und 2 Bezug genommen werden.

Aufgrund der genannten Unstimmigkeiten und Fehler regt die RTR-GmbH an, die Änderungen rückgängig zu machen und stattdessen den vom Bundesministerium für Justiz mit den ExpertInnen von RTR-GmbH und A-SIT erarbeiteten Text zu verwenden.

Zu den einzelnen Bestimmungen in den §§ 3 bis 5:

- § 3 Abs. 1: Wie oben bereits erwähnt, wurde die „Speicherung von Signaturen“ mit der „Speicherung von Signaturerstellungsdaten“ verwechselt. Unklar ist auch die Formulierung, derzufolge die technischen Komponenten nicht „nach § 9 geprüft“, sondern bloß (?) „im Hinblick auf das Erfordernis ihrer Überprüfbarkeit den Anforderungen des § 9 entsprechen“ müssen. Dies erweckt den Anschein, Signaturerstellungseinheiten müssten nicht geprüft, sondern nur „überprüfbar“ sein. Für die RTR-GmbH ist nicht nachvollziehbar, wie diese Bestimmung vollzogen werden soll.

- § 3 Abs. 2: Der zweite Satz betreffend den „Stand der Technik“ ist – wie bereits erwähnt – für die RTR-GmbH nicht nachvollziehbar. Vgl. dazu auch die Anmerkungen zum Anhang.

- § 4 Abs. 1: Es ist unklar, welche Bedeutung die einleitende Formulierung „Zusätzlich zu den in § 3 aufgezählten Erfordernissen ...“ hat und warum die Bestimmungen des § 4 Abs. 1 und 2 überhaupt von den Bestimmungen in § 3 getrennt wurden. Insbesondere ist nicht ganz klar, ob Viewer-Programme nach § 9 geprüft und bescheinigt werden müssen. Aus dem Verweis auf § 3 – und somit auch auf § 3 Abs. 1 – ergibt sich nach Ansicht der RTR-GmbH ein Fortbestehen der Bescheinigungspflicht, was allerdings im Widerspruch zu den öffentlichen Ankündigungen des Bundeskanzleramtes für die Novelle der Signaturverordnung stehen würde.

- Die Überschrift des § 5 passt nicht zum Inhalt des § 5 Abs. 2.

- § 5 Abs. 1: Gegenüber dem BMJ-Entwurf wurde der Verweis auf § 5 Abs. 3 SigG und der Verweis auf den Anhang gestrichen. Die von den

Zertifizierungsdiensteanbietern verwendeten Algorithmen sind somit völlig ungeregelt. Auch im Anhang selbst findet sich keine Bestimmung zur Signatur qualifizierter Zertifikate.

- § 5 Abs. 2: Der erste Satz wurde gegenüber § 6 Abs. 3 im BMJ-Entwurf sprachlich umformuliert und erweckt nun auf den ersten Blick den Anschein, als ob sie für alle Zertifizierungsdiensteanbieter gelten würde. Die Formulierung im BMJ-Entwurf war nach Ansicht der RTR-GmbH verständlicher.

§ 9 – Prüfung der technischen Komponenten und Verfahren für sichere Signaturen

Zunächst sei auf den allgemeinen Teil unserer Stellungnahme verwiesen.

Im ersten Satz wurde gegenüber dem BMJ-Entwurf der Halbsatz „die bei der Erstellung sicherer Signaturen zum Einsatz kommen“ eingefügt. Durch diese Einschränkung würden technische Komponenten der Zertifizierungsdienste-anbieter (z. B. Hardware-Sicherheitsmodule zur Signatur qualifizierter Zertifikate) und technische Komponenten zur Erzeugung von Signaturerstellungsdaten (z. B. wenn ein Schlüsselpaar nicht in der Chipkarte selbst, sondern von einem eigenen Schlüsselgenerierungsmodul erzeugt werden) aus dem Anwendungsbereich des § 9 herausfallen, was sicher nicht beabsichtigt war. Der Halbsatz sollte daher wieder gestrichen werden.

§ 11 – Antrag auf Ausstellung eines qualifizierten Zertifikats

Der BMJ-Entwurf hätte vorgesehen, in § 11 Abs. 2 Z 1 das Wort „Adresse“ durch „Hauptwohnsitz“ zu ersetzen. Dies wäre aus Sicht der RTR-GmbH eine sinnvolle Änderung, zumal bei der Ausstellung qualifizierter Zertifikate üblicherweise ohnehin auch eine Personenbindung nach § 4 Abs. 2 E-GovG ausgestellt werden wird, wofür eine Abfrage beim Zentralen Melderegister erforderlich ist. Warum diese Änderung im Begutachtungsentwurf nicht mehr enthalten ist, ist für die RTR-GmbH nicht ersichtlich.

Die im Begutachtungsentwurf enthaltene Neufassung des § 11 Abs. 1 SigV ist offenbar als Reaktion auf Anregungen vor allem der Banken zur Vereinfachung des Registrierungsprozesses gedacht. Soweit diese Anregungen der RTR-GmbH bekannt sind, ginge es den Banken vor allem darum, dass die Registrierung auf Standard-Bildschirmarbeitsplätzen in den Bankfilialen möglich wäre, ohne dass Scanner als technische Zusatzausstattung vorgesehen werden müssen. Dies könnte erreicht werden, wenn das Erfordernis der Herstellung einer Ablichtung des Lichtbildausweises (§ 11 Abs. 1 dritter Satz der geltenden SigV) gestrichen würde – die Daten des Ausweises (Ausstellungsdatum, Nummer und ausstellende Behörde) müssen ohnehin nach § 11 Abs. 2 Z 1 SigV separat erfasst werden. Der Begutachtungsentwurf hingegen enthält nur für elektronisch lesbare Ausweise eine Vereinfachung. Diese Einschränkung ist für die RTR-GmbH nicht nachvollziehbar. Aus Sicht der RTR-GmbH könnte einerseits eine Regelung vorgesehen werden, nach der das Erfassen der Ausweisdaten ohne

Herstellung einer Kopie ausreicht. Andererseits könnte die bestehende Regelung beibehalten werden, wenn der Verordnungsgeber z. B. Wert darauf legt, dass der Ausweis in seiner Gesamtheit dokumentiert wird. Der Mittelweg, einerseits auf die Ausweiskopie zu verzichten, andererseits aber weiterhin Scanner am Registrierungsarbeitsplatz de facto vorzuschreiben, würde die Nachteile beider Regelungsansätze verbinden.

Im Entwurf des § 11 Abs. 1 wäre nun nicht mehr vorgesehen, dass es sich um einen „amtlichen" Lichtbildausweis handeln muss. Das würde aber dem Wortlaut des § 8 SigG widersprechen.

§ 12

Im BMJ-Entwurf war vorgesehen, dass die Formate für qualifizierte Zertifikate „formal und vollständig zu spezifizieren sind", dies wurde nun auf „eindeutig und vollständig" geändert. Nach Ansicht der RTR-GmbH hat der Begriff „formal" besser wiedergegeben, was erwünscht ist, nämlich eine Notation in einer formalen Sprache wie ASN.1.

In den Erläuterungen zur Änderung des § 12 Abs. 4 wurde ein im BMJ-Entwurf enthaltener Satz nun in kursive Schrift gesetzt und mit drei Fragezeichen versehen. Die RTR-GmbH erlaubt sich, die Hintergründe für die Änderung des § 12 Abs. 4 zu erläutern: Zertifikate sind in Hierarchien geordnet. Auf der untersten Ebene dieser Hierarchien befinden sich die den Benutzern ausgestellten Zertifikate. Diese werden also z. B. zur Signatur von Dokumenten verwendet. Auf dieser Ebene ist es unerwünscht, dass zu ein- und demselben Schlüsselpaar verschiedene Zertifikate bestehen, als einzige Ausnahme wird die Gültigkeitsdauer gesehen. Es wird also z. B. auch bei einer Änderung des Namens des Signators, bei der Aufnahme zusätzlicher Daten in das Zertifikat, bei Änderungen der Codierung etc. für den Signator ein neues Schlüsselpaar erzeugt. Auf höheren Ebenen der Hierarchie wird dies hingegen nicht so gesehen. Diese Zertifikate werden nicht zur Signatur von Dokumenten, sondern nur zur Signatur von Zertifikaten und Widerrufslisten verwendet. Da von den Schlüsselpaaren der höheren Ebenen letztlich die Überprüfbarkeit aller in der Hierarchie darunter angeordneten Zertifikate abhängt, kann dort auch nicht ohne weiteres ein Schlüssel ausgetauscht werden. Es ist auch nicht unüblich, dass für Schlüssel der höheren Ebenen mehrere Zertifikate mit unterschiedlichen Inhalten (z. B. ein selbstsigniertes Zertifikat des Anbieters, ein Cross-Zertifikat eines anderen Anbieters und ein von der Aufsichtsstelle für das Verzeichnis nach § 13 Abs. 3 SigG ausgestelltes Zertifikat) existieren. Hätte man den geltenden § 12 Abs. 4 SigV wörtlich ausgelegt, dann hätte man die meisten Zertifikate auf höheren hierarchischen Ebenen als automatisch kompromittiert ansehen müssen. Dieser Fehler wird durch die Neufassung des § 12 Abs. 4 SigV nun behoben.

§ 14

Wir verweisen auf unsere E-Mail vom 02.07.2004, in welcher wir dem Bundeskanzleramt und dem Bundesministerium für Justiz mitgeteilt haben, dass mehrere Anfragen zu Zeitstempeldiensten an die Aufsichtsstelle

herangetragen wurden und es sich in der Praxis offenbar als ein Problem darstellt, dass laut § 14 Abs. 1 der geltenden SigV für sichere Zeitstempeldienste nur qualifizierte Zertifikate verwendet werden dürfen.

Die RTR-GmbH geht davon aus, dass mit dem Verweis auf das Erfordernis eines qualifizierten Zertifikates vor allem die Anforderungen an Anbieter qualifizierter Zertifikate auf die Anbieter von sicheren Zeitstempeldiensten übernommen werden sollten. Das macht ja auch Sinn, denn der Anbieter eines sicheren Zeitstempeldienstes sollte ja z. B. auch kein vorbestraftes oder sachunkundiges Personal beschäftigen. Wenn sich der Zeitstempeldienstanbieter das qualifizierte Zertifikat aber z. B. von einem Markt bereits tätigen Anbieter ausstellen lässt, dann gelten die Anforderungen an das Personal für ihn nicht.

Aus Sicht der RTR-GmbH wäre es daher sinnvoller, das Erfordernis der Verwendung qualifizierter Zertifikate in § 14 Abs. 1 SigV durch einen Verweis auf jene Bestimmungen der SigV zu ersetzen, die für die Anbieter qualifizierter Zertifikate gelten und die auch für die Erbringer sicherer Zeitstempeldienste gelten sollen, z. B.: „Für die Erbringung sichere Zeitstempeldienste gelten die Anforderungen der §§ ... an die Anbieter, die qualifizierte Zertifikate ausstellen oder sichere elektronische Signaturen anbieten, sinngemäß."

§ 15 und § 18

Wie bereits in unserer E-Mail vom 06.10.2003 regen wir an, im Einleitungssatz des neuen § 15 Abs. 2 durch Einfügung des Wortes „sicheren" vor „Zeitstempeldienst" klarzustellen, dass sich diese Bestimmung nur auf einen sicheren Zeitstempeldienst bezieht. Dies geht zwar bereits aus dem Titel des neuen § 15 hervor, der Wortlaut des § 15 Abs. 2 würde aber irreführend nahe legen, dass alle Anbieter von Zeitstempeldiensten ein so detailliertes Sicherheits- und Zertifizierungskonzept vorlegen müssten.

Weiters wiederholen wir die Anregung aus unserer E-Mail vom 06.10.2003, in den neuen Bestimmungen § 15 Abs. 3 und § 18 Abs. 1 jeweils „XML mit Darstellungsfunktion" durch „XML mit Darstellungstransformation" oder durch „XML mit XSL-Transformation" zu ersetzen, was dem Fachbegriff „XSL Transformations" (vgl. http://www.w3.org/TR/xslt) besser entsprechen würde.

§ 17 – Nachsignieren

In unserer oben bei § 14 erwähnten E-Mail vom 02.07.2004 an das Bundeskanzleramt und das Bundesministerium für Justiz haben wir auch darauf hingewiesen, dass von potenziellen Anbietern sicherer Zeitstempeldienste das Nachsignieren als ein Hauptanwendungsfall gesehen wird. Allerdings sieht § 17 der geltenden SigV vor, dass eine „neue sichere elektronische Signatur" angebracht werden muss, was eher auf einen willentlichen Akt des Nachsignierens samt der Möglichkeit, sich das nachzusignierende Dokument davor gesichert anzeigen zu lassen, hindeutet.

Wir regen daher nochmals an, in § 17 SigV klarzustellen, dass für das Nachsignieren kein neuerlicher willentlicher Akt erforderlich ist, sondern dass

auch ein sicherer Zeitstempel verwendet werden kann. Man könnte z. B. statt „eine neue sichere Signatur“ schreiben: „ein sicherer Zeitstempel oder eine neue sichere Signatur“.

§ 20 – Verlautbarungen

Im neu eingefügten § 20 wird die Aufsichtsstelle verpflichtet, die „in § 9 und in der Fußnote zum Anhang zitierten Unterlagen mit technischem Inhalt“ über ihre Homepage elektronisch abrufbar zu machen.

Die RTR-GmbH geht davon aus, dass mit den „in § 9 ... zitierten Unterlagen“ die Common Criteria und ITSEC sowie die von der Europäischen Kommission nach Art. 3 Abs. 5 der Signaturrichtlinie veröffentlichten Standards (derzeit CWA 14167-1, CWA 14167-2 und CWA 14169) gemeint sind, nicht aber die „von einer Bestätigungsstelle anerkannten“ Schutzprofile oder Security Targets, da es sich bei diesem Anerkennungsakt nicht um einen Rechtsakt, sondern um eine gutachterliche Vorfrage im Zuge der Prüfung und Bescheinigung handelt. Auch Prüfberichte von Evaluatoren oder Bestätigungsstellen sind in der Regel vertraulich zu behandeln und können daher nicht auf der Website der RTR-GmbH veröffentlicht werden. Zu den „in der Fußnote zum Anhang zitierten Unterlagen“ verweisen wir darauf, dass der in Begutachtung übersandte Anhang keine Fußnoten mehr hat.

Die Aufsichtsstelle hat auf ihrer Website bereits jetzt zahlreiche Links veröffentlicht, über welche unter anderem auch alle genannten Unterlagen auffindbar sind (http://www.signatur.rtr.at/de/links/). Wir gehen davon aus, dass auch nach dem neuen § 20 grundsätzlich ein Link auf die jeweiligen Unterlagen ausreichen würde. Die meisten Dokumente stehen zwar auf den Websites der jeweiligen Institutionen frei zum Download zur Verfügung, sind aber urheberrechtlich geschützt, weshalb die RTR-GmbH nicht gewährleisten kann, dass die Rechteinhaber einem direkten Download von der Website der RTR-GmbH zustimmen.

Anhang

Zunächst verweisen wir auf die Ausführungen im allgemeinen Teil unserer Stellungnahme, wo wir vorgeschlagen haben, statt der in Begutachtung gesandten Kurzfassung entweder auf ETSI SR 002 176 zu verweisen oder die vorbereitete Übersetzung dieses Dokumentes als Anhang abzudrucken.

Im Einzelnen enthält der Anhang des Begutachtungsentwurfs folgende Fehler, Ungenauigkeiten und Unvollständigkeiten:

- Der Titel bezieht sich ausschließlich auf die „Signaturerstellungsdaten sicherer elektronischer Signaturen“ umfasst also nicht die Paddingverfahren und die Hashverfahren. Richtiger wäre „Algorithmen und Parameter für sichere elektronische Signaturen“ wie es im BMJ-Entwurf vorgesehen war.

- Die Definition der kryptographischen Hashfunktion ist in mehreren Punkten unpräzise bzw. falsch: die wesentliche Eigenschaft der Kollisionsresistenz ist in der Definition nicht erwähnt. Ebensowenig ist erwähnt, dass bei einer Hashfunktion üblicherweise als wesentlich angesehen ist, dass das Ergebnis eine konstante Länge hat. Die beiden Klammerausdrücke sind eher verwirrend. Zum Vergleich: die Definition in ETSI SR 002 176 lautet übersetzt: „Eine kryptographische Hashfunktion ist eine schwach kollisionsresistente Einweg-Funktion mit einem Ergebnis konstanter Länge."

- In Tabelle 1a wurde in der Zeile 004 als Padding-Verfahren „emsa-pss 2" statt „emsa-pss" eingetragen.

- Tabelle 1b stammt nicht aus Kapitel 4 des Algorithmenpapiers, sondern aus Anhang B dieses Dokuments. Dabei handelt es sich nicht um eine normative, sondern lediglich um eine informative Zusammenstellung von Objektbezeichnern. Im Sinne der Technologieneutralität sollte durch Tabelle 1b nicht der Eindruck erweckt werden, nur diese Objektbezeichner dürften in qualifizierten Zertifikaten bzw. in sicheren elektronischen Signaturen vorkommen. Im Gegenteil: Für einige der zulässigen Algorithmen bzw. Kombinationen von Algorithmen werden in der Tabelle gar keine Objektbezeichner genannt. Aufgrund des nicht normativen Inhalts regt die RTR-GmbH an, Tabelle 1b zu entfernen.

- Mehrere Tabellen enthalten eine Spalte „Datum der Annahme", die ohne die gestrichenen Teile von ETSI SR 002 176 nicht verständlich ist.

- Aus den Tabellen wurden die Verweise auf die jeweiligen normativen Referenzen gestrichen. Es ist fraglich, was der normative Gehalt z. B. der ersten Zeile von Tabelle 2 (die SHA-1 als zulässiges Hashverfahren festlegt) sein soll, wenn die Verweise auf ISO/IEC 10118-3 und FIPS 180-1 gestrichen werden.

- In Punkt 7.1 wurden bei der Beschreibungen der Anforderungen an das RSA-Verfahren wichtige Anforderungen gestrichen, insbesondere dass p und q etwa die selbe Länge aufweisen sollen und dass ausreichend viele Primzahlen zur Auswahl stehen und diese hinreichend gleichverteilt werden sollen. Dass Implementierungen nach dem chinesischen Restsatz zulässig sind, wurde wieder gestrichen.

- In den Abschnitten 7.2.2 und 7.2.4 wird eine Gruppe $E(F_{2m})$ genannt. Diese Notation ist mathematisch falsch, weil eine elliptische Kurve über einem endlichen Körper der Ordnung 2^m (nicht $2m$) gemeint ist. Korrekt müsste die Gruppe mit $E(\mathbf{F}_{2^m})$ oder – typographisch einfacher – mit $E(\mathrm{GF}(2^m))$ bezeichnet werden (GF für Galois Field).

- Überhaupt wurden sämtliche Anforderungen an die Schlüsselerzeugungsverfahren gestrichen, obwohl diese ja einen der wesentlichsten Bestandteile des Anhangs darstellen müssten.

- Auch sämtliche Beschreibungen der Verfahren zur Erzeugung von Zufallszahlen wurden gestrichen. Damit geht der normative Gehalt der Tabelle 6 völlig verloren. Was soll es bedeuten, dass „Trueran“ und „Pseuran“ als zulässige Verfahren festgelegt werden, wenn die Passagen gestrichen wurden, in denen diese Verfahren definiert werden?

Mit freundlichen Grüßen

RTR-GmbH
Rundfunk und Telekom
Regulierungs-GmbH

Dr. Georg Serentschy
Geschäftsführer Fachbereich Telekommunikation