Rundfunk & Telekom Regulierungs-GmbH
RTR

Per E-Mail: i11@bka.gv.at, begutachtungsverfahren@parlament.gv.at

Bundeskanzleramt
Abteilung I/11
zH Herrn Mag. Peter Kustor
Ballhausplatz 2
1014 Wien

A 2/2010-4, ANOR 2/2010-4
UL/JW

Wien, am 08.03.2010

Stellungnahme zum Entwurf eines Bundesgesetzes, mit dem das SigG geändert wird (GZ BKA-410.004/0012-I/11/2010)

Sehr geehrte Damen und Herren!

Die Telekom-Control-Kommission und die Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH) erlauben sich, im Begutachtungsverfahren zum oben genannten Entwurf Stellung zu nehmen.

Die vorgesehene Änderung des § 12 SigG bezweckt, für die Weiterführung von Zertifizierungsdiensten nach Einstellung der Tätigkeit eines Zertifizierungsdiensteanbieters (ZDA) Vorsorge zu treffen. Dieses Vorhaben wird von Telekom-Control-Kommission und RTR-GmbH grundsätzlich unterstützt. Die im Entwurf vorgeschlagenen Maßnahmen werfen in dieser Form jedoch zahlreiche Fragen auf, die die Erreichung des angestrebten Zieles fraglich erscheinen lassen.

Keine Aufsicht bei Ausstellung qualifizierter Zertifikate durch den Bund

Aus dem vorliegenden Entwurf würde sich ein unlösbarer Konflikt zwischen verfassungsrechtlichen und unionsrechtlichen Vorschriften ergeben. **Wie im Folgenden präzisiert wird, sind Anbieter qualifizierter Zertifikate aus unionsrechtlichen Gründen zu beaufsichtigen, wohingegen eine Aufsicht über den Bund als Anbieter qualifizierter Zertifikate aus verfassungsrechtlichen Gründen nicht möglich ist.**

RUNDFUNK UND TELEKOM
REGULIERUNGS-GMBH

A-1060 Wien, Mariahilfer Straße 77-79
Tel: +43 (0) 1 58058 - 0
Fax: +43 (0) 1 58058 - 9191
http://www.rtr.at
e-mail: rtr@rtr.at
FN: 208312t HG Wien
DVR-Nr.: 0956732 Austria
UID-Nr.: ATU43773001

Gemäß Art 3 Abs 3 der Signaturrichtlinie[1] tragen die Mitgliedstaaten dafür Sorge, dass ein geeignetes System zur Überwachung der in ihrem Hoheitsgebiet niedergelassenen ZDA, die öffentlich qualifizierte Zertifikate ausstellen, eingerichtet wird. Implizit bedeutet dies, dass ZDA, die öffentlich qualifizierte Zertifikate ausstellen, zu überwachen sind – und zwar unabhängig davon, ob es sich bei einem ZDA um eine natürliche Person, ein Unternehmen, eine Körperschaft öffentlichen Rechts oder eine sonstige rechtsfähige Einrichtung handelt. Stellt der Bund als Gebietskörperschaft qualifizierte Zertifikate aus, so ist der Bund per definitionem ZDA und hinsichtlich der Ausstellung qualifizierter Zertifikate zu überwachen.

In Österreich ist das System zur Überwachung von ZDA, die qualifizierte Zertifikate ausstellen, durch §§ 13 bis 16 SigG eingerichtet, wobei der Telekom-Control-Kommission als Aufsichtsstelle gemäß § 13 Abs 1 SigG die laufende Aufsicht über die Einhaltung der Bestimmungen des SigG und der auf seiner Grundlage ergangenen Verordnungen obliegt.

In den Erläuterungen zum gegenständlichen Gesetzesentwurf wird dargelegt, dass der Bund vorbereitende Maßnahmen ergreift, um qualifizierte Zertifikate im Fall der Einstellung der Tätigkeit eines ZDA selbst weiterzuführen. Unter Weiterführung von Zertifikaten ist dabei nicht nur die Weiterführung von Verzeichnis- und Widerrufsdiensten, sondern auch die Ausstellung qualifizierter Zertifikate zu verstehen. Dies ergibt sich aus dem ebenfalls zur Begutachtung ausgesandten Entwurf einer Verordnung des Bundeskanzlers, mit der die SigV 2008 geändert wird (GZ BKA-410.004/0011-I/11/2010), denn darin wird die erneute Ausstellung eines qualifizierten Zertifikats im Fall der Weiterführung geregelt.

Da der zu novellierende § 12 SigG vorsieht, dass der Bund (subsidiär) dafür Sorge zu tragen hat, dass die Zertifikate weitergeführt werden, ist nicht auszuschließen, dass der Bund selbst diese Tätigkeit übernimmt. In diesem Fall würde sich daher die Aufsichtstätigkeit der Telekom-Control-Kommission wohl auf den Bundeskanzler beziehen, der gemäß Art 19 B-VG oberstes Organ der Vollziehung ist. Eine derartige Aufsichtstätigkeit ist jedoch unzulässig, weil der Verfassungsgerichtshof mit Erkenntnis VfSlg 13.626/1993 die Betrauung eines (einfachgesetzlich eingerichteten) Verwaltungsorgans mit der nachprüfenden Kontrolle der Rechtmäßigkeit des Verhaltens eines obersten Organs der Vollziehung für verfassungswidrig erklärt hat. Dass die Argumentation des Verfassungsgerichtshofs sinngemäß auch auf die Tätigkeit der Aufsichtsstelle nach SigG anzuwenden ist, hat das Bundeskanzleramt in einem Schreiben an die RTR-GmbH vom 16.05.2003 (GZ 810.200/001-V/3/2003) bestätigt.

---

[1] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl L 13/12 v 19.01.2000.

Kontrolle der Einstellung der Tätigkeit

Die Aufsichtspraxis der vergangenen Jahre hat gezeigt, dass Kontrolle und Aufsichtsmaßnahmen gerade bei der Einstellung der Tätigkeit eines ZDA und bei der Übernahme der Verzeichnis- und Widerrufsdienste durch einen anderen ZDA in besonderem Maße erforderlich sind.

Wenn die Weiterführung der Zertifikate sowie der Verzeichnis- und Widerrufsdienste durch den Bund erfolgt, ist die Telekom-Control-Kommission als Aufsichtsstelle aus den oben dargelegten Gründen nicht mehr ermächtigt, zu kontrollieren, inwieweit der Bund die Pflichten des ZDA bereits übernommen hat und inwieweit der ZDA daher seine Tätigkeit einstellen kann. Eine Kontrolle der Einstellung der Tätigkeit eines ZDA durch die Aufsichtsstelle wäre somit rechtlich nicht möglich.

Unionsrechtskonforme Alternative

Um die gemäß Art 3 Abs 3 der Signaturrichtlinie erforderliche Überwachung zu ermöglichen, regen Telekom-Control-Kommission und RTR-GmbH an, den gegenständlichen Entwurf so abzuändern, dass nicht ein oberstes Organ mit Tätigkeiten eines ZDA betraut werden kann. So könnte etwa das Wort „Bund" durch „Bundesrechenzentrum GmbH" ersetzt werden.

Soweit hierorts bekannt, verfügt die Bundesrechenzentrum GmbH aufgrund ihrer Tätigkeit im Zusammenhang mit dem digitalen Kontrollgerät und dem im Reisepass befindlichen elektronischen Datenträger über umfassende Erfahrung in den Bereichen Sicherheitstechnologie, Kryptographie, elektronische Signatur, Public Key Infrastructure und technische Normen. Die Bundesrechenzentrum GmbH wendet ein Informationssicherheits-Managementsystem entsprechend den Anforderungen der internationalen Norm ISO/IEC 27001:2005 an und ist dafür von der akkreditierten Zertifizierungsorganisation CIS – Certification & Information Security Services GmbH zertifiziert worden. Die Bundesrechenzentrum GmbH verfügt nach Ansicht von Telekom-Control-Kommission und RTR-GmbH über ideale Voraussetzungen für die Ausstellung qualifizierter Zertifikate.

Für die Ermöglichung einer Aufsichtstätigkeit wäre dabei wesentlich, dass die Bundesrechenzentrum GmbH qualifizierte Zertifikate nicht im Namen des Bundes oder des Bundeskanzlers, sondern im eigenen Namen ausstellt und somit selbst eine Tätigkeit als ZDA iSd § 2 Z 10 SigG ausübt.

Mögliche Verzögerung eines unverzüglich erforderlichen Widerrufs

Laut dem vorliegenden Entwurf wird für den Fall, dass ein ZDA seine Tätigkeit einstellt und der Aufsichtsstelle (noch) kein Antrag des Bundeskanzlers vorliegt, offenbar ein öffentliches Interesse an der Weiterführung der Zertifikate unterstellt. Die gültigen Zertifikate dürfen in diesem Fall nicht widerrufen werden.

Dem steht gegenüber, dass gemäß § 9 Abs 1 SigG Zertifikate unter bestimmten Voraussetzungen jedoch unverzüglich zu widerrufen sind. Gemäß § 14 Abs 1 SigG kann der Widerruf oder die Anordnung des Widerrufs von Zertifikaten durch die Aufsichtsstelle erforderlich sein. Die im Entwurf vorgesehene Vorschrift kann also in konkreten Fällen zu § 9 Abs 1 SigG bzw zu § 14 Abs 1 SigG in Konflikt stehen.

Telekom-Control-Kommission und RTR-GmbH regen daher an, die Formulierung in § 12 dritter Satz SigG in der Entwurfsfassung dahingehend zu präzisieren, dass nur ein „Widerruf der gültigen Zertifikate aufgrund der Einstellung der Tätigkeit des ZDA" gemeint ist.

Im Übrigen ergibt sich aus dem Entwurf nicht klar, wie der Bundeskanzler Kenntnis davon erlangen soll, dass ein ZDA bei der Aufsichtsstelle die geplante Einstellung seiner Tätigkeit angezeigt hat.

Anforderungen für die Weiterführung qualifizierter Zertifikate

Telekom-Control-Kommission und RTR-GmbH gehen davon aus, dass der Bund im Fall, dass er öffentlich qualifizierte Zertifikate ausstellt, ZDA iSd § 2 Z 10 SigG ist und somit die Pflichten eines ZDA zu erfüllen hat. Zu diesen gehört auch, dass der Aufsichtsstelle jene Informationen zu übermitteln sind, die zur Führung der Verzeichnisse gemäß § 13 Abs 3 SigG (dazu zählt auch die gemäß Entscheidung der Kommission 2009/767/EG zu veröffentlichende vertrauenswürdige Liste der beaufsichtigten bzw akkreditierten ZDA; idF der Berichtigung ABL L 299/18 v 14.11.2009) erforderlich sind.

Dauer der Weiterführung qualifizierter Zertifikate

Die Signaturrichtlinie zielt offenkundig auf die Bildung eines Marktes für Zertifizierungsdienste ab (konkret ergibt sich dies aus Erwägungsgründen 10 bis 12 sowie Art 3 und 4 der Signaturrichtlinie). Die Bildung eines solchen Marktes wird jedoch beeinträchtigt, wenn als dominierender ZDA eine öffentliche Stelle auftritt, welche die Zertifizierungsdienste im Unterschied zu einem privaten ZDA nicht notwendigerweise kostendeckend erbringen muss.

Telekom-Control-Kommission und RTR-GmbH regen daher an, die Weiterführung im öffentlichen Bereich nur solange zuzulassen, bis sich ein von der Aufsichtsstelle akkreditierter oder überprüfter ZDA zur Weiterführung bereit erklärt.

Mit freundlichen Grüßen

Telekom-Control-Kommission

Dr. Elfriede Solé
Vorsitzende

RTR-GmbH
Rundfunk und Telekom Regulierungs-GmbH

Dr. Georg Serentschy
Geschäftsführer Fachbereich Telekommunikation