A 7/2001-114

Bescheid

Die Telekom-Control-Kommission hat durch Dr. Eckhard Hermann als Vorsitzenden sowie durch Dkfm. Dr. Oskar Grünwald und Dipl.-Ing. Peter Knezu als weitere Mitglieder über den Antrag der Datakom Austria GmbH, Wiedner Hauptstraße 73, 1040 Wien auf Akkreditierung gemäß § 17 SigG in ihrer Sitzung vom 17. Dezember 2001 einstimmig beschlossen:

I. Spruch

1. Die Datakom Austria GmbH wird gemäß § 17 SigG iVm § 18 Abs. 8 SigV hinsichtlich des von ihr erbrachten Zertifizierungsdienstes „a-sign Premium“ akkreditiert.

   Die Datakom Austria GmbH ist berechtigt, sich im Geschäftsverkehr als „Akkreditierter Zertifizierungsdiensteanbieter“ zu bezeichnen und das Bundeswappen mit dem Schriftzug „Akkreditierter Zertifizierungsdienste-anbieter“ zu führen.

   Im Zusammenhang mit Signatur- und Zertifizierungsdiensten sowie mit Signaturprodukten darf diese Bezeichnung nur verwendet werden, soweit sie sich auf den Zertifizierungsdienst „a-sign Premium“ (oder einen zukünftigen anderen Zertifizierungsdienst, bei dem sichere elektronische Signatur-verfahren bereitgestellt werden) bezieht.

2. Die Akkreditierung erfolgt unter den folgenden Auflagen:

   a) Der Zertifizierungsdienst „a-sign Premium“ ist binnen drei Monaten ab Rechtskraft dieses Bescheides öffentlich anzubieten. Die Aufnahme des Zertifizierungsdienstes ist der Aufsichtsstelle anzuzeigen.

   b) Der Aufsichtsstelle sind alle Änderungen des Sicherheits- und Zertifizierungskonzeptes gemäß § 6 Abs. 2 SigG spätestens mit dem Inkrafttreten anzuzeigen. Dazu gehören insbesondere:

      aa) die Aufnahme eines weiteren Zertifizierungsdienstes, bei dem sichere elektronische Signaturverfahren bereitgestellt werden;

bb) eine Änderung des Namens (Firma) oder einer der im Zusammenhang mit den Zertifizierungsdiensten verwendeten Adressen (postalische Adresse, Telefonnummer, E-Mail- oder Internetadresse) des Zertifizierungsdiensteanbieters, eine Änderung der Bezeichnung des Zertifizierungsdienstes oder eine Änderung jener Internetadressen, an denen das Sicherheits- und Zertifizierungskonzept, die Verzeichnisdienste oder die Widerrufsdienste abgerufen werden können;

cc) Änderungen der für den Zertifizierungsdienst verwendeten Signaturprüfdaten;

dd) Änderungen der Codierungen in den ausgestellten Zertifikaten und

ee) Änderungen in der Liste der eingesetzten, bereitgestellten und empfohlenen Signaturprodukte oder in der Liste der anwendbaren Formate für zu signierende Dokumente bzw. anzuwendender Methoden zur Verhinderung dynamischer Veränderungen.

c) Im Rahmen des Zertifizierungsdienstes „a-sign Premium“ ausgestellte Zertifikate dürfen ausschließlich als qualifizierte Zertifikate iSd § 2 Z 9 SigG ausgestellt werden.

d) Im Rahmen des Zertifizierungsdienstes „a-sign Premium“ dürfen Zertifikate ausschließlich an Signatoren ausgestellt werden, die über eine sichere Signaturerstellungseinheit verfügen, welche gemäß § 18 Abs. 5 SigG von einer Bestätigungsstelle oder von einer gemäß § 18 Abs. 5 Satz 3 oder § 24 Abs. 3 SigG gleichzuhaltenden Stelle bescheinigt wurde.

e) Für die Erstellung und Speicherung qualifizierter Zertifikate sind ausschließlich vertrauenswürdige Systeme, Produkte und Verfahren, die vor Veränderungen geschützt sind und für die technische und kryptographische Sicherheit sorgen, zu verwenden (§ 7 Abs. 2 SigG). Sicherheitsrelevante Änderungen im Trustcenter-Netzwerk oder auf den für die Erbringung des Zertifizierungsdiensteanbieters eingesetzten Rechnern, insbesondere Änderungen auf der für die fortgeschrittene Signatur qualifizierter Zertifikate eingesetzten Signaturerstellungseinheit, sind der Aufsichtsstelle anzuzeigen.

f) Gemäß § 6 Abs. 5 SigG hat die Datakom Austria GmbH alle Umstände, die eine ordnungsgemäße und dem Sicherheits- und Zertifizierungskonzept entsprechende Tätigkeit nicht mehr ermöglichen, unverzüglich der Aufsichtsstelle anzuzeigen. Dazu zählen insbesondere:

aa) eine Systemstörung gemäß Punkt 5.1 des „CA Operation Manual“, wenn diese nicht binnen 24 Stunden behoben wurde – insbesondere ein Ausfall des Widerrufsdienstes,

bb) der Eintritt eines Personalnotstandes gemäß Punkt 5.2 des „CA Operation Manual“,

cc) der Verdacht einer Kompromittierung der eingesetzten Signaturerstellungsdaten,

dd) die Audit-Berichte des internen Audits einer „a-sign Premium CA“ gemäß 2.6.6.1 des Dokuments „Sicherheits- und Zertifizierungskonzept für User Zertifikate Premium“, wenn beim Audit Mängel im Betrieb der CA hervorgekommen sind.

g) In wirtschaftlicher Hinsicht hat die Datakom Austria GmbH der Aufsichtsstelle umgehend anzuzeigen:

aa) das Unterschreiten der Mindestkapitalausstattung gemäß § 2 Abs. 1 SigV,

bb) Änderungen im Versicherungsvertrag betreffend die Haftpflichtversicherung gemäß § 2 Abs. 2 SigV, welche den Versicherungsschutz der Datakom Austria GmbH betreffen, sowie der Eintritt von Versicherungsfällen, wenn dadurch die Deckung für das laufende Versicherungsjahr auf weniger als zwei Versicherungsfälle mit einer Mindestversicherungssumme von 1 Million Euro je Versicherungsfall reduziert wird, und

cc) die Eröffnung eines Konkurs- oder Ausgleichsverfahrens über ihr Vermögen sowie die Ablehnung eines sie betreffenden Antrages auf Konkurseröffnung mangels eines zur Kostendeckung voraussichtlich hinreichenden Vermögens.

dd) Alle die Datakom Austria GmbH betreffenden Änderungen der Eintragungen in das Firmenbuch – ausgenommen solche, die lediglich Änderungen der Organe und vertretungsbefugten Personen betreffen – sind binnen 14 Tagen unter Vorlage eines Firmenbuchauszuges anzuzeigen.

ee) Weiters ist jährlich gleichzeitig mit der Vorlage an das Handelsgericht der Jahresabschluss der Datakom Austria GmbH der Aufsichtsstelle zu übermitteln.

h) Die Datakom Austria GmbH hat der Aufsichtsstelle zumindest eine Ansprechperson samt Telefonnummer, Faxnummer und E-Mail-Adresse zu nennen, die bei einem Störfall oder dem Verdacht eines Störfalls der Aufsichtsstelle erste Auskünfte im Sinne des § 16 SigG erteilen kann. Änderungen betreffend die Ansprechperson(en) sind der Aufsichtsstelle ebenfalls bekannt zu geben.

i) Gemäß § 12 SigG hat die Datakom Austria GmbH der Aufsichtsstelle die Einstellung ihrer Tätigkeit unverzüglich anzuzeigen. Dabei ist dafür Sorge zu tragen, dass zumindest die Widerrufsdienste weitergeführt werden.

Wenn die Widerrufsdienste nicht von der Datakom Austria GmbH oder einem anderen Zertifizierungsdiensteanbieter weitergeführt werden, so hat die Datakom Austria GmbH alle Zertifikate zu widerrufen und die Widerrufsliste im Format X.509v2 (siehe RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile) an die Aufsichtsstelle zu

übergeben. Als „Next Update“ (RFC 2459, Punkt 5.1.2.5) ist ein Datum anzugeben, welches nach dem Gültigkeitsende sämtlicher ausgestellter Zertifikate liegt. Die Datakom Austria GmbH hat die Widerrufsliste noch für zumindest einen Monat nach dieser Übergabe an der ursprünglich dafür vorgesehenen Adresse abrufbar zu halten.

j) Hinsichtlich des eingesetzten IBM-Kryptoadapters 4758-23 mit CCA Version 2.40 muss der Aufsichtsstelle bis spätestens 31.05.2002 ein Evaluierungsbericht oder ein Bericht über den Status der Evaluierung (CP/Q++ gemäß FIPS 140-1 bzw. CCA gemäß Common Criteria) vorgelegt werden.

k) Hinsichtlich der angebotenen Viewersoftware ProSIGN Version 2.0 ist bis spätestens 12 Monate nach Aufnahme des Dienstes die Bescheinigung einer Bestätigungsstelle gemäß § 18 Abs. 5 SigG oder die Bescheinigung einer gemäß § 18 Abs. 5 Satz 3 oder § 24 Abs. 3 SigG gleichzuhaltenden Stelle vorzulegen.

   Wenn die Datakom Austria GmbH für einen Zertifizierungsdienst, bei dem sichere elektronische Signaturverfahren angeboten werden, andere Viewer als ProSIGN Version 2.0 einsetzt, dann ist dies der Aufsichtsstelle anzuzeigen und dabei entweder die Bescheinigung einer Bestätigungsstelle gemäß § 18 Abs. 5 SigG oder die Bescheinigung einer gemäß § 18 Abs. 5 Satz 3 oder § 24 Abs. 3 SigG gleichzuhaltenden Stelle oder die Erklärung einer Bestätigungsstelle oder eines allgemein anerkannten Evaluators vorzulegen, aus der sich ergibt, dass eine Evaluierung und Bescheinigung in Auftrag gegeben wurde, dass aus Sicht des Evaluators derzeit keine Umstände vorliegen, die eine erfolgreiche Evaluierung von vornherein ausschließen, und wann (spätestens 12 Monate nach Auslieferung des Produkts) die Evaluierung voraussichtlich abgeschlossen sein wird. Spätestens 12 Monate nach Auslieferung des Produkts ist die Bescheinigung einer Bestätigungsstelle gemäß § 18 Abs. 5 SigG oder die Bescheinigung einer gemäß § 18 Abs. 5 Satz 3 oder § 24 Abs. 3 SigG gleichzuhaltenden Stelle vorzulegen.

l) Bis spätestens 30.06.2002 ist ein den Anforderungen des § 16 SigV entsprechendes elektronisches Dokumentationssystem in Betrieb zu nehmen und die bis dahin angefallene Papierdokumentation ist bis spätestens 30.09.2002 nachzuerfassen. Der Aufsichtsstelle ist darüber zu berichten.

m) Wenn bis zum 31.12.2003 kein für das Nachsignieren geeigneter Zeitstempeldienst am Markt angeboten wird, hat die Datakom Austria GmbH bis spätestens 30.06.2004 einen geeigneten Zeitstempeldienst anzubieten.

n) Vor der Aufnahme des Betriebs von Registrierungsstellen durch andere Rechtsträger ist zwischen der Datakom Austria GmbH und dem anderen Rechtsträger ein entsprechender Vertrag abzuschließen.

3. a) Die Gebühr für die Überprüfung der Datakom Austria GmbH anlässlich der Akkreditierung wird gemäß § 1 Abs. 1 Z 3 SigV mit 6.000 Euro (82.561,80 ATS) bestimmt.

Die Gebühr für die Heranziehung der Bestätigungsstelle „Zentrum für sichere Informationstechnologie – Austria (A-SIT)“ im Akkreditierungsverfahren wird gemäß § 1 Abs. 3 SigV iVm § 76 und § 53a AVG mit 221.718,75 ATS (16.112,93 Euro) bestimmt.

Beide Gebühren enthalten keine Umsatzsteuer.

Diese Gebühren sind binnen 14 Tagen auf das Konto der Rundfunk und Telekom Regulierungs-GmbH, Bank Austria AG, BLZ 20151, Konto-Nr. 696 170 133, zu überweisen.

b) Gemäß § 1 Abs. 4 SigV hat die Datakom Austria GmbH der Aufsichtsstelle jeweils bis zum 15. eines jeden Monats die Anzahl der von ihr ausgestellten qualifizierten Zertifikate bekannt zu geben, die am Monatsersten gültig waren.

4. Der Antrag der Datakom Austria GmbH im Schreiben vom 11.12.2001, die Frist für die Aufnahme des Dienstes (siehe Spruchpunkt 2a) auf sechs Monate zu verlängern, wird abgewiesen.

5. Dem Antrag der Datakom Austria GmbH im Schreiben vom 11.12.2001 hinsichtlich der für Spruchpunkt 2k geplanten Auflage wurde durch eine andere Formulierung in diesem Spruchpunkt teilweise stattgegeben. Im übrigen wird der Antrag abgewiesen.

II. Begründung

[Von der Veröffentlichung des Gangs des Verfahrens, des festgestellten Sachverhaltes und der Beweiswürdigung wurde abgesehen.]

4 Rechtliche Beurteilung

4.1 Akkreditierung

4.1.1 Voraussetzungen und Umfang der Akkreditierung

Gemäß § 17 Abs. 1 SigG sind Zertifizierungsdiensteanbieter, die sichere elektronische Signaturverfahren bereitstellen und der Aufsichtsstelle vor der Aufnahme ihrer Tätigkeit als akkreditierte Zertifizierungsdiensteanbieter die Einhaltung der Anforderungen des SigG und der auf seiner Grundlage ergangenen Verordnungen nachweisen, auf Antrag von der Aufsichtsstelle zu akkreditieren.

Die Datakom Austria GmbH war bereits vor dem Inkrafttreten des Signaturgesetzes (01.01.2000) als Zertifizierungsdiensteanbieter tätig, erbringt aber bislang keine Dienste, bei denen sichere elektronische Signaturverfahren bereitgestellt werden. Im Rahmen des verfahrensgegenständlichen Zertifizierungsdienstes „a-sign Premium“, welcher noch nicht angeboten wird, werden sichere elektronische Signaturverfahren bereitgestellt werden.

Ein Zertifizierungsdiensteanbieter kann unterschiedliche Zertifizierungsdienste anbieten, die unterschiedlichen Anforderungen genügen (vgl. § 3 Abs. 1 SigG, § 12 Abs. 1 SigV und die Feststellungen des Justizausschusses zu § 2 Z 11 SigG – 2065 BlgNR XX. GP, 6). Die gemäß § 17 SigG nachzuweisenden Anforderungen des SigG und der SigV betreffen teilweise den Zertifizierungsdiensteanbieter als solchen (z. B. § 7 Abs. 1 Z 1, 5 und 6 SigG), teilweise nur jene Zertifizierungsdienste, bei denen sichere elektronische Signaturverfahren bereitgestellt werden. Einer Akkreditierung gemäß § 17 SigG steht also nicht entgegen, dass der Zertifizierungsdiensteanbieter neben jenen Zertifizierungsdiensten, auf die sich die Akkreditierung bezieht, auch andere Zertifizierungsdienste anbietet, die diesen Anforderungen nicht genügen.

Ein akkreditierter Zertifizierungsdiensteanbieter, der verschiedene Zertifizierungsdienste unterschiedlicher Qualität anbietet, darf jedoch gemäß § 17 Abs. 1 Satz 3 SigG die ihm verliehene Bezeichnung im Zusammenhang mit Signatur- und Zertifizierungsdiensten sowie mit Signaturprodukten nur verwenden, sofern die Sicherheitsanforderungen nach § 18 SigG erfüllt werden. Die gemäß § 17 SigG iVm § 18 Abs. 8 SigV verliehene Bezeichnung „Akkreditierter Zertifizierungsdiensteanbieter“ sowie das Bundeswappen mit dem Schriftzug „Akkreditierter Zertifizierungsdiensteanbieter“ dürfen also nur in allgemeinem Zusammenhang (auf das Unternehmen bezogen) oder aber in Zusammenhang mit jenen Diensten, auf die sich die Akkreditierung bezieht, verwendet werden.

Akkreditierungsfähig sind gemäß § 17 Abs. 1 SigG Zertifizierungsdiensteanbieter, „die sichere elektronische Signaturverfahren bereitstellen“, die es also ihren Kunden ermöglichen, sichere elektronische Signaturen iSd § 2 Z 3 SigG zu erstellen. Für die Erstellung einer sicheren elektronischen Signatur ist gemäß § 2 Abs. 3 lit. e) SigG insbesondere erforderlich, dass die Signatur auf einem qualifizierten Zertifikat beruht und unter der Verwendung von technischen Komponenten und Verfahren, die den Sicherheitsanforderungen des SigG und der SigV entsprechen erstellt wird.

Die Akkreditierung eines Zertifizierungsdiensteanbieters kann sich also nur auf solche Zertifizierungsdienste beziehen, bei welchen der Zertifizierungsdiensteanbieter den Inhabern sicherer Signaturerstellungseinheiten qualifizierte Zertifikate ausstellt.

Die Datakom Austria GmbH erbringt derzeit keine derartigen Dienste. Der verfahrensgegenständliche Zertifizierungsdienste „a-sign Premium“ wird der erste solche Zertifizierungsdienst sein. Gemäß § 6 SigG steht es der Datakom Austria GmbH frei, darüber hinaus jederzeit weitere Zertifizierungsdienste aufzunehmen – darunter können solche sein, die den Anforderungen an eine Akkreditierung nach § 17 SigG entsprechen (aber sich vom verfahrensgegenständlichen Zertifizierungsdienst „a-sign Premium“ unterscheiden), oder auch solche, die diesen Anforderungen nicht entsprechen.

Der Datakom Austria GmbH war daher die Auflage zu erteilen, die Bezeichnung „Akkreditierter Zertifizierungsdiensteanbieter“ im Zusammenhang mit Signatur- und Zertifizierungsdiensten sowie mit Signaturprodukten nur dann zu verwenden, soweit sie sich auf den Zertifizierungsdienst „a-sign Premium“ (oder einen zukünftigen anderen Zertifizierungsdienst, bei dem sichere elektronische Signaturverfahren bereitgestellt werden) bezieht. (Spruchpunkt 1, 3. Absatz)

4.1.2 Prüfungsmaßstab

Als Prüfungsmaßstab für eine Akkreditierung ist in § 17 SigG vorgesehen, dass die zu akkreditierenden Zertifizierungsdiensteanbieter der Aufsichtsstelle „vor Aufnahme ihrer Tätigkeit als akkreditierte Zertifizierungsdiensteanbieter die Einhaltung der Anforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen“ nachweisen.

Prüfungsmaßstab sind also die Anforderungen des SigG und der SigV. Zu untersuchen ist, inwieweit auch einschlägige technische Normen als Prüfungsmaßstab in Betracht kommen.

Zu nennen wäre dabei insbesondere die auf europäischer Ebene im Rahmen von EESSI (European Electronic Signature Standardization Initiative) erörterte und als ETSI TS 101 456 V1.1.1 (2000-12) veröffentlichte Norm betreffend „Policy requirements for certification authorities issuing qualified certificates“, welche europaweit zu einer Harmonisierung der Anforderungen an die Zertifizierungsdiensteanbieter, welche qualifizierte Zertifikate ausstellen, beitragen soll. Weiters wären auch andere von EESSI erarbeitete Dokumente zu nennen, insbesondere die Security Requirements for Secure Signature-creation Devices (es liegen zwei Varianten vor, nämlich die CEN Workshop Agreements CWA 14168 und CWA 14169).

SigG und SigV nehmen auf solche technischen Normen nur an wenigen Stellen Bezug:

4.1.2.1 § 18 Abs. 6 SigG

§ 18 Abs. 6 SigG idF BGBl I 2000/137 verweist auf Normen, die nach Art. 3 Abs. 5 der Signaturrichtlinie 1999/93/EG von der Europäischen Kommission festgelegt werden. Es sind zwar einige der von EESSI erarbeiteten Normen dafür bestimmt, letztlich in dieser Form beschlossen zu werden (insbesondere eines der beiden genannten CEN Workshop Agreements), aber bislang wurde keine dieser Normen durch die Europäische Kommission festgelegt. (CWA 14168 bzw. CWA 14169 sind aber Sicherheitsprofile nach den Common Criteria und könnten daher nach § 9 Abs. 1 SigV von einer Bestätigungsstelle der Bescheinigung einer sicheren Signaturerstellungseinheit zu Grunde gelegt werden.)

4.1.2.2 § 9 SigV

In § 9 SigV werden für die Prüfung der technischen Komponenten und Verfahren für qualifizierte Zertifikate und sichere elektronische Signaturen verschiedene Kriterien genannt, nämlich die Common Criteria, ITSEC, FIPS 140-1 und BS 7799. Die Formulierungen in § 9 SigV sind aber offen gehalten („sind geeignete und von einer Bestätigungsstelle anerkannte Sicherheitsprofile ... anwendbar“, „kann auch nach den Kriterien ... erfolgen“) und bieten einen breiten Spielraum für die Anwendung geeigneter technischer Normen.

Wie sich aus § 9 Abs. 2 SigV ergibt, handelt es sich bei § 9 SigV nicht nur um eine Bestimmung, welche den § 18 Abs. 5 SigG (Anforderungen an technische Komponenten und Verfahren des Signators) konkretisiert, sondern auch um

eine Konkretisierung des § 7 Abs. 2 SigG (Anforderungen an technische Komponenten und Verfahren des Zertifizierungsdiensteanbieters) und des § 10 SigG (Zeitstempeldienste). § 9 SigV ist daher nicht nur für die Tätigkeit der Bestätigungsstellen bei der Bescheinigung von technischen Komponenten und Verfahren nach § 18 Abs. 5 SigG, sondern auch für die aufsichtsbehördliche Tätigkeit in einem Akkreditierungsverfahren oder bei der Prüfung einer Anzeige nach § 6 Abs. 2 SigG von Bedeutung.

Die in § 9 SigV genannten Kriterien Common Criteria, ITSEC und FIPS 140-1 sind aber weniger für die technische Prüfung eines Gesamtsystems, sondern eher für die Prüfung einzelner technischer Komponenten geeignet. Dies zeigt sich auch in den Erläuterungen des BMJ zum Begutachtungsentwurf der SigV (abgedruckt in Brenn/Posch, SigV (2000) 53ff), in welchem nur auf die Prüfung einzelner technischer Komponenten eingegangen wird. Es ist also nicht das Gesamtsystem eines Zertifizierungsdiensteanbieters z. B. nach ITSEC zu evaluieren, vielmehr kommen die genannten Evaluierungsnormen nur für einzelne Komponenten (insbesondere die Signaturerstellungseinheit des Zertifizierungsdiensteanbieters) in Betracht.

Für die Prüfung technischer Komponenten hat das SigG den Bestätigungsstellen eine besondere Rolle zugewiesen. Die Prüfung technischer Komponenten und Verfahren für die Erzeugung sicherer elektronischer Signaturen (also insbesondere von Komponenten und Verfahren, die beim Signator eingesetzt werden) ist nach § 18 Abs. 5 SigG den Bestätigungsstellen vorbehalten. Die Bestätigungsstellen wurden aber auch für die Beratung der Aufsichtsstelle in technischen Fragen eingerichtet (§ 13 Abs. 5 SigG).

Die Telekom-Control-Kommission hat daher in ihrer Sitzung vom 13.07.2001 beschlossen, sich gemäß § 13 Abs. 5 SigG mit einer Bestätigungsstelle zu beraten und dazu die Bestätigungsstelle „Zentrum für sichere Informationstechnologie – Austria (A-SIT)“ beizuziehen. A-SIT wurde ersucht, ein Gutachten zur Sicherheit und zur Evaluierung der Sicherheit der vom Zertifizierungsdiensteanbieter Datakom Austria GmbH eingesetzten technischen Komponenten und Systeme zu erstellen. Für die technischen Kernkomponenten – insbesondere die Signaturerstellungseinheit der Datakom Austria GmbH – war für die Aufsichtsstelle das Gutachten von A-SIT maßgeblich.

4.1.2.3 Anhang 2 Punkt 5 SigV

In Anhang 2 Punkt 5 SigV („Formate für qualifizierte Zertifikate“) wird auf die Arbeiten von EESSI hingewiesen, Formate und Normen für die Darstellung qualifizierter Zertifikate auszuarbeiten. Diese Arbeiten sind seit Ende 2000 abgeschlossen und resultieren im Wesentlichen in den Normen ETSI TS 101 862 V1.1.1 (2000-12) („Qualified certificate profile“) und ETSI TS 101 456 V1.1.1 (2000-12) „Policy requirements for certification authorities issuing qualified certificates“. Erstere Norm enthält eine Standardisierung der Codierung von qualifizierten Zertifikaten, zweitere Anforderungen an die Policy von Anbietern qualifizierter Zertifikate.

Von Bedeutung ist in diesem Zusammenhang insbesondere, dass in Punkt 5.2 ETSI TS 101 456 zwei Object Identifier festgelegt werden, deren Verwendung in einem Zertifikat (vgl. Punkt 4.2.1 von ETSI TS 101 862) zum Ausdruck bringt, dass das Zertifikat als qualifiziertes Zertifikat ausgestellt wurde (bei Verwendung

des Object Identifiers itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(1456) policy-identifiers(1) qcp-public (2)), oder dass es als qualifiziertes Zertifikat für den Inhaber einer sicheren Signaturerstellungseinheit ausgestellt wurde (bei Verwendung des Object Identifiers: itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(1456) policy-identifiers(1) qcp-public-with-sscd (1)).

Würde die Datakom Austria GmbH einen der beiden Object Identifier in ihren Zertifikaten verwenden, dann brächte sie damit öffentlich zum Ausdruck, dass sie sich an die Anforderungen des Standards ETSI TS 101 456 gebunden fühlt. Das Signaturgesetz ist technologieneutral und verfolgt einen liberalen Regelungsansatz (vgl. § 6 Abs. 1 SigG und die ErläutRV zu § 2 Z 1 SigG). Aus § 6 Abs. 4 SigG ergibt sich aber, dass ein Zertifizierungsdiensteanbieter die im Sicherheits- und im Zertifizierungskonzept dargelegten Angaben (dazu gehört auch die Codierung der Zertifikate, vgl. § 15 Abs. 1 Z 16 SigV) sowohl bei der Aufnahme als auch während der Ausübung seiner Dienste zu erfüllen hat. Würde die Datakom Austria GmbH einen der beiden genannten Object Identifier in ihren Zertifikaten verwenden, dann wäre sie daher auch an den Anforderungen von ETSI TS 101 456 zu messen.

Die Verwendung der von EESSI erarbeiteten ETSI-Standards für die Codierung der Zertifikate ist aber nicht verpflichtend. Dies ergibt sich aus § 12 Abs. 2 SigV: „Als Formate für qualifizierte Zertifikate sind insbesondere die im Anhang 2 Punkt 5 genannten Formate geeignet. Das Gleiche gilt für die Codierungen in qualifizierten Zertifikaten."

Da die Datakom Austria GmbH nicht die in ETSI TS 101 456 und ETSI TS 101 862 festgelegten Object Identifier, sondern selbst festgelegte Object Identifier verwendet (siehe oben 2.3), ist sie auch nicht am Standard ETSI TS 101 456 zu messen.

4.1.2.4 Zusammenfassung

Zusammenfassend ergibt sich für den bei einem Akkreditierungsverfahren maßgeblichen Prüfungsmaßstab, dass die rechtlichen Normen SigG und SigV selbst den Prüfungsmaßstab bilden und technische Normen nur sehr eingeschränkt zur Anwendung kommen.

Der technische Standard ETSI TS 101 456 V1.1.1 (2000-12) käme dann als Prüfungsmaßstab zur Anwendung, wenn der Zertifizierungsdiensteanbieter in seinen Zertifikaten auf einen der in diesem Standard genannten Object Identifier verweisen würde, was im konkreten Fall aber nicht der Fall ist.

Zur Sicherheit und zur Evaluierung der Sicherheit der vom Zertifizierungsdiensteanbieter Datakom Austria GmbH eingesetzten technischen Komponenten und Systeme wurde ein Gutachten der Bestätigungsstelle A-SIT eingeholt.

4.1.3 Bescheinigungen nach § 18 Abs. 5 SigG

Wie oben unter 4.1.1 ausgeführt wurde, ist Voraussetzung der Akkreditierung, dass der Zertifizierungsdiensteanbieter sichere elektronische Signaturverfahren bereitstellt. Die Definition der sicheren elektronischen Signatur in § 2 Z 3 SigG

verweist in ihrer lit. e) auf die Sicherheitsanforderungen des SigG und der SigV und damit insbesondere auf die Anforderung des § 18 Abs. 5 SigG, dass die technischen Komponenten und Verfahren für die Erstellung sicherer elektronischer Signaturen nach dem Stand der Technik hinreichend und laufend geprüft sind und die Erfüllung der Sicherheitsanforderungen von einer Bestätigungsstelle (oder einer gleichwertigen Stelle) bescheinigt sind.

Nicht mehr erforderlich ist hingegen seit der Novelle BGBl I 2000/137, dass die Signaturerstellungseinheit des Zertifizierungsdiensteanbieters bescheinigt ist. Nach der Stammfassung des § 5 Abs. 3 SigG war es erforderlich, dass qualifizierte Zertifikate mit der sicheren elektronischen Signatur des Zertifizierungsdiensteanbieters versehen sind (also mit Hilfe bescheinigter Komponenten erzeugt werden). Seit der Novelle ist nur mehr erforderlich, dass qualifizierte Zertifikate mit einer den Anforderungen des § 2 Z 3 lit. a) bis d) entsprechenden Signatur (also einer sogenannten „fortgeschrittenen elektronischen Signatur", vgl. Art. 2 Z 2 Signaturrichtlinie) versehen sind. Solange der Zertifizierungsdiensteanbieter also (wie im konkreten Fall, siehe 2.3) nicht den Anspruch erhebt, Zertifikate mit seiner sicheren Signatur zu versehen, ist eine Bescheinigung für die Signaturerstellungseinheit des Zertifizierungsdiensteanbieters nicht erforderlich.

4.1.3.1 Anforderungen des § 18 Abs. 5 SigG

Gemäß § 18 Abs. 5 SigG (idF der Novelle BGBl I 2000/137) müssen „die technischen Komponenten und Verfahren für die Erstellung sicherer elektronischer Signaturen" nach dem Stand der Technik hinreichend und laufend geprüft sein. Die Erfüllung der Sicherheitsanforderungen muss von einer Bestätigungsstelle (oder einer gleichwertigen Stelle) bescheinigt sein.

Für die Auslegung dieser Bestimmung ist zunächst der Begriffsumfang der „technischen Komponenten und Verfahren für die Erstellung sicherer elektronischer Signaturen" (im Folgenden: „technische Komponenten") zu klären. Der Begriff der „technischen Komponenten" wird im SigG und in der SigV an verschiedenen Stellen verwendet:

In § 2 Z 3 lit. e) SigG wird die sichere elektronische Signatur unter anderem damit definiert, dass sie mit „technischen Komponenten und Verfahren, die den Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen entsprechen" erstellt wird. Die ersten beiden Sätze des § 18 Abs. 5 SigG lauten: „Die technischen Komponenten und Verfahren für die Erstellung sicherer elektronischer Signaturen müssen nach dem Stand der Technik hinreichend und laufend geprüft sein. Die Erfüllung der Sicherheitsanforderungen nach diesem Bundesgesetz und den auf seiner Grundlage ergangenen Verordnungen muss von einer Bestätigungsstelle (§ 19) bescheinigt sein."

An beiden Stellen besteht eine enge systematische Verknüpfung zwischen dem Begriff „technische Komponenten" und den Sicherheitsanforderungen nach dem SigG und der SigV. Es ist daher davon auszugehen, dass die Begriffe der „technischen Komponenten" in § 2 Z 3 SigG und in § 18 Abs. 5 SigG einander entsprechen und in beiden Fällen durch diesen Begriff alle Sicherheitsanforderungen des SigG und der SigV abgedeckt werden sollen.

Die Abgrenzung zwischen jenen von einem Signator eingesetzten Komponenten, die zu den „technischen Komponenten“ iSd § 18 Abs. 5 SigG zu rechnen sind (und daher der Prüfung und Bescheinigung durch eine Bestätigungsstelle bedürfen) und allen anderen Komponenten (wie z. B. typischerweise der PC-Hardware oder dem Betriebssystem) kann daher durch eine Analyse der Sicherheitsanforderungen des SigG und der SigV getroffen werden.

In derzeit üblichen Konfigurationen bildet eine als „Secure Signature Creation-Device“ (SSCD) im Sinne des Art. 2 Z 6 der Signaturrichtlinie 1999/93/EG geprüfte und bescheinigte Chipkarte das Kernstück der Signaturerstellung. Diese Chipkarte deckt den Großteil der Sicherheitsanforderungen des SigG und der SigV ab. Zu nennen sind weiters die Anforderungen des § 7 Abs. 1 bis 3 SigV. § 7 Abs. 1 SigV richtet Anforderungen an die Hashbildung, die je nach Konfiguration in der Signatursoftware, auf einem eigenen Gerät, auf der Chipkarte oder in einer Kombination dieser Möglichkeiten erfolgt. Für die Erfüllung der Anforderungen des § 7 Abs. 2 SigV an die Anzeige der zu signierenden Daten wird in der Regel Viewersoftware verwendet, die das zu signierende Dokument am normalen Computerbildschirm darstellt. Denkbar wäre auch eine Darstellung auf einem eigenen Display. Weiters benötigt der Signator eine Software oder Hardware, mittels der er den Signaturvorgang auslöst (§ 7 Abs. 3 SigV). Dies wird in der Praxis durch PIN-Eingabe realisiert, wobei die PIN-Eingabe entweder über die normale Tastatur (in Verbindung mit entsprechender Software) oder auf Chipkartenlesern mit integrierter Tastatur erfolgt.

Aus den Erläuterungen der Regierungsvorlage zu § 18 SigG ergibt sich, dass der Gesetzgeber davon ausging, dass sowohl die PIN-Eingabe als auch die Viewersoftware zu den „technischen Komponenten“ iSd § 18 SigG gehören. Für den Viewer legt dies auch § 18 Abs. 2 SigG nahe, demzufolge die „technischen Komponenten“ die Darstellung der zu signierenden Daten „ermöglichen müssen“, weiters § 23 Abs. 2 SigG, demzufolge der Zertifizierungsdienste-anbieter, der sichere Signaturverfahren bereitstellt, auch dafür haftet, dass „für die von ihm bereitgestellten oder als geeignet bezeichneten Produkte, Verfahren und sonstigen Mittel für die Erstellung elektronischer Signaturen sowie für die Darstellung zu signierender Daten nur technische Komponenten und Verfahren nach § 18 verwendet werden“.

Zusammengefasst ergibt sich, dass bei den derzeit üblichen technischen Realisierungen neben der Chipkarte auch die Komponenten der Hashbildung und der PIN-Eingabe und die Viewer-Software zu den „technischen Komponenten“ iSd § 18 Abs. 5 SigG gehören, also der Prüfung (Evaluierung) und Bescheinigung durch eine Bestätigungsstelle bedürfen.

Die Aufsichtsstelle geht davon aus, dass sich bei getrennter Bescheinigung verschiedener solcher Komponenten aus den in den Bescheinigungen enthaltenen Angaben (§ 9 Abs. 3 SigV) ergeben muss, mit welchen anderen Komponenten und unter welchen Bedingungen die Komponenten kombiniert werden können. (Beispielsweise wird in der Bescheinigung von Viewer-Komponenten typischerweise angeführt werden, mit welchen Komponenten für die PIN-Eingabe und mit welchen Chipkarten der Viewer eingesetzt werden kann und ob ein sicherheitsgeprüfter Chipkartenleser eingesetzt werden muss.)

Wenn sich die Sicherheit der kombiniert eingesetzten Komponenten nicht aus den jeweiligen Bescheinigungen ergibt, dann müsste für die Kombination eine eigene Bescheinigung gemäß § 18 Abs. 5 SigG vorliegen.

4.1.3.2 Secure Viewer

Der Aufsichtsstelle ist bekannt, dass die Erfüllung der Anforderungen des § 18 Abs. 5 SigG in einem Punkt problematisch ist, weil auf dem Markt noch keine geeigneten Produkte zur Verfügung stehen – nämlich im Hinblick auf die Anforderungen des § 7 Abs. 2 SigV an Secure Viewer.

Die Aufsichtsstelle geht aber davon aus, dass die Bestimmung des § 14 Abs. 6 SigG (derzufolge von der Untersagung der Tätigkeit eines Zertifizierungsdiensteanbieters abzusehen ist, wenn die Anordnung gelinderer Mittel ausreicht) sinngemäß auch im Akkreditierungsverfahren gemäß § 17 SigG anzuwenden ist (siehe dazu ausführlicher unten unter 4.1.4). Im Hinblick darauf, dass zwar relativ einfach plausibel gemacht werden kann, dass ein Produkt die Anforderungen des § 7 Abs. 2 SigV erfüllt, dass es aber im günstigsten Fall einige Monate dauert, bis eine Prüfung nach § 9 SigV erfolgt ist und eine Bescheinigung nach § 18 Abs. 5 SigG ausgestellt wurde, wäre es unbillig, einem Akkreditierungswerber die Akkreditierung zu verweigern, wenn ein Produkt zwar augenscheinlich die Anforderungen erfüllt, dies aber noch nicht nach den in § 9 SigV vorgesehenen Kriterien überprüft wurde.

Ähnliches gilt für die Anforderungen nach § 7 Abs. 1 und 3 SigV (Hashberechnung und PIN-Eingabe). Für diese gibt es zwar am Markt bereits bescheinigte Produkte, allerdings werden die Anforderungen in der Praxis häufig durch die selbe Software abgedeckt, welche auch die Darstellung der zu signierenden Daten (§ 7 Abs. 2 SigV) besorgt. Es wäre unverhältnismäßig, den Hersteller einer solchen Software dazu zu zwingen, aufwändig ein bereits bescheinigtes Produkt für die Hashberechnung und die PIN-Eingabe zu integrieren, wenn sein Produkt diese Anforderungen bereits augenscheinlich erfüllt, aber noch nicht bescheinigt ist.

Die Aufsichtsstelle ist daher der Ansicht, dass eine Akkreditierung auch dann auszusprechen ist, wenn eine technische Komponente, welche die Anforderungen des § 7 Abs. 1 bis 3 SigV abdeckt,

a) bereits in auslieferbarer Form vorhanden ist,

b) eine Evaluierung und Bescheinigung bereits in Auftrag gegeben wurde und

c) der Aufsichtsstelle eine Erklärung einer Bestätigungsstelle oder eines allgemein anerkannten Evaluators vorliegt, aus der sich ergibt, dass eine Evaluierung und Bescheinigung in Auftrag gegeben wurde, dass aus Sicht des Evaluators derzeit keine Umstände vorliegen, die eine erfolgreiche Evaluierung von vornherein ausschließen, und wann die Evaluierung voraussichtlich abgeschlossen sein wird – spätestens 12 Monate nach Auslieferung des Produkts.

Zur Erfüllung dieser Anforderungen durch die Datakom Austria GmbH siehe unten 4.1.5.13, zur entsprechenden Auflage in Spruchpunkt 2k des Bescheides siehe unten 4.2.2.10.

4.1.4 Auflagen zur Mängelbehebung

Es ist zu untersuchen, inwieweit die Aufsichtsstelle im Falle, dass in einem Akkreditierungsverfahren Mängel hervorkommen, den Antrag auf Akkreditierung abzuweisen bzw. zurückzuweisen hat und in welchen Fällen dennoch eine Akkreditierung – allenfalls unter Auflagen zur späteren Mängelbehebung – auszusprechen ist.

Grundsätzlich haben Akkreditierungswerber nach § 17 SigG der Aufsichtsstelle die Einhaltung der Anforderungen des SigG und der SigV „vor der Aufnahme ihrer Tätigkeit“ nachzuweisen.

Zu beachten ist aber auch, dass § 6 Abs. 1 SigG den Grundsatz eines freien Marktzutrittes ohne gesonderte Genehmigung vorsieht. Gemäß § 14 Abs. 2 SigG hat die Aufsichtsstelle einem Zertifizierungsdiensteanbieter, der in diesem Sinne die Tätigkeit aufgenommen hat, unter bestimmten Umständen die Tätigkeit zu untersagen. Gemäß § 14 Abs. 6 SigG ist aber von einer Untersagung der Tätigkeit abzusehen, soweit die Anordnung gelinderer Mittel ausreicht, um die Einhaltung der Bestimmungen des SigG und der SigV sicherzustellen. § 14 Abs. 6 SigG nennt insbesondere Auflagen und die Androhung von Maßnahmen unter Setzung einer angemessenen Frist zur Behebung aufgezeigter Mängel.

Die Aufsichtsstelle ist der Ansicht, dass § 14 Abs. 6 SigG auch im Akkreditierungsverfahren sinngemäß anzuwenden ist und daher ein Antrag auf Akkreditierung nicht abgewiesen werden darf, wenn die Einhaltung der Bestimmungen des SigG und der SigV auch durch gelindere Maßnahmen – insbesondere durch Auflagen sichergestellt werden kann.

Die noch bestehenden Mängel und die daraus resultierenden Auflagen werden im Folgenden unter Punkt 4.1.5 und 4.2.2 näher erörtert.

4.1.5 Einzelne Anforderungen

4.1.5.1 Zertifikatsinhalt (§ 5 SigG, § 12 Abs. 2 SigV)

Die von der Datakom Austria GmbH ausgestellten Zertifikate enthalten die von § 5 Abs. 1 SigG geforderten Angaben (siehe oben 2.3).

Das Format bzw. die Codierung der Zertifikate folgt nicht dem Standard ETSI TS 101 862 V1.1.1 (2000-12). Vielmehr wird ein selbst definiertes Format verwendet.

§ 12 Abs. 2 SigV verlangt nicht, dass qualifizierte Zertifikate nach einem bestimmten Standard codiert sind, sondern verweist nur darauf, dass die Formate aus Anhang 2 Punkt 5 der SigV „geeignet sind“. (Anhang 2 Punkt 5 SigV verweist auf die Normierung durch EESSI, welche inzwischen durch den ETSI TS 101 862 V1.1.1 (2000-12) abgeschlossen wurde.) Es handelt sich hier also nur um eine Empfehlung.

Verbindlich ist aufgrund von Anhang 2 Punkt 5 SigV hingegen, dass die detaillierte Ausprägung des Formates im Sicherheits- und Zertifizierungskonzept

dargestellt wird und zur Beschreibung eine formale Notation (z. B. ASN.1) verwendet wird. Eine Codierung in ASN.1 wurde der Aufsichtsstelle vorgelegt.

4.1.5.2 Zuverlässigkeit des Zertifizierungsdiensteanbieters (§ 7 Abs. 1 Z 1 SigG)

Im Verfahren sind keine Zweifel an der von § 7 Abs. 1 Z 1 SigG geforderten Zuverlässigkeit des Zertifizierungsdiensteanbieters hervorgekommen (siehe 2.4). – Zur Zuverlässigkeit des Personals siehe unten 4.1.5.6.

4.1.5.3 Verzeichnisdienst und Widerrufsdienst (§ 7 Abs. 1 Z 2 SigG, § 9 SigG, § 13 SigV)

§ 7 Abs. 1 Z 2 SigG: Aus dem oben unter 2.5 Festgestellten ergibt sich, dass der Betrieb eines schnellen und sicheren Verzeichnisdienstes und eines unverzüglichen und sicheren Widerrufsdienstes sichergestellt ist.

§ 9 SigV: Die Signatur der Widerrufslisten erfolgt durch die selbe Signaturerstellungseinheit und die selben Signaturerstellungsdaten wie die Signatur der qualifizierten Zertifikate, weshalb eine separate Überprüfung der Sicherheit der dafür verwendeten Signaturerstellungseinheiten und ihrer Evaluierung unterbleiben konnte.

§ 13 Abs. 1 SigV: Die von der Datakom Austria GmbH für die Verzeichnisdienste und Widerrufsdienste verwendeten Formate sind spezifiziert. Für die Widerrufslisten liegt eine Spezifikation in ASN.1 vor. Die Zertifikate und Widerrufslisten sind mittels HTTP, HTTPS, LDAP und LDAP-SSL abrufbar. Eine Abfrage mittels OCSP ist nicht möglich, ist durch die SigV aber auch nicht gefordert.

Die Möglichkeit der Weiterführung der Widerrufsdienste durch die Aufsichtsstelle ist durch die Auflage in Spruchpunkt 2i (vgl. unten 4.2.2.8) sicher gestellt.

§ 13 Abs. 2 SigV: Es besteht eine jederzeitige telefonische Widerrufsmöglichkeit und eine persönliche Widerrufsmöglichkeit zu den Geschäftszeiten (siehe oben 2.5). Die Geschäftszeiten entsprechen nicht den in § 13 Abs. 4 SigV genannten Geschäftszeiten, dies ist aber in diesem Zusammenhang nicht von Belang, da die Geschäftszeiten des § 13 Abs. 4 SigV nur für die Aktualisierung der Widerrufsdienste, nicht für die Entgegennahme der Widerrufe gelten. – Für den Widerruf ist ein Authentifizierungsverfahren vorgesehen (siehe oben 2.5).

§ 13 Abs. 3 SigV: Der Schutz der Verzeichnis- und Widerrufsdienste ergibt sich aus den unter 2.12 und 2.13 dargestellten Sicherheitsmaßnahmen. Sperren sind nicht vorgesehen, Widerrufe können nicht rückgängig gemacht werden (siehe oben 2.5).

§ 13 Abs. 4 SigV: Die Aktualisierung der Widerrufsdienste erfolgt nicht nur während der Geschäftszeiten, sondern rund um die Uhr alle 5 Minuten. Der Anforderung, außerhalb der Geschäftszeiten „jedenfalls“ dafür Sorge zu tragen, dass ein Verlangen auf Widerruf automatisiert entgegengenommen wird, wird dadurch Rechnung getragen, dass rund um die Uhr ein telefonischer Widerruf möglich ist.

§ 13 Abs. 5 SigV: Sowohl Widerrufsdienste als auch Verzeichnisdienste sind rund um die Uhr verfügbar. Für Wartungs- und Ausfallssituationen des Widerrufsdienstes ist ein Ersatzsystem vorhanden.

Das Ersatzsystem befindet sich in den selben Räumlichkeiten wie das Hauptsystem. Aus § 13 Abs. 5 SigG ergibt sich aber keine Notwendigkeit, einen katastrophensicheren Widerrufsdienst durch Betrieb von zwei räumlich entsprechend weit getrennten Systemen sicherzustellen. Vielmehr verlangt § 13 Abs. 5 SigG nur für „Wartungs- und Ausfallssituationen" ein Ersatzsystem, also für übliche Problemfälle. Für einen längeren Ausfall ist in § 13 Abs. 5 SigG eine Anzeigepflicht an die Aufsichtsstelle vorgesehen (vgl. auch die Auflage in Spruchpunkt 2f Unterpunkt aa).

§ 13 Abs. 7 SigV: Sperren sind nicht vorgesehen.

4.1.5.4 Zeitangaben (§ 7 Abs. 1 Z 3 SigG)

Dass in Zertifikaten und Widerrufslisten qualitätsgesicherte Zeitangaben verwendet werden, ergibt sich aus 2.6. Seit der Novelle BGBl I 2000/137 sieht § 7 Abs. 1 Z 3 SigG keine Gleichsetzung „qualitätsgesicherte Zeitangaben (Zeitstempel)" vor, sondern „qualitätsgesicherte Zeitangaben ‚(zB sichere Zeitstempel)'". Die Anforderungen an qualitätsgesicherte Zeitangaben sind daher jedenfalls erfüllt, wenn auch die Anforderungen an sichere Zeitstempel (§ 14 SigV) erfüllt sind. Die Abweichung von der tatsächlichen Zeit darf bei diesen höchstens eine Minute betragen.

Die Genauigkeit der eingesetzten GPS-Funkuhr befindet sich in der Größenordnung von Millisekunden. Durch automatische und manuelle Prüfroutinen wird sichergestellt, dass der Systemadministrator alarmiert wird, wenn Zeitabweichungen von mehr als 20 Sekunden auftreten.

Die verwendete Zeitzone wird in den Zertifikaten und Widerrufslisten angegeben.

Zeitstempeldienste werden von der Datakom Austria GmbH derzeit nicht angeboten, sind aber für 2002 geplant. Das Angebot von Zeitstempeldiensten ist auch nicht verpflichtend, solange es nicht für das Nachsignieren benötigt wird (siehe 4.2.2.12).

4.1.5.5 Identitätsprüfung (§ 7 Abs. 1 Z 4 SigG, § 8 SigG, § 11 SigV)

§ 8 Abs. 1 SigG: Vor der Ausstellung eines qualifizierten Zertifikates erfolgt eine Überprüfung anhand eines amtlichen Lichtbildausweises (siehe oben 2.7).

§ 8 Abs. 2 SigG: Die Datakom Austria GmbH wird sich für den Betrieb von Registrierungsstellen (zunächst) der Österreichischen Post AG bedienen. Diese wird also gemäß § 8 Abs. 2 SigG im Auftrag der Datakom Austria GmbH tätig werden, um Verlangen auf Ausstellung eines qualifizierten Zertifikates entgegenzunehmen, die Identität zu prüfen und die nötigen Tätigkeiten zur Erzeugung von Signaturerstellungsdaten auf der Chipkarte und die Ausstellung des Zertifikates vorzunehmen.

Zwischen der Datakom Austria GmbH und der Österreichischen Post AG muss noch ein entsprechender Vertrag abgeschlossen werden (siehe unten 4.2.2.13 zu Spruchpunkt 2n).

§ 8 Abs. 3 SigG: Die Aufnahme von Angaben über die Vertretungsmacht oder andere rechtlich erhebliche Eigenschaften in das qualifizierte Zertifikat ist nicht vorgesehen (siehe oben 2.3).

§ 8 Abs. 4 SigG: Pseudonyme werden nicht unterstützt (siehe oben 2.3).

§ 11 Abs. 1 SigV: Der Antrag auf Ausstellung eines qualifizierten Zertifikates muss vom Zertifikatswerber eigenhändig unterschrieben sein. Vom vorgelegten Lichtbildausweis wird eine Ablichtung hergestellt und zur Dokumentation genommen. Anträge sicher elektronisch zu signieren ist noch nicht vorgesehen (siehe oben 2.7).

Der Umfang der dokumentierten Daten entspricht § 11 Abs. 2 SigV.

§ 11 Abs. 3 SigV: Die Aufnahme von Angaben über die Vertretungsmacht oder andere rechtlich erhebliche Eigenschaften in das qualifizierte Zertifikat ist nicht vorgesehen.

4.1.5.6 Personal und Management (§ 7 Abs. 1 Z 5 SigG, § 10 Abs. 4 und 5 SigV)

Gemäß § 7 Abs. 1 Z 5 SigG muss ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, zuverlässiges Personal mit den für die bereitgestellten Dienste erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen, insbesondere mit Managementfähigkeiten sowie mit Kenntnissen der Technologie elektronischer Signaturen und angemessener Sicherheitsverfahren, beschäftigen und geeignete Verwaltungs- und Managementverfahren einhalten, die anerkannten Normen entsprechen.

Die Anforderungen an die Fachkenntnisse, Erfahrungen und Qualifikationen sind in § 10 Abs. 5 SigV näher ausgeführt (siehe gleich unten).

Hinsichtlich der Verwaltungs- und Managementverfahren verfügt die Datakom Austria GmbH über ein detailliertes Sicherheits- und Zertifizierungskonzept, welches insbesondere im Rollenkonzept des CA Operation Manual die Aufgabenverteilung und Verantwortung unter Berücksichtigung exakt definierter Unvereinbarkeiten beschreibt.

§ 10 Abs. 4 SigV: Für das Personal, welches Zutritt zum Trustcenterbereich hat, wurden der Aufsichtsstelle Strafregisterauszüge vorgelegt, die durchwegs keine Verurteilungen aufweisen und nicht älter als zwei Jahre sind. Von den LRA-Operatoren werden vor Betriebsaufnahme Strafregisterauszüge eingeholt werden (siehe oben 2.8).

§ 10 Abs. 5 SigV erfordert für das Fachwissen des technischen Personals entweder eine mindestens einjährige einschlägige Ausbildung an anerkannten Bildungseinrichtungen (genannt sind HTLs, Fachhochschulen und einschlägige Studien) oder durch eine mindestens dreijährige fachlich einschlägige Tätigkeit. Aus den Erhebungen (siehe oben 2.8) ergab sich, dass das technische

Personal den im Rollenmodell vorgesehenen Aufgaben entsprechend ausgebildet ist, dass bei Abwesenheit einzelner Mitarbeiter deren Aufgaben durch andere entsprechend ausgebildete Personen wahrgenommen werden können und dass dort, wo für besondere Aufgaben spezialisiertes Personal von Lieferanten in Anspruch genommen wird, die Leistungen dieses Fremdpersonals sachkundig überwacht und abgenommen werden können.

4.1.5.7 Finanzmittel und Versicherung (§ 7 Abs. 1 Z 6 SigG, § 2 SigV)

Gemäß § 7 Abs. 1 Z 6 SigG muss ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, über ausreichende Finanzmittel verfügen, um den Anforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen zu entsprechen, weiters muss er Vorsorge für die Befriedigung von Schadenersatzansprüchen, etwa durch Eingehen einer Haftpflichtversicherung, treffen. § 2 SigV führt diese Anforderungen näher aus.

Gemäß § 2 Abs. 1 SigV muss ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, über ein Mindestkapital (Eigenmittel im Sinn des § 224 Abs. 3A und B HGB) in Höhe von 300.000 Euro verfügen. Die Eigenmittel der Datakom Austria GmbH betrugen am 31.12.2000 71.399.256,38 Euro, davon entfielen auf das Stammkapital 14.534.566,83 Euro. Die erforderliche Kapitalausstattung ist also gegeben. Auch die weitere Überprüfung der Finanzlage der Antragstellerin (siehe oben 2.9) hat keine Anhaltspunkte dafür gegeben, dass den Anforderungen des § 7 Abs. 1 Z 6 SigV nicht entsprochen wäre.

Betreffend die Anforderungen an die von § 2 Abs. 2 SigV geforderte Haftpflichtversicherung mit einer Mindestversicherungssumme von 1.000.000 Euro je Versicherungsfall (wobei der Wortlaut des § 2 Abs. 2 SigV keine Möglichkeit der Beschränkung der Anzahl der Versicherungsfälle pro Jahr vorsieht) ist bei der Aufsichtsstelle amtsbekannt, dass eine solche Versicherung auf dem Markt nicht erhältlich ist. Die Versicherungsunternehmen bieten Haftpflichtversicherungen für Zertifizierungsdiensteanbieter nur mit einer Beschränkung der Anzahl der Versicherungsfälle pro Jahr an. Die Datakom Austria GmbH hat der Aufsichtsstelle nachgewiesen, dass die Konzernmutter Telekom Austria AG eine Haftpflichtversicherung abgeschlossen hat, durch welche auch die Datakom Austria GmbH versichert ist und ein Risiko von drei Versicherungsfällen pro Versicherungsjahr mit jeweils 1 Mio. Euro bedeckt ist (wobei eine Klausel des Vertrages sicherstellt, dass der Versicherungsschutz für die Tätigkeit als Zertifizierungsdiensteanbieter auch dann gegeben ist, wenn die maximale Deckungssumme der Haftpflichtversicherung durch andere Versicherungsfälle im Konzern bereits erschöpft wäre).

Die Aufsichtsstelle hält es zwar für denkbar, dass durch einen Versicherungsfall in rascher Folge viele Schadensfälle eintreten und eine größere Zahl von Personen geschädigt wird). Dass es aber in rascher Folge mehrere Versicherungsfälle gibt, bei denen die Schäden auf unterschiedlichen Ursachen zurückzuführen ist, ist im Hinblick auf die strengen Sicherheitsanforderungen bei Anbietern qualifizierter Zertifikate sehr unwahrscheinlich. Die Aufsichtsstelle ist daher der Ansicht, dass durch die von der Datakom Austria GmbH nachgewiesene Haftpflichtversicherung in Verbindung mit der Auflage in Spruchpunkt 2 g) bb) (siehe unten 4.2.2.6) ein ausreichender Schutz gegeben ist. Sollte der Versicherungsschutz durch den Eintritt von Versicherungsfällen zu

stark geschmälert werden, dann müsste die Datakom Austria GmbH für eine Erweiterung des Versicherungsschutzes Sorge tragen (§ 7 Abs. 6 SigG) und der Aufsichtsstelle aufgrund der Auflage in Spruchpunkt 2 g) bb) den Umstand der verringerten Deckung anzeigen, sodass die Aufsichtsstelle notfalls Aufsichtsmaßnahmen ergreifen könnte.

4.1.5.8 Dokumentation (§ 7 Abs. 1 Z 7 SigG, § 11 SigG, § 16 SigV)

Wie sich aus 2.10 ergibt, haben die Überprüfungen gezeigt, dass die Datakom Austria GmbH alle maßgeblichen Umstände über ein verwendetes Zertifikat aufzeichnet, sodass insbesondere in gerichtlichen Verfahren die Zertifizierung nachgewiesen werden kann (§ 7 Abs. 1 Z 7 SigG).

Die Dokumentation umfasst die Sicherheitsmaßnahmen (dieser Teil der Dokumentation wurde auch der Aufsichtsstelle im Verfahren vorgelegt), das Ausstellen und den Widerruf von Zertifikaten (eine Sperre wird von der Datakom Austria GmbH nicht durchgeführt). (§ 11 Abs. 1 SigG).

Das Dokumentationssystem ist noch nicht in elektronischer Form geführt (siehe 2.10), obwohl § 16 SigV dies vorschreibt. Die Aufsichtsstelle ist dennoch der Ansicht, dass es sich dabei um einen Mangel handelt, aufgrund dem der Antrag auf Akkreditierung nicht abgewiesen werden darf (siehe oben 4.1.4). Das elektronische Dokumentationssystem im Sinne des § 16 SigV ist vor allem für den schnellen Zugriff auf eine große Datenmenge, die Möglichkeit der katastrophensicheren Archivierung durch externe Lagerung von Backups und für die Sicherstellung der Möglichkeit der leichten Übergabe der Dokumentation im Falle der Einstellung der Tätigkeit von Bedeutung.

In der Anfangsphase der Tätigkeit eines Zertifizierungsdiensteanbieters als Anbieter qualifizierter Zertifikate gibt es nur eine relativ kleine Datenmenge. Die baldige Einstellung der Tätigkeit ist zudem nicht zu erwarten. Die Aufsichtsstelle ist daher der Ansicht, dass es vorerst genügt, die Daten in Papierform zu erfassen. Es war aber die Auflage zu erteilen, diesen Mangel zu beheben (Spruchpunkt 2l, siehe unten 4.2.2.11).

4.1.5.9 Signaturerstellungsdaten der Signatoren (§ 7 Abs. 1 Z 8 SigG, § 3 SigV, § 4 SigV)

§ 7 Abs. 1 Z 8 SigG: Dass die Signaturerstellungsdaten weder vom Zertifizierungsdiensteanbieter selbst noch von Dritten gespeichert oder kopiert werden können, ergibt sich daraus, dass die Signaturerstellungsdaten erst bei der Ausfolgung der Chipkarte an den Signator erzeugt werden und es sich um eine entsprechend evaluierte und bescheinigte Chipkarte handelt (siehe 2.11).

Auch die Anforderungen der §§ 3 und 4 SigV werden durch die Evaluierung und Bescheinigung der Chipkarte abgedeckt (siehe 2.11).

4.1.5.10 Technische Komponenten des Zertifizierungsdiensteanbieters (§ 7 Abs. 2 SigG, § 6 SigV, § 9 SigV, § 10 Abs. 1 bis 2 und 6 SigV, § 12 Abs. 1 SigV)

Die Telekom-Control-Kommission hat in ihrer Sitzung vom 13.07.2001 beschlossen, sich im gegenständlichen Verfahren gemäß § 13 Abs. 5 SigG mit

einer Bestätigungsstelle zu beraten und dazu die Bestätigungsstelle „Zentrum für sichere Informationstechnologie – Austria (A-SIT)“ beizuziehen. A-SIT wurde ersucht, ein Gutachten zur Sicherheit und zur Evaluierung der Sicherheit der vom Zertifizierungsdiensteanbieter Datakom Austria GmbH eingesetzten technischen Komponenten und Systeme zu erstellen.

Das Gutachten (ON 90) und die ergänzende gutachterliche Stellungnahme (ON 104) ergaben, dass nach eingehender Untersuchung der von der Datakom Austria GmbH eingesetzten technischen Komponenten und Systeme durch die Bestätigungsstelle A-SIT keine Sicherheitsmängel hervorgekommen sind (vgl. im Einzelnen die Feststellungen oben in 2.12). Die Bestätigungsstelle A-SIT hat sich dabei insbesondere mit dem Kryptoadapter IBM 4758-023 und dem Status der Evaluierung des Kryptoadapters befasst.

Die einzige von A-SIT vorgeschlagene Auflage besteht darin, dass bis spätestens 31.05.2002 ein Evaluierungsbericht oder ein Bericht über den Status der Evaluierung des Kryptoadapters IBM 4758-023 (CP/Q++ gemäß FIPS 140-1 bzw. CCA gemäß den Common Criteria) nachgereicht wird.

Konkret hält die Bestätigungsstelle A-SIT in ihrer ergänzenden gutachterlichen Stellungnahme fest:

„Die Vorkehrungen, um die Signaturerstellungsdaten des Zertifizierungsdiensteanbieters geheim zu halten und vor unbefugtem Zugriff zu schützen, sind ausreichend, falls die [oben genannte] Auflage zusätzlich erfüllt wird.“ (Punkt 4.1) und „Die Systeme, Produkte und Verfahren, die für die Signatur- und Zertifizierungsdienste sowie für die Erstellung und Speicherung von Zertifikaten verwendet werden, sind vertrauenswürdig, werden vor Veränderungen geschützt und sorgen für die technische und kryptographische Sicherheit, sofern die [oben genannte] Auflage ... zusätzlich erfüllt wird.“ (Punkt 4.7)

Die Anforderungen des § 7 Abs. 2 SigG sind daher erfüllt, allerdings war die von A-SIT vorgeschlagene Auflage vorzuschreiben (Spruchpunkt 2j, 4.2.2.9).

Wie bereits oben unter 4.1.3 ausgeführt wurde, ist seit der Novelle BGBl I 2000/137 nicht mehr erforderlich, dass qualifizierte Zertifikate mit der sicheren elektronischen Signatur des Zertifizierungsdiensteanbieters versehen werden (also mit Hilfe bescheinigter Komponenten erzeugt werden). Die Aufsichtsstelle benötigt zur Beurteilung der Sicherheit der Signaturerstellungseinheit des Zertifizierungsdiensteanbieters daher keine formelle Bescheinigung nach § 18 Abs. 5 SigG, sondern kann sich (insbesondere hinsichtlich der Anforderungen des § 7 Abs. 2 SigG und des § 9 SigV) auch auf das vorliegende Gutachten der Bestätigungsstelle A-SIT stützen.

§ 6 Abs. 1 SigV: Die eingesetzten Systeme sind dokumentiert (siehe oben 2.10).

§ 6 Abs. 2 SigV: Diese Bestimmung ist im gegenständlichen Fall nicht anwendbar, da die Datakom Austria GmbH für die Signatur qualifizierter Zertifikate keine sicheren elektronischen Signaturen verwendet. Die Datakom Austria GmbH verwendet aber dennoch die in Anhang 2 SigV genannten

Algorithmen (SHA-1 als Hashverfahren, RSA mit Schlüssellänge 1024 Bit zur Verschlüsselung des Hashwerts).

§ 6 Abs. 3 SigV: Der von der Datakom Austria GmbH eingesetzte Viewer ProSIGN Version 2.0 kann sichere elektronische Signaturen sowohl erstellen als auch prüfen. Hinsichtlich beider Funktionen liegt eine Bestätigung vor der deutschen Bestätigungsstelle TÜV Informationstechnik GmbH, dass eine Evaluierung und Bestätigung in Auftrag gegeben wurde (vgl. auch 4.1.3.2). Die Datakom Austria GmbH ist also – wenn die beauftragte Bestätigung vorliegt – auch zur sicheren Signaturprüfung in der Lage. Die entsprechende Funktionalität des Programmes ist aber schon jetzt vorhanden (2.15).

Die Anforderungen des § 10 Abs. 1 und 2 SigV (Kommunikation zwischen verschiedenen organisatorisch oder technisch getrennten Einrichtungen, Trennung von anderen Funktionen) werden durch die oben in 2.12 und 2.13, insbesondere 2.13.2 festgestellten Sicherheitsmaßnahmen erfüllt.

Zu § 10 Abs. 6 SigV: Die Signaturerstellungsdaten des Signators werden im Zuge der Registrierung des Signators und der Ausfolgung der Chipkarte erzeugt. (vgl. 2.11).

§ 12 Abs. 1 SigV: Für die Signatur der qualifizierten Zertifikate des Zertifizierungsdienstes „a-sign Premium“ werden gesonderte Signaturerstellungsdaten verwendet.

4.1.5.11 Schutz vor unbefugtem Zutritt und Zugriff (§ 7 Abs. 3 SigG, § 8 SigV, § 10 Abs. 3 SigV)

Gemäß § 7 Abs. 3 SigG sind die Signaturerstellungsdaten des Zertifizierungsdiensteanbieters vor unbefugtem Zugriff zu sichern. § 8 SigV enthält detailliertere Regelungen für den Schutz vor unbefugtem Zugriff auf die technischen Komponenten des Zertifizierungsdiensteanbieters. Gemäß § 10 Abs. 3 SigV sind die Einrichtungen zur Erbringung von Signatur- und Zertifizierungsdiensten vor unbefugtem Zutritt zu sichern.

Wie oben in 2.12 und 2.13 festgestellt wurde, sieht die Datakom Austria GmbH zahlreiche Maßnahmen zum Schutz vor unbefugtem Zugriff und Zutritt vor. Aus dem Bericht der RTR-GmbH und dem Gutachten von A-SIT haben sich diesbezüglich keine Mängel ergeben.

4.1.5.12 Information darüber, dass es sich um eine sichere elektronische Signaturen handelt (§ 7 Abs. 5 SigG)

Gemäß § 7 Abs. 5 SigG muss der Umstand, dass es sich um eine sichere elektronische Signatur handelt, im Zertifikat oder in einem elektronisch jederzeit allgemein zugänglichen Verzeichnis aufscheinen.

Beim gegenständlichen Zertifizierungsdienst scheint der Umstand im Zertifikat auf (siehe oben 2.14). Ein Signaturprüfer kann daran, dass das Zertifikat im Rahmen des Zertifizierungsdienstes „a-sign Premium“ ausgegeben wurde (dies ist insbesondere daran erkennbar, dass es mit den für den Zertifizierungsdienst „a-sign Premium“ vorgesehenen Signaturerstellungsdaten signiert wurde, weiters siehe oben 2.14) in Verbindung mit den veröffentlichten Dokumenten

des Sicherheits- und Zertifizierungskonzeptes erkennen, dass es sich um ein Zertifikat handelt, welches als qualifiziertes Zertifikat für die sichere elektronische Signatur ausgegeben wurde. Durch die Auflagen in den Spruchpunkten 2 c), 2 d) und 2 k) (siehe 4.2.2.3 und 4.2.2.10) wird sichergestellt, dass die Datakom Austria GmbH das Sicherheits- und Zertifizierungskonzept auch zu einem späteren Zeitpunkt nicht dahingehend abändern kann, dass im Zertifizierungsdienst „a-sign Premium“ auch Zertifikate ausgestellt würden, die nicht qualifizierte Zertifikate sind, die nicht an Inhaber sicherer Signaturerstellungseinheiten ausgegeben würden oder die für den Einsatz mit nicht den Anforderungen an Softwarekomponenten (siehe 4.1.3.2, 4.2.2.10) entsprechender Viewersoftware bestimmt wären.

Die von § 7 Abs. 5 SigG geforderte Erkennbarkeit für den Signaturprüfer ist insbesondere dann von Bedeutung, wenn der Vorgang der Signaturprüfung automatisiert oder standardisiert durchgeführt werden soll. Wenn etwa ein Unternehmen oder eine Behörde es für erforderlich hält, für einen bestimmten Vorgang (z. B. eine Bestellung oder einen Antrag) ausschließlich sicher elektronisch signierte Dokumente zuzulassen, dann muss in der Software für die Signaturprüfung und/oder in Dienstanweisungen an das Personal, welches die Bestellungen bzw. die Anträge bearbeitet, klar vorgegeben werden können, dass ausschließlich Zertifikate des Zertifizierungsdienstes „a-sign Premium“ (neben anderen entsprechenden Zertifizierungsdiensten anderer Anbieter), nicht aber Zertifikate der Zertifizierungsdienste „a-sign Light“, „a-sign Medium“ oder „a-sign Strong“ akzeptiert werden. Es würde ein Sicherheitsproblem darstellen, wenn zu einem späteren Zeitpunkt im selben Zertifizierungsdienst (oder in einem anderen, ebenfalls „a-sign Premium“ genannten Zertifizierungsdienst) Zertifikate mit geringeren Sicherheitsanforderungen ausgestellt würden, da nicht gewährleistet ist, dass alle potenziellen Signaturprüfer, die in den Einstellungen ihrer Software oder in Dienstanweisungen an ihr Personal bereits vorgegeben haben, „a-sign Premium“-Zertifikate für bestimmte Vorgänge zu akzeptieren, von der Änderung erfahren und ihre Prozeduren entsprechend adaptieren könnten.

4.1.5.13 Technische Komponenten der Signatoren (§ 18 SigG, § 3 SigV, § 4 SigV, § 7 SigV, § 9 SigV)

Die Definition der sicheren elektronischen Signatur in § 2 Z 3 SigG verweist in ihrer lit. e) auf die Sicherheitsanforderungen des SigG und der SigV und damit insbesondere auf die Anforderung des § 18 Abs. 5 SigG, dass die technischen Komponenten und Verfahren für die Erstellung sicherer elektronischer Signaturen nach dem Stand der Technik hinreichend und laufend geprüft sind und die Erfüllung der Sicherheitsanforderungen von einer Bestätigungsstelle (oder einer gleichwertigen Stelle) bescheinigt sind.

Wie bereits oben unter Punkt 4.1.3 ausgeführt wurde, ergibt sich aus § 18 Abs. 5 SigG, dass bei den derzeit üblichen technischen Realisierungen neben der Chipkarte auch die Komponenten der Hashbildung und der PIN-Eingabe und die Viewer-Software zu den „technischen Komponenten“ iSd § 18 Abs. 5 SigG gehören, also der Prüfung (Evaluierung) und Bescheinigung durch eine Bestätigungsstelle bedürfen.

Die von der Datakom Austria GmbH beim gegenständlichen Zertifizierungsdienst eingesetzte Chipkarte ist von der Bestätigungsstelle A-SIT bescheinigt (siehe oben 2.15).

Hinsichtlich des Secure Viewer wurde oben unter 4.1.3.2 ausgeführt, dass die Aufsichtsstelle der Ansicht ist, dass unter der Voraussetzung, dass eine Evaluierung und Bescheinigung bereits in Auftrag gegeben wurde, unter Vorschreibung einer entsprechenden Auflage davon abgesehen werden kann, dass bereits eine Bescheinigung vorliegt. Die in Punkt 4.1.3.2 genannten Voraussetzungen wurden durch die Erklärung der deutschen Bestätigungsstelle TÜV Informationstechnik GmbH erfüllt. Um sicherzustellen, dass die von der Datakom Austria GmbH eingesetzten Produkte bescheinigt werden, wurde die Auflage in Spruchpunkt 2k (siehe unten 4.2.2.10) vorgeschrieben.

Die Erfüllung der verschiedenen Anforderungen der §§ 3 und 4 SigV iVm § 9 SigV ergeben sich aus der Bescheinigung der Chipkarte, zu den Anforderungen aus § 7 SigV iVm § 9 SigV vgl. oben 4.1.3 (insbesondere 4.1.3.2).

4.1.5.14 Informationspflichten (§ 20 SigG, § 10 Abs. 7 SigV, § 17 SigV)

§ 20 Abs. 1 SigG sieht eine Reihe von Informationen vor, über die der Zertifizierungsdiensteanbieter den Zertifikatswerber vor Vertragsschließung schriftlich und unter Verwendung eines dauerhaften Datenträgers zu unterrichten hat. Wie unter 2.16 festgestellt wurde, sind die entsprechenden Informationen im Zertifikatswerber-Vertrag angeführt.

Gemäß § 20 Abs. 2 SigG sind diese Angaben auch Dritten, die ein rechtliches Interesse daran glaubhaft machen, zugänglich zu machen. Die Datakom Austria GmbH veröffentlicht den (nicht mit personenbezogenen Daten versehenen Text) des Zertifikatswerber-Vertrages.

Gemäß § 20 Abs. 3 SigG hat der Zertifizierungsdiensteanbieter den Zertifikatswerber darüber zu unterrichten, welche technischen Komponenten und Verfahren für das verwendete Signaturverfahren geeignet sind bzw. die Anforderungen für die Erzeugung oder Prüfung sicherer Signaturen erfüllen. Die Datakom Austria GmbH kann dem Zertifikatswerber (abgesehen von der ausgegebenen Chipkarte) derzeit nur das Produkt ProSIGN Version 2.0 empfehlen, später können aber (siehe Spruchpunkt 2k, 4.1.3.2 und 4.2.2.10) auch weitere technische Komponenten und Verfahren geeignet sein. Die Datakom Austria GmbH sieht vor, eine Liste der jeweils empfohlenen Signaturprodukte zu veröffentlichen.

In Punkt 10 des Zertifikatswerber-Vertrages ist auch eine Information über das Nachsignieren enthalten (vgl. auch die Ausführungen unten in 4.2.2.12).

4.1.6 Zusammenfassung

Alle Anforderungen des SigG und der SigV an einen Zertifizierungsdienste-anbieter, der sichere elektronische Signaturverfahren, bereitstellt, sind entweder erfüllt, oder ihre noch nicht erfolgte Erfüllung kann nach Maßgabe der Ausführungen in 4.1.4 durch Auflagen in ausreichender Form sichergestellt werden (siehe gleich unten unter 4.2).

Die Datakom Austria GmbH war daher zu akkreditieren.

Da antragsgemäß entschieden wurde, kann eine weitere Begründung gemäß § 58 Abs. 2 AVG unterbleiben. Zu den (teilweise) abgewiesenen Anträgen im Schreiben vom 11.12.2001 vgl. unten 4.4 und 4.5.

4.2 Auflagen

4.2.1 Allgemeines

Einen Zertifizierungsdiensteanbieter treffen – insbesondere dann, wenn er qualifizierte Zertifikate ausstellt oder sichere elektronische Signaturverfahren bereitstellt – nach dem Signaturgesetz und der Signaturverordnung zahlreiche Verpflichtungen.

Gemäß § 14 Abs. 1 SigG hat die Aufsichtsstelle den Zertifizierungsdiensteanbietern Maßnahmen zur Sicherstellung der Erfüllung dieser Pflichten vorzuschreiben. Solche Maßnahmen können grundsätzlich allen Zertifizierungsdiensteanbietern – also auch solchen, die keine qualifizierten Zertifikate ausstellen – vorgeschrieben werden.

Akkreditierte Zertifizierungsdiensteanbieter genießen wegen der von der Aufsichtsstelle vorgenommenen Prüfung ein besonders hohes Ansehen (vgl. EG 11 der Signaturrichtlinie). Daher besteht bei akkreditierten Zertifizierungsdiensteanbietern ein besonderer Bedarf danach, dass die Aufsichtsstelle Änderungen, die für die aufsichtsbehördliche Tätigkeit von besonderer Relevanz sind, umgehend erfährt, um gegebenenfalls rasch aufsichtsbehördlich tätig werden zu können.

Die in Spruchpunkt 2 dieses Bescheides enthaltenen Auflagen konkretisieren eine Reihe der sich aus dem SigG und der SigV für einen akkreditierten Zertifizierungsdiensteanbieter ergebenden Verpflichtungen – insbesondere seine Anzeigepflichten gegenüber der Aufsichtsstelle.

4.2.2 Zu den einzelnen Auflagen

4.2.2.1 Dienstaufnahme (Spruchpunkt 2a)

Mit Schreiben vom 11.12.2001 hat die Datakom Austria GmbH den Antrag gestellt, die in Spruchpunkt 2a vorgesehene Frist von drei Monaten für die Dienstaufnahme auf sechs Monate zu verlängern. Diesem Antrag konnte aus den folgenden Gründen nicht stattgegeben werden.

Das Signaturgesetz sieht vor, dass im Rechts- und Geschäftsverkehr Signaturverfahren mit unterschiedlichen Sicherheitsstufen und unterschiedlichen Zertifikatsklassen verwendet werden können (§ 3 Abs. 1 SigG). Für den Vertrauensschutz in die angebotenen Zertifizierungsdienste ist daher von besonderer Bedeutung, dass der Zertifizierungsdiensteanbieter die jeweiligen Sicherheits- und Zertifizierungskonzepte erfüllt (§ 6 Abs. 4 SigG) und gegenüber der Öffentlichkeit nicht mit einem Angebot von Zertifizierungsdiensten auftritt, die eine Qualität vorspiegeln, die er tatsächlich nicht erfüllen kann.

Die Aufsichtsstelle hätte daher z. B. auch Aufsichtsmaßnahmen zu ergreifen, wenn ein Zertifizierungsdiensteanbieter öffentlich behaupten würde, er könne sichere elektronische Signaturen anbieten, wenn er tatsächlich aber nicht dazu in der Lage wäre. Der Zertifizierungsdiensteanbieter hätte in diesem Falle zumindest seine Anzeigepflicht nach § 6 Abs. 2 SigG verletzt (§ 14 Abs. 2 Z 6 SigG).

Da eine Akkreditierung gemäß § 17 SigG vor der Aufnahme des entsprechenden Dienstes vorzunehmen ist, bedeutet eine Akkreditierung noch nicht automatisch, dass die Tätigkeit als akkreditierter Zertifizierungsdiensteanbieter auch aufgenommen wird. Es besteht vielmehr naturgemäß ein gewisser zeitlicher Abstand zwischen der Akkreditierung und der Dienstaufnahme. In diesem Zeitraum kann der Zertifizierungsdiensteanbieter sich – da ja der Anbieter und nicht der Dienst akkreditiert wird, siehe oben 4.1.1 – aber bereits als „Akkreditierter Zertifizierungsdiensteanbieter“ bezeichnen.

Im Sinne des vom Signaturgesetz in den genannten Bestimmungen vorgesehenen Vertrauensschutzes in die angebotenen Zertifizierungsdienste muss die Frist, während der sich ein Unternehmen sich als „Akkreditierter Zertifizierungsdiensteanbieter“ bezeichnen kann, ohne eine entsprechende Tätigkeit auszuüben, auf das Mindestmaß beschränkt werden. Die Datakom Austria GmbH kann den Dienst binnen drei Monaten ab Akkreditierung aufnehmen (2.18), daher war auch die Auflage vorzusehen, dass der Zertifizierungsdienst, auf welchen sich die Akkreditierung bezieht, binnen drei Monaten aufgenommen wird.

Der Antrag auf Fristverlängerung war daher abzuweisen (siehe unten 4.4).

Die Verpflichtung, der Aufsichtsstelle die Aufnahme der Tätigkeit als Zertifizierungsdiensteanbieter anzuzeigen, ergibt sich aus § 6 Abs. 2 SigG.

4.2.2.2 Änderungen des Sicherheits- und Zertifizierungskonzeptes (Spruchpunkt 2b)

Die Verpflichtung, der Aufsichtsstelle alle Änderungen des Sicherheits- und Zertifizierungskonzeptes anzuzeigen, ergibt sich ebenfalls aus § 6 Abs. 2 SigG. Nach dieser Bestimmung sind alle Änderungen der Dienste des Anbieters anzuzeigen. Da jeder Zertifizierungsdienst dem zugehörigen Sicherheits- und Zertifizierungskonzept entsprechen muss (§ 6 Abs. 3 SigG), ist mit jeder Änderung des Dienstes auch eine Änderung des Sicherheits- und Zertifizierungskonzeptes verbunden. Die Aufsichtsstelle geht davon aus, dass prinzipiell jede Änderung des Inhaltes eines Sicherheits- und Zertifizierungskonzeptes (§ 15 SigV) der Anzeigepflicht unterliegt. Die Auflage in Spruchpunkt 2 b) konkretisiert lediglich die wichtigsten sich daraus ergebenden Anzeigepflichten.

§ 6 SigG verfolgt – dem Art. 3 Signaturrichtlinie entsprechend – ein liberales Konzept, welches vor der Aufnahme von Zertifizierungsdiensten kein Genehmigungsverfahren und auch keine Fristen zwischen der Anzeige und der Dienstaufnahme vorsieht. Dementsprechend wird man auch bei einer Änderung grundsätzlich davon auszugehen haben, dass eine Anzeige spätestens zum Zeitpunkt des Inkrafttretens der Änderung ausreicht. – Es ist aber festzuhalten, dass § 6 Abs. 2 SigG sich nur auf öffentlich-rechtliche Verpflichtungen eines

Zertifizierungsdiensteanbieters gegenüber der Aufsichtsstelle bezieht. Inwieweit eine zivilrechtliche Verpflichtung des Zertifizierungsdiensteanbieters gegenüber den Signatoren oder anderen Personen, welche auf seine Dienste vertrauen, besteht, wesentliche Änderungen nicht überraschend, sondern mit angemessenen Übergangsfristen vorzunehmen, braucht in diesem Zusammenhang nicht erörtert zu werden. Weiters wird darauf verwiesen, dass mit der Auflage das Sicherheits- und Zertifizierungskonzept iSd SigG – also auch die nicht veröffentlichten Teile der Dokumentation des Zertifizierungsdienstes – gemeint ist und nicht bloß das Dokument „Sicherheits- und Zertifizierungskonzept für User Zertifikate Premium“.

In Spruchpunkt 2 b) aa) wird klargestellt, dass die Aufnahme eines weiteren Zertifizierungsdienstes, bei dem sichere elektronische Signaturverfahren bereitgestellt werden, keiner neuerlichen Akkreditierung bedarf, sondern lediglich anzuzeigen ist.

Durch Spruchpunkt 2 b) bb) wird sichergestellt, dass Benutzer elektronischer Signaturen auch bei einer Änderung des Namens oder einer Adresse des Zertifizierungsdiensteanbieters – insbesondere einer Internetadresse – über die Verzeichnisse der Aufsichtsstelle weiterhin Zugangsmöglichkeiten zum Zertifizierungsdiensteanbieter, seinen Diensten und zum Sicherheits- und Zertifizierungskonzept finden können.

Durch Spruchpunkt 2 b) dd) betreffend Änderungen der Codierungen in den ausgestellten Zertifikaten wird insbesondere sicher gestellt, dass der Aufsichtsstelle eine Änderung der Codierung der Policy, zu deren Einhaltung sich die Datakom Austria GmbH im Zertifikat bekennt, bekannt wird. Anzeigepflichtig ist es insbesondere, wenn die Datakom Austria GmbH auf die in ETSI TS 101 456 und ETSI TS 101 862 festgelegten Object Identifier umsteigt (vgl. die Ausführungen unter 4.1.2.3).

Da zu erwarten ist, dass die Datakom Austria GmbH laufend zusätzliche Signaturprodukte und Dokumentenformate unterstützen wird, wird in Spruchpunkt 2 b) ee) klargestellt, dass die entsprechenden Listen – welche gemäß § 15 Abs. 1 Z 13 und 15 SigV einen Teil des Sicherheits- und Zertifizierungskonzeptes bilden – der Aufsichtsstelle bekannt zu geben sind.

4.2.2.3 Ausschließlich qualifizierte Zertifikate und sichere Signaturerstellungseinheiten (Spruchpunkte 2c und 2d)

Gemäß § 3 Abs. 1 SigG können im Rechts- und Geschäftsverkehr Signaturverfahren mit unterschiedlichen Sicherheitsstufen und unterschiedlichen Zertifikatsklassen verwendet werden. Die Unterscheidungen zwischen „einfachen“ und qualifizierten Zertifikaten und zwischen „einfachen“ und sicheren elektronischen Signaturen stellen dabei die wesentlichsten Unterscheidungen dar.

Die klare und eindeutige Unterscheidbarkeit zwischen den verschiedenen Sicherheitsstufen und Zertifikatsklassen ist von besonderer Bedeutung für das in die Zertifizierungsdienste gesetzte Vertrauen.

Bei den Diensten der Datakom Austria GmbH wird diese Unterscheidbarkeit unter anderem durch die unterschiedliche Bezeichnung der Zertifikatsklassen

gewährleistet („a-sign Light“, „a-sign Medium“, „a-sign Strong“, „a-sign Premium“). Im Sicherheits- und Zertifizierungskonzept der Datakom Austria GmbH für den Zertifizierungsdienst „a-sign Premium“ ist vorgesehen, dass im Rahmen dieses Dienstes ausschließlich qualifizierte Zertifikate ausgestellt werden und dass diese Zertifikate ausschließlich an Signatoren ausgestellt werden, die über eine sichere Signaturerstellungseinheit verfügen. Die Auflagen in Spruchpunkt 2 c) und 2 d) untersagen es der Datakom Austria GmbH, zu einem späteren Zeitpunkt durch Änderung des Sicherheits- und Zertifizierungskonzeptes des Dienstes „a-sign Premium“ den Sicherheitsstandard dahingehend abzuändern, dass auch nicht qualifizierte Zertifikate ausgestellt würden oder dass Zertifikate an Personen ausgestellt würden, die nicht über eine sichere Signaturerstellungseinheit verfügen.

4.2.2.4 Komponenten zur Erstellung und Speicherung qualifizierter Zertifikate (Spruchpunkt 2e)

Diese Auflage konkretisiert die Verpflichtungen des Zertifizierungsdienste-anbieters gemäß § 7 Abs. 2 SigG.

Es wird klargestellt, dass Änderungen der vom Zertifizierungsdiensteanbieter für die Erbringung des Dienstes, auf den sich die Akkreditierung bezieht, eingesetzten System, Produkte und Verfahren, zulässig sind, ohne dass die Änderung einer neuerlichen Akkreditierung bedarf. Vielmehr ist der Zertifizierungsdiensteanbieter dazu verpflichtet, ausschließlich vertrauenswürdige Komponenten zu verwenden und diese gegebenenfalls rechtzeitig auszutauschen.

4.2.2.5 Störfälle (Spruchpunkt 2f)

Diese Auflage konkretisiert anhand des Sicherheits- und Zertifizierungskonzeptes die sich aus § 6 Abs. 5 SigG ergebende Verpflichtung, der Aufsichtsstelle alle Umstände, die eine ordnungsgemäße und dem Sicherheits- und Zertifizierungskonzept entsprechende Tätigkeit nicht mehr ermöglichen, unverzüglich anzuzeigen.

Punkt 5.1 des „CA Operation Manual“ der Datakom Austria GmbH enthält eine Auflistung wesentlicher Systemstörungen, die insbesondere die Verfügbarkeit der Verzeichnis- und Widerrufsdienste betreffen. Die Frist von 24 Stunden wurde entsprechend § 13 Abs. 5 SigV festgelegt.

Punkt 5.2 des „CA Operation Manual“ der Datakom Austria GmbH enthält Regelungen für den Fall eines Personalnotstandes. In diesem Fall könnte die Datakom Austria GmbH die im Rollenmodell des „CA Operation Manual“ vorgesehenen Rollen nicht mit zuverlässigem und qualifiziertem Personal (§ 10 Abs. 4 und 5 SigV) besetzen.

Unter dem in Spruchpunkt 2 f) cc) genannten Verdacht einer Kompromittierung der eingesetzten Signaturerstellungsdaten sind jene Beeinträchtigungen von Sicherheitsmaßnahmen oder Sicherheitstechnik zu verstehen, durch die das von der Datakom Austria GmbH zugrundegelegte Sicherheitsniveau nicht eingehalten ist (§ 2 Z 14 SigG). Dies wird insbesondere dann der Fall sein, wenn der Verdacht vorliegt, dass die Signaturerstellungsdaten der Datakom Austria GmbH die Signaturerstellungseinheit verlassen haben oder ausgelesen

bzw. errechnet werden konnten; oder wenn der Verdacht vorliegt, dass Unbefugte in der Lage waren, unter Verwendung der Signaturerstellungsdaten der Datakom Austria GmbH in deren Namen Zertifikate auszustellen. Vgl. auch Punkt 6.2.3 der Zertifizierungsrichtlinie.

Punkt 2.6 des Dokuments „Sicherheits- und Zertifizierungskonzept für User Zertifikate Premium“ sieht die Durchführung von internen Audits vor. Überprüft werden einerseits die Certification Authority, andererseits globale und lokale Registrierungsstellen. Die Aufsichtsstelle geht davon aus, dass Mängel bei den Registrierungsstellen im Regelfall nicht grundsätzlicher Art sein werden und vom Zertifizierungsdiensteanbieter umgehend abgestellt werden, dass aber bei einem Audit hervorgekommene Mängel im Betrieb der Certification Authority – also des technischen Kernbereichs – schwerwiegender und schwieriger zu beheben sein können. Solche Mängel sind also daraufhin zu überprüfen, ob Aufsichtsmaßnahmen zu ergreifen sind, weshalb für diese Audit-Berichte die Anzeigepflicht als Auflage vorzusehen war.

Um Missverständnisse zu vermeiden wird darauf hingewiesen, dass das „Sicherheits- und Zertifizierungskonzept für User Zertifikate Premium“ in Punkt 2.6.6.2 dritter Absatz vorsieht, dass vor der Veröffentlichung eines Audit-Berichtes der betroffenen Einheit die Möglichkeit zugestanden wird, die Mängel zu beheben und eine zweite Überprüfung durchführen zu lassen. Nur der Audit-Bericht der zweiten Überprüfung wird veröffentlicht. Von der Anzeigepflicht umfasst ist der erste Audit-Bericht.

4.2.2.6 Wirtschaftliches (Spruchpunkt 2g)

Gemäß § 7 Abs. 1 Z 5 SigG hat ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, über ausreichende Finanzmittel zu verfügen, um den Anforderungen des SigG und der SigV zu entsprechen, sowie Vorsorge für die Befriedigung von Schadenersatzansprüchen, etwa durch Eingehen einer Haftpflichtversicherung, zu treffen.

§ 2 Abs. 1 und 2 SigV konkretisieren diese Bestimmung im Hinblick auf die Mindestkapitalausstattung und eine obligatorische Haftpflichtversicherung.

Mit der in Spruchpunkt 2 g) aa) vorgesehenen Anzeigepflicht wird vorgesorgt, dass umgehend Aufsichtsmaßnahmen ergriffen werden können, wenn die Mindestkapitalausstattung unter die Grenze des § 2 Abs. 1 SigV absinkt.

Mit der in Spruchpunkt 2 g) bb) vorgesehenen Anzeigepflicht wird vorgesorgt, dass umgehend Aufsichtsmaßnahmen ergriffen werden können, wenn der Versicherungsschutz reduziert wird. Die Datakom Austria GmbH hat der Aufsichtsstelle nachgewiesen, dass die Konzernmutter Telekom Austria AG eine Haftpflichtversicherung abgeschlossen hat, durch welche auch die Datakom Austria GmbH versichert ist und ein Risiko von drei Versicherungsfällen pro Versicherungsjahr mit jeweils 1 Mio. Euro bedeckt ist. Wie oben unter 4.1.5.7 ausgeführt wurde, ist die Aufsichtsstelle der Ansicht, dass dadurch ein ausreichender Versicherungsschutz gegeben ist. Um Aufsichtsmaßnahmen ergreifen zu können, wenn der Versicherungsschutz erlischt, ist es insbesondere erforderlich, dass die Aufsichtsstelle in Kenntnis gesetzt wird,

a) wenn der Versicherungsvertrag in einer Weise geändert wird, die den Versicherungsschutz der Datakom Austria GmbH betrifft – insbesondere bei Kündigung des Vertrages;

b) wenn sich das Rechtsverhältnis zwischen Telekom Austria AG und Datakom Austria GmbH dergestalt ändert (z. B. durch Verkauf eines Anteils von mehr als 50 % an der Datakom Austria GmbH), dass die Datakom Austria GmbH in der Versicherung nicht mehr mitversichert ist;

c) oder wenn durch Eintritt von Versicherungsfällen der Versicherungsschutz so weit geschmälert wird, dass Aufsichtsmaßnahmen zu prüfen sind. Die in der Auflage gewählte Grenze wurde so bestimmt, dass nicht jeder Versicherungsfall zu melden ist – wohl aber eine Reduktion des Versicherungsschutzes auf weniger als zwei Versicherungsfälle für das verbleibende Versicherungsjahr.

Im Falle eines Insolvenzverfahrens muss die Aufsichtsstelle besonders rasch reagieren und gegebenenfalls dafür Sorge tragen, dass die Zertifizierungsdienste in geordneter Form eingestellt oder von einem anderen Zertifizierungsdienst weitergeführt werden. Die in Spruchpunkt 2 g) cc) vorgesehene Anzeigepflicht trägt dem Rechnung.

Mit der in Spruchpunkt 2 g) dd) vorgesehenen Anzeigepflicht wird vorgesorgt, dass die Aufsichtsstelle über wesentliche, den Zertifizierungsdiensteanbieter betreffende, gesellschaftsrechtliche Änderungen (wie z. B. eine Spaltung, Verschmelzung oder Umgründung, Änderungen der Firma oder des Sitzes) informiert wird. Von Bedeutung ist insbesondere auch eine Änderung der Eigentumsverhältnisse – siehe oben unter Punkt b) –, da das Bestehen des Versicherungsschutzes davon abhängig ist.

4.2.2.7 Ansprechperson (Spruchpunkt 2h)

Gemäß § 16 SigG hat ein Zertifizierungsdiensteanbieter zur Durchführung der Aufsicht unter anderem Auskünfte zu erteilen und jede sonst erforderliche Unterstützung zu gewähren.

Um im Falle eines Störfalles rasch erste Auskünfte einholen zu können, ist der Aufsichtsstelle zumindest eine Ansprechperson samt Telefonnummer, Faxnummer und E-Mail-Adresse zu nennen, die solche Auskünfte erteilen kann.

4.2.2.8 Einstellung der Tätigkeit (Spruchpunkt 2i)

Die Verpflichtung zur Anzeige der Einstellung der Tätigkeit ergibt sich aus § 12 SigG. Für den Fall, dass die Widerrufsdienste nicht von der Datakom Austria GmbH oder einem anderen Zertifizierungsdiensteanbieter weitergeführt werden können, ist sicherzustellen, dass die Aufsichtsstelle für die Weiterführung der Widerrufsdienste Sorge tragen kann. Die Pflicht, in diesem Fall alle Zertifikate zu widerrufen, ergibt sich aus § 9 Abs. 1 Z 4 SigG. Dazu wird das Format spezifiziert, in welchem die Widerrufsliste an die Aufsichtsstelle zu übergeben ist (X.509v2). Es handelt sich dabei um jenes Format, das die Datakom Austria GmbH auch für die eigenen Widerrufsdienste verwendet. Um sicherzustellen, dass die Widerrufsliste für einen gewissen Übergangszeitraum sowohl an der ursprünglichen Adresse als auch an der neuen Adresse (bei der Aufsichtsstelle)

abrufbar ist, wird die Datakom Austria GmbH dazu verpflichtet, die Widerrufsliste noch zumindest einen Monat nach der Übergabe an der ursprünglich dafür vorgesehenen Adresse abrufbar zu halten.

4.2.2.9 Evaluierungsberichte des IBM-Kryptoadapters (Spruchpunkt 2j)

Die Bestätigungsstelle A-SIT hat in ihrem Gutachten festgestellt, dass die Vorkehrungen, um die Signaturerstellungsdaten des Zertifizierungsdienste-anbieters geheim zu halten und vor unbefugtem Zugriff zu schützen, ausreichend sind, falls bis spätestens 31.05.2002 ein Evaluierungsbericht oder ein Bericht über den Status der Evaluierung (CP/Q++ gemäß FIPS 140-1 bzw. CCA gemäß Common Criteria) nachgereicht wird.

Die Auflage gründet sich auf § 7 Abs. 2 zweiter Satz SigG iVm § 9 SigV. Bei der Festsetzung der Frist 31.05.2001 folgt die Aufsichtsstelle der Empfehlung im Gutachten der Bestätigungsstelle A-SIT (siehe auch oben 4.1.5.10).

4.2.2.10 Viewersoftware (Spruchpunkt 2k)

Wie oben in Punkt 4.1.3.2 ausgeführt, ist die Aufsichtsstelle der Ansicht, dass eine Akkreditierung auch dann auszusprechen ist, wenn eine technische Komponente, welche die Anforderungen des § 7 Abs. 1 bis 3 abdeckt, zwar noch nicht bescheinigt ist, aber doch die in Punkt 4.1.3.2 genannten Kriterien erfüllt.

Die Datakom Austria GmbH verfügt noch nicht über eine bescheinigte Viewersoftware (siehe oben 2.15, 4.1.3, 4.1.5.13). Die Software ProSIGN Version 2.0 entspricht aber den in Punkt 4.1.3.2 genannten Kriterien (siehe oben 4.1.5.13). Der Datakom Austria GmbH war daher bezüglich dieser Software aufzutragen, eine Bescheinigung nachzureichen (ein Statusbericht über die Evaluierung reicht nicht aus, siehe dazu unten 4.5).

Hinsichtlich anderer Viewer (wie insbesondere dem zum Siemens Sign@tor noch zu entwickelnden Viewer) war die Auflage anzuordnen, diese Viewer nur nach den in Punkt 4.1.3.2 genannten Kriterien anzubieten.

4.2.2.11 Dokumentationssystem (Spruchpunkt 2l)

Gemäß § 16 SigV muss die Dokumentation nach § 11 SigG einschließlich der Störfälle und der besonderen Betriebssituationen sowie der Unterrichtung der Zertifikatswerber nach § 20 SigG „jedenfalls in elektronischer Form erfolgen“. Die Datakom Austria GmbH verfügt noch nicht über ein solches Dokumentationssystem (siehe oben 2.10). Wie oben unter 4.1.5.8 ausgeführt, stellt das Fehlen eines elektronischen Dokumentationssystems keinen so schwerwiegenden Mangel dar, dass der Antrag auf Akkreditierung deshalb abzuweisen wäre, aufgrund von § 16 SigV war aber als Auflage vorzuschreiben, dass das elektronische Dokumentationssystem zu implementieren ist. und die in Papierform archivierten Informationen nachzuerfassen sind.

Die Datakom Austria GmbH hat angekündigt, dass die Errichtung eines elektronischen Dokumentationssystems für das erste Quartal 2002 geplant sei (E-Mail vom 06.11.2001, ON 71). Die in Spruchpunkt 2l vorgesehenen Fristen sind daher jedenfalls angemessen.

4.2.2.12 Nachsignieren (Spruchpunkt 2m)

Der Sicherheitswert elektronischer Signaturen verringert sich mit fortschreitender Zeit (§ 17 SigV), weshalb zur Erhaltung des Sicherheitswertes nach einiger Zeit eine erneute elektronische Signatur unter Verwendung eines Zeitstempels erforderlich ist (Nachsignieren). Die erneute Signatur umfasst dabei die alte Signatur und beweist in Verbindung mit dem Zeitstempel, dass die alte Signatur zu einem Zeitpunkt vorlag, zu dem die verwendeten Verfahren noch als sicher angesehen wurden.

Das Nachsignieren ist ein rein technischer Vorgang und stellt keine Willenserklärung dar. Die Signatur muss also nicht von einer bestimmten Person ausgelöst werden, vielmehr kann das Nachsignieren von jeder Person veranlasst werden, die an der Erhaltung des Sicherheits- oder Beweiswertes der elektronischen Signatur ein Interesse hat.

Die Aufsichtsstelle geht davon aus, dass bis zum Ablauf des 31.12.2005, der in Anhang 1 SigV und in Punkt 10 des Zertifikatswerbervertrages als maßgebliche Frist für die im gegenständlichen Fall eingesetzten Verfahren angesehen wird, Zeitstempeldienste am Markt angeboten werden, die für das Nachsignieren geeignet sein werden.

Um den Sicherheitswert der von der Datakom Austria GmbH angebotenen sicheren elektronischen Signaturen dauerhaft sicherzustellen, war der Akkreditierungswerberin aber die Auflage zu erteilen, selbst einen Zeitstempeldienst anzubieten, wenn ein solcher nicht von anderen Marktteilnehmern angeboten wird.

4.2.2.13 Registrierungsstellen (Spruchpunkt 2n)

Gemäß § 8 Abs. 2 SigG ist es zulässig, Tätigkeiten im Zusammenhang mit der Ausstellung qualifizierter Zertifikate an andere im Auftrag des Zertifizierungsdiensteanbieters tätige Stellen auszulagern. Die Datakom Austria GmbH hat insbesondere mitgeteilt, dass die Österreichische Post AG Registrierungsstellen betreiben werde. Ein entsprechender Vertrag ist noch nicht unterschrieben. Aus § 8 Abs. 2 SigG („im Auftrag“) ergibt sich aber, dass ein entsprechendes Rechtsverhältnis zwischen dem Zertifizierungsdienste-anbieter und dem Betreiber der Registrierungsstelle bestehen muss.

Es war daher als Auflage vorzusehen, dass vor Aufnahme des Betriebs von externen Registrierungsstellen ein entsprechender Vertrag abgeschlossen werden muss. Der der Aufsichtsstelle vorgelegte Vertragsentwurf ist grundsätzlich geeignet, die Rechte und Pflichten der Vertragspartner in einer für die Verantwortung von Anbietern qualifizierter Zertifikate nach dem SigG geeigneten Weise umzusetzen.

In diesem Zusammenhang ist auch darauf hinzuweisen, dass der Vertragsentwurf zwischen Datakom Austria GmbH und Österreichischer Post AG auch Teile des Sicherheitskonzeptes (insbesondere zum Schutz der technischen Einrichtungen der Registrierungsstelle z. B. durch eine Firewall) enthält, die sonst nirgendwo geregelt sind. Änderungen dieser Teile des Vertrages sind daher eine Änderung des Sicherheits- und Zertifizierungs-konzeptes und gemäß § 6 Abs. 2 SigG anzeigepflichtig.

4.3 Gebühren

Die Vorschreibung der Gebühr von 6000 Euro (82.561,80 ATS) für die Überprüfung der Datakom Austria GmbH anlässlich der Akkreditierung gründet sich auf § 1 Abs. 1 Z 3 SigV.

Gemäß § 1 Abs. 3 SigV hat die Aufsichtsstelle, wenn sie sich einer Bestätigungsstelle bedient, deren Gebühren nach § 53a AVG zu bestimmen und dem betroffenen Zertifizierungsdiensteanbieter als Barauslagen im Sinn des § 76 AVG vorzuschreiben.

§ 53a AVG verweist auf das Gebührenanspruchsgesetz. Nach dessen § 34 ist die Gebühr nach richterlichem Ermessen nach der aufgewendeten Zeit und Mühe und nach den Einkünften, die der Sachverständige für eine gleiche oder ähnliche Tätigkeit im außergerichtlichen Erwerbsleben üblicherweise bezöge, zu bestimmen.

Die Bestätigungsstelle A-SIT hat 118,25 Arbeitsstunden (gerundet 14,78 Mitarbeitertage) aufgewendet. Der Tagsatz von 15.000 ATS entspricht dem Expertentagsatz aus dem veröffentlichten Preisblatt von A-SIT (siehe http://www.a-sit.at/signatur/bestaetigungsstelle/bescheinigung/Preisblatt.pdf), wie ihn A-SIT auch für die (privatrechtliche) Tätigkeit der Ausstellung von Bescheinigungen nach § 18 Abs. 5 SigG verrechnet.

Es war daher gemäß § 1 Abs. 3 SigV iVm § 76 und § 53a AVG für die Heranziehung der Bestätigungsstelle A-SIT die Gebühr von 221.718,75 ATS (16.112,93 Euro) vorzuschreiben.

Das von der RTR-GmbH geführte Verzeichnis der Zertifizierungsdiensteanbieter erfüllt noch nicht die vom Signaturgesetz geforderten Sicherheitsanforderungen. Von der Vorschreibung einer Gebühr gemäß § 1 Abs. 1 Z 10 SigV war daher vorerst abzusehen.

Die Auflage in Spruchpunkt 3. b) gründet sich auf § 1 Abs. 4 SigV.

4.4 Fristverlängerung für die Dienstaufnahme

Mit Schreiben vom 11.12.2001 hat die Datakom Austria GmbH den Antrag gestellt, die in Spruchpunkt 2a vorgesehene Frist auf sechs Monate zu verlängern.

Wie oben unter Punkt 4.2.2.1 ausgeführt wurde, konnte diesem Antrag nicht stattgegeben werden. Der Antrag war daher abzuweisen.

4.5 Bescheinigung von ProSIGN 2.0

Ebenfalls mit Schreiben vom 11.12.2001 hat die Datakom Austria GmbH einen Antrag betreffend die in Spruchpunkt 2k vorgesehene Auflage gestellt. Die Aufsichtsstelle hatte vorgesehen, die Datakom Austria GmbH dazu zu verpflichten, bis zum 30.09.2002 eine Bescheinigung der Software ProSIGN Version 2.0 vorzulegen. Die Datakom Austria GmbH hat beantragt, stattdessen auch einen Bericht über den Status der Evaluierung vorlegen zu können.

Die Aufsichtsstelle hat dem Antrag insofern stattgegeben, als die Frist für die Vorlage der Bescheinigung auf die in 4.1.3.2 genannte Frist von 12 Monaten ab Auslieferung des Produktes (hier: ab Dienstaufnahme, da es sich um den ersten zur Verfügung stehenden Viewer handelt) geändert wurde.

Im Hinblick auf die unter 4.1.3.2 ausgeführten Überlegungen war der Antrag darüber hinaus aber abzuweisen. Es ist erforderlich, dass eine Bescheinigung vorgelegt wird. Der bloße Statusbericht über den Stand der Evaluierung genügt nicht.

Die Frist ist aber jedenfalls angemessen, da gemäß der der Aufsichtsstelle vorliegenden Erklärung der deutschen Bestätigungsstelle TÜV Informationstechnik GmbH ohnehin der Abschluss der Evaluierung innerhalb des ersten Halbjahres 2002 avisiert sei und keine Erkenntnisse vorlägen, die einen erfolgreichen Abschluss des Verfahrens innerhalb dieses Zeitraums gefährden würden.

III. Rechtsmittelbelehrung

Gegen diesen Bescheid ist gemäß § 115 Abs. 2 TKG kein ordentliches Rechtsmittel zulässig.

IV. Hinweise

Gegen diesen Bescheid kann binnen sechs Wochen ab der Zustellung Beschwerde an den Verfassungsgerichtshof und ebenso an den Verwaltungsgerichtshof erhoben werden. Die Beschwerde muss von einem Rechtsanwalt unterschrieben sein. Bei der Einbringung der Beschwerde ist eine Gebühr von ATS 2.500,– (Euro 181,68) zu entrichten.

Telekom-Control-Kommission
Wien, am 17. Dezember 2001

Der Vorsitzende
Dr. Eckhard Hermann