Aufsichtsstelle für elektronische Signaturen

Informationen zur Anzeigepflicht nach dem Signaturgesetz

Version 1.0

01.06.2001

Aufsichtsstelle für elektronische Signaturen
Telekom-Control-Kommission & Rundfunk und Telekom Regulierungs-GmbH
Mariahilfer Straße 77–79, 1060 Wien, Tel. +43/1/58058-0, Fax: +43/1/58058-9191
http://www.signatur.rtr.at/, signatur@signatur.rtr.at

1. Einleitung

Gemäß § 6 Abs. 2 SigG hat jeder Zertifizierungsdiensteanbieter die Aufnahme seiner Tätigkeit unverzüglich der Aufsichtsstelle für elektronische Signaturen anzuzeigen. Im vorliegenden Dokument soll ein Überblick darüber gegeben werden, wer zur Anzeige verpflichtet ist und was der Aufsichtsstelle angezeigt werden muss.

Der Zweck der Anzeigepflicht besteht darin, der Aufsichtsstelle einen Überblick über das Angebot von Zertifizierungsdiensten in Österreich zu verschaffen. Die Aufsichtsstelle veröffentlicht – unter Wahrung der Betriebs- und Geschäftsgeheimnisse der Anbieter – einen Teil der dabei erhaltenen Informationen auch in dem von ihr geführten Verzeichnis der Zertifizierungsdiensteanbieter (http://www.signatur.rtr.at/) und ermöglicht dadurch auch den Nutzern elektronischer Signaturen, einen Überblick über die angebotenen Dienste zu erhalten.

Um den Zertifizierungsdiensteanbietern die Anzeige zu erleichtern, hat die Aufsichtsstelle auch einige Formulare erstellt, die im Anhang dieses Dokuments abgedruckt sind. Es wird empfohlen, diese Formulare zu verwenden.

Für weitere Fragen steht Ihnen das Team der Aufsichtsstelle jederzeit zur Verfügung: signatur@signatur.rtr.at, Tel. +43/1/58058-0.

2. Wer unterliegt der Anzeigepflicht?

Zur Anzeige verpflichtet ist jeder Zertifizierungsdiensteanbieter (§ 6 Abs. 2 SigG). Der Begriff des Zertifizierungsdiensteanbieters ist in § 2 Z 10 und 11 SigG sehr breit gefasst. Zertifizierungsdiensteanbieter ist demzufolge jede natürliche oder juristische Person oder sonstige rechtsfähige Einrichtung, die **Zertifikate ausstellt** oder andere Signatur- und Zertifizierungsdienste (wie z. B. **Zeitstempeldienste**) erbringt.

Prinzipiell fällt jeder Anbieter von Zertifikaten – nicht nur Anbieter qualifizierter Zertifikate – unter die Anzeigepflicht. Im folgenden Abschnitt wird detaillierter erläutert, welche Zertifizierungsdienste der Aufsicht und der Anzeigepflicht unterliegen.

3. Welche Zertifizierungsdienste sind anzuzeigen?

3.1 Was ist ein Zertifizierungsdienst?

Ein **Zertifizierungsdiensteanbieter** bietet in der Regel mehrere **Zertifizierungsdienste** an. Innerhalb eines Zertifizierungsdienstes kann es eine weitere Untergliederung der erbrachten Dienstleistungen geben, insbesondere wird häufig zwischen verschiedenen **Zertifikatsklassen** unterschieden.

Für die Unterscheidung zwischen verschiedenen Zertifizierungsdiensten knüpft die Aufsichtsstelle grundsätzlich an den für den jeweiligen Zertifizierungsdienst verwendeten Signaturerstellungsdaten (private Schlüssel) an. Die Aufsichtsstelle stellt bei der Registrierung der Zertifizierungsdiensteanbieter im sicheren Verzeichnis der Aufsichtsstelle grundsätzlich ein Zertifikat pro Zertifizierungsdienst, d. h. ein Zertifikat pro eingesetztem Schlüsselpaar aus.

Werden für die Ausstellung verschiedener Zertifikatsklassen auch verschiedene Signaturerstellungsdaten verwendet, dann sieht die Aufsichtsstelle dies auch als verschiedene Zertifizierungsdienste an. Dem Zertifizierungsdiensteanbieter werden dann von

der Aufsichtsstelle auch mehrere Zertifikate ausgestellt und im sicheren Verzeichnis der Aufsichtsstelle eingetragen.

Verwendet der Zertifizierungsdiensteanbieter hingegen für alle von ihm ausgestellten Zertifikate die selben Signaturerstellungsdaten, dann sieht die Aufsichtsstelle dies als einen Zertifizierungsdienst an und stellt dem Zertifizierungsdiensteanbieter auch nur ein Zertifikat aus.

Zu beachten ist in diesem Zusammenhang §12 Abs. 1 SigV, demzufolge für qualifizierte Zertifikate und für andere Zertifikate unterschiedliche Signaturerstellungsdaten verwendet werden müssen. Es ist also nicht zulässig, innerhalb desselben Zertifizierungsdienstes einfache Zertifikate und qualifizierte Zertifikate gemischt auszustellen.

Weiters ist § 7 Abs. 5 SigG zu beachten: Stellt der Zertifizierungsdiensteanbieter ein sicheres elektronisches Signaturverfahren bereit, dann muss der Umstand, dass es sich um eine sichere elektronische Signatur handelt, im Zertifikat oder in einem elektronisch jederzeit allgemein zugänglichen Verzeichnis aufscheinen. Die Aufsichtsstelle empfiehlt daher, qualifizierte Zertifikate, die für die sichere elektronische Signatur vorgesehen sind, innerhalb eines eigenständigen Zertifizierungsdienstes anzubieten.

3.2 Welche Zertifizierungsdienste sind anzeigepflichtig?

3.2.1 Offenes oder geschlossenes System?

§ 1 Abs. 2 SigG sieht vor, dass das Signaturgesetz auch in geschlossenen Systemen anzuwenden ist, sofern deren Teilnehmer dies vereinbart haben. Im Umkehrschluss bedeutet das, dass ein Zertifizierungsdienst nicht der Aufsicht und der Anzeigepflicht unterliegt, wenn es sich dabei um ein geschlossenes System handelt und die Teilnehmer nicht vereinbart haben, dass das Signaturgesetz anwendbar sein soll.

Zur Abgrenzung, was als offenes und was als geschlossenes System anzusehen ist, liegt zum Zeitpunkt der Abfassung dieses Dokumentes noch kaum Rechtsprechung der Aufsichtsstelle vor. Grundsätzlich kann festgehalten wird, dass jedenfalls ein offenes System vorliegt, wenn der Zertifizierungsdiensteanbieter an einen offenen bzw. unbestimmten Kreis von Personen Zertifikate ausstellt – mag es sich dabei auch um eine kleine Zahl von Zertifikaten handelt.

Es wird empfohlen, den Zertifizierungsdienst im Zweifel jedenfalls der Aufsichtsstelle anzuzeigen. Wenn ein Zertifizierungsdienst angezeigt wird, für den keine Anzeigepflicht besteht, dann weist die Aufsichtsstelle die Anzeige mangels Zuständigkeit zurück, ohne dass dadurch Rechtsfolgen für den Anbieter entstehen. Wird hingegen nicht angezeigt, obwohl Anzeigepflicht besteht, so besteht gegen den Anbieter auch die Möglichkeit eines Verwaltungsstrafverfahrens (§ 26 Abs. 3 Z 1 SigG).

3.2.2 Signatur oder Verschlüsselung?

In der Praxis werden Zertifikate sowohl zur Verschlüsselung als auch zur Signatur eingesetzt. In einem X.509-Zertifikat ist der öffentliche Schlüssel eines asymmetrischen kryptographischen Verfahrens (z. B. RSA) enthalten, welcher in der Regel sowohl für die Verschlüsselung als auch für die Signaturprüfung verwendet werden kann.

Ein Zertifikat nach dem Signaturgesetz liegt jedoch nur vor, wenn „Signaturprüfdaten“ einer bestimmten (natürlichen oder juristischen) Person zugeordnet werden und deren Identität bestätigt wird (§ 2 Z 8 SigG). Die Aufsichtsstelle erachtet sich daher nicht für solche Zertifizierungsdienste zuständig, bei welchen ausschließlich Zertifikate für

Verschlüsselungszwecke ausgestellt werden. – Sehr wohl erachtet die Aufsichtsstelle aber ihre Zuständigkeit hinsichtlich sogenannter Serverzertifikate als gegeben, da diese auch der Authentifizierung dienen.

In technischer Hinsicht bedeutet das: Bei einem X.509v3-Zertifikat, in welchem das Feld KeyUsage verwendet wird, ist grundsätzlich davon auszugehen, dass ein Zertifikat iSd Signaturgesetzes vorliegt, wenn in diesem Feld zumindest eines der Bits digitalSignature, nonRepudiation, keyCertSign oder cRLSign gesetzt ist. Sind hingegen nur die Bits keyAgreement, keyEncipherment, dataEncipherment, encipherOnly oder decipherOnly gesetzt, dann dient der öffentliche Schlüssel ausschließlich zur Verschlüsselung und es handelt sich nicht um ein Zertifikat iSd Signaturgesetzes.

Bietet ein Zertifizierungsdiensteanbieter einen eigenständigen Zertifizierungsdienst an, dessen Zertifikate ausschließlich zur Verschlüsselung gewidmet sind, so unterliegt dieser Zertifizierungsdienst nicht der Aufsicht und muss nicht angezeigt werden.

Werden aber innerhalb eines Zertifizierungsdienstes mehrere verschiedene Arten von Zertifikaten ausgestellt, die auch nur teilweise der Aufsicht unterliegen, so ist der Dienst in seiner Gesamtheit anzuzeigen. Wenn ein Zertifizierungsdiensteanbieter also mit denselben Signaturerstellungsdaten sowohl Zertifikate für die Signatur als auch Zertifikate für die Verschlüsselung signiert, dann muss er diesen Zertifizierungsdienst und alle diesen Dienst betreffenden Änderungen der Aufsichtsstelle anzeigen.

3.2.3 Testzertifikate

In einem Anlassfall hat die Aufsichtsstelle entschieden, dass dem Signaturgesetz (insbesondere den Begriffsbestimmungen des § 2 SigG) nicht unterstellt werden kann, dass es sich auch auf rein experimentelle „Zertifizierungsdienste“ bezieht, bei denen Zertifikate in geringer Zahl zwar an eine (beschränkte) Öffentlichkeit ausgestellt werden und auch öffentlich nachprüfbar sind, bei denen aber aus dem Sicherheits- und Zertifizierungskonzept, aus sonstigen Publikationen bzw. aus den Zertifikaten selbst für jedermann deutlich ersichtlich ist, dass es sich um reine Testzertifikate handelt. Zertifikate iSd Signaturgesetzes dienen nämlich der Sicherung des Vertrauens in die elektronische Kommunikation. Muss aber für jedermann schon von vornherein klar sein, dass ein Zertifikat nicht für diesen Zweck der Sicherung des Vertrauens in die elektronische Kommunikation und die Identität des Kommunikationspartners ausgestellt wurde, sondern ausschließlich für Forschungs- oder Testzwecke, so besteht kein Bedarf an einer rechtlichen Regelung und einer aufsichtsbehördlichen Tätigkeit.

Die Aufsichtsstelle hat aber gleichzeitig festgehalten, dass bei der Bewertung von Zertifizierungsdiensten, die angeblich nur für Forschungs- oder Testzwecke oder dergleichen betrieben werden, ein strenger Maßstab anzulegen sein wird, sodass ein Zertifizierungsdienst im Zweifel jedenfalls als unter den Geltungsbereich des SigG und damit unter die Aufsicht und unter die Anzeigepflicht fallend anzusehen ist.

4. Wann muss man eine Anzeige erstatten?

Das SigG unterscheidet die folgenden Fälle

Aufnahme eines Dienstes	§ 6 Abs. 2	Anzeige spätestens mit Aufnahme der Tätigkeit
Änderung eines Dienstes	§ 6 Abs. 2	Anzeige spätestens mit Wirksamwerden der Änderung
Ordnungsgemäße Tätigkeit nicht mehr möglich	§ 6 Abs. 5	unverzügliche Anzeige
Einstellung des Dienstes	§ 12	unverzügliche Anzeige

Gemäß §6 Abs. 2 SigG ist die Anzeige „spätestens mit Aufnahme der Tätigkeit oder bei Änderung seiner Dienste“ zu erstatten. Gemäß § 6 Abs. 5 SigG hat ein Zertifizierungsdiensteanbieter alle Umstände, die eine ordnungsgemäße und dem Sicherheits- sowie dem Zertifizierungskonzept nicht mehr entsprechende Tätigkeit nicht mehr ermöglichen, unverzüglich der Aufsichtsstelle anzuzeigen. Gemäß §12 SigG hat ein Zertifizierungsdiensteanbieter die Einstellung seiner Tätigkeit „unverzüglich der Aufsichtsstelle anzuzeigen“.

Anzeigepflichtig ist also die Aufnahme jedes einzelnen Zertifizierungsdienstes, jede Änderung betreffend einen Zertifizierungsdienst und jede Einstellung eines Zertifizierungsdienstes, weiters jeder Umstand, der eine ordnungsgemäße Tätigkeit nicht mehr ermöglicht.

Obwohl es bei der Anzeige der Aufnahme des Dienstes und bei der Anzeige von Änderungen prinzipiell genügt, wenn die Anzeige spätestens zum Zeitpunkt der Dienstaufnahme bzw. zum Zeitpunkt des Wirksamwerdens der Änderung einlangt, wird insbesondere den Anbietern qualifizierter Zertifikate oder sicherer elektronischer Signaturen empfohlen, die Aufsichtsstelle möglichst frühzeitig zu kontaktieren.

Gemäß §6 Abs. 4 SigG hat ein Zertifizierungsdiensteanbieter die im (der Aufsichtsstelle angezeigten) Sicherheits- oder Zertifizierungskonzept dargelegten Angaben während der gesamten Ausübung seiner Tätigkeit zu erfüllen. Es muss also jeder Änderung der faktischen Tätigkeit eines Zertifizierungsdiensteanbieters auch eine Änderung des Konzeptes und eine entsprechende Anzeige an die Aufsichtsstelle vorausgehen.

5. Was muss die Anzeige enthalten?

Gemäß § 6 Abs. 2 SigG ist der Anzeige für jeden angebotenen Signatur- und Zertifizierungsdienst ein Sicherheitskonzept sowie ein Zertifizierungskonzept samt den verwendeten technischen Komponenten und Verfahren vorzulegen.

Für die Anbieter qualifizierter Zertifikate ist in §15 SigV der Mindestinhalt des Sicherheits- und Zertifizierungskonzeptes vorgegeben. Gemäß § 18 Abs. 2 SigV sind der Anzeige neben dem Sicherheits- und Zertifizierungskonzept auch anzuschließen: eine Darstellung der spezifischen sicherheitsrelevanten Bedrohungen und Risiken beim Zertifizierungsdiensteanbieter; der Nachweis der finanziellen Ausstattung sowie der erforderlichen Haftpflichtversicherung und der Nachweis des Fachwissens des technischen Personals.

Der im SigG und in der SigV verwendete Begriff des „Sicherheits- und Zertifizierungskonzeptes“ geht über den üblichen Umfang eines Certification Practice

Statement hinaus und umfasst z. B. auch die Signaturprüfdaten bzw. das Zertifikat des Zertifizierungsdiensteanbieters sowie Unterlagen, die nicht zur Veröffentlichung bestimmt sind.

Weder das SigG noch die SigV schreiben dem Zertifizierungsdiensteanbieter eine bestimmte Gliederung der anzuzeigenden Dokumente vor. An die Aufsichtsstelle werden regelmäßig Anfragen gerichtet, ob ein Zertifizierungsdiensteanbieter etwa eine Bedrohungsanalyse, ein Rollenmodell, ein Betriebshandbuch, ein Certification Practice Statement, interne Schulungsunterlagen oder dergleichen erstellen müsse. Dazu kann festgehalten werden, dass weder durch das SigG noch durch die SigV konkrete derartige Dokumente gefordert werden, dass aber die vom SigG und der SigV für ein Sicherheits- und Zertifizierungskonzept geforderten Inhalte häufig in derartigen Dokumenten behandelt werden. Es gilt also:

- Der Zertifizierungsdiensteanbieter ist nicht verpflichtet, derartige Dokumente zu erstellen, dies bedeutet aber nicht, dass der Zertifizierungsdiensteanbieter sich mit Fragen, die üblicherweise in solchen Dokumenten behandelt werden, nicht beschäftigen muss. Vielmehr müssen alle von der SigG und dem SigV aufgeworfenen Fragen im Sicherheits- und Zertifizierungskonzept behandelt werden – in welche Dokumenten auch immer dieses gegliedert sein mag.

- Wenn der Zertifizierungsdiensteanbieter derartige Dokumente erstellt, dann werden sie ihrem Inhalt nach typischerweise als Teile des Sicherheits- und Zertifizierungskonzeptes anzusehen sein und sollen daher im Regelfall der Anzeige angeschlossen werden – insbesondere dann, wenn andere der Aufsichtsstelle angezeigten Dokumente darauf verweisen.

Für die Zusammenstellung aller Dokumente, die für die Anzeige erforderlich sein können, können Sie die folgende Checkliste verwenden:

- Formular „Angaben zum Zertifizierungsdiensteanbieter“
- Formular „Angaben zum Zertifizierungsdienst“ für jeden einzelnen Dienst
- Sicherheits- und Zertifizierungskonzept im engeren Sinne. Dies kann z. B. in Form eines Certification Practice Statement und einer Certification Policy formuliert sein. Die Aufsichtsstelle empfiehlt, sich dabei an internationalen Standards (z. B. RFC 2527) zu orientieren
- Zum Nachweis der erforderlichen finanziellen Ausstattung:
  - Beim nicht kommerziell tätigen Anbieter: Allgemeine Angaben, wie die Finanzierung sichergestellt ist.
  - Bei einem Anbieter, der keine qualifizierten Zertifikate ausstellt: Businessplan (siehe Muster-Businessplan)
  - Bei einem Anbieter, der qualifizierte Zertifikate ausstellt: Businessplan, Firmenbuchauszug, letzter Jahresabschluss, Polizze der Haftpflichtversicherung
- Wenn sichere elektronische Signaturverfahren angeboten werden: Formular „Unterstützte technische Komponenten“ samt Beilagen (Bestätigungen und Prüfberichte von Bestätigungsstellen) und Formular „Unterstützte Dokumentenformate“ samt Beilagen (Spezifikationen der Dokumentenformate)
- Der nötige Umfang des Nachweises der „Darstellung der spezifischen sicherheitsrelevanten Bedrohungen und Risiken beim Zertifizierungsdiensteanbieter“ ist von der Qualität des Dienstes abhängig. Das Formblatt „Angaben zum Zertifizierungsdienst“ enthält auch die aus der Sicht der Aufsichtsstelle wichtigsten diesbezüglichen Fragen. Unter Umständen hat der Zertifizierungsdiensteanbieter dafür aber auch ein eigenes Dokumenten erstellt.
- Der Nachweis des Fachwissens des Personals ist nur bei Anbietern qualifizierter Zertifikate oder sicherer elektronischer Signaturen erforderlich (oder dann, wenn im

Sicherheits- und Zertifizierungskonzept besondere Zusicherungen gemacht werden.) Als Nachweis kommen insbesondere entsprechende Zeugnisse oder eine Darlegung der fachlich einschlägigen Tätigkeit (Lebenslauf) in Frage (§ 10 Abs. 5 SigV).

- Der Nachweis der Zuverlässigkeit des Personals ist ebenfalls nur bei Anbietern qualifizierter Zertifikate oder sicherer elektronischer Signaturen erforderlich (oder dann, wenn im Sicherheits- und Zertifizierungskonzept besondere Zusicherungen gemacht werden.) Für den Nachweis sollen Strafregisterauskünfte (beschränkte Auskunft iSd § 6 Tilgungsgesetz) des relevanten Personals vorgelegt werden.
- Weitere Beilagen einer Anzeige können z. B. sein:
  - Wenn andere Rechtsträger als Registrierungsstellen tätig werden: Angaben zu den Rechtsbeziehungen mit den Registrierungsstellen (Verträge), Angaben zur Auswahl der Registrierungsstellen, Dienstvorschriften oder Schulungsunterlagen für die Mitarbeiter der Registrierungsstelle
  - Unterlagen zur Belehrung des Signators

Die Aufsichtsstelle hat einige Formulare aufgelegt, die für die Anzeige verwendet werden können. Dieses Dokument und die Formulare können – als ZIP-Datei zusammengefasst – am Webserver der Aufsichtsstelle (http://www.signatur.rtr.at/, Rubrik „Zertifizierungsdiensteanbieter – Informationen für Anbieter“) gemeinsam abgerufen werden.

6. Welche Formvorschriften sind bei der Anzeige zu beachten

Gemäß §18 Abs. 1 SigV ist für die Anzeige eines der Formate RTF, PDF, Ascii oder Postscript zu verwenden. Die Anzeige muss elektronisch signiert sein.

Bei Verwendung der gemeinsam mit diesem Dokument abrufbaren Formulare wird empfohlen, die ausgefüllten Formulare sowie weitere Beilagen (z. B. das Certification Practice Statement) in RTF oder PDF zu konvertieren und alle Dokumente per E-Mail (nach Möglichkeit S/MIME) an signatur@signatur.rtr.at zu übermitteln.

Ist es nicht möglich, die Anzeige firmenmäßig elektronisch zu signieren (z. B. wenn eine firmenmäßige Zeichnung nur durch zwei Personen gemeinsam erfolgen kann, dies aber von der eingesetzten Signaturtechnologie nicht unterstützt wird), dann sollte die Anzeige zusätzlich zur elektronischen Übermittlung auch firmenmäßig gezeichnet postalisch übermittelt werden.

Bei der Anzeige von Umständen, die eine ordnungsgemäße Tätigkeit nicht mehr ermöglichen, soll ungeachtet allfälliger Formvorschriften der schnellstmögliche Weg gewählt werden, die Aufsichtsstelle zu verständigen. Insbesondere sollte auch versucht werden, Mitarbeiter der Aufsichtsstelle telefonisch vorab zu informieren.

7. Wie wird die Anzeige von der Aufsichtsstelle behandelt?

7.1 Anzeige der Aufnahme des Dienstes

Die Anzeige wird zunächst von der RTR-GmbH (der Geschäftsstelle der Telekom-Control-Kommission) formal geprüft. Dabei wird insbesondere geprüft, ob es sich überhaupt um eine Anzeige iSd SigG handelt, ob Unklarheiten hinsichtlich der Identität oder Rechtspersönlichkeit des Zertifizierungsdiensteanbieters bestehen oder ob die Vollmacht des Einschreiters zweifelhaft ist. Gibt es ein solches formales Problem, so fordert die RTR-GmbH im Auftrag der Telekom-Control-Kommission den Einschreiter auf, den Mangel zu beheben.

Bestehen keine formalen Mängel, so veröffentlicht die RTR-GmbH das Einlangen der Anzeige auf der Website http://www.signatur.rtr.at/ mit dem Vermerk „wird derzeit geprüft“. Dabei wird im Regelfall nur veröffentlicht, dass eine Anzeige eingelangt ist, nicht aber Details zum Inhalt der Anzeige. Um Missverständnisse auszuschließen, wird außerdem ein erklärender Zusatz angefügt, aus dem hervorgeht, dass der Zertifizierungsdiensteanbieter das Ergebnis der Überprüfung durch die Aufsichtsstelle nicht abwarten muss, um seine Dienste anbieten zu können.

Die RTR-GmbH legt die Anzeige dann der Telekom-Control-Kommission zur Entscheidung über allfällige Aufsichtsmaßnahmen oder Mängelbehebungsaufträge im Sinne des § 13 Abs. 3 AVG vor. Gegebenenfalls trägt die Telekom-Control-Kommission dem Zertifizierungsdiensteanbieter die Behebung von Mängeln auf. Die Aufsichtsstelle kann unter Umständen auch Aufsichtsmaßnahmen ergreifen oder dem Anbieter sogar die weitere Tätigkeit untersagen.

Wenn keine Mängel (mehr) vorliegen, beschließt die Telekom-Control-Kommission, die Anzeige zur Kenntnis zu nehmen und keine Aufsichtsmaßnahmen zu ergreifen. Dies wird dem Zertifizierungsdiensteanbieter auch in einem formlosen Schreiben mitgeteilt. Gleichzeitig schreibt die Telekom-Control-Kommission per Bescheid die für die Anzeige zu entrichtende Gebühr vor (§ 1 Abs. 1 SigV).

Ab Herbst 2001 wird die RTR-GmbH daraufhin dem Zertifizierungsdiensteanbieter ein Zertifikat ausstellen und dieses Zertifikat im sicheren Verzeichnis der Aufsichtsstelle veröffentlichen. Spätestens zu diesem Zeitpunkt werden auch alle weitere Detailinformationen über die angezeigten Zertifizierungsdienste auf der Website der Aufsichtsstelle veröffentlicht und der Vermerk „wird derzeit geprüft“ wird entfernt.

7.2 Anzeige von Änderungen

Bei der Anzeige von Änderungen der Zertifizierungsdienste geht die Aufsichtsstelle sinngemäß so vor wie bei der Anzeige der Aufnahme des Dienstes.

7.3 Anzeige von Umständen, die eine ordnungsgemäße Tätigkeit nicht mehr ermöglichen

Wie die Aufsichtsstelle eine solche Anzeige behandelt, hängt von der Schwere des Problems, von den vom Zertifizierungsdiensteanbieter bereits eingeleiteten Maßnahmen zu seiner Behebung und vom Informationsstand der Aufsichtsstelle ab. Die §§ 14 bis 16 SigG stellen der Aufsichtsstelle eine breite Palette an möglichen Aufsichtsmitteln zur Verfügung, die aber nach dem Grundsatz der Verhältnismäßigkeit anzuwenden sind.

Die Aufsichtsstelle empfiehlt, bei auftauchenden Problemen, die eine Einhaltung des Sicherheits- und Zertifizierungskonzeptes unmöglich machen, möglichst frühzeitig die Aufsichtsstelle zu kontaktieren. Es wird darauf hingewiesen, dass ein Unterbleiben der Anzeige verwaltungsrechtlich strafbar ist (§ 26 Abs. 3 Z 2 SigG).

7.4 Anzeige der Einstellung des Dienstes

Die Anzeige der Einstellung des Dienstes wird von der Aufsichtsstelle sinngemäß so behandelt wie die Anzeige der Aufnahme eines Dienstes oder der Änderung von Diensten.

Zusätzlich wird geprüft, wie der Verzeichnis- und Widerrufsdienst hinsichtlich der bei Einstellung des Dienstes noch gültigen Zertifikate weitergeführt wird. § 12 SigG sieht grundsätzlich die folgenden Möglichkeiten vor:

- Der Zertifizierungsdienst (oder auch nur die Verzeichnis- und Widerrufsdienste) werden von einem anderen Zertifizierungsdiensteanbieter weitergeführt. In diesem Fall ist auch eine entsprechende Anzeige des neuen Zertifizierungsdiensteanbieters erforderlich.

- Der Zertifizierungsdiensteanbieter stellt nur die Ausgabe neuer Zertifikate ein, führt aber den Verzeichnisdienst und den Widerrufsdienst (Entgegennahme und Bearbeitung von Widerrufsanträgen, Abrufbarkeit der Widerrufsliste) noch weiter, bis der Gültigkeitszeitraum des letzten von ihm ausgestellten Zertifikates abgelaufen ist. In diesem Fall ist eine neuerliche Anzeige erforderlich, wenn der Zertifizierungsdiensteanbieter entgegen seiner ursprünglichen Absicht den Widerrufsdienst doch zu einem früheren Zeitpunkt einstellt.

- Der Zertifizierungsdiensteanbieter widerruft alle zum Zeitpunkt der Einstellung der Tätigkeit noch gültigen Zertifikate, stellt eine letzte Widerrufsliste mit einem entsprechend weit in der Zukunft liegenden Ablaufdatum aus und hält diese noch abrufbar, bis der Gültigkeitszeitraum des letzten von ihm ausgestellten Zertifikates abgelaufen ist.

- Kommt der Zertifizierungsdiensteanbieter seiner Verpflichtung gemäß §12 SigG nicht nach, seine Dienste im nötigen Ausmaß weiter zu führen, dann trägt die Aufsichtsstelle für die Weiterführung der Widerrufsdienste auf Kosten des Zertifizierungs-diensteanbieters Sorge. Die Aufsichtsstelle kann dem Zertifizierungsdiensteanbieter beispielsweise auftragen, alle noch gültigen Zertifikate zu widerrufen und eine letzte Widerrufsliste mit einem entsprechend weit in der Zukunft liegenden Ablaufdatum auszustellen. Die Aufsichtsstelle hält dann diese Widerrufsliste auf Kosten des Zertifizierungsdiensteanbieters (§ 1 Abs. 1 Z 9 SigV) abrufbar, bis der Gültigkeitszeitraum des letzten von ihm ausgestellten Zertifikates abgelaufen ist.

8. Anmerkungen

Einige Antworten auf häufig gestellte Fragen bzw. in der Praxis aufgetretene Probleme:

- Das Sicherheits- und Zertifizierungskonzept ist nicht nur für die Aufsichtsstelle von Interesse, sondern für jeden potenziellen Nutzer des Zertifizierungsdienstes. Die Aufsichtsstelle hat daher schon mehrfach entschieden, dass die Anzeige in der Amtssprache (also in deutscher Sprache) zu erfolgen hat.

- Die Anzeige muss alle maßgeblichen Dokumente enthalten und muss elektronisch signiert sein. Der Anbieter kann sich also in der Anzeige nicht darauf beschränken, im Internet (z. B. auf der Website des Zertifizierungsdiensteanbieters) abrufbare Dokumente zu zitieren.

9. Adressen

Alle Anzeigen nach dem SigG sind an die Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen zu richten. Für alle Fragen betreffend die Anzeigepflicht wenden Sie sich bitte an die Geschäftsstelle der Telekom-Control-Kommission:

Rundfunk und Telekom Regulierungs-GmbH
Mariahilfer Straße 77–79, 1060 Wien
Tel. +43/1/58058-0, Fax: +43/1/58058-9191
http://www.signatur.rtr.at/, signatur@signatur.rtr.at

Telekom-Control-Kommission
Mariahilfer Straße 77–79, 1060 Wien
Tel. +43/1/58058-0, Fax: +43/1/58058-9191
http://www.signatur.rtr.at/, signatur@signatur.rtr.at

Anzeige gemäß § 6/§ 12 Signaturgesetz

Name des Zertifizierungsdiensteanbieters

Bitte übermitteln Sie auch die Angaben im Formular „Angaben zum Zertifizierungsdiensteanbieter“, wenn seit der letzten Anzeige Änderungen eingetreten sind.

Allgemeine Angaben

☐ Anzeige der Aufnahme der Tätigkeit als Zertifizierungsdiensteanbieter

Bitte beachten Sie das Dokument „Informationen zur Anzeige nach dem Signaturgesetz“ und legen Sie die dort genannten Beilagen bei.

☐ Anzeige der Aufnahme eines weiteren/weiterer Zertifizierungsdienste(s)

Wenn der neue Zertifizierungsdienst auf bereits angezeigten Dokumenten beruht, dann verweisen Sie bitte auf diese Dokumente. Wenn die Neuaufnahme des Zertifizierungsdienstes auch Auswirkungen auf bestehende Dienste hat (z. B. Änderung eines für alle Dienste geltenden CPS), dann zeigen Sie auch die Änderungen hinsichtlich der bereits erbrachten Dienste an.

☐ Anzeige einer Änderung hinsichtlich der erbrachten Zertifizierungsdienste

- ☐ Änderung des Sicherheits- und Zertifizierungskonzeptes ieS
- ☐ Wechsel der eingesetzten Signaturerstellungsdaten
- ☐ Änderungen hinsichtlich der unterstützten technischen Komponenten zur Erzeugung sicherer elektronischer Signaturen oder der unterstützten Dokumentenformate für sichere elektronische Signaturen

☐ Anzeige von Umständen, die eine ordnungsgemäße Tätigkeit nicht mehr ermöglichen

☐ Anzeige der Einstellung eines oder mehrerer Zertifizierungsdienste

☐ Anzeige der Einstellung der Tätigkeit als Zertifizierungsdiensteanbieter

☐ Sonstige Anzeige (z. B. Änderung des Namens oder der Adresse)

Allgemeine Beschreibung des Inhaltes der Anzeige

Für die Anzeige maßgebliches Datum

Bei der Anzeige der Aufnahme eines oder mehrerer Zertifizierungsdienste: Geben Sie den Tag an, an dem der Dienst aufgenommen wird.

Bei der Anzeige von Änderungen: Geben Sie den Tag an, an dem die Änderungen wirksam werden.

Bei der Einstellung eines oder mehrerer Zertifizierungsdienste: Geben Sie den Tag an, an dem der Dienst eingestellt wird und kreuzen Sie eine der folgenden Alternativen an bzw. beschreiben Sie, wie die Widerrufsdienste weitergeführt werden:

☐ Hinsichtlich der nach Einstellung des Zertifizierungsdienstes noch gültigen Zertifikate wird der Verzeichnisdienst und der Widerrufsdienst (Entgegennahme und Bearbeitung von Widerrufsanträgen, Abrufbarkeit der Widerrufsliste) noch bis zum weitergeführt.

☐ Alle zum Zeitpunkt der Einstellung des Zertifizierungsdienstes noch gültigen Zertifikate werden bzw. wurden widerrufen. Die Widerrufsliste wird noch bis zum abrufbar gehalten.

☐ Der Verzeichnis- und der Widerrufsdienst werden von einem anderen Zertifizierungsdiensteanbieter – nämlich von – weitergeführt.

Vertraulichkeit

☐ Die Anzeige soll von der Aufsichtsstelle bis zum oben genannten Datum vertraulich behandelt werden.

Hinweis: Die Aufsichtsstelle behält sich vor, auch entgegen dem Wunsch des Anbieters Informationen zu veröffentlichen oder an andere Behörden zu übermitteln, wenn dies rechtlich geboten ist – insbesondere bei der geplanten Einstellung eines Dienstes oder bei der Anzeige von Umständen, die eine ordnungsgemäße Tätigkeit nicht mehr ermöglichen.

Beilagen

Bitte führen Sie die Beilagen zu dieser Anzeige an und geben Sie dabei an, welche Dokumente von der Aufsichtsstelle vertraulich behandelt werden sollen. Als Beilagen kommen z. B. ein Certification Practice Statement, eine Certification Policy, Bescheinigungen einer Bestätigungsstelle, interne Sicherheitskonzepte, etc. in Frage.

Bezeichnung des Dokuments	Version	Datum	vertraulich
☒ Formular „Angaben zum Zertifizierungsdiensteanbieter“			☐
☒ Formular(e) „Angaben zum Zertifizierungsdienst“			teilweise
☒ Signaturprüfdaten der angebotenen Dienste (PKCS#10)			☐
☒ Businessplan			☒
☐ Formular „Unterstützte technische Komponenten“			☐
☐ Formular „Unterstützte Dokumentenformate“			☐
			☐
			☐
			☐

Datum und firmenmäßige Zeichnung

Hinweis: Gemäß § 18 Abs. 1 SigV muss die Anzeige der Aufnahme der Tätigkeit eines Zertifizierungsdiensteanbieters in elektronischer Form erfolgen und elektronisch signiert sein.

Telekom-Control-Kommission
Mariahilfer Straße 77–79, 1060 Wien
Tel. +43/1/58058-0, Fax: +43/1/58058-9191
http://www.signatur.rtr.at/, signatur@signatur.rtr.at

Beilage zur Anzeige nach § 6/§ 12 SigG: Angaben zum Zertifizierungsdiensteanbieter

Bitte legen Sie die folgenden Angaben jeder Anzeige nach § 6 bzw. § 12 SigG bei, wenn sich seit der letzten Anzeige eine Änderung ergeben hat, bzw. teilen Sie der Aufsichtsstelle alle diesbezüglichen Änderungen mit.

Name des Zertifizierungsdiensteanbieters

Adresse (PLZ, Ort, Straße, Hausnummer)

Telefonnummer

Faxnummer

E-Mail-Adresse

Homepage

X.500-Adresse (falls verfügbar)

ASN.1 Object Identifier (falls verfügbar)

Firmenbuchnummer und Firmenbuchgericht (falls verfügbar)

Sonstige Angaben (falls erforderlich)

Wenn der Zertifizierungsdienst (insbesondere die Trust-Center-Komponenten) tatsächlich an einem anderen Standort als am oben angegebenen Sitz des Zertifizierungsdiensteanbieters erbracht wird, dann geben Sie bitte auch diesen Standort an. Diese Information wird von der Aufsichtsstelle vertraulich behandelt.

Telekom-Control-Kommission
Mariahilfer Straße 77–79, 1060 Wien
Tel. +43/1/58058-0, Fax: +43/1/58058-9191
http://www.signatur.rtr.at/, signatur@signatur.rtr.at

TKK

Beilage zur Anzeige nach § 6/§ 12 SigG: Angaben zum Zertifizierungsdienst

Viele der Fragen in diesem Formular werden häufig in einem Certification Practice Statement oder einer Certification Policy behandelt. Wenn Sie solche Dokumente erstellt haben, können Sie dieses Formular auch als Checkliste verwenden und entweder nur diese Dokumente übermitteln oder bei den einzelnen Fragen jeweils auf die beigelegten Dokumente verweisen.

Das Formular wurde vor allem für die Anbieter einfacher Zertifikate konzipiert. Es wurde zwar so abgefasst, dass auch das Angebot qualifizierter Zertifikate prinzipiell berücksichtigt wurde, deckt aber die Anforderungen an Anbieter qualifizierter Zertifikate nicht vollständig ab. Insbesondere wurde in diesem Formular nicht berücksichtigt: Lebenszyklus der eingesetzten Schlüssel, Nachsignieren, Format der Dokumentation, Genauigkeit der verwendeten Zeitgeber.

Bezeichnung des Zertifizierungsdiensteanbieters

Bezeichnung des Zertifizierungsdienstes

Werden im Rahmen dieses Dienstes qualifizierte Zertifikate ausgestellt?

☐ Ja ☐ Nein

Werden im Rahmen dieses Dienstes sichere elektronische Signaturverfahren bereitgestellt?

☐ Ja ☐ Nein

In welcher Form wird ein Verzeichnisdienst geführt?

☐ Nicht ☐ HTTP ☐ LDAPv2 ☐ LDAPv3 ☐ OCSP ☐ Andere

Wie kann auf den Verzeichnisdienst zugegriffen werden?

Geben Sie z. B. die URL eines Web-Formulars oder Name, Port und Suchbasis eines LDAP-Servers an.

In welcher Form wird ein Widerrufsdienst geführt (Entgegennahme der Widerrufsanträge)?

☐ Nicht ☐ Telefon ☐ Fax ☐ E-Mail ☐ HTTP ☐ Brief
☐ RFC 2510 ☐ RFC 2797 ☐ Andere

Geschäftszeiten zur Entgegennahme der Widerrufsanträge, maximale Dauer bis zur Veröffentlichung des Widerrufs

In welcher Form wird ein Widerrufsdienst geführt (Abrufbarkeit der CRL oder des Status eines Zertifikates)?

☐ Nicht ☐ HTTP ☐ LDAPv2 ☐ LDAPv3 ☐ OCSP ☐ Andere

Wie kann auf den Widerrufsdienst (z. B. die CRL) zugegriffen werden?

Geben Sie z. B. die URL eines Web-Formulars oder Name, Port und Suchbasis eines LDAP-Servers an.

In welchem Format werden Zertifikate ausgestellt?

☐ X.509v1 ☐ X.509v3 ☐ Andere

Datenstruktur des Zertifikats (nach Möglichkeit in ASN.1)

In welchem Format werden Widerrufslisten (CRLs) ausgestellt?

☐ X.509v1 ☐ X.509v2 ☐ Andere

Datenstruktur der CRL (nach Möglichkeit in ASN.1)

Welche Attribute werden zur (eindeutigen) Beschreibung des Signators im Zertifikat angegeben?

z. B. Vorname, Nachname, E-Mail-Adresse, Adresse, Vertretungsmacht; Zusätze, die bei Namensgleichheit angefügt werden, um Eindeutigkeit zu erhalten; Kennzeichnung eines Namens als Pseudonym etc.

Wie lange sind Zertifikate gültig?

Wie ist der Anwendungsbereich der Zertifikate gegebenenfalls eingeschränkt oder der Transaktionswert begrenzt?

Wie wird die Identität bzw. wie werden die anderen Attribute des Signators im Zertifikat geprüft?

Geben Sie eine detaillierte Beschreibung des Vorganges der Identitätsprüfung an oder verweisen Sie auf ein Dokument, in welchem die Identitätsprüfung beschrieben ist.

Mit welchem Verfahren werden Zertifikate signiert?

- ☐ RSA
- ☐ DSA
- ☐ ISO/IEC 14883-3, Annex A.2.2 („Agnew-Mullin-Vanstone analogue“)
- ☐ IEEE P1363, Section 5.3.3 („Nyberg-Rueppel version“)
- ☐ IEEE P1363, Section 5.3.4 („DSA version“)
- ☐ Andere

Wieviel Bit beträgt die Länge des Schlüssels, mit dem Zertifikate signiert werden?

Übermitteln Sie auch die korrespondierenden Signaturprüfdaten (wenn möglich als PKCS#10-Antrag) an die Aufsichtsstelle.

Welches Hash-Verfahren wird für die Signatur von Zertifikaten verwendet?

☐ SHA-1 ☐ RIPEMD-160 ☐ MD5 ☐ Andere

Für welche Verfahren eignen sich die Schlüssel der Signatoren?

- ☐ RSA
- ☐ DSA
- ☐ ISO/IEC 14883-3, Annex A.2.2 („Agnew-Mullin-Vanstone analogue“)
- ☐ IEEE P1363, Section 5.3.3 („Nyberg-Rueppel version“)
- ☐ IEEE P1363, Section 5.3.4 („DSA version“)
- ☐ Andere

Wieviel Bit beträgt die Länge der Schlüssel der Signatoren?

Wann wurde bzw. wird der Dienst aufgenommen?

Wann wurde bzw. wird der Dienst eingestellt?

Worin besteht die Dokumentation (z. B. Certificate Policy, Certification Practice Statement, Sicherheits- und Zertifizierungskonzept)? Bitte jeweils um Angabe von Bezeichnung, Version und Datum des Dokuments sowie um einen Hinweis, ob das Dokument öffentlich zugänglich oder vertraulich ist!

Bitte legen Sie die entsprechenden Dokumente bei, wenn sie nicht schon einer früheren Anzeige beigelegt wurden.

Angaben zu den technischen Komponenten beim Signator

Wo werden die Signaturerstellungsdaten des Signators aufbewahrt?

☐ In einer sicheren Signaturerstellungseinheit

Wenn dies der Fall ist, dann füllen Sie bitte auch das Formular „Unterstützte technische Komponenten“ aus. Die beiden nächsten Fragen erübrigen sich dann.

☐ Auf einem nicht lesbaren Datenträger (z. B. Prozessor-Chipkarte), der aber nicht als sichere Signaturerstellungseinheit evaluiert und bescheinigt ist

☐ Auf einem lesbaren Datenträger (z. B. Diskette, Festplatte oder Speicher-Chipkarte)

☐ Die Auswahl des Speichermediums bleibt dem Signator überlassen.

Wo werden die Schlüssel der Signatoren erzeugt?

☐ Beim Signator ☐ Beim Anbieter ☐ Anderswo

Werden die Schlüssel in den Signaturerstellungseinheiten erzeugt?

☐ Ja ☐ Nein ☐ Entscheidung obliegt dem Signator

Die folgenden Informationen dienen ausschließlich zur Information der Aufsichtsstelle und werden vertraulich behandelt.

Angaben zur allgemeinen IT-Sicherheit

Durch welche Maßnahmen ist der Schutz vor unbefugtem Zutritt zu den technischen Komponenten des Zertifizierungsdiensteanbieters gewährleistet?

Durch welche Maßnahmen ist der Schutz vor unbefugtem Zugriff von außen (z. B. über das Internet) gewährleistet?

Durch welche Maßnahmen ist der Schutz vor unbefugtem Zugriff von innen (z. B. durch unbefugte Mitarbeiter) gewährleistet?

Wenn die Identitätsprüfung über Registrierungsstellen durchgeführt wird: Wie wird der Datenverkehr zwischen den Registrierungsstellen und der Zertifizierungsstelle gesichert?

Beschreiben Sie die Schutzmaßnahmen gegen Elementarereignisse (Feuer, Wassereinbruch, Stromausfall) und gegen Datenverlust (z. B. Angaben zur Backupstrategie)?

Angaben zur Signatur von Zertifikaten und Widerrufslisten

Wenn qualifizierte Zertifikate angeboten werden, legen Sie detaillierte Unterlagen zum Aufbau des Systems, zur Abgrenzung gegenüber Systemen, die für andere Aufgabenbereiche eingesetzt werden und zu den getroffenen Schutzmaßnahmen bei. Beschreiben Sie diesfalls auch, ob für die Signatur der Zertifikate sichere Signaturerstellungseinheiten eingesetzt oder ob die Zertifikate mit fortgeschrittenen elektronischen Signaturen signiert werden und legen Sie entsprechende Unterlagen zur Evaluation der Signaturerstellungseinheiten bei.

Erfolgt die Signatur der Zertifikate bzw. der Widerrufslisten online?

☐ Ja ☐ Nein

Wo erfolgt die Erstellung und Anzeige des Zertifikats, die Anwendung des Hash-Verfahrens auf das vorbereitete Zertifikat und die Anwendung der Signaturerstellung auf den Hashwert? Wo erfolgt die Signatur von Widerrufslisten?

☐ In einer dezidiert dafür eingesetzten und abgeschlossenen Hardwareeinheit

☐ Auf einem dezidiert für Zertifizierungszwecke gewidmeten Rechner

☐ Auf einem Rechner, der auch der Verwaltung der Signatoren dient

☐ Auf einem Rechner, der auch für andere Aufgaben eingesetzt wird

Wo werden die Signaturerstellungsdaten zum Signieren von Zertifikaten aufbewahrt?

☐ In einer sicheren Signaturerstellungseinheit

☐ Auf einem nicht lesbaren Datenträger (z. B. Prozessor-Chipkarte), der aber nicht als sichere Signaturerstellungseinheit evaluiert und bescheinigt ist

☐ Auf einem lesbaren Datenträger (z. B. Diskette, Festplatte oder Speicher-Chipkarte)

Wodurch wird die Zufallsqualität bei der Schlüsselerzeugung gewährleistet (eigene Hardwareeinrichtung, Systemereignisse, Pseudozufallszahlen)?

Angaben zum Verzeichnis- und Widerrufsdienst

Gibt es Einschränkungen der Verfügbarkeit des Verzeichnis- und Widerrufsdienstes?

Z. B.: Wird nur eine bestimmte zeitliche Verfügbarkeit (nur während der Geschäftszeiten) garantiert? Kann nur ein bestimmter Personenkreis auf die Dienste zugreifen? Ist der Zugriff entgeltpflichtig?

Hat der Signator die Möglichkeit, der Veröffentlichung seines Zertifikates im Verzeichnis zu widersprechen?

☐ Ja ☐ Nein

Welche Maßnahmen werden zur Ausfallsicherheit und zur Sicherung des schnellen und sicheren Zugriffs auf Verzeichnis- und Widerrufsdienst getroffen?

Angaben zu personellen Sicherheitsmaßnahmen

Ist für bestimmte Maßnahmen ein Vier-Augen-Prinzip vorgesehen? Wird dieses auch technisch sichergestellt?

Beilage zur Anzeige nach § 6/§ 12 SigG: Businessplan
Firma

PLAN G&V		2000 EUR	2001 EUR	2002 EUR	2003 EUR	2004 EUR
	nicht qualifizierte Zertifikate					
	qualifizierte Zertifikate					
	Sonstige					
Erträge	**Gesamt**					
	Personal eigenes					
	Leasingpersonal und freie Mitarbeiter					
	techn.Aufwand					
	Aufwand für externe Registrierungsstellen					
	Aufwand für Haftpflichtversicherung					
	Abschreibung auf techn. Anlagevermögen					
	sonstige Abschreibung					
	sonstiger Aufwand					
Aufwand	**Gesamt**					
Betriebsergebnis						
Cash Flow						

PLANBILANZ		2000 EUR	2001 EUR	2002 EUR	2003 EUR	2004 EUR
	technisches Anlagevermögen					
	sonstiges Anlagevermögen					
	Anlagevermögen Gesamt					
	Sonstige Aktiva					
Aktiva	**Gesamt**					
	Eigenkapital					
	Verbindlichkeiten verbundene Unternehmen bis 3 Jahre					
	Verbindlichkeiten verbundene Unternehmen länger 3 Jahre					
	Verbindlichkeiten sonstige bis 3 Jahre					
	Verbindlichkeiten sonstige länger 3 Jahre					
	Sonstige					
Passiva	**Gesamt**					

Investitionen und Finanzierung		2000 EUR	2001 EUR	2002 EUR	2003 EUR	2004 EUR
Investitionen	techn. Ausstattung					
	sonstige					
	Gesamt					
Finanzierung	Eigenmittel					
	Fremdmittel verbundene Unternehmen bis 3 Jahre					
	Fremdmittel verbundene Unternehmen länger 3 Jahre					
	Fremdmittel sonstige bis 3 Jahre					
	Fremdmittel sonstige länger 3 Jahre					
	Gesamt					

sonstige Kennzahlen		2000	2001	2002	2003	2004
Personal						
	Anzahl Mitarbeiter (in Ganztageskraft) techn. Personal					
	Anzahl Mitarbeiter (in Ganztageskraft) sonstiges Personal					
	Leasingpersonal und freie Mitarbeiter					
	Gesamt					
Anzahl Zertifikate						
	Anzahl nicht qualifizierte Zertifikate					
	Anzahl qualifizierte Zertifikate					
	Gesamt					
Anzahl Registrierungsstellen						

Telekom-Control-Kommission
Mariahilfer Straße 77–79, 1060 Wien
Tel. +43/1/58058-0, Fax: +43/1/58058-9191
http://www.signatur.rtr.at/, signatur@signatur.rtr.at

Beilage zur Anzeige nach § 6/§ 12 SigG: Unterstützte technische Komponenten zur Erzeugung sicherer elektronischer Signaturen

Name des Zertifizierungsdiensteanbieters

Bezeichnung des Zertifizierungsdienstes/der Zertifizierungsdienste, für welche die in der folgenden Liste angeführten technischen Komponenten eingesetzt, bereitgestellt oder empfohlen werden

---

Maßgebliches Datum, ab dem die folgende Liste Anwendung findet

---

Bitte vervielfältigen Sie den folgenden Abschnitt entsprechend oft.

Komponente

Bezeichnung der Komponente

Bitte geben Sie den Hersteller, die exakte Produktbezeichnung und die Versionsnummer an.

Beschreibung der Komponente

Z. B. „Als Secure Signature Creation Device (SSCD) evaluierte Chipkarte“, „Chipkartenleser mit eigenem Pinpad und Display“, „Clientsoftware zur sicheren Pin-Eingabe“, „Secure Viewer zur Darstellung des Dokumentenformates ...“

Bescheinigung

Bitte geben Sie die Bestätigungsstelle bzw. gleichwertige Stelle an, welche die Komponente bescheinigt hat, das Datum und die Bezugszahl der Bescheinigung. Bitte legen Sie auch eine Ausfertigung oder Kopie der Bescheinigung und des Prüfberichtes bei (wird von der Aufsichtsstelle nicht veröffentlicht).

Telekom-Control-Kommission
Mariahilfer Straße 77–79, 1060 Wien
Tel. +43/1/58058-0, Fax: +43/1/58058-9191
http://www.signatur.rtr.at/, signatur@signatur.rtr.at

Beilage zur Anzeige nach § 6/§ 12 SigG: Unterstützte Dokumentenformate für sichere elektronische Signaturen

Name des Zertifizierungsdiensteanbieters

Bezeichnung des Zertifizierungsdienstes/der Zertifizierungsdienste, bei welchen die in der folgenden Liste angeführten Dokumentenformate unterstützt werden

---

Maßgebliches Datum, ab dem die folgende Liste Anwendung findet

---

Bitte vervielfältigen Sie den folgenden Abschnitt entsprechend oft.

Dokumentenformat

Bezeichnung und Versionsnummer

Spezifikation des Formates

Geben Sie Autoren, Titel und eine allgemein zugängliche Fundstelle (z. B. URI) der Spezifikation an. Bitte legen Sie bei der erstmaligen Anzeige des Dokumentenformates die Spezifikation bei.

Komponenten (Viewer), welche dieses Format unterstützen

Bitte geben Sie an, welche der auf der Liste „Unterstützte technische Komponenten“ angeführten Komponenten (Viewer) dieses Dokumentenformat unterstützen.