# Vorblatt

**Problem**

Die Entwicklung des Signaturwesens auf der europäischen Ebene und die bisherigen Erfahrungen mit der Vollziehung des Signaturrechts durch die Aufsichtsstelle (Telekom Control Kommission und die RTR GmbH) sowie das als Bestätigungsstelle fungierende Zentrum für Sichere Informationstechnologie Austria (A-SIT) erfordern einige Anpassungen der Signaturverordnung.

**Ziel**

Die Verordnung soll an die technischen Normen und Standards, die in jüngster Zeit auf europäischer Ebene erarbeitet worden sind, angeglichen werden. Zudem soll sie tunlichst vereinfacht werden.

**Inhalt**

Die Vorgaben der Signaturverordnung über die Anforderungen an Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, sowie an sichere Signaturerstellungseinheiten werden an die in der Entscheidung der Kommission vom 14. Juli 2003, ABl. Nr. L 175 vom 15. Juli 2003, S. 45, genannten Referenznummern über die Systemsicherheit, die kryptografischen Module sowie die sicheren Signaturerstellungseinheiten angeglichen. Zudem werden ua. für Signaturerstellungsdaten Anforderungen vorgesehen, die einem vom Europäischen Institut für Telekommunikationsnormen (ETSI) erarbeiteten Standard entsprechen. Darüber hinaus sollen einige Vollzugserfahrungen der Aufsichtsstelle und der bisher zugelassenen Bestätigungsstelle berücksichtigt werden.

**Kosten**

Das Vorhaben wird zu keiner Kostenbelastung der öffentlichen Haushalte führen.

**Auswirkungen auf den Wirtschaftsstandort und die Beschäftigung**

Die Novelle kann sich auf den Wirtschaftsstandort und die Beschäftigung in diesem speziellen Bereich nicht negativ auswirken. Die Angleichung der österreichischen Vorgaben an die auf europäischer Ebene maßgeblichen Standards trägt im Gegenteil zur Konkurrenzfähigkeit der in diesem Bereich tätigen österreichischen Unternehmen bei.

**Aspekte der Deregulierung**

Der Entwurf berührt die in Art. 1 § 1 Abs. 1 des Deregulierungsgesetzes 2001 genannten Anliegen nicht. Die geplante Vereinfachung der Signaturverordnung soll das Verständnis dieses Rechtsbereichs erleichtern.

**Besonderheiten des Normerzeugungsverfahrens**

Der vorliegende Entwurf wird unter einem der Europäischen Kommission auf der Grundlage des Notifikationsgesetzes 1999 notifiziert.

**Vereinbarkeit mit dem Gemeinschaftsrecht**

Der Entwurf trägt der jüngsten Entwicklung auf der Ebene der Europäischen Gemeinschaft Rechnung.

## Allgemeiner Teil

Das Europäische Komitee für Normung (CEN) und das Europäische Institut für Telekommunikationsnormen (ETSI) haben im Rahmen der „Europäischen Initiative zur Normung elektronischer Signaturen“ (EESSI) Normen für elektronische Signaturprodukte auf der Grundlage der Anhänge zur Signaturrichtlinie erarbeitet. Die Europäische Kommission hat mit der Entscheidung vom 14. Juli 2003, ABl. Nr. 175 vom 15. Juli 2003, S 45, gemäß Art. 3 Abs. 5 der Signaturrichtlinie „Referenznummern“ für die Normen festgelegt, die den Anhängen II (F) und III der Signaturrichtlinie entsprechen. Darüber hinaus hat das ETSI ein „Algorithmenpapier“ erarbeitet, in dem ua. weitere technische Anforderungen an Signaturprodukte enthalten sind (ETSI SR 002 176 V1.1.1 2003-03, Reference DSR/ESI-000016, „Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures). Diese Normen und das „Algorithmenpapier“ sollen in die Signaturverordnung eingebaut werden, um das österreichische Signaturrecht an die internationale Entwicklung auf diesem Gebiet anzupassen und um den Anforderungen des Art. 3 Abs. 5 der Signaturrichtlinie nachzukommen.

Diese Notwendigkeit zur Änderung der Verordnung eröffnet die Möglichkeit, einige Schwächen der Signaturverordnung zu beheben. Dabei kann auf die bisherigen Erfahrungen der Telekom Control Kommission und der RTR GmbH (Aufsichtsstelle) einerseits sowie auf die Beobachtungen des Zentrums für Sichere Informationstechnologie A-SIT (Bestätigungsstelle) andererseits zurückgegriffen werden. Diese Änderungen der Verordnung betreffen insbesondere das Verfahren vor der Telekom Control GmbH bzw. der RTR GmbH als Aufsichtsstelle, aber auch die rechtlichen Anforderungen an Signaturerstellungsdaten für sichere elektronische Signaturen, an Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, und an die von der Aufsichtsstelle verwendeten Signaturen sowie technischen Komponenten und Verfahren.

Die geplanten Änderungen sollen nicht zuletzt dazu beitragen, die Verordnung in ihrem normativen Teil leichter lesbar und damit verständlicher zu gestalten. Die technischen Belange werden vornehmlich im Anhang geregelt, der an die Stelle der bisherigen Anhänge 1 und 2 treten soll. Dabei sollen die von ETSI ausgearbeiteten Normen für Algorithmen und Parameter in das österreichische Signaturrecht übernommen werden.

## Besonderer Teil

**Zu Z 1 (Inhaltsübersicht)**

Die Inhaltsübersicht soll auf Grund der vorgeschlagenen Änderungen einiger Überschriften geändert werden.

**Zu den Z 2 (§ 1 SigV)**

Eine übersichtlichere Darstellung der gebührenpflichtigen Leistungen der Aufsichtsstelle war Ziel der Neufassung des Abs. 1. Weiters wird klargestellt, dass die (verhältnismäßig hohen) Gebührenansätze von 6 000 und 4 000 Euro nur für Zertifizierungsdiensteanbieter gelten, die qualifizierte Zertifikate ausstellen oder sichere elektronische Signaturverfahren bereitstellen. Weiters werden Gebühren für sichere Zeitstempeldienste vorgegeben, die unter jenen für Zertifizierungsdienste betr. sichere Signaturen liegen, da die Aufsicht für Zeitstempeldienste technisch weniger aufwendig ist.

Von der Entrichtung einer Gebühr von 2 Euro pro ausgestelltem qualifiziertem Zertifikat (§ 1 Abs. 2 SigV) soll in Zukunft Abstand genommen werden, weshalb Abs. 2 entfallen soll: Diese Gebühr bewirkt einen nicht unwesentlichen Wettbewerbsnachteil einheimischer Zertifizierungsdienste, was im Extremfall zu einer Abwanderung der Zertifizierungsdienste in das EU-Ausland führen könnte – ein Effekt, der zu vermeiden ist.

**Zu den Z 3 und 4 (§ 2 SigV)**

In § 2 Abs. 1 wird klargestellt, dass das Mindestkapital auch gegeben sein muss, wenn der Zertifizierungsdiensteanbieter sichere elektronische Signaturverfahren bereitstellt.

In § 2 Abs. 2 wird klargestellt, dass die Haftpflichtversicherung nach § 6 Abs. 2 SigG mindestens drei Versicherungsfälle im Jahr decken muss. Ist das Haftungsrisiko des Zertifizierungsdiensteanbieters nachweislich geringer als die geforderte Mindestversicherungssumme von 1 000 000 Euro, so kann eine entsprechend geringere Versicherungssumme als ausreichend angesehen werden. Derart geringere Haftungsrisiken des Zertifizierungsdiensteanbieters können sich nach § 23 Abs. 4 SigG durch eingeschränkten Anwendungsbereich oder Transaktionswert des qualifizierten Zertifikats ergeben. Mit der Möglichkeit geringerer Deckungssummen wurde im Sinne von der EU Kommission im Notifizierungsverfahren aufgezeigten Bedenken ein potentielles Markteintrittshemmnis für kleinere Diensteanbieter ausgeräumt.

In § 3 Abs. 3 wurde die Ausnahme von der Haftpflichtversicherung um die Träger der Sozialversicherungen, die die e-card betreiben, erweitert.

**Zu Z 5 (§§ 3 – 7)**

Unter den „technischen Komponenten und Verfahren für die Erzeugung sicherer Signaturen“ sind nur jene zu verstehen, die den Vorgang der Signaturerzeugung selbst betreffen, d.h. die bewirken, dass „elektronische Daten anderen elektronischen Daten beigefügt oder mit ihnen logisch verknüpft werden“ (§ 2 Z 1 SigG). Die Anwendung der Autorisierungscodes oder die Anzeige der zu signierenden Daten geschieht hingegen in der Systemumgebung der Signaturerstellungseinheit; dies sind somit Vorgänge, die von der „Erzeugung der elektronischen Signatur“ zu unterscheiden sind. Eine Prüfung der hiefür eingesetzten technischen Komponenten ist daher durch § 18 Abs. 5 SigG auch nicht vorgeschrieben. Diese Sichtweise steht auch im Einklang mit dem relevanten Gemeinschaftsrecht: EG 15 der RL 93/99/EG führt Folgendes aus: „Anhang III enthält die Anforderungen für die sichere Signaturerstellungseinheiten zur Gewährleistung der Funktionalität fortgeschrittener elektronischer Signaturen. Er deckt nicht die gesamte Systemumgebung ab, in der die Einheit betrieben wird“. Auch Art. 3 Abs. 4 der RL bezieht sich einzig auf Anhang III – eine darüber hinaus gehende Verpflichtung zur Prüfung von Komponenten zur Signaturerstellung ist nicht vorgesehen. Der Umstand, dass sich die Prüfung der technischen Komponenten auf die Signaturerstellungseinheit beschränkt und Komponenten der Systemumgebung nach § 4 (z.B. Viewer oder Chipkartenleser) keiner Bescheinigung oder Prüfung durch eine Bestätigungsstelle oder die Aufsichtsstelle bedürfen, entbindet den Zertifizierungsdiensteanbieter nicht davon, den Signator nach § 20 Abs. 3 SigG über derartige geeignete Komponenten zu unterrichten.

Die Komponenten und Verfahren, die für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung sicherer Signaturen eingesetzt werden, müssen den Anforderungen des § 9 und damit auch den von der Europäischen Kommission mitgeteilten Referenznummern entsprechen (§ 3 Abs. 1). Signaturerstellungsdaten für sichere elektronische Signaturen müssen künftig die Vorgaben des Anhangs erfüllen, der die von ETSI erarbeiteten Standards enthält (§ 3 Abs. 2).

§ 3 Abs. 3 lässt es zu, dass Signaturerstellungsdaten für sichere elektronische Signaturen auf mehrere Signaturerstellungseinheiten verteilt werden dürfen. Die Sicherheitsanforderungen müssen in einem solchen Fall durch die Gesamtheit dieser Einheiten erfüllt werden.

§ 4 Abs. 1 regelt ein Erfordernis, das für die Sicherheit des Konzepts der elektronischen Signatur wesentlich ist, nämlich die Möglichkeit für den Signator, vor Auslösen des Signaturmechanismus zu sehen, was er zu signieren im Begriffe ist. Es wird weiters klargestellt, dass die Formate der zu signierenden Daten so spezifiziert sein müssen, dass die Darstellung sowohl vor der Erstellung der sicheren Signatur durch den Sinator, als auch bei späterer Prüfung der signierten Daten zum selben Ergebnis kommt.

§ 4 Abs. 2 präzisiert die Anforderungen an die Systemumgebung der Signaturerstellungseinheit hinsichtlich des Auslösens der sicheren Signatur. Das Auslösen mehrerer sicherer Signaturen erfordert, dass dieser Umstand bzw. die Anzahl der auszulösenden Signaturen dem Signator bekannt gegeben wird (§ 4 Abs. 2 zweiter Satz). Es wird dabei klargestellt, dass die Autorisierungscodes nur so lange im Speicher verbleiben dürfen, wie dies für den Signaturvorgang selbst notwendig ist (§ 4 Abs. 2 vierter Satz). Ein Verwechseln der Funktion „sichere Signatur“ mit anderen Anwendungen (z.B. Bankomatfunktion) oder ein unbewusstes Auslösen einer sicheren Signatur wird verhindert, indem für die sichere Signatur andere Autorisierungscodes vorzusehen sind (§ 4 Abs. 2 dritter Satz) oder Eingabeerleichterungen (z.B. ein Speichern einer PIN über den eigentlichen Signaturvorgang hinaus) ausgeschlossen werden.

§ 5 regelt die Anforderungen an Signaturerstellungsdaten von Anbietern, die qualifizierte Zertifikate ausstellen. Für die Algorithmen und deren Parameter für qualifizierte Zertifikate verweist Abs. 1 letzter Satz auf den Anhang, der die von ETSI erarbeiteten Standards enthält. Die Vorgaben des Abs. 1 gelten nicht für alle Signatur- und Zertifizierungsdienste eines solchen Anbieters, sondern nur für die diejenigen Dienste, mit denen qualifizierte Zertifikate erbracht werden. Gleiches gilt für andere Regelungen der Verordnung, die sich an solche Zertifizierungsdiensteanbieter richten. Abs. 2 stellt weiters klar, dass der Zertifizierungsdiensteanbieter in der Lage sein muss, die sichere elektronische Signatur, die auf seinem qualifizierten Zertifikat beruht, zu prüfen. Dass es sich dabei um eine „sichere“ Prüfung handelt, wird nicht mehr verlangt.

Zu einem Signaturalgorithmus gehört jeweils ein passender Prüfalgorithmus, der die gleichen Verfahren verwendet - für RSA z.B. SHA1 etc.

§ 6 regelt die besonderen Vorkehrungen an die Signaturerstellungsdaten der Aufsichtsstelle für die sicheren elektronischen Signaturen, die sie nach § 13 Abs. 3 SigG vorletzter Satz zur Führung der Verzeichnisse (z.B. Verzeichnis der Zertifikate der Zertifizierungsdiensteanbieter) verwendet. Auch werden der Aufsichtsstelle eigene Vorgaben für die von ihr verwendeten Systeme gemacht.

In § 7 wurde die bisherig zwingende Forderung eines Zweitsystems aufgegeben. Dies eliminiert zukünftig einen Kostenfaktor der Aufsicht, nachdem aus einer Äußerung der EU Kommission im Notifizierungsverfahren die Gebühren der Aufsicht, die nach § 13 Abs. 4 SigG kostendeckend sein müssen, als zu hoch angesehen werden.

**Zu Z 6 (§ 9 SigV):**

Abs. 1 und Abs. 2 nehmen auf die von der Kommission getroffenen „Feststellungen" Bedacht (siehe dazu die allgemeinen Ausführungen der Erläuterungen). In der Prüfung sind Sicherheitsvorgaben anzuwenden, die von einer Bestätigungsstelle als geeignet anerkannt werden (Abs. 1 erster Satz). Schutzprofile nach den Common Criteria oder Sicherheitsvorgaben nach ITSEC stellen dabei die in der Praxis wesentlichen Normen dar, sind jedoch in Abs. 1 zweiter Satz nicht taxativ aufgezählt, um etwaige Alternativen zu ermöglichen. Gleiches gilt für die bei Zertifizierungsdiensteanbietern eingesetzten vertrauenswürdigen Systeme zur Erstellung von qualifizierten Zertifikaten oder Signaturerstellungsdaten des Signators (Abs. 1 letzter Satz). Jedenfalls sind die Referenznummern nach § 9 Abs. 2 zu beachten.

Die Prüfung der Komponenten und Verfahren in einer kontrollierten Umgebung tritt nach Abs. 3 an die Stelle der in Abs. 1 genannten Erfordernisse. Geht es dabei um den Einsatz technischer Komponenten und Verfahren für die Erstellung sicherer elektronischer Signaturen, so handelt es sich beim Ergebnis des Berichtes um eine Bescheinigung nach § 18 Abs. 5 SigG. Geht es dagegen um den Einsatz technischer Komponenten und Verfahren bei Zertifizierungsdiensteanbietern, die qualifizierte Zertifikate ausstellen (s. § 7 Abs. 2 SigG), so ist das Prüfergebnis der Bestätigungsstelle als Gutachten im verwaltungsverfahrensrechtlichen Sinn zu werten. Die in Abs. 3 genannten organisatorischen bzw. technisch-organisatorischen Maßnahmen müssen den Sicherheitsanforderungen entsprechen, die die in Abs. 1 genannten Instrumente vorsehen, dies auch dann, wenn die Maßnahmen nach Abs. 3 im Einzelfall nicht den in Abs. 1 genannten Instrumenten entsprechen. Es bleibt einem Zertifizierungsdiensteanbieter im Übrigen unbenommen, nur evaluierte Produkte zu empfehlen.

Abs. 4 regelt, dass die Bestätigungsstelle dann etwaige für die Bescheinigung herangezogene oder erstellte Prüfberichte an die Aufsichtsstelle zu übermitteln hat, wenn diese Berichte der Bestätigungsstelle zugänglich sind und die Weitergabe zulässig ist.

**Zu den Z 7 - 9 (§ 10 SigV)**

Die Änderung des Abs. 2 dient der Behebung eines redaktionellen Versehens. Die Anpassung des ersten Satzes des Abs. 6 nimmt auf den Umstand Bedacht, dass Signaturerstellungsdaten auch bei der Produktion der Signaturerstellungseinheit erzeugt werden können. In Abs. 7 wird die bisher in § 7 Abs. 3 letzter Satz enthaltene Belehrungspflicht zu Maßnahmen zur Auslösung der Signaturfunktion übernommen.

**Zu Z 10 (§ 11 Abs. 1 SigV):.**

Der bisherige § 11 Abs. 1 soll mehr Möglichkeiten des elektronischen Nachweises der Identität bieten. Die im Zusammenhang mit der Identitätsfeststellung erforderliche Dokumentation kann elektronisch beispielsweise durch die Dokumentation der Ausweisdaten erfolgen (z.B. durch Auslesen einer maschinenlesbaren Zone im Ausweis oder durch die Kopie elektronischer Ausweiselemente (Chipinhalte) durch entsprechende Lesegeräte). Auch die manuelle Eingabe der zu dokumentierenden Daten ist zulässig, wenn eine entsprechende Prüfung der Vollständigkeit und Richtigkeit vorgesorgt ist.

Ist der Antrag elektronisch signiert, ist die sichere Signatur samt dem zugehörigen Zertifikat in die Dokumentation aufzunehmen.

**Zu Z 11 (§ 12 SigV)**

Auch diese Änderungen ergeben sich im Wesentlichen aus der Übernahme der wesentlichen Teile des „Algorithmenpapiers" in den Anhang der Verordnung. Formate im Sinn des Abs. 2 sind beispielsweise ASN.1 und XML. Aus der Änderung ergibt sich auch, dass erkennbar sein muss, ob ein qualifiziertes Zertifikat vorliegt oder nicht (s. § 5 Abs. 1 SigG). Das ist mit dem Ausdruck *„vollständig"* gemeint. Aus der vom Verordnungstext verlangten vollständigen Spezifikation muss zweifelsfrei hervorgehen, mit welchen Verfahren (Signatur und Hash Verfahren) das Zertifikat erstellt wurde. Diese Signaturverfahren können durchaus andere sein als die Signaturverfahren des Signators. Es ist z.B. durchaus sinnvoll und zulässig, dass ein Zertifizierungsdiensteanbieter alle seine Zertifikate mit der gleichen Signatur (aus der Sicht des Algorithmus) versieht und dennoch gemischte Verfahren (z.B. RSA bzw. ECDSA) anbietet. Für Standard X.509-Zertifikate stellt sich diese Frage in der Regel nicht, da entsprechende Beschreibungsfelder im Zertifikat fixiert sind.

Mit der teilweisen Streichung des bisherigen Abs. 3 ist keine inhaltliche Änderung intendiert.

Die Erhöhung der maximalen Gültigkeitsdauer qualifizierter Zertifikate von fünf Jahren trägt dem Umstand Rechnung, dass die Ausgabepraxis von Chipkarten mit einer Gültigkeitsdauer von z.B. drei Kalenderjahren (etwa Bankomatkarte) eine darüber hinausgehende Verwendungsdauer der Karte erfordert.

In Abs. 4 wird klargestellt, dass diese Regelung nur für qualifizierte Zertifikate gilt, die zu Signaturzwecken ausgestellt werden. Nicht davon betroffen sind qualifizierte Zertifikate, die von der Aufsichtsstelle ausgestellt werden können (s. § 13 Abs. 3 drittletzter Satz SigG).

Abs. 4 erlaubt neben der Gültigkeitsdauer die Änderung der eindeutigen Kennung (Seriennummer) des Zertifikats bei dessen Neuausstellung. Dies berücksichtigt diesbezügliche Vorgaben in maßgeblichen Standards, dass jedes Zertifikat eine eindeutige Seriennummer aufweisen muss.

**Zu den Z 12 und 13 (§ 13 SigV)**

Widerrufsdienste müssen auch die Feststellung zulassen, ob eine Signatur im bestimmten Zeitpunkt der Erstellung gültig war oder ob das Zertifikat widerrufen war (§ 13 Abs. 1).

Die bisherige Frist von drei Werktagen erwies sich in der Praxis als zu kurz. Es war oft nicht möglich, die erforderlichen Nachweise innerhalb der drei Tage zu erhalten (§ 13 Abs. 7).

**Zu Z 14 (§ 14 SigV)**

In der ersten Novelle des SigG (BGBl. I Nr. 137/2000) wurde für die in der Erstfassung des SigG (BGBl. I Nr. 190/1999) enthaltene Vorschrift, dass qualifizierte Zertifikate mit der sicheren Signatur des Zertifizierungsdiensteanbieters versehen sein müssen, auf fortgeschrittene Signaturen im Sinne der Signaturrichtlinie zurückgenommen. Derselben Logik folgend sind auch sichere Zeitstempeldienste nicht notwendigerweise einem qualifizierten Zertifikat zu unterstellen. In § 14 Abs. 1 werden die technischen Bedingungen für sichere Zeitstempeldienste angelehnt an Zertifizierungsdienste für qualifizierte Zertifikate definiert. Da Zeitstempeldienste nicht unbedingt auf Zertifikaten basieren müssen, werden besondere Bedingungen für die zertifikatsbasierten Fälle aufgestellt.

Der Zertifizierungsdiensteanbieter muss - bei nicht-zertifikatsbasierten Zeitstempeldiensten - im Sicherheitskonzept auch angeben, welche Sicherheitsmaßnahmen zur automatischen Auslösung der Zeitstempelfunktion vorgesehen sind.

**Zu den Z 15 - 18 (§ 15 SigV)**

Zunächst wird klargestellt, dass die vorgesehenen Anforderungen nur für Anbieter, die qualifizierte Zertifikate ausstellen, gelten (Einleitungssatz des Abs. 1). Weiters wird in § 15 Abs. 1 Z 15 ein Redaktionsversehen behoben. In Abs. 2 werden besondere Anforderungen an Sicherheitskonzepte für Zeitstempeldienste vorgesehen. Abs. 3 entspricht dem geltenden Abs. 2.

**Zu Z 19 (§ 16 SigV)**

Die Änderung passt die Verordnung an die mit der Signaturgesetz-Novelle BGBl. I Nr. 137/2000 geschaffene Rechtslage an.

**Zu Z 20 (§ 17 SigV)**

Die Änderung nimmt auf die vorgeschlagene Anfügung nur eines Anhangs Bedacht.

Abs. 2 trägt dem Umstand Rechnung, dass auch über Zeitstempel der Sicherheitswert eines signierten Dokuments trotz im Lauf der Zeit schwächer werdender Algorithmen erhalten werden kann.

**Zu den Z 21 - 24 (§ 18 SigV)**

Nach Abs. 1 soll an die Stelle des RTF-Formats das XML-Format (mit Darstellungsfunktion) treten. In Abs. 2 wird klargestellt, dass es in diesem Zusammenhang nur um die Anzeige der Aufnahme einer Tätigkeit für qualifizierte Zertifikate geht. Auch soll sich die periodische Prüfpflicht der Aufsichtsstelle nach Abs. 4 nur auf Anbieter, die qualifizierte Zertifikate ausstellen, erstrecken. In Abs. 6 wird schließlich auf den Umstand Bedacht genommen, dass der bisherige Anhang 2 entfällt.

**Zu Z 25 (§ § 19 SigV)**

Die Bestimmung nimmt auf die Notifikation der Novelle Bedacht.

**Zu Z 26 (§§ § 20 - 22 SigV)**

Zur Erleichterung der Auffindbarkeit der maßgeblichen technischen Referenztexte wird die Aufsichtsstelle verpflichtet, auf ihrer Homepage jeweils aktuelle Darstellungen bzw. Verweise zu veröffentlichen.

Es empfiehlt sich, anlässlich der Novelle eine In-Kraft-Tretens-Regelung vorzusehen. Bescheinigungen einer Bestätigungsstelle, die vor dem In-Kraft-Treten der Novelle ausgestellt worden sind, sollen weiterhin wirksam bleiben.

**Zum Anhang:**

Die im vorliegenden Anhang festgelegten Algorithmen und Parameter richten sich nach dem ALGO Papier („Algorithmenpapier“), welches im Ausschuss für elektronische Signaturen (A9C) nach der Signatur-Richtlinie diskutiert wurde.

Dieses Papier ist implizit auch Teil der in § 9 angesprochenen „Protection Profiles“ (SSCD), da ein konkretes Signaturerstellungsgerät ohne Algorithmen nicht funktionsfähig ist. Es wurden daher bewusst die Erläuterungen und näheren Bestimmungen aus dem derzeit aktuellen ALGO Papier (Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures", ETSI SR 002 176, V1.1.1; 2003-03) im Anhang nicht wiederholt.

Vielmehr listet der Anhang die grundsätzlichen Algorithmen auf und gibt die verbindlichen Tabellen wieder; dadurch können in flexibler Weise in die Verordnung durch Novellierung die jeweils aktuellen Gültigkeitsdaten und Algorithmen bzw. Signatursuiten eingebracht werden, ohne die Übersichtlichkeit der Darstellung zu gefährden.

Da gerade im Sicherheitsbereich neue Entwicklungen und Erkenntnisse eine besondere Rolle spielen, ist der Anhang – so wie dies § 3 Abs. Abs. 2 ausdrücklich anordnet – so zu verstehen, dass bei seiner Umsetzung der jeweilige Stand der Technik immer mitbedacht werden muss. In diesem Sinne wurden die Gültigkeitszeiträume des ursprünglichen Algorithmenpapiers, dessen inhaltliche Basis am Stand der Technik aus 2001aufsetzt, im Anhang nicht wiedergegeben. Werden Algorithmen für sichere Signaturen als anerkannte Normen gemeinschaftsrechtlich im Sinne Art. 3 Abs. 5 der Signaturrichtlinie als Referenznummern vorgegeben, sind diese nach § 18 Abs. 6 SigG jedenfalls zu beachten. Ebenso wäre bei einem über Technologiebeobachtung zu vermutenden Sicherheitsverlust einer angegebenen Signatursuite oder ihrer Komponenten national ein Nachziehen der SigV erforderlich, um diesem Umstand Rechnung zu tragen. Anbieter von Signaturprodukten für sichere Signaturen sind deshalb angehalten, bei Verwendung der angegebenen Signatursuiten zu berücksichtigen, dass dem Stand der Technik nach § 3 Abs. 2 zu entsprechen ist und gemeinschaftsrechtliche Vorgaben oder technische Entwicklungen kurzfristig ein entsprechend höheres Sicherheitsniveau erforderlich machen können.