Begründung

zur
Verordnung zur elektronischen Signatur

(Entwurf)

A. Allgemeiner Teil

Die Verordnung enthält die erforderlichen Bestimmungen zur Ausgestaltung des Signaturgesetzes (SigG) gemäß der Verordnungsermächtigung nach § 24 SigG. Sie löst die Verordnung zur digitalen Signatur vom 22. Oktober 1997 ab.

Es werden in der Verordnung insbesondere die Vorgaben des SigG zu den strukturellen Anpassungen aufgrund der EG-Signaturrichtlinie 1999/93/EG sowie hinsichtlich der freiwilligen Akkreditierung näher ausgestaltet. Es sind außerdem die Erkenntnisse aus der Evaluierung des bis 21. Mai 2001 geltenden Signaturgesetzes von 1997 und seiner Verordnung (Bericht der Bundesregierung BT-Drs 14/1191 v. 18.6. 1999) in die Bestimmungen eingeflossen. Die Regelungen ermöglichen eine dynamische Aufnahme der Vorgaben für Produkte für qualifizierte elektronische Signaturen aufgrund der Festlegungen nach der EG-Signaturrichtlinie. Sie legen außerdem für Produkte, die von akkreditierten Zertifizierungsdiensteanbietern eingesetzt werden, bestimmte Anforderungen fest, die als Option für den Markt dem Erhalt des anerkannten hohen Sicherheitsniveaus aufgrund der bisher geltenden Regelungen des Signaturgesetzes und der Signaturverordnung von 1997 dienen.

B. Besonderer Teil

Zu § 1

Ermächtigungsgrundlage der Vorschrift ist § 24 Nr. 1 i.V.m. § 4 Abs. 3 SigG.

Zu Abs. 1:

Die Vorschrift dient der Rechtssicherheit des Anzeigenden. Die Anzeige kann schriftlich erfolgen oder alternativ hierzu auch mit einer elektronischen Signatur nach dem Signaturgesetz versehen sein.

zur Veröffentlichung freigegeben

Zu Abs. 2

Die Vorschrift enthält die Mindestangaben des Zertifizierungsdiensteanbieters gegenüber der zuständigen Behörde, die für die Durchführung einer effizienten Aufsicht nach Maßgabe des Art. 3 Abs. 3 EGSRL erforderlich sind.

Der Nachweis der Führungszeugnisse nach Nr. 3 des Absatzes dient der Feststellung der Zuverlässigkeit des Zertifizierungsdiensteanbieters und der für ihn handelnden Personen nach Maßgabe der allgemeinen Anforderungen von Anh. II Buchst. a) EGSRL.

Eine dem in Nr. 4 genannten Handelsregisterauszug vergleichbare Unterlage ist z.B. ein Auszug aus dem Genossenschaftsregister.

Der Nachweis der Fachkunde nach Nr. 5 setzt die Anforderungen des Anhangs II Buchst. e) EGSRL um. Es handelt sich um den Kern des Kompetenznachweises des Zertifizierungsdiensteanbieters. Die Fachkunde kann insbesondere durch Zeugnisse der beruflichen und fachlichen Qualifikation nachgewiesen werden; möglich ist auch ein Nachweis in anderer Form, z.B. durch einschlägige Publikationen der vom Anbieter eingesetzten Personen. Zur Fachkunde zählen neben den theoretischen Kenntnissen insbesondere auch praktische Erfahrungen auf dem Gebiet der Technologie elektronischer Signaturen und Vertrautheit mit entsprechenden Sicherheitsverfahren sowie betriebswirtschaftliche Kenntnisse. Außerdem muss als Mindestvoraussetzung juristischer Fachverstand in bezug auf die Erfüllung der Anforderungen von Signaturgesetz und dieser Verordnung bestehen; die juristische Fachkunde kann auch mittels Hinzuziehung entsprechender Anwälte bzw. Fachanwälte, die vom Zertifizierungsdiensteanbieter zu benennen sind, erfüllt werden.

Der Nachweis nach Nr. 6 betrifft die genaue Darlegung des in § 2 näher beschriebenen Sicherheitskonzepts. Wegen der umfassenden Übertragungsmöglichkeiten von Aufgaben an Dritte und zur Sicherstellung einer effizienten Aufsicht durch die zuständige Behörde wurden diese Angaben unter Nr. 6 aufgenommen. Diese Darlegungen sind Voraussetzung dafür, dass die Behörde aufgrund der eingereichten Unterlagen zunächst eine allgemeine Schlüssigkeitsprüfung dahingehend durchführen kann, ob und inwieweit der Zertifizierungsdiensteanbieter die Vorgaben aus

dem Signaturgesetz und dieser Verordnung erfüllt und in welchen Fällen noch weitere Unterlagen nachzureichen oder gegebenenfalls Prüfungen vor Ort zu veranlassen sind.

Der Nachweis der Deckungsvorsorge nach Nr. 7 setzt Anhang II Buchs. h) EGSRL um, wonach Zertifizierungsdiensteanbieter über ausreichende Finanzmittel verfügen müssen. Zu den Einzelheiten der vorzulegenden Nachweise wird auf § 9 und die Ausführungen verweisen.

Die Vorschrift des Satzes 2 dient der Sicherstellung der Informationen über den Zertifizierungsdiensteanbieter, die zur Aufrechterhaltung der Aufsicht erforderlich sind; dies sind die Angaben zu Nr. 1 und zu Nr. 6. Zu meldende sicherheitserhebliche Änderungen im Bereich des Zertifizierungsdiensteanbieters betreffen alle Umstände, die in § 2 umschrieben sind soweit diese der Schwere nach einen nicht unerheblichen Einfluß auf die Aufrechterhaltung eines ordnungsgemäßen Betriebes haben.

zu Abs. 3

Soweit Teile eines Zertifizierungsdienstes im Ausland betrieben werden, ist dies im Grundsatz (Ausnahme: akkreditierte Zertifizierungsdiensteanbieter) nur in Staaten nach § 23 Abs. 1 Satz 1 SigG sowie in Drittstaaten unter den Bedingungen des § 23 Abs. 1 Satz 3 SigG zulässig.

Der Zertifizierungsdiensteanbieter muß in allen Staaten, in denen er niedergelassen ist, sicherstellen, dass er einer dem SigG gleichwertigen Aufsicht unterliegt. Unterliegt der Anbieter einer Aufsicht in einem Mitgliedstaat der EU oder des EWR so ist im Grundsatz die Gleichwertigkeit der Aufsicht zu unterstellen, es sei denn, diese ist noch nicht in Konformität mit der Richtlinie eingerichtet. Im übrigen bleibt die Möglichkeit, nach § 23 Abs. 2 Satz 2 Nr. 2 SigG-E für einen anderen Zertifizierungsdiensteanbieter in einem Drittstaat einzustehen, unberührt.

Bei nach § 15 SigG akkreditierten Zertifizierungsdiensteanbietern – die regelmäßigen Prüfungen durch nach § 18 anerkannte private Prüf- und Bestätigungsstellen unterliegen – ist es grundsätzlich unerheblich, in welchem Staat sie niedergelassen sind (vgl. auch Begründung zu § 23 Abs. 2 SigG).

Zu § 2

Ermächtigungsgrundlage der Vorschrift ist § 24 Nr. 1 i.V.m. § 4 Abs. 2 Satz 4 SigG.

Mit der Vorschrift werden die Anforderungen des Anhangs II EGSRL, wie sie im SigG und dieser Verordnung umgesetzt sind, in allgemeiner Form beschrieben. Sie dienen dem Zertifizierungsdiensteanbieter der Orientierung und Information über die notwendigen Anforderungen zur Einhaltung der rechtlichen Vorgaben für den Betrieb, insbesondere im Antragsverfahren. Der Begriff "Sicherheitskonzept" greift auf die Formulierung des § 12 der Signaturverordnung vom 1. November 1997 (im Folgenden: SigV 97) zurück, die eine allgemeine Beschreibung der Voraussetzungen nach Signaturgesetz und Verordnung ist. Sofern eine Prüf- und Bestätigungsstelle nach § 18 SigG bereits das Sicherheitskonzept überprüft hat, kann im Rahmen der Anzeige auf die entsprechenden Teile im Bericht, die die Erfüllung der Anforderungen dieser Vorschrift bestätigt und beschreibt, Bezug genommen werden.

Die in Nr. 1 beschriebenen Anforderungen umfasst die Beschreibung aller erforderlichen technisch-organisatorischen Voraussetzungen einschließlich der entsprechenden baulichen Vorkehrungen für den Betrieb eines Zertifizierungsdienstes nach Maßgabe des SigG und des Anhangs II EGSRL.

Aus der unter Nr. 2 genannten Übersicht müssen die Bezeichnung des jeweiligen Produkts, der Hersteller und die Bestätigung der Gesetzeskonformität mit einer entsprechenden Herstellererklärung nach § 17 Abs. 4 SigG hervorgehen; für akkreditierte Zertifizierungsdiensteanbieter gelten die Anforderungen nach § 15 Abs. 7 SigG.

Die unter Nr. 3 genannte Übersicht betrifft den Kern der Tätigkeit des Zertifizierungsdiensteanbieters. Der Anbieter muss darlegen, wie er die Anforderungen des Gesetzes in der Praxis umsetzt. Dies betrifft insbesondere die Tätigkeiten nach §§ 5 und 6, 8 bis 10 sowie §§ 13 und 14 SigG nach Maßgabe des Anhangs II Buchst. a) bis d), g), i) bis l) EGSRL. Im Rahmen der Ablauforganisation ist vor allem auch darzustellen, wie die zum Signieren der Zertifikate und Zeitstempel eingesetzten Signaturschlüssel vor unbefugter Nutzung und Entwendung geschützt werden. Wichtig ist auch die Darlegung der Maßnahmen zum Schutze der für ein Zertifikat bestimmten Daten vor Fälschung und Verfälschung sowie zur Wahrung der Vertraulichkeit in den Fällen, in denen die Zertifikate nach dem Willen des Betroffenen nur nachprüfbar und nicht abrufbar zu halten sind. So müssen solche Daten zwischen den Registrierungsstellen, bei denen die

Anträge auf Zertifikate gestellt werden, und dem Zertifizierungsdienst bei Online-Übertragung signiert und zuverlässig verschlüsselt übermittelt werden. Vom Zertifizierungsdienst ausgestellte Zertifikate sollten auf Übereinstimmung mit den Daten im Antrag auf ein Zertifikat überprüft werden. Soweit der Zertifizierungsdiensteanbieter Aufgaben nach § 4 Abs. 5 SigG an Dritte übertragen hat, muss aus dem Sicherheitskonzept auch hervorgehen, wie die Anforderungen des Signaturgesetzes und dieser Verordnung bei den Dritten sowie im Ablauf zwischen allen Beteiligten erfüllt werden; dies gilt auch bei Auslagerungen von Aufgaben in das Ausland.

Die unter Nr. 4 genannten Vorkehrungen sollen die jederzeitige Erfüllung der Voraussetzungen nach Gesetz und Verordnung sicherstellen - nach Maßgabe des Anhangs II Buchst. a) und b) EGSRL. Die Notfallkonzepte werden als Beispiel aufgeführt; sie umfassen insbesondere die Organisation eines 24-Stunden-Bereitschaftsdienstes, Sicherungen gegen Stromausfall, Spannungsschwankungen, Maßnahmen im Falle von Bränden, Wasserschäden oder vergleichbaren Vorfällen.

Das unter Nr. 5 genannte Verfahren dient der Sicherstellung, dass jederzeit und nicht nur bei Aufnahme des Betriebes zuverlässiges Personal zum Einsatz kommt, nach Maßgabe des § 4 Abs. 2 SigG und Anhang II Buchst. a) und c) EGSRL. Zur Beurteilung der Zuverlässigkeit des Personals bei Einstellung kommen insbesondere das polizeiliche Führungszeugnis und Zeugnisse früherer Arbeitgeber sowie der Gesamteindruck der Person in Betracht.

Die Abschätzung und Bewertung verbleibender Sicherheitsrisiken nach Nr. 6 ist notwendige Voraussetzung für die Bewertung der erforderlichen Zuverlässigkeit des Zertifizierungsdienstes nach Maßgabe des § 4 Abs. 2 SigG und Anhang II Buchst. a) und b) EGSRL. Auch bei größter Anstrengung verbleibt ein Restrisiko des Betriebsausfalls bzw. einer Betriebsstörung insbesondere im Hinblick auf die eingesetzte Technik. Hier kann insbesondere auch auf Einschätzungen seitens der Prüf- und Bestätigungsstelle und gegebenenfalls der Versicherer oder der Hersteller der eingesetzten Produkte und Technik zurückgegriffen werden.

Zu § 3

Ermächtigungsgrundlage der Vorschrift ist § 24 Nr. 1 i.V.m. § 5 Abs. 1 und 2 SigG. Sie greift auf § 3 der SigV 97 zurück.

Zu Abs. 1

Die Identifikation des Antragstellers kann im Grundsatz unverändert gegenüber der Regelung des § 3 Abs. 1 der SigV 97 mittels amtlicher Dokumente erfolgen. Da die ordnungsgemäße Identifizierung zentral für das Vertrauen in die Richtigkeit der qualifizierten Zertifikate ist, kommen als zugelassene amtliche Dokumente der Personalausweis oder der Reisepass in Betracht. Dies gilt uneingeschränkt für amtliche Dokumente aus der EU oder des EWR. Grundsätzlich sind auch Reisepässe aus Drittstaaten zur Identifizierung zulässig; bei Personalausweisen gilt dies insoweit uneingeschränkt, sofern diese für die Einreise in die Staaten des Abkommens von Schengen zugelassen sind. Weitere Dokumente zur Identifikation können in Betracht kommen, wenn diese eine den in Satz 1 genannten amtlichen Dokumenten gleichwertige Sicherheit aufweisen, wie z.B. amtliche Dokumente Staatenloser oder bestimmte Flüchtlingsausweise. Führerscheine reichen gegenwärtig mangels Aktualität der Daten nicht aus; sie sind auch kein Identifikationspapier, sondern vielmehr ein Dokument, in dem eine bestimmte Befähigung bestätigt wird. Zu den Einzelheiten der nach dieser Vorschrift zulässigen amtlichen Dokumente wird ein Leitfaden durch die betreffenden Sicherheitsbehörden erstellt, der dann von der zuständigen Behörde veröffentlicht wird. Die Identifikation erfolgt durch die Registrierungsstelle des Zertifizierungsdiensteanbieters.

Sofern ein Antrag mit einer qualifizierten elektronischen Signatur versehen ist, ist eine erneute Identifikation entbehrlich, da davon ausgegangen werden muß, daß der Antragsteller die zur Erzeugung der qualifizierten elektronische Signatur erforderliche sichere Signaturerstellungseinheit durch ordnungsgemäße Identifizierung nach § 5 Abs. 1 SigG erlangt hat.

Die Festlegung des spätesten Zeitpunkts der Identifikation nach Satz 3 ist zur Konkretisierung des Ordnungswidrigkeitentatbestandes nach § 21 Abs. 1 Nr. 3 SigG ("rechtzeitig") erforderlich.

Zu Abs. 2

Die Anpassungen gegenüber § 3 Abs. 2 der SigV 97 beruhen auf den Änderungen der Begriffe in § 2 SigG und tragen den Anliegen der Kammern im Rahmen der Evaluierung des Signaturgesetzes von 1997 (im Folgenden: SigG 97) Rechnung. Außerdem ist nun neben der Schriftform für die Bestätigung oder Einwilligung auch alternativ die Vorlage eines elektronischen Dokuments

mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz zugelassen. Die Bestätigung kann auch in Form eines (bereits vorhandenen) Zertifikates mit entsprechenden Attributen oder entsprechenden Attribut-Zertifikaten erfolgen.

Den Anliegen der Kammern zur Sicherung ihrer Steuerungsmöglichkeiten im Rahmen der Ausstellung von Attribut-Zertifikaten wird in zweifacher Hinsicht Rechnung getragen: Zum einen soll die Einwilligung oder Bestätigung zuverlässig nachgewiesen werden und zum anderen soll die dritte Person oder die zuständige Stelle über den Inhalt des Zertifikats sowie die Möglichkeit, dessen Sperrung zu veranlassen, unterrichtet sein.

Unter „dritte Person“ fallen auch juristische Personen, für die eine natürliche Person als Organ oder gesetzlicher Vertreter handelt. Ist bei der Übertragung von Vertretungsrechten in ein Zertifikat die dritte Person eine juristische Person, so muss zunächst festgestellt werden, ob die für die juristische Person handelnde natürliche Person ihrerseits vertretungsberechtigt ist (z.B. Geschäftsführer). Auch bei Personen, die für eine für berufsbezogene oder sonstige Angaben zur Person zuständige Stelle handeln, muss die Berechtigung dazu zweifelsfrei nachgewiesen sein, z.B. bei Bestätigungen in elektronischer Form z.B. durch ein entsprechendes Attribut in einem qualifizierten Zertifikat.

Zu § 4

Ermächtigungsgrundlage dieser Vorschrift ist § 24 Nr. 1 SigG i.V.m. § 5 Abs. 1 Satz 2 bzw. § §15 Abs. 1 und 16 Abs. 1 Satz 2 SigG. Sie greift auf § 8 Abs. 1 und 2 der SigV 97 sowie für Abs. 3 auf § 14 Abs. 4 der SigV 97 zurück.

Zu Abs. 1

In dieser Vorschrift werden die Mindestanforderungen an Zertifizierungsdiensteanbieter hinsichtlich der Führung eines Zertifikatsverzeichnisses beschrieben. Innerhalb des genannten Mindestzeitraums von fünf Jahren müssen die qualifizierten Zertifikate nachprüfbar sein. Dieser Zeitraum erscheint im Hinblick auf die übliche Abwicklungsdauer der meisten Rechtsgeschäfte sowie eines grossen Teiles der Verjährungsfristen - einschließlich der meisten Vermögensdelikte des StGB - und auch im europäischen Kontext angemessen. Es bleibt dem Zertifizierungsdiensteanbieter und auch dem Nutzer (Private oder öffentliche Stellen) unbenommen, auf frei-

willliger Basis längere Fristen zu wählen oder solche für bestimmte Bereiche (z.B. Medizin, Jurisprudenz, Steuerwesen) gesondert zu vereinbaren. Die Richtlinie enthält weder Angaben zur Aufbewahrungszeit von Zertifikaten noch irgendwelche Beschränkungen hierzu.

Zu Abs. 2

In dieser Vorschrift werden die höheren Anforderungen an akkreditierte Zertifizierungsdiensteanbieter im Hinblick auf die zentrale Aufgabe der Führung eines Zertifikatsverzeichnisses definiert. Die Frist von 30 Jahren ist vor dem Hintergrund möglicher zusätzlicher Anforderungen im öffentlichen Bereich, dem Bereich der Medizin und des Sozialversicherungswesens die Untergrenze. Es sind auch längere Zeiträume denkbar und langfristig in bestimmten Anwendungsfeldern erforderlich (z.B. Rentenwesen, Baugenehmigungen usw.). Es soll jedoch vor dem Hintergrund der noch nicht gesicherten Erfahrungen auf diesem Gebiet und der Vermeidung unnötiger Belastungen für die Diensteanbieter mit Akkreditierung erst zu einem späteren Zeitpunkt über ggf. längere Fristen entschieden werden. Art. 3 Abs. 7 der Richtlinie gibt dem nationalen Gesetzgeber im Hinblick auf zusätzliche Anforderungen im öffentlichen Bereich einen entsprechenden Spielraum, der dann bezogen auf die spezifischen Anwendungen - auch im Hinblick auf die Ausgestaltung der Fristen - genutzt werden kann.

Zu Abs. 3

Die Vorschrift soll sicherstellen, dass die nach § 5 Abs. 1 Satz 2 SigG verlangte Nachprüfbarkeit von qualifizierten Zertifikaten auch bei Einstellung der Betriebes eines Zertifizierungsdienstes erhalten bleibt.

Zu § 5

Ermächtigungsgrundlage ist § 24 Nr. 1 i.V.m. §§ 5 Abs. 4 bis 6 und 17 Abs. 3 Nr. 1 SigG.

Zu Abs. 1:

Satz 1 beschreibt die Anforderungen an die Geheimhaltung des Signaturschlüssels als Grundvoraussetzung dafür, dass Signaturen nicht gefälscht werden können. Die Bezeichnung "geeignete

Maßnahmen" ist offen für zulässige technisch-administrative Verfahren entsprechend dem Stand der Technik und der bewährten Praxis.

Die Vorschrift enthält auch die notwendigen Regelungen zur Geheimhaltung der wissensbasierten Identifikationsdaten. Diese sind erforderlich, um eine Nutzung sicherer Signaturerstellungsdaten durch Unbefugte auszuschließen. Die Vorschrift bezieht sich sowohl auf Wissensdaten, z.B. PIN-basiert, als auch auf Referenzdaten biometrischer Merkmale. Die Verknüpfung der Wissensdaten zur Identifikation des Satzes 2 mit den technischen Komponenten zur Erfassung biometrischer Merkmale durch "oder" soll deutlich machen, dass biometrische Merkmale hinsichtlich der Identifikationsdaten entweder ergänzend zu den Wissensdaten oder alternativ hierzu zur Anwendung kommen können. Sowohl für die Wissensdaten als auch für die biometrischen Merkmale gelten nach Satz 2 die gleichen Anforderungen hinsichtlich der Vorkehrungen zur Geheimhaltung.

Durch die Formulierung "nach Einbringen in dieselbe" in Satz 2 wird klargestellt, dass temporäre, technisch nicht vermeidbare Zwischenspeicherungen beim Einbringen unberührt bleiben. Im übrigen kann die Forderung nach Geheimhaltung und der nicht zulässigen Speicherung außerhalb der sicheren Signaturerstellungseinheit z.B. durch PIN-Briefe oder das sog. 0-PIN-Verfahren bzw. durch die getrennte Versendung von zwei Zahlenreihen, die durch Subtrahieren oder Addieren die PIN ergeben, erfüllt werden.

Zu Abs. 2

Die Vorschrift dient der Ausgestaltung des § 5 Abs. 6 SigG. Als Grundmodell der Übergabemodalitäten greift die Regelung auf § 6 der SigV 97 zurück. Zusätzlich sind die Übergabemodalitäten gegenüber der SigV 97 dahingehend erweitert worden, dass schriftlich oder mittels qualifizierter elektronischer Signatur nach dem Signaturgesetz eine andere Übergabe als die der persönlichen Übergabe vereinbart werden kann. Die Form der Übergabe ist dispositiv, nicht jedoch die Übergabebestätigung. Die Regelung dient vor allem der Sicherheit des Signaturschlüssel-Inhabers, in dem sie einen Mißbrauch der sicheren Signaturerstellungseinheit durch Unbefugte vor Inbesitznahme verhindert.

Zu Abs. 3

Die Vorschrift dient der Ausgestaltung von § 5 Abs. 5 SigG; sie greift auf § 10 der SigV 97 zurück. Es gelten hier nach wie vor strenge Maßstäbe für die Zuverlässigkeit des Personals als allgemeine Voraussetzung der Zuverlässigkeit des Betriebes insgesamt. Dies wird durch die Aufnahme des Begriffs "auf geeignete Weise" in Satz 1 verdeutlicht: Eine rein formale Prüfung reicht nicht aus. Dies ist auch für die Darlegungen im Rahmen des Sicherheitskonzepts relevant (vgl. näher dort unter § 2).

Zu § 6

Ermächtigungsgrundlage der Vorschrift ist § 24 Nr. 1 i.V.m. § 6 Abs. 1 SigG.

Die Vorschrift wurde gegenüber der Regelung des § 4 der SigV 97 gestrafft, bleibt jedoch im Hinblick auf die einzelnen inhaltlichen Anforderungen der Unterrichtung unverändert. Die Straffung ermöglicht einen größeren Spielraum bei der Gestaltung der Unterrichtung und erleichtert die Aufnahme neuer Entwicklungen. Gleichzeitig werden mit der Vorschrift die Informationspflichten nach Anhang II Buchst. k) EGSRL konkretisiert. Die Art und Weise der Unterrichtung (schriftlich, in elektronischer Form, mittels CD-ROM usw.) bleibt dem Zertifizierungsdiensteanbieter überlassen. Im Hinblick auf die Dokumentationspflicht der Unterrichtung nach § 8 Abs. 2 Nr. 3 sind entsprechend leicht überprüfbare Kommunikationen gegenüber dem Nutzer sinnvoll.

Die Informationspflicht nach Satz 2 gegenüber Dritten setzt die Anforderungen von Anhang II k) EGSRL um. Diese Informationspflicht umfasst nur die allgemeinen Informationen, die dem Antragsteller nach § 6 Abs. 1 SigG zur Verfügung gestellt werden; sie beinhaltet keine persönlichen Daten des Antragstellers im Sinne der Regelungen zum Datenschutz. Für Daten des Antragstellers gelten die Regelungen von § 14 SigG.

Zu § 7

Ermächtigungsgrundlage der Vorschrift ist § 24 Nr. 1 i.V.m. § 8 SigG.

Zu Abs. 1

Die Regelung dient dem Schutz der Signaturschlüsselinhaber sowie dritter Personen und zuständigen Stellen nach § 5 Abs. 2 und 3 SigG, deren Angaben in ein qualifiziertes Zertifikat aufge-

nommen wurden. Die Bekanntgabe der Rufnummer (Telefonverbindung) soll eine unverzügliche Sperrung ermöglichen, da eine Telefonverbindung im Gegensatz zu anderen Netzverbindungen nach gegenwärtigem Stand der Technik inzwischen praktisch überall in Deutschland und jederzeit rasch hergestellt werden kann.

Zu Abs. 2

Als Überprüfung der Identität nach Satz 1 ("auf geeignete Weise") kommen verschiedene technische und organisatorische Maßnahmen, insbesondere Authentisierungsverfahren wie beispielsweise ein Passwortverfahren, in Betracht. Diese sowie weitere Möglichkeiten zur Authentisierung sind zwischen dem Antragsteller und dem Zertifizierungsdiensteanbieter zu vereinbaren. Die Vereinbarung kann z.B. auch die Berechtigung weiterer Personen zur Sperrung einschließen und zusätzliche Vorkehrungen zum Schutz gegen mißbräuchliche Sperrungen.

Die Regelung des Satzes 2 greift auf § 9 der SigV 97 zurück. Die in § 9 der SigV 97 geregelte Unzulässigkeit der rückwirkenden Sperrung ist bereits durch § 8 Abs. 1 Satz 3 des Signaturgesetzes erfasst und bedarf nicht der Wiederholung in dieser Regelung.

Zu § 8

Ermächtigungsgrundlage dieser Vorschrift ist § 24 Nr. 1 i.V.m. § 10 SigG; sie greift auf § 13 der SigV 97 zurück.

Die Dokumentation der Sicherheitsmaßnahmen ist für die Durchführung von geeigneten Aufsichtsmaßnahmen nach §19 SigG sowie zur Beweisführung in einem Rechtsstreit, z.B. zwischen dem Zertifizierungsdiensteanbieter und Kunden oder einem Dritten im Haftungsfall, erforderlich. Außerdem werden damit die Anforderungen nach Anhang II Buchst. i) EGSRL umgesetzt.

Zu Abs. 1

Die Dokumentation umfasst die Nachweise zur Umsetzung des Sicherheitskonzepts nach § 4 Abs. 2 SigG und § 2 dieser Verordnung. In welcher Form die Dokumentation erfolgt, bleibt dem Zertifizierungsdiensteanbieter überlassen; er hat jedoch die umfassende Nachprüfbarkeit der

Dokumentation durch die zuständige Behörde und für die in Abs. 3 beschriebenen Fälle sicherzustellen.

Zu Abs. 2

Die Vorschrift enthält die Benennung aller Unterlagen, die im Zusammenhang mit einem qualifizierten elektronischen Zertifikat - bezogen auf den jeweiligen Antragsteller - relevant sind. Sie greift auf die Anforderungen des § 13 der SigV 97 zurück und nimmt diese zur leichteren Lesbarkeit jetzt in einer enumerative Auflistung auf. Neu ist die Aufnahme der Nachweise der Einwilligungen nach Nr. 4 und der Bestätigungen nach Nr. 5 sowie in Nr. 6 die Dokumentation zum Zeitpunkt der Einstellung in das Zertifikatsverzeichnis.

Zu Abs. 3

Die Aufbewahrungsfristen entsprechen denen nach § 4 Abs. 1 und 2 dieser Verordnung. Bei Gerichtsverfahren nach Satz 1 verlängert sich die Aufbewahrungsfrist bis zum rechtskräftigen Abschluß des Verfahrens in Umsetzung der Anforderungen des Anhangs II Buchst. i); dies gilt sowohl für akkreditierte als auch für nicht-akkreditierte Zertifizierungsdiensteanbieter. Für die Dokumentation der Auskünfte nach § 14 Abs. 2 SigG wird entsprechend der vergleichbaren Regelung des § 90 Abs. 4 TKG eine Aufbewahrungsfrist von 12 Monaten bestimmt.

Zu § 9

Ermächtigungsgrundlage ist die Vorschrift des § 24 Nr. 1 i.V.m. § 12 SigG.
Die Vorschrift setzt die Anforderungen des Anhangs II Buchst. h) EGSRL um.

Zu Abs. 1

Absatz 1 beschreibt die zulässigen Mittel zur Erfüllung der Deckungsvorsorge nach § 12 SigG. Unter Nr. 1 ist der Abschluss einer Haftpflichtversicherung genannt, der in der Praxis das häufigste Mittel zur Erbringung der Deckungsvorsorge darstellen wird. Darüber hinaus steht es dem Zertifizierungsdiensteanbieter frei, die Deckungsvorsorge auch auf anderem Wege, nämlich durch eine in Nr. 2 genannte Freistellungs- oder Gewährleistungsverpflichtung, insbesondere

eine Bankbürgschaft, beizubringen. Diese Ausgestaltung entspricht den Vorgaben in Anhang II Buchst. h) EGSRL, die den Abschluss einer Versicherung ebenfalls nur als eine beispielhafte Möglichkeit der Deckungsvorsorge vorsieht.

Zu Abs. 2

Die Bestimmungen des Absatzes 2 gelten nur für den Fall, dass eine Deckungsvorsorge durch eine Versicherung vorgenommen wird.

Zu Nr. 1

Nummer 1 erklärt die §§ 158c bis 158k VVG für entsprechend anwendbar. Die ausdrückliche Anordnung ist erforderlich, da sich die genannten Bestimmungen gemäß § 158b Abs. 1 VVG unmittelbar nur auf eine Haftpflichtversicherung beziehen, zu deren Abschluss eine gesetzliche Verpflichtung besteht, wovon die hier geregelte Versicherung wegen der anderweitigen Möglichkeiten zur Deckungsvorsorge nicht erfasst wird. Daneben wird auch § 158b Abs.2 VVG, der die Verpflichtung zur Ausstellung einer Versicherungsbescheinigung enthält, für entsprechend anwendbar erklärt. Die Angabe der zuständigen Behörde in Satz 2 erfolgt im Hinblick auf die Nachhaftung des Versicherers nach Beendigung des Versicherungsverhältnisses (bis einen Monat) gemäß § 158c Abs. 2 VVG.

Zu Nr. 2

Nummer 2 regelt die erforderliche Mindestdeckungssumme. Obwohl eine Bestimmung der erforderlichen Deckungssumme nur schwerlich möglich ist, gibt der Verordnungsgeber in Nr. 2 gleichwohl eine Mindestversicherungssumme vor, hinter der der Versicherungsschutz nicht zurückbleiben darf. Eine solche Angabe ist erforderlich, um sicherzustellen, dass jedenfalls in dieser Höhe ein Versicherungsschutz vorhanden ist und der Umfang der erforderlichen Versicherung nicht unzulässigerweise der Anerkennung der zuständigen Behörde überlassen bleibt.

Aufgrund der Besonderheiten der Tätigkeit von Zertifizierungsdiensteanbietern ist eine klarstellende Differenzierung zwischen Versicherungsfall und einzelnem Schaden erforderlich, die in dieser Bestimmung vorgenommen wird. Diese Unterscheidung liegt bereits § 12 Satz 2 SigG zu Grunde; die dort festgesetzte Mindestdeckungssumme von 250.000 Euro bezieht sich ausdrücklich auf den einzelnen eingetretenen Schaden. Demgegenüber betrifft die in Nr. 2 Satz 1 festgelegte Mindestversicherungssumme den Versicherungsfall. Satz 2 stellt hierzu klar: Ein „Versi-

cherungsfall“ im Sinne des Satzes 1, ist das einzelne haftungsauslösende Ereignis, das die Anforderungen des Signaturgesetzes oder dieser Verordnung verletzt , also z.B. die individuelle falsche Angabe in einem Zertifikat, bei dessen Verwendung mehrere Schadensfälle auftreten können. Als Gesamtdeckungssumme für die aus einer falschen Angabe folgenden Schäden setzt Nr. 2 Satz 1 die Höhe von 2, 5 Millionen Euro fest, das ist das Zehnfache der für den einzelnen Schadensfall festgesetzten Mindestdeckungssumme in § 12 Satz 2 SigG. Maßstab für diese Summe ist die Höhe eines durchschnittlich zu erwartenden Schadens in einem Versicherungsfall, nicht eine theoretische Maximalhöhe. Mangels Erfahrungswerten kann sich die Festlegung nicht auf empirische Erkenntnisse stützen; es ist aber davon auszugehen, dass die zehnfache Summe der – für sich genommen schon hoch liegenden – gesetzlichen Einzelschadensabdeckung einen hinreichenden Gesamtschutz für alle Geschädigten bietet, die beispielsweise auf eine falsche Angabe im Zertifikat vertraut haben, bevor diese aufgedeckt wird.

Satz 3 bestimmt , dass der Begriff des „Versicherungsfalls“ nicht im Wege einer Vereinbarung zwischen Versicherer und Versicherungsnehmer dahingehend abgeändert werden darf, dass für den Begriff des Versicherungsfalls auf einen (einzigen) Fehler beim Zertifizierungsdiensteanbieter abgestellt wird, der möglicherweise zu einer Vielzahl von fehlerhaften Zertifikaten führt, die dann nur insgesamt einmal von der Deckungssumme von 2,5 Millionen Euro umfasst wären. Bezugspunkt des „Versicherungsfalles“ ist vielmehr immer die individuelle Falschangabe im einzelnen Zertifikat oder Zeitstempel oder in der Auskunft nach § 5 Abs. 1 Satz 2 SigG, die zu einer Haftung nach § 11 SigG führt.

Den Versicherungen wird die Möglichkeit belassen, die Versicherungssumme pro Kalenderjahr zu begrenzen. Satz 4 bestimmt für diesen Fall, dass die vereinbarte Jahreshöchstleistung mindestens das Vierfache der Mindestversicherungssumme für den einzelnen Versicherungsfall betragen muss. Derselbe Faktor findet sich auch in den Bestimmungen zur Ausgestaltung der Berufshaftpflichtversicherung in § 51 Abs. 4 BRAO und § 52 Abs. 3 DVStB.

Zu Nr. 3

Nummer 3 stellt klar, dass der räumliche Geltungsbereich des Versicherungsschutzes auf den Geltungsbereich der Richtlinie beschränkt werden kann. Diese Regelung ermöglicht eine zulässige Risikoeingrenzung für die Versicherungsunternehmen, da nur im Geltungsbereich der Richtlinie eine wirksame Aufsicht und Kontrolle der Zertifizierungsdiensteanbieter gewährleistet

ist. Die Beschränkung kann sich sowohl auf den Ort, an dem z.B. das falsche Angaben enthaltende Zertifikat verwendet wird, beziehen, als auch auf den Ort, an dem bei der Person, die auf diese Angaben vertraut hat, der Schaden eingetreten ist.

Zu Nr. 4

Nummer 4 bestimmt die zulässigen Möglichkeiten des Leistungsausschlusses durch die Versicherung gegenüber dem Zertifizierungsdiensteanbieter. Diese sind entsprechend dem gesetzlichen Leitbild des § 152 VVG beschränkt auf Fälle der vorsätzlich begangenen Pflichtverletzung. Die Vereinbarung eines Haftungsausschlusses für grob fahrlässige Pflichtverletzung des Zertifizierungsdiensteanbieters ist demgegenüber nicht möglich. Diese Einschränkung ist erforderlich, um dem geschädigten Dritten auch in diesen Fällen die Absicherung durch die Deckungsvorsorge zukommen zu lassen. Über den nach Nummer 5 möglichen Selbstbehalt besteht trotz des Versicherungsschutzes bei grober Fahrlässigkeit ein hinreichend großer Anreiz für den Zertifizierungsdiensteanbieter, sich nicht leichtfertig zu verhalten.

Zu Nr. 5

Nummer 5 sieht die Möglichkeit vor, einen Selbstbehalt zu vereinbaren. Dieser darf allerdings nicht höher als 1 Prozent der Mindestversicherungssumme liegen . Durch diese Festlegung wird ein angemessener Ausgleich zwischen den Interessen der Beteiligten geschaffen. Die Höhe von 1 % der Mindestversicherungssumme ist dem Modell der Berufshaftpflichtversicherung in § 51 Abs. 5 BRAO nachgebildet.

Zu § 10

Ermächtigungsgrundlage dieser Vorschrift ist § 24 Nr. 1 SigG i.V.m. § 13 SigG. Sie greift auf § 14 Abs. 1 bis 3 SigV 97 zurück; § 14 Abs. 4 der SigV 97 wurde in § 4 Abs. 3 übernommen.

Zu Absatz 1

Durch die Vorschrift soll die zuständige Behörde in die Lage versetzt werden, das nach Absatz 2 bis 3 vorgesehene Verfahren bei Einstellung der Tätigkeit eines Zertifizierungsdienstes zu überwachen. Die bisherigen Fristen von vier Monaten nach § 14 Abs. 1 der SigV 97 werden auf zwei

Monate verkürzt. Die verkürzte Frist erscheint ausreichend, damit die zuständige Behörde ihre Aufgaben rechtzeitig erfüllen kann.

Zu Absatz 2

Die Signaturschlüssel-Inhaber sollen durch die frühzeitige Unterrichtung nach Satz 1 u. a. in die Lage versetzt werden, sich rechtzeitig neue Zertifikate bei einem anderen Zertifizierungsdiensteanbieter zu beschaffen. Die Verkürzung von drei Monaten nach § 14 Abs. 2 der SigV 97 auf zwei Monate erscheint ausreichend, damit die Betroffenen ihre Rechte wahren können.

Die Signaturschlüssel-Inhaber sollen vor allem auch darüber unterrichtet werden, ob ein anderer Zertifizierungsdiensteanbieter ihre Zertifikate übernimmt, da nur in diesem Falle die von ihnen signierten elektronischen Dokumente weiterhin überprüfbar bleiben.

Zu Absatz 3

Die Formerfordernisse dienen der Rechtssicherheit der Beteiligten.

Zu § 11

Ermächtigungsgrundlage dieser Vorschrift ist § 24 Nr. 1 i.V.m. § 15 SigG.

Zu Abs. 1

Die Formerfordernisse dienen der Rechtssicherheit der Beteiligten. Sofern der Antragsteller mit der Einreichung des Antrags auf freiwillige Akkreditierung die nach § 1 dieser Verordnung vorgesehenen Voraussetzungen nach Form und Inhalt erfüllt, gilt der Antrag zugleich als Anzeige. Der Antragsteller kann nach seiner Wahl in diesem Falle entscheiden, ob er sich bereits dann der Aufsicht und dem Verfahren für die Zertifizierungsdiensteanbieter unterstellen und den Betrieb aufnehmen will, oder ob er für die Betriebsaufnahme den Abschluss des Verfahrens der freiwilligen Akkreditierung abwarten möchte. Der Antragsteller sollte sich in diesem Falle gegenüber der zuständigen Behörde deutlich erklären.

Zu Abs. 2

Die Nachweise nach Satz 1 und die Vorlage der Ergebnisse der Prüf - und Bestätigungsstellen bilden den Kern der zusätzlichen erhöhten Anforderungen an akkreditierte Zertifizierungsdiensteanbieter. Neben der Schriftform ist die qualifizierte elektronische Signatur nach dem Signaturgesetz zugelassen.

Satz 2 sieht einen Prüfungszyklus von drei Jahren vor, der auf den Erfahrungen mit dem SigG 97 beruht. Nur durch regelmäßige und in relativ kurzen Zeitabständen durchzuführende Prüfungen kann ein kontinuierlich hohes Sicherheitsniveau der akkreditierten Zertifizierungsdiensteanbieter gewährleistet werden.

Zu Abs. 3
und zur Anlage 1, Abschnitt I.

In der Anlage 1 Abschnitt I. zu dieser Vorschrift werden weitere Vorgaben für die Prüfung und Bestätigung von Produkten für qualifizierte elektronische Signaturen, die im Rahmen der freiwilligen Akkreditierung gelten, geregelt. Die Anlage 1 Abschnitt I. greift auf § 17 Abs. 2 bis 4 der SigV 97 zurück und berücksichtigt darüber hinaus die Arbeiten auf Europäischer Ebene im Rahmen des Artikel-9-Ausschusses der EGSRL soweit diese ein entsprechend vertretbares Sicherheitsniveau, vergleichbar mit dem des SigG 97 vorsehen. Die bisherigen Anforderungen nach dem SigG 97 und der SigV 97, die in der Praxis bereits erprobt und markteingeführt sind, werden auf diese Weise im Rahmen des Verfahrens der freiwilligen Akkreditierung im Kern beibehalten. Gegenüber den Regelungen der SigV 97 wurden vor allem sprachliche Anpassungen an das SigG sowie einige Straffungen im Text vorgenommen. Es kann daher ergänzend auf die Ausführungen zur Begründung der SigV 97 verwiesen werden.

Zu Anlage 1 Abschnitt I Nr. 1
Die Vorschrift greift auf § 17 Abs. 1 der SigV 97 zurück und wird an die aktuellen Entwicklungen auf internationaler Ebene angepasst. Die Vorschriften beruhen auf den derzeit gültigen und dem Stand der Technik entsprechenden Kriterien für die Prüfung und Bestätigung von Produkten qualifizierter elektronischer Signaturen.

Gleichwertig nebeneinander gelten als zulässige und internationale Kriterienwerke die in Nummer I. 1.1 genannten "Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit in

der Informationstechnik (*Common Criteria*)" und die "Kriterien für die Bewertung der Sicherheit von Systemen in der Informationstechnik (*ITSEC*)".

Bei den Anforderungen an die Prüfung nach Nummer I 1.1. a) bis d) wird hinsichtlich der erforderlichen Prüftiefe zwischen verschiedenen Produkten und Anwendungsumgebungen differenziert, um den unterschiedlichen Sicherheitsaspekten angemessen Rechnung tragen zu können. Für die unter I. 1.1. a bis b) genannten Produkte ist vor dem Hintergrund der möglichen Angriffspotenziale ein entsprechend hohes Sicherheitsniveau erforderlich. Bei den technischen Komponenten für Zertifizierungsdienste nach Nummer I. 1.1. c) wird danach unterschieden, ob diese außerhalb oder innerhalb eines gesicherten Bereichs eingesetzt werden. Unter dem Begriff "gesicherter Bereich" sind alle Baulichkeiten zu verstehen, worin eine sichere Anwendungsumgebung für den Einsatz von Produkten für qualifizierte elektronische Signaturen geschaffen wurde, um einen autorisierten Zugriff auf die relevanten Daten zu gewährleisten. Dies betrifft die organisatorisch-administrativen, technischen und infrastrukturellen Sicherheitsmaßnahmen, wie sie insbesondere in § 2 dieser Verordnung (Sicherheitskonzept) näher beschrieben sind. Aus diesem Grunde sind für die Prüfung der Produkte innerhalb des gesicherten Bereichs geringere Anforderungen zu stellen, als dies außerhalb des Bereichs mit vielfältigen Angriffsmöglichkeiten der Fall ist.

An Signaturanwendungskomponenten nach Nummer I. 1.1. d) und gemäss § 2 Nr. 11 SigG sind, wie bereits in der SigV 97, geringere Prüfanforderungen zu stellen als an die unter den Buchstaben a) bis c) genannten Produkte, da hier grundsätzlich ein geringeres Gefährdungspotenzial besteht und im übrigen die Marktsituation höhere Prüfanforderungen auch nicht zulässt.

Unter Nummer 1.2. werden die Anforderungen an die Schwachstellenbewertung und die Mechanismenstärke näher beschrieben.

Die *Common Criteria* unterscheiden zwischen den Prüf- bzw. Evaluationsstufen „EAL 1“ bis „EAL 7“ und die *ITSEC* zwischen den Prüf- bzw. Evaluationsstufen „E 1“ bis „E 6“. Bei der Stärke der zur Erreichung der Sicherheitsziele eingesetzten Mechanismen wird bei *ITSEC* jeweils nach gering, mittel und hoch differenziert.

Ein Mechanismus mit der Stärke „hoch“ im Rahmen von ITSEC erfordert eine Prüfung unter Zugrundelegung eines hohen Angriffspotenzials und eine vollständige Risikoanalyse. Soweit die

Prüfkriterien in Details voneinander abweichen oder Ermessensspielraum lassen, wird die zuständige Behörde über den Arbeitskreis der nach § 18 SigG anerkannten Prüf- und Bestätigungsstellen auf eine möglichst einheitliche Prüfpraxis hinwirken.

Bei dem Schutz der Sicherheitskomponenten für Produkte qualifizierter elektronischer Signaturen geht es im Kern darum, marktkonforme Lösungen zu finden, die zugleich die wesentlichen Sicherheitsanforderungen erfüllen. Dies kann dadurch umgesetzt werden, eine Prüfstufe vorzusehen, die alle Anforderungen der Sicherheitsstufe "EAL 5" mit Ausnahme des vergleichsweise aufwändigen formalen Sicherheitsmodells erfüllt -, d.h. eine Stufe "EAL 4 +". Grundlage für eine solche höhere Zwischenstufe innerhalb des EAL 4 ist das sog. Schutzprofil (*Protection Profile*), das auf dem CEN/ISSS-Workshop E-Sign entwickelt wurde und nach gegenwärtigem Stand der Diskussion Grundlage für europäische (Zusatz-)Anforderungen für die Stufe EAL 4 werden wird. Diese Zusatzanforderungen - EAL 4 "plus" - werden in Nummer 1.2. beschrieben. Die Stufe E 3 "hoch" von *ITSEC* entspricht der höheren Zwischenstufe des oben beschriebenen "EAL 4+" von *Common Criteria*.

Die in Nummer 1.1. a) bis c) i) aufgeführten Produkte für qualifizierte elektronische Signaturen sind potenziell einer großen Bedrohung ausgesetzt und daher besonders sicherheitsrelevant. Aus diesem Grunde wird für diese Komponenten die Stufe "EAL 4 +" der *Common Criteria* mit ihren Maßnahmen gegen ein hohes Angriffspotenzial, AVA_VLA.4, eine vollständige Mißbrauchsanalyse, AVA_MSU.3 und die Stärke der Funktionen AVA_SOF. mit SOF "hoch" (näheres siehe beim o.g. Schutzprofil für Nummer I, 1.1. a) und b)) vorgeschrieben. Alternativ zu den *Common Criteria* ist für die genannten Produkte die Stufe E 3 "hoch" von *ITSEC* vorgesehen.

Kommen in Ergänzung zu der Identifikation durch Wissensdaten auch biometrische Merkmale zur Anwendung, so genügt wegen der bereits bestehenden ausreichenden Sicherheit eine Mechanismenstärke von "mittel" im Rahmen der ITSEC-Kriterien. Werden biometrische Merkmale anstelle von Wissensdaten eingesetzt, so muss aufgrund der Forderung aus § 15 Abs. 1 nach gleichwertiger Sicherheit eine Mechanismenstärke "hoch" gegeben sein.

In Nummer 1.3. wird geregelt, dass sich die Anforderungen an die Algorithmen und zugehörigen Parameter nach Nummer I. 2. richten (siehe näher dort).

zu Anlage 1 Abschnitt I Nr. 2

Die Vorschrift greift auf § 17 Abs. 2 SigV 97 zurück, die unverändert übernommen wird. Der Zeitraum der Eignung von sechs Jahren erscheint im Hinblick auf eine mögliche zeitbedingte Minderung des Sicherheitswertes von Algorithmen mit den zugehörigen Parametern ausreichend und hinreichend überschaubar. Soweit es sachlich begründet ist, lässt die Regelung auch die Wahl kürzerer oder längerer Zeiträume zu ("soll").

zu Anlage 1 Abschnitt I Nr. 3

Die Vorschrift greift auf § 17 Abs. 3 der SigV 97 zurück, die inhaltlich unverändert übernommen wird; es wurden lediglich Untergliederungen des Textes und redaktionelle Anpassungen an die neuen Begriffsbestimmungen des SigG ("Produkte" statt "technische Komponenten") vorgenommen.

Zu Anlage 1 Abschnitt I Nr. 4

Die Vorschrift greift auf § 17 Abs. 4 der SigV 97 zurück, die im wesentlichen unverändert übernommen wurde. Weggefallen ist die nach Satz 2 der SigV 97 vorgesehene unmitttelbare Bekanntgabe an die Zertifizierungsdiensteanbieter, da diese die benötigten Informationen jederzeit abrufen können.

Zu § 12

Ermächtigungsgrundlage ist § 24 Nr. 2 i.V.m. § 22 Abs. 1 SigG. Die Regelung ist aufgrund der neuen gesetzlichen Aufgaben und Aufgabenstruktur der zuständigen Behörde gegenüber § 2 der SigV 97 vollständig überarbeitet worden. Die Vielzahl der möglichen Amtshandlungen und das im Vorblatt zum SigG formulierte Ziel, den Personal- und Sachaufwand durch die Erhebung von Kosten zu decken, machen eine detaillierte Auflistung der kostenpflichtigen Tatbestände erforderlich. Um den Text der Verordnung nicht zu überfrachten, sind die Übersichtstabellen und die begleitenden Regelungen dazu als Anlage 2 dieser Verordnung beigefügt.

In dieser Vorschrift wird hinsichtlich der Gebührenhöhe auf die einzelnen Gebührentatbestände in Anlage 2 zu dieser Verordnung verwiesen. Die Bemessung der Gebührensätze richtet sich

nach dem Verwaltungsaufwand gemäß § 3 VwKostG. Da in § 24 Nr. 2 SigG eine Deckung des Verwaltungsaufwandes durch die Gebühren gesetzlich vorgesehen ist, gilt für die Bemessung auch § 3 Satz 2 VerwKostG. Es gelten in der Regel feste Gebührensätze, die auf Mittelwerten, basierend auf dem durchschnittlichen Verwaltungsaufwand, beruhen. Für bestimmte Amtshandlungen ist eine Gebühr nach Zeitaufwand vorgesehen. Es handelt sich um die Amtshandlungen, bei denen nach Art und Umfang der Prüfungen und Maßnahmen eine genaue Abschätzung des Aufwandes pauschal nicht möglich ist und damit dem Grundsatz der Gebührengerechtigkeit widerspräche. Die Stundensätze und die Km-Pauschale sind vergleichbaren Sätzen von Verordnungen im Telekommunikationsbereich nachgebildet (vgl. z.B. TKZulV). Der Hinweis auf § 10 VerwKostG dient der Klarstellung, dass die Kosten für beauftragte Dritte (z.B. für Prüf- und Bestätigungsstellen) durch die Bestimmung erfasst sind.

Zu § 13

Ermächtigungsgrundlage der Vorschrift ist § 24 Nr. 2 i.V.m. § 22 Abs. 2 SigG.

Zu Abs. 1

Der Personal- und Sachaufwand im Sinne dieser Vorschrift berechnet sich nach den Kosten, die im Zusammenhang mit den in § 22 Abs. 2 Satz 1 SigG genannten Tätigkeiten entstehen, unter Abzug der Kosten, die durch Gebühren nach § 12 dieser Verordnung abgedeckt sind. Zur Klarstellung hinsichtlich des zu berechnenden Sachaufwandes ist der Investitionsaufwand als zu berücksichtigender Kostenfaktor besonders erwähnt.

In Satz 2 wird der Beitragssatz festgelegt. Er berücksichtigt die Personal- und Sachkosten der zuständigen Behörde, die in einem direkten Zusammenhang zu den Kosten für das Führen der Verzeichnisse nach § 16 Abs. 2 und nach § 19 Abs. 6 SigG stehen. Hierbei wurde - basierend auf den gegenwärtigen Kosten - eine Schätzung des voraussichtlichen Personal- und Sachaufwandes der nächsten drei Jahre vorgenommen und ein Mittelwert hieraus gebildet. Der Beitragssatz wird pro ausgestelltem Zertifikat festgesetzt. Er beruht auf einer Schätzung durch die zuständige Behörde der in den nächsten drei Jahren im Geltungsbereich des Signaturgesetzes ausgestellten qualifizierten Zertifikate, auf der Basis der heute ausgestellten qualifizierten Zertifikate und einer Einschätzung der Entwicklung des Marktes im genannten Zeitraum.

Satz 3 sieht die beitragsmindernde Berücksichtigung des Allgemeininteresses bei der Festsetzung der Beitragshöhe vor. Dies trägt dem Urteil des Bundesverwaltungsgerichts (BVerwG)

vom 22. November 2000 (Az.: 6 C 8.99) Rechnung, das im Zusammenhang mit der Festsetzung der Beiträge im Rahmen des Gesetzes über die elektromagnetische Verträglichkeit von Geräten (im Folgenden EMVG-Urteil) erging. Die Erwägungen des BVerwG im EMVG-Urteil sind im Einzelfall auf ihre Anwendbarkeit vor dem Hintergrund des jeweiligen Regelungserfordernisses zu Beiträgen zu prüfen. Im vorliegenden Fall wird eine Beitragsregelung für das Führen der Verzeichnisdienste zur Erfüllung der Aufgaben nach dem SigG und dieser Verordnung getroffen. Aus den im Folgenden näher ausgeführten Gründen erscheint es sachgerecht, die Grundsätze des BVerwG aus dem EMVG-Urteil zur Berücksichtigung des Allgemeininteresses im Falle der Festsetzung des Beitragssatzes im Rahmen dieser Verordnung mit heranzuziehen.

Die Überlegungen zur beitragsmindernden Berücksichtigung des Allgemeininteresses im Rahmen dieser Vorschrift beruhen auf dem derzeitigen Kenntnisstand und können zum gegenwärtigen Zeitpunkt nur vor dem Hintergrund noch nicht gesicherter Erfahrungen getroffen werden. Nach § 22 Abs. 2 Satz 1 SigG haben die Zertifizierungsdiensteanbieter für die ständige Erfüllung der Voraussetzungen nach § 19 Abs. 6 eine Abgabe zu entrichten, die als Jahresbeitrag erhoben wird. Es handelt sich in diesem Fall wie auch im Fall des Absatzes 3 jeweils um Verzeichnisse, die eine jederzeitige Nachprüfbarkeit bestimmter zentraler Informationen in bezug auf die angezeigten Anbieter (§ 19 Abs. 6 SigG) oder hinsichtlich der akkreditierten Anbieter einschließlich eines Widerrufsdienstes (§ 16 Abs. 2 SigG) ermöglichen. Diese Regelungen des SigG dienen dem Schutz des Vertrauens Dritter in die Integrität der sich im Verkehr befindlichen Zertifikate und der verfügbaren Anbieter. Diese Informationen, die "für jeden" über öffentlich erreichbare Kommunikationsverbindungen abrufbar zu halten sind, kommen damit der Gesamtbevölkerung ("Allgemeinheit") zugute. Jeder hat ein potenzielles Interesse an der Funktionsfähigkeit dieses Systems, selbst wenn er aktuell (noch) nicht über Einrichtungen verfügt, die ihm eine Teilnahme am Verkehr mit elektronischen Signaturen ermöglicht, diese aber jederzeit in Anspruch nehmen kann. Im Rahmen des § 16 Abs. 2 SigG nimmt die Regulierungsbehörde darüber hinaus auch eine der Notarfunktion angenäherte Aufgabe im Zusammenhang mit der Führung des Verzeichnisses wahr.

Auf der anderen Seite ist als Faktor, der zur Minderung des Allgemeininteresses führt, zu berücksichtigen, dass zur Zeit nur eine geringe Zahl an Nutzern dieser Infrastruktur vorhanden ist. Darüber hinaus kommen die Verzeichnisse auch den Zertifizierungsdiensteanbietern in erheblichem Maße zugute: Sie bedienen sich einer öffentlich vertrauenswürdigen Infrastruktur, die die entscheidende Grundlage für dieses in erster Linie auf Vertrauen beruhenden Geschäft bildet.

Zusammenfassend kann daher bei der Festsetzung des Beitragssatzes nicht von einem Übergewicht des Allgemeininteresses gesprochen werden. Auf der anderen Seite sind die Faktoren, die für eine angemessene und entsprechende Berücksichtigung des Allgemeininteresses sprechen, nicht unerheblich. Diese genannten Faktoren führen dazu, das Allgemeininteresse bei der Festsetzung der Beitragssätze mit 30 Prozent beitragsmindernd zu berücksichtigen. Da es sich hier um einen dynamischen Prozess handelt, kann sich diese Gewichtung im Laufe der Zeit ändern. Hierfür ist zur Feststellung des beitragsmindernden Anteils des Allgemeininteresses das flexible Instrument der Verordnung das Geeignete, wie durch das BVerwG im oben genannten Urteil ausgeführt wurde. Es kann hier sowohl für den Fall des Absatzes 1 als auch des Absatzes 3 derzeit ein einheitlicher Beitragssatz in Höhe von [ ] Euro[1] zugrunde gelegt werden. Die im Vergleich zur Erfüllung der Aufgaben nach § 16 Abs. 2 SigG geringeren Kosten im Zusammenhang mit denen des § 19 Abs. 6 SigG, werden dadurch aufgewogen, dass zum Zeitpunkt des Inkrafttretens dieser Verordnung keine bzw. nur eine sehr geringe Zahl von Anbietern qualifizierter Zertifikate ohne Anbieterakkreditierung auf dem Markt vorhanden ist und daher auch die Kosten, die umzulegen sind, für jeden Anbieter dieser Zertifikate dem entsprechend höher sind. Auf der anderen Seite gibt es zum Zeitpunkt des Inkrafttretens der Verordnung bereits acht akkreditierte Anbieter und das derzeitige Marktverhalten und die Marktprognosen sprechen für einen weiteren und dynamischen Wachstum in diesem Bereich, so dass die höheren Kosten für die Erfüllung der Aufgaben nach § 16 Abs. 2 SigG durch die größere Anzahl der Zertifikate wieder ausgeglichen werden.

In Satz 4 ist der Umlageschlüssel der Beitragskosten geregelt. Hierfür wird die Zahl der ausgestellten qualifizierten Zertifikate zugrundegelegt, um eine gerechte und größenbezogene Festsetzung der Beiträge zu ermöglichen.

Die Schätzung nach Satz 6 bedarf einer Grundlage. Eine Schätzung allein basierend auf der Zahl der im Vorjahr ausgestellten Zertifikate würde eine dynamische Marktentwicklung nicht berücksichtigen und könnte einen Anreiz geben, keine neuen Zahlen vorzulegen. Daher kommt auch der Schätzung aufgrund von Marktprognosen Bedeutung zu, wobei die zuständige Behörde grundsätzlich frei ist, wie sie die Marktprognosen in die Schätzung einbezieht.

[1] Anmerkung: Der Beitragssatz wird zur Zeit ermittelt

Zu Abs. 2

Die Regelung bedeutet, dass nicht alle Investitionskosten der zuständigen Behörde, die im Zusammenhang mit der Erfüllung der Bestimmungen des § 16 Abs. 2 und 19 Abs. 6 SigG anfallen, in einem Betrag umgelegt werden, sondern entsprechend der steuerlichen Abschreibungsregelungen auf mehrere Jahre zu verteilen sind. Die Abschreibung von Investitionsgütern richtet sich nach der betriebsgewöhnlichen Nutzungsdauer, die sich in der Regel nach den AfA-Tabellen orientiert und im Einzelfall von der zuständigen Behörde festzustellen ist.

Zu Abs. 3

Die Beitragsregelungen der Absätze 1 und 2 sind entsprechend auch auf die akkreditierten Zertifizierungsdiensteanbieter anzuwenden. Dies gilt auch für den Beitragssatz. Es wird auf die Ausführungen zu Absatz1 verwiesen.

Zu Abs. 4

Die Vorschrift regelt den Beginn und das Ende der Beitragspflicht sowie die Berechnungsgrundlagen auf Basis des vorangegangenen Kalenderjahres einschließlich der anteiligen Berechnungen, sofern diese erforderlich sein sollten.

Zu § 14

Ermächtigungsgrundlage der Vorschrift ist § 24 Nr. 4 i.V.m. § 7 SigG. Hinsichtlich der Gültigkeitsdauer von Zertifikaten greift die Regelung auf § 7 der SigV 97 zurück.

Zu Abs. 1

Die Regelung beschreibt allgemein die Kernanforderung an die Angaben in einem qualifizierten elektronischen Zertifikat.

Zu Abs. 2

Kern der Regelung sind die näheren Anforderungen an qualifizierte Attribut-Zertifikate. Die Vorschrift bestimmt die Informationen, die ein Attribut-Zertifikat selbst enthalten muß und nicht

durch einfache Verweisung auf das zugrundeliegende Signaturschlüssel-Zertifikat abgedeckt werden können.

Die Informationen nach Nummer 1 sind erforderlich, damit das Zertifikat auf seine Echtheit und Unverfälschtheit überprüft werden kann. Die Informationen nach Nummer 2 und 3 müssen erfolgen, um eine Nachprüfung der Zertifikate über das Zertifikat-Verzeichnis des Zertifizierungsdiensteanbieters durchführen zu können. Die Informationen nach Nummer 4 sind notwendig, um die qualifizierten Attribut-Zertifikate von anderen unterscheiden zu können. Die Informationen nach Nummer 5 machen den entscheidenden Inhalt der Attribut-Zertifikate aus.

Die Angabe des Staates nach Nummer 3 orientiert sich nach Anhang I Buchst. b) EGSRL an der Niederlassung. So darf „Deutschland“ in einem Zertifikat nur angegeben werden, wenn der ausstellende Zertifizierungsdiensteanbieter in Deutschland auch tatsächlich niedergelassen ist und seinen Betrieb gemäß § 4 Abs.3 SigG bei der zuständigen Behörde angezeigt oder eine Akkreditierung nach § 15 Abs. 1 SigG erhalten hat. Bei gleichzeitiger Niederlassung in mehreren Staaten hat der Zertifizierungsdiensteanbieter zu entscheiden, welchen der Staaten er im Zertifikat angibt. Die Angabe des Staates im Zertifikat erfolgt i.d.R. durch ein Kürzel (z.B. „I“ für Italien).

Zu Abs. 3

Die begrenzte Gültigkeitsdauer von Signaturschlüssel-Zertifikaten nach Satz 1 ergibt sich dadurch, dass die kryptographischen Verfahren für qualifizierte elektronische Signaturen nur für einen begrenzten Zeitraum sicher bewertet werden können.

Im übrigen muss der Signaturschlüssel-Inhaber sich darauf verlassen können, dass die im Zertifikat aufgeführten Algorithmen und zugehörigen Parameter für den Zeitraum der Gültigkeit des Zertifikates die erforderliche Eignung aufweisen. Um bei der Signatur zu dem Zertifikat ein Nachsignieren nach §16 zu vermeiden, muss der Zertifizierungsdiensteanbieter auch deren Eignung bei der Vergabe von Zertifikaten mit berücksichtigen.

Zu § 15

Ermächtigungsgrundlage dieser Vorschrift ist § 24 Nr. 4 i.V.m. § 17 Abs. 1 bis 4 SigG; die Vorschrift greift im Kern auf § 16 der SigV 97 zurück. Neue Entwicklungen im Bereich der Biometrie werden aufgegriffen und ein dynamischer Verweis in Abs.6 zur Geltung der Ergebnisse der europäischen Standardisierung aufgrund des Artikel-9-Ausschusses der Richtlinie geschaffen.

Zu Abs. 1

Die Vorschrift enthält die erforderlichen Spezifikationen für sichere Signaturerstellungseinheiten nach § 17 Abs. 1 SigG. Eine sichere Signaturerstellungseinheit wird in der Regel in Form einer Chipkarte oder einer vergleichbaren Komponente (z.B. PCMCIA-Karte) realisiert.

Um eine unbefugte Nutzung des Signaturschlüssels nach Möglichkeit auszuschließen, wird eine Identifikation durch Besitz (Karte) und Wissen (PIN oder Passwort) oder durch Besitz und ein biometrisches Merkmal (z.B. Gesicht, eigenhändige Unterschrift oder Fingerstruktur) verlangt.

Damit wird die Identifikation anhand biometrische Merkmaler erstmals auch alternativ zur Identifikation anhand von Wissen zugelassen, nachdem bereits in der SigV 97 die kumulative Nutzung von Besitz, Wissen und biometrischen Merkmalen zur Identifikation zugelassen ist. Dies schafft einen Anreiz für entsprechend innovative Lösungen. Allerdings müssen diese Anwendungen mit entsprechenden Anforderungen im Sinne einer gleichwertigen Sicherheit mit wissensbasierten Verfahren verbunden sein: Bei Nutzung biometrischer Merkmale muss deshalb insbesondere gewährleistet sein, dass ein erfolgreiches Vortäuschen der biometrischen Merkmale und ein Einspielen der Referenzdaten sowie andere Eingriffe, die eine Nutzung des Signaturschlüssels durch Unbefugte ermöglichen können, hinreichend ausgeschlossen sind.

Sichere Signaturanwendungskomponenten können so gestaltet werden, dass optional vor jeder Signatur, nach einer zuvor festgelegten Anzahl von Signaturen oder nach bestimmtem Zeitablauf bei Nichtbenutzung der Signaturerstellungseinheit die Identifikationsdaten erneut eingegeben werden müssen. Es liegt im Ermessen des Nutzers, wie er – abhängig von seinem individuellen Bedarf und der Anwendungsumgebung – verfährt. Im Regelfall sollte vor jeder neuen Signatur auch eine erneute Identifikation erfolgen oder es sollte nur ein kurzes „Zeitfenster“ geöffnet bleiben, innerhalb dessen weitere Signaturen möglich sind.

Nach Satz 2 muss sichergestellt sein, dass der Signaturschlüssel nicht aus der sicheren Signaturerstellungseinheit exportiert werden kann. Dies erfordert z.B. eine Chipkarte oder Spezialkomponente für Großrechnereinsatz, die nach dem Stand der Technik nicht ausgelesen werden kann (auch nicht durch den Signaturschlüssel-Inhaber selbst). Das Laden von Signaturschlüsseln muss technisch-administrativ so abgesichert sein, dass ein unberechtigter Zugriff (im Sinne der Nutzung) auf Signaturschlüssel ausgeschlossen ist. Eine Speicherung außerhalb der sicheren Signaturerstellungseinheit muss ausgeschlossen sein; ausgenommen sind technisch nicht vermeidbare temporäre Zwischenspeicherungen beim Erzeugen und Laden der Schlüssel.

Die Vorschrift nach Satz 4 enthält erforderliche Spezifikationen zu § 17 Abs. 1 und Abs. 3 Nr. 1 SigG, um die Geheimhaltung und Einmaligkeit der Signaturschlüssel zu gewährleisten. Die Forderung nach Einmaligkeit des Schlüssels kann mit verfügbaren Schlüsselgeneratoren erfüllt werden, so dass mit an Sicherheit grenzender Wahrscheinlichkeit ein Schlüssel kein zweites Mal erzeugt wird; selbst ein doppelt erzeugter Schlüssel stellt dann kein Problem dar, wenn beim Signieren das zugehörige Zertifikat oder ein Bezug darauf in die Signatur mit einbezogen wird. Die Forderung richtet sich zum einen an die Güte des Schlüsselgenerators und zum anderen an die Güte des Zugriffsschutzes beim Laden und Speichern der Signaturerstellungseinheit. Aus der Vorschrift ergibt sich auch, dass eine sichere Signaturerstellungseinheit einen geheimen und einmaligen Signaturschlüssel enthalten muss. Die Vorschrift erstreckt sich auf Komponenten zum Erzeugen und – soweit das Erzeugen nicht auf der sicheren Signaturerstellungseinheit selbst erfolgt – zum Laden von Signaturschlüsseln. Die Forderung, dass ein Signaturschlüssel nicht berechnet werden kann, richtet sich an die Güte der zugrunde gelegten kyrptographischen Verfahren bei der Schlüsselgenerierung und des Signaturverfahrens.

Zu Abs. 2

Die Vorschrift enthält die erforderlichen Spezifikationen für Signaturanwendungskomponenten nach § 17 Abs. 2 SigG. Dabei wird differenziert nach Erzeugung und Prüfung einer Signatur.

Damit die Erzeugung einer Signatur nur durch die berechtigte Person erfolgen kann, dürfen bei der Aktivierung der Signaturerstellungseinheit die Identifikationsdaten (z.B. die PIN) beim Vergleich mit den auf der Signaturerstellungseinheit gespeicherten Referenzdaten nicht auslesbar oder speicherbar sein (Nummer 1 Buchst. a)). Ihre Geheimhaltung ist zu jedem Zeitpunkt zu gewährleisten. Die Signaturkomponente darf nicht ohne Anwendung der Identifikationsdaten genutzt werden können, es sei denn, Signaturen sollen für ein festes Zeitfenster oder eine be-

stimmte Anzahl ohne jeweilige Identifizierung erzeugt werden. In diesem Falle ist sicherzustellen, dass Unberechtigte keine Signaturen veranlassen können (Nummer 1 Buchst. b)). Die Erzeugung einer Signatur muss durch einen Warnhinweis vorher angezeigt werden (Nummer 1 Buchst. c)). Insbesondere bei der automatischen Erzeugung von Signaturen ("Massensignaturen") muss sichergestellt sein, dass Signaturen nur zu dem voreingestellten Zweck (z.B. Signaturen zu Zahlungsanweisungen bei Grossanwendern) und durch eine zuvor geprüfte und abgenommene Anwendung vorgenommen werden können.

Bei der Prüfung einer Signatur muss der technische Vorgang der Prüfung zuverlässig erfolgen und das Ergebnis muss korrekt angezeigt werden (Nummer 2 Buchst. a)); es darf nicht vorkommen, dass nicht korrekte Ergebnisse vorgetäuscht werden können. Dies gilt entsprechend für die Nachprüfung von Zertifikaten (Nummer 2 Buchst. b)). Die Regelung zu Nummer 2 Buchst. b) ist technologieneutral.

Zu Abs. 3

Die Vorschrift enthält die erforderlichen Spezifikationen zu § 17 Abs. 3 Nr. 2 und 3 SigG.

Die Vorschrift in Satz 1 hat zum Ziel, die Zertifikatverzeichnisse vor der Aufnahme gefälschter Zertifikate und vor unbefugten Veränderungen (z.B. dem Herausnehmen gesperrter Zertifikate) zu schützen. Das Rückgängigmachen von Sperrungen durch zugriffsberechtigte Personen kann zwar mit Hilfe von technischen Mitteln nicht verhindert werden, dies darf zumindest jedoch nicht unbemerkt möglich sein.

Die nach § 5 Abs. 1 Satz 2 SigG geforderte Nachprüfbarkeit von qualifizierten Zertifikaten erfordert auch, dass die Auskünfte zuverlässig auf ihre Echtheit überprüft werden können, so dass die unbemerkte Nutzung eines vorgetäuschten echten aber tatsächlich kompromittierten Verzeichnisdienstes ausgeschlossen ist.

Um Totalfälschungen von Zertifikaten vorzubeugen und solche feststellen zu können, müssen die Auskünfte neben einer Aussage zur Sperrung auch eine Aussage darüber enthalten, ob das jeweilige Zertifikat zu einem angegebenen Zeitpunkt der Erzeugung der zu prüfenden Signatur im öffentlichen Verzeichnis der Zertifikate vorhanden war. Wer bei diesem Verfahren eine Totalfälschung eines Zertifikates erfolgreich in den Verkehr bringen wollte, müsste nicht nur eine

Zertifikatsfälschung erstellen, sondern diese zugleich in das Verzeichnis einstellen und - im Hinblick auf mögliche Kontrollen - einen gefälschten Antrag auf ein Zertifikat zur Dokumentation geben, was im Ergebnis den Beweis für die Fälschung liefern würde.

Der Nutzer muss bei Nachprüfung eines Zertifikates feststellen können zum einen, ob das Zertifikat zum angegeben Zeitpunkt im Verzeichnis vorhanden war oder nicht, zum anderen, ob es zum betreffenden Zeitpunkt gesperrt war. Bei gesperrten Zertifikaten ist eine Auskunft über das Datum und die Uhrzeit der Sperrung erforderlich.

Die Formulierung "gültige gesetzliche Zeit" in Satz 4 betrifft die gesetzliche Zeit nach dem Zeitgesetz vom 25. Juli 1978 (BGBl. I S. 1262, geändert durch Gesetz vom 13. September 1994, BGBl. I S. 2322). Danach sind im amtlichen und geschäftlichen Verkehr Datum und Uhrzeit nach der gesetzlichen Zeit zu verwenden.

Bei Verlust und anschließender Manipulation einer technischen Komponente nach Satz 4 könnten Zeitstempel nach Belieben gefälscht und verfälscht werden, wobei die Fälschungen und Verfälschungen nicht von echten Zeitstempeln zu unterscheiden wären. Damit würden auch alle zuvor mit der technischen Komponente erzeugten Zeitstempel wertlos. Technische Lösungen, die den Schutz vor Fälschung und Verfälschung zum Gegenstand haben, sind vorhanden (z.B. eine „Sicherheitsbox“, die bei Öffnung automatisch zu einer Löschung des zum Signieren von Zeitstempeln eingesetzten Signaturschlüssels führt) und können auch außerhalb eines Zertifizierungsdienstes (etwa in Behörden, Kliniken und großen Unternehmen) zum Einsatz kommen.

Zu Abs. 4

Durch das Erkennbarmachen sicherheitstechnischer Veränderungen soll der Nutzer vor sicherheitstechnischen Veränderungen geschützt werden, die z.B. eine Preisgabe des privaten Signaturschlüssels oder von Identifikationsdaten zum Ziel haben können.

Eine sicherheitstechnische Veränderung (gegenüber dem geprüften und bestätigten sicheren Zustand) liegt vor, wenn durch eine technische Veränderung die durch das Signaturgesetz und die Verordnung vorgeschriebene Sicherheit bei der Komponente nicht mehr gegeben ist. Dies kann z.B. durch äußere Zerstörung oder Funktionsausfall erkennbar werden.

Zu Abs. 5

Satz 1 enthält die Mindestanforderungen an die Bestätigungen und Herstellererklärungen nach § 17 Abs. 4 SigG, damit diese die erforderliche Aussagekraft erhalten.

Satz 2 verweist auf die Anforderungen nach Anlage 1 Abschnitt II für die Prüfung und Bestätigung von Produkten von Zertifizierungsdiensteanbietern, die nicht akkreditiert sind.

Zu Anlage 1 Abschnitt II.

Es gelten zunächst grundsätzlich auch für die nicht-akkreditierten Zertifizierungsdiensteanbieter die Anforderungen der Anlage 1 Abschnitt I. Dies gilt nach § 15 Abs. 6 und nach Anlage 1 Abschnitt II, erster Anstrich, jedoch nur, soweit noch keine Festlegungen im Rahmen des Artikel-9-Ausschusses zur Richtlinie getroffen worden sind. Ausnahmen gelten außerdem in bezug auf die in Anlage 1 Abschnitt II, zweiter Anstrich, genannten Fälle für Produkte nach § 17 Abs. 2 und 3 Nr. 2 und 3 SigG.

Zu Abs. 6

In dieser Vorschrift wird klargestellt, dass die Bestimmungen der Absätze 1 bis 5 nur solange Geltung haben, wie nicht durch Festlegungen des Artikel-9-Ausschusses etwas anderes bestimmt ist. Diese "dynamische Klausel" ermöglicht eine Übernahme der europäischen Standards ohne in jedem Fall die Verordnung zwingend ändern zu müssen. Liegen keine entsprechenden Festlegungen des Artikel-9-Ausschusses vor, so gelten die Bestimmungen der Absätze 1 bis 5 insoweit fort. In Satz 1 wird auch klargestellt, dass die Regelungen für Produkte nach § 15 Abs. 7 SigG und der Absätze 1 bis 5 von den genannten Festlegungen auf europäischer Ebene unberührt bleiben. Soweit Unternehmen die Standards nach den Absätzen 1 bis 5 i.V.m. Anlage 1 Abschnitte I oder II. erfüllen, ist eine Anpassung an die Festlegungen des Artikel-9-Ausschusses nicht erforderlich, so lange die Anforderungen nach Abs. 1 bis 5 höher liegen als die der Festlegungen des Artikel-9-Ausschusses aufgrund des Art. 3 Abs. 5 EGSRL. Da die Anforderungen nach Abs. 1 bis 5 in der Tendenz ein hohes Sicherheitsniveau, ausgehend vom SigG 97, vorschreiben, ist es nach derzeitigen Erkenntnissen nicht wahrscheinlich, dass entsprechende Anpassungen in absehbarer Zeit vorgenommen werden müssen. Die "dynamische Klausel" ermöglicht es auf der anderen Seite jedem Unternehmen in Deutschland, im Geltungsbereich der EGSRL oder im Falle der

Anerkennung des ausländischen Zertifikates nach § 23 des Signaturgesetzes auch Produkte einzusetzen, die unterhalb der Anforderungen der Abs. 1 bis 5 liegen, sofern diese verbindlich im Sinne des Absatzes 6 festgelegt worden sind.

Zur Rechtssicherheit der Beteiligten hinsichtlich der aktuell gültigen Festlegungen veröffentlicht die zuständige Behörde unverzüglich nach Vorliegen von verbindlichen Festlegungen nach der Richtlinie die dann gültigen Kriterien. Hierbei ist insbesondere auch darzulegen, wie sich diese Festlegungen in die bestehenden Standards einfügen.

Zu § 16

Ermächtigungsgrundlage dieser Vorschrift ist § 24 Nr. 5 i.V.m. § 18 SigG. In der SigV 97 wird das Verfahren der Anerkennung von Prüf- und Bestätigungsstellen nicht ausdrücklich geregelt; es finden sich dort nur zum Teil Regelungen, die die Tätigkeiten der Prüf- und Bestätigungsstellen betreffen.

Die Vorschrift ist den §§ 5, 6 und 7 UmweltauditG (Bestellung von Umweltgutachtern) entlehnt. Die Regelung trägt hinsichtlich der näheren Ausgestaltung des Verfahrens der Anerkennung und der Tätigkeit von Prüf- und Bestätigungsstellen sowohl den Anregungen aus der Rechtswissenschaft im Rahmen der Evaluierung des Signaturgesetzes (vgl. näher Begründung zu § 18 SigG) als auch den Anforderungen zur Schaffung von Kriterien für diese Stellen nach Artikel 9 i.V.m. Art. 3 Abs. 4 EGSRL Rechnung. Zugleich wird mit dieser Regelung die Entscheidung der Europäische Kommission vom 6. November 2000 über die "Mindestkriterien, die von den Mitgliedstaaten bei der Benennung der Stellen gemäss Artikel 3 Absatz 4 der Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen zu berücksichtigen sind″ (E 2000/709/EG, ABl. EG v. 16.11.2000 Nr. L 289 S. 42 - nachfolgend: "Mindestkriterien") umgesetzt.

Zu Abs. 1

Die in dieser Vorschrift aufgeführten Angaben sind zur Feststellung der Geeignetheit der Prüf- und Bestätigungsstelle erforderlich. Die Anforderungen nach Nr. 1 bis 3 enthalten Angaben gemäß Artt. 2 und 3 der Mindestkriterien. Die in der Stelle tätigen Mitarbeiter müssen angesichts der sicherheitsrelevanten Arbeiten zuverlässig sein; daher sind aktuelle Führungszeugnisse min-

destens der unter Nr. 1 und 2 genannten Personen zwingend erforderlich. Die Angaben gemäß den Anforderungen nach Nr. 4 sind zentral für die Feststellung der Unabhängigkeit der Stelle und erfüllen zugleich Art. 3 und 8 der Mindestkriterien. Die Regelung nach Nr. 5 erfüllt die Mindestkriterien nach Artt. 3, 4 und 6 bis 8; die Regelung stellt klar, dass die administrative Fachkunde auch die juristische Fachkunde umfasst: Die Ausführungen zu § 1 Abs. 2 Nr. 5 gelten entsprechend auch für diese Regelung. Die Erklärung in Nr. 6 der Vorschrift ist für die Zuordnung der gesetzlichen Tätigkeiten im Rahmen der Anerkennung der Stelle erforderlich. Die Bestimmungen zur Deckungsvorsorge in Art. 9 der Mindestkriterien gelten unmittelbar; sie können mangels Ermächtigungsgrundlage im SigG nicht in dieser Verordnung umgesetzt werden. Das Gleiche gilt für die Anforderungen an die Vertraulichkeit der Informationen nach Art. 10 der Mindestkriterien, die in der Regel durch die geltenden Datenschutzbestimmungen bereits abgedeckt sind und für die Regelung des Art. 11 der Mindestkriterien hinsichtlich der Übertragung von Aufgaben an Dritte, wobei nach § 18 SigG eine Aufgabenübertragung an Dritte nicht ausgeschlossen ist.

Zu Abs. 2

Diese Vorschrift enthält die erforderlichen zusätzlichen Anforderungen an Prüf- und Bestätigungsstellen, die im Rahmen des Verfahrens der freiwilligen Akkreditierung die Produkte für qualifizierte elektronische Signaturen nach § 15 Abs. 7 SigG evaluieren.

Zu Abs. 3

In dieser Vorschrift werden die zentralen allgemeinen Anforderungen an die Prüf- und Bestätigungsstellen zusammengefasst. In Nr. 1 werden vor allem die Anforderungen nach Artt. 3, 4, 6 und 9 der Mindestkriterien beschrieben, die eine hohe Zuverlässigkeit und Professionalität der Arbeit der Stellen und deren Beauftragten garantieren sollen. Die in Nr. 2 genannten Anforderungen beschreiben vor allem die Mindestkriterien gemäß Artt. 3 und 8 in bezug auf die Unabhängigkeit und finanzielle Absicherung der Stellen. Die Unabhängigkeit der Stelle muss umfassend sein - sie betrifft sowohl die finanzielle Unabhängigkeit als auch die sonstige Unabhängigkeit von Entwicklern, Herstellern, Lieferanten oder Installierer sicherer Signaturerstellungseinheiten. Nur eine unabhängige Stelle kann unparteiisch sein und damit die Vertrauens-Grundlage für die Sicherheit der Produkte für qualifizierte elektronische Signaturen schaffen. Die in Nr. 3

genannte Fachkunde ist Voraussetzung zur Erfüllung der in Artt. 3, 4, 6 und 7 beschriebenen Mindestkriterien hinsichtlich der Professionalität der Stelle.

Zu Abs. 4

Da die Prüf- und Bestätigungsstellen die wesentliche Verantwortung für die Einhaltung der Sicherheitsstandards der eingesetzten Produkte des Zertifizierungsdiensteanbieters tragen, ist ein hoher Maßstab hinsichtlich der Zuverlässigkeit dieser Stellen anzusetzen, der insbesondere das zum Einsatz kommende Personal betrifft.

Zu Abs. 5

Zur Rechtssicherheit der Beteiligten veröffentlicht die zuständige Behörde die näheren Einzelheiten der Anforderungen, die an die Prüf- und Bestätigungsstellen nach den Vorgaben der Richtlinie zu stellen sind.

Zu § 17

Die Vorschrift hat ihre Ermächtigungsgrundlage in § 24 Nr. 6 SigG i.V.m. § 6 Abs. 1 Satz 1 SigG-E. Sie greift auf § 18 der SigV 97 zurück.

Wenn für qualifizierte elektronische Signaturen eingesetzte Algorithmen und zugehörige Parameter – und dadurch die damit erzeugten digitalen Signaturen – infolge neuer wissenschaftlicher Erkenntnisse oder des technischen Fortschritts (z.B. Einsatz von „Quantenrechnern“) an Sicherheitswert verlieren, so ist vor Ablauf der Eignung der Algorithmen und zugehörigen Parameter eine neue qualifizierte elektronische Signatur, die mit neuen technischen Komponenten zu erzeugen ist, erforderlich. Über die Eignung der Algorithmen und zugehörigen Parameter entscheidet bei qualifizierten elektronischen Signaturen nach EG-Mindeststandard der Hersteller der jeweiligen Produkte bzw. die von ihm beauftragte Stelle nach § 18 SigG und bei qualifizierten elektronischen Signaturen nach § 15 SigG gemäß § 15 Abs. 5 dieser Verordnung die zuständige Behörde (vgl. näher Begründung zu § 15 Abs.5).

Die Anwendung neuer sicherer Signaturerstellungseinheiten ist dadurch sichergestellt, dass sich der Zertifizierungsdiensteanbieter vor der Ausstellung eines qualifizierten Zertifikates von der

Eignung der sicheren Signaturerstellungseinheit zu überzeugen hat (vgl. § 5 Abs. 6 SigG) und der Gültigkeitszeitraum für Zertifikate den Zeitraum der Eignung nicht überschreiten darf (vgl. auch § 14 Abs. 2 dieser Verordnung).

Um zu verhindern, dass neue qualifizierte elektronische Signaturen zu einem späteren Zeitpunkt angebracht und zurückdatiert werden, wenn der Sicherheitswert der früheren digitalen Signatur möglicherweise bereits so gering geworden ist, dass Fälschungen möglich sind, ist für diese ein qualifizierter Zeitstempel erforderlich.

Damit frühere qualifizierte elektronische Signaturen im Hinblick auf eventuelle spätere Fälschungsmöglichkeiten nicht bestritten werden können, müssen diese in die neue Signatur eingeschlossen und damit „konserviert“ werden. Ein Zeitstempel ist dabei ein vollständig signiertes Dokument über das gesamte zeitzustempelnde Dokument. Es ist deshalb keine weitere Signatur, z.B. eines Archivars, erforderlich. Es reicht vielmehr aus, dem Zeitstempeldienst den Hashwert des zeitzustempelnden Dokuments zu schicken, wobei das Hash-Verfahren von dem Zeitstempeldienst vorgegeben ist.

Unterbleibt bei einer vorhandenen qualifizierten elektronischen Signatur mit Ablauf der Eignung der Algorithmen und zugehörigen Parameter eine erneute Signatur, so verliert sie damit die vorgegebene Sicherheit. Unabhängig davon kann sie noch über eine längere Zeit einen hohen Sicherheitswert behalten.

Zu § 18

Ermächtigungsgrundlage dieser Vorschrift ist § 24 Nr. 7 i.V.m. § 23 SigG. In der SigV 97 findet sich eine solche Regelung nicht. Die jetzige Regelung ist vor dem Hintergrund des Erfordernisses der richtlinienkonformen Anerkennung ausländischer Zertifikate und des neu geschaffenen Verfahrens der freiwilligen Akkreditierung und der damit verbundenen spezifischen Anerkennungserfordernisse erforderlich.

Zu Absatz 1

Die Vorschrift bezieht sich auf die Anerkennung qualifizierter Zertifikate mit Rechtswirkung von Zertifizierungsdiensteanbietern aus Drittstaaten, d.h. aus Staaten außerhalb des Europäi-

schen Wirtschaftsraumes (EWR - umfasst die Europäischen Gemeinschaften, die EU-Mitgliedstaaten und die Staaten Island, Liechtenstein, Norwegen und die Schweiz) nach § 23 Abs. 1 Satz 2 Nr. 2 SigG.

Soweit ein Zertifizierungsdiensteanbieter für einen anderen Zertifizierungsdiensteanbieter in einem Drittstaat eintritt, muss bei dem anderen Zertifizierungsdiensteanbieter gleiche oder gleichwertige Sicherheit gewährleistet sein. Anderenfalls könnten die Sicherheitsbestimmungen der Richtlinie und des Signaturgesetzes umgangen werden. Die Folge wären qualifizierte Zertifikate und qualifizierte elektronische Signaturen ohne einen entsprechenden Sicherheitswert.

Die zuständige Behörde muss sich daher auch in den in Absatz 1 genannten Fällen hinreichend von der Sicherheit überzeugen können. Im Zweifelsfalle kann sie geeignete Maßnahmen im Rahmen der Aufsicht (§ 19 Abs.2 SigG) ergreifen. So kann sie z.B. von dem Zertifizierungsdiensteanbieter verlangen, dass dieser bei dem anderen Zertifizierungsdiensteanbieter eine Prüfung durch eine anerkannte Prüf- und Bestätigungsstelle (vgl. § 18 SigG) veranlasst und den Prüfbericht vorlegt.

Zu Abs. 2

Diese Vorschrift regelt die Anerkennung ausländischer elektronischer Signaturen im Hinblick auf das Verfahren der freiwilligen Akkreditierung nach § 15 SigG. Es gelten in diesem Falle für die Anerkennung ausländischer elektronischer Signaturen die gleichen Bedingungen wie für Anbieter, die das Verfahren der freiwilligen Akkreditierung nach § 15 SigG durchlaufen. Die zuständige Behörde erhält hinsichtlich der Ausgestaltung des Verfahrens zur Feststellung der gleichwertigen Sicherheit mit der zuständigen ausländischen Stelle die erforderliche Flexibilität, um die Spielräume vor dem Hintergrund der unterschiedlichen ausländischen Regelungsansätze effektiv nutzen zu können. Dies gilt jedoch nur dann, wenn es keine bilateralen oder mulitlateralen Abkommen gibt, die etwas anderes regeln. Eine "ausländische Stelle" kann eine Behörde sein oder jede andere Stelle, die in dem betreffenden ausländischen Staat mit der Anerkennung der Zertifikate betraut ist.

Zu Abs. 3

Die Vorschrift regelt die Ausgestaltung der Anerkennung von Produkten für qualifizierte elektronische Signaturen. Satz 1 betrifft die (automatische) Anerkennung von diesen Produkten aus einem EU-Mitgliedstaat oder aus dem EWR sofern diese den Anforderungen der Richtlinie entsprechen. Satz 2 betrifft die Produkte nach § 15 Abs. 7 SigG, die im Rahmen des Verfahrens der freiwilligen Akkreditierung zum Einsatz kommen. Auch hier gelten die gleichen Bedingungen wie zu Abs. 2 ausgeführt.

Zu Abs. 4

Die Vorschrift beschreibt die Pflichten der zuständigen Behörde im Zusammenhang mit der Führung des Verzeichnisdienstes im Rahmen der freiwilligen Akkreditierung - bezogen auf die qualifizierten Zertifikate nach § 23 Abs. 2 SigG.

Das Verzeichnis für die akkreditierten Zertifizierungsdiensteanbieter ist von den Verzeichnissen nach § 4 für die angezeigten Zertifizierungsdiensteanbieter zu trennen.

Soweit in einem ausländischen Staat mehrere oberste Zertifizierungsdiensteanbieter oder nur gleichrangige Zertifizierungsdiensteanbieter mit gegenseitiger Zertifizierung bestehen ("Cross-Zertifizierung"), hat die Behörde ggf. alle in ihrem Verzeichnis aufzuführen.

Die zuständige Behörde hält das Verzeichnis - wie auch die anderen Verzeichnisse nach § 16 Abs.2 SigG - unabhängig von den Vorschriften zur Bekanntmachung, auch online abrufbar.

Zu § 19

In dieser Vorschrift wird bestimmt, dass diese Verordnung die SigV 97 ablöst. Diese Regelung wurde wegen der vielfältigen Änderungen gegenüber der SigV 97 erforderlich.

Zu Anlage 1

Es wird zu Abschnitt I auf die Ausführungen zu § 11 Abs. 3 und zu Abschnitt II auf die Ausführungen zu § 15 Abs. 5 verwiesen.

Zu Anlage 2

Es wird zu Anlage 2 auf die Ausführungen zu § 12 verwiesen.