

**Begründung zur
Verordnung zur digitalen Signatur
(in der Fassung
des Beschlusses der Bundesregierung vom 8.10.1997)**

A. Allgemeiner Teil

Die Verordnung enthält die erforderlichen Ausführungsbestimmungen zum Signaturgesetz. Sie enthält wie das Gesetz grundsätzlich nur Zielvorgaben, um Raum für innovative Lösungen zu lassen. Die Regelungen beschränken sich darauf, sichere digitale Signaturen im Sinne von § 1 Abs. 1 des Signaturgesetzes zu gewährleisten. Technische Standards und betriebliche Abläufe bei der Erzeugung und Prüfung digitaler Signaturen sind nicht Regelungsgegenstand der Verordnung. Auf technische Details und betriebliche Abläufe wird in den nach § 12 Abs. 2 und § 16 Abs. 6 vorgesehenen Katalogen der zuständigen Behörde eingegangen.

B. Besonderer Teil

Zu § 1 (Verfahren bei Erteilung, Rücknahme und Widerruf von Genehmigungen)

Zu Absatz 1

Die Schriftform soll der Rechtssicherheit der Beteiligten dienen.

Zu Absatz 2

Der Antragsteller soll durch Satz 2 verpflichtet werden, der zuständigen Behörde die erforderlichen Unterlagen vorzulegen. Dazu kann z.B. auch ein Handelsregisterauszug (vgl. § 9 Abs. 2 und 3 des Handelsgesetzbuches) gehören. Darüber hinaus kann die zuständige Behörde nach pflichtgemäßem Ermessen weitere Informationen bei Dritten einholen (vgl. § 24 Verwaltungsverfahrensgesetz), z.B. über die Erfüllung von Steuerpflichten und die Liquidität des Antragstellers. Die erforderliche Fachkunde der einzelnen Mitarbeiter richtet sich nach der Art der Tätigkeit. Eine Zertifizierungsstelle benötigt in jedem Falle juristischen und informationstechnischen Sachverstand, um die Vorgaben aus dem Gesetz und der Rechtsverordnung sachgerecht erfüllen zu können. Dabei sind strenge Maßstäbe anzulegen.

Soweit eine Zertifizierungsstelle Teilaufgaben durch Dritte erledigen läßt, bleibt ihre Gesamtverantwortung unberührt. Sie hat sicherzustellen, daß von ihr mit der Durchführung von Teilaufgaben beauftragte Dritte allen Pflichten aus dem Signaturgesetz und der Signaturverordnung uneingeschränkt nachkommen. Andernfalls kann die Genehmigung versagt oder widerrufen werden.

Das Zertifizierungsverfahren umfaßt alle Abläufe von der Beantragung eines Zertifikates über das Nachprüfbarhalten der Zertifikate bis zur abschließenden Dokumentation nach § 13.

Zu Absatz 3

Durch die Regelung wird dem Verhältnismäßigkeitsgrundsatz Rechnung getragen. Abweichend von § 28 Abs. 2 und 3 Verwaltungsverfahrensgesetz ist die Anhörung in jedem Falle durchzuführen, um im Hinblick auf die teilweise komplexen organisatorischen und technischen Sachverhalte falsche Entscheidungen auszuschließen.

Zu § 2 (Kosten)

In Absatz 1 werden die gebührenpflichtigen Tatbestände bestimmt. Es sind alle wesentlichen Tatbestände, die einem einzelnen Nutznießer zugerechnet werden können, erfaßt. Die jeweilige Gebühr soll aufgrund des tatsächlichen Aufwandes im Einzelfall anhand der Gebührensätze in Absatz 2, in die die Sachkosten einbezogen sind, berechnet werden. Ausnahmen aus Gründen der Billigkeit regelt Absatz 3, wobei Ausgangspunkt die für die Erteilung der Genehmigung errechnete Gebühr ist. Im übrigen findet das Verwaltungskostengesetz Anwendung. Die Gebühr für eine Genehmigung dürfte höchstens etwa 3.000,- bis 5.000,- DM betragen. Insgesamt wird eine volle Kostendeckung für die individuell zurechenbaren Leistungen erreicht. Die Gebührensätze werden, um auch in Zukunft eine Kostenunterdeckung bei den genannten Leistungen zu vermeiden, durch die zuständige Behörde regelmäßig überprüft.

Zu § 3 (Antragsverfahren bei Vergabe von Zertifikaten)

Zu Absatz 1

Die Identifikation (Satz 1) kann auch durch örtliche Annahmestellen der Zertifizierungsstelle erfolgen. Eine Identifikation „auf andere geeignete Weise“ erfordert vergleichbare Sicherheit.

Der eigenhändig unterschriebene Antrag auf ein Zertifikat (Satz 2) ist in Verbindung mit der Identifikation nach Satz 1 und der Dokumentation nach § 13 Abs. 1 (Kopie des vorgelegten Ausweises) ein wichtiges Beweismittel, wenn ein Verdacht auf Fälschung eines Zertifikates (z.B. durch untreue Mitarbeiter der Zertifizierungsstelle oder Vorlage eines gefälschten Ausweises durch einen Antragsteller) entsteht. Damit im Rahmen der Identifikation auch ein aussagekräftiger Vergleich der Unterschrift im Ausweis und auf dem Antrag erfolgen kann, muß der Antrag bei der Annahmestelle unterschrieben werden.

Es können für eine Person für mehrere Signaturschlüssel Zertifikate ausgestellt werden. Ist ein Signaturschlüssel-Zertifikat erteilt, können weitere Anträge online mit digitaler Signatur nach dem Signaturgesetz gestellt werden (Satz 3). Einzelheiten bleiben den vertraglichen Vereinbarungen zwischen der Zertifizierungsstelle und dem Antragsteller vorbehalten.

Zu Absatz 2

Hier soll die Aufnahme einer bestehenden Vertretungsmacht oder Zulassung in ein Zertifikat geregelt werden, die nach § 5 Abs. 2 des Signaturgesetzes auf Verlangen des Antragstellers vorzunehmen ist. Dabei werden zwei Ziele verfolgt: Zum einen muß die Vertretungsmacht oder Zulassung zuverlässig nachgewiesen werden; dies erfordert eine fachkundige Prüfung der Nachweise und Angaben durch die Zertifizierungsstelle. Zum anderen muß bei Aufnahme von Vertretungsrechten die dritte Person über den Inhalt des Zertifikates sowie die Möglichkeit, dessen Sperrung zu veranlassen (vgl. § 8 Abs. 2 des Signaturgesetzes), unterrichtet sein.

Unter „dritte Personen“ 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). Dies kann z.B. durch eine notarielle Vertretungsbescheinigung, über Registerauszüge nach § 9 des Handelsgesetzbuches oder durch Attribut-Zertifikate mit Angaben über die Vertretungsmacht erfolgen. Unter „dritte Person“ fallen nur (natürliche oder juristische) Personen, deren Vertretungsrechte in ein Zertifikat aufgenommen werden (vgl. § 7 Abs. 2 des Signaturgesetzes), jedoch nicht Stellen, deren Angaben über berufsrechtliche oder sonstige Zulassungen aufgenommen werden.

Bei der Aufnahme von Angaben über Zulassungen (Satz 3) genügt die Vorlage der Zulassungsurkunde. Eine Unterrichtung der zulassenden Stelle ist nicht vorgeschrieben. Einrichtungen, die eine öffentlich-rechtliche Berufsaufsicht ausüben (z.B. Ärztekammern) können für die Aufnahme von entsprechenden beruflichen Angaben in ein Zertifikat eine eigene Zertifizierungsstelle betreiben oder mit einer bestimmten Zertifizierungsstelle einen Kooperationsvertrag schließen und Personen, die ihrer Berufsaufsicht unterliegen, anhalten, nur bei dieser Stelle entsprechende Angaben in ein Zertifikat aufnehmen zu lassen. Kommunikationspartner können auf einem Zertifikat dieser Stelle bestehen (z.B. bei Nutzung digitaler Signaturen zum Zwecke der Authentisierung).

Außer den in § 5 Abs. 2 des Signaturgesetzes vorgesehenen Angaben können auf vertraglicher Basis auch andere Angaben in Zertifikate aufgenommen werden.

Zu § 4 (Unterrichtung des Antragstellers)

Durch die vorgesehene Unterrichtung soll der Antragsteller als künftiger Signaturschlüssel-Inhaber in die Lage versetzt werden, die seinerseits erforderlichen Maßnahmen zu treffen, um sichere digitale Signaturen zu erzeugen, digitale Signaturen zuverlässig zu prüfen und einen Mißbrauch seines Signaturschlüssels durch Unbefugte sowie ein Signieren falscher Daten zu verhindern.

Es liegt alleine in der Verantwortung des Antragstellers, die notwendigen Maßnahmen, über die er unterrichtet wurde, zu treffen. Soweit er notwendige Maßnahmen (z.B. Verwendung geeigneter technischer Komponenten) unterläßt, ändert dies nichts an der Gültigkeit der mit seinem privaten Signaturschlüssel erzeugten digitalen Signaturen.

Zu Absatz 1

Zu Nummer 1

Mit der Regelung in Nummer 1 Satz 3 soll einer mißbräuchlichen Verwendung des Signaturschlüssels zusätzlich vorgebeugt werden. Ihr kann auch entsprochen werden, indem die Zertifizierungsstelle die sachgerechte Vernichtung (z.B. von Chipkarten mit Signaturschlüsseln) übernimmt.

Zu Nummer 2

Die nach Nummer 2 vorgesehene Änderung der persönlichen Identifikationsnummer oder anderer Daten (z.B. des Paßwortes) im Falle der Preisgabe kann bei modernen Verfahren durch den Nutzer selbst erfolgen.

Zu Nummer 3

Nach Nummer 3 ist der Antragsteller über die Notwendigkeit des Einsatzes geeigneter technischer Komponenten und darüber zu unterrichten, welche technischen Komponenten die gesetzlichen Anforderungen erfüllen.

Zu Nummer 4

Durch die Regelung in Nummer 4 soll der Empfänger signierter Daten unmittelbar Kenntnis erhalten, welche Beschränkungen nach § 7 Abs. 1 Nr. 7 des Signaturgesetzes und Angaben nach § 7 Abs. 2 des Signaturgesetzes er zu beachten hat.

Zu Nummer 5

Ob für die Verwendung signierter Daten ein Zeitpunkt von „erheblicher Bedeutung“ ist (Nummer 5), muß im Einzelfall geprüft werden. Erforderlich ist ein Zeitstempel z.B. bei neuen digitalen Signaturen (vgl. § 18).

Zu Nummer 6

Bezüglich Nummer 6 vgl. § 18 mit Begründung.

Zu Nummer 7

Die Feststellung der Gültigkeit der Zertifikate nach Nummer 7 schließt die Überprüfung der digitalen Signaturen zu den Zertifikaten ein. Ob die Zertifikate darüber hinaus über das jeweilige öffentliche Verzeichnis der Zertifikate nachgeprüft werden (ob sie dort verzeichnet sind und zum Zeitpunkt der Signaturerzeugung gültig waren), ist der die Signatur prüfenden Person anheimgestellt.

Zu Absatz 2

Ist eine Unterrichtung erfolgt, kann bei weiteren Anträgen auf ein Zertifikat eine Unterrichtung unterbleiben.

Zu § 5 (Erzeugung und Speicherung von Signaturschlüsseln und Identifikationsdaten)

Zu Absatz 1

Durch die Regelung wird in Verbindung mit der Unterrichtung nach § 4 ein hoher Verbraucherschutz erreicht. Die Zertifizierungsstelle muß sich zur Erfüllung der Vorgaben überzeugen, daß der Signaturschlüssel-Inhaber z.B. eine Chipkarte verwendet, deren Sicherheit nach § 17 geprüft und bestätigt ist. Zu diesem Zwecke kann der Hersteller in der Chipkarte eine Authentisierung vorsehen. Kann sich die Zertifizierungsstelle nicht in geeigneter Weise von der Sicherheit der eingesetzten technischen Komponenten überzeugen, muß die Vergabe eines Signaturschlüssel-Zertifikates unterbleiben.

Zu Absatz 2

Die Regelung soll ausschließen, daß Schlüssel oder Identifikationsdaten bei der Zertifizierungsstelle preisgegeben oder gespeichert werden. Soweit eine Preisgabe nicht vollständig ausgeschlossen werden kann, soll sie zumindest feststellbar sein. Die Eignung der von einer Zertifizierungsstelle für die Erzeugung der Schlüssel eingesetzten technischen Komponenten wird bereits im Rahmen der Kontrollen nach § 15 überprüft. Im übrigen wird eine Speicherung des privaten Signaturschlüssels außerhalb des vorgesehenen Schlüsseldatenträgers bereits durch die technischen Komponenten (vgl. § 16 Abs. 1) ausgeschlossen.

Bezüglich der Identifikationsdaten (Satz 2) können moderne technische Komponenten auch so eingestellt werden, daß der Signaturschlüssel-Inhaber vor der erstmaligen Erzeugung einer digitalen Signatur neue (selbst gewählte) Daten eingeben kann.

Zu § 6 (Übergabe von Signaturschlüsseln und Identifikationsdaten)

Die Regelung in Satz 1 hat eine zuverlässige Übergabe der privaten Signaturschlüssel und Identifikationsdaten zum Ziel. Als andere Form der Übergabe kommt, soweit der vorgesehene Signaturschlüssel-Inhaber sie verlangt und damit möglicherweise verbundene Risiken in Kauf nimmt, z.B. eine förmliche Zustellung nach der Zivilprozeßordnung an den Signaturschlüssel-Inhaber persönlich in Betracht.

Den öffentlichen Schlüssel der zuständigen Behörde (Satz 2) benötigt der Signaturschlüssel-Inhaber, um bei Bedarf überprüfen zu können, ob vorliegende Zertifikate von einer Zertifizierungsstelle nach § 4 des Signaturgesetzes stammen. Der öffentliche Schlüssel der zuständigen Behörde ist auch dann zu übergeben, wenn der Signaturschlüssel-Inhaber seine Schlüssel selbst erzeugt und von der Zertifizierungsstelle nur ein Zertifikat erhält.

Zu § 7 (Gültigkeitsdauer von Zertifikaten)

Die begrenzte Gültigkeitsdauer von Signaturschlüssel-Zertifikaten nach Satz 1 ergibt sich dadurch, daß die kryptographischen Verfahren für digitale Signaturen nur für einen begrenzten Zeitraum sicher bewertet werden können (vgl. Begründung zu § 17 Abs. 2). 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 digitalen Signatur auf dem Zertifikat ein Nachsignieren nach § 18 zu vermeiden (wenn bei den dafür eingesetzten Algorithmen und Parametern die Eignung vor Ablauf des Gültigkeitszeitraumes des Zertifikates nicht mehr gegeben sein sollte), muß die Zertifizierungsstelle auch deren Sicherheit bei der Vergabe von Zertifikaten mit berücksichtigen.

Zu § 8 (Öffentliche Verzeichnisse von Zertifikaten)

Zu Absatz 1

Innerhalb des genannten Zeitraumes müssen digitale Signaturen überprüfbar sein.

Um die Prüfung digitaler Signaturen insbesondere bei Massenanwendungen (z.B. in Banken oder Kaufhäusern) möglichst praktikabel zu gestalten, können die Zertifizierungsstellen über einen Verbund ihrer Verzeichnisse der Zertifikate jeweils alle relevanten Zertifikate (auch die der zuständigen Behörde und ggf. ausländischer Stellen) zentral nachprüfbar halten. Zur Vermeidung wiederholter Online-Anfragen können an Großanwender Sperrlisten sowie automatisch neue Sperrungen übermittelt werden, so daß bei Großanwendern nur noch ein Abgleich mit dem Datenbestand im eigenen Rechner zu erfolgen braucht. Entsprechende kommerzielle Angebote bleiben den Zertifizierungsstellen überlassen.

Eine Zertifizierungsstelle kann als zusätzliche Dienstleistung auch die Überprüfung digitaler Signaturen anbieten, die mit anderen Algorithmen oder Parametern erzeugt wurden.

Zu Absatz 2

Die Zertifizierungsstellen können ihre Signaturschlüssel selbst erzeugen und die Formate der von der zuständigen Behörde für sie auszustellenden Zertifikate selbst bestimmen (z.B. gleiches Format wie bei den selbst ausgestellten Zertifikaten), indem sie die Zertifikate vollständig vorbereiten, so daß sie von der Behörde nur noch signiert werden müssen. Die Behörde sollte für die Erzeugung ihrer Signatur auf Wunsch der Zertifizierungsstelle auch die gleichen Algorithmen und zugehörigen Parameter einsetzen wie diese.

Die Entwicklung einheitlicher Standards bei den Zertifikaten und technischen Komponenten ist Aufgabe der zuständigen Normungsgremien und der Wirtschaft. Dabei sind die internationalen Entwicklungen zu berücksichtigen.

Soweit in einem ausländischen Staat, aus dem digitale Signaturen nach § 15 des Signaturgesetzes anerkannt werden, mehrere oberste Zertifizierungsstellen (Satz 2) bestehen, sind die Zertifikate von allen anerkannten obersten Zertifizierungsstellen aufzunehmen. Da diese von der Behörde zusätzlich signiert werden (Satz 3), kann eine Überprüfung der Anerkennung der mittelbar darauf zurückzuführenden digitalen Signaturen nach § 15 des Signaturgesetzes online erfolgen.

Mit der nach Satz 4 verlangten öffentlichen Bekanntgabe der öffentlichen Schlüssel und Telekommunikationsanschlüsse für das öffentliche Verzeichnis der Zertifikate der zuständigen Behörde soll eine authentische Nachprüfung der dort geführten Zertifikate ermöglicht werden.

Zu Absatz 3

In den genannten Fällen brauchen die Zertifikate nicht mehr ständig abrufbar gehalten zu werden, da sie nur noch ausnahmsweise von Bedeutung sind (z.B. bei Überprüfung alter Signaturen, die durch neue Signaturen nach § 18 „konserviert“ wurden). In diesen Fällen genügt es, wenn auf Anfrage im Einzelfall Auskunft erteilt wird. Es steht aber nichts entgegen, diese Zertifikate bis zum Ablauf der Frist nach § 13 Abs. 2 auch weiterhin online abrufbar zu halten. Siehe auch Begründung zu § 13 Abs. 2.

Zu § 9 (Verfahren zur Sperrung von Zertifikaten)

Zu Absatz 1

Die Regelung dient dem Schutz der Signaturschlüssel-Inhaber sowie der dritten Personen, deren Angaben zur Vertretungsmacht in ein Zertifikat aufgenommen wurden. Durch die verlangte Bekanntgabe einer Rufnummer (Telefon) soll eine unverzügliche Sperrung ermöglicht werden, da eine Telefonverbindung praktisch jederzeit hergestellt werden kann. Die Bekanntgabe weiterer Telekommunikationsanschlüsse (z.B. Fax) bleibt unbenommen. Als Authentisierungsverfahren kommt z.B. ein Paßwortverfahren in Betracht.

Zu Absatz 2

Eine Sperrung soll nur unter den genannten Voraussetzungen möglich sein, um unbefugte Sperrungen auszuschließen.

Zu Absatz 3

Um keine Zweifel aufkommen zu lassen, wann ein Zertifikat gesperrt war, muß eine Sperrung endgültig sein. Bei Bedarf ist ein neues Zertifikat auszustellen. Eine mögliche Bestätigung der Sperrung gegenüber dem Signaturschlüssel-Inhaber bleibt vertraglichen Vereinbarungen überlassen. Eine rückwirkende Sperrung ist nach § 8 Abs. 1 Satz 3 des Signaturgesetzes ausgeschlossen.

Zu § 10 (Zuverlässigkeit des Personals)

Um eine Fälschung oder Verfälschung von Daten für ein Zertifikat oder einen Zeitstempel möglichst auszuschließen, müssen die beteiligten Personen zuverlässig sein. Dabei sind strenge Maßstäbe anzulegen. Die Zuverlässigkeit ist insbesondere nicht gegeben, wenn einschlägige Straftaten (z.B. Betrug, Unterschlagung oder Urkundenfälschung) begangen wurden.

Zu § 11 (Schutz der technischen Komponenten)

Der Schutz der technischen Komponenten vor unbefugtem Zugriff soll möglichen technischen Manipulationen vorbeugen. Es muß ein unbefugter Zugriff (physikalisch oder logisch, z.B. über Kommunikationsnetze) vor einer erneuten Nutzung zumindest erkannt werden, so daß ein Austausch oder eine Überprüfung der technischen Komponenten erfolgen kann.

Die Datenträger mit privaten Signaturschlüsseln, die zum Signieren von Zertifikaten oder Zeitstempeln eingesetzt werden, müssen auch vor Entwendung geschützt sein, um einem möglichen Mißbrauch vorzubeugen.

Zu § 12 (Sicherheitskonzept)

Zu Absatz 1

Das Sicherheitskonzept soll eine umfassende Übersicht über die Sicherheitsmaßnahmen der Zertifizierungsstelle geben. 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 sind. Hohe Bedeutung kommt auch den Maßnahmen zum Schutze der für ein Zertifikat bestimmten Daten vor Fälschung und Verfälschung sowie in den Fällen, in denen die Zertifikate nach dem Willen des Betroffenen nur nachprüfbar und nicht abrufbar zu halten sind, den Maßnahmen zur Wahrung der Vertraulichkeit zu. Zu diesem Zwecke können z.B. die Daten zwischen den Annahmestellen für Anträge auf Zertifikate und der jeweiligen zentralen Stelle (vgl. Begründung zu § 3 Abs. 1) bei Online-Übertragung signiert und verschlüsselt werden. Von der zentralen Stelle ausgestellte Zertifikate können von der Annahmestelle auf Übereinstimmung mit den Daten im Antrag auf ein Zertifikat überprüft werden.

Eine Zertifizierungsstelle benötigt mindestens folgende technische Komponenten: Eine Signierkomponente (z.B. Chipkarte) und einen PC für die Ausstellung von Zertifikaten/Zeitstempeln sowie einen Server für das Verzeichnis der Zertifikate nach § 8. Bei Bedarf kommen technische Komponenten zum Erzeugen und Laden von Signaturschlüsseln und Identifikationsdaten sowie ein spezieller Server für Zeitstempel hinzu. Bezüglich der Eignung der technischen Komponenten vgl. Begründung zu § 16.

Die Aufgabenwahrnehmung der Zertifizierungsstelle kann in verschiedener Weise (z.B. auch über Kooperationsverträge) organisatorisch gestaltet werden, soweit dies transparent und die Einhaltung des Signaturgesetzes und der Signaturverordnung für die Pflichtdienstleistungen gewährleistet ist. Die Gesamtverantwortung liegt beim jeweiligen Betreiber (vgl. auch Begründung zu § 1 Abs. 2). Die zuständige Behörde kann die Genehmigung für den Betrieb nach Bedarf mit Auflagen versehen.

Soweit die Zertifizierungsstelle neben den Pflichtdienstleistungen (Zertifikat- und Zeitstempelvergabe) auf vertraglicher Grundlage weitere Leistungen im Zusammenhang mit digitalen Signaturen anbietet (z.B. Überprüfung digitaler Signaturen mit fremden Algorithmen und Parametern), sollten diese in das Sicherheitskonzept einbezogen sein.

Das Sicherheitskonzept schließt auch eine Darstellung der spezifischen Bedrohungen und Risiken bei der Zertifizierungsstelle ein. Allgemeine Bedrohungen und Risiken sind bereits bei den detaillierten Sicherheitsforderungen des Signaturgesetzes und der Signaturverordnung sowie bei den Maßnahmenkatalogen nach § 12 Abs. 2 und § 16 Abs. 6 berücksichtigt.

Zu Absatz 2

Mit dem Maßnahmenkatalog sollen beispielhaft praktische Lösungen aufgezeigt werden, mit denen die Vorgaben aus Gesetz und Verordnung erfüllt werden können. Die Maßnahmen haben empfehlenden Charakter. Abweichungen bleiben möglich, um Raum für innovative andere Lösungen zu lassen. Entscheidend ist die Bestätigung der Gesetzeskonformität durch eine der anerkannten fachkompetenten Stellen. Nicht Gegenstand des Kataloges sind - direkte oder indirekte - juristische Interpretationen. Dies wird in einem Vorwort oder der Einleitung zum Katalog in geeigneter Weise zum Ausdruck gebracht.

Die zuständige Behörde (Regulierungsbehörde nach § 66 Telekommunikationsgesetz) ist Adressat dieser Vorschrift. Sie ist insgesamt verantwortlich für das Führen und die Veröffentlichung des Kataloges. Hinsichtlich der Erstellung des Kataloges berücksichtigt die Verordnung - unbeschadet der Gesamtzuständigkeit der Regulierungsbehörde - die vorhandene Fachkompetenz des Bundesamtes für Sicherheit in der Informationstechnik (BSI), das nach dem BSI-Errichtungsgesetz die Aufgabe der Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen sowie der Beratung in Fragen der informationstechnischen Sicherheit hat. Das BSI wird unter verwaltungsverfahrensrechtlichen Gesichtspunkten nicht im Wege der Amtshilfe tätig, sondern es unterstützt die Tätigkeit der zuständigen Behörde im Rahmen seiner Aufgaben nach dem BSI-Errichtungsgesetz mit einem Entwurf des Kataloges. Damit soll der Aufbau einer weiteren Fachkompetenz im Bereich der Bundesbehörden in diesen Fragen vermieden werden. Um einen möglichst breiten Konsens hinsichtlich der aufzunehmenden Sicherheitsmaßnahmen sicherzustellen, sind Experten aus Wirtschaft und Wissenschaft in den verschiedenen Verfahrensabschnitten zu beteiligen. Die verantwortliche Regulierungsbehörde ist berechtigt und verpflichtet, Bedenken, die sich aus der Beteiligung von Wissenschaft und Wirtschaft ergeben, einer Klärung und Entscheidung zuzuführen

Zu § 13 (Dokumentation)

Zu Absatz 1

Die Dokumentation der Sicherheitsmaßnahmen ist insbesondere für die Durchführung von Kontrollen nach § 13 des Signaturgesetzes und § 15 der Signaturverordnung erforderlich. Die Dokumentation der weiteren Unterlagen ist z.B. bei Verdacht auf Fälschung von Zertifikaten erforderlich. Soweit darüber hinaus automatisch Protokolldaten (z.B. zur Nutzung der privaten Signaturschlüssel der Zertifizierungsstelle) erstellt werden, liegt deren Dokumentation im Ermessen der Zertifizierungsstelle.

Durch die Regelung im letzten Satz soll die Unverfälschtheit der dokumentierten Daten gewährleistet werden. Für das Signieren der Aufzeichnungen ist ein gesonderter Signaturschlüssel erforderlich (vgl. Begründung zu § 4 Abs. 5 des Signaturgesetzes).

Zu Absatz 2

Die Bemessung der Aufbewahrungsfrist berücksichtigt insbesondere, daß auch in den Anwendungsfällen digitaler Signaturen, in denen eine regelmäßige Verjährungsfrist nach § 195 BGB (30 Jahre) relevant sein kann, eine entsprechende Aufbewahrungsfrist gewährleistet ist; sie berücksichtigt auch die zulässige Gültigkeitsdauer von Zertifikaten. Für den Fall, daß alte digitale Signaturen durch neue digitale Signaturen nach § 18 auf lange Zeit „konserviert“ werden, soll innerhalb der Verjährungsfrist eine Überprüfung der alten digitalen Signaturen möglich bleiben (z.B. durch Gerichte). Soweit in bestimmten Bereichen (z.B. der Medizin) längere Aufbewahrungsfristen erforderlich sind, muß dies über eigene Zertifizierungsstellen oder vertragliche Vereinbarungen sichergestellt werden.

Soweit die Dokumentation in digitaler Form erfolgt (z.B. bei den Zertifikaten), schließt „verfügbar“ (Satz 1) die Überprüfbarkeit ein, das heißt, es muß dafür geeignete Hard-/Software zur Verfügung stehen. Vergleichbar lange Fristen bestehen z.B. für „digitale Dokumente“ beim Flugzeugbau (50 Jahre) oder beim elektronischen Grundbuch, das auf Dauer geführt wird.

Für die Dokumentation der Auskünfte nach § 12 Abs. 2 des Signaturgesetzes wurde analog § 90 Telekommunikationsgesetz eine Aufbewahrungsfrist von 12 Monaten bestimmt.

Zu § 14 (Einstellung der Tätigkeit)

Zu Absatz 1

Durch die Regelung soll die zuständige Behörde in die Lage versetzt werden, das nach Absatz 2 bis 4 vorgeschriebene Verfahren bei Einstellung der Tätigkeit einer Zertifizierungsstelle zu überwachen.

Die genannte Frist sowie die Frist nach Absatz 2 gelten für eine normale Einstellung der Tätigkeit. Im Falle eines Konkurses sowie der Rücknahme oder des Widerrufs einer Betriebsgenehmigung können kürzere Mitteilungsfristen erforderlich sein.

Zu Absatz 2

Stellt eine Zertifizierungsstelle ihre Tätigkeit ein, so sollen die betroffenen Signaturschlüssel-Inhaber frühzeitig unterrichtet werden, um sich rechtzeitig neue Zertifikate bei einer anderen Zertifizierungsstelle beschaffen zu können. Soweit die vorhandenen Zertifikate an eine andere Zertifizierungsstelle übergeben werden sollen, können die Signaturschlüssel-Inhaber ihre Zertifikate sperren lassen, sofern sie mit der Weitergabe nicht einverstanden sind.

Werden die Zertifikate von der Zertifizierungsstelle gesperrt, weil diese keine andere Zertifizierungsstelle für die Übernahme der Zertifikate gefunden hat, so sollen die Signaturschlüssel-Inhaber über den Vorgang der Sperrung zum aktuellen Zeitpunkt unterrichtet werden.

Zu Absatz 3

Die Formerfordernisse für die Mitteilung sollen eine Fälschung der Mitteilungen verhindern.

Zu Absatz 4

Die Regelung soll sicherstellen, daß die nach dem Signaturgesetz und der Signaturverordnung vorgesehene Nachprüfbarkeit von Zertifikaten auch bei Einstellung der Tätigkeit einer Zertifizierungsstelle erhalten bleibt.

Die zuständige Behörde kann im Falle der Übernahme auch eine andere Zertifizierungsstelle mit der Verwaltung beauftragen. Die Kosten hat die abgebende Zertifizierungsstelle zu tragen (vgl. § 2 Abs. 1 Nr. 7).

Zu § 15 (Kontrolle der Zertifizierungsstellen)

Zu Absatz 1

Durch die Prüfungen soll die erforderliche Sicherheit auf Dauer gewährleistet werden. Unter „Betriebsaufnahme“ fällt nur die erstmalige Aufnahme des Betriebs. Wann eine Veränderung sicherheitserheblich ist und damit eine erneute Prüfung (neben den Regelprüfungen im Abstand von 2 Jahren) und Bestätigung nach § 4 Abs. 3 Satz 3 des Signaturgesetzes erfordert, ist im Zweifelsfalle von der Zertifizierungsstelle einvernehmlich mit der zuständigen Behörde zu klären. Bei der in der Regel üblichen dezentralen Struktur der Zertifizierungsstelle mit verteilten Annahmestellen genügt es, wenn bezüglich der praktischen Umsetzung von Gesetz und Verordnung die zentrale Stelle sowie stichprobenartig die Abwicklung bei einzelnen Annahmestellen sowie zwischen diesen und der zentralen Stelle überprüft wird.

Die nach § 4 Abs. 3 Satz 3 des Signaturgesetzes anerkannten Stellen, die die Einhaltung der Vorgaben des Signaturgesetzes und der Signaturverordnung prüfen und bestätigen, werden für die Behörde als „Verwaltungshelfer“ tätig. Die Auswahl und Anerkennung der Stellen erfolgt unter fachlichen Gesichtspunkten nach Bedarf und pflichtgemäßem Ermessen. Voraussetzung für

Prüfungen und Bestätigungen nach § 4 Abs. 3 Satz 3 des Signaturgesetzes ist der Nachweis praktischer Erfahrungen auf dem Gebiete der administrativen und technischen Sicherheit (Vorweisung von Referenzen) und ein oder mehrere erfolgreiche Prüfungen nach Absatz 1 unter fachlicher Aufsicht der zuständigen Behörde und unter Mitwirkung des BSI sein. Entsprechend den DIN EN 45000 ff. sind die Prüfung und Bestätigung durch zwei voneinander unabhängige Stellen vorzunehmen. Die Prüf- und Bestätigungsstellen bedürfen einer Anerkennung durch die zuständige Behörde. Hierfür steht zum Beispiel das Bundesamt für Sicherheit in der Informationstechnik (BSI), dem nach dem BSI-Errichtungsgesetz die Prüfung von informationstechnischen Systemen und die Beratung der Anwender in Fragen der informationstechnischen Sicherheit übertragen wurde (vgl. auch Begründung zu § 14 Abs. 4 des Signaturgesetzes), als anerkannte Stelle zur Verfügung. Es kommen aber auch weitere Prüf- und Bestätigungsstellen in Betracht.

Zu Absatz 2

Im Hinblick auf die regelmäßigen umfassenden Prüfungen nach Absatz 1 werden zusätzliche stichprobenweise und anlaßbezogene Kontrollen durch die zuständige Behörde für ausreichend angesehen. Die Häufigkeit und den Umfang der Kontrollen bestimmt sie nach pflichtgemäßem Ermessen. Im Durchschnitt ist etwa eine Kontrolle je Zertifizierungsstelle im Jahr als angemessen anzusehen. Die Kontrollen können auch technische Überprüfungen einschließen.

Zu § 16 (Anforderungen an die technischen Komponenten)

Hier sollen die Sicherheitsanforderungen an die technischen Komponenten aus § 14 des Signaturgesetzes spezifiziert werden, ohne den Raum für technische Innovation einzuengen. Die Anforderungen sind deshalb auf Zielvorgaben beschränkt.

Zu Absatz 1

Die Forderung nach Einmaligkeit des Schlüssels in Satz 1 kann mit verfügbaren Schlüsselgeneratoren erfüllt werden.

Die Geheimhaltung des Schlüssels nach Satz 2 erfordert für die Schlüsselspeicherung eine technische Komponente (z.B. Chipkarte oder Spezialkomponente für Großrechnereinsatz), die nach dem Stand der Technik nicht ausgelesen werden kann (auch nicht durch den Signaturschlüssel-Inhaber selbst). Die Signaturschlüssel können extern erzeugt und auf die Chipkarten übertragen oder bei modernen Chipkarten künftig auf diesen selbst erzeugt werden. Die Erzeugung der Schlüssel auf dem Schlüssel-datenträger selbst sollte im Hinblick auf die damit verbundene Sicherheit künftig Standard sein.

Eine sicherheitstechnische Veränderung (gegenüber dem geprüften und bestätigten sicheren Zustand) nach Satz 3 liegt vor, wenn durch eine technische Veränderung die Sicherheit der Komponente nicht mehr ausreichend gegeben ist. Sie kann z.B. durch äußere Zerstörung oder Funktionsausfall erkennbar werden. Dadurch soll der Nutzer der technischen Komponenten vor sicherheitstechnischen

Manipulationen geschützt werden, die hier insbesondere eine Preisgabe privater Signaturschlüssel zum Ziel haben können.

Zu Absatz 2

Die Signiertechnik wird in der Regel im wesentlichen auf einer Chipkarte oder einem vergleichbaren Träger (z. B. PCMCIA-Karte) realisiert. Um über Besitz (Karte) und Wissen (PIN oder Paßwort) hinaus eine Bindung des Signaturschlüssels an den Inhaber zu erreichen, können biometrische Merkmale (z.B. Gesicht, eigenhändige Unterschrift oder Fingerstruktur) genutzt werden.

Die technischen Komponenten können so gestaltet sein, daß optional vor jeder digitalen Signatur, nach einer zuvor festgelegten Anzahl von digitalen Signaturen oder nach bestimmtem Zeitablauf bei Nichtbenutzung der Signiertechnik die Identifikationsdaten erneut eingegeben werden müssen. Es liegt im Ermessen des Nutzers, wie er - abhängig von der Anwendungsumgebung - verfährt.

Durch das Erkennbarmachen sicherheitstechnischer Veränderungen nach Satz 6 soll der Nutzer vor sicherheitstechnischen Veränderungen geschützt werden, die hier insbesondere eine Preisgabe des privaten Signaturschlüssels oder der Identifikationsdaten zum Ziel haben können. Vgl. auch Begründung zu Absatz 1.

Zu Absatz 3

Wer eine digitale Signatur erzeugt, muß sicher sein können, daß angezeigte und signierte Daten (z.B. aufgerufene Datei) übereinstimmen und daß ihm nicht andere Daten zum Signieren „untergeschoben“ werden (Satz 1). Bei der Prüfung einer digitalen Signatur muß er sicher sein können, daß die Signatur der angezeigten Daten geprüft wurde und er muß sich auf die Korrektheitsbestätigung verlassen können (Satz 2).

Bei der Nachprüfung von Zertifikaten (vgl. § 4 Abs. 5 Satz 3 und § 5 Abs. 1 Satz 2 des Signaturgesetzes) muß sich der Prüfende auf die Korrektheit der in Satz 3 aufgeführten Aussagen verlassen können. Die Regelung wird ergänzt durch entsprechende Vorgaben für die technischen Komponenten zum Führen der Verzeichnisse der Zertifikate nach Absatz 4 Satz 2. Der Nutzer hat folgende Möglichkeiten, sich von der Gültigkeit von Zertifikaten zu überzeugen:

- Er kann durch eine interne Überprüfung mit Hilfe des öffentlichen Schlüssels der Regulierungsbehörde feststellen, ob das Zertifikat von einer behördlich genehmigten Zertifizierungsstelle stammt und nach den Eintragungen im Zertifikat zum (angegebenen oder vermutlichen) Zeitpunkt der Erzeugung der digitalen Signatur, die geprüft werden soll, gültig war.
- Er kann zusätzlich online eine Nachprüfung beim Verzeichnis der Zertifikate der Zertifizierungsstelle veranlassen, ob das Zertifikat dort verzeichnet und zum Zeitpunkt der Erzeugung der digitalen Signatur nicht gesperrt war. Alternativ kann er auch eine aktuelle interne Sperrliste abfragen (vgl. Begründung zu § 8 Abs. 1 und § 9 Abs. 3).

- Bei ausländischen Zertifikaten kann er zusätzlich online eine Nachprüfung beim Verzeichnis der Zertifikate der Regulierungsbehörde veranlassen, ob das Zertifikat der ausländischen Wurzelinstanz dort verzeichnet ist (vgl. § 8 Abs. 2 Satz 2 und 3).

Die digitale Signatur bezieht sich nach § 14 Abs. 2 des Signaturgesetzes nur auf die digitalen Daten und ist unabhängig von deren Interpretation (z.B. Text, Sprache, Musik, Software). Wer eine Signatur erzeugt oder prüft, muß jedoch nach Bedarf (speziell bei Texten) auch den Inhalt der zu signierenden oder signierten Daten „hinreichend“ erkennen können (Satz 4). Für bestimmte Anwendungen (z.B. home banking) können spezielle Formate und Anwendungsprogramme benutzt werden.

Werden technische Komponenten geschäftsmäßig Dritten zur Nutzung angeboten, müssen die Nutzer in die Lage versetzt werden, deren Echtheit bei Nutzungsbeginn automatisch zu überprüfen (Satz 5), um ein „Unterschieben“ von Daten über manipulierte technische Komponenten zu verhindern. Die Echtheit und der Sicherheitszustand der technischen Komponenten kann z.B. über eine automatische Authentisierung gegenüber der Chipkarte des Nutzers festgestellt werden.

Das Erkennbarmachen sicherheitstechnischer Veränderungen nach Satz 6 bezieht sich auch auf privat genutzte technische Komponenten. Vgl. auch Begründung zu Absatz 1.

Zu Absatz 4

Die Regelung hat in Ergänzung zu § 14 Abs. 3 des Signaturgesetzes zum Ziel, die vorgeschriebenen Verzeichnisse der Zertifikate vor der Aufnahme gefälschter Zertifikate und vor unbefugten Veränderungen (z.B. Herausnahme gesperrter Zertifikate) sowie die nicht abrufbar gehaltenen Zertifikate (z.B. Attribut-Zertifikate über Vertretungsrechte) vor unbefugtem Zugriff zu schützen. Soweit ein Rückgängigmachen von Sperrungen durch zugriffsberechtigte Personen (vgl. § 9 Abs. 3) technisch nicht ausgeschlossen werden kann, darf es zumindest nicht unbemerkt möglich sein.

Weiter muß eine zuverlässige Überprüfung der Echtheit der Auskünfte möglich sein, um ein Vortäuschen eines echten Verzeichnisses („sogenannte Maskerade“) auszuschließen.

Um auch Totalfälschungen vorzubeugen und solche zumindest feststellen zu können, sollen die Auskünfte neben einer Aussage zur Sperrung auch eine Aussage darüber enthalten, ob das Zertifikat im öffentlichen Verzeichnis der Zertifikate vorhanden ist. Wer bei diesem Verfahren eine Totalfälschung erfolgreich in den Verkehr bringen wollte, müßte nicht nur ein falsches Zertifikat ausstellen, sondern dieses zugleich in das Verzeichnis einstellen und im Hinblick auf mögliche Kontrollen einen gefälschten Antrag auf ein Zertifikat zur Dokumentation geben (was später ein Beweis für die Fälschung wäre). Bei Nachprüfung eines Zertifikates kann der Nutzer damit zumindest feststellen, ob das Zertifikat im Verzeichnis vorhanden ist (ja/nein) und ob es zum angegebenen Zeitpunkt (der Signaturerzeugung) gesperrt war (ja/nein). Bei gesperrten Zertifikaten ist auch eine Auskunft über das Datum und die Uhrzeit der Sperrung erforderlich.

Zertifikate, die aufgrund der Zustimmung der Signaturschlüssel-Inhaber öffentlich abrufbar gehalten werden, können außer in dem gesetzlich vorgeschriebenen Verzeichnis in gesonderten Verzeichnissen geführt werden, die nicht den gesetzlichen Bestimmungen unterliegen. Dies gilt auch für Sperrlisten (vgl. Begründung zu § 9 Abs. 3). Die Zertifikate selbst sind bereits durch ihre digitale Signatur vor Fälschung und unbemerkter Verfälschung geschützt. Ebenso können Verzeichnisse der Zertifikate und Sperrlisten durch digitale Signaturen vor unbemerkter Verfälschung geschützt werden.

Zu Absatz 5

Nach § 1 Abs. 1 des Zeitgesetzes vom 25. Juli 1978 (BGBl. I S. 1110, 1262; geändert durch Gesetz vom 13. September 1994, BGBl. I S. 2322) werden im amtlichen und geschäftlichen Verkehr Datum und Uhrzeit nach der gesetzlichen Zeit verwendet. Der Begriff „gesetzliche Zeit“ ist in § 1 Abs. 4 Zeitgesetz definiert als mitteleuropäische Zeit und schließt die Sommerzeit ein.

Die technischen Komponenten zur Erzeugung von Zeitstempeln sind in § 14 des Signaturgesetzes nicht ausdrücklich erwähnt. Ihre Einbeziehung ergibt sich mittelbar aus § 9 des Signaturgesetzes in Verbindung mit § 14 des Signaturgesetzes.

Zu Absatz 6

Mit dem Maßnahmenkatalog sollen beispielhaft praktische Maßnahmen aufgezeigt werden, mit denen die Vorgaben aus Gesetz und Verordnung erfüllt werden können. Der Katalog soll vor allem auch zu einheitlichen Standards (z.B. bei den Algorithmen mit den zugehörigen Parametern und den Formaten der Zertifikate) beitragen. Abweichungen bleiben möglich, um Raum für innovative andere Lösungen zu lassen, soweit diese den Vorgaben in Gesetz und Verordnung entsprechen. Entscheidend ist die Bestätigung der Gesetzeskonformität der technischen Komponenten durch eine der anerkannten fachkompetenten Stellen (vgl. § 14 Abs. 4 des Signaturgesetzes und § 17 Abs. 4). Der Katalog soll Produktherstellern zur Orientierung dienen und eine beschleunigte Produktprüfung (vgl. § 17) ermöglichen. Er soll in allgemeiner Form möglichst verschiedene technische Maßnahmen beschreiben, mit denen die Zielvorgaben im Gesetz und in der Verordnung erfüllt werden können. Im übrigen gelten die Ausführungen zu § 12 Abs. 2 entsprechend.

Zu § 17 (Prüfung der technischen Komponenten)

Zu Absatz 1

Die zu prüfenden technischen Komponenten und die Anforderungen an diese sind in § 16 abschließend aufgeführt.

Die genannten Kriterien (englische Bezeichnung: „Information Technology Security Evaluation Criteria - ITSEC“) sind ein internationaler Maßstab für die Bewertung der Sicherheit von informationstechnischen Komponenten und Systemen (siehe auch Ratsempfehlung 95/144/EG vom 7. April 1995). Sie unterscheiden zwischen der Prüf- bzw. Evaluationsstufe (die Skala reicht von „E 1“ bis „E 6“) und der

Stärke der zur Erreichung der Sicherheitsziele eingesetzten Mechanismen (differenziert nach gering, mittel und hoch). Sie werden ergänzt durch das (nicht im Bundesanzeiger veröffentlichte, aber den zuständigen Experten bekannte) „Handbuch für die Bewertung der Sicherheit von Systemen der Informationstechnik“ (englische Bezeichnung: „Information Technology Security Evaluation Manual - ITSEM“). Falls künftig praktisch erprobte neue Kriterien vorliegen, wird die Verordnung bei Bedarf angepaßt.

Bei der entscheidenden Stärke der Mechanismen verlangt die Verordnung durchgehend die Stufe „hoch“ und bei den Algorithmen und zugehörigen Parametern nach Absatz 2 zusätzlich eine ausdrückliche Eignungsfeststellung. Die Voraussetzungen für die Bewertung eines Mechanismus mit „hoch“ sind in den ITSEC wie folgt beschrieben: „Damit die Mindeststärke eines kritischen Mechanismus als hoch eingestuft werden kann, muß erkennbar sein, daß er nur von Angreifern überwunden werden kann, die über sehr gute Fachkenntnisse, Gelegenheiten und Betriebsmittel verfügen, wobei ein solcher erfolgreicher Angriff als normalerweise nicht durchführbar beurteilt wird.“

Bei der Prüfstufe werden - abhängig von den unterschiedlichen Risiken - differenzierte Anforderungen gestellt. Die hohe Prüfstufe „E 4“ wird für die technischen Komponenten gefordert, die der Sicherheit der Signaturschlüssel und der Geheimhaltung des privaten Signaturschlüssels dienen sowie für technische Komponenten, die geschäftsmäßig Dritten zur Nutzung angeboten werden. In beiden Fällen können versteckte Fehler/Manipulationen breite Auswirkungen haben. Andererseits handelt es sich dabei um überschaubare Spezialkomponenten, so daß die aufwendige Prüfung (z.B. mit Erstellung eines formalen Sicherheitsmodells) mit vertretbarem Aufwand durchgeführt werden kann. Im übrigen erscheint die heutige Standardprüfstufe „E 2“ (z.B. mit einer Überprüfung der Implementierung der Mechanismen, einer Schwachstellenanalyse und Tests zur Fehlersuche) ausreichend und nach dem Stand der Technik mit einem vertretbaren Aufwand realisierbar. Dies gilt auch für die technischen Komponenten zur Prüfung einer digitalen Signatur, da dafür nur der öffentliche Schlüssel eingesetzt wird.

Durch die Eignungsfeststellung der mathematischen Verfahren, die geforderte Mechanismenstärke „hoch“ und risikobezogene Prüfungen wird ein einheitlich hohes Mindestmaß an Sicherheit erreicht. Hinzu kommen stichprobenweise sowie anlaßbezogene Nachprüfungen in Form von Gutachten nach Absatz 3 Satz 3. Die vorgegebene Mindesthöhe der Prüfstufen kann im Rahmen des freien Wettbewerbs auch übertroffen werden, etwa bei speziellen Komponenten für electronic banking.

Bezogen auf die einzelnen technischen Komponenten ergibt sich danach folgendes:

- Komponente zur Schlüsselerzeugung (einschl. Ladvorgang) E 4 hoch
- Komponente zur Speicherung und Anwendung des privaten Signaturschlüssels E 4 hoch
- Übrige Komponente zur Erzeugung digitaler Signaturen einschließlich E 2 hoch
 - Erfassen und Prüfen von Identifikationsdaten
 - Darstellen zu signierender Daten
- Komponenten zur Prüfung digitaler Signaturen einschließlich E 2 hoch
 - Darstellen signierter Daten
 - Nachprüfen von Zertifikaten
- Komponente zum Nachprüfbarhalten von Zertifikaten E 2 hoch
- Komponente zum Erzeugen von Zeitstempeln E 2 hoch
- Komponente zur Erzeugung und Prüfung digitaler Signaturen, die geschäftsmäßig Dritten zur Nutzung angeboten werden E 4 hoch

Die Algorithmen und zugehörigen Parameter müssen den Vorgaben nach Absatz 2 entsprechen.

Zu Absatz 2

Die Grundlage für die Sicherheit digitaler Signaturen bilden die eingesetzten Algorithmen (kryptographischen Verfahren) und zugehörigen Parameter (z.B. Schlüssellänge). Ihre Eignung soll deshalb unter Nutzung des kryptographischen Sachverständes in Behörden, Wirtschaft und Wissenschaft festgestellt und die Eignungsfeststellung auf einen Zeitraum beschränkt werden, für den zuverlässige Aussagen getroffen werden können. Der Zeitraum von sechs Jahren ist nach Einschätzung der Experten im Hinblick auf eine mögliche zeitbedingte Minderung des Sicherheitswertes von Algorithmen mit den zugehörigen Parametern hinreichend überschaubar. Soweit es sachlich begründet ist, kann der Zeitraum auch kürzer oder länger gewählt werden („soll“). Die dem BSI auferlegte Zurückhaltung bei der Bewertung von Algorithmen zum Ver- und Entschlüsseln (wegen der teilweisen Geheimhaltungsbedürftigkeit des dortigen „know-how“) gilt nicht für Algorithmen, die für die digitale Signatur benötigt werden.

Beim „Hashen“ zu signierender Daten wird von diesen ein einmaliger „digitaler Fingerabdruck“ genommen, der dann anstelle der Gesamtdaten signiert wird. Der Hash-Algorithmus muß sicherstellen, daß nicht zu unterschiedlichen Daten gleiche Hash-Werte erzielt werden können.

Der im Regelfall vorgesehene Mindestzeitraum von sechs Jahren für die Eignungsfeststellung und die jährliche Neubewertung belassen bei frühzeitiger Ankündigung einer ausbleibenden Verlängerung der Eignungsfeststellung um ein weiteres Jahr einen Zeitraum von mindestens einem Jahr für die Einführung neuer Produkte (dann beginnt die Frist von fünf Jahren für die Gültigkeit neuer Zertifikate nach § 7 Abs. 2 Satz 1, die vollständig durch die Verwendung geeigneter Algorithmen und Parameter abgedeckt sein muß).

Da die Ablösung durch neue geeignete technische Komponenten in der Regel nur sukzessive erfolgen kann, wird es notwendig sein, daß alte und neue technische Komponenten für eine Übergangszeit gleichzeitig eingesetzt werden.

Bezüglich der Mitwirkung des Bundesamtes für Sicherheit in der Informationstechnik gelten die Ausführungen zu § 12 Abs. 2 und § 16 Abs. 6 entsprechend.

Zu Absatz 3

Satz 1 soll eindeutige Aussagen über die Eignung von Produkten sicherstellen.

Die folgenden Bestimmungen sollen im Rahmen der gewählten Struktur (private Stellen im Wettbewerb) eine einheitlich hohe Sicherheitsqualität bei den technischen Komponenten sicherstellen.

Bei Gutachten nach Satz 3 kann die zuständige Behörde auf das Bundesamt für Sicherheit in der Informationstechnik zurückgreifen, soweit die Prüfung oder Bestätigung nicht von diesem selbst stammt.

Stellt sich heraus, daß die Prüfung oder Bestätigung einer anerkannten Stelle für technische Komponenten nicht korrekt war, kann die Behörde dieser die Anerkennung entziehen.

Wird eine Bestätigung für eine technische Komponente für ungültig erklärt (Satz 5), so ist dies gemäß Absatz 4 öffentlich bekannt zu geben. Darüber hinaus kann die zuständige Behörde, wenn Komponenten zum Erzeugen von Signaturschlüsseln oder Speichern und Anwenden privater Signaturschlüssel betroffen sind, unter den Voraussetzungen von § 13 Abs. 5 Satz 2 des Signaturgesetzes auch eine Sperrung von Zertifikaten anordnen. Die Zertifizierungsstellen haben bei der Ausstellung von Zertifikaten in jedem Falle sicherzustellen, daß die betroffene technische Komponente nicht mehr zum Einsatz kommt (vgl. § 5 Abs. 1).

Zu Absatz 4

Die nach § 14 Abs. 4 des Signaturgesetzes anerkannten Stellen und die technischen Komponenten mit einer Bestätigung dieser Stellen sollen öffentlich bekannt sein, damit sich jedermann nach Bedarf danach richten kann.

Die nach § 14 Abs. 4 des Signaturgesetzes anerkannten Stellen werden für die Behörde als „Verwaltungshelfer“ tätig. Es sollen mehrere private (Sicherheitszertifizierungs-) Stellen anerkannt werden, die die Gesetzeskonformität von technischen Komponenten nach § 14 Abs. 4 des Signaturgesetzes bestätigen dürfen.

Zu § 18 (Erneute digitale Signatur)

Wenn für digitale Signaturen eingesetzte Algorithmen und zugehörige Parameter - und dadurch die damit erzeugten digitalen Signaturen - infolge neuer wissenschaftlicher Erkenntnisse oder des technischen Fortschritts (z. B. schnellere Rechner) an Sicherheitswert verlieren, so ist vor Ablauf der Eignung der Algorithmen und zugehörigen Parameter eine neue digitale Signatur (mit neuen technischen Komponenten) erforderlich. Die Anwendung neuer technischer Komponenten für die Erzeugung neuer Signaturen ist dadurch sichergestellt, daß sich die Zertifizierungsstelle vor der Ausstellung eines Signaturschlüssel-Zertifikates von der Eignung der technischen Komponenten zu überzeugen hat (vgl. § 5 Abs. 1) und der Gültigkeitszeitraum für Zertifikate den Zeitraum der Eignung nicht überschreiten darf (vgl. § 7 Abs. 2).

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

Damit frühere digitale Signaturen im Hinblick auf eventuelle spätere Fälschungsmöglichkeiten nicht bestritten werden können, müssen diese in die neue Signatur eingeschlossen und damit „konserviert“ werden. Dabei genügt für eine beliebige Anzahl signierter Daten eine (übergreifende) neue digitale Signatur, die von einer beliebigen Person (z.B. Archivar) angebracht werden kann.

Unterbleibt bei einer vorhandenen digitalen Signatur mit Ablauf der Eignung der Algorithmen und zugehörigen Parameter nach § 17 Abs. 2 eine erneute digitale Signatur, so verliert sie damit die gesetzlich vorgegebene Sicherheit. Unabhängig davon kann sie noch über eine längere Zeit einen hohen Sicherheitswert behalten. Dessen Bewertung bleibt im Streitfalle dann jedoch Gerichten und Sachverständigen überlassen.

Zu § 19 (Inkrafttreten)

Die Verordnung soll zum 1. November 1997 und damit zeitnah zum Gesetz in Kraft treten. Die nach der Verordnung vorgesehenen Maßnahmenkataloge nach § 12 Abs. 2 und § 16 Abs. 6 sollen ebenfalls zeitnah veröffentlicht werden.