Verordnung zur digitalen Signatur
(Signaturverordnung - SigV)

Aufgrund des § 16 des Signaturgesetzes vom 22. Juli 1997 (BGBl. I S. 1870, 1872) verordnet die Bundesregierung:

Inhaltsübersicht

§ 1 Verfahren bei Erteilung, Rücknahme und Widerruf von Genehmigungen

(1) Eine Genehmigung für den Betrieb einer Zertifizierungsstelle nach § 4 Abs. 1 des Signaturgesetzes ist schriftlich bei der zuständigen Behörde zu beantragen.

(2) Zur Prüfung der Voraussetzungen für die Erteilung der Genehmigung trifft die zuständige Behörde die erforderlichen Feststellungen. Sie kann vom Antragsteller verlangen, daß dieser erforderliche Unterlagen, insbesondere einen aktuellen Handelsregisterauszug und aktuelle Führungszeugnisse nach § 30 Abs. 5 des Bundeszentralregistergesetzes für die gesetzlichen Vertreter der Zertifizierungsstelle, beibringt. Zur Feststellung der erforderlichen Fachkunde hat der Antragsteller darzulegen, daß das am Zertifizierungsverfahren oder an der Ausstellung von Zeitstempeln beteiligte Personal über die erforderlichen beruflichen Qualifikationen verfügt.

(3) Vor Ablehnung, Rücknahme oder Widerruf einer Genehmigung hat die zuständige Behörde den Antragsteller anzuhören und ihm Gelegenheit zu geben, die Gründe für die Ablehnung, die Rücknahme oder den Widerruf zu beseitigen.

§ 2 Kosten

(1) Für folgende öffentliche Leistungen werden Kosten (Gebühren und Auslagen) erhoben:

1. die Erteilung einer Genehmigung für den Betrieb einer Zertifizierungsstelle,
2. die Ablehnung eines Antrags auf Erteilung einer Genehmigung,
3. die Rücknahme oder den Widerruf einer Genehmigung,
4. die vollständige oder teilweise Zurückweisung eines Widerspruchs,
5. die Ausstellung von Zertifikaten,
6. die Überprüfung von Prüfberichten und Bestätigungen nach § 15 Abs. 1,
7. die Kontrollen nach § 15 Abs. 2, wenn im Rahmen der Kontrolle ein nicht nur unerheblicher Verstoß gegen das Signaturgesetz oder gegen diese Verordnung festgestellt wird,
8. die Übernahme einer Dokumentation nach § 11 Abs. 2 des Signaturgesetzes.

Kosten werden auch dann erhoben, wenn ein Antrag auf Erteilung einer Genehmigung oder ein Widerspruch nach Beginn der sachlichen Bearbeitung, aber vor deren Beendigung zurückgenommen wird.

(2) Bei der Berechnung der Gebühren für öffentliche Leistungen nach Absatz 1 Nr. 1, 5, 6, 7 und 8 sind folgende Stundensätze zugrunde zu legen:

1. Beamte des mittleren Dienstes oder vergleichbare Angestellte: 85 Deutsche Mark,
2. Beamte des gehobenen Dienstes oder vergleichbare Angestellte: 105 Deutsche Mark,
3. Beamte des höheren Dienstes oder vergleichbare Angestellte: 135 Deutsche Mark.

Für jede angefangene Viertelstunde ist ein Viertel dieser Stundensätze zu berechnen. Werden öffentliche Leistungen durch Angehörige der zuständigen Behörde außerhalb der Behörde erbracht, so sind Gebühren ferner zu berechnen für Reisezeiten, die innerhalb der üblichen Arbeitszeit liegen oder von der zuständigen Behörde besonders abgegolten werden, sowie für Wartezeiten, die der Kostenschuldner verursacht hat.

(3) Für die Fälle der Ablehnung oder Zurücknahme eines Antrages auf Erteilung einer Genehmigung sowie der Rücknahme oder des Widerrufs einer Genehmigung gilt § 15 des Verwaltungskostengesetzes. Für die vollständige oder teilweise Zurückweisung eines Widerspruchs kann eine Gebühr bis zur Höhe der für den angefochtenen Verwaltungsakt erhobenen Gebühr erhoben werden. Für die Zurückweisung und in den Fällen der Zurücknahme eines ausschließlich gegen eine Kostenentscheidung gerichteten Widerspruchs kann eine Gebühr bis zur Höhe von 10 vom Hundert des streitigen Betrages erhoben werden.

§ 3 Antragsverfahren bei Vergabe von Zertifikaten

(1) Die Zertifizierungsstelle hat die Identifikation des Antragstellers gemäß § 5 Abs. 1 Satz 1 des Signaturgesetzes anhand des Bundespersonalausweises oder Reisepasses oder auf andere geeignete Weise vorzunehmen. Der Antrag auf ein Zertifikat muß eigenhändig unterschrieben sein. Soweit ein Antrag auf ein Zertifikat mit einer digitalen Signatur des Antragstellers versehen ist, kann die Zertifizierungsstelle von einer erneuten Identifikation und eigenhändigen Unterschrift absehen.

(2) Sollen nach § 5 Abs. 2 des Signaturgesetzes in ein Zertifikat Angaben über die Vertretungsmacht für eine dritte Person aufgenommen werden, muß die Vertretungsmacht zuverlässig nachgewiesen sein und eine schriftliche oder mit einer digitalen Signatur versehene Einwilligung der dritten Person vorliegen. Die dritte Person ist schriftlich oder in digitaler Form mit digitaler Signatur über den Inhalt des Zertifikates zu unterrichten und auf die Möglichkeit der Sperrung nach § 9 Abs. 1 hinzuweisen. Eine berufsrechtliche oder sonstige Zulassung ist insbesondere durch Vorlage der Zulassungsurkunde nachzuweisen.

§ 4 Unterrichtung des Antragstellers

(1) Die Zertifizierungsstelle hat einen Antragsteller im Rahmen des § 6 Satz 1 und 3 des Signaturgesetzes insbesondere über folgende erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der digitalen Signatur zu unterrichten:

1. Der Datenträger mit dem privaten Signaturschlüssel ist in persönlichem Gewahrsam zu halten. Bei dessen Verlust ist unverzüglich die Sperrung des Signaturschlüssel-Zertifikates zu veranlassen. Wird der Datenträger mit dem privaten Signaturschlüssel nicht mehr benötigt, ist er unbrauchbar zu machen und die Sperrung des Signaturschlüssel-Zertifikates zu veranlassen, falls es nicht abgelaufen ist.

2. Persönliche Identifikationsnummern oder andere Daten zur Identifikation gegenüber dem Datenträger mit dem privaten Signaturschlüssel sind geheim zu halten. Bei Preisgabe oder Verdacht der Preisgabe dieser Identifikationsdaten ist unverzüglich deren Änderung vorzunehmen.

3. Für die Erzeugung und Prüfung digitaler Signaturen sowie die Darstellung von zu signierenden oder zu prüfenden signierten Daten sind technische Komponenten einzusetzen, die den Anforderungen des Signaturgesetzes und dieser Verordnung entsprechen und deren Sicherheit nach dem Signaturgesetz und dieser Verordnung bestätigt wurde. Sie sind vor unbefugtem Zugriff zu schützen.

4. Soweit ein Zertifikat Beschränkungen nach § 7 Abs. 1 Nr. 7 des Signaturgesetzes oder Angaben nach § 7 Abs. 2 des Signaturgesetzes enthält und dies für die Aussage von signierten Daten von Bedeutung ist, ist das Zertifikat den Daten beizufügen und in die digitale Signatur einzuschließen.

5. Soweit für die Verwendung signierter Daten ein Zeitpunkt von erheblicher Bedeutung sein kann, ist ein Zeitstempel anzubringen.

6. Werden Daten über längere Zeit in signierter Form benötigt, ist gemäß § 18 erneut eine digitale Signatur anzubringen.

7. Bei der Prüfung digitaler Signaturen ist festzustellen, ob das Signaturschlüssel-Zertifikat und Attribut-Zertifikate zum Zeitpunkt der Signaturerzeugung gültig waren, das Signaturschlüssel-Zertifikat gemäß § 7 Abs. 1 Nr. 7 des Signaturgesetzes Beschränkungen enthält und gegebenenfalls die Nummern 4 und 5 beachtet wurden.

(2) Soweit ein Antragsteller bereits über ein Zertifikat verfügt, kann eine erneute Unterrichtung unterbleiben.

§ 5 Erzeugung und Speicherung von Signaturschlüsseln und Identifikationsdaten

(1) Werden Signaturschlüssel durch den Signaturschlüssel-Inhaber erzeugt, so hat sich die Zertifizierungsstelle zu überzeugen, daß er hierfür sowie für die Speicherung und Anwendung des privaten Signaturschlüssels geeignete technische Komponenten nach dem Signaturgesetz und dieser Verordnung einsetzt.

(2) Werden Signaturschlüssel durch die Zertifizierungsstelle bereitgestellt, so hat diese Vorkehrungen zu treffen, um eine Preisgabe von privaten Schlüsseln und eine Speicherung bei der Zertifizierungsstelle auszuschließen. Dies gilt auch für persönliche Identifikationsnummern oder andere Daten zur Identifikation des Signaturschlüssel-Inhabers gegenüber dem Datenträger mit dem privaten Signaturschlüssel.

§ 6 Übergabe von Signaturschlüsseln und Identifikationsdaten

Soweit die Zertifizierungsstelle Signaturschlüssel oder Identifikationsdaten nach § 5 Abs. 2 bereitstellt, hat sie den privaten Signaturschlüssel sowie die Identifikationsdaten dem Signaturschlüssel-Inhaber persönlich zu übergeben und die Übergabe von diesem schriftlich bestätigen zu lassen, es sei denn, dieser verlangt schriftlich eine andere Übergabe. Mit Übergabe des privaten Signaturschlüssels oder Signaturschlüssel-Zertifikates hat sie auch den öffentlichen Signaturschlüssel der zuständigen Behörde zu übergeben.

§ 7 Gültigkeitsdauer von Zertifikaten

Die Gültigkeitsdauer eines Zertifikates darf höchstens fünf Jahre betragen und den Zeitraum der Eignung der eingesetzten Algorithmen und zugehörigen Parameter nach § 17 Abs. 2 nicht überschreiten. Die Gültigkeit eines Attribut-Zertifikates endet spätestens mit der Gültigkeit des Signaturschlüssel-Zertifikates, auf das es Bezug nimmt.

§ 8 Öffentliche Verzeichnisse von Zertifikaten

(1) Die Zertifizierungsstelle hat die von ihr ausgestellten Zertifikate mindestens solange in einem Verzeichnis gemäß den Vorgaben nach § 5 Abs. 1 Satz 2 des Signaturgesetzes zu führen, wie der im Zertifikat aufgeführte Algorithmus mit den dazugehörigen Parametern nach § 17 Abs. 2 als geeignet beurteilt wird.

(2) Die zuständige Behörde hat die von ihr ausgestellten Zertifikate für die in Absatz 1 genannte Dauer in einem Verzeichnis gemäß den Vorgaben nach § 4 Abs. 5 Satz 3 des Signaturgesetzes zu führen. Dies gilt auch für Zertifikate für öffentliche Signaturschlüssel oberster ausländischer Zertifizie-

rungsstellen, soweit ausländische Zertifikate anerkannt werden. Bei den im Verzeichnis enthaltenen ausländischen Zertifikaten hat die zuständige Behörde die Anerkennung durch eine digitale Signatur zu bestätigen. Die zuständige Behörde hat die Telekommunikationsanschlüsse, unter denen die Zertifikate abrufbar sind, sowie ihre öffentlichen Schlüssel im Bundesanzeiger zu veröffentlichen und den Zertifizierungsstellen unmittelbar bekanntzugeben.

(3) Nach Ablauf der in Absatz 1 genannten Frist haben die Zertifizierungsstelle und die zuständige Behörde eine Nachprüfung der Zertifikate bis zum Ablauf der in § 13 Abs. 2 genannten Frist auf Antrag im Einzelfall zu ermöglichen.

§ 9 Verfahren zur Sperrung von Zertifikaten

(1) Die Zertifizierungsstelle hat den Signaturschlüssel-Inhabern und dritten Personen, von denen Angaben zur Vertretungsmacht in ein Zertifikat aufgenommen wurden, sowie der zuständigen Behörde eine Rufnummer bekanntzugeben, unter der diese jederzeit eine unverzügliche Sperrung der Zertifikate veranlassen können und dafür ein Authentisierungsverfahren anzubieten.

(2) Die Zertifizierungsstelle hat ein Zertifikat unter den Voraussetzungen des § 8 des Signaturgesetzes zu sperren, wenn ein mit einer digitalen Signatur versehener oder schriftlicher Antrag des Signaturschlüssel-Inhabers oder seines Vertreters oder einer berechtigten dritten Person nach Absatz 1 vorliegt oder wenn ein vereinbartes Authentisierungsverfahren angewandt wurde.

(3) Die Sperrung von Zertifikaten ist mit Angabe des Datums und der Uhrzeit im Verzeichnis nach § 8 des Signaturgesetzes eindeutig kenntlich zu machen und darf nicht rückgängig gemacht werden.

§ 10 Zuverlässigkeit des Personals

Die Zertifizierungsstelle hat sich von der Zuverlässigkeit von Personen, die am Zertifizierungsverfahren oder an der Ausstellung von Zeitstempeln mitwirken, zu überzeugen. Sie kann hierzu insbesondere die Vorlage eines Führungszeugnisses nach § 30 Abs. 1 des Bundeszentralregistergesetzes verlangen. Unzuverlässige Personen sind vom Zertifizierungsverfahren und der Ausstellung von Zeitstempeln auszuschließen.

§ 11 Schutz der technischen Komponenten

Die Zertifizierungsstelle hat Vorkehrungen zu treffen, um private Signaturschlüssel und die zum Erstellen der Zertifikate und Zeitstempel sowie zum Nachprüfbarhalten der Zertifikate eingesetzten technischen Komponenten vor unbefugtem Zugriff zu schützen.

§ 12 Sicherheitskonzept

(1) Das Sicherheitskonzept nach § 4 Abs. 3 Satz 3 des Signaturgesetzes hat alle Sicherheitsmaßnahmen sowie insbesondere eine Übersicht über die eingesetzten technischen Komponenten und eine Darstellung der Ablauforganisation der Zertifizierungstätigkeit zu enthalten. Im Falle sicherheitserheblicher Veränderungen ist das Konzept unverzüglich anzupassen.

(2) Die zuständige Behörde führt einen Katalog von geeigneten Sicherheitsmaßnahmen, den sie im Bundesanzeiger veröffentlicht. Die Maßnahmen sollen bei der Erstellung des Sicherheitskonzeptes berücksichtigt werden. Der Katalog wird nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik erstellt. Experten aus Wirtschaft und Wissenschaft sind zu beteiligen.

§ 13 Dokumentation

(1) Die Dokumentation nach § 10 des Signaturgesetzes hat sich auf das Sicherheitskonzept einschließlich der Änderungen, die Prüfberichte und Bestätigungen nach § 15 Abs. 1, die vertraglichen Vereinbarungen mit den Antragstellern und die von der zuständigen Behörde erhaltenen Zertifikate zu erstrecken. Zu den eingegangenen Anträgen auf Zertifikate und Vereinbarungen mit den Antragstellern sind eine Ablichtung des vorgelegten Ausweises oder eines anderen Identitätsnachweises, die für die Aufnahme von Angaben dritter Personen erforderlichen Unterlagen, die Vergabe eines Pseudonyms, der Nachweis über die vorgeschriebene Unterrichtung des Antragstellers und dritter Personen, die erteilten Zertifikate mit dem jeweiligen Zeitpunkt der Ausstellung und der Übergabe, die Sperrung von Zertifikaten und Auskünfte nach § 12 Abs. 2 des Signaturgesetzes zu dokumentieren. Soweit die Zertifizierungsstelle Signaturschlüssel oder Identifikationsdaten nach § 5 Abs. 2 bereitstellt, sind der Zeitpunkt der Übergabe und die Übergabebestätigung zu dokumentieren. In digitaler Form geführte Aufzeichnungen müssen digital signiert sein.

(2) Die Dokumentation nach Absatz 1 ist mindestens 35 Jahre ab dem Zeitpunkt der Ausstellung des Signaturschlüssel-Zertifikates aufzubewahren und so zu sichern, daß sie innerhalb dieses Zeitraums verfügbar bleibt. Die Dokumentation von Auskünften nach § 12 Abs. 2 Satz 2 des Signaturgesetzes ist zwölf Monate aufzubewahren.

§ 14 Einstellung der Tätigkeit

(1) Die Zertifizierungsstelle hat, wenn sie ihre Tätigkeit nach § 11 Abs. 1 des Signaturgesetzes einstellen will, dies spätestens vier Monate vorher der zuständigen Behörde mitzuteilen.

(2) Vor Beendigung ihrer Tätigkeit hat die Zertifizierungsstelle für jedes nicht gesperrte und zum Zeitpunkt der Beendigung der Tätigkeit nicht abgelaufene Zertifikat dem Signaturschlüssel-Inhaber mit

einer Frist von mindestens drei Monaten mitzuteilen, daß sie ihre Tätigkeit als Zertifizierungsstelle einstellen will und ihn zu unterrichten, ob eine andere Zertifizierungsstelle das Zertifikat übernimmt und diese zu benennen. Soweit nicht eine andere Zertifizierungsstelle die Zertifikate übernimmt, sind nach Ablauf der in Absatz 1 genannten Frist alle Zertifikate zu sperren, die zu diesem Zeitpunkt nicht bereits gesperrt oder abgelaufen sind. Die Signaturschlüssel-Inhaber der zu sperrenden Zertifikate sind darüber zu unterrichten.

(3) Die Mitteilung an die zuständige Behörde und die Unterrichtung der Signaturschlüssel-Inhaber haben in digitaler Form mit digitaler Signatur oder schriftlich zu erfolgen.

(4) Die Zertifizierungsstelle, die nach § 11 Abs. 2 des Signaturgesetzes die Dokumentation übernimmt, oder andernfalls die zuständige Behörde hat die Zertifikate in einem Verzeichnis nach § 8 Abs. 1 und 3 zu führen.

§ 15 Kontrolle der Zertifizierungsstellen

(1) Die Zertifizierungsstelle hat vor Betriebsaufnahme, nach sicherheitserheblichen Veränderungen sowie regelmäßig im Abstand von zwei Jahren eine Prüfung nach § 4 Abs. 3 Satz 3 des Signaturgesetzes zu veranlassen und der zuständigen Behörde einen Prüfbericht und eine Bestätigung darüber vorzulegen, daß sie die Vorgaben aus dem Signaturgesetz und dieser Verordnung erfüllt.

(2) Die zuständige Behörde kann in angemessenen Zeitabständen sowie bei Anhaltspunkten für eine Verletzung von Vorschriften des Signaturgesetzes oder dieser Verordnung Kontrollen durchführen.

§ 16 Anforderungen an die technischen Komponenten

(1) Die zur Erzeugung von Signaturschlüsseln erforderlichen technischen Komponenten müssen so beschaffen sein, daß ein Schlüssel mit an Sicherheit grenzender Wahrscheinlichkeit nur einmal vorkommt und aus dem öffentlichen Schlüssel nicht der private Schlüssel errechnet werden kann. Die Geheimhaltung des privaten Schlüssels muß gewährleistet sein und er darf nicht dupliziert werden können. Sicherheitstechnische Veränderungen an den technischen Komponenten müssen für den Nutzer erkennbar werden.

(2) Die zur Erzeugung oder Prüfung digitaler Signaturen erforderlichen technischen Komponenten müssen so beschaffen sein, daß aus der Signatur nicht der private Signaturschlüssel errechnet oder die Signatur auf andere Weise gefälscht werden kann. Der private Signaturschlüssel darf erst nach Identifikation des Inhabers durch Besitz und Wissen angewendet werden können und bei der Anwendung nicht preisgegeben werden. Zur Identifikation des Signaturschlüssel-Inhabers können zusätzlich biometrische Merkmale genutzt werden. Die zum Erfassen von Identifikationsdaten erforderlichen

technischen Komponenten müssen so beschaffen sein, daß sie die Identifikationsdaten nicht preisgeben und diese nur auf dem Datenträger mit dem privaten Signaturschlüssel gespeichert werden. Sicherheitstechnische Veränderungen an den technischen Komponenten müssen für den Nutzer erkennbar werden.

(3) Die zum Darstellen zu signierender Daten erforderlichen technischen Komponenten müssen so beschaffen sein, daß die signierende Person die Daten, auf die sich die Signatur erstrecken soll, eindeutig bestimmen kann, eine digitale Signatur nur auf ihre Veranlassung erfolgt und diese vorher eindeutig angezeigt wird. Die zum Prüfen signierter Daten erforderlichen technischen Komponenten müssen so beschaffen sein, daß die prüfende Person die Daten, auf die sich die digitale Signatur erstreckt, sowie den Signaturschlüssel-Inhaber eindeutig feststellen kann und die Korrektheit der digitalen Signatur zuverlässig geprüft und zutreffend angezeigt wird. Die technischen Komponenten zum Nachprüfen von Zertifikaten müssen eindeutig erkennen lassen, ob die nachgeprüften Zertifikate im Verzeichnis der Zertifikate zu einem angegebenen Zeitpunkt vorhanden und nicht gesperrt waren. Die technischen Komponenten müssen nach Bedarf den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen. Werden technische Komponenten nach den Sätzen 1 bis 4 geschäftsmäßig Dritten zur Nutzung angeboten, muß die eindeutige Interpretation der Daten sichergestellt sein und müssen die technischen Komponenten bei Benutzung automatisch auf ihre Echtheit überprüft werden. Sicherheitstechnische Veränderungen an den technischen Komponenten müssen für den Nutzer erkennbar werden.

(4) Die technischen Komponenten, mit denen Zertifikate nach § 4 Abs. 5 Satz 3 oder § 5 Abs. 1 Satz 2 des Signaturgesetzes nachprüfbar gehalten werden, müssen so beschaffen sein, daß nur befugte Personen Eintragungen und Veränderungen vornehmen können, die Sperrung eines Zertifikates nicht unbemerkt rückgängig gemacht werden kann und die Auskünfte auf ihre Echtheit überprüft werden können. Die Auskünfte müssen beinhalten, ob die nachgeprüften Zertifikate im Verzeichnis der Zertifikate zum angegebenen Zeitpunkt vorhanden und nicht gesperrt waren. Nur nachprüfbar gehaltene Zertifikate dürfen nicht öffentlich abrufbar sein. Sicherheitstechnische Veränderungen an den technischen Komponenten müssen für den Betreiber erkennbar werden.

(5) Die technischen Komponenten, mit denen Zeitstempel nach § 9 des Signaturgesetzes erzeugt werden, müssen so beschaffen sein, daß die zum Zeitpunkt der Erzeugung des Zeitstempels gültige gesetzliche Zeit unverfälscht in diesen aufgenommen wird. Sicherheitstechnische Veränderungen an den technischen Komponenten müssen für den Betreiber erkennbar werden.

(6) Die zuständige Behörde führt einen Katalog von geeigneten Sicherheitsmaßnahmen, den sie im Bundesanzeiger veröffentlicht. Die Maßnahmen sollen bei den technischen Komponenten berücksichtigt werden. Der Katalog wird nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik erstellt. Experten aus Wirtschaft und Wissenschaft sind zu beteiligen.

§ 17 Prüfung der technischen Komponenten

(1) Die Prüfung der technischen Komponenten nach § 14 Abs. 4 des Signaturgesetzes hat nach den "Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik" (GMBl. 1992, S. 545) zu erfolgen. Die Prüfung muß bei technischen Komponenten zum Erzeugen von Signaturschlüsseln oder zum Speichern oder Anwenden privater Signaturschlüssel und bei technischen Komponenten, die geschäftsmäßig Dritten zur Nutzung angeboten werden, mindestens die Prüfstufe „E 4“ und im übrigen mindestens die Prüfstufe „E 2“ umfassen. Die Stärke der Sicherheitsmechanismen muß mit "hoch" und die Algorithmen und zugehörigen Parameter müssen nach Absatz 2 als geeignet bewertet sein.

(2) Die zuständige Behörde veröffentlicht im Bundesanzeiger eine Übersicht über die Algorithmen und zugehörigen Parameter, die zur Erzeugung von Signaturschlüsseln, zum Hashen zu signierender Daten oder zur Erzeugung und Prüfung digitaler Signaturen als geeignet anzusehen sind, sowie den Zeitpunkt, bis zu dem die Eignung jeweils gilt. Der Zeitpunkt soll mindestens sechs Jahre nach dem Zeitpunkt der Bewertung und Veröffentlichung liegen. Die Eignung ist jährlich sowie bei Bedarf neu zu bestimmen. Die Eignung ist gegeben, wenn innerhalb des bestimmten Zeitraumes nach dem Stand von Wissenschaft und Technik eine nicht feststellbare Fälschung von digitalen Signaturen oder Verfälschung von signierten Daten mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen werden kann. Die Eignung wird nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik unter Berücksichtigung internationaler Standards festgestellt. Experten aus Wirtschaft und Wissenschaft sind zu beteiligen.

(3) In der Bestätigung der Erfüllung der Anforderungen für technische Komponenten nach § 14 Abs. 4 des Signaturgesetzes ist anzugeben, für welche Anforderungen nach § 16 die Bestätigung gilt und unter welchen Einsatzbedingungen, welche Algorithmen und zugehörigen Parameter nach Absatz 2 eingesetzt und bis zu welchem Zeitpunkt diese mindestens geeignet sind sowie nach welcher Stufe die technischen Komponenten nach Absatz 1 geprüft wurden. Eine Ausfertigung des Prüfberichtes und der Bestätigung ist bei der zuständigen Behörde zu hinterlegen. Diese kann bei Anhaltspunkten für Mängel bei Prüfungen oder bei bestätigten technischen Komponenten sowie stichprobenweise Gutachten eines unabhängigen Dritten darüber einholen, ob die technischen Komponenten gemäß Absatz 1 geprüft wurden und ob diese die Anforderungen des Signaturgesetzes und dieser Verordnung erfüllen. Betroffene Hersteller, Vertreiber und Prüfstellen haben die dafür erforderliche Unterstützung zu gewähren. Wird diese nicht gewährt oder stellt sich heraus, daß bestätigte technische Komponenten nicht ausreichend geprüft wurden oder Anforderungen nicht erfüllen, so kann die zuständige Behörde erteilte Bestätigungen für ungültig erklären.

(4) Die zuständige Behörde hat die nach § 14 Abs. 4 des Signaturgesetzes anerkannten Stellen sowie die technischen Komponenten, die von diesen eine Bestätigung nach Absatz 3 erhalten haben, im Bundesanzeiger zu veröffentlichen und den Zertifizierungsstellen unmittelbar bekannt zu geben. Zu den technischen Komponenten ist anzugeben, bis zu welchem Zeitpunkt die Bestätigung gilt. Wird eine Anerkennung entzogen oder eine Bestätigung für ungültig erklärt, so ist dies ebenfalls im Bundesanzeiger zu veröffentlichen und den Zertifizierungsstellen unmittelbar bekannt zu geben.

§ 18 Erneute digitale Signatur

Werden Daten über längere Zeit in signierter Form benötigt, als die für ihre Erzeugung und Prüfung eingesetzten Algorithmen und zugehörigen Parameter nach § 17 Abs. 2 als geeignet beurteilt sind, so sind die Daten vor Ablauf des Zeitpunktes der Eignung der Algorithmen und zugehörigen Parameter mit einer neuen digitalen Signatur zu versehen. Diese muß mit neuen Algorithmen oder zugehörigen Parametern erfolgen, frühere digitale Signaturen einschließen und einen Zeitstempel tragen.

§ 19 Inkrafttreten

Diese Verordnung tritt am 1. November 1997 in Kraft.