P. b. b. Verlagspostamt 1030 Wien WoGZ 213U

BUNDESGESETZBLATT

FÜR DIE REPUBLIK ÖSTERREICH

Jahrgang 2000 Ausgegeben am 2. Februar 2000 Teil II

30. Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung – SigV)

Auf Grund des § 25 Signaturgesetz, BGBl. I Nr. 190/1999, wird im Einvernehmen mit dem Bundesminister für Justiz verordnet:

Inhaltsübersicht

Gebühren für Aufsichtstätigkeiten

§ 1. (1) Für folgende individuelle Leistungen der Aufsichtsstelle und der Telekom-Control GmbH sind von den Zertifizierungsdiensteanbietern nachstehende Gebühren zu entrichten:

1. Überprüfung und Registrierung eines Zertifizierungsdiensteanbieters anlässlich der Anzeige der Aufnahme seiner Tätigkeit (§ 6 Abs. 2 SigG),
   a) sofern der Zertifizierungsdiensteanbieter keine qualifizierten Zertifikate ausstellt und keine sicheren elektronischen Signaturverfahren bereitstellt ..... 100 Euro;
   b) sofern der Zertifizierungsdiensteanbieter qualifizierte Zertifikate ausstellt oder sichere elektronische Signaturverfahren bereitstellt ..... 6 000 Euro;
2. Überprüfung eines Zertifizierungsdiensteanbieters anlässlich der Anzeige eines weiteren Sicherheits- und Zertifizierungskonzepts,
   a) sofern der Zertifizierungsdiensteanbieter keine qualifizierten Zertifikate ausstellt und keine sicheren elektronischen Signaturverfahren bereitstellt ..... 50 Euro;

b) sofern der Zertifizierungsdiensteanbieter qualifizierte Zertifikate ausstellt oder sichere elektronische Signaturverfahren bereitstellt:	
aa) bei der Anzeige eines weiteren Sicherheits- und Zertifizierungskonzepts mit sicherheitsrelevanten Veränderungen	4 000 Euro,
bb) bei der Anzeige eines weiteren Sicherheits- und Zertifizierungskonzepts ohne sicherheitsrelevante Veränderungen	1 000 Euro;
3. Überprüfung eines Zertifizierungsdiensteanbieters anlässlich seiner beantragten Akkreditierung (§ 17 SigG)	6 000 Euro;
4. Überprüfung eines Zertifizierungsdiensteanbieters im Falle der Anzeige grundlegender sicherheitsrelevanter Veränderungen eines bestehenden Sicherheits- und Zertifizierungskonzepts (§ 6 Abs. 5 SigG), wenn der Zertifizierungsdiensteanbieter qualifizierte Zertifikate ausstellt	4 000 Euro;
5. a) regelmäßige Überprüfung eines Zertifizierungsdiensteanbieters (§ 13 Abs. 1 SigG)	4 000 Euro;
b) zusätzliche Überprüfung eines Zertifizierungsdiensteanbieters, wenn ein nicht nur unerheblicher Verstoß gegen die Bestimmungen des Signaturgesetzes oder der auf seiner Grundlage ergangenen Verordnungen festgestellt wird	6 000 Euro;
c) Überprüfung eines Zertifizierungsdiensteanbieters bei sicherheitsrelevanten Veränderungen des Sicherheits- und Zertifizierungskonzepts, sofern diese nicht der Aufsichtsstelle angezeigt wurden	6 000 Euro;
6. bescheidmäßig erteilte Auflagen bei sicherheitsrelevanten Mängeln (§ 14 Abs. 6 SigG)	1 000 Euro;
7. bescheidmäßige Untersagung der Tätigkeit eines Zertifizierungsdiensteanbieters (§ 14 Abs. 2 bis 4 SigG)	1 000 Euro;
8. Kontrolle der Einstellung der Tätigkeit eines Zertifizierungsdiensteanbieters (§ 12 SigG)	100 Euro;
9. Weiterführung des Widerrufsdienstes eines Zertifizierungsdiensteanbieters durch die Aufsichtsstelle (§ 12 und § 14 Abs. 5 SigG)	1 Euro pro im Widerrufsdienst geführtem Zertifikat und Jahr;
10. Führung der Verzeichnisse bei der Aufsichtsstelle (§ 13 Abs. 3 und § 17 Abs. 1 SigG)	500 Euro pro Zertifizierungsdiensteanbieter und Jahr;
11. Beurteilung der Gleichwertigkeit von Prüfberichten einer staatlich anerkannten Stelle eines Drittstaates (§ 24 Abs. 3 SigG)	6 000 Euro.

(2) Zur Abdeckung der laufenden Fixkosten der Aufsichtsstelle und der Telekom-Control GmbH haben die Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, eine Gebühr von 2 Euro pro ausgestelltem und gültigem qualifizierten Zertifikat und Jahr zu entrichten.

(3) Soweit sich die Aufsichtsstelle oder die Telekom-Control GmbH im Rahmen der Aufsicht nach dem Signaturgesetz oder der auf seiner Grundlage ergangenen Verordnungen einer Bestätigungsstelle oder anderer nichtamtlicher Personen oder Einrichtungen bedient, werden deren Gebühren nach § 53a AVG bestimmt und dem betroffenen Zertifizierungsdiensteanbieter als Barauslagen im Sinn des § 76 AVG vorgeschrieben.

(4) Die Gebühren werden von der Aufsichtsstelle mit Bescheid vorgeschrieben. Die Gebühren nach Abs. 2 werden anteilig für jedes Quartal im Nachhinein eingehoben. Zu diesem Zweck haben die Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, der Aufsichtsstelle jeweils bis zum 15. eines jeden Monats die Anzahl der von ihnen ausgestellen qualifizierten Zertifikate, die am Monatsersten gültig waren, bekannt zu geben.

Finanzielle Ausstattung der Zertifizierungsdiensteanbieter

§ 2. (1) Die für die Ausübung der Tätigkeit als Zertifizierungsdiensteanbieter regelmäßig zur Verfügung stehenden Finanzmittel sind der Aufsichtsstelle mit Anzeige der Aufnahme der Tätigkeit nach § 6 Abs. 2 SigG bekannt zu geben. Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen,

haben ein Mindestkapital in Höhe von 300 000 Euro aufzuweisen. Dieses Mindestkapital muss in Form von Eigenmitteln im Sinn des § 224 Abs. 3A und B HGB vorliegen. Unter Nennkapital im Sinn des § 224 Abs. 3A HGB ist das eingezahlte Kapital im Sinn des § 23 Abs. 3 BWG zu verstehen.

(2) Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, haben zudem der Aufsichtsstelle mit Anzeige der Aufnahme der Tätigkeit nach § 6 Abs. 2 SigG das Eingehen einer Haftpflichtversicherung mit einer Mindestversicherungssumme von 1 000 000 Euro je Versicherungsfall nachzuweisen.

(3) Von den Verpflichtungen nach den Abs. 1 und 2 sind der Bund, die Länder, Gemeindeverbände und Ortsgemeinden mit mehr als 50 000 Einwohnern befreit.

Erzeugung von Signaturerstellungsdaten für sichere elektronische Signaturen

§ 3. (1) Die Signaturerstellungsdaten der Aufsichtsstelle müssen dem **Anhang 1** Punkt 1 entsprechen (Hauptsystem). Das Erzeugungssystem muss isoliert, ausschließlich für diesen Zweck bestimmt und auf angemessene Weise vor Eingriffen und Störungen geschützt sein. Die Aufsichtsstelle hat zu ihren Signaturerstellungsdaten ein Zweitsystem an Signaturerstellungsdaten (Zweitschlüssel) zu erzeugen und alle eigenen elektronischen Signaturen, mit denen die bei ihr geführten Verzeichnisse signiert werden, auch mit diesem Zweitsystem als Backup durchzuführen. Die Signaturprüfdaten (der öffentliche Signaturschlüssel) des Zweitsystems sind mit den Signaturerstellungsdaten der Aufsichtsstelle zu signieren. Das Zweitsystem ist unter Verschluss zu halten. Die Signaturprüfdaten des Zweitsystems dürfen nur bei einem Ausfall des Hauptsystems verwendet werden, sodass auch in einem solchen Fall der ungestörte Betrieb der Signatur- und Zertifizierungsdienste der Aufsichtsstelle sichergestellt ist. Werden von der Aufsichtsstelle zusätzlich auch andere als die im Anhang 1 Punkt 1 genannten Signaturerstellungsdaten eingesetzt, so sind die Zertifikate, die die entsprechenden Signaturprüfdaten enthalten, mit dem Hauptsystem zu signieren und elektronisch jederzeit allgemein abrufbar zu halten. Die Aufsichtsstelle hat sicherzustellen, dass die von ihr eingesetzten Signaturerstellungsdaten und die Signaturprüfdaten des entsprechenden Zertifikats in komplementärer Weise anwendbar sind.

(2) Die Signaturerstellungsdaten der Zertifizierungsdiensteanbieter müssen in deren Signaturerstellungseinheit erzeugt werden und dürfen diese nicht verlassen. Die erzeugten Signaturprüfdaten müssen der Aufsichtsstelle im Sicherheits- und Zertifizierungskonzept des Zertifizierungsdiensteanbieters bekannt gegeben werden. Im Übrigen gelten die Anforderungen für sichere elektronische Signaturen der übrigen Signatoren.

(3) Die Signaturerstellungsdaten für sichere elektronische Signaturen der Signatoren müssen die im Anhang 1 Punkt 2 festgesetzte Mindestlänge aufweisen. Im Sicherheitskonzept des Zertifizierungsdiensteanbieters ist die tatsächliche Schlüssellänge der bereitgestellten Signaturverfahren unter Angabe des oberen und des unteren Grenzwertes anzuführen. Die verwendeten Algorithmen müssen offengelegt sein. Die Signaturerstellungsdaten für sichere elektronische Signaturen dürfen mit an Sicherheit grenzender Wahrscheinlichkeit ausschließlich beim Signator vorkommen. Sie müssen nach dem jeweiligen Stand der Technik den eindeutigen Rückschluss auf den Signator ermöglichen. Die wiederholte Erzeugung von Signaturerstellungsdaten für sichere elektronische Signaturen darf nicht dazu führen, dass sich die Schlüsselqualität unter das für das jeweilige Signaturverfahren maßgebliche Sicherheitsniveau vermindert.

(4) Wiederholte Anwendungen der Signaturerstellungsdaten für sichere elektronische Signaturen dürfen nicht zu einer Verminderung der Schlüsselqualität führen. Anwendungen, die die Qualität der Signaturerstellungsdaten vermindern können (zB RSA-Anwendungen auf zufällig gewählte Daten), müssen wirksam ausgeschlossen sein. Die Signaturerstellungsdaten dürfen nur für diejenigen Zwecke verwendet werden, für die sie bestimmt sind.

(5) Die Erzeugung der Signaturerstellungsdaten für sichere elektronische Signaturen muss auf einer tatsächlichen Zufälligkeit beruhen, der ein technischer Zufall oder ein signatorbezogener Zufall zu Grunde liegt. Die Signaturerstellungsdaten müssen in der im Anhang 1 Punkt 3 festgelegten Anzahl von Bitstellen durch tatsächliche Zufallselemente beeinflusst sein (qualitätsvoller Zufall). Die Zufallselemente müssen auf ihre Eignung hin ausreichend geprüft sein. Pseudozufallszahlen dürfen nicht als Ausgangsbasis verwendet werden. Wird das Erzeugungssystem für Signaturerstellungsdaten unterschiedlicher Signatoren eingesetzt, so ist ein verwendeter technischer Zufall periodisch, zumindest in Abständen von einem Monat, auf die statistische Zufallsqualität zu überprüfen. Die Prüfprotokolle sind zu dokumentieren. Liegt ein negatives Prüfergebnis vor, so sind die auf den betroffenen Signaturerstellungsdaten beruhenden Zertifikate, die seit dem letzten Prüfzeitpunkt mit positivem Ergebnis ausgestellt wurden, zu widerrufen.

(6) Werden die Signaturerstellungsdaten für sichere elektronische Signaturen beim Zertifizierungsdiensteanbieter erzeugt, so hat dieser geeignete Vorkehrungen zu treffen, die ein Bekanntwerden der Signaturerstellungsdaten oder anderer Daten, von denen sich die Signaturerstellungsdaten ableiten lassen, sowie eine Speicherung dieser Daten außerhalb der Signaturerstellungseinheit des Signators ausschließen. Dies gilt auch für die Übertragung solcher Signaturerstellungsdaten auf die Signaturerstellungseinheit des Signators sowie für die Daten zur Identifikation des Signators gegenüber der Signaturerstellungseinheit (zB PIN). Erfolgt die Erzeugung der Signaturerstellungsdaten außerhalb der Signaturerstellungseinheit des Signators, so sind Erzeugungssysteme zu verwenden, die auf angemessene Weise vor Eingriffen und Störungen geschützt sind. Der Zugriff auf das Erzeugungssystem muss überwacht, jeder Anwender identifiziert und jede Verwendung registriert werden.

(7) Werden die Signaturerstellungsdaten für sichere elektronische Signaturen in der Signaturerstellungseinheit des Signators erzeugt, so darf der Zertifizierungsdiensteanbieter für die Erzeugung sowie die Speicherung der Signaturerstellungsdaten nur technisch geeignete Signaturerstellungseinheiten bereitstellen oder empfehlen.

Speicherung von Signaturerstellungsdaten für sichere elektronische Signaturen

§ 4. (1) Die Speicherung der Signaturerstellungsdaten für sichere elektronische Signaturen hat so zu erfolgen, dass deren Bekanntwerden ausgeschlossen ist und ihre Verwendung unter der ausschließlichen Kontrolle des Signators steht. Das Duplizieren von Signaturerstellungsdaten nach deren Erzeugung ist nicht zulässig.

(2) Zu besonderen Sicherheitszwecken können die Signaturerstellungsdaten für sichere elektronische Signaturen auf mehrere Signaturerstellungseinheiten verteilt werden. Die Sicherheitsanforderungen müssen in diesem Fall durch die Gesamtheit der betroffenen Signaturerstellungseinheiten erfüllt sein. Der Signator ist über die zur Auslösung der Signaturfunktion erforderlichen Maßnahmen zu unterrichten (§ 10 Abs. 7).

Technische Komponenten und Verfahren der Aufsichtsstelle

§ 5. Die von der Aufsichtsstelle eingesetzten Systeme, insbesondere Produkte und technische Verfahren, müssen den Sicherheitsanforderungen für sichere elektronische Signaturen entsprechen. Die Aufsichtsstelle darf nur Algorithmen, die im **Anhang 2** genannt sind, einsetzen.

Technische Komponenten und Verfahren der Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen

§ 6. (1) Die von einem Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, eingesetzten Systeme, insbesondere Produkte und technische Verfahren, sind entsprechend ihrem aktuellen Stand und auf nachprüfbare Weise zu dokumentieren. Das Vorhandensein nicht dokumentierter Systemelemente sowie ein sicherheitsrelevantes Abweichen von der Dokumentation ist als Kompromittierung der Sicherheitsvorkehrungen zu werten. Dies gilt auch dann, wenn diese Systemelemente nicht für die Erbringung der Signatur- oder Zertifizierungsdienste notwendig sind. Werden die Systemelemente, die der Zertifizierungsdiensteanbieter zur Erbringung der Signatur- und Zertifizierungsdienste einsetzt, auch für andere Tätigkeiten verwendet, so dürfen die Systemelemente für die Erbringung der Signatur- und Zertifizierungsdienste in ihrer Wirkung nicht beeinflusst werden.

(2) Zur Erstellung sicherer elektronischer Signaturen sind Hashverfahren, die im Anhang 2 Punkt 2 genannt sind, einzusetzen. Die Algorithmen zur Erzeugung des Hashwerts sind bis zu dem im Anhang 2 Punkt 2 genannten Zeitpunkt als sicher anzusehen. Zur Ergänzung des Hashwerts dürfen auch Pseudozufallszahlen verwendet werden. Zur Verschlüsselung des Hashwerts sind Algorithmen, die im Anhang 2 Punkt 3 genannt sind, einzusetzen. Die Algorithmen zur Signaturerstellung sind bis zu dem im Anhang 2 Punkt 3 genannten Zeitpunkt als sicher anzusehen. Bei der Anwendung von Signaturalgorithmen, die Zufallszahlen benötigen (zB DSA), dürfen auch Pseudozufallszahlen verwendet werden.

(3) Ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, muss in der Lage sein, elektronische Signaturen sicher zu prüfen. Die Verfahren und Algorithmen zur Signaturprüfung bilden mit den Verfahren und Algorithmen zur Signaturerstellung eine logische Einheit und sind gemeinsam zu dokumentieren.

Technische Komponenten und Verfahren der Anwender für sichere elektronische Signaturen

§ 7. (1) Die Signatoren dürfen für die Erstellung sicherer elektronischer Signaturen nur solche Hashverfahren und Verfahren zur Verschlüsselung des Hashwerts einsetzen, die im Anhang 2 Punkt 2 und 3 genannt sind.

(2) Die von den Signatoren eingesetzten technischen Komponenten und Verfahren zur Erstellung sicherer elektronischer Signaturen müssen die vollständige Anzeige der zu signierenden Daten ermöglichen. Für die zu signierenden Daten dürfen nur die vom Zertifizierungsdiensteanbieter empfohlenen Formate verwendet werden. Die Spezifikation dieser Formate muss allgemein verfügbar sein. Können in einem Format auch dynamische Veränderungen oder unsichtbare Daten codiert werden, so dürfen die betreffenden Codierungen nicht verwendet werden. Der Zertifizierungsdiensteanbieter hat die Anwender anzuweisen oder ihnen Methoden bereitzustellen, um dynamische Veränderungen oder unsichtbare Daten auszuschließen.

(3) Die Signaturfunktion in der Signaturerstellungseinheit des Signators darf nur nach Verwendung von Autorisierungscodes (zB PIN-Eingabe, Fingerabdruck) auslösbar sein. Die Anzahl der Signaturen, die mit einer Autorisierung des Signators gegenüber seiner Signaturerstellungseinheit ausgelöst wird, muss dem Signator bekannt gegeben werden. Das unbefugte Erfahren der Autorisierungscodes muss durch dessen Gestaltung und durch wirksame Sperrmechanismen praktisch ausgeschlossen sein. Derselbe Autorisierungscode darf nicht für unterschiedliche Anwendungen (zB Signatur- und Bankomatfunktion) verwendbar sein. Signaturerstellungseinheiten, die mehrere Anwendungen zulassen, wie zB Multiapplikationskarten oder Multiapplikationsterminals, dürfen nur verwendet werden, wenn die Maßnahmen und Methoden, die das Auslösen unterschiedlicher Anwendungen mit denselben Autorisierungscodes verhindern, im Sicherheitskonzept beschrieben sind. Die eingegebenen Autorisierungscodes dürfen von den verwendeten Systemelementen nicht gespeichert werden. Eingabeerleichterungen bei wiederholter Eingabe von Autorisierungscodes müssen ausgeschlossen sein. Zu besonderen Sicherheitszwecken können die Autorisierungscodes auf mehrere Systemelemente verteilt werden. Der Signator ist über die zur Auslösung der Signaturfunktion erforderlichen Maßnahmen zu unterrichten (§ 10 Abs. 7).

(4) Als Signaturformate sind insbesondere die im Anhang 2 Punkt 4 genannten Formate geeignet.

(5) Will der Empfänger einer elektronisch signierten Erklärung eine sichere Signaturprüfung vornehmen, so hat er dafür Signaturprüfeinheiten zu verwenden, die im Sicherheitskonzept des Zertifizierungsdiensteanbieters, der das Zertifikat ausgestellt hat, für die sichere Signaturprüfung als geeignet bezeichnet sind. Diese Signaturprüfeinheiten müssen den Anforderungen des § 18 Abs. 4 SigG entsprechen.

Schutz der technischen Komponenten für sichere elektronische Signaturen beim Zertifizierungsdiensteanbieter

§ 8. Der Zertifizierungsdiensteanbieter hat geeignete Vorkehrungen zu treffen, die die Signaturerstellungsdaten sowie die zum Erstellen der Zertifikate und die zum Abrufbarhalten der Verzeichnis- und Widerrufsdienste eingesetzten technischen Komponenten vor Kompromittierung und unbefugtem Zugriff schützen. Unbefugte Zugriffe müssen erkennbar sein.

Prüfung der technischen Komponenten und Verfahren für qualifizierte Zertifikate und sichere elektronische Signaturen

§ 9. (1) Zur Prüfung der technischen Komponenten und Verfahren für qualifizierte Zertifikate und sichere elektronische Signaturen sind geeignete und von einer Bestätigungsstelle anerkannte Sicherheitsprofile (Protection Profiles) der Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Technology Security Evaluation, ISO 15408) anwendbar.

(2) Die Prüfung der technischen Komponenten und Verfahren nach § 7 Abs. 2, § 10 und § 18 SigG kann auch nach den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), soweit anwendbar auch nach den Security Requirements for Cryptographic Modules (FIPS 140-1, level 2) oder dem British Standard (BS) 7799, erfolgen. Bei der Anwendung von ITSEC muss für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung sicherer elektronischer Signaturen und gegebenenfalls für die sichere Signaturprüfung die Evaluationsstufe E 3 mit der Mindeststärke der Sicherheitsmechanismen „hoch“ eingehalten sein; bei den übrigen technischen Komponenten und Verfahren muss die Evaluationsstufe E 2 mit der Mindeststärke der Sicherheitsmechanismen „hoch“ eingehalten sein.

(3) In der Bescheinigung der Erfüllung der Sicherheitsanforderungen für technische Komponenten und Verfahren ist anzugeben, für welche Anwendungen, unter welchen Bedingungen und bis zu welchem Zeitpunkt diese gilt. Eine Ausfertigung des Prüfberichts und der Bescheinigung ist der Aufsichtsstelle zu übermitteln.

Erbringung von Signatur- und Zertifizierungsdiensten für qualifizierte Zertifikate und sichere elektronische Signaturen

§ 10. (1) Werden die Einrichtungen eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt, organisatorisch oder technisch getrennt geführt, so ist durch Sicherheitsmaßnahmen sicherzustellen, dass die Übertragung der Daten zwischen den Teileinrichtungen nicht zu einer Kompromittierung der Signatur- oder Zertifizierungsdienste führt.

(2) Die technischen Einrichtungen eines Zertifizierungsdiensteanbieters sind so zu gestalten, dass deren Funktionen und Anwendungen, die zu den bereitgestellten Signatur- und Zertifizierungsdiensten gehören, von anderen Funktionen und Anwendungen getrennt sind. Eine Beeinflussung der Signatur- und Zertifizierungsdienste durch andere Funktionen und Anwendungen muss ausgeschlossen sein. Dies muss sowohl für den regulären Betrieb als auch für besondere Betriebssituationen und außerhalb des Betriebs sichergestellt sein. Besondere Betriebssituationen (zB Wartung) sind zu dokumentieren.

(3) Ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, hat geeignete Vorkehrungen zu treffen, die seine Einrichtungen zur Erbringung von Signatur- und Zertifizierungsdiensten vor unbefugtem Zutritt schützen.

(4) Ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, darf im Rahmen der bereitgestellten Signatur- und Zertifizierungsdienste nicht Personen beschäftigen, die wegen einer mit Vorsatz begangenen strafbaren Handlung zu einer Freiheitsstrafe von mehr als einem Jahr oder wegen strafbarer Handlungen gegen das Vermögen oder gegen die Zuverlässigkeit von Urkunden und Beweiszeichen zu einer Freiheitsstrafe von mehr als drei Monaten verurteilt wurden. Verurteilungen, die nach den Bestimmungen des Tilgungsgesetzes 1972 getilgt sind oder der beschränkten Auskunft unterliegen, bleiben außer Betracht. Die Zuverlässigkeit des Personals ist vom Zertifizierungsdiensteanbieter in Abständen von zumindest zwei Jahren zu überprüfen.

(5) Das technische Personal eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt, muss über ausreichendes Fachwissen in folgenden Bereichen verfügen:

1. allgemeine EDV-Ausbildung,
2. Sicherheitstechnologie, Kryptographie, elektronische Signatur und Public Key Infrastructure,
3. technische Normen, insbesondere Evaluierungsnormen, sowie
4. Hard- und Software.

Auf Verlangen der Aufsichtsstelle muss der Zertifizierungsdiensteanbieter darlegen, durch welche einschlägige Ausbildung an anerkannten Bildungseinrichtungen oder durch welche einschlägigen fachlichen Tätigkeiten das ausreichende Fachwissen des Personals gegeben ist. Die Ausbildung des technischen Personals in den einzelnen Bereichen muss zumindest ein Jahr gedauert haben. Das ausreichende Fachwissen kann zB durch Absolvierung einer einschlägigen Höheren Technischen Lehranstalt (HTL), einer solchen Fachhochschule oder eines einschlägigen Studiums erworben werden. Diese Ausbildung kann durch eine fachlich einschlägige Tätigkeit in der Dauer von zumindest drei Jahren ersetzt werden.

(6) Werden die Signaturerstellungsdaten beim Zertifizierungsdiensteanbieter erzeugt, so dürfen sie nur an den Signator ausgehändigt werden. Die Möglichkeit der Verwendung der Signaturerstellungsdaten vor der Aushändigung an den Signator muss ausgeschlossen sein. In jedem Fall hat sich der Zertifizierungsdiensteanbieter darüber zu vergewissern, dass die Signaturerstellungsdaten des Signators und die Signaturprüfdaten des entsprechenden Zertifikats in komplementärer Weise anwendbar sind.

(7) Ein Zertifizierungsdiensteanbieter hat den Signator vor der erstmaligen Verwendung der Signaturerstellungsdaten über alle sicherheitsrelevanten Maßnahmen bei deren Anwendung (zB Sicherheit der Autorisierungscodes, Prüfung des Ausschlusses fremder Verwendung, Inanspruchnahme der Verzeichnis- und Widerrufsdienste, Möglichkeit der Anzeige zu signierender Daten, Verwendung geeigneter Formate) schriftlich oder unter Verwendung eines dauerhaften Datenträgers klar und allgemein verständlich zu unterrichten.

Antrag auf Ausstellung eines qualifizierten Zertifikats

§ 11. (1) Der Zertifizierungsdiensteanbieter hat die Identität des Zertifikatswerbers anhand eines gültigen amtlichen Lichtbildausweises festzustellen. Der Antrag auf Ausstellung eines qualifizierten Zertifikats muss vom Zertifikatswerber eigenhändig unterschrieben sein. Vom vorgelegten Lichtbildausweis ist eine Ablichtung herzustellen, die mit dem Antrag zu dokumentieren ist. Ist ein solcher Antrag mit der sicheren elektronischen Signatur des Zertifikatswerbers versehen, so kann von der erneuten Feststellung seiner Identität abgesehen werden.

(2) Der Antrag auf Ausstellung eines qualifizierten Zertifikats hat insbesondere zu enthalten:

1. Namen, Datum und Ort der Geburt sowie Adresse des Zertifikatswerbers, Datum der Ausstellung und Nummer des vorgelegten Lichtbildausweises sowie die Behörde, die diesen ausstellte;
2. gegebenenfalls Angaben, ob das Zertifikat eine Einschränkung des Anwendungsbereichs oder eine Begrenzung des Transaktionswerts enthalten soll,
3. gegebenenfalls Angaben darüber, ob eine Vertretungsmacht für Dritte, andere rechtlich erhebliche Eigenschaften des Zertifikatswerbers, wie etwa eine berufsrechtliche oder sonstige Zulassung, oder weitere Angaben in das qualifizierte Zertifikat aufgenommen werden sollen.

(3) Wenn in ein qualifiziertes Zertifikat Angaben über die Vertretungsmacht für einen Dritten aufgenommen werden sollen, muss die Vertretungsmacht zuverlässig nachgewiesen sein und eine schriftliche oder mit einer sicheren elektronischen Signatur versehene Einwilligung des Dritten vorliegen. Dieser ist über den Inhalt des qualifizierten Zertifikats schriftlich oder unter Verwendung eines dauerhaften Datenträgers zu unterrichten und auf die Möglichkeit des Widerrufs nach § 9 Abs. 1 Z 1 SigG hinzuweisen. Eine berufsrechtliche oder sonstige Zulassung muss vor deren Aufnahme in ein qualifiziertes Zertifikat ebenfalls zuverlässig nachgewiesen sein. Untersteht der Signator im Hinblick auf eine eingetragene berufsrechtliche Qualifikation einer öffentlich-rechtlichen Berufsaufsicht, so ist die Einrichtung, die die Berufsaufsicht ausübt, über den Inhalt des qualifizierten Zertifikats schriftlich oder unter Verwendung eines dauerhaften Datenträgers zu unterrichten.

Qualifizierte Zertifikate

§ 12. (1) Stellt ein Zertifizierungsdiensteanbieter neben qualifizierten auch andere Zertifikate aus, so muss er für die Signatur der qualifizierten Zertifikate gesonderte Signaturerstellungsdaten verwenden.

(2) Als Formate für qualifizierte Zertifikate sind insbesondere die im Anhang 2 Punkt 5 genannten Formate geeignet. Das Gleiche gilt für die Codierungen in qualifizierten Zertifikaten.

(3) Die Gültigkeitsdauer eines qualifizierten Zertifikats darf höchstens drei Jahre betragen und den Zeitraum der Eignung der eingesetzten technischen Komponenten und Verfahren sowie der zugehörigen Parameter nach den Anhängen 1 und 2 nicht überschreiten.

(4) Bis zum Ablauf der Gültigkeit eines qualifizierten Zertifikats ist es zulässig, mit Ausnahme der Gültigkeitsdauer dieselben Inhalte samt denselben Signaturprüfdaten neu zu zertifizieren und auf diese Weise ein neues Zertifikat auszustellen. In allen anderen Fällen bewirken Zertifikate mit denselben Signaturprüfdaten und unterschiedlichen Inhalten eine Kompromittierung der betroffenen Zertifikate.

(5) Ein Zertifizierungsdiensteanbieter ist berechtigt, mit Zustimmung eines anderen Zertifizierungsdiensteanbieters dessen Zertifikat oder die von diesem ausgestellten Zertifikate zu zertifizieren. Die Zertifikate, die er auf diese Weise ausstellt, dürfen keine Modifikationen aufweisen; er hat auch für die Erbringung der Verzeichnis- und Widerrufsdienste Sorge zu tragen und gegebenenfalls die Widerrufe des anderen Zertifizierungsdiensteanbieters unmittelbar nachzuvollziehen.

Verzeichnis- und Widerrufsdienste für qualifizierte Zertifikate

§ 13. (1) Als Formate für Verzeichnis- und Widerrufsdienste sind insbesondere die im Anhang 2 Punkt 6 genannten Formate geeignet. Die Verzeichnis- und Widerrufsdienste können auch in unterschiedlichen Formaten bereitgestellt werden. Der Zertifizierungsdiensteanbieter hat sicherzustellen, dass die Formate der Widerrufsdienste für deren Weiterführung durch die Aufsichtsstelle geeignet sind. Werden die Verzeichnis- und Widerrufsdienste von einem anderen Zertifizierungsdiensteanbieter übernommen, so müssen diese weiterhin in denselben Formaten bereitgestellt werden.

(2) Der Zertifizierungsdiensteanbieter hat den Signatoren sowie Dritten, für die Angaben über die Vertretungsmacht des Signators in ein qualifiziertes Zertifikat aufgenommen wurden, geeignete Kommunikationsmöglichkeiten bekannt zu geben, mit denen diese jederzeit einen unverzüglichen Widerruf des Zertifikats veranlassen können. Dafür muss ein Authentifizierungsverfahren vorgesehen werden. Der Widerruf eines qualifizierten Zertifikats muss jedenfalls auch in Papierform möglich sein.

(3) Die Verzeichnis- und Widerrufsdienste müssen vor Fälschung, Verfälschung und unbefugtem Abruf ausreichend geschützt sein. Es muss sichergestellt sein, dass nur befugte Personen Eintragungen und Veränderungen in den Verzeichnissen vornehmen können. Weiters muss sichergestellt sein, dass eine Sperre oder ein Widerruf nicht unbemerkt rückgängig gemacht werden kann.

(4) Die Aktualisierung der Widerrufsdienste muss während der Geschäftszeiten spätestens innerhalb von drei Stunden ab Bekanntwerden des Widerrufsgrundes erfolgen. Die Geschäftszeiten müssen zumindest an Werktagen den Zeitraum von 9 bis 17 Uhr und an Samstagen den Zeitraum von 9 bis 12 Uhr umfassen. Außerhalb der Geschäftszeiten hat der Zertifizierungsdiensteanbieter jedenfalls dafür Sorge zu

tragen, dass ein Verlangen auf Widerruf eines qualifizierten Zertifikats jederzeit automatisiert entgegengenommen wird und die Sperre auslöst.

(5) Die zeitliche Verfügbarkeit der Verzeichnisdienste muss im Sicherheitskonzept angegeben werden. Die Verzeichnisdienste müssen zumindest während der Geschäftszeiten nach Abs. 4 verfügbar sein. Die Widerrufsdienste müssen ständig verfügbar sein. Eine durchgehende Unterbrechung der Verzeichnis- oder der Widerrufsdienste von mehr als 30 Minuten während des Verfügbarkeitszeitraums ist als Störfall zu dokumentieren. Für Wartungs- und Ausfallsituationen des Widerrufsdienstes ist ein Ersatzsystem bereitzustellen. Fällt auch das Ersatzsystem aus, so ist dies innerhalb eines Kalendertags der Aufsichtsstelle anzuzeigen. Diese hat innerhalb von drei Kalendertagen den Widerrufsdienst wiederherzustellen. Die Widerrufsdienste müssen allgemein frei zugänglich sein. Die Abfrage der Widerrufsdienste muss unentgeltlich und ohne Identifikation möglich sein.

(6) Ein Zertifizierungsdiensteanbieter hat die Verzeichnis- und Widerrufsdienste zumindest bis zum Zeitpunkt des erforderlichen Nachsignierens (§ 17) zu führen. Nach Ablauf dieser Frist hat der Zertifizierungsdiensteanbieter eine Überprüfung der qualifizierten Zertifikate bis zum Ablauf der in § 16 Abs. 2 genannten Frist im Einzelfall zu ermöglichen. Das Gleiche gilt für die Weiterführung der Widerrufsdienste durch die Aufsichtsstelle im Falle der Einstellung oder Untersagung der Tätigkeit eines Zertifizierungsdiensteanbieters.

(7) Der Zeitraum, während dessen eine Sperre wirksam sein kann, muss im Sicherheitskonzept angegeben werden. Dieser Zeitraum darf drei Werktage nicht übersteigen. Während dieses Zeitraums kann eine Sperre aufgehoben werden. Eine aufgehobene Sperre hat auf die Gültigkeit des Zertifikats keinen Einfluss. Wird eine Sperre während des genannten Zeitraums nicht aufgehoben, so ist das Zertifikat zu widerrufen. Erfolgt auf Grund einer Sperre der Widerruf eines Zertifikats, so gilt bereits die Sperre als Widerruf.

(8) Werden die Signaturerstellungsdaten des Signators bekannt oder kommen diese außer beim Signator als Signaturerstellungsdaten oder in anderer Form ein weiteres Mal vor, so liegt eine Kompromittierung der Signaturerstellungsdaten vor, die zum Widerruf des Zertifikats des Signators führen muss. Der Widerruf ist vom Signator zu verlangen (§ 9 Abs. 1 Z 1 SigG) oder vom Zertifizierungsdiensteanbieter aus Eigenem vorzunehmen (§ 9 Abs. 1 Z 6 SigG), sobald er von der Kompromittierung Kenntnis erlangt.

Sichere Zeitstempeldienste

§ 14. (1) Für die Erbringung sicherer Zeitstempeldienste dürfen ausschließlich qualifizierte und nur für diesen Zweck ausgestellte Zertifikate verwendet werden. Dieser Verwendungszweck ist im Zertifikat zu bezeichnen.

(2) Die bescheinigte Zeitangabe (Datum und Uhrzeit) hat sich nach Mitteleuropäischer Zeit (MEZ) unter Beachtung der Sommerzeit zu richten; andere Zeitzonen sind ausdrücklich anzugeben. Die Abweichung von der tatsächlichen Zeit darf beim Anbieter des Zeitstempeldienstes höchstens eine Minute betragen.

(3) Die zeitliche Verfügbarkeit sicherer Zeitstempeldienste muss im Sicherheitskonzept des Zertifizierungsdiensteanbieters, der solche Dienste bereitstellt, angegeben werden.

Sicherheits- und Zertifizierungskonzept für qualifizierte Zertifikate

§ 15. (1) Das Sicherheits- und Zertifizierungskonzept hat insbesondere folgenden Inhalt aufzuweisen:

1. Namen des Zertifizierungsdiensteanbieters,
2. Adresse des Zertifizierungsdiensteanbieters und Staat seiner Niederlassung,
3. Art, Anwendungsbereich und Erbringung der bereitgestellten Signatur- und Zertifizierungsdienste,
4. Verfahren zur Antragstellung,
5. gegebenenfalls Art und Weise der Aufnahme von Pseudonymen sowie von Angaben über eine Vertretungsmacht oder sonstige rechtlich erhebliche Eigenschaften des Signators in das Zertifikat,
6. Geschäftszeiten,
7. Erzeugung der Signaturerstellungsdaten des Zertifizierungsdiensteanbieters,
8. Format der Signaturerstellungsdaten des Zertifizierungsdiensteanbieters,
9. Signaturprüfdaten, gegebenenfalls das Zertifikat des Zertifizierungsdiensteanbieters,
10. Erzeugung der Signaturerstellungsdaten der Signatoren,

11. Format der Signaturerstellungsdaten der Signatoren,
12. eingesetzte Verfahren zur Erstellung der bereitgestellten Signaturen (Hashverfahren und Verfahren zur Verschlüsselung des Hashwerts),
13. Liste der eingesetzten, bereitgestellten und empfohlenen Signaturprodukte,
14. Sicherheit der Autorisierungscodes,
15. anwendbare Formate für zu signierende Dokumente und gegebenenfalls Methoden zur Verhinderung dynamischer Veränderungen,
16. Formate und Gültigkeitsdauer der Zertifikate,
17. technische Normen, Zugangsmodalitäten sowie Aktualisierungs- und Verfügbarkeitszeitraum für die bereitgestellten Verzeichnis- und Widerrufsdienste einschließlich des Zeitraums der Sperre,
18. gegebenenfalls Verfügbarkeitszeitraum bereitgestellter Zeitstempeldienste,
19. nachvollziehbare und allgemein verständliche Methode zur sicheren Signaturprüfung,
20. Format der Dokumentation von Sicherheitsvorkehrungen, Störfällen und besonderen Betriebssituationen,
21. Zeitraum und Verfahren des Nachsignierens,
22. Schutz der technischen Komponenten vor unbefugtem Zugriff,
23. Schutz der Einrichtungen des Zertifizierungsdiensteanbieters vor unbefugtem Zutritt.

(2) Das Sicherheits- und Zertifizierungskonzept ist der Aufsichtsstelle in elektronischer Form im Format RTF, PDF, Ascii oder Postscript vorzulegen. Es muss mit der sicheren elektronischen Signatur des Zertifizierungsdiensteanbieters signiert sein. Der Zertifizierungsdiensteanbieter hat das Sicherheits- und Zertifizierungskonzept sowie eine Zusammenfassung klar und allgemein verständlich im Format RTF, PDF, Ascii oder Postscript elektronisch jederzeit allgemein abrufbar zu halten.

Dokumentation

§ 16. (1) Die Dokumentation nach § 11 SigG, einschließlich der Störfälle und der besonderen Betriebssituationen sowie der Unterrichtung der Zertifikatswerber nach § 20 SigG, muss jedenfalls in elektronischer Form erfolgen. Soweit die Erzeugung der Signaturerstellungsdaten außerhalb der Signaturerstellungseinheit des Signators erfolgt, gilt dies auch für den Zeitpunkt der Übertragung der Signaturerstellungsdaten auf die Signaturerstellungseinheit. Die in der Dokumentation eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt, enthaltenen Daten müssen mit seiner sicheren elektronischen Signatur versehen sein und sichere Zeitstempel (§ 14) enthalten.

(2) Die Dokumentation nach Abs. 1 ist zumindest 33 Jahre ab der letzten Eintragung aufzubewahren und so zu sichern, dass sie innerhalb dieses Zeitraums lesbar und verfügbar bleibt.

Erneuerte elektronische Signatur (Nachsignieren)

§ 17. Der Zeitraum, nach dem eine neue sichere elektronische Signatur wegen drohender Verringerung des Sicherheitswerts angebracht werden sollte, muss im Sicherheits- und Zertifizierungskonzept des Zertifizierungsdiensteanbieters angegeben werden. Dieses muss ein Nachsignieren jedenfalls vor Ablauf der in den Anhängen für die Sicherheit der eingesetzten Signaturerstellungsverfahren angegebenen Perioden vorsehen. Beim Anbringen einer neuen Signatur muss ein Zeitstempel verwendet werden.

Aufsicht und Akkreditierung

§ 18. (1) Die Anzeige der Aufnahme der Tätigkeit eines Zertifizierungsdiensteanbieters nach § 6 Abs. 2 SigG muss in elektronischer Form erfolgen. Soweit spezielle Inhalte der Anzeige nicht ein anderes Format erfordern, ist das Format RTF, PDF, Ascii oder Postscript zu verwenden. Die Anzeige muss elektronisch signiert sein. Die Aufsichtsstelle muss in der Lage sein, sich von der Echtheit der Daten zu überzeugen. Zu diesem Zweck kann sie auch das persönliche Erscheinen des Zertifizierungsdiensteanbieters oder eines vertretungsbefugten Organs anordnen. Stellt der Zertifizierungsdiensteanbieter qualifizierte Zertifikate aus, so hat sich die Aufsichtsstelle darüber zu vergewissern, dass die Signaturerstellungsdaten des Zertifizierungsdiensteanbieters und die Signaturprüfdaten des entsprechenden Zertifikats in komplementärer Weise anwendbar sind.

(2) Der Anzeige sind insbesondere anzuschließen:
1. Sicherheits- und Zertifizierungskonzept,
2. Darstellung der spezifischen sicherheitsrelevanten Bedrohungen und Risiken beim Zertifizierungsdiensteanbieter,
3. Nachweis der finanziellen Ausstattung sowie der erforderlichen Haftpflichtversicherung und
4. Nachweis des Fachwissens des technischen Personals.

(3) Die Anordnungen des Abs. 1 gelten für die Anzeige weiterer Sicherheits- und Zertifizierungskonzepte sowie für die Anzeige sicherheitsrelevanter Veränderungen bestehender Sicherheits- und Zertifizierungskonzepte sinngemäß.

(4) Die Aufsichtsstelle hat Zertifizierungsdiensteanbieter zumindest in regelmäßigen Abständen von zwei Jahren sowie bei sicherheitsrelevanten Veränderungen des Sicherheits- und Zertifizierungskonzepts zu überprüfen. Darüber hinaus ist die Aufsichtsstelle berechtigt, jederzeit stichprobenartige Überprüfungen der Zertifizierungsdiensteanbieter vorzunehmen. Die Aufsichtsstelle hat eine solche zusätzliche Überprüfung vorzunehmen, wenn ein begründeter Verdacht des Vorliegens sicherheitsrelevanter Mängel besteht.

(5) Die Aufsichtsstelle, ihre Organe sowie die für sie tätigen Personen und Einrichtungen unterliegen der Amtsverschwiegenheit im Sinn des Art. 20 Abs. 3 B-VG.

(6) In die bei der Aufsichtsstelle geführten Verzeichnisse dürfen nur solche Umstände aufgenommen werden, die auf ihre Richtigkeit hin überprüft wurden. Für diese Verzeichnisse muss eines der im Anhang 2 Punkt 6 genannten Formate verwendet werden. Die Aufsichtsstelle muss eine allgemein zugängliche Homepage führen, in der ihre Adresse, ihre Signaturprüfdaten sowie die Formate der bei ihr geführten Verzeichnisse und die Zugangsmodalitäten zu diesen angegeben sind.

(7) Im Fall einer freiwilligen Akkreditierung nach § 17 SigG tritt der Antrag auf Akkreditierung an die Stelle der Anzeige der Aufnahme der Tätigkeit des Zertifizierungsdiensteanbieters.

(8) Die Kennzeichnung akkreditierter Zertifizierungsdiensteanbieter nach § 17 SigG hat die Wortfolge „Akkreditierter Zertifizierungsdiensteanbieter“ zu enthalten. Akkreditierte Zertifizierungsdiensteanbieter sind berechtigt, das Bundeswappen mit dem Schriftzug „Akkreditierter Zertifizierungsdiensteanbieter“ zu führen.

Hinweis auf die Notifikation

§ 19. Diese Verordnung wurde unter Einhaltung der Bestimmungen der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften in der Fassung der Richtlinie 98/48/EG der Europäischen Kommission notifiziert (Notifikationsnummer 99/0448/A).

Klima

Anhang 1

Parameter für technische Komponenten und Verfahren für sichere elektronische Signaturen

1. Signaturerstellungsdaten der Aufsichtsstelle

Die Signaturerstellungsdaten der Aufsichtsstelle müssen dem Verfahren RSA (zur Verschlüsselung des Hashwerts) entsprechen (Hauptsystem).

Werden von der Aufsichtsstelle zusätzlich andere Signaturerstellungsdaten eingesetzt (§ 3 Abs. 1 vorletzter Satz), so muss es sich dabei um Signaturerstellungsdaten für sichere elektronische Signaturen handeln.

2. Signaturerstellungsdaten für sichere elektronische Signaturen

Die Schlüssellänge der Signaturerstellungsdaten für sichere elektronische Signaturen muss zumindest betragen:
- beim Verfahren RSA 1023 Bit,
- beim Verfahren DSA 1023 Bit,
- bei DSA-Varianten, die auf elliptischen Kurven basieren, 160 Bit.

Führende Nullbit sind in die Schlüssellänge nicht einzurechnen. Die Schlüssellänge ist jedenfalls für den geheimen Teil der Signaturerstellungsdaten maßgeblich.

3. Zufälle für Signaturerstellungsdaten für sichere elektronische Signaturen

Die Signaturerstellungsdaten für sichere elektronische Signaturen müssen zumindest in folgender Anzahl von Bitstellen durch tatsächliche Zufallselemente beeinflusst sein:
- bei den Verfahren RSA und DSA 1023 Bit,
- bei DSA-Varianten, die auf elliptischen Kurven basieren, 160 Bit.

In diesen Fällen liegt ein qualitätsvoller Zufall vor.

Werden zur Sicherstellung der Einzigartigkeit von Signaturerstellungsdaten bei deren Erzeugung weitere Schlüsselelemente, zB führende oder nachlaufende Bit, in festgelegter oder in zufälliger Form eingebunden, so darf die Anzahl der durch einen qualitätsvollen Zufall beeinflussten Bitstellen dadurch nicht verringert werden.

4. Sicherheitsperiode

Die unter Punkt 1 bis 3 aufgezählten Schlüssellängen der Signaturerstellungsdaten sind unter Verwendung der genannten Algorithmen bis 31. Dezember 2005 für den Einsatz bei sicheren elektronischen Signaturen als sicher anzusehen.

Anhang 2

Technische Verfahren und Formate

1. Technische Verfahren der Aufsichtsstelle

Bei der Aufsichtsstelle ist als Hashverfahren das Verfahren SHA-1 und zur Verschlüsselung des Hashwerts das Verfahren RSA einzusetzen (Hauptsystem). Die Verwendung des Chinese Remainder Theorem (CRT) ist nicht zulässig.

Werden von der Aufsichtsstelle zusätzlich andere Signaturerstellungsdaten eingesetzt (§ 3 Abs. 1 vorletzter Satz), so muss es sich bei den entsprechenden Verfahren zur Verschlüsselung des Hashwerts um solche für sichere elektronische Signaturen handeln.

2. Hashverfahren für sichere elektronische Signaturen

Folgende Hashverfahren werden als sicher anerkannt:

a) RIPEMD-160,
b) Funktion SHA-1.

Diese Hashverfahren sind bis 31. Dezember 2005 für den Einsatz bei elektronischen Signaturen als sicher anzusehen.

Diesen Hashverfahren sind andere Verfahren gleichgestellt, die zumindest die gleiche Sicherheit aufweisen und von einer Bestätigungsstelle als solche anerkannt und veröffentlicht wurden.

3. Verfahren zur Signaturerstellung (Verschlüsselung des Hashwerts) für sichere elektronische Signaturen

Folgende Verfahren zur Signaturerstellung werden als sicher anerkannt:

a) RSA,
b) DSA,
c) DSA-Varianten, die auf elliptischen Kurven basieren:
   – ISO/IEC 14883-3, Annex A.2.2 („Agnew-Mullin-Vanstone analogue“),
   – IEEE-Standard P1363, Abschnitt 5.3.3 („Nyberg-Rueppel version“),
   – IEEE-Standard P1363 [5], Abschnitt 5.3.4 („DSA version“).

Für die Umsetzung sind nach Möglichkeit international anerkannte Methoden zu verwenden.

Die genannten Algorithmen sind bis 31. Dezember 2005 für den Einsatz bei elektronischen Signaturen als sicher anzusehen.

Diesen Verfahren zur Signaturerstellung sind andere Verfahren gleichgestellt, die zumindest die gleiche Sicherheit aufweisen und von einer Bestätigungsstelle als solche anerkannt und veröffentlicht wurden.

4. Formate für sichere elektronische Signaturen

Die für sichere elektronische Signaturen eingesetzten Formate sollten einem international anerkannten Standard oder einer anerkannten Empfehlung (zB PKCS#7 Cryptographic Message Syntax Standard) entsprechen.

5. Formate für qualifizierte Zertifikate

Die European Electronic Signatures Standardization Initiative (EESSI) ist derzeit damit beschäftigt, Formate und Normen für die Darstellung qualifizierter Zertifikate sowie für deren Inhalte auszuarbeiten. Vorläufig wird empfohlen, international anerkannte Normungsvorschläge (zB X.509 v3 certificate oder X.509 v2 CRL for use in the Internet) anzuwenden. Die detaillierte Ausprägung des Formats ist im Sicherheits- und Zertifizierungskonzept darzustellen. Zur Beschreibung ist eine Formale Notation (zB CCITT bzw. ITU-T Recommendation X.208: Specification of Abstract Syntax Notation One – ASN.1 – 1988) zu verwenden. Dies gilt auch für die Codierung der Kennzeichnung „qualifiziert“ in einem qualifizierten Zertifikat.

6. Formate für Verzeichnis- und Widerrufsdienste für qualifizierte Zertifikate

Die Verzeichnis- und Widerrufsdienste sollten in einem international anerkannten Format geführt werden. Für den Zugang zu den Verzeichnis- und Widerrufsdiensten werden insbesondere folgende internationale Normen empfohlen:

a) 1988 CCITT (ITU-T) X.500 / ISO IS9594,
b) RFC 2587 Internet X.509 Public Key Infrastructure LDAPv2 Schema,
c) RFC 2459 Internet X.509 Public Key Infrastructure Certificate and CRL Profile,
d) RFC 2589 Lightweight Directory Access Protocol (LDAPv3) Extensions for Dynamic Directory Services.

Druck der Print Media Austria AG (vormals Österreichische Staatsdruckerei AG)