

**Langtitel**

Verordnung des Bundeskanzlers über elektronische Signaturen  
(Signaturverordnung - SigV)  
StF: BGBl. II Nr. 30/2000

**Änderung**

idF: BGBl. II Nr. 527/2004

**Präambel/Promulgationsklausel**

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

## Inhaltsverzeichnis

§ 1.	Gebühren für Leistungen der Aufsichtsstelle
§ 2.	Finanzielle Ausstattung der Zertifizierungsdiensteanbieter
§ 3.	Technische Sicherheitserfordernisse für sichere elektronische Signaturen
§ 4.	Anzeige der zu signierenden Daten
§ 5.	Signaturen für qualifizierte Zertifikate
§ 6.	Signaturen der Aufsichtsstelle
§ 7.	Systeme der Aufsichtsstelle
§ 8.	Schutz der technischen Komponenten für sichere elektronische Signaturen beim Zertifizierungsdiensteanbieter
§ 9.	Prüfung der technischen Komponenten und Verfahren
§ 10.	Erbringung von Signatur- und Zertifizierungsdiensten für qualifizierte Zertifikate und sichere elektronische Signaturen
§ 11.	Antrag auf Ausstellung eines qualifizierten Zertifikats
§ 12.	Qualifizierte Zertifikate
§ 13.	Verzeichnis- und Widerrufsdienste für qualifizierte Zertifikate
§ 14.	Sichere Zeitstempeldienste
§ 15.	Sicherheits- und Zertifizierungskonzept für qualifizierte Zertifikate und sichere Zeitstempeldienste
§ 16.	Dokumentation
§ 17.	Erneuerte elektronische Signatur (Nachsignieren)
§ 18.	Aufsicht und Akkreditierung
§ 19.	Hinweis auf die Notifikation
§ 20.	Verlautbarungen
§ 21.	In-Kraft-Treten
§ 22.	Schlussbestimmung
Anhang	

## Gebühren für Aufsichtstätigkeiten

§ 1. (1) Für folgende individuelle Leistungen im Rahmen der Aufsicht sind von den Zertifizierungsdiensteanbietern nachstehende Gebühren zu entrichten:

- |    |   |             |
|----|---|-------------|
| 1. | Registrierung der Anzeige der Aufnahme der Tätigkeit eines Zertifizierungsdiensteanbieters bzw. der Einstellung seiner Tätigkeit (§ 6 Abs. 2 erster Satz SigG)  | 100 Euro;   |
| 2. | Entgegennahme des Sicherheits- sowie des Zertifizierungskonzepts anlässlich der Aufnahme der Tätigkeit oder bei Änderung eines Dienstes (§ 6 Abs. 2 zweiter Satz SigG)  | 50 Euro;    |
| 3. | Prüfung des Sicherheits- und Zertifizierungskonzepts eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt oder sichere elektronische Signaturverfahren bereitstellt, anlässlich der Anzeige der Aufnahme seiner Tätigkeit (§ 6 Abs. 3 und § 13 Abs. 2 SigG) | 6 000 Euro; |
| 4. | Prüfung des Sicherheits- und Zertifizierungskonzepts eines Zertifizierungsdiensteanbieters, der sichere Zeitstempeldienste anbietet   | 2 000 Euro; |

5. Prüfung der Änderung eines Sicherheits- und Zertifizierungskonzepts eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt oder sichere elektronische Signaturverfahren bereitstellt (§ 6 Abs. 2 zweiter Satz SigG),
    - a) ohne sicherheitsrelevante Änderungen 1 000 Euro;
    - b) mit sicherheitsrelevanten Änderungen 4 000 Euro;
  6. Freiwillige Akkreditierung eines Zertifizierungsdiensteanbieters gemäß § 17 SigG, sofern die Akkreditierung nicht im Zuge der Prüfung nach Z 3 geschieht 6 000 Euro;
  7. regelmäßige Überprüfung eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt oder sichere elektronische Signaturverfahren bereitstellt (§ 13 Abs. 2 Z 1 SigG):
    - pro Jahr 4 000 Euro;
  8. regelmäßige Überprüfung eines Zertifizierungsdiensteanbieters, der sichere Zeitstempel ausstellt (§ 13 Abs. 1 SigG):
    - pro Jahr 2 000 Euro;
  9. anlassbezogene Überprüfung eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt oder sichere elektronische Signaturverfahren bereitstellt, die wegen eines nicht nur unerheblichen Verstoßes gegen das SigG oder die auf seiner Grundlage ergangenen Verordnungen bzw. wegen der Unterlassung der Anzeige sicherheitsrelevanter Veränderungen zu Aufsichtsmaßnahmen nach Z 10 geführt hat (§ 14 SigG) 6 000 Euro;
  10. in Bescheidform ergehende Aufsichtsmaßnahmen (§ 14 SigG)
    - a) Erteilung von Auflagen wegen sicherheitsrelevanter Mängel:
      - zusätzlich zu Z 7 1 000 Euro;
    - b) Untersagung der weiteren Ausübung der Tätigkeit als Zertifizierungsdiensteanbieter:
      - zusätzlich zu Z 7 1 000 Euro;
  11. Weiterführung des Widerrufsdienstes eines Zertifizierungsdiensteanbieters durch die Aufsichtsstelle (§ 12 und § 14 Abs. 5 SigG).
    - pro Zertifikat, das im Widerrufsdienst geführt wird 1 Euro;
  12. Führung der Verzeichnisse bei der Aufsichtsstelle (§ 13 Abs. 3 und § 17 Abs. 1 SigG):
    - pro aufgenommenem Zertifizierungsdiensteanbieter und Jahr 500 Euro;
  13. Beurteilung der Gleichwertigkeit von Prüfberichten einer staatlich anerkannten Stelle eines Drittstaates (§ 24 Abs. 3 SigG) 6 000 Euro;
- (2) Soweit sich die Aufsichtsstelle im Rahmen der Aufsicht nach dem Signaturgesetz oder der auf seiner Grundlage ergangenen Verordnungen einer Bestätigungsstelle oder anderer nichtamtlicher Personen oder Einrichtungen als Sachverständiger bedient, sind die Gebühren nach § 53a AVG dem betroffenen Zertifizierungsdiensteanbieter als Barauslage im Sinne des § 76 AVG vorzuschreiben.
- (3) Die Gebühren sind von der Aufsichtsstelle mit Bescheid vorzuschreiben.

#### 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 oder sichere elektronische Signaturverfahren bereitstellen, haben ein Mindestkapital in Höhe von 300 000 Euro aufzuweisen. 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 oder sichere elektronische Signaturverfahren bereitstellen, haben zudem der Aufsichtsstelle gleichzeitig mit der Anzeige der Aufnahme ihrer Tätigkeit nach § 6 Abs. 2 SigG nachzuweisen, dass sie eine Haftpflichtversicherung mit einer Mindestversicherungssumme von 700 000 Euro eingegangen sind, die zumindest drei Versicherungsfälle im Jahr deckt.

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

#### Technische Sicherheitserfordernisse für Signaturerstellungsdaten und Signaturerstellungseinheiten bei sicheren Signaturen

§ 3. (1) Die technischen Komponenten und Verfahren, die bei der Erzeugung und Speicherung von Signaturerstellungsdaten für sichere elektronische Signaturen zum Einsatz kommen, müssen im Hinblick auf das Erfordernis ihrer Überprüfung nach § 18 Abs. 5 SigG den Anforderungen des § 9 entsprechen. Dasselbe gilt hinsichtlich der Signaturerstellungseinheit für sichere elektronische Signaturen, und zwar für solche technische Komponenten und Verfahren, die zur Verarbeitung der Signaturerstellungsdaten verwendet werden.

(2) Für sichere elektronische Signaturen dürfen nur solche Algorithmen und Parameter eingesetzt werden, die die Anforderungen des Anhangs erfüllen. Die für die technische Sicherheit dieser Algorithmen und Parameter geltenden Randbedingungen sind so zu wählen, dass sie dem jeweiligen Stand der Technik entsprechen.

(3) Die Signaturerstellungsdaten für sichere elektronische Signaturen können auf mehrere getrennte Komponenten verteilt sein. Die Sicherheitsanforderungen müssen in einem solchen Fall durch die Signaturerstellungseinheit als Gesamtheit der Komponenten erfüllt werden.

#### Technische Sicherheitserfordernisse für die Systemumgebung der Signaturerstellungseinheit bei sicheren Signaturen

§ 4. (1) Für die Darstellung des Inhalts der zu signierenden Daten vor der Auslösung des Signaturvorgangs dürfen nur die vom Zertifizierungsdiensteanbieter empfohlenen Formate verwendet werden. Die Spezifikation eines solchen Formats muss allgemein verfügbar sein. Die Spezifikation muss sicherstellen, dass die signierten Daten sowohl bei der Signaturerstellung als auch bei der Signaturprüfung zweifelsfrei und mit gleichem Ergebnis darstellbar sind. Können in einem Format dynamische Veränderungen codiert werden, so dürfen jene Elemente, die dynamische Veränderungen hervorrufen können, nicht verwendet werden.

(2) Die Signaturfunktion in der Signaturerstellungseinheit des Signators darf nur nach Verwendung von Autorisierungs-codes (zB PIN-Eingabe, Fingerabdruck) auslösbar sein. Die Anzahl der Signaturen, die mit einer Autorisierung des Signators gegenüber seiner Signaturerstellungseinheit ausgelöst wird, muss dem Signator im Zeitpunkt des Auslösens des Signaturvorgangs bekannt sein. Derselbe Autorisierungscode darf nicht für unterschiedliche Anwendungen (zB Signatur- und Bankomatfunktion) verwendbar sein. Die eingegebenen Autorisierungs-codes dürfen von den verwendeten Systemelementen nicht über den Signaturvorgang hinaus im Speicher verbleiben. Eingabeerleichterungen bei wiederholter Eingabe von Autorisierungs-codes müssen ausgeschlossen sein. Das unbefugte Erfahren der Autorisierungs-codes muss durch dessen Gestaltung und durch Sperrmechanismen wirksam ausgeschlossen sein.

#### Signaturen für qualifizierte Zertifikate

§ 5. (1) Signaturerstellungsdaten, die Zertifizierungsdiensteanbieter bei der Ausstellung qualifizierter Zertifikate verwenden, müssen in einer nach § 9 geprüften Signaturerstellungseinheit erzeugt sein. Sie dürfen außerhalb dieser Signaturerstellungseinheit nicht zur Verfügung stehen. Die

verwendeten Algorithmen und Parameter müssen dem Anhang entsprechen.

(2) Ein Zertifizierungsdiensteanbieter muss in der Lage sein, sichere elektronische Signaturen, die auf der Basis eines von ihm ausgestellten qualifizierten Zertifikats erstellt wurden, zu prüfen. Die Verfahren und Algorithmen zur Signaturprüfung bilden mit den Verfahren und Algorithmen zur Signaturerstellung eine logische Einheit und sind gemeinsam zu dokumentieren.

#### Signaturen der Aufsichtsstelle

§ 6. Signaturerstellungsdaten, die die Aufsichtsstelle für sichere elektronische Signaturen bei der Führung der Verzeichnisse der Zertifikate für Zertifizierungsdiensteanbieter gemäß § 13 Abs. 3 SigG verwendet, müssen § 3 Abs. 2 entsprechen und in einer nach § 9 geprüften Signaturerstellungseinheit erzeugt und gespeichert werden. Sie dürfen außerhalb dieser Signaturerstellungseinheit nicht zur Verfügung stehen.

#### Systeme der Aufsichtsstelle

§ 7. Das Erzeugungssystem sowohl für die Signaturerstellungsdaten als auch für die sicheren Signaturen muss isoliert und ausschließlich für die Zwecke des § 6 bestimmt sowie angemessen vor Eingriffen und Störungen geschützt sein.

#### 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

§ 9. (1) Bei der Prüfung der technischen Komponenten und Verfahren für die Erzeugung sicherer Signaturen sind Sicherheitsvorgaben anzuwenden, die von einer Bestätigungsstelle (§ 19 SigG) als geeignet anerkannt sind. Hiebei können insbesondere Schutzprofile (Protection Profiles) herangezogen werden, die nach den „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Security Evaluation - ISO/IEC 15408)“ oder nach den „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (Information Technology Security Evaluation Criteria - ITSEC)“ erstellt wurden. Das Gleiche gilt für die Prüfung von vertrauenswürdigen Systemen, Produkten und Verfahren, die für die Erstellung von qualifizierten Zertifikaten, für die Speicherung von Signaturerstellungsdaten für qualifizierte Zertifikate oder für sichere Zeitstempeldienste eingesetzt werden.

(2) Bei den Prüfungen nach Abs. 1 sind insbesondere Referenznummern zu beachten, die im Amtsblatt der Europäischen Gemeinschaften nach Art. 3 Abs. 5 der Signaturrechtlinie 1999/93/EG für sichere Signaturerstellungseinheiten (Secure Signature-Creation Devices - SSCD) oder vertrauenswürdige Systeme oder Produkte des Zertifizierungsdiensteanbieters veröffentlicht wurden.

(3) Wenn technische Komponenten und Verfahren in einer kontrollierten Umgebung eingesetzt werden, können Sicherheitsanforderungen, die nach Abs. 1 technisch sichergestellt werden müssen, auch organisatorisch durch Einsatz qualifizierten und vertrauenswürdigen Personals oder technisch-organisatorisch durch Einsatz geeigneter Zugriffs- und Zutrittskontrollmaßnahmen erfüllt werden. Die Erfüllung dieser Sicherheitsanforderungen ist durch eine Bestätigungsstelle zu prüfen.

(4) In der Bescheinigung der Bestätigungsstelle über die Erfüllung

der Sicherheitsanforderungen für technische Komponenten und Verfahren für die Erzeugung sicherer Signaturen (§ 18 Abs. 5 SigG) ist anzugeben, für welche Anwendungen, unter welchen Einsatzbedingungen und bis zu welchem Zeitpunkt sie gilt. Ausfertigungen der Bescheinigung und allfällige Prüfberichte sind 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, der qualifizierte Zertifikate ausstellt oder sichere elektronische Signaturverfahren bereitstellt, 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 oder bei der Produktion der Signaturerstellungseinheit erzeugt, so dürfen diese Signaturerstellungsdaten vom Zertifizierungsdiensteanbieter 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 erforderliche Maßnahmen zur Auslösung der Signaturfunktion, Sicherheit der Autorisierungs-codes, 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. Die Daten des vorgelegten Lichtbildausweises sind, zB durch Herstellung einer Ablichtung, zu erfassen und mit dem Antrag zu dokumentieren. Wenn der vorgelegte Ausweis dies aufgrund seiner technischen Ausstattung zulässt, kann die Pflicht zur Erfassung und Dokumentation auch in ausschließlich elektronischer Form erfüllt werden. Der Antrag auf Ausstellung eines qualifizierten Zertifikats muss vom Zertifikatswerber eigenhändig unterschrieben sein. Verwendet er hiezu eine elektronische Signatur, der eine eindeutige Identität zugeordnet ist, kann von der neuerlichen Identitätsfeststellung anlässlich der Antragstellung 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) Die Formate für qualifizierte Zertifikate sind eindeutig und vollständig zu spezifizieren, so dass deren automatische Prüfung möglich ist.

(3) Die Gültigkeitsdauer eines qualifizierten Zertifikats darf höchstens fünf Jahre betragen.

(4) Bis zum Ablauf der Gültigkeit eines qualifizierten Zertifikats ist es zulässig, mit Ausnahme der Gültigkeitsdauer und der eindeutigen Kennung dieselben Inhalte samt denselben Signaturprüfdaten neu zu zertifizieren und auf diese Weise ein neues Zertifikat auszustellen. In allen anderen Fällen bewirkt der Umstand, dass für Signaturzwecke ausgestellte qualifizierte Zertifikate dieselben Signaturprüfdaten, aber unterschiedliche Inhalte aufweisen, 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 und Widerrufen des anderen Zertifizierungsdiensteanbieters unmittelbar nachzuvollziehen.

#### Verzeichnis- und Widerrufsdienste für qualifizierte Zertifikate

§ 13. (1) Die Verzeichnis- und Widerrufsdienste können in unterschiedlichen Formaten bereitgestellt werden. Der Zertifizierungsdiensteanbieter hat sicherzustellen, dass die Formate der Widerrufsdienste für deren Weiterführung durch die Aufsichtsstelle geeignet sind. Die Formate der Widerrufsdienste, die sich auf ein qualifiziertes Zertifikat beziehen, dürfen während der Geltungsdauer des qualifizierten Zertifikats nicht verändert werden. Jedenfalls müssen Widerrufsdienste die Feststellung zulassen, ob eine Signatur zu einem bestimmten Zeitpunkt der Erstellung gültig oder das Zertifikat widerrufen war.

(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 zehn Tage 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 nur Systeme, Produkte und Verfahren eingesetzt werden, die vor Veränderung geschützt und technisch und kryptographisch sicher sind. Die Zeitstempel müssen in einer nach § 9 geprüften Signaturerstellungseinheit erzeugt werden. Die dabei verwendeten Algorithmen und Parameter müssen dem Anhang entsprechen. Sofern für Zeitstempeldienste Zertifikate eingesetzt werden, dürfen nur solche verwendet werden, die ausschließlich für diesen Zweck ausgestellt wurden und diesen Verwendungszweck ausdrücklich 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 und die Sicherheitsmaßnahmen zur automatischen Auslösung der Zeitstempelfunktion müssen im Sicherheitskonzept des Zertifizierungsdiensteanbieters, der solche Dienste bereitstellt, angegeben werden.

#### Sicherheits- und Zertifizierungskonzept für qualifizierte Zertifikate und sichere Zeitstempeldienste

§ 15. (1) Das Sicherheits- und Zertifizierungskonzept von Zertifizierungsdiensteanbietern, die qualifizierte Zertifikate ausstellen, hat insbesondere folgende Angaben zu enthalten:

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 Autorisierungs-codes,
15. anwendbare Formate für zu signierende Daten 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 für einen sicheren Zeitstempeldienst hat insbesondere folgende Angaben zu enthalten:

1. Namen des Zertifizierungsdiensteanbieters,
2. Adresse des Zertifizierungsdiensteanbieters und Staat seiner Niederlassung,
3. Art, Anwendungsbereich und Erbringung der bereitgestellten Zeitstempeldienste,
4. Signaturprüfdaten des Zeitstempeldienstes,
5. eingesetzte Verfahren zur Erstellung der bereitgestellten Zeitstempel,
6. Formate des Zeitstempels,
7. Verfügbarkeitszeitraum der Zeitstempeldienste,
8. nachvollziehbare und allgemein verständliche Methode zur Prüfung der Zeitstempel,
9. Form der Dokumentation von Sicherheitsvorkehrungen, Störfällen und besonderen Betriebssituationen,
10. Schutz der technischen Komponenten vor unbefugten Veränderungen.

(3) Das Sicherheits- und Zertifizierungskonzept ist der Aufsichtsstelle in elektronischer Form im Format XML mit Darstellungsfunktion, PDF, Ascii oder Postscript vorzulegen. Es muss mit der elektronischen Signatur (§ 5 Abs. 3 SigG) des Zertifizierungsdiensteanbieters versehen sein. Zusätzlich hat der Zertifizierungsdiensteanbieter das Sicherheits- und Zertifizierungskonzept sowie eine klar und allgemein verständlich formulierte Zusammenfassung des Konzepts im Format XML mit Darstellungsfunktion, PDF, Ascii oder Postscript elektronisch jederzeit allgemein abrufbar bereit 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 oder sichere elektronische Signaturverfahren bereitstellt, enthaltenen Daten müssen mit seiner elektronischen Signatur (§ 5 Abs. 3 SigG) versehen sein und sichere Zeitangaben (§ 14 Abs. 2) enthalten.

(2) Die Dokumentation nach Abs. 1 ist zumindest 35 Jahre ab der letzten Eintragung aufzubewahren und so zu sichern, dass sie innerhalb dieses Zeitraums lesbar und verfügbar bleibt.

(3) Zertifizierungsdiensteanbieter, die keine qualifizierten Zertifikate ausstellen, haben eine Dokumentation über die Signaturprüfdaten des Zertifizierungsdiensteanbieters, die ausgestellten Zertifikate und die Widerrufe zu führen. Die Aufbewahrungsdauer der Dokumentation ist im Sicherheits- und Zertifizierungskonzept anzugeben.

#### Erneuerte elektronische Signatur (Nachsignieren)

§ 17. (1) 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. Ein Nachsignieren muss jedenfalls vor Ablauf der für die Sicherheit der eingesetzten Signaturerstellungsverfahren maßgeblichen Periode erfolgen. Der Zeitpunkt des Nachsignierens muss aus dem nachsignierten Dokument ersichtlich sein.

(2) Die drohende Verringerung des Sicherheitswertes eines Dokuments kann auch durch das Anbringen eines Zeitstempels verhindert 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 XML mit Darstellungsfunktion, 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 entsprechenden Zertifikats in komplementärer Weise anwendbar sind.

(2) Der Anzeige für qualifizierte Zertifikate 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, die qualifizierte Zertifikate ausstellen, 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. 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. (1) 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).

(2) Die Verordnung, mit der die Signaturverordnung geändert wird, BGBl. II Nr. 527/2004, wurde unter Einhaltung der Bestimmungen der Richtlinie 98/34/EG über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften, ABl. Nr. L 204 vom 21.07.1998 S 37, in der Fassung der Richtlinie 98/48/EG, ABl. Nr. L 217 vom 05.08.1998 S 18, der Kommission notifiziert (Notifikationsnummer 2004/321/A).

#### Verlautbarungen

§ 20. Die in § 9 zitierten Unterlagen mit technischem Inhalt sind über die Internetseite der Aufsichtsstelle jeweils elektronisch abrufbar zu machen.

#### In-Kraft-Treten

§ 21. Die §§ 1 bis 7 und 9 bis 22 in der Fassung der Verordnung BGBl. II Nr. 527/2004 treten mit 1. Jänner 2005 in Kraft.

#### Schlussbestimmung

§ 22. Bescheinigungen einer Bestätigungsstelle, die vor dem in § 21 genannten In-Kraft-Tretens-Zeitpunkt ausgestellt wurden, bleiben weiterhin wirksam.

#### ANHANG

##### Algorithmen und Parameter für sichere elektronische Signaturen

###### 1. Definitionen

1. Signatursuite: Eine Signatursuite besteht aus folgenden Komponenten:
  - einem Signaturalgorithmus mit Parametern,
  - einem Algorithmus zur Schlüsselerzeugung,
  - einem Padding-Verfahren und
  - einer kryptographischen Hashfunktion.
2. Bitlänge: Die Bitlänge einer natürlichen Zahl  $p$  ist  $r$ , wenn  $2^{\text{hoch } r-1} \leq p < 2^{\text{hoch } r}$  gilt.
3. Kryptographische Hashfunktion: Der Algorithmus „Hash-Funktion“

ist eine nicht umkehrbare Funktion, die eine umfangreiche Datenmenge (i.d.R. einen Text) auf eine im Allgemeinen wesentlich kleinere Zielmenge fester Länge (Hash-Wert) abbildet.

## 2. Abkürzungen

A9C	„Article 9 Committee“ (Ausschuss für elektronische Signaturen gemäß Art. 9 der Richtlinie 1999/93/EG)
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
ECGDSA	Elliptic Curve German Digital Signature Algorithm
RSA	Verfahren von Rivest, Shamir und Adleman
ZDA	Zertifizierungsdiensteanbieter

## 3. Zulässige Signatursuiten

Algorithmen und Parameter für sichere elektronische Signaturen dürfen nur in vordefinierten Kombinationen verwendet werden, die als Signatursuiten bezeichnet werden.

Falls eine Komponente der Suite ungültig ist, ist auch die gesamte Suite ungültig. Falls eine Komponente der Suite aktualisiert worden ist, ist auch die gesamte Suite zu aktualisieren.

Tabelle 1a - Liste der zulässigen Signatursuiten:

Kennzahl des Signatur-suite-Eintrags	Signatur-Algorithmus	Parameter des Signatur-algorithmus	Algorithmus zur Schlüssel-erzeugung	Padding-Verfahren	Krypto-graphische Hash-funktion
001	rsa	MinModLen = 1020	rsagen1	emsa-pkcs1-v1_5	sha1
002	rsa	MinModLen = 1020	rsagen1	emsa-pss	sha1
003	rsa	MinModLen = 1020	rsagen1	emsa-pkcs1-v1_5	ripemd160
004	rsa	MinModLen = 1020	rsagen1	emsa-pss	ripemd160
005	dsa	pMinLen = 1024 qMinLen = 160	dsagen1	-	sha1
006	ecdsa-Fp	qMinLen = 160 r0Min = 10 hoch 4 MinClass = 200	ecgen1	-	sha1
007	ecdsa-F2m	qMinLen = 160 r0Min = 10 hoch 4 MinClass = 200	ecgen2	-	sha1
008	ecgdsa-Fp	qMinLen = 160 r0Min = 10 hoch 4	ecgen1	-	sha1

		MinClass = 200			
009	ecgdsa-Fp	qMinLen = 160 r0Min = 10 hoch 4 MinClass = 200	ecgen1	-	ripemd160
010	ecgdsa-F2m	qMinLen = 160 r0Min = 10 hoch 4 MinClass = 200	ecgen2	-	sha1
011	ecgdsa-F2m	qMinLen = 160 r0Min = 10 hoch 4 MinClass = 200	ecgen2	-	ripemd160

Einige der in diesem Anhang gegebenen Algorithmen sind über Objektidentifikatoren registriert. Diese werden als Information in Tabelle 1b wiedergegeben.

Tabelle 1b - Objektidentifikatoren (OID)

Objekt-Kurzbezeichnung	OID	Bezeichnung in diesem Anhang
rsa	{ joint-iso-ccitt(2) ds(5) module(1) algorithm(8) encryptionAlgorithm(1) 1 }	rsa
sha-1 WithRSA Encryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }	rsa, sha1, emsapkcs, etc.
id-dsa	{ iso(1) member-body(2) us(840) x9-57(10040)x9cm(4)	dsa
id-dsa-with-sha1	{ iso(1) member-body(2) us(840) x9-57(10040)x9cm(4) 3 }	dsa, sha1
sha1	{ iso(1) identifiedOrganization (3) oIW(14) oIWSecSig(3) oIWSec Algorithm(2) 26 }	sha1
ripemd160	{ iso(1) identifiedOrganization (3) teletrust(36) algorithm(3) hashAlgorithm(2) 1 }	ripemd160
id-ecdsa-with-sha1	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) 1 }	ecdsa, sha1
id-rsassa-pss	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10 }	emsa-pss

#### 4. Zulässige kryptographische Hashverfahren

Für sichere elektronische Signaturen dürfen nur kollisionsresistente Hashfunktionen eingesetzt werden. Diese Voraussetzung ist erfüllt, wenn es rechnerisch nicht realisierbar ist, zwei Dokumente zu finden, die denselben Hashwert liefern.

Tabelle 2 - Liste der derzeit zulässigen Hashfunktionen

Kennzahl der Hashfunktion	Kurzbezeichnung der Hashfunktion
2.01	sha1
2.02	ripemd160

## 5. Zulässige Padding-Verfahren

Tabelle 3 - Liste der zulässigen Padding-Verfahren

Kennzahl des Padding- Verfahrens	Kurzbezeichnung des Füllverfahrens	Erzeugung der Zufallszahlen	Parameter des Zufallszahlen- generators
3.01	emsa-pkcs1-v1_5	-	-
3.02	emsa-pss	noch zu definieren	noch zu definieren

## 6. Zulässige Signaturalgorithmen

Tabelle 4 - Liste der zulässigen Signaturalgorithmen

Kennzahl des Signatur- algorithmus	Kurzbezeichnung des Signatur- algorithmus	Parameter des Signatur- algorithmus	Algorithmus zur Schlüssel- und Parametererzeugung
1.01	rsa	MinModLen = 1020	rsagen1
1.02	dsa	pMinLen = 1024 qMinLen = 160	dsagen1
1.03	ecdsa-Fp	qMinLen = 160 r0Min = 10 hoch 4 MinClass = 200	ecgen1
1.04	ecdsa-F2m	qMinLen = 160 r0Min = 10 hoch 4 MinClass = 200	ecgen2
1.05	ecgdsa-Fp	qMinLen = 160 r0Min = 10 hoch 4 MinClass = 200	ecgen1
1.06	Ecgdsa-F2m	qMinLen = 160 r0Min = 10 hoch 4 MinClass = 200	ecgen2

Tabelle 5 - Liste der zulässigen Schlüsselerzeugungsalgorithmen für die in Tabelle 4 aufgelisteten Signaturalgorithmen

Kennzahl des	Kurzbezeichnung des Schlüssel-	Signatur- algorithmus	Verfahren der	Parameter des Zufalls-
-----------------	-----------------------------------	--------------------------	------------------	---------------------------

Schlüssel- erzeugungs- algorithmus	erzeugungs- algorithmus		Zufalls- zahlen- erzeugung	zahlen- erzeugungs- verfahrens
4.01	rsagen1	rsa	trueran oder pseuran	Entropy Bits $\geq 128$ or SeedLen $\geq 128$
4.02	dsagen1	dsa	trueran oder pseuran	Entropy Bits $\geq 128$ or SeedLen $\geq 128$
4.03	ecgen1	ecdsa-Fp, ecgdsa-Fp	trueran oder pseuran	Entropy Bits $\geq 128$ or SeedLen $\geq 128$
4.04	ecgen2	ecdsa-F2m, ecgdsa-F2m	trueran oder pseuran	Entropy Bits $\geq 128$ or SeedLen $\geq 128$

## 7. Erläuterungen zu einzelnen Parametern der zulässigen Signaturalgorithmen

### 7.1 RSA

Die Sicherheit des RSA-Algorithmus beruht auf der Schwierigkeit, große ganze Zahlen zu faktorisieren. Um die Signaturerstellungsdaten und Signaturprüfdaten zu erzeugen, sind zufällig und unabhängig zwei Primzahlen  $p$  und  $q$  zu erzeugen, wobei die Bitlänge des Moduls  $n = pq$  mindestens  $\text{MinModLen}$  betragen muss; seine Länge wird auch als  $\text{ModLen}$  bezeichnet; Jede Primzahl muss effektiv von  $\text{EntropyBits}$  Bits tatsächlichem Zufall oder einem Ausgangswert der Länge  $\text{SeedLen}$  beeinflusst sein.  $p$  und  $q$  sollten etwa dieselbe Länge aufweisen, z.B. soll ein Bereich wie  $0,5 < |\log_2 p - \log_2 q| < 30$  festgelegt werden.

### 7.2 DSA

Die Sicherheit des DSA-Algorithmus beruht auf der Schwierigkeit, den diskreten Logarithmus in der multiplikativen Gruppe eines Primkörpers  $F$  tief  $p$  zu berechnen.

Die Signaturerstellungsdaten bestehen aus

- den öffentlichen Parametern  $p$ ,  $q$  und  $g$ ,
- einer zufällig oder pseudozufällig erzeugten ganzen Zahl  $x$ ,  $0 < x < q$ , die signaturspezifisch ist, und
- einer zufällig oder pseudozufällig erzeugten ganzen Zahl  $k$ ,  $0 < k < q$ , die für jede Signatur neu zu erzeugen ist.

Die öffentlichen Parameter  $p$ ,  $q$  und  $g$  dürfen für eine Gruppe von Benutzern gleich sein. Der prime Modul  $p$  muss mindestens  $p\text{MinLen}$  Bits lang sein.  $q$ , das ein Primfaktor von  $(p-1)$  ist, muss mindestens  $q\text{MinLen}$  Bits lang sein.

Die Signaturprüfdaten bestehen aus  $p$ ,  $q$ ,  $g$  und einer ganzen Zahl  $y$ , die als  $y = g \text{ hoch } x \text{ mod } p$  berechnet wird.

#### 7.2.1 DSA-Varianten mit elliptischen Kurven basierend auf einer Gruppe $E(F$ tief $p)$

Die Sicherheit des Algorithmus  $\text{ecdsa-Fp}$  beruht auf der Schwierigkeit, den diskreten Logarithmus über elliptischen Kurven zu berechnen.

Die öffentlichen Parameter sind wie folgt:

- $p$  eine große Primzahl,

- $q$  eine große Primzahl mit einer Länge von mindestens  $q_{\text{MinLen}}$  Bits,  $p$  (Anm.: Zeichen nicht darstellbar)  $q$ ;
- $E$  eine elliptische Kurve über dem endlichen Körper  $F$  tief  $p$ , deren Ordnung durch  $q$  teilbar ist, und
- $P$  ein fixer Punkt auf  $E$  mit der Ordnung  $q$ .

Die Klassenzahl der maximalen Ordnung des Endomorphismenrings von  $E$  muss mindestens  $\text{MinClass}$  betragen. Der Wert  $r$  tief  $0 := \min(r: q \text{ teilt } p \text{ hoch } r - 1)$  muss größer als  $r_{0\text{Min}}$  sein.

Die Signaturerstellungsdaten bestehen aus

- den öffentlichen Parametern  $E$ ,  $q$  und  $P$ ;
- einer statistisch einzigartigen und nicht voraussagbaren ganzen Zahl  $x$ ,  $0 < x < q$ , die signatorspezifisch ist und
- einer statistisch einzigartigen und nicht voraussagbaren ganzen Zahl  $k$ ,  $0 < k < q$ , die für jede Signatur neu zu erzeugen ist.

Die Signaturprüfdaten bestehen aus  $E$ ,  $q$ ,  $P$  und einem Punkt  $Q$  auf  $E$ , der als  $Q = xP$  berechnet wird. Die elliptische Kurve über  $F$  tief  $p$  muss so gewählt werden, dass ihre Ordnung durch eine Primzahl  $q$  der Länge  $\geq q_{\text{MinLen}} \geq 160$  teilbar ist.

#### 7.2.2 DSA-Varianten mit elliptischen Kurven basierend auf einer Gruppe $E(F$ tief $2 m)$

Die Sicherheit des Algorithmus  $\text{ecdsa-F2m}$  beruht auf der Schwierigkeit, den diskreten Logarithmus über elliptischen Kurven zu berechnen.

Die öffentlichen Parameter sind wie folgt:

- $m$  eine Primzahl,
- $q$  eine große Primzahl mit einer Länge von mindestens  $q_{\text{MinLen}}$  Bits,
- $E$  eine elliptische Kurve über dem endlichen Körper  $F$  tief  $2 m$ , deren Ordnung durch  $q$  teilbar ist,
- es darf nicht möglich sein,  $E$  über  $F$  tief  $2$  zu definieren, und
- $P$  ein fixer Punkt auf  $E$  mit der Ordnung  $q$ .

Die Klassenzahl der maximalen Ordnung des Endomorphismenrings von  $E$  muss mindestens  $\text{MinClass}$  betragen. Der Wert  $r$  tief  $0 := \min(r: q \text{ teilt } 2 \text{ hoch } mr - 1)$  muss größer als  $r_{0\text{Min}}$  sein.

Die Signaturerstellungsdaten bestehen aus

- den öffentlichen Parametern  $E$ ,  $q$  und  $m$ ;
- einer statistisch einzigartigen und nicht voraussagbaren ganzen Zahl  $x$ ,  $0 < x < q$ , die signatorspezifisch ist, und
- einer statistisch einzigartigen und nicht voraussagbaren ganzen Zahl  $k$ ,  $0 < k < q$ , die für jede Signatur neu zu erzeugen ist.

Die Signaturprüfdaten bestehen aus  $E$ ,  $q$ ,  $P$  und einem Punkt  $Q$  auf  $E$ , der als  $Q = xP$  berechnet wird. Die elliptische Kurve über  $F$  tief  $2 m$  muss so gewählt werden, dass ihre Ordnung durch eine Primzahl  $q$  der Länge  $\geq q_{\text{MinLen}} \geq 160$  teilbar ist.

#### 7.2.3 EC-GDSA basierend auf einer Gruppe $E(F$ tief $p)$

Der  $\text{ecgdsa-Fp}$  Algorithmus ist eine Variante des  $\text{ecdsa-Fp}$  Algorithmus mit modifizierter Gleichung zur Signaturerstellung und modifiziertem Verfahren zur Signaturprüfung. Die Parameter sind dieselben wie für  $\text{ecdsa-Fp}$ .

#### 7.2.4 EC-GDSA basierend auf einer Gruppe $E(F$ tief $2 m)$

Der Algorithmus  $\text{ecgdsa-F2m}$  ist eine Variante des Algorithmus  $\text{ecdsa-F2m}$  mit modifizierter Gleichung zur Signaturerstellung und modifiziertem Verfahren zur Signaturprüfung.

### 8. Erzeugung von Zufallszahlen

Tabelle 6 - Liste der zulässigen Verfahren zur Erzeugung von Zufallszahlen

Kennzahl des Zufallsgenerators	Kurzbezeichnung des Zufallsgenerators	Parameter der Zufallszahlenerzeugung
5.01	Trueran	EntropyBits

5.02	Pseuran	SeedLen
5.03	cr_to_X9.30_x	SeedLen
5.04	cr_to_X9.30_k	SeedLen

### 8.1 Anforderungen an Zufallszahlengeneratoren trueran

Ein physikalischer Zufallszahlengenerator basiert auf einer physikalischen Rauschquelle (Primärauschen) und einer kryptographischen oder mathematischen Nachbehandlung des Primärauschens. Das Primärauschen muss regelmäßig einer geeigneten statistischen Prüfung unterzogen werden. Der erwartete Aufwand des Erratens eines kryptographischen Schlüssels soll mindestens gleich groß sein, wie der Aufwand des Ratens eines Zufallswerts der Länge  $\text{EntropyBits}$ .

### 8.2 Anforderungen an Zufallszahlengeneratoren pseuran

Ein Pseudo-Zufallszahlengenerator muss mit einer echten Zufallszahl initialisiert werden. Der Anfangswert wird als „Seed“ bezeichnet und hat die Länge  $\text{SeedLen}$ . Die Ausgabe des Generators muss folgenden Anforderungen genügen:

- keine Information hinsichtlich der erzeugten Ausgabebits ist vorab bestimmbar;
- die Kenntnis einer Teilsequenz der Ausgabe erlaubt keinen Rückschluss auf ein verbleibendes Bit mit einer Wahrscheinlichkeit, die sich nicht-vernachlässigbar von Zufall unterscheidet;
- es gibt kein verwendbares Verfahren, um aus der Ausgabe des Generators eine zuvor generierte oder zukünftige Ausgabe, einen internen Status oder den Anfangswert („Seed“) zu erlangen.

Der erwartete Aufwand des Erlangens jedweden internen Status des Generators soll im Wesentlichen der Schwierigkeit des Erratens eines Zufallswerts der Länge  $\text{SeedLen}$  Bits sein.

Wenn der Generator mit mindestens  $\text{SeedLen}$  Bits initialisiert wurde, können bis zu  $n = 100$  Folge erzeugte Signaturerstellungsdaten

gleichermaßen verwendet werden, als ob sie von einem Generator trueran erzeugt worden wären. Für die Massenproduktion (durch den Zertifizierungsdiensteanbieter ZDA) von  $k$  Schlüsseln,  $k > n$  ist es zulässig, dass zusätzlich zur initialen Entropieanforderung echter Zufall (von einem trueran Generator) langsam mit einer Rate von  $j = 8$  Bits pro Ausgabewert beigegeben wird, andernfalls sollte der Generator komplett neu initialisiert werden.

Wenn Re-Initialisierung angewandt wird, muss die Sicherheit des Re-Initialisierungsprozesses zumindest so stark sein, wie die ursprüngliche Initialisierung und Prozeduren folgen, die der Erstellung von Root-Schlüsseln ähnlich sind. Die Re-Initialisierung von Smartcards ist nicht zulässig.

Keine Backups des Anfangswerts („Seed“) oder interner Stati von Pseudo-Zufallszahlengeneratoren sind zulässig.