BUNDESGESETZBLATT
FÜR DIE REPUBLIK ÖSTERREICH

Jahrgang 2004 Ausgegeben am 30. Dezember 2004 Teil II

527. Verordnung des Bundeskanzlers, mit der die Signaturverordnung geändert wird

Auf Grund des § 25 des Signaturgesetzes, BGBl. I Nr. 190/1999, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 152/2001, wird im Einvernehmen mit dem Bundesminister für Justiz verordnet:

Die Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung – SigV), BGBl. II Nr. 30/2000, wird wie folgt geändert:

1. Die Inhaltsübersicht samt Überschrift lautet:

„Inhaltsverzeichnis

2. § 1 samt Überschrift lautet:

„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 50 Euro;

	zweiter Satz SigG)	
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.“

3. § 2 Abs. 1 zweiter Satz lautet:

„Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen oder sichere elektronische Signaturverfahren bereitstellen, haben ein Mindestkapital in Höhe von 300 000 Euro aufzuweisen.“

4. In § 2 lauten die Abs. 2 und 3:

„(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."

5. Die §§ 3 bis 7 lauten samt Überschriften:

„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 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 im Zeitpunkt des Auslösens des Signaturvorgangs bekannt sein. Derselbe Autorisierungscode darf nicht für unterschiedliche Anwendungen (zB Signatur- und Bankomatfunktion) verwendbar sein. Die eingegebenen Autorisierungscodes dürfen von den verwendeten Systemelementen nicht über den Signaturvorgang hinaus im Speicher verbleiben. Eingabeerleichterungen bei wiederholter Eingabe von Autorisierungscodes müssen ausgeschlossen sein. Das unbefugte Erfahren der Autorisierungscodes 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."

6. § 9 lautet samt Überschrift:

„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 Signaturrichtlinie 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.“

7. In § 10 Abs. 2 erster Satz wird nach dem Wort „Zertifizierungsdiensteanbieters*“ der Ausdruck* „ , der qualifizierte Zertifikate ausstellt oder sichere elektronische Signaturverfahren bereitstellt,*“ eingefügt.*

8. § 10 Abs. 6 erster Satz lautet:

„Werden die Signaturerstellungsdaten beim Zertifizierungsdiensteanbieter oder bei der Produktion der Signaturerstellungseinheit erzeugt, so dürfen diese Signaturerstellungsdaten vom Zertifizierungsdiensteanbieter nur an den Signator ausgehändigt werden.“

9. In § 10 Abs. 7 wird nach der Abkürzung „zB“ *der Ausdruck* „erforderliche Maßnahmen zur Auslösung der Signaturfunktion,“ *eingefügt.*

10. § 11 Abs. 1 lautet:

„(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.“

11. In § 12 lauten die Abs. 2 bis 4:

„(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.“

12. § 13 Abs. 1 lautet:

„(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."

13. In § 13 Abs. 7 lautet der zweite Satz:

„Dieser Zeitraum darf zehn Tage nicht übersteigen."

14. § 14 Abs. 1 lautet:

„(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."

15. In § 14 Abs. 3 wird das Wort „muss" *durch die Wendung* „und die Sicherheitsmaßnahmen zur automatischen Auslösung der Zeitstempelfunktion müssen" *ersetzt.*

16. In § 15 lautet die Überschrift:

„Sicherheits- und Zertifizierungskonzept für qualifizierte Zertifikate und sichere Zeitstempeldienste"

17. In § 15 Abs. 1 lautet der Einleitungssatz:

„Das Sicherheits- und Zertifizierungskonzept von Zertifizierungsdiensteanbietern, die qualifizierte Zertifikate ausstellen, hat insbesondere folgende Angaben zu enthalten:"

18. In § 15 Abs. 1 Z 15 wird das Wort „Dokumente" *durch das Wort* „Daten" *ersetzt.*

19. § 15 Abs. 2 wird durch folgende Abs. 2 und 3 ersetzt:

„(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."

20. § 16 Abs. 1 letzter Satz lautet:

„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."

*21. In § 16 Abs. 2 werden die Worte „*33 Jahre*“ durch die Worte „*35 Jahre*“ ersetzt.*

22. Nach § 16 Abs. 2 wird folgender Abs. 3 angefügt:

„(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.“

23. § 17 lautet:

„**§ 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.“

24. In § 18 Abs. 1 wird der Ausdruck „RTF,“ *durch den Ausdruck* „XML mit Darstellungsfunktion,“ *ersetzt.*

25. In § 18 Abs. 2 lautet der Einleitungssatz:

„Der Anzeige für qualifizierte Zertifikate sind insbesondere anzuschließen:“

26. In § 18 Abs. 4 erster Satz wird nach dem Wort „Zertifizierungsdiensteanbieter“ *die Wendung* “, die qualifizierte Zertifikate ausstellen,“ *eingefügt.*

27. In § 18 Abs. 6 entfällt der zweite Satz.

28. In § 19 erhält der bisherige Text die Absatzbezeichnung „(1)*“ und es wird folgender Abs. 2 angefügt:*

„(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).“

29. Nach dem § 19 werden folgende §§ 20 bis 22 samt Überschrift angefügt:

„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.“

30. Die Anhänge 1 und 2 werden durch folgenden Anhang ersetzt:

„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 $2^{r-1} \leq p < 2^r$ 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 Signatursuite-Eintrags	Signatur-Algorithmus	Parameter des Signaturalgorithmus	Algorithmus zur Schlüsselerzeugung	Padding-Verfahren	Kryptographische Hashfunktion
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 = 10^4 MinClass = 200	ecgen1	-	sha1
007	ecdsa-F2m	qMinLen = 160 r0Min = 10^4 MinClass = 200	ecgen2	-	sha1
008	ecgdsa-Fp	qMinLen = 160 r0Min = 10^4 MinClass = 200	ecgen1	-	sha1
009	ecgdsa-Fp	qMinLen = 160 r0Min = 10^4 MinClass = 200	ecgen1	-	ripemd160
010	ecgdsa-F2m	qMinLen = 160 r0Min = 10^4 MinClass = 200	ecgen2	-	sha1
011	ecgdsa-F2m	qMinLen = 160 r0Min = 10^4 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 WithRSAEncryption	{ 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) 1 }	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) oIWSecAlgorithm(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 Zufallszahlengenerators
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 Signaturalgorithmus	Kurzbezeichnung des Signaturalgorithmus	Parameter des Signaturalgorithmus	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 = 10^4 MinClass = 200	ecgen1

Kennzahl des Signatur-algorithmus	Kurzbezeichnung des Signaturalgorithmus	Parameter des Signatur-algorithmus	Algorithmus zur Schlüssel- und Parameter-erzeugung
1.04	ecdsa-F2m	qMinLen = 160 r0Min = 10^4 MinClass = 200	ecgen2
1.05	ecgdsa-Fp	qMinLen = 160 r0Min = 10^4 MinClass = 200	ecgen1
1.06	Ecgdsa-F2m	qMinLen = 160 r0Min = 10^4 MinClass = 200	ecgen2

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

Kennzahl des Schlüssel-erzeugungs-algorithmus	Kurzbezeichnung des Schlüsselerzeugungs-algorithmus	Signaturalgorithmus	Verfahren der Zufallszahlen-erzeugung	Parameter des Zufallszahlen-erzeugungs-verfahrens
4.01	rsagen1	rsa	trueran oder pseuran	EntropyBits≥128 or SeedLen≥128
4.02	dsagen1	dsa	trueran oder pseuran	EntropyBits≥128 or SeedLen≥128
4.03	ecgen1	ecdsa-Fp, ecgdsa-Fp	trueran oder pseuran	EntropyBits≥128 or SeedLen≥128
4.04	ecgen2	ecdsa-F2m, ecg-dsa-F2m	trueran oder pseuran	EntropyBits≥128 or SeedLen≥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 MinModLen betragen muss; seine Länge wird auch als ModLen bezeichnet; Jede Primzahl muss effektiv von EntropyBits Bits tatsächlichem Zufall oder einem Ausgangswert der Länge SeedLen beeinflusst sein. p und q sollten etwa dieselbe Länge aufweisen, z.B. soll ein Bereich wie $\mathbf{0.5 < |\log_2 p - \log_2 q| < 30}$ festgelegt werden.

7.2 DSA

Die Sicherheit des DSA-Algorithmus beruht auf der Schwierigkeit, den diskreten Logarithmus in der multiplikativen Gruppe eines Primkörpers F_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 signatorspezifisch 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 pMinLen Bits lang sein. q, das ein Primfaktor von $(p-1)$ ist, muss mindestens qMinLen Bits lang sein.

Die Signaturprüfdaten bestehen aus p, q, g und einer ganzen Zahl y, die als $y = g^x \bmod p$ berechnet wird.

7.2.1 DSA-Varianten mit elliptischen Kurven basierend auf einer Gruppe $E(F_p)$

Die Sicherheit des Algorithmus 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 qMinLen Bits, $p \neq q$;
- E eine elliptische Kurve über dem endlichen Körper F_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 MinClass betragen. Der Wert r_0:=min(r: q teilt p^r-1) muss größer als r0Min 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_p muss so gewählt werden, dass ihre Ordnung durch eine Primzahl q der Länge $\geq \mathbf{qMinLen} \geq \mathbf{160}$ teilbar ist.

7.2.2 DSA-Varianten mit elliptischen Kurven basierend auf einer Gruppe $E(F_2\mathrm{m})$

Die Sicherheit des Algorithmus 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 qMinLen Bits,
- E eine elliptische Kurve über dem endlichen Körper $F_2\mathrm{m}$, deren Ordnung durch q teilbar ist,
- es darf nicht möglich sein, E über F_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 MinClass betragen. Der Wert r_0:=min(r: q teilt 2^{mr} -1) muss größer als r0Min 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 $F_2\mathrm{m}$ muss so gewählt werden, dass ihre Ordnung durch eine Primzahl q der Länge $\geq \mathbf{qMinLen} \geq \mathbf{160}$ teilbar ist.

7.2.3 EC-GDSA basierend auf einer Gruppe $E(F_p)$

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

7.2.4 EC-GDSA basierend auf einer Gruppe $E(F_2\mathrm{m})$

Der Algorithmus ecgdsa-F2m ist eine Variante des Algorithmus 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 Zufalls-generators	Kurzbezeichnung des Zufallgenerators	Parameter der Zufallszahlen-erzeugung
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 (Primärrauschen) und einer kryptographischen oder mathematischen Nachbehandlung des Primärrauschens. Das Primärrauschen 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 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 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 SeedLen Bits sein.

Wenn der Generator mit mindestens 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.“

Schüssel