BUNDESGESETZBLATT
FÜR DIE REPUBLIK ÖSTERREICH

Jahrgang 2008 Ausgegeben am 7. Jänner 2008 Teil II

3. Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung 2008 – SigV 2008)

Auf Grund des § 25 des Signaturgesetzes, BGBl. I Nr. 190/1999, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 8/2008, wird im Einvernehmen mit der Bundesministerin für Justiz verordnet:

Gebühren für Aufsichtstätigkeiten

§ 1. (1) Von den Zertifizierungsdiensteanbietern (ZDA) sind für Leistungen im Rahmen der Aufsichtstätigkeit folgende Gebühren zu entrichten:

1. Prüfung des Sicherheits- und Zertifizierungskonzepts anlässlich der Aufnahme der Tätigkeit (§ 6 Abs. 3 SigG) ..... 4 500 Euro;
2. Prüfung des Sicherheits- und Zertifizierungskonzepts eines ZDA, der qualifizierte Zeitstempeldienste bereitstellt ..... 1 500 Euro;
3. Prüfung der Änderung des Sicherheits- und Zertifizierungskonzepts (§ 6 Abs. 2 SigG)
   a) ohne sicherheitsrelevante Änderungen ..... 700 Euro;
   b) mit sicherheitsrelevanten Änderungen ..... 3 000 Euro;
4. freiwillige Akkreditierung (§ 17 SigG), sofern diese nicht im Zuge der Prüfung nach Z 1 erfolgt ..... 4 500 Euro;
5. regelmäßige Prüfung der Umsetzung der Angaben im Sicherheits- und Zertifizierungskonzept pro Jahr ..... 3 000 Euro;
6. regelmäßige Prüfung eines ZDA, der qualifizierte Zeitstempeldienste bereitstellt pro Jahr ..... 1 500 Euro;
7. anlassbezogene Prüfung, die wegen eines erheblichen Verstoßes gegen das SigG oder der auf seiner Grundlage ergangenen Verordnungen oder wegen der Unterlassung der Anzeige sicherheitsrelevanter Veränderungen zu Aufsichtsmaßnahmen nach Z 8 geführt hat (§ 14 SigG) ..... 4 500 Euro;
8. in Bescheidform ergehende Aufsichtsmaßnahmen (§ 14 SigG)
   a) Erteilung von Auflagen aufgrund sicherheitsrelevanter Mängel zusätzlich zu Z 5 ..... 700 Euro;
   b) Untersagung der weiteren Ausübung der Tätigkeit als ZDA zusätzlich zu Z 5 ..... 700 Euro;
9. Weiterführung eines Widerrufsdienstes durch die Aufsichtsstelle (§ 12 und § 14 Abs. 5 SigG) pro Jahr und Zertifikat, das im Widerrufsdienst geführt wird ..... 1 Euro, jedoch insgesamt pro Jahr nicht mehr als 5 000 Euro;
10. Führung der Verzeichnisse bei der Aufsichtsstelle (§ 13 Abs. 3 und § 17 Abs. 1 SigG): pro aufgenommenen ZDA und Jahr 300 Euro;
11. Beurteilung der Gleichwertigkeit von Prüfberichten einer staatlich anerkannten Stelle eines Drittstaates (§ 24 Abs. 3 SigG) ..... 4 500 Euro.

(2) Die Gebühren sind von der Aufsichtsstelle mit Bescheid vorzuschreiben.

(3) Wenn sich die Aufsichtsstelle bei der Aufsicht einer

1. Bestätigungsstelle oder
2. nichtamtlicher Personen oder Einrichtungen als Sachverständiger bedient,

sind die Gebühren nach § 53a AVG dem betroffenen ZDA als Barauslage im Sinne des § 76 AVG vorzuschreiben.

(4) Von den Gebühren nach Abs. 1 Z 1 bis 6 sowie 10 sind der Bund, die Länder, Gemeindeverbände und Gemeinden, sonstige Körperschaften des öffentlichen Rechts sowie die Träger der Sozialversicherung befreit.

(5) Zur Finanzierung der notwendigen Kosten der Aufsichtsstelle und der RTR-GmbH, die nicht durch Gebühreneinahmen gemäß Abs. 1 abgedeckt sind, ist der RTR-GmbH aus dem Bundeshaushalt jährlich per 30. Jänner ein Kostenersatz in der Höhe von 90 000 Euro zu leisten. Sofern sich die Anzahl der zu beaufsichtigenden ZDA nach dem Inkrafttreten dieser Verordnung erhöht, sind die Kosten für dadurch notwendige zusätzliche Tätigkeiten der Aufsichtsstelle und der RTR-GmbH, die nicht durch Gebühreneinahmen gemäß Abs. 1 abgedeckt sind, bis zu einem Betrag von zusätzlich jährlich 60 000 Euro zu ersetzen. Die RTR-GmbH hat dem Bundeskanzler jährlich bis zum 30. April des Folgejahres über die Verwendung dieser Mittel zu berichten und einen Rechnungsabschluss vorzulegen.

Finanzielle Ausstattung der ZDA

§ 2. (1) Die für die Ausübung der Tätigkeit als ZDA regelmäßig zur Verfügung stehenden Finanzmittel sind der Aufsichtsstelle mit Anzeige der Aufnahme der Tätigkeit nach § 6 Abs. 2 SigG bekannt zu geben. Gleichzeitig ist ihr nachzuweisen, dass eine Haftpflichtversicherung mit einer Mindestversicherungssumme von 700 000 Euro, die zumindest drei Versicherungsfälle im Jahr deckt, abgeschlossen worden ist. ZDA haben ein Mindestkapital in Höhe von 300 000 Euro in Form von Eigenmitteln im Sinn des § 224 Abs. 3A und B UGB aufzuweisen oder ein eingezahltes Nennkapital im Sinn des § 224 Abs. 3A UGB in der Höhe von 300 000 Euro nachzuweisen. Im zweiten Fall ist der Jahresabschluss von einem Abschlussprüfer zu prüfen. Unter Nennkapital im Sinn des § 224 Abs. 3A UGB ist das eingezahlte Kapital im Sinn des § 23 Abs. 3 BWG zu verstehen.

(2) Von den Verpflichtungen nach Abs. 1 sind der Bund, die Länder, Gemeindeverbände und Gemeinden, sonstige Körperschaften des öffentlichen Rechts sowie die Träger der Sozialversicherung befreit.

Technische Sicherheitserfordernisse für Signaturerstellungsdaten und –einheiten bei qualifizierten Signaturen

§ 3. (1) Die technischen Komponenten und Verfahren zur Verarbeitung der Signaturerstellungsdaten müssen in Hinblick auf das Erfordernis der Prüfung nach § 18 Abs. 5 SigG den Anforderungen des § 6 entsprechen.

(2) Es dürfen nur jene Algorithmen und Parameter eingesetzt werden, die die Anforderungen des Anhangs erfüllen. Die Rahmenbedingungen für die technische Sicherheit sind so zu wählen, dass sie dem jeweiligen Stand der Technik entsprechen.

(3) Die Signaturerstellungsdaten können auf mehrere getrennte Komponenten verteilt sein. Die Sicherheitsanforderungen müssen in diesem Fall durch die Signaturerstellungseinheit als Gesamtheit der Komponenten erfüllt sein.

Technische Sicherheitserfordernisse für die Systemumgebung der Signaturerstellungseinheit bei qualifizierten Signaturen

§ 4. (1) Die Spezifikation eines Formats für zu signierende Daten muss allgemein verfügbar sein und 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 Änderungen codiert werden, so dürfen jene Elemente, die dynamische Änderungen 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 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) Bei der Ausstellung qualifizierter Zertifikate müssen die vom ZDA verwendeten Signaturerstellungsdaten in einer nach § 6 geprüften Signaturerstellungseinheit erzeugt sein und dürfen außerhalb dieser nicht zur Verfügung stehen. Die verwendeten Algorithmen und Parameter müssen dem Anhang entsprechen.

(2) Der ZDA muss qualifizierte elektronische Signaturen, die auf der Basis eines von ihm ausgestellten qualifizierten Zertifikats erstellt wurden, prüfen können. Die Verfahren und Algorithmen zur Signaturprüfung und Signaturerstellung sind gemeinsam zu dokumentieren.

(3) Der ZDA 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

§ 6. (1) Bei der Prüfung der technischen Komponenten und Verfahren für die Erzeugung qualifizierter Signaturen sind Sicherheitsvorgaben anzuwenden, die von einer Bestätigungsstelle (§ 19 SigG) als geeignet anerkannt sind. Es 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 qualifizierte 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 ZDA 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 an sichere Signaturerstellungseinheiten (§ 18 Abs. 5 SigG) ist anzugeben, unter welchen Einsatzbedingungen und bis zu welchem Zeitpunkt sie gilt. Ausfertigungen der Bescheinigung und allfällige Prüfberichte sind der Aufsichtsstelle zu übermitteln.

(5) Die in den Abs. 1 bis 4 zitierten Unterlagen mit technischem Inhalt sind über die Internetseite der Aufsichtsstelle jeweils elektronisch abrufbar zu machen.

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

§ 7. (1) Werden die Einrichtungen eines ZDA 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 ZDA sind so zu gestalten, dass deren Funktionen und Anwendungen, die zu den bereitgestellten Signatur- und Zertifizierungsdiensten gehören, von anderen Funktionen und Anwendungen getrennt sind und eine Beeinflussung ausgeschlossen ist. Dies muss sowohl für den regulären Betrieb, für besondere Betriebssituationen und außerhalb des Betriebs sichergestellt sein. Besondere Betriebssituationen wie beispielweise eine Wartung sind zu dokumentieren.

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

(4) Ein ZDA 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.

(5) Das technische Personal eines ZDA 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 hat der ZDA Auskunft über das erforderliche Fachwissen des Personals zu geben. Das erforderliche Fachwissen des Personals kann insbesondere durch

1. Absolvierung einer einschlägigen Höheren Technischen Lehranstalt (HTL),
2. einer solchen Fachhochschule,
3. eines einschlägigen Studiums, oder durch
4. eine fachlich einschlägige Tätigkeit in der Dauer von zumindest drei Jahren

erworben werden.

(6) Werden die Signaturerstellungsdaten beim ZDA oder bei der Produktion der Signaturerstellungseinheit erzeugt, so muss vom ZDA sichergestellt werden, dass die Signaturerstellungsdaten 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 ZDA darüber zu vergewissern, dass die Signaturerstellungsdaten des Signators und die Signaturprüfdaten des entsprechenden Zertifikats in komplementärer Weise anwendbar sind.

(7) Der ZDA hat den Zertifikatswerber vor Vertragsabschluss gemäß § 20 SigG schriftlich oder unter Verwendung eines dauerhaften Datenträgers klar und allgemein verständlich zu unterrichten, wobei die Informationen über den Inhalt des Sicherheits- und Zertifizierungskonzepts jedenfalls Erläuterungen zu sämtlichen anwendbaren Angaben nach § 12 Abs. 1 und 2 zu enthalten haben.

Antrag auf Ausstellung eines qualifizierten Zertifikats

§ 8. (1) Zur Feststellung der Identität des Zertifikatswerbers geeignet sind ein

1. amtlicher Lichtbildausweis oder
2. ein Nachweis der bescheinigt, dass die Identität zumindest mit jener Verlässlichkeit geprüft wurde, wie sie bei der Zustellung zu eigenen Handen (§ 21 ZustG) einzuhalten ist.

Die Daten des Lichtbildausweises oder des Nachweises (§ 8 Abs. 1 SigG) sind zu erfassen und mit dem Antrag zu dokumentieren, sofern sie nicht schon dokumentiert wurden. Die Erfassung und Dokumentation kann auch in ausschließlich elektronischer Form erfolgen.

(2) 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 qualifizierten 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

§ 9. (1) Stellt ein ZDA 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 ZDA ist berechtigt, mit Zustimmung eines anderen ZDA 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 ZDA unmittelbar nachzuvollziehen.

Verzeichnis- und Widerrufsdienste für qualifizierte Zertifikate

§ 10. (1) Der ZDA hat sicherzustellen, dass die Formate der Widerrufsdienste für deren Weiterführung durch die Aufsichtsstelle geeignet sind. Die Formate der Widerrufsdienste dürfen während der Geltungsdauer des Zertifikats nicht verändert werden. Jedenfalls müssen Widerrufsdienste die Feststellung zulassen, ob das Zertifikat zu einem bestimmten Zeitpunkt widerrufen war. Die Widerrufsdienste müssen allgemein frei zugänglich sein. Die Abfrage der Widerrufsdienste muss unentgeltlich und ohne Identifikation möglich sein.

(2) Der ZDA hat den Signatoren sowie Dritten, für die Angaben über die Vertretungsmacht des Signators in ein 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 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 darf eine Sperre oder ein Widerruf nicht unbemerkt rückgängig gemacht werden können.

(4) Die Aktualisierung der Widerrufsdienste muss an Werktagen, ausgenommen Samstag, von 9 bis 17 Uhr spätestens innerhalb von drei Stunden ab Bekanntwerden des Widerrufsgrundes erfolgen. Außerhalb dieser Zeit hat der ZDA jedenfalls dafür Sorge zu tragen, dass ein Verlangen auf Widerruf eines qualifizierten Zertifikats jederzeit automatisiert entgegengenommen wird und die Sperre spätestens innerhalb von sechs Stunden auslöst.

(5) Die zeitliche Verfügbarkeit der Verzeichnisdienste muss zumindest nach den in Abs. 4 erster Satz bestimmten Zeiten gegeben sein und im Sicherheitskonzept angegeben werden. 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.

(6) Ein ZDA hat eine Prüfung der Zertifikate bis zum Ablauf der in § 13 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 ZDA.

(7) Der Zeitraum, während dessen eine Sperre wirksam sein kann, muss im Sicherheitskonzept angegeben werden und 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 ZDA selbst vorzunehmen (§ 9 Abs. 1 Z 6 SigG), sobald er von der Kompromittierung Kenntnis erlangt hat.

Qualifizierte Zeitstempeldienste

§ 11. (1) Für die Erbringung qualifizierter 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 § 6 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 qualifizierter Zeitstempeldienste und die Sicherheitsmaßnahmen zur automatischen Auslösung der Zeitstempelfunktion müssen im Sicherheitskonzept des ZDA, der solche Dienste bereitstellt, angegeben werden.

Sicherheits- und Zertifizierungskonzept

§ 12. (1) Das Sicherheits- und Zertifizierungskonzept des ZDA hat insbesondere folgende Angaben zu enthalten:

1. Namen des ZDA,
2. Adresse und Staat der Niederlassung des ZDA,
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 ZDA,
8. Format der Signaturerstellungsdaten des ZDA,
9. Signaturprüfdaten, gegebenenfalls das Zertifikat des ZDA,
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. gängige Formate, die die Voraussetzungen des § 4 Abs. 1 erfüllen, sowie 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. Schutz der technischen Komponenten vor unbefugtem Zugriff,
22. Schutz der Einrichtungen des ZDA vor unbefugtem Zutritt.

(2) Das Sicherheits- und Zertifizierungskonzept für einen qualifizierten Zeitstempeldienst hat insbesondere folgende Angaben zu enthalten:

1. Namen des ZDA,
2. Adresse und Staat der Niederlassung des ZDA,
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 in einem gängigen Format vorzulegen. Es muss mit der elektronischen Signatur (§ 5 Abs. 3 SigG) des ZDA versehen sein. Zusätzlich hat der ZDA das Sicherheits- und Zertifizierungskonzept sowie eine klar und allgemein verständlich formulierte Zusammenfassung des Konzepts in einem gängigen Format bereit zu halten.

Dokumentation

§ 13. (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 ZDA enthaltenen Daten müssen mit seiner elektronischen Signatur (§ 5 Abs. 3 SigG) versehen sein und Zeitangaben nach § 11 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.

Aufsicht und Akkreditierung

§ 14. (1) Die Anzeige der Aufnahme der Tätigkeit eines ZDA nach § 6 Abs. 2 SigG muss in elektronischer Form erfolgen. Soweit spezielle Inhalte der Anzeige nicht ein anderes Format erfordern, ist ein gängiges Format 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 ZDA oder eines vertretungsbefugten Organs anordnen. Die Aufsichtsstelle hat sich darüber zu vergewissern, dass die Signaturerstellungsdaten des ZDA 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 ZDA,
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 ZDA zumindest in regelmäßigen Abständen von zwei Jahren sowie bei sicherheitsrelevanten Veränderungen des Sicherheits- und Zertifizierungskonzepts zu prüfen. Darüber hinaus ist die Aufsichtsstelle berechtigt, jederzeit stichprobenartige Prüfungen der ZDA vorzunehmen. Die Aufsichtsstelle hat eine zusätzliche Prüfung jedenfalls 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 ZDA.

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

Hinweis auf die Notifikation

§ 15. (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 2006/96/EG des Rates notifiziert (Notifikationsnummer 2007/534/A).

Inkrafttreten

§ 16. Diese Verordnung samt Anhang tritt mit Kundmachung in Kraft. Gleichzeitig tritt die Verordnung des Bundeskanzlers über elektronische Signaturen, BGBl. II Nr. 30/2000, in der Fassung der Verordnung BGBl. II Nr. 527/2004, samt Anhang außer Kraft.

Gusenbauer

ANHANG

Algorithmen und Parameter für qualifizierte 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 (in der Regel 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

3. Zulässige Signatursuiten

Algorithmen und Parameter für qualifizierte 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 Schlüssel-erzeugung	Padding-Verfahren	Kryptographische Hashfunktion
001	rsa	MinModLen = 1024	rsagen1	siehe Tabelle 3	siehe Tabelle 2
002	dsa	pMinLen = 1024 qMinlen = 160	dsagen1	-	siehe Tabelle 2
003	ecdsa-Fp	qMinLen = 160 r0Min = 10^4 MinClass = 200	ecgen1	-	siehe Tabelle 2
004	ecdsa-F2m	qMinlen = 160 r0Min = 10^4 MinClass = 200	ecgen2	-	siehe Tabelle 2
005	ecgdsa-Fp	qMinLen = 160 r0Min = 10^4 MinClass = 200	ecgen1	-	siehe Tabelle 2
006	ecgdsa-F2m	qMinLen = 160 r0Min = 10^4 MinClass = 200	ecgen2	-	siehe Tabelle 2

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	Objektidentifikator OID	Bezeichnung in diesem Anhang
rsa	{ joint-iso-ccitt(2) ds(5) module(1) algorithm(8) encryptionAlgorithm(1) 1 }	rsa

Objekt-Kurzbezeichnung	Objektidentifikator OID	Bezeichnung in diesem Anhang
rsaEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }	rsa
id-dsa	{ iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1 }	dsa
id-ecPublicKey	{ iso(1) member-body(2) us(840) 10045 2 1 }	ecdsa
ecgPublicKey	{ iso(1) identified-organization(3) teletrust(36) algorithm(3) signatureAlgorithm(3) ecSign(2) ecgDsaStd(5) ecgKeyType(2) 1 }	ecgdsa
id-sha1	{ iso(1) identifiedOrganization(3) oIW(14) oIWSecSig(3) oIWSecAlgorithm(2) 26 }	sha1
ripemd160	{ iso(1) identifiedOrganization(3) teletrust(36) algorithm(3) hashAlgorithm(2) ripemd160(1) }	ripemd160
id-sha224	{ joint-iso-itu-t(2)country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) sha224(4) }	sha224
id-sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 }	sha256
id-sha384	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 2 }	sha384
id-sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }	sha512
whirlpool	{ iso(1) standard(0) encryption-algorithms(10118) part3(3) algorithm(0) whirlpool(55) }	whirlpool
sha-1WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }	rsa; emsa-pks1; sha1
sha224WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 14 }	rsa; emsa-pks1; sha224
sha256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }	rsa; emsa-pks1; sha256
sha384WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12 }	rsa; emsa-pks1; sha384
sha512WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13 }	rsa; emsa-pks1; sha512
id-RSASSA-PSS mit mgf1SHA1Identifier, mgf1SHA224Identifier, mgf1SHA256Identifier; mgf1SHA384Identifier oder mgf1SHA512Identifier	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10 }	rsa; emsa-pss; sha1, sha224, sha256, sha384, sha512
rsaSignatureWithripemd160	{iso(1) identified-organization(3) teletrust(36) algorithm(3) signatureAlgorithm(3) rsaSignature(1) rsaSignatureWithripemd160(2)}	rsa; ripemd160
id-dsa-with-sha1	{ iso(1) member-body(2) us(840) x9-57 (10040) x9cm(4) 3 }	dsa; sha1
id-dsa-with-sha224	{ joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) csor(3) algorithms(4) id-dsa-with-sha2(3) 1 }	dsa; sha224
id-dsa-with-sha256	{ joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) csor(3) algorithms(4) id-dsa-with-sha2(3) 2 }	dsa; sha256
ecdsa-with-SHA1	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) sha1(1) }	ecdsa; sha1
ecdsa-with-Recommended	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) recommended(2) }	ecdsa; sha1, sha224, sha256, sha384, sha512

Objekt-Kurzbezeichnung	Objektidentifikator OID	Bezeichnung in diesem Anhang
ecdsa-with-Sha224	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) 1 }	ecdsa; sha224
ecdsa-with-Sha256	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) 2 }	ecdsa; sha256
ecdsa-with-Sha384	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) 3 }	ecdsa; sha384
ecdsa-with-Sha512	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) specified(3) 4 }	ecdsa; sha512
ecdsa-plain-RIPEMD160	{itu-t(0) identified-organization(4) etsi(0) reserved(127) etsi-identified-organization(0) bsi-de(7) algorithms (1) id-ecc(1) signatures(4) ecdsa-signatures(1) 6 }	ecdsa; ripemd160
ecgSignatureWithripemd160	{ iso(1) identified-organization(3) teletrust(36) algorithm(3) signatureAlgorithm(3) ecSign(2) ecgDsaStd(5) ecgSignature(4) 1 }	ecgdsa; ripemd160
ecgSignatureWithsha1	{ iso(1) identified-organization(3) teletrust(36) algorithm(3) signatureAlgorithm(3) ecSign(2) ecgDsaStd(5) ecgSignature(4) 2 }	ecgdsa; sha1
ecgSignatureWithsha224	{ iso(1) identified-organization(3) teletrust(36) algorithm(3) signatureAlgorithm(3) ecSign(2) ecgDsaStd(5) ecgSignature(4) 3 }	ecgdsa; sha224
ecgSignatureWithsha256	{ iso(1) identified-organization(3) teletrust(36) algorithm(3) signatureAlgorithm(3) ecSign(2) ecgDsaStd(5) ecgSignature(4) 4 }	ecgdsa; sha256
ecgSignatureWithsha384	{ iso(1) identified-organization(3) teletrust(36) algorithm(3) signatureAlgorithm(3) ecSign(2) ecgDsaStd(5) ecgSignature(4) 5 }	ecgdsa; sha384
ecgSignatureWithsha512	{ iso(1) identified-organization(3) teletrust(36) algorithm(3) signatureAlgorithm(3) ecSign(2) ecgDsaStd(5) ecgSignature(4) 6 }	ecgdsa; sha512

4. Zulässige kryptographische Hashverfahren

Für qualifizierte 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
2.03	sha224
2.04	sha256
2.05	sha384
2.06	sha512
2.07	whirlpool

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	trueran oder pseuran	min. 64 bit
3.03	emsa-pkcs1-v2_1	-	-
3.04	iso9796ds2	trueran oder pseuran	min. 64 bit
3.05	iso9796-din-rn	trueran oder pseuran	min. 64 bit

Kennzahl des Padding-Verfahrens	Kurzbezeichnung des Füllverfahrens	Erzeugung der Zufallszahlen	Parameter des Zufallszahlengenerators
3.06	iso9796ds3	-	-

6. Zulässige Signaturalgorithmen

Tabelle 4 - Liste der zulässigen Signaturalgorithmen

Kennzahl des Signatur-algorithmus	Kurzbezeichnung des Signaturalgorithmus	Parameter des Signatur-algorithmus	Algorithmus zur Schlüssel- und Parameter-erzeugung
1.01	rsa	MinModLen = 1024	rsagen1
1.02	dsa	pMinLen = 1024 qMinLen = 160	dsagen1
1.03	ecdsa-Fp	qMinLen = 160 r0Min = 10^4 MinClass = 200	ecgen1
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 $\geq$ 80 or SeedLen $\geq$ 80
4.02	dsagen1	dsa	trueran oder pseuran	EntropyBits $\geq$ 80 or SeedLen $\geq$ 80
4.03	ecgen1	ecdsa-Fp, ecgdsa-Fp	trueran oder pseuran	EntropyBits $\geq$ 80 or SeedLen $\geq$ 80
4.04	ecgen2	ecdsa-F2m, ecgdsa-F2m	trueran oder pseuran	EntropyBits $\geq$ 80 or SeedLen $\geq$ 80

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, zB 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 $\geq$ **qMinLen** $\geq$ **160** teilbar ist.

7.2.2 DSA-Varianten mit elliptischen Kurven basierend auf einer Gruppe E(F2m)

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 F2m, 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 F2m muss so gewählt werden, dass ihre Ordnung durch eine Primzahl q der Länge $\geq$ **qMinLen** $\geq$ **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 $E(F2m)$

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-zahlengenerators	Kurzbezeichnung des Zufallszahlengenerators	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 $n = 100$ in Folge erzeugte Signaturerstellungsdaten gleichermaßen verwendet werden, als ob sie von einem Generator trueran erzeugt worden wären. Für die Massenproduktion (durch den 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.“