Liechtensteinisches Landesgesetzblatt
Jahrgang 2004 Nr. 130 ausgegeben am 8. Juni 2004

Verordnung
vom 1. Juni 2004
über elektronische Signaturen (Signaturverordnung; SigV)

Aufgrund von Art. 27 des Gesetzes vom 18. September 2003 über elektronische Signaturen (Signaturgesetz; SigG), LGBl. 2003 Nr. 215[1], verordnet die Regierung:

I. Finanzielle und persönliche Anforderungen an Zertifizierungsdiensteanbieter für qualifizierte Zertifikate

Art. 1

Finanzielle Ausstattung eines Zertifizierungsdiensteanbieters

1) Die für die Ausübung der Tätigkeit als Zertifizierungsdiensteanbieter regelmässig zur Verfügung stehenden Finanzmittel sind der Aufsichtsstelle mit Anzeige der Aufnahme der Tätigkeit nach Art. 6 Abs. 2 des Gesetzes bekannt zu geben. Ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, hat ein Mindestkapital in Höhe von 500 000 Franken aufzuweisen. Dieses Mindestkapital muss in Form von Eigenmitteln (Nennkapital bzw. eingezahltes Kapital, Kapitalrücklagen, Gewinnrücklagen, Bilanzgewinn, unversteuerte Rücklagen) oder gleichwertigen sofort liquiden Finanzmitteln vorliegen.

2) Ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, hat zudem der Aufsichtsstelle mit Anzeige der Aufnahme der Tätig-

keit nach Art. 6 Abs. 2 des Gesetzes den Abschluss einer Haftpflichtversicherung mit einer Mindestversicherungssumme von 1 500 000 Franken nachzuweisen, die zumindest drei Versicherungsfälle im Jahr deckt. Die Vereinbarung eines Selbstbehalts bis zu einem Prozent der Mindestversicherungssumme ist zulässig. Von der Leistungspflicht der Versicherung können nur Ersatzansprüche aus einer vorsätzlich begangenen Pflichtverletzung des Zertifizierungsdiensteanbieters oder der für ihn handelnden Personen, für die er einzustehen hat, ausgeschlossen werden.

Art. 2

Zuverlässigkeit eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt, und seines Personals

1) Ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, darf im Rahmen der erbrachten Signatur- und Zertifizierungsdienste nicht Personen beschäftigen oder sonst einsetzen, 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 getilgt sind, bleiben ausser Betracht. Die Zuverlässigkeit des Personals ist vom Zertifizierungsdiensteanbieter in Abständen von zumindest zwei Jahren zu überprüfen.

2) Soweit anwendbar, gelten die Anforderungen des Abs. 1 auch für den Zertifizierungsdiensteanbieter selbst.

Art. 3

Fachkenntnisse des Personals eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt

1) Das technische Personal eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt, muss über ausreichende Fachkenntnisse in folgenden Bereichen verfügen:

a) allgemeine EDV-Ausbildung;

b) Sicherheitstechnologie, Kryptographie, elektronische Signatur und Public Key Infrastructure;

c) technische Normen, insbesondere Evaluierungsnormen; sowie

d) Hard- und Software.

2) Die Fachkenntnisse können insbesondere durch Absolvierung einer technischen Fachhochschule oder eines einschlägigen Studiums erworben werden. Diese Ausbildung des technischen Personals in den einzelnen Bereichen muss mindestens ein Jahr gedauert haben. Sie kann durch eine fachlich einschlägige Tätigkeit in der Dauer von jeweils mindestens drei Jahren ersetzt werden.

3) Auf Verlangen der Aufsichtsstelle muss der Zertifizierungsdiensteanbieter darlegen, durch welche einschlägige Ausbildung an anerkannten Bildungseinrichtungen oder durch welche einschlägigen fachlichen Tätigkeiten die Fachkenntnisse des Personals gegeben sind.

II. Technische und organisatorische Sicherheitsanforderungen

Art. 4

Signaturerstellungsdaten, Systeme, Produkte und Verfahren der Aufsichtsstelle

1) Die Signaturerstellungsdaten sowie deren Parameter (insbesondere Schlüssellängen, Zufallselemente) und Verfahren (insbesondere Algorithmen, Hashverfahren) der Aufsichtsstelle müssen den Anforderungen des Kapitels "Algorithmen und Parameter für sichere elektronische Signaturen" des ETSI-Algorithmenpapiers (Art. 8 Abs. 5) entsprechen. Diesen Signaturerstellungsverfahren sind andere Verfahren gleichgestellt, die zumindest die gleiche Sicherheit aufweisen und von einer Bestätigungsstelle als solche anerkannt und veröffentlicht wurden.

2) Diese Signaturerstellungsdaten müssen in einer Signaturerstellungseinheit erzeugt werden, die den Sicherheitsanforderungen des Art. 8 Abs. 3 entspricht. Sie dürfen ausserhalb dieser Signaturerstellungseinheit nicht zur Verfügung stehen. Das Erzeugungssystem muss isoliert, ausschliesslich zu diesem Zweck bestimmt und angemessen vor Eingriffen und Störungen geschützt sein. Im Übrigen gelten die Anforderungen für fortgeschrittene elektronische Signaturen.

3) Die Aufsichtsstelle hat ein Hauptsystem und ein technisch gleichwertiges Zweitsystem mit jeweils eigenen Signaturerstellungsdaten einzusetzen und für alle im Hauptsystem geführten Zertifikate für Zertifizierungsdiensteanbieter korrespondierende Zertifikate im Zweitsystem zu führen. Diese Systeme müssen isoliert, ausschliesslich zu diesem Zweck bestimmt und

angemessen vor Eingriffen und Störungen geschützt sein. Die Signaturprüfdaten des Zweitsystems sind mit den Signaturerstellungsdaten des Hauptsystems elektronisch zu signieren. Das Zweitsystem ist unter Verschluss zu halten. Die Signaturprüfdaten des Zweitsystems dürfen nur bei einem Ausfall des Hauptsystems veröffentlicht werden.

Art. 5

Signaturerstellungsdaten, Systeme, Produkte und Verfahren eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt

1) Die Signaturerstellungsdaten sowie deren Parameter (insbesondere Schlüssellängen, Zufallselemente) und Verfahren (insbesondere Algorithmen, Hashverfahren) eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt, müssen den Anforderungen des Kapitels "Algorithmen und Parameter für sichere elektronische Signaturen" des ETSI-Algorithmenpapiers (Art. 8 Abs. 5) entsprechen. Diesen Signaturerstellungsverfahren sind andere Verfahren gleichgestellt, die zumindest die gleiche Sicherheit aufweisen und von einer Bestätigungsstelle als solche anerkannt und veröffentlicht wurden.

2) Diese Signaturerstellungsdaten müssen in einer Signaturerstellungseinheit erzeugt werden, die den Sicherheitsanforderungen des Art. 8 Abs. 3 entspricht. Sie dürfen ausserhalb dieser Signaturerstellungseinheit nicht zur Verfügung stehen. Im Übrigen gelten die Anforderungen für fortgeschrittene elektronische Signaturen.

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

4) Ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, muss in der Lage sein, sichere elektronische Signaturen, die auf seinen qualifizierten Zertifikaten beruhen, sicher zu prüfen. Die Verfahren und

Algorithmen zur Signaturprüfung bilden mit den Verfahren und Algorithmen zur Signaturerstellung eine logische Einheit und sind gemeinsam zu dokumentieren.

Art. 6

Schutz der Signaturprodukte bei einem Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt

Ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, hat geeignete Vorkehrungen zu treffen, die die Signaturerstellungsdaten sowie die zur Erzeugung der Zertifikate und die zum Abrufbarhalten der Verzeichnis- und Widerrufsdienste verwendeten Signaturprodukte vor Kompromittierung und unbefugtem Zugriff schützen. Unbefugte Zugriffe müssen erkennbar sein.

Art. 7

Signaturerstellungsdaten, Produkte und Verfahren für sichere elektronische Signaturen

1) Die Signaturerstellungsdaten sowie deren Parameter (insbesondere Schlüssellängen, Zufallselemente) und Verfahren (insbesondere Algorithmen, Hashverfahren) für sichere elektronische Signaturen müssen den Anforderungen des Kapitels "Algorithmen und Parameter für sichere elektronische Signaturen" des ETSI-Algorithmenpapiers (Art. 8 Abs. 5) entsprechen. Diesen Signaturerstellungsverfahren sind andere Verfahren gleichgestellt, die zumindest die gleiche Sicherheit aufweisen und von einer Bestätigungsstelle als solche anerkannt und veröffentlicht wurden.

2) Für die Erzeugung und Speicherung von Signaturerstellungsdaten für sichere elektronische Signaturen sowie für die Erstellung sicherer elektronischer Signaturen müssen Signaturprodukte eingesetzt werden, die den Sicherheitsanforderungen des Art. 8 Abs. 1 entsprechen und nach Art. 8 Abs. 2 bescheinigt sind (sichere Signaturerstellungseinheiten).

3) Die Signaturerstellungsdaten für sichere elektronische Signaturen können auf mehrere Signaturerstellungseinheiten verteilt werden. In einem solchen Fall müssen die Sicherheitsanforderungen durch die Gesamtheit der Signaturerstellungseinheiten erfüllt werden.

4) Die von den Signatoren für die Erstellung sicherer elektronischer Signaturen verwendeten Signaturprodukte müssen die vollständige Anzeige der zu signierenden Daten ermöglichen. Die Spezifikation der Formate für

die zu signierenden Daten muss allgemein verfügbar sein und sicherstellen, dass die elektronisch signierten Daten sowohl bei der Signaturerstellung als auch der Signaturprüfung in gleicher Weise zweifelsfrei feststellbar sind. Können in einem Format dynamische Veränderungen codiert werden, so dürfen die betreffenden Codierungen nicht verwendet werden.

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

Art. 8

Sicherheitsanforderungen an Signaturprodukte, Prüfung und Bescheinigung

1) Zur Prüfung von Signaturprodukten für die Erzeugung und Speicherung von Signaturerstellungsdaten für sichere elektronische Signaturen sowie für die Erstellung sicherer elektronischer Signaturen (sicheren Signaturerstellungseinheiten) sind Schutzprofile (Protection Profiles) anzuwenden, die als Referenznummern für sichere Signaturerstellungseinheiten (Secure Signature-Creation Devices; SSCD) im Amtsblatt der Europäischen Union nach Art. 3 Abs. 5 der Signaturrichtlinie veröffentlicht wurden. Im Übrigen sind entsprechende geeignete und von einer Bestätigungsstelle anerkannte Schutzprofile der Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria for Information Security Evaluation; ISO/IEC 15408) oder Sicherheitsvor-

gaben (Security Targets) nach den Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (Information Technology Security Evaluation Criteria; ITSEC) bzw. gleichwertiger technischer Standards anwendbar.

2) Die Erfüllung der Sicherheitsanforderungen nach Abs. 1 ist von einer Bestätigungsstelle nach Art. 18 Abs. 3 des Gesetzes zu bescheinigen. In dieser Bescheinigung ist anzugeben, für welche Anwendungen, unter welchen Bedingungen und bis zu welchem Zeitpunkt sie gilt. Ausfertigungen des Prüfberichts und der Bescheinigung sind der Aufsichtsstelle zu übermitteln.

3) Die Sicherheitsanforderungen für Systeme, Produkte und Verfahren der Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, sowie der Aufsichtsstelle richten sich nach den Schutzprofilen (Protection Profiles), die als Referenznummern für vertrauenswürdige Systeme und Produkte der Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, im Amtsblatt der Europäischen Union nach Art. 3 Abs. 5 der Signaturrichtlinie veröffentlicht wurden. Im Übrigen findet Abs.1 Satz 2 Anwendung.

4) Wenn Signaturprodukte in einer kontrollierten Umgebung eingesetzt werden, können Sicherheitsanforderungen, die nach Abs. 1 oder 3 technisch sichergestellt werden müssen, auch organisatorisch unter Einsatz qualifizierten und vertrauenswürdigen Personals oder technisch-organisatorisch unter Einsatz geeigneter Zugriffs- und Zutrittskontrollmassnahmen erfüllt werden.

5) Beim ETSI-Algorithmenpapier handelt es sich um den vom European Telecommunications Standards Institute veröffentlichten Sonderbericht (ETSI SR 002 176 v 1.1.1) vom März 2003. Dieser Sonderbericht kann beim Amt für Kommunikation eingesehen und bezogen werden und ist zudem im Internet abrufbar.[2]

Art. 9

Nachsignieren

Der Zeitraum, nach dem eine neue sichere elektronische Signatur wegen drohender Verringerung des Sicherheitswerts zur Aufrechterhaltung der technischen Sicherheit anzubringen ist, muss im Sicherheits- und Zertifizierungskonzept des Zertifizierungsdiensteanbieters angegeben werden. Dieses muss ein Nachsignieren jedenfalls vor Ablauf der im Kapitel "Algorithmen und Parameter für sichere elektronische Signaturen" des ETSI-

Algorithmenpapiers oder der anderen Signaturerstellungsverfahren zugrunde liegenden technischen Normen für die Sicherheit der bereitgestellten oder empfohlenen Signaturerstellungsverfahren angegebenen Perioden vorsehen. Beim Anbringen einer neuen elektronischen Signatur muss ein sicherer Zeitstempel (Art. 14) verwendet werden.

III. Signatur- und Zertifizierungsdienste für qualifizierte Zertifikate

Art. 10

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

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

2) Die technischen Einrichtungen eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt, sind so zu gestalten, dass deren Funktionen und Anwendungen, die zu den erbrachten 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 (insbesondere 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) Werden die Signaturerstellungsdaten beim Zertifizierungsdiensteanbieter oder bei der Produktion der Signaturerstellungseinheit erzeugt, so dürfen diese 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 zu vergewissern, dass die Signaturerstellungsdaten des

Signators und die Signaturprüfdaten des entsprechenden Zertifikats in komplementärer Weise anwendbar sind.

5) Ein Zertifizierungsdiensteanbieter hat den Signator vor der erstmaligen Verwendung der Signaturerstellungsdaten über alle sicherheitsrelevanten Massnahmen bei deren Anwendung (insbesondere erforderliche Massnahmen zur Auslösung der Signaturfunktion, Sicherheit der Autorisierungscodes, Prüfung des Ausschlusses fremder Verwendung, Inanspruchnahme der Verzeichnis- und Widerrufsdienste, Möglichkeit der Darstellung zu signierender Daten, Verwendung geeigneter Formate) schriftlich oder unter Verwendung eines dauerhaften Kommunikationsmittels in elektronischer Form klar und allgemein verständlich zu unterrichten.

Art. 11

Antrag auf Ausstellung eines qualifizierten Zertifikats

1) Der Antrag auf Ausstellung eines qualifizierten Zertifikats muss vom Zertifikatswerber eigenhändig unterschrieben sein. Vom vorgelegten Lichtbildausweis ist eine Ablichtung herzustellen, die mit dem Antrag in elektronischer Form zu dokumentieren ist. Ist ein solcher Antrag mit der sicheren elektronischen Signatur des Zertifikatswerbers versehen, so kann von der erneuten Feststellung seiner Identität abgesehen werden.

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

a) Namen, Datum und Ort der Geburt sowie Wohnsitz des Zertifikatswerbers, Datum der Ausstellung und Nummer des vorgelegten Lichtbildausweises sowie die Behörde, die diesen ausgestellt hat;

b) gegebenenfalls Angaben darüber, ob das Zertifikat eine Einschränkung des Anwendungsbereichs oder eine Begrenzung des Transaktionswerts enthalten soll;

c) gegebenenfalls Angaben darüber, ob eine Vertretungsmacht für einen Dritten, andere rechtlich erhebliche Eigenschaften des Zertifikatswerbers, wie etwa eine berufsrechtliche oder sonstige Zulassung, oder weitere rechtlich erhebliche Umstände 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 Kommunikationsmittels in elektronischer Form zu unterrichten und auf die Möglichkeit des Widerrufs nach Art. 9 Abs. 1 Bst. a des Gesetzes hinzuweisen. Eine andere rechtlich erhebliche Eigenschaft, wie etwa eine berufsrechtliche oder sonstige Zulassung, oder ein rechtlich erheblicher Umstand muss vor der Aufnahme in ein qualifiziertes Zertifikat ebenfalls zuverlässig nachgewiesen sein. Untersteht der Signator im Hinblick auf eine eingetragene berufsrechtliche Zulassung einer öffentlich-rechtlichen Berufsaufsicht, so ist die Einrichtung, die die Berufsaufsicht ausübt, über den Inhalt des qualifizierten Zertifikats schriftlich oder unter Verwendung eines dauerhaften Kommunikationsmittels in elektronischer Form zu unterrichten.

Art. 12

Qualifizierte Zertifikate

1) Stellt ein Zertifizierungsdiensteanbieter neben qualifizierten auch andere Zertifikate aus, so muss er zum Signieren der qualifizierten Zertifikate gesonderte Signaturerstellungsdaten verwenden.

2) Die Formate für qualifizierte Zertifikate sind formal und vollständig so zu spezifizieren, dass deren automatisierte Prüfung möglich ist.

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

4) Bis zum Ablauf der Gültigkeit eines qualifizierten Zertifikats ist es zulässig, mit Ausnahme der Gültigkeitsdauer dieselben Inhalte samt denselben Signaturprüfdaten neu zu zertifizieren und auf diese Weise ein neues Zertifikat auszustellen. In allen anderen Fällen bewirken qualifizierte Zertifikate mit den selben Signaturprüfdaten und unterschiedlichen Inhalten eine Kompromittierung der betroffenen Zertifikate, die zu deren Widerruf führen muss. Der Widerruf ist vom Signator zu verlangen (Art. 9 Abs. 1 Bst. a des Gesetzes) oder vom Zertifizierungsdiensteanbieter selbst vorzunehmen (Art. 9 Abs. 1 Bst. f des Gesetzes), sobald er von der Kompromittierung Kenntnis erlangt.

5) 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 qualifizierten Zertifikats des Signators führen muss. Abs. 4 letzter Satz gilt sinngemäss.

6) Ein Zertifizierungsdiensteanbieter ist berechtigt, mit Zustimmung eines anderen Zertifizierungsdiensteanbieters dessen Zertifikat oder die von

diesem ausgestellten qualifizierten Zertifikate zu zertifizieren. Die Zertifikate, die er auf diese Weise ausstellt, dürfen keine Modifikationen aufweisen; er hat auch für die Erbringung der Verzeichnis- und Widerrufsdienste Sorge zu tragen und gegebenenfalls die Widerrufe des anderen Zertifizierungsdiensteanbieters unmittelbar nachzuvollziehen.

7) Ein qualifiziertes Attributzertifikat ist ein qualifiziertes Zertifikat im Sinne von Art. 2 Abs. 1 Bst. l des Gesetzes, das mindestens folgende Angaben enthalten muss:

a) den Hinweis darauf, dass es sich um ein qualifiziertes Zertifikat handelt;

b) den unverwechselbaren Namen des Zertifizierungsdiensteanbieters und den Staat seiner Niederlassung;

c) die eindeutige Kennung des Attributzertifikats; und

d) ein oder mehrere Attribute im Sinne von Art. 5 Abs. 1 Bst. d des Gesetzes.

Zudem muss ein qualifiziertes Attributzertifikat eine eindeutige Referenz auf das zugrunde liegende qualifizierte Zertifikat (Hauptzertifikat) enthalten. Die Gültigkeit eines qualifizierten Attributzertifikats endet spätestens mit der Gültigkeit des qualifizierten Zertifikats, auf das es Bezug nimmt. Ein qualifiziertes Attributszertifikat kann auch gesondert widerrufen werden.

Art. 13

Verzeichnis- und Widerrufsdienste für qualifizierte Zertifikate

1) Die Verzeichnis- und Widerrufsdienste können in unterschiedlichen Formaten geführt werden. Der Zertifizierungsdiensteanbieter hat sicherzustellen, dass die Formate der Widerrufsdienste für deren Weiterführung durch die Aufsichtsstelle geeignet sind. Werden die Verzeichnis- und Widerrufsdienste von einem anderen Zertifizierungsdiensteanbieter übernommen, so müssen sie weiterhin in den selben Formaten geführt werden. Die Widerrufsdienste müssen jedenfalls die Feststellung zulassen, ob das qualifizierte Zertifikat zum Zeitpunkt der Erstellung der darauf beruhenden elektronischen Signatur gesperrt oder 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 Authentifizie-

rungsverfahren vorgesehen werden. Der Widerruf eines qualifizierten Zertifikats muss jedenfalls auch in Papierform möglich sein.

3) Die zeitliche Verfügbarkeit der Verzeichnisdienste muss im Sicherheits- und Zertifizierungskonzept angegeben werden. Die Verzeichnisdienste müssen zumindest während der Geschäftszeiten (jedenfalls an Werktagen von 9 bis 17 Uhr und an Samstagen von 9 bis 12 Uhr) 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.

4) Ein Zertifizierungsdiensteanbieter hat die Verzeichnis- und Widerrufsdienste zumindest bis zum Zeitpunkt des erforderlichen Nachsignierens (Art. 9) zu führen. Nach Ablauf dieser Frist hat der Zertifizierungsdiensteanbieter eine Überprüfung der qualifizierten Zertifikate bis zum Ablauf der in Art. 16 Abs. 2 genannten Frist im Einzelfall zu ermöglichen. Das Gleiche gilt für die Weiterführung der Widerrufsdienste durch die Aufsichtsstelle im Fall der Einstellung oder Untersagung der Tätigkeit eines Zertifizierungsdiensteanbieters.

5) Die Aktualisierung der Widerrufsdienste muss spätestens innerhalb von drei Stunden ab Bekanntwerden des Widerrufsgrundes erfolgen. Der Zertifizierungsdiensteanbieter kann statt dessen auch vorsehen, dass ein Verlangen auf Widerruf eines qualifizierten Zertifikats jederzeit automatisiert entgegengenommen wird und unverzüglich die Sperre auslöst. Von dieser Möglichkeit kann insbesondere auch ausserhalb der Geschäftszeiten Gebrauch gemacht werden.

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

Art. 14

Sichere Zeitstempeldienste und Zeitstempelgeräte

1) Für die Bereitstellung sicherer Zeitstempeldienste dürfen ausschliesslich qualifizierte und nur für diesen Zweck ausgestellte Zertifikate verwendet werden. Dieser Verwendungszweck ist im Zertifikat anzugeben.

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 sowie die Sicherheitsvorkehrungen zur automatisierten Auslösung der Zeitstempelfunktion müssen im Sicherheits- und Zertifizierungskonzept des Zertifizierungsdiensteanbieters, der solche Dienste bereitstellt, angegeben werden.

4) Geräte für sichere Zeitstempel, die beim Anwender verwendet werden, müssen die Anforderungen der Abs. 1 und 2 sowie Art. 10 des Gesetzes erfüllen.

Art. 15

Sicherheits- und Zertifizierungskonzept für qualifizierte Zertifikate

1) Das Sicherheits- und Zertifizierungskonzept eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt, hat insbesondere folgende Angaben zu enthalten:

a) Namen des Zertifizierungsdiensteanbieters;

b) Adresse des Zertifizierungsdiensteanbieters und Staat seiner Niederlassung;

c) Art, Anwendungsbereich und Erbringung der Signatur- und Zertifizierungsdienste;

d) Verfahren zur Antragstellung;

e) gegebenenfalls Art und Weise der Aufnahme von Pseudonymen sowie von Angaben über eine Vertretungsmacht für einen Dritten oder andere rechtlich erhebliche Eigenschaften oder Umstände des Signators in das Zertifikat;

f) Geschäftszeiten;

g) Erzeugung der Signaturerstellungsdaten des Zertifizierungsdiensteanbieters;

h) Format der Signaturerstellungsdaten des Zertifizierungsdiensteanbieters;

i) Signaturprüfdaten, gegebenenfalls das Zertifikat des Zertifizierungsdiensteanbieters;

k) Erzeugung der Signaturerstellungsdaten der Signatoren;

l) Format der Signaturerstellungsdaten der Signatoren;

m) bereitgestellte und empfohlene Verfahren zur Erstellung der elektronischen Signaturen (Hashverfahren und Verfahren zur Verschlüsselung des Hashwerts);

n) Liste der verwendeten, bereitgestellten und empfohlenen Signaturprodukte;

o) Sicherheit der Autorisierungscodes;

p) anwendbare Formate für zu signierende Daten und gegebenenfalls Methoden zur Verhinderung dynamischer Veränderungen;

q) Formate und Gültigkeitsdauer der Zertifikate;

r) technische Normen, Zugangsmodalitäten sowie Aktualisierungs- und Verfügbarkeitszeitraum der geführten Verzeichnis- und Widerrufsdienste einschliesslich des Zeitraums der Sperre;

s) nachvollziehbare und allgemein verständliche Methode zur sicheren Signaturprüfung;

t) Format der Dokumentation von Sicherheitsvorkehrungen, Störfällen und besonderen Betriebssituationen;

u) Zeitraum und Verfahren des Nachsignierens;

v) Schutz der technischen Komponenten vor unbefugtem Zugriff;

w) Schutz der Einrichtungen des Zertifizierungsdiensteanbieters vor unbefugtem Zutritt.

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

a) Namen des Zertifizierungsdiensteanbieters;

b) Adresse des Zertifizierungsdiensteanbieters und Staat seiner Niederlassung;

c) Art, Anwendungsbereich und Erbringung der Signatur- und Zertifizierungsdienste;

d) Signaturprüfdaten des Zeitstempeldienstes;

e) eingesetzte Verfahren zur Erstellung der elektronischen Signaturen (Hashverfahren und Verfahren zur Verschlüsselung des Hashwerts);

f) Sicherheit der Autorisierungscodes;

g) Formate des Zeitstempels;

h) Verfügbarkeitszeitraum der bereitgestellten Zeitstempeldienste;

i) nachvollziehbare und allgemein verständliche Methode zur sicheren Signaturprüfung;

k) Format der Dokumentation von Sicherheitsvorkehrungen, Störfällen und besonderen Betriebssituationen;

l) Schutz der technischen Komponenten vor unbefugtem Zugriff;

m) Schutz der Einrichtungen des Zertifizierungsdiensteanbieters vor unbefugtem Zutritt.

3) Das Sicherheits- und Zertifizierungskonzept ist der Aufsichtsstelle in elektronischer Form im Format XML mit Darstellungsfunktion, PDF, Ascii oder Postscript vorzulegen. Es muss zumindest mit der fortgeschrittenen elektronischen Signatur des Zertifizierungsdiensteanbieters versehen sein. Dieser hat das Sicherheits- und Zertifizierungskonzept sowie eine Zusammenfassung davon klar und allgemein verständlich im Format XML mit Darstellungsfunktion, PDF, Ascii oder Postscript elektronisch jederzeit allgemein abrufbar zu halten.

Art. 16

Dokumentation

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

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

IV. Aufsicht und Akkreditierung; Bestätigungsstellen

Art. 17

Aufsicht

1) Die Anzeige der Aufnahme der Tätigkeit eines Zertifizierungsdiensteanbieters nach Art. 6 Abs. 2 des Gesetzes 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 er die Anzeige zumindest mit seiner fortgeschrittenen elektronischen Signatur zu versehen. Die Aufsichtsstelle hat sich zu vergewissern, dass die Signaturerstellungsdaten des Zertifizierungsdiensteanbieters und die Signaturprüfdaten des entsprechenden Zertifikats in komplementärer Weise anwendbar sind.

2) Der Anzeige für die Ausstellung qualifizierter Zertifikate oder die Bereitstellung sicherer elektronischer Signaturverfahren sind insbesondere anzuschliessen:

a) Sicherheits- und Zertifizierungskonzept;

b) Darstellung der spezifischen sicherheitsrelevanten Bedrohungen und Risiken beim Zertifizierungsdiensteanbieter;

c) Nachweis der Finanzmittel sowie der erforderlichen Haftpflichtversicherung; und

d) Nachweis der Fachkenntnisse 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.

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 Webseite führen, in der ihre Adresse, ihre Signaturprüfdaten sowie die Formate der bei ihr geführten Verzeichnisse und die Zugangsmodalitäten zu diesen angegeben sind.

Art. 18

Freiwillige Akkreditierung

1) Im Fall einer freiwilligen Akkreditierung nach Art. 17 des Gesetzes tritt der Antrag auf Akkreditierung an die Stelle der Anzeige der Aufnahme der Tätigkeit des Zertifizierungsdiensteanbieters.

2) Die Kennzeichnung akkreditierter Zertifizierungsdiensteanbieter hat durch Darstellung des Staatswappens mit dem darunter angebrachten Schriftzug "Akkreditierter Zertifizierungsdiensteanbieter" zu erfolgen.

Art. 19

Bestätigungsstellen

Für die Eignung einer Bestätigungsstelle sind neben den Anforderungen des Art. 19 Abs. 2 des Gesetzes die in der Entscheidung der Europäischen Kommission 2000/709/EG vom 6. November 2000 über die Mindestkriterien bei der Benennung solcher Stellen (EWR-Rechtssammlung: Anh. XI - 5ga.01) festgelegten Anforderungen massgeblich.

V. Gebühren

Art. 20

Gebühren

1) Für folgende Massnahmen der Aufsichtsstelle sind von den betroffenen Zertifizierungsdiensteanbietern nachstehende Gebühren zu entrichten:

a) Überprüfung eines Zertifizierungsdiensteanbieters bei der Anzeige der Aufnahme seiner Tätigkeit (Art. 6 Abs. 2 des Gesetzes), wenn der Zertifizierungsdiensteanbieter:

   aa) keine qualifizierten Zertifikate ausstellt und keine sicheren elektronischen Signaturverfahren bereitstellt: 150 Franken;

   bb) qualifizierte Zertifikate ausstellt oder sichere elektronische Signaturverfahren bereitstellt: 9 000 Franken;

b) Überprüfung eines Zertifizierungsdiensteanbieters bei der Anzeige eines weiteren Sicherheits- und Zertifizierungskonzepts, wenn der Zertifizierungsdiensteanbieter nach diesem Konzept:

   aa) keine qualifizierten Zertifikate ausstellt und keine sicheren elektronischen Signaturverfahren bereitstellt: 80 Franken;

   bb) qualifizierte Zertifikate ausstellt oder sichere elektronische Signaturverfahren bereitstellt:

      1. bei wesentlichen sicherheitsrelevanten Veränderungen: 6 000 Franken;

      2. ohne wesentliche sicherheitsrelevante Veränderungen: 1 500 Franken;

c) Überprüfung eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt, bei der Anzeige von Veränderungen eines bestehenden Sicherheits- und Zertifizierungskonzepts:

   aa) bei wesentlichen sicherheitsrelevanten Veränderungen: 6 000 Franken;

   bb) ohne wesentliche sicherheitsrelevante Veränderungen: 1 500 Franken;

d) Überprüfung eines Zertifizierungsdiensteanbieters anlässlich seiner beantragten Akkreditierung (Art. 17 Abs. 1 des Gesetzes): 9 000 Franken;

e) Entziehung einer Akkreditierung (Art. 17 Abs. 3 des Gesetzes): 1 500 Franken;

f) regelmässige Überprüfung eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt: 6 000 Franken;

g) zusätzliche Überprüfung eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt, wenn ein nicht nur unerheblicher Verstoss gegen die Bestimmungen des Gesetzes oder dieser Verordnung festgestellt wird: 9 000 Franken;

h) Überprüfung eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt, bei sicherheitsrelevanten Veränderungen des Sicher-

heits- und Zertifizierungskonzepts, die nicht der Aufsichtsstelle angezeigt wurden: 9 000 Franken;

i) Erteilung von Auflagen bei sicherheitsrelevanten Mängeln (Art. 14 Abs. 6 des Gesetzes): 1 500 Franken;

k) Untersagung der Ausübung der Tätigkeit eines Zertifizierungsdiensteanbieters (Art. 14 Abs. 2 bis 4 des Gesetzes): 1 500 Franken;

l) Kontrolle der Einstellung der Tätigkeit eines Zertifizierungsdiensteanbieters (Art. 12 des Gesetzes): 150 Franken;

m) Beurteilung der Gleichwertigkeit von Prüfberichten einer staatlich anerkannten Stelle eines Drittstaats (Art. 18 Abs. 5 des Gesetzes): 9 000 Franken.

2) Für die Führung der Verzeichnisse bei der Aufsichtsstelle sind von den betroffenen Zertifizierungsdiensteanbietern folgende Jahresgebühren zu entrichten:

a) Führung der Zertifikatsverzeichnisse (Art. 13 Abs. 3 und Art. 17 Abs. 3 des Gesetzes), pro Zertifikat eines Zertifizierungsdiensteanbieters und Jahr: 1 000 Franken;

b) Führung des elektronischen Verzeichnisses nach Art. 13 Abs. 4 des Gesetzes, pro Zertifizierungsdiensteanbieter und Jahr: 200 Franken;

c) Weiterführung des Widerrufsdienstes eines Zertifizierungsdiensteanbieters durch die Aufsichtsstelle (Art. 12 Abs. 1 und Art. 14 Abs. 5 des Gesetzes), pro im Widerrufsdienst geführtem Zertifikat und Jahr: 2 Franken.

3) Soweit sich die Aufsichtsstelle im Rahmen der Aufsicht oder der Akkreditierung nach dem Gesetz oder dieser Verordnung einer Bestätigungsstelle oder anderer geeigneter Personen oder Einrichtungen bedient (Art. 13 Abs. 5 des Gesetzes), werden deren Kosten und Auslagen von der Aufsichtsstelle beim betroffenen Zertifizierungsdiensteanbieter als Barauslagen eingehoben.

4) Die Gebühren und Barauslagen werden von der Aufsichtsstelle nach Durchführung der jeweiligen Massnahme mit Verfügung vorgeschrieben. Die Gebühren nach Abs. 2 werden für jedes Kalenderjahr im Vorhinein eingehoben. Erfolgt die Aufnahme eines Zertifikats oder eines Zertifizierungsdiensteanbieters in ein Verzeichnis während eines Kalenderjahres, so ist für dieses Kalenderjahr die nach Monaten anteilige Gebühr zu entrichten. Wird ein Zertifikat oder ein Zertifizierungsdiensteanbieter während eines Kalenderjahres aus einem Verzeichnis entfernt, so gebührt keine Rückzahlung.

VI. Schlussbestimmung

Art. 21

Inkrafttreten

Diese Verordnung tritt am Tage der Kundmachung in Kraft.

Fürstliche Regierung:
gez. *Otmar Hasler*
Fürstlicher Regierungschef

1 *LR 784.11*

2 *http://webapp.etsi.org/action%5CPU/20030401/sr_002176v010101p.pdf.*