

Nachdruck vom 30. 7. 1999

Regierungsvorlage

Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG)

Der Nationalrat hat beschlossen:

1. Abschnitt

Gegenstand und Begriffsbestimmungen

Gegenstand und Anwendungsbereich

§ 1. (1) Dieses Bundesgesetz regelt den rechtlichen Rahmen für die Erstellung und Verwendung elektronischer Signaturen sowie für die Erbringung von Signatur- und Zertifizierungsdiensten.

(2) Dieses Bundesgesetz ist auch anzuwenden in geschlossenen Systemen, sofern deren Teilnehmer dies vereinbart haben, sowie im offenen elektronischen Verkehr mit Gerichten und anderen Behörden, sofern durch Gesetz nicht anderes bestimmt ist.

Begriffsbestimmungen

§ 2. Im Sinn dieses Bundesgesetzes bedeuten

1. elektronische Signatur: elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Authentifizierung, also der Feststellung der Identität des Signators, dienen;
2. Signator: eine natürliche Person, der Signaturerstellungsdaten und die entsprechenden Signaturprüfdaten zugeordnet sind und die entweder im eigenen oder im fremden Namen eine elektronische Signatur erstellt, oder ein Zertifizierungsdiensteanbieter, der Zertifikate für die Erbringung von Zertifizierungsdiensten verwendet;
3. sichere elektronische Signatur: eine elektronische Signatur, die
 - a) ausschließlich dem Signator zugeordnet ist,
 - b) die Identifizierung des Signators ermöglicht,
 - c) mit Mitteln erstellt wird, die der Signator unter seiner alleinigen Kontrolle halten kann,
 - d) mit den Daten, auf die sie sich bezieht, so verknüpft ist, daß jede nachträgliche Veränderung der Daten festgestellt werden kann, sowie
 - e) auf einem qualifizierten Zertifikat beruht und unter Verwendung von technischen Komponenten und Verfahren, die den Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen entsprechen, erstellt wird;
4. Signaturerstellungsdaten: einmalige Daten wie Codes oder private Signaturschlüssel, die vom Signator zur Erstellung einer elektronischen Signatur verwendet werden;
5. Signaturerstellungseinheit: eine konfigurierte Software oder Hardware, die zur Verarbeitung der Signaturerstellungsdaten verwendet wird;
6. Signaturprüfdaten: Daten wie Codes oder öffentliche Signaturschlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden;
7. Signaturprüfeinheit: eine konfigurierte Software oder Hardware, die zur Verarbeitung der Signaturprüfdaten verwendet wird;
8. Zertifikat: eine elektronische Bescheinigung, mit der Signaturprüfdaten einer bestimmten Person zugeordnet werden und deren Identität bestätigt wird;
9. qualifiziertes Zertifikat: ein Zertifikat, das die Angaben des § 5 enthält und von einem den Anforderungen des § 7 entsprechenden Zertifizierungsdiensteanbieter ausgestellt wird;

10. Zertifizierungsdiensteanbieter: eine natürliche oder juristische Person oder eine sonstige rechtsfähige Einrichtung, die Zertifikate ausstellt oder andere Signatur- und Zertifizierungsdienste erbringt;
11. Signatur- und Zertifizierungsdienste: die Bereitstellung von Signaturprodukten und -verfahren, die Ausstellung, Erneuerung und Verwaltung von Zertifikaten, Verzeichnis-, Widerrufs-, Registrierungs- und Zeitstempeldienste sowie Rechner- und Beratungsdienste im Zusammenhang mit elektronischen Signaturen;
12. Zeitstempeldienst: eine elektronisch signierte Bescheinigung eines Zertifizierungsdiensteanbieters, daß bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegt sind.

2. Abschnitt

Rechtserheblichkeit elektronischer Signaturen

Allgemeine Rechtswirkungen

§ 3. (1) Im Rechts- und Geschäftsverkehr können Signaturverfahren mit unterschiedlichen Sicherheitsstufen und unterschiedlichen Zertifikatsklassen verwendet werden.

(2) Die rechtliche Wirksamkeit einer elektronischen Signatur und deren Verwendung als Beweismittel können nicht allein deshalb ausgeschlossen werden, weil die elektronische Signatur nur in elektronischer Form vorliegt, weil sie nicht auf einem qualifizierten Zertifikat oder nicht auf einem von einem akkreditierten Zertifizierungsdiensteanbieter ausgestellten qualifizierten Zertifikat beruht oder weil sie nicht unter Verwendung von technischen Komponenten und Verfahren im Sinn des § 18 erstellt wurde.

Besondere Rechtswirkungen

§ 4. (1) Eine sichere elektronische Signatur erfüllt das rechtliche Erfordernis einer eigenhändigen Unterschrift, insbesondere der Schriftlichkeit im Sinn des § 886 ABGB, sofern durch Gesetz oder Parteienvereinbarung nicht anderes bestimmt ist.

(2) Eine sichere elektronische Signatur entfaltet nicht die Rechtswirkungen der Schriftlichkeit im Sinn des § 886 ABGB bei

1. Rechtsgeschäften des Familien- und Erbrechts, die an die Schriftform oder ein strengeres Formerfordernis gebunden sind,
2. anderen Willenserklärungen oder Rechtsgeschäften, die zu ihrer Wirksamkeit an die Form einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsakts gebunden sind,
3. Willenserklärungen, Rechtsgeschäften oder Eingaben, die zu ihrer Eintragung in das Grundbuch, das Firmenbuch oder ein anderes öffentliches Register einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsakts bedürfen, und
4. einer Bürgschaftserklärung (§ 1346 Abs. 2 ABGB).

(3) Die Bestimmung des § 294 ZPO über die Vermutung der Echtheit des Inhalts einer unterschriebenen Privaturkunde ist auf elektronische Dokumente, die mit einer sicheren elektronischen Signatur versehen sind, anzuwenden.

(4) Die Rechtswirkungen der Abs. 1 und 3 treten nicht ein, wenn nachgewiesen wird, daß die Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen nicht eingehalten oder die zur Einhaltung dieser Sicherheitsanforderungen getroffenen Vorkehrungen kompromittiert wurden.

Qualifizierte Zertifikate

§ 5. (1) Ein qualifiziertes Zertifikat hat zumindest folgende Angaben zu enthalten:

1. den Hinweis darauf, daß es sich um ein qualifiziertes Zertifikat handelt,
2. den unverwechselbaren Namen des Zertifizierungsdiensteanbieters und den Staat seiner Niederlassung,
3. den Namen des Signators oder ein Pseudonym, das als solches bezeichnet sein muß,
4. gegebenenfalls auf Verlangen des Zertifikatswerbers Angaben über eine Vertretungsmacht oder eine andere rechtlich erhebliche Eigenschaft des Signators,
5. die dem Signator zugeordneten Signaturprüfdaten,
6. Beginn und Ende der Gültigkeit des Zertifikats,
7. die eindeutige Kennung des Zertifikats,

8. gegebenenfalls eine Einschränkung des Anwendungsbereichs des Zertifikats und
9. gegebenenfalls eine Begrenzung des Transaktionswerts, auf den das Zertifikat ausgestellt ist.

(2) Auf Verlangen des Zertifikatswerbers können weitere rechtlich erhebliche Angaben in das qualifizierte Zertifikat aufgenommen werden.

(3) Ein qualifiziertes Zertifikat muß mit der sicheren elektronischen Signatur des Zertifizierungsdiensteanbieters versehen sein.

3. Abschnitt

Zertifizierungsdiensteanbieter

Tätigkeit der Zertifizierungsdiensteanbieter

§ 6. (1) Die Aufnahme und die Ausübung der Tätigkeit eines Zertifizierungsdiensteanbieters bedürfen keiner gesonderten Genehmigung.

(2) Ein Zertifizierungsdiensteanbieter hat die Aufnahme seiner Tätigkeit unverzüglich der Aufsichtsstelle (§ 13) anzuzeigen. Er hat der Aufsichtsstelle spätestens mit Aufnahme der Tätigkeit oder bei Änderung seiner Dienste ein Sicherheitskonzept sowie ein Zertifizierungskonzept für jeden von ihm angebotenen Signatur- und Zertifizierungsdienst samt den verwendeten technischen Komponenten und Verfahren vorzulegen.

(3) Ein Zertifizierungsdiensteanbieter, der sichere elektronische Signaturverfahren bereitstellt, hat in seinem Sicherheitskonzept die Einhaltung der Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen darzulegen.

(4) Ein Zertifizierungsdiensteanbieter hat die im Sicherheits- und im Zertifizierungskonzept dargelegten Angaben sowohl bei der Aufnahme als auch während der Ausübung seiner Tätigkeit zu erfüllen.

(5) Ein Zertifizierungsdiensteanbieter hat alle Umstände, die eine ordnungsgemäße und dem Sicherheits- sowie dem Zertifizierungskonzept entsprechende Tätigkeit nicht mehr ermöglichen, unverzüglich der Aufsichtsstelle anzuzeigen.

(6) Stellt ein Zertifizierungsdiensteanbieter Zertifikate aus, so hat er im Sicherheitskonzept darzulegen, ob und gegebenenfalls in welcher Form Verzeichnis- und Widerrufsdienste geführt werden.

(7) Ein von der Aufsichtsstelle ausgestelltes Zertifikat für Zertifizierungsdiensteanbieter darf von diesen nur für die Erbringung von Zertifizierungsdiensten verwendet werden.

Zertifizierungsdiensteanbieter für qualifizierte Zertifikate

§ 7. (1) Ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, hat

1. die erforderliche Zuverlässigkeit für die von ihm bereitgestellten Signatur- oder Zertifizierungsdienste aufzuweisen,
2. den Betrieb eines schnellen und sicheren Verzeichnisdienstes sowie eines unverzüglichen und sicheren Widerrufsdienstes sicherzustellen,
3. in qualifizierten Zertifikaten sowie für Verzeichnis- und Widerrufsdienste qualitätsgesicherte Zeitangaben (Zeitstempel) zu verwenden und jedenfalls sicherzustellen, daß der Zeitpunkt der Ausstellung und des Widerrufs eines qualifizierten Zertifikats bestimmt werden kann,
4. anhand eines amtlichen Lichtbildausweises die Identität und gegebenenfalls besondere rechtlich erhebliche Eigenschaften der Person, für die ein qualifiziertes Zertifikat ausgestellt wird, zuverlässig zu überprüfen,
5. zuverlässiges Personal mit den für die bereitgestellten Dienste erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen, insbesondere mit Managementfähigkeiten sowie mit Kenntnissen der Technologie elektronischer Signaturen und angemessener Sicherheitsverfahren, zu beschäftigen und geeignete Verwaltungs- und Managementverfahren, die anerkannten Normen entsprechen, einzuhalten,
6. über ausreichende Finanzmittel zu verfügen, um den Anforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen zu entsprechen, sowie durch Eingehen einer Haftpflichtversicherung mit einer Versicherungssumme von mindestens 56 000 000 S je Versicherungsfall Vorsorge dafür zu treffen, daß Schadenersatzansprüche befriedigt werden können,
7. alle maßgeblichen Umstände über ein qualifiziertes Zertifikat während eines für den Verwendungszweck angemessenen Zeitraums – gegebenenfalls auch elektronisch – aufzuzeichnen,

sodaß insbesondere in gerichtlichen Verfahren die Zertifizierung nachgewiesen werden kann, sowie

8. Vorkehrungen dafür zu treffen, daß die Signaturerstellungsdaten der Signatoren weder vom Zertifizierungsdiensteanbieter noch von Dritten gespeichert oder kopiert werden können.

(2) Ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, hat für die Signatur- und Zertifizierungsdienste sowie für die Erstellung und Speicherung von Zertifikaten vertrauenswürdige Systeme, Produkte und Verfahren, die vor Veränderungen geschützt sind und für die technische und kryptographische Sicherheit sorgen, zu verwenden. Er hat insbesondere geeignete Vorkehrungen dafür zu treffen, daß Signaturerstellungsdaten geheim gehalten werden, daß Daten für qualifizierte Zertifikate nicht unerkannt gefälscht oder verfälscht werden können und daß diese Zertifikate nur mit Zustimmung des Signators öffentlich abrufbar sind. Für die Bereitstellung von Signaturerstellungsdaten sowie für die Erstellung und Speicherung von qualifizierten Zertifikaten sind technische Komponenten und Verfahren, die den Anforderungen des § 18 entsprechen, zu verwenden.

(3) Signaturerstellungsdaten der Zertifizierungsdiensteanbieter sind vor unbefugtem Zugriff zu sichern.

(4) Für sichere elektronische Signaturen kann das Vorliegen der Voraussetzungen der Abs. 1 bis 3 im Rahmen der freiwilligen Akkreditierung (§ 17) bescheinigt werden.

(5) Stellt der Zertifizierungsdiensteanbieter ein sicheres elektronisches Signaturverfahren bereit, so muß der Umstand, daß es sich um eine sichere elektronische Signatur handelt, im Zertifikat oder in einem elektronisch jederzeit allgemein zugänglichen Verzeichnis aufscheinen.

(6) Auf Ersuchen von Gerichten oder anderen Behörden hat ein Zertifizierungsdiensteanbieter die Prüfung der auf seinen qualifizierten Zertifikaten beruhenden sicheren Signaturen vorzunehmen.

Ausstellung qualifizierter Zertifikate

§ 8. (1) Ein Zertifizierungsdiensteanbieter hat die Identität von Personen, denen ein qualifiziertes Zertifikat ausgestellt werden soll, anhand eines amtlichen Lichtbildausweises zuverlässig festzustellen. Er hat die Zuordnung bestimmter Signaturprüfdaten zu dieser Person durch ein qualifiziertes Zertifikat zu bestätigen.

(2) Das Verlangen auf Ausstellung eines qualifizierten Zertifikats kann auch bei einer im Auftrag des Zertifizierungsdiensteanbieters tätigen anderen Stelle eingebracht werden, die die Überprüfung der Identität des Zertifikatswerbers vorzunehmen hat.

(3) Ein Zertifizierungsdiensteanbieter hat nach Maßgabe des Zertifizierungskonzepts auf Verlangen des Zertifikatswerbers Angaben über seine Vertretungsmacht oder eine andere rechtlich erhebliche Eigenschaft in das qualifizierte Zertifikat aufzunehmen, sofern ihm oder einer anderen Stelle (Abs. 2) diese Umstände zuverlässig nachgewiesen werden.

(4) Ein Zertifizierungsdiensteanbieter kann nach Maßgabe des Zertifizierungskonzepts auf Verlangen des Zertifikatswerbers im Zertifikat anstatt des Namens des Signators ein Pseudonym angeben. Das Pseudonym darf weder anstößig noch offensichtlich zur Verwechslung mit Namen oder Kennzeichen geeignet sein.

Widerruf von Zertifikaten

§ 9. (1) Ein Zertifizierungsdiensteanbieter hat ein Zertifikat unverzüglich zu widerrufen, wenn

1. der Signator oder ein im Zertifikat genannter Machtgeber dies verlangt,
2. der Zertifizierungsdiensteanbieter Kenntnis vom Ableben des Signators oder sonst von der Änderung im Zertifikat bescheinigter Umstände erlangt,
3. das Zertifikat auf Grund unrichtiger Angaben erwirkt wurde,
4. der Zertifizierungsdiensteanbieter seine Tätigkeit einstellt und seine Verzeichnis- und Widerrufsdienste nicht von einem anderen Zertifizierungsdiensteanbieter übernommen werden,
5. die Aufsichtsstelle gemäß § 14 den Widerruf des Zertifikats anordnet oder
6. die Gefahr einer mißbräuchlichen Verwendung des Zertifikats besteht.

(2) Können die in Abs. 1 genannten Umstände nicht sofort zweifelsfrei festgestellt werden, so hat der Zertifizierungsdiensteanbieter das Zertifikat jedenfalls unverzüglich zu sperren.

(3) Die Sperre und der Widerruf müssen den Zeitpunkt enthalten, ab dem sie wirksam werden. Eine rückwirkende Sperre oder ein rückwirkender Widerruf ist unzulässig. Der Signator bzw. sein Rechtsnachfolger ist von der Sperre oder dem Widerruf unverzüglich zu verständigen.

(4) Ein Zertifizierungsdiensteanbieter hat ein elektronisch jederzeit allgemein zugängliches Verzeichnis der gesperrten und der widerrufenen qualifizierten Zertifikate zu führen.

(5) Die Aufsichtsstelle hat die von ihr für den Zertifizierungsdiensteanbieter ausgestellten Zertifikate unverzüglich zu widerrufen, wenn

1. dem Zertifizierungsdiensteanbieter die Ausübung seiner Tätigkeit untersagt wird und seine Verzeichnis- und Widerrufsdienste nicht von einem anderen Zertifizierungsdiensteanbieter übernommen werden oder
2. der Zertifizierungsdiensteanbieter seine Tätigkeit einstellt und seine Verzeichnis- und Widerrufsdienste nicht von einem anderen Zertifizierungsdiensteanbieter übernommen werden.

Zeitstempeldienste

§ 10. Stellt ein Zertifizierungsdiensteanbieter Zeitstempeldienste bereit, so hat er im Sicherheits- und im Zertifizierungskonzept die näheren Angaben darzulegen. Für sichere Zeitstempeldienste sind technische Komponenten und Verfahren zu verwenden, die die Richtigkeit und Unverfälschtheit der Zeitangabe sicherstellen und den Anforderungen des § 18 entsprechen.

Dokumentation

§ 11. (1) Ein Zertifizierungsdiensteanbieter hat die Sicherheitsmaßnahmen, die er zur Einhaltung dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen getroffen hat, sowie das Ausstellen und gegebenenfalls die Sperre und den Widerruf von Zertifikaten zu dokumentieren. Dabei müssen die Daten und ihre Unverfälschtheit sowie der Zeitpunkt ihrer Aufnahme in das Protokollierungssystem jederzeit nachprüfbar sein.

(2) Auf Ersuchen von Gerichten oder anderen Behörden hat ein Zertifizierungsdiensteanbieter die Dokumentation nach Abs. 1 auszufolgen.

Einstellung der Tätigkeit

§ 12. Ein Zertifizierungsdiensteanbieter hat die Einstellung seiner Tätigkeit unverzüglich der Aufsichtsstelle anzuzeigen. Weiters hat er die im Zeitpunkt der Einstellung seiner Tätigkeit gültigen Zertifikate zu widerrufen oder dafür Sorge zu tragen, daß zumindest seine Verzeichnis- und Widerrufsdienste von einem anderen Zertifizierungsdiensteanbieter übernommen werden. Die Signatoren sind von der Einstellung der Tätigkeit sowie vom Widerruf oder der Übernahme unverzüglich zu verständigen. Auch im Fall des Widerrufs der Zertifikate hat der Zertifizierungsdiensteanbieter sicherzustellen, daß die Widerrufsdienste weitergeführt werden; kommt er dieser Verpflichtung nicht nach, so hat die Aufsichtsstelle für die Weiterführung der Widerrufsdienste auf Kosten des Zertifizierungsdiensteanbieters Sorge zu tragen.

4. Abschnitt

Aufsicht

Aufsichtsstelle

§ 13. (1) Aufsichtsstelle ist die Telekom-Control-Kommission (§ 110 TKG). Ihr obliegt die laufende Aufsicht über die Einhaltung der Bestimmungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen sowie die Ausstellung von Zertifikaten für Zertifizierungsdiensteanbieter.

(2) Die Aufsichtsstelle hat insbesondere

1. die Umsetzung der Angaben im Sicherheits- und im Zertifizierungskonzept zu überprüfen,
2. im Fall der Bereitstellung sicherer elektronischer Signaturen die Verwendung geeigneter technischer Komponenten und Verfahren (§ 18) zu überwachen,
3. Zertifizierungsdiensteanbieter nach § 17 zu akkreditieren und
4. die organisatorische Aufsicht über Bestätigungsstellen (§ 19) durchzuführen.

(3) Auf die Ausstellung von Zertifikaten für Zertifizierungsdiensteanbieter sind die Vorschriften für die Ausstellung von qualifizierten Zertifikaten durch Zertifizierungsdiensteanbieter anzuwenden; die Aufsichtsstelle hat die für Zertifizierungsdiensteanbieter ausgestellten Zertifikate mit ihrer sicheren elektronischen Signatur zu versehen. Das Zertifikat der Aufsichtsstelle ist im "Amtsblatt zur Wiener Zeitung" zu veröffentlichen. Die Aufsichtsstelle hat dafür Sorge zu tragen, daß ein elektronisch jederzeit allgemein zugängliches Verzeichnis der gültigen, der gesperrten und der widerrufenen Zertifikate für Zertifizierungsdiensteanbieter geführt wird. Weiters hat die Aufsichtsstelle dafür Sorge zu tragen, daß ein elektronisch jederzeit allgemein zugängliches Verzeichnis der im Inland niedergelassenen

Zertifizierungsdiensteanbieter, der von ihr akkreditierten Zertifizierungsdiensteanbieter und der Drittstaaten-Zertifizierungsdiensteanbieter, für deren Zertifikate ein im Inland niedergelassener Zertifizierungsdiensteanbieter nach § 24 Abs. 2 Z 2 entsteht, geführt wird. Auf Antrag sind auch andere im Ausland niedergelassene Zertifizierungsdiensteanbieter in dieses Verzeichnis aufzunehmen.

(4) Die Aufsichtsstelle hat den Zertifizierungsdiensteanbietern für ihre Tätigkeit und für die Heranziehung der Telekom-Control GmbH eine mit Verordnung festgelegte kostendeckende Gebühr vorzuschreiben. Die Einnahmen aus dieser Gebühr fließen der Aufsichtsstelle zu und sind nach Heranziehung der Telekom-Control GmbH oder der Bestätigungsstelle nach deren Aufwand weiterzuleiten.

(5) Die Aufsichtsstelle kann zur Wahrnehmung ihrer Aufgaben eine Bestätigungsstelle (§ 19) beauftragen.

(6) Die Mitglieder der Aufsichtsstelle sind gemäß Art. 20 Abs. 2 B-VG bei Ausübung ihres Amtes an keine Weisungen gebunden. Sofern gesetzlich nicht anderes bestimmt ist, hat die Aufsichtsstelle das AVG 1991 anzuwenden. Sie entscheidet in oberster Instanz. Die Anrufung des Verwaltungsgerichtshofs ist zulässig.

(7) Die Tätigkeit der Aufsichtsstelle nach diesem Bundesgesetz ist von ihrer Tätigkeit nach anderen Bundesgesetzen organisatorisch und finanziell zu trennen.

Aufsichtsmaßnahmen

§ 14. (1) Die Aufsichtsstelle hat den Zertifizierungsdiensteanbietern Maßnahmen zur Sicherstellung der Erfüllung der Pflichten aus diesem Bundesgesetz und der auf seiner Grundlage ergangenen Verordnungen vorzuschreiben. Sie kann einem Zertifizierungsdiensteanbieter insbesondere die Verwendung ungeeigneter technischer Komponenten und Verfahren oder die Ausübung der Tätigkeit ganz oder teilweise untersagen. Weiters kann die Aufsichtsstelle Zertifikate für Zertifizierungsdiensteanbieter oder von Signatoren widerrufen oder den Widerruf der Zertifikate von Signatoren durch den Zertifizierungsdiensteanbieter anordnen.

(2) Einem Zertifizierungsdiensteanbieter ist die Ausübung der Tätigkeit ganz oder teilweise zu untersagen, wenn

1. er oder sein Personal nicht die für die bereitgestellten Signatur- oder Zertifizierungsdienste erforderliche Zuverlässigkeit aufweist,
2. er oder sein Personal nicht über die erforderlichen Fachkenntnisse verfügt,
3. ihm keine ausreichenden Finanzmittel zur Verfügung stehen,
4. er bei der Ausübung seiner Tätigkeit die im Sicherheits- oder im Zertifizierungskonzept dargelegten Angaben nicht erfüllt,
5. er die vorgeschriebenen Verzeichnis- oder Widerrufsdienste nicht oder nicht ordnungsgemäß führt oder der Sperr- oder Widerrufspflicht (§ 9) nicht oder nur unzureichend nachkommt oder
6. er der Anzeigepflicht nach § 6 Abs. 2 nicht nachkommt.

(3) Einem Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, ist die Ausübung seiner Tätigkeit zudem ganz oder teilweise zu untersagen, wenn die übrigen für die Ausübung einer solchen Tätigkeit erforderlichen Voraussetzungen nach diesem Bundesgesetz oder den auf seiner Grundlage ergangenen Verordnungen nicht erfüllt werden.

(4) Einem Zertifizierungsdiensteanbieter, der sichere elektronische Signaturverfahren bereitstellt, ist die Ausübung seiner Tätigkeit auch dann ganz oder teilweise zu untersagen, wenn die verwendeten technischen Komponenten und Verfahren nicht die Sicherheitsanforderungen nach § 18 erfüllen.

(5) Wenn die Aufsichtsstelle einem Zertifizierungsdiensteanbieter die Ausübung seiner Tätigkeit untersagt, hat sie für den Widerruf der Zertifikate des Zertifizierungsdiensteanbieters und der Signatoren Sorge zu tragen oder die Übernahme der erbrachten Signatur- und Zertifizierungsdienste oder zumindest seiner Verzeichnis- und Widerrufsdienste durch einen anderen Zertifizierungsdiensteanbieter zu veranlassen, sofern die beteiligten Zertifizierungsdiensteanbieter der Übernahme zustimmen. Die Signatoren sind von der Untersagung sowie vom Widerruf oder der Übernahme unverzüglich zu verständigen. Auch im Fall des Widerrufs der Zertifikate hat der Zertifizierungsdiensteanbieter sicherzustellen, daß die Widerrufsdienste weitergeführt werden; kommt er dieser Verpflichtung nicht nach, so hat die Aufsichtsstelle für die Weiterführung der Widerrufsdienste auf Kosten des Zertifizierungsdiensteanbieters Sorge zu tragen.

(6) Statt einer Untersagung im Sinn der Abs. 2 bis 4 kann die Aufsichtsstelle andere geeignete Maßnahmen anordnen, soweit diese zur Erreichung des angestrebten Zwecks ausreichen. Sie kann insbesondere Auflagen erteilen oder unter Setzung einer angemessenen Frist zur Behebung von ihr aufgezeigter Mängel Maßnahmen androhen.

Heranziehung der Telekom-Control GmbH

§ 15. (1) Die Aufsichtsstelle kann sich bei der Durchführung der Aufsicht der Telekom-Control GmbH (§ 108 TKG) bedienen.

(2) Die Telekom-Control GmbH hat insbesondere

1. die Aufsichtsstelle bei der laufenden Aufsicht der Zertifizierungsdiensteanbieter zu unterstützen und die technischen Produkte, Verfahren und sonstigen Mittel, die im Rahmen der bereitgestellten Signatur- und Zertifizierungsdienste eingesetzt werden, sowie die Qualifikation des Personals zu überprüfen,
2. die Zertifizierungsdiensteanbieter nach der Anzeige der Aufnahme ihrer Tätigkeit zu registrieren,
3. Verzeichnisse der von der Aufsichtsstelle ausgestellten Zertifikate und der Zertifizierungsdiensteanbieter (§ 13 Abs. 3) sowie ein Verzeichnis der akkreditierten Zertifizierungsdiensteanbieter (§ 17 Abs. 1) zu führen,
4. für den Fall der Einstellung oder Untersagung der Tätigkeit eines Zertifizierungsdiensteanbieters einen Widerrufsdienst zu führen, sofern keine Übernahme im Sinn der §§ 12 oder 14 Abs. 5 erfolgt,
5. auf Anordnung der Aufsichtsstelle die Erfüllung der Voraussetzungen einer freiwilligen Akkreditierung (§ 17) zu erheben,
6. bei der Feststellung der Gleichwertigkeit von Prüfberichten aus Drittstaaten im Sinn des § 24 Abs. 3 mitzuwirken und
7. im Fall des begründeten Verdachts, daß die Sicherheitsanforderungen dieses Bundesgesetzes oder der auf seiner Grundlage ergangenen Verordnungen nicht eingehalten werden, oder auf Verlangen eines Zertifizierungsdiensteanbieters unmittelbar die vorläufige Untersagung der Tätigkeit des Zertifizierungsdiensteanbieters oder vorläufig Maßnahmen im Sinn des § 14 Abs. 1 anzuordnen.

(3) Die Telekom-Control GmbH hat alle organisatorischen Vorkehrungen dafür zu treffen, daß sie ihre Aufgaben erfüllen und die Aufsichtsstelle bei Erfüllung ihrer Aufgaben unterstützen kann. Sie kann zur Wahrnehmung ihrer Aufgaben eine Bestätigungsstelle (§ 19) beauftragen. Die Wahrnehmung ihrer Aufgaben in technischen Belangen hat in Abstimmung mit einer Bestätigungsstelle (§ 19) zu erfolgen. Im Rahmen ihrer Tätigkeit für die Aufsichtsstelle ist das Personal der Telekom-Control GmbH an die Weisungen des Vorsitzenden oder des in der Geschäftsordnung bezeichneten Mitgliedes gebunden.

(4) Unbeschadet der Zuständigkeit der ordentlichen Gerichte können Kunden oder Interessenvertretungen Streit- oder Beschwerdefälle, insbesondere über die Qualität eines Zertifizierungsdienstes, die mit dem Zertifizierungsdiensteanbieter nicht befriedigend gelöst worden sind, der Telekom-Control GmbH vorlegen. Die Telekom-Control GmbH hat sich zu bemühen, innerhalb angemessener Frist eine einvernehmliche Lösung herbeizuführen. Die Zertifizierungsdiensteanbieter sind verpflichtet, an einem solchen Verfahren mitzuwirken und alle zur Beurteilung der Sachlage erforderlichen Auskünfte zu erteilen. Die Telekom-Control GmbH hat Richtlinien für die Durchführung dieses Verfahrens festzulegen, die in geeigneter Form zu veröffentlichen sind.

(5) § 13 Abs. 7 über die organisatorische und finanzielle Trennung ist auf die Tätigkeit der Telekom-Control GmbH anzuwenden.

Durchführung der Aufsicht

§ 16. (1) Die Zertifizierungsdiensteanbieter haben den im Auftrag der Aufsichtsstelle handelnden Personen das Betreten der Geschäfts- und Betriebsräume während der Geschäftszeiten zu gestatten, die in Betracht kommenden Bücher und sonstigen Aufzeichnungen oder Unterlagen einschließlich der Dokumentation nach § 11 vorzulegen oder zur Einsicht bereitzuhalten, Auskünfte zu erteilen und jede sonst erforderliche Unterstützung zu gewähren. Bestehende gesetzliche Verschwiegenheits- und Aussageverweigerungsrechte bleiben unberührt.

(2) Die Organe des öffentlichen Sicherheitsdienstes haben der Aufsichtsstelle und den in ihrem Auftrag handelnden Personen über deren Ersuchen zur Durchführung der Aufsicht im Rahmen ihres gesetzmäßigen Wirkungsbereichs Hilfe zu leisten.

(3) Die Durchführung der Aufsicht nach den Abs. 1 und 2 ist unter möglicher Schonung der Betroffenen und ohne unnötiges Aufsehen so durchzuführen, daß dadurch die Sicherheit der Signatur- und Zertifizierungsdienste nicht verletzt wird.

Freiwillige Akkreditierung

§ 17. (1) Zertifizierungsdiensteanbieter, die sichere elektronische Signaturverfahren bereitstellen und der Aufsichtsstelle vor der Aufnahme ihrer Tätigkeit als akkreditierte Zertifizierungsdiensteanbieter die Einhaltung der Anforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen nachweisen, sind auf Antrag von der Aufsichtsstelle zu akkreditieren. Akkreditierte Zertifizierungsdiensteanbieter dürfen sich mit Zustimmung der Aufsichtsstelle im Geschäftsverkehr als solche bezeichnen. Im Zusammenhang mit Signatur- und Zertifizierungsdiensten sowie mit Signaturprodukten darf diese Bezeichnung nur verwendet werden, wenn die Sicherheitsanforderungen nach § 18 erfüllt werden. Die Aufsichtsstelle hat dafür Sorge zu tragen, daß die akkreditierten Zertifizierungsdiensteanbieter in ein elektronisch jederzeit allgemein zugängliches Verzeichnis aufgenommen werden.

(2) Die freiwillige Akkreditierung eines Zertifizierungsdiensteanbieters ist in das qualifizierte Zertifikat aufzunehmen oder sonst in geeigneter Weise zugänglich zu machen.

(3) Die Aufsichtsstelle hat für die laufende Aufsicht über die von ihr akkreditierten Zertifizierungsdiensteanbieter Sorge zu tragen.

5. Abschnitt

Technische Sicherheitserfordernisse

Technische Komponenten und Verfahren für sichere Signaturen

§ 18. (1) Für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung sicherer Signaturen sind solche technische Komponenten und Verfahren einzusetzen, die die Fälschung von Signaturen sowie die Verfälschung signierter Daten zuverlässig erkennbar machen und die die unbefugte Verwendung von Signaturerstellungsdaten verlässlich verhindern.

(2) Die bei der Erstellung einer sicheren Signatur verwendeten technischen Komponenten und Verfahren müssen zudem sicherstellen, daß die zu signierenden Daten nicht verändert werden; sie müssen es weiters ermöglichen, daß dem Signator die zu signierenden Daten vor Auslösung des Signaturvorgangs dargestellt werden. Die Signaturerstellungsdaten dürfen mit an Sicherheit grenzender Wahrscheinlichkeit nur einmal vorkommen, sie dürfen weiters mit hinreichender Sicherheit nicht ableitbar sein; ihre Geheimhaltung muß sichergestellt sein.

(3) Bei der Erstellung und Speicherung von qualifizierten Zertifikaten sind solche technische Komponenten und Verfahren einzusetzen, die die Fälschung und Verfälschung von Zertifikaten verhindern.

(4) Für die Überprüfung von sicher signierten Daten sind solche technische Komponenten und Verfahren anzubieten, die sicherstellen, daß

1. die signierten Daten nicht verändert worden sind,
2. die Signatur zuverlässig überprüft und das Ergebnis dieser Überprüfung korrekt angezeigt wird,
3. der Überprüfer feststellen kann, auf welche Daten sich die elektronische Signatur bezieht,
4. der Überprüfer feststellen kann, welchem Signator die elektronische Signatur zugeordnet ist, wobei die Verwendung eines Pseudonyms angezeigt werden muß, und
5. daß sicherheitsrelevante Veränderungen der signierten Daten erkannt werden können.

(5) Die technischen Komponenten und Verfahren für die Erzeugung sicherer Signaturen müssen nach dem Stand der Technik hinreichend und laufend geprüft sein. Die Erfüllung der Sicherheitsanforderungen muß von einer Bestätigungsstelle (§ 19) bescheinigt sein.

Bestätigungsstelle

§ 19. (1) Die nach diesem Bundesgesetz und den auf seiner Grundlage ergangenen Verordnungen einer Bestätigungsstelle zugewiesenen Aufgaben können nur von einer dazu geeigneten Einrichtung wahrgenommen werden.

(2) Eine Einrichtung ist zur Wahrnehmung der einer Bestätigungsstelle zugewiesenen Aufgaben geeignet, wenn sie

1. die erforderliche Zuverlässigkeit aufweist,

2. zuverlässiges Personal mit den für diese Aufgaben erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen, insbesondere mit Kenntnissen über elektronische Signaturen, angemessene Sicherheitsverfahren, Kryptographie, Kommunikations- und Chipkartentechnologien sowie die technische Begutachtung solcher Komponenten, beschäftigt,
3. über ausreichende technische Einrichtungen und Mittel sowie eine ausreichende wirtschaftliche Leistungsfähigkeit verfügt und
4. die erforderliche Unabhängigkeit, Unparteilichkeit und Unbefangenheit sicherstellt.

(3) Der Bundeskanzler hat im Einvernehmen mit dem Bundesminister für Justiz und dem Bundesminister für Wissenschaft und Verkehr mit Verordnung festzustellen, daß eine Einrichtung als Bestätigungsstelle geeignet ist. Eine solche Verordnung kann nur auf Antrag der betreffenden Einrichtung erlassen werden. Die Eignung kann nur festgestellt werden, wenn die Einrichtung nach ihren Statuten oder Satzungen oder nach ihrem Gesellschaftsvertrag, nach ihrer Organisation und nach ihrem Sicherheits- und Finanzierungskonzept die in Abs. 2 genannten Anforderungen erfüllt.

(4) Eine Bestätigungsstelle kann zur Erfüllung der ihr nach diesem Bundesgesetz oder der auf seiner Grundlage ergangenen Verordnungen zugewiesenen Aufgaben von anderen Einrichtungen oder Stellen Prüfberichte zu technischen Komponenten und Verfahren einholen.

(5) Die Bestätigungsstelle hat den Zertifizierungsdiensteanbietern für ihre Tätigkeit eine mit Verordnung festgelegte kostendeckende Gebühr vorzuschreiben. Die Einnahmen aus dieser Gebühr fließen der Bestätigungsstelle zu.

6. Abschnitt

Rechte und Pflichten der Anwender

Allgemeine Informationspflichten der Zertifizierungsdiensteanbieter

§ 20. (1) Ein Zertifizierungsdiensteanbieter hat den Zertifikatswerber vor Vertragsschließung schriftlich oder unter Verwendung eines dauerhaften Datenträgers klar und allgemein verständlich über den Inhalt des Sicherheits- und des Zertifizierungskonzepts zu unterrichten. Bei der Ausstellung eines qualifizierten Zertifikats hat der Zertifizierungsdiensteanbieter zudem die Bedingungen der Verwendung des Zertifikats, wie etwa Einschränkungen seines Anwendungsbereichs oder des Transaktionswerts, bekanntzugeben; weiters ist auf eine freiwillige Akkreditierung (§ 17) sowie auf besondere Streitbeilegungsverfahren hinzuweisen.

(2) Auf Verlangen sind die in Abs. 1 genannten Angaben auch Dritten, die ein rechtliches Interesse daran glaubhaft machen, zugänglich zu machen.

(3) Ein Zertifizierungsdiensteanbieter hat weiters den Zertifikatswerber darüber zu unterrichten, welche technischen Komponenten und Verfahren für das verwendete Signaturverfahren geeignet sind, gegebenenfalls auch darüber, welche technischen Komponenten und Verfahren sowie sonstigen Maßnahmen die Anforderungen für die Erzeugung und Prüfung sicherer Signaturen erfüllen. Ferner ist der Zertifikatswerber über die möglichen Rechtswirkungen des von ihm verwendeten Signaturverfahrens, über die Pflichten eines Signators sowie über die besondere Haftung des Zertifizierungsdiensteanbieters zu belehren. Der Zertifikatswerber ist auch darüber zu unterrichten, daß und wie gegebenenfalls eine neue elektronische Signatur anzubringen ist, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird.

Pflichten des Signators

§ 21. Der Signator hat die Signaturerstellungsdaten sorgfältig zu verwahren, soweit zumutbar Zugriffe auf Signaturerstellungsdaten zu verhindern und deren Weitergabe zu unterlassen. Er hat den Widerruf des Zertifikats zu verlangen, wenn die Signaturerstellungsdaten abhanden kommen, wenn Anhaltspunkte für eine Kompromittierung der Signaturerstellungsdaten bestehen oder wenn sich die im Zertifikat bescheinigten Umstände geändert haben.

Datenschutz

§ 22. (1) Ein Zertifizierungsdiensteanbieter darf nur jene personenbezogenen Daten verwenden, die er zur Durchführung der erbrachten Dienste benötigt. Diese Daten dürfen nur unmittelbar beim Betroffenen selbst oder mit seiner ausdrücklichen Zustimmung bei einem Dritten erhoben werden.

(2) Bei Verwendung eines Pseudonyms hat der Zertifizierungsdiensteanbieter die Daten über die Identität des Signators zu übermitteln, sofern an der Feststellung der Identität ein überwiegendes berech-

tigtes Interesse im Sinn des § 8 Abs. 1 Z 4 und Abs. 3 DSG glaubhaft gemacht wird. Die Übermittlung ist zu dokumentieren.

(3) Die Auskunfts- und Mitwirkungspflichten des Zertifizierungsdiensteanbieters gegenüber Gerichten und anderen Behörden bleiben unberührt.

Haftung der Zertifizierungsstellen

§ 23. (1) Ein Zertifizierungsdiensteanbieter, der ein Zertifikat als qualifiziertes Zertifikat ausstellt oder für ein solches Zertifikat nach § 24 Abs. 2 Z 2 einsteht, haftet gegenüber jeder Person, die auf das Zertifikat vertraut, dafür, daß

1. alle Angaben im qualifizierten Zertifikat im Zeitpunkt seiner Ausstellung richtig sind,
2. der im qualifizierten Zertifikat angegebene Signator im Zeitpunkt der Ausstellung des Zertifikats im Besitz jener Signaturerstellungsdaten ist, die den im Zertifikat angegebenen Signaturprüfdaten entsprechen,
3. die Signaturerstellungsdaten und die ihnen zugeordneten Signaturprüfdaten einander bei Verwendung der von ihm bereitgestellten oder als geeignet bezeichneten Produkte und Verfahren in komplementärer Weise entsprechen,
4. das Zertifikat bei Vorliegen der Voraussetzungen unverzüglich widerrufen wird und die Widerrufsdienste verfügbar sind sowie
5. die Anforderungen des § 7 erfüllt und für die Erzeugung und Speicherung von Signaturerstellungsdaten technische Komponenten und Verfahren nach § 18 verwendet werden.

(2) Ein Zertifizierungsdiensteanbieter, der sichere elektronische Signaturverfahren bereitstellt, haftet zudem dafür, daß für die von ihm bereitgestellten oder als geeignet bezeichneten Produkte, Verfahren und sonstigen Mittel für die Erstellung elektronischer Signaturen sowie für die Darstellung von signierender Daten nur technische Komponenten und Verfahren nach § 18 verwendet werden.

(3) Der Zertifizierungsdiensteanbieter haftet nicht, wenn er nachweist, daß ihn und seine Leute an der Verletzung der Verpflichtungen nach Abs. 1 und 2 kein Verschulden trifft. Kann der Geschädigte als wahrscheinlich dartun, daß die Verpflichtungen nach Abs. 1 und 2 verletzt oder die zur Einhaltung der Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen getroffenen Vorkehrungen kompromittiert wurden, so wird vermutet, daß der Schaden dadurch verursacht wurde.

(4) Enthält ein qualifiziertes Zertifikat eine Einschränkung des Anwendungsbereichs, so haftet der Zertifizierungsdiensteanbieter nicht für Schäden, die sich aus einer anderen Verwendung des Zertifikats ergeben. Enthält ein qualifiziertes Zertifikat einen bestimmten Transaktionswert, bis zu dem das Zertifikat verwendet werden darf, so haftet der Zertifizierungsdiensteanbieter nicht für Schäden, die sich aus der Überschreitung dieses Transaktionswerts ergeben.

(5) Die Haftung eines Zertifizierungsdiensteanbieters nach Abs. 1 bis 3 kann im vorhinein weder ausgeschlossen noch beschränkt werden.

(6) Bestimmungen des Allgemeinen Bürgerlichen Gesetzbuchs und anderer Rechtsvorschriften, nach denen Schäden in anderem Umfang oder von anderen Personen als nach diesem Bundesgesetz zu ersetzen sind, bleiben unberührt.

7. Abschnitt

Anerkennung ausländischer Zertifikate

Anerkennung

§ 24. (1) Zertifikate, die von einem in der Europäischen Gemeinschaft niedergelassenen Zertifizierungsdiensteanbieter ausgestellt wurden und deren Gültigkeit vom Inland aus überprüft werden kann, sind inländischen Zertifikaten gleichgestellt. Qualifizierte Zertifikate solcher Zertifizierungsdiensteanbieter entfalten dieselben Rechtswirkungen wie inländische qualifizierte Zertifikate.

(2) Zertifikate, die von einem in einem Drittstaat niedergelassenen Zertifizierungsdiensteanbieter ausgestellt wurden und deren Gültigkeit vom Inland aus überprüft werden kann, werden im Inland anerkannt. Qualifizierte Zertifikate werden inländischen qualifizierten Zertifikaten rechtlich gleichgestellt, wenn

1. der Zertifizierungsdiensteanbieter die Anforderungen nach § 7 erfüllt und unter einem freiwilligen Akkreditierungssystem eines Mitgliedstaates der Europäischen Union akkreditiert ist,
2. ein in der Europäischen Gemeinschaft niedergelassener Zertifizierungsdiensteanbieter, der die Anforderungen nach § 7 erfüllt, für das Zertifikat haftungsrechtlich einsteht oder
3. im Rahmen einer bilateralen oder multilateralen Vereinbarung zwischen der Europäischen Gemeinschaft einerseits und Drittstaaten oder internationalen Organisationen andererseits das Zertifikat als qualifiziertes Zertifikat oder der Zertifizierungsdiensteanbieter als Aussteller qualifizierter Zertifikate anerkannt ist.

(3) Ist in einem Drittstaat zum Nachweis der Sicherheitsanforderungen für sichere elektronische Signaturen eine staatlich anerkannte Stelle eingerichtet, so werden Bescheinigungen dieser Stelle über die Einhaltung der Sicherheitsanforderungen für die Erzeugung sicherer elektronischer Signaturen den Bescheinigungen einer Bestätigungsstelle (§ 19) gleichgehalten, soweit die Aufsichtsstelle feststellt, daß die den Beurteilungen dieser Stellen zugrunde liegenden technischen Anforderungen, Prüfungen und Prüfverfahren jenen der Bestätigungsstelle gleichwertig sind.

8. Abschnitt

Schlußbestimmungen

Signaturverordnung

§ 25. Der Bundeskanzler hat mit Verordnung im Einvernehmen mit dem Bundesminister für Justiz und dem Bundesminister für Wissenschaft und Verkehr, hinsichtlich der Z 1 und 2 auch im Einvernehmen mit dem Bundesminister für Finanzen, die nach dem jeweiligen Stand der Wissenschaft und Technik zur Durchführung dieses Bundesgesetzes erforderlichen Rechtsvorschriften zu erlassen über

1. die Festsetzung pauschaler kostendeckender Gebühren für die Leistungen der Aufsichtsstelle, der Telekom-Control GmbH und der Bestätigungsstellen sowie die Vorschreibung dieser Gebühren,
2. die Festsetzung der zur Erfüllung der Anforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen ausreichenden Finanzmittel,
3. die Zuverlässigkeit des Zertifizierungsdiensteanbieters und seines Personals (§§ 7 Abs. 1 und 14 Abs. 2),
4. die näheren Sicherheitsanforderungen an die technischen Komponenten und Verfahren in Ausführung des § 18, die Durchführung der Prüfung der technischen Komponenten und Verfahren sowie die Ausstellung der Bestätigung, daß diese Anforderungen erfüllt sind,
5. die Dauer der Weiterführung der Widerrufsdienste durch die Aufsichtsstelle (§ 12 und § 14 Abs. 5),
6. die Anwendungsbereiche, Anforderungen und Toleranzen von sicheren Zeitstempeldiensten,
7. die Gültigkeitsdauer und die Erneuerung der qualifizierten Zertifikate sowie den Zeitraum und das Verfahren, nach denen eine neue elektronische Signatur angebracht werden sollte (Nachsignieren),
8. die Form, Darstellung und Verfügbarkeit des Zertifizierungskonzepts (zB Klartext),
9. die Dauer der Aufbewahrung einer Dokumentation (§ 11) und
10. die Art und Form der Kennzeichnung akkreditierter Zertifizierungsdiensteanbieter.

Inkrafttreten und Verweisungen

§ 26. (1) Dieses Bundesgesetz tritt mit 1. Jänner 2000 in Kraft.

(2) Soweit in diesem Bundesgesetz auf Bestimmungen anderer Bundesgesetze verwiesen wird, sind diese in ihrer jeweils geltenden Fassung anzuwenden.

Vollzug

§ 27. Mit der Vollziehung dieses Bundesgesetzes sind betraut:

1. hinsichtlich der §§ 3, 4 und 23 der Bundesminister für Justiz,
2. hinsichtlich der §§ 13 bis 17 der Bundesminister für Wissenschaft und Verkehr,
3. hinsichtlich des § 22 der Bundeskanzler,
4. hinsichtlich der §§ 7 Abs. 1 Z 6, 13 Abs. 4 und 19 Abs. 6 der Bundeskanzler im Einvernehmen mit dem Bundesminister für Justiz, dem Bundesminister für Wissenschaft und Verkehr und dem Bundesminister für Finanzen und
5. hinsichtlich der übrigen Bestimmungen der Bundeskanzler im Einvernehmen mit dem Bundesminister für Justiz und dem Bundesminister für Wissenschaft und Verkehr.

Vorblatt

Problem:

Die weitere Entwicklung des elektronischen Geschäfts- und Rechtsverkehrs über das Internet und andere offene Netzwerke hängt nicht zuletzt davon ab, daß die Teilnehmer diesen Kommunikationsmitteln **uneingeschränkt vertrauen**. Sie müssen sich insbesondere auf die Identität ihres Ansprechpartners verlassen können und Gewißheit darüber haben, daß die ihnen zugesandten oder von ihnen abgeschickten Daten nicht verändert werden. Die Voraussetzungen für dieses Vertrauen können nicht allein durch freiwillige Maßnahmen und Selbstverpflichtungen der Wirtschaft geschaffen werden. Vielmehr bedarf es auch gewisser **gesetzlicher Regelungen**, die ein hohes Maß an Sicherheit bieten.

Ziele:

Mit der Einführung und Anerkennung elektronischer Signaturen sollen die **rechtlichen Grundlagen** für den Einsatz **sicherer Technologien und Verfahren** im Internet und anderen elektronischen Netzwerken geschaffen werden. Dabei sollen unter anderem die Tätigkeit und die Verantwortung von Zertifizierungseinrichtungen, die in einem Zertifikat die Identität einer Person bescheinigen, geregelt werden. Weiters sollen die Rechtswirkungen elektronisch signierter Erklärungen klargestellt werden. Auf Grund des grenzüberschreitenden Charakters der neuen elektronischen Medien soll auch der Anerkennung ausländischer Regelungen über die elektronische Signatur besonderes Augenmerk gewidmet werden.

Inhalt:

- Zulassung und **Nichtdiskriminierung elektronischer Signaturen** im Geschäfts- und Rechtsverkehr;
- weitgehende Gleichstellung der **Rechtswirkungen einer sicheren elektronischen Signatur** mit den Rechtswirkungen einer eigenhändigen Unterschrift;
- Einführung eines **Aufsichtssystems über Zertifizierungseinrichtungen** einschließlich der Schaffung eines Systems zur freiwilligen Akkreditierung;
- Einführung von **Haftungsregelungen** für Zertifizierungseinrichtungen;
- Regelung der Voraussetzungen einer **Anerkennung ausländischer elektronischer Signaturen**.

Alternativen:

Keine.

Kosten:

Die Einführung eines Aufsichtssystems wird **geringfügige Mehrbelastungen** für das Budget des Bundes nach sich ziehen. Die Haushalte der Länder und der Gemeinden werden durch die im Entwurf vorgesehenen Regelungen nicht belastet.

Besonderheiten des Normerzeugungsverfahrens:

Keine.

Auswirkungen auf Beschäftigung und Wirtschaftsstandort:

Das Vorhaben verspricht **positive Auswirkungen** sowohl auf die Beschäftigung als auch auf den Wirtschaftsstandort. Vor allem werden mit dem Entwurf rechtliche Unsicherheiten und Ungewißheiten, die sich bislang als Investitionshindernis ausgewirkt haben, beseitigt.

Vereinbarkeit mit dem EU-Recht:

Das Vorhaben ist **gemeinschaftskonform**, zumal damit die Umsetzung der Richtlinie über gemeinsame Rahmenbedingungen für elektronische Signaturen vorbereitet werden soll.

Erläuterungen Allgemeiner Teil

1. Einleitung

Das **Internet**, das in den 70er Jahren in den USA entwickelt wurde, ist heute ein gängiges und alltäglich eingesetztes Kommunikationsmittel vieler Unternehmen und privater Haushalte. Die fortschreitende Entwicklung der Informations- und Kommunikationstechnologie erfaßt nahezu alle Wirtschafts- und Lebensbereiche. Informationstechnologische Produkte und Dienstleistungen bilden weltweit eine der prosperierendsten Branchen mit ständig zunehmenden Steigerungsraten und noch größeren Wachstumspotentialen. Die Anzahl der Teilnehmer am Internet verdoppelt sich alle 12 bis 18 Monate. Neueste Schätzungen gehen von über 40 Millionen angeschlossenen Systemen aus, die Anzahl der Menschen, die Zugriff auf Informationen im Internet haben, wird derzeit auf über 150 Millionen geschätzt, davon rund 34 Millionen in Europa und rund 600 000 in Österreich. 100 Millionen Menschen sind täglich online, in wenigen Jahren könnte es eine Milliarde sein. Das Einkaufen und Bestellen per mouse-click gehört für viele Menschen bereits zum Alltag.

Für die neuen elektronischen Medien und die mit ihnen verbundenen Phänomene werden oft die Schlagworte "Datenhighway", "Infoweb", "Informationsgesellschaft" oder "elektronischer Geschäftsverkehr" verwendet. Wurde als "**Electronic Commerce**" zunächst nur der strukturierte Datenaustausch zwischen Computersystemen angesehen, so versteht man heute darunter einen globalen Marktplatz, dem sämtliche wirtschaftliche Tätigkeiten und Transaktionen über interaktive Dienste bzw. Dienste der Informationsgesellschaft zugerechnet werden. Dabei handelt es sich um Informations- und Kommunikationsmöglichkeiten, die über elektronische Verarbeitungs- und Speichersysteme im Fernabsatz und auf individuellen Abruf erbracht werden, im wesentlichen also um das Internet sowie um sonstige **online-Dienste**. Durch die weltumspannende Vernetzung interaktiver und multimedialer Dienste können grenzüberschreitende wirtschaftliche Transaktionen in kürzester Zeit abgewickelt werden. Online-Dienste ermöglichen nicht nur die Anbahnung und Abwicklung von Geschäftstätigkeiten, sondern auch den direkten Bezug von Waren und Dienstleistungen.

Die **Einsatzbereiche der neuen Medien** beschränken sich nicht nur auf den elektronischen Handel, sondern erstrecken sich auf die verschiedensten Gebiete, von der Telearbeit angefangen über die Vernetzung des Hochschul-, Forschungs- und Gesundheitswesens bis hin zu spezifischen Anwendungen. Das Internet und andere Dienste der Informationsgesellschaft haben schon zu umfassenden Änderungen in Handel und Industrie ebenso wie im privaten Bereich geführt, und sie werden aller Voraussicht nach die Geschäfts- und Arbeitswelt sowie selbst die privaten Lebensverhältnisse großer Teile der Bevölkerung weiter tiefgreifend ändern.

Zu einer Veränderung traditioneller Verhaltensformen durch den vermehrten Einsatz elektronischer Kommunikation wird es insbesondere auch im Verhältnis zwischen den **Bürgern und der öffentlichen Hand** kommen. Durch die Bereitstellung aktueller Informationen kann die Situation des rat- oder hilfeschreitenden Bürgers verbessert werden. Ständig verfügbare interaktive Kanäle ermöglichen eine schnellere Kommunikation, die jederzeit in Anspruch genommen werden kann. Auch tragen die modernen Medien dazu bei, die Bearbeitungs- und Erledigungszeiten entscheidend zu verkürzen. Die Bundesregierung hat jüngst mit dem Projekt "Amtshelfer online" einen wesentlichen Anstoß zur Modernisierung der öffentlichen Verwaltung gegeben. In einzelnen Bereichen der Verwaltung ist der elektronische Rechtsverkehr bereits Realität, in anderen werden die erforderlichen Maßnahmen gerade vorbereitet.

Eine unerläßliche Voraussetzung des Einsatzes und des weiteren Erfolges elektronischer Medien im Rechts- und Geschäftsverkehrs bildet das **Vertrauen** der beteiligten Akteure, also der Anbieter und Kunden ebenso wie der öffentlichen Hand und ihrer Ansprechpartner, in die elektronischen Informations-, Kommunikations- und Lieferkanäle. Grundlage dieses Vertrauens in die elektronischen Netze und Instrumente ist zunächst die Sicherstellung der **Identität** der an den Kommunikationsabläufen bzw. den rechtlichen und wirtschaftlichen Transaktionen beteiligten Kommunikations- oder Geschäftspartner. Die neuen elektronischen Medien können ihre Vorteile in vielen, zum Teil außerordentlich sensiblen Bereichen erst dann voll entfalten, wenn die Anwender die Möglichkeit haben, sich über die Identität ihres Gegenübers verlässlich und rasch zu informieren. Weiters müssen sie sich darauf verlassen können, daß die elektronischen Daten auf dem Weg von und zu ihnen nicht verändert und verfälscht werden. Geeignete Technologien zur Gewährleistung der **Authentizität** (Echtheit) und der **Integrität** (Unverfälschtheit) elektronischer Daten stehen mit den **elektronischen Signaturen** zur Verfügung.

Die praktisch derzeit wichtigste Technologie ist die **digitale Signatur**. Sie beruht – vereinfacht gesagt – auf der Verschlüsselung einer für den Dokumenteninhalte repräsentativen Datenkombination. Dem Anwender werden von einer neutralen Einrichtung, der Zertifizierungsstelle, zwei entsprechende Datensätze, zwei “Schlüssel”, zugeordnet. Dieses Schlüsselpaar besteht aus einem privaten und einem dazu passenden öffentlichen Signaturschlüssel. Der private Schlüssel ist geheim und nicht einmal dem Anwender bekannt. Der öffentliche Schlüssel wird frei zugänglich gemacht, er dient der Überprüfung der elektronischen Signatur. Mit Hilfe mathematischer Verfahren wird auf dem Dokument ein unverfälschbarer “elektronischer Fingerabdruck” erzeugt, der mit dem auf einer Chipkarte gespeicherten privaten Schlüssel kodiert wird. Dem Empfänger wird das Dokument, der “Fingerabdruck” und die Signatur übermittelt. Die Identität des Anwenders wird durch das **Zertifikat** einer Zertifizierungsstelle bescheinigt. Der Empfänger kann mit dem durch das Zertifikat dem Absender zugeordneten öffentlichen Schlüssel die Signatur wieder entschlüsseln. Das Zertifikat kann entweder der Signatur angefügt sein oder elektronisch über ein Verzeichnis abgerufen werden. Stimmen die vom Empfänger ermittelten Werte mit dem “elektronischen Fingerabdruck” überein, so liegt ein positives Prüfergebnis vor.

Der Einsatz der digitalen Signatur und anderer Technologien wirft nun eine Reihe heikler Fragen auf, angefangen von der Zulässigkeit solcher Instrumente im Rechtsverkehr bis hin zur gegenseitigen Anerkennung von rechtlichen Regelungen.

2. Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen

Auf gemeinschaftsrechtlicher Ebene sind derzeit eine Reihe von Initiativen im Gang, die die Informations- und Kommunikationsdienste für die Wirtschaft nutzbar machen und die Weichen für die vollwertige Entwicklung des elektronischen Geschäftsverkehrs stellen sollen. Ein Hauptanliegen dieser Bemühungen besteht darin, **Rechtssicherheit** zu schaffen und für einen angemessenen **Kunden- und Verbraucherschutz** Sorge zu tragen.

Zu den spezifischen Fragen der elektronischen Signaturen präsentierte die Kommission im Mai 1998 den Vorschlag für eine **Richtlinie über gemeinsame Rahmenbedingungen für elektronische Signaturen** (ABl. Nr. C 325 vom 23. 10. 1998, S 5). Der Entwurf wurde im Rat unter österreichischem Vorsitz und daran anschließend auch unter deutscher Präsidentschaft intensiv diskutiert. Das Europäische Parlament nahm zu dem Vorschlag in Erster Lesung im Jänner 1999 Stellung (ABl. Nr. C 104 vom 14. 4. 1999, S 49). Das Parlament trat dabei auf der Grundlage des Berichtes des federführenden Ausschusses für Recht und Bürgerrechte insbesondere für eine Stärkung der Sicherheitsaspekte ein. Die Abänderungsanträge des Parlaments wurden im Zuge der weiteren Beratungen im Rat teilweise übernommen. Am 22. April 1999 erzielte der (Telekomminister-)Rat eine politische Einigung über einen **Gemeinsamen Standpunkt**.

Es kann realistischerweise davon ausgegangen werden, daß der Richtlinientext keine wesentlichen Änderungen erfahren wird, zumal – wie erwähnt – eine Reihe von Abänderungsanträgen des Parlaments bereits übernommen wurde und die Mitgliedstaaten den erzielten Kompromiß tragen. Daher kann die **Umsetzung** der Richtlinie schon frühzeitig in die Wege geleitet werden. Österreich wird damit als einer der ersten Mitgliedstaaten der Europäischen Union über ein Signaturgesetz verfügen, das mit den gemeinschaftsrechtlichen Vorgaben im Einklang steht. Regelungen, die vor dem Inkrafttreten der Richtlinie noch nicht innerstaatlich erlassen werden können, werden im Gesetz nach dem Inkrafttreten der Richtlinie einzufügen sein.

Den Kern der Richtlinie bildet deren Art. 5, der die **Rechtswirkungen** elektronischer Signaturen regelt. Dabei geht der Gemeinsame Standpunkt vom Prinzip aus, daß elektronische Signaturen im geschäftlichen Verkehr **nicht diskriminiert** und von den Mitgliedstaaten nicht verboten werden dürfen. Elektronisch signierte Dokumente dürfen von den nationalen Gerichten nicht allein deshalb als unbeachtlich qualifiziert werden, weil sie “nur” elektronisch vorliegen. Dieser Grundsatz der “Nichtdiskriminierung” (Art. 5 Abs. 2) gilt für alle elektronischen Signaturen, auch für solche, die nicht auf einem Zertifikat eines Zertifizierungsdiensteanbieters beruhen oder die die besonders hohen Anforderungen der Anhänge I, II und III nicht erfüllen. Für quantitativ große Bereiche des elektronischen Geschäftsverkehrs sorgt dieser Grundsatz der “Nichtdiskriminierung” für eine den Bedürfnissen des alltäglichen Verkehrs entsprechende Anerkennung elektronischer Signaturen.

Der Grundsatz der “Nichtdiskriminierung” sagt aber noch nichts darüber aus, unter welchen Voraussetzungen elektronische Signaturen den **eigenhändigen Unterschriften entsprechen**. Diese besondere Rechtswirkung wird in Art. 5 Abs. 1 geregelt: Eine solche Gleichstellung kommt nach dem Gemeinsamen Standpunkt nur dann in Betracht, wenn spezifische Sicherheitsstandards eingehalten

werden. Diese Standards werden in den Anhängen der Richtlinie näher definiert. Sowohl das einer "sicheren Signatur" zugrunde liegende qualifizierte Zertifikat als auch der Aussteller dieses Zertifikats und die verwendeten Signaturerstellungseinheiten (das sind etwa Chipkarten) müssen den in den Anhängen vorgesehenen hohen Anforderungen genügen.

Die Richtlinie regelt darüber hinaus aber noch weitere wichtige Aspekte elektronischer Signaturen: So dürfen die Mitgliedstaaten für die Aufnahme der Tätigkeit einer Zertifizierungsstelle **keine vorherige Genehmigung**, also keine Lizenz, vorsehen. Untersagt sind auch Maßnahmen gleicher Wirkung, wie etwa eine Vorlagepflicht mit Wartezeit oder eine Verpflichtung zum Abwarten einer Registrierung. Es ist jedoch zulässig, daß Akkreditierungssysteme eingerichtet werden, in deren Rahmen sich die Anbieter von Zertifizierungsdiensten einer – freiwilligen – Überprüfung unterziehen (Art. 3 Abs. 1 und 2).

Jeder Mitgliedstaat muß aber für ein geeignetes **Aufsichtssystem** zur Überwachung der in seinem Hoheitsgebiet niedergelassenen Zertifizierungsdiensteanbieter Sorge tragen (Art. 3 Abs. 3). Im Rahmen eines solchen Aufsichtssystems sind etwa Anzeigepflichten sowie regelmäßige Kontrollen zulässig. Weiters sind die Mitgliedstaaten verpflichtet, geeignete Stellen, die die Einhaltung der Sicherheitsanforderungen des Anhangs III durch (sichere) Signaturerstellungseinheiten bestätigen, gegenüber der Europäischen Kommission zu notifizieren (Art. 3 Abs. 4). Die Kriterien für solche Stellen werden nach Verabschiedung der Richtlinie im Rahmen eines Komitologieverfahrens von der Kommission in Zusammenarbeit mit den Mitgliedstaaten ausgearbeitet. Die Entscheidungen dieser Stellen müssen von allen übrigen Mitgliedstaaten anerkannt werden. Die Mitgliedstaaten haben also für die Erbringung vertrauenswürdiger Signatur- und Zertifizierungsdienste geeignete **Infrastrukturen** zu schaffen.

Der Gemeinsame Standpunkt enthält weiters eine Regelung über die **Haftung der Zertifizierungsdiensteanbieter** (Art. 6). Diese müssen schadenersatzrechtlich insbesondere für die Richtigkeit aller Informationen im qualifizierten Zertifikat zum Ausstellungszeitpunkt einstehen. Die Haftung der Zertifizierungsdiensteanbieter ist als Verschuldenshaftung mit Umkehr der Beweislast zu Lasten der Zertifizierungsdiensteanbieter ausgestaltet. Die Richtlinie sieht im Bereich der Haftung allerdings nur **Mindeststandards** vor. Die Mitgliedstaaten können also auch strengere Haftungsvorschriften vorsehen oder beibehalten.

Wie schon einleitend erwähnt, sind im elektronischen Geschäftsverkehr grenzüberschreitende Transaktionen alltäglich. Für den Bereich der elektronischen Signaturen ergibt sich aus diesem Charakteristikum ua. das Problem der **gegenseitigen Anerkennung** der jeweiligen nationalen rechtlichen Voraussetzungen. Der Gemeinsame Standpunkt bestimmt dazu, daß die – auf harmonisierten Rechtsgrundlagen beruhenden – qualifizierten Zertifikate innerhalb der Europäischen Union ohne weitere Voraussetzungen anerkannt werden müssen. Für die Anerkennung von qualifizierten Zertifikaten aus Drittstaaten werden dagegen besondere Voraussetzungen aufgestellt (Art. 7).

Im Interesse des **Datenschutzes** ist in Art. 8 vorgesehen, daß die Zertifizierungsdiensteanbieter personenbezogene Daten nur unmittelbar beim Betroffenen oder mit seiner ausdrücklichen Zustimmung und nur insoweit erheben dürfen, als dies zur Ausstellung und Aufrechterhaltung des Zertifikats erforderlich ist. Die Zertifizierungsdiensteanbieter dürfen nicht daran gehindert werden, Zertifikate unter einem Pseudonym auszustellen. Die Aufdeckung von Pseudonymen richtet sich nach den innerstaatlichen Rechtsvorschriften.

Für die Umsetzung der Richtlinie ist eine Frist von **18 Monaten** nach ihrem Inkrafttreten vorgesehen (Art. 13 Abs. 1).

3. Rechtslage in anderen Ländern, internationale Bestrebungen

In **Deutschland** steht seit 1. August 1997 das Signaturgesetz (Art. 3 des Informations- und Kommunikationsdienstegesetzes, BGBl. I 1997, S 1870) in Kraft. Auf seiner Grundlage wurde am 22. Oktober 1997 die Signaturverordnung erlassen. Beide Normenwerke regeln die Sicherheitsinfrastruktur, das zwingende Lizenzierungsverfahren für als sicher geltende digitale Signaturen sowie Datenschutzfragen. Ziel dieser legislativen Maßnahme ist die Schaffung eines geordneten Rahmens zur Erprobung der digitalen Signatur. Inhaltlich regelt das deutsche Signaturgesetz derzeit "nur" die technischen und organisatorischen Vorgaben für den gesetzlich geregelten Sicherheitsstandard der digitalen Signatur. Mit der digitalen Signatur werden hingegen keine rechtlichen Wirkungen, wie die Zurechnung elektronischer Willenserklärungen zu einem bestimmten Rechtssubjekt, besondere Beweiswirkungen oder die Einhaltung materiell-rechtlicher Formvorschriften, verknüpft. Das deutsche Signaturgesetz entspricht damit in seiner geltenden Fassung nicht in allen Belangen der geplanten Richtlinie.

Von den Mitgliedstaaten der Europäischen Union verfügt bisher außerdem nur **Italien** über ein Gesetz betreffend elektronische Dokumente und Schriftstücke.

In den **USA** haben mehrere Bundesstaaten jeweils eigene Signaturgesetze erlassen, ohne auf Fragen der Interoperabilität besonderes Augenmerk zu legen. Aus diesem Grund ist die amerikanische Bundesregierung bemüht, ein bundesweit einheitliches Signaturgesetz zu schaffen. Diese Bestrebungen stoßen jedoch nicht zuletzt auf kompetenzrechtliche Schwierigkeiten.

Japan verfügt derzeit noch über kein Signaturgesetz.

Auf Grund des globalen Charakters der neuen Medien empfehlen sich im Prinzip möglichst **globale Regelungen** zur Schaffung des notwendigen Ordnungsrahmens. Mit dem Themenbereich "elektronische Signaturen" beschäftigen sich insbesondere die UNCITRAL und die OECD. Im Rahmen der **UNCITRAL** wurde im Jahr 1996 von der Arbeitsgruppe "Electronic Commerce" ein Modellgesetz über rechtliche Aspekte des elektronischen Handels samt einem Wegweiser für die Umsetzung ausgearbeitet. Im Februar 1997 nahm diese Arbeitsgruppe die Arbeiten zu einem Modellgesetz für elektronische Signaturen auf. Diese Arbeiten sind jedoch noch nicht abgeschlossen. Im Rahmen der **OECD** fand unter anderem im Oktober 1998 in Ottawa eine Ministerkonferenz zum elektronischen Geschäftsverkehr statt, bei der auch eine Ministererklärung zur Authentizität verabschiedet wurde. In einem Follow up sollen weitere Maßnahmen zur Förderung eines rechtlichen Rahmens für elektronische Signaturen geprüft werden. Zu diesem Zweck wurde im März 1999 ein Fragebogen an die Vertragsstaaten ausgesandt.

Da die internationalen Regelungsbestrebungen vielfach keine konkreten Vorschriften vorsehen und zudem für die Staatengemeinschaft in der Regel nicht verbindlich sind, bestehen zu nationalen Rechtsvorschriften auf Grund gemeinschaftsrechtlicher Vorgaben **keine Alternativen**. Werden die europäischen Lösungsansätze von den Mitgliedstaaten gemeinsam in die Arbeiten auf internationaler Ebene eingebracht, so kann die europäische Position auch mit entsprechendem Gewicht vertreten werden.

4. Ziele, wesentliche Inhalte und Vorgeschichte des Entwurfs

Nach dem Gemeinsamen Standpunkt für eine Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen reicht es nicht aus, wenn in einem Signaturgesetz nur technische Standards für Verfahren, die zur Authentifizierung elektronischer Daten geeignet sind, vorgesehen werden. Vielmehr muß auch ein rechtlicher Rahmen für die vollwertige rechtliche Anerkennung elektronischer Signaturen im Sinn einer Gleichstellung ihrer Rechtswirkungen mit der eigenhändigen Unterschrift geschaffen werden. Derartige **besondere Rechtswirkungen**, die in der Zurechnung elektronischer Erklärungen zum Signator bzw. besonderen Beweiswirkungen und in der Einhaltung materiellrechtlicher Formvorschriften bestehen, können elektronischen Signaturen jedoch nur zuerkannt werden, wenn der Schutz vor Fälschung elektronischer Signaturen und Verfälschung elektronischer Dokumente in einem ausreichend hohen Maß gewährleistet ist.

Die Sicherheitsgarantien müssen – soweit dies möglich ist – bewirken, daß sich nicht ein anderer als der Signaturrechtliche (der Entwurf verwendet hier den Begriff Signator) als derjenige ausgeben kann, der das elektronische Dokument signiert hat. Ausreichende Sicherheitsanforderungen an das Signaturverfahren und die – auch beim Anwender – verwendeten Signaturprodukte stellen somit die Basis für die vollwertige rechtliche Anerkennung elektronischer Signaturen dar. Nur unter dieser Voraussetzung können die Nutzer und Anwender auf die elektronischen Interaktionen **vertrauen**, und nur auf einer solchen Basis kann auch die gegenseitige grenzüberschreitende Anerkennung der Signaturverfahren und damit ihre technische Interoperabilität angestrebt werden. Für die Zuerkennung besonderer Rechtswirkungen muß der nach dem Stand der Technik **höchste**, mit vertretbarem Aufwand durchführbare **Sicherheitsstandard** eingehalten werden. Dementsprechend sieht auch der Gemeinsame Standpunkt (Art. 5 Abs. 1) die Gleichstellung mit der eigenhändigen Unterschrift nur für **sichere elektronische Signaturen** vor.

Die vollwertige Anerkennung elektronischer Signaturen im Geschäftsverkehr und im Verkehr mit Behörden ist ein wesentliches Anliegen des Entwurfs. Darüber hinaus will er aber auch ein Mindestmaß an Rechtssicherheit für diejenigen Signaturen schaffen, die nicht die – in manchen Fällen unerläßlichen – hohen Sicherheitsanforderungen erfüllen. Vor allem sollen auch solche "einfache" Signaturen, die im elektronischen Verkehr die Regel sind, einer gewissen **Aufsicht** unterliegen, die Mißbräuche in diesem Bereich rasch und zuverlässig abstellt. Mit der Aufsicht soll die Telekom-Control-Kommission, die sich schon als Regulator im Telekommunikationswesen bewährt hat, betraut werden. Ihr soll in Anlehnung an die im Telekommunikationsgesetz vorgegebene Struktur die Telekom-Control GmbH zur Seite

gestellt werden. Daneben sind auf Grund der Richtlinie Einrichtungen zur Überprüfung der Sicherheitsanforderungen vorzusehen, die im Entwurf als "Bestätigungsstelle" bezeichnet werden.

Ein weiteres Schwergewicht des Entwurfs bildet die Regelung der Tätigkeit von **Zertifizierungsstellen**. Hier statuiert der Entwurf – abgestuft nach den Sicherheitserfordernissen – bestimmte Vorgaben, wobei – wiederum richtlinienkonform – keine besonderen Genehmigungen für die Aufnahme der Tätigkeit solcher Einrichtungen vorgesehen werden. Die Zertifizierungsstellen sollen privatwirtschaftlich auf dem Markt agieren, ihre Tätigkeit wird nur dort reguliert, wo dies im Einklang mit der Richtlinie erforderlich ist. Weiters regelt der Entwurf aber auch das **Verhältnis zwischen den Zertifizierungseinrichtungen und den Anwendern**. In erster Linie sind hier die Informations- und Beratungspflichten und die Haftungsregelungen zu nennen.

Letztlich wird aus der Richtlinie insbesondere auch das System der **Anerkennung** ausländischer Zertifikate übernommen.

An den **Verhandlungen zur Richtlinie** waren Vertreter des Bundesministeriums für Wissenschaft und Verkehr, des Bundesministeriums für Justiz und des Bundeskanzleramts (Verfassungsdienst und Büro für Konsumentenschutz) beteiligt. Der **vorliegende Entwurf** wurde vom Bundesministerium für Justiz in Abstimmung mit dem Verfassungsdienst vorbereitet und mit dem Verkehrsressort sowie Vertretern der Telekom-Control GmbH akkordiert. Den Vorbereitungen wurde als Sachverständiger Univ.-Prof. Dr. Reinhard Posch von der Technischen Universität Graz beigezogen.

5. Nicht verwirklichte Vorschläge

Im Begutachtungsverfahren ist von verschiedenen Stellen gefordert worden, nicht nur Regelungen für die Erstellung und Verwendung elektronischer Signaturen sowie die Erbringung von Zertifizierungsdiensten zu schaffen, sondern **weitere ergänzende Maßnahmen** zu treffen. Im besonderen gilt dies für die Vorschläge, die Identitätsfeststellung gemäß § 40 Abs. 1 BWG 1993 in Hinkunft auch unter Heranziehung der elektronischen Signatur zuzulassen und die Identitätsprüfungspflicht gemäß § 18a VAG beim Betrieb zur Lebensversicherung bei Verwendung einer elektronischen Signatur entfallen zu lassen, für den Wunsch, die strafrechtlichen Vorschriften über Urkunden auch auf elektronische Dokumente zu erstrecken, und für die Anregung, durch eine Ergänzung der Notariatsordnung die berufsrechtlichen Voraussetzungen für den Einsatz der elektronischen Signatur im Notariat zu schaffen. Weiters ist hier der Vorschlag zu nennen, einen **allgemeinen rechtlichen Rahmen** für die elektronische Signatur durch Änderungen "des Strafrechts, Verwaltungsrechts, Gerichtsorganisationsrechts, Bundesarchivgesetzes bzw. sonstiger Rechtsvorschriften" zeitgleich mit dem Signaturgesetz abzustecken. Der Entwurf will sich diesen Anregungen keineswegs verschließen. Die dazu erforderlichen umfangreichen weiteren Änderungen in der Rechtsordnung können aber wohl nur nach einer umfassenden Diskussion vorbereitet und verabschiedet werden. Diese Diskussion benötigt auf Grund der Schwierigkeiten im Detail längere Zeit, die auf Grund des im Begutachtungsverfahren weithin begrüßten Vorhabens, das Signaturgesetz noch in dieser Legislaturperiode zu verabschieden, nicht in ausreichendem Maß zur Verfügung steht. Dazu wird aber die nach Inkrafttreten der Richtlinie erforderliche Anpassung des Signaturgesetzes Gelegenheit bieten.

Von manchen Seiten ist weiters gefordert worden, zumindest einige Verhaltensweisen von Zertifizierungsdiensteanbietern nach dem Vorbild des Telekommunikationsgesetzes unter **Verwaltungsstrafdrohung** zu stellen. Auch davon sieht der Entwurf vorläufig ab, zumal er ein effektives Aufsichtssystem statuiert. Gegebenenfalls werden aber nach den Erfahrungen mit diesem Instrumentarium bei der erwähnten Novelle Verwaltungsstrafbestimmungen einzuführen sein.

6. Zuständigkeit

Die Verwendung und Anerkennung elektronischer Signaturen im elektronischen Geschäftsverkehr betrifft in erster Linie das Zivilrechtswesen (Art. 10 Abs. 1 Z 6 B-VG). Der Zugang zur Tätigkeit als Zertifizierungsdiensteanbieter zählt zu den Angelegenheiten des Gewerbes und der Industrie (Art. 10 Abs. 1 Z 8 B-VG). Die Kommunikation zwischen den Bürgern und der öffentlichen Hand betrifft – soweit sie nicht dem Zivilrechtswesen unterliegt – das Verwaltungsverfahren. Ein Bedarf zur Erlassung einheitlicher Vorschriften im Sinn des Art. 11 Abs. 2 B-VG ist gegeben. Darüber hinaus betrifft der Entwurf auch Belange des Post- und Fernmeldewesens (Art. 10 Abs. 1 Z 9 B-VG). Die **Kompetenz** zur Umsetzung der zugrunde liegenden Richtlinie steht daher jedenfalls **dem Bund** zu.

7. Kosten

Damit im elektronischen Rechts- und Geschäftsverkehr vertrauenswürdige Signatur- und Zertifizierungsdienste in Anspruch genommen werden können, muß eine geeignete **Infrastruktur** zur Verfügung stehen. Dementsprechend sind die Mitgliedstaaten der Europäischen Gemeinschaft nach dem Gemeinsamen Standpunkt verpflichtet, ein **funktionierendes Aufsichtssystem** über die Zertifizierungsdiensteanbieter einzurichten. Zudem müssen (eine oder mehrere) geeignete Stellen zur Beurteilung der Einhaltung der normierten Sicherheitsanforderungen für sichere Signaturerstellungseinheiten (technische Komponenten für sichere Signaturen) gegenüber der Europäischen Kommission benannt werden. Die Entscheidungen dieser sogenannten **„Bestätigungsstellen“** sind von allen anderen Mitgliedstaaten anzuerkennen.

Als **Aufsichtsstelle** ist – wie erwähnt – die Telekom-Control-Kommission vorgesehen. Zur Durchführung der operativen Aufsichtstätigkeit muß sich die nur sporadisch (in der Regel alle 14 Tage) tagende Kommission der ebenfalls nach dem TKG (§ 108) eingerichteten, nicht gewinnorientierten Telekom-Control GmbH bedienen können. Die Finanzierung der Aufsichtstätigkeiten, insbesondere der operativen Tätigkeit der Telekom-Control GmbH, muß über den Markt, also durch die Zertifizierungsdiensteanbieter erfolgen, sodaß daraus **keine dauerhafte zusätzliche Belastung** der öffentlichen Hand entstehen wird.

Die Finanzierung könnte – nach dem Vorbild des Telekommunikationsgesetzes – durch regelmäßige Beiträge der Zertifizierungsdiensteanbieter in Abhängigkeit von ihrem Umsatz erfolgen. Insbesondere aus Gründen der Transparenz und der Kostenwahrheit erscheint es aber zweckmäßiger, die von der Aufsichtsstelle sowie der Telekom-Control GmbH erbrachten Leistungen über ein hierfür im Einzelfall zu **zahlendes, kostendeckendes Entgelt zu finanzieren**. Die nähere Festlegung dieser Entgelte ist der Signaturverordnung vorbehalten.

Die Aufgaben der Telekom-Control-Kommission und -GmbH im Rahmen der Regulierung des Telekomwesens sind von den Aufgaben nach diesem Bundesgesetz **finanziell und organisatorisch zu trennen**.

Als **„Bestätigungsstellen“** sollen nach dem Entwurf geeignete und mit Verordnung anerkannte Einrichtungen fungieren. Die Schaffung einer öffentlich-rechtlichen Einrichtung, etwa eines Amtes oder einer Anstalt, erscheint derzeit aus Kosten-Nutzen-Erwägungen nicht sinnvoll. Dennoch muß die öffentliche Hand dafür Sorge tragen, daß eine vertrauenswürdige und fachlich kompetente Stelle auch im Inland zur Wahrnehmung der sensiblen Aufgaben einer **„Bestätigungsstelle“** zur Verfügung steht. Daher wurde ein Verein **„Zentrum für sichere Informationstechnologie – Austria (A-SIT)“** eingerichtet, der ua. aus dem Bundeshaushalt finanziert wird und neben den Aufgaben einer **„Bestätigungsstelle“** auch folgende Agenden wahrnimmt:

- **Evaluationsmanagement**, das heißt Evaluierung sicherheitsrelevanter Infrastrukturen, insbesondere Evaluierung technischer Prüfergebnisse für sichere Signaturprodukte und Bestätigung der Einhaltung der vorgeschriebenen Sicherheitsanforderungen durch die fraglichen Produkte,
- **Ansprech- und Koordinationsstelle** für Belange der Sicherheit in der Informationstechnik und Beratung öffentlicher Institutionen,
- **öffentliche Bewußtseinsbildung** betreffend die Verwendung sicherer Informationstechnik,
- **Technologiebeobachtung** sowie Wahrung strikter und nachweislicher Objektivität und Unabhängigkeit insbesondere in den Bereichen elektronische Signaturen, Gesundheitswesen, öffentliche Sicherheit, Finanzwesen, Behördenkommunikation und Datenschutz,
- **technische Hilfestellung** für öffentliche Einrichtungen und Betreibern von Informationsdiensten,
- Förderung und Durchführung von Forschungsprojekten und
- Koordination mit dem internationalen Normenwesen.

Als **Mitglieder dieses Vereins** fungieren derzeit das Bundesministerium für Finanzen, die Oesterreichische Nationalbank und die Technische Universität Graz.

Nach den derzeit vorliegenden Schätzungen wäre für das restliche Jahr 1999 für die Tätigkeit des A-SIT an Bundesmitteln insgesamt ein Betrag von 8 Millionen Schilling in Anschlag zu bringen. Aus konkreten Projektaufträgen der öffentlichen Hand und privater Auftraggeber soll ebenfalls ein Betrag zur Kostendeckung des Vereins geleistet werden. Insgesamt gesehen wird die Mitwirkung des A-SIT bei der Vollziehung dieses Bundesgesetzes also nur **geringfügige Belastungen** des Budgets des Bundes nach sich ziehen.

8. Besonderheiten des Normerzeugungsverfahrens

Es bestehen **keine besonderen Beschlußerfordernisse** im Nationalrat und auch keine Abweichungen bei der Mitwirkung des Bundesrats.

Die Haushalte der Länder und der Gemeinden werden durch das Vorhaben **nicht belastet**.

Der Entwurf ist **nicht** der Europäischen Kommission **zu notifizieren**, zumal die Bestimmungen der Richtlinie 98/34/EG idF der Richtlinie 98/48/EG über Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft noch nicht anzuwenden sind.

9. Auswirkungen auf die Beschäftigung und den Wirtschaftsstandort Österreich

Das Signaturgesetz wird **positive Effekte** auf die Beschäftigung und den Wirtschaftsstandort Österreich haben, weil damit die Rechtsgrundlagen für einen neuen Dienstleistungssektor geschaffen werden. Mehrere österreichische Unternehmen und Einrichtungen (etwa Internet-Service-Provider und Kreditinstitute) haben schon ihr Interesse an diesem Betätigungsfeld dargelegt. Von der Datakom Austria GmbH werden solche Dienste – in einem Feldversuch – bereits angeboten. Die derzeit bestehenden Rechtsunsicherheiten sind vielfach als größtes Hindernis für die doch hohen Investitionen – die geschätzten Kosten für die Einrichtung einer Zertifizierungsstelle für sichere elektronische Signaturen belaufen sich auf 40 bis 60 Millionen Schilling – bezeichnet worden. Mit der Schaffung der technischen Vorgaben und der rechtlichen Rahmenbedingungen können Fehlentwicklungsrisiken ausgeschlossen werden.

Auch auf die **Beschäftigung** werden sich die Signatur- und Zertifizierungsdienste **positiv** auswirken. Selbst wenn durch den vermehrten Einsatz der neuen Medien gesellschaftliche, soziale und kulturelle Umstrukturierungen zu erwarten sind, werden mit der Entwicklung hin zur Informationsgesellschaft doch neue Märkte und neue Berufe entstehen. Nach Schätzungen der Europäischen Kommission könnten im Zusammenhang mit dem elektronischen Geschäftsverkehr in den nächsten Jahren in der Europäischen Gemeinschaft 500 000 neue Arbeitsplätze geschaffen werden. Dieses Potential gilt es auch für Österreich zu nutzen.

10. EU-Konformität

Das Vorhaben dient der Umsetzung der Richtlinie über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen. Ausgehend von dieser Richtlinie werden für das Anbieten und die Verwendung vor allem sicherer elektronischer Signaturen die notwendigen Infrastrukturen, die organisatorischen und technischen Vorgaben sowie die rechtlichen Rahmenbedingungen geschaffen. Österreich wird einer der ersten Mitgliedstaaten der Europäischen Union sein, der über ein mit den gemeinschaftsrechtlichen Vorgaben im Einklang stehendes Signaturgesetz verfügt. Das Vorhaben ist in allen Belangen **europarechtskonform**.

Besonderer Teil

Vorbemerkung: In der Folge wird mit dem Ausdruck "Richtlinie" der (in der Sprachfassung revidierte) Gemeinsame Standpunkt des Rates im Hinblick auf den Erlaß der Richtlinie des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen bezeichnet.

Zu § 1 des Entwurfs:

1. So wie die Richtlinie hat auch das Signaturgesetz zum Ziel, **rechtliche Rahmenbedingungen** für die Bereitstellung und die Verwendung elektronischer Signaturen festzulegen und die Voraussetzungen für deren vollwertige rechtliche Anerkennung zu schaffen. Die Normierung insbesondere der organisatorischen und technischen Vorgaben für die Bereitstellung von Signatur- und Zertifizierungsdiensten ermöglicht es den potentiellen Zertifizierungsdiensteanbietern, die erforderlichen Investitionen zu tätigen und ihre wirtschaftliche Aktivitäten auf gesetzlich gesicherter Basis auszuführen.

Das Vorhaben legt vor allem die Bedingungen für elektronische Signaturen, die nach dem jeweiligen Stand der Technik als **sicher** anzusehen sind, fest. Solche Signaturen bieten Gewähr, daß sie nicht unerkannt **gefälscht** und signierte Daten nicht unerkannt **verfälscht** werden können. Unter Verfälschung ist dabei jede Art der Veränderung der signierten Daten, auch in Folge technischer Fehler, zu verstehen. In Übereinstimmung mit der Richtlinie werden mit solchen elektronischen Signaturen **besondere Rechtswirkungen** im Sinne einer Gleichstellung mit der **eigenhändigen Unterschrift**

verknüpft. Damit wird eine gesetzliche Grundlage für den sicheren online-Datenaustausch im Rechts- und Geschäftsverkehr über **offene** elektronische Netzwerke geschaffen.

In der Praxis werden elektronische Signaturverfahren in großer Zahl und mit unterschiedlicher Sicherheit angeboten. Das Signaturgesetz will diese Vielfalt in keiner Weise einschränken. Daher wird in § 3 im Sinne einer – gemeinschaftskonformen – Nichtdiskriminierungsklausel angeordnet, daß **sämtliche elektronischen Signaturverfahren** grundsätzlich (vgl. Abs. 2) im Rechts- und Geschäftsverkehr verwendet werden dürfen (siehe näher § 3 und die Erläuterungen dazu).

2. § 1 Abs. 2 sieht vor, daß das Signaturgesetz auch in sogenannten **“geschlossenen Systemen”** anzuwenden ist, sofern dies von den Teilnehmern vereinbart wird. Dabei handelt es sich um Systeme, in denen die angebotenen elektronischen Dienste einem eingeschränkten Personenkreis zur Verfügung stehen. Musterbeispiel sind die von Kreditinstituten angebotenen elektronischen Netze. Hier können die Art der elektronischen Kommunikation bzw. die Verwendung und die Art elektronischer Signaturen – im Rahmen der sonst bestehenden Schranken, etwa nach den Bestimmungen des Konsumentenschutzgesetzes – frei vereinbart werden. Dementsprechend führt die Richtlinie in Erwägungsgrund 16 aus, daß elektronische Signaturen, die in geschlossenen Systemen verwendet werden, keine rechtliche Regelungen benötigen. Allerdings sollten auch solche elektronische Signaturen, die den Anforderungen der Richtlinie entsprechen, rechtlich anerkannt werden. Die Teilnehmer an einem geschlossenen System können also entscheiden, ob sie sich dem Signaturgesetz – mit den entsprechenden Folgen (zB besondere Rechtswirkungen, Aufsichtssystem) – unterwerfen wollen oder nicht.

Weiters soll das Signaturgesetz grundsätzlich auch im **öffentlichen Bereich** gelten, also vor allem für die elektronische Kommunikation in und mit der Verwaltung. Die in den jeweils anwendbaren gesetzlichen Vorschriften normierten Bedingungen müssen jedoch eingehalten sein. Die Richtlinie sieht in Art. 3 Abs. 4 vor, daß die Mitgliedstaaten den Einsatz elektronischer Signaturen im öffentlichen Bereich zusätzlichen Anforderungen unterwerfen können. Demnach können im öffentlichen Bereich über die Bestimmungen des Signaturgesetzes hinausgehende Anforderungen an das Signaturverfahren gestellt werden. Die Bestimmungen etwa des AVG (§ 13) oder des GOG (§§ 89a ff) sind also zu beachten. Im Sinn der Bürgernähe (Stichwort “multifunktionale Chipkarten”) sollte nach Möglichkeit aber danach getrachtet werden, auch im öffentlichen Bereich mit den sicheren elektronischen Signaturen im Sinn des Signaturgesetzes das Auslangen zu finden.

Die Bestimmung des § 1 Abs. 2 bedeutet nicht, daß im öffentlichen Bereich die technische Ausstattung zum Austausch signierter Erklärungen vorhanden sein muß. Voraussetzung für die Verwendung elektronischer Signaturen ist, daß die elektronische Kommunikation mit neuen Medien über offene Netzwerke überhaupt zugelassen wird (vgl. § 3 Abs. 1 und die Erläuterungen dazu).

Zu § 2 des Entwurfs:

Die Begriffsbestimmungen entsprechen den in der Richtlinie vorgesehenen Definitionen. Zum Teil werden sprachliche Anpassungen oder Klarstellungen vorgenommen.

Z 1 bringt den **technologieneutralen** Ansatz der Richtlinie zum Ausdruck. Um den Geltungsbereich der Regelungen nicht auf eine bestimmte Signaturmethode einzuschränken, wird allgemein von elektronischen Signaturen gesprochen. Die Definition einer **elektronischen Signatur** wird dabei sehr weit gefaßt. Darunter ist jedes technische Verfahren zur Authentifizierung elektronischer Daten, also der Feststellung der **Identität** des Ausstellers einer Nachricht (Echtheit), zu verstehen. Mit dem Begriff “elektronische Signatur” werden jedoch noch keine konkreten technischen Leistungs- bzw. Qualitätsmerkmale verknüpft.

Z 2 beschreibt den **berechtigten Inhaber** der Signaturerstellungsdaten, also – bei der digitalen Signatur – des privaten Signaturschlüssels. Der Entwurf verwendet hier – in Anlehnung an die englischsprachige Fassung der Richtlinie – den Ausdruck **Signator**. Damit wird die Ähnlichkeit der elektronischen Signatur mit der Beifügung eines Siegels herausgestrichen. Dem Signator sind die Signaturprüfdaten (öffentlicher Signaturschlüssel) und damit zwangsläufig auch die Signaturerstellungsdaten (privater Signaturschlüssel) zugeordnet.

Die Richtlinie überläßt es den Mitgliedstaaten, ob sie – entsprechend der innerstaatlichen Rechtssystematik – Signaturerstellungsdaten nur natürlichen Personen oder auch juristischen Personen zuordnen. Der Entwurf sieht vor, daß Signaturdaten (Signaturschlüssel) nur **natürlichen Personen** zugeordnet werden können, zumal auch die Vertretungsmacht für juristische Personen letztlich an natürliche Personen gebunden ist. In ein Zertifikat können aber Angaben über die Vertretungsmacht für eine dritte

Person (vgl. § 5 Abs. 1 Z 4) aufgenommen werden. In einem solchen Fall kann der Signator auch für einen anderen Rechtsträger elektronisch signierte Erklärungen abgeben.

Aus Gründen der Praktikabilität werden bei **“Zertifikaten für Zertifizierungsdiensteanbieter”** ausnahmsweise auch juristische Personen – oder andere Rechtsträger, wie etwa Personenhandelsgesellschaften – als Signatoren zugelassen. Ein solches Zertifikat darf nur zum Signieren von Anwender-Zertifikaten oder zur Erbringung anderer Zertifizierungsdienste verwendet werden (vgl. § 6 Abs. 7). Dadurch wird verhindert, daß der Bestand eines Zertifikats für Zertifizierungsdiensteanbieter vom aufrechten Organschafts- oder Vollmachtsverhältnis der handlungsbefugten Person abhängt. Dies gilt auch für die Aufsichtsstelle. Im rechtsgeschäftlichen und behördlichen Bereich kann eine elektronische Signatur als Ersatz der eigenhändigen Unterschrift jedoch nur natürlichen Personen zugeordnet werden. Dies schließt freilich nicht aus, daß etwa in einem geschlossenen System ein Zertifikat auf eine juristische Person ausgestellt wird. In diesem Fall kann das Signaturgesetz aber nicht zur Anwendung gelangen.

Z 3 definiert den Kernbereich des Signaturgesetzes, nämlich die **sichere elektronische Signatur**. Dabei handelt es sich um eine elektronische Signatur, die den in der Richtlinie vorgesehenen Qualitätsmerkmalen und Sicherheitsanforderungen entspricht. Nach der Richtlinie ergeben sich die Kriterien für eine **sichere** elektronische Signatur aus Art. 5 Abs. 1. Dabei muß es sich um eine fortgeschrittene elektronische Signatur, die auf einem qualifizierten Zertifikat beruht und unter Verwendung einer sicheren Signaturerstellungseinheit erstellt wurde, handeln. Der Entwurf faßt diese Elemente zur Vereinfachung zu einem Begriff zusammen.

Die Merkmale für eine sogenannte **“fortgeschrittene elektronische Signatur”** finden sich in Art. 2 Z 2 der Richtlinie. Hiebei handelt es sich um die in den **lit. a bis d** der Z 3 aufgezählten Kriterien. **“Ausschließlich dem Signator zugeordnet” (lit. a)** bedeutet, daß über dieselben Signaturerstellungsdaten (etwa denselben privaten Signaturschlüssel) nicht mehrere Personen (berechtigt) verfügen dürfen. Bestimmte Signaturerstellungsdaten (etwa ein bestimmter privater Signaturschlüssel) und ebenso die entsprechenden (komplementären) Signaturprüfdaten (der öffentliche Signaturschlüssel) dürfen also – jedenfalls innerhalb eines Zertifizierungsdiensteanbieters – nur ein einziges Mal vorkommen. In **lit. b** wird die Funktion der **Authentizität** zum Ausdruck gebracht. Eine fortgeschrittene elektronische Signatur muß darüber Auskunft geben können, von wem die signierten, elektronisch übermittelten Daten stammen, wem sie zugeordnet sind. Sie müssen also die **Identität** des Signators feststellbar machen. Dazu müssen folgende Bedingungen erfüllt sein: Es muß praktisch unmöglich sein, daß ein Schlüsselpaar (versehentlich oder absichtlich) doppelt erzeugt wird. Weiters muß sichergestellt sein, daß eine mit einem öffentlichen Schlüssel prüfbare Signatur nur unter Einsatz des zugehörigen privaten Schlüssels erzeugt worden ist. Und vor allem muß es praktisch ausgeschlossen sein, daß der private Schlüssel aus dem öffentlichen berechnet bzw. abgeleitet wird. Geht man davon aus, daß der Signator die Signaturerstellungsdaten verwendet, so kann eine solche Signatur die **Echtheit** der Erklärung garantieren. **Lit. d** beschreibt die Funktion der sogenannten **Integrität**. Mit Hilfe fortgeschrittener elektronischer Signaturen kann zuverlässig erkannt werden, ob elektronisch signierte Daten unversehrt, das heißt inhaltlich unverfälscht sind. Zur Erreichung dieser Vorgabe muß es praktisch ausgeschlossen sein, daß verschiedene elektronische Daten mit derselben Signatur oder elektronische Daten zu einer vorgegebenen Signatur existieren. Nach **lit. c** muß der Signator seine Signaturerstellungsdaten (etwa private Signaturschlüssel) vor unbefugtem Zugriff schützen können. Die Signaturfunktion soll nur vom Berechtigten ausgelöst werden können. Ein solcher Schutz kann technisch in Form eines Paßwortes oder einer PIN (Personenidentifikationsnummer) vorgesehen werden. In Zukunft werden auch biometrische Merkmale (Fingerabdrücke, Körperfrequenzmesser, auch elektronische Schreibstifte oder Stimmerkennungsverfahren) zur Identifikation des Signators gegenüber seinem privaten Signaturschlüssel eingesetzt werden können. In diesem Zusammenhang wird gelegentlich auch von der Bindung des privaten Signaturschlüssels durch Besitz (zB Chipkarte) und Wissen (zB Paßwort oder PIN) an den Signator gesprochen.

Lit. e verbindet die fortgeschrittene elektronische Signatur mit den weiteren in Art. 5 Abs. 1 der Richtlinie vorgesehenen Anforderungen. Damit eine **“fortgeschrittene”** Signatur zur **“sicheren”** Signatur werden kann, muß sie auf einem **qualifizierten Zertifikat** (Anhang I und II zur Richtlinie; siehe weiter Z 9 und die Erläuterungen dazu) beruhen. Weiters muß sie unter Verwendung **sicherer Signaturerstellungseinheiten** im Sinn des Anhangs III der Richtlinie erstellt werden. Diese Sicherheitsanforderungen werden in § 18 umgesetzt.

Eine sichere Signatur ist also – richtlinienkonform – eine (im Sinn der Richtlinie) fortgeschrittene elektronische Signatur, bei der die Anforderungen der Anhänge I, II und III der Richtlinie eingehalten

sind. Nach Art. 5 Abs. 1 der Richtlinie sind nur mit einer solchen elektronischen Signatur **besondere Rechtswirkungen** zu verbinden. Nach heutigem Stand der Technik sind nur digitale Signaturen in der Lage, die Anforderungen an sichere elektronische Signaturen zu erfüllen.

In **Z 4** werden die **Signaturerstellungsdaten** und in **Z 5** die **Signaturerstellungseinheiten** entsprechend der Richtlinie (Art. 2 Z 4 bzw. Z 5) definiert. Die Sicherheitsanforderungen des **Anhangs III** sind funktional, das heißt in Beziehung auf eine Kombination von Hardware- und Softwarekomponenten zu sehen. Sie decken aber nicht die gesamte Systemumgebung, in der eine Einheit betrieben wird, ab.

In **Z 6** werden die **Signaturprüfdaten** und in **Z 7** die **Signaturprüfeinheiten** entsprechend der Richtlinie (Art. 2 Z 7 bzw. Z 8) definiert. Anhand der Signaturprüfdaten – bei digitalen Signaturen ist dies der öffentliche Signaturschlüssel – kann vom Empfänger einer elektronischen Signatur nachgeprüft werden, ob die signierten Daten vom Signator stammen. Für die Vornahme einer sicheren Signaturprüfung enthält Anhang IV der Richtlinie Empfehlungen für Sicherheitsanforderungen an den Signaturprüfvorgang. Die Zertifizierungsdiensteanbieter sollen ermutigt werden, sichere Signaturprüfkomponenten bereitzustellen.

Digitale Signaturen sind in der Regel an die Voraussetzung gebunden, daß sie mit einem privaten Signaturschlüssel erstellt werden, für den ein komplementärer öffentlicher Schlüssel besteht, der dem Signator durch einen Zertifizierungsdiensteanbieter zugeordnet ist. Damit eine digitale Signatur den Signator erkennen läßt, muß also ein **Zertifikat (Z 8)** vorliegen, dem insbesondere der öffentliche Schlüssel einer bestimmten Person entnommen werden kann. Das Zertifikat muß entweder (automatisch) mit der Signatur an den Empfänger mitübermittelt werden oder für diesen – in der Regel online – abrufbar sein. Mit der Zuordnung des öffentlichen Signaturschlüssels zu einer Person ist zwangsläufig das gesamte Schlüsselpaar, also auch der private Signaturschlüssel, zugeordnet.

In **Z 9** wird eine der Voraussetzungen für eine sichere elektronische Signatur, nämlich das **qualifizierte Zertifikat** definiert. Ein qualifiziertes Zertifikat muß zunächst einen gewissen Mindestinhalt aufweisen, der sich aus Anhang I zur Richtlinie bzw. aus der korrespondierenden Bestimmung des § 5 Abs. 1 ergibt. Dabei handelt es sich im wesentlichen um die Bezeichnung des Zertifizierungsdiensteanbieters, den (unverwechselbaren) Namen des Signators, die Gültigkeitsdauer des Zertifikats sowie allfällige Beschränkungen des Anwendungsbereichs des Zertifikats (zB für bestimmte Verträge) und gegebenenfalls den Transaktionswert, bis zu dem das Zertifikat gilt. Die – mit der Z 9 übernommene – Definition des Art. 2 Z 10 der Richtlinie verknüpft den Begriff des qualifizierten Zertifikats zudem mit Anhang II zur Richtlinie. Dies bedeutet, daß ein qualifiziertes Zertifikat nur von einem Zertifizierungsdiensteanbieter ausgestellt werden darf, der den organisatorischen, personellen und technischen Anforderungen des Anhangs II der Richtlinie entspricht. Diese Anforderungen werden in § 7 Abs. 1 bis 3 umgesetzt. Nach diesen Anforderungen müssen solche Zertifizierungsdiensteanbieter insbesondere die erforderliche Zuverlässigkeit aufweisen und die Einhaltung der maßgeblichen Rechtsvorschriften gewährleisten, weiters über qualifiziertes Personal und ausreichende Finanzmittel verfügen sowie für eine verlässliche Identitätsprüfung und eine ausreichende Belehrung der Anwender sorgen. Sie müssen auch über zuverlässige technische Systeme und Signaturprodukte verfügen, sichere Verzeichnis- und Widerrufsdienste führen sowie Vorkehrungen für die Verhinderung der Zertifikatsfälschung treffen.

Z 10 beschreibt die **Zertifizierungsdiensteanbieter**, die durch die ihnen zukommenden Aufgaben charakterisiert sind. Sie zählen zur notwendigen Infrastruktur für die Bereitstellung von Signatur- und Zertifizierungsdiensten. Der Aufbau und der Betrieb der Zertifizierungsdiensteanbieter sollen privatwirtschaftlich im freien Wettbewerb, jedoch unter staatlicher Aufsicht erfolgen. Nur im Wege der Zertifizierungsdiensteanbieter kann sichergestellt werden, daß die vorgeschriebenen Sicherheitsmaßnahmen eingehalten und die Signatoren über die von ihnen in ihrem eigenen Interesse zu veranlassenden Maßnahmen entsprechend belehrt sind.

Die Tätigkeit eines Zertifizierungsdiensteanbieters kann jede Person oder sonstige rechtsfähige Einrichtung, die über das entsprechende Know-how und die erforderlichen technischen und finanziellen Mittel verfügt, ausüben. Die Anzahl der Zertifizierungsdiensteanbieter wird **nicht beschränkt**.

Primäre Aufgabe der Zertifizierungsdiensteanbieter wird in der Regel die Ausstellung und Verwaltung von Zertifikaten, also die Zuordnung öffentlicher Schlüssel zu einer Person, sein. Für die Bereitstellung elektronischer Signaturen, insbesondere für sichere Signaturen, sind aber noch eine Reihe anderer **Dienste** notwendig. Neben der Ausstellung, Erneuerung und Verwaltung von Zertifikaten stellen vor allem Verzeichnis- und Widerrufsdienste weitere Zertifizierungsdienste dar. Dazu gehören weiters aber auch Registrierungs- und Zeitstempeldienste. Signaturdienste sind darüber hinaus auch

Signaturverfahren und damit im Zusammenhang stehende Signaturprodukte, die von einem Zertifizierungsdiensteanbieter bereitgestellt werden. Die wesentlichen, in Betracht kommenden Signatur- und Zertifizierungsdienste werden in **Z 11** angeführt. Der Katalog entspricht jenem des Erwägungsgrundes 9 der Richtlinie. Ein Zertifizierungsdiensteanbieter kann auch nur einen der erwähnten Dienste betreiben. So ist es etwa denkbar, daß Zeitstempel- oder Registrierungsdienste, aber auch Widerrufsdienste ausgegliedert betrieben werden.

Beschafft sich ein Anwender Signaturprodukte (zB eine Chipkarte) etwa bei einem **Hard- und Softwarehändler**, der selbst keine Signaturverfahren bzw. Zertifizierungsdienste bereitstellt, so handelt es sich bei einem solchen Unternehmen nicht um einen Zertifizierungsdiensteanbieter.

Zu § 3 des Entwurfs:

1. § 3 Abs. 1 macht deutlich, daß die Zertifizierungsdiensteanbieter **jede Art von Signaturverfahren** anbieten können. Die Anwendung von Signaturverfahren, die nicht den Anforderungen dieses Gesetzes entsprechen, ist also freigestellt. Die Zertifizierungsdiensteanbieter können damit auch unterschiedliche Zertifikatsklassen (zB Light, Medium, Strong und Premium der Datakom) oder unterschiedliche Sicherheitsstufen (zB kein Zertifikat, einfaches Zertifikat, qualifiziertes Zertifikat, sichere Signaturen) anbieten.

In welchen Bereichen sichere elektronische Signaturen verwendet werden müssen bzw. in welchen Fällen nur sicher signierte Erklärungen **Rechtswirkungen** entfachen können, ergibt sich entweder aus speziellen Rechtsvorschriften (zB bei der Kommunikation mit der öffentlichen Verwaltung) oder – für den zivilrechtlichen Bereich – aus **§ 4**, allenfalls auch aus einer Parteienvereinbarung (siehe auch die Ausführungen zu den §§ 1 und 4).

Im **elektronischen Geschäftsverkehr** bestehen derzeit keine gesetzlichen Beschränkungen für die Verwendung elektronischer Signaturen, auch sind solche nicht geplant. Für den formgebundenen Bereich, in dem – etwa für Verträge, Rechtsgeschäfte oder andere rechtlich erhebliche Erklärungen (Willenserklärungen) – das Erfordernis der Schriftlichkeit vorgeschrieben ist, bedeutet der Grundsatz der Zulässigkeit freilich noch nicht, daß die elektronische Signatur Rechtswirkungen entfaltet, eine signierte Erklärung also wirksam ist (siehe näher die Erläuterungen zu § 4).

Elektronische Signaturen sind das Ergebnis technischer Verfahren, die im elektronischen Bereich einen Ersatz für die Unterschrift darstellen sollen. Die Frage nach der Wirksamkeit **elektronischer Signaturen** betrifft somit ausschließlich das Problem, ob die elektronische Signatur eine “normale” Unterschrift ersetzen kann. Davon ist die Frage der Zulässigkeit **elektronischer Kommunikation** an sich zu unterscheiden. Hier geht es etwa um die Annahme bzw. den nachweislichen **Zugang** einer (signierten) elektronischen Erklärung beim Empfänger. Damit im Zusammenhang stehen die Fragen, ob der Empfänger eine Signaturprüfung vornimmt, welche Geräte und Produkte er dafür einsetzt und welches Format er verwendet. Alle diese Problembereiche (rechtliche Aspekte des Zugangs und des Empfangs einer Erklärung oder der Verantwortlichkeit für das Vorliegen der technischen Ausstattung) sind nicht Gegenstand des Signaturgesetzes, sie sind in allgemeinem Zusammenhang (etwa im Rahmen der Umsetzung der in Ausarbeitung befindlichen Richtlinie über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt) zu regeln. Das Signaturgesetz beschäftigt sich nur mit der **Signaturerstellung**, also mit der Zuordnung einer elektronischen Signatur zum Sender.

Damit elektronisch signierte Dokumente überhaupt ausgetauscht werden können, muß zwischen den Beteiligten eine **elektronische Kommunikation** möglich sein. Sie müssen zumindest über einen Computer mit Anschluß zum entsprechenden Netzwerk, also über die erforderliche technische Ausstattung, verfügen.

Die Zulässigkeit elektronischer Kommunikation – zumindest im rechtsgeschäftlichen Verkehr – wird grundsätzlich an eine **Vereinbarung** zwischen den Beteiligten zu knüpfen sein. Die bloße Einrichtung einer e-mail-Adresse wird hierfür noch nicht ausreichen. Bei Verwendung unlesbarer Formate wird vom Vorliegen einer wirksamen Erklärung nicht ausgegangen werden können. Im **rechtsgeschäftlichen Bereich** haben die Vertragsparteien im Sinn der Privatautonomie die Möglichkeit, die elektronische Kommunikation an sich und damit im Zusammenhang die Verwendung elektronischer Signaturen **auszuschließen**.

2. § 3 Abs. 2 normiert die in Art. 5 Abs. 2 der Richtlinie vorgesehene **“Nichtdiskriminierungsklausel”** für jede Art elektronischer Signaturen, also auch für solche, die nicht den Anforderungen der Anhänge I bis III zur Richtlinie entsprechen und somit nicht als sicher im Sinn des § 2 Z 3 anzusehen sind (“einfache Signaturen”). Auch elektronische Signaturen, die auf keinem oder auf einem “einfachen”

Zertifikat beruhen, dürfen somit im rechtsgeschäftlichen Verkehr nicht verboten werden. Elektronisch signierte Dokumente dürfen von einem Gericht nicht allein deshalb als rechtlich unbeachtlich qualifiziert werden, weil sie in elektronischer Form vorliegen. Zudem müssen elektronisch signierte Dokumente sowohl im gerichtlichen als auch im behördlichen Verfahren als Beweismittel verwendet werden können.

Im **nicht formgebundenen Bereich** (vgl. § 4) ist die Verwendung elektronischer Signaturen im (rechts)geschäftlichen Verkehr grundsätzlich (sofern die Vertragspartner nicht etwas anderes vereinbart haben und über die erforderliche technische Ausstattung verfügen) **zulässig**. In den für den elektronischen Geschäftsverkehr hauptsächlich in Betracht kommenden Anwendungsbereichen spielen (gesetzliche) Schriftformerfordernisse nur eine untergeordnete Rolle. Die üblicherweise über Informations- und Kommunikationsdienste angebahnten und abgewickelten Geschäfte und Transaktionen sind in der Regel nicht an die Verwendung sicherer elektronischer Signaturen geknüpft. Insbesondere wird bei Transaktionen mit geringem wirtschaftlichen Wert oder bei Massentransaktionen mit einfachen, keine besonderen Sicherheitsanforderungen erfüllenden Signaturverfahren durchaus das Auslangen gefunden werden können, weil sich die Geschäftspartner in diesen Fällen in der Regel damit begnügen, daß sie "mit einiger Wahrscheinlichkeit" von der Identität des Geschäftspartners ausgehen können. Eine nähere gesetzliche Regelung oder Klassifizierung derartiger Verfahren ist weder notwendig noch möglich. Die entsprechenden Festlegungen müssen in der Policy des Zertifizierungsdiensteanbieters erfolgen.

Zu § 4 des Entwurfs:

1. § 4 Abs. 1 verwirklicht die in Art. 5 Abs. 1 der Richtlinie vorgesehene **Gleichstellung** der Rechtswirkungen **sicherer** elektronischer Signaturen mit jenen der **eigenhändigen Unterschrift**. Art. 5 Abs. 1 der Richtlinie schreibt vor, daß die besonderen Rechtswirkungen, die nach den nationalen Rechtssystemen einer eigenhändigen Unterschrift zukommen, auch den sicheren elektronischen Signaturen im Sinn der Richtlinie (das sind fortgeschrittene elektronische Signaturen unter Einhaltung der Anforderungen der Anhänge I bis III) zuerkannt werden müssen.

Gesetzlichen Schriftform- bzw. Schriftlichkeitserfordernissen soll vorbehaltlich abweichender gesetzlicher Regelungen (insbesondere des § 4 Abs. 2) auch durch eine sichere elektronische Signatur entsprochen werden. Dies soll nicht nur für den zivilrechtlichen Bereich, sondern grundsätzlich auch **für den Verwaltungsbereich** und für die elektronische Kommunikation zwischen Bürgern und der öffentlichen Verwaltung gelten. Da auf gemeinschaftsrechtlicher Ebene für sichere elektronische Signaturen ausreichende Sicherheitsgarantien verankert wurden, bestehen dagegen grundsätzlich auch keine rechtspolitischen Bedenken.

Im österreichischen Zivilrecht wird das Erfordernis der **einfachen Schriftform** in § 886 ABGB geregelt. Ist für einen Vertrag gesetzlich oder auf Grund einer Parteienvereinbarung das Erfordernis der **Schriftlichkeit** vorgesehen, so kommt ein Vertrag durch die Unterschrift der Parteien zustande. Der schriftliche Abschluß des Vertrags kann durch die gerichtliche oder notarielle Beurkundung ersetzt werden. Eine Nachbildung der eigenhändigen **Unterschrift** auf mechanischem Weg ist nur dann ausreichend, wenn dies im Geschäftsverkehr üblich ist. Die Nichtbeachtung gesetzlicher Formvorschriften hat die Ungültigkeit des Rechtsgeschäfts zur Folge. Soweit durch das formungültige Rechtsgeschäft eine Leistungsverpflichtung des Schuldners herbeigeführt werden sollte, wird grundsätzlich eine **Naturalobligation** erzeugt, also eine Leistungsverbindlichkeit, die zwar nicht vor Gericht durchsetzbar, aber erfüllbar ist. Die tatsächliche Leistung des Versprochenen heilt den Mangel der Form.

Nach § 886 ABGB wird somit das Erfordernis der "Schriftlichkeit" im Prinzip durch die **eigenhändige Unterschrift** des Erklärenden erfüllt. Für das wirksame Zustandekommen eines formgebundenen Vertrags ist somit die Unterschrift der Parteien maßgeblich. Im Gegensatz etwa zu § 126 dBGB wird nicht auf das Vorliegen einer Urkunde (Verkörperung in Papierform) abgestellt.

Das österreichische Zivilrecht geht vom **Grundsatz der Formfreiheit** aus und überläßt es regelmäßig den Parteien, in welcher Form sie ein Rechtsgeschäft abschließen wollen (§§ 883 und 863 ABGB). Dieser Grundsatz wird jedoch durch zahlreiche Sonderregelungen eingeschränkt, wobei sich die Formgebundenheit entweder aus dem Gesetz oder aus der Parteienvereinbarung ergeben kann.

Vielfach verlangen zivilrechtliche **Rechtsvorschriften** für die Gültigkeit eines Rechtsgeschäfts die Einhaltung der (einfachen) Schriftform im Sinn des § 886 ABGB. Dies gilt beispielsweise für die Abgabe einer Bürgschaftserklärung durch einen Nichtkaufmann (§ 1346 Abs. 2 ABGB), die Begründung von Wohnungseigentum (§ 2 Abs. 2 Z 1 WEG), den Abschluß eines befristeten

Mietvertrags (§ 29 Abs. 1 Z 3 MRG), den Bauträgervertrag (§ 3 Abs. 1 BTVG) oder für bestimmte Regelungen im Maklervertrag (§ 31 KSchG). Unbeschadet der Rechtswirksamkeit verlangt das Gesetz die Schriftlichkeit etwa für den Verbraucherkreditvertrag und den Verbrauchergirokontovertrag (§§ 33 und 34 BWG 1993) sowie den Vertrag über das Abzahlungsgeschäft (§ 24 KSchG). Außer für das Zustandekommen bestimmter Verträge ist das Erfordernis der Schriftlichkeit vor allem aus Gründen der Beweissicherung für bestimmte rechtsgeschäftlich relevante Erklärungen vorgesehen. In diesem Zusammenhang sind diverse, im Interesse des Verbraucherschutzes normierte Rücktrittserklärungen – etwa vom Haustürgeschäft (§ 3 Abs. 3 KSchG), vom Immobiliengeschäft (§ 30a KSchG), vom Teilzeitnutzungsvertrag (§ 6 Abs. 3 TNG) oder vom Bauträgervertrag (§ 5 Abs. 4 BTVG) – zu erwähnen.

Formvorschriften finden sich nicht nur im Gesetz, sie können auch durch **Parteienvereinbarung** festgelegt werden. Bisweilen sind solche Klauseln auch in Allgemeinen Geschäftsbedingungen enthalten. Haben die Parteien ohne gesetzliche Anordnung für einen Vertrag eine bestimmte Form, zumeist die Schriftform, vorgesehen, so wird gesetzlich vermutet, daß die Einhaltung dieser Form ein Gültigkeitserfordernis für das Rechtsgeschäft darstellen soll (§ 884 ABGB). Diese Vermutung kann jedoch bei gegenteiligem Willen der Parteien von ihnen entkräftet werden.

Auch den vertraglich **vereinbarten** Schriftformerfordernissen soll mit einer sicheren elektronischen Signatur Genüge getan werden, sofern nicht etwas anderes vereinbart ist. Die Vertragsparteien haben jedoch die Möglichkeit zu vereinbaren, daß im Geschäftsverkehr zwischen ihnen die Schriftform auch bei Verwendung von Telefax oder anderen elektronischen Medien (zB E-mail) gegeben ist (vgl. Punkt 1.2.2. der Allgemeinen Geschäftsbedingungen der Datakom Austria GmbH). Dies gilt insbesondere auch für die sogenannten **“geschlossenen Systeme”** (vgl. die Erläuterungen zu § 1).

2. Nach Art. 5 Abs. 1 der Richtlinie sind sichere elektronische Signaturen in ihren Rechtswirkungen der **eigenhändigen Unterschrift** gleichzustellen. Dies bedeutet, daß grundsätzlich auch **formgebundene Verträge** unter Verwendung sicherer elektronischer Signaturen wirksam zustande kommen müssen. Den Mitgliedstaaten bleibt jedoch die Entscheidung überlassen, in welchen **Bereichen** sie die **elektronische Form** einführen. In diesem Zusammenhang wird in den Erwägungsgründen ausgeführt, daß die Verwendung elektronischer Dokumente und elektronischer Signaturen dem einzelstaatlichen Recht unterliegt; die Regelungen über Formvorschriften bleiben unberührt. Diese Entscheidungsfreiheit der Mitgliedstaaten soll jedoch mit Art. 9 des Vorschlags für eine Richtlinie über bestimmte rechtliche Aspekte des elektronischen Geschäftsverkehrs im Binnenmarkt (ABl. Nr. C 30 vom 5. 2. 1999, S 4) eingeschränkt werden. Nach dieser Bestimmung sollen die Mitgliedstaaten den wirksamen Abschluß elektronischer Verträge ermöglichen. Mit dieser **“Ermöglichungsklausel”** soll ausgedrückt werden, daß grundsätzlich alle Verträge – das heißt auch **formgebundene** – auf elektronischem Weg wirksam zustande kommen müssen. **Ausnahmen** können nur für die im **Ausnahmekatalog** des Art. 9 Abs. 2 des genannten Richtlinien vorschlags angeführten Verträge vorgesehen werden.

Wie bereits erwähnt, spricht auf Grund der hohen Anforderungen an sichere elektronische Signaturen einiges dafür, diese in ihren Rechtswirkungen eigenhändigen Unterschriften grundsätzlich gleichzustellen. Die Bereiche, in denen die **elektronische Form** im rechtsgeschäftlichen Verkehr nicht zugelassen wird, finden sich in § 4 Abs. 2. Bei der Erstellung dieses Ausnahmekatalogs soll auf die in Art. 9 Abs. 2 des Vorschlags für eine Richtlinie über den elektronischen Geschäftsverkehr im Binnenmarkt vorgesehenen Ausnahmen Bedacht genommen werden.

§ 4 Abs. 2 nennt zunächst die formgebundenen Rechtsgeschäfte des **Familien- und des Erbrechts (Z 1)**. Sie sollen ausgenommen werden, weil diese Bereiche besonders sensibel sind, häufig vermögensrechtliche Belange besonders schutzbedürftiger Personen betreffen und der Beweis hier vielfach nur schwer erbracht werden kann. Ein Testament in elektronischer Form soll daher zumindest vorläufig nicht wirksam sein. Demgegenüber ist etwa eine Unterhaltspflichtungserklärung eines – gesetzlich zum Unterhalt verpflichteten – Elternteils nicht als formgebundenes Rechtsgeschäft zu qualifizieren, sie kann daher auch in elektronisch signierter Form abgegeben werden (**Z 1**).

Die Erfüllung von Formvorschriften durch sichere elektronische Signaturen bezieht sich nur auf die einfache Schriftform. Die sogenannte **“öffentliche Form”** soll unberührt bleiben, ihr kann durch elektronische Signaturen derzeit noch nicht entsprochen werden. Dies gilt vor allem für die nach § 1 des Notariatszwangsgesetzes oder sonst notariatsaktspflichtigen Rechtsgeschäfte (zB Kauf-, Tausch- und Darlehensverträge zwischen Ehegatten oder Schenkungsverträge ohne wirkliche Übergabe, Ehepakete und anderes), aber auch für sämtliche Willenserklärungen oder Rechtsgeschäfte, die zu **ihrer Wirksamkeit** an das Erfordernis einer öffentlichen Beglaubigung oder Beurkundung gebunden sind

(Z 2). Beglaubigungen durch die Kanzleien nach der Beglaubigungsverordnung (“Für die Richtigkeit der Ausfertigung”) sind keine Beglaubigungen im Sinn dieser Bestimmung. Besteht eine solche Bindung nicht, so kann die sichere elektronische Signatur zulässigerweise verwendet werden, sofern entsprechende Strukturen vorliegen.

Zum Teil bedürfen Willenserklärungen oder Rechtsgeschäfte, aber auch förmliche Eingaben zu ihrer **Eintragung in bestimmte Register** (zB Grundbuch und Firmenbuch) einer öffentlichen Beglaubigung (Bestätigung der Echtheit der Unterschrift), einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsakts. Auch hierfür soll eine Ausnahme vorgesehen werden (Z 3).

In Z 4 wird eine Ausnahmeregelung für die **Bürgschaftserklärung** eines Nichtkaufmanns normiert. Nach § 1346 Abs. 2 ABGB muß die Verpflichtungserklärung des Bürgen zu ihrer Gültigkeit **schriftlich** abgegeben werden. Diese Ausnahme betrifft die **einfache Schriftform**. Sie ist – abweichend vom Grundsatz, daß sichere elektronische Signaturen die einfache Schriftform erfüllen sollen – sachlich gerechtfertigt, weil Bürgschaften für den Bürgen in der Regel mit einem beträchtlichen Risiko verbunden sind. Die Unterschrift soll dem Erklärenden die mit der Abgabe seiner Willenserklärung möglicherweise verbundenen Gefahren und Nachteile deutlich vor Augen führen. Die schutzwürdige Partei soll sich die Abgabe der Erklärung gründlich überlegen und damit insbesondere vor Übereilung geschützt werden. Das Erfordernis der Schriftlichkeit zielt in diesem Zusammenhang auf die besondere **Warnfunktion** der eigenhändigen Unterschrift ab.

Der Entwurf sieht aber davon ab, weitere Ausnahmen zu schaffen. Zum einen gewährleisten die hohen Anforderungen an die sichere elektronische Signatur einen bestmöglichen Gleichklang mit dem Vorgang einer “normalen” Unterschrift (siehe insbesondere auch die sogenannte “Viewer-Funktion”, die es dem Signator ermöglicht, die Daten vor Auslösen des Signaturvorgangs noch einmal zu studieren). Zum anderen wäre eine Auswahl unter den zahlreichen Schriftformgeboten in der Zivilrechtsordnung in jedem Fall mit dem Verdacht der Willkürlichkeit behaftet. Schließlich müssen – wie schon erwähnt – die gemeinschaftsrechtlichen Vorgaben beachtet werden.

3. Sichere elektronische Signaturen sind in der Lage, den Signator zu identifizieren. Die Signaturerstellungsdaten (etwa ein privater Signaturschlüssel) werden durch Besitz (zB einer Chipkarte) und Wissen (zB eines Paßworts oder einer PIN) an ihn, also an eine bestimmte natürliche Person, gebunden. Zudem ist der Signator verpflichtet, den Zugriff auf seine Signaturerstellungsdaten zu verhindern und deren Weitergabe zu unterlassen. Kommen dem Signator diese Daten abhanden, so ist er verpflichtet, unverzüglich den Widerruf seines Zertifikats zu veranlassen (vgl. dazu näher § 21). Durch die Kombination dieser Maßnahmen ermöglicht die digitale Signatur einen zuverlässigen Rückschluß auf den Signator.

Im österreichischen Zivilverfahrensrecht ist der Urkundenbegriff nicht mit dem Erfordernis einer Unterschrift verknüpft. Urkunden im Sinn der ZPO sind schriftliche Aufzeichnungen von Gedanken, die Tatsachen festhalten. Der Urkundenbegriff ist an die Papierform geknüpft (Verkörperung des Inhalts in Papierform), setzt aber keine Unterschrift des Erklärenden voraus. Der Unterschrift kommt aber auch im Beweisrecht eine wichtige Bedeutung zu. Für **unterschiedene Privaturkunden** gelangt nämlich eine besondere zivilprozessuale Beweisregel (§ 294 ZPO) zur Anwendung. Ist eine Unterschrift unbestritten oder nachgewiesenermaßen echt, so begründet eine Privaturkunde vollen Beweis dafür, daß der Inhalt vom Aussteller, also vom Namensträger der Unterschrift, stammt. Dabei handelt es sich um eine **qualifizierte Echtheitsvermutung** für den **Erklärungsinhalt**, die eine Zuordnung der in einer Urkunde enthaltenen Erklärung zum Unterzeichner bewirkt. Der Beweis des Gegenteils ist zulässig. Dies bedeutet, daß die Beweislast für die Unechtheit des Inhalts der Urkunde den Gegner des Beweisführers trifft. Die Umkehr der Beweislast bezieht sich aber nur auf den **Urkundeninhalt**, hinsichtlich der Echtheit der Unterschrift gelangen die normalen Beweislastregeln zur Anwendung. Demnach trägt jede Partei die Beweislast für das Vorliegen aller tatsächlichen Voraussetzungen der ihr günstigen Rechtsnorm, also für die für ihren Prozeßstandpunkt günstigen Tatsachen.

Da eine sichere elektronische Signatur einen zuverlässigen Rückschluß auf den Signator ermöglicht, ist eine Gleichsetzung der sicheren elektronischen Signatur mit der eigenhändigen Unterschrift auch im Beweisrecht gerechtfertigt. Da sich die Bestimmung des § 294 ZPO nur auf (eigenhändig unterschriebene) **Privaturkunden** bezieht, muß ihre Anwendbarkeit auf mit einer sicheren elektronischen Signatur signierte **elektronische Dokumente** ausdrücklich angeordnet werden (§ 4 Abs. 3). Obwohl dies von der Richtlinie nicht vorgeschrieben ist, werden damit im zivilrechtlichen Bereich die sicher signierten **elektronischen Dokumente** den eigenhändig unterschriebenen **Privaturkunden** in Papierform gleichgestellt. Die Voraussetzungen der Gleichstellung elektronischer

Dokumente mit den Urkunden etwa im strafrechtlichen Bereich bedarf weiterer Überlegungen, weshalb derartige Fragestellungen späteren Regelungen vorbehalten bleiben müssen.

Eine – widerlegbare – **Vermutung**, daß die Signaturerstellungsdaten vom Signator verwendet wurden, wird nicht mehr vorgeschlagen, weil darin eine Besserstellung elektronischer Signaturen gegenüber der eigenhändigen Unterschrift gelegen wäre. Für eine derartige Maßnahme sind ausreichende Erfahrungen im Umgang mit dem neuen elektronischen Unterschriftenersatz erforderlich.

Nach derzeitigem Beweisrecht stellt ein elektronisches Dokument im visualisiertem Zustand ein Augenscheinsobjekt dar. Wird ein elektronisches Dokument ausgedruckt, so liegt eine – jedoch nicht unterschriebene – Urkunde vor.

4. In § 4 Abs. 4 wird schließlich zum Ausdruck gebracht, daß für sichere elektronische Signaturen eine **Sicherheitsvermutung** besteht.

Für sichere elektronische Signaturverfahren dürfen gemäß § 18 Abs. 5 nur **sicherheitsgeprüfte Produkte** verwendet werden. Damit wird dafür vorgesorgt, daß die normierten Sicherheitsanforderungen auch eingehalten werden. Die Möglichkeit, daß diese Sicherheitsanforderungen in einem konkreten Einzelfall verletzt werden, kann dadurch aber nicht ganz ausgeschlossen werden. Denkbar wären beispielsweise die Fälle, daß der private Schlüssel ausgespäht, der Chipspeicher gebrochen oder der Algorithmus mathematisch ausgeforscht wird. Mit den normierten Sicherheitsanforderungen wird dieses Restrisiko zwar auf ein Mindestmaß reduziert. Es muß aber dennoch die Möglichkeit bestehen, daß in einem gerichtlichen Verfahren sicherheitsrelevante Manipulationen, Veränderungen oder Eingriffe nachgewiesen werden können. Das gleiche gilt für nachträgliche technische Eingriffe und Manipulationen, also die Kompro mittierung der zur Einhaltung der Sicherheitsanforderungen getroffenen technischen Vorkehrungen. Von diesen Überlegungen geht auch die Richtlinie aus. Im Erwägungsgrund 21 wird hiezu festgehalten, daß die Richtlinie die Möglichkeit für ein Gericht, die Übereinstimmung mit den Anforderungen der Richtlinie zu überprüfen, unberührt läßt.

Wie schon ausgeführt, führt die Nichteinhaltung zivilrechtlicher Schriftformerfordernisse zu einer Naturalobligation, was zur Folge hat, daß die tatsächliche Leistung des Versprochenen den Formmangel heilt. Eine Rückabwicklung formmangelhafter Verträge ist damit grundsätzlich ausgeschlossen (§ 1432 ABGB).

Zu § 5 des Entwurfs:

1. § 5 Abs. 1 übernimmt den Mindestinhalt eines **qualifizierten Zertifikats**, wie er sich aus **Anhang I** zur Richtlinie ergibt. Der Inhalt ist an das für Zertifikate derzeit gebräuchliche ITU-T (International Telecommunication Union – Telecommunication) Standardformat X.509v.3 angepaßt.

Die Eindeutigkeit des **Namens des Zertifizierungsdiensteanbieters (Z 2)** muß sichergestellt sein. Damit wird die lit. a des Anhangs I zur Richtlinie umgesetzt.

Das Zertifikat muß einem bestimmten Signator eindeutig **zuordenbar** sein (**Z 3**). Dies ist jedenfalls innerhalb des Betriebes eines Zertifizierungsdiensteanbieters sicherzustellen, weil die Unterscheidbarkeit des Zertifikats gegenüber anderen Zertifizierungsdiensteanbietern durch die Angabe einer eindeutigen Kennung des Zertifikats (**Z 7**) gewährleistet ist (für denselben Signaturschlüssel können auch mehrere Zertifikate von unterschiedlichen Zertifizierungsdiensteanbietern ausgestellt werden). Sollten mehrere Personen mit dem gleichen Vor- und Nachnamen Kunden ein und desselben Zertifizierungsdiensteanbieters sein, so muß die Unverwechselbarkeit durch einen geeigneten Zusatz, etwa das Geburtsdatum, hergestellt werden. Verwechslungsmöglichkeiten müssen ausgeschlossen sein. Wird im Zertifikat anstatt des Namens des Signators ein Pseudonym verwendet, so muß dieses gekennzeichnet werden (siehe auch die Erläuterungen zu § 8 Abs. 4 und zu § 22 Abs. 2). Auch hier darf keine Verwechslungsgefahr bestehen.

In **Z 4** wird die Möglichkeit vorgesehen, in das Zertifikat eine **Vertretungsmacht** beispielsweise für eine juristische Person (organschaftliche Vertretungsmacht, Prokura), aufzunehmen. Das gleiche gilt für andere rechtlich erhebliche Eigenschaften des Signators, etwa gewerberechtliche oder berufsrechtliche Befugnisse (zB für Ärzte oder Rechtsanwälte) oder sonstige Zulassungen. Derartige Eigenschaften des Signators dürfen nur dann in das Zertifikat aufgenommen werden, wenn sie tatsächlich gegeben sind. Der Zertifizierungsdiensteanbieter hat also die Richtigkeit dieser Angaben – wie auch jene der anderen Angaben in einem qualifizierten Zertifikat – zu überprüfen. Nach § 21 ist der Signator verpflichtet, sein Zertifikat widerrufen zu lassen, wenn sich Umstände, die im Zertifikat bescheinigt sind, ändern (vgl. auch § 9 Abs. 1 Z 2). Je nach dem zum Einsatz gelangenden technischen Verfahren könnten solche

Angaben auch in ein Attribut-Zertifikat aufgenommen werden. In einem solchen – in der Praxis seltenen – Fall müßte in das (Haupt-)Zertifikat ein Hinweis auf das Attribut-Zertifikat aufgenommen werden.

Bei den in **Z 5** genannten **Signaturprüfdaten** handelt es sich – bei digitalen Signaturen – um den öffentlichen Signaturschlüssel, der dem Signator durch den Zertifizierungsdiensteanbieter zugeordnet wird (siehe die Erläuterungen zu § 2 Z 6).

Die **Gültigkeitsdauer** eines Zertifikats (**Z 6**) ist der Zeitraum, während dessen das Zertifikat zum Signieren verwendet werden darf. Eine Signatur nach Ablauf dieses Zeitraums wäre nicht mehr gültig. Die Verfügbarkeit und insbesondere die Sicherheit der Signatur(prüf-)daten muß aber – dem Verwendungszweck des Zertifikats angepaßt – wesentlich länger sein.

Die eindeutige **Kennung des Zertifikats (Z 7)** ermöglicht die eindeutige Zuordnung des Zertifikats zum ausstellenden Zertifizierungsdiensteanbieter.

Die Angaben in **Z 8 (Einschränkung des Anwendungsbereichs)** und in **Z 9 (Begrenzung des Transaktionswerts)** korrespondieren mit den Bestimmungen über die Haftungsbeschränkung in § 23 Abs. 4 (Anhang I lit. i und j bzw. Art. 6 Abs. 3 und 4 der Richtlinie). Im Zertifikat kann angegeben werden, daß sein Anwendungsbereich beschränkt ist, dieses also zB nur für bestimmte Rechtsgeschäfte verwendet werden darf. Ebenso kann im Zertifikat eine Begrenzung des Transaktionswerts, bis zu dem das Zertifikat gilt (zB 5 000 S), enthalten sein. Nach dem Konzept der Richtlinie sollen diese Beschränkungen des Anwendungsbereichs in erster Linie vom Zertifizierungsdiensteanbieter vorgenommen werden können, um auf diese Weise seine Haftung zu beschränken. Aus diesem Grund finden sich die korrespondierenden inhaltlichen Regelungen auch in der Bestimmung über die Haftung (Art. 6 der Richtlinie). Wird also ein Zertifikat entgegen der Beschränkung im Zertifikat zweckwidrig verwendet oder wird eine Zahlungsverpflichtung über einen höheren Betrag begründet, so hat dies zur Folge, daß der Zertifizierungsdiensteanbieter – trotz Vorliegens der übrigen Haftungsvoraussetzungen – für die Überschreitung des Anwendungsbereichs bzw. des Transaktionswerts nicht haftet. Die Gültigkeit des Rechtsgeschäfts im Verhältnis zum Signator bleibt jedoch unberührt. Die betragsmäßige Begrenzung in **Z 9** bezieht sich auf Einzeltransaktionen des Signators. Eine absolute Haftungshöchstgrenze des Zertifizierungsdiensteanbieters ist nicht vorgesehen. Eine solche käme wegen der vorgesehenen Verschuldenshaftung auch nicht in Betracht.

2. Der Aufnahme **weitergehender Angaben** im Zertifikat (zB bei **Minderjährigen** das Geburtsdatum) im Rahmen vertraglicher Vereinbarungen zwischen dem Zertifikatswerber und dem Zertifizierungsdiensteanbieter steht nichts entgegen (siehe § 5 Abs. 2).

3. Der Zertifizierungsdiensteanbieter hat die entsprechenden Inhalte in das qualifizierte Zertifikat aufzunehmen und deren Richtigkeit zu bestätigen. Um sicherzustellen, daß eine elektronische Signatur – die auf einem qualifizierten Zertifikat beruht – bei Einhaltung der Sicherheitsmaßnahmen nur der berechtigten Person (Signator) zugeordnet werden kann, muß der Zertifizierungsdiensteanbieter die Inhalte, insbesondere die Identität des Signators, zuverlässig überprüfen. Für die Richtigkeit der Angaben haftet er nach den Bestimmungen des § 23. Die **Bestätigung der Inhalte** eines qualifizierten Zertifikats durch den Zertifizierungsdiensteanbieter erfolgt dadurch, daß er das von ihm ausgestellte Zertifikat mit seiner **eigenen sicheren elektronischen Signatur** versieht. Erst dadurch wird die bloße elektronische Erfassung von Daten zum qualifizierten Zertifikat. Ausnahmsweise kann dabei ein auf eine juristische Person ausgestelltes Zertifikat verwendet werden (vgl. § 2 Z 2 und die Erläuterungen dazu).

Die sichere Signatur des Zertifizierungsdiensteanbieters muß den **Anforderungen des § 18** entsprechen.

Zu § 6 des Entwurfs:

1. § 6 Abs. 1 stellt klar, daß für die Aufnahme (den Marktzugang) und die Ausübung der Tätigkeit (den Betrieb) eines Zertifizierungsdiensteanbieters **keine spezifische Genehmigung** erforderlich ist. Eine gesonderte vorherige Genehmigung bzw. Lizenzierung von Zertifizierungsdiensteanbietern ist damit ausgeschlossen.

Das Prinzip der **Genehmigungsfreiheit** ist gemeinschaftsrechtlich vorgegeben. Art. 3 Abs. 1 der Richtlinie bestimmt, daß die Bereitstellung von Signatur- und Zertifizierungsdiensten von keiner vorherigen Genehmigung abhängig gemacht werden darf. Dadurch soll das gemeinschaftsweite Anbieten von Zertifizierungsdiensten über alle offenen Netze gefördert werden. In Erwägungsgrund 10 wird eine "vorherige Genehmigung" nicht nur als Erlaubnis zur Aufnahme der Tätigkeit beschrieben, vielmehr sind auch sonstige Maßnahmen gleicher Wirkung untersagt. Nicht zulässig wären damit etwa formelle

Zugangsbeschränkungen, die gleiche Auswirkungen wie eine Genehmigungs-, Konzessions- oder Lizenzierungspflicht hätten (zB eine Vorlagepflicht mit Wartezeit oder eine Verpflichtung zum Abwarten einer Registrierung). Die Aufnahme der Tätigkeit darf also nicht von der Entscheidung oder Maßnahme einer Behörde oder sonstigen Aufsichtsstelle abhängig gemacht werden.

Untersagt sind aber nur **spezielle, für die Tätigkeit als Zertifizierungsdiensteanbieter vorgesehene Genehmigungen**. Andere, nach allgemeinen Regelungen (auch für den offline-Bereich) bestehende Zulassungsvoraussetzungen und Zulassungsverfahren bleiben unberührt. Dies gilt insbesondere für die Vorschriften der Gewerbeordnung 1994. Zertifizierungsdiensteanbieter werden in der Regel als Datenverarbeiter zu qualifizieren sein. Diese Tätigkeit ist als freies Gewerbe nach der Gewerbeordnung 1994 anmeldungspflichtig.

Von Genehmigungsverfahren sind **Aufsichtsmaßnahmen** zu unterscheiden, die nach der Richtlinie zulässig und geboten sind. Nach Art. 3 Abs. 3 leg.cit. hat jeder Mitgliedstaat für ein geeignetes Aufsichtssystem über die in seinem Hoheitsgebiet niedergelassenen Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, Sorge zu tragen. Die Richtlinie beschränkt die Mitgliedstaaten nicht in ihrer Aufsicht über andere Zertifizierungsdiensteanbieter. Als **Aufsichtsmaßnahmen** sind etwa Notifizierungs- oder Registrierungsverfahren anzusehen. Ebenso zulässig ist auch die Durchführung regelmäßiger Kontrollen der Zertifizierungsdiensteanbieter.

Die Einhaltung der vorgeschriebenen Sicherheitsanforderungen sowie die Bereitstellung vertrauenswürdiger Signatur- und Zertifizierungsdienste kann letztlich nur durch ein gut funktionierendes, effektives und über angemessene technologische Ausstattung sowie entsprechende Fachkompetenz verfügendes Aufsichtssystem sichergestellt werden. Diese Anforderungen machen etwa auch ständige **Technologiebeobachtungen** und entsprechende Adaptierungen der Sicherheitsanforderungen notwendig.

2. Jeder Mitgliedstaat hat also für ein geeignetes Aufsichtssystem über die Zertifizierungsdiensteanbieter zu sorgen. Damit ein solches System ordnungsgemäß funktionieren kann, muß bekannt sein, welche Unternehmen oder sonstigen Einrichtungen Signatur- und Zertifizierungsdienste bereitstellen, also als Zertifizierungsdiensteanbieter tätig sind. Aus diesem Grund muß (spätestens) mit Aufnahme der Tätigkeit diese der Aufsichtsstelle **angezeigt** werden.

Ab der Anzeige der Tätigkeit unterliegt der Zertifizierungsdiensteanbieter der (regelmäßigen) **Kontrolle** der Aufsichtsstelle. Damit diese über die ausgeübte Tätigkeit, insbesondere über die bereitgestellten Zertifizierungsdienste sowie über die verwendeten und angebotenen Signaturverfahren und Signaturprodukte, genau Bescheid weiß, muß ihr – ebenfalls spätestens mit Aufnahme der Tätigkeit oder bei Änderung der Dienste des Zertifizierungsdiensteanbieters – ein **Sicherheitskonzept** sowie ein **Zertifizierungskonzept** für jeden bereitgestellten Dienst vorgelegt werden (§ 6 Abs. 2).

In einer sogenannten **“Policy”** wird in der Regel ein Überblick über die bereitgestellten Dienste sowie über die Zertifizierungsinfrastruktur bzw. Zertifizierungshierarchie gegeben. Weiters werden die Aufgaben (zB Ausstellung von Zertifikaten, Informations- bzw. Verzeichnis- und Widerrufsdienst) und die Pflichten des Zertifizierungsdiensteanbieters (zB Belehrung des Anwenders, Datenschutz) umschrieben und seine Haftung sowie das von ihm verlangte Entgelt dargelegt. Ebenso werden die Pflichten der Anwender (zB Schutz des privaten Schlüssels und unverzüglicher Widerruf bei Verlust oder Kompromittierung) festgelegt.

Bei einem **Sicherheitskonzept** handelt es sich um die festgelegten Aussagen eines Zertifizierungsdiensteanbieters über technische und organisatorische Sicherheitsmaßnahmen und die für die von ihm bereitgestellten Signaturverfahren einzuhaltenden Sicherheitsanforderungen. Der Zertifizierungsdiensteanbieter hat in diesem Konzept darzulegen, welchem Sicherheitsniveau die von ihm eingesetzten und bereitgestellten Signaturverfahren und Produkte sowie die von ihm bereitgestellten Dienste entsprechen, welche Sicherheitsanforderungen hierfür festgelegt sind und durch welche Maßnahmen diese erreicht werden. Anhand des Sicherheitskonzepts muß eine verlässliche Aussage über die Vertrauenswürdigkeit des Betriebes des Zertifizierungsdiensteanbieters getroffen werden können. Insbesondere sind die **infrastrukturellen** (geeignete Räumlichkeiten, Schutz vor Zutritt unbefugter Personen, Schutz der technischen Ausstattung vor unbefugtem Zugriff, Aufbewahrung der Produkte und des Schlüsselmaterials), **personellen** (Zuverlässigkeit und Fachkunde, Schulungsmaßnahmen), **organisatorischen** (sichere Protokollierung und Archivierung der Zertifizierungsdaten, geeignetes Backup, Verhinderung des unbefugten Zugriffs auf private Schlüssel und Verzeichnisse, geeignete Vernichtung nicht mehr benötigter oder ungültiger Daten) sowie **technischen Sicherheitsanforderungen** (gegebenenfalls sichere Schlüsselgenerierung und -speicherung, sichere

Erzeugung und Speicherung von Zertifikaten, Verhinderung der Aktivierung des privaten Signaturschlüssels durch Unbefugte, Maßnahmen bei Verlust oder Kompromittierung des eigenen Signaturschlüssels, Notfallvorsorge sowie die zugrunde liegenden technischen und kryptographischen Normen) verständlich und nachvollziehbar darzulegen.

Bei einem **Zertifizierungskonzept** handelt es sich um die festgelegten Aussagen eines Zertifizierungsdiensteanbieters über die bei der Ausstellung von Zertifikaten eingehaltene Vorgangsweise. Darin wird die Art der Erbringung der Zertifizierungsdienste näher beschrieben. Insbesondere ist darzulegen, auf welche Weise die **Identifizierung** der Anwender (zB lediglich Existenz der E-mail-Adresse; Personenidentifizierung anhand übermittelter Dokumente; Personenidentifizierung anhand vorgelegter Dokumente und persönliches Erscheinen) erfolgt, wie die **Antragstellung** und die Generierung des privaten **Schlüssels** bzw. des Schlüsselpaares (zB Selbstgenerierung) vorzunehmen sind, wie der Erhalt des Zertifikats (zB online) sowie eine Erneuerung des Zertifikats (derselbe öffentliche Schlüssel wird nochmals zertifiziert; auch Aussage über die Gültigkeitsdauer des Zertifikats an sich sowie die maximale Gesamtdauer bei Erneuerung) erfolgen, sowie auf welche Weise Zertifikate abgerufen und überprüft werden können (**Verzeichnisdienst**) und wie der **Widerruf** von Zertifikaten veranlaßt und durchgeführt wird (auch zB Information des Signators; kein rückwirkender Widerruf; Widerruf kann nicht rückgängig gemacht werden).

3. Da mit **sicheren** elektronischen Signaturen **besondere Rechtswirkungen** verknüpft sind, kommt der Einhaltung der normierten Sicherheitsanforderungen besondere Bedeutung zu. Nur auf Grund der vorgesehenen Kombination von Maßnahmen – Personenidentifikation, zuverlässige Schlüsselzuordnung durch ein Zertifikat, Bindung des privaten Schlüssels durch Besitz und Wissen an eine bestimmte Person sowie sichere technische Komponenten – ist eine **zuverlässige Zuordnung** einer sicheren elektronischen Signatur zum Signator möglich.

Daraus ergibt sich, daß die Sicherheit der Signaturverfahren gewährleistet sein muß. Technische Manipulationen oder Fehler, die dazu führen, daß Daten ungewollt signiert oder andere als die angezeigten Daten signiert werden, müssen verhindert werden. Dies kann durch die Verwendung geeigneter **technischer Komponenten und Verfahren** (beim Zertifizierungsdiensteanbieter und beim Anwender) erreicht werden. Die entsprechenden Sicherheitsanforderungen sind – in Übereinstimmung mit den Vorgaben in der Richtlinie – in § 18 festgelegt.

Ein Zertifizierungsdiensteanbieter, der sichere elektronische Signaturverfahren bereitstellt, muß die Einhaltung der vorgeschriebenen Sicherheitsanforderungen im **Sicherheitskonzept** darlegen (§ 6 Abs. 3).

4. Die Erbringung der Zertifizierungsdienste sowie das im Zertifizierungskonzept angegebene Sicherheitsniveau müssen auch während der Ausübung der Tätigkeit eines Zertifizierungsdiensteanbieters **qualitativ unverändert** bleiben (§ 6 Abs. 4). Es darf nicht etwa nachträglich ein Qualitätsverlust eintreten. Nimmt ein Zertifizierungsdiensteanbieter Änderungen hinsichtlich der von ihm bereitgestellten Dienste vor oder ändert er die Bedingungen hierfür ab, so muß er dies unverzüglich der Aufsichtsstelle anzeigen.

5. Ist es dem Zertifizierungsdiensteanbieter nicht mehr möglich, die Bedingungen im Sicherheits- oder im Zertifizierungskonzept einzuhalten, kann er die Dienste also nicht mehr in der ursprünglichen Qualität erbringen oder ist er sonst nicht mehr in der Lage, seine Aufgaben zu erfüllen, so hat er dies nach § 6 Abs. 5 unverzüglich der **Aufsichtsstelle anzuzeigen**.

6. Die Qualität und das Sicherheitsniveau des bereitgestellten Signaturverfahrens (auch allfällige Sicherheitsstufen und Zertifikatsklassen) müssen in der **Policy** dargestellt werden, damit für den **Anwender nachvollziehbar** ist, in welchen Bereichen er das angebotene Signaturverfahren verwenden kann. Aus der Policy muß sich auch ergeben, ob die verwendete elektronische Signatur auf einem Zertifikat beruht und ob bzw. in welcher Form ein Verzeichnis- und ein Widerrufsdienst geführt wird. Bei Zertifikaten mit nur kurzer Gültigkeitsdauer (zB drei Monate) wird in der Regel kein Widerrufsdienst angeboten. Das gleiche gilt beispielsweise für Gratiszertifikate im Kleinstanwendungsbereich.

Zu § 7 des Entwurfs:

1. Nach den Vorgaben der Richtlinie **dürfen qualifizierte Zertifikate** nur von einem Zertifizierungsdiensteanbieter, der den Anforderungen des Anhangs II zur Richtlinie entspricht, ausgestellt werden (Art. 2 Z 10). Diese Anforderungen werden in den Abs. 1 bis 3 umgesetzt; sie können in organisatorische, personelle und technische Anforderungen unterschieden werden.

§ 7 Abs. 1 gibt die Anforderungen in lit. a bis e sowie lit. h bis j des Anhangs II zur Richtlinie wieder.

“Erforderliche **Zuverlässigkeit**” (**Z 1**) bedeutet, daß Gewähr für die Einhaltung der maßgeblichen Rechtsvorschriften bestehen muß.

Da der Widerruf eines Zertifikats **sofort** registriert werden muß, ist für einen “unverzöglichen” **Widerrufsdienst** zu sorgen (**Z 2**).

Ein **Zeitstempel** (**Z 3**) ist eine elektronisch signierte Bescheinigung eines Zertifizierungsdiensteanbieters, daß (ihm) bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen sind. Die Bereitstellung von Zeitstempeldiensten ist für die Tätigkeit als Zertifizierungsdiensteanbieter nicht notwendig oder wesentlich. Diese Dienste können auch “ausgliedert” sein, das heißt von einer anderen Einrichtung erbracht werden. Sind in qualifizierten Zertifikaten oder in Zertifikatsverzeichnissen oder Widerrufslisten Zeitangaben enthalten, so müssen diese **qualitätsgesichert** sein, das heißt den Sicherheitsanforderungen des § 18 entsprechen. Für allfällige Streitfälle müssen aber jedenfalls Datum und Uhrzeit (der Zeitpunkt) der Ausstellung und des Widerrufs eines qualifizierten Zertifikats vom Diensteanbieter bereitgestellt werden können.

Die Überprüfung der **Identität** des Signators sowie der sonstigen im qualifizierten Zertifikat enthaltenen Angaben (**Z 4**) ist wesentlich, weil sich jeder Empfänger einer signierten Erklärung darauf verlassen können muß und den Zertifizierungsdiensteanbieter zudem die Haftung für die Richtigkeit der Angaben im Zertifikat trifft (§ 23 Abs. 1). In diesem Zusammenhang ist die Datenschutzbestimmung des § 22 zu beachten, wonach personenbezogene Daten nur beim Betroffenen selbst oder nur mit seiner ausdrücklichen Zustimmung bei einem Dritten erhoben bzw. überprüft werden dürfen. Gibt der Zertifikatswerber die Informationen, die zur Ausstellung eines qualifizierten Zertifikats benötigt werden, nicht bekannt oder stimmt er deren Überprüfung nicht zu, **so darf ein qualifiziertes Zertifikat nicht ausgestellt werden**. Besondere rechtlich erhebliche Eigenschaften des Signators dürfen nur auf sein Verlangen in das Zertifikat aufgenommen werden. Die wirtschaftlichen Verhältnisse oder die finanzielle Leistungsfähigkeit eines Signators, also seine Bonität, gehören nicht zu seiner Identität und dürfen daher zur Ausstellung eines qualifizierten Zertifikats nicht erhoben werden.

Die Maßnahmen, die getroffen werden, um geeignetes **Personal** mit den erforderlichen technischen, organisatorischen und wirtschaftlichen Fähigkeiten einzusetzen, sind in der Policy darzulegen. Beschrieben werden müssen etwa die Ausbildungserfordernisse der Bediensteten sowie bestehende Schulungsmaßnahmen (**Z 5**).

Zur Abdeckung des Haftungsrisikos der Zertifizierungsdiensteanbieter wird eine Haftpflichtversicherung mit einer Mindestversicherungssumme von 56 000 000 S (je Versicherungsfall, also nicht je Schadensfall) vorgeschrieben. Dieser Betrag erscheint als Mindestsockel ausreichend.

Zu den zur Erfüllung der Verpflichtungen aus diesem Bundesgesetz ausreichenden **Finanzmitteln** sind in der Signaturverordnung nähere Aussagen zu treffen (**Z 6**).

Die **Protokollierung** der ein qualifiziertes Zertifikat betreffenden Umstände (zB Ausstellung, Widerruf) ist für mögliche Streitfälle notwendig. Die Aufzeichnungsdauer ist dabei vom Verwendungszweck des Zertifikats abhängig. Für zivilrechtliche Rechtsgeschäfte wird mit Rücksicht auf die Verjährungsbestimmungen eine zumindest 30jährige (zuzüglich der Gültigkeitsdauer des Zertifikats) Protokollierungsdauer erforderlich sein. Bei Dauerschuldverhältnissen wird sie entsprechend länger sein müssen. Der Verfügbarkeitszeitraum muß im Zertifizierungskonzept festgehalten werden (**Z 7**).

Wird der private Schlüssel (die Signaturerstellungsdaten) eines Signators einem **Unbefugten bekannt**, so können elektronische Signaturen gefälscht und somit mißbräuchlich verwendet werden. Das Speichern oder Kopieren von Signaturerstellungsdaten könnte daher die Rechtssicherheit und das Vertrauen in elektronische Signaturen erschüttern. Aus diesem Grund dürfen vom Zertifizierungsdiensteanbieter Signaturerstellungsdaten – außer für die im Zusammenhang mit der Bereitstellung der Signatur- und Zertifizierungsdienste notwendigen Zwecke – weder gespeichert noch kopiert werden (**Z 8**). Dem Zertifizierungsdiensteanbieter ist es auch untersagt, Informationen über die Schlüsselerzeugung oder das technische Know-how hierüber bekanntzugeben. Er darf auch in keiner wie immer gearteten Form etwa an der Erzeugung eines Nachschlüssels mitwirken.

In § 7 Abs. 2 und 3 werden die Anforderungen der lit. f, g und l des **Anhangs II** zur Richtlinie umgesetzt. Dabei handelt es sich um die **technischen Sicherheitsanforderungen**, die vom Zertifizierungsdiensteanbieter eingehalten werden müssen. Das Erfordernis der Verwendung **vertrauenswürdiger** Systeme, Produkte und Verfahren, die insbesondere die technische und kryptographische Sicherheit gewährleisten, wird näher konkretisiert. Vor allem muß sichergestellt sein, daß Signaturerstellungsdaten (private Signaturschlüssel) geheimgehalten werden und

Zertifikatsfälschungen ausgeschlossen sind. Die Erstellung und Speicherung der Zertifikate hat so zu erfolgen, daß diese nicht verfälscht und nur mit Zustimmung des Signators öffentlich abgerufen werden können. Für die Bereitstellung von Signaturerstellungsdaten (insbesondere Generierung und Speicherung) sowie für die Erstellung und Speicherung von Zertifikaten sind sichere technische Komponenten und Verfahren im Sinn des § 18 zu verwenden.

Nach **Abs. 3** sind die Signaturerstellungsdaten eines Zertifizierungsdiensteanbieters vor unbefugtem Zugriff zu schützen. Es reicht dabei nicht aus, daß der private Signaturschlüssel des Zertifizierungsdiensteanbieters geheimgehalten wird, vielmehr müssen auch geeignete physikalische Sicherheitsmaßnahmen (zB geeignete Behältnisse bzw. Tresore, Brandschutzmaßnahmen) getroffen werden.

2. Eine der Voraussetzungen für eine **sichere** elektronische Signatur liegt darin, daß die Anforderungen des Anhangs II zur Richtlinie (siehe § 7 Abs. 1 bis 3) eingehalten werden. Die Einhaltung dieser Anforderungen ist im Rahmen des **Aufsichtssystems** sicherzustellen. Nach außen tritt dieser Umstand dadurch in Erscheinung, daß ein **qualifiziertes Zertifikat** vorliegt, das als solches bezeichnet sein muß (§ 5 Abs. 1 Z 1). Der Diensteanbieter soll zudem aber auch die Möglichkeit haben (§ 7 Abs. 4), sich **freiwillig akkreditieren** zu lassen (siehe dazu § 17). Dabei handelt es sich um eine zusätzliche vertrauensbildende Maßnahme, da die Einhaltung der beschriebenen Anforderungen schon von vornherein aufsichtsbehördlich bestätigt ist.

3. Verwendet der Signator eine **sichere** elektronische Signatur (besondere Rechtswirkungen möglich), so muß dieser Umstand nach § 7 Abs. 5 für den Empfänger der signierten Erklärung erkennbar sein, und zwar entweder im Zertifikat selbst oder im Zertifikatsverzeichnis (Verzeichnisdienst). Dies ist in der Praxis auch die Regel, weshalb diese Bestimmung in erster Linie der Klarstellung dient. Im Hinblick auf eine von einem **ausländischen Diensteanbieter** bereitgestellte **sichere** elektronische Signatur kann der Eintritt der besonderen Rechtswirkungen formal aber nicht von der Einhaltung dieser Voraussetzung abhängig gemacht werden, weil Art. 5 Abs. 1 der Richtlinie die Zuerkennung besonderer Rechtswirkungen (gegenseitige Anerkennung sicherer Signaturen im EU-Bereich) ausschließlich an die Einhaltung der Anforderungen in den Anhängen I bis III knüpft.

4. Elektronisch signierte Dokumente können als Beweismittel Gegenstand gerichtlicher oder behördlicher Verfahren sein. Da derzeit weder die Gerichte noch andere Behörden über die technische Ausstattung zum Empfangen und Verifizieren sicher elektronisch signierter Dokumente (zB Chipkartenleser) verfügen, muß von den Zertifizierungsdiensteanbietern sichergestellt werden, daß von ihnen bereitgestellte sichere Signaturen im gerichtlichen oder behördlichen Verfahren verifiziert werden können, eine **Signaturprüfung** also möglich ist (§ 7 Abs. 6). Die dafür auflaufenden Kosten sind grundsätzlich als Kosten des Verfahrens anzusehen.

Zu § 8 des Entwurfs:

1. § 8 Abs. 1 beschreibt die **typische Aufgabe** eines Zertifizierungsdiensteanbieters, nämlich die **Zuordnung** bestimmter Signaturprüfdaten (eines öffentlichen Signaturschlüssels) zu einer natürlichen Person durch **Ausstellen eines Zertifikats**. Für die Ausstellung **qualifizierter Zertifikate** müssen bestimmte Bedingungen eingehalten sein. So muß die **Identität** des Zertifikatswerbers (des künftigen Signators) **eindeutig** festgestellt werden, weil die zuverlässige Identifikation Voraussetzung dafür ist, daß auf den Urheber einer elektronischen Signatur geschlossen werden kann. Bei qualifizierten Zertifikaten ist die Identitätsfeststellung anhand eines **amtlichen Lichtbildausweises** durchzuführen. Wurde einer bestimmten Person von einem Zertifizierungsdiensteanbieter schon ein Zertifikat ausgestellt, so ist für die Ausstellung weiterer Zertifikate durch denselben Zertifizierungsdiensteanbieter die neuerliche Vorlage eines Lichtbildausweises entbehrlich.

Zur Überprüfung der Identität sei auch auf die Erläuterungen zu § 7 Abs. 1 Z 4 verwiesen. Die Zuordnung der Signaturprüfdaten (des öffentlichen Signaturschlüssels) zu einer bestimmten Person schafft die Voraussetzungen dafür, daß ein vorliegendes Zertifikat jederzeit auf seine Echtheit und Gültigkeit überprüft werden kann.

Die Veröffentlichung eines qualifizierten Zertifikats darf nur mit Zustimmung des Signators erfolgen (§ 7 Abs. 2 bzw. Anhang II lit. 1 zur Richtlinie). Auch für den Fall, daß keine solche Veröffentlichung erfolgt, kann das Zertifikat der Signatur angeschlossen werden, um dem Empfänger die Überprüfung der Signatur zu ermöglichen. Eine **gültige bzw. ordnungsgemäße** Signatur, die auf einem qualifizierten Zertifikat beruht, setzt voraus, daß das Zertifikat gültig ist und die **Signatur** nach dem im Zertifizierungskonzept angegebenen Verfahren **überprüft** werden kann. Zu diesem Zweck muß das Zertifikat bereitstehen. Dies erfolgt dadurch, daß das Zertifikat entweder (durch den Signator) der

Signatur angeschlossen ist oder das Zertifikat sonst (in der Regel online) zugänglich ist. Der Zertifizierungsdiensteanbieter muß die Abrufbarkeit des Zertifikats technisch ermöglichen.

Das Verfahren zur **Antragstellung** ist im Zertifizierungskonzept zu beschreiben (siehe § 6 Abs. 2).

2. § 8 Abs. 2 sieht vor, daß das Verlangen auf Ausstellung eines Zertifikats auch bei einer sogenannten **Registrierungsstelle** eingebracht werden kann, die für den Zertifizierungsdiensteanbieter tätig ist. Eine solche Stelle ist im Verhältnis zum Zertifikatswerber als Erfüllungsgehilfe des Zertifizierungsdiensteanbieters anzusehen. Zwischen Registrierungsstelle und Zertifikatswerber besteht in der Regel kein Vertragsverhältnis.

Eine Registrierungsstelle ist als **“Beauftragte”** eines Zertifizierungsdiensteanbieters berechtigt, die zur Ausstellung eines Zertifikats benötigten personenbezogenen Daten nach § 22 Abs. 1 zu erheben. Aus dem Tätigwerden einer Registrierungsstelle dürfen dem Zertifikatswerber – im Verhältnis zum Diensteanbieter – jedoch keine Nachteile entstehen.

Definitionsgemäß (§ 2 Z 11) handelt es sich bei einem Registrierungsdienst um einen eigenen **Zertifizierungsdienst**. Auch eine Registrierungsstelle kann daher die Haftung nach § 23 treffen.

3. Eine **Vertretungsmacht** für einen anderen Rechtsträger oder andere rechtlich erhebliche Eigenschaften des Zertifikatswerbers, also des künftigen Signators (zB berufsrechtliche Befugnisse oder sonstige Zulassungen), dürfen nur auf sein Verlangen und nur dann in das Zertifikat aufgenommen werden, wenn diese Umstände **zuverlässig nachgewiesen** werden (§ 8 Abs. 3). Bei Angaben über Dritte muß zudem deren Einverständnis nachgewiesen sein.

4. § 8 Abs. 4 ermöglicht die Verwendung von **Pseudonymen** in einem qualifizierten Zertifikat. Nach Art. 8 Abs. 3 der Richtlinie müssen die Zertifizierungsdiensteanbieter die Möglichkeit haben, Zertifikate unter Verwendung von Pseudonymen anzubieten. Insbesondere bei Massengeschäften soll es einem Anwender freistehen, grundsätzlich anonym zu bleiben. Durch die Verwendung von Pseudonymen dürfen geschützte Rechtsgüter, insbesondere Namens- und Kennzeichenrechte, nicht beeinträchtigt werden.

Die **Aufdeckung** von Pseudonymen, insbesondere bei Rechtsverletzungen durch den Signator im Zusammenhang mit der elektronischen Kommunikation, richtet sich gemäß § 22 Abs. 2 nach § 8 Abs. 1 Z 4 und Abs. 3 DSGVO.

Der Umstand, daß im Zertifikat ein Pseudonym angegeben ist, muß im Zertifikat **gekennzeichnet** sein (§ 5 Abs. 1 Z 3).

Zu § 9 des Entwurfs:

1. § 9 Abs. 1 regelt die Gründe für den **Widerruf** von Anwender-Zertifikaten. Die Bestimmung gilt auch für einfache Zertifikate, sofern vom Zertifizierungsdiensteanbieter ein Widerrufsdienst geführt wird (siehe die Erläuterungen zu § 6 Abs. 6). Bei **qualifizierten** Zertifikaten **muß** nach § 7 Abs. 1 Z 2 ein unverzüglicher und sicherer Widerrufsdienst geführt werden.

§ 9 Abs. 1 **Z 1** (Widerruf auf Verlangen des Signators oder eines Machtgebers) ist notwendig, um bei Verlust oder Kompromittierung eines Signaturschlüssels einen möglichen Mißbrauch zu verhindern. Außerdem soll sich der Signator jederzeit aus dem elektronischen Rechts- und Geschäftsverkehr zurückziehen können. Enthält ein Zertifikat Angaben über eine dritte Person (Vertretungsmacht), so kann – wenn sich hinsichtlich dieser Angaben Änderungen ergeben – auch diese den Widerruf verlangen. Weitergehende vertragliche Vereinbarungen, nach denen auch andere Personen einen Widerruf veranlassen können, bleiben unberührt.

Die Angaben, die im Zertifikat bescheinigt werden können, sind grundsätzlich nicht beschränkt. Es muß nur die Zustimmung des Signators, gegebenenfalls auch einer dritten Person (§ 5 Abs. 2 in Verbindung mit § 8 Abs. 3) vorliegen. Bei sonstigen **Änderungen** im Zertifikat bescheinigter Angaben (**Z 2**) kann es sich somit um die verschiedensten Umstände handeln, etwa den Entzug einer behördlichen oder berufsrechtlichen Befugnis oder einer sonstigen Zulassung, die Aberkennung der Staatsbürgerschaft oder die Verlegung des Wohnsitzes.

Z 4 betrifft die (freiwillige) **Einstellung der Tätigkeit** eines Zertifizierungsdiensteanbieters (§ 12). Ab diesem Zeitpunkt kann er keine neuen Zertifikate mehr ausstellen. Werden die **Verzeichnis- und Widerrufsdienste** von einem anderen Zertifizierungsdiensteanbieter **fortgeführt**, so können die auf den von ihm ausgestellten Zertifikaten beruhenden Anwender-Signaturen weiterhin überprüft werden, sodaß weder sein eigenes Zertifikat (vgl. § 9 Abs. 5 Z 2) noch die Anwender-Zertifikate widerrufen werden müssen.

Die Aufsichtsstelle hat – als Aufsichtsmittel – nicht nur die Möglichkeit, das Zertifikat eines Zertifizierungsdiensteanbieters sowie die von ihm ausgestellten Anwender-Zertifikate zu widerrufen (vgl. § 14 Abs. 5), sie kann den Widerruf von Anwender-Zertifikaten auch gegenüber dem Zertifizierungsdiensteanbieter **anordnen** (§ 14 Abs. 1). In diesem Fall muß der Zertifizierungsdiensteanbieter den Widerruf ausführen (**Z 5**).

Die Gefahr einer **mißbräuchlichen Verwendung (Z 6)** besteht etwa bei Verlust oder Kompromittierung des Signaturschlüssels, wenn Signaturschlüssel im Zusammenhang mit Straftaten verwendet werden oder wenn das eingesetzte kryptographische Verfahren nach dem Stand der Technik unsicher wird.

2. In § 9 Abs. 2 wird zwischen dem endgültigen **Widerruf** und der vorläufigen **Sperre** unterschieden. Während ein Widerruf die vorzeitige Beendigung der Gültigkeit eines Zertifikats darstellt, ist eine Sperre als vorübergehendes Aussetzen der Gültigkeit eines Zertifikats zu verstehen. Die Sperre eines Zertifikats muß **unverzüglich** vorgenommen werden. Für den endgültigen Widerruf muß das Eintreten des jeweiligen Widerrufsgrundes feststehen.

3. Der **Zeitpunkt** der Sperre bzw. des Widerrufs (§ 9 Abs. 3) umfaßt das Datum und die Uhrzeit. Angegeben werden muß der Zeitpunkt, zu dem diese Maßnahmen wirksam werden. Aus Gründen der Rechtssicherheit sind **rückwirkende** Maßnahmen **verboten**. Unzulässig ist auch die **Rückgängigmachung** eines Widerrufs.

Die Gültigkeit einer Signatur, die vor dem Zeitpunkt der Sperre (oder des Widerrufs) erstellt wurde, wird durch diese Maßnahmen nicht tangiert. Sicherheit darüber, ob eine Signatur vor oder nach einer solchen Maßnahme erzeugt wurde, kann ein Zeitstempel (§ 10) geben. Das Zertifikat selbst enthält Angaben über Beginn und Ende seiner Gültigkeit. Außerdem muß jedenfalls der Zeitpunkt der Ausstellung und des Widerrufs (Sperre) eines Zertifikats durch den Zertifizierungsdiensteanbieter dokumentiert werden (§ 7 Abs. 1 Z 3).

4. § 9 Abs. 4 betrifft den **Widerrufsdienst**. Jeder Zertifizierungsdiensteanbieter, der einen Widerrufsdienst führt (siehe § 6 Abs. 6) muß elektronische **Sperr- bzw. Widerrufslisten** (in der Regel online) zur Verfügung stellen (§ 6 Abs. 6 und § 7 Abs. 1 Z 2).

5. Die Aufsichtsstelle hat die Zertifikate für die Zertifizierungsdiensteanbieter – die zum Signieren von Anwender-Zertifikaten verwendet werden – auszustellen, wobei die Vorschriften des § 8 (Ausstellung qualifizierter Zertifikate durch Zertifizierungsdiensteanbieter) sinngemäß gelten (§ 13 Abs. 3). § 9 Abs. 5 regelt die Fälle, in denen die **Zertifikate für Zertifizierungsdiensteanbieter** zu widerrufen sind. Die Widerrufsgründe korrespondieren mit den Regelungen in § 12 und in § 14 Abs. 5.

Wird das Zertifikat eines Zertifizierungsdiensteanbieters widerrufen, so sind alle nach diesem Zeitpunkt von den Anwendern erstellten Signaturen ungültig. In diesem Fall müssen auch die bestehenden Anwender-Zertifikate widerrufen werden (§ 9 Abs. 1 Z 4 und § 14 Abs. 5). Die Fortführung der Widerrufsdienste muß jedoch sichergestellt sein, damit die **vor** dem Widerruf des Diensteanbieter-Zertifikats erstellten Anwender-Signaturen ordnungsgemäß überprüft werden können.

Zu § 10 des Entwurfs:

Ein **Zeitstempel** ist eine automatisch erteilte, elektronisch signierte Bescheinigung eines Zertifizierungsdiensteanbieters, daß (ihm) bestimmte elektronische Daten zu einem bestimmten Zeitpunkt vorgelegen sind (vgl. auch die Erläuterungen zu § 7 Abs. 1 Z 3 und zu § 9 Abs. 3).

Auch ein **reiner “Zeitstempeldiensteanbieter”** ist nach den Begriffsbestimmungen des § 2 Z 10 und 11 als Zertifizierungsdiensteanbieter zu qualifizieren und unterliegt daher der Aufsicht.

Die bereitgestellten Zeitstempeldienste sind im Sicherheits- und im Zertifizierungskonzept zu beschreiben. **Sichere** Zeitstempeldienste (vgl. § 7 Abs. 1 Z 3) müssen auf einem qualifizierten Zertifikat beruhen und dürfen nur mit **geeigneten** technischen Komponenten und Verfahren im Sinn des § 18 erstellt werden.

Zu § 11 des Entwurfs:

1. Die **Dokumentation (Protokollierung)** der Sicherheitsmaßnahmen soll vor allem dazu beitragen, daß wirksame Kontrollen durchgeführt und mögliche – auch haftungsrelevante – Pflichtverletzungen festgestellt werden können. Die Dokumentation der Zertifikate ist erforderlich, um elektronische Signaturen jederzeit zuverlässig überprüfen zu können. Die Aufbewahrungsdauer der Dokumentation wird durch die Signaturverordnung festgelegt (§ 25 Z 9).

2. In § 11 Abs. 2 wird angeordnet, daß die Dokumentation auch für gerichtliche oder behördliche Verfahren zur Verfügung stehen muß. Das Auskunftsersuchen muß im Einklang mit den jeweils anwendbaren Verfahrensvorschriften stehen.

Zu § 12 des Entwurfs:

Diese Bestimmung betrifft den Fall, daß ein Zertifizierungsdiensteanbieter **freiwillig** seinen Betrieb (zur Gänze) **einstellt**. Die Regelung soll nach Möglichkeit sicherstellen, daß die Anwender-Signaturen auch nach Einstellung der Tätigkeit zuverlässig überprüft werden können. Dies setzt voraus, daß zumindest die **Verzeichnis- und Widerrufsdienste** – von einem anderen Zertifizierungsdiensteanbieter – **fortgeführt** werden. Im Fall der Übernahme der Zertifikate (samt der Dokumentation nach § 11) durch einen anderen Zertifizierungsdiensteanbieter liegt eine Vertragsübernahme vor, die jedoch ex lege nicht an die Zustimmung des Signators geknüpft ist, zumal er den Widerruf seines Zertifikats jederzeit veranlassen kann. Findet eine Übernahme der Verzeichnis- und Widerrufsdienste nicht statt, so muß der Zertifizierungsdiensteanbieter alle gültigen Anwender-Zertifikate widerrufen (§ 9 Abs. 1 Z 4). Allfällige Ansprüche der Signatoren aus der vorzeitigen Beendigung des Vertragsverhältnisses bleiben unberührt. Im Interesse der Rechtssicherheit müssen jedenfalls die **Widerrufsdienste** weitergeführt werden, damit die vor der Einstellung der Tätigkeit erstellten Anwender-Signaturen ordnungsgemäß überprüft werden können (siehe auch die Erläuterungen zu § 9 Abs. 5 und zu § 14 Abs. 5). Nötigenfalls hat die Aufsichtsstelle auf Kosten des Zertifizierungsdiensteanbieters hiefür Sorge zu tragen.

Die Vorschriften des § 12 gelten auch im Falle eines **Konkurs- oder Ausgleichsverfahrens** über das Vermögen des Zertifizierungsdiensteanbieters. Wird das Unternehmen vom Masseverwalter bzw. Ausgleichsverwalter nicht selbst weitergeführt, so kann er sämtliche Dienste oder nur die Verzeichnis- und Widerrufsdienste an einen anderen Zertifizierungsdiensteanbieter weitergeben. Andernfalls sind die Anwender-Zertifikate zu widerrufen. Die in einem solchen Fall für die Weiterführung der Widerrufsdienste durch die Aufsichtsstelle auflaufenden Kosten stellen bevorrechtete Forderungen im Insolvenzverfahren über das Vermögen des Zertifizierungsdiensteanbieters dar.

Zu § 13 des Entwurfs:

1. Als **Aufsichtsstelle** für Zertifizierungsdiensteanbieter ist die **Telekom-Control-Kommission** vorgesehen. Es handelt sich dabei um eine nach § 110 TKG eingerichtete Kollegialbehörde mit richterlichem Einschlag. Sie hat die – auch in Art. 3 Abs. 3 der Richtlinie vorgesehene – Aufgabe, die Aufsicht über die heimischen Zertifizierungsdiensteanbieter auszuüben. Die Durchführung der Aufsicht wird vor allem in der Vornahme **regelmäßiger Kontrollen** bestehen, bei denen geprüft wird, ob die gesetzlichen Bestimmungen bei der Ausübung der Tätigkeit als Zertifizierungsdiensteanbieter eingehalten werden. Weiters hat die Aufsichtsstelle die Zertifikate für Zertifizierungsdiensteanbieter auszustellen, die nur zum Signieren von Anwender-Zertifikaten verwendet werden dürfen. Die Gültigkeitsdauer der Zertifikate für Zertifizierungsdiensteanbieter muß mit dem spätest möglichen Zeitpunkt der nächsten Kontrolle begrenzt werden. Auf Antrag und bei Vorliegen der Voraussetzungen hat die Aufsichtsstelle auch Zertifikate für **ausländische** Zertifizierungsdiensteanbieter auszustellen.

2. In § 13 Abs. 2 werden die **wesentlichen Aufgaben** der Aufsichtsstelle beispielhaft angeführt. Insbesondere muß sichergestellt werden, daß die Zertifizierungsdiensteanbieter die Angaben im Sicherheits- und im Zertifizierungskonzept einhalten (**Z 1**) und daß für **sichere** elektronische Signaturen nur geeignete technische Komponenten und Verfahren verwendet werden (**Z 2**). Der Aufsichtsstelle kommt weiters die organisatorische Aufsicht über die Bestätigungsstellen (zB Entgegennahme und Behandlung von Beschwerden über deren Tätigkeit, ohne daß damit ein Rechtsanspruch verbunden wäre) zu (**Z 4**), sie hat diesen gegenüber – wegen deren Unabhängigkeit – jedoch kein Weisungsrecht in technischen Belangen.

3. Wie schon dargelegt, hat die Aufsichtsstelle die **Zertifikate für Zertifizierungsstellen** auszustellen (§ 13 Abs. 3). Hiefür gelten die Bestimmungen des § 8 sinngemäß. Wie alle qualifizierten Zertifikate (§ 5 Abs. 3) müssen auch die von der Aufsichtsstelle ausgestellten Zertifikate sicher signiert werden. Das hiefür erforderliche qualifizierte Zertifikat stellt sich die Aufsichtsstelle selbst aus. Der Widerruf der von der Aufsichtsstelle – für Zertifizierungsdiensteanbieter – ausgestellten Zertifikate ist in § 9 Abs. 5 geregelt. Die von der Aufsichtsstelle verwendeten technischen Produkte, Verfahren und sonstige Mittel müssen den Anforderungen des § 18 entsprechen. Im Sinn des § 6 Abs. 1 ist die Aufnahme der Tätigkeit eines Zertifizierungsdiensteanbieters nicht daran geknüpft, daß für ihn ein Zertifikat bereits ausgestellt wurde.

Bei der Aufsichtsstelle sind – von der Telekom-Control GmbH (siehe § 15 Abs. 2 Z 3) – elektronisch (online) **Verzeichnisse** zu führen über

- die Zertifikate für Zertifizierungsdiensteanbieter sowie eine entsprechende Widerrufsliste,
- die im Inland niedergelassenen Zertifizierungsdiensteanbieter,
- die akkreditierten Zertifizierungsdiensteanbieter (siehe § 17 Abs. 1),
- die Drittstaaten-Zertifizierungsdiensteanbieter nach § 24 Abs. 2 Z 2 und
- allfällige andere ausländische Zertifizierungsdiensteanbieter (auf Antrag).

4. Die **Finanzierung** der Tätigkeit der Aufsichtsstelle – und der Telekom-Control GmbH – erfolgt dadurch, daß für die konkret erbrachten Leistungen von den Zertifizierungsdiensteanbietern ein kostendeckendes Entgelt erbracht werden muß (§ 13 Abs. 4). Bedient sich die Aufsichtsstelle oder die Telekom-Control GmbH der Bestätigungsstelle (§ 13 Abs. 5 bzw. § 15 Abs. 3), so gehören die für die Tätigkeit der Bestätigungsstelle auflaufenden Kosten zu den Kosten des Aufsichtsverfahrens, die ebenfalls von der Aufsichtsstelle vorzuschreiben sind.

5. Die Aufsichtsstelle hat auch für die **fortwährende Einhaltung** der Sicherheitsanforderungen durch die Zertifizierungsdiensteanbieter Sorge zu tragen. Dabei ist vor allem auf die ständige Aufrechterhaltung der Qualität der bereitgestellten Signatur- und Zertifizierungsdienste Bedacht zu nehmen. Die technische Sachkunde ist insbesondere bei der Bestätigungsstelle (oder den Bestätigungsstellen) nach § 19 konzentriert. Soweit dies aus technischer Sicht für die Durchführung der Aufsicht angezeigt ist, hat die Aufsichtsstelle daher ein **Gutachten** einer Bestätigungsstelle einzuholen (§ 13 Abs. 5).

6. In § 13 Abs. 6 werden die **Weisungsfreiheit** der Mitglieder der Aufsichtsstelle (wie in § 114 TKG) statuiert sowie die anzuwendenden Verfahrensvorschriften und der Instanzenzug (vgl. § 115 TKG) festgelegt. Aus rechtsstaatlicher Sicht erscheint die Anrufbarkeit des Verwaltungsgerichtshofs geboten.

Zu § 14 des Entwurfs:

1. In § 14 Abs. 1 werden die **Aufsichtsmittel** beschrieben. Die Aufsichtsstelle kann alle geeigneten Maßnahmen ergreifen, um die Einhaltung der gesetzlichen Vorschriften zu gewährleisten. Sie kann etwa die Verwendung bestimmter technischer Komponenten und Verfahren verbieten, Zertifikate für Zertifizierungsdiensteanbieter oder der Signatoren widerrufen (vgl. auch § 9 Abs. 1 Z 5). Weiters kann sie einem Zertifizierungsdiensteanbieter die Ausübung der Tätigkeit (ganz oder teilweise) **untersagen**. Eine teilweise Untersagung kann zB darin bestehen, daß zunächst keine weiteren Anwender-Zertifikate ausgestellt werden dürfen.

2. In § 14 Abs. 2 wird näher geregelt, unter welchen Voraussetzungen eine – gänzliche oder teilweise – **Untersagung** angeordnet werden kann. Diese Bestimmung gilt gegenüber allen Zertifizierungsdiensteanbietern, also auch gegenüber solchen, die keine oder nur einfache Zertifikate anbieten.

Für die Tätigkeit eines Zertifizierungsdiensteanbieters ist zunächst Voraussetzung, daß die für die angebotenen Dienste erforderliche **Zuverlässigkeit** gegeben ist (**Z 1**; vgl. auch § 7 Abs. 1 Z 1).

Die geforderte **Fachkunde** (**Z 2**) erstreckt sich auf den rechtlichen sowie den technisch-administrativen Bereich und soll eine vollständige und wirksame Umsetzung der gesetzlichen Vorgaben gewährleisten (vgl. auch § 7 Abs. 1 Z 5).

Über die ausreichenden **Finanzmittel** (**Z 3**) sind in der Signaturverordnung nähere Aussagen zu treffen (vgl. auch § 7 Abs. 1 Z 6).

Z 4 unterstreicht die Bedeutung des Sicherheits- sowie des Zertifizierungskonzepts.

In **Z 5** wird zum Ausdruck gebracht, daß den **Verzeichnis- und Widerrufsdiensten** – insbesondere zur zuverlässigen Überprüfung elektronischer Signaturen – besondere Bedeutung zukommt. Diese Bestimmung gilt nur, sofern solche Dienste geführt werden (vgl. § 6 Abs. 6). In der Policy muß angegeben werden, wie der Verzeichnis- und der Widerrufsdienst bei nicht-qualifizierten Zertifikaten erbracht wird (etwa auch per E-mail). Zur Sperr- und Widerrufspflicht eines Zertifizierungsdiensteanbieters sei auf die Erläuterungen zu § 9 Abs. 1 und Abs. 2 verwiesen.

3. § 14 Abs. 3 sieht **weitere** Untersagungsgründe für Diensteanbieter, die qualifizierte Zertifikate ausstellen, vor. Dabei wird insbesondere auf die Anforderungen der §§ 5 und 7 abgestellt.

4. Für die Bereitstellung **sicherer** elektronischer Signaturverfahren kommt der Einhaltung der vorgeschriebenen Sicherheitsanforderungen größte Bedeutung zu, weil mit sicheren elektronischen Signaturen besondere Rechtswirkungen verknüpft sind. Diesem Problem trägt § 14 Abs. 4 Rechnung. Die Verwendung sicherheitsgeprüfter technischer Komponenten und Verfahren im Sinn des § 18 ist wesentlicher Bestandteil der gesetzlich vorgegebenen Maßnahmenkombination, die es ermöglicht, eine sichere elektronische Signatur dem Signator zuverlässig zuzuordnen. Gelangen keine **geeigneten** technischen Komponenten und Verfahren zum Einsatz, so liegt ebenfalls ein Untersagungsgrund vor.

5. In § 14 Abs. 5 werden die im Fall der **Untersagung** der Tätigkeit eines Zertifizierungsdiensteanbieters zu treffenden Maßnahmen festgelegt. Die Aufsichtsstelle hat zunächst die Möglichkeit, die Übernahme entweder der gesamten Tätigkeit oder nur der Verzeichnis- und Widerrufsdienste durch einen anderen Zertifizierungsdiensteanbieter vorzusehen. Bei einer bloß teilweisen Untersagung können die **Verzeichnis- und Widerrufsdienste** auch vom betroffenen Zertifizierungsdiensteanbieter fortgeführt werden. Werden diese Dienste nicht weitergeführt, so müssen sowohl das Zertifikat des Zertifizierungsdiensteanbieters als auch jene der Signatoren widerrufen werden. Einer Übernahme müssen alle beteiligten Zertifizierungsdiensteanbieter, also auch der "Untersagte", zustimmen. Es muß also ein **Übernahmevertrag** abgeschlossen werden. Eine Zustimmung der Signatoren ist hingegen nicht notwendig, weil sie die Möglichkeit haben, das Zertifikat zu widerrufen oder nicht zu verwenden (siehe dazu auch die Erläuterungen zu § 12).

Kommt eine Übernahme der Tätigkeit oder eine Weiterführung der Verzeichnis- und Widerrufsdienste nicht zustande, so hat die Aufsichtsstelle den **Widerruf** der Zertifikate des Zertifizierungsdiensteanbieters und der Signatoren zu veranlassen. Im Interesse der Rechtssicherheit ist auch im Widerrufsfall sicherzustellen, daß die **Widerrufsdienste** fortgeführt werden, damit die Anwender-Signaturen, die vor dem Widerruf der Zertifikate erstellt wurden, ordnungsgemäß überprüft werden können (siehe auch die Erläuterungen zu § 12 und § 9 Abs. 5). Dafür hat zunächst der untersagte Zertifizierungsdiensteanbieter Sorge zu tragen. Kommt er dieser Verpflichtung nicht nach, so hat dies die Aufsichtsstelle – auf Kosten des "untersagten" Zertifizierungsdiensteanbieters – zu veranlassen.

6. § 14 Abs. 6 sieht vor, daß die Aufsichtsstelle gegenüber den Zertifizierungsdiensteanbietern auch **gelindere Mittel** einsetzen kann, um die Einhaltung der gesetzlichen Vorschriften sicherzustellen. Die Untersagung der Tätigkeit soll letztlich die ultima ratio darstellen.

Zu § 15 des Entwurfs:

1. Zur Durchführung der operativen Aufsichtstätigkeit muß sich die in der Regel nur alle 14 Tage tagende Telekom-Control-Kommission der nach § 108 TKG eingerichteten, nicht gewinnorientierten **Telekom-Control GmbH** bedienen können (siehe § 15 Abs. 1). Die Telekom-Control GmbH übt insbesondere vorbereitende und unterstützende Tätigkeiten für die Aufsichtsstelle aus.

2. In § 15 Abs. 2 werden die Aufgaben der Telekom-Control GmbH beispielhaft beschrieben.

Nach **Z 1** hat die Telekom-Control GmbH das sogenannte "Tagesgeschäft" im Rahmen der Aufsichtstätigkeit auszuüben. Sie hat auch die laufenden Kontrollen der Zertifizierungsdiensteanbieter **vor Ort** vorzunehmen und dabei insbesondere die zum Einsatz gelangenden technischen Mittel auf ihre Eignung sowie das dort tätige Personal auf seine Fachkunde hin zu überprüfen. Die Telekom-Control GmbH wird dabei jeweils **auf Anordnung** der Aufsichtsstelle tätig. Sie hat dafür Sorge zu tragen, daß die Aufsicht schnell und effektiv ausgeübt werden kann.

Weiters hat die Telekom-Control GmbH die Registrierung der Zertifizierungsdiensteanbieter nach deren Anmeldung vorzunehmen (**Z 2**), die bei der Aufsichtsstelle einzurichtenden Verzeichnisse (siehe dazu § 13 Abs. 3 und § 17 Abs. 1, auch § 12 und § 14 Abs. 5) zu führen (**Z 3 und 4**) sowie das Akkreditierungsverfahren durchzuführen (**Z 5**).

Ist die Gleichwertigkeit von Produktbewertungen aus Drittstaaten (§ 24 Abs. 3) zu beurteilen, so hat die Telekom-Control GmbH die entsprechenden Vorarbeiten zu leisten (**Z 6**).

Besteht ein begründeter Verdacht, daß die vorgeschriebenen Sicherheitsanforderungen, etwa durch Kompromittierung oder Verlust des Signaturschlüssels des Zertifizierungsdiensteanbieters oder durch einen Einbruch oder einen Brand, nicht mehr eingehalten sind, so muß im Rahmen der Aufsicht rasch reagiert werden. In einem solchen Fall hat daher die Telekom-Control GmbH **unverzüglich die notwendigen Veranlassungen** (Untersagung der Tätigkeit; Sperre der Zertifikate oder Anordnung, keine Zertifikate auszustellen; Untersagung ungeeigneter Komponenten) zu treffen (**Z 7**). Diese Maßnahmen sind **vorläufiger** Natur. Die endgültige Entscheidung hat die Aufsichtsstelle zu treffen, die

die Maßnahmen der Telekom-Control GmbH auch rückgängig machen kann. Hat die Telekom-Control GmbH den Widerruf von Zertifikaten zu Unrecht angeordnet, so können die Widerrufsinformationen ausnahmsweise rückgängig gemacht werden.

3. In § 15 Abs. 3 wird ausdrücklich angeordnet, daß die Telekom-Control GmbH die Aufsichtsstelle in organisatorischer Hinsicht sowie im operativen Bereich zu **unterstützen** hat. Diese Bestimmung entspricht § 109 letzter Satz TKG.

Soweit dies für die Besorgung der Aufgaben der Telekom-Control GmbH aus **technischer Sicht** erforderlich ist, hat auch sie eine Bestätigungsstelle beizuziehen.

Da die Telekom-Control GmbH als **beliehener Unternehmer** anzusehen ist, unterliegen ihr Personal sowie die sonst für sie tätigen Personen der Verpflichtung zur Amtsverschwiegenheit nach Art. 20 Abs. 3 B-VG. Diese Verpflichtung trifft alle Organe, die mit Aufgaben der Bundes-, Landes- oder Gemeindeverwaltung betraut sind, unabhängig von ihrer Rechtsstellung und unabhängig davon, ob das betreffende Organ Aufgaben der Hoheits- oder der Privatwirtschaftsverwaltung zu besorgen hat.

4. In § 15 Abs. 4 wird – ohne dadurch den Justizgewährungsanspruch auszuschließen – ein Streit-schlichtungsverfahren, das den Bestimmungen des § 116 Abs. 1 und 2 TKG nachgebildet ist, eingerichtet.

Zu § 16 des Entwurfs:

1. In § 16 Abs. 1 werden der Aufsichtsstelle und den in ihrem Auftrag handelnden Personen (insbesondere den Bediensteten der Telekom-Control GmbH) die zur Vornahme der Aufsicht notwendigen prozessualen **Eingriffsbefugnisse** (Betretungs-, Besichtigungs- und Auskunftsrechte) eingeräumt. Der Aufsichtsstelle und den in ihrem Auftrag handelnden Personen sind alle aufsichtsrelevanten, also für die Vollziehung des Signaturgesetzes (und der Signaturverordnung) notwendigen Informationen zu erteilen.

Nach den jeweils anwendbaren Verfahrensvorschriften bestehende berufliche **Verschwiegenheitspflichten** und **Aussageverweigerungsrechte** bleiben unberührt.

2. Die **Hilfeleistungspflicht** der Organe des öffentlichen Sicherheitsdienstes nach § 16 Abs. 2 soll sicherstellen, daß die Aufsichtsmaßnahmen, insbesondere die regelmäßigen Kontrollen, auch tatsächlich durchgeführt werden können.

3. § 16 Abs. 3 sieht für die Vornahme der Aufsichtsmaßnahmen eine **„Schonungsklausel“** zugunsten der Betroffenen vor. Die eingesetzten Aufsichtsmittel müssen **verhältnismäßig** sein. Weiters wird hervorgehoben, daß die **Sicherheit** der Signatur- und Zertifizierungsdienste die oberste Maxime ist. Aufsichtsmaßnahmen dürfen also etwa nicht dazu führen, daß der private Signaturschlüssel des Zertifizierungsdiensteanbieters bekannt wird.

Zu § 17 des Entwurfs:

1. Nach Art. 3 Abs. 2 der Richtlinie sind – quasi als Ausgleich für das Verbot von Genehmigungs- bzw. Lizenzierungsverfahren – **freiwillige Akkreditierungssysteme**, die auf höherwertige Zertifizierungsdienste abzielen, zulässig. Die Anzahl der akkreditierten Zertifizierungsdiensteanbieter darf von den Mitgliedstaaten nicht beschränkt werden. In Erwägungsgrund 11 wird ausgeführt, daß durch die Bereitstellung **hochwertiger Dienste** das notwendige Maß an Vertrauen, Sicherheit und Qualität erreicht werden könne. Unter freiwilliger Akkreditierung sei eine Erlaubnis der Überwachungsbehörde (Aufsichtsstelle) zu verstehen, mit der Rechte und Pflichten eines Zertifizierungsdiensteanbieters auf seinen Antrag hin festgelegt werden. Die besonderen Rechte dürften erst mit Zustellung des **„Bescheides“** der Überwachungsstelle ausgeübt werden.

Die Akkreditierung (§ 17 Abs. 1) ist also eine von der Aufsichtsstelle vorgenommene **ex ante-Überprüfung** der Einhaltung der im Gesetz vorgeschriebenen Anforderungen (insbesondere der §§ 5, 7 und 18) durch die Zertifizierungsdiensteanbieter. Sie kann nur auf Antrag des Zertifizierungsdiensteanbieters, also **freiwillig** erfolgen. Die Akkreditierung stellt eine zusätzliche vertrauensbildende Maßnahme dar, weil von vornherein feststeht, daß die gesetzlichen Anforderungen erfüllt sind.

Mit der Akkreditierung sollen für den Zertifizierungsdiensteanbieter **besondere Rechte** verbunden sein. Als solche Rechte kommen besondere Werbe- und Marketingmaßnahmen, wie die Bezeichnung als **„akkreditierter Zertifizierungsdiensteanbieter“** im Geschäftsverkehr oder die Verwendung eines Logos, in Betracht. Die Bezeichnung **„akkreditierter Zertifizierungsdiensteanbieter“** kann etwa auf dem

Briefpapier oder einer Webseite verwendet werden. Die besonderen Rechtswirkungen nach §4 (Art. 5 Abs. 1 der Richtlinie) dürfen aber **nicht** von einer Akkreditierung abhängig gemacht werden.

Da die Akkreditierung auf **hochwertige**, also qualitätsgesicherte Dienste abzielt, kommt sie nur in Verbindung mit **sicheren Signaturen** in Betracht. Auch eine nachträgliche Akkreditierung, also nach Aufnahme der Tätigkeit als Zertifizierungsdiensteanbieter, ist denkbar. In einem solchen Fall dürfen die sicheren Signaturen und die entsprechenden qualifizierten Zertifikate, auf die sich die Akkreditierung bezieht, aber erst nach erfolgter Akkreditierung bereitgestellt werden. Werden die gesetzlichen Anforderungen nach erfolgter Akkreditierung nicht mehr erfüllt, so darf diese Bezeichnung auch nicht mehr geführt werden. Die akkreditierten Zertifizierungsdiensteanbieter sind in ein bei der Aufsichtsstelle zu führendes Verzeichnis aufzunehmen (vgl. auch § 13 Abs. 3).

2. Eine freiwillige Akkreditierung muß – als wichtiger Beitrag zur Schaffung von Vertrauen – **auch im Außenverhältnis** bei der Verwendung von Zertifikaten in Erscheinung treten. Dieser Umstand soll für jeden Empfänger einer auf akkreditierten Diensten beruhenden Signatur transparent sein. Die Akkreditierung muß daher gemäß § 17 Abs. 2 in das Zertifikat aufgenommen **oder auf sonstige Weise** (in der Regel online) **zugänglich gemacht** werden.

3. Mit § 17 Abs. 3 wird klargestellt, daß die Aufsicht, also die laufende Überprüfung der Zertifizierungsdiensteanbieter, auch im Falle der Akkreditierung **unberührt** bleibt. Die Anforderungen, insbesondere die Sicherheitsanforderungen, müssen ständig eingehalten sein. Läßt sich ein **ausländischer** Zertifizierungsdiensteanbieter im Inland akkreditieren, so erstreckt sich die Aufsicht der Aufsichtsstelle auch auf diesen Zertifizierungsdiensteanbieter.

Zu § 18 des Entwurfs:

1. Die Abs. 1 bis 3 des § 18 enthalten die **sicherheitstechnischen** Zielvorgaben, die von den technischen Komponenten und Verfahren – für **sichere** Signaturen – erfüllt werden müssen. Nähere Aussagen über deren technische und kryptographische Realisierung sind in der Signaturverordnung zu treffen.

Diese Vorschriften beziehen sich sowohl auf die **Signaturprodukte und Verfahren**, die beim Zertifizierungsdiensteanbieter zum Einsatz gelangen (siehe dazu § 7 Abs. 2), als auch auf jene, die von den **Signatoren** verwendet werden. Die Signatoren müssen über das Erfordernis geeigneter technischer Komponenten sowie über die in Frage kommenden technischen Produkte und Verfahren vom Zertifizierungsdiensteanbieter unterrichtet werden (siehe dazu § 20). Dies gilt insbesondere für die bei der Aufbereitung und **Darstellung** zu signierender (oder zu prüfender) Daten zu verwendenden geeigneten Komponenten.

Die **sicherheitstechnischen** Anforderungen entsprechen den Vorgaben der Richtlinie. Für **Zertifizierungsdiensteanbieter** ergeben sich diese Anforderungen aus Anhang II, sie werden – systemkonform – in § 7 Abs. 2 dargestellt. Während die dortigen Anforderungen sowohl **organisatorische** als auch **technische** Aspekte betreffen, bezieht sich § 18 allein auf **sicherheitstechnische** Belange. Bei der Erzeugung (Generierung) und Speicherung privater Signaturschlüssel (von Signaturerstellungsdaten) muß deren **Vertraulichkeit** gewahrt werden. Es muß auch ein wirksamer Schutz vor dem Ausspähen oder einem sonstigen Ermitteln der Signaturerstellungsdaten durch Dritte gegeben sein. Die **Zertifikate** (Abs. 3) müssen vor Fälschung, Verfälschung, unbefugtem Widerruf sowie vor Beseitigung der Widerrufsinformation geschützt sein.

Die **zwingenden** Sicherheitsanforderungen, die Produkte und Verfahren der Anwender betreffen, beziehen sich (nur) auf die **Erstellung** sicherer Signaturen, also auf die **Signaturerstellungseinheiten und Signaturerstellungsdaten** (Hardware, Software und mathematische Verfahren). Die technischen Komponenten (und Verfahren) müssen gewährleisten, daß eine sichere Signatur nicht unbemerkt gefälscht und signierte Daten nicht unbemerkt verfälscht werden können. Werden für die Erstellung einer sicheren Signatur geeignete technische Komponenten eingesetzt und werden der private Signaturschlüssel und die zu seiner Anwendung benötigten Identifikationsdaten (PIN oder Paßwort) vor unbefugtem Zugriff geschützt, so sind die signierten Daten mit an Sicherheit grenzender Wahrscheinlichkeit **sicher** vor Fälschung und Verfälschung (**Abs. 1**).

Die **Sicherheitsanforderungen** an die Signaturerstellungseinheiten (Produkte und Verfahren) werden in **Abs. 2** umgesetzt. Die Erstellung einer **sicheren** Signatur erfordert, daß der durch einen Zertifizierungsdiensteanbieter zugeordnete Signaturschlüssel "praktisch" nur ein Mal vorkommt. Dies kann mathematisch/technisch gewährleistet werden. Es stehen Schlüsselgenerierungs-Algorithmen zur Verfügung, die eine nahezu unbegrenzte Anzahl unterschiedlicher Signaturschlüssel erzeugen, sodaß die Erzeugung von zwei gleichen Schlüsselpaaren praktisch ausgeschlossen ist.

Der private Signaturschlüssel kann zB auf einer Chipkarte so gespeichert werden, daß er nicht ausgelesen werden kann (allenfalls mit aufwendigsten Analyseverfahren bei Zerstörung einer Karte). Die Erzeugung des Schlüsselpaars kann **auf der Chipkarte** selbst erfolgen, und zwar derart, daß der private Signaturschlüssel die Karte niemals verläßt. Erfolgt die Schlüsselgenerierung außerhalb der Karte, so kann das Laden der Chipkarte mit dem privaten Schlüssel technisch und organisatorisch so gestaltet werden, daß die Einmaligkeit und Geheimhaltung des privaten Schlüssels zuverlässig gewahrt ist. Denkbar ist auch, daß bestimmte Teile des Signaturschlüssels beim Diensteanbieter (Qualität des Zufalls und Einzigartigkeit) und die restlichen Teile auf der Chipkarte (persönliche, geheimgehaltene Zufallskomponenten) erzeugt werden.

Die zum Signieren benötigten mathematischen Verfahren (Hash-Algorithmen und Signatur-Algorithmen) sind laufend Gegenstand weltweiter wissenschaftlicher Diskussion und werden – zB je nach Länge des Signaturschlüssels – **nach dem jeweiligen Stand der Technik** als brauchbar oder nicht brauchbar beurteilt. Die technische Implementierung der mathematischen Verfahren kann nach dem Stand der Technik ebenfalls auf eine Weise erfolgen und geprüft werden, bei der sicherheitsrelevante Fehler oder Manipulationen ausreichend ausgeschlossen sind. Die **Signaturkomponenten**, insbesondere auch Chipkarten, können daher als “sicher” bezeichnet werden.

Um eine **mißbräuchliche Verwendung** von Signaturkomponenten **auszuschließen**, muß eine zuverlässige Zuordnung des Signaturschlüsselpaars zum Signator (durch ein fälschungssicheres Zertifikat) und eine zuverlässige Identifikation des Signators durch die Signaturerstellungseinheit (zB Chipkarte) **vor** Auslösung der Signaturfunktion durch Besitz (Chipkarte) und Wissen (PIN oder Paßwort) erfolgen.

Der Signator muß die Möglichkeit haben, daß ihm die zu signierenden Daten **vor dem Signaturvorgang dargestellt** werden. Diese Darstellung muß so erfolgen, daß der Nutzer sicher sein kann, daß die auf dem Bildschirm angezeigten Daten mit den signierten Daten übereinstimmen (“Viewer-Funktion”). Da die Darstellung vor Erstellung der Signatur erfolgen muß, ist auch gewährleistet, daß dem Signator der Signaturvorgang **bewußt** ist.

Die dargestellten Sicherheitsanforderungen müssen auch für die **sicheren** Signaturen der Zertifizierungsdiensteanbieter sowie der Aufsichtsstelle erfüllt sein (vgl. § 5 Abs. 3 und § 13 Abs. 3).

2. In § 18 Abs. 4 werden die Anforderungen an technische Komponenten und Verfahren für eine **sichere Signaturprüfung** dargestellt. Entsprechend den Vorgaben der Richtlinie (Art. 3 Abs. 6) handelt es sich dabei um **Empfehlungen**, die in **Anhang IV** zur Richtlinie aufgelistet werden. Der bloß empfehlende Charakter des Anhangs IV stellte in der Ratsarbeitsgruppe letztlich den Kompromiß zwischen den Mitgliedstaaten, die auf die Sicherstellung eines ausreichenden Sicherheitsstandards Wert legten, und den hier eher “liberalen” Mitgliedstaaten dar.

Bei der (automatischen) sicheren **Prüfung** einer elektronischen Signatur muß insbesondere gewährleistet sein, daß die signierten Daten korrekt dargestellt sind und keine unrichtige Korrektheitsbestätigung der Signatur erfolgt. Sowohl bei einer Fälschung der Signatur als auch bei einer Verfälschung der signierten Daten muß eine Fehlermeldung erfolgen. Außerdem muß (über den zertifizierten öffentlichen Schlüssel) der Signator erkennbar sein.

3. Die Sicherheitsanforderungen an technische Komponenten und Verfahren hängen maßgeblich vom **Stand der Technik** ab. Daher müssen etwa auch laufende Technologiebeobachtungen stattfinden. Im Interesse der Rechtssicherheit sowie aus Gründen des Kunden- und Verbraucherschutzes erscheint es nicht ausreichend, daß sich die beteiligten Verkehrskreise auf Sicherheitsangaben der Hersteller oder der Zertifizierungsdiensteanbieter verlassen müssen. Die Einhaltung der normierten **Sicherheitsstandards** durch die verwendete Technologie und die eingesetzten Verfahren ist insbesondere für den Anwender kaum durchschaubar. Sie muß daher verlässlich nachgewiesen werden, damit er in das technische Verfahren Vertrauen haben und sich auf das Eintreten der gewünschten Rechtsfolgen verlassen kann. Die Einhaltung der Sicherheitsanforderungen für **sichere** elektronische Signaturen muß durch eine vertrauenswürdige, objektive und über das erforderliche technische Know-how verfügende Stelle nachgewiesen werden. Dem Anwender muß schon vor Verwendung eines bestimmten Signaturverfahrens klar sein, welche Rechtswirkungen damit ausgelöst werden können.

Aus diesen Erwägungen heraus müssen Signaturprodukte und technische Verfahren, die zur Bereitstellung und Verwendung **sicherer** elektronischer Signaturen eingesetzt werden, auf die Einhaltung der normierten Sicherheitsanforderungen durch eine **Bestätigungsstelle** (§ 19) evaluiert sein (§ 18 Abs. 5). Für **sichere** elektronische Signaturverfahren dürfen also nur von einer Bestätigungsstelle nach dem Stand der Technik **sicherheitsgeprüfte technische Komponenten** zum Einsatz gelangen (siehe auch die Erläuterungen zu § 6 Abs. 3 und zu § 7 Abs. 2). Dieses Konzept ist letztlich auch in die Richtlinie

aufgenommen worden: Nach ihrem Art. 3 Abs. 4 haben die Mitgliedstaaten geeignete "Bestätigungsstellen" der Europäischen Kommission zu notifizieren. Die von solchen **Bestätigungsstellen** anderer EU-Staaten ausgestellten Bescheinigungen (Produktbewertungen) müssen in allen übrigen Mitgliedstaaten der Europäischen Union anerkannt werden.

Für die Überprüfung informationstechnologischer Komponenten auf ihre Sicherheit hin sowie für die entsprechenden **Bestätigungen** über die Einhaltung der Sicherheitsanforderungen bedarf es insbesondere der höchsten Fachkunde und Objektivität. Die betreffenden Institutionen müssen etwa auch über aktuelle Erkenntnisse der Sicherheitsbehörden zu relevanten kriminellen Aktivitäten (zB spezielle technische Eingriffe) sowie über relevante Erkenntnisse von vergleichbaren Einrichtungen im Ausland verfügen.

Zur Gründung des Vereins "**Zentrum für sichere Informationstechnologie – Austria (A-SIT)**" sei auf die Ausführungen im Allgemeinen Teil zum Abschnitt "Kosten" verwiesen. Dem A-SIT soll aber keine "Monopolstellung" eingeräumt werden. In § 19 Abs. 3 ist eine entsprechende Verordnungsermächtigung vorgesehen, derzufolge auch andere Institutionen mit der Funktion als Bestätigungsstelle betraut werden können, soweit sie insbesondere über entsprechende Fachkunde und technische Mittel verfügen sowie Unabhängigkeit und Objektivität gewährleisten.

Zu § 19 des Entwurfs:

1. Zur Gewährleistung der **Sicherheit** elektronischer Signaturverfahren kommt der Vertrauenswürdigkeit und fachlichen Kompetenz der **Bestätigungsstelle** entscheidende Bedeutung zu. Entsprechend der Bestimmung des Art. 3 Abs. 4 der Richtlinie wird daher in § 19 Abs. 1 angeordnet, daß mit den Aufgaben einer Bestätigungsstelle nur eine **geeignete Einrichtung** betraut werden kann.

2. In § 19 Abs. 2 werden die **Kriterien der Eignung** einer Bestätigungsstelle näher umschrieben. Im besonderen wird ausdrücklich festgehalten, daß eine derartige Einrichtung über die erforderlichen Fachkenntnisse und technischen Mittel verfügen sowie Unabhängigkeit und Objektivität gewährleisten muß. Da sich die Beurteilung der Sicherheitsanforderungen nach dem jeweiligen **Stand der Technik** zu richten hat, muß auch eine laufende Technologiebeobachtung stattfinden.

3. In Art. 3 Abs. 4 der Richtlinie ist vorgesehen, daß die **Kriterien** für die Eignung einer (Bestätigungs-) Stelle zur Beurteilung der Einhaltung der Sicherheitsanforderungen des Anhangs III (§ 18) durch Signaturerstellungseinheiten von der Europäischen Kommission im **Komitologieverfahren** (Verwaltungsausschuß) festgelegt werden. Sobald solche harmonisierten Kriterien vorliegen, muß sich die Beurteilung der Eignung einer solchen Stelle nach diesen Kriterien richten.

4. § 19 Abs. 3 enthält die **Verordnungsermächtigung** zur Benennung von Bestätigungsstellen. Für eine solche Benennung muß die Einhaltung der maßgeblichen Kriterien nachgewiesen sein.

Zu den **Aufgaben** einer Bestätigungsstelle sei insbesondere auf die Ausführungen zu den §§ 18 Abs. 5, 7 Abs. 2, 13 Abs. 5 und 15 Abs. 3 sowie auf die Erläuterungen im Allgemeinen Teil im Abschnitt Kosten verwiesen. Die **organisatorische Aufsicht** über die Bestätigungsstellen kommt der Aufsichtsstelle zu (§ 13 Abs. 2 Z 4).

5. Die Bestätigungsstelle hat vor allem die Einhaltung der vorgeschriebenen Sicherheitsanforderungen durch Signaturprodukte und Verfahren (technische Komponenten) zu beurteilen und durch ihre Expertise zu objektivieren. Insbesondere bei der Verwendung von Chipkartentechnologien oder Technologien für Sicherheitsmodule müssen zur Vornahme dieser Beurteilungen in der Regel technische **Prüfergebnisse** zur Verfügung stehen, die nur anhand komplizierter und kostspieliger Prüf- und Meßverfahren (zB Strom- und Signalmessungen im Nano- und Picoampere- bzw. -voltbereich; chemische und optische Technologien sowie kombinierte mechanische und elektronische Verfahren zur Analyse des Verhaltens integrierter Bausteine mit Probenadeln im Micrometerbereich) ermittelt werden können. Da die Anschaffungskosten für derartige Spezialprüf- und -meßgeräte, die in der Regel nur im Herstellungsprozeß verwendet werden können, außerordentlich hoch sind, sollen bestehende Infrastrukturen vor allem bei Herstellern von hochintegrierten elektronischen Bausteinen und anderen Technologieunternehmen genützt werden. Aus diesem Grund wird in § 19 Abs. 4 vorgesehen, daß die Bestätigungsstelle von sonstigen Unternehmen oder Einrichtungen **sicherheitstechnische Prüfberichte** zu Signaturprodukten und Verfahren **einholen** kann. Ein Zertifizierungsdiensteanbieter hat die Möglichkeit, seine Produkte und Verfahren der Bestätigungsstelle vorzulegen, die erforderlichenfalls ihrerseits Prüfberichte einholt. Er kann sich die nötigen Prüfberichte aber auch selbst beschaffen und diese der Bestätigungsstelle zur Evaluierung vorlegen.

6. Im Rahmen des Evaluationsmanagements (siehe die in § 7 Abs. 2 und in § 18 Abs. 5 genannten Befugnisse) obliegt die Beurteilung der anstehenden Fragen allein der Bestätigungsstelle. In diesem Bereich wird sie als beliebige Einrichtung tätig. Bei ihren Stellungnahmen handelt es sich um **gutachterliche Äußerungen** gegenüber dem Antragsteller. Beschwerden über die Tätigkeit der Bestätigungsstelle können nach § 13 Abs. 2 Z 4 an die Aufsichtsstelle herangetragen werden.

Für die Leistungen, die die Bestätigungsstelle als **beliehener Unternehmer** erbringt, hat sie gemäß § 19 Abs. 5 die ihr **zustehenden Gebühren** direkt den Zertifizierungsdiensteanbietern vorzuschreiben (siehe dazu auch § 13 Abs. 4). Die Festlegung des Entgelts für die von der Bestätigungsstelle zu erbringenden Leistungen erfolgt in der Signaturverordnung.

Zu § 20 des Entwurfs:

1. Der **Unterrichtung und Belehrung** der Anwender im Umgang mit Signaturverfahren und Signaturkomponenten kommt besondere Bedeutung zu, um mißbräuchliche Verwendungen zu vermeiden und das Risiko für den einzelnen Anwender zu minimieren. § 20 Abs. 1 gibt die in Anhang II lit. k zur Richtlinie vorgesehenen Belehrungspflichten wieder. Die möglichst umfassende Aufklärung der Anwender ist derart wichtig, daß sie für alle Zertifizierungsdiensteanbieter vorgesehen wird. Diese haben insbesondere die Bedingungen des Sicherheits- und des Zertifizierungskonzepts sowie den Anwendungsbereich des Zertifikats darzulegen.

Die Informationen können entweder **schriftlich oder elektronisch übermittelt** werden, wobei der Anwender die Möglichkeit haben muß, sich die Informationen dauerhaft zugänglich zu machen. Diesem Erfordernis wird entsprochen, wenn der Anwender die Informationen abspeichern oder ausdrucken kann. Die entsprechende Formulierung in der Richtlinie wurde bewußt in Abweichung zu Art. 5 der Fernabsatzrichtlinie (Richtlinie 97/7 EG, ABl. Nr. L 144 vom 4. 6. 1997, S 19) gewählt.

2. Entsprechend den Vorgaben der Richtlinie sind die einschlägigen **Informationen auch dritten Personen** zur Verfügung zu stellen, soweit sie ein rechtliches Interesse daran haben (§ 20 Abs. 2). Dies gilt insbesondere für Geschäftspartner der Signatoren, die signierte Dokumente erhalten und in der Regel unter Heranziehung der Zertifikate Signaturprüfungen vornehmen müssen.

3. Die in § 20 Abs. 3 vorgesehenen Belehrungspflichten beziehen sich auf die **Sicherheitsaspekte** elektronischer Signaturen. Den Anwendern ist insbesondere die Eignung technischer Komponenten vor Augen zu führen.

Um **sichere** Signaturen gewährleisten zu können, müssen die Signatoren über die von ihnen zu veranlassenden Maßnahmen (sorgsame Verwahrung des Signaturschlüssels; Verwendung einer PIN oder eines Paßworts) sowie über sichere technische Komponenten unterrichtet werden. Darüber hinaus müssen die Anwender auch darüber beraten werden, welche Rechtswirkungen mit dem von ihnen verwendeten Signaturverfahren ausgelöst werden können. Dadurch können die Funktionsweisen und Rechtsfolgen elektronischer Signaturen (Rechtswirkungen der Signaturen, Haftung der Zertifizierungsdiensteanbieter) transparent gemacht werden, sodaß ein sorgfältiger Umgang mit elektronischen Signaturen sichergestellt ist.

Im Zusammenhang mit **sicheren** Signaturen sind die Anwender (Signatoren) etwa auch darüber zu belehren, wann die Verwendung eines Zeitstempels geboten ist. Auch sind sie darüber zu informieren, daß eine neue Signatur angebracht werden sollte, bevor der Sicherheitswert der vorhandenen Signatur durch Zeitablauf geringer wird.

Zu § 21 des Entwurfs:

In dieser Bestimmung werden die **Pflichten der Signatoren** im Umgang mit Signaturerstellungsdaten (dem privaten Signaturschlüssel) beschrieben, um Mißbräuche zu vermeiden. Der Signator hat die Signaturerstellungsdaten sorgfältig zu verwahren, ihre Weitergabe zu unterlassen und einen Zugriff auf sie zu unterbinden. Der unbefugte Zugriff kann etwa durch eine PIN oder ein Paßwort geschützt werden. Insbesondere bei Verlust oder Kompromittierung des Signaturschlüssels hat der Signator den Widerruf des entsprechenden Zertifikats zu verlangen.

Zu § 22 des Entwurfs:

1. § 22 Abs. 1 regelt die **Datenverwendung und die Datenerhebung** durch den Zertifizierungsdiensteanbieter im Zusammenhang mit der Erbringung seiner Dienste. Diese Bestimmung entspricht dem Art. 8 Abs. 2 der Richtlinie. Sie soll die Erhebung personenbezogener Daten für Zwecke der elektronischen Signatur auf das notwendige Maß begrenzen. Diese Erhebungen

sollen grundsätzlich beim Betroffenen erfolgen und bei Dritten nur mit seiner ausdrücklichen Zustimmung zulässig sein. Die Verwendung der erhobenen personenbezogenen Daten unterliegt einer engen Zweckbindung.

Nennt ein Zertifikatswerber etwa **nicht alle Angaben**, die zur Ausstellung eines qualifizierten Zertifikats notwendig sind, oder stimmt er der Überprüfung dieser Angaben nicht zu, so darf ein solches Zertifikat nicht ausgestellt werden (siehe auch § 7 Abs. 1 Z 4 und § 8 Abs. 1). Zu den Registrierungsstellen sei auf die Erläuterungen zu § 8 Abs. 2 verwiesen

2. Ein Zertifizierungsdiensteanbieter kann auch Zertifikate unter Verwendung eines **Pseudonyms** anstatt des Namens des Signators anbieten (vgl. § 8 Abs. 4). Mit der Verwendung von Pseudonymen kann der Teilnehmer am elektronischen Geschäftsverkehr verhindern, daß er bei jeder Transaktion im Netz eine Datenspur mit seiner Identität hinterläßt. Verhält sich ein unter einem Pseudonym handelnder Vertragspartner aber nicht vertrags- oder gesetzeskonform, so muß die Aufdeckung des Pseudonyms möglich sein. Die Voraussetzungen der Aufdeckung des Pseudonyms und damit der Preisgabe der wahren Identität des Signators, etwa zur Wahrung gesetzlicher Aufgaben (zB Aufklärung und Verfolgung von Straftaten) oder zur Durchsetzung von Rechtsansprüchen, richten sich gemäß § 22 Abs. 2 nach den einschlägigen Bestimmungen des Datenschutzgesetzes (§ 8 Abs. 1 Z 4 und Abs. 3 DSG). Dies gilt insbesondere auch für das **Auskunftsrecht (§ 26 DSG) oder das Recht auf Richtigstellung oder Löschung (§ 27 DSG)** von Daten.

Bei der Verfolgung strafbarer Handlungen hat die Aufdeckung des Pseudonyms gegenüber den Strafverfolgungsbehörden zu erfolgen. In zivilrechtlichen Angelegenheiten muß die Aufdeckung – bei Vorliegen der gesetzlichen Voraussetzungen (§ 8 Abs. 1 Z 4 DSG: überwiegende berechnigte Interessen eines Dritten) – gegenüber dem **potentiellen Kläger** erfolgen, weil eine Klageeinbringung unter Angabe eines Pseudonyms nicht möglich ist.

Es gibt zahlreiche Geschäftskontakte, bei denen die Verwendung von Pseudonymen nicht angebracht erscheint. Bei qualifizierten Zertifikaten müssen Pseudonyme kenntlich gemacht werden. Legt der Geschäftspartner darauf wert, daß ihm die Identität seines Gegenübers bekannt ist, so hat er die Möglichkeit, die Annahme einer unter Angabe eines Pseudonyms signierten Erklärung abzulehnen.

Zu § 23 des Entwurfs:

1. Mit § 23 werden die Haftungsregelungen des Art. 6 der Richtlinie umgesetzt. Die Bestimmung knüpft an die Ausstellung eines **qualifizierten Zertifikats** an. Maßgeblich für die Anwendbarkeit der Haftungsbestimmung ist, daß der Zertifizierungsdiensteanbieter das Zertifikat als "qualifiziertes" bezeichnet, wobei dieser Hinweis nach § 5 Abs. 1 Z 1 im Zertifikat enthalten sein muß. Die Haftungsbestimmung bezieht sich auch auf den Fall, daß ein Zertifizierungsdiensteanbieter nach § 24 Abs. 2 Z 2 die Haftung für ein Drittstaaten-Zertifikat übernimmt.

Die Anwendbarkeit der Haftungsbestimmungen – sowie sämtlicher zivilrechtlicher Regelungen – richtet sich nach dem **Internationalen Privatrecht**. Dessen Vorschriften über das anwendbare Recht bleiben ebenso wie die Vorschriften über die Zuständigkeit der Gerichte unberührt.

Auf die Haftungsbestimmung kann sich **jeder**, insbesondere auch ein Geschäftspartner des vermeintlichen Signators, der sich auf das Zertifikat verlassen hat und diesem gutgläubig gegenübersteht, **berufen**.

2. § 23 Abs. 1 übernimmt mit den **Z 1 bis 3** die Bestimmungen des Art. 6 Abs. 1 der Richtlinie. **Z 1** bezieht sich auf den Inhalt eines qualifizierten Zertifikats (siehe § 5 Abs. 1 bzw. Anhang I zur Richtlinie). **Z 2** stellt auf die Verpflichtung ab, daß die Zuordnung der Signaturprüfdaten (des öffentlichen Schlüssels und damit zwangsläufig auch des privaten Signaturschlüssels) zum Signator korrekt erfolgt. **Z 3** betrifft die sicherheitsrelevante Anforderung, daß es sich bei den Signaturerstellungsdaten und den ihnen zugeordneten Signaturprüfdaten um **komplementäre Komponenten** (komplementäre Signaturschlüssel) handelt. Dies muß für sämtliche Signaturverfahren gelten, also unabhängig davon, ob die Signaturschlüssel beim Zertifizierungsdiensteanbieter oder etwa vom Anwender selbst unter Verwendung der vom Zertifizierungsdiensteanbieter angegebenen Produkte und Verfahren erzeugt (generiert) werden.

§ 23 Abs. 1 **Z 4** entspricht der Regelung in Art. 6 Abs. 2 der Richtlinie.

Die Richtlinie sieht ausdrücklich eine **Mindesthaftung** vor. Dies bedeutet, daß die Mitgliedstaaten strengere Haftungsregeln vorsehen bzw. beibehalten können. Da sich die **harmonisierte** Haftung

der Richtlinie ausschließlich auf **qualifizierte Zertifikate** erstreckt und nach § 2 Z 9 (Art. 2 Z 10 der Richtlinie) solche Zertifikate nur von qualifizierten Zertifizierungsdiensteanbietern (§ 7 Abs. 1 bis 3) ausgestellt werden dürfen, wird in **Z 5** – systemkonform – vorgesehen, daß ein solcher Zertifizierungsdiensteanbieter auch für die Einhaltung der dann für ihn geltenden Anforderungen einzustehen hat.

3. Für **sichere** elektronische Signaturen soll mit § 23 Abs. 2 sichergestellt werden, daß die Bestimmungen des **Anhangs III** zur Richtlinie eingehalten werden, daß also für die **Erstellung** solcher elektronischer Signaturen ausschließlich geeignete und sicherheitsgeprüfte (§ 18) **technische Komponenten und Verfahren** verwendet werden. Der Zertifizierungsdiensteanbieter haftet auch dafür, daß das von ihm bereitgestellte Signaturverfahren diesen Anforderungen entspricht. Dies gilt nicht nur für die vom Zertifizierungsdiensteanbieter selbst zur Verfügung gestellten Produkte und Verfahren, sondern auch für jene, die er für das von ihm bereitgestellte Signaturverfahren als geeignet bezeichnet.

4. Im harmonisierten Haftungsbereich sieht die Richtlinie eine **Verschuldenshaftung mit Umkehr der Beweislast** zu Lasten des Zertifizierungsdiensteanbieters vor. Diese Beweislastumkehr wird mit § 23 Abs. 3 umgesetzt. Der Zertifizierungsdiensteanbieter muß im Schadensfall nachweisen, daß ihn an der schadensbegründenden Pflichtverletzung bzw. objektiven Sorgfaltswidrigkeit kein Verschulden trifft. Er haftet den Geschädigten gegenüber auch für das Verschulden seiner Gehilfen bzw. der für ihn tätigen Personen (seiner Leute). Dazu zählen etwa seine Bediensteten und andere in seinem Auftrag tätige Personen, aber auch das Personal anderer, vom Zertifizierungsdiensteanbieter mit Teilleistungen beauftragter Einrichtungen.

Wie für jeden Schadenersatzanspruch nach den allgemeinen Vorschriften des ABGB ist vorausgesetzt, daß durch die Pflichtverletzung des Zertifizierungsdiensteanbieters bei einem Dritten ein Schaden **kausal** herbeigeführt wird. Die Verpflichtungen nach Abs. 1 und 2 sind als Schutznormen im Sinn des § 1311 ABGB anzusehen. Nach der Rechtsprechung bedarf es im Falle einer Schutzgesetzverletzung keines strikten Nachweises des Kausalzusammenhangs, weil die Kausalität der in der Mißachtung der Norm liegenden Pflichtwidrigkeit für die Schadensfolgen, deren Eintritt das Schutzgesetz gerade zu verhindern bestimmt ist, vermutet wird. Steht die Übertretung des Schutzgesetzes fest, so kann sich der Beklagte von der Haftung dadurch befreien, daß er sein mangelndes Verschulden an der Übertretung der Norm beweist oder die Kausalität der Pflichtwidrigkeit – durch Außerkraftsetzung des ihn belastenden Anscheinsbeweises – zweifelhaft macht (Dittrich/Tades, ABGB³⁵ E 39 zu § 1311 ABGB).

In Fortschreibung dieser Rechtsprechung und im Hinblick auf den Umstand, daß einem Zertifizierungsdiensteanbieter hinsichtlich der Einhaltung der ihm durch dieses Bundesgesetz auferlegten Verpflichtungen eine größere Nähe zum Beweis zukommt, wird eine Beweiserleichterung zugunsten des Geschädigten angeordnet. Eine Pflichtwidrigkeit des Zertifizierungsdiensteanbieters wird dann als Schadensursache vermutet, wenn der Geschädigte die Pflichtverletzung als wahrscheinlich dartun kann. Diese Beweiserleichterung umfaßt aber auch die (nachträgliche) Kompromittierung der zur Einhaltung der normierten Sicherheitsanforderungen getroffenen technischen Vorkehrungen (vgl. auch § 4 Abs. 4). Die Entkräftung der Vermutung steht dem Zertifizierungsdiensteanbieter offen.

5. Nach § 5 Abs. 1 Z 8 und 9 können (vom Zertifizierungsdiensteanbieter) in das Zertifikat Beschränkungen des Anwendungsbereichs (zB für bestimmte Verträge) oder des Transaktionswerts für Einzeltransaktionen aufgenommen werden. Nach den Vorgaben der Richtlinie (Anhang I lit. i und j bzw. Art. 6 Abs. 3 und 4) hat eine Überschreitung des Anwendungsbereichs oder des Transaktionswerts des qualifizierten Zertifikats zur Folge, daß der Zertifizierungsdiensteanbieter dafür nicht haftet, im Umfang der sachlichen oder betragsmäßigen Überschreitung also eine Haftungsbefreiung eintritt. Diese Regelung wird mit § 23 Abs. 4 umgesetzt.

6. Um den von der Richtlinie vorgegebenen Charakter als **harmonisierte Mindesthaftung** sicherzustellen, wird in § 23 Abs. 5 angeordnet, daß die Haftungsregelungen der Abs. 1 bis 3 nicht abgedungen werden können.

7. Wie bereits dargestellt, handelt es sich bei den harmonisierten Haftungsregelungen der Richtlinie um eine **Mindesthaftung**. Bestehende und künftige Haftungsbestimmungen in anderen einschlägigen Rechtsvorschriften bleiben unberührt. Dies wird mit § 23 Abs. 6 klargestellt.

Zu § 24 des Entwurfs:

1. § 24 Abs. 1 dient lediglich der Klarstellung. Die Zertifikate aller **EU-Zertifizierungsdiensteanbieter** sind den inländischen Zertifikaten rechtlich **gleichgestellt**. Voraussetzung ist jedoch, daß die **Überprüfung der Signatur** von inländischen Empfängern ordnungsgemäß durchgeführt werden kann. Dies

bedeutet nur, daß die Verzeichnis- und Widerrufsdienste – sofern sie geführt werden (siehe § 6 Abs. 6) – auch von Österreich aus zugänglich sein müssen.

Entsprechend dem Art. 5 Abs. 1 der Richtlinie ist für die Zuerkennung **besonderer Rechtswirkungen** – wie bei inländischen Signaturen – vorausgesetzt, daß – abgesehen vom Erfordernis eines qualifizierten Zertifikats (§§ 5 und 7; Anhang I und II zur Richtlinie) – auch die technischen Sicherheitsanforderungen (§ 18; Anhang III zur Richtlinie) eingehalten werden.

2. Die Abs. 2 und 3 des § 24 regeln die Anerkennung von Zertifikaten und elektronischen Signaturen, die von **Drittstaaten-Zertifizierungsdiensteanbietern** ausgestellt werden. In **Abs. 2** wird zunächst angeordnet, daß **einfache** Zertifikate von Drittstaaten-Zertifizierungsdiensteanbietern im Inland anzuerkennen sind. Sie entfalten die Rechtswirkungen des § 3 Abs. 2.

Mit § 24 Abs. 2 zweiter Satz wird Art. 7 Abs. 1 der Richtlinie umgesetzt. Die Voraussetzungen für die Anerkennung **qualifizierter** Zertifikate sind in dieser Bestimmung (lit. a bis c) angeführt. **Z 2** (lit. b der Richtlinie) sieht eine rechtliche Anerkennung durch eine bloße **Haftungsübernahme** vor. Hiefür reicht es aus, daß ein “qualifizierter” EU-Zertifizierungsdiensteanbieter für die qualifizierten Zertifikate des Drittstaaten-Zertifizierungsdiensteanbieters haftungsrechtlich wie für seine eigenen einsteht, also die Haftung nach § 23 übernimmt. Über die Drittstaaten-Zertifizierungsdiensteanbieter, für die ein inländischer Zertifizierungsdiensteanbieter diese Haftung übernimmt, ist bei der Aufsichtsstelle nach § 13 Abs. 3 ein Verzeichnis zu führen.

Während im EU-Bereich infolge des zwingenden **Aufsichtssystems** (Art. 3 Abs. 3 der Richtlinie) davon ausgegangen werden kann, daß ein Zertifizierungsdiensteanbieter, der qualifizierte Zertifikate ausstellt, auch die entsprechenden Anforderungen (§ 7 bzw. Anhang II zur Richtlinie) erfüllt, besteht hiefür im Verhältnis zu Drittstaaten keine Garantie. Der die Haftung übernehmende EU-Zertifizierungsdiensteanbieter wird sich daher von der Einhaltung dieser Anforderungen zu vergewissern haben und nur in diesem Fall die Haftung übernehmen dürfen.

In entsprechenden **internationalen Vereinbarungen (Z 3)** wird auch sicherzustellen sein, daß Haftungstitel gegen Drittstaaten-Zertifizierungsdiensteanbieter auch im Ausland zwangsweise (gerichtlich) vollstreckt werden können.

3. Die rechtliche Anerkennung qualifizierter Zertifikate ist **eine** der Voraussetzungen dafür, daß mit einer “ausländischen” elektronischen Signatur **besondere Rechtswirkungen** im Sinn des § 4 verknüpft sein können. Neben diesen Anforderungen (**Anhang I und II** zur Richtlinie) müssen aber – wie bei inländischen elektronischen Signaturen – auch die Sicherheitsanforderungen des **Anhangs III** zur Richtlinie eingehalten sein. Bei Vorliegen aller Voraussetzungen liegt eine **sichere** elektronische Signatur im Sinn des Art. 5 Abs. 1 der Richtlinie vor.

§ 24 Abs. 3 sieht vor, daß Bescheinigungen von “Drittstaaten-**Bestätigungsstellen**” – über die Einhaltung von Sicherheitsanforderungen durch Signaturprodukte und Verfahren – unter bestimmten Voraussetzungen den Bescheinigungen einer inländischen Bestätigungsstelle über **sicherheitsgeprüfte** technische Komponenten gleichgehalten werden. Hiefür wird verlangt, daß die technischen Anforderungen, insbesondere Sicherheitsanforderungen, sowie die zugrunde liegenden Prüfverfahren den inländischen qualitativ gleichwertig sind. Das Vorliegen dieser Voraussetzungen durch eine bestimmte “Drittstaaten-Bestätigungsstelle” muß zuvor von der **Aufsichtsstelle** festgestellt werden.

Voraussetzung einer derartigen Entscheidung der Aufsichtsstelle ist es auch, daß die im betreffenden Drittstaat bestehenden **Sicherheitsanforderungen** – für sichere elektronische Signaturen im Sinn des Art. 5 Abs. 1 der Richtlinie – den gemeinschaftsrechtlichen Sicherheitsanforderungen **gleichwertig** sind. Die Aufsichtsstelle könnte etwa auch – auf Antrag und Kosten von Drittstaaten-Zertifizierungsdiensteanbietern – ein Verzeichnis über die in Drittstaaten bestehenden Sicherheitsanforderungen führen.

Zu § 25 des Entwurfs:

Diese Bestimmung enthält eine ausdrückliche Ermächtigung zur Erlassung einer **Signaturverordnung**. Sie bezieht sich insbesondere auf die Festlegung der Gebühren für die Aufsichtstätigkeiten, weiters die Festsetzung ausreichender Finanzmittel für Zertifizierungsdiensteanbieter und die Konkretisierung der verschiedenen Sicherheitsanforderungen an vertrauenswürdige Signatur- und Zertifizierungsdienste.

Zu den §§ 26 und 27 des Entwurfs:

Dabei handelt es sich um die üblichen Bestimmungen zum Inkrafttreten und zum Vollzug des Gesetzes.