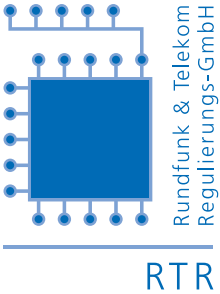
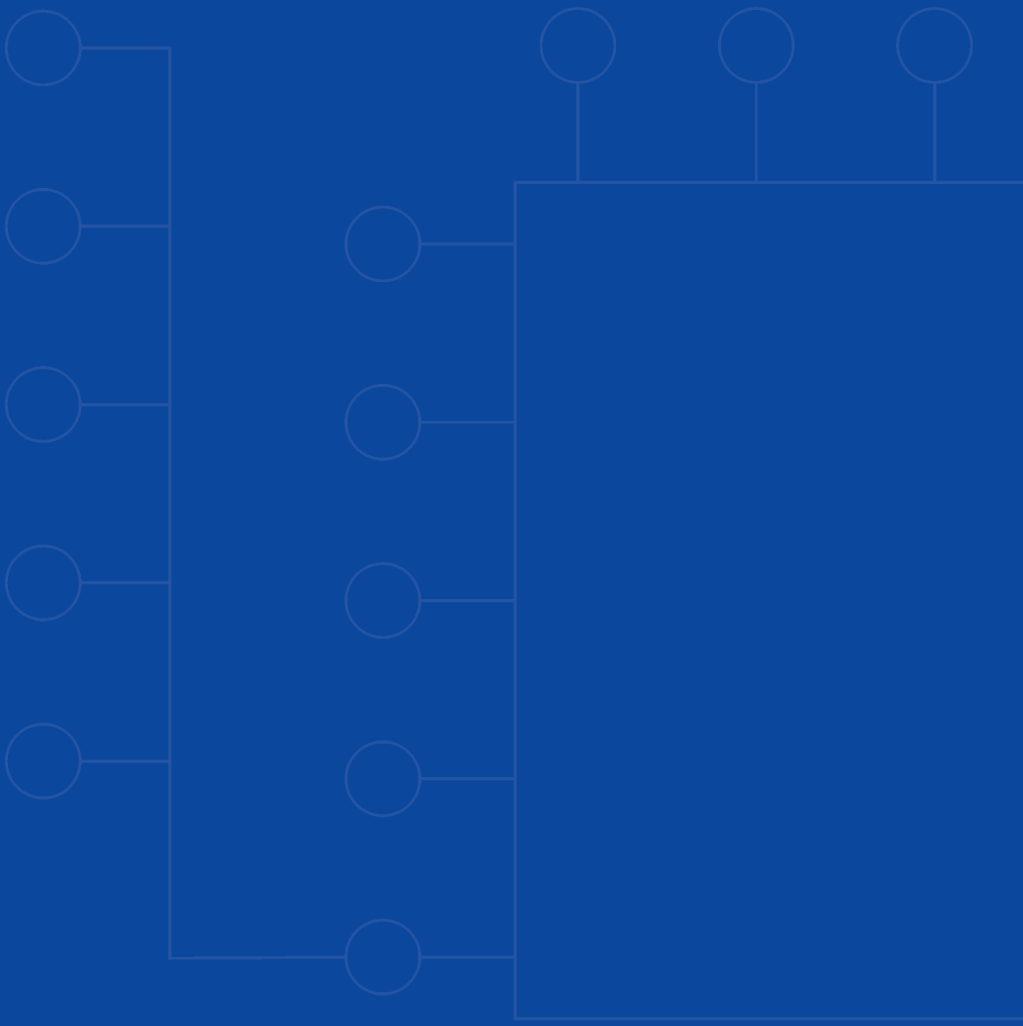
4 Jahre Signaturgesetz



Schriftenreihe der Rundfunk und Telekom Regulierungs-GmbH



4 Jahre Signaturgesetz

Schriftenreihe der
Rundfunk und Telekom Regulierungs-GmbH

Band 1/2004

Inhaltsverzeichnis

Vorwort

Am 01.01.2000 trat das österreichische Signaturgesetz in Kraft, einige Wochen darauf die europäische Signaturrichtlinie. Mittlerweile liegen also vier Jahre an Erfahrungen mit den beiden Rechtsgrundlagen vor. Der hier vorgelegte Bericht zieht eine Zwischenbilanz über die Erfahrungen mit dem Signaturgesetz und die Tätigkeiten der Aufsichtsstelle. Er soll aber nicht bloß die Aktivitäten der Aufsichtsstelle darlegen, sondern darüber hinaus auch einen kompakten Überblick über die Technik der elektronischen Signatur, die angebotenen Zertifizierungsdienste und den internationalen Rahmen bieten, in dem sich diese Aktivitäten bewegen.

Kapitel 1 stellt die Grundlagen der elektronischen Signatur dar. Dabei wird einerseits eine vertiefte Darlegung der technischen Grundlagen vorgenommen (Abschnitt 1.1), andererseits werden das Signaturgesetz (SigG) und die Signaturverordnung (SigV) dargestellt (Abschnitt 1.2).

In Kapitel 2 werden die Tätigkeiten der Aufsichtsstelle beschrieben. Im Sommer 1999, kurz nach der Beschlussfassung über das Signaturgesetz, wurden erste Vorbereitungen aufgenommen; als das Signaturgesetz am 01.01.2000 in Kraft trat, konnte mit den aufsichtsbehördlichen Tätigkeiten umgehend begonnen werden. Abschnitt 2.1 beschreibt die 45 aufsichtsbehördlichen Verfahren, die seither vor der Telekom-Control-Kommission (TKK) geführt wurden. Ein Schwerpunkt der Tätigkeit der Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH) bei der Vollziehung des Signaturgesetzes lag im Aufbau und dem Betrieb des sicheren Verzeichnisses der Zertifizierungsdienste. Die zu diesem Zweck errichtete Public-Key-Infrastruktur der Aufsichtsstelle, die im September 2002 in Betrieb genommen wurde, wird in Abschnitt 2.2 dargestellt. Abschnitt 2.3 gibt einen Überblick über weitere Aktivitäten der RTR-GmbH im Zusammenhang mit dem Signaturgesetz.

Kapitel 3 stellt den Markt dar, welcher der Aufsicht der TKK unterliegt. Dabei wird einerseits ein Überblick über die in Österreich angebotenen Zertifizierungsdienste gegeben (Abschnitt 3.1), andererseits werden Signaturprodukte und -anwendungen beschrieben (Abschnitt 3.2).

Den internationalen Zusammenhang stellt Kapitel 4 her. Die Anwendbarkeit elektronischer Signaturen ist stark davon abhängig, dass Produkte und Dienstleistungen Interoperabilität gewährleisten. In verschiedenen Normungsgremien wurde daher eine Fülle von Standards geschaffen, die jeweils ein Stück dazu beitragen sollen, dass die elektronische Kommunikation durch Signaturen und Zertifikate gesichert wird. Abschnitt 4.1 gibt einen Überblick über die Fülle dieser Standards und Normen. Abschnitt 4.2 stellt das rechtliche Umfeld dar. Die detailliertesten Regelungen finden sich hier in der Signaturrichtlinie der Europäischen Union. Die aufgrund dieser Richtlinie in den Mitgliedstaaten eingerichteten Aufsichtsstellen haben sich im Forum of European Supervisory Authorities for Electronic Signatures (FESA) informell zusammengeschlossen, um gemeinsame Sichtweisen zu Auslegungsfragen der Signaturrichtlinie zu entwickeln und den Meinungsaustausch zwischen den Aufsichtsstellen zu fördern. Die Aktivitäten von FESA werden in Abschnitt 4.3 beschrieben.

Die seit dem In-Kraft-Treten des Signaturgesetzes vergangenen vier Jahre waren vom Aufbau gekennzeichnet. Die ursprünglich erwartete rasche Verbreitung der Nutzung elektronischer Signaturen verzögerte sich – ein Phänomen, das sich nicht nur auf Österreich beschränkte. Es hat sich gezeigt, dass die Schaffung rechtlicher Grundlagen alleine nicht ausreicht, um eine neue Technologie in die Breite zu bringen. Allerdings wurden in Österreich sowohl bei den Zertifizierungsdiensten als auch bei den Signaturprodukten und -anwendungen in den vergangenen vier Jahren beträchtliche Investitionen getätigt. Seit Februar 2002 gibt es mehrere Zertifizierungsdienste, bei denen qualifizierte Zertifikate für die sichere elektronische Signatur angeboten werden. Mehrere österreichische Unternehmen haben Secure Viewer entwickelt, die dem Nutzer größtmögliche Sicherheit bieten, dass tatsächlich das auf dem Bildschirm angezeigt wird, was er damit elektronisch signiert.

Die Bausteine, die den Einsatz elektronischer Signaturen möglich machen, sind damit vorhanden. Insbesondere im Bereich des E-Government und von Banken wurde und wird auch eine Reihe von Anwendungen geschaffen, wo elektronische Signaturen eingesetzt werden können. Es ist daher zu erwarten, dass es in den nächsten Jahren tatsächlich zu einer beträchtlichen Ausweitung der Nutzung der elektronischen Signatur kommen wird. Mit diesem Bericht will die Aufsichtsstelle aufzeigen, welche Dienstleistungen angeboten werden, welche Nutzungen möglich sind, und wie durch rechtliche und technische Anforderungen die Sicherheit der elektronischen Signatur gewährleistet wird.

Abschließend sei den beiden Mitarbeitern der RTR-GmbH, Dipl.-Ing. Mag. Dieter Kronegger und Mag. Ulrich Latzenhofer, für die Erstellung des vorliegenden Berichts gedankt.

Dr. Georg Serentschy
Geschäftsführer des Fachbereichs Telekommunikation der RTR-GmbH

Grundlagen

1.1 Technische Grundlagen

1.1.1 Asymmetrische Kryptografie

Der Begriff digitale Signatur wurde 1976 von Whitfield Diffie und Martin E. Hellman in einem bahnbrechenden Aufsatz[1] geprägt und beruht auf dem von Diffie und Hellman erstmals veröffentlichten Konzept der asymmetrischen Kryptografie[2].

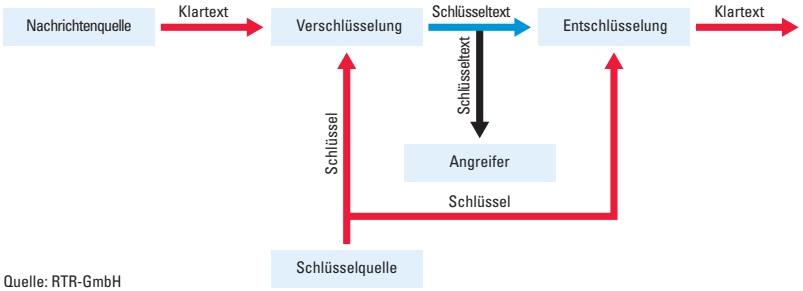
Jahrtausendelang verstand man unter Verschlüsselung symmetrische Kryptografie. Diese ist bestimmt durch einen fixen Algorithmus und durch einen variablen Schlüssel. Um einen Klartext zu verschlüsseln, wendet man den Algorithmus mit dem Schlüssel auf den Klartext an und erhält den Schlüsseltext. Zum Entschlüsseln wird ein inverser Algorithmus mit demselben Schlüssel verwendet, der den Schlüsseltext in den zugehörigen Klartext umwandelt. Die Sicherheit sollte nicht auf der Geheimhaltung der Algorithmen beruhen – im Gegenteil: Diese sind meistens veröffentlicht und können somit von zahlreichen Experten hinsichtlich ihrer Sicherheit erforscht und begutachtet werden. Wesentlich ist vielmehr die Geheimhaltung des Schlüssels. Das größte Problem dabei besteht in der Frage, wie die Kommunikationspartner Kenntnis des Schlüssels erlangen. In der Regel wird der Schlüssel auf einem sicheren Kommunikationskanal übermittelt, der vor Angriffen geschützt werden muss. Abb. 1 veranschaulicht dies, wobei sichere Kommunikationskanäle rot und unsichere blau dargestellt sind.

Die Arbeit von Diffie und Hellman beschreibt Verfahren, bei denen jeder Kommunikationspartner über zwei unterschiedliche Schlüssel verfügt: Der eine wird zum Verschlüsseln, der andere zum Entschlüsseln eingesetzt (asymmetrische Kryptografie). Einer der beiden Schlüssel ist öffentlich bekannt und wird daher als öffentlicher Schlüssel bezeichnet (engl. public key, daher auch die Bezeichnung Public-Key-Kryptografie). Der andere Schlüssel

1) Diffie, Whitfield; Hellman, Martin E.: New Directions in Cryptography. In: IEEE Transactions on Information Theory 22 (1976), S. 644–654.
2) Bis 1997 galten Diffie und Hellman als Entdecker der asymmetrischen Verschlüsselung. Erst zu dieser Zeit wurden vom britischen Geheimdienst GCHQ Dokumente aus den Jahren 1970/73 freigegeben, welche die im Dienste der GCHQ stehenden Mathematiker James H. Ellis und Clifford C. Cocks als die eigentlichen Entdecker ausweisen. http://www.cesg.gov.uk/site/publications/media/possnse.pdf, http://www.cesg.gov.uk/site/publications/media/notense.pdf.

sollte sich unter der alleinigen Kontrolle seines Inhabers befinden und wird daher privater Schlüssel genannt. Zwischen den beiden Schlüsseln besteht ein dermaßen komplexer mathematischer Zusammenhang, dass aus einem hinreichend langen öffentlichen Schlüssel der zugehörige private Schlüssel praktisch (d. h. mit angemessenem Ressourcenaufwand) nicht ermittelt werden kann. Man spricht in diesem Zusammenhang von einer Einwegfunktion: Jene Funktion, die einem privaten Schlüssel den entsprechenden öffentlichen Schlüssel zuordnet, ist einfach zu berechnen. Die Umkehrfunktion aber, die einem öffentlichen Schlüssel den entsprechenden privaten Schlüssel zuordnet, ist aus komplexitätstheoretischen Gründen praktisch nicht berechenbar. Grundlage solcher Einwegfunktionen sind beispielsweise algebraische Probleme, z. B. die Schwierigkeit der Berechnung des diskreten Logarithmus in großen endlichen Körpern (siehe Fußnote 1 auf Seite 11) bzw. die Schwierigkeit der Zerlegung großer ganzer Zahlen in ihre Primfaktoren[3].

Abb. 1: Symmetrische Verschlüsselung



Quelle: RTR-GmbH

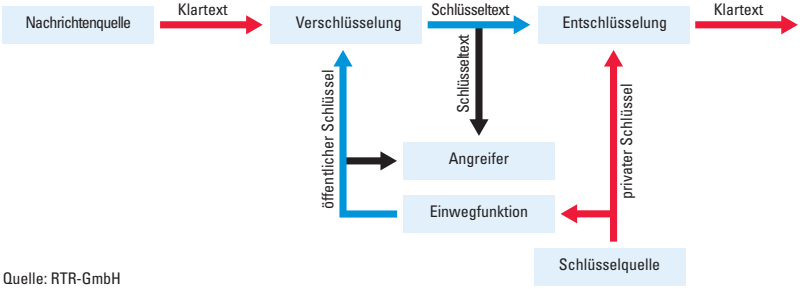
Öffentlicher und privater Schlüssel wirken komplementär: Der Klartext wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Zum Entschlüsseln wird der private Schlüssel des Empfängers eingesetzt (Abb. 2).

Der primäre Vorteil ist offenkundig: Ein sicherer Kommunikationskanal zwischen Sender und Empfänger zur Vereinbarung des Schlüssels ist nicht erforderlich. Sofern der private Schlüssel unter alleiniger Kontrolle des Empfängers ist, kann die Entschlüsselung nur durch den Empfänger erfolgen. Überdies sind in Systemen mit vielen Kommunikationspartnern wesentlich

3) Rivest, Ronald L.; Shamir, Adi; Adleman, Leonard M.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. In: Communications of the ACM (2) 21 (1978), S. 120–126.

weniger Schlüssel erforderlich, damit je zwei Kommunikationspartner vertrauliche Informationen austauschen können: Für *n* Kommunikationspartner werden bei symmetrischer Kryptografie ½ ($n^2 - n$) Schlüssel benötigt (je zwei Partner benötigen einen eigenen Schlüssel), bei asymmetrischer Kryptografie hingegen nur *n* Schlüsselpaare (jeder Partner benötigt nur ein Schlüsselpaar). Negativ schlägt sich bei asymmetrischer Kryptografie zu Buche, dass der Aufwand an Rechenzeit im Allgemeinen wesentlich höher als bei symmetrischer Kryptografie ist.

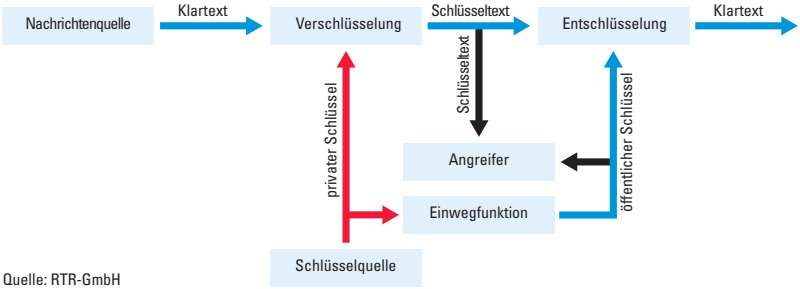
Abb. 2: Asymmetrische Verschlüsselung



Quelle: RTR-GmbH

Die revolutionäre Idee von Diffie und Hellman und die Basis der digitalen Signatur bestehen darin, die Rollen von öffentlichen und privaten Schlüsseln zu tauschen: Die Verschlüsselung erfolgt mit dem privaten Schlüssel des Senders, zum Entschlüsseln wird der öffentliche Schlüssel des Senders eingesetzt (Abb. 3).

Abb. 3: Digitale Signatur



Quelle: RTR-GmbH

Worin besteht der Zweck einer Verschlüsselung, wenn das Ergebnis mit einem öffentlich bekannten Schlüssel entschlüsselt werden kann? Die Antwort ist einfach: Die erfolgreiche Entschlüsselung lässt erkennen, dass die ursprüngliche Verschlüsselung durch den Inhaber des privaten Schlüssels erfolgt ist (Authentizität). Sie beweist weiters, dass die Daten seit der Verschlüsselung nicht verändert worden sind (Integrität). Dies sind die wesentlichen Eigenschaften der digitalen Signatur (in juristischem Kontext: der elektronischen Signatur).

Bekannte asymmetrische Verfahren sind insbesondere RSA (siehe Fußnote 3 auf Seite 12) (benannt nach Rivest, Shamir und Adleman) und DSA[4] (Digital Signature Algorithm). Seit den späten achtziger Jahren sind asymmetrische Verfahren bekannt, die auf elliptischen Kurven über endlichen Körpern beruhen (kurz ECC für Elliptic Curve Cryptography). Da bei diesen Verfahren eine mit RSA und DSA vergleichbare Sicherheit bereits mit einem Bruchteil der Schlüssellänge erzielt wird, sind weniger Speicherplatz und ein geringerer zeitlicher Aufwand für die Ausführung der Berechnungen erforderlich. ECC-Verfahren eignen sich besonders für den Einsatz in Chipkarten, denn für diese sind geringer Speicherplatz und vergleichsweise niedrige Rechengeschwindigkeit charakteristisch.

Zahlreiche komplexere Anwendungen beruhen ebenfalls auf asymmetrischer Kryptografie:

- Vereinbarung eines Schlüssels für symmetrische Kryptografie über einen unsicheren Kommunikationskanal (siehe Fußnote 1 auf Seite 11): Zwei Kommunikationspartner können sich auf einen gemeinsamen Schlüssel einigen, indem sie voneinander unabhängig Berechnungen durchführen, die zum selben Ergebnis führen und die jeweils nur den eigenen privaten Schlüssel sowie den öffentlichen Schlüssel des anderen Kommunikationspartners involvieren. Wer weder den einen noch den anderen privaten Schlüssel kennt, kann diese Berechnung nicht durchführen.
- Zeitstempeldienste: In vielen Situationen ist ein Nachweis dafür erforderlich, dass ein Dokument zu einem bestimmten Zeitpunkt existiert hat. Im einfachsten Fall werden das Dokument und die aktuelle Zeitangabe zusammengefasst und von einer unabhängigen Stelle, die einen Zeitstempeldienst anbietet, digital signiert. Um Datenschutz zu gewähren und um den Kommunikationsaufwand zu reduzieren, wird dem Anbieter des Zeitstempeldienstes meist nicht das Dokument selbst, sondern dessen Hashwert (siehe Abschnitt 1.1.2) zum Signieren vorgelegt.

4) Digital Signature Standard (DSS). FIPS PUB 186–2.
National Institute of Standards and Technology, 2000, vgl. Abschnitt 4.1.6.3.

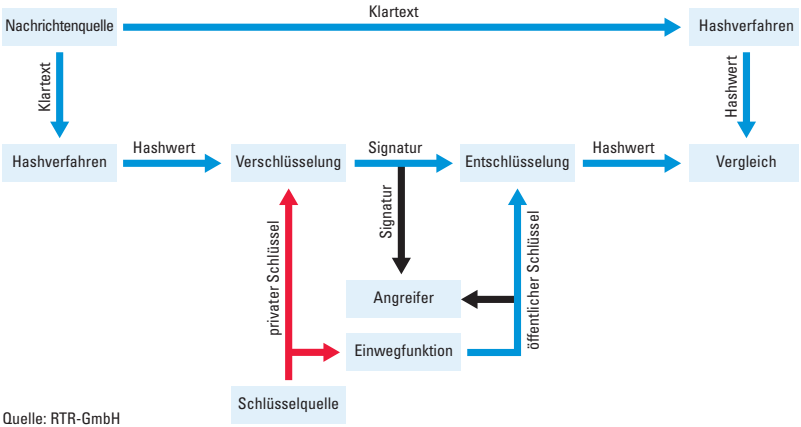
- Digitale Signaturen in Vertretung: Unter Beifügung einer digital signierten Ermächtigung (z. B. in Form eines Attributzertifikats) können digitale Signaturen in Vertretung einer anderen Person erstellt werden.
- Nachweis der Kenntnis einer Sache ohne Preisgabe der Information (Zero-Knowledge Proof).
- Beglaubigte digitale Signaturen: Ähnlich wie beim Zeitstempeldienst signiert ein „Notar" nur den Hashwert eines signierten Dokuments und beglaubigt somit die ursprüngliche Signatur, ohne sich mit dem Inhalt des Dokuments zu befassen.
- Elektronische Wahlen: Mittels kryptografischer Protokolle wird gewährleistet, dass nur Wahlberechtigte ihre Stimme abgeben können, dass jeder Wahlberechtigte nur einmal seine Stimme abgeben kann, dass das Wahlergebnis überprüft werden kann und dass trotzdem das Wahlgeheimnis gewahrt bleibt.
- Elektronische Zahlungssysteme: Als Beispiel sei das von Kreditkartenunternehmen entwickelte, mittlerweile aber nicht mehr favorisierte System Secure Electronic Transaction (SET) genannt.

1.1.2 Hashverfahren und Padding

Ein Hashverfahren ordnet Daten beliebiger Länge (dem Urbild) einen Wert (den Hashwert) zu, der einen ähnlichen Zweck wie eine Prüfsumme erfüllt. Exakter formuliert, handelt es sich beim Hashverfahren um eine Einwegfunktion mit einem Ergebnis fester Länge (z. B. 160 Bit). Die Einwegfunktion muss überdies so komplex sein, dass es praktisch nicht möglich ist, zwei Urbilder mit demselben Hashwert zu finden (diese Eigenschaft wird als Kollisionsresistenz bezeichnet).

Um beim Erstellen einer digitalen Signatur den relativ hohen zeitlichen Aufwand asymmetrischer Verfahren zu umgehen, wird das asymmetrische Verfahren meistens nicht auf die zu signierenden Daten selbst, sondern auf den einfacher berechenbaren Hashwert dieser Daten angewandt. Da diese Form der digitalen Signatur lediglich Teilinformationen über die signierten Daten enthält, muss zum Prüfen der digitalen Signatur auch das Urbild des Hashwerts bereitgestellt werden (Abb. 4).

Abb. 4: Digitale Signatur eines Hashwerts



Quelle: RTR-GmbH

Nach diesem Konzept kommt der Kollisionsresistenz besondere Bedeutung zu. Die Hashverfahren SHA-1 (Secure Hash Algorithm[5]) und RIPEMD-160 (RIPE[6] Message Digest[7]) werden von Experten als kollisionsresistent anerkannt. Das ältere, aber nach wie vor sehr gebräuchliche Hashverfahren MD5 gilt hingegen seit der Konstruktion von Kollisionen[8] im Jahr 1996 als gebrochen.

Hashwerte sind relativ kurz: Beispielsweise liefern SHA-1 und RIPEMD-160 Werte mit einer Länge von 160 Bit. Ein Klartext für klassische asymmetrische Verfahren wie RSA und DSA könnte jedoch bei typischen Schlüssellängen um ein Vielfaches länger sein. Der Hashwert wird daher mit zusätzlichen Bits aufgefüllt, bevor er mit dem privaten Schlüssel chiffriert wird. Dieses Auffüllen bezeichnet man als Padding.

Einem Angreifer, dem eine digitale Signatur vorliegt, ist jedenfalls bekannt, dass das Verschlüsselungsverfahren nur auf einen kurzen Hashwert angewandt worden ist. Würde beim Padding ein einfaches Muster aus Nullen und Einsen verwendet werden, so würde der Angreifer über wertvolle Zusatzinformationen verfügen, die ihm beim Brechen des privaten Schlüssels

5) Secure Hash Standard. FIPS PUB 180–2.
National Institute of Standards and Technology, 2002, vgl. Abschnitt 4.1.6.2.
6) RIPE = RACE Integrity Primitives Evaluation, ein EU-Projekt aus den Jahren 1988 bis 1992; RACE = Research and Development in Advanced Communication Technologies.
7) Dobbertin, Hans; Bosselaers, Antoon; Preneel, Bart: RIPEMD-160, A Strengthened Version of RIPEMD. Manuskript, 1996, http://www.esat.kuleuven.ac.be/~cosicart/pdf/AB-9601/AB-9601.pdf.
8) Dobbertin, Hans: Cryptanalysis of MD5 Compress. Manuskript, 1996, http://www.cs.ucsd.edu/users/bsy/dobbertin.ps.

nützlich sein könnten. Aus diesem Grund ist auch die Sicherheit des Padding-Verfahrens bedeutsam.

1.1.3 Zertifikate

Mit den in Abschnitt 1.1.1 und 1.1.2 beschriebenen Techniken kann überprüft werden, ob Daten mit einem bestimmten Schlüssel digital signiert worden sind. Wem dieser Schlüssel aber gehört, kann so nicht zuverlässig festgestellt werden.

Deshalb werden von sogenannten Zertifizierungsstellen, die als vertrauenswürdig anerkannt sind, Zertifikate ausgestellt: Ein Zertifikat ist eine elektronische Bestätigung der Zuordnung eines öffentlichen Schlüssels zu einer Person und muss zumindest folgende Daten enthalten:

- einen öffentlichen Schlüssel,
- Daten zur Bezeichnung des Schlüsselinhabers (z. B. den Namen),
- eine digitale Signatur der Zertifizierungsstelle.

Die Überprüfung einer digitalen Signatur erfordert nicht nur die Entschlüsselung der Signatur mit dem im zugehörigen Zertifikat angegebenen öffentlichen Schlüssel, sondern auch eine Überprüfung des Zertifikats. Zu diesem Zweck muss festgestellt werden, ob die digitale Signatur im Zertifikat tatsächlich jene der Zertifizierungsstelle ist. Dafür wird wiederum ein Zertifikat verwendet, welches die korrekte Zuordnung des öffentlichen Schlüssels einer Zertifizierungsstelle bestätigt. Dieses Zertifikat kann von der Zertifizierungsstelle selbst, von einer anderen Zertifizierungsstelle oder von einer (staatlichen) Aufsichtsstelle ausgestellt sein. So ergibt sich eine Zertifizierungshierarchie, in der auf mehreren Ebenen die Zuordnung öffentlicher Schlüssel zu Personen oder zu Zertifizierungsstellen bestätigt wird. Ein Beispiel für eine Zertifizierungshierarchie ist im Abschnitt 2.2.5 über die Verzeichnisse der Aufsichtsstelle grafisch dargestellt.

Eine besondere Form des Zertifikats ist das qualifizierte Zertifikat, das aufgrund rechtlicher Vorgaben bestimmte Mindestinhalte aufweist (siehe Abschnitt 1.2.1.2.4). Darüber hinaus muss ein Aussteller qualifizierter Zertifikate in technischer, organisatorischer, finanzieller und personeller Hinsicht zuverlässig sein, sichere Verzeichnis- und Widerrufsdienste bereitstellen, seine Tätigkeit ausführlich dokumentieren und die Identität von Personen, für die qualifizierte Zertifikate ausgestellt werden, anhand amtlicher Lichtbildausweise überprüfen.

Ein qualifiziertes Zertifikat signalisiert somit vor allem Sicherheit auf der Seite des Zertifizierungsdiensteanbieters. Sicherheit auf der Seite des Signators ist nur insofern gewährleistet, als der Zertifizierungsdiensteanbieter Vorkehrungen dafür zu treffen hat, dass die Signaturerstellungsdaten der Signatoren weder vom Zertifizierungsdiensteanbieter noch von Dritten gespeichert oder kopiert werden können.

1.1.4 Erzeugung von Zufallszahlen

Ein wesentliches Kriterium für die Sicherheit kryptografischer Systeme ist die Zufallsqualität der eingesetzten Schlüssel und anderer „zufälliger" Parameter, die beim Padding und für einige Verschlüsselungsverfahren (z. B. die nur jeweils einmal verwendbaren temporären DSA-Schlüssel) erforderlich sind.

Im Idealfall werden echte Zufallszahlen (d. h. eine Folge unabhängiger, gleichverteilter Zufallsvariablen) verwendet. Viele Quellen echter Zufallszahlen scheiden allerdings für kryptografische Zwecke aus, weil sie öffentlich zugänglich und somit nicht geheim sind. Hochwertige Zufallszahlen, die auch für kryptografische Zwecke geeignet sind, können beispielsweise durch teure Spezialgeräte erzeugt werden, die auf Quanteneffekten beruhen[9]. In einer etwas preisgünstigeren Rechnerumgebung können Mausbewegungen und die zeitlichen Abstände gewisser Ereignisse (Tastaturanschläge, Festplattenzugriffe usw.) zur Ermittlung von Zufallszahlen herangezogen werden, wobei allerdings mathematische Modelle und statistische Tests zum Nachweis einer ausreichenden Zufallsqualität unverzichtbar sind. In einfachen Umgebungen wie Chipkarten erweist sich die Erzeugung von Zufallszahlen als besonders schwierig, weil kaum Interaktionen mit der Außenwelt stattfinden und weil fast alle im Gerät erfolgenden Abläufe deterministisch sind. Einfache Mechanismen, z. B. Paare asynchroner Taktgeber, sind üblicherweise in Chipkarten implementiert, bedürfen aber einer ausführlichen Analyse. Bei allen genannten Beispielen werden keine echten Zufallszahlen im eingangs erwähnten mathematischen Sinn erzeugt. Um diesen Umstand zu verschleiern, werden Zufallsdaten aus unterschiedlichen Quellen gesammelt und mit hohen Verlustraten einem Hashverfahren unterzogen. Die daraus resultierenden Hashwerte können mit mathematischen Methoden kaum von echten Zufallszahlen unterschieden werden.

In Anwendungen, bei denen viele Zufallszahlen erforderlich oder echte Zufallsquellen nicht verfügbar sind, schaffen Pseudozufallszahlen Abhilfe. Dabei wird aus einem zufälligen Anfangswert eine Folge von Zahlen abgeleitet, die mit mathematischen Methoden von echten Zufallszahlen erst

9) Standard Specifications for Public-Key Cryptography. IEEE P1363. Institute of Electrical and Electronics Engineers, Inc., 2000.

bei hinreichender Anzahl von Folgengliedern unterschieden werden können. Das wesentliche Merkmal von Pseudozufallszahlen besteht in ihrer deterministischen Erzeugung: Verwendet man zweimal denselben Anfangswert, so erhält man zweimal dieselbe Folge von Pseudozufallszahlen.

Nach österreichischem Recht ist die Verwendung von Pseudozufallszahlen zur Erzeugung der Signaturerstellungsdaten (d. h. des privaten Schlüssels) für sichere elektronische Signaturen unzulässig (§ 3 Abs. 5 SigV). Für Padding-Verfahren dürfen hingegen auch Pseudozufallszahlen herangezogen werden (§ 6 Abs. 2 SigV).

1.1.5 Algorithmen und Parameter für sichere elektronische Signaturen

Die Sicherheit elektronischer Signaturen hängt maßgeblich davon ab, dass die eingesetzten Algorithmen und deren Parameter gewisse Mindestkriterien erfüllen. Diese sind in den Anhängen der Signaturverordnung (SigV) festgelegt.

Demnach werden bis 31.12.2005 folgende Algorithmen als sicher angesehen:

- die Verfahren zur Signaturerstellung RSA (siehe Fußnote 3 auf Seite 12), DSA (siehe Fußnote 4 auf Seite 14) und gewisse DSA-Varianten, die auf elliptischen Kurven beruhen (siehe Fußnote 9 auf Seite 18),
- die Hashverfahren SHA-1 (siehe Fußnote 5 auf Seite 16) und RIPEMD-160 (siehe Fußnote 7 auf Seite 16).

Eine Schlüssellänge von mindestens 1.023 Bit bei den Verfahren RSA und DSA bzw. von mindestens 160 Bit bei DSA-Varianten, die auf elliptischen Kurven beruhen, wird ebenfalls bis 31.12.2005 als sicher angesehen.

Ob diese Schlüssellängen auch nach dem 31.12.2005 als sicher angesehen werden können, ist aus heutiger Sicht fraglich. Eine von den Kryptologen Lenstra und Verheul vorgenommene Schätzung[10] lässt vermuten, dass RSA- und DSA-Schlüssel mit einer Länge von 1.068 Bit bereits im Jahr 2003 mit einem Aufwand von USD 171 Mio. innerhalb eines Tages gebrochen werden können. Zum Zeitpunkt der Schätzung waren die signifikanten kryptoanalytischen Fortschritte von Bernstein[11] sowie Shamir und Tromer[12] noch nicht bekannt.

10) Lenstra, Arjen K.; Verheul, Eric R.: Selecting Cryptographic Key Sizes. In: Journal of Cryptology, 14(4) (2001), S. 255–293.
11) Bernstein, Daniel: Circuits for Integer Factorization: A Proposal. Manuskript, 2001, http://cr.yp.to/papers/nfscircuit.ps.
12) Shamir, Adi; Tromer, Eran: Factoring Large Numbers with the TWIRL Device. Manuskript, 2003, http://www.wisdom.weizmann.ac.il/~tromer/papers/twirl.pdf.

Im Sinne des Binnenmarkts würde die RTR-GmbH eine Festlegung von Algorithmen und Parametern für sichere elektronische Signaturen durch eine allgemein anerkannte Norm auf europäischer Ebene bevorzugen. Von einer Arbeitsgruppe der EESSI wurde bereits 2001 ein Vorschlag zur Festlegung von Algorithmen und Parametern ausgearbeitet, der mittlerweile als ETSI SR 002 176 (vgl. Abschnitt 4.1.5.2.1) veröffentlicht ist. Dieser Vorschlag ist aber weder als Norm allgemein anerkannt, noch bietet er eine Perspektive für die Zeit nach 2005. Weiterhin wird auf Ebene der Mitgliedstaaten entschieden, welche Algorithmen und Parameter als sicher angesehen werden.

In Frankreich etwa akzeptiert die staatliche Bestätigungsstelle DCSSI seit Juli 2003 nur die Einreichung von Produkten zur Evaluierung nach Common Criteria EAL4+ (vgl. Abschnitt 4.1.1.7), die das Verfahren RSA mit Schlüssellängen von mindestens 1.536 Bit unterstützen. Wie lange die bis dahin eingereichten und anschließend evaluierten Produkte eingesetzt werden dürfen, ist offenbar nicht generell geregelt, sondern geht aus den jeweiligen Bescheinigungen hervor.

Die in Deutschland für die Festlegung geeigneter Algorithmen und Parameter[13] zuständige Regulierungsbehörde für Telekommunikation und Post empfiehlt für die Verfahren RSA und DSA eine Schlüssellänge von 2.048 Bit, lässt aber die Verwendung von Schlüsseln mit einer Länge von 1.024 Bit bis zum Ende des Jahres 2007 zu (mindestens 1.280 Bit bis Ende 2008). Für einen zweiten, in Österreich bislang ungeregelten DSA-Parameter (vgl. Abschnitt 4.1.6.3) ist eine Länge von mindestens 160 Bit vorgegeben. Für ECC-Verfahren wird ab 2006 zwischen zwei Parametern unterschieden. Jener Parameter, für den wie auch in der österreichischen SigV schon bisher Bedingungen vorgegeben waren, muss nach 2006 eine Länge von mindestens 180 Bit aufweisen. Der zweite, bisher nicht geregelte Parameter ist eine Primzahl mit einer Länge von mindestens 191 oder 192 Bit (je nach der zugrunde liegenden algebraischen Struktur).

1.1.6 Sichere Signaturerstellungseinheiten

Eine wesentliche Voraussetzung für die Gleichwertigkeit elektronischer Signaturen mit eigenhändigen Unterschriften besteht darin, dass zum Signieren eine sichere Signaturerstellungseinheit (im Sinne von Anhang III der Signaturrichtlinie[14]) verwendet wird, welche die Signaturerstellungsdaten eines Signators vor der Verwendung durch andere verlässlich schützt. Durch

13) Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung. In: Bundesanzeiger Nr. 48 (11.03.2003), S. 4202–4203.
14) Vgl. Abschnitt 4.2.1.

Speicherung von Signaturerstellungsdaten auf einem herkömmlichen Datenträger wird diese Voraussetzung nicht erfüllt, weil nicht ausgeschlossen werden kann, dass die Daten von Unbefugten gelesen werden.

Bestmöglichen Schutz der Signaturerstellungsdaten bieten Geräte, die ein Lesen der Signaturerstellungsdaten gar nicht erst zulassen. Solche Geräte können nur nützlich sein, wenn sie die Verschlüsselung des Hashwerts selbst durchführen können. Damit der Vorgang der Verschlüsselung lediglich vom rechtmäßigen Inhaber der Signaturerstellungsdaten ausgelöst werden kann, ist eine Authentifizierung (z. B. durch Eingabe einer PIN über einen sicheren Kommunikationskanal) erforderlich. Ein solches Gerät kann nur dann zur Erstellung sicherer elektronischer Signaturen verwendet und somit als sichere Signaturerstellungseinheit bezeichnet werden, wenn von einer Bestätigungsstelle die Erfüllung der technischen Sicherheitserfordernisse bescheinigt worden ist.

In der Praxis werden als sichere Signaturerstellungseinheiten ausschließlich Chipkarten eingesetzt, die nicht nur Speicher, sondern auch einen eigenen Prozessor enthalten. Die sichere Authentifizierung der Signatoren wird durch Lesegeräte ermöglicht, die über eine eigene Tastatur verfügen. So kann verhindert werden, dass PINs über die Tastatur des Rechners eingegeben werden und durch eine Verarbeitung im Betriebssystem unerwünschte Nebenwirkungen auslösen.

Manche Kartenchips sind auch in USB-Dongles erhältlich. Probleme bei der sicheren Authentifizierung der Signatoren verhindern aber bislang den Einsatz von USB-Dongles als sichere Signaturerstellungseinheiten.

Eine andere Möglichkeit, kryptografische Funktionen in eine abgeschlossene Einheit auszulagern, bieten sogenannte Hardware Security Modules (HSMs). Dabei handelt es sich um Geräte, die entweder in einen Computer eingebaut oder an einen solchen angeschlossen werden. Auch aus diesen Geräten können private Schlüssel bei geeigneter Konfiguration nicht ausgelesen werden: Der Zugriff erfolgt ausschließlich über eine Applikationsschnittstelle, die das Ausführen kryptografischer Operationen und administrativer Tätigkeiten, wie z. B. der Schlüsselverwaltung, ermöglicht. HSMs erlauben üblicherweise eine Steuerung der Zugriffsrechte, bei der für jeden Benutzer die zulässigen Operationen detailliert festgelegt werden können. Das Auslesen privater Schlüssel durch physische Eingriffe wird durch technische Vorkehrungen verhindert: Beispielsweise führen zu große Abweichungen der Spannung oder der Temperatur, Änderungen von Leitereigenschaften oder

eine zu hohe ionisierende Strahlung dazu, dass der HSM-Speicher gelöscht wird. HSMs eignen sich besonders für den Einsatz als vertrauenswürdige Systeme (im Sinne von Anhang II f der Signaturrichtlinie (vgl. Abschnitt 4.2.1) zum Signieren von Zertifikaten. Die technischen Sicherheitserfordernisse für einen derartigen Einsatz unterscheiden sich jedoch von jenen für sichere Signaturerstellungseinheiten.

1.1.7 Risken

Der hohe Schaden, den die Erstellung elektronischer Signaturen durch Unbefugte verursachen kann, erfordert eine ausführliche Beschäftigung mit Szenarien, die derartige „Unterschriftfälschungen" ermöglichen.

In der Praxis stellt zweifellos der sorglose Umgang mit Authentifizierungsdaten (PIN) die größte Gefahr dar. Authentifizierungsdaten werden bisweilen vertrauten Mitarbeitern oder den nächsten Angehörigen bewusst überlassen, damit diese für den rechtmäßigen Signator Unterschriften leisten können. Im Kampf gegen die Vergesslichkeit werden Authentifizierungsdaten gelegentlich auch in Form von geöffneten PIN-Kuverts oder schriftlichen Notizen am Arbeitsplatz aufbewahrt. Dabei sind dem Signator meist nicht einmal alle Personen bekannt, die Zugang zum Arbeitsplatz haben. Im Vertrauen gefragt: Wissen Sie, wer täglich vor Ihrer Ankunft im Büro den Papierkorb leert?

Praktisch relevant sind auch Angriffe durch Spyware oder trojanische Pferde: Für die Erstellung sicherer elektronischer Signaturen werden zwar ausnahmslos Chipkarten-Lesegeräte mit eingebauter PIN-Tastatur empfohlen. Fehler bei der Installation der Treiber können aber nachweislich dazu führen, dass die PIN über die PC-Tastatur eingegeben und somit durch das Betriebssystem verarbeitet wird. Als potenzielle Gefahr erweisen sich dabei bösartige Computerprogramme, welche die Tastaturanschläge protokollieren. Eine so erfasste PIN könnte unbefugten Personen zugänglich gemacht werden oder ebenfalls durch bösartige Software dazu verwendet werden, Daten gegen den Willen des Signators mit dessen sicherer elektronischer Signatur zu versehen. Die Existenz solcher Programme kann in kaum einer Büroumgebung mit Internetanbindung gänzlich ausgeschlossen werden. Man kann lediglich an das Verantwortungsbewusstsein der Signatoren appellieren, keine PIN über die PC-Tastatur einzugeben.

Wesentlich aufwändiger sind kryptoanalytische Angriffe, bei denen versucht wird, aus öffentlichen Schlüsseln sowie aus signierten bzw. verschlüsselten Daten private Schlüssel zu ermitteln. Nach dem gegenwärtigen Stand der

Technik verursachen derartige Angriffe extrem hohe Kosten (siehe Fußnote 10 auf Seite 19) und können noch am ehesten durch die finanziell bestausgestatteten Geheimdienste der Welt durchgeführt werden. Der dafür erforderliche Ressourceneinsatz ist so hoch, dass jedenfalls nur wenige und dann wohl gezielt ausgewählte Schlüssel gebrochen werden können. Praktisch undurchführbar erscheint derzeit die Fälschung sicherer elektronischer Signaturen auf Basis von Hashwert-Kollisionen. Die Gültigkeit dieser Aussagen könnte sich jedoch schlagartig ändern, wenn ein Glied der Kette Schlüsselerzeugung – Berechnung des Hashwerts – Padding – Verschlüsselung sich als schwach erweist.

Eine breitere Werkzeugpalette steht dem Angreifer zur Verfügung, wenn er auf die Signaturerstellungseinheit zugreifen kann. Seit 1995 sind Timing-Attacken[15] bekannt, durch die aus der für kryptografische Operationen aufgewandten Rechenzeit Information über private Schlüssel gewonnen wird. Bei Simple Power Analysis (SPA) und Differential Power Analysis[16] (DPA) wird der Stromverbrauch zwecks Ermittlung der Signaturerstellungsdaten analysiert. Noch mächtiger sind Verfahren, bei denen die elektromagnetische Strahlung analysiert wird (SEMA und DEMA), weil durch die Verfügbarkeit verschiedener Quellen mehr Information bereitsteht. Durch physische Manipulation einer Chipkarte (Lösen des Schutzsiegels, chemische Behandlung und mikroskopische Untersuchung der Siliziumschicht) können weitere wertvolle Erkenntnisse erlangt werden. Mittels fokussierter Ionenbestrahlung sind sogar gezielte Eingriffe in die Schaltkreise des Chips möglich.

Das Konzept der Einwegfunktionen ist im Grunde genommen lediglich eine Annahme: Dass solche Funktionen praktisch nicht invertiert werden können, beruht neben mathematischen Hypothesen auch auf den für gegenwärtige Computer charakteristischen deterministischen Rechenmodellen. Nichtdeterministische Modelle, bei denen sämtliche mögliche Lösungen parallel auf Korrekt- oder Inkorrektheit überprüft werden können, schließen den Begriff der Einwegfunktion per definitionem aus. Sie könnten langfristig im Quantencomputer Gestalt annehmen und so der digitalen Signatur ein jähes Ende bereiten. Die Entwicklung effizienter Verfahren zur Primfaktorzerlegung und zur Berechnung diskreter Logarithmen auf einem Quantencomputer[17] gelang bereits 1995 und verhalf Peter W. Shor 1998 zum begehrten Nevan-

15) Kocher, Paul C.: Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In: Koblitz, Neal (Hrsg.): Advances in Cryptology – CRYPTO '96. Berlin: Springer-Verlag, 1996, S. 104–113.
16) Kocher, Paul; Jaffe, Joshua; Jun, Benjamin: Differential Power Analysis. In: Wiener, Michael (Hrsg.): Advances in Cryptology – CRYPTO '99. Berlin: Springer-Verlag, 1999, S. 388–397.
17) Shor, Peter W.: Polynomial Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. In: SIAM Journal on Computing, 26(5) (1997), S. 1484–1509.

linna-Preis, der nur alle vier Jahre von der International Mathematical Union verliehen wird. Mit Shors Faktorisierungsverfahren wurde 2001 auf einem 7-Qubit-Quantencomputer die Zahl 15 korrekt in ihre Primfaktoren 3 und 5 zerlegt. Mit der gegenwärtigen Technologie, die nach Meinung der Experten auf maximal 15 Qubits beschränkt ist, lassen sich allerdings höchstens dreistellige Zahlen faktorisieren.

1.2 Rechtliche Grundlagen

Die maßgeblichsten rechtlichen Grundlagen zur elektronischen Signatur sind auf nationaler Ebene das Signaturgesetz (SigG) und die Signaturverordnung (SigV), auf europäischer Ebene die Signaturrichtlinie (siehe Abschnitt 4.2.1).

1.2.1 Signaturgesetz (SigG)

1.2.1.1 Allgemeines

Durch das Signaturgesetz[18], das am 01.01.2000 in Kraft getreten ist, wurde in Österreich eine Rechtsgrundlage für elektronische Signaturen und für das Aufsichtssystem geschaffen.

Auch vor dem In-Kraft-Treten des SigG war es bereits möglich, elektronische Signaturen im Rechts- und Geschäftsverkehr zu verwenden, da das österreichische Recht nur wenige Formvorschriften kennt. Sowohl im Zivilrecht (z. B. zum Abschluss von Verträgen) als auch im öffentlichen Recht (insbesondere für die Kommunikation mit Behörden) herrscht weithin Formfreiheit. Grundsätzlich konnten also schon seit langem Verträge mittels elektronischer Kommunikation geschlossen werden oder mit Verwaltungsbehörden elektronisch kommuniziert werden – Sicherheitsprobleme bei vielen Formen der Kommunikation können aber im Nachhinein zu Beweisproblemen führen. Daher wurden elektronische Formen der Kommunikation sowohl im E-Commerce als auch beim E-Government nur selten eingesetzt.

Mit dem SigG reagierte der Gesetzgeber auf die bestehenden Sicherheitsprobleme und das daraus resultierende mangelnde Vertrauen in elektronische Kommunikation. Die Diskussion in Österreich entwickelte sich dabei parallel

18) Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG), BGBl I Nr 190/1999 idF BGBl I Nr 137/2000, BGBl I Nr 32/2001 und BGBl I Nr 152/2001.

zu einer entsprechenden Diskussion auf europäischer Ebene. Das österreichische SigG und die europäische Signaturrichtlinie[19] wurden etwa zeitgleich diskutiert, das SigG wurde etwas früher (im Sommer 1999), die Richtlinie kurz darauf (im Dezember 1999) beschlossen.

Das SigG entspricht weitestgehend der Signaturrichtlinie, Österreich war somit der erste Mitgliedstaat der Europäischen Union, der die Richtlinie umgesetzt hat.

Die wesentlichsten Neuerungen, die das SigG für die österreichische Rechtsordnung brachte, sind Folgende:

- Das SigG hat Voraussetzungen für die „sichere elektronische Signatur" definiert und dieser Form der elektronischen Signatur besondere Rechtswirkungen zuerkannt. Die sichere elektronische Signatur erfüllt grundsätzlich das an anderen Stellen der Rechtsordnung aufgestellte Erfordernis der eigenhändigen Unterschrift. Damit wurden rechtliche Barrieren für den Einsatz der elektronischen Signatur beseitigt.
- Das SigG hat ein Aufsichtssystem über die in Österreich niedergelassenen Zertifizierungsdiensteanbieter geschaffen. Dadurch soll Vertrauen in Zertifikate und Signaturprodukte geschaffen werden, was wiederum die faktische Barriere beseitigen soll, dass elektronische Kommunikation in vielen Bereichen des Rechts- und Geschäftsverkehrs mangels Vertrauen der Nutzer nicht eingesetzt wird.

1.2.1.2 Die wesentlichsten Bestimmungen des Signaturgesetzes (SigG)

1.2.1.2.1 Allgemeine Rechtswirkungen

§ 3 SigG regelt als Grundsatzbestimmung die allgemeinen Rechtswirkungen elektronischer Signaturen. Im Rechts- und Geschäftsverkehr können Signaturverfahren mit unterschiedlichen Sicherheitsstufen und unterschiedlichen Zertifikatsklassen verwendet werden. Dabei kann die rechtliche Wirksamkeit einer elektronischen Signatur nicht alleine deshalb ausgeschlossen werden, weil die elektronische Signatur irgendwelche Voraussetzungen nicht erfüllen würde – z. B. dass sie nicht auf einem qualifizierten Zertifikat beruht oder nicht mit technischen Komponenten erstellt wurde, welche die Sicherheitsanforderungen des SigG nicht erfüllen würden.

19) Vgl. Abschnitt 4.2.1.

Auch einer sehr einfachen und leicht fälschbaren Form der Signatur – ein Beispiel dafür wäre, dass man einfach seinen Namen am Ende einer E-Mail anfügt – darf die rechtliche Wirksamkeit daher nicht von vornherein abgesprochen werden. Im Streitfall unterliegt eine solche Nachricht dem in allen Verfahrensgesetzen verankerten Grundsatz der freien Beweiswürdigung. Wenn die Echtheit der Nachricht bestritten wird, wird sie jedoch umso schwerer beweisbar sein, je weniger Sicherheit das jeweilige Signaturverfahren gewährleistet.

1.2.1.2.2 Besondere Rechtswirkungen

Die Kernbestimmung des SigG ist dessen § 4, der die besonderen Rechtswirkungen der sicheren elektronischen Signatur regelt. Eine sichere elektronische Signatur erfüllt das rechtliche Erfordernis der eigenhändigen Unterschrift, insbesondere der Schriftlichkeit[20], sofern durch Gesetz oder Parteienvereinbarung nicht anderes bestimmt ist.

Aufgrund von § 4 SigG ist eine sichere elektronische Signatur also insbesondere dann verwendbar, wenn in Gesetzen, Verträgen oder Allgemeinen Geschäftsbedingungen verlangt wird, dass bestimmte Mitteilungen oder Vereinbarungen „schriftlich" zu erfolgen haben. Insbesondere in Allgemeinen Geschäftsbedingungen wird häufig geregelt, dass etwa eine Kündigung nur wirksam sei, wenn sie schriftlich erfolgt, oder dass Nebenvereinbarungen zum Vertrag der Schriftform bedürfen. Eine gewöhnliche E-Mail würde nicht ausreichen, um dieses Erfordernis zu erfüllen, eine sicher elektronisch signierte Nachricht hingegen erfüllt es, wenn dies nicht ausdrücklich anders bestimmt ist.

Für einige Fälle, die der Gesetzgeber als besonders sensibel angesehen hat, wurden in § 4 Abs. 2 SigG Ausnahmen vorgesehen. In diesen Fällen ist weiterhin eine eigenhändige Unterschrift erforderlich:

- Rechtsgeschäfte des Familien- und Erbrechts, die an die Schriftform oder ein strengeres Formerfordernis gebunden sind – beispielsweise das eigenhändige Testament (das überhaupt zur Gänze eigenhändig geschrieben werden muss) oder ein Ehevertrag (der als Notariatsakt geschlossen werden muss),

20) Vgl. § 886 des Allgemeinen Bürgerlichen Gesetzbuches (ABGB).

- andere Willenserklärungen oder Rechtsgeschäfte, die zu ihrer Wirksamkeit an die Form einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsaktes (z. B. Schenkungen ohne Übergabe der geschenkten Sache, Kaufverträge zwischen Ehegatten) bedürfen,
- Willenserklärungen, Rechtsgeschäfte oder Eingaben, die zu ihrer Eintragung in das Grundbuch, das Firmenbuch oder ein öffentliches Register einer Beglaubigung oder Beurkundung bedürfen, und
- Bürgschaftserklärungen, die von Personen außerhalb ihrer gewerblichen, geschäftlichen oder beruflichen Tätigkeit abgegeben werden.

1.2.1.2.3 Sichere elektronische Signatur

Der Begriff der sicheren elektronischen Signatur ist der zentrale Begriff des SigG. Alle Sicherheitsanforderungen des Gesetzes zielen letztlich darauf ab und auch die besonderen Rechtswirkungen knüpfen an das Vorliegen einer sicheren elektronischen Signatur an. Damit eine sichere elektronische Signatur vorliegt, müssen vor allem folgende Anforderungen erfüllt sein:

- Allgemeine Anforderungen an die verwendete Signaturtechnologie: die Signatur muss ausschließlich dem Signator zugeordnet sein; die Identifizierung des Signators muss möglich sein; die Signatur muss mit Mitteln erstellt worden sein, die der Signator unter seiner alleinigen Kontrolle halten kann, und die Signatur muss mit den signierten Daten so verknüpft sein, dass jede nachträgliche Veränderung der Daten festgestellt werden kann. Die Signaturrichtlinie fasst diese Anforderungen mit dem Begriff der „fortgeschrittenen elektronischen Signatur" zusammen.
- Anforderungen an den Zertifizierungsdiensteanbieter: Sichere elektronische Signaturen müssen auf einem „qualifizierten Zertifikat" beruhen. An diesen Begriff knüpft das SigG eine Fülle von Sicherheitsanforderungen an den Zertifizierungsdiensteanbieter, der solche Zertifikate ausstellt – insbesondere die Identitätsüberprüfung anhand eines amtlichen Lichtbildausweises vor der Ausstellung des Zertifikates.
- Anforderungen an die technischen Komponenten und Verfahren: Eine sichere elektronische Signatur muss mit einer sogenannten „sicheren Signaturerstellungseinheit" erstellt werden – das ist in der Praxis bislang immer eine besonders auf Sicherheit geprüfte Chipkarte, könnte aber auch durch eine andere Technologie realisiert werden. Weitere Anforderungen richtet die SigV z. B. auch an die Software, mittels der die Signatur erstellt wird („Secure Viewer").

1.2.1.2.4 Qualifiziertes Zertifikat

Unter dem Begriff des qualifizierten Zertifikates fasst das SigG alle Anforderungen an den Zertifizierungsdiensteanbieter zusammen. Insgesamt sollen diese Anforderungen gewährleisten, dass der Zertifikatsinhaber zuverlässig identifiziert werden kann: bevor das qualifizierte Zertifikat ausgestellt wird, muss die Identität des Signators anhand eines amtlichen Lichtbildausweises geprüft werden. Und die Gesamtheit der organisatorischen und technischen Anforderungen soll sicherstellen, dass Zertifikate nicht gefälscht werden können und auch wirklich nur dann ausgestellt werden, wenn die Identitätsprüfung erfolgt ist. Für Fälle, in denen es dennoch zu einem Fehler kommt, sieht das SigG die Haftung des Zertifizierungsdiensteanbieters vor.

Aus rechtlicher Sicht muss ein qualifiziertes Zertifikat nicht zwangsläufig in Kombination mit einer sicheren Signaturerstellungseinheit verwendet werden. Es könnte auch qualifizierte Zertifikate geben, die für die einfache elektronische Signatur verwendet werden. In der Praxis kommt dies jedoch kaum vor (vgl. aber Kapitel 2.1.4).

§ 5 SigG enthält Anforderungen an den Inhalt eines qualifizierten Zertifikates. Das qualifizierte Zertifikat ist sozusagen der Ausweis im Internet. Es muss folgende Mindestangaben enthalten:

- den Hinweis darauf, dass es sich um ein qualifiziertes Zertifikat handelt[21],
- den unverwechselbaren Namen des Zertifizierungsdiensteanbieters und den Staat seiner Niederlassung (da nach der Signaturrichtlinie jeder Mitgliedstaat die Aufsicht über jene Zertifizierungsdiensteanbieter ausübt, die in seinem Staatsgebiet niedergelassen sind, ist aus dem qualifizierten Zertifikat daher auch erkennbar, welcher Staat für die Aufsicht zuständig ist),
- den Namen des Signators
  (oder ein Pseudonym, das als solches gekennzeichnet sein muss),
- die dem Signator zugeordneten Signaturprüfdaten, also den öffentlichen Schlüssel,
- Beginn und Ende der Gültigkeit des Zertifikates,
- eine eindeutige Kennung des Zertifikates (z. B. eine Seriennummer),
- gegebenenfalls eine Einschränkung des Anwendungsbereiches oder eine Begrenzung des Transaktionswertes.

21) Zum Zertifikatsprofil und zur Kennzeichnung als qualifiziertes Zertifikat gibt es auch technische Normen in RFC 3039 (vgl. Abschnitt 4.1.3.1) und ETSI TS 101 862 (vgl. Abschnitt 4.1.5.2.6).

Auf Verlangen des Zertifikatwerbers können weitere Angaben in das Zertifikat aufgenommen werden, etwa Angaben über die Vertretungsmacht oder andere rechtlich erhebliche Eigenschaften. Solche Angaben werden aber häufig nicht in das qualifizierte Zertifikat selbst aufgenommen, damit der Nutzer sie nicht bei jedem Kommunikationsvorgang offenlegen muss – sondern in andere elektronische Bestätigungen, die nach Wahl des Nutzers beigelegt werden können oder auch nicht.

1.2.1.2.5 Aufsichts- und Akkreditierungssystem

Zertifikate erfüllen im Internet eine ähnliche Funktion wie Ausweise in der nichtelektronischen Welt. Bei der Diskussion über die gesetzliche Regelung von elektronischen Signaturen und von Zertifikaten wurde daher auch die Variante erörtert, staatliche Zertifizierungsstellen einzurichten, welche Zertifikate ausgeben. In manchen Staaten wurden auch solche Wege eingeschlagen, etwa in Finnland, wo das staatliche Bevölkerungsregister Zertifikate ausgibt. Auf europäischer Ebene wurde aber jedenfalls vorgesehen, dass der Staat auch private Zertifizierungsdiensteanbieter zulassen muss, und auch Österreich hat den Weg eingeschlagen, die Ausstellung von Zertifikaten dem Markt zu überlassen und keinen staatlichen Zertifizierungsdienst einzurichten[22].

Um das Vertrauen in die Zertifikate zu schützen, wurde stattdessen ein staatliches Aufsichts- und Akkreditierungssystem eingerichtet. Nach deutschem Vorbild wurde die Aufgabe der Aufsichtsstelle dem Telekom-Regulator übertragen. Die Telekom-Control-Kommission (TKK) hat nach den §§ 13 bis 17 SigG die Aufsicht über Zertifizierungsdiensteanbieter und die Akkreditierung von Zertifizierungsdiensteanbietern wahrzunehmen, die Telekom-Control GmbH (nun: RTR-GmbH) unterstützt die TKK dabei.

Die wesentlichsten aufsichtsbehördlichen Aufgaben liegen bei der TKK. § 13 Abs. 2 SigG zählt dazu auf, dass die Aufsichtsstelle bei allen Zertifizierungsdiensteanbietern die Umsetzung der Angaben im Sicherheits- und Zertifizierungskonzept zu prüfen hat, dass sie im Fall der Bereitstellung sicherer elektronischer Signaturen die Verwendung geeigneter technischer Komponenten und Verfahren zu überwachen hat und dass sie Zertifizierungsdiensteanbieter

22) Durch das E-Government-Gesetz wird dies insofern relativiert werden, als für den Kontakt mit Verwaltungsbehörden das Zertifikat des privaten Zertifizierungsdiensteanbieters nicht ausreichen wird, vielmehr muss eine von einer staatlichen Stelle – dem Zentralen Melderegister im Auftrag der Datenschutzkommission als Stammzahlregisterbehörde – ausgestellte Bescheinigung, die sogenannte „Personenbindung", zusätzlich zum Zertifikat übermittelt werden.

auf deren Antrag hin akkreditieren muss. Weiters obliegt es der TKK, die organisatorische Aufsicht über Bestätigungsstellen durchzuführen.

Der RTR-GmbH kommt gemäß § 15 SigG die Aufgabe zu, die TKK bei der laufenden Aufsicht zu unterstützen. Dabei nimmt die RTR-GmbH insbesondere die Aufgaben der Geschäftsstelle für die TKK wahr. Hervorzuheben ist, dass die RTR-GmbH im Auftrag der TKK das Verzeichnis der Zertifizierungsdienste führt (vgl. Abschnitt 2.2). Im Fall eines begründeten Verdachtes, dass die Sicherheitsanforderungen des SigG oder der SigV nicht eingehalten werden, können von der RTR-GmbH vorläufige Aufsichtsmaßnahmen angeordnet werden (§ 15 Abs. 2 Z 7 SigG). Von dieser Kompetenz hat die RTR-GmbH bisher noch nie Gebrauch gemacht. Weiters ist die RTR-GmbH als Schlichtungsstelle für Streitfälle zwischen Kunden bzw. Interessenvertretungen einerseits und Zertifizierungsdiensteanbietern andererseits zuständig. Während die entsprechende Kompetenz nach dem Telekommunikationsgesetz[23] stark genützt wird (im Jahr 2002 z. B. waren es 1.528 Fälle), gab es bislang keinen einzigen Schlichtungsfall nach § 15 Abs. 4 SigG.

Entsprechend den europarechtlichen Vorgaben wurde für die Aufsicht kein Lizenzierungssystem eingerichtet, sondern die bloße Anzeigepflicht statuiert. Wer eine Tätigkeit als Zertifizierungsdiensteanbieter aufnehmen will, muss dies der Aufsichtsstelle gemäß § 6 Abs. 2 SigG anzeigen. Dabei ist ein Sicherheits- und Zertifizierungskonzept vorzulegen, das die Tätigkeit näher beschreibt. Anzeigepflichtig sind auch Änderungen des Konzepts (ebenfalls gemäß § 6 Abs. 2 SigG) und die Einstellung des Dienstes (§ 12 SigG). Der Anbieter braucht eine Entscheidung der Aufsichtsstelle über seine Anzeige nicht abzuwarten; er kann seine Tätigkeit sofort aufnehmen bzw. die angezeigten Änderungen sofort anwenden. Die Aufsichtsstelle kann bzw. muss den Anbieter aber aufgrund der Anzeige überprüfen und könnte Aufsichtsmaßnahmen ergreifen, wenn den Anforderungen des SigG oder der SigV nicht entsprochen wird.

Für Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate für die sichere elektronische Signatur bereitstellen, besteht die Möglichkeit der Akkreditierung nach § 17 SigG. Die Akkreditierung ist freiwillig. Die Anforderungen an einen akkreditierten Anbieter sind dieselben wie die Anforderungen an jeden anderen Anbieter sicherer elektronischer Signaturen. Der Unterschied besteht

23) § 116 und § 66 TKG (1997), § 122 TKG 2003,
vgl. auch die jährlichen Streitschlichtungsberichte der RTR-GmbH.

darin, dass bei der Akkreditierung eine Überprüfung im Vorhinein erfolgt: erst nach dem erfolgreichen Abschluss des Akkreditierungsverfahrens darf sich der Anbieter „akkreditierter Zertifizierungsdiensteanbieter" nennen (vgl. 2.1.4).

Für die Signaturprodukte wurde in Europa der Regelungsansatz gewählt, dass von den Mitgliedstaaten benannte Bestätigungsstellen die Erfüllung der technischen Anforderungen an die Produkte bescheinigen. Dabei kann es sich um staatliche oder um private Einrichtungen handeln. Im österreichischen SigG finden sich die entsprechenden Regelungen in § 18 Abs. 5 und § 19 SigG. Nach dem Konzept des SigG könnte es mehrere Bestätigungsstellen geben, bislang hat nur der Verein A-SIT den Status einer Bestätigungsstelle (vgl. Abschnitt 1.2.3.2). Auch in anderen Mitgliedstaaten der EU gibt es nur wenige Bestätigungsstellen, in Deutschland sind es z. B. drei, in manchen Staaten gibt es gar keine Bestätigungsstelle. Die von Bestätigungsstellen ausgestellten Bescheinigungen gelten im gesamten Europäischen Wirtschaftsraum.

1.2.1.3 Novellen des Signaturgesetzes (SigG)

Das SigG wurde bislang dreimal novelliert, es handelte sich aber dabei jeweils nur um geringfügige Änderungen.

In der ersten Novelle[24], die mit 01.10.2000 in Kraft trat, wurden einige Anpassungen an die mittlerweile verabschiedete Signaturrichtlinie (vgl. Abschnitt 4.2.1) vorgenommen. Da das Gesetz von vornherein im Hinblick auf die Signaturrichtlinie konzipiert war, mussten nur wenige Änderungen beschlossen werden, vor allem im Hinblick auf die Anerkennung ausländischer Bescheinigungen von Signaturprodukten (§ 18 Abs. 5 SigG), auf die Anerkennung von Normen, die von der Europäischen Kommission festgelegt werden (§ 18 Abs. 6 SigG) und auf die Anerkennung von Zertifikaten, die von einem Anbieter ausgestellt werden, der im Europäischen Wirtschaftsraum niedergelassen ist (§ 24 SigG).

Die im Hinblick auf die Systematik des Gesetzes wesentlichste Änderung wurde in § 5 Abs. 3 SigG vorgenommen. In der Stammfassung des SigG wurde versucht, die Anforderungen an die Signaturerstellungseinheiten der Signatoren und die Anforderungen an die Signaturerstellungseinheiten der Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, gleich-

24) BGBl I Nr 137/2000.

zusetzen. Daher verlangte § 5 Abs. 3 SigG in der Stammfassung, dass qualifizierte Zertifikate mit der sicheren elektronischen Signatur des Zertifizierungsdiensteanbieters zu versehen sind. Da dies nicht dem Konzept der Signaturrichtlinie entsprochen hatte und auch die europäischen Normungsgremien (EESSI, CEN, ETSI) an die verschiedenen Arten von Signaturerstellungseinheiten unterschiedliche Maßstäbe angelegt hatten, wurde im § 5 Abs. 3 SigG eine Anpassung vorgenommen. Seit dem In-Kraft-Treten dieser Änderung müssen die Signaturerstellungseinheiten der Zertifizierungsdiensteanbieter nicht mehr die Anforderungen an sogenannte „sichere Signaturerstellungseinheiten" erfüllen und benötigen insbesondere keine Bescheinigung einer Bestätigungsstelle mehr. Da die Anforderungen der SigV sich großteils auf sichere Signaturerstellungseinheiten beziehen, entstand durch die Novelle des SigG im Hinblick auf die Signaturerstellungseinheiten der Zertifizierungsdiensteanbieter eine Regelungslücke, die wohl erst durch die kommende Novelle der SigV geschlossen werden wird. Die Aufsichtsstelle hat sich daher in den Akkreditierungsverfahren zur Beurteilung der technischen Sicherheit der Signaturerstellungseinheiten der Zertifizierungsdiensteanbieter jeweils auf ein Gutachten der Bestätigungsstelle A-SIT gestützt (siehe Abschnitt 2.1.4).

Durch das KommAustria-Gesetz[25] wurde eine Neuordnung der Behördenstruktur im Rundfunkbereich vorgenommen. Dabei wurde aus der Telekom-Control GmbH die RTR-GmbH, welche zusätzlich zu den bestehenden Aufgaben der Telekom-Regulierung (nach dem TKG 1997) und nach dem SigG nun auch Aufgaben im Bereich der Rundfunkregulierung – insbesondere die Geschäftsführung für die neue Kommunikationsbehörde Austria (KommAustria) – wahrzunehmen hat. Das KommAustria-Gesetz trat am 01.04.2001 in Kraft, im SigG wurde inhaltlich nichts geändert, es wurde lediglich die Bezeichnung „Telekom-Control GmbH" durch „RTR-GmbH" ersetzt.

Mit dem E-Commerce-Gesetz[26] wurde eine kleine Änderung betreffend die Bürgschaftserklärung vorgenommen. Bis zum In-Kraft-Treten des E-Commerce-Gesetzes am 01.01.2002 konnten Bürgschaftserklärungen nicht sicher elektronisch signiert werden, sondern mussten eigenhändig unterschrieben werden. Nun gilt dies nur mehr für den privaten Bereich, im Rahmen der gewerblichen, geschäftlichen oder beruflichen Tätigkeit können Bürgschaftserklärungen auch mit einer sicheren elektronischen Signatur versehen werden.

25) BGBl I Nr 32/2001.
26) BGBl I Nr 152/2001.

1.2.2 Signaturverordnung (SigV)

Die Signaturverordnung konkretisiert die technischen und organisatorischen Anforderungen des Signaturgesetzes, insbesondere die Folgenden:

- Anforderungen an die finanzielle Ausstattung der Anbieter qualifizierter Zertifikate sowie an deren Haftpflichtversicherung (§ 2 SigV),
- Anforderungen an die Signaturerstellungsdaten (private Schlüssel) für sichere elektronische Signaturen (§§ 3 und 4 SigV),
- Anforderungen an technische Komponenten und Verfahren der Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen (§§ 6 und 8 SigV),
- Anforderungen an technische Komponenten und Verfahren der Anwender sicherer elektronischer Signaturen (§ 7 SigV) – hier ist insbesondere auf die Anforderungen an die sichere Anzeige und an die PIN-Eingabe hinzuweisen,
- Anforderungen an die Prüfung der technischen Komponenten und Verfahren durch eine Bestätigungsstelle (§ 9 SigV),
- organisatorische Anforderungen zur Ausstellung qualifizierter Zertifikate, insbesondere zur Qualifikation und Zuverlässigkeit des Personals (§ 10 SigV), zur Identitätsprüfung (§ 12 SigV), zu den Verzeichnis- und Widerrufsdiensten (§ 13 SigV), zu den Inhalten des Sicherheits- und Zertifizierungskonzepts (§ 15 SigV) und zur Dokumentation (§ 16 SigV).

Weiters sind in der SigV noch administrative Fragen näher geregelt: die Gebühren in § 1 SigV sowie einige nähere Bestimmungen zur Anzeige und zur Akkreditierung in § 18 SigV.

Besonders hervorzuheben sind die Bestimmungen in § 7 Abs. 1 bis 3 SigV, da sie Anforderungen an die von den Signatoren zu verwendenden technischen Komponenten enthalten, die über die Chipkarte hinausgehen. Grundsätzlich ist die für die sichere elektronische Signatur eingesetzte Technik so konzipiert, dass dem Signator möglichst wenig Sorgfaltspflichten zukommen. Der Idealfall wäre, dass der Signator lediglich darauf achten muss, dass ihm die Chipkarte nicht gemeinsam mit dem PIN-Code entwendet wird und dass er sich – wie auch in der nichtelektronischen Welt – Texte durchliest, bevor er sie signiert. Der Signator soll sich nicht darum kümmern müssen, dass seine Chipkarte sicher ist – dazu wurde sie evaluiert und bescheinigt – oder dass sein Zertifizierungsdiensteanbieter sorgfältig arbeitet – dazu wurde ein Aufsichtssystem eingerichtet. Daher beziehen sich fast alle Anforderungen der SigV auf die sichere Signaturerstellungseinheit und auf den Zertifizierungsdiensteanbieter.

Es hat sich aber gezeigt, dass es – zumindest bei den heute üblicherweise verwendeten Betriebssystemen und Dokumentenformaten – nicht ausreicht, dass man dem Signator eine sichere Chipkarte ausfolgt. Wenn der Computer des Signators mit Viren und Trojanern verseucht ist oder wenn der Signator Dokumente signiert, die sich dynamisch verändern können, dann ergibt sich daraus die Gefahr, dass der Signator etwas signiert, was ihm in dieser Form nicht angezeigt wurde. Dem österreichischen Gesetz- und Verordnungsgeber war es ein besonderes Anliegen, auch diesen Risken zu begegnen. Daher wurden auch Bestimmungen vorgesehen, welche sich auf die zu verwendenden Dokumentenformate und die Möglichkeit der sicheren Anzeige des zu signierenden Dokuments und auf die sichere PIN-Eingabe beziehen.

Gemäß § 7 Abs. 2 SigV müssen die von den Signatoren eingesetzten technischen Komponenten und Verfahren zur Erstellung sicherer elektronischer Signaturen die vollständige Anzeige der zu signierenden Daten ermöglichen. Der Zertifizierungsdiensteanbieter muss dem Signator Dokumentenformate und entsprechende Software (Secure Viewer) bereitstellen oder empfehlen, welche sicher elektronisch signiert werden können. Der Signator darf nur die vom Zertifizierungsdiensteanbieter empfohlenen Formate verwenden. § 7 Abs. 2 SigV verlangt weiters, dass die Spezifikation der Dokumentenformate allgemein verfügbar sein muss. Können in einem Format auch dynamische Veränderungen (das könnte z. B. ein in Abhängigkeit vom aktuellen Datum unterschiedlich angezeigter Geldbetrag sein) oder unsichtbare Daten codiert werden, so dürfen die betreffenden Codierungen nicht verwendet werden.

Gemäß § 7 Abs. 3 SigV darf die sichere elektronische Signatur nur durch Verwendung von Autorisierungscodes (z. B. durch PIN-Eingabe) auslösbar sein. Es ist möglich, dass mehrere Signaturen durch eine einzige PIN-Eingabe ausgelöst werden, dem Signator muss aber vor der PIN-Eingabe bekannt sein, wie viele Dokumente er nun signiert und er muss die Möglichkeit haben, diese Dokumente zu sehen. Auch die Zwischenspeicherung des PIN-Codes ist untersagt. Diese Bestimmung soll sicherstellen, dass die sichere elektronische Signatur willentlich ausgelöst wird – damit kann der Signator sie nachträglich nicht mehr abstreiten, was der Rechtssicherheit dient. In der Praxis wird allerdings oft bedauert, dass es im SigG und der SigV keine Regelungen für automatisch ausgelöste Signaturen gibt. In manchen Konfigurationen wäre es wünschenswert, dass ein einmal aktiviertes Gerät automatisch alles signiert, was ihm vorgelegt wird – nicht im Sinne eines Willensaktes, sondern etwa um Dokumente mit einem Zeitstempel zu versehen. Die sichere elektronische Signatur kann aufgrund von § 7 Abs. 3 SigV für eine solche Anwendung nicht eingesetzt werden, ein ähnlich sicheres Pendant für automatisch ausgelöste Signaturen gibt es nicht.

Eine Novelle der SigV ist in Vorbereitung. Die Novelle soll vor allem die folgenden Punkte regeln:

- Anpassung an die Änderungen der Novelle des § 5 Abs. 3 SigG. Seit dieser Novelle müssen qualifizierte Zertifikate nicht mehr mit sicheren elektronischen Signaturen versehen werden, daher sind viele technische Anforderungen an die Signaturerstellungseinheiten der Zertifizierungsdiensteanbieter weggefallen. Die Novelle der SigV soll diese Regelungslücke wieder schließen, indem eine Reihe von technischen Anforderungen – etwa an die verwendeten kryptografischen Algorithmen – nicht bloß an die Erstellung sicherer elektronischer Signaturen durch den Endkunden, sondern auch wieder an die Anbieter qualifizierter Zertifikate gerichtet werden.
- Im Hinblick auf die auf europäischer Ebene geführten Diskussionen über eine Harmonisierung der Anforderungen an kryptografische Algorithmen und Parameter (vgl. Abschnitte 1.1.5 und 4.1.5.2.1) sollen die bisherigen Anhänge der SigV sowie eine Reihe von bisher in den §§ 3 bis 7 SigV geregelten technischen Anforderungen durch das europäische Algorithmenpapier von ETSI ersetzt werden. Bedauerlich ist allerdings, dass dieses Dokument lediglich Anforderungen bis Ende 2005 festlegt und auf europäischer Ebene noch keine Einigkeit darüber erzielt wurde, welche Anforderungen danach gelten sollen und welches Gremium die laufende Aktualisierung der Anforderungen übernehmen soll. Die Novelle der SigV bringt diesbezüglich also eine Änderung der Regelungstechnik – österreichische Anforderungen werden durch europaweit harmonisierte Anforderungen ersetzt –, aber keine Perspektive für die Anbieter und Nutzer, welche Anforderungen ab 2006 gelten werden, insbesondere wie lange die derzeit eingesetzten Chipkarten, die RSA mit einer Schlüssellänge von 1.024 Bit verwenden, noch eingesetzt werden dürfen.
- Weiters soll die Novelle der SigV eine Reihe von Erfahrungen aus der Praxis berücksichtigen.

1.2.3 Bestätigungsstellen

1.2.3.1 Rechtliche Grundlagen

Auf europäischer Ebene wurde in Art. 3 Abs. 4 der Signaturrichtlinie vorgesehen, dass die Übereinstimmung von sicheren Signaturerstellungseinheiten von geeigneten öffentlichen oder privaten Stellen festgestellt wird, die von den Mitgliedstaaten benannt werden. Die Signaturrichtlinie hat damit einerseits den Bedarf festgestellt, dass sichere Signaturerstellungseinheiten

von einer herstellerunabhängigen Stelle geprüft werden, andererseits den Mitgliedstaaten einen Spielraum offen gelassen, nach welchen Kriterien die benannten Stellen ausgewählt werden, insbesondere ob es sich dabei um öffentliche oder um private Stellen handelt.

Die Signaturrichtlinie sieht aber auch vor, dass die Europäische Kommission Mindestkriterien festsetzt, anhand derer die Mitgliedstaaten bestimmen, ob eine Stelle geeignet ist. Diese Mindestkriterien wurden am 16.11.2000 kundgemacht[27].

In Österreich hat der Gesetzgeber bereits in der Stammfassung des SigG Kriterien für Bestätigungsstellen aufgestellt. § 19 Abs. 2 SigG verlangt Zuverlässigkeit, entsprechende Fachkenntnisse des Personals, ausreichende technische Einrichtungen und wirtschaftliche Leistungsfähigkeit sowie die erforderliche Unabhängigkeit, Unparteilichkeit und Unbefangenheit. In der ersten Novelle des SigG wurde weiters verlangt, dass die auf europäischer Ebene festgelegten Mindestkriterien durch eine Verordnung des Bundeskanzlers ins österreichische Recht übernommen werden. Dies geschah irrtümlich sogar zweimal, es gibt zwei fast gleich lautende Bestätigungsstellenverordnungen[28].

Nach österreichischem Recht wird eine Einrichtung zur Bestätigungsstelle, indem der Bundeskanzler auf Antrag der Einrichtung im Einvernehmen mit dem Bundesminister für Justiz eine Verordnung erlässt, in welcher die Eignung der Einrichtung festgestellt wird. Bislang ist eine solche Verordnung erlassen worden, mit welcher der Verein „Zentrum für sichere Informationstechnologie – Austria (A-SIT)“ zur Bestätigungsstelle wurde.

Die Bestätigungsstellen haben nach dem SigG zwei Aufgaben:

- Einerseits haben Bestätigungsstellen technische Komponenten und Verfahren für sichere elektronische Signaturen zu prüfen und die Erfüllung der Sicherheitsanforderungen des SigG und der SigV zu bescheinigen (§ 18 Abs. 5 SigG). In diesem Bereich werden Bestätigungsstellen hoheitlich

27) Entscheidung der Europäischen Kommission vom 06.11.2000 über die Mindestkriterien, die von den Mitgliedstaaten bei der Benennung der Stellen gemäß Art. 3 Abs. 4 der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen zu berücksichtigen sind, ABl. L 289 vom 16.11.2000, S. 42.

28) Verordnung des Bundeskanzlers über die Eignung von Bestätigungsstellen (Bestätigungsstellenverordnung – BestV), BGBl II Nr 117/2002 und BGBl II Nr 299/2002. Die beiden Kundmachungen unterscheiden sich an etwa 15 Stellen, aber nur in unwesentlichen Details (Interpunktion, Groß- und Kleinschreibung, Schreibweise der zitierten CELEX-Nr., Datumsschreibweise, Silbentrennung, Seitenumbruch).

tätig. Durch die von der Bestätigungsstelle ausgestellte Bescheinigung erlangt das geprüfte Gerät einen besonderen rechtlichen Status – es kann zur Erstellung sicherer elektronischer Signaturen verwendet werden. Die Bescheinigungen der Bestätigungsstellen werden aufgrund der Signaturrichtlinie im gesamten Europäischen Wirtschaftsraum anerkannt; für die Hersteller reicht es daher grundsätzlich aus, wenn sie ihre Geräte nur von einer notifizierten Bestätigungsstelle prüfen und bescheinigen lassen.

- Andererseits kommt Bestätigungsstellen nach dem österreichischen SigG auch die Aufgabe zu, die Aufsichtsstelle (Telekom-Control-Kommission – TKK) und die RTR-GmbH zu beraten. Sowohl die TKK als auch die RTR-GmbH können sich zur Beratung geeigneter Personen oder Einrichtungen wie insbesondere einer Bestätigungsstelle bedienen. Die RTR-GmbH hat sich darüber hinaus in technischen Fragen (dies betrifft insbesondere die von der RTR-GmbH betriebene Public-Key-Infrastruktur, siehe Abschnitt 2.2) mit einer Bestätigungsstelle abzustimmen. Die TKK hat daher insbesondere in allen Verfahren betreffend das Angebot qualifizierter Zertifikate bzw. sicherer elektronischer Signaturen ein Gutachten der Bestätigungsstelle A-SIT eingeholt.

Die Rechtsgrundlage für Bestätigungsstellen findet sich zwar im SigG, aber auch in anderen Rechtsvorschriften wird auf Bestätigungsstellen zurückgegriffen. Nach § 34 Abs. 6 Hochschülerschaftsgesetz (HSG) sind die bei elektronischen Hochschülerschaftswahlen eingesetzten technischen Komponenten von einer Bestätigungsstelle zu prüfen und zu bescheinigen, bei einer Beeinträchtigung der Sicherheit während der Wahl hat die Wahlkommission bei der Entscheidung über die Gültigkeit der vor dem Abbruch abgegebenen elektronischen Stimmen eine Bestätigungsstelle beizuziehen (§ 39 Abs. 6 HSG), weiters kann eine Bestätigungsstelle auch zur Beratung bei Einsprüchen gegen die elektronische Wahl herangezogen werden (§ 44 Abs. 8 und § 45 Abs. 8 HSG). Ähnliche Bestimmungen finden sich im Wirtschaftskammergesetz (WKG) über die elektronische Stimmabgabe bei Wahlen der Wirtschaftskammer: Nach § 74 Abs. 4 WKG muss die Erfüllung der Sicherheitsanforderungen von einer Bestätigungsstelle bescheinigt sein, nach § 78 Abs. 6 WKG hat die Hauptwahlkommission bei der Entscheidung über den Abbruch einer elektronisch geführten Wahl im Falle dass die Funktionsfähigkeit des verwendeten Systems nicht mehr gegeben ist, eine Bestätigungsstelle beizuziehen.

1.2.3.2 Zentrum für sichere Informationstechnologie – Austria (A-SIT)

Dass die technischen Komponenten zur Erstellung sicherer elektronischer Signaturen einer unabhängigen Prüfung bedürfen und dazu entsprechende Stellen einzurichten sind, wurde bei den Verhandlungen über die Signaturrichtlinie vor allem von Deutschland (wo bereits ein entsprechendes Aufsichtssystem mit einer Aufsichtsstelle und drei Bestätigungsstellen etabliert war) und von Österreich forciert. In Österreich wurde daher parallel dazu auch eine entsprechende Einrichtung gegründet. Einerseits wollte man mit diesen Aufgaben keine bestehende staatliche Stelle betrauen, zumal auch noch keine existierende staatliche Stelle vergleichbare Aufgaben wahrgenommen hat, andererseits aber bestand auch kein erkennbares privatwirtschaftliches Interesse an der Gründung einer Bestätigungsstelle.

Daher ging man einen Mittelweg und gründete eine Bestätigungsstelle zwar in der privaten Rechtsform eines Vereines, allerdings mit jenen staatlichen Stellen als Vereinsmitgliedern, die ein besonderes Interesse an der Etablierung einer Bestätigungsstelle hatten. Gründungsmitglieder des im Mai 1999 gegründeten Vereines „Zentrum für sichere Informationstechnologie – Austria (A-SIT)" waren das Bundesministerium für Finanzen (BMF), die Oesterreichische Nationalbank (OeNB) und die Technische Universität Graz (TU Graz). Seit Mitte 2003 ist auch die Steirische Wirtschaftsförderung Mitglied von A-SIT. Für die OeNB war für die Gründung von A-SIT vor allem ihr Interesse im Hinblick auf die Aufsicht über den Zahlungsverkehr bedeutsam, für das BMF vor allem die erwartete Verwendung elektronischer Signaturen im Bereich des E-Government. Die TU Graz trug zur Vereinsgründung bei, indem die Expertise des Institutes für Angewandte Informationsverarbeitung und Kommunikationstechnologie in den Verein eingebracht wurde. A-SIT hat seinen Vereinssitz und einen Standort in Wien, einen weiteren Standort in Graz.

Mit einer Verordnung, die am 03.02.2000 in Kraft trat[29], wurde der Verein A-SIT zur Bestätigungsstelle nach dem SigG.

Abschnitt 3.2 gibt einen Überblick über die von A-SIT ausgestellten Bescheinigungen nach dem SigG. Für die TKK hat A-SIT in drei Verfahren betreffend Anträge auf Akkreditierung ein Gutachten erstellt (in einem der drei Verfahren wurde das Gutachten nicht völlig abgeschlossen, da der Antrag

29) Verordnung des Bundeskanzlers über die Feststellung der Eignung des Vereins „Zentrum für sichere Informationstechnologie – Austria (A-SIT)" als Bestätigungsstelle, BGBl II Nr 31/2000.

auf Akkreditierung zurückgezogen wurde). Weiters wurde A-SIT in einigen weiteren Verfahren betreffend Anbieter qualifizierter Zertifikate um Stellungnahmen ersucht oder mit Gutachten beauftragt[30]. Die RTR-GmbH hat sich in technischen Fragen mit A-SIT abgestimmt, dabei hat A-SIT insbesondere ein ausführliches Gutachten (das von Umfang und Detailgrad etwa mit den in den Akkreditierungsverfahren erstatteten Gutachten vergleichbar war) betreffend die Public-Key-Infrastruktur der Aufsichtsstelle erstellt.

Neben den Aufgaben nach dem SigG nimmt A-SIT auch weitere Aufgaben wahr, unter anderem die Beratung der Bundesregierung in verschiedenen sicherheitstechnischen Fragen (z. B. im Zusammenhang mit der Bürgerkarte) und gutachterliche Tätigkeiten für die OeNB im Zusammenhang mit der Zahlungssystemaufsicht nach § 44a Nationalbankgesetz.

Im Rahmen der EESSI war A-SIT maßgeblich an Arbeitsgruppen zur Erstellung von Common-Criteria-Schutzprofilen für sichere Signaturerstellungseinheiten (siehe Abschnitt 4.1.5.3.3) und für vertrauenswürdige Komponenten von Zertifizierungsdiensteanbietern (siehe Abschnitt 4.1.5.3.2) beteiligt.

1.2.4 Andere Rechtsvorschriften

1.2.4.1 E-Government-Gesetz

Maßgebliche Änderungen für die Anwendung sicherer elektronischer Signaturen im Bereich der öffentlichen Verwaltung bringt das E-Government-Gesetz[31].

Bereits die Erlassung des SigG war von der Absicht getragen, dass damit die Grundlage für die elektronische Kommunikation mit der Verwaltung gelegt wurde. § 1 Abs. 2 SigG sieht vor, dass das Gesetz auch „im offenen elektronischen Verkehr mit Gerichten und anderen Behörden" anzuwenden sei, „sofern durch Gesetz nicht anderes bestimmt ist". Grundsätzlich wären also spätestens mit der Erlassung des SigG rechtliche Hindernisse für den Einsatz von E-Government-Lösungen beseitigt gewesen.

30) Z. B. wurde A-SIT im April 2002 um Stellungnahme ersucht, ob die von der Datakom Austria empfohlenen Kombinationen aus Chipkarte, Chipkartenleser und Viewersoftware jeweils die Auflagen in den Bescheinigungen erfüllen (A 7/2001). Im Juni 2002 wurde eine Stellungnahme von A-SIT eingeholt, als A-Trust eine Änderung vornahm und statt drei Fehlversuchen bis zu zehn Fehlversuche für die PIN-Eingabe zuließ (A 6/2002). Im Juli 2002 wurde ein Gutachtensauftrag an A-SIT erteilt, als die Datakom Austria neue Chipkarten einführte und dabei auch der Prozess der Personalisierung der Chipkarten geändert wurde (A 7/2002).

31) Zum Redaktionsschluss für diesen Bericht lag das E-Government-Gesetz als Regierungsvorlage vom 29.10.2003 vor, es wird voraussichtlich im ersten Quartal 2004 im Parlament beschlossen.

In der Praxis hingegen wurden elektronische Signaturen in der Verwaltung nur spärlich eingesetzt. Zunächst warteten die meisten Verwaltungsbehörden darauf, dass sichere elektronische Signaturen angeboten würden, weil andere Formen der elektronischen Signatur zu wenig sicher erschienen. In weiterer Folge wurde aber als unbefriedigend empfunden, dass die sichere elektronische Signatur den Bürger nur hinsichtlich seines Namens identifiziert, oft aber eine genauere Identifikation erwünscht ist. Ein qualifiziertes Zertifikat weist nämlich als Identifikationsmerkmal des Zertifikatsinhabers im Regelfall nur seinen Namen auf, alle anderen Angaben (z. B. das Geburtsdatum oder die Adresse) können nur mit Zustimmung des Zertifikatsinhabers in das Zertifikat aufgenommen werden. Das qualifizierte Zertifikat wird zwar nur nach einer Identitätsüberprüfung anhand eines amtlichen Lichtbildausweises ausgestellt, sodass bei Streitfällen im Nachhinein auch bei Namensgleichheit eindeutig klärbar wäre, wer eine sichere elektronische Signatur erstellt hat (der Zertifizierungsdiensteanbieter muss eine Ausweiskopie aufbewahren und die Daten des Ausweises protokollieren). Diese Klärbarkeit im Nachhinein genügt der Verwaltung aber in vielen Fällen nicht, gewünscht war eine eindeutige Zuordnung des Zertifikatsinhabers zu bestehenden staatlichen Registern. Wenn eine Eva Müller oder ein Hans Mayer eine Eingabe an das Finanzamt signiert, dann soll sofort eine zuverlässige Zuordnung zum richtigen Steuerakt vorgenommen werden können – die nachträgliche Überprüfung in Streitfällen, ob Eva Müller in ihren eigenen Steuerakt Einsicht genommen hat oder in den einer Person gleichen Namens, erscheint für automationsunterstützte Verarbeitung nicht ausreichend sicher zu sein.

Manche Staaten lösen dieses Problem, indem ein staatliches Personenkennzeichen verpflichtend in das Zertifikat aufgenommen werden muss. In Italien etwa wird die Sozialversicherungsnummer in das Zertifikat aufgenommen. Da die Sozialversicherungsnummer auch als Ordnungsbegriff in zahlreichen Datenbanken der Verwaltung verwendet wird, kann bei einer signierten Eingabe schnell und zuverlässig eine Verbindung zwischen dem Zertifikat und dem richtigen Akt in der Datenbank hergestellt werden. Ein solches einheitliches Personenkennzeichen für die gesamte Verwaltung war in Österreich aber aus Datenschutzerwägungen nicht erwünscht. Wenn ein Bürger in allen staatlichen Datenbanken mit derselben Nummer gekennzeichnet wird, dann lassen sich leicht alle Datenbanken zu einer großen Datenbank zusammenführen – der Bürger wird für den Staat zum gläsernen Bürger.

Der – höchst komplexe – Lösungsansatz des E-Government-Gesetzes für diese Problematik besteht darin, dass eine Person in den verschiedenen Verwaltungsbereichen jeweils mit unterschiedlichen Personenkennzeichen eindeutig gekennzeichnet wird; dass sich die einzelnen bereichsspezifischen Personenkennzeichen aber nicht aus anderen bereichsspezifischen Personenkennzeichen ableiten lassen. Es soll also z. B. die Finanzverwaltung andere Personenkennzeichen verwenden als die Führerscheinbehörde. Damit die Personenkennzeichen dennoch eindeutig vergeben werden, sollen sie alle nach einem bestimmten mathematischen Verfahren aus einem einheitlichen Personenkennzeichen, der sogenannten Stammzahl, abgeleitet werden, die wiederum aus der ZMR-Zahl des Zentralen Melderegisters abgeleitet wird. Ein komplexes System an Schutzmechanismen soll verhindern, dass Behörden dennoch verwaltungsbereichsübergreifend die über die Bürger gespeicherten Daten zusammenführen können.

Die durch das E-Government-Gesetz vorgesehene Kennzeichnung der Bürger durch Stammzahl und bereichsspezifische Personenkennzeichen hat einige Auswirkungen auf die elektronische Kommunikation zwischen Bürgern und Behörden. Zunächst einmal benötigt der Bürger nicht bloß ein Zertifikat eines Zertifizierungsdiensteanbieters (welches seinen öffentlichen Schlüssel und damit alle von ihm signierten Nachrichten seinem Namen zuordnet), sondern auch die sogenannte „Personenbindung", eine vom Staat ausgestellte Bescheinigung, welche die Stammzahl des Bürgers enthält. Weiters muss bei der elektronischen Kommunikation nicht bloß die signierte Nachricht und das Zertifikat übermittelt werden, sondern es muss auch die „Personenbindung" beigelegt werden. Für die Kommunikation ist daher ein eigenes Protokoll erforderlich, dieses wurde von der Stabsstelle IKT-Strategie im Bundeskanzleramt in den letzten Jahren unter dem Namen „Security Layer" entwickelt (vgl. Abschnitt 3.2.5).

Eine weitere einschneidende Neuerung durch das E-Government-Gesetz besteht darin, dass das E-Government-Gesetz die durch das SigG vorgesehenen Begriffe der (einfachen) elektronischen Signatur und der sicheren elektronischen Signatur um einen weiteren Begriff bereichert, die sogenannte „Verwaltungssignatur". Eine Verwaltungssignatur ist vom Standpunkt der Sicherheit aus betrachtet zwischen der einfachen und der sicheren elektronischen Signatur angesiedelt. Die Verwaltungssignatur soll für einen Übergangszeitraum (nach der Regierungsvorlage zum E-Government-Gesetz: bis Ende 2007) für den Bereich des E-Government einen Ersatz für die sichere elektronische Signatur darstellen. Die Sicherheitsanforderungen werden also

in der Kommunikation mit der Hoheitsverwaltung eingeschränkt. Die genaueren Voraussetzungen für das Vorliegen einer Verwaltungssignatur sollen durch eine Verordnung des Bundeskanzlers festgelegt werden[32].

Als weitere Form der elektronischen Signatur führt das E-Government-Gesetz den Begriff der „Amtssignatur" ein. Dabei handelt es sich um eine elektronische Signatur im Sinn des SigG, deren Besonderheit durch ein entsprechendes Attribut im Signaturzertifikat gekennzeichnet ist. Dies soll die Erkennbarkeit erleichtern, dass die Signatur von einer Behörde erstellt wurde. Die Regierungsvorlage zum E-Government-Gesetz enthält auch Vorschriften zur optischen Darstellung der Amtssignatur in Ansichten elektronischer Dokumente und zur Beweiskraft von auf Papier ausgedruckten elektronischen Dokumenten von Behörden, die mit einer Amtssignatur signiert sind[33].

1.2.4.2 Weitere Gesetze

Im Umsatzsteuergesetz spielt die Rechnungslegung eine zentrale Rolle – nur mit einer Rechnung kann der Unternehmer sich die geleistete Umsatzsteuer über den Vorsteuerabzug wieder zurückholen. Gemäß § 11 Abs. 2 UStG sind auch auf elektronischem Wege übermittelte Rechnungen gültig, wenn der Empfänger zustimmt und die Echtheit der Herkunft sowie die Unversehrtheit des Inhalts gewährleistet sind. Der Bundesminister für Finanzen hat mit Verordnung die Anforderungen zu bestimmen, bei deren Vorliegen diese Voraussetzungen erfüllt sind. Ein Verordnungsentwurf ist im Februar 2003 bekannt geworden, die Verordnung soll Ende 2003 im Bundesgesetzblatt kundgemacht werden.

Verschiedene Gesetze sehen zur Bekämpfung von Geldwäscherei und Terrorismusfinanzierung besondere Sorgfaltspflichten vor: vor der Anknüpfung einer dauerhaften Geschäftsbeziehung müssen etwa Kredit- und Finanzinstitute nach § 40 Bankwesengesetz eine Identitätsüberprüfung des Kunden anhand eines amtlichen Lichtbildausweises vornehmen, dasselbe gilt für Transaktionen von mindestens EUR 15.000. Eine ähnliche Regelung sieht § 365o Gewerbeordnung für Gewerbetreibende vor, die mit hochwertigen Gütern wie Edelsteinen, Edelmetallen oder Kunstwerken handeln; ebenso für gewerbliche Buchhalter, für Immobilienmakler und für Versteigerer. § 18a Versicherungsaufsichtsgesetz enthält (mit anderen Wertgrenzen)

32) § 25 Abs. 1 der Regierungsvorlage zum E-Government-Gesetz, ein Begutachtungsentwurf der Verordnung lag zum Redaktionsschluss dieses Berichts noch nicht vor.
33) §§ 19 und 20 der Regierungsvorlage zum E-Government-Gesetz.

eine Pflicht zur Identitätsfeststellung vor dem Abschluss von Lebensversicherungen. Nach allen drei genannten Bestimmungen ist es aber nun möglich, bei Ferngeschäften auf eine Identitätsüberprüfung mittels Ausweis zu verzichten, wenn der Kunde eine sichere elektronische Signatur verwendet.

Nur in wenigen gesetzlichen Bestimmungen ist ausdrücklich angeordnet, dass sichere elektronische Signaturen verwendet werden müssen. Hervorzuheben ist hier das Vergaberecht. Nach verschiedenen Bestimmungen[34] des Bundesvergabegesetzes sind für die elektronische Kommunikation (insbesondere auch für elektronisch übermittelte Angebote) sichere elektronische Signaturen zu verwenden. Eine Verordnung, die dies näher konkretisiert („E-Procurement-Verordnung") war bis Mitte Oktober 2003 in Begutachtung und bei Redaktionsschluss dieses Berichts noch nicht erlassen.

Die verpflichtende Verwendung der sicheren elektronischen Signatur im Fall elektronischer Kommunikation ist auch in § 9 der Verordnung betreffend die Meldung unerwünschter Arzneimittelwirkungen (Meldepflicht-Verordnung) vorgesehen.

An einigen Stellen der Rechtsordnung wird nochmals klargestellt, dass sichere elektronische Signaturen anstelle von Unterschriften verwendet werden können, obwohl dies ohnehin durch § 4 Abs. 1 SigG generell so geregelt ist. Solche Regelungen finden sich etwa in § 5 Abs. 7 Datenverarbeitungsregister-Verordnung 2002 (wo bloß wiederholt wird, was gemäß § 13 Abs. 4 Allgemeines Verwaltungsverfahrensgesetz – AVG und § 4 Abs. 1 SigG ohnehin für jedes Verwaltungsverfahren gilt), in § 3 Rezeptpflichtgesetz oder in § 3 Magnetfeldtherapiegeräteverordnung.

§ 9 Meldegesetz-Durchführungsverordnung verlangt für den Schutz der Verbindungen zwischen den Meldebehörden und dem Zentralen Melderegister „Software-Zertifikate". Der Verordnungstext setzt aber in irreführender Weise die Begriffe „Zertifikat" und „Schlüssel" gleich. Gemeint ist mit der Bestimmung wohl, dass die Verbindung verschlüsselt und beiderseits authentifiziert erfolgen soll und für die Verschlüsselung und Authentifizierung Zertifikate eingesetzt werden.

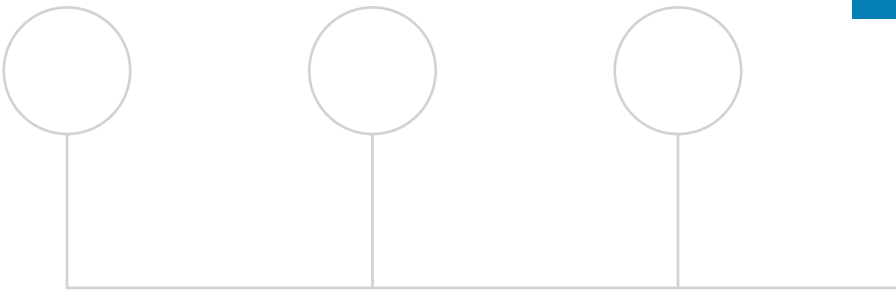
34) § 22 Abs. 2, § 52 Abs. 3, § 82 Abs. 3 und 4, § 83 Abs. 1 Z 8, § 89 Abs. 4, § 102 Abs. 3 BVergG.

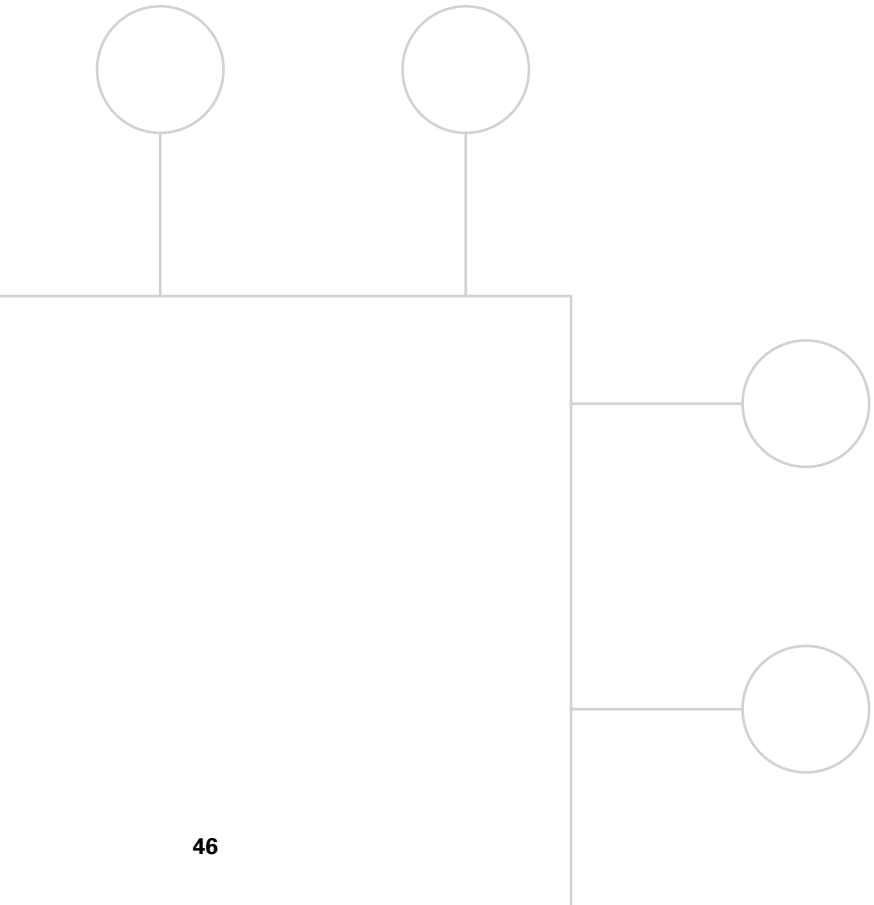
§ 39 Studienförderungsgesetz 1992 regelt die elektronische Einbringung von Anträgen auf Studienbeihilfe. In Abs. 5 ist die Festlegung von Beginn und Form der elektronischen Antragstellung aber „nach Maßgabe der technischen und organisatorischen Möglichkeiten unter Verwendung sicherer elektronischer Signaturen" einer (noch nicht erlassenen) Verordnung vorbehalten.

Für die Hochschülerschaftswahlen und die Wirtschaftskammerwahlen ist in den jeweiligen Gesetzen (§§ 34 ff HSG 1998 und §§ 74 ff WKG 1998) die Möglichkeit der elektronischen Wahl vorgesehen. Dabei wird darauf verwiesen, dass sichere elektronische Signaturen einzusetzen sind, weitere Zusatzanforderungen sollen das Wahlgeheimnis sichern.

Die Begriffe „Zertifikat" und „Signatur" werden in der Rechtsordnung auch in anderen Zusammenhängen verwendet als in dem der elektronischen Signatur. Nach dem Akkreditierungsgesetz[35] werden Prüf- und Überwachungsstellen sowie Zertifizierungsstellen akkreditiert. Die Prüf- und Überwachungsstellen erstellen Prüfberichte, die Zertifizierungsstellen bescheinigen die Konformität mit einschlägigen Rechtsvorschriften und Normen. Die von den Zertifizierungsstellen ausgestellten Bescheinigungen werden dabei „Zertifikate" genannt – werden aber in der Regel nicht elektronisch ausgestellt. Akkreditierungsgesetz und Signaturgesetz (SigG) sind voneinander völlig unabhängige Regelungswerke. Die Begriffe des Akkreditierungsgesetzes kommen z. B. auch in § 4 Bauproduktegesetz oder in § 6 Maschinen-Sicherheitsverordnung vor. In manchen Rechtsvorschriften werden die Begriffe „Zertifikat" und „Signatur" auch mit völlig anderen Bedeutungen verwendet, so z. B. der Begriff „Zertifikat" anstelle von „Zeugnis" sowie im Wertpapierrecht und im Ökostromgesetz und der Begriff „Signatur" im Arzneimittelrecht und im Zusammenhang mit der Kartografie.

35) BGBl Nr 468/1992.





Tätigkeit der Aufsichtsstelle

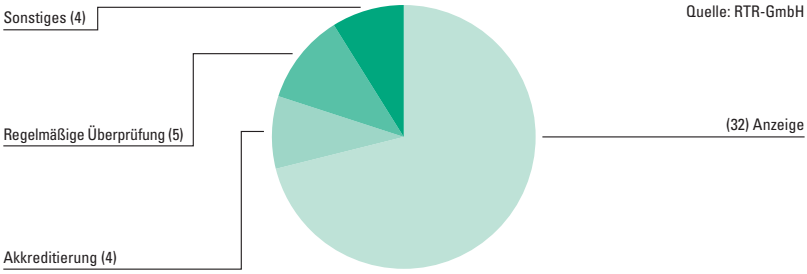
2.1 Verfahren der Telekom-Control-Kommission (TKK)

2.1.1 Übersicht

Zu den wesentlichsten Verfahrensarten nach dem SigG gehören die Anzeige der Aufnahme der Tätigkeit von Zertifizierungsdiensteanbietern, die Anzeige von Änderungen und die Anzeige der Einstellung der Tätigkeit sowie Anträge auf Akkreditierung. Weiters hat die Aufsichtsstelle die Zertifizierungsdiensteanbieter nicht nur im Rahmen von Anzeigen und Anträgen auf Akkreditierung, sondern auch regelmäßig zumindest alle zwei Jahre, darüber hinaus stichprobenartig zu überprüfen.

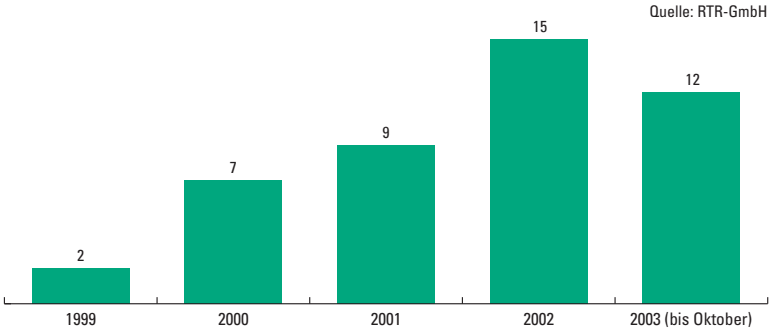
Insgesamt wurden im Berichtszeitraum 01.01.2000 bis 31.10.2003 45 Verfahren nach dem SigG anhängig, Abb. 5 zeigt jeweils das verfahrenseinleitende Ereignis: Anzeigen nach § 6 SigG oder nach § 12 SigG, Anträge auf Akkreditierung nach § 17 SigG, regelmäßige Überprüfung nach maximal zwei Jahren gemäß § 18 Abs. 4 SigV oder sonstige Verfahren:

Abb. 5: Verfahrensarten nach dem SigG



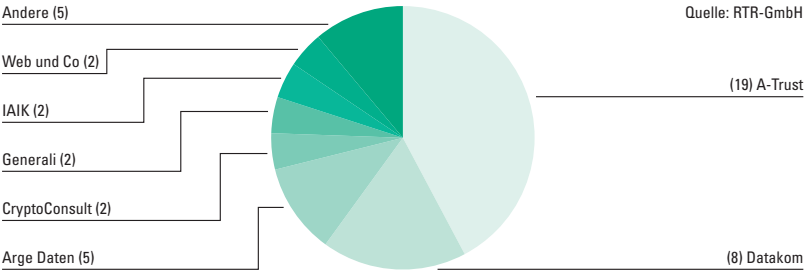
Die Verteilung dieser Verfahren auf die einzelnen Jahre zeigt Abb. 6 (dargestellt ist jeweils das Jahr, in dem das Verfahren begonnen wurde, zwei Anzeigen wurden in den letzten Dezembertagen des Jahres 1999 knapp vor In-Kraft-Treten des SigG eingebracht).

Abb. 6: Anzahl der Verfahren nach dem SigG



Die meisten Verfahren betrafen den Zertifizierungsdiensteanbieter A-Trust. Abb. 7 zeigt die Verteilung auf die einzelnen Zertifizierungsdiensteanbieter[36].

Abb. 7: Verfahren nach Zertifizierungsdiensteanbietern



2.1.2 Anzeigen nach § 6 SigG

Gemäß § 6 Abs. 2 SigG ist der Aufsichtsstelle die Aufnahme der Tätigkeit als Zertifizierungsdiensteanbieter unverzüglich anzuzeigen. Spätestens mit Aufnahme der Tätigkeit und auch bei Änderung seiner Dienste ist dabei jeweils ein Sicherheits- und Zertifizierungskonzept für jeden angebotenen Zertifizierungsdienst vorzulegen. Diese Verpflichtung zur Anzeige gilt für alle Zertifizierungsdiensteanbieter unabhängig davon, ob sie einfache oder qualifizierte Zertifikate ausstellen.

36) Vgl. zu den einzelnen Zertifizierungsdiensteanbietern die Beschreibung in Abschnitt 3.1, dort sind auch die vollständigen Namen der Anbieter angeführt.

Für die Anbieter einfacher Zertifikate spielt das angezeigte Sicherheits- und Zertifizierungskonzept eine besondere Rolle. Da es für einfache Zertifikate im SigG kaum Anforderungen gibt, ist das Sicherheits- und Zertifizierungskonzept eine Form der Selbstbindung durch den Zertifizierungsdiensteanbieter. Was er darin festhält, muss er in weiterer Folge auch einhalten (§ 6 Abs. 4 SigG). Durch entsprechende Gestaltung des Sicherheits- und Zertifizierungskonzepts kann also zwischen einem sehr einfachen Zertifizierungsdienst mit einem nur wenige Seiten umfassenden Konzept und sehr komplexen und sicheren Konzepten, die an die Sicherheitsanforderungen für qualifizierte Zertifikate herankommen, variiert werden.

Im Berichtszeitraum 01.01.2000 bis 31.10.2003 hatte die Aufsichtsstelle 18 Anzeigen betreffend die Aufnahme von neuen Zertifizierungsdiensten und 19 Anzeigen betreffend Änderungen bestehender Zertifizierungsdienste erhalten. (Da manchmal in derselben Anzeige die Aufnahme neuer Dienste und die Änderung bestehender Dienste bekannt gegeben werden, entspricht diese Anzahl nicht den angegebenen 32 Verfahren (siehe Abb. 5), die durch eine Anzeige eingeleitet wurden. In manchen Fällen wurden auch im selben Verfahren mehrere Anzeigen eingebracht, weil sich während des Verfahrens herausgestellt hat, dass die ursprüngliche Anzeige unvollständig war. Weiters wurde bei zwei Verfahren, die als regelmäßige Überprüfung nach § 18 Abs. 4 SigV eingeleitet wurden, festgestellt, dass noch nicht angezeigte Änderungen des Sicherheits- und Zertifizierungskonzepts vorlagen. Die Anzeige wurde dann im Rahmen des Überprüfungsverfahrens nachgeholt.)

2.1.2.1 Anzeigen betreffend nicht qualifizierte Zertifikate

Die meisten Anzeigen, welche der Aufsichtsstelle übermittelt werden, betreffen Zertifizierungsdienste, bei denen keine qualifizierten Zertifikate ausgestellt werden. Im Regelfall werden diese Anzeigen nach kurzer formaler Überprüfung in der jeweils nächsten Sitzung der TKK mit dem Beschluss, keine Aufsichtsmaßnahmen zu ergreifen, zur Kenntnis genommen. Über diesen Beschluss wird der Zertifizierungsdiensteanbieter verständigt.

Gleichzeitig beschließt die TKK die Erlassung eines Bescheides über die Gebühren für die Behandlung der Anzeige und beauftragt die RTR-GmbH, für den jeweiligen Zertifizierungsdienst ein Zertifikat auszustellen.

Auf der Website der Aufsichtsstelle, http://www.signatur.rtr.at/, werden einlangende Anzeigen in der Regel umgehend am Tag des Einlangens oder am darauf folgenden Werktag auf der den jeweiligen Zertifizierungsdiensteanbieter beschreibenden Seite mit dem Vermerk angeführt, dass die Anzeige derzeit geprüft wird. Im Zuge der Bearbeitung der Anzeige wird dann deren Inhalt auf der Seite eingearbeitet, wo der jeweilige Zertifizierungsdienst beschrieben wird. Weiters werden auch die vom Zertifizierungsdiensteanbieter vorgelegten Dokumente des Sicherheits- und Zertifizierungskonzepts auf der Website veröffentlicht, soweit es sich nicht um vertrauliche Unterlagen handelt. Nach der Sitzung der TKK, in welcher beschlossen wird, keine Aufsichtsmaßnahmen zu ergreifen, wird der Vermerk, dass die Anzeige gerade geprüft wird, von der Website der Aufsichtsstelle entfernt.

Ins Detail gehende Ermittlungen sind bei Zertifizierungsdiensten, die keine qualifizierten Zertifikate betreffen, in der Regel nicht erforderlich. Da es kaum Anforderungen für diese Zertifizierungsdienste gibt, handelt es sich im Wesentlichen um eine formale Überprüfung, ob das vorgelegte Sicherheits- und Zertifizierungskonzept eine schlüssige Beschreibung des Zertifizierungsdienstes enthält und alle wesentlichen Informationen darin enthalten sind. Um den Anbietern die Anzeige zu erleichtern, hat die Aufsichtsstelle ein Formular[37] aufgelegt, das aber selten verwendet wird.

Weist eine Anzeige formale oder inhaltliche Mängel auf, dann hat die Aufsichtsstelle – da sie das AVG anzuwenden hat – den Zertifizierungsdiensteanbieter zunächst zur Verbesserung aufzufordern und eine angemessene Frist dafür zu setzen. Wird dem Mängelverbesserungsauftrag entsprochen, dann gilt die Anzeige als ursprünglich richtig eingebracht (§ 13 Abs. 3 AVG). Es ist dann also auch der Mangel saniert, dass der Zertifizierungsdiensteanbieter in der Zwischenzeit einen Zertifizierungsdienst erbracht hat, der nicht ordnungsgemäß angezeigt wurde.

Wird der Mangel hingegen nicht behoben, dann ist die Anzeige zurückzuweisen. Wenn der Zertifizierungsdiensteanbieter seinen Dienst bereits aufgenommen hat, hat er in diesem Fall also seine Anzeigepflicht verletzt. Das kann aufsichtsbehördliche Maßnahmen (insbesondere die Untersagung der Tätigkeit nach § 14 Abs. 2 Z 6 SigG) oder ein Verwaltungsstrafverfahren (§ 26 Abs. 3 Z 1 SigG) zur Folge haben.

37) Vgl. http://www.signatur.rtr.at/de/repository/rtr-csp-notification-10-20010601.html

Nur in einem Fall musste die TKK eine Anzeige zurückweisen, weil einem Mängelverbesserungsauftrag nicht entsprochen wurde[38]. Im konkreten Fall wurde das Sicherheits- und Zertifizierungskonzept nur in englischer Sprache vorgelegt und nicht in der Amtssprache. Die Aufsichtsstelle verwies diesbezüglich darauf, dass das Sicherheits- und Zertifizierungskonzept für alle Personen relevant ist, die auf die ausgestellten Zertifikate vertrauen, und daher in deutscher Sprache zu verfassen ist. Weiters wurde im Sicherheits- und Zertifizierungskonzept nicht die richtige Bezeichnung des Zertifizierungsdiensteanbieters verwendet, sodass dessen Identität aus dem Konzept nicht ersichtlich war. In dem die Anzeige zurückweisenden Bescheid wurde gleichzeitig als Aufsichtsmaßnahme aufgetragen, entweder den Zertifizierungsdienst binnen vierzehn Tagen einzustellen oder eine mängelfreie Anzeige zu erstatten. Der Anbieter erstattete eine neue Anzeige.

2.1.2.2 Anzeigen betreffend qualifizierte Zertifikate

Zeigt ein Zertifizierungsdiensteanbieter an, dass er einen Zertifizierungsdienst für qualifizierte Zertifikate erbringt, dann wird von der Aufsichtsstelle eine wesentlich detailliertere Überprüfung vorgenommen als bei nicht qualifizierten Zertifikaten. Insbesondere wird im Regelfall die RTR-GmbH beauftragt, einen Augenschein vor Ort durchzuführen und einen Bericht über die Erfüllung der Voraussetzungen des SigG und der SigV an die TKK zu erstatten, und die Bestätigungsstelle A-SIT wird mit einem Gutachten zur technischen Sicherheit beauftragt.

Der Überprüfungsumfang ist aber unabhängig davon zu sehen, ob der Zertifizierungsdiensteanbieter den Dienst bloß anzeigt, oder ob er eine Akkreditierung beantragt. Für die Aufnahme eines Zertifizierungsdienstes für qualifizierte Zertifikate haben alle Anbieter, die dies in Österreich angestrebt haben, jeweils die Variante bevorzugt, nicht erst mit der Betriebsaufnahme eine Anzeige zu erstatten, sondern schon einige Zeit vorher eine Akkreditierung zu beantragen. A-Trust hat sich aber kurzfristig doch dazu entschlossen, eine Anzeige zu erstatten und sich erst einige Monate später akkreditieren zu lassen (siehe dazu Abschnitt 2.1.4).

38) Telekom-Control-Kommission, A 1/2001 vom 27.03.2001

Ist ein Anbieter aber einmal akkreditiert, dann benötigt er für die Aufnahme weiterer Zertifizierungsdienste oder für Änderungen keine neue Akkreditierung mehr. Inwieweit eine Anzeige eine neuerliche Überprüfung durch die Aufsichtsstelle nach sich zieht, hängt vom Umfang der Änderungen ab. Folgende Anzeigen hatte die TKK zu prüfen:

Die Datakom Austria hatte einige Wochen nach der erfolgten Akkreditierung (17.12.2001) am 04.02.2002 angezeigt, den Zertifizierungsdienst a-sign Premium, für welchen sie akkreditiert worden war, ab 05.02.2002 aufzunehmen. Dabei wurden auch einige kleine Änderungen des Sicherheits- und Zertifizierungskonzepts angezeigt. Die Aufsichtsstelle hat die Dienstaufnahme zum Anlass genommen, einige Wochen später eine stichprobenartige Überprüfung vor Ort vorzunehmen und dabei die Praxis der Ausgabe qualifizierter Zertifikate zu prüfen (vgl. Abschnitt 2.1.5). Dabei wurde insbesondere geprüft, ob aus der Dokumentation nachvollziehbar ist, dass vor der Ausstellung von qualifizierten Zertifikaten eine Identitätsprüfung vorgenommen wird und eine Kopie des vorgewiesenen Lichtbildausweises zur Dokumentation genommen wird.

Als die Datakom Austria im Juni 2002 anzeigte, weitere Chipkartentypen zu unterstützen und dabei auch den Vorgang der Personalisierung der Chipkarten zu ändern, wurde ein neuerlicher Augenschein vor Ort durchgeführt und auch ein weiteres Gutachten von A-SIT eingeholt.

Mehrfach wurden von der Datakom Austria bzw. der Telekom Austria als ihrer Rechtsnachfolgerin Änderungen der Liste der empfohlenen Signaturprodukte angezeigt. Die TKK hat in diesem Zusammenhang einmal die Bestätigungsstelle A-SIT um Stellungnahme ersucht, ob nach Ansicht der Bestätigungsstelle die Auflagen aus den verschiedenen Bescheinigungen der Produkte eingehalten sind. Als bezüglich des Secure Viewer proSIGN Version 2.0 im Februar 2003 die von der TKK im Akkreditierungsbescheid gewährte zwölfmonatige Frist, eine Bescheinigung des Viewers nachzureichen, ergebnislos verstrichen ist, wurde die Telekom Austria von der Aufsichtsstelle dazu aufgefordert, das Produkt von der Liste der empfohlenen Signaturprodukte zu streichen – was am 10.02.2003 auch getan wurde.

Die A-Trust hat kurz nach der Aufnahme ihres Zertifizierungsdienstes trust|sign, bei dem ursprünglich qualifizierte Zertifikate für die einfache Signatur angeboten wurden, eine Änderungsanzeige übermittelt, dass qualifizierte Zertifikate für die sichere elektronische Signatur ausgestellt

werden. Die Aufsichtsstelle hat dies deshalb als unproblematisch angesehen, da in den wenigen Wochen, in denen der Zertifizierungsdienst offiziell in Betrieb war, noch kein einziges Zertifikat verkauft worden war. Problematisch wäre gewesen, wenn im Rahmen desselben Zertifizierungsdienstes zwei verschiedene Arten von Zertifikaten mit unterschiedlichen Rechtswirkungen ausgegeben worden wären.

In weiterer Folge wurde das Sicherheits- und Zertifizierungskonzept von trust|sign mehrere Male überarbeitet. In der Mehrzahl der Fälle waren die Änderungen so geringfügig, dass keine detaillierten Überprüfungen notwendig waren. Als die A-Trust die ausgegebenen Chipkarten dahingehend änderte, dass zusätzliche Datenelemente auf die Karte aufgenommen wurden und statt drei Fehlversuchen bei der PIN-Eingabe zehn Fehlversuche möglich waren[39], wurde eine Stellungnahme der Bestätigungsstelle A-SIT eingeholt.

Ende September 2003 nahm die A-Trust den Zertifizierungsdienst a.sign Uni auf – technisch weitgehend identisch mit dem zuvor von der Datakom Austria angebotenen Dienst a.sign Premium, aber in der neuen Konstellation, dass ein neues Unternehmen für die bestehende Infrastruktur verantwortlich wurde, wobei teilweise dieselbe Infrastruktur für die alten Zertifizierungsdienste der Datakom Austria und die neuen Dienste der A-Trust genutzt wurde (insbesondere die Räume, das Netzwerk und der Verzeichnisdienst; für die Ausstellung der Zertifikate und Widerrufsliste wurden verschiedene Server verwendet, die aber fast identisch konfiguriert wurden). Daher wurden im Verfahren vor allem die neuen organisatorischen Rahmenbedingungen ermittelt, dazu wurde auch Personal der A-Trust und der Telekom Austria einvernommen.

2.1.3 Anzeigen nach § 12 SigG – Einstellung der Tätigkeit

Dreimal wurde der Aufsichtsstelle eine Einstellung von einzelnen Zertifizierungsdiensten bzw. überhaupt der Tätigkeit als Zertifizierungsdiensteanbieter angezeigt. Hervorzuheben ist dabei vor allem die Anzeige der Datakom Austria, am 27.09.2002 um 24 Uhr alle Zertifizierungsdienste einzustellen und keine weiteren Zertifikate mehr auszugeben. Der Grund für diese Einstellung der Dienste lag in einer Umstrukturierung im Telekom Austria-Konzern (vgl. dazu Abschnitte 3.1.2 und 3.1.3).

39) Anmerkung: Die Chipkarten, die A-Trust für die sichere elektronische Signatur ausgibt, sind so konfiguriert, dass kein PUK-Code zum Entsperren der Karte vorgesehen ist. Wird der PIN-Code zu oft falsch eingegeben, dann muss die Karte ausgetauscht werden.

Erst in der Praxis hat sich herausgestellt, dass die Einstellung der Tätigkeit komplexer ist als im SigG beschrieben. In der Regel stellt ein Zertifizierungsdiensteanbieter seine Tätigkeit nämlich nicht abrupt ein, sondern ist bemüht, seine bestehenden Verträge einzuhalten. Daher wird zunächst einmal die Ausgabe neuer Zertifikate eingestellt. Die bereits verkauften Zertifikate hingegen werden weiterhin betreut, Verzeichnisdienst und Widerrufsdienst bleiben also in Betrieb. Erst dann, wenn der Gültigkeitszeitraum aller Zertifikate abgelaufen ist oder wenn nur mehr wenige Zertifikate gültig sind und diesen Kunden eine Entschädigung oder eine Ersatzlösung geboten werden kann, werden die Zertifizierungsdienste völlig eingestellt.

Eine vom SigG und der SigV nicht ausdrücklich behandelte Rechtsfrage ist in diesem Zusammenhang, unter welchem Namen nach einer Namensänderung des Zertifizierungsdiensteanbieters Widerrufslisten signiert werden dürfen. Für die Ausstellung von Zertifikaten hat die Aufsichtsstelle wiederholt aus den allgemeinen Rechtsschutzzwecken des SigG abgeleitet, dass der korrekte Name des Zertifizierungsdiensteanbieters im Issuer-Feld des Zertifikates genannt sein muss. Für das Zertifikat jenes Schlüssels, mit dem die Widerrufslisten signiert werden, wurde das nicht ausdrücklich festgestellt, im Regelfall wird aber derselbe Schlüssel für die Signatur von Zertifikaten und von Widerrufslisten verwendet. Stellt der Zertifizierungsdiensteanbieter nun im Zusammenhang mit einer Umbenennung oder einer Umstrukturierung im Konzern einen Dienst ein – wie es etwa im September/Oktober 2002 der Fall war, als die Datakom Austria ihre Dienste eingestellt hatte und danach in die Telekom Austria verschmolzen wurde – dann stellt sich die Frage, welcher Name danach für die Signatur der Widerrufslisten verwendet werden soll:

- Wenn der Zertifizierungsdiensteanbieter weiterhin den alten Namen verwendet, dann gibt es technisch die wenigsten Probleme – allerdings ist unschön, dass der alte Name verwendet wird.
- Wenn der Zertifizierungsdiensteanbieter einen neuen Namen, aber weiterhin den selben Schlüssel verwendet, dann wird derselbe Schlüssel zwei verschiedenen Namen zugeordnet. Dies ist zwar nur für qualifizierte Zertifikate ausdrücklich untersagt (§ 12 Abs. 4 SigV), widerspricht aber dem grundsätzlichen Konzept der elektronischen Signatur, einen Schlüssel immer eindeutig einer bestimmten Person zuzuordnen.

- Wenn der Zertifizierungsdiensteanbieter einen neuen Schlüssel erzeugt und ein neues Zertifikat verwendet, dann ist es rechtlich die korrekteste Lösung, aber es kann zu technischen Problemen bei der Signaturprüfung führen. Es könnte vorkommen, dass Software die Widerrufslisten nicht auswerten kann und daher dem Benutzer nicht anzeigt, dass ein Zertifikat bereits widerrufen wurde. Das wiederum ist nicht im Sinne des SigG, das ja zur Sicherheit der elektronischen Kommunikation beitragen soll.

Die Datakom Austria hat bei der Einstellung ihrer Zertifizierungsdienste die erste hier geschilderte Variante gewählt und die Widerrufslisten weiterhin mit demselben Schlüssel und einem auf den Namen „Datakom Austria" ausgestellten Zertifikat signiert. Im Hinblick darauf, dass diese Frage rechtlich nicht ausdrücklich geregelt ist und diese Lösung technisch die wenigsten Probleme bringt, hat die Aufsichtsstelle dies gebilligt und keine Aufsichtsmaßnahmen ergriffen.

2.1.4 Anträge auf Akkreditierung nach § 17 SigG

Grundsätzlich steht es dem Anbieter qualifizierter Zertifikate für die sichere elektronische Signatur frei, ob er eine Anzeige nach § 6 SigG erstattet (und seine Tätigkeit somit am nächsten Tag aufnehmen kann, ohne das Ende des aufsichtsbehördlichen Verfahrens abzuwarten) oder ob er lieber eine Akkreditierung nach § 17 SigG beantragt (diesfalls darf er sich erst nach Zustellung des stattgebenden Bescheides der TKK „akkreditierter Zertifizierungsdiensteanbieter" nennen). Einen Unterschied in den Anforderungen an den Anbieter gibt es nicht.

Da die Aufnahme der Tätigkeit eines Zertifizierungsdiensteanbieters, der qualifizierte Zertifikate ausstellt, ohnehin ein langwieriges Projekt ist, tendieren die Anbieter dazu, sich bereits einige Monate vor der geplanten Betriebsaufnahme formell an die Aufsichtsstelle zu wenden und eine Akkreditierung zu beantragen. Für den Anbieter ist dies die sicherere Variante: Er kann sich darauf verlassen, dass offene Fragen im Akkreditierungsverfahren geklärt und rechtskräftig entschieden werden und er danach getrost den Betrieb aufnehmen kann, ohne von einer Auslegung des Gesetzes durch die Aufsichtsstelle überrascht zu werden, die er nicht bedacht hat. Außerdem dient die Akkreditierung auch als Gütesiegel, mit dem man am Markt werben kann –

z. B. führt A-Trust das bei der Akkreditierung verliehene Bundeswappen sowohl auf der Website als auch am Briefpapier. Auch in anderen Staaten ziehen Zertifizierungsdiensteanbieter die Akkreditierung der Aufsicht vor. In Deutschland etwa haben alle Zertifizierungsdiensteanbieter mit einer Ausnahme den Weg der Akkreditierung gewählt und auch der eine Anbieter, der seine Tätigkeit zunächst bloß angezeigt hatte, hat kurz darauf die Akkreditierung beantragt.

Eine ähnliche Vorgangsweise hat in Österreich A-Trust gewählt. Zunächst wurde die Akkreditierung angestrebt, im Spätherbst 2001 wurde aber bekannt, dass die Datakom Austria (damals noch Konkurrentin von A-Trust) demnächst akkreditiert werden könnte. Zwischen den beiden Unternehmen setzte ein Wettrennen ein, wer als erster am Markt sei. Am 19.11.2001 wurde bei der Aufsichtsstelle die Anzeige nach § 6 Abs. 2 SigG eingebracht, die Tätigkeit am 15.12.2001 aufzunehmen. Somit konnte A-Trust damit werben, der erste Anbieter qualifizierter Zertifikate in Österreich zu sein. Zwei Tage danach wurde die Datakom Austria als erster österreichischer Zertifizierungsdiensteanbieter akkreditiert. Zur tatsächlichen Ausstellung der ersten qualifizierten Zertifikate kam es bei beiden Unternehmen erst im Februar 2002.

Bei der Entscheidung über die Akkreditierung der A-Trust hatte die Aufsichtsstelle abzuwägen, ob es zulässig sei, einen Zertifizierungsdiensteanbieter, der seine Tätigkeit bereits aufgenommen hat, zu akkreditieren. Dies wurde bejaht. Es ist möglich, dass ein Zertifizierungsdienst, der bereits Dienste betreibt, die das Erfordernis einer Akkreditierung (die sichere Signatur) nicht erfüllen, einen Zertifizierungsdienst für sichere elektronische Signaturen aufnimmt und sich dafür akkreditieren lässt. Und da für die besonderen Rechtswirkungen der sicheren elektronischen Signatur unerheblich ist, ob der Anbieter akkreditiert ist oder nicht, ist es auch zulässig, wenn der Anbieter hinsichtlich eines Zertifizierungsdienstes akkreditiert wird, den er bereits anbietet. Es besteht kein Grund, den Anbieter dazu zu zwingen, den bereits betriebenen Dienst einzustellen und sich für einen anderen, gleichartigen Dienst akkreditieren zu lassen. Die Akkreditierung kann also auch im Nachhinein erfolgen, aber – und das ist der wesentliche Unterschied zwischen Akkreditierung und Anzeige – erst mit dem rechtskräftigen Abschluss des Akkreditierungsverfahrens kann sich der Anbieter als „akkreditierter Zertifizierungsdiensteanbieter" bezeichnen und das Bundeswappen führen[40].

40) Vgl. im Detail Punkt 4.1.1 des Akkreditierungsbescheides: Telekom-Control-Kommission A 3/2002 vom 11.03.2002, http://www.signatur.rtr.at/de/repository/supervision.html.

Insgesamt gab es vier Anträge auf Akkreditierung. Der erste Antrag wurde bereits im Sommer des Jahres 2000 eingebracht. Da weder eine Bescheinigung für die Chipkarten noch eine (vor der ersten Novelle des SigG noch notwendige) Bescheinigung für die Signaturerstellungseinheit des Zertifizierungsdiensteanbieters vorlag, wurde dem Zertifizierungsdiensteanbieter die Verbesserung dieser Mängel aufgetragen. Auf seinen Antrag hin wurde die gewährte Frist zur Mängelverbesserung auch erstreckt, als aber nach knapp drei Monaten noch immer keine Bescheinigungen vorlagen, wurde ein neuerlicher Antrag auf Fristerstreckung abgewiesen und der Antrag auf Akkreditierung zurückgewiesen[41].

Hinsichtlich des Antrages eines anderen Zertifizierungsdiensteanbieters vom 23.05.2001 war das Ermittlungsverfahren relativ weit fortgeschritten. Die RTR-GmbH hatte gemeinsam mit A-SIT bereits einen Augenschein im grundsätzlich schon funktionsfähigen Trust-Center vorgenommen, A-SIT hatte das Gutachten noch nicht abgeschlossen, aber einen ausführlichen Zwischenbericht an die TKK gelegt. Da noch einige Mängel vorlagen, waren die Voraussetzungen für eine Akkreditierung aber auch ein halbes Jahr nach Antragstellung noch nicht erfüllt. Aufgrund der aufgetretenen Verzögerungen beschloss der Zertifizierungsdiensteanbieter im Dezember 2001, den Antrag auf Akkreditierung zurückzuziehen; die TKK stellte das Verfahren daraufhin ein.

Zwei Anträge auf Akkreditierung waren erfolgreich. Dem Akkreditierungsantrag der Datakom Austria vom 26.06.2001 wurde am 17.12.2001 stattgegeben, dem Antrag der A-Trust vom 29.01.2002 am 11.03.2002. Die kurze Verfahrensdauer des Akkreditierungsverfahrens der A-Trust ist darauf zurückzuführen, dass aufgrund einer Anzeige der A-Trust bereits Ende November 2001 Ermittlungen aufgenommen worden waren. Insgesamt ist für ein Akkreditierungsverfahren ein Zeitraum von etwa zwei bis sechs Monaten zu veranschlagen, wobei die Zeit vor allem davon abhängt, wie schnell der Antragsteller offene Fragen beantwortet bzw. auftauchende Probleme behebt.

Bei den Akkreditierungsverfahren wurden jeweils ein Augenschein vor Ort vorgenommen und A-SIT mit der Erstellung eines Gutachtens zur technischen Sicherheit beauftragt. Beim Antrag von A-Trust wurden dabei sogar mehrere Unternehmen besichtigt, da die sicherheitsrelevanten Funktionen verteilt sind: Die Personalisierung der Chipkarten erfolgt beim Lieferanten derselben, das Trust-Center ist in einem Rechenzentrum untergebracht. Die RTR-GmbH

41) Telekom-Control-Kommission A 4/2000 vom 09.10.2000.

erstellt in den Verfahren jeweils einen Bericht an die TKK, in dem die Erfüllung der Voraussetzungen des SigG und der SigV geprüft wird. Erhebt ein Zertifizierungsdiensteanbieter über die österreichischen Rechtsvorschriften hinaus den Anspruch, bestimmte Anforderungen zu erfüllen, dann werden auch diese geprüft. In diesem Zusammenhang ist vor allem darauf hinzuweisen, dass A-Trust für sich in Anspruch nimmt, die Anforderungen nach ETSI TS 101 456 zu erfüllen (vgl. Abschnitt 4.1.5.2.3). Daher wurde von der RTR-GmbH auch nach diesem Standard geprüft.

Die wichtigsten Rechtsfragen zur Auslegung des SigG und der SigV, welche die TKK in den Akkreditierungsverfahren zu lösen hatte, waren die Folgenden[42]:

- Prüfungsmaßstab für eine Akkreditierung sind in erster Linie das SigG und die SigV, technische Normen kommen nur eingeschränkt zur Anwendung. Nimmt ein Zertifizierungsdiensteanbieter aber für sich in Anspruch, bestimmte Standards (z.B. ETSI TS 101 456, vgl. Abschnitt 4.1.5.2.3) zu erfüllen, dann ist auch nach diesen Standards zu prüfen[43].
- Bescheinigungen einer Bestätigungsstelle sind für die Signaturerstellungseinheiten des Zertifizierungsdiensteanbieters seit der ersten Novelle des SigG nicht mehr erforderlich, stattdessen hat die TKK sich in ihren Entscheidungen diesbezüglich auf das Gutachten der Bestätigungsstelle gestützt[44].
- Für die technischen Komponenten der Signatoren sind Bescheinigungen einer Bestätigungsstelle erforderlich. Welche Komponenten genau einer Bescheinigung bedürfen, ergibt sich aus den Sicherheitsanforderungen des SigG und der SigV. In den derzeit üblichen Konfigurationen sind dabei neben der Chipkarte, welche die meisten Sicherheitsanforderungen abdecken kann, auch die Anforderungen von § 7 Abs. 1 bis 3 SigV an die Hashberechnung, die sichere Anzeige und die PIN-Eingabe relevant. Daher bedürfen insbesondere auch die Secure Viewer (vgl. Abschnitt 3.2.3) einer Bescheinigung und aus den jeweiligen Einsatzbedingungen in den Bescheinigungen ist zu entnehmen, ob für die PIN-Eingabe ein sicherheitsgeprüfter Chipkartenleser mit eigener PIN-Tastatur erforderlich ist (oder ob die Sicherheitsanforderungen an die PIN-Eingabe vom Secure Viewer abgedeckt werden können)[45].

42) Die Akkreditierungsbescheide sind in gekürzter Form auf der Website der Aufsichtsstelle veröffentlicht: http://www.signatur.rtr.at/de/repository/supervision.html.
43) Vgl. Punkt 4.1.2.4 der Akkreditierungsbescheide.
44) Vgl. die Punkte 4.1.2.5 und 4.1.5.10 der Akkreditierungsbescheide.
45) Vgl. Punkt 4.1.3.1 der Akkreditierungsbescheide.

- Werden einzelne Anforderungen des SigG oder der SigV nicht erfüllt, dann kann die Aufsichtsstelle den Antrag auf Akkreditierung nicht alleine deshalb abweisen, sondern muss den Grundsatz der Verhältnismäßigkeit nach § 14 Abs. 6 SigG anwenden und prüfen, ob die erforderliche Sicherheit auch durch entsprechende Auflagen im Akkreditierungsbescheid gewährleistet werden kann[46].
- Ein Anwendungsfall dieser aus dem Verhältnismäßigkeitsgrundsatz abgeleiteten Regel betraf die Secure Viewer. Der Aufsichtsstelle war das Problem bekannt, dass es keine Viewer gab, für welche bereits eine Bescheinigung vorlag, und dass es zeitaufwändig ist, Software bescheinigen zu lassen. Es wäre unverhältnismäßig gewesen, die Akkreditierung nur deshalb zu verweigern, weil für die Secure Viewer noch keine Bescheinigung vorgelegt werden konnte. Daher wurden trotz der fehlenden Bescheinigungen Akkreditierungen ausgesprochen, in den Akkreditierungsbescheiden wurde aber die Auflage erteilt, dass jeweils nachgewiesen werden muss, dass eine Evaluierung und Bescheinigung in Auftrag gegeben wurde und dass die Bescheinigung spätestens innerhalb von 12 Monaten, nachdem ein Secure Viewer erstmals eingesetzt wird, der Aufsichtsstelle vorgelegt werden muss[47].
- Hinsichtlich der Haftpflichtversicherung verlangt § 2 Abs. 2 SigV, dass die Mindestversicherungssumme EUR 1 Mio. „je Versicherungsfall" beträgt. Da sich in allen Akkreditierungsverfahren herausgestellt hat, dass keine Versicherung bereit ist, eine Versicherung anzubieten, die beliebig viele Versicherungsfälle pro Jahr abdecken würde, hat die Aufsichtsstelle auch hier eine Auflage vorgeschrieben. Als ausreichend wurde angesehen, dass die Haftpflichtversicherung auf drei Versicherungsfälle[48] pro Jahr beschränkt wird, allerdings wurde eine zusätzliche Anzeigepflicht als Auflage vorgeschrieben, wenn Versicherungsfälle eintreten[49].

Zu den in den Akkreditierungsverfahren geprüften Unterlagen und Beweismitteln gehörten beispielsweise die folgenden Dokumente: das von der TKK in Auftrag gegebene Gutachten der Bestätigungsstelle A-SIT, die Certificate Policy und das Certification Practice Statement des Zertifizierungsdiensteanbieters, darüber hinausgehende Teile des Sicherheitskonzepts des

46) Vgl. Punkt 4.1.4 der Akkreditierungsbescheide.
47) Vgl. Punkt 4.1.3.2 der Akkreditierungsbescheide.
48) Im Versicherungsrecht ist zwischen Versicherungsfall und Schadensfall zu unterscheiden. Werden durch ein Ereignis mehrere Personen geschädigt, dann handelt es sich um einen Versicherungsfall, aber mehrere Schadensfälle. Die Haftpflichtversicherung muss also zumindest drei voneinander unabhängige Ereignisse abdecken.
49) Vgl. die Punkte 4.1.5.7 und 4.2.2.6 (A 7/2001) bzw. 4.2.2.5 (A 3/2002) der Akkreditierungsbescheide.

Anbieters (z. B. Risiko- und Bedrohungsanalyse, interne Betriebsanweisungen), die Belehrung des Signators, die Liste der empfohlenen technischen Komponenten, eine exakte technische Spezifikation der Zertifikate und der Widerrufsliste, der Firmenbuchauszug, die Versicherungspolizze der Haftpflichtversicherung, der Businessplan, Verträge mit den Registrierungsstellen sowie Handbücher für deren Personal, Protokolle zu den durchgeführten Augenscheinen sowie Bescheinigungen zu den eingesetzten und empfohlenen Signaturprodukten. In beiden erfolgreich abgeschlossenen Akkreditierungsverfahren umfasste der Schriftverkehr jeweils mehr als hundert Aktenstücke mit insgesamt etwa 3.000 Seiten.

2.1.5 Regelmäßige Überprüfung von Zertifizierungsdiensteanbietern

Gemäß § 18 Abs. 4 SigV hat die Aufsichtsstelle Zertifizierungsdiensteanbieter zumindest in regelmäßigen Abständen von zwei Jahren sowie bei sicherheitsrelevanten Veränderungen des Sicherheits- und Zertifizierungskonzepts zu überprüfen. Darüber hinaus ist die Aufsichtsstelle berechtigt, stichprobenartige Überprüfungen vorzunehmen.

Die TKK hat die ersten Verfahren zur regelmäßigen Überprüfung im Jänner 2002, zwei Jahre nach dem In-Kraft-Treten des SigG eingeleitet. Überprüft wurden dabei die Zertifizierungsdiensteanbieter Generali und Arge Daten. Mit der regelmäßigen Überprüfung der Datakom Austria – die ihren Dienst ebenfalls bereits vor dem In-Kraft-Treten des SigG aufgenommen hatte – wurde etwas zugewartet, da die Datakom Austria ohnehin erst kurz zuvor im Zuge des Akkreditierungsverfahrens gründlich überprüft worden war. Einige Wochen, nachdem die Datakom Austria begonnen hatte, qualifizierte Zertifikate auszustellen, wurden im März 2002 eine stichprobenartige Überprüfung des neu aufgenommen Zertifizierungsdienstes und eine regelmäßige Überprüfung der anderen Zertifizierungsdienste kombiniert. Auch die A-Trust wurde kurz nach dem Beginn der Ausstellung qualifizierter Zertifikate stichprobenartig überprüft (Juni 2002). Im Jänner 2003 wurde eine regelmäßige Überprüfung des Zertifizierungsdiensteanbieters IAIK vorgenommen, im Juni 2003 eine regelmäßige Überprüfung der A-Trust.

In all diesen Fällen wurde die RTR-GmbH von der TKK jeweils auch mit der Vornahme eines Augenscheins vor Ort beauftragt. Während bei der Aufnahme eines Zertifizierungsdienstes jeweils nur bei Anbietern qualifizierter Zertifikate ein Augenschein vor Ort vorgenommen wurde (Dienste für nicht qualifizierte Zertifikate wurden ausschließlich anhand der vorgelegten Unterlagen geprüft), hat es die Aufsichtsstelle für zweckmäßig erachtet, den

laufenden Betrieb vor Ort zu prüfen. Dies erwies sich auch als sinnvoll, da vor Ort einige kleinere Missstände festgestellt werden konnten, die bei der bloßen Überprüfung anhand schriftlicher Unterlagen wahrscheinlich nicht festgestellt werden hätten können. Einen Anlass für die Auferlegung von Aufsichtsmaßnahmen mittels Bescheid oder gar für die Untersagung des Dienstes hat die Aufsichtsstelle in keinem Fall gefunden, da die festgestellten Missstände jeweils geringfügig waren und von den Zertifizierungsdiensteanbietern rasch behoben wurden.

Im Zuge der vorgenommenen Überprüfungen wurde jeweils auch stichprobenartig in die Dokumentation Einsicht genommen. Zu diesem Zweck wurden vor der Überprüfung einige Zertifikate aus dem Verzeichnis bzw. aus der Widerrufsliste herausgesucht und der Zertifizierungsdiensteanbieter wurde vor Ort aufgefordert, die Dokumentation zur Ausstellung und zum Widerruf des Zertifikates vorzuweisen.

Mehrfach wurde dabei festgestellt, dass Test-Zertifikate in einer Weise ausgestellt wurden, die nicht dem Sicherheits- und Zertifizierungskonzept entsprochen hatten. Die betroffenen Zertifizierungsdiensteanbieter wurden dazu angehalten, Test-Zertifikate entweder in einer separaten Test-Umgebung auszustellen, die eindeutig als solche gekennzeichnet ist, oder sich an das Sicherheits- und Zertifizierungskonzept zu halten – also keine Fantasienamen zu verwenden (sondern den Namen des Mitarbeiters, für den das Zertifikat tatsächlich ausgestellt wurde) und auch die Dokumentation (z. B. Ausweiskopien, Erfassung der vollständigen Adresse, ...) in dem im Konzept vorgesehenen Umfang vorzunehmen.

Im Zuge einer Überprüfung wurde festgestellt, dass in der Praxis ein anderes Sicherheits- und Zertifizierungskonzept verwendet wurde als der Aufsichtsstelle angezeigt worden war. Das neue Konzept umfasste eine zusätzliche Klasse von Zertifikaten. Nach den Angaben des Zertifizierungsdiensteanbieters sei eine Anzeige der Änderungen einige Monate zuvor an die Aufsichtsstelle abgefertigt worden, allerdings nicht eingeschrieben und mit einer falschen Postleitzahl. Bei der Aufsichtsstelle ist diese Anzeige nicht eingelangt. Jedenfalls wurde im Überprüfungsverfahren eine nochmalige Änderung von Details des Sicherheits- und Zertifizierungskonzepts und eine neuerliche Anzeige an die Aufsichtsstelle vorgenommen.

Bei einer anderen Überprüfung wurde festgestellt, dass bei der Ausstellung von Server-Zertifikaten nicht entsprechend dem Sicherheits- und Zertifizierungskonzept vorgegangen wurde. Dabei wurden Server-Zertifikate für eine

andere juristische Person ausgestellt als für jene, die als Inhaber der entsprechenden Internet-Domain eingetragen war. Weiters wurden einigen natürlichen Personen Zertifikate ausgestellt, ohne dass in der Dokumentation ein Nachweis vorlag, dass die Organisation, die ebenfalls im Zertifikat eingetragen wurde, von der Ausstellung des Zertifikates dem Sicherheits- und Zertifizierungskonzept entsprechend unterrichtet worden war. Da die Zertifikate bereits abgelaufen waren, waren keine Aufsichtsmaßnahmen erforderlich. Der Zertifizierungsdiensteanbieter wurde aber aufgefordert, in Hinkunft die Einhaltung des Sicherheits- und Zertifizierungskonzepts zu beachten.

2.1.6 Sonstige Verfahren der Telekom-Control-Kommission (TKK)

In vierteljährlichen Abständen schreibt die TKK jenen Zertifizierungsdiensteanbietern, die qualifizierte Zertifikate ausstellen, eine Gebühr von EUR 2 pro qualifiziertem Zertifikat und Jahr vor. Die Gebühr wird anhand von monatlichen Meldungen über die Anzahl der gültigen Zertifikate berechnet.

Bei der Einführung dieser Gebühr wurde erwartet, dass sie langfristig die Kosten der Aufsichtsstelle abdeckt. Da erst etwa 10.000 qualifizierte Zertifikate im Umlauf sind, kann die Gebühr aber nur einen kleinen Teil der jährlichen Kosten der Aufsichtsstelle decken.

Seit die Aufsichtsstelle im September 2002 ihre Public-Key-Infrastruktur in Betrieb genommen hat (vgl. Abschnitt 2.2), wird den in das sichere Verzeichnis der Aufsichtsstelle aufgenommenen Zertifizierungsdiensteanbietern (das sind alle Anbieter) außerdem eine Gebühr von EUR 500 pro Jahr vorgeschrieben.

Sonstige Gebühren werden jeweils im Anlassfall vorgeschrieben, z. B. die Gebühr für die Anzeige der Aufnahme der Tätigkeit (EUR 100, wenn es sich um einfache Zertifikate handelt, EUR 6.000 für qualifizierte Zertifikate) oder die Gebühr für eine Akkreditierung (ebenfalls EUR 6.000).

Aufgrund einer Mitteilung der Bestätigungsstelle A-SIT wurde im März 2003 ein aufsichtsbehördliches Verfahren eingeleitet, um eine bestimmte Sicherheitsfrage im Zusammenhang mit dem Registrierungsverfahren des Zertifizierungsdiensteanbieters A-Trust zu überprüfen. Im Verfahren wurde aber kein Anlass für Aufsichtsmaßnahmen festgestellt, das Verfahren wurde eingestellt.

2.2 Verzeichnis der Zertifizierungsdienste

2.2.1 Motivation

Ob man einer elektronischen Signatur vertrauen kann, hängt auch vom Vertrauen in das Zertifikat des Signators ab. Die Beziehung zwischen Signatur und Zertifikat kann automatisch überprüft werden. Doch Zertifikate können nicht nur von seriösen Anbietern, sondern von jedermann mit frei erhältlichen Werkzeugen wie z. B. OpenSSL[50] auf einfache Weise hergestellt werden. Man könnte mit solchen Werkzeugen sogar die Zertifizierungshierarchie eines seriösen Anbieters nachbilden – mit dem einzigen Unterschied, dass dabei andere Schlüssel verwendet werden. Zur Verhinderung derartigen Missbrauchs wurde im SigG dafür vorgesorgt, dass jedermann überprüfen kann, ob die verwendeten Schlüssel tatsächlich einem Zertifizierungsdiensteanbieter gehören.

2.2.2 Rechtsgrundlagen

Nach § 13 Abs. 3 SigG hat die Aufsichtsstelle dafür Sorge zu tragen, dass ein elektronisch jederzeit allgemein zugängliches Verzeichnis geführt wird, das Folgendes enthält:

- die gültigen, die (vorübergehend) gesperrten und die (endgültig) widerrufenen Zertifikate für Zertifizierungsdiensteanbieter,
- die im Inland niedergelassenen Zertifizierungsdiensteanbieter,
- die von der Aufsichtsstelle akkreditierten Zertifizierungsdiensteanbieter,
- Drittstaaten-Zertifizierungsdiensteanbieter, für deren Zertifikate ein im Inland niedergelassener Zertifizierungsdiensteanbieter einsteht,
- im Ausland niedergelassene Zertifizierungsdiensteanbieter (auf Antrag).

In das Verzeichnis sind die qualifizierten Zertifikate für die Erbringung von Zertifizierungsdiensten einzutragen. Da nicht alle Anbieter qualifizierte Zertifikate ausstellen, können die in das Verzeichnis eingetragenen Zertifikate auch von der Aufsichtsstelle ausgestellt werden. Die Verzeichnisse müssen mit der sicheren elektronischen Signatur der Aufsichtsstelle versehen sein. Die Verzeichnisse werden gemäß § 15 Abs. 2 Z 3 SigG von der RTR-GmbH geführt.

50) Vgl. http://www.openssl.org/

Vorgaben für die technische Umsetzung finden sich in § 3 Abs. 1 SigV: Die Signaturerstellungsdaten der Aufsichtsstelle werden auf einem Hauptsystem und auf einem unter Verschluss gehaltenen Zweitsystem (als Backup) erzeugt. Da sich diese Signaturerstellungsdaten voneinander unterscheiden, müssen die elektronischen Signaturen der Aufsichtsstelle sowohl im Hauptsystem als auch im Zweitsystem erstellt werden. Die Signaturprüfdaten des Zweitsystems dürfen nur bei Ausfall des Hauptsystems verwendet werden, damit der ungestörte Betrieb der Signatur- und Zertifizierungsdienste der Aufsichtsstelle sichergestellt ist. In den Anhängen zur SigV ist festgelegt, dass bei der Aufsichtsstelle SHA-1 als Hashverfahren und RSA zur Verschlüsselung des Hashwerts zu verwenden ist. Die Schlüssellänge beim RSA-Verfahren muss mindestens 1.023 Bit betragen.

2.2.3 Umsetzung als Public-Key-Infrastruktur (PKI)

Die rechtliche Vorgabe, dass die Aufsichtsstelle qualifizierte Zertifikate für Zertifizierungsdiensteanbieter ausstellen kann, legt die Einrichtung einer Public-Key-Infrastruktur durch die Aufsichtsstelle nahe. Damit kann die Aufsichtsstelle qualifizierte Zertifikate für alle Schlüssel ausstellen, mit denen in Österreich niedergelassene Anbieter Zertifikate signieren.

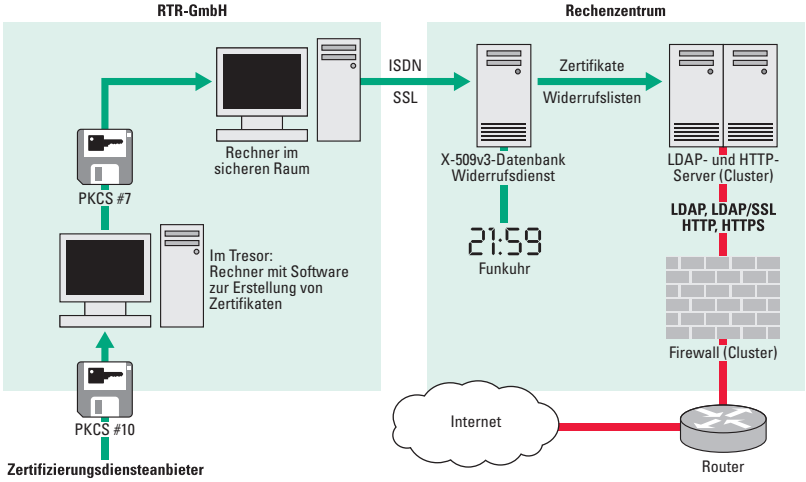
Diese Lösung besticht vor allem dadurch, dass beim Anwender zur Überprüfung beliebiger Zertifikate, die von österreichischen Anbietern ausgestellt sind, in der Regel keine zusätzliche Software installiert werden muss. Neuere Versionen von Microsoft Windows verfügen von vornherein über Komponenten zur Zertifikatsverwaltung, die insbesondere durch Internet Explorer, Outlook Express und Outlook genutzt werden. Unabhängig vom Betriebssystem verfügen auch die meisten Webbrowser (z. B. Mozilla) über ähnliche Komponenten.

In Windows 2000 (bei Installation des Windows-Updates vom 23.07.2003) und in Windows XP werden die von der Aufsichtsstelle ausgestellten Zertifikate automatisch erkannt. Bei anderen Betriebssystemen bzw. in Webbrowsern (ausgenommen Internet Explorer) muss das selbstsignierte Zertifikat der Aufsichtsstelle (das Zertifikat mit der Bezeichnung „Telekom-Control-Kommission Top 1“) vor der erstmaligen Verwendung heruntergeladen (http://www.signatur.rtr.at/currenttop.cer) und im Zertifikatspeicher abgelegt werden. Wie man dabei vorgeht, ist in der Browserdokumentation beschrieben.

2.2.4 Technische Infrastruktur

Abb. 8 bietet einen Überblick über die bei der Aufsichtsstelle eingesetzten technischen Komponenten und zeigt den Ablauf bei der Ausstellung eines Zertifikats durch die Aufsichtsstelle.

Abb. 8: Infrastruktur der Aufsichtsstelle



Quelle: RTR-GmbH

Der Zertifizierungsdiensteanbieter übergibt der Aufsichtsstelle einen Datenträger (Diskette oder CD-ROM) mit einem Zertifizierungsantrag im Format PKCS #10 (eine Datei, die u. a. den Namen und den öffentlichen Schlüssel des Zertifizierungsdienstes enthält und die mit dem zugehörigen privaten Schlüssel signiert ist, vgl. Abschnitt 4.1.2.3). Indem die Signatur auf dem Zertifizierungsantrag mit dem darin enthaltenen öffentlichen Schlüssel geprüft wird, kann nachgewiesen werden, dass der Zertifizierungsdiensteanbieter über den privaten Schlüssel verfügt.

Aufgrund der im Zertifizierungsantrag enthaltenen Daten wird auf einem speziell geschützten Rechner das Zertifikat erstellt. Dieser Rechner wird stets offline betrieben und ist in einem Tresor untergebracht, der nur von zwei Mitarbeitern der RTR-GmbH gemeinsam geöffnet werden kann. Der Tresor befindet sich seinerseits in einem sicheren Raum, den ebenfalls nur zwei Mitarbeiter gemeinsam betreten können. Auch beim Signieren des Zertifikats, das durch eine kryptografische Hardware-Komponente erfolgt, ist ein Vier-Augen-Prinzip technisch verwirklicht.

Aufgrund wachsender Bedenken gegen zu kurze Schlüssel werden Zertifikate der Aufsichtsstelle mit einem RSA-Schlüssel der Länge 2.048 Bit signiert. Solche Schlüssel werden nach Expertenmeinung noch ca. 20 Jahre genügend Sicherheit bieten, sofern keine revolutionären Forschungsergebnisse das RSA-Verfahren grundsätzlich in Frage stellen.

Zertifikate der Aufsichtsstelle werden unabhängig von der Technologie des Zertifizierungsdienstes immer im Format ITU-T X.509 v3 ausgestellt und in eine Datenstruktur nach PKCS #7 (vgl. Abschnitt 4.1.2.2) eingebettet. Falls der Zertifizierungsdienst eine andere Technologie verwendet, deren Einbindung in X.509 nicht genormt ist, so legt die Aufsichtsstelle einen ASN.1 Object Identifier (vgl. Abschnitt 4.1.1.1) fest, mit dem die Technologie der im Zertifikat enthaltenen Signaturprüfdaten beschrieben wird. Da beispielsweise ein österreichischer Anbieter Zertifikate auf Basis von PGP ausstellt, wurde für PGP der Object Identifier 1.2.40.0.21.0.4.0 festgelegt.

Die Erstellung des Zertifikats wird elektronisch dokumentiert. Das Zertifikat und die Dokumentation werden mittels Diskette auf einen zweiten Rechner übertragen, der sich ebenfalls im sicheren Raum befindet, und von dort aus über eine ISDN-Verbindung verschlüsselt zu einem Rechenzentrum übertragen. Dort werden das Zertifikat, ergänzende Angaben über den Zertifizierungsdiensteanbieter (Kontaktinformation usw.) sowie die Dokumentation in eine Datenbank eingetragen.

Ein aus zwei Rechnern bestehender Cluster stellt die Verbindung zum Internet her: Auf diesen Rechnern werden HTTP- und LDAP-Dienste betrieben, optional kann der Zugriff auch mit Server-Authentifizierung (SSL bzw. TLS) erfolgen. Sollte es einem Angreifer trotz bestmöglicher Schutzmaßnahmen gelingen, die Inhalte dieser Server zu manipulieren, würde sich dies trotzdem kaum auf den Inhalt der Verzeichnisse auswirken: Verzeichniszugriffe über HTTP werden mit Protokollbruch an den weniger exponierten Datenbankrechner weitergeleitet und von diesem beantwortet. Manipulationen in der lokalen Datenbank des LDAP-Servers können jederzeit durch Replikation korrigiert werden. Der Server-Cluster ist im Normalfall so konfiguriert, dass einer der Rechner HTTP-Zugriffe und der andere Rechner LDAP-Zugriffe bearbeitet. Fällt einer der beiden Rechner aus, so werden dessen Aufgaben durch den anderen Rechner übernommen.

Geschützt werden die Server durch zwei Firewall-Rechner, die einen High-Availability-Cluster bilden: Im Normalfall wirkt nur ein Rechner als Firewall, bei Ausfall wird automatisch der zweite Rechner aktiviert.

2.2.5 Zertifizierungshierarchie

Eine Übersicht über die Zertifizierungshierarchie der Aufsichtsstelle ist in Abb. 9 dargestellt.

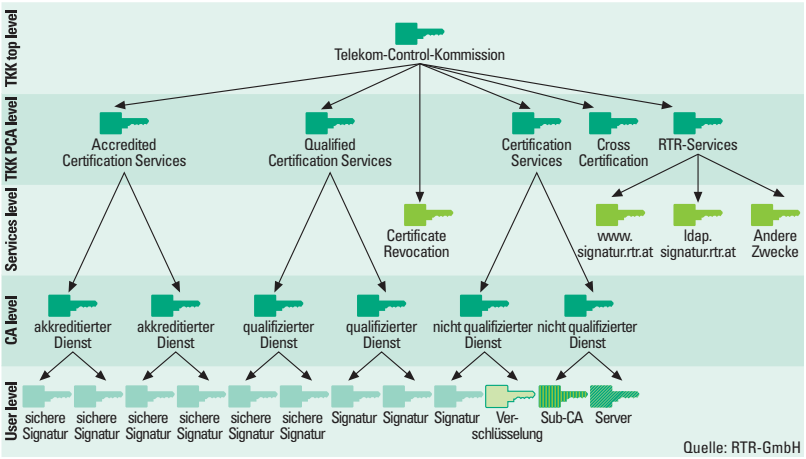
Auf der obersten Ebene („TKK top level") befinden sich ausschließlich der TOP-Schlüssel der Aufsichtsstelle, seine Vorgänger und Nachfolger.

Auf der zweiten Ebene („TKK PCA level") befinden sich die Policy Certification Authorities der Aufsichtsstelle. Die an Zertifizierungsdiensteanbieter für deren Zertifizierungsdienste ausgestellten Zertifikate werden mit unterschiedlichen Schlüsseln signiert. Mit dem ACCREDITED-CERTIFICATION-SERVICES-Schlüssel werden Zertifikate für Zertifizierungsdienste signiert, auf welche sich eine Akkreditierung bezieht. Mit dem QUALIFIED-CERTIFICATION-SERVICES-Schlüssel werden Zertifikate für andere Zertifizierungsdienste, bei denen qualifizierte Zertifikate ausgegeben werden, signiert. Der CERTIFICATION-SERVICES-Schlüssel signiert Zertifikate für andere (nicht qualifizierte) Dienste. Der RTR-SERVICES-Schlüssel signiert Zertifikate für Services der RTR-GmbH im Zusammenhang mit dem Betrieb der Public-Key-Infrastruktur der Aufsichtsstelle (insbesondere signiert er Zertifikate für den HTTPS- und den LDAP/SSL-Server). Ein weiterer Schlüssel ist für die Cross-Zertifizierung vorgesehen.

Auf der dritten Ebene („Services Level") sind die Schlüssel der Aufsichtsstelle dargestellt, die nicht für das Signieren von Zertifikaten vorgesehen sind. Für diese Schlüssel sind teilweise geringere Sicherheitsmaßnahmen vorgesehen (im Gegensatz zu den Schlüsseln der ersten beiden Ebenen werden sie z. B. nicht ausschließlich offline eingesetzt.) Vorgesehen ist der CERTIFICATE-REVOCATION-Schlüssel, mit dem Widerrufslisten signiert werden, ein Schlüssel für den HTTPS- und einer für den LDAP/SSL-Zugang zum Verzeichnisdienst der Aufsichtsstelle sowie weitere ausschließlich intern verwendete Schlüssel. (Die zu den ausschließlich intern zur Verwaltung der Verzeichnis-, Widerrufs- und WWW-Dienste und zur Erstellung von Zeitstempeln in der Dokumentation vorgesehenen Zertifikate werden nur veröffentlicht, wenn sie für die Öffentlichkeit von Belang sind).

Auf der Ebene „CA level" sind die Schlüssel der verschiedenen Diensteanbieter dargestellt, auf der Ebene „User level" die Schlüssel der Signatoren und anderer Nutzer.

Abb. 9: Zertifizierungshierarchie der Aufsichtsstelle



2.2.6 Certification Practice Statement

Da auch die Aufsichtsstelle gewissermaßen Zertifizierungsdienste erbringt, indem sie Zertifikate für Zertifizierungsdienste ausstellt, wendet sie die rechtlichen Bestimmungen für Zertifizierungsdienste, soweit dies möglich ist, auch auf sich selbst an. In diesem Sinne hat die Aufsichtsstelle ein umfangreiches Sicherheits- und Zertifizierungskonzept erstellt, dessen wichtigster Teil das veröffentlichte Certification Practice Statement (CPS) ist. Die derzeit aktuelle Version 1.1 des CPS ist unter http://www.signatur.rtr.at/de/repository/tkk-cps-11-20030714.html verfügbar.

Das CPS orientiert sich in Gliederung und Inhalt an den Vorgaben von RFC 2527. Es beschreibt

- allgemeine Richtlinien (Pflichten, Haftung, Veröffentlichung, interne Prüfungen usw.),
- Identifizierung und Authentifizierung (Erstregistrierung, Zertifikatserneuerung, Antrag auf Widerruf usw.),
- Anforderungen an den Betrieb (Antrag auf Ausstellung eines Zertifikats, Ausgabe von Zertifikaten, Überprüfung von Zertifikaten, Widerruf von Zertifikaten, Protokolle, Archivierung, Austausch von Schlüsseln, Katastrophenfälle usw.),

- physikalische, organisatorische und personelle Sicherheitsmaßnahmen,
- technische Sicherheitsmaßnahmen (Schlüsselerzeugung, Schlüsselverwaltung, Aktivierungsdaten, IT-Sicherheit etc.),
- Profil der Zertifikate und Widerrufslisten,
- Administration des Sicherheits- und Zertifizierungskonzepts,
- Glossar.

Neben der veröffentlichten Fassung existiert auch eine erweiterte Fassung des CPS. Diese enthält Erläuterungen, die spezifische Kenntnisse über die Infrastruktur voraussetzen oder die zur Wahrung des Sicherheitsniveaus nicht veröffentlicht werden (z. B. Firewall-Regeln). Unveröffentlicht sind auch ergänzende Dokumente (z. B. zur detaillierten Beschreibung des Rollenmodells).

2.2.7 Zugriff auf das Verzeichnis

Der Zugriff auf das Verzeichnis erfolgt über

- HTTP: http://www.signatur.rtr.at/ShowSearchCertificatesServlet?locale=de
- HTTPS: https://www.signatur.rtr.at/ShowSearchCertificatesServlet?locale=de
- LDAP: Server ldap.signatur.rtr.at, Port 389, Suchbasis c=AT
- LDAP-SSL: Server ldap.signatur.rtr.at, Port 636, Suchbasis c=AT

Der Zugriff auf die aktuelle Widerrufsliste erfolgt (ohne Authentifizierung des Servers) über http://www.signatur.rtr.at/current.crl oder (mit Authentifizierung des Servers) über https://www.signatur.rtr.at/current.crl.

Das im Web verfügbare Suchformular ermöglicht eine Einschränkung der Suchergebnisse nach verschiedenen Kriterien („Distinguished Name", Zertifizierungsstelle, Gültigkeitszeitraum, Seriennummer, Widerrufszeitpunkt und Status). Zertifikate können sowohl binär als auch Base64-codiert in den Formaten X.509 und PKCS #7 abgerufen werden. Unix-Anwendern kommt zugute, dass auch ein Download mit dem Netscape-eigenen MIME-Typ möglich ist.

2.3 Weitere Aktivitäten der RTR-GmbH

Neben der Unterstützung der TKK bei den Verfahren nach dem SigG hat die RTR-GmbH auch eine Reihe von weiteren Aktivitäten im Vorfeld und Umfeld der gesetzlichen Aufgaben wahrzunehmen. Tabelle 1 zeigt einen summarischen Überblick über diese Aktivitäten (soweit sie aktenmäßig erfasst wurden), danach folgt eine Beschreibung der besonders hervorzuhebenden Tätigkeiten. Erfasst wurde die Anzahl der einzelnen Aktenstücke (z. B. eingehende und ausgehende Briefe und E-Mails, Aktenvermerke über Telefonate und Besprechungen, Berichte an die TKK etc.).

Tabelle 1: Überblick über die Aktivitäten der RTR-GmbH

Anzahl der Aktenstücke	**2000**	**2001**	**2002**	**2003** bis 31.10.
Aktenführung für die TKK	81	339	296	204
Tätigkeiten im Vorfeld von Verfahren vor der TKK, z. B. Beantwortung von Anfragen der Anbieter, Teilnahme an Besprechungen, Aufforderung zur Anzeige von Änderungen am Sicherheits- und Zertifizierungskonzept, ...	25	61	32	35
Korrespondenz mit der Bestätigungsstelle, Abstimmung in technischen Fragen, insbesondere im Zusammenhang mit der Errichtung der Public-Key-Infrastruktur	30	133	125	18
Korrespondenz im Zusammenhang mit der Errichtung der Public-Key-Infrastruktur, insbesondere mit Lieferanten	86	162	119	42
Korrespondenz im Zusammenhang mit der Finanzierung der Aufsichtsstelle	19	11	1	10
Internationale Korrespondenz, z. B. mit der Europäischen Kommission und anderen Aufsichtsstellen, nicht erfasst ist die Korrespondenz über die Mailingliste von FESA	12	16	21	40
Stellungnahmen in Begutachtungsverfahren zu Gesetzen und Verordnungen, Teilnahme an Besprechungen mit Ministerien etc.	12	5	8	19
Allgemeine Anfragen, Presseanfragen und Sonstiges	54	86	92	43
Summe	**319**	**813**	**694**	**411**

Hervorzuheben sind dabei insbesondere die folgenden Aktivitäten:

Gleich nach In-Kraft-Treten des SigG hat die Aufsichtsstelle eine Konsultation vorgenommen, um den damaligen Stand der Technik (§ 18 Abs. 5 SigG) zu erkunden und festzustellen, wie die Anforderungen des SigG und der SigV umgesetzt werden können. Hauptthemen der Konsultation waren Dokumentenformate (wie kann sicher gestellt werden, dass das signierte Dokument sich nicht dynamisch verändert und dass es auf verschiedenen Rechnern immer in gleicher Weise dargestellt wird), Speicherung des privaten Schlüssels (z. B. mittels Chipkarte), Kontrolle des Signators über den Signaturvorgang (insbesondere Sicherheitsfragen des Betriebssystems), Verwendung von Schlüsseln für andere Zwecke (Verschlüsselung, Authentifizierung, etc.) und die sichere Signaturprüfung.

In unregelmäßigen Abständen veröffentlicht die Aufsichtsstelle den per E-Mail versandten „Newsletter der Aufsichtsstelle für elektronische Signaturen". Zwischen September 1999 und August 2003 wurden 26 Exemplare des Newsletters versandt, zuletzt an 644 subskribierte Personen.

Das Bundesministerium für Justiz (BMJ), welches das SigG und die SigV legistisch betreut, hat bei den vorgenommenen Novellen des SigG und bei der geplanten Novelle der SigV die Aufsichtsstelle jeweils eingebunden. Insbesondere wurde die bevorstehende Novelle der SigV in einer Reihe von Besprechungen vorbereitet, zu denen das BMJ jeweils Vertreter der RTR-GmbH und von A-SIT eingeladen hatte, um auch die Erfahrungen aus der Vollziehung der Verordnung zu berücksichtigen. Zum E-Government-Gesetz, welches legistisch vom Bundeskanzleramt betreut wird, hat die RTR-GmbH eine umfangreiche Stellungnahme[51] im Begutachtungsverfahren abgegeben.

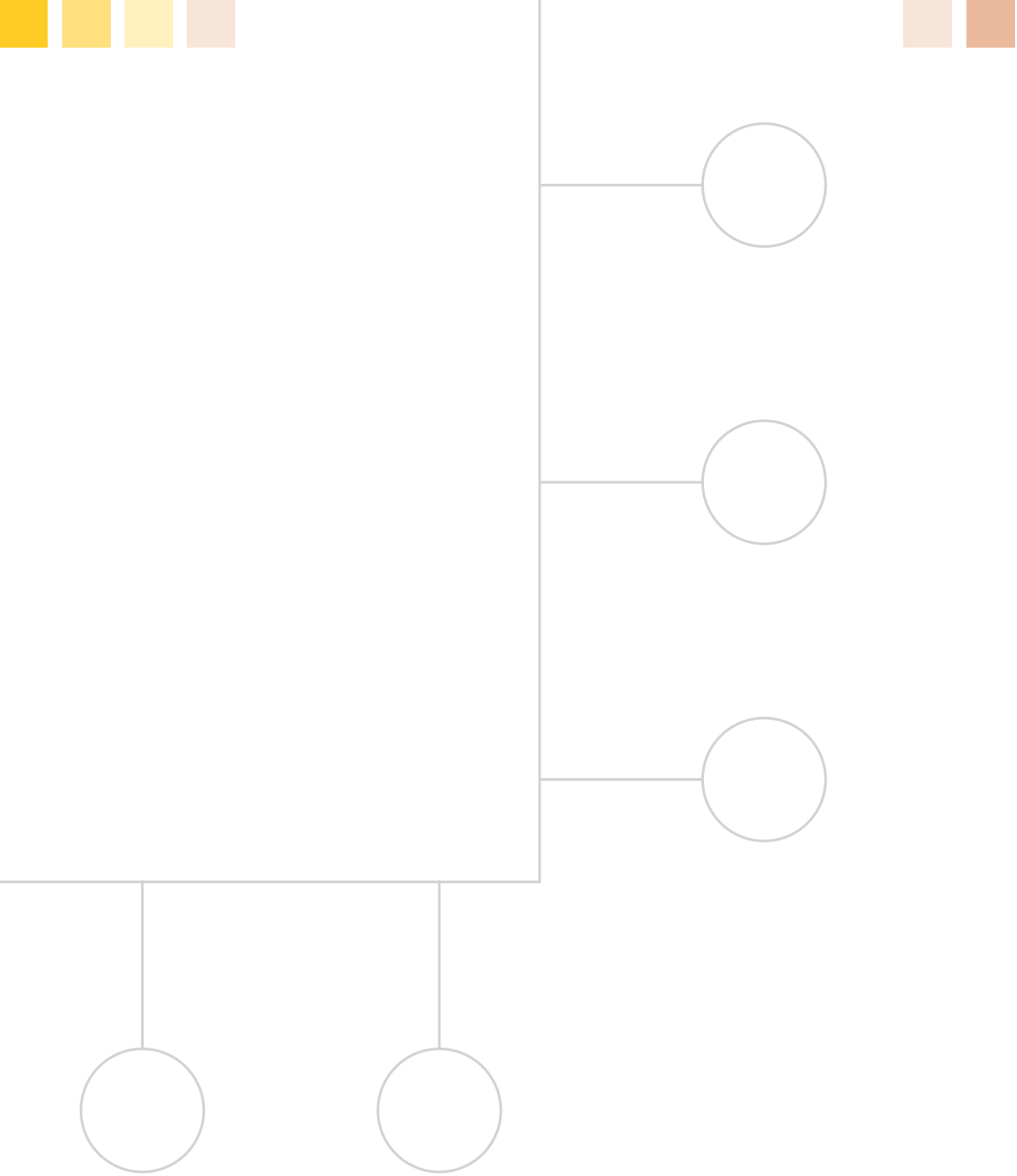
Nach den gesetzlichen Vorgaben des SigG werden die Aufgaben der TKK bzw. der RTR-GmbH nach dem SigG von den Aufgaben nach anderen Gesetzen kostenrechnerisch getrennt. Die RTR-GmbH erfasst ihre Kosten derzeit getrennt nach den Aufgabenbereichen Telekommunikation (dieser Aufwand wird von den Anbietern von Kommunikationsnetzen und -diensten in Form von durch die Regulierungsbehörde vorgeschriebenen Finanzierungsbeiträgen getragen), Rundfunk (Finanzierungsbeiträge für diesen Aufwand haben die Rundfunkveranstalter zu begleichen) und Signatur. Ab dem

51) Vgl. http://www.signatur.rtr.at/de/repository/rtr-egovg-20030825.html

01.01.2004 werden auch die Aufwände für die neu zu verwaltenden Fonds (Digitalisierungsfonds und Fernsehfilmförderungsfonds) getrennt erfasst und aus den Finanzmitteln dieser Fonds beglichen.

Für die Aufwände nach dem SigG sah das Gesetz ursprünglich nur vor, dass die Aufsichtsstelle „kostendeckende Gebühren" vorzuschreiben habe. Bei den Beratungen über die SigV, welche diese Gebühren näher regeln sollte, wurde aber klar, dass der erst im Entstehen befindliche Markt erstickt würde, wenn er alle Aufwände der Aufsichtsstelle sofort zu tragen hätte. Im Unterschied zur etablierten Branche der Telekommunikation gab es im Signaturbereich eben noch keine Anbieter, die mit ihren Diensten bereits entsprechende Erträge erwirtschaften konnten. Daher wurden in der SigV nur Gebühren für die einzelnen aufsichtsbehördlichen Handlungen vorgesehen, für die Deckung des laufenden Aufwandes – insbesondere für die Errichtung und den Betrieb der Public-Key-Infrastruktur der Aufsichtsstelle – wurde im SigG „für die ersten drei Jahre der operativen Tätigkeit" (§ 13 Abs. 4 SigG) eine Kapitalerhöhung der Telekom-Control GmbH um insgesamt ATS 29 Mio. (EUR 2,11 Mio.) vorgesehen. Nach Ablauf der ersten drei Jahre sollten diese Aufwände aus einer Gebühr von EUR 2 pro qualifiziertem Zertifikat und Jahr gedeckt werden. Die Kapitalerhöhung erfolgte erst im Dezember 2000 – fast ein Jahr nach dem In-Kraft-Treten des Gesetzes, weshalb die Ausschreibung für die Public-Key-Infrastruktur der Aufsichtsstelle erst im April 2001 vorgenommen werden konnte und die Public-Key-Infrastruktur erst im September 2002 in Betrieb ging.

Da sich der Markt beträchtlich langsamer entwickelt hat als erwartet und somit auch weniger aufsichtsbehördliche Tätigkeiten notwendig waren, reichten die Mittel aus der gewährten Kapitalerhöhung länger als geplant. Die Aufsichtsstelle konnte die Aufwände der ersten vier Jahre ihrer Tätigkeit damit bedecken. Die Einnahmen aus der Gebühr von EUR 2 pro qualifiziertem Zertifikat und Jahr blieben aber vernachlässigbar. Bislang hat die Anzahl der qualifizierten Zertifikate die Schwelle von 10.000 Zertifikaten noch nicht überstiegen, für eine dauerhafte Finanzierung der aufsichtsbehördlichen Tätigkeit aus Gebühren wären etwa 200.000 bis 250.000 qualifizierte Zertifikate erforderlich. Im Jahr 2004 wird auf politischer Ebene eine dauerhafte Lösung gefunden werden müssen, welche die Finanzierung der Aufgaben der Aufsichtsstelle sicherstellen kann.



Der Markt

3.1 Zertifizierungsdiensteanbieter

Bereits vor dem In-Kraft-Treten des SigG haben drei Anbieter ihre Tätigkeit aufgenommen – der Verein Arge Daten, die Datakom Austria und die Generali. Ein viertes Unternehmen, Innovation Systems, vertrieb in Österreich Zertifikate des belgischen Zertifizierungsdiensteanbieters Globalsign. Die einzelnen Anbieter hatten aber jeweils nur ein bis zwei Zertifizierungsdienste mit eher niedrigem Sicherheitsniveau im Angebot. Zwar gab es teilweise schon Dienste, bei denen eine Identitätsüberprüfung mit einem Lichtbildausweis Voraussetzung für die Ausstellung des Zertifikates war. Ein im Hinblick auf das spätere Angebot von qualifizierten Zertifikaten ausgerüstetes und betriebenes Trust-Center mit einem entsprechend detaillierten Sicherheits- und Zertifizierungskonzept hatte aber zu diesem Zeitpunkt nur die Datakom Austria.

Das Angebot hat sich in den vergangenen vier Jahren verbreitert und ist teilweise schon schwer überschaubar geworden, da die Markennamen oft wenig über die sicherheitsrelevanten Eigenschaften der Dienste aussagen. Im Wesentlichen kann man die wichtigsten Gruppen der angebotenen Dienste wie folgt zusammenfassen:

Qualifizierte Zertifikate für die sichere elektronische Signatur: Diese Zertifikate werden ausschließlich nach Identitätsprüfung anhand eines amtlichen Lichtbildausweises und ausschließlich für Schlüssel, die auf einer sicheren Signaturerstellungseinheit gespeichert sind, ausgegeben. Es gibt derzeit einen Zertifizierungsdienst, bei dem qualifizierte Zertifikate kommerziell ausgegeben werden – a.sign Premium von der A-Trust. Zwei weitere Zertifizierungsdienste der A-Trust sollen auslaufen und durch a.sign Premium ersetzt werden – a.sign Uni (qualifizierte Zertifikate für die Wirtschaftsuniversität Wien, die von der A-Trust im ehemaligen Trust-Center der Datakom Austria ausgestellt werden) und trust|sign (technisch weitgehend identisch mit a.sign Premium, der Zertifizierungsdienst soll aufgrund der Änderung der Marke eingestellt werden). Zwischen Februar und September 2002 hat die Datakom Austria den Zertifizierungsdienst a-sign Premium betrieben. Dieser Dienst wurde Ende September 2002 eingestellt, die A-Trust hat die Marke a.sign übernommen (vgl. dazu die Abschnitte 3.1.2 und 3.1.3).

Einfache Zertifikate für Schlüssel, die auf Chipkarten gespeichert sind: A-Trust erstellt auf den a.sign Premium-Chipkarten jeweils zwei Schlüsselpaare und gibt zwei Zertifikate aus: a.sign Premium als qualifiziertes Zertifikat für die sichere elektronische Signatur und a.sign Premium encryption als einfaches Zertifikat für die einfache elektronische Signatur, für die Authentifizierung und für die Verschlüsselung. Ein weiteres Produkt, bei dem Chipkarten ausgegeben werden, ist a.sign token. Auch hier werden zwei Schlüsselpaare erzeugt und zwei Zertifikate ausgegeben, die allerdings beide keine qualifizierten Zertifikate sind: Der Zertifizierungsdienst a.sign token stellt Zertifikate für die Signatur aus, der Zertifizierungsdienst a.sign token encryption Zertifikate für die Authentifizierung und die Verschlüsselung. Auch die Datakom Austria hatte einen Zertifizierungsdienst, der einfache Zertifikate für Schlüssel auf Chipkarten ausgestellt hat. Der Zertifizierungsdienst a-sign Strong existierte in zwei Varianten, bei a-sign Strong+ wurden Chipkarten ausgegeben. Bei den Serverzertifikaten stellt A-Trust die Zertifikate a.sign corporate medium und a.sign corporate strong für Schlüssel aus, die auf eigens dafür bestimmter Hardware gespeichert werden. Allen hier beschriebenen Zertifizierungsdiensten ist gemeinsam, dass die Identität anhand eines amtlichen Lichtbildausweises geprüft wird.

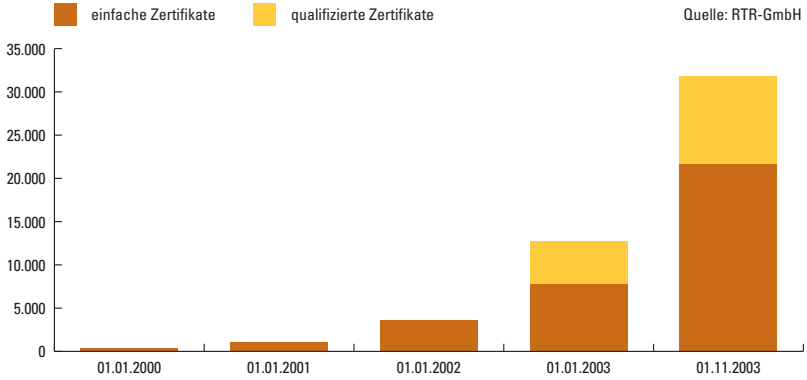
Weitere einfache Zertifikate mit Identitätsprüfung anhand eines amtlichen Lichtbildausweises werden bei folgenden Zertifizierungsdiensten ausgestellt: Bei dem von der Arge Daten angebotenen Zertifizierungsdienst A-CERT (an die Stelle einer von der Arge Daten selbst durchgeführten Überprüfung der Identität kann dabei auch eine notarielle oder gerichtliche Beglaubigung des Antrages treten), bei dem von der Generali angebotenen Zertifizierungsdienst net.surance security (ausgenommen ist die Zertifikatsklasse Light, dabei wird nur die E-Mail-Adresse geprüft) und bei den beiden vom IAIK angebotenen Zertifizierungsdiensten (ein Dienst für Signaturzertifikate, einer für Serverzertifikate; beim IAIK kann die Vorlage eines Ausweises entfallen, wenn der Zertifikatswerber persönlich bekannt ist).

Weitere einfache Zertifikate, bei denen nicht notwendigerweise eine Identitätsprüfung anhand eines amtlichen Lichtbildausweises vorgenommen wird: Zu dieser Gruppe zählen insbesondere einige Dienste, bei denen bloß die E-Mail-Adresse geprüft wird, z. B. a.sign light von der A-Trust und die Zertifikatsklasse Light des Zertifizierungsdienstes net.surance security der Generali.

In den folgenden Abschnitten werden in alphabetischer Reihenfolge die einzelnen Zertifizierungsdiensteanbieter dargestellt, die ihren Sitz in Österreich haben oder die auf ihren Antrag hin in das Verzeichnis der Aufsichtsstelle aufgenommen wurden. Dabei sind auch jene Zertifizierungsdienste angeführt, die in den vier oben genannten Gruppen nicht aufgezählt wurden.

Im Zuge der Erstellung dieses Berichtes hat die RTR-GmbH die Zertifizierungsdiensteanbieter um Angaben zur Anzahl der von ihnen ausgestellten Zertifikate ersucht. Die meisten Anbieter sind diesem Ersuchen nachgekommen, die Zertifikate der anderen Anbieter wurden geschätzt. Daten zur Anzahl der qualifizierten Zertifikate sind der Aufsichtsstelle gemäß § 1 Abs. 2 SigV monatlich zu melden. Abb. 10 zeigt die Gesamtanzahl der zu den jeweiligen Stichtagen gültigen einfachen bzw. qualifizierten Zertifikate summiert über alle Anbieter. Bemerkenswert ist, dass sich die Gesamtanzahl pro Jahr etwa verdreifacht.

Abb. 10: Anzahl der in Österreich ausgestellten Zertifikate



3.1.1 Arge Daten – Österreichische Gesellschaft für Datenschutz

Der Verein Arge Daten beschäftigt sich vor allem mit Fragen des Datenschutzes und der Privatsphäre. Im Jahr 1996 wurde vom Verein ein Zertifizierungsdienst für die damals für Signatur und Verschlüsselung am

weitesten verbreitete Software „Pretty Good Privacy“ (PGP) aufgenommen. Der zunächst unter dem Namen AD-CERT angebotene, im August 2000 in A-CERT umbenannte Zertifizierungsdienst setzt für die Ausstellung eines Zertifikates eine Identitätsprüfung anhand eines amtlichen Lichtbildausweises voraus. Diese kann durch eine notarielle oder gerichtliche Beglaubigung ersetzt werden, wobei der Zertifikatswerber ein Formular mit seinem öffentlichen Schlüssel unterschreibt und die eigenhändige Unterschrift des Zertifikatswerbers von einem Notar oder Gericht beglaubigt wird. Im Juni 2001 nahm die Arge Daten einen weiteren Zertifizierungsdienst auf, der Serverzertifikate ausstellt: A-CERT/GLOBALTRUST. Bei beiden Zertifizierungsdiensten handelt es sich um einfache Zertifikate, die Zertifikatsinhaber können ihren privaten Schlüssel auf einem lesbaren Datenträger (z. B. der Festplatte) speichern.

3.1.2 A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH

Der Zertifizierungsdiensteanbieter A-Trust wurde von einer Reihe österreichischer Banken gegründet. Zunächst wurde das Projekt im Rahmen der STUZZA[52] ausgearbeitet, später in die APSS[53] übernommen. Schließlich wurde das Unternehmen A-Trust gegründet. Eigentümer von A-Trust sind neben zahlreichen Banken auch die Wirtschaftskammer Österreich, der Rechtsanwaltskammertag, die Notartreuhandbank und die Telekom Austria.

Von Anfang an zielte A-Trust darauf ab, qualifizierte Zertifikate für die sichere elektronische Signatur auf den Markt zu bringen und dafür auch eine staatliche Akkreditierung anzustreben. Von allen Zertifizierungsdiensteanbietern hat A-Trust die komplexeste technische Infrastruktur installiert, insbesondere hat A-Trust als einziger Anbieter zwei räumlich voneinander getrennte Trust-Center und eine komplexe Logistik der Ausgabe von Chipkarten, die auf die Besonderheiten der österreichischen Bankenlandschaft abgestimmt ist. A-Trust hat über 40 Registrierungsstellen in Betrieb, im Lauf des Jahres 2004 will A-Trust dieses Netz auf über 300 Registrierungsstellen ausweiten.

52) Studiengesellschaft für Zusammenarbeit im Zahlungsverkehr GmbH, ein 1991 von verschiedenen österreichischen Banken gegründetes Unternehmen, das sich mit der Normierung des Zahlungsverkehrs befasst, vgl. http://www.stuzza.at/.

53) Austrian Payment System Services GmbH, wurde 1993 im Zuge des Zusammenschlusses der Geldausgabeautomaten-Service Gesellschaft GABE und der Europay Austria gegründet und betreibt insbesondere die österreichischen Bankomaten, vgl. http://www.apss.at/.

Im Sommer 2002 hat die Telekom Austria beschlossen, einige Tochterunternehmen – unter anderem die Datakom Austria – in die Muttergesellschaft zu verschmelzen. Da die Telekom Austria an zwei Zertifizierungsdiensteanbietern beteiligt war – an der Datakom Austria zu 100 % und an der A-Trust zu 12 % – wurde dabei beschlossen, die Zertifizierungsdienste zu fusionieren. Es wurden daher zunächst die Zertifizierungsdienste der Datakom Austria in die A-Trust eingebracht (dadurch stieg der Anteil der Telekom Austria an der A-Trust von 12 % auf 19,9 %), anschließend wurde mit Stichtag vom 01.10.2002 die Datakom Austria in die Telekom Austria verschmolzen (vgl. dazu im Detail Abschnitt 3.1.3).

A-Trust bietet bei weitem die meisten Zertifizierungsdienste an. Zum Teil ist dies allerdings dadurch bedingt, dass bei der Übernahme der Zertifizierungsdienste der Datakom Austria auch deren Marke „a-sign" (leicht verändert zu „a.sign") übernommen wurde. Ursprünglich hatte die A-Trust die Marken „trust|mark" (für nicht qualifizierte Zertifikate) und „trust|sign" (für qualifizierte Zertifikate) verwendet. Da man einen in Betrieb befindlichen Zertifizierungsdienst nicht ohne weiteres umbenennen kann (die Bezeichnung des Dienstes ist in den ausgestellten Zertifikaten und auch in den Zertifikaten des Dienstes selbst enthalten), wurde dabei so vorgegangen, dass man die alten Zertifizierungsdienste auslaufen ließ (dabei werden keine neuen Zertifikate mehr ausgestellt, die Verzeichnis- und Widerrufsdienste für die bereits ausgegebenen Zertifikate werden aber weiterhin betrieben) und stattdessen neue Zertifizierungsdienste aufnahm.

Den ersten Zertifizierungsdienst, „trust|mark|vsc" hat A-Trust im Mai 2001 aufgenommen. Dabei handelte es sich um Zertifikate für Schlüssel, die vom Benutzer auf einem lesbaren Datenträger, z. B. der Festplatte, gespeichert werden (die Abkürzung „vsc" aus dem Namen des Zertifizierungsdienstes steht für „virtual smartcard"). Im Vergleich zu den anderen Zertifizierungsdiensteanbietern, die vergleichbare Produkte teilweise bereits seit mehreren Jahren angeboten hatten, hat A-Trust diesen Zertifizierungsdienst relativ spät aufgenommen, die Geschäftsstrategie von A-Trust war allerdings von Anfang an auf qualifizierte Zertifikate ausgerichtet. Daher wurde der erste Zertifizierungsdienst erst aufgenommen, als die Arbeiten für die Bereitstellung qualifizierter Zertifikate bereits weit fortgeschritten waren.

Im Oktober 2001 hat A-Trust unter dem Namen „trust|mark|token“ einen Zertifizierungsdienst aufgenommen, der Zertifikate für Chipkarten (allerdings noch nicht als sichere Signaturerstellungseinheit bescheinigte Chipkarten) ausstellte.

Kurz darauf, am 19.11.2001, zeigte A-Trust der Aufsichtsstelle an, am 15.12.2001 den Zertifizierungsdienst „trust|sign“ aufzunehmen und dabei qualifizierte Zertifikate auszugeben. Da noch Bescheinigungen für die einzusetzenden Secure Viewer fehlten, wurde vorerst noch nicht der Anspruch gestellt, dass diese Zertifikate für die sichere elektronische Signatur bestimmt seien. Diese Änderung erfolgte erst einige Wochen später im Februar 2002. Ab dem 25.02.2002 gab A-Trust im Rahmen des Zertifizierungsdienstes „trust|sign“ qualifizierte Zertifikate für die sichere elektronische Signatur aus. Am 11.03.2002 wurde A-Trust hinsichtlich dieses Zertifizierungsdienstes auch akkreditiert.

Im August 2002 ergänzte A-Trust sein Produktportfolio um Serverzertifikate und nahm den Zertifizierungsdienst „trust|mark|server“ auf.

Nach der Übernahme der Infrastruktur der Datakom Austria wurde eine Reihe neuer Zertifizierungsdienste aufgenommen. Zunächst wurden am 30.09.2002 zwei Zertifizierungsdienste der A-Trust in Betrieb genommen, die im Trust-Center der ehemaligen Datakom Austria laufen. Diese Zertifizierungsdienste dienten dazu, Kunden der Datakom Austria, die aus technischen Gründen nicht sofort mit Zertifikaten aus dem Trust-Center der A-Trust versorgt werden konnten, weiterhin mit Zertifikaten auszustatten. Zu diesem Zweck wurde insbesondere der Zertifizierungsdienst a.sign Uni aufgenommen, mit dem die Studenten und Studentinnen der Wirtschaftsuniversität Wien qualifizierte Zertifikate erhielten. Der neue Zertifizierungsdienst a.sign projects belieferte ehemalige Kunden der Datakom Austria mit einfachen Zertifikaten – beispielsweise Sachverständige zur gesicherten Kommunikation mit den Gerichten im Rahmen des elektronischen Rechtsverkehrs.

In weiterer Folge wurde eine Reihe von Zertifizierungsdiensten mit der von der Datakom Austria übernommenen Marke „a.sign“ aufgenommen, die die alten Zertifizierungsdienste „trust|sign“ und „trust|mark“ ersetzen sollten.

Insgesamt hat A-Trust bis zum 31.10.2002 die folgenden Zertifizierungsdienste aufgenommen:

Qualifizierte Zertifikate

- a.sign Premium: Qualifizierte Zertifikate für die sichere elektronische Signatur, die ausgegebenen Chipkarten sind auch mit Bürgerkartenfunktionalität (siehe Abschnitt 3.2.5) ausgestattet.
- trust|sign: Diese Zertifikate entsprechen technisch weitgehend den Zertifikaten des Dienstes a.sign Premium, aufgrund der Änderung der Marke läuft dieser Zertifizierungsdienst aus.
- a.sign Uni: Diese Zertifikate wurden im ehemaligen Trust-Center der Datakom Austria erstellt, der Zertifizierungsdienst wurde Ende November 2003 eingestellt.

Einfache Zertifikate

- a.sign Premium encryption: Dabei handelt es sich um Zertifikate, die in Kombination mit dem qualifizierten Zertifikat a.sign Premium ausgegeben werden. Auf jeder dabei ausgegebenen Chipkarte werden zwei Schlüsselpaare erzeugt und es werden zwei Zertifikate ausgestellt. Das a.sign Premium-Zertifikat ist ein qualifiziertes Zertifikat und dient der sicheren elektronischen Signatur. Das a.sign Premium-encryption-Zertifikat ist ein einfaches Zertifikat und dient der Authentifizierung, der einfachen Signatur und der Verschlüsselung.
- a.sign corporate light/a.sign corporate medium/a.sign corporate strong: Bei diesen drei Zertifizierungsdiensten werden Serverzertifikate ausgestellt, die Dienste unterscheiden sich danach, wie sicher der private Schlüssel des Kunden auf dessen Server verwaltet wird: Bei a.sign corporate light kann der Schlüssel auf einem lesbaren Datenträger (z. B. der Festplatte) gespeichert werden, bei den beiden anderen Diensten muss er auf einer eigenen Hardware gespeichert sein, die bei a.sign corporate strong außerdem noch auf Sicherheit evaluiert und zertifiziert sein muss.
- a.sign developer: Diese Zertifikate dienen zur Signatur von Software.
- a.sign light: Dabei handelt es sich um Zertifikate, die ohne Identitätsprüfung ausgestellt werden. Es wird dabei nur die Korrektheit der E-Mail-Adresse geprüft sowie ein Rückruf an der vom Zertifikatswerber angegeben Telefonnummer durchgeführt.
- a.sign Projects: Dieser Zertifizierungsdienst wird im ehemaligen Trust-Center der Datakom Austria erbracht und ist der Nachfolgedienst zu deren Zertifizierungsdiensten a-sign Light und a-sign Strong. Der Zertifizierungsdienst a.sign Projects soll eingestellt werden.

- a.sign token und a.sign token encryption: Bei diesen beiden Zertifizierungsdiensten werden Zertifikate für Chipkarten ausgegeben. Das eine Zertifikat dient der Signatur, das andere der Authentifizierung und Verschlüsselung. Es handelt sich bei beiden Diensten nicht um qualifizierte Zertifikate.

Eine Reihe weiterer Zertifizierungsdienste soll aufgrund der Markenänderung eingestellt werden bzw. wurde schon eingestellt: trust|mark|server (eingestellt am 21.11.2002, Nachfolgeprodukt: a.sign corporate light), trust|mark|vsc (Nachfolgeprodukt: a.sign light), trust|mark|token und TrustMarkToken-Enc (Nachfolgeprodukte: a.sign token und a.sign token encryption) und trust|sign Enc (Nachfolgeprodukt: a.sign Premium encryption).

3.1.3 Datakom Austria GmbH (seit 01.10.2002: Telekom Austria AG)

Die Datakom Austria hat erstmals im Frühjahr 1998 einen Zertifizierungsdienst vorgestellt. Nach dem damaligen Konzept wurde zwischen drei unterschiedlich sicheren Klassen von Zertifikaten unterschieden: a-sign Light, a-sign Medium und a-sign Strong. Bei a-sign Light wird gar keine Identitätsprüfung vorgenommen, das Zertifikat wird vollautomatisch nach einer Überprüfung der E-Mail-Adresse des Zertifikatswerbers ausgestellt. Bei a-sign Medium wird die Identität anhand eines an den Zertifizierungsdiensteanbieter gefaxten Lichtbildausweises geprüft.

Der Zertifizierungsdienst a-sign Strong wurde erst im Mai 2001 aufgenommen, dabei wird die Identität anhand eines amtlichen Lichtbildausweises geprüft. Der Dienst wurde in zwei Varianten angeboten: a-sign Strong stellte Zertifikate für Schlüssel aus, die auf einem lesbaren Datenträger gespeichert wurden, a-sign Strong+ stellte Zertifikate für Chipkarten aus (die allerdings nicht als sichere Signaturerstellungseinheiten bescheinigt waren).

Im Februar 2002 wurde schließlich der Zertifizierungsdienst a-sign Premium aufgenommen. Dabei handelte es sich um qualifizierte Zertifikate für die sichere elektronische Signatur, im Dezember 2001 war die Datakom Austria im Hinblick auf diesen Zertifizierungsdienst akkreditiert worden.

Die Datakom Austria war eine 100 %-Tochter der Telekom Austria. Im Herbst 2002 leitete die Telekom Austria eine gesellschaftsrechtliche Umstrukturierung ein, mehrere Tochterfirmen wurden in die Telekom Austria integriert. Dabei wurde auch die Datakom Austria am 01.10.2002 in die Telekom Austria

verschmolzen. Zuvor jedoch wurden die von der Datakom Austria betriebenen Zertifizierungsdienste in die A-Trust eingebracht (siehe Abschnitt 3.1.2). Die Datakom Austria hat ihre Zertifizierungsdienste daher Ende September 2002 eingestellt und keine neuen Zertifikate mehr ausgegeben, ihre Rechtsnachfolgerin Telekom Austria hat nur mehr den Widerrufsdienst betrieben und regelmäßig Widerrufslisten ausgestellt (und sich dazu der A-Trust bedient).

3.1.4 Generali Office-Service und Consulting AG/Generali IT-Solutions GmbH

Die Generali hatte ihren Zertifizierungsdienst schon im April 1999, also noch vor dem In-Kraft-Treten des SigG, aufgenommen. Eine Besonderheit dieses unter dem Namen „net.surance security" angebotenen Dienstes ist, dass er mit einer Vermögensschaden-Haftpflichtversicherung und einer Rechtsschutzversicherung kombiniert wird.

In technischer Hinsicht bietet Generali nur einen Zertifizierungsdienst an, da alle Zertifikate von derselben Certification Authority ausgestellt, d. h. mit demselben Schlüssel signiert werden. Generali unterscheidet aber verschiedene Klassen von Zertifikaten: Light-Zertifikate werden kostenlos und ohne Identitätsprüfung angeboten. Dabei wird bloß die E-Mail-Adresse des Zertifikatswerbers geprüft. Bei Medium-Zertifikaten (diese dienen für die elektronische Signatur und die Verschlüsselung) und bei Server-Zertifikaten wird die Identität anhand eines amtlichen Lichtbildausweises geprüft.

Im März 2002 wurde das Sicherheits- und Zertifizierungskonzept erweitert, seither werden auch Business-Zertifikate ausgegeben (auch hier erfolgt eine Identitätsüberprüfung). Diese Zertifikate dienen insbesondere der Authentifizierung gegenüber einer Internet-Plattform, über welche Versicherungsmakler untereinander kommunizieren können.

Im Jahr 2003 fand im Generali-Konzern eine Umstrukturierung statt, die auch den erbrachten Zertifizierungsdienst betraf. Die (in eine GmbH – die Generali VIS Informatik GmbH – umgewandelte) Generali Office-Service und Consulting AG stellte ihren Zertifizierungsdienst ein, die Generali IT-Solutions GmbH nahm mit einem ähnlichen Sicherheits- und Zertifizierungskonzept einen Zertifizierungsdienst gleichen Namens („net.surance security") auf. Die von der Generali Office-Service und Consulting AG ausgestellten Zertifikate behalten ihre Gültigkeit, die Generali IT-Solutions GmbH wurde diesbezüglich mit der Weiterführung der Verzeichnis- und Widerrufsdienste betraut.

Der neue Zertifizierungsdienst der Generali IT-Solutions GmbH unterscheidet zwischen den Zertifikatsklassen Light-Zertifikate, Medium-Zertifikate, Server-Zertifikate und Together-Zertifikate. Letztere sind einem eingeschränkten Benutzerkreis für die Web-Anwendungen der TOGETHER Internet Services GmbH vorbehalten und entsprechen den vorher von Generali angebotenen Business-Zertifikaten.

3.1.5 Innovation Systems Informationstechnologie GmbH

Innovation Systems hat der Aufsichtsstelle einige Tage nach dem In-Kraft-Treten des SigG angezeigt, dass eine Tätigkeit als Zertifizierungsdiensteanbieter ausgeübt wird. Allerdings hat Innovation Systems keine eigenen Zertifikate ausgestellt, sondern Zertifikate vertrieben, die vom belgischen Anbieter GlobalSign NV/SA ausgestellt wurden und als Aussteller auch diesen belgischen Anbieter ausgewiesen haben.

Die Aufsichtsstelle hatte daher ihre Zuständigkeit zu prüfen. Nach Art. 4 der Signaturrichtlinie wendet jeder Mitgliedstaat die innerstaatlichen Bestimmungen, die er aufgrund der Signaturrichtlinie erlässt, auf die in seinem Hoheitsgebiet niedergelassenen Zertifizierungsdiensteanbieter und deren Dienste an. Die TKK entwickelte den Grundsatz, dass sie, wenn mehrere Unternehmen an der Ausstellung von Zertifikaten beteiligt sind, im Zweifel jenes Unternehmen als Zertifizierungsdiensteanbieter betrachtet, das in den Zertifikaten als Aussteller ausgewiesen wird.

Daher sah sich die TKK für den angezeigten Zertifizierungsdienst als nicht zuständig an und wies die Anzeige der Innovation Systems wegen Unzuständigkeit zurück.

3.1.6 Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK)

Das IAIK an der Technischen Universität Graz (TU Graz) beschäftigt sich schon seit vielen Jahren mit verschiedensten Fragen der Informationssicherheit. Beim IAIK ist der Grazer Standort der Bestätigungsstelle A-SIT (siehe Abschnitt 1.2.3.2) angesiedelt, der sich vor allem mit Fragen der Technologiebeobachtung beschäftigt (die TU Graz war auch Gründungsmitglied von A-SIT). Seit der Vorstand des Institutes, Prof. Reinhard Posch, im Jahr

2001 zum Leiter der Stabstelle IKT-Strategie des Bundes (Chief Information Officer) berufen wurde, besteht auch eine enge Zusammenarbeit zwischen dem IAIK und der Stabsstelle, insbesondere im Zusammenhang mit der Bürgerkarte (siehe Abschnitt 3.2.5).

Im Jänner 2001 hat das IAIK mehrere Zertifizierungsdienste aufgenommen, die Teil des EuroPKI-Projektes sind. Das IAIK bildet dabei den österreichischen Zweig dieser europaweiten Public-Key-Infrastruktur und betreibt je einen Zertifizierungsdienst für Signaturzertifikate, für Serverzertifikate und für Verschlüsselungszertifikate (da letztere ausschließlich der Verschlüsselung dienen, fallen sie nicht unter das SigG und damit nicht unter die Aufsicht). Die ausgestellten Zertifikate sind jeweils einfache Zertifikate, die privaten Schlüssel können vom Zertifikatsinhaber auf einem lesbaren Datenträger gespeichert werden. Die Identitätsprüfung erfolgt anhand eines amtlichen Lichtbildausweises, dessen Vorlage aber entfallen kann, wenn der Zertifikatswerber persönlich bekannt ist.

Die Zertifizierungsdienste werden vom IAIK nicht kommerziell betrieben, es wurde jeweils nur eine geringe Zahl von Zertifikaten ausgestellt, vor allem an Mitarbeiter und Mitarbeiterinnen des Institutes, von A-SIT und an einige im Bereich E-Government tätige Personen.

3.1.7 Mag. Ulrich Latzenhofer (CryptoConsult)

Mag. Ulrich Latzenhofer nahm als Einzelunternehmer unter der Bezeichnung „CryptoConsult“ im Juni 2000 zwei Zertifizierungsdienste („Basic Services“ und „Distinguished Services“) auf. Kurz darauf schrieb die Aufsichtsstelle die Stelle eines technischen Experten für die elektronische Signatur aus. Mag. Latzenhofer stellte im September 2000 seine Tätigkeit als Zertifizierungsdiensteanbieter ein und ist seither Angestellter der RTR-GmbH (bzw. bis März 2001 der Telekom-Control GmbH).

3.1.8 TeleTrusT Deutschland e. V.

Die TKK ist als Aufsichtsstelle zwar nur für Zertifizierungsdiensteanbieter zuständig, die ihren Sitz in Österreich haben, auf Antrag können sich aber auch ausländische Zertifizierungsdiensteanbieter in das Verzeichnis der Aufsichtsstelle aufnehmen lassen.

Der Verein TeleTrusT hat seinen Sitz in Erfurt (Deutschland) und beschäftigt sich mit verschiedenen Fragen der Sicherheit und des Vertrauensschutzes in der elektronischen Kommunikation. Insbesondere betreibt TeleTrusT seit Anfang 2001 die European Bridge-CA, einen Zertifizierungsdienst, der das Ziel hat, verschiedenste europäische Public-Key-Infrastrukturen untereinander zu vernetzen. Mitglieder der European Bridge-CA sind unter anderem die Deutsche Bank, die Deutsche Telekom, Siemens, SAP sowie einige Public-Key-Infrastrukturen deutscher Ministerien. Im Sommer 2003 trat auch die RTR-GmbH der European Bridge-CA bei; das TOP-Zertifikat der Aufsichtsstelle wurde daher auch in die European Bridge-CA aufgenommen.

Im Gegenzug stellte TeleTrusT einen Antrag, ihrerseits in das Verzeichnis der österreichischen Aufsichtsstelle aufgenommen zu werden. Diesem Antrag wurde am 20.10.2003 stattgegeben, der TeleTrusT wurde für die European Bridge-CA auch ein Zertifikat der österreichischen Aufsichtsstelle ausgestellt.

3.1.9 Web und Co – Webdesign, Multimedia und Consulting GmbH & Co KG

Das Grazer Softwarehaus Web und Co ist der jüngste der österreichischen Zertifizierungsdiensteanbieter, der Zertifizierungsdienst webundco security wurde der Aufsichtsstelle am 01.02.2003 angezeigt. Neben dem Zertifizierungsdienst bietet Web und Co eine Reihe von Sicherheitslösungen basierend auf biometrischen Technologien an.

Der Zertifizierungsdienst webundco security ist für Projekte gedacht, bei denen Mitarbeiter von Unternehmen oder Behörden mit Zertifikaten ausgestattet werden sollen. Die Ausstellung der Zertifikate erfolgt anhand einer Liste der Personen, für die ein Zertifikat ausgestellt werden soll, durch den Kunden. Bei den Zertifikaten handelt es sich um einfache Zertifikate, die Signaturerstellungsdaten des Zertifikatsinhabers können auf einem lesbaren Datenträger, z. B. der Festplatte, gespeichert werden. Nach Angaben von Web und Co können die Signaturerstellungsdaten auch auf eine von Web und Co ausgegebene und durch biometrische Daten des Signators abgesicherte Chipkarte geschrieben werden.

3.2 Anwendungen und Produkte

3.2.1 Signaturerstellungseinheiten

Für folgende Signaturerstellungseinheiten liegen Bescheinigungen der österreichischen Bestätigungsstelle A-SIT gemäß § 18 Abs. 5 SigG vor:

- Prozessorchipkarte mit Philips Smart Card Controller P8WE5032V0G und Betriebssystem STARCOS SPK 2.3: Bescheinigung gültig bis 30.06.2004. Die Chipkarte wurde im Rahmen des von Datakom Austria erbrachten, mittlerweile eingestellten Zertifizierungsdienstes a-sign Premium ausgegeben.
- Prozessorchipkarte mit Philips Smart Card Controller P8WE5032V0G, Betriebssystem STARCOS SPK 2.3 Version 6 und Digital Signature Application TrustSign Version 1.2: Bescheinigung gültig bis 30.06.2004. Diese Chipkarte wird im Rahmen der von A-Trust erbrachten Zertifizierungsdienste trust|sign und a.sign Premium ausgegeben.
- Prozessorchipkarte mit Philips Smart Card Controller P8WE5032V0G, Betriebssystem STARCOS SPK 2.3 Version 7.0 und Digital Signature Application StarCert Version 2.2: Bescheinigung gültig bis 23.05.2004. Diese Chipkarte wurde bei keinem in Österreich niedergelassenen Zertifizierungsdiensteanbieter eingesetzt.
- Prozessorchipkarte mit Infineon SLE 66CX320P, Betriebssystem CardOS/M4.01 Version C803 und Applikation für digitale Signatur 0.20: Bescheinigung gültig bis 13.05.2004. Diese Chipkarte wurde im Rahmen des von Datakom Austria erbrachten, mittlerweile eingestellten Zertifizierungsdienstes a-sign Premium ausgegeben und wurde bei Redaktionsschluss auch für den von A-Trust erbrachten Zertifizierungsdienst a.sign Uni eingesetzt.
- E4 KeyCard V3.0: Prozessor Infineon SLE 66CX320P, Betriebssystem TCOS Version 2.0 Release 3 (Bescheinigung am 01.06.2003 abgelaufen). Diese Chipkarte wurde bei keinem in Österreich niedergelassenen Zertifizierungsdiensteanbieter eingesetzt.

Unter den in Deutschland ausgestellten Bestätigungen wecken einige besonderes Interesse:

- MICARDO Elliptic Version 2.3 136/32 R1.0 Signaturkarte Version 1.0 der ORGA Kartensysteme GmbH: Diese Chipkarte verwendet zur Signaturerstellung eine elliptische Kurve über dem Körper GF(2191) nach dem Verfahren ECDSA (ANSI X9.62). Nach Kenntnis der RTR-GmbH handelt es sich um die erste von einer notifizierten Bestätigungsstelle für sicher befundene Signaturerstellungseinheit, die auf elliptischen Kurven beruht. Die Bestätigung wurde am 29.08.2002 ausgestellt.
- Mehrere Bestätigungen liegen für Signaturkarten auf Basis des Prozessors SLE66CX322P von Infineon vor. Obwohl in Bestätigungen bezüglich des RSA-Verfahrens nur eine Schlüssellänge von 1.024 Bit genannt wird, würde der Prozessor laut Evaluierungsbericht und IT-Sicherheitszertifikat BSI-DSZ-CC-0169-2002 des Bundesamts für Sicherheit in der Informationstechnik auch Schlüssellängen bis 2.048 Bit zulassen. Dies könnte angesichts der gegenwärtigen Diskussion über die Sicherheit von 1.024 Bit-Schlüsseln künftig bedeutsam sein (siehe auch Abschnitt 1.1.5).

3.2.2 Chipkarten-Lesegeräte

Fast alle in Österreich bescheinigten Chipkarten-Lesegeräte verfügen über eine eigene Tastatur zur PIN-Eingabe, damit diese nicht durch das Betriebssystem oder andere Programme verarbeitet werden kann. Funktionelle Unterschiede bestehen vor allem bezüglich der unterstützten Schnittstellen (seriell oder USB) sowie in der Ausgabe (Display oder LEDs).

Ein Hersteller bietet PC-Tastaturen mit eingebautem Chipkarten-Lesegerät an. Hierbei signalisiert eine LED den sicheren Modus während der PIN-Eingabe.

Dennoch ist die Interoperabilität zwischen Lesegerät und Signatur-Software sowie zwischen Lesegerät und Chipkarte nicht in jeder Kombination gewährleistet. Genauere Informationen sind in den von der Bestätigungsstelle A-SIT veröffentlichten Bescheinigungen (http://www.a-sit.at/) sowie in den Produktinformationen der Hersteller zu finden.

Folgende Chipkarten-Lesegeräte sind in Österreich bescheinigt:

- Kobil KAAN Professional, Hardware-Version KCT100, Firmware-Version 2.08 GK 1.04,
- Reiner cyberJack[54], Hardware- und Firmware-Version 3.0,
- Reiner cyberJack e-com, Hardware- und Firmware-Version 2.0,
- Reiner cyberJack pinpad, Hardware- und Firmware-Version 2.0,
- Siemens Sign@tor Terminal Version 1.0,
- Siemens Sign@tor Terminal Version 2.0.

Bestätigungen nach dem deutschen Signaturgesetz liegen für folgende Chipkarten-Lesegeräte[55] vor:

- Cherry PC-Tastaturen mit Chipkartenterminal G83-6700LPZxx/00, G83-6700LQZxx/00, G81-7015LQZxx/00, G81-8015LQZxx/00, G81-12000LTZxx/00, G81-12000LVZxx/00,
- Kobil Systems B1 Professional, Hardware-Version KCT100, Firmware-Version 2.08 GK 1.04,
- Kobil Systems KAAN Standard Plus, Firmware-Version 02121852, und SecOVID Reader Plus, Firmware-Version 02121812,
- ORGA HML 5010 oder 5020 oder 5021 oder 5022, Version 1.0,
- SCM Microsystems SPR 132, SPR 332, SPR 532, Firmware-Version 4.15,
- Utimaco Safeware CardMan, CardMan Compact, CardMan Keyboard, CardMan Mobile (abgelaufen am 15.09.2003).

3.2.3 Secure Viewer

Dieser Abschnitt enthält Kurzbeschreibungen von Signaturprodukten mit Secure Viewer (vgl. Abschnitt 1.2.1.2.3), für die Bescheinigungen der Bestätigungsstelle A-SIT vorliegen.

3.2.3.1 MBS-Sign

MBS-Sign wurde von BDC EDV Consulting GmbH für Anwendungen im Rahmen des Multibank-Standards entwickelt. Es handelt sich um einen Client zur Erstellung sicherer elektronischer Signaturen auf „elektronischen

54) Bei diesem Gerät wird die PIN zwar über die PC-Tastatur eingegeben, die Daten werden aber direkt von der Tastatur an das Chipkarten-Lesegerät übermittelt, das zwischen PC und Tastatur angeschlossen wird.

55) In dieser Liste sind jene Chipkarten-Lesegeräte nicht erfasst, für die neben einer deutschen Bestätigung auch eine österreichische Bescheinigung vorliegt.

Begleitzetteln". Das Produkt enthält eine API-Schnittstelle mit Funktionen zur Signaturerstellung, zum Ändern und Entsperren der PIN, zur Signaturprüfung und zur Zertifikatprüfung. Neben einer existierenden Linux-Version wird Plattformunabhängigkeit durch einen Java-Layer gewährleistet. Die zu signierenden Daten müssen als Text in einem eingeschränkten ASCII-Zeichensatz vorliegen. Der eingeschränkte Zeichensatz und zusätzliche Sicherheitsprüfungen schließen aus, dass unsichtbare Elemente signiert werden.

Das MBS Modul zur Erstellung sicherer Signaturen, Version 1.0, Release 2.2, wurde für diverse Versionen des Betriebssystems Windows am 12.04.2002 bescheinigt. Die Bescheinigung gilt bis 30.06.2004. Für die aktuelle Version 2.0, Release 1.2, liegt eine Bescheinigung vom 03.11.2003 vor, die ab Ausstellung zwei Jahre lang gültig bleibt.

3.2.3.2 hot:Sign

hot:Sign wurde von BDC EDV Consulting GmbH entwickelt. Es handelt sich um einen Client mit integriertem Secure Viewer zur Erstellung sowohl einfacher als auch sicherer elektronischer Signaturen. Als Transportprotokoll wird HTTP, als Applikationsprotokoll XML eingesetzt. Die von A-Trust ausgegebenen Signaturkarten a.sign Premium, trust|sign und trust|mark|token werden unterstützt. Die Software ermöglicht die sichere Anzeige von XHTML, XML und Text. Signaturen können in den Formaten XMLDSIG (vgl. Abschnitt 4.1.3.4) und CMS (vgl. Abschnitt 4.1.2.2) erzeugt und verifiziert werden. Weiters ermöglicht das Produkt auch die Bearbeitung von PIN und PUK. Für die Unterstützung von Funktionen des Security Layers 1.1 (siehe Abschnitt 3.2.5) wurde das E-Government-Gütesiegel an den Hersteller verliehen.

Auf den HTTP-Responder kann zugegriffen werden:

- mit Hilfe eines Browser-Plugins
  (Internet Explorer ab Version 6.0, Netscape Navigator ab Version 4.5),
- durch Loopback-Verbindung (direct HTTP) unabhängig vom
  jeweiligen Browser und
- durch Aufruf aus anderen Anwendungen.

Für die Version 1.0 liegt eine Bescheinigung vom 20.06.2002 vor, die bis zum 30.06.2004 gültig ist. Für die Version 1.2 SR3 liegt eine Bescheinigung vom 04.08.2003 vor, die zwei Jahre lang gültig ist.

3.2.3.3 trustview

trustview ist der von IT Solution GmbH entwickelte Secure Viewer, der im Softwarepaket trustDesk enthalten ist. Das Produkt eignet sich zur vertrauenswürdigen Anzeige und zur Bereitstellung der zu signierenden Daten sowie zur Signaturprüfung von elektronisch signierten XML-Dokumenten (insbesondere Webformularen). Elektronische Signaturen können aber über einen virtuellen Drucker für nahezu jedes Dokument auch offline erstellt werden, wobei die zu signierenden (grafischen) Daten in XML umgewandelt werden.

Auch ein Plugin für Adobe Acrobat ist verfügbar, mit dem elektronische Signaturen auf PDF-Dateien erstellt werden können. Mögliche dynamische Elemente sind dabei irrelevant, weil für die Erstellung der elektronischen Signatur nicht die PDF-Datei an sich, sondern deren grafische Darstellung herangezogen wird. Allenfalls vorhandene dynamische Elemente in der PDF-Datei würden somit zwangsläufig ein negatives Ergebnis der Signaturprüfung hervorrufen.

Für die Version 2.1.0 der Software trustview liegt eine Bescheinigung vom 23.01.2003 vor, die zwei Jahre lang gültig ist. Zuvor wurde dieses Produkt von der TÜVIT in Essen nach Common Criteria EAL3+ mit Mechanismenstärke hoch evaluiert, zertifiziert und gemäß deutschem SigG bestätigt.

3.2.4 Vertrauenswürdige Systeme

Eine Bescheinigung der Bestätigungsstelle A-SIT nach § 18 Abs. 5 SigG liegt für das Gerät IBM 4758-023 PCI Cryptographic Coprocessor mit Miniboot 0 und Miniboot 1 V2.41 und CP/Q++ V2.41 und Common Cryptographic Architecture V2.41 vor. Die Hardware sowie die Layer Miniboot 0, Miniboot 1 und CP/Q++ wurden einer erfolgreichen Evaluierung nach FIPS 140-2, Evaluationsstufe „Level 3“, unterzogen. Eine Evaluation des gesamten Geräts einschließlich der Common Cryptographic Architecture nach Common Criteria, Evaluationsstufe EAL4+, SoF high, ist noch nicht abgeschlossen und wird fortgesetzt.

Bestätigungen über die Eignung als vertrauenswürdige Systeme im Sinne von Anhang II f der Signaturrichtlinie (siehe Abschnitt 4.2.1) wurden von der Bestätigungsstelle A-SIT für folgende Geräte ausgestellt:

- PC Card Chrysalis-ITS® Luna® CA3, Firmware Version 3.9, und
- Hardware Security Module Baltimore SureWare Keyper Professional, Version 2, Release 1.

Beide Bestätigungen sind bis 31.12.2005 gültig.

3.2.5 Bürgerkarte und E-Government

Das Konzept Bürgerkarte ist die Grundlage des österreichischen E-Government-Gesetzes (vgl. Abschnitt 1.2.4.1). Zentraler Bestandteil des Konzepts ist der Security Layer: eine Programmierschnittstelle auf hoher Abstraktionsebene, über die Anwendungen auf Funktionen eines kryptografischen Tokens zugreifen können. Der Security Layer erlaubt sowohl Signaturerstellung als auch Signaturprüfung nach CMS (vgl. Abschnitt 4.1.2.2) und nach XMLDSIG (vgl. Abschnitt 4.1.3.4). Darüber hinaus ermöglicht er den Zugriff auf Infoboxen, die Schlüsselvereinbarung nach Diffie-Hellman (vgl. Abschnitt 1.1.1) sowie das Abfragen von Umgebungseigenschaften und Tokenstatus. Die Infoboxen werden insbesondere zur Speicherung der Personenbindung eingesetzt: eine elektronisch signierte Bestätigung der Stammzahlenregisterbehörde, dass der in der Bürgerkarte als Inhaberin bezeichneten natürlichen Person eine bestimmte Stammzahl zur eindeutigen Identifikation zugeordnet ist.

Basis für eine rasche Umsetzung des Konzepts in konkreten E-Government-Anwendungen sind drei vom Chief Information Office der Bundesregierung entwickelte Module für Online-Applikationen (MOA), die serverseitig eingesetzt werden:

- MOA Signaturprüfung: zur Überprüfung der elektronischen Signatur eines Bürgers in einem Anbringen.
- MOA Server-Signatur: zur Erstellung elektronischer Signaturen durch Behörden.
- MOA Identifikation und Authentifikation: zur Überprüfung der Identität eines Bürgers, der in einem Online-Verfahren mit der Behörde in Kontakt tritt.

Exemplarische Anwendungen, bei denen elektronische Signaturen eingesetzt werden, sind schon jetzt unter http://www.help.gv.at/28/Seite.280000.html verfügbar:

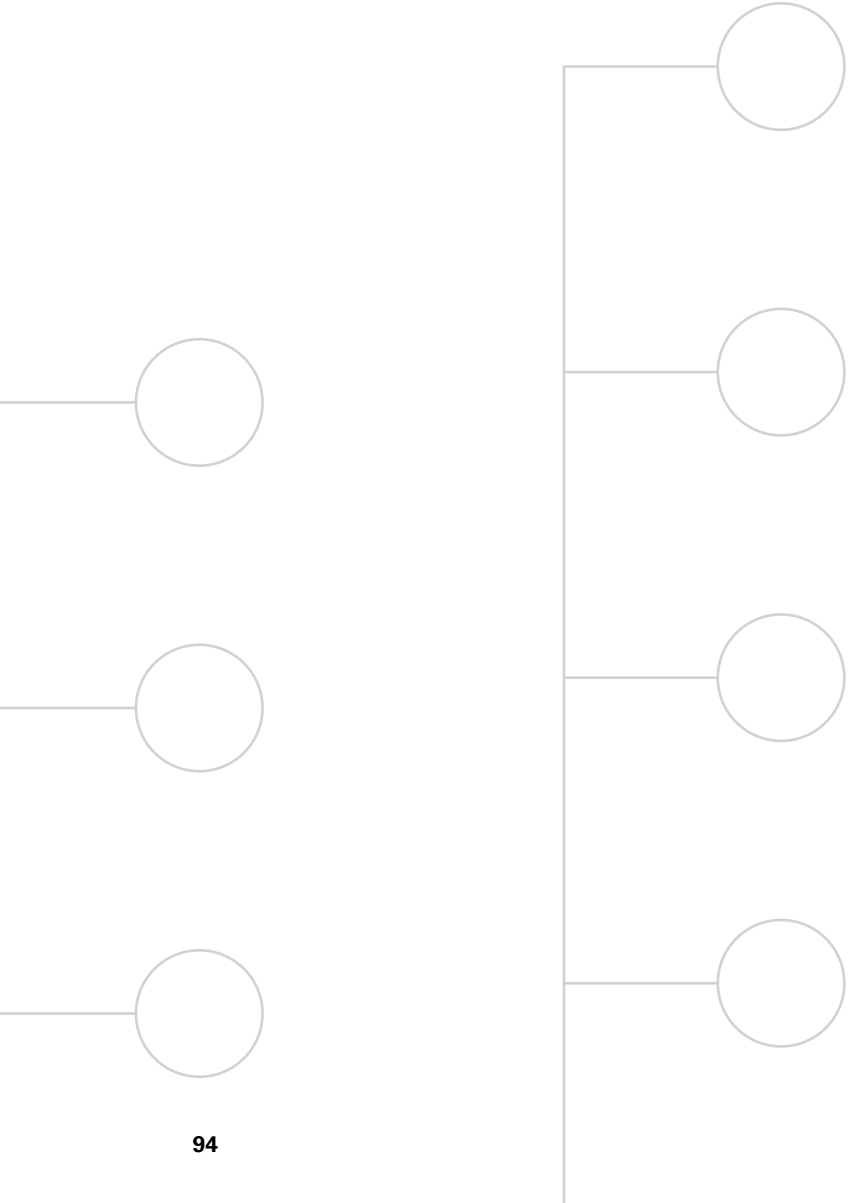
- Antrag auf Meldebestätigung,
- Antrag auf Ausstellung einer Strafregisterbescheinigung,
- Anmeldung des Wohnsitzes,
- Bauanzeigen für Abänderungen im Inneren eines Gebäudes,
- Baubeginnmeldung,
- Antrag auf Ausstellung eines Duplikates einer Heiratsurkunde oder einer Geburtsurkunde,
- Antrag auf Kinderbetreuungsgeld,
- Erklärung über den Verzicht auf Leistungen nach dem Kinderbetreuungsgeldgesetz,
- Meldungen von Kinderpornografie, Umweltkriminalität oder nationalsozialistischer Wiederbetätigung,
- Antrag auf Gewährung von Studienbeihilfe/Studienzuschuss und
- allgemeines Anbringen an die Gemeinde.

Unter http://www.sozialversicherung.at/esvapps/page/page.jsp?p_pageid=110&p_menuid=6287&p_id=5 können folgende Informationen mittels elektronischer Signatur abgefragt werden:

- Versicherungsdatenauszug,
- Grunddaten zur Krankenversicherung und
- Versicherungsnummern (für Vertragspartner der Sozialversicherung).

Bei diversen Anbietern können das Firmenbuch und das Grundbuch online abgefragt werden. Zumindest bei der Telekom Austria sind solche Abfragen auch mittels elektronischer Signatur möglich.

Die ARA Altstoff Recycling Austria AG, ein Sammel- und Verwertungssystem im Sinne des § 11 VerpackVO, nimmt von Vertragspartnern (Herstellern, Importeuren, Abpackern und Vertreibern) elektronisch signierte Meldungen über die Menge der in Umlauf gebrachten Packstoffe entgegen.



Internationales Umfeld

4.1 Normen und Empfehlungen

Eine Voraussetzung dafür, dass die elektronische Signatur und andere Sicherheitstechnologien weite Verbreitung finden, ist die Standardisierung der zugrunde liegenden Technik und der verwendeten Protokolle. Mit diesen Fragen der Standardisierung haben sich in den letzten Jahrzehnten verschiedenste Gremien befasst. Dieser Abschnitt gibt einen Überblick über die wichtigsten Normen und Empfehlungen – gegliedert nach den Organisationen.

4.1.1 ITU-T und ISO/IEC

4.1.1.1 Abstract Syntax Notation One (ASN.1)

Abstract Syntax Notation One (ASN.1) ist eine Notation, mit der komplexe Datentypen relativ einfach beschrieben werden können. Diese Notation wird auch im Kontext der digitalen Signatur verwendet, insbesondere zur formalen Beschreibung von Zertifikaten und Widerrufslisten nach ITU-T X.509. Die erste Spezifikation von ASN.1 war bereits 1984 in der mittlerweile obsoleten Norm CCITT X.409 enthalten. Als die Notation zunehmend für Anwendungsgebiete eingesetzt wurde, für die sie ursprünglich nicht vorgesehen war, wurde sie 1988 in eigene Normen ausgegliedert: ITU-T X.208 (ISO/IEC 8824) und ITU-T X.209 (ISO/IEC 8825): ITU-T X.208 enthält die Spezifikation der Notation, und in ITUT-T X209 werden die Basic Encoding Rules (BER) beschrieben, mit denen die in ASN.1 definierten Datenstrukturen in Bits und Bytes codiert werden. Codierungen nach BER sind nicht immer eindeutig: Eine in ASN.1 definierte Datenstruktur kann möglicherweise auf unterschiedliche Weise codiert werden. Speziell bei digitalen Signaturen werden oft eindeutige Codierungen benötigt. Unter anderem wurde diese Schwäche mit den 1993 geschaffenen Normen ITU-T X.680 bis X.683 (ISO/IEC 8824-1 bis 8824-4) und ITU-T X.690 und X.691 (ISO/IEC 8825-1 und 8825-2) behoben. Insbesondere wurde in ITU-T X.690 mit den Distinguished Encoding Rules (DER) eine eindeutige Codierung ermöglicht.

4.1.1.2 Zertifikate und Widerrufslisten

Die meisten Zertifizierungsdienste stellen Zertifikate auf Basis der technischen Empfehlung ITU-T X.509 (ISO/IEC 9594-8) aus. Dieses Dokument wurde

erstmals 1988 publiziert und beschreibt neben der Datenstruktur von Zertifikaten und Widerrufslisten auch Attributzertifikate (zur Darstellung zusätzlicher Eigenschaften, z. B. Vertretungsbefugnisse) und Anwendungen im Zusammenhang mit X.500-Verzeichnissen.

In der ursprünglichen Version der Empfehlung war eine Datenstruktur für Zertifikate vorgesehen, die folgende Angaben enthielt:

- die X.509-Version, nach der das Zertifikat erstellt wurde (v1),
- die Seriennummer des Zertifikats,
- eine Bezeichnung des Algorithmus, mit dem das Zertifikat signiert wurde,
- den Namen des Ausstellers,
- Anfang und Ende des Gültigkeitszeitraums,
- den Namen des Zertifikatinhabers,
- den öffentlichen Schlüssel des Zertifikatinhabers und
- die digitale Signatur des Ausstellers.

Die Namen von Aussteller und Inhaber des Zertifikats werden als Distinguished Name im Sinne von ITU-T X.501 (ISO/IEC 9594-2), d.h. als Folge von Attributen (z. B. Land, Organisation, Organisationseinheit, gängiger Name, Familienname, Vorname), angegeben. Ausgewählte Attributtypen werden in ITU-T X.520 (ISO/IEC 9594-6) definiert.

In der zweiten, 1994 veröffentlichten Version von ITU-T X.509 wurden zusätzlich eindeutige Bezeichner für den Aussteller und den Inhaber des Zertifikats eingeführt. Diese Bezeichner haben sich aber nicht durchgesetzt und werden von anderen Empfehlungen ausdrücklich verworfen. Weiters enthält diese Version die noch heute gültige Spezifikation für Widerrufslisten. Diese enthalten folgende Angaben:

- die X.509-Version, nach der die Widerrufsliste erstellt wurde (optional v2),
- eine Bezeichnung des Algorithmus, mit dem die Widerrufsliste signiert wurde,
- den Namen des Ausstellers,
- den Zeitpunkt der Ausstellung der Widerrufsliste,
- den Zeitpunkt der Ausstellung der nächsten Widerrufsliste (optional),
- eine Liste widerrufener Zertifikate,
- optionale Erweiterungen und
- die digitale Signatur des Ausstellers.

Die Liste widerrufener Zertifikate enthält die Seriennummer sowie den Widerrufszeitpunkt jedes widerrufenen Zertifikats. Darüber hinaus können zertifikatspezifische Erweiterungen (z. B. Grund des Widerrufs) vorhanden sein.

Die dritte, 1997 veröffentlichte Version brachte ein flexibles Konzept für Zertifikaterweiterungen, durch die z. B. der Verwendungszweck (Verschlüsselung, digitale Signatur, Authentifizierung usw.), die Certificate Policy, die Nutzungsdauer für den privaten Schlüssel etc. festgelegt werden können. Einige dieser Erweiterungen werden in ITU-T X.509 definiert. Das Konzept ist aber offen für neue Erweiterungen, die in späteren Dokumenten (z. B. RFC 3280) beschrieben werden.

4.1.1.3 ISO/IEC 7816: Identifikationskarten – Chipkarten mit Kontakten

ISO/IEC 7816 ist eine mehrteilige Norm zur Spezifikation von Chipkarten mit Kontakten.

- ISO/IEC 7816-1 (1998) behandelt die physischen Eigenschaften.
- ISO/IEC 7816-2 (1999) legt die Abmessungen und die Lokalisierung der Kontakte fest.
- ISO/IEC 7816-3 (1997) spezifiziert die elektronischen Eigenschaften und die Übertragungsprotokolle. Eine Änderung aus dem Jahr 2002 beschreibt elektrische Charakteristiken und Klassenanzeige für Chipkarten, die bei 5 V, 3 V und 1,8 V arbeiten.
- ISO/IEC 7816-4 (1995) definiert interindustrielle Kommandos. Eine Ergänzung aus dem Jahr 1997 beschreibt die Auswirkung des Secure-Messaging-Verfahrens[56] auf die APDU-Strukturen[57].
- ISO/IEC 7816-5 (1994/96) legt das Nummerierungssystem und die Verwaltung der Anwenderkennzeichen fest.
- ISO/IEC 7816-6 (1996/98) ist ein Verzeichnis von interindustriellen Datenelementen, die in Anwendungen gemäß Teil 4 verwendet werden können.
- ISO/IEC 7816-7 (1999) definiert interindustrielle Kommandos für die strukturierte Kartenabfragesprache SCQL[58].
- ISO/IEC 7816-8 (1999) definiert interindustrielle sicherheitsbezogene Kommandos.
- ISO/IEC 7816-9 (2000) definiert zusätzliche interindustrielle Kommandos und Sicherheitsattribute.
- ISO/IEC 7816-10 (1999) spezifiziert elektronische Signale und „Answer to Reset“ für synchrone Karten.

56) Sichere Kommunikation zwischen Anwendungskomponenten außer- und innerhalb der Chipkarte.
57) APDU = Application Protocol Data Units (Datenstrukturen zur Information mit der Chipkarte).
58) SCQL = Structured Card Query Language.

4.1.1.4 ISO/IEC 9796: Digitaler Unterschriftsmechanismus mit Rückgewinnung der Nachricht

ISO/IEC 9796 spezifiziert digitale Signaturen, bei denen die signierten Daten aus der Signatur wieder hergestellt werden können. Diese Norm wird in Österreich unter anderem im Produkt MBS-Sign (siehe Abschnitt 3.2.3.1) angewandt.

4.1.1.5 ISO/IEC 10118: Hash-Funktionen

ISO/IEC 10118 besteht aus mehreren Teilen: Der erste Teil (1994) enthält Definitionen und beschreibt allgemeine Konzepte von Hashverfahren. Der zweite Teil (1994) spezifiziert zwei Methoden zur Konstruktion von Hashverfahren aus Blockchiffren. Der dritte Teil (1997) spezifiziert u. a. die gemäß Anhang 2 der SigV als sicher angesehenen Hashverfahren SHA-1 und RIPEMD-160.

4.1.1.6 ISO/IEC 14888: Digitale Signaturen mit Anhang

ISO/IEC 14888 spezifiziert digitale Signaturen, bei denen die signierten Daten aus der Signatur nicht wieder hergestellt werden können. In dieser Norm wird insbesondere eine auf elliptischen Kurven beruhende DSA-Variante genannt, die laut Anhang 2 der SigV für sichere elektronische Signaturen geeignet ist („Agnew-Mullin-Vanstone analogue“).

4.1.1.7 ISO/IEC 15408: Evaluationskriterien für IT-Sicherheit

„Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik“ (Common Criteria for Information Technology Security Evaluation) sind unter Beteiligung zahlreicher Staaten entstanden und eignen sich für die Bewertung der Sicherheitseigenschaften fast aller informationstechnischer Produkte und Systeme. Dabei wird zwischen funktionalen Sicherheitsanforderungen und Anforderungen an die Vertrauenswürdigkeit unterschieden. Letztere werden durch sieben Vertrauenswürdigkeitsstufen (Evaluation Assurance Level, kurz EAL) dargestellt, die mit EAL1 bis EAL7 bezeichnet werden (die Stufen EAL2 bis EAL7 entsprechen inhaltlich etwa den Stufen E1 bis E6 von ITSEC, vgl. Abschnitt 4.1.8).

Die Anforderungen an die Funktionalität und an die Vertrauenswürdigkeit können in Schutzprofilen für bestimmte Produktgruppen zusammengefasst werden. Beispielsweise existiert ein Schutzprofil für sichere Signaturerstellungseinheiten, das von der Europäischen Kommission als allgemein anerkannte Norm veröffentlicht wurde (CWA 14169, siehe Abschnitt 4.1.5.3.3).

Eine wichtige Voraussetzung für die internationale Anerkennung der Evaluierung ist die in einem gesonderten Dokument beschriebene Gemeinsame Evaluationsmethodologie (Common Evaluation Methodology, CEM).

4.1.1.8 ISO/IEC 17799: Leitfaden für das Management der Informationssicherheit

Dieses Dokument, das inhaltlich dem ersten Teil des in § 9 Abs. 2 SigV genannten britischen Standards BS 7799 entspricht, ist eine allgemeine IT-Sicherheitsnorm, die folgende Themenbereiche abdeckt: Sicherheitskonzept, Sicherheitsorganisation, Schutz der IT-Infrastruktur, personelle Sicherheit, physische und Umweltsicherheit, Management des IT-Betriebs, Zugriffskontrolle, Entwicklung und Wartung von Systemen, Wahrung der Kontinuität der Geschäfte, Entwicklung und Wartung von Systemen, Einhaltung von Vorschriften.

4.1.2 RSA Security, Inc.

Von RSA Security, Inc., dem Betreiber der RSA Laboratories, werden seit 1991 sogenannte Public-Key Cryptography Standards (PKCS) entwickelt, die teilweise auf Normen der ITU-T aufbauen. Obwohl die PKCS-Dokumente nicht von Normungsinstituten veröffentlicht werden, haben einige von ihnen im Laufe der Zeit doch den Rang von Industriestandards gewonnen.

4.1.2.1 PKCS #1: RSA Cryptography Standard

Dieses Dokument enthält Empfehlungen zur Implementierung des RSA-Verfahrens. Es beschreibt auch Padding-Verfahren, insbesondere Optimal Asymmetric Encryption Padding (OAEP). Weiters werden in diesem Dokument einige ASN.1 Object Identifier festgelegt, die in Zusammenhang mit dem RSA-Verfahren bedeutsam sind.

Die aktuelle Fassung ist PKCS #1 Version 2.1. Ältere Versionen sollten aufgrund kryptografischer Schwächen[59] nach Möglichkeit nicht mehr verwendet werden.

4.1.2.2 PKCS #7: Cryptographic Message Syntax Standard

Dieses Dokument beschreibt eine allgemeine Syntax für Daten, auf die kryptografische Operationen angewandt werden. Diese Syntax ermöglicht beispielsweise die Zusammenfassung einer Zertifikatskette in einer einzigen Datenstruktur. Sie wird aber auch zum Verschlüsseln und Signieren von E-Mails mittels S/MIME Version 2 (siehe Abschnitt 4.1.3.2) verwendet.

PKCS #7 wurde seit einigen SET-spezifischen Änderungen aus dem Jahr 1997 nicht mehr geändert und gilt mittlerweile als obsolet, jedoch werden die dort definierten Datenstrukturen weiterhin verwendet. Inhaltlich entspricht PKCS #7 dem von der IETF veröffentlichten RFC 2315. Dieses wurde durch RFC 2630 abgelöst, das seinerseits inzwischen durch RFC 3369 und RFC 3370 ersetzt ist. S/MIME Version 3 nimmt nicht mehr auf PKCS #7 Bezug.

4.1.2.3 PKCS #10: Certification Request Syntax Standard

Dieses Dokument beschreibt die Syntax eines Zertifizierungsantrags. Eine derartige Datenstruktur wird verwendet, wenn ein Zertifikat für einen Schlüssel ausgestellt werden soll, über den der Zertifikatswerber bereits vor Ausstellung des Zertifikats verfügt.

Ein Zertifizierungsantrag enthält folgende Daten:

- die Version, nach der der Zertifizierungsantrag erstellt wurde,
- den Namen des Zertifikatswerbers,
- den öffentlichen Schlüssel des Zertifikatswerbers und die Bezeichnung des zugehörigen Verfahrens,
- allfällige Attribute und
- eine digitale Signatur, die mit dem privaten Schlüssel des Zertifikatswerbers erstellt wurde und mit der überprüft werden kann, ob der Zertifikatswerber tatsächlich über den privaten Schlüssel verfügt.

59) Bleichenbacher, Daniel; Kaliski, Burt; Staddon, Jessica: Recent Results on PKCS #1: RSA Encryption Standard. Bulletin #7. RSA Laboratories, 1998, ftp://ftp.rsasecurity.com/pub/pdfs/bulletn7.pdf.

4.1.2.4 PKCS #11: Cryptographic Token Interface Standard

Dieses Dokument definiert eine auch als Cryptoki bezeichnete, technologieneutrale Applikationsschnittstelle, über die ein oder mehrere Rechner auf ein oder mehrere kryptografische Geräte wie Chipkarten und HSMs zugreifen können.

Über PKCS #11 können beispielsweise Webbrowser und Mail-Clients wie Mozilla auf Chipkarten zugreifen. Ebenso erlaubt PKCS #11 aber auch vergleichsweise komplexe Operationen, wie sie etwa von Zertifizierungsdiensteanbietern ausgeführt werden.

Die aktuelle Fassung ist PKCS #11 Version 2.11. Ein Entwurf für Version 2.20 wurde bis Oktober 2003 zur öffentlichen Begutachtung bereitgestellt. Als Ergänzung ist eine „Conformance Profile Specification" veröffentlicht worden.

4.1.2.5 PKCS #12: Personal Information Exchange Syntax Standard

Dieses Dokument spezifiziert ein Format, in dem nicht nur Zertifikate und Zertifikatsketten (wie in PKCS #7), sondern auch private Schlüssel und andere vertrauliche Daten gespeichert und transportiert werden können.

Die aktuelle Fassung ist PKCS #12 Version 1.0 aus dem Jahr 1999 und beruht auf einer älteren, von Microsoft beigesteuerten Spezifikation mit der Bezeichnung PFX.

4.1.2.6 PKCS #15: Cryptographic Token Information Format Standard

PKCS #15 soll gewährleisten, dass Benutzer unabhängig vom Cryptoki-Anbieter auf standardkonforme kryptografische Token zugreifen können. Das Dokument beschreibt u.a. Dateisysteme und Dateiformate, wie sie auf Chipkarten verwendet werden.

Die aktuelle Fassung ist PKCS #11 Version 1.1. Als Ergänzung ist eine „Conformance Profile Specification" veröffentlicht worden.

4.1.3 IETF und W3C

Die von Normungsinstituten bereitgestellten Dokumente sind in manchen Bereichen zu abstrakt, um die Interoperabilität konkreter Implementierungen zu ermöglichen. Die Internet Engineering Task Force (IETF) und das World Wide Web Consortium (W3C) haben erheblich dazu beigetragen, existierende Normen in praxistauglicher Weise zu verfeinern. Viele Dokumente, die von diesen Organisationen geschrieben werden, werden zunächst als Internet-Draft mit befristeter Gültigkeit veröffentlicht. Bewährte Dokumente werden als Request For Comments (RFC) grundsätzlich ohne Befristung publiziert.

4.1.3.1 PKIX

PKIX ist eine Arbeitsgruppe der IETF, die sich mit Public-Key-Infrastruktur auf der Grundlage von X.509 befasst und die einige bedeutende Meilensteine beigetragen hat:

4.1.3.1.1 RFC 2459, 3279 und 3280: Certificate and CRL Profile

Das Dokument RFC 2459 kann als Verfeinerung von ITU-T X.509 aufgefasst werden: Es beschreibt Zertifikate nach X.509 v3 und Widerrufslisten nach X.509 v2 detailliert und bietet Ergänzungen insbesondere für Internet-spezifische Anwendungen (z. B. Attribute zur Darstellung von IP-Adressen in Namen). Standarderweiterungen werden beschrieben und zusätzliche definiert. Eine Menge notwendiger Zertifikaterweiterungen wird festgelegt. Darüber hinaus wird ein Algorithmus zur Überprüfung eines Zertifizierungspfads beschrieben.

Im Jahr 2002 wurde RFC 2459 durch die Dokumente RFC 3279 und 3280 abgelöst. Während in RFC 3280 das Profil von Zertifikaten und Widerrufslisten beschrieben wird, werden in RFC 3279 die zugehörigen Algorithmen und ASN.1 Object Identifier definiert.

4.1.3.1.2 RFC 2527: Certificate Policy and Certification Practices Framework

In RFC 2527 werden die Unterschiede zwischen Certificate Policy und Certification Practice Statement erörtert. Für beide Dokumentarten wird eine Gliederung vorgeschlagen. Weiters wird eine umfassende Liste von Themen bereitgestellt, die in einer Certificate Policy bzw. in einem Certification Practice Statement behandelt werden sollen.

4.1.3.1.3 RFC 2559, 2587 und 3494: LDAPv2

RFC 2559 beschreibt die Verwendung des Lightweight Directory Access Protocol (LDAP) Version 2 für den Zugriff auf Verzeichnisse von Zertifikaten. RFC 2587 definiert das hierbei eingesetzte Schema (insbesondere Objekte mit PKI-Bezug). RFC 3494 empfiehlt die Verwendung von LDAPv3 anstelle von LDAPv2 (und somit RFC 2559).

4.1.3.1.4 RFC 2560: Online Certificate Status Protocol (OCSP)

Während Widerrufslisten in der Regel nur einen verzögerten Zugriff auf Widerrufsinformationen erlauben, können mittels OCSP jederzeit aktuelle Informationen über die Gültigkeit eines Zertifikats eingeholt werden.

4.1.3.1.5 RFC 3039: Qualified Certificates Profile

Auf der Grundlage von RFC 2459 wird in RFC 3039 ein Profil für qualifizierte Zertifikate (siehe Abschnitt 1.2.1.2.4) zur Verwendung im Internet spezifiziert. Qualifizierte Zertifikate im Sinne von RFC 3039 werden ausschließlich an natürliche Personen ausgestellt.

4.1.3.2 S/MIME

S/MIME steht für Secure Multipurpose Internet Mail Extensions und besteht aus mehreren zusammengehörigen Standards, die primär zum Verschlüsseln und zum Signieren von E-Mails entwickelt wurden.

S/MIME Version 2 ist durch RFC 2268, 2311, 2312, 2313, 2314 und 2315 spezifiziert. Wie schon in Abschnitt 4.1.2.2 erwähnt, beruht es u. a. noch auf PKCS #7.

S/MIME Version 3 ist durch RFC 2631, 2632, 2633, 3369 und 3370 spezifiziert. Erweiterungen wie z. B. signierte Empfangsbestätigungen werden in RFC 2634 beschrieben.

Nach Ansicht der RTR-GmbH eignet sich S/MIME nicht für sichere elektronische Signaturen auf E-Mails, weil Kopfzeilen (z. B. der Betreff) nicht mitsigniert werden und weil an das Datenformat von Attachments keine hinreichenden Anforderungen gestellt werden (etwa zur Verhinderung der Darstellung dynamischer Elemente).

4.1.3.3 OpenPGP

OpenPGP erfüllt in der Welt von PGP ähnliche Aufgaben wie S/MIME in der Welt von X.509. OpenPGP wird durch RFC 1991 und 2015 definiert. Da PGP nicht auf dem Konzept von Zertifizierungsdiensten, sondern auf der Idee eines „Web of Trust" beruht, wird hier auf eine nähere Beschreibung verzichtet[60].

4.1.3.4 XMLDSIG

XMLDSIG ist eine gemeinsame Initiative von IETF und W3C zur Standardisierung von Signaturen im Format XML. Voraussetzungen für XML-Signaturen werden in RFC 2807 beschrieben. Syntax und Verarbeitung der Signatur werden in RFC 3275 spezifiziert.

Um mehrere zusammengehörige Objekte gemeinsam zu signieren, wird ein sogenanntes Manifest verwendet: eine Sammlung von Referenzen auf die zu signierenden Objekte.

Um eine XML-Signatur überprüfen zu können, müssen die Daten beim Signieren und bei der Signaturprüfung einheitlich repräsentiert werden. Zu diesem Zweck wird in RFC 3076 ein kanonisches XML definiert: Wenn zwei XML-Dokumente dieselbe kanonische Darstellung aufweisen, gelten sie als logisch äquivalent.

Weitere Informationen sind unter http://www.w3.org/Signature/ verfügbar.

4.1.4 IEEE P1363: Standard Specifications for Public-Key Cryptography

P1363 besteht derzeit aus vier Teilen:

- P1363-2000 und P1363a beschreiben Schemen für digitale Signatur und Schlüsselfestlegung, die u. a. auf den in Abschnitt 1.1.1 genannten algebraischen Problemen beruhen,
- P1363.1 beschreibt Schemen für Verschlüsselung und digitale Signatur, die auf Gittern beruhen,
- P1363.2 beschreibt Schemen für Schlüsselvereinbarung und -rückgewinnung auf Basis der Authentifizierung mit Hilfe von Passwörtern.

60) Vgl. http://www.imc.org/smime-pgpmime.html

In dieser Norm werden insbesondere zwei auf elliptischen Kurven beruhende DSA-Varianten genannt, die laut Anhang 2 der SigV für sichere elektronische Signaturen geeignet sind („Nyberg-Rueppel Version“ und „DSA Version“).

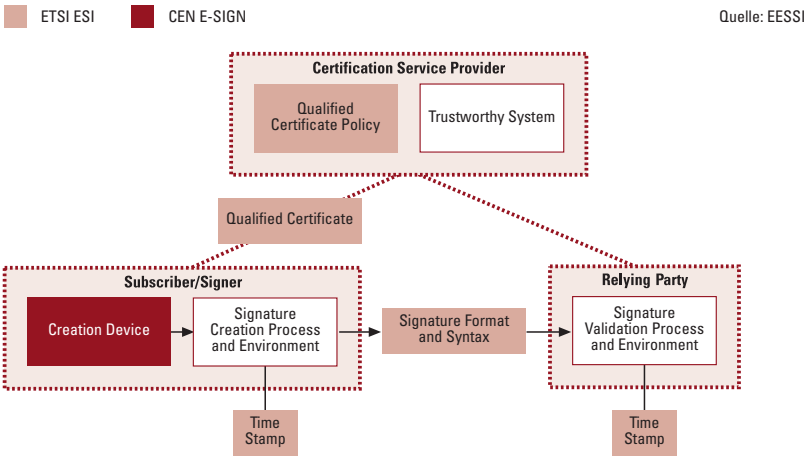
4.1.5 EESSI

Die European Electronic Signature Standardization Initiative (EESSI) wurde vom European ICT Standards Board mit Unterstützung der Europäischen Kommission gegründet, um dem Mangel an Konsistenz und Kohärenz bestehender Normen für elektronische Signaturen entgegenzuwirken. Im Rahmen der EESSI sollen Industrie, Behörden, Experten und andere Marktteilnehmer zusammenwirken. Die Standardisierung im Rahmen der EESSI geschieht durch die europäischen Normungsinstitute CEN und ETSI.

Bisher hat die Europäische Kommission nach den Bestimmungen der Signaturrichtlinie lediglich drei Dokumente in den Rang von allgemein anerkannten Normen erhoben (vgl. Abschnitt 4.1.5.3). Tatsächlich hat die EESSI seit Juli 1999 wesentlich mehr Empfehlungen hervorgebracht. Über die wichtigsten unter ihnen soll dieser Abschnitt einen Überblick bieten.

4.1.5.1 Überblick

Abb. 11: Arbeitspakete der EESSI



Der Arbeitsschwerpunkt der EESSI liegt in der Standardisierung von Sicherheitsvorgaben und Datenstrukturen, die beim Zertifizierungsdiensteanbieter, beim Signator und bei vertrauenden Parteien angewandt werden. In Abb. 11 werden das Arbeitsprogramm und die Zuständigkeiten der Normungsinstitute beschrieben.

4.1.5.2 ETSI TC ESI

4.1.5.2.1 SR 002 176: Algorithms and Parameters for Secure Electronic Signatures

Das sogenannte Algorithmenpapier, das bereits 2001 von einer Expertengruppe unter dem Dach der EESSI entwickelt wurde, wurde erst 2003 von ETSI als Special Report publiziert. Es beschreibt Algorithmen und Parameter, die bis Ende 2005 als sicher angesehen werden. Obwohl sogar in der allgemein anerkannten Norm CWA 14169 (siehe Abschnitt 4.1.5.3.3) Bezug auf das Algorithmenpapier genommen wird, wird diesem der Rang einer Norm bislang verweigert. Die für sichere elektronische Signaturen als sicher angesehenen Algorithmen und Parameter werden daher weiterhin auf Ebene der Mitgliedstaaten festgelegt. Innerhalb der EESSI und seitens zahlreicher Aufsichtsstellen mehren sich aber die Bestrebungen, dieses Problem auf europäischer Ebene durch eine allgemein anerkannte Norm (einschließlich entsprechender Wartungsmechanismen) zu lösen.

Das Algorithmenpapier legt nicht nur Hash-, Padding- und Verschlüsselungsverfahren fest, sondern stellt auch geeignete Kombinationen solcher Verfahren in sogenannten „Signatursuiten" zusammen. Darüber hinaus werden geeignete Algorithmen zur Schlüsselerzeugung definiert. Die Qualität der Parameter entspricht in der Größenordnung etwa jener, die auch in Anhang 1 der SigV gefordert wird.

4.1.5.2.2 TR 102 030: Provision of Harmonized Trust Service Provider Status Information

Dieses Dokument geht der Frage nach, wie ein Benutzer feststellen kann, ob ein Trust Service Provider (TSP, z. B. ein Zertifizierungsdiensteanbieter) zu einem bestimmten Zeitpunkt mit Zustimmung eines anerkannten Schemas (z. B. einer Akkreditierungsstelle) operiert hat. Zu diesem Zweck wird eine als TSP Status List (TSL) bezeichnete Datenstruktur definiert, die detaillierte Information über alle unter einem bestimmten Schema operierenden TSPs enthält.

Ob das Konzept TSL vom Markt angenommen wird, kann derzeit noch nicht abgeschätzt werden. Sollte sich eine derartige Entwicklung abzeichnen, wird auch seitens der RTR-GmbH erwogen, als Ergänzung zum bereits vorhandenen Verzeichnis der Zertifizierungsdienste (siehe Abschnitt 2.2) eine TSL bereitzustellen.

4.1.5.2.3 TS 101 456: Policy Requirements for Certification Authorities Issuing Qualified Certificates

Dieser Standard legt primär organisatorische Erfordernisse für Anbieter qualifizierter Zertifikate fest. Das Dokument definiert auch zwei Certificate Policies und die zu ihrer Bezeichnung verwendeten ASN.1 Object Identifier: eine allgemeine Policy für öffentlich angebotene qualifizierte Zertifikate und eine spezielle Policy für öffentlich angebotene qualifizierte Zertifikate, die den Einsatz sicherer Signaturerstellungseinheiten erfordern. Die aktuelle Version 1.2.1 wurde 2002 publiziert.

Die Einhaltung dieses Standards ist nach österreichischem Recht nicht vorgeschrieben. Die Aufsichtsstelle überprüft einen Zertifizierungsdiensteanbieter nur dann gemäß ETSI TS 101 456, wenn im Sicherheits- und Zertifizierungskonzept des Anbieters die Einhaltung dieses Standards behauptet wird. A-Trust, der zur Zeit einzige in Österreich niedergelassene Anbieter qualifizierter Zertifikate, entspricht den Vorgaben von ETSI TS 101 456. Auch die Aufsichtsstelle hat ihr Certification Practice Statement an ETSI TS 101 456 ausgerichtet, die Erfüllung der Vorgaben des Standards wurde von der Bestätigungsstelle A-SIT im Juli 2003 bestätigt.

4.1.5.2.4 TS 101 733: Electronic Signature Formats

ETSI TS 101 733 ist eine umfassende, weit über den Titel des Dokuments hinausgehende Beschreibung von Signaturformaten und ihren verschiedenartigen Einsatzmöglichkeiten. Die vorgeschlagene Datenstruktur der elektronischen Signatur baut auf der existierenden Cryptographic Message Syntax (RFC 2630, nunmehr RFC 3369 und 3370) auf. Vorgesehen sind insbesondere Signature Policies und Signature Validation Policies, die durch Datenstrukturen in ASN.1 repräsentiert werden. Auch spezielle Anwendungen wie Zeitstempel und das Nachsignieren werden behandelt. Die aktuelle Version 1.4.0 wurde 2002 publiziert.

4.1.5.2.5 TS 101 861: Time Stamping Profile

Dieses Dokument spezifiziert Zeitstempel auf der Grundlage von RFC 3161, wobei die Vielzahl der dort erwähnten Optionen eingeschränkt wird. Die aktuelle Version 1.2.1 wurde 2002 publiziert.

4.1.5.2.6 TS 101 862: Qualified Certificate Profile

Dieses Dokument beschreibt Erweiterungen zur Verwendung in qualifizierten Zertifikaten, insbesondere:

- den Hinweis darauf, dass es sich um ein qualifiziertes Zertifikat handelt,
- eine Begrenzung des Transaktionswerts, auf den das Zertifikat ausgestellt ist,
- Angaben über den Zeitraum, in dem der Aussteller des Zertifikats relevante Informationen archiviert und im Falle eines Disputs bereitstellt.

Das Dokument baut auf RFC 3039 (vgl. Abschnitt 4.1.3.1.5) auf. Die vorliegende Version 1.2.1 wurde 2001 publiziert.

4.1.5.2.7 TS 101 903: XML Advanced Electronic Signatures (XAdES)

Dieser Standard beschreibt XML-Formate für fortgeschrittene elektronische Signaturen, die den Vorgaben der Signaturrichtlinie entsprechen, über einen langen Zeitraum gültig bleiben und in häufigen Anwendungsfällen zusätzliche Information bereitstellen. Dabei wird auf XMLDSIG (siehe Abschnitt 4.1.3.4) und auf ETSI TS 101 733 (siehe Abschnitt 4.1.5.2.4) aufgebaut. Die vorliegende Version 1.1.1 wurde 2002 publiziert.

4.1.5.3 CEN E-SIGN

Die Dokumente CWA 14167-1, 14167-2 und 14169 sind die ersten und bislang letzten, für welche die Europäische Kommission nach Art. 3 Abs. 5 der Signaturrichtlinie (siehe Abschnitt 4.2.1) Referenznummern für allgemein anerkannte Normen festgelegt und im Amtsblatt der Europäischen Gemeinschaften veröffentlicht hat[61].

61) Entscheidung der Kommission vom 14.07.2003 über die Veröffentlichung von Referenznummern für allgemein anerkannte Normen für Produkte für elektronische Signaturen gemäß der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates, ABl L 175 vom 15.07.2003, S. 45.

4.1.5.3.1 CWA 14167-1: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements

Diese Norm in der Fassung vom März 2003 beschreibt Erfordernisse hinsichtlich der Sicherheit vertrauenswürdiger Systeme im Sinne von Anhang II f der Signaturrichtlinie (siehe Abschnitt 4.2.1). Zahlreiche inhaltliche Überschneidungen mit ETSI TS 101 456 werden in Anhang A dieser Norm tabellarisch dargestellt.

4.1.5.3.2 CWA 14167-2: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 2: Cryptographic Module for CSP Signing Operations – Protection Profile (MCSO-PP)

Dieses Dokument in der Fassung vom März 2002 spezifiziert ein Schutzprofil zur Evaluierung vertrauenswürdiger Systeme nach den „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik"(siehe Abschnitt 4.1.1.7). Die Evaluierung des Schutzprofils, das nach eben diesen Kriterien selbst einer Prüfung unterzogen werden muss, konnte bislang nicht positiv abgeschlossen werden. Somit entsteht die paradoxe Situation, dass eine „allgemein anerkannte Norm" nicht ohne Missachtung ihrer eigenen Grundlage angewandt werden kann.

4.1.5.3.3 CWA 14169: Secure Signature-Creation Devices „EAL4+"

Dieses Dokument in der Fassung vom März 2002 spezifiziert ein Schutzprofil für sichere Signaturerstellungseinheiten nach den „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik" (siehe Abschnitt 4.1.1.7). Dieses Schutzprofil bildet künftig die Grundlage für die Evaluierung von Signaturchipkarten.

4.1.6 NIST

4.1.6.1 FIPS 140-2: Security Requirements for Cryptographic Modules

Insbesondere die in den USA hergestellten kryptografischen Geräte werden häufig nach FIPS 140-2 validiert. FIPS 140-2 berücksichtigt nicht die besonderen Erfordernisse für vertrauenswürdige Systeme bzw. für sichere Signaturerstellungseinheiten. Eine Validierung solcher Geräte nach FIPS 140-2

wird zwar als nützlich empfunden, unter europäischen Experten besteht aber weitgehend Konsens darüber, dass sie eine Evaluierung anhand spezifischer Schutzprofile nach den „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik“ (siehe Abschnitt 4.1.1.7) nicht ersetzen kann.

4.1.6.2 FIPS 180-2: Secure Hash Standard

Dieses Dokument enthält die Spezifikation des Hashverfahrens SHA-1 sowie der neueren Varianten SHA-256, SHA-384 und SHA-512.

4.1.6.3 FIPS 186-2: Digital Signature Standard

Dieses Dokument enthält die Spezifikation der Signaturverfahren DSA und ECDSA. Die Spezifikation von ECDSA baut auf ANSI X9.62 (siehe Abschnitt 4.1.7.4) auf.

4.1.7 ANSI

4.1.7.1 X9.17: Financial Institution Key Management

Dieses Dokument beschreibt u. a. Algorithmen zur Erzeugung von Pseudozufallszahlen, die in ETSI SR 002 176 zitiert werden.

4.1.7.2 X9.30: DSA

ANSI X9.30 enthält die von der US-Finanzwirtschaft verwendete Spezifikation des Signaturverfahrens DSA.

4.1.7.3 X9.31: RSA

ANSI X9.31 enthält die von der US-Finanzwirtschaft verwendete Spezifikation des Signaturverfahrens RSA.

4.1.7.4 X9.62: ECDSA

ANSI X9.62 enthält die Spezifikation des Signaturverfahrens ECDSA.

4.1.8 ITSEC

Die „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik“ (Information Technology Security Evaluation Criteria, ITSEC) sind noch immer ein anerkannter Vorläufer der „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik“ (siehe Abschnitt 4.1.1.7). Bei ITSEC wird erstmals zwischen Funktionalität und Vertrauenswürdigkeit differenziert. Bezüglich der Vertrauenswürdigkeit wird weiters zwischen Korrektheit und Wirksamkeit unterschieden. Zur Bewertung der Wirksamkeit werden die Mechanismenstärken „niedrig“, „mittel“ und „hoch“ herangezogen. Das Vertrauen in die Korrektheit wird durch Evaluationsstufen E1 bis E6 bewertet, die insbesondere den Umfang der Dokumentation und den Aufwand bei der Evaluation zum Ausdruck bringen.

4.2 Rechtlicher Überblick

4.2.1 Europäische Union: Signaturrichtlinie

Im internationalen Vergleich ist die Signaturrichtlinie[62] der Europäischen Union zweifellos das detaillierteste Regelungswerk. Die Signaturrichtlinie enthält eine Reihe technischer und organisatorischer Anforderungen an die Anbieter qualifizierter Zertifikate und verlangt EU-weite Anerkennung der diesen Anforderungen entsprechend ausgestellten Zertifikate. Die Europäische Union hat auch große Anstrengungen unternommen, das rechtliche Regelungswerk in die Praxis umzusetzen. Im Auftrag der Europäischen Kommission haben die Normungsgremien CEN und ETSI eine Fülle technischer Standards erstellt (vgl. Abschnitt 4.1.5), welche zum Teil auch über die Grenzen Europas hinweg weite Anerkennung gefunden haben.

Die Signaturrichtlinie ist relativ kurz, sie enthält nur 15 Artikel. Die technischen und organisatorischen Anforderungen sind in vier Anhängen enthalten, die ebenfalls kurz gehalten sind und jeweils nicht mehr als eine Seite umfassen.

4.2.1.1 Technologieneutralität

Ein wesentlicher Grundsatz der Signaturrichtlinie ist die Technologieneutralität. Für die Signatur elektronischer Dokumente sollen beliebige

62) Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13.12.1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. L 13 vom 19.01.2000, S. 12.

geeignete Technologien verwendet werden können. Um diesen Grundsatz zum Ausdruck zu bringen, wurde auch bewusst eine neue Terminologie eingeführt. Der Begriff der „elektronischen Signatur" soll mehr umfassen als der Begriff der „digitalen Signatur", soll also nicht bloß die asymmetrische Kryptografie umfassen, sondern auch allfällige neue Verfahren abdecken. Statt dem „privaten Schlüssel" wird der Begriff der „Signaturerstellungsdaten", statt dem „öffentlichen Schlüssel" der Begriff der „Signaturprüfdaten" eingeführt.

Die Technologieneutralität der Richtlinie kann allerdings positiv und negativ gesehen werden. Zum einen wird die Technologie der elektronischen Signatur laufend weiterentwickelt (vgl. Abschnitt 4.1), eine zu frühe Festlegung auf bestimmte technologische Details in der Richtlinie hätte diese Entwicklung bremsen können. Zum anderen kann die Richtlinie den Grundsatz der Technologieneutralität aber auch nicht konsequent einhalten. Die Begriffe des Zertifikates und des Zertifizierungsdiensteanbieters gehören zu den zentralen Begriffen der Richtlinie, die elektronische Signatur im Sinne der Richtlinie ist jedenfalls eine Technologie, bei welcher der Signator zur Signaturerstellung Daten verwendet, über welche er die alleinige Kontrolle ausübt, und wo die solcherart erstellte Signatur über Zertifikate, die von einem Zertifizierungsdiensteanbieter ausgestellt wurden, seiner Person zugeordnet werden können. Die Regelung ist daher genau auf die asymmetrische Kryptografie und auf Public-Key-Infrastrukturen zugeschnitten. Andere Formen der Authentifizierung sind benachteiligt, sie werden insbesondere nicht durch die in Umsetzung der Richtlinie entwickelten Normen (vgl. Abschnitt 4.1.5) unterstützt.

Weiters ist darauf zu verweisen, dass ein großes Problem der Praxis derzeit in der mangelhaften Interoperabilität vieler Signaturprodukte und Signaturverfahren besteht. Der Grundsatz der Technologieneutralität trägt natürlich nicht dazu bei, dieses Problem zu verringern, und auch die vorliegenden Normen konnten dieses Problem nur zum Teil beseitigen.

4.2.1.2 Freier Marktzugang und Binnenmarkt

Bei der Signaturrichtlinie handelt es sich um eine typische Harmonisierungsrichtlinie. Durch gemeinschaftsweit gleiche Anforderungen soll der Binnenmarkt verwirklicht werden. Jeder Mitgliedstaat soll dazu verpflichtet sein, die Zertifikate, Zertifizierungsdienste und Signaturprodukte der anderen Mitgliedstaaten zu akzeptieren.

Ergänzt wird dies durch die Einführung bzw. Sicherung des freien Marktzuganges. Die Bereitstellung von Zertifizierungsdiensten darf von keiner vorherigen Genehmigung abhängig gemacht werden, d. h. über allgemeine rechtliche Anforderungen wie z. B. Regelungen zur Unternehmensgründung oder zur Erlangung einer Gewerbeberechtigung hinaus dürfen keine zusätzlichen Genehmigungsverfahren eingerichtet werden, die spezifisch auf die elektronische Signatur oder die Tätigkeit als Zertifizierungsdiensteanbieter abstellen. Deutschland musste sein existierendes Genehmigungssystem daher umstellen. In den meisten Mitgliedstaaten ist nun ein System etabliert, bei welchem der Zertifizierungsdiensteanbieter gleichzeitig mit der Aufnahme seiner Tätigkeit oder kurz davor Anzeige an die Aufsichtsstelle erstatten muss. Der Zertifizierungsdiensteanbieter wird dann gegebenenfalls von der Aufsichtsstelle überprüft, muss das Ergebnis der Überprüfung aber nicht abwarten.

Um gemeinschaftsweit Vertrauen in die Sicherheit von Zertifizierungsdiensten herzustellen, verlangt die Signaturrichtlinie die Einrichtung eines Aufsichtssystems für die Anbieter qualifizierter Zertifikate. Jeder Mitgliedstaat hat dabei die in seinem Hoheitsgebiet niedergelassenen Anbieter durch ein „geeignetes System" zu beaufsichtigen. Für die Ausgestaltung dieses Aufsichtssystems hat die Richtlinie aber keine näheren Vorgaben gegeben, weshalb die Mitgliedstaaten sehr unterschiedliche Ansätze gewählt haben. Auch die Europäische Kommission hat kaum Aktivitäten gesetzt, um zu einer einheitlichen Umsetzung der Richtlinie beizutragen.

Neben dem verpflichtend einzuführenden Aufsichtssystem soll die Möglichkeit einer freiwilligen Akkreditierung zu einer Steigerung des Niveaus der erbrachten Zertifizierungsdienste abzielen. Auch hier gibt es keine nähere Beschreibung, wie das Akkreditierungsschema ausgestaltet sein sollte, weshalb die Mitgliedstaaten sehr unterschiedliche Lösungen realisiert haben. Einigkeit besteht in der europäischen Diskussion darüber, dass der Begriff der „Akkreditierung" unglücklich gewählt wurde, weil offenbar etwas anderes gemeint ist als bei der herkömmlichen Akkreditierung technischer Prüfstellen.

Die deutlichsten Unterschiede in der Umsetzung des Aufsichts- und Akkreditierungssystems sind erkennbar, wenn man Deutschland und Großbritannien vergleicht. Deutschland hat seine bestehenden, sehr ins technische Detail gehenden Regelungen weitestgehend beibehalten und sich darauf beschränkt, an die Stelle der Genehmigungspflicht den Begriff der freiwilligen Akkreditierung zu stellen. Da die Regelungen weiterhin so detailliert geblieben sind, haben es bislang fast alle deutschen Zertifizierungsdiensteanbieter

vorgezogen, sich freiwillig akkreditieren zu lassen. Die Akkreditierung bietet dem Anbieter eben Gewissheit, dass er alle Anforderungen erfüllt und die Behörde keine Aufsichtsmaßnahmen ergreifen wird. Großbritannien hingegen hat sich bemüht, die Richtlinie durch ein minimalistisches Aufsichtssystem umzusetzen. Das britische Wirtschaftsministerium führt eine Liste von Zertifizierungsdiensteanbietern und wartet darauf, dass sich jemand über deren Tätigkeit beschwert. So lange keine Beschwerden vorliegen, geht man davon aus, dass kein Bedarf an aufsichtsbehördlicher Tätigkeit gegeben ist. Die Akkreditierung wurde einem privaten Verein überlassen, der das Akkreditierungsschema tScheme betreibt.

Unterschiede in der Aufsicht sind auch darin erkennbar, wie die Aufsicht faktisch ausgeübt wird. In manchen Staaten (etwa in Österreich oder Deutschland) sieht die Aufsichtsstelle aufgrund des jeweiligen Verfahrensrechtes die Notwendigkeit, Zertifizierungsdiensteanbieter auch durch eigenes Personal oder durch beauftragte Gutachter vor Ort aufzusuchen und die Einrichtungen der Anbieter und ihre Dokumentation in Augenschein zu nehmen. In anderen Staaten (z. B. in Dänemark) hingegen wurde ein System gewählt, bei dem der Zertifizierungsdiensteanbieter selbst einen unabhängigen Gutachter auswählen kann, der in seinem Auftrag ein Gutachten erstellt, welches der Behörde vorgelegt wird. Dieses System ähnelt den in den meisten Staaten etablierten Systemen zur Prüfung der Bilanzen und Jahresabschlüsse von Unternehmen durch Wirtschaftsprüfer; die großen internationalen Wirtschaftsprüfungskanzleien haben daher auch Expertenwissen zur Überprüfung von Zertifizierungsdiensteanbietern aufgebaut.

Unterschiede bei der Akkreditierung bestehen darin, auf welchem Sicherheitsniveau eine Akkreditierung möglich ist. In Deutschland etwa entspricht eine Akkreditierung dem höchsten möglichen Sicherheitsniveau, der akkreditierte Anbieter muss noch höhere Anforderungen erfüllen als ein Anbieter, der seine Tätigkeit der Aufsichtsstelle bloß anzeigt. Auch in Österreich kann sich nur ein Anbieter akkreditieren lassen, der die höchstmögliche Sicherheit (qualifizierte Zertifikate für die sichere elektronische Signatur) anbietet, die Anforderungen für die Akkreditierung sind aber die gleichen wie die Anforderungen für die Anzeige (vgl. Abschnitt 1.2.1.2.5 und 2.1.4). Im Vergleich dazu ist etwa in Großbritannien eine Akkreditierung auch auf sehr niedrigem Niveau möglich[63]. Akkreditierung wird dort nicht als ein

63) Die zuständigen Stellen in Großbritannien lehnen den Begriff der „Akkreditierung" der Signaturrichtlinie überhaupt als irreführend ab und verwenden stattdessen den Begriff „Approval". Vgl. zu den einzelnen Möglichkeiten, von tScheme ein „Approval" zu erlangen, die Website von tScheme: https://www.tscheme.org/profiles/index_digest3.html.

besonderes Qualitätssiegel verstanden, sondern vor allem als eine Bestätigung, dass der Anbieter jene Anforderungen erfüllt, die er von sich selbst behauptet. Daher ist nicht bloß eine Akkreditierung für Anbieter qualifizierter Zertifikate möglich, sondern auch eine Akkreditierung von Anbietern einfacher Zertifikate, und sogar eine Akkreditierung von Systemen, die überhaupt nicht auf Zertifikaten und Signaturtechnologien basieren, sondern etwa auf der Eingabe von User-ID und Passwort.

4.2.1.3 Harmonisierte Anforderungen

In ihren Anhängen legt die Signaturrichtlinie die europaweit harmonisierten technischen und organisatorischen Anforderungen fest. Anhang I nennt die Mindestinhalte eines qualifizierten Zertifikates – unter anderem, dass es als solches zu kennzeichnen ist, den Namen und Sitzstaat des Ausstellers, den Namen des Zertifikatsinhabers (oder ein als solches zu kennzeichnendes Pseudonym), die Signaturprüfdaten (öffentliche Schlüssel) und die Gültigkeitsdauer. In Österreich wurde Anhang I der Signaturrichtlinie in § 5 SigG umgesetzt.

Anhang II enthält einen Katalog mit allen Anforderungen an Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen. Es handelt sich dabei um eine Liste mit zwölf Punkten, die sowohl organisatorische als auch technische Anforderungen umfasst. Beispielhaft seien genannt: Zuverlässigkeit des Anbieters, Identitätsprüfung nach dem jeweiligen Recht des Mitgliedstaates, Beschäftigung von Personal mit den erforderlichen Fachkenntnissen, Verwendung vertrauenswürdiger Produkte und Systeme mit der erforderlichen technischen und kryptografischen Sicherheit, ausreichende Finanzmittel, Aufzeichnung aller einschlägigen Informationen insbesondere für Gerichtsverfahren etc. Österreich hat Anhang II der Signaturrichtlinie in § 7 SigG übernommen.

Anhang III war bei den Beratungen der Signaturrichtlinie die umstrittenste Bestimmung; dieser Anhang beschreibt die „sichere Signaturerstellungseinheit". Die Bestimmung verlangt unter anderem, dass die Signaturerstellungsdaten praktisch nur einmal auftreten können und ihre Geheimhaltung gewährleistet ist, und dass der rechtmäßige Unterzeichner die Signaturerstellungsdaten vor der Verwendung durch andere verlässlich schützen kann. Weiters wird durch Punkt 2 des Anhangs verlangt, dass die sichere Signaturerstellungseinheit die zu unterzeichnenden Daten nicht verändert und nicht verhindert, dass die Daten dem Unterzeichner vor dem Signaturvorgang dargestellt werden. In fast allen Mitgliedstaaten der EU

wurde Anhang III so verstanden, dass damit die Anforderungen an Chipkarten oder vergleichbare Geräte geregelt werden. Die Chipkarte speichert und schützt die Signaturerstellungsdaten und sie verhindert nicht, dass die Daten vor der Signaturerstellung angezeigt werden. Österreich hat Anhang III weiter interpretiert und daraus auch das Erfordernis abgeleitet, dass die Signaturerstellungseinheit selbst dafür Sorge zu tragen hat, dass sich der Signator vor der Signaturerstellung die zu signierenden Daten anzeigen lassen kann (§ 18 SigG, § 7 SigV). In Österreich wird daher nicht bloß die Chipkarte als sichere Signaturerstellungseinheit verstanden, sondern die Chipkarte muss durch geeignete Software zur Anzeige („Secure Viewer") und im Regelfall auch durch einen geeigneten Chipkartenleser mit eigener PIN-Eingabe ergänzt werden (vgl. Kapitel 2.1.4).

Anhang IV ist nicht verpflichtend, sondern bloß eine Empfehlung, und regelt die sichere Signaturprüfung. Österreich hat den Anhang in § 18 Abs. 4 SigG übernommen, auch in Österreich handelt es sich nicht um verpflichtende Anforderungen.

4.2.1.4 Review der Signaturrichtlinie

In Art. 12 der Signaturrichtlinie ist vorgesehen, dass die Europäische Kommission eine Überprüfung der Durchführung der Richtlinie vornimmt und dem Europäischen Parlament und dem Rat insbesondere zur Frage, ob die Richtlinie geändert werden soll, Bericht erstattet. Zur Vorbereitung dieses Berichts hat die Europäische Kommission eine Studie in Auftrag gegeben, welche die rechtlichen und wirtschaftlichen Aspekte der Signaturrichtlinie erforschen sollte. Die umfangreiche Studie[64] wurde im Oktober 2003 veröffentlicht. Darin werden teilweise beträchtliche Unterschiede bei der Umsetzung der Signaturrichtlinie in das nationale Recht der Mitgliedstaaten festgestellt. Die Autoren empfehlen der Europäischen Kommission allerdings, die Signaturrichtlinie im Wesentlichen nicht zu verändern. Der Bericht der Europäischen Kommission wird für Anfang 2004 erwartet.

4.2.2 Signaturgesetze außerhalb der Europäischen Union

Außerhalb der Europäischen Union gibt es nur in wenigen Staaten eine ähnlich detaillierte Gesetzgebung zur elektronischen Signatur.

64) Dumortier, Jos; Kelm, Stefan; Nilsson, Hans, Skouma, Georgia; Van Eecke, Patrick: The Legal and Market Aspects of Electronic Signatures in Europe, Study for the European Commission within the eEurope 2005 Framework. Katholieke Universiteit Leuven, 2003, http://europa.eu.int/information_society/eeurope/2005/all_about/security/electronic_sig_report.pdf.

Da die Signaturrichtlinie auch in den Europäischen Wirtschaftsraum übernommen wurde, ist sie auch in den EWR-Staaten Norwegen, Island und Liechtenstein anzuwenden.

Grundsätzlich ist allen Signaturgesetzen gemeinsam, dass sie die elektronische Kommunikation fördern sollen und daher formale Hemmnisse der Verwendung elektronischer Signaturen abbauen. Daher haben alle Gesetze in der einen oder anderen Form eine Bestimmung, die den Beweiswert elektronisch signierter Dokumente anerkennt – etwa in der Form, dass einem Dokument nicht allein deshalb der Beweiswert abgesprochen werden darf, weil es elektronisch signiert ist. Dass die Signaturgesetze solche Regelungen aufweisen, liegt in der Natur der Sache. Ein Staat, der die elektronische Kommunikation nicht fördern will, würde kein Gesetz gegen die elektronische Signatur erlassen, sondern gar kein Signaturgesetz.

Deutliche Unterschiede in den Regelungsansätzen gibt es in der Frage, ob bzw. welche Sicherheitsbestimmungen für die elektronische Signatur (oder besondere Formen der elektronischen Signatur) vorgesehen werden und ob ein Aufsichtssystem für die Zertifizierungsdiensteanbieter eingerichtet wird.

Im Jahr 2001 hat die UNCITRAL[65] ein Modellgesetz für elektronische Signaturen beschlossen[66]. Das nur zwölf Artikel lange Modellgesetz bezieht sich auf elektronische Signaturen, die im Zusammenhang mit wirtschaftlichen Tätigkeiten verwendet werden. Konsumentenschutzbestimmungen sollten unberührt bleiben (Art. 1). Wie die Signaturrichtlinie verwendet auch das Modellgesetz technologieneutrale Begriffe („elektronische Signatur" statt „digitale Signatur"), stützt sich aber dann doch auf das Zertifikat und den Zertifizierungsdiensteanbieter (Art. 2). Das Modellgesetz sieht auch einige Sicherheitsbestimmungen und Anforderungen an Zertifizierungsdiensteanbieter vor, diese sind aber nicht ausdrücklich als Mindestkriterien formuliert wie in den Anhängen der Signaturrichtlinie. Vielmehr wird allgemein festgehalten, dass die elektronische Signatur so zuverlässig sein muss wie es für den Zweck, für den sie erstellt wurde, angemessen ist (Art. 6 Abs. 1). Die aufgezählten Anforderungen können dazu dienen, die Zuverlässigkeit zu beurteilen (Art. 10). Ein Aufsichtssystem wird nicht ausdrücklich verlangt, dies allenfalls einzurichten ist dem Staat überlassen, der das Modellgesetz umsetzt.

65) United Nations Commission on International Trade Law.
66) UNCITRAL Model Law on Electronic Signatures (2001), http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf.

In den Vereinigten Staaten haben einige Bundesstaaten Signaturgesetze erlassen, im Jahr 2000 wurde dann als bundesweites Gesetz der „Electronic Signatures in Global and National Commerce Act“[67] beschlossen. Dieses Gesetz ist völlig anders aufgebaut als die Signaturrichtlinie oder das UNCITRAL-Modellgesetz. Es gibt keine Definition der elektronischen Signatur, auch die Begriffe des Zertifikates oder des Zertifizierungsdiensteanbieters kommen im Gesetz nicht vor. Schon allein deshalb wird auch kein Aufsichtssystem vorgesehen. Technische Sicherheitsbestimmungen gibt es nicht, dafür eine Reihe von Konsumentenschutzregelungen. Dem Konsumenten muss insbesondere die Möglichkeit gewährt werden, zwischen elektronischer und nichtelektronischer Kommunikation zu wählen und er muss über eine Reihe von im Gesetz aufgezählten Informationen verfügen. In einer ziemlich kasuistischen Regelungstechnik stellt das Gesetz darüber hinaus für viele Einzelbereiche klar, dass die elektronische Kommunikation in diesen Bereichen möglich ist – allerdings werden dabei auch viele Ausnahmen gemacht.

Das japanische Signaturgesetz[68] ähnelt stärker dem europäischen Ansatz. Die Definition der elektronischen Signatur verweist beispielhaft auf kryptografische Methoden. Für Zertifizierungsdiensteanbieter wird ein Akkreditierungssystem eingerichtet, das auch ausländischen Zertifizierungsdiensteanbietern offen steht. Über die akkreditierten Zertifizierungsdiensteanbieter wird auch Aufsicht durch eine Aufsichtsbehörde ausgeübt.

4.3 Forum of European Supervisory Authorities for Electronic Signatures (FESA)

Aufgrund der allen europäischen Aufsichtsstellen gemeinsamen Problemstellungen haben sich die Aufsichtsstellen nach einigen Treffen im Sommer 2002 zu einer informellen Gruppe zusammengeschlossen, die sich etwa dreimal jährlich trifft und ansonsten über eine Mailingliste kommuniziert.

Die Mitgliedschaft in diesem Forum steht allen Aufsichts- und Akkreditierungsstellen offen, welche die europäische Signaturrichtlinie anzuwenden haben (werden), also sowohl den Stellen der EU- und EWR-Mitgliedsstaaten, als auch den Stellen der Beitrittskandidaten. Die Organisation der Treffen der Aufsichtsstelle wird von einem dreiköpfigen Board wahrgenommen, derzeit unter österreichischem Vorsitz.

67) 15 U.S.C. § 7001 et. seq., http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_bills&docid=f:s761enr.txt.pdf.
68) Eine nicht offizielle englische Übersetzung ist abrufbar unter http://www.soumu.go.jp/joho_tsusin/eng/Resources/Legislation/eSignLaw/eSignLaw.pdf.

Zum Zeitpunkt des Redaktionsschlusses dieses Berichts hatte FESA die in der Tabelle 2 aufgezeigten Mitglieder. Die Tabelle zeigt dabei jeweils auch, ob das Mitglied im jeweiligen Staat für Aufsicht, für Akkreditierung oder für beides zuständig ist. Die mit einem Stern gekennzeichneten Organisationen wurden ursprünglich als Telekom-Regulierungsbehörden gegründet und später mit Aufgaben betreffend die elektronische Signatur betraut.

Tabelle 2: Mitglieder von FESA

Staat	Name der Organisation	Aufsicht	Akkred.
AT	Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH)* Austrian Regulatory Authority for Broadcasting and Telecommunications	✔	✔
BE	Federal Public Service Economy, S.M.Es., Self-employed and Energy	✔	✔
CZ	Ministerstvo informatiky, Ministry of Informatics	✔	✔
DE	Regulierungsbehörde für Telekommunikation und Post (RegTP)* Regulatory Authority for Telecommunications and Posts	✔	✔
DK	IT- og Telestyrelsen*, National IT and Telecom Agency	✔	✘
ES	State Secretariat for Telecommunications and for the Information Society (SETSI). Ministry of Science and Technology (MCYT).	✔	✔
FI	Viestintävirasto* Finnish Communications Regulatory Authority (FICORA)	✔	✘
FR	Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) Central Directorate for Information and Network Security	✔	✘
FR	Ministère de l'Économie, des Finances et de l'Industrie Ministry of Economics, Finance and Industry	✘	✔
GB	Department of Trade and Industry	✔	✘
GR	National Telecommunications and Post Commission (EETT)*	✔	✔
HU	Hírközlési Felügyelet*, Communications Authority of Hungary	✔	✘
IS	Löggildingarstofa	✔	✘
IT	National Center for IT in the Public Administration (on behalf of Department for Innovation and Technologies)	✔	✔
NL	Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA)* Independent Post and Telecommunications Authority	✔	✘
NO	Post- og teletilsynet* Norwegian Post and Telecommunications Authority	✔	✘
SE	Post- och telestyrelsen*, National Post and Telecom Agency	✔	✘
SE	Styrelsen för ackreditering och teknisk kontroll Swedish Board for Accreditation and Conformity Assessment	✘	✔
SK	National Security Authority	✔	✔
TR	Telekomünikasyon Kurumu* Turkish Telecommunications Authority	✔	✔

Im Rahmen von FESA werden Fragen und Problemstellungen erörtert, die allen Aufsichtsstellen gemeinsam sind, insbesondere Auslegungsfragen der Richtlinien. Zu den dabei geklärten Fragen gehören die Folgenden:

- Nach der Signaturrichtlinie ist es grundsätzlich zulässig, dass ein Zertifizierungsdiensteanbieter grenzüberschreitend tätig wird, also z. B. seinen Sitz in einem Mitgliedsstaat hat, seine technischen Einrichtungen in einem anderen und dass er in mehreren verschiedenen Staaten Zertifikate ausstellt. Außerdem ist es möglich, dass ein Zertifizierungsdiensteanbieter für Einzelbereiche seiner Tätigkeit Subunternehmen einsetzt, die wiederum in einem anderen Mitgliedstaat ihren Sitz haben können. Für solche Fallkonstellationen, die auch bereits durchaus in der Praxis auftreten, wurde im Rahmen von FESA die gemeinsame Interpretation der Signaturrichtlinie gefunden, dass man sich in diesen Fällen für die Bestimmung der Zuständigkeit am Inhalt der Zertifikate orientieren wird. Nach Anhang I der Richtlinie muss im qualifizierten Zertifikat der Name des Ausstellers und der Staat, in dem er niedergelassen ist, angeführt werden. Der hier genannte Zertifizierungsdiensteanbieter wird für die Gesamtheit der Tätigkeit als verantwortlich angesehen und die Aufsichtsstelle in dem Staat, in dem er niedergelassen ist, ist nach ihrem jeweiligen Recht für die Aufsicht über die gesamte Tätigkeit des Zertifizierungsdiensteanbieters zuständig, auch wenn diese teilweise in anderen Mitgliedstaaten erbracht wird.
- Aus dieser Zuständigkeitsverteilung ergibt sich die Problemstellung, dass Aufsichtsstellen für Tätigkeiten von Zertifizierungsdiensteanbietern in anderen Mitgliedstaaten zuständig sein können, aber aus völkerrechtlichen Erwägungen nicht selbst in diesen Staaten aufsichtsbehördlich tätig sein können bzw. auch kein eigenes Personal oder selbst beauftragte Gutachter für Ermittlungsmaßnahmen oder Aufsichtsmaßnahmen in den anderen Staat entsenden können. Auch diese Problemstellung wurde und wird im Rahmen von FESA erörtert.
- Nach der Signaturrichtlinie müssen nur Zertifizierungsdiensteanbieter beaufsichtigt werden, die „öffentlich qualifizierte Zertifikate ausstellen" (englisch: „to the public"). In Österreich wurde dies z. B. so umgesetzt, dass das SigG auf „geschlossene Systeme" keine Anwendung findet (§ 1 Abs. 2 SigG). Im Rahmen von FESA wurden gemeinsame Kriterien entwickelt, wie man geschlossene Systeme von einem Angebot von Zertifikaten für die Öffentlichkeit unterscheidet.

- Die Mitgliedstaaten haben innerstaatlich unterschiedliche Anforderungen an die Identitätsprüfung vor der Ausstellung qualifizierter Zertifikate gestellt, wobei viele Staaten nicht ins Detail gegangen sind. Insbesondere ist in vielen Staaten ungeregelt geblieben, ob es zulässig ist, dass die Identitätsprüfung nicht unmittelbar im Zuge der Ausstellung des Zertifikates erfolgt, sondern dass auf eine zuvor erfolgte Identitätsprüfung zurückgegriffen werden kann. Darf etwa eine Bank, die bereits vor Jahren bei der Kontoeröffnung die Identität des Kunden geprüft hat und seither eine bestehende Kontoverbindung mit dem Kunden hat, diesem Kunden ein qualifiziertes Zertifikat ausstellen, ohne dass der Kunde nochmals mit einem Ausweis in einer Filiale erscheinen muss? In den Diskussionen im Rahmen von FESA hat sich herausgestellt, dass dies von den meisten Aufsichtsstellen als zulässig angesehen würde, wenn ein geeignetes Verfahren etabliert werden kann, durch welches die Bank sicherstellt, dass das Zertifikat nun tatsächlich der Person ausgestellt wird, deren Identität vor einigen Jahren überprüft wurde.
- Für den Review der Signaturrichtlinie (vgl. Abschnitt 4.2.1.4) wurde im Rahmen von FESA eine Liste von wichtigen Themen erarbeitet, die nach Ansicht der Mitglieder bei der Überarbeitung der Richtlinie bedacht werden sollen. Dieses Dokument[69] wurde von 16 FESA-Mitgliedern unterstützt und Anfang Juli 2003 an die Europäische Kommission und das von der Kommission beauftragte Projektteam zur Erarbeitung einer Studie zur Vorbereitung des Review übersandt.

69) Important Topics for the Review of Directive 1999/93/EC from the Supervisory Authorities' Point of View, http://www.fesa.rtr.at/documents.html.

Glossar

Akkreditierung	Siehe Abschnitte 2.1.4 und 4.2.1.2 sowie § 17 SigG.
Anbieter	In diesem Bericht als Kurzform für → Zertifizierungsdiensteanbieter verwendet.
ANSI	American National Standards Institute, http://www.ansi.org/, vgl. Abschnitt 4.1.7.
Aufsichtsstelle	Eine gemäß Art. 3 Abs. 3 der → Signaturrichtlinie eingerichtete Behörde, die die Aufsicht über Zertifizierungsdiensteanbieter wahrnimmt. In Österreich ist gemäß § 13 → SigG die Telekom-Control-Kommission (TKK) Aufsichtsstelle für elektronische Signaturen, siehe Abschnitt 1.2.1.2.5.
Bestätigungsstelle	Eine gemäß Art. 3 Abs. 4 der → Signaturrichtlinie eingerichtete Stelle, die die Übereinstimmung → sicherer Signaturerstellungseinheiten mit Anhang III der Richtlinie feststellt. In Österreich werden Bestätigungsstellen gemäß § 19 → SigG durch Verordnung als solche anerkannt, siehe Abschnitt 1.2.3.
CEN	Comité Européen de Normalisation, Europäisches Komitee für Normung, http://www.cenorm.be/, vgl. Abschnitt 4.1.5.3.
Certification Authority (CA)	Dieser Begriff wird meist verwendet, um jene technische Einrichtung zu beschreiben, mittels der Zertifikate ausgestellt und verwaltet werden. Ein → Zertifizierungsdiensteanbieter betreibt eine oder mehrere Certification Authorities (Zertifizierungsstellen).

Certificate Policy (CP)	Ein Teil des → Sicherheits- und Zertifizierungskonzepts, in welchem die Regeln für die Ausstellung einer bestimmten Klasse von → Zertifikaten veröffentlicht werden (siehe → RFC 2527, Punkt 3.1).
Certification Practice Statement (CPS)	Ein Teil des → Sicherheits- und Zertifizierungskonzepts, in welchem ein → Zertifizierungsdiensteanbieter darlegt, wie er bei der Ausstellung von → Zertifikaten vorgeht (siehe → RFC 2527, Punkt 3.5).
Common Criteria	Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik, siehe Abschnitt 4.1.1.7.
CP	→ Certificate Policy
CPS	→ Certification Practice Statement
CRL	Certificate Revocation List, → Widerrufsliste
Cross-Zertifizierung	Die Ausstellung von Zertifikaten durch → Zertifizierungsdiensteanbieter für andere Zertifizierungsdiensteanbieter.
Dienst	In diesem Bericht als Kurzform für → Zertifizierungsdienst verwendet.
EESSI	European Electronic Signature Standardization Initiative, http://www.ict.etsi.fr/EESSI_home.htm, vgl. Abschnitt 4.1.5.
Einwegfunktion	siehe Abschnitt 1.1.1
ETSI	European Telecommunications Standards Institute, http://www.etsi.org/, vgl. Abschnitt 4.1.5.2
FESA	Forum of European Supervisory Authorities for Electronic Signatures, siehe Abschnitt 4.3

Hashverfahren	siehe Abschnitt 1.1.2
Hardware Security Module (HSM)	Spezielle Hardware, welche beim → Zertifizierungsdiensteanbieter für sicherheitsrelevante Aufgaben wie z. B. die Speicherung von → privaten Schlüsseln und die Signaturerstellung eingesetzt wird, vgl. Abschnitte 1.1.6 und 3.2.4.
IEEE	Institute of Electrical and Electronics Engineers, http://www.ieee.org/, vgl. Abschnitt 4.1.4.
IETF	Internet Engineering Task Force, http://ietf.org/, vgl. Abschnitt 4.1.3.
ISO	International Organization for Standardization, http://www.iso.org/, vgl. Abschnitt 4.1.1.
ITSEC	Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik, siehe Abschnitt 4.1.8.
ITU	International Telecommunication Union, http://www.itu.int/, vgl. Abschnitt 4.1.1.
KeyUsage	Ein Attribut von → X.509v3-Zertifikaten, das ausdrückt, für welchen Verwendungszweck das Zertifikat gewidmet ist, → vgl. RFC 3280, Punkt 4.2.1.3.
NIST	National Institute of Standards and Technology, http://www.nist.gov/, vgl. Abschnitt 4.1.6.
Object Identifier (OID)	Objektkennung. Ein eindeutiger Name für ein Informationsobjekt, der aus einer Folge von ganzen, nicht negativen Zahlen besteht.

öffentlicher Schlüssel	Jener Teil des Schlüsselpaares eines asymmetrischen kryptografischen Verfahrens, welcher (z. B. in einem → Zertifikat) veröffentlicht und zur Signaturprüfung verwendet wird, siehe Abschnitt 1.1.1. Vgl. auch → Signaturprüfdaten
Padding	siehe Abschnitt 1.1.2
PCA	→ Policy Certification Authority
PKCS	Public-Key Cryptography Standards, siehe Abschnitt 4.1.2.
PKI	→ Public-Key-Infrastruktur
PKIX	Eine Arbeitsgruppe innerhalb der → IETF, die an Standards im Bereich „Public-Key Infrastructure (X.509)“ arbeitet, vgl. Abschnitt 4.1.3.1.
Policy Certification Authority (PCA)	Eine → Certification Authority, die nicht dazu dient, Zertifikate an Endkunden auszustellen, sondern Zertifikate an andere → Certification Authorities ausstellt. Durch den Einsatz verschiedener PCAs können z. B. verschiedene Zertifikatsklassen unterschieden werden.
privater Schlüssel	Jener Teil des Schlüsselpaares eines asymmetrischen kryptografischen Verfahrens, welcher geheimgehalten und z. B. zur Erstellung von Signaturen verwendet wird, siehe Abschnitt 1.1.1. Vgl. auch → Signaturerstellungsdaten.
Public-Key-Infrastruktur (PKI)	Das technische Umfeld, in welchem mittels asymmetrischer Kryptografie gesicherte Kommunikation möglich ist. Der Begriff umfasst → Zertifizierungsstellen und → Registrierungsstellen bzw. → Zertifizierungsdiensteanbieter, die Inhaber von → Zertifikaten sowie die eingesetzte Hardware und Software. Innerhalb der PKI ist z. B. der Austausch digital signierter Nachrichten möglich.

qualifiziertes Zertifikat	siehe → Zertifikat, qualifiziertes
Registrierungsstelle	Jene Einrichtung, welche die Identität des → Zertifikatswerbers überprüft. Ein → Zertifizierungsdiensteanbieter betreibt in der Regel eine oder mehrere Registrierungsstellen oder beauftragt andere Unternehmen, die unter seiner Verantwortung als Registrierungsstellen tätig sind.
RFC	Request for Comments, Standardisierungsdokumente des → IETF, siehe Abschnitt 4.1.3.
RSA	Ein asymmetrisches kryptografisches Verfahren, mit welchem – in Kombination mit einem Hashverfahren – elektronische Signaturen erstellt werden können, vgl. Abschnitte 1.1.1, 4.1.2.1, 4.1.7.3.
Schlüsselpaar	In einer → Public-Key-Infrastruktur hat jeder Teilnehmer ein Schlüsselpaar, bestehend aus einem → öffentlichen Schlüssel und einem → privaten Schlüssel. Der private Schlüssel wird geheimgehalten und z. B. für die Erstellung von Signaturen verwendet. Der öffentliche Schlüssel dient der Signaturprüfung. Vgl. Abschnitt 1.1.1.
Schlüssel, öffentlicher	siehe → öffentlicher Schlüssel
Schlüssel, privater	siehe → privater Schlüssel
Secure Viewer	Software zur sicheren Anzeige der zu signierenden Daten vor der Signaturerstellung, vgl. Abschnitte 2.1.4 und 3.2.3.
Sicherheits- und Zertifizierungskonzept	Eine Sammlung von Dokumenten, nach denen ein Zertifizierungsdiensteanbieter bei der Ausstellung von Zertifikaten vorgeht. Das Sicherheits- und Zertifizierungskonzept umfasst Teile, die vom Anbieter veröffentlicht werden und Teile, die er nur intern verwendet oder der Aufsichtsstelle zugänglich macht. Vgl. § 15 → SigV.

SigG	Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG), vgl. Abschnitt 1.2.1.
Signaturerstellungs-daten	Einmalige Daten wie Codes oder private Signaturschlüssel, die vom Signator zur Erstellung einer elektronischen Signatur verwendet werden (§ 2 Z 4 → SigG), siehe auch Abschnitt 1.1.1. Vgl. → privater Schlüssel.
Signaturerstellungs-einheit, sichere	Eine Signaturerstellungseinheit, welche die Anforderungen des Anhangs III der → Signaturrichtlinie erfüllt, vgl. die Abschnitte 1.1.6, 1.2.1.2.3 und 3.2.1.
Signaturprüfdaten	Daten wie Codes oder öffentliche Signaturschlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden (§ 2 Z 6 → SigG), siehe auch Abschnitt 1.1.1. Vgl. → öffentlicher Schlüssel.
Signaturrichtlinie	Richtlinie 1999/93/EG des Europäischen Parlamentes und des Rates vom 13.12.1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. L 13 vom 19.01.2000, S. 12, vgl. Abschnitt 4.2.1.
SigV	Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung – SigV), vgl. Abschnitt 1.2.2.
URL	Uniform Ressource Locator. Die Adresse einer Ressource im Internet, z. B. http://...
W3C	World Wide Web Consortium, http://www.w3.org/, vgl. Abschnitt 4.1.3.

Widerrufsliste	(Certificate Revocation List, CRL) Eine Liste, auf der die Seriennummern gesperrter oder widerrufener Zertifikate veröffentlicht werden, siehe Abschnitte 4.1.1.2 und 4.1.3.1.
X.509	Ein Standard für die Codierung von Zertifikaten und Widerrufslisten, siehe Abschnitte 4.1.1.2 und 4.1.3.1.
Zertifikat	Eine elektronische Bescheinigung, mit der → Signaturprüfdaten einer bestimmten Person zugeordnet werden und deren Identität bestätigt wird (→ § 2 Z 8 SigG), siehe Abschnitt 1.1.3.
Zertifikat, qualifiziertes	Ein → Zertifikat, das die Angaben des § 5 → SigG enthält und von einem den Anforderungen des § 7 → SigG entsprechenden Zertifizierungsdiensteanbieter ausgestellt wird, siehe Abschnitte 1.1.3 und 1.2.1.2.4.
Zertifizierungsdienst	Ausstellung, Erneuerung, Verwaltung und Widerruf von Zertifikaten (vgl. auch die Definition in § 2 Z 11 → SigG). Ein → Zertifizierungsdiensteanbieter kann mehrere Zertifizierungsdienste unterschiedlicher Qualität betreiben.
Zertifizierungsdiensteanbieter	Eine natürliche oder juristische Person oder eine sonstige rechtsfähige Einrichtung, die Zertifikate ausstellt oder andere Signatur- und Zertifizierungsdienste erbringt (§ 2 Z 10 → SigG).
Zertifizierungshierarchie	Zertifikate können auch an Zertifizierungsstellen ausgestellt werden, die ihrerseits weitere Zertifikate ausstellen. Auf diese Weise kann eine Hierarchie gebildet werden, wie sie beispielsweise in → Abschnitt 2.2.5 beschrieben ist.

Zertifizierungsstelle	Auch: Certification Authority (CA). Dieser Begriff wird meist verwendet, um jene technische Einrichtung zu beschreiben, mittels der Zertifikate ausgestellt und verwaltet werden. Ein → Zertifizierungsdiensteanbieter betreibt eine oder mehrere Certification Authorities (Zertifizierungsstellen).
Zufallszahlen	Zufallszahlen stellen eine wesentliche Voraussetzung für die Sicherheit von → Signaturerstellungsdaten und anderer bei Signaturverfahren eingesetzter Parameter dar. Man unterscheidet echte Zufallszahlen und Pseudozufallszahlen, siehe Abschnitt 1.1.4.

Verzeichnisse

Abbildungen

Tabellen

Impressum:

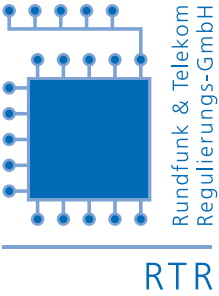
Schriftenreihe der Rundfunk und Telekom Regulierungs-GmbH
Band 1/2004: 4 Jahre Signaturgesetz

Medieninhaber (Verleger), Herausgeber und Redaktion:
Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH)
A-1060 Wien, Mariahilfer Straße 77–79
E-Mail: rtr@rtr.at; Internet: http://www.rtr.at

Grafische Konzeption:
Satz & Graphik Ges.m.b.H., A-1140 Wien, Linzer Straße 383

Druck:
AV-Druck Plus GmbH., A-1032 Wien, Faradaygasse 6

Verlags- und Herstellungsort: Wien
Einzelverkaufspreis: EUR 10


Rundfunk & Telekom
Regulierungs-GmbH
RTR