I. Elektronische Signaturen

Elektronische Signaturen dienen dazu, die traditionelle handschriftliche Unterschrift durch eine elektronische Form zu ersetzen. In diesem Abschnitt wird das österreichische Signaturgesetz (SigG), welches in Durchführung der Signatur-Richtlinie (SigRL) der Europäischen Union beschlossen wurde, behandelt. Neben den verschiedenen rechtlichen Aspekten wird einerseits besprochen, worauf sich diese Vorschriften genau beziehen, andererseits, welche Rechtsfolgen sich aus qualifizierten elektronischen Signaturen ergeben. Augenmerk wird weiters auf die Akkreditierung gelegt, mit der ein Anbieter von Zertifizierungsdiensten (ZDA) eine besonders überprüfte Qualität nachweisen kann. Im Jahre 2008 wurde eine starke Vereinfachung (Das SigG ist nur mehr auf Zertifizierungsdiensteanbieter anzuwenden, die qualifizierte Zertifikate ausstellen oder qualifizierte Zeitstempeldienste anbieten[1]) und Anpassung der Terminologie an die EU-RL vorgenommen (wie in der RL heißt es nun "qualifizierte" anstatt "sichere" Signaturen – Nicht-qualifizierte Signaturen waren ja nicht notwendigerweise unsicher!). Zum Abschluss wird kurz der Electronic Signatures Act aus den USA besprochen.

Die rechtliche Anerkennung von Signaturen ist im E-Business deshalb wichtig, da nur dann die sichere Beweisbarkeit von Forderungen, beispielsweise aus Kaufverträgen, gegeben ist[2]. Weiters ermöglichen sie die sichere Erkennung des Geschäftsinhabers über dessen Zertifikat, was dazu beiträgt, das Vertrauen der Konsumenten zu erhöhen und damit den el. Handel fördert. Dies ist insbesondere ein Anliegen der Europäischen Union, da auf diese Weise der freie Waren- und Dienstleistungsverkehr verstärkt wird. Deshalb wurde auch eine Signatur-Richtlinie geschaffen, sodass in der gesamten EU einheitliche Regelungen bestehen, Signaturen gegenseitig anerkannt werden, und grenzüberschreitende Transaktionen mit ihnen problemlos möglich sind. In der Praxis ist jedoch zu beobachten, dass el. Signaturen bzw. Zertifikate praktisch fast nirgends eingesetzt werden um rechtlich eine Unterschrift zu ersetzen, hingegen sehr oft um technisch eine höhere Sicherheit zu gewährleisten.

Zwei weitere Aspekte sind zwar allgemein von großer Bedeutung, werden hier aber nicht besprochen: Die el. Rechnung, welche in bestimmten Fällen ebenfalls el. Signaturen voraussetzt, sowie der Einsatz von Signaturen im Verwaltungsbereich. Letzterer betrifft sowohl den el. Rechtsverkehr als auch interne Verwaltungsvorgänge sowie den Zugang von Personen zu Verwaltungsprozessen[3] (Stichwort Bürgerkarte, welche auch als Träger für ein qualifiziertes Zertifikat dient).

---

[1] Für alle anderen ZDA gelten lediglich die Genehmigungsfreiheit, die Datenschutzvorschriften und die Anerkennung ausländischer Zertifikate: § 1 Abs 3 SigG

[2] Der Beweiswert von E-Mails oder Logs von WWW-Formularen alleine ist äußerst gering (anders im Zusammenhang mit bei Dritten gespeicherten Daten, z.B. E-Mail Server Logs beim Provider!). Dies sollte jedoch nicht darüber hinwegtäuschen, dass in der Praxis anscheinend nur sehr wenige Probleme durch diesen "Mangel" auftreten!

[3] Etwa die elektronische Abgabe der Steuererklärung nach der Identifizierung mit der Bürgerkarte oder auch den Datenverkehr von Unternehmen mit der Krankenversicherung.

I.1. Einleitung

Elektronische Signaturen sollen es ermöglichen, dass Dokumente nicht nur in physischer Form sondern auch elektronisch unterschrieben (=signiert) werden können. Dadurch ist es möglich, die Beweisbarkeit von Rechtsgeschäften zu verbessern, insbesondere im Hinblick auf Geschäfte mit hohem Transaktionswert und damit hohem Sicherheitsbedürfnis. Grundsätzlich kann nach der SigRL jedes Rechtsgeschäft, welches die einfache Schriftform (=Unterschrift) erfordert, nun auch el. abgeschlossen werden. Solche Formvorschriften sind jedoch zumindest in Österreich selten. Meist ist die Unterschrift eine freiwillige Form der "Bekräftigung" mit dem einzigen Zweck der Beweiserleichterung, da mündliche Verträge zwar fast überall möglich und gültig sind, aber nur schwer bewiesen werden können.

Höherwertige Formen (notarielle Beurkundung, Notariatsakt, gerichtliche Beglaubigung, ...) sind inzwischen ebenso erfasst und können in Zusammenwirkung mit der entsprechenden Stelle durch eine doppelte el. Signatur erfolgen: Vom eigentlichen Signator und z.B. dem Notar ("elektronischer Notariatsakt"). Meist ist noch eine zusätzliche Belehrung/Information des Signators erforderlich. Mit dieser Möglichkeit soll insbesondere auch die Einrichtung eines Urkunden-Archivs für elektronische Daten ermöglicht werden.

El. Signaturen ähneln sehr stark physischen Unterschriften, doch existiert ein besonderer Unterschied: Sie besitzen ein "Ablaufdatum". Durch den technischen Fortschritt ist eine Signatur, die heute noch unfälschbar ist, in einigen Jahren wahrscheinlich ohne großen Aufwand zu brechen und damit fälschbar. Als Konsequenz ist zwar der dadurch beurkundete Rechtsakt weiterhin gültig, doch der Beweis hierüber geht verloren. Da Unterschriften mit rechtlicher Bedeutung aber oft sehr lange gültig sein müssen (3-40 Jahre Verjährungsfrist![4]), kann es notwendig sein, später eine erneute (Nach-)Signierung durchzuführen. Dies hat aber natürlich nur dann einen Sinn, wenn mit der Nachsignierung ein Zeitstempel einer unabhängigen Instanz, meist eines Zertifizierungsdiensteanbieters (ZDA), verbunden ist, der den tatsächlichen Zeitpunkt der Nachsignierung bzw. Vorlage bestätigt. Die Nachsignierung oder das Versehen mit einem Zeitstempel und damit der Nachweis der Existenz und Korrektheit zu einem bestimmten Zeitpunkt muss natürlich innerhalb des Gültigkeitszeitraums der ursprünglichen Signatur liegen[5].

In geschlossenen Gruppen, z.B. firmenintern oder bei dauernder Geschäftsverbindung, können beliebige Signaturen und Verfahren verwendet werden. Diese werden auch rechtlich anerkannt, sofern sie die entsprechenden Eigenschaften erfüllen und besitzen dann Beweiswert vor Gericht. Dessen Ausmaß ist jedoch an Hand der Technik, der Sicherheitsvorkehrungen etc. individuell zu beurteilen. Es kann daher im gegenseitigen Übereinkommen jederzeit eine andere el. Signatur vereinbart und verwendet werden.

Wichtig ist zu bemerken, dass durch das Signaturgesetz *nicht* die allgemeine Zulässigkeit el. Kommunikation mit irgendjemandem, insbesondere nicht mit Behörden, festgelegt wird. In diesem Bereich ergeben sich durch eine Signatur keinerlei Änderungen. Wenn allerdings el. Kommunikation bzw. Einbringung von Anträgen akzeptiert wird, dann ermöglichen Signaturen eine besondere *Qualität* der Eingaben und daher ev. einen größeren Anwendungsbereich. Im Gegenzug ist es aber so, dass ohne Signaturen el. Kommunikation

[4] Siehe § 11 SigG zur Dokumentationspflicht der ZDA: Die Dokumentation von Ausstellung, Sperre und Widerruf eines qualifizierten Zertifikates ist bis zum Ablauf der allgemeinen Verjährungszeit aufzubewahren, d.h. für 30 Jahre, gerechnet ab dem Ende des Gültigkeitszeitraums des Zertifikats (= letztem möglichen Nutzungszeitpunkt).

[5] Eine Belehrung darüber war früher beim Vertragsabschluss mit dem ZDA erforderlich, fiel aber inzwischen weg!

immer eine unsichere und daher seltene Ausnahme bleiben könnte. Praktisch werden von Behörden derzeit jedoch vielfach elektronische Eingaben ohne jegliche Unterschrift/Signatur akzeptiert, z.B. per Fax oder E-Mail. Nur wenn Fragen der Gültigkeit auftauchen ist eine schriftliche Version im Nachhinein vorzulegen: Auf Papier oder el. signiert. Grundsätzlich wird davon ausgegangen, dass qual. Signaturen, soweit el. Kommunikation vorgesehen ist, auch für den Verkehr mit Behörden sicher genug sind. In besonders zu begründenden Fällen könnten jedoch auch besondere Vorkehrungen gefordert werden, so etwa nur Signaturen, die auf Chipkarten mit Fingerabdruck zur Autorisierung basieren und keine "rein" el. Signaturen. Zur Zeit sind jedoch keine solchen Zusatzerfordernisse vorgesehen, sondern es wurden eher Reduktionen der Anforderungen eingebaut.

In der SigRL ist explizit festgelegt, dass die Aufnahme des Betriebes eines Zertifizierungsdiensteanbieters für qual. Zertifikate nicht von einer Genehmigung abhängig gemacht werden darf, d.h. ein Konzessionssystem verboten ist. Werden die Vorschriften erfüllt, was im Laufe der Zeit und wiederholt überprüft wird, so kann sofort mit der Tätigkeit begonnen werden. Hierdurch wird eine Mindestqualität garantiert, die jedoch bei Betriebsbeginn noch nicht unbedingt tatsächlich gegeben sein muss, auch wenn sie es rechtlich gesehen sein müsste. Um daher das Vertrauen der Konsumenten zu erhöhen, steht es einem Anbieter frei, sich einer besonderen Prüfung, genannt Akkreditierung, zu unterziehen, wodurch von staatlicher Seite aus eine *besondere* Qualität bestätigt wird. Inhaltlich ist diese Qualität jedoch nichts Außergewöhnliches, da es sich *ausschließlich* um die ohnehin gesetzlich für alle vorgeschriebene handelt! Dies darf jedoch nicht verpflichtend vorgesehen sein und auch zu keiner Wettbewerbsverzerrung führen.

I.1.1. Anforderungen an eine elektronische Unterschrift

Handschriftliche Unterschriften entsprechen meistens den unten angeführten Anforderungen. Eine äquivalente Unterschrift auf elektronischem Wege muss, bzw. soll, alle diese Punkte ebenso erfüllen. In vielen Fällen der Praxis ist jedoch ein el. Unterschrift sogar sicherer als eine konventionelle[6]! Eine „Unterschrift“ muss folgende Punkte erfüllen:

- *Personenabhängigkeit:* Die Unterschrift ist eindeutig mit einer bestimmten Person verbunden, welcher der Inhalt deshalb zugerechnet wird (=Zuordnung zu einem bestimmten Namen). Die Unterschrift ist also "lesbar", wodurch der, allerdings ebenso wie auf Papier (Lesbarkeit!) nicht unbedingt eindeutige[7], Name herausgefunden werden kann.
- *Dokumentenabhängigkeit:* Die Unterschrift ist untrennbar mit dem Dokument verbunden und kann nicht auf ein anderes übertragen werden (=kein Ausschneiden und Aufkleben bzw. kopieren; Computerfaxe!). Vergleiche hierzu früher verwendete Siegel[8]!
- *Überprüfbarkeit:* Die Unterschrift kann durch jeden überprüft werden, insbesondere, ob sie von einer bestimmten Person stammt oder nicht. Diese Eigenschaft ist handschriftlich sehr selten: Wer hat schon Referenzunterschriften und kann gut verstellte Unterschriften erkennen! El. ist dies über das Zertifikat und Widerrufslisten relativ einfach.

---

[6] Siehe z.B. die Überprüfbarkeit: Welcher Versandhändler besitzt Referenzunterschriften von Erstkunden?

[7] Beispiel: Es unterschreibt "Johann Müller". In Wien existieren 28, österreichweit ca. 250 Personen dieses Namens. Bei einer el. Signatur wird hingegen zwischen allen diesen eindeutig unterschieden (Seriennummer des Zertifikats).

[8] "Offizielles" Beispiel: Das Privilegium Maius, bei welchem das kaiserliche Siegel von einer älteren Urkunde (Privilegium Minus) entfernt und an dieser Fälschung angebracht wurde. Thomas, C.: Privilegium maius (1358/1359) als Erweiterung des Privilegium minus, 1156 September 17 http://www.uni-klu.ac.at/kultdoku/kataloge/20/html/1818.htm

- *Fälschungssicherheit:* Die Unterschrift kann nur durch eine einzige Person erzeugt werden. Fälschungen sind daher unmöglich, genauso wie der echte Unterzeichner nicht abstreiten kann, selbst unterschrieben zu haben (=auf Papier nur durch Experten möglich). El. kann dies durch Geheimhalten der Signaturerstellungsdaten[9] bzw. Beschränkung des Zugriffs darauf realisiert werden.
- *Dokumentenechtheit:* Das Dokument kann nach der Unterschrift nicht mehr verändert werden. Die Unterschrift bildet einen Abschluss des Dokumentes. Auf Papier sind hierzu besondere Formatierungsrichtlinien einzuhalten; siehe das besondere Aussehen von Notariatsurkunden. Elektronisch ist die Dokumentenechtheit ein automatisches Nebenprodukt der Signatur; beachte jedoch die Kollisionsproblematik bei Hashfunktionen.

I.2. Begriffsbestimmungen

In diesem Abschnitt werden die im Folgenden verwendeten Begriffe definiert, und zwar wie sie nach der SigRL bzw. dem SigG zu verstehen sind. Diese Definitionen können sich von technischen Definitionen unterscheiden und dienen einer einheitlichen Auslegung. Zu beachten ist, dass das SigG inzwischen nur mehr für Anbieter qual. Zertifikate/Zeitstempeldienste gilt. Für alle anderen ZDA gelten nur die § 6 Abs 1 (Keine Genehmigung erforderlich), 22 (Datenschutz) sowie 24 (Annerkennung ausländ. Zertifikate).

Zusätzlich zu den hier besprochenen einfachen, fortgeschrittenen und qualifizierten Signaturen existieren noch weitere Varianten. Eine davon ist die Amtssignatur[10], welche eine fortgeschrittene Signatur mit einer besonderen Kennzeichnung (Attribut) im Zertifikat ist und die ausschließlich im öffentlichen Bereich verwendet wird. Es handelt sich daher hierbei nicht um eine technische sondern eine organisatorische Bezeichnung. Amtssignaturen werden für Bescheide/Erledigungen verwendet, um kenntlich zu machen, dass es sich um amtliche Schriftstücke in elektronischer Form handelt.

I.2.1. Elektronische Signatur

Eine Definition ist in § 2 Z 1 SigG und in Art 2 Z 1 SigRL enthalten.

Eine elektronische Signatur sind elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Authentifizierung dienen.

Die Beschränkung auf elektronische Daten hat den Grund, dass ein Ausdruck auf Papier unter Umständen nicht mehr unverändert in die Originaldaten zurückgewandelt werden kann: Nicht-druckbare Zeichen, Zeilenumbrüche, Elemente der Codierung, redundante Elemente in den Daten, die beim Ausdruck wegfallen etc. Dies würde dazu führen, dass originale signierte Daten ohne Veränderung des Inhalts als unecht angesehen werden könnten. Selbst wenn eine unverwechselbare Codierung vorliegt, z.B. durch Ausdruck als Byte-Codes, kann nicht mehr von einer "elektronischen" Signatur gesprochen werden, obwohl dann eine solche wiederhergestellt werden kann (wie z.B. bei manchen Amtssignaturen).

[9] In der Praxis: Des Passwortes oder PIN-Codes das den Zugang zum privaten Schlüssel ermöglicht. Genau hier besteht meist das größte Sicherheitsproblem von el. Signaturen.

[10] § 19 E-Government-Gesetz. Eine durchgeführte Signatur enthält nicht nur die mathematischen Daten sondern auch eine Bildmarke, die meist einem Rundstempel nachgebildet ist. Die Signatur kann u.U. selbst bei ausgedruckten Dokumenten noch überprüft werden, sodass derartige Ausdrucke dann ebenfalls voll gültig sind (§ 20 E-Government-Gesetz): Beweiskraft einer öffentlichen Urkunde. Siehe dazu auch http://www.digitales.oesterreich.gv.at/site/5318/default.aspx

Diese Bedingung ist hier noch nicht besonders wichtig, wenn auch für den Geltungsbereich des Gesetzes sinnvoll. Bei qualifizierten Signaturen ist sie jedoch eine unbedingt notwendige Voraussetzung.

Die "Beifügung" entspricht einer externen Signierung (=Verlängerung des Textes), während die "logische Verknüpfung" auf eine Signierung ohne Verlängerung hinweist (interne Signatur). Bei der zweiten Variante werden die gesamten Daten mit dem privaten Teil des Schlüssels verschlüsselt. Der Nachteil dieses Verfahrens ist, dass immer eine Entschlüsselung nötig ist, um den (Klar-) Text zu erhalten. Bei externer Signierung kann die Prüfung auf Zweifelsfälle beschränkt werden.

Da die Daten der Identifizierung des Signators (siehe I.2.2) dienen, ist es mit einer (technischen) Signatur alleine nicht getan: Es muss u.U. auch ein Zertifikat beigefügt werden, aus welchem dann die Identität feststellbar ist, wenn auch nicht unbedingt der Name, so etwa bei Pseudonymen. Dieses Zertifikat ermöglicht weiters die Prüfung der Signatur bzw. die Entschlüsselung des Textes. Alternativ würde dem Gesetzestext ein eindeutiger Hinweis entsprechen, welches Zertifikat zu verwenden ist. Dieser Vermerk hat jedoch allgemein verständlich zu sein, sodass potentiell jeder dieses Zertifikat ausheben kann. Achtung: Qualifizierte Zertifikate sind nur mit Zustimmung des Inhabers öffentlich abrufbar: § 7 Abs 2 SigG. Bei "geheimen" Zertifikaten ist daher eine Einbettung erforderlich, um dem Empfänger die Prüfung zu ermöglichen. Fehlt das Zertifikat ist die Signatur dennoch gültig, auch wenn sie für Empfänger nicht überprüfbar ist und diese sie daher ablehnen würden. Gerichte und Behörden können diese Veröffentlichungs-Einschränkung umgehen und sind immer in der Lage, das notwendige Zertifikat zu erlangen: § 22 Abs 2, 3 SigG.

Es muss sich bei einer einfachen el. Signatur nicht unbedingt um Kryptographie und Zertifikate handeln, sondern auch eine rein textuelle Angabe des Namens des Signators erfüllt die Anforderungen an eine *einfache* el. Signatur, natürlich dann nur mit äußerst geringer Sicherheit und keinen besonderen Rechtsfolgen (etwa nicht die in Abschnitt I.3 angeführten).

I.2.2. Unterzeichner/Signator

Eine Definition ist in § 2 Z 2 SigG und in Art 2 Z 3 SigRL enthalten.

Ein Signator ist eine Person oder eine sonstige rechtsfähige Einrichtung, der Signaturerstellungsdaten und Signaturprüfdaten zugeordnet sind und die im eigenen oder fremden Namen eine elektronische Signatur erstellt.

Unter "Signaturerstellungsdaten" ist der private Schlüssel zu verstehen, während "Signaturprüfdaten" den öffentlichen Schlüssel bezeichnet. Diese Benennung wurde gewählt, um eine Technik-indifferente Fassung zu ermöglichen, sodass auch etwaige andere Systeme darunter subsumiert werden können, wenn auch derzeit keine anderen spezifiziert sind[11].

Ein Signator kann sowohl im eigenen als auch unter fremdem Namen handeln (Vollmacht, Auftrag, Geschäftsführung, ...), ebenso wie bei händischen Unterschriften. Die tatsächliche Signierung kann nicht nur persönlich durch eine natürliche Person erfolgen, sondern auch automatisiert, was insbesondere für juristische Personen relevant ist, wo die Signatur oh-

[11] Elektronische Signaturen sind damit derzeit nur in Form von digitalen Signaturen möglich.

nehin nicht einer einzelnen Person sondern der Einrichtung als solcher zuzuordnen ist (Beispiel: Amts- und Justizsignatur; fortgeschrittene Signatur).

I.2.3. Fortgeschrittene elektronische Signatur

Eine Definition ist in § 2 Z 3 SigG bzw. Art 2 Z 2 SigRL enthalten. Sie muss ausschließlich dem Signator zugeordnet sein, dessen Identifizierung ermöglichen, mit Mitteln erstellt werden, welche dieser unter seiner alleinigen Kontrolle halten kann, sowie so mit den Daten verknüpft sein, dass jede nachträgliche Veränderung von diesen feststellbar ist.

Es wird vorausgesetzt, dass der Signator die Mittel zur Erstellung unter seiner alleinigen Kontrolle halten kann[12]. Dies ist notwendig, da sonst keine Rechtsfolgen an eine (darauf basierende!) qualifizierte Signatur geknüpft werden könnten: Jeder könnte behaupten, dass er nicht in der Lage ist, eine Fälschung zu verhindern und daher die Signatur ihm nicht zugerechnet werden darf. Sie könnte genauso von jemandem anderen stammen. Dies bedeutet jedoch keinen Ausschluss dieser Möglichkeit: Wurde das Sicherungsmittel, z.B. die Smartcard und der PIN-Code, tatsächlich von einem Dritten verwendet, so kann darüber ein Beweis geführt und etwaige Rechtswirkungen abgewendet werden. Diese Anforderung kann sowohl durch technische (Chipkarte, aus welcher der private Schlüssel nicht ausgelesen werden kann) als auch organisatorische Maßnahmen erfolgen (→ Keine sichere hardwarebasierte Signaturerstellungseinheit notwendig). Es ist daher auch eine fortgeschrittene Signatur möglich, wenn der private Schlüssel auf einem Server mit Zugriffsschutz liegt. Problematisch ist, dass hieran zwar die Qualifikation einer Signatur als "fortgeschritten" hängt, dieser Faktor aber von einem Empfänger nicht beurteilt werden kann: Er weiß nicht (und kann es auch nicht feststellen!), welche Sicherheitsmaßnahmen der Ersteller der Signatur getroffen hat.

Jegliche nachträgliche Veränderung der Daten muss erkennbar sein, um die Dokumentenechtheit zu gewährleisten. Dies erfolgt bei externen Signaturen dadurch, dass sich bei der Überprüfung ein anderer Hashwert ergibt als der Signatur entspricht, während bei internen Signaturen eine (sinnvolle) Entschlüsselung nicht mehr möglich ist. In Hinsicht auf Dokumentenformate ist in der SigVO in § 4 Abs 1 vorgeschrieben, dass Elemente in einem Format, welche dynamische Änderungen hervorrufen können, verboten sind.

Bedeutung besitzt die fortgeschrittene Signatur durch die elektronische Rechnung[13], für welche eine fortgeschrittene el. Signatur ausreicht und nicht unbedingt eine qualifizierte elektronische Signatur erforderlich ist. Daher ist hiermit eine automatische Massensignierung von Rechnungen möglich.

Rechtlich gesehen handelt es sich bei der fortgeschrittenen Signatur um eine "normale" bzw. einfache Signatur ohne besondere Rechtswirkungen.

---

[12] Trifft etwa bei einer rein textuellen Unterschrift, siehe oben, nicht zu: Jeder kann einen beliebigen Namen an das Ende einer E-Mail schreiben.

[13] Verordnung des Bundesministers für Finanzen, mit der die Anforderungen an eine auf el. Weg übermittelte Rechnung bestimmt werden, BGBl. II Nr. 583/2003. Dort wird jedoch nur auf § 2 Z 3 lit. a bis d der alten Fassung des SigG verwiesen (lit e kommt nicht vor); der äquivalente heutige Begriff "fortgeschrittene Signatur" kommt nicht vor.

I.2.4. Qualifizierte elektronische Signatur

Eine Definition ist in § 2 Z 3a SigG enthalten: Es handelt sich um eine fortgeschrittene Signatur, welche zusätzlich auf einem qualifizierten Zertifikat beruht und von einer sicheren Signaturerstellungseinheit erzeugt wird.

Für sichere elektronische Signaturen kommen derzeit nur Public-Key-Systeme in Frage, wobei die Verknüpfung einer Person mit einem öffentlichen Schlüssel durch qualifizierte Zertifikate erfolgt. Die sichere Signaturerstellungseinheit (§ 2 Z 5 SigG) soll ein besonders hohes Maß an Sicherheit bringen: Dass z.B. zwischen dem Willensakt des Signators (=Eingabe der PIN) und der technischen Berechnung keine Änderung möglich ist und auch genau das signiert wird, was angezeigt wird.

Entweder aus dem Zertifikat (obligatorisch, siehe § 5 Abs 1 Z 1 SigG), der el. Signatur selbst oder aus dem Sicherheits- & Zertifizierungskonzept, auf das im Zertifikat Bezug genommen wird, muss hervorgehen, dass es sich um eine qualifizierte Signatur handelt. Dieser Passus ist problematisch, da aus der Markierung im Zertifikat gerade nicht eindeutig hervorgeht, dass eine Signatur auch tatsächlich "qualifiziert" ist: Es kommt ja zusätzlich auf die eingesetzten Geräte (→ Sichere Signaturerstellungseinheit!) an. Auch aus dem Zertifizierungskonzept lässt sich höchstens eine Verpflichtung zum Einsatz solcher Geräte und Verfahren ablesen.

Inzwischen ist auch eine Stapelsignatur möglich: Es ist lediglich sicherzustellen, dass bei der Auslösung der Signierung klar dargestellt wird, wie viele Signaturen erzeugt werden. Hiermit können z.B. 20 Dokumente auf einmal signiert werden: Es wird jedes Dokument separat signiert (→ 20 qual. Signaturen), nicht alle Dokumente auf einmal zusammen (→ 1 qual. Signatur).

Da qualifizierte Zertifikate ausschließlich auf natürliche Personen ausgestellt werden können, sind qualifizierte, im Gegensatz zu fortgeschrittenen, Signaturen für juristische Personen nicht möglich (siehe dazu auch I.2.6).

I.2.5. Zertifikat

Eine Definition ist in § 2 Z 8 SigG und in Art 2 Z 9 SigRL enthalten.

Ein Zertifikat ist eine elektronische Bescheinigung, mit der Signaturprüfdaten einer bestimmten Person zugeordnet werden und deren Identität bestätigt wird.

Diese rechtliche Definition entspricht der technischen: Es wird eine Verbindung zwischen einem öffentlichen Schlüssel und einer konkreten Person hergestellt. Die Personenidentifizierung erfolgt über einen Namen, welcher ihr eindeutig zugeordnet sein muss. Pseudonyme sind zwar im Zertifikat möglich, doch der ZDA muss die wahre Identität kennen.

"Wurzel"-Zertifikate der ZDA sind entweder selbst-signiert oder werden mit einem Zertifikat der Aufsichtsstelle (Telekom-Control-Kommission) signiert, sodass im zweiten Fall deren Wurzel-Zertifikat automatisch die Wurzel aller derartigen österreichischen Zertifikate darstellt (derzeit der Fall[14]; Siehe Abbildung 1). Daraus könnte sich theoretisch ein Sicherheitsproblem ergeben (siehe aber die Angaben zur Sicherung gegen unbefugten Zugriff

[14] Sicherheits- und Zertifizierungskonzept (Certification Practice Statement) der TKK http://www.signatur.rtr.at/de/directory/cps.html

durch Mitarbeiter bzw. Externe im CPS), gleichzeitig ist jedoch eine Prüfung der Gültigkeit von Zertifikaten stark erleichtert.

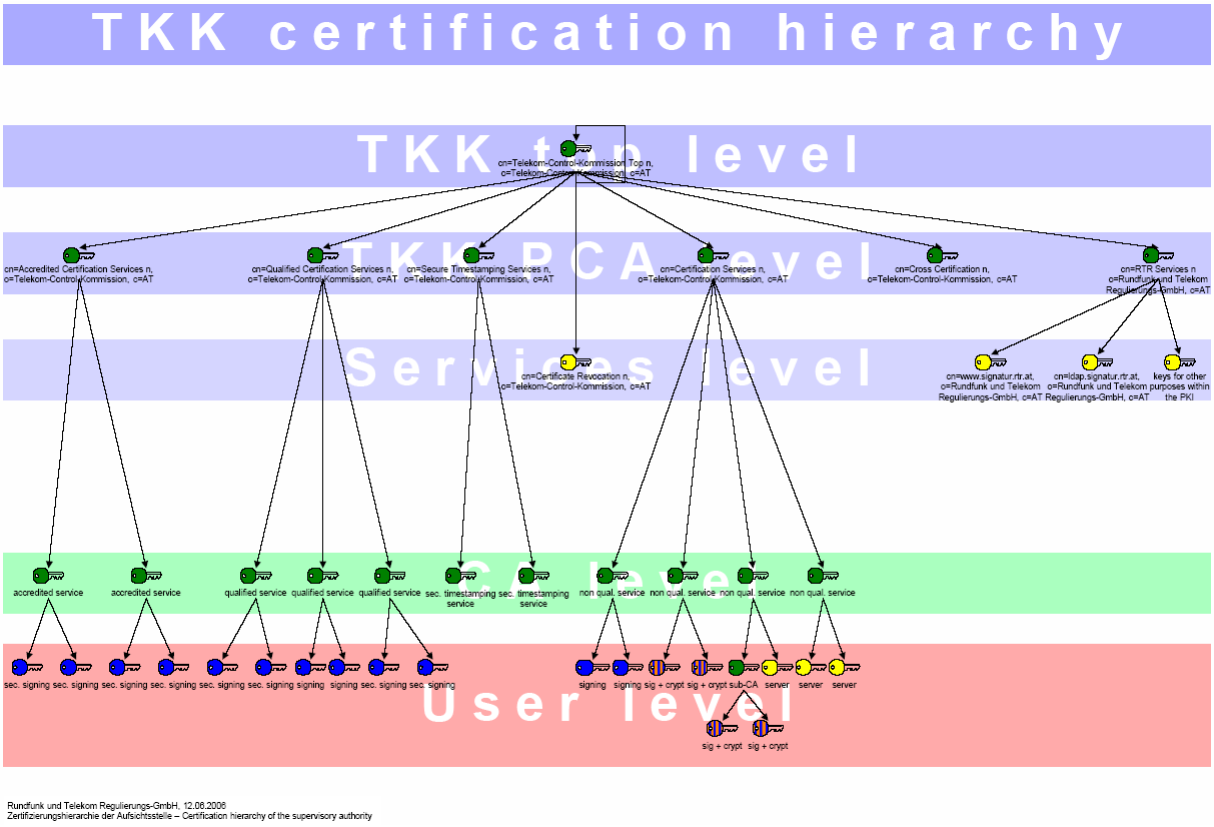

Abbildung 1: Zertifizierungshierarchie der RTR

I.2.6. Qualifiziertes Zertifikat

Eine Definition ist in § 2 Z 9 SigG iVm § 5, 7 SigG und in Art 2 Z 10 SigRL iVm Anhang I, II SigRL enthalten.

Ein Zertifikat einer natürlichen Person, das zumindest die folgenden Angaben enthält und von einem Zertifizierungsdiensteanbieter für qualifizierte Zertifikate ausgestellt wird und mit der fortgeschrittenen el. Signatur des Zertifizierungsdiensteanbieters versehen ist:

a) den Hinweis darauf, dass es sich um ein qualifiziertes Zertifikat handelt,
b) den unverwechselbaren Namen des ZDA und den Staat seiner Niederlassung,
c) den Namen des Signators oder ein Pseudonym, das als solches bezeichnet sein muss,
d) gegebenenfalls auf Verlangen des Zertifikatswerbers Angaben über eine Vertretungsmacht, eine andere rechtlich erhebliche Eigenschaft des Signators oder weitere rechtlich erhebliche Angaben,
e) die dem Signator zugeordneten Signaturprüfdaten,
f) Beginn und Ende der Gültigkeit des Zertifikates,
g) die eindeutige Kennung des Zertifikates,
h) gegebenenfalls eine Einschränkung des Anwendungsbereichs des Zertifikats und
i) gegebenenfalls eine Begrenzung des Transaktionswerts, auf den das Zertifikat ausgestellt ist,
j) gegebenenfalls weitere rechtlich erhebliche Angaben

Dem Zertifikat muss einerseits zu entnehmen sein, dass es sich um ein qualifiziertes Zertifikat handelt[15], und andererseits von welchem Zertifizierungsdiensteanbieter es ausgestellt wurde. Dadurch soll es dem Empfänger ermöglicht werden zu entscheiden, welches Vertrauen er in das Zertifikat setzt. Hierzu ist eine genaue Identifikation des Ausstellers notwendig[16]. Die Angabe des Staates der Niederlassung des ZDA hat den Sinn, die tatsächliche Überprüfung zu ermöglichen, da in der EU keine Land ein vollständiges Verzeichnis für alle Länder führen muss und dies auch nicht für eine separate EU-Instanz vorgesehen ist. In Österreich ist zwar eine zentrale Stelle vorgesehen, bei der alle Zertifikate der inländischen ZDA hinterlegt werden müssen, doch sind auch hier ausländische Zertifikate nur auf Antrag aufzunehmen, also freiwillig (§ 13 Abs 3 SigG).

Auch Pseudonyme sind als Inhalt von Zertifikaten zulässig, dürfen jedoch weder anstößig sein noch offensichtlich Verwechslungen mit Namen oder Kennzeichen hervorrufen (§ 8 Abs 4 SigG). Dies bedeutet keine echte Anonymität: Dem ZDA muss die tatsächliche Identität immer bekannt sein, auch wenn diese nicht im Zertifikat aufscheint.

Angaben über eine Vertretungsmacht betreffen insbesondere die Befugnis zur Außenvertretung von Gesellschaften: Prokura, Handlungsvollmacht, Eigenschaft als Notar/Rechtsanwalt etc. Diese Eigenschaften müssen dem Zertifizierungsdiensteanbieter nachgewiesen werden, bevor ein entsprechendes Zertifikat ausgestellt werden darf. Siehe dazu I.5.1.

Weiters können Einschränkungen des Anwendungsbereichs vorgesehen werden. Denkbar sind diese beispielsweise in Bezug auf bestimmte Rechtsgeschäfte, wie etwa Kaufverträge über bewegliche Sachen (Ausschluss von Kaufverträgen über Grundstücke, Darlehensgewährung, bestimmte Gebiete etc.). Optional kann auch eine Beschränkung des Transaktionswertes erfolgen, der mit dem Zertifikat möglich ist. Dies hat zwar keine Auswirkung auf die Zulässigkeit der Verwendung bei höherwertigen oder sonstigen[17] Verträgen, welche dadurch nicht ungültig sind, doch wird hiermit die Haftung des ZDA eingeschränkt. Besonders geeignet sind derartige Zusatzmerkmale für Personen, deren Ausgaben eingeschränkt werden sollen (Kinder, Unmündige, ...). Wer ein solches Zertifikat akzeptiert, kann sich später nicht darauf berufen, dass er von der Beschränkung nichts gewusst hat.

Qualifizierte Zertifikate dürfen ausschließlich auf natürliche Personen ausgestellt werden. Der dahinterstehende Grund ist, dass mit diesen qualifizierten Signaturen erzeugt werden können, welche besondere Rechtsfolgen erzeugen und damit immer eindeutig einer einzigen verantwortlichen Person zuordenbar sein sollen. Juristische Personen sind hingegen nie handlungsfähig, sondern bedürfen zur Vornahme einer Unterschrift immer eines physischen Organs oder "Vertreters", der "stellvertretend" für sie handelt. Mit dieser Vorschrift soll daher sichergestellt werden, dass eine rechtlich verbindliche Unterschrift immer einer natürlichen Person zugeordnet werden kann, welche den Signierungsvorgang auslöst und dazu auch (hoffentlich, aber jedenfalls extern überprüfbar) berechtigt ist. Bei juristischen Personen könnte sonst oft der Fall eintreten, dass mehrere Person dazu berechtigt und in der Lage sind, eine Firmensignatur anzubringen, ohne dass sich später aus der Signatur

[15] Diese Anmerkung darf auch *nur* bei diesen eingebaut werden. Eine Anbringung kann auch in der Signatur selbst oder im Sicherheits- & Zertifizierungskonzept des ZDA enthalten sein, auf das im Zertifikate Bezug genommen wird. Dies bedeutet, dass diese Qualität nur sehr schwer verlässlich feststellbar ist!

[16] Praxis: Voreinstellungen der Webbrowser, welche u.U. für das gesamte Betriebssystem gelten. Beispiel: Internet Explorer und die häufigen "Stammzertifikate" Updates.

[17] Die monetäre Beschränkung einer qual. Signatur steht der Wirksamkeit einer el. übermittelten Klageschrift nicht entgegen: Bundesfinanzhof 18.10.2006, XI R 22/06

feststellen ließe, wer dafür konkret verantwortlich war. Es ist jedoch zu beachten, dass dieses Ziel auch auf einem anderen Wege erreichbar wäre: Mit der Richtlinie vereinbar wäre es, z.B. eine Doppelsignatur[18] durch die juristische Person und diejenige natürliche Person, welche die Signierung auslöste, zu verlangen.

I.3. Rechtswirkungen elektronischer Signaturen

Aus der Verwendung el. statt handschriftlicher Unterschriften ergeben sich großteils idente Rechtswirkungen: Sie sind gleichgestellt und dürfen nicht diskriminiert werden.

I.3.1. Erfüllung der Schriftform

Eine qualifizierte elektronische Signatur, d.h. auf einem qualifizierten elektronischen Zertifikat beruhend, erfüllt die Anforderung einer eigenhändigen Unterschrift und damit das Erfordernis der Schriftlichkeit gemäß § 886 ABGB[19]. Besondere Formen der Schriftlichkeit, wie etwa Notariatsakt, notarielle Beurkundung etc. sind davon ebenfalls betroffen und können daher inzwischen auch el. erfolgen; ebenso die (raren) Rechtsgeschäfte des Familien- oder Erbrechts mit Schriftformerfordernis.

Es bleiben daher lediglich folgende Bereiche von einer elektronischen Unterschrift ausgenommen (siehe dazu auch E-Commerce RL Art. 9):

- Rechtsgeschäfte des Familien- oder Erbrechts mindestens mit Schriftformerfordernis. Diese Einschränkung kann seit dem Jahr 2007 umgangen werden, wenn zusätzlich ein Notar oder Rechtsanwalt mit seiner Signatur bestätigt, dass er den Signator über die Rechtsfolgen aufgeklärt hat. Hiermit soll der besonderen Übereilungsschutz einer physischen Unterschrift im el. Bereich substituiert werden. Weiters sind diese Bereiche besonders sensibel, da sie häufig vermögensrechtliche Belange besonders schutzbedürftiger Personen betreffen (z.B. Minderjährige). Immer unzulässig in el. Form sind letztwillige Anordnungen, d.h. nicht einmal zusammen mit einer Notarsignatur. Ein Testament in el. Form ist daher nicht möglich.
- Bürgschaftserklärungen[20]. Hierfür ist gemäß § 1346 Abs 2 ABGB explizit die Schriftform gefordert. Diese Ausnahme existiert, um die besondere Warnfunktion der eigenhändigen handschriftlichen Unterschrift nicht zu entwerten. Analog dem vorigen Punkt ist hier eine elektronische Form möglich, wenn zusätzlich ein Notar oder Rechtsanwalt mit seiner Signatur bestätigt, den Bürgen über die Rechtsfolgen der Verpflichtung aufgeklärt zu haben.
- Willenserklärungen oder Rechtsgeschäfte, die einer öffentlichen Beglaubigung, einer gerichtlichen oder notariellen Beurkundung oder eines Notariatsaktes für ihre Wirksamkeit oder für eine Eintragung in ein öffentliches Register[21] bedürfen. Auch diese

[18] Sonntag: Electronic Signatures for Legal Persons. In: Hofer/Beneder (Hrsg.): IDIMT'00. 8th Interdisciplinary Information Management Talks. Linz: Trauner 2000, 233-256

[19] Im Gegensatz zu Deutschland erfordert "Schriftlichkeit" *nicht* das Vorliegen einer Urkunde, was in Österreich mangels physischer Festlegung bei elektronische Daten auch nicht möglich ist.

[20] Dies findet analoge Anwendung auf Garantieerklärungen. Ein Fax, selbst mit Original-Unterschrift, reicht nicht aus, da das "Aus-der-Hand-geben" ein wichtiges Element der Warnfunktion ist.

[21] Insbesondere Grund- und Firmenbuch.

Ausnahme wurde mit 2007 praktisch beseitigt, da der jeweilige Akt dann auch elektronisch erfolgen kann[22].

Absolute Ausnahme ist daher lediglich die letztwillige Verfügung, typischerweise ein Testament. Alle anderen Rechtsgeschäfte können el. durchgeführt werden, wobei in manchen Fällen besondere Zusatzvorkehrungen erforderlich sind. In der Praxis werden alle diese Bereiche jedoch anscheinend weiterhin rein handschriftlich durchgeführt.

Die Nichteinhaltung zivilrechtlicher Schriftformerfordernisse führt zu einer Naturalobligation, welche zwar erfüllbar, aber nicht einklagbar ist. Dies hat zur Folge, dass eine tatsächliche Leistung den Formmangel heilt. Eine Rückabwicklung formmangelhafter Verträge ist damit ausgeschlossen (§ 1432 ABGB). Gleiches gilt für Signaturen, die nicht allen Anforderungen für sichere Signaturen entsprechen: Ihre Verwendung führt zwar nicht zu einem Vertrag, aber zu einer Naturalobligation.

Wichtig ist festzustellen, dass hierdurch keine Formvorschriften berührt werden: Rechtsgeschäfte die Schriftlichkeit erfordern benötigen diese weiterhin. Sie kann nun eben zusätzlich anders als nur handschriftlich erfüllt werden. Nicht formgebundene Geschäfte bleiben auch weiterhin formfrei.

I.3.2. Vermutung der Echtheit

Der Unterschrift kommt auch im Beweisrecht eine wichtige Bedeutung zu. Für unterschriebene Privaturkunden gelangt die besondere zivilprozessuale Beweisregel des § 294 ZPO zur Anwendung: Ist eine Unterschrift unbestritten oder nachgewiesenermaßen echt, so erbringt eine Privaturkunde vollen Beweis dafür, dass der Inhalt vom Aussteller, also vom Namensträger der Unterschrift, stammt. Dabei handelt es sich um eine qualifizierte Echtheitsvermutung für den Erklärungsinhalt, die eine Zuordnung der in einer Urkunde enthaltenen Erklärung zum Unterzeichner bewirkt[23]. Der Beweis des Gegenteils ist zulässig, dann jedoch vom Gegner zu führen. Dies bedeutet, dass die Beweislast für die Unechtheit des Inhalts der Urkunde den Gegner des Beweisführers trifft, d.h. denjenigen, der unterschrieben hat. Diese Umkehr bezieht sich aber nur auf den Urkundeninhalt, hinsichtlich der Echtheit der Unterschrift (=el. Signatur) gelangen die normalen Beweislastregeln zur Anwendung. Die Richtigkeit der Signatur hat also der zu beweisen, der die Datei als Beweis verwenden möchte.

Diese Rechtswirkungen treten nicht ein wenn nachgewiesen wird, dass die Sicherheitsanforderungen durch den ZDA nicht eingehalten oder die Signaturerstellungsdaten kompromittiert wurden, also z.B. der private Schlüssel jemandem anderen bekannt ist. Wenn dies auch unwahrscheinlich ist, können sich dadurch Personen doch von ihrer Haftung befreien, sofern sie ihren Sorgfaltspflicht bei der Schlüssel-Geheimhaltung entsprachen!

[22] D.h. ein Notariatsakt bedarf entweder einer physischen Unterschrift mit Anwesenheit vor dem Notar oder einer elektronischen Signatur vor einem Notar zusammen mit einer elektronischen Signatur des Notars. Eine elektronische Signatur vor einem Notar, welche dieser handschriftlich beglaubigt, z.B. auf einem Ausdruck, reicht nicht aus.

[23] Damit wird nicht die Wahrheit/Tatsächlichkeit des Inhalts bewiesen, sondern nur, dass der Unterzeichner genau diesen Inhalt erklärte. Es verbleibt dann kein Platz mehr für ein Abstreiten.

I.3.3. Zulässigkeit als Beweismittel vor Gericht

Sichere el. Signaturen müssen vor Gericht als Beweismittel zugelassen werden. Dies ist in Österreich kein besonderes Problem, da fast keine Beweisverbote existieren. Nach derzeitigem Beweisrecht stellt ein el. Dokument im visualisiertem Zustand ein Augenscheinsobjekt dar. Wird ein el. Dokument ausgedruckt, so liegt eine – jedoch nicht unterschriebene – Urkunde vor.

Aber auch nicht-qualifizierte, d.h. einfache oder fortgeschrittene, Signaturen, also solche, die nicht auf einem qualifizierten Zertifikat beruhen oder bei denen sonstige Punkte fehlen, müssen vor Gericht beachtlich sein. Weder dass sie nur in el. Form vorliegen, nicht auf einem qualifizierten Zertifikat beruhen, nicht von einem akkreditierten Zertifizierungsdiensteanbieter stammen oder nicht mit einer sicheren Signaturerstellungseinheit erzeugt wurden, darf einen grundsätzlichen Ausschluss bedeuten. Ihr Beweiswert ist jedoch weiterhin der freien Beweiswürdigung unterworfen und wird daher in der Praxis geringer sein als bei sicheren Signaturen. Er darf jedoch nicht ohne Begründung einfach ausgeschlossen werden[24]. Dies gilt nur für Gerichte; Verwaltungsbehörden müssen solchen Signaturen keinen Wert beilegen[25] und können z.B. einen Verbesserungsauftrag erteilen.

I.4. Widerruf von Zertifikaten

Manchmal ist es nötig, Zertifikate zu widerrufen, bevor ihr Geltungszeitraum abgelaufen ist. Dies sind folgende Fälle:

- Es wurde zufällig ein gleiches Schlüsselpaar erzeugt,
- der private Schlüssel der Zertifizierungsinstanz wurde bekannt,
- der private Schlüssel des Signators wurde bekannt,
- die Aufsichtsstelle ordnet den Widerruf an,
- der ZDA stellt seine Tätigkeit ein und die Verzeichnis-/Widerrufsdienste werden nicht von einem anderen ZDA übernommen,
- der Signator ist tot oder nicht mehr im Besitz des privaten Schlüssels,
- die Angaben im Zertifikat sind nicht mehr gültig (Namensänderung, Änderung der Vertretungsmacht etc.) oder waren schon Anfangs falsch (Erschleichung) oder
- der Signator oder ein im Zertifikat genannter Machtgeber verlangt es.

Es ist zwischen "Sperren" und "Widerrufen" von Zertifikaten zu unterscheiden: Eine Sperre bedeutet nur eine temporäre Ungültigkeit von maximal zehn Werktagen, während ein Widerruf die Gültigkeit eines Zertifikates endgültig beseitigt. Eine Sperre erfolgt dann, wenn es anscheinend Gründe gibt, das Zertifikat zu widerrufen, aber noch genauere Ermittlungen notwendig sind, ob diese tatsächlich vorliegen. Ab einer Sperre erfolgt daher die Akzeptierung des Zertifikates auf eigene Gefahr: Wird es widerrufen, so wirkt der Widerruf rückwirkend mit dem Zeitpunkt der Sperre. Stellen sich die Gründe jedoch als falsch

[24] In der Praxis wird wohl ein Gutachten über den Sicherheitsgrad und die Schwierigkeit einer Fälschung über den konkreten Beweiswert entscheiden.

[25] Achtung: Der europäische Begriff "Gericht" umfasst mehr als in der österreichischen Rechtssprache, z.B. auch die unabhängigen Verwaltungssenate (UVS), welche in Österreich zur Verwaltung zählen.

heraus, so war das Zertifikat während der gesamten Zeit gültig (=rückwirkende Aufhebung der Sperre) und bleibt es auch weiterhin.

Sowohl Sperre als auch Widerruf müssen den Zeitpunkt ihrer Wirksamkeit enthalten; dieser darf höchstens eine Stunde nach der Eintragung liegen. Sperren und Widerrufe mit einem Zeitpunkt in der Vergangenheit zu erstellen ist unzulässig. Der Signator bzw. sein Rechtsnachfolger ist von Sperre bzw. Widerruf unverzüglich zu verständigen. Um vorzeitige Beendigungen der Gültigkeit qualifizierter Zertifikate Betroffenen auch zur Kenntnis zu bringen, muss jeder Zertifizierungsdiensteanbieter entsprechende Verzeichnisse el. und frei zugänglich führen. Deren Abfrage hat gratis und ohne Identifizierung des Abfragenden möglich zu sein. Unterbrechungen, wie etwa Systemzeiten, sind nicht erlaubt. Für diese Fälle ist ein Ersatzsystem vorzusehen. Daher ist jede länger als 30 Minuten dauernde Unterbrechung als Störfall zu protokollieren. Ein Widerruf, der auch schriftlich möglich ist, muss von Montag bis Freitag spätestens drei Stunden, ansonsten binnen sechs Stunden nach Bekannt werden des Widerrufsgrundes erfolgen und veröffentlicht sein (Postweg: 2 Werktage).

Für die Praxis ist wichtig, dass eine Prüfung des Widerrufs des Zertifikates immer dann notwendig ist, wenn der Transaktionswert eine bestimmte Höhe erreicht, die von der eigenen Risikobereitschaft abhängt. Da Sperr- und Widerrufsverzeichnisse el. und unentgeltlich zur Verfügung stehen müssen, ist aber auch eine grundsätzliche Prüfung in allen Fällen möglich. Problematisch kann hierbei sein, dass die technologische Unterstützung nicht in allen Produkten (insbesondere Web-Browsern) gegeben ist. Damit später ein Beweis möglich ist, muss in einen Vertrag ein gesicherter Zeitstempel aufgenommen werden: Ansonsten ist es nicht möglich zu beweisen, wann exakt die Signierung durchgeführt worden war. Ohne diesen Stempel kann nicht festgestellt werden, ob die Signatur noch vor dem Widerruf erfolgte und damit gültig ist, oder danach, und auf eine Überprüfung wegen etwaigen Widerrufs verzichtet wurde, und somit ungültig ist.

I.5. Zertifizierungsdiensteanbieter (ZDA)

An Anbieter von (qualifizierten) Zertifizierungsdiensten (Engl.: "Certificate Authority", CA) werden hohe Anforderungen gestellt. Dies ist auch notwendig, da an eine Signatur unter Umständen erhebliche rechtliche und finanzielle Folgen geknüpft sind. Es ist daher ein Missbrauch so weit wie nur irgend möglich auszuschließen. Dies soll auch das Vertrauen der Benutzer fördern, da ansonsten keine weite Verbreitung und die damit verbundenen Vorteile wie einfachere und schnellere Erledigung, mehr Möglichkeiten für Kontakte mit der Verwaltung etc. zu erwarten sind. Werden hingegen nur "einfache" Zertifikate ausgestellt, so ist eine derart aufwendige Aufsicht nicht erforderlich: Jeder kann ohne besondere Voraussetzungen und inzwischen auch ohne Anmeldung solche Dienste betreiben.

I.5.1. Datenschutz

Zertifikate besitzen nicht nur Vorteile: Durch ihre Verwendung wird jede Anonymität beseitigt. Die einzige Möglichkeit dagegen ist, entweder keine Zertifikate zu verwenden, was eher ungünstig ist, oder solche mit einem Pseudonym anstatt des "echten" Namens einzusetzen. Zusätzliche Zertifikate bedeuten jedoch höhere Kosten und mehr Organisationsaufwand. Um die Gefahr des "gläsernen Menschen" nicht zu groß werden zu lassen, werden an den Datenschutz in Bezug auf alle Zertifikate, qualifizierte wie auch sonstige, besonders hohe Anforderungen gestellt:

- Zertifizierungsdiensteanbieter dürfen nur diejenigen personenbezogenen Daten verwenden, welche für die Durchführung der Dienste notwendig sind (§ 22 SigG). Insbesondere dürfen keine Aufzeichnungen und Auswertungen von Anfragen bezüglich eines etwaigen Widerrufs durchgeführt werden, da sich dadurch eine Datenspur ergibt und Gewohnheiten des Zertifikatsinhabers (besuchte Webseiten, bevorzugte Internet-Geschäfte, ...) festgestellt werden könnten.
- Alle notwendigen Daten für die Überprüfung der Ausstellung inklusive Angaben über besondere Eigenschaften, etwa die Vertretungsmacht, dürfen ausschließlich beim Antragsteller erhoben werden. Mit seiner *ausdrücklichen* Zustimmung ist auch eine Erhebung bei Dritten möglich. Werden keine Nachweise erbracht, so sind weitere Prüfungen verboten: In diesem Fall darf eben kein Zertifikat ausgestellt werden.
- Wird ein Pseudonym verwendet, so hat der ZDA die Identität des Signators auch Dritten zu übermitteln, sofern diese ein überwiegendes berechtigtes Interesse glaubhaft machen. Eine richterliche Genehmigung ist nicht erforderlich. Alle solchen Auskünfte sind exakt zu dokumentieren.

I.5.2. Die Anforderungen im Detail

Sollen qualifizierte Zertifikate ausgestellt werden oder ein qualifizierter Zeitstempeldienst betrieben werden, so muss vorher ein Sicherheits- und ein Zertifizierungskonzept an die Aufsichtsstelle gemeldet und dieses eingehalten werden. Dieses Konzept ist in el. Form ("in einem gängigen Format") zu übersenden und muss mit einer fortgeschrittenen Signatur signiert sein. Das Konzept ist zusätzlich in klar und allgemein verständlicher Form bereit zu halten.

Werden Schlüsselpaare von der Zertifizierungsstelle und nicht vom Zertifikatsantragsteller erzeugt, so muss dafür ein besonderer Zufallszahlengenerator[26] verwendet werden und die erzeugten Schlüssel sind auf ihre Zufälligkeit und Eignung zu prüfen. Diese Generatoren sind auch regelmäßig auf ihre Qualität zu überprüfen bzw. neu zu initialisieren.

Weiters ist der Antragsteller zuverlässig zu identifizieren, beispielsweise durch einen amtlichen Lichtbildausweis[27] oder eine Zustellung per RSa-Brief. Diese Prüfung ist auch zu dokumentieren. Bei einer Verlängerung eines bestehenden Zertifikates, d.h. nur während der Gültigkeitsdauer des qualifizierten Zertifikats, ist es wohl ausreichend, wenn ein solcher Antrag mit der (noch) gültigen Signatur versehen ist, ansonsten ist eine handschriftliche Unterschrift nötig. Im ersten Fall ist deshalb persönliches Erscheinen nicht mehr erforderlich. Diese Option ist nur bis zum Ablauf der Gültigkeit des verwendeten Algorithmus bzw. der Schlüssellänge möglich. Die Identitätsprüfung des Antragstellers kann auch von einer beauftragten Stelle erfolgen. Dieser Passus wurde vermutlich für die Post vorgesehen (Prüfung in jedem Postamt), doch könnten auch andere Firmen mit breitem Filialnetz davon Gebrauch machen, z.B. Banken.

---

[26] Früher: Physikalischer Zufallszahlengenerator. Jetzt sind nach der SigVO auch Pseudozufallszahlengeneratoren erlaubt. Der Grund ist nicht ganz einsichtig, da physikalische Generatoren auch nicht übermäßig komplex oder teuer sind und nur ein einziges Exemplar benötigt wird! Nach den Ausführungen in der SigVO könnte der Grund darin liegen, dass physische Generatoren (im Vergleich zu Pseudozufallszahlengeneratoren) sehr langsam arbeiten und damit die rasche Ausstellung einer großen Zahl an Zertifikaten problematisch wäre.

[27] Ein solcher ist nicht mehr "absolut" erforderlich, z.B. um auch Banken eine einfachere Ausstellung zu ermöglichen. Diese mussten ihre Kunden schon vorher aufgrund anderer Vorschriften überprüfen, sodass eine neuerliche Identitätsprüfung entfallen kann. Siehe § 8 SigVO

An besonderen Anforderungen ist in § 7 SigG für Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, u.a. folgendes festgelegt:

- Er muss die erforderliche Zuverlässigkeit aufweisen
- Ein schneller und sicherer Verzeichnisdienst sowie ein sicherer und unverzüglicher Widerrufsdienst muss gewährleistet werden. Wie dies erfolgt ist im Sicherheitskonzept detailliert zu beschreiben.
- Qualitätsgesicherte[28] Zeitstempel müssen verwendet werden, insbesondere für die Zeitpunkte des Ausstellens und Widerrufens von qualifizierten Zertifikaten.
- Zuverlässiges Personal[29] mit den erforderlichen Fachkenntnissen, Erfahrungen und Qualifikationen (Management, Technik, Sicherheit) muss beschäftigt werden.
- Geeignete Verwaltungs- und Managementverfahren sind einzurichten, welche anerkannten Normen entsprechen müssen (→ Zertifizierungen!).
- Genügend Finanzmittel für Betrieb und insbes. Haftung müssen vorhanden sein[30].
- Alle maßgeblichen Umstände über ein qualifiziertes Zertifikat sind aufzuzeichnen, um später die Zertifizierung nachweisen zu können, insbesondere in Gerichtsverfahren.
- Vorkehrungen sind zu treffen, damit Signaturerstellungsdaten weder vom Zertifizierungsdiensteanbieter noch von Dritten gespeichert oder kopiert werden können.
- Für die Erbringung der Dienste sind vertrauenswürdige und gesicherte Systeme, Produkte und Verfahren einzusetzen.
- Die Signaturerstellungsdaten der ZDA sind gegen unbefugten Zugriff zu sichern.
- Technische Einrichtungen zur Erbringung von Signatur- und Zertifizierungsdiensten sind sowohl im Normalbetrieb wie auch bei Störfällen von anderen Funktionen und Anwendungen zu trennen.
- Die Einrichtungen sind gegen unbefugten Zutritt zu sichern.

Grob gesagt ist ein sicheres Rechenzentrum mit besonderer Hard- und Software, speziellen Vorkehrungen, und ein gleichartiges Ersatzrechenzentrum gefordert. Aus diesem Grund kann davon ausgegangen werden, dass qualifizierte Zertifikate in der Praxis nur von relativ wenigen Anbietern ausgegeben werden.

Interessant ist, dass nach der SigVO (§ 6 Abs 3) technische Komponenten und Verfahren in bestimmten Fällen durch organisatorische substituiert werden können, wenn qualifiziertes und vertrauenswürdiges Personal eingesetzt wird. Dies gilt allerdings nur für kontrollierte Umgebungen, d.h. innerhalb eines Rechenzentrums. Verfahren, die von Signatoren verwendet werden, sind also nicht betroffen.

---

[28] Eine etwas seltsam anmutende Bezeichnung, die jedoch ihren Grund hat: Es handelt sich eben nicht immer um qualifizierte Zeitstempel. Z.B. ist der Ausstellungszeitpunkt in einem Zertifikat kein Zeitstempel (als solcher unsigniert), der Zeitpunkt eines Widerrufs (Zeitstempel der Widerrufsliste) aber schon.

[29] Z.B. keine Personen, die wegen einer Vorsatztat zu einer Freiheitsstrafe von mehr als einem Jahr (betreffend Vermögen/Urkunden/Beweiszeichen: 3 Monate) bestraft wurden.

[30] Die SigVO legt hierzu fest, dass ein Mindestkapital von € 300.000 erforderlich ist. Davon sind jedoch der Bund, die Länder, Gemeindeverbände, Gemeinden, Körperschaften des öff. Rechts sowie die Sozialversicherungsträger befreit. Der Grund liegt wohl darin, dass z.B. der Bund kein "Grundkapital" besitzt und die angeführten Organisationen nicht, oder nur sehr unwahrscheinlich, in Konkurs gehen (können).

I.5.3. Haftung der Zertifizierungsdiensteanbieter

Ein Zertifizierungsdiensteanbieter haftet gegenüber dritten Personen gemäß § 23 SigG, sofern diese auf das qualifizierte Zertifikat vertrauten, für folgende Punkte:

- Alle Angaben im qualifizierten Zertifikat sind zum Zeitpunkt der Ausstellung richtig und dieses ist vollständig.
- Der Empfänger ist zum Ausstellungszeitpunkt im Besitz der Signaturerstellungsdaten.
- Die Signaturerstellungs- und die Signaturprüfdaten entsprechen einander komplementär, wenn von ihm empfohlene/bereitgestellte Produkte/Verfahren verwendet werden.
- Ein Widerruf erfolgt sofort nach Bekannt werden der Erfüllung der dafür notwendigen Voraussetzungen.
- Die Widerrufsdienste sind verfügbar.
- Er erfüllt alle Anforderungen an einen ZDA (§ 7 SigG).
- Für die Erstellung der Zertifikate werden nur sichere Komponenten und Verfahren verwendet (§ 18 SigG).
- Von ihm bereitgestellte oder als geeignet bezeichnete Produkte bzw. Verfahren für die Signaturerstellung und die Darstellung zu signierender Daten[31] verwenden nur sichere Komponenten und Verfahren (§ 18 SigG).

Alle diese Punkte sind unverzichtbar. Es kann daher nur *nach* Entstehen eines Anspruchs darauf verzichtet werden. Ein Ausschluss oder Verzicht im vorhinein ist unwirksam.

Diese Haftung unterliegt jedoch auch Einschränkungen: Der ZDA haftet nicht wenn er nachweist, dass ihn kein Verschulden trifft. Für Handlungen seiner Gehilfen muss er jedoch sehr wohl einstehen. Darin enthalten ist eine Haftung bis hinab zu leichter Fahrlässigkeit. Ausnahmsweise fällt diese weg, wenn das Zertifikat entgegen darin enthaltener Beschränkungen verwendet wurde. Es trifft ihn gar keine Haftung, wenn das Zertifikat für ein nicht in den Einschränkungen enthaltenes Rechtsgeschäft verwendet wurde bzw. nur in Höhe der Beschränkung des Transaktionswertes bei einer Überschreitung desselben.

Um einem Benutzer von Zertifikaten in einem Prozess den Beweis zu erleichtern, genügt es, wenn dieser *wahrscheinlich* macht, dass die Kompromittierung in der Sphäre des ZDA erfolgte. Daraus resultiert jedoch keine Umkehr der Beweislast, da der ZDA sein Haftung dadurch abwenden kann, dass er gleichfalls nur wahrscheinlich macht, dass die Kompromittierung in der Sphäre des Signators liegt: Hiermit wird der Anscheinsbeweises des Signators außer Kraft gesetzt.

Gemäß § 2 Abs 1 SigVO ist ein Zertifizierungsdiensteanbieter in Hinsicht auf die Haftung verpflichtet, eine Haftpflichtversicherung in Höhe von € 700.000 pro Versicherungsfall für mindestens drei Fälle pro Jahr abzuschließen, bevor er seine Tätigkeit aufnehmen darf.

[31] Nicht geprüft werden daher die Signaturprüfeinrichtungen!

I.5.4. Aufsichtsstelle

Im SigG ist als Aufsichtsstelle die Telekom-Control-Kommission (TKK) vorgesehen[32]. Diese agiert als eine oberste Zertifizierungsstelle (Root-CA), signiert also die Zertifikate der einzelnen ZDA. Alternativ können diese auch selbst-signiert sein und werden dann in eine Liste aufgenommen, welche von der Aufsichtsstelle signiert ist. Sie ist dafür verantwortlich, dass ein el. und frei zugängliches gesichertes Verzeichnis[33] der gültigen, gesperrten und widerrufenen Zertifikate der österreichischen, auf Antrag unter Einschluss der ausländischen, ZDA geführt wird. Das zugehörige Zertifikat wurde früher im Amtsblatt zur Wiener Zeitung veröffentlicht; dies erfolgt inzwischen nicht mehr. An diese Stelle soll eine Kreuz-Zertifizierung mit möglichst vielen anderen ZDAs und die Veröffentlichung auf der RTR-Homepage (http://www.signatur.rtr.at/) treten.

Da in der TKK weder die notwendige detaillierte Fachkenntnis noch die personelle Ausstattung vorhanden ist, um diese Aufgaben zu erfüllen, bedient sie sich einer oder mehrerer "Bestätigungsstellen". Zusätzlich kann die Telekom-Control-GmbH mit der Durchführung der von der Kommission vorzunehmenden Aufsicht beauftragt werden. Sowohl Bestätigungsstellen wie Telekom-Control-GmbH werden dann als beliehene Unternehmen tätig und üben behördliche Funktionen aus. Ihre Entscheidungen erfolgen daher in solchen Fällen in der Form eines Bescheides. Bestätigungsstellen werden vom Bundeskanzler und dem Justizminister im Einvernehmen per Verordnung ernannt[34]. Als Bestätigungsstelle ist derzeit ein einziger Verein vorgesehen: "Zentrum für sichere Informationstechnologie – Austria (A-SIT)". Als Mitglieder fungieren das Bundesministerium für Finanzen, die Oesterreichische Nationalbank sowie die Technische Universität Graz. Dies ist einer der Kritikpunkte an dem Gesetz, da hiermit ein weiterer privater Verein mit behördlichen Aufgaben betraut wird. Als Alternative wurde beispielsweise der TÜV (Technischer Überwachungsverein) vorgeschlagen, der bereits umfangreiche Technikprüfungen durchführt.

I.6. Akkreditierung

Die Akkreditierung eines Zertifizierungsdiensteanbieters bringt keine zusätzlichen Qualitätsmerkmale mit sich: Es handelt sich nur um eine Bestätigung, dass die ohnedies einzuhaltenden Bestimmungen besonders überprüft wurden und ihnen entsprochen wird. Die erfolgreiche Akkreditierung berechtigt, das Bundeswappen zu führen und sich als "Akkreditierter Zertifizierungsdiensteanbieter" zu bezeichnen, was hauptsächlich Werbezwecken dient. Für diese ZDA ist bei der Aufsichtsstelle ein eigenes Verzeichnis zu führen bzw. werden sie im allgemeinen Verzeichnis besonders gekennzeichnet.

Dass ein Zertifikat von einem akkreditierten Zertifizierungsdiensteanbieter ausgestellt wurde, ist in das Zertifikat aufzunehmen oder sonst kenntlich zu machen, sodass ein Empfänger deswegen (eventuell) ein höheres Vertrauen darin setzen kann. In Zertifikate nicht akkreditierter Anbieter darf diese Bezeichnung nicht eingebaut werden. Rechtlich sind Signaturen von "normalen" und "akkreditieren" ZDA jedoch absolut gleichgestellt.

---

[32] Siehe dazu § 116 TKG; dies ist ein unabhängiges und weisungsfreies Kollegialorgan mit richterlichem Einschlag gemäß Art 133 Z 4 B-VG, das in erster und oberster Instanz entscheidet. Die Anrufung des Verwaltungsgerichtshofes als außerordentliches Rechtsmittel ist explizit gestattet.

[33] http://www.signatur.rtr.at/de/providers/providers.html Die sichere Version ist über HTTPS bzw. LDAP/SSL erreichbar.

[34] Derzeit die einzige: Feststellung der Eignung des Vereins "Zentrum für sichere Informationstechnologie – Austria (A-SIT)" als Bestätigungsstelle, BGBl II 31/2000 vom 2.2.2000

Nach der SigRL ist eine Beschränkung der Anzahl der akkreditierten Anbieter nicht zulässig. Es hat daher jeder Anbieter die Möglichkeit, eine Akkreditierung zu erhalten, sofern er qualifizierte Zertifikate ausstellt. Anbieter "einfacher" Zertifikate können sich nicht akkreditieren lassen.

I.7. Rechte und Pflichten: ZDA und Signator

Der Signator der qualifizierte Signaturen erstellt hat die Pflicht, seine Signaturerstellungsdaten sicher zu verwahren und sie nicht weiterzugeben. Verliert er die Erstellungsdaten oder vermutet er, dass sie bekannt wurden, so hat er selbst den Widerruf des Zertifikates zu veranlassen. Ebenso ist er verpflichtet, das Zertifikat widerrufen zu lassen, wenn die Angaben im Zertifikat nicht mehr richtig sind. Er darf nur die vom ZDA bereitgestellten oder empfohlenen Hash- und Signatur-Verfahren verwenden, wenn eine sichere Signatur erstellt werden soll[35]. Dies gilt nicht für einfache oder fortgeschrittene Zertifikate!

Im Gegensatz dazu ist der Zertifizierungsdiensteanbieter verpflichtet, den Zertifikatswerber umfassend, klar und allgemein verständlich zu unterrichten. Dies muss vor der Vertragsschließung erfolgen und hat entweder schriftlich oder auf einem dauerhaften Datenträger zu erfolgen (d.h. CD-ROM, aber wohl nicht E-Mail[36]). Der Zertifikatswerber ist vor Vertragsschluss bzw. bei der Zertifikatsausstellung über folgende Punkte aufzuklären (§ 20 Abs 1 SigG):

- Inhalt des Sicherheits- und Zertifizierungskonzeptes des ZDA
- Bedingungen der Verwendung des Zertifikates (Anwendungsbereichs- oder Transaktionswertsbeschränkungen), wenn zwangsweise vorgesehen oder gewünscht
- Erfolgte Akkreditierung des Zertifizierungsdiensteanbieters, sofern zutreffend
- Besondere Streitbeilegungsverfahren, sofern festgelegt
- Mögliche Rechtswirkungen des verwendeten Signaturverfahrens
- Pflichten eines Signators (siehe oben)
- Haftung des Zertifizierungsdiensteanbieters

I.8. Verwaltungsstrafbestimmungen

In § 26 des SigG sind einige Verwaltungsstrafbestimmungen festgelegt, welche aber nur dann zur Anwendung kommen, falls die Tat nicht nach anderen Gesetzen strenger zu bestrafen ist oder in die Zuständigkeit der Gerichte fällt (Subsidiarität).

Für den Benutzer ist relevant, dass eine Verwaltungsübertretung begeht, wer vorsätzlich fremde Signaturerstellungsdaten ohne Wissen und Willen des Signators missbräuchlich verwendet (Strafrahmen bis € 4.000). Wichtig zu beachten ist, dass auch eine Benutzung ohne Wissen des Berechtigten straflos ist, wenn sie in dessen Interesse erfolgt, also kein

[35] Andernfalls ist die Signatur ev. rechtlich nicht gültig (siehe § 2 Abs 3a SigG) bzw. die Haftung des ZDA fällt weg.

[36] Siehe dazu auch die Diskussion über "dauerhafte Datenträger" nach Fernabsatz und E-Commerce RL (**Fehler! Verweisquelle konnte nicht gefunden werden.**).

Missbrauch vorliegt, sowie wenn sie mit dessen Wissen und Willen erfolgt, z.B. zur Schädigung Dritter[37].

Für ZDA sind die Strafen zahlreicher und mit einem höheren Strafrahmen ausgestattet: Eine Verwaltungsübertretung mit Geldstrafe bis € 8.000 begeht, wer die Widerrufspflicht oder die Dokumentationspflicht verletzt oder den Zertifikatswerber nicht ordnungsgemäß unterrichtet. In allen diesen Fällen reicht schon die Verletzung in Beziehung auf einen einzelnen Benutzer aus. Mit bis zu € 16.000 werden ZDA bestraft, wenn sie verschiedene der Vorschriften verletzen, welche die Sicherheit in ihrem Betrieb oder die der Zertifikate gewährleisten sollen.

Weiters können Gegenstände, mit denen eine strafbare Handlung begangen wurde, für verfallen erklärt werden. Dies betrifft insbesondere Computer oder Geräte, mit denen Schlüssel berechnet wurden oder die zur Duplizierung von Erstellungsdaten dienen.

I.9. Derzeitige Parameter nach der SigVO

Einige wichtige Elemente der Signaturverordnung, welche die möglichen kryptographischen Verfahren, die Schlüssellängen und die Dauer deren Zulässigkeit beschreiben, sind:

- Gültigkeitsdauer von qualifizierten Zertifikaten: Maximal fünf Jahre
- Signaturerstellungsdaten sind mit physikalischen oder Pesudo-Zufallszahlengeneratoren zu erzeugen. Letztere sind jedoch mit echten Zufallszahlen zu initialisieren. Es dürfen dann maximal 100 Pseudo-Zufallszahlen erstellt werden. Größere Mengen sind zulässig, wenn kontinuierlich zumindest 8 tatsächlich zufällige Bits pro Ausgabewert integriert werden.
- Eine Signatur darf nur nach einer Autorisierung ausgeführt werden, z.B. Eingabe eines PIN oder Scannen des Fingerabdrucks. Eingabeerleichterungen sind explizit verboten und es sind Sicherungen gegen ausspähen oder ausprobieren einzurichten.
- Signaturerstellungsdaten für sichere Zertifikate (privater Schlüssel):
    - RSA, zumindest 1024 Bit Schlüssellänge
    - DSA, zumindest 1024/160 Bit Schlüssellänge
    - Vier DSA-Varianten auf Basis elliptischer Kurven, zumindest 160/10/200 Bit
    - Zulässige Hashverfahren: RIPEMD-160, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, Whirlpool
    - Zulässige Padding-Verfahren: EMSA-PKCS 1 (Version 1.5, 2.1); EMSA-PSS, ISO 9796 ds 2, ISO 9796 din rn, ISO 9796 ds 3

I.10. US Electronic Signatures Act

Bei diesem Bundesgesetz (USSigAct[38]) handelt es sich um eine breitere Regelung als bei der EU Signatur-Richtlinie, da auch el. Urkunden und Inhaberpapiere geregelt werden. Es

[37] Hier ist dann jedoch an (Computer-)Betrug zu denken.

[38] Abgedruckt in DuD 24 (2000), 1 Electronic Signatures in Global and National Commerce Act http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_bills&docid=f:s761enr.txt.pdf

betrifft jedoch ausschließlich den Handelsverkehr zwischen einzelnen Bundesstaaten sowie mit dem Ausland, nicht jedoch innerstaatlichen Handel, welcher Angelegenheit der einzelnen Bundesstaaten ist (es bestehen in jedem Staat separate Regelungen).

I.10.1. Elektronische Urkunden und elektronische Signaturen

Eine el. Signatur wird als Geräusch, Symbol oder Prozess definiert, der zu einer el. Urkunde hinzugefügt oder logisch mit ihr verknüpft ist und von einer Person mit der Absicht zu unterzeichnen erzeugt wurde. Es handelt sich daher um eine sehr breite Definition, die insbesondere vollkommen unabhängig von der verwendeten Technologie ist. Auch eine el. Urkunde wird sehr breit definiert: Ein Vertrag oder eine Urkunde, die mit elektronischen Mitteln erzeugt, generiert, gesendet, übermittelt, empfangen, oder gespeichert wird. Hierbei ist "elektronisch" extrem weit reichend zu verstehen: Auch optische und elektromagnetische Technologien oder solche mit ähnlichen Eigenschaften sind enthalten.

El. Signaturen oder Urkunden dürfen gegenüber handschriftlichen nicht diskriminiert werden, analog der EU-RL, sowohl als Beweismittel als auch beim Abschluss von Verträgen. Demgegenüber besteht jedoch ebenso keine Verpflichtung, sich dieser Möglichkeiten zu bedienen, ausgenommen für Behörden, welche entsprechende Anträge akzeptieren müssen (Title I Sec. 101 lit b Z 2), sofern es sich nicht um privatrechtliche Verträge mit ihnen handelt.

Weiters sind detaillierte Regelungen enthalten, in welchen Fällen eine el. Mitteilung an einen Konsumenten ausreichend und rechtsgültig ist (vorherige Zustimmung = opt-in, jederzeitige Widerrufsmöglichkeit, Information über Hard- und Software-Anforderungen etc.).

Auch Aufbewahrungsvorschriften können durch el. Urkunden erfüllt werden. Die enthaltene Information ist exakt zu repräsentieren und hat für alle beteiligten Personen zugänglich zu sein. Dies ist wohl besonders im Hinblick auf die Aufbewahrungsvorschriften für Belege sinnvoll.

Von Bedeutung ist weiters, dass auch höherwertige Formen durch el. Signaturen erfüllt werden können: Notarielle Beurkundungen oder besondere Beglaubigungen können durch el. Urkunden ersetzt werden, wenn sie mit der el. Signatur sowie ev. zusätzlichen erforderlichen Daten dessen versehen sind, der sie sonst handschriftlich beglaubigen müsste. Eine Notarsunterschrift kann daher voll rechtsgültig durch die el. Signatur eines Notars ersetzt werden.

Eine besondere Vorschrift sieht vor, dass el. Agenten im Geschäftsverkehr nicht diskriminiert werden dürfen. Erfolgt daher ein Teil eines Vertragsabschlusses automatisch (Hard-/Software), ist er dennoch rechtsgültig. Die el. Signatur eines Agenten ist daher rechtserheblich, auch wenn sie ohne direkte Beeinflussung oder ohne Aufsicht durch den Besitzer des Agenten erfolgte. Dies stellt in Österreich normalerweise kein Problem dar und gilt gleichfalls so: Wer sich eines Werkzeuges bedient, hat die damit verbundenen Folgen zu tragen.

I.10.2. Ausnahmen

Einige Bereiche sind, analog zur SigRL/SigG, vom Geltungsbereich ausgenommen (Title I Sec. 103):

- Rechtsgeschäfte des Erbrechts
- Adoption, Scheidung und andere familienrechtliche Angelegenheiten
- Alle handelsrechtlichen Angelegenheiten außer Kauf, Miete, schriftliche Verzichtserklärungen und unterschriebene Kaufverträge (UCC[39] 1 107, 1 206, Art. 2, 2A)

Folgende Dokumente müssen auch weiterhin in physikalischer Form ausgestellt werden und sind einer elektronischen Signatur/Übermittlung nicht zugänglich:

- Gerichtsdokumente (Urteile, schriftliche Anträge etc.)
- Beendigung von Infrastrukturleistungen (Wasser, Strom, Heizung, …)
- Bestimmte Mitteilungen (z.B. Kündigung) im Zusammenhang mit Mietverträgen oder Kreditverträgen für den Hauptwohnsitz einer Person
- Beendigung einer Kranken- oder Lebensversicherung sowie von Leistungen daraus
- Rückruf von Produkten oder Mitteilung über Produktfehler, welche Gesundheit oder Sicherheit beeinträchtigen können
- Begleitdokumente für Gefahrenguttransporte

I.10.3. Inhaberpapiere

Unter Inhaberpapieren versteht man Urkunden, bei denen der Rechtsbesitz schon durch den Besitz der Urkunde bewiesen wird, z.B. Schecks mit "Zahlung an den Überbringer", d.h. analog zu Geldscheinen. Dies ist natürlich bei el. Repräsentation ein besonderes Problem, da jederzeit absolut identische Kopien in beliebiger Anzahl hergestellt werden können. Mittels Kryptographie kann jedoch Ähnliches realisiert werden, doch ist dann keine Anonymität mehr gegeben.

Voraussetzung für die rechtliche Anerkennung sind:

- Eine einzige "Autoritative Kopie" muss existieren, die einmalig und identifizierbar ist.
- Sie muss den Besitzer und zusätzlich einen etwaigen Nachbesitzer angeben.
- Der Besitzer oder dessen Beauftragter muss die tatsächliche Kontrolle besitzen.
- Änderungen des Originals können nur mit Zustimmung des Besitzers durchgeführt werden. Unberechtigte Änderungen müssen erkannt werden können.
- Jede Kopie, sowohl des Originals wie auch von weiteren Kopien, ist eindeutig als solche zu identifizieren.

Weiters muss ein Besitzer nachweisen können, dass er Inhaber der autoritativen Kopie ist, d.h. Änderungen vornehmen und damit das Papier weiter übertragen kann.

[39] Uniform Commercial Code, das US Handelsrecht http://www.law.cornell.edu/ucc/ucc.table.html

I.11. Literatur

I.11.1. Allgemein

A-SIT: http://www.a-sit.at/

Baum, Michael: Die el. Identität? Der Name als Zertifikatsbestandteil - ein Interpretationsvorschlag, DuD 1999, 511ff

Bizer, Johann: Das Schriftformprinzip im Rahmen rechtsverbindlicher Telekooperation, DuD 1992, 169 ff

Bertsch, Andreas, Pordesch, Ulrich: Zur Problematik von Prozeßlaufzeiten bei der Sperrung von Zertifikaten. DuD 23, 9/1999, 514ff

Brenn, Christoph: Verbürgung durch mouse-click?, ecolex 1999, 243ff

Brenn, Christoph: Signaturgesetz, Wien: Manz 1999

Brenn, Christoph, Posch, Reinhard: Signaturverordnung, Wien: Manz 2000

Brisch, Klaus: Gemeinsame Rahmenbedingungen für el. Signaturen. Richtlinienvorschlag der Europäischen Kommission, CR 1998, 492ff

Dobbertin, Hans: Digitale Fingerabdrücke. Sichere Hashfunktionen für digitale Signaturen, DuD 1997, 82 ff

Erber-Faller, Sigrun: Notarielle Funktionen im el. Rechtsverkehr, DuD 1994, 680ff

Fallenböck, Markus, Schwab, Guido: Zu der Charakteristik und den Rechtswirkungen el. Signaturen: Regelungsmodelle in den USA und Europa, MR 1999, 370

Fischer, Peter; Köck, Heribert: Europarecht. 3. Auflage, Wien: Linde 1997

Forgó, Nikolaus: Was sind und wozu dienen digitale Signaturen?, ecolex 1999, 235ff

Forgó, Nikolaus: Sicher ist Sicher? - Das Signaturgesetz, ecolex 1999, 607ff

Fox, Dirk: Fälschungssicherheit digitaler Signaturen, DuD 1997, 69ff

Fox, Dirk: Zu einem prinzipiellen Problem digitaler Signaturen, DuD 1998, 386ff

Hammer, Volker: Signaturprüfungen nach SigI, DuD 2000, 96ff

Hein, Werner, Rieder, Markus: Digitale Signatur in den USA. Stand der Gesetzgebung und Praxis, DuD. Datenschutz und Datensicherheit 8/1997, 469

Jud, Waldemar, Högler-Pracher, Renate: Die Gleichsetzung el. Signaturen mit der eigenhändigen Unterschrift, ecolex 1999, 610ff

Kilches, Ralph: Electronic Commerce Richtlinie, MR 1999, 3ff

Kresbach, Georg: E-Commerce. Nationale und internationale Rechtsvorschriften zum Geschäftsverlehr über el. Medien. Wien: Linde 2000

Kuner, Chris, Barcelo, Rosa, Baker, Stewart, Greenwald, Eric: An Analysis of International Electronic and Digital Signature Implementation Initiatives. http://www.ilpf.org/groups/analysis_IEDSII.htm

Lenstra, Arten, Verheul, Eric: Selecting Cryptographic Key Sizes, DuD 2000, 166

Mack, HolgeR: Sperren von Zertifikaten in der Praxis – ein Fallanalyse, DuD 2001, 464f

Mayer-Schönberger, Viktor: Bedauerlich: Signatur-Dienstleister nach der SigV, ecolex 2000, 130f

Mayer-Schönberger, Viktor, Pilz, Michael, Reiser, Christian, Schmölzer, Gabriele: Signaturgesetz. Praxiskommentar, Orac: Wien 1999

Menzel, Thomas, Schweighofer, Erich: Das österreichische Signaturgesetz. Umsetzung des EG-Richtlinienvorschlages in einem österreichischen Signaturgesetz. DuD 23, 9/1999, 503ff

Menzel, Thomas: El. Signaturen, Wien: Verlag Österreich, 2000

Miedbrodt, Anja: Regelungsansätze und -strukturen US-amerikanischer Signaturgesetzgebung, DuD. Datenschutz und Datensicherheit 7/1998, 389

Nöcker, Gregor: Urkunden und EDI-Dokumente, CR 2000, 176ff

Öhlberger, Veith: Die el. Signatur im österreichischen Recht: Ein Überblick. In: Schweighofer, Erich, Menzel, Thomas, Kreuzbauer, Günther (Hg.): Auf dem Weg zur ePerson. Wien: Verlag Österreich 2001

Pordesch, Ulrich: Risiken el. Signaturverfahren, DuD 1993, 561ff

Schumacher, Stephan: Digitale Signaturen in Deutschland, Europa und den U.S.A. Ein Problem, zwei Kontinente, drei Lösungen?, Computer und Recht 12/1998, 758

Sonntag, Michael: Electronic Signatures for Legal Persons. In: Hofer Susanne, Beneder Manfred (Ed.): IDIMT-2000. 8th Interdisciplinary Information Management Talks. Linz: Universitätsverlag Rudolf Trauner 2000, 233ff

Sontag, Michael: El. Signaturen. Rechtswirkungen, Haftung von ZDA sowie Sonderprobleme. In: Plöckinger, Duursma, Helm (Hrsg.): Aktuelle Entwicklungen im Internet-Recht. Wien: NWV 2002

Sterbenz, Andreas: Digitale Signaturen - Eine Einführung. Institut für Angewandte Informationsverarbeitung und Kommunikationstechnik, TU Graz. http://akitsicherheit.iaik.tu-graz.ac.at/DiGSig-prinzip.htm (16.3.2000; nicht mehr online)

Telekom Control Kommission: Aufsichtsstelle für el. Signaturen http://www.signatur.rtr.at/de/index.html

Telekom Control Kommission: Sicherheits- und Zertifizierungskonzept (Certification Practice Statement) http://www.signatur.rtr.at/de/repository/tkk-cps-14-20060612.html

Telekom Control Kommission: Positionspapier der Aufsichtsstelle zu § 2 Z 3 lit.a bis d SigG ("fortgeschrittene el. Signatur") http://www.signatur.rtr.at/de/repository/rtr-advancedsignature-10-20040413.html

Timm, Birte: Signaturgesetz und Haftungsrecht, DuD 1997, 525ff

Zieschang, Thilo: Sicherheitsrisiken bei der Schlüsselzertifizierung, DuD 1997, 341ff

I.11.2. Rechtsvorschriften

SigRL: Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für el. Signaturen, ABl. 19.1.2000 L 13/12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:DE:HTML

EC-RL: Richtlinie 2000/31/EG des Europäischen Parlamentes und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des el. Geschäftsverkehrs, im Binnenmarkt ("Richtlinie über den el. Geschäftsverkehr"), ABl. 17.7.2000 L 178/1 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:DE:HTML

SigG: Bundesgesetz über el. Signaturen (Signaturgesetz - SigG), BGBl I 190/1999 idF BGBl I 8/2008

SigVO: Verordnung des Bundeskanzlers über el. Signaturen (Signaturverordnung 2008 – SigV 2008) vom 7.1.2008, BGBl II 3/2008

Bericht des Justizausschusses über die Regierungsvorlage (1999 der Beilagen): Bundesgesetz über el. Signaturen (Signaturgesetz – SigG) JAB 2065 BlgNR XX. GP http://www.parlinkom.gv.at/pls/portal/docs/page/PG/DE/XX/I/I_02065/FNAMEORIG_000000.HTML

Verordnung des Bundesministers für Finanzen, mit der die Anforderungen an eine auf el. Weg übermittelte Rechnung bestimmt werden, BGBl. II Nr. 583/2003

Electronic Signatures in Global and National Commerce Act, DuD 24 (2000), 1 http://www.dud.de/dud/documents/usesignact0608.pdf

Uniform Commercial Code http://www.law.cornell.edu/ucc/ucc.table.htm