PGP-Zertifikate

„...des Signaturrechts vergessene Kinder?“

Die Teilnahme am Rechtsleben mit OpenPGP im europäischen und österreichischen Rechtsrahmen

Studie im Rahmen der netidee 2007

mit freundlicher Unterstützung der Internet Privatstiftung Austria (IPA)

Ziviltechniker DDipl.-Ing. Gernot W. Schmied

Gernot Schmied

Digital unterschrieben von Gernot Schmied
DN: cn=Gernot Schmied, sn=Schmied, givenName=Gernot, initials=0, c=AT, l=Wien, o=Ingenieurkonsulent für Wirtschaftsingenieur-, ou=wesen für Informatik & für technische Physik, title=DDipl.-Ing.MSc, serialNumber=668521725337
Grund: Ich bin der Verfasser dieses Dokuments
Speicherort: Wien
Datum: 2008.06.23 09:00:35 +02'00'

Inhaltsverzeichnis

1. Vorwort

Die vorliegende Studie untersucht die Verankerung der elektronischen Signatur- und Verschlüsselungs-Suite *„Pretty Good Privacy" (PGP)* im österreichischen und EU-weiten Rechtsrahmen anhand ihrer führenden quelloffenen (*„GNU Privacy Guard"*, GnuPG) und kommerziellen (PGP Corp.) Implementierungen in Form der OpenPGP-Standards. Die technische und konzeptionelle Erörterung der Wesensunterschiede, Stärken und Schwächen von PGP einerseits und X.509 andererseits beschränkt sich dabei auf das für die grundsätzliche legistische Diskussion erforderliche Ausmaß, Basiskenntnisse des Signaturwesens werden vorausgesetzt.

Detaillierte Erörterungen der elektronischen Willenserklärung *per se*, der kryptographischen Methoden der PGP-Implementierungen und des Umgangs mit elektronischen Signaturen in *Legal Proceedings* würden ebenso den Rahmen dieser Studie sprengen wie z.B. Rechtsvergleiche mit den U.S. Digital Signature Acts. Aufgrund dieser Komplexität und Vielschichtigkeit der Materie habe ich die Absicht, die angesprochenen technischen und rechtlichen Themen in Form einer Dissertation zu vertiefen und das Ergebnis ebenfalls der Allgemeinheit zur Verfügung zu stellen.

Die Studie wendet sich an Rechtserzeuger, -pfleger und -anwender, somit an alle Stakeholder, die mit der Gestaltung des und der Teilnahme am Rechtsleben der Informationsgesellschaft in unterschiedlichen Rollen und mit unterschiedlichen Anforderungen zu tun haben oder an Weichenstellungen beteiligt sind. Ihr Ziel ist es, dem privaten, dem unternehmerischen und dem öffentlich-rechtlichen PGP-Anwender einen Überblick über die Möglichkeiten zur Teilnahme am Rechtsleben in einem *de facto* X.509-lastigen Rechtsrahmen zu geben. Sie soll aber auch der Sensibilisierung der Adressaten für die enorme Wichtigkeit signaturrechtlicher Weichenstellungen, Begriffsdefinitionen und Rahmenvorgaben für die Entwicklung der Informationsgesellschaft dienen.

Ich bedanke mich herzlich bei der Internet Privatstiftung Austria (IPA) für die finanzielle Unterstützung dieser Studie, bei Herrn Werner Koch vom GnuPG-Projekt für das Feedback, bei Herrn Ing. Wolfgang Fabics für die kritische Durchsicht des Manuskripts und wertvolle Anregungen sowie bei Herrn Christian Kirsch (PGP Corp.) für detaillierte Auskünfte über das PGP Open Directory sowie andere kommerzielle Verbreitungskennzahlen.

Abschließend darf ich darauf hinweisen, dass ich Ziviltechniker für Wirtschaftsingenieurwesen für Informatik und technische Physik bin, kein ausgebildeter Jurist. Diese Studie reflektiert deshalb zwar einerseits meine berufliche Erfahrung mit technischen und materierechtlichen Normen und andererseits mein persönliches Interesse an der Querschnittsmaterie Informatikrecht; sie gibt aber ausschließlich meine rein persönliche Einschätzung wieder und erhebt keinesfalls den Anspruch, ein einschlägiger juristischer Leitfaden zu sein.

Wien, im Juni 2008

Ziviltechniker DDipl.-Ing. Gernot Schmied

IKTech Ziviltechnikerbüro für Informations- & Kommunikationstechnologie

2. Urherberschaft, Verbreitung und Verwertung

3. Begriffskonvention

Im folgenden Text wird der Begriff „PGP“[1] aus historischen Gründen gelegentlich als Überbegriff für die vorhandenen freien und kommerziellen Implementierungen der OpenPGP Standards und das Wesen der *„Web Of Trust“*-Architektur verwendet, sofern er sich aus dem Kontext oder einem expliziten Hinweis heraus nicht auf ein Produkt oder die Implementierung der PGP Corporation bezieht.

Aus Gründen der Konsistenz und Begriffssorgfalt wird in dieser Studie im Zusammenhang mit unterschriebenen (signierten bzw. beglaubigten) öffentlichen PGP-Signaturschlüsseln von PGP-Zertifikaten gesprochen und nicht – wie umgangssprachlich üblich – pauschal von *PGP Keys*. Der Begriff des Schlüssels (*„Key“*) ist den zugrunde liegenden *Private/Public Keys* bzw. *Keypairs* oder *Keyrings* vorbehalten.

1 "PGP" und "Pretty Good Privacy" sind registered trademarks der PGP Corporation

4. Kernfragen der Studie

Im Zusammenhang mit der Recherche der Rechtsstellung von OpenPGP Zertifikaten bzw. damit erstellter elektronischer Signaturen (Unterschriften) ergaben sich folgende Kernfragen:

- Welche Rechtsfolgen sind an die Verwendung von PGP (auf Basis von OpenPGP) ggw. gebunden? Welchen rechtlichen Status haben solchermaßen signierte Dokumente *de facto* und *de iure*?
- Wie sind Beweiswert und Beweiskraft PGP-signierter Dokumente einzuschätzen?
- Was bedeutet dies für die Teilnahme am Rechtsleben der Informations-gesellschaft für natürliche und juristische Personen?
- Ist PGP *de iure* und *de facto* der X.509-Suite gleichgestellt oder nicht (Diskriminierungsverbot, *„Negative Incentives“*, Suggestivformulierungen)? Woher stammt die *de facto* X.509-Lastigkeit des europäischen Signaturrechts?
- Sind Aussteller und Beglaubiger (*Notary Services, Key-signing Parties*) von PGP-Zertifikaten Zertifizierungsdiensteanbieter (ZDA)? Entsteht aus der Einbindung von ZDA in das *PGP Trust Model* Rechtssicherheit?
- Eignet sich PGP für die Erstellung qualifizierter Zertifikate und Signaturen? Falls nein: Woran scheitert dies?

5. Einleitung und historischer Rückblick

Die Studie behandelt den ggw. Stand der Technik auf Basis der OpenPGP Standards und befasst sich explizit nicht mit historischen PGP-Releases, z.B. denen des *International PGP Project* (PGPi). Dies gilt auch für die Betrachtung der Internet PGP Keyserver, hier werden eingedenk der erheblichen Mannigfaltigkeit die nach subjektiver Meinung des Autors ggw. vielversprechendsten, modernsten und öffentlich zugänglichen Implementierungen erörtert (*Global Directory* der PGP Corp. und der freie Keyserver-Verbund auf Basis SKS). Diese Auswahl ist jedoch mit keinerlei Wertigkeitsaussage hinsichtlich anderer Keyserver-Betreiber und -Implementierungen verbunden.

5.1. von Phil Zimmermann bis GnuPG & PGP Corp.

Die Erfolgsgeschichte von PGP reicht zurück bis in das Jahr 1991. Damals wurde PGP von Phil Zimmermann entwickelt und im Internet als Freeware zur Verfügung gestellt. Zimmermann wurde damit zu einer Galionsfigur der Bürgerrechtsbewegung und des *Digital Privacy Movement,* PGP die Instrumentalisierung der Auflehnung gegen überwachungsstaatliche Unterwanderung der digitalen Privatsphäre. Dies resultierte in einer dreijährigen Untersuchung der U.S.-Regierung bzgl. des Vorwurfs der Verletzung von Patenten und Exportbestimmungen für kryptographische Software, die allerdings 1996 eingestellt wurde. Die Ursprünge von PGP sind daher im Schutz der Privatsphäre (Vertraulichkeit) zu sehen, daraus erklärt sich auch der historische Einsatzbereich als Transportsicherung für E-Mail unter den Paradigmen *„no backdoors“* (nur bei Quelloffenheit glaubwürdig) und starker Kryptographie

bestehend aus asymmetrischer (*Private/Public Key*) und symmetrischer Verschlüsselung. Die unterschiedlichen PGP Versionen bildeten die Entwicklungsbasis für die späteren OpenPGP-Standards.

Meilensteine der Entwicklung:

- 1991 Phil Zimmermann stellt PGP 1.0 im Internet zur Verfügung
- „PGPi Scanning Project“ nützt U.S.-Gesetzeslücke und exportiert den PGP Source Code in gedruckter Form
- seit 1998 offener IETF Draft-Standard „OpenPGP“ (RFC2440, 2440bis); Pflege des Standards durch die OpenPGP-Arbeitsgruppe der IETF und (seit 2001) durch die OpenPGP Alliance
- 1999 lockert die U.S. Regierung die Exportkontrolle für kryptographische Software
- 2001 wird die OpenPGP Alliance von Phil Zimmermann gegründet
- 2007 feierte das GnuPG Projekt 10-jähriges Jubiläum und die PGP Corporation 5-jähriges Bestehen, neuer RFC4880

kommerzielle Involvierung:

- 1994 Viacrypt
- 1996 Zimmermann gründet PGP Inc., Merger mit Viacrypt
- 1997 Rechte von *Network Associates International* (NAI) gekauft
- seit 2002 Rechte von PGP & „Pretty Good Privacy“ bei der PGP Corporation (Markeninhaber und Marktführer bei kommerziellen Produkten auf Basis OpenPGP)

5.2. Verbreitung von OpenPGP (GnuPG & PGP Corp.)

Kommerzielle wie auch freie PGP-Implementierungen haben die Entwicklung der Internet- und Open Source Community seit 1991 begleitet und sind durch hohe Akzeptanz in allen gesellschaftlichen Schichten und Altersgruppen geprägt. Darauf weist auch der rege Zustrom zu regelmäßig und in großer Anzahl international veranstalteten *„Key-Signing Parties“* hin.

Es ist wohl generell genauso unmöglich, quantitative Aussagen über die Anzahl weltweit verwendeter PGP-Zertifkate zu treffen, wie dies für X.509 der Fall ist. Dies liegt einerseits im Wesen der Zertifikatsserver und in deren eingeschränktem Abgleich begründet, andererseits auch in der nicht abschätzbaren Anzahl von Benutzern, die PGP-Zertifikate als Attachment oder konventionelle E-Mail-Signatures[2] verwenden. Ebenso ist es ohne empirische Umfragen unmöglich, die Zahl der in Unternehmen oder Insel-Communities verwendeten X.509-Zertifikate und Certificate Authorities (CAs) abzuschätzen, ebensowenig wie die Anzahl der PGP-Keyserver von Unternehmen und deren Repository-Größe.

2 Gemeint ist hier z.B. ein Firmenbanner und nicht eine kryptographische Unterschrift im Sinne einer „elektronischen Signatur“.

Dennoch seien an dieser Stelle einige Anhaltspunkte dargelegt:

- Nach eigener Auskunft verwaltet die A-Trust GmbH in Österreich zwischen ca. 150.000 und 200.000 X.509-Zertifikate unterschiedlichster Ausprägung über deren gesamten Lebenszyklus, einschließlich widerrufener und abgelaufener Zertifikate.
- Lt. aktuellen Angaben verwaltet CACert 340.000 Zertifikate, von denen dzt. 115.000 verifizierten Benutzern zugeordnet sind.
- Gemäß eigener Angaben der PGP Corporation befinden sich ggw. ca. 100.000 PGP-Zertifikate im Open Directory.

  Anmerkung: *Diese Zahl bezieht sich auf ausschließlich aktive und validierte Zertifikate. Die Zertifikate müssen alle sechs Monate vom Benutzer bestätigt werden, es handelt sich dabei nur um private Nutzer (Einzellizenzen).*
- Die PGP Corporation betreut nach eigenen Angaben 90.000 Firmenkunden, wovon ein erheblicher Anteil eigene Keyserver betreibt.
- Die Synchronisationsbasis eines der führenden freien Keyserver-Verbunde (SKS OpenPGP) beträgt ca. 2.600.000 Keys, die Keyserver gleichen sich mit durchschnittlich 5 – 20 anderen Keyservern des Verbundes (*„Gossip Peers“*) ab.
- Gemäß einer Studie der Zeitschrift KES gemeinsam mit Microsoft (http://www.kes.info) wurde unter deutschen Unternehmen (keine Privatbenutzer) angefragt, welchen Verschlüsselungsstandard sie für E-Mail-Verschlüsselung verwenden. Die Verteilung ergab 2/3 OpenPGP, 1/3 S/MIME.

6. Anforderungen der Informationsgesellschaft

6.1. wirtschaftliche und gesellschaftliche Aspekte – das Wesen der Informationsgesellschaft

Legisten und Politiker hängen gleichermaßen gerne der Sichtweise an, die Informationsgesellschaft sei eine Industriegesellschaft mit Internet- und Computer-„Anhängsel“, anstatt sie als neue Gesellschaftsform mit völlig anderen Gesetzmäßigkeiten, Gebarungen, Anforderungen, anderer Dynamik und anderen sozio-kulturellen Ausprägungen zu erkennen.

Es wurde verabsäumt, die Zeichen der Zeit zu erkennen und sich rechtzeitig zu fragen, ob der teilweise noch aus der Monarchie stammende Rahmen unserer Rechtsordnung diesen Anforderungen gewachsen ist und inwieweit Analogieschlüsse aus der „Papierwelt“ überhaupt praktikabel sind. Diese Unterschätzung erklärt die erheblichen Schwierigkeiten vieler materierechtlicher Ansätze, die Inhomogenität der Querschnittsmaterie und die Verwunderung, fehlende Akzeptanz und teilweise Ablehnung der Bevölkerung trotz aufwendigem Lobbying.

Ein prominentes Beispiel für diese Schwierigkeiten ist die Geschichte unseres österr. Signaturrechts mit der anfänglichen Übernormierung bei gleichzeitig unglücklich gewählten Begriffsdefinitionen sowie das darauffolgende und in der ggw. Fassung des SigG abgebildete „Zurückrudern zum Richtlinien-Ausgangspunkt“.

Die wirtschaftliche und gesellschaftliche Bedeutung sind schwer voneinander zu trennen, dies liegt im Wesen der Sache begründet: Die Informationsgesellschaft entscheidet sich aufgrund von länderübergreifendem Konsens und gemeinsamer Sicht von Vorteilen für Anwendungen und Prozeduren der Informationstechnik und verwendet diese sowohl im privaten als auch beruflichen bzw. unternehmerischen Umfeld (*„Pervasive Use“*). Auf diese Weise entstehen *de facto* Standards, Handelsbräuche und Verkehrssitten der Informationsgesellschaft. Vor dem Ergreifen legistischer Maßnahmen sollte zudem darauf Bedacht genommen werden, dass diese Entscheidungs- und Innovationszyklen i.d.R. wesentlich schneller ablaufen als rechtliche Regelungen dies abbilden können.

Die Informationsgesellschaft hängt wesentlich weniger von „Face-To-Face“-Kommunikation und Interaktion ab als die „herkömmliche“ (vor-)industrielle Gesellschaft. Entfernungen spielen keine Rolle, die sozialen Strukturen im Internet nehmen völlig neue Formen an (Communities; Social, Business & Government Networks; Foren usw.). Es wäre daher wichtig, diesen Gegebenheiten bei der Entwicklung eines materierechtlichen Rahmens im Bereich des Daten-, Informations- und Telekommunkationsrechts Rechnung zu tragen und mit Fingerspitzengefühl aus einer schwierig zu überblickenden Querschnittsmaterie ein intuitiv-konsolidiertes und zeitgemäßes Informationsrecht zu schaffen.

Besondere Bedeutung kommt hier dem Gesetzwerdungsprozess zu. Die Informationsgesellschaft erreicht einen Konsens durch unbehinderte öffentliche Diskussion und Feedback-Prozeduren aller interessierten Kreise. Gesetzesentwürfe zum Informationsrecht erfordern daher umfangreichere Involvierung der Stakeholder. Man kann hier auch nicht von einer isolierten österr. Informationsgesellschaft sprechen, da sich der oben beschriebene Konsens bzw. die Ausübung der Wahlfreiheit auf globaler Ebene abspielen.

6.2. Rollen von Signatur und Verschlüsselung

Die Anwendungsszenarien sind für X.509 und OpenPGP nahezu wesensgleich. Das Anliegen besteht einerseits im Vertraulichkeits- und Manipulationsschutz von gespeicherten Daten bzw. der Datenübertragung über unsichere Kanäle (z.B. E-Mail-Transport), andererseits im rechtssicheren Nachweis der Identität bzw. damit verbundener Abgabe elektronischer Willenserklärungen. Legisten sprechen in diesem Zusammenhang gerne vom Nachweis der Herkunft und der Unversehrtheit des Inhalts eines Dokuments oder einer Erklärung.

Diente – wie eingangs erwähnt – PGP vorwiegend der Vertraulichkeit der elektronischen Korrespondenz durch Verschlüsselung, so tritt dieser Aspekt im Signaturrecht (richtigerweise) in den Hintergrund. An dieser Stelle sei dennoch positiv hervorgehoben, dass die Europäische Union sich – im starken Gegensatz zu den USA – historisch grundsätzlich für einen liberalen und freien Umgang mit Verschlüsselungstechnologie ausgesprochen hat und und sich zum Schutz der Privatsphäre bekennt. Selbst in den USA wurden auf Druck der Bevölkerung und der Wirtschaft Exportbestimmungen für kryptographische Software gelockert. In welche Richtung sich die etwaige rechtliche Normierung hierzulande entwickelt, bleibt abzuwarten. Es steht zu hoffen, dass aufgrund der besorgniserregenden aktuellen Entwicklungen in Richtung „Überwachungsunion“ auf europäischer Ebene nicht auch diese Freiheit einem schleichenden, aber fatalen

Paradigmenwechsel (*„Wer verschlüsselt, hat sicher etwas zu verbergen“*) zum Opfer fallen wird.

Auch die heute im Privatgebrauch überwiegende Verwendung als „Transportsiegel“ (Unversehrtheit des Inhalts) spielt *per se* kaum eine Rolle im Signaturrecht. Rechtlich bedeutsam wird diese Integritätsfunktion lediglich als Mittel zur sicheren logischen Verknüpfung signierter Daten mit einem elektronischen Zertifikat, über das die Authentifizierung der Mitteilung und die Identifizierung des Absenders bzw. Erklärenden erfolgen können.

7. OpenPGP Public Key Infrastructure (PKI)

Public Key Infrastructures (PKI) sind das Herzstück von Zertifikats-Architekturen. Sie stellen ein Repository von öffentlichen Zertifikaten bereit, pflegen dieses (Housekeeping, E-Mail-Validierung, Life-Cycle Management) und beantworten Validierungsanfragen von Anwendungen oder Personen. Erst PKI gewährleisten den skalierbaren Umgang mit Zertifikaten.

7.1. Standardisierung & kryptographische Verfahren

PGP verwendet bewährte kryptographische Verfahren (Transformationen, Hashes usw.[3]) nach dem Stand der Technik und unterscheidet sich darin nicht wesentlich von X.509. Das Kernparadigma der GnuPG-Implementierung ist darüber hinaus der Einsatz von ausschließlich patentfreien[4] kryptographischen Verfahren.

OpenPGP ist innerhalb der IETF-Arbeitsgruppe „An Open Specification for Pretty Good Privacy“ spezifiziert:

„PGP is used both for protecting e-mail and File Storage. It presents a way to digitally sign and encrypt information "objects." As such it is well suited for any store and forward application. The goal of the OpenPGP working group is to provide IETF standards for the algorithms and formats of PGP processed objects as well as providing the MIME framework for exchanging them via e-mail or other transport protocols.“

Quelle: http://www.ietf.org/html.charters/openpgp-charter.html

Die OpenPGP Alliance (http://www.openpgp.org) hingegen kümmert sich um Implementierungsaspekte und ist um Kompatibilität und Interoperabilität verschiedener Hersteller und Produkte untereinander bemüht.

Die wesentlichen IETF-Standards zu PGP sind:

- RFC3156 - MIME Security with OpenPGP
- RFC4880 - OpenPGP Message Format

7.2. Keyserver, Keyserver-Abgleich, Verteilung & Verbreitung von PGP-Zertifikaten

Inhaber von PGP-Zertifikaten können Kommunikationspartnern ihre *Public Keys* auf verschiedene Weise mitteilen: entweder als Attachment bzw. konventionellen

3 Eine ECC-Erweiterung (Elliptic Curve Cryptography) wird gerade in der IETF-WG diskutiert.
4 In der Zwischenzeit sind etliche Patente ausgelaufen (z.B. RSA).

E-Mail-Signature-Text innerhalb einer E-Mail oder als durch den Upload zu einem oder mehreren Keyservern (in diesem Fall reicht ein Hinweis auf die Key-ID und/oder den Fingerprint in allen sonstigen Mitteilungen aus). Keyserver können öffentlicher oder unternehmensinterner/privater Natur sein und können in diversen Applikationen als Abfrageziel hinterlegt werden. Keyserver können ferner ihr Repository an Zertifikaten mit anderen privaten oder öffentlichen Key-Servern abgleichen oder sich dafür entscheiden, dies nicht zu tun. PGP bildet somit eine verteilte und dezentrale Zertifikats-Infrastruktur.

Alle heutigen Keyserver sind OpenPGP-konform, unterstützen mehrere Synchronisations- und Abfrageprotokolle und verfügen i.d.R. über ein Web-Frontend für Key-Upload und Validierung.

Anfragen an Keyserver erfolgen via HKP (HTTP-based port 11371), LDAP, oder HTTP Port 80.

Keyserver synchronisieren untereinander via E-Mail (PKS), HTTP/HKP oder LDAP, der SKS Keyserver-Verbund tut dies mittels SKS Synchronization (effektiver Reconciliation-Algorithmus).

Ferner besteht die Möglichkeit, PKI via DNS-Mechanismen zu betreiben und so die Vorteile von DNS (geographisch und logisch verteilt, stets gut erreichbare Server in der Nähe, Caching-Mechanismen usw.) zu nutzen:

- RFC4398 „Storing Certificates in the Domain Name System“
- draft-josefsson-cert-openpgp „OpenPGP data in the CERT RR“
- DNS Keyserver front-end und GnuPG DNS Keyserver Client plugin

Beispiele für prominente Keyserver:

- hkp://pgp.mit.edu:11371
- ldap://keyserver.pgp.com
- http://gnv.us.ks.cryptnet.net
- hkp://www.nongnu.org/sks/
- hkp://keyserver.ubuntu.com:11371/

7.3. Keyrings, Keyring-Manager & Passphrase-Agenten

Die Schlüsselverwaltung in einem Web Of Trust erfolgt mit Hilfe elektronischer „Schlüsselbunde“ (*Public Keyring & Private Keyring*), von denen jeder Benutzer zumindest diese beiden besitzt. Im öffentlichen Schlüsselbund (*Public Keyring*) eines Benutzers werden eigene und fremde öffentliche Schlüssel und die zugehörigen Zertifikate gespeichert, der private Schlüsselbund (*Private Keyring*) enthält eigene private Schlüssel.

Keyring-Manager verwalten und administrieren die lokalen PGP-Schlüsselbunde auf den Endsystemen der Benutzer und ermöglichen die Auswahl von Default-Schlüsseln. Sog. *Caching Agents* können für eine bestimmte Zeit eingegebene Passphrases für die Dauer einer Window-Manager-Sitzung, die Laufzeit einer Anwendung oder eine vordefinierte Zeitspanne zwischenspeichern; damit eignen sich diese Agenten auch für die Stapelverarbeitung.

Anmerkung: *Die Verwendung von Passphrase Caches u.ä. ist in Österreich für qualifizierte Signaturen nicht zulässig, Stapelsignaturen müssen also anderweitig unterstützt werden (§ 4 Abs. 2 SigV: „Eingabeerleichterungen bei wiederholter Eingabe von Autorisierungscodes müssen ausgeschlossen sein“).*

7.4. Behältnisse für PGP Private Keys – Schlüsselerzeugung, sichere Verwahrung und Zugriffschutz

Dafür werden bevorzugt Smart Cards (Chipcards), Smart Card Token (z.B. USB Sticks) sowie onboard TPM-Chips verwendet. Hierbei ist eine weitere Absicherung durch Fingerprint-Reader oder alternative Ansätze für 2- bzw 3-Factor Authentication möglich.

Geht es um die reine Aufbewahrungs- und Verlustsicherheit, so können kryptografische Dateisysteme herangezogen werden, z.B. auf Solid State Discs oder USB-Sticks. Es ist bei GnuPG und PGP gleichermaßen möglich, Keys auf bestimmten Chipkartentypen zu generieren oder auf solche zu importieren (z.B. Aladdin eToken PRO, g10 Code OpenPGP Card). Dabei kann bei GnuPG nur zum Zeitpunkt der Erzeugung des Schlüsselpaars ein Backup gezogen werden; nimmt man diese Option nicht in Anspruch, so ist ein nachträgliches Auslesen des privaten Schlüssels nicht mehr möglich. Weiters gehört es zur empfohlenen Standardprozedur im Umgang mit PGP Keys, bei der Schlüsselerstellung ein eigenes Widerrufszertifikat (*Revocation Certificate*) zur allfälligen späteren Verwendung zu generieren. Der große Vorteil besteht darin, dass von PGP-Schlüsseln einfach Sicherungskopien erstellt werden können (zuverlässige Aufbewahrung), die bei Bedarf (z.B. bei defektem oder technisch überholtem Trägermedium) einfach auf einen neuen/besseren Zertifikatsträger geladen werden. Zudem haben solcherart Änderungen im Bereich des Zertifikatsträgers keinen Einfluss auf die Gültigkeit des Zertifikats.

7.5. Vertrauensmodelle („Trust Models“)

Einleitend sei festgehalten, dass es drei unterschiedliche Ausprägungen von Trust Models gibt: verteilte wie bei PGP, zentralistische wie bei X.509 und hybride Ansätze, die ein "X.509 Web Of Trust” zu realisieren versuchen (z.B. CACert & Thawte).

Das streng hierarchische PKI-Modell von X.509 basiert auf der impliziten Annahme der Vertrauenswürdigkeit und Sicherheit einer „Wurzelinstanz“ (*„Root CA“*), die damit aber auch einen „Single Point Of Failure“ darstellt.

Anmerkung: *Bilaterale Cross-Zertifizierung bzw. "Hub & Spoke-Architekturen" via neutraler Bridge-CA sind keine befriedigenden Lösungen für dieses inhärente Defizit.*

PGP hingegen verwendet ein verteiltes *„ad hoc“ Trust Model*, d.h. zum Zeitpunkt der Entscheidung über die Vertrauenswürdigkeit eines Zertifikates wird das persönliche Web Of Trust (die eigene Sicht der Welt) konsultiert.

Besonders stark wird der Unterschied zwischen PGP und X.509 darin spürbar, dass ein Benutzer einem anderen unterschiedliche Stufen des Vertrauens aussprechen kann und sich dies noch in zwei wichtige Aspekte unterteilt, nämlich: „Wie sehr vertraue ich darauf, dass derjenige tatsächlich der ist, der er in seinem Zertifikat zu sein vorgibt?“ *(PGP Validity)* und zusätzlich „Wie sehr vertraue ich darauf, dass diejenigen, deren Zertifikate seine Unterschrift tragen,

tatsächlich die sind, die sie in ihren Zertifikaten zu sein vorgeben?“ *(PGP Trust)*. Der Benutzer kann bei einem Zertifikat einen Trust Level (typischerweise *none, unknown, marginal* oder *full*) lokal hinterlegen. Die letztendliche Trust-Entscheidung bei Verwendung eines öffentlichen Zertifikats hängt von mehreren konfigurierbaren Parametern ab, wesentlich sind die Pfadlänge und die Anzahl der *marginally* und *fully trusted* Zertifikate.

Anmerkung: *Der Trust Level eines Schlüssels stellt eine private und lokal gehaltene Information dar (wird in in einer eigenen Trust-DB unabhängig von den Schlüsselbunden gespeichert und beim Export eines Schlüssels nicht mitgeschickt).*

Das PGP Trust Model stellt somit eine Übermenge dar, in dem das hierarchische X.509-Modell sowohl enthalten ist als auch willentlich gewählt werden kann. Es ist in der PGP-Welt ebenfalls möglich, dass alle Beteiligten ein und demselben Trust-Center als *Special Introducer* gleichermaßen vertrauen und dies lokal so hinterlegen. Damit verhält sich ein solches PGP Trust Model wie das von X.509. Die Erfahrung zeigt jedoch, dass die Internet-Community eher zur Abbildung von Social Networks neigt, für den Business-Anwender jedoch die zusätzliche Einbeziehung eines Trust Centers aus Gründen der Rechtssicherheit attraktiv sein kann. Die großen Vorteile von PGP liegen in der fehlertoleranten Architektur des verteilten Trust Models sowie einer besseren Kontrolle des Benutzers über seine Sicht der PGP-PKI.

Anmerkung: *Der PGP Universal Server kann neben OpenPGP auch X.509 Zertifikate sowohl als "subsidiary CA to a third-party CA" oder aber auch als "Self-Signed CA" ausstellen.*

7.6. ein Netz von Vertrauensbeziehungen: „Web of Trust“ – Konzept, Aufzucht & Hege

7.6.1. soziale Netzwerke & „*Introducer*“

Ein Web Of Trust entsteht aus unterschiedlichem Kontext, seien es nun soziale, geschäftliche oder sonstige Netzwerke (z.B. Vereine, Spiele-Communities, Foren). Wie bereits diskutiert manifestiert sich Vertrauen im Web Of Trust dadurch, dass eine Person als *„Trusted Introducer“* akzeptiert und eingestuft wird. Nehmen besonders vertrauenswürdige Entitäten an einem Web Of Trust teil, so spricht man im PGP-Jargon von *„Special Introducers“*.

Hier geht es also vorrangig um das Vertrauen in (dem Benutzer bekannte) Menschen, während die aktuelle Signaturgesetzgebung das Vertrauen in technische Methoden und betriebliche Abläufe bei den ZDA (die beide für den Benutzer i.d.R. undurchschaubar und eben nicht *a priori* vertrauenswürdig sind) reglementiert und durch hoheitliche Legitimation oder Akkreditierung in einen besonderen Vertrauens- und Sicherheitsstatus hebt.

7.6.2. Key-Signing Parties & Notary Services

Key-Signing Parties sind beliebte Veranstaltungen zur effektiven und sicheren Erweiterung des persönlichen Web Of Trust, dessen Qualität und Anwendungseffektivität ja nicht nur von den Credentials der Introducer, sondern auch vom Vernetzungsgrad und der Pfadtiefe abhängt.

Einen sehr effizienten Beginn der Aufzucht eines Web Of Trust stellt die Beglaubigung durch eine Stelle allgemein anerkannter oder hoheitlich verbriefter Glaubwürdigkeit (eines „Trust Center“) dar, z.B. durch Ziviltechniker, Notare oder akkreditierte Zertifizierungsstellen. Für viele Anwendungsfälle genügt dieses "verkürzte" Web Of Trust bereits für eine erhebliche rechtliche Beweiskraftsteigerung, die *de facto* Anwendungsnützlichkeit hängt jedoch nach wie vor von der Kultivierung des eigenen sozialen Netzwerks ab.

7.6.3. „Web Of Trust“-Visualisierung – Vernetzungsgrad, Güte & Ausdehnung

Zur besseren Veranschaulichung des Web Of Trust existieren einige Software-Tools, die graphisch den Grad der Vernetzung (Verbindungen) sowie die Teilnehmer (Knoten) und die Ausdehnung des eigenen sozialen Netzwerks darstellen; wichtige Parameter (Validity, Trust, Anzahl der Beglaubigungen eines Schlüssels usw.) können farblich hervorgehoben werden.

Beispiele mit Screenshots bzw. Web-Eingabemasken:

- pathfinder (http://pgp.cs.uu.nl)
- wotsap (http://www.lysator.liu.se/~jc/wotsap/index.html)
- sig2dot (http://www.chaosreigns.com/code/sig2dot)
- sims (http://tokkee.org/sims)

7.6.4. Widerruf & Ablauf von PGP-Zertifikaten

X.509 verwendet für diesen Zweck CRL und OCSP. Im PGP-Kontext laufen PGP-Zertifikate entweder durch zeitliche Begrenzung der Gültigkeit ab oder der Widerruf erfolgt mittels eines speziellen Update-Vorgangs an die Keyserver unter Verwendung eines (tunlichst bei der Schlüsselerzeugung generierten) *Revocation Certificate* (Schlüsselwiderruf-Zertifikats).

8. Teilnahme am Rechtsleben der Informationsgesellschaft mit PGP

8.1. europäischer Rechtsrahmen: die Signaturrichtlinie

Mit der Richtlinie 1999/93/EG (Signaturrichtlinie, SigRL) wurde versucht, einen europaweit harmonisierten Rahmen für den rechtlichen Umgang mit elektronischen Signaturen zu schaffen. Dies hatte man für erforderlich gehalten, nachdem sich bereits seit den frühen 90er-Jahren national tlw. höchst unterschiedliche Ansätze in diesem Bereich entwickelt hatten.

Die SigRL versucht zunächst, begriffliche Klarheit unter den Methoden für die Anbringung elektronischer Unterschriften zu schaffen, die zum Zeitpunkt ihrer Entstehung als im Rechtsleben gebräuchlich erkannt wurden:

8.1.1. „einfache“ elektronische Signaturen

Die Richtlinie kennt „elektronische Signaturen“ in Form eines Überbegriffs. Die „einfache“ elektronische Signatur wird üblicherweise (aber nicht in der SigRL expliziert) als diejenige Signatur verstanden, die nicht den nachfolgend dargelegten Anforderungen an höherwertige Signaturen (nämlich der fortgeschrittenen und der „qualifizierten“ Signatur) entspricht. Dabei wird in der Richtlinie ganz allgemein von *elektronischen Daten* gesprochen, *die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und der Authentifizierung dienen*. Darunter fallen definitionsgemäß alle, auch einfachste „Signaturverfahren“ wie z.B. das Einbetten eines gescannten Unterschriftszuges als Bild in eine Datei, das Fax eines unterschriebenen Dokuments oder auch die vom absendenden Faxgerät typischerweise angebrachte Informationszeile mit Uhrzeit, Anschlussnummer und dem Absendernamen. Grundsätzlich kann auch das Bereitstellen einer gesonderten Hash-Datei zur Prüfung einer anderen heruntergeladenen bzw. übermittelten Datei als einfache elektronische Signatur aufgefasst werden.

Leider wurde verabsäumt zu definieren, was unter „Authentifizierung“ konkret zu verstehen ist, insbesondere auch, welche rechtlichen Vermutungen bzgl. der signierten Daten eine erfolgreiche Authentifizierung nach sich ziehen kann oder muss. Aus den Materialien zur Richtlinie geht an einigen Stellen zwar hervor, dass die Richtliniengeber unter Authentifizierung die Feststellung der Echtheit der Herkunft signierter Daten verstehen dürften; es wird zwischen der *Authentizität* (Echtheit der Herkunft) und der *Integrität* (Unversehrtheit des Inhalts) der signierten Daten einerseits sowie der *Identität* des Unterzeichners andererseits unterschieden. Allerdings ist auch hier unklar, wie weit sich der Authentizitätsbegriff in der Beschreibung der „Herkunft“ erstrecken kann bzw. muss (Absender? Ersteller? Erklärender? Technische oder persönliche Merkmale?) und welche Rolle die tatsächliche Identifizierung des Unterzeichners dabei spielt.

8.1.2. fortgeschrittene elektronische Signaturen

Hier werden zusätzliche Forderungen an das Signaturverfahren erhoben, mit deren Erfüllung eine erhöhte Zuverlässigkeit (Nachprüfbarkeit und Nichtabstreitbarkeit) der elektronischen Signatur einhergehen soll. So muss eine fortgeschrittene elektronische Signatur

- *ausschließlich dem Unterzeichner zugeordnet sein*, wobei die Art und der Zeitpunkt dieser Zuordnung aber völlig offen bleiben;
- *die Identifizierung des Unterzeichners ermöglichen*, was z.B. eine eingescannte Unterschrift allerdings auch leisten könnte, Anforderungen an die Zuverlässigkeit der Identifizierung werden ja nicht erhoben; allerdings kann eine „einfache“ Signatur (z.B. die eingescannte Unterschrift) nicht
- *mit Mitteln erzeugt werden, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann*; hier kam und kommt es zu den meisten Fehlinterpretationen bei der Abbildung der Anforderung auf die technischen Rahmenbedingungen für fortgeschrittene Signaturen.

Explizit *nicht* gefordert ist nämlich, dass der Unterzeichner die Signaturmittel jederzeit unter seiner alleinigen Kontrolle halten *muss*, und schon gar nicht, dass die technischen Signaturmittel bzw. -verfahren dies *sicherstellen oder erzwingen* sollen (dergleichen wird nur für qualifizierte Signaturen gefordert!). Vielmehr geht es hier um eine weitere Abgrenzung zur einfachen Signatur, die nämlich typischerweise prinzipbedingt nicht in der alleinigen Kontrolle des Signators verbleiben *kann*. Bei der Übermittlung z.B. einer eingescannten Unterschrift oder eines Fax-Kennzeichengebers ist es ja bereits prinzipiell nötig und unvermeidbar, die Signaturdaten zu übermitteln, damit also aus der Hand zu geben. Der Unterzeichner muss deshalb die alleinige Kontrolle aufgeben und kann gar nicht beeinflussen, was der Empfänger oder allfällige Dritte mit seinen Signaturdaten möglicherweise anstellen; deshalb qualifizieren solche Verfahren nicht für die Erstellung einer fortgeschrittenen elektronischen Signatur und ist dies nach Überzeugung des Autors der einzige Definitionszweck dieser Bestimmung.

Anmerkung: *Gemäß dieser Definition sind nach dem dztg. Stand der Technik ausschließlich asymmetrische Public/Private Key Verfahren zur Erstellung fortgeschrittener Signaturen geeignet (die Signaturerstellungsdaten müssen beim Unterschreiben nicht aus der Hand gegeben werden, der Unterzeichner kann sie daher unter seiner alleinigen Kontrolle halten) und sie sind dies auf jeden Fall. . Hingegen ist dies mit rein symmetrischen Krypto-Verfahren nicht möglich, da hier ein gemeinsamer Schlüssel benötigt wird; sie fallen also trotz ihrer allenfalls hohen kryptographischen Sicherheit in die Kategorie der „einfachen“ Signaturverfahren.*

8.1.3. qualifizierte elektronische Signaturen

Dieser Begriff wird in der SigRL selbst nicht verwendet, sondern hat sich im Laufe der Zeit europaweit als Sammelbegriff für als besonders zuverlässig erachtete elektronische Signaturen gem. Art. 5 Abs. 1 SigRL etabliert. Bis zur SigG-Novelle 2007/2008 wurden diese Signaturen im österreichischen SigG als „sichere Signaturen“ bezeichnet.

Es handelt sich dabei um fortgeschrittene elektronische Signaturen, die zusätzlich

- auf einem *qualifizierten elektronischen Zertifikat* beruhen und
- von einer *sicheren Signaturerstellungseinheit* erstellt werden.

Hierbei müssen weitere Legaldefinitionen betrachtet werden, nämlich das

8.1.4. Zertifikat

als eine *elektronische Bescheinigung, mit der Signaturprüfdaten einer Person zugeordnet werden und die Identität dieser Person bestätigt wird*; wobei unter den „Signaturprüfdaten“ angesichts des dztgen. Standes der Technik schlichtweg der öffentliche Schlüssel eines Public/Private Keypairs zu verstehen ist (egal ob bei PGP oder X.509), sowie ein

8.1.5. qualifiziertes Zertifikat

als ein *Zertifikat, das die Anforderungen des Anhangs I erfüllt und von einem Zertifizierungsdiensteanbieter bereitgestellt wird, der die Anforderungen des Anhangs II erfüllt*.

Zum einen ist hier *nicht* gefordert, dass der ZDA das qualifizierte Zertifikat *ausstellt*, er braucht es nur *bereitzustellen*. Dies wäre vmtl. bereits dann der Fall, wenn jemand als Serviceleistung Zertifikate auf einem Server veröffentlicht (z.B. wenn Microsoft im Rahmen des „Windows Update“ Services ein Paket mit den aktualisierten Root-Zertifikaten der wichtigsten ZDA zum Download anbietet).

Anmerkung: *Bedeutet das nun, dass ein qualifiziertes Zertifikat, das von einem „qualifizierten ZDA“ gem. Anhang II ausgestellt wurde, dann seine „Qualifikation“ verliert, wenn es von einem „unqualifizierten ZDA“ bereitgestellt wird? Oder erlangt ein Zertifikat diese Qualifikation, wenn es zwar von einem „unqualifizierten ZDA“ ausgestellt wurde, dieser es jedoch einem „qualifizierten ZDA“ zur Veröffentlichung im Internet (= „Bereitstellung“) übergibt?*

Zum anderen ist in der Definition des qualifizierten Zertifikats an sich nicht festgelegt, in welcher Form oder Qualität die Zuordnung zu einer Person erfolgen kann oder muss. Dies geschieht erst einesteils in Anhang I, aus dem implizit hervorgeht, dass die Zuordnung zu einer Person über den Eintrag ihres Namens oder eines Pseudonyms im Zertifikat erfolgt, und andernteils in Anhang II, in dem die Prüfung der Identität dieser Person mit geeigneten Mitteln nach einzelstaatlichem Recht dem ausstellenden ZDA auferlegt wird (z.B. durch Vorlage eines amtlichen Lichtbildausweises).

Eine weitere beachtliche Rolle bei der Betrachtung der SigRL als Mittel zur Förderung beliebiger elektronischer Signaturverfahren spielt der

8.1.6. Zertifizierungsdiensteanbieter (ZDA)

Dieser ist definiert als *Stelle oder juristische oder natürliche Person, die Zertifikate ausstellt oder anderweitige Dienstleistungen im Zusammenhang mit elektronischen Signaturen bereitstellt.* Diese extrem weit gefasste Begriffsbestimmung bedeutet theoretisch nichts anderes, als dass jedermann, der irgendwelche Dienstleistungen im Signaturbereich (und sei es nur die Beratung darüber) erbringt, als ZDA einzustufen ist. Dies verdeutlicht zusätzlich die Formulierung des Erwägungsgrundes 9 der SigRL:

„Die Definition solcher Produkte und Dienste sollte sich nicht auf die Ausstellung und Verwaltung von Zertifikaten beschränken, sondern sollte auch alle sonstigen Dienste und Produkte einschließen, die elektronische Signaturen verwenden oder mit ihnen zusammenhängen, wie Registrierungsdienste, Zeitstempel, Verzeichnisdienste, Rechnerdienste oder Beratungsdienste in Verbindung mit elektronischen Signaturen.“

Abgesehen davon, dass sich der praktische Sinn einer solchen Generaldefinition *a priori* nicht erschließt, wäre zudem sinnvollerweise spätestens hier klar zu stellen gewesen, was unter dem „Ausstellen“ eines Zertifikats tatsächlich und konkret zu verstehen ist (insbesondere auch im Unterschied zur bloßen „Bereitstellung“ desselben, wie oben erwähnt). Die einzige ausschließlich anhand des Richtlinientexts konkludente Annahme dazu

ergibt sich aus der Definition des Zertifikats selbst: Es handelt sich dabei definitionsgemäß um eine *Bescheinigung, mit der Signaturprüfdaten einer Person zugeordnet werden und die Identität dieser Person bestätigt wird*. Daraus ergibt sich nun schlüssigerweise, dass das Ausstellen einer solchen Bescheinigung die Tätigkeiten der Personenzuordnung und der Identitätsfeststellung umfasst, nicht jedoch notwendigerweise die Erzeugung oder Bereitstellung der zu bescheinigenden Signaturprüfdaten oder des „Zertifikats-Containers“. Diese Annahme wird noch durch Bestimmung g) des Anhangs II untermauert, in der von *„Fällen, in denen [die ZDA] Signaturerstellungsdaten erzeugen“* die Rede ist; daraus muss geschlossen werden, dass auch andere Fälle denkbar sind.

Aus all dem ergibt sich, dass unter dem „Ausstellen“ eines Zertifikats wohl jedenfalls die Beglaubigung der im Zertifikat enthaltenen Angaben (durch Hinzufügen der eigenen elektronischen Unterschrift) zu verstehen sein wird, unabhängig davon, ob diese Angaben vom Zertifikatswerber oder vom ZDA im Zertifikat eingetragen wurden und insbesondere unabhängig davon, wer die zugrunde liegenden Signaturerstellungs- und -prüfdaten (das Public/Private Keypair) erzeugt hat. Allfällige Einschränkungen in der Mannigfaltigkeit dieser Aufgabenteilung ergeben sich wohl aus dem jeweils konkret eingesetzten technischen Verfahren, sind jedoch für die rechtliche Definition der Zertifikatsausstellung als Tätigkeit unbeachtlich.

Bei der Betrachtung der „qualifizierten elektronischen Signatur“ fehlt noch eine wichtige Definition, nämlich die

8.1.7. sichere Signaturerstellungseinheit (SSEE)

Die SigRL definiert diese (zusammengefasst) als *konfigurierte Software oder Hardware, die zur Implementierung der Signaturerstellungsdaten verwendet wird und die Anforderungen des Anhangs III erfüllt*. Da eine gesonderte Definition dessen fehlt, was unter der „Signaturerstellung“ zu verstehen ist, muss man also wohl hilfsweise davon ausgehen, dass damit die „Implementierung der Signaturerstellungsdaten“ gemeint ist. Was das wiederum genau heißen soll, erschließt sich leider weder aus dem Begriff der „Implementierung“ (der technisch alles mögliche bedeuten kann) noch aus der Definition der Signaturerstellungsdaten selbst; diese erfolgt nämlich nur eher beispielhaft als *„einmalige Daten wie Codes oder private kryptographische Schlüssel, die vom Unterzeichner zur Erstellung einer elektronischen Signatur verwendet werden“*. Betrachtet man übliche asymmetrische Private/Public Key Verfahren wie X.509 oder PGP, so dürfte der Begriff der „Signaturerstellungsdaten“ verschiedene Dinge umfassen, nämlich sowohl

- den privaten Schlüssel des Unterzeichners als auch
- den Hashwert über die zu unterzeichnenden Daten sowie
- die Berechtigungscodes, unter deren Eingabe der Signaturvorgang überhaupt erst ausgelöst werden kann (PIN-Code bzw. Passphrase).

Dies hat aber nun schwerwiegende Konsequenzen hinsichtlich dessen, was eine sichere Signaturerstellungseinheit konkret alles zu können hat, um den Anforderungen des Anhangs III zu entsprechen. Sie müsste dazu lt. Richtlinie u.a. sicherstellen, dass *die für die Erzeugung der Signatur verwendeten*

Signaturerstellungsdaten praktisch nur einmal auftreten können und dass ihre Geheimhaltung hinreichend gewährleistet ist.

Allein diese Anforderung führt zum logischen Schluss, dass eine sichere Signaturerstellungseinheit keinesfalls nur der „bloßen“ Signaturerstellung dienen darf. Vielmehr muss sie

- den Hashwert über die zu signierenden Daten ausschließlich selbst erzeugen,
- diesen Hashwert mit dem privaten Schlüssel des Unterzeichners verschlüsseln (was die eigentliche „Signaturerstellung“ bedeutet),
- diesen privaten Schlüssel vorher selbst erzeugt haben, deshalb auch
- den zugehörigen öffentlichen Schlüssel (also das Private/Public Keypair) selbst erzeugt haben,
- den privaten Schlüssel strikt geheimhalten und dessen Export keinesfalls zulassen; sie wird damit zum alleinigen Trägermedium des privaten Schlüssels bzw. des Keypairs.

8.2. Umsetzung in Österreich (SigG & SigV)

Da in der Novelle 2008 des Signaturgesetzes (SigG) eine weitgehende Annäherung an die Richtlinie vorgenommen wurde, sollen nachfolgend nur die im Zusammenhang mit PGP und der „täglichen“ Teilnahme am Rechtsleben relevantesten Punkte der Situation in Österreich herausgegriffen werden:

- Anders als in der SigRL besteht im SigG keine Einschränkung des Diskriminierungsverbots auf Gerichtsverfahren, es gilt also z.B. auch im Verwaltungsverfahren oder im Schiedsverfahren (also richtigerweise in allen *„Legal Proceedings“*).
- Stellt die SigRL es grundsätzlich frei, beliebige Zertifikate (inkl. qualifizierter Zertifikate) auch juristischen Personen („nichtnatürlichen Personen“ in neuerer Diktion der „Plattform Digitales Österreich“) auszustellen, so schränkt die österr. Gesetzgebung die Inhaberschaft von qualifizierten Zertifikaten auf natürliche Personen ein. Dies wird einerseits mit mangelndem Bedarf begründet (*„Auch juristische Personen handeln nur durch ihre zeichnungsberechtigten physischen Personen“*), andererseits als unabdingbare Notwendigkeit aufgrund der Gleichstellung mit der eigenhändigen Unterschrift dargestellt (z.B. in den Materialien zum SigG §2 Z 9: *„Insbesondere im Hinblick auf die Rechtswirkungen qualifizierter Signaturen ist es notwendig, dass es eine Beschränkung auf natürliche Personen gibt.“*).

  Anmerkung: *Der Autor kann beide Ansichten nicht teilen und hält diese für einen schwerwiegenden Nachteil. Nicht zuletzt die Erfahrungen mit der Verwaltungs- und der Amtssignatur, jedoch vornehmlich die Probleme bei der korrekten Abbildung öffentlicher Berufssiegel (z.B. bei Ziviltechnikern: persönliche Befugnisse <-> ZT-Büro als handelnde juristische Person) haben deutlich gemacht, wie nützlich – wenn nicht sogar unabdingbar – Zertifikate solch hoher Vertrauenswürdigkeit und Beweiskraft in einem durchgängigen Datenmodell der elektronischen Signatur sind bzw. wären. Schließlich müsste richtliniengemäß auch jede öffentliche Dienststelle in Österreich qualifizierte*

Zertifikate einer (EU-)ausländischen juristischen Person anerkennen, wenn in deren Sitzstaat solche Zertifikate ausgestellt werden (§ 24 Abs. 1 SigG). Wie verhält es sich in diesem Fall mit der Sicht auf die„eigenhändige Unterschrift“?

***Anmerkung:** Wie aus der der Beschreibung der österr. Bürgerkartenumgebung hervorgeht (http://www.buergerkarte.at), wird u.a. auch an eine Personenbindung für juristische Personen gedacht (über Verknüpfung mit den entsprechenden öffentlichen Datenbanken wie Firmenbuch od. Vereinsregister) – ein überaus begrüßenswerter Gedanke!*

- Mit der SigG-Novelle 2008 wurde aus Einheitlichkeitsgründen der Begriff der sicheren Signaturerstellungseinheit in die Definitionen des SigG aufgenommen. Bedeutsam ist dies v.a. im Zusammenhang mit § 18 Abs. 5, in dem nunmehr klargestellt wird, dass für qualifizierte Signaturen ausschließlich die „sichere Signaturerstellungseinheit“ von der Bestätigungsstelle bescheinigt werden muss (und nicht die gesamte Signaturumgebung).

  ***Anmerkung:** Noch eindeutiger hätte diese Feststellung wohl getroffen werden können, indem man anstatt der (aus Sicht der SigRL überflüssigen) Wortfolge „technische Komponenten und Verfahren“ sowohl im gesamten 5. Abschnitt des SigG als auch in der Nichtdiskriminierungsbestimmung des § 3 Abs. 2 einheitlich den Begriff „sichere Signaturerstellungseinheit“ verwendet hätte. Zudem ist immer noch nicht klar, wie ein Signator die in § 18 Abs. 5 geforderte „hinreichende und laufende Prüfung“ seiner SSEE bzw. der von ihr verwendeten technischen Komponenten und Verfahren bewerkstelligen sollte.*

- Eine immer noch vorhandenes und erstaunlich novellierungsresistentes "Austriacum" besteht darin, dass die SSEE lt. § 18 Abs. 2 die Darstellung der zu signierenden Daten vor Auslösen des Signaturvorgangs *ermöglichen* muss. Das ist mehr, als die SigRL in Anhang III fordert, nämlich dass die SSEE eine solche Anzeige nur *nicht verhindert* (z.B. über frei definierbare externe Formatbetrachter). Dies bedingt erhebliche und unnötige Schwierigkeiten bei der Umsetzung von Workflows, Zeitstempelung und Stapelverarbeitung und Sonderformaten der Film- & Tonarchivierung (*„cui bono“?*)

- Eine weitere Über-Umsetzung der SigRL besteht in der Forderung des § 4 Abs. 1 SigV, dass *die Spezifikation eines Formats für zu signierende Daten allgemein verfügbar* sein (und darüber hinaus noch einiges andere sicherstellen) muss. Abgesehen davon fragt sich, ob man deshalb nun proprietäre Dateiformate nicht qualifiziert signieren kann/darf (erneut: *„cui bono?“*). Diese Bestimmung ist wohl im Zusammenhang mit der Kritik des vorhergehenden Punktes zur "Darstellung" zu betrachten.

Der Autor teilt im übrigen die in den Materialien zur SigG-Novelle 2008 enthaltene Erläuterung, dass mit dem Begriff der fortgeschrittenen Signatur keine *„besondere rechtliche Konsequenz“* verknüpft wäre, keineswegs. Hier wird nämlich (wie auch in div. einschlägigen Informationen zum Thema „elektronische Signaturen“) ganz offenkundig davon ausgegangen, dass unter der „elektronischen Signatur“ ausschließlich eine „einfache“ elektronische Signatur zu verstehen wäre; tatsächlich handelt es sich dabei jedoch um einen Überbegriff, der sowohl die (weder in der SigRL noch im SigG explizit erwähnten) „einfachen“ Signaturen als auch die fortgeschrittenen und die (in der SigRL gleichfalls nicht namentlich erwähnten) qualifizierten Signaturen umfasst. Eine „einfache“ Signatur ist daher jede elektronische Signatur, die nicht den

Anforderungen an eine fortgeschrittene Signatur (damit natürlich auch nicht denen an eine qualifizierte) genügt. Für die unterschiedliche Rechtsstellung der fortgeschrittenen Signatur ist dies nun insofern bedeutsam, als einer (d.h. jeder!) elektronischen Signatur die rechtliche Gültigkeit und Beweiskraft *nicht alleine deshalb abgesprochen werden darf, weil sie*

- *nur elektronisch vorliegt,*
- *nicht auf einem qualifizierten Zertifikat beruht oder*
- *nicht unter Verwendung von technischen Komponenten und Verfahren im Sinne des § 18* (SigRL: „von einer sicheren Signaturerstellungseinheit“) *erstellt wurde.*

Anmerkung: *Die beiden letzten Gründe bilden die Anforderungen an eine qualifizierte Signatur ab.*

Da diese Aufzählung von (Nicht-)Ausschlussgründen wohl als taxativ anzusehen ist, kann offenbar einer elektronischen Signatur die Rechtswirksamkeit z.B. deshalb abgesprochen werden, weil sie die Anforderungen an eine fortgeschrittene Signatur nicht erfüllt. Dies begründet also sehr wohl eine besondere Rechtsstellung der fortgeschrittenen Signatur im Vergleich zur „einfachen“.

Gleichfalls nicht schlüssig scheint die in den Materialien enthaltene Interpretation, dass sich die Anforderung der „alleinigen Kontrolle“ über die Mittel zur Signaturerstellung in irgendeiner Weise auf die technischen Verfahren zur Absicherung der Signaturumgebung bezöge; dieser Aspekt wurde jedoch bereits grundsätzlich in Punkt 8.1.2. erörtert.

8.3. Einordnung von PGP im Rechtsrahmen

8.3.1. PGP als Signaturverfahren

Zweifelsfrei handelt es sich bei PGP um ein Verfahren, mit dem *elektronische Signaturen* im Sinne der SigRL bzw. des SigG erstellt werden können. Es erzeugt beim Signieren *elektronische Daten* (die „PGP Signature“), *die anderen elektronischen Daten* (dem zu unterzeichnenden Datensatz, E-Mail, Dokument etc.) *beigefügt* (im Falle eines OpenPGP-unterschriebenen Dokuments gem. RFC-4880 bzw. PGP/MIME gem. RFC-3156) *oder mit ihnen logisch verknüpft sind* (im Falle einer externen Unterschriftsdatei, „PGP Detached Signature“) *und die der Authentifizierung dienen* (die Herkunft der unterschriebenen Daten kann vom Empfänger geprüft werden).

Des weiteren sind die mit PGP erzeugten Signaturen nach Auffassung des Autors auch als *fortgeschrittene Signaturen* einzustufen (vgl. 8.1.2. & 8.2.), da PGP ein asymmetrisches Public/Private Key Verfahren nutzt und der Unterzeichner somit die Signaturerstellungsdaten bei der Erzeugung der Unterschrift oder der Übermittlung des signierten Dokuments nicht aus der Hand geben muss (sie also unter *seiner alleinigen Kontrolle halten kann*). Auch sind PGP-Signaturen ausschließlich dem Unterzeichner zugeordnet (einerseits über den im PGP-Zertifikat eingetragenen Namen bzw. die E-Mail-Adresse, andererseits über die nur dem Unterzeichner bekannte Passphrase) und ermöglichen deshalb die Identifizierung des Unterzeichners. Zudem ist eine

PGP-Signatur durch die Bildung, Verschlüsselung und Übermittlung eines faktisch kollisionsfreien Hashwertes über das signierte Dokument (der ja die eigentliche Unterschrift darstellt) *so mit den Daten, auf die sie sich bezieht, verknüpft, dass eine nachträgliche Veränderung der Daten festgestellt werden kann (§ 2 Z 2 lit d SigG).*

Anmerkung: *Tatsächlich ist diese Verwendung als „Transportsiegel“ wie zuvor bereits erwähnt nach wie vor der häufigste Einsatzzweck von PGP-Signaturen. Diese „fortgeschrittene“ Funktionalität könnte grundsätzlich sogar mit einem „neugeborenen“, also self-signed PGP-Key erreicht werden.*

Ob sich PGP auch zur Erstellung *qualifizierter Signaturen* verwenden lässt, soll nach einigen weiteren Betrachtungen in Punkt 8.3.5. analysiert werden.

8.3.2. PGP-Keys und Zertifikate im Rechtssinne

Wenngleich im Zusammenhang mit PGP meist von „PGP Keys“ gesprochen wird, so handelt es sich bei einem unterschriebenen öffentlichen PGP-Key jedoch tatsächlich meist um ein vollwertiges Zertifikat im signaturrechtlichen Sinne. Kann ein solcher PGP-Key im einfachsten Fall zwar nur aus einem öffentlichen Schlüssel, einer einzigen User-ID (ggf. nur einer E-Mail-Adresse) und der Unterschrift des Schlüsselinhabers selbst („Self-Signed Key“ bzw. „Self-Signed Certificate“) bestehen, so entfaltet er seine Funktionalität als Zertifikat erst unter Beifügung zumindest einer (im Gegensatz zu X.509 tunlichst aber mehrerer!) Unterschrift/en (Beglaubigungen) seines Inhalts durch andere Teilnehmer am Web Of Trust.

Anmerkung: *Durch das initiale Self-Signing wird ein PGP-Key streng genommen noch nicht zum Zertifikat. Dabei wird nämlich ausschließlich der öffentliche Schlüssel unterschrieben und so unmittelbar nach der Ausstellung vor Veränderung geschützt (versiegelt).*

Dazu werden üblicherweise auch zusätzliche Angaben aufgenommen wie z.B. der volle Name des Inhabers, eine Beschreibung des Zertifikats oder seines Verwendungszwecks, die Organisation, der der Inhaber angehört oder die er vertritt, ggf. auch ein Lichtbild oder weitere E-Mail-Adressen, unter denen der Inhaber erreichbar ist bzw. als Absender von Nachrichten auftritt. Tatsächlich ist die Menge an Angaben in einem PGP-Zertifikat theoretisch unbegrenzt, limitierende Faktoren stellen lediglich die praktisch verwendbare Größe des Zertifikats und die Leistungsfähigkeit der jeweiligen Software-Implementierungen dar.

Durch Beifügung von Namens- und ggf. sonstigen Attributen an den PGP-Key werden also die Signaturprüfdaten (der öffentliche Schlüssel) einer Person zugeordnet, durch die Unterschrift/en über den Schlüssel samt diesen Angaben wird die Identität dieser Person bestätigt.

Anmerkung: *Ob im Lichte dieser Anforderungen auch ein wirklicher „Self-Signed Key“ (also ein selbstsigniertes PGP-Zertifikat einschließlich der Personendaten!) ein Zertifikat im signaturrechtlichen Sinne darstellt, mag in Frage gestellt werden; schließlich bestätigt sich dabei der Schlüsselinhaber seine Identität de facto selbst. Tut man dies jedoch, so müsste man wohl konsequenterweise auch allen self-signed X.509-Zertifikaten (wie sie häufig z.B. bei Zeitstempeldiensten oder Server-Zertifikaten eingesetzt werden) die grundlegende Zertifikatseigenschaft absprechen.*

8.3.3. PGP-Introducer und Zertifizierungsdiensteanbieter

Die Verankerung der Rolle und Ausstattung eines ZDA stellt wohl die größte grundsätzliche Herausforderung bei der rechtlichen Einordnung von PGP dar. Die SigRL nimmt – was aus dem Hintergrund ihrer Entstehung verständlich sein mag – eine überaus zentralistische Sicht der Rollenverteilung beim Umgang mit öffentlichen Signatur-Infrastrukturen ein, die sich auch im SigG wiederspiegelt.

Wenngleich man sich in der SigRL offensichtlich bemüht hat, möglichst technologieneutrale Formulierungen zu finden (was sowohl vom Wirtschafts- und Sozialausschuss als auch vom Ausschuss der Regionen in ihren jeweiligen Stellungnahmen ausdrücklich gefordert bzw. begrüßt wurde), so muss der faktische Erfolg dieses Bemühens wohl als bescheiden bezeichnet werden: Einerseits sind viele Formulierungen „derart technologieneutral“, dass sie auf eine konkrete Technologie nur mit Kunstgriffen anwendbar sind, andererseits ist der eigentlichen Gedankenstruktur dahinter eine deutliche „X.509-Lastigkeit“ wohl nicht abzusprechen; die besondere Ausprägung des ZDA ist zwar nicht die einzige, wohl aber die stärkste Manifestation dieses Gedankenguts.

Das grundlegende Begriffsproblem beim ZDA besteht in Zusammenhang mit PGP darin, dass es eine solche "prominente" Entität dort typischerweise nicht gibt. Ein PGP-Zertifikat soll ja von jedermann unterschrieben, also beglaubigt werden dürfen und können (Rolle des *Introducers*). Die Beurteilung der Zuverlässigkeit und Glaubwürdigkeit eines PGP-Zertifikats erfolgt ausschließlich im Endgerät aufgrund mit der jeweiligen Software-Implementierung mitgelieferter und von der Community akzeptierter „Trust Models“ in Verbindung mit den Einstellungen (Entscheidungen) des jeweiligen Benutzers. Personen, die das PGP-Zertifikat eines anderen erweitern (also seine Glaubwürdigkeit erhöhen), indem sie ihre Unterschrift unter dessen öffentlichen Schlüssel setzen, tun dies i.d.R. nicht als Dienstleistung oder in Gewinnabsicht, sondern einfach deshalb, weil das „Web Of Trust“ nur so funktioniert.

Anmerkung: *Ähnliche Vorgangsweisen lassen sich seit langem auch in anderen Bereichen des Internet beobachten, man denke nur an die „Buddy“-Listen verschiedener P2P-Kommunikationsprogramme oder an das Kontaktnetzwerk von XING.*

Daraus zeigt sich, dass der Begriff des ZDA *per se* einesteils zu eng (nämlich als Begriff selbst) und andernteils zu weit (von seiner Definition her) gefasst ist, um bei PGP überhaupt anwendbar zu sein. Auf den ersten Blick ist es schwierig, zweifelsfrei festzustellen, ob ein Introducer als ZDA anzusehen ist, weil

- nicht definiert ist, was unter dem *Ausstellen eines Zertifikats* zu verstehen ist (wie vorstehend erörtert könnte darunter die Beglaubigung/Bestätigung verstanden werden, insofern wäre also jeder Introducer gleichzeitig ZDA),
- nicht definiert ist, was unter einem Zertifizierungsdienst bzw. unter einem *Dienst im Zusammenhang mit elektronischen Signaturen* im engeren Sinne zu verstehen ist (fällt also u.a. auch der persönliche Gefallen unter diesen Begriff?).

Liest man u.a. den Erwägungsgrund 12 der Richtlinie, so scheinen ausschließlich gewerbliche Dienstleistungen (!) im Zusammenhang mit elektronischen Signaturen als Zertifizierungsdienste zu gelten:

[..] „Es ist darauf zu achten, dass Akkreditierungssysteme den Wettbewerb im Bereich der Zertifizierungsdienste nicht einschränken."

Die Wortwahl der Richtlinie *„oder anderweitige Dienste im Zusammenhang mit elektronischen Signaturen"* legt zudem nahe, dass auch die Ausstellung von Zertifikaten unter die Definition des Zertifizierungsdienstes fällt; diese tritt damit nicht im Sinne einer „Oder"-Bestimmung neben die *Dienste im Zusammenhang mit elektronischen Signaturen*, sondern stellt einen besonders hervorgehobenen Spezialfall eines solchen Dienstes dar. Ein privater Introducer scheint somit nicht vom Begriff des ZDA erfasst zu sein.

Insgesamt scheint ein Kerngedanke der Richtliniengeber bei der Festlegung der Position des qualifizierten Zertifikats – bzw. der hierarchisch-zentralistischen Gedankenstruktur der Richtlinie überhaupt – die Frage nach der Haftung für allenfalls falsch ausgestellte oder nachträglich kompromittierte Zertifikate bzw. Schlüsseldaten gewesen zu sein. Im Web Of Trust würde dies bedeuten, dass sich die Haftungsfrage auf einen weltweiten Verbund von Introducern erstreckt (sofern nicht Special Introducer involviert sind, die i.d.R. nach Ihrer jeweiligen Rechtsordnung berufsrechtlich und/oder nach den nationalen Regelungen über ZDA haften).

8.3.4. Zertifizierungsdiensteanbieter als *Special Introducer*

Mag die Rolle des „einfachen" Introducers bei PGP innerhalb des aktuellen Rechtsrahmens auch nicht verankert sein, so lohnt sich jedoch die Betrachtung dessen, was passiert, wenn ein „echter" ZDA am Web Of Trust teilnimmt (bei PGP seiner Bedeutung entsprechend als *Special Introducer* bezeichnet). In den lokalen PGP-Einstellungen des Benutzers wird ein solcher Special Introducer sinnvollerweise mit vollständigem, wenn nicht gar mit absolutem Vertrauen auszustatten sein. Absolutes Vertrauen wird zwar normalerweise nur in diejenigen Schlüssel gesetzt, die man selbst erzeugt hat, jedoch entspräche dies dem Verständnis von X.509: Ein X.509-Zertifikat ist entweder absolut vertrauenswürdig oder gar nicht. Dies würde also bedeuten, dass alle PGP-Zertifikate, die eine Unterschrift eines Special Introducers beinhalten, sofort als unbedingt glaubwürdig eingestuft werden können und die Notwendigkeit anderer Unterschriften theoretisch entfiele.

Natürlich ist es dabei sinnvoll, wenn sich alle Benutzer im Vertrauen in diese Special Introducer einig sind. Da es eine Vielzahl solcher Introducer geben kann (insbesondere kommen neben den „gewerblichen" ZDA auch öffentliche Stellen, Notare, Rechtsanwälte, Ziviltechniker usw. in Frage), wird es dem Benutzer i.d.R. unzumutbar sein, all diese Special Introducer als solche zu erkennen und seine lokale PGP-Konfiguration manuell entsprechend anzupassen. In Wirklichkeit ist dies aber gar nicht unbedingt nötig: Da das Signaturrecht die rein privatrechtliche Beurteilung elektronischer Signaturen nicht berührt, ist lediglich die öffentlich-rechtliche Anerkennung solcher Signaturen (d.h. die Anerkennung des Special Introducers als notwendige und hinreichende vertrauenswürdige Zertifizierungsinstanz in *Legal Procedures*) zu regeln. Dieser Aspekt ist mit der sonstigen Anerkennung der ZDA, (vor

allem der akkreditierten ZDA und derjenigen, die qualifizierte Zertifikate ausstellen) bereits erledigt.

8.3.5. qualifizierte PGP-Zertifikate & -Signaturen

Aus den vorstehenden Überlegungen ergibt sich zunächst, dass ein rein „Web Of Trust“-basiertes PGP-Zertifikat in der dztg. Rechtslage nicht als *qualifiziertes Zertifikat* wird ausgestellt werden können. Neben den umfangreichen Anforderungen an ZDA, die qualifizierte Zertifikate ausstellen (dürfen), und vor allem in Anbetracht der umfänglichen Haftung gegenüber *jedermann, der auf das Zertifikat vertraut*, existiert vor allem eine *conditio sine qua non*:

Personen, die öffentliche PGP-Keys nicht gewerbsmäßig signieren (also PGP-Zertifikate ausstellen) entziehen sich offenbar der Eigenschaft des ZDA; da ein qualifiziertes Zertifikat aber *„von einem ZDA, der den Anforderungen [..] entspricht“* ausgestellt werden muss, kann dies von solchen Personen schon rein definitionsgemäß nicht erbracht werden.

Stellt jedoch ein „echter“ ZDA, der dazu befugt ist, ein entsprechend ausgerüstetes PGP-Zertifikat aus, so scheint in rechtlicher Hinsicht nichts dagegen zu sprechen, das er dieses auch als qualifiziertes Zertifikat bereitstellen kann.

Anmerkung: *Nach ggw. Rechtslage müsste – wiederum anders als im PGP-Modell vorgesehen – der ZDA hier auch das Schlüsselpaar erstellen und auf einer sicheren Signaturerstellungseinheit (z.B. geeignete Chipkarte) ablegen (tunlichst sollte er es von dieser generieren lassen). Das initiale Self-Signing (Versiegelung des Schlüssels) wäre dann vom Zertifikatswerber unter Verwendung seiner frisch gewählten Passphrase vorzunehmen, woraufhin der ZDA endlich diesen öffentlichen Schlüssel samt Personendaten mit seinem eigenen fortgeschrittenen Zertifikat unterzeichnet und solcherart das qualifizierte PGP-Zertifikat für den Benutzer ausstellt.*

Mit einem solchen Zertifikat könnte der Benutzer nun grundsätzlich auch qualifizierte Signaturen erstellen. Darüber hinaus dürfte auch nichts dagegen sprechen, dass weitere Teilnehmer an seinem Web Of Trust den erhaltenen öffentlichen Schlüssel signieren, ganz wie im PGP-Modell gewünscht. Das einmal ausgestellte Zertifikat des ZDA wird dabei ja nicht angetastet, sondern gewissermaßen stellt jedes Mitglied im Web Of Trust sein eigenes Zertifikat (immer für einen und denselben öffentlichen Schlüssel) aus.

Eine Erhebung bzw. Analyse der Verfügbarkeit und des Funktionsumfangs der für ein solches Unterfangen erforderlichen Hard- und Software-Ausrüstung (sowohl auf Benutzer- als auch auf ZDA-Seite) würde den Rahmen der vorliegenden Studie bei weitem sprengen; schließlich müsste für eine zuverlässige Aussage *de facto* ein detailliertes Prüfverfahren der Bestätigungsstelle nachvollzogen werden. Die aktuelle Technologie-beobachtung stimmt jedoch durchaus zuversichtlich, dass entsprechende Produkte – sollte es sie nicht schon geben – in allernächster Zukunft verfügbar sein werden. Jedenfalls soll dies ein Thema für die im Vorwort angesprochene Dissertation sein.

Abschließend sei auf folgende mögliche Erleichterung der Ausstattungs-anforderungen in "*kontrollierten Umgebungen*" hingewiesen:

§ 6 Abs. 3 SigV: *Wenn technische Komponenten und Verfahren in einer kontrollierten Umgebung eingesetzt werden, können Sicherheitsanforderungen, die nach Abs. 1 technisch sichergestellt werden müssen, auch organisatorisch durch Einsatz qualifizierten und vertrauenswürdigen Personals oder technischorganisatorisch durch Einsatz geeigneter Zugriffs- und Zutrittskontrollmaßnahmen erfüllt werden. Die Erfüllung dieser Sicherheitsanforderungen ist durch eine Bestätigungsstelle zu prüfen.*

8.4. Der Beweiswert/die Beweiskraft von PGP-Unterschriften

Für die Beweiskraft aller elektronisch unterschriebenen Dokumente gilt grundsätzlich das Diskriminierungsverbot lt. SigRL in der österr. Umsetzung:

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

Obwohl hier zwar davon die Rede ist, dass *die rechtliche Wirksamkeit einer elektronischen Signatur* [..] nicht ausgeschlossen werden kann, so entfaltet jedoch eine (elektronische oder andere) Unterschrift *per se* eigentlich keinerlei Beweiskraft. Vielmehr geht es hier um die

- *Echtheit und Unverfälschtheit der Unterschrift* einerseits und um die
- *Beweiskraft des unterschriebenen Dokuments* andererseits.

Konkret bedeutet dies – auch wenn fortgeschrittene PGP-Signaturen nicht *ex lege* der eigenhändigen Unterschrift gleichzuhalten sind – , dass PGP-signierte Dokumente als Beweis zugelassen werden müssten, solange ihre Echtheit oder Unverfälschtheit nicht bestritten wird. Geschieht dies, so wird wohl derjenige, der das vermeintlich rechtskräftig unterschriebene Dokument vorlegt, dessen Authentizität bzw. Integrität beweisen müssen. Im Zusammenhang mit der freien richterlichen Beweiswürdigung dürfte es sich dabei aber eher um ein Randthema handeln, da zur Beurteilung des wahren Sachverhalts typ. auch Aspekte wie Plausibilität, schlüssiges Handeln der Parteien usw. herangezogen werden.

Anmerkung: *Aus Art. 5 Abs. 1 SigRL erschließt sich eigentlich nicht eindeutig, ob die Mitgliedsstaaten diese Gleichstellung „jedenfalls“ oder aber „ausschließlich“ für die qualifizierte Signatur vorzunehmen haben. Der österr. Gesetzgeber hat sich offenbar für die „ausschließlich“-Interpretation entschieden.*

Anders verhält es sich bei *qualifiziert* unterschriebenen Dokumenten, die auch unter Verwendung von PGP grundsätzlich denkbar wären (vgl. Punkt 8.3.5.). Hier erfolgt aufgrund Art. 5 Abs. 1 SigRL eine rechtliche Gleichstellung mit einem eigenhändig unterschriebenen Dokument durch das SigG:

§ 4 SigG:

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

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

Bei einem qualifiziert unterschriebenen Dokument wird also explizit eine (widerlegbare) Echtheitsvermutung ausgesprochen; ein Privileg, das die fortgeschrittene Signatur nicht genießt. Muss also die Echtheit einer fortgeschrittenen Signatur bei ihrer Strittigkeit *bewiesen* werden, so ist im Gegenteil bei der qualifizierten Signatur deren Echtheit zu *widerlegen*. Unter welchen Umständen dies gelingen kann, normiert § 4 Abs. 4 SigG:

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

In dieser Beweislastumkehr im Strittigkeitsfall liegt wohl vor allem der rechtliche Unterschied zwischen fortgeschrittenen und qualifizierten Signaturen begründet. Insofern ist auch der beträchtliche Aufwand z.B. zur Identitätsprüfung bei qualifizierten Signaturen verständlich: Abgesehen von den rein erklärungsinhärenten Rechtswirkungen eines eigenhändig unterschriebenen Dokuments bewirkt diese besondere Rechtsstellung vor allem eine wesentlich erschwerte Abstreitbarkeit der eigenen Unterschriftsleistung.

Anmerkung: *Obwohl einesteils die SigRL privatrechtliche Verträge von ihrem Regelungsgegenstand vehement ausnimmt und andernteils das SigG seinen Gültigkeitbereich ausschließlich anhand der ZDA definiert, so scheint durch den Bezug auf die Schriftform gem. ABGB doch ein Präjudiz der vertragschließenden Privatparteien vorzuliegen: Demnach müssten z.B. vertragliche Änderungen, für die zwingend die Schriftform vereinbart ist, jedenfalls und ex lege dann anerkannt werden, wenn sie mit qualifizierten Signaturen versehen sind. Einer gesonderten Vereinbarung darüber bedarf es nicht, vielmehr müsste diese Rechtswirkung der qualifizierten Signatur per Parteienvereinbarung explizit ausgeschlossen werden.*

9. Zusammenfassung

Der erste Abschnitt dieser Studie behandelte die historische Entwicklung, Verbreitung und gesellschaftliche Bedeutung von freien und kommerziellen Lösungen auf Basis OpenPGP. Dabei wurde gezeigt, dass PGP sich seit der Ersteinführung durch Phil Zimmermann 1991 weltweit stark verbreitet hat und insbesondere durch die Standardisierungsbemühungen innerhalb der IETF heute zu Recht als einer der bedeutetsten *de facto* Standards für email-Transportsicherung (OpenPGP/MIME neben S/MIME) und Verschlüsselung gilt. In diesem Zusammenhang wurde auf die Besonderheiten des "Web Of Trust", des PGP Trust Models und der PGP PKI eingegangen. Ebenso wurde die Entstehung solcher *de facto* Standards in der Internet Community diskutiert und der staatlichen Regelung durch Rechtsnormen gegenübergestellt.

Für die Anwender von OpenPGP steht eine umfangreiche und ausgereifte Integration in Betriebssysteme und Desktop Environments (Gnome, KDE, OSX, Windows) sowie eine vielfältige Anwendungslandschaft zur Verfügung. Diese reicht von Keyring-Managern, Passphrase-Agents, E-mail-, Newsreader-, Browser- und

Dateimanagerintegration bis zu SSH, VPN und UNIX-PAM[5] Integration und Adobe Acrobat Plugins. Weiters stehen reichhaltige Entwicklungsbibliotheken für die Integration in eigene Anwendungen und Workflows zur Verfügung.

Die erweiterten Anforderungen von Unternehmen bestehen insbesondere im Policy Management, dem Rollout & Deployment, Key Splitting & Recovery Models, Stapelsignaturen (Batch-Verarbeitung), Single Sign-On (SSO) und TPM/Chipcard/USB Token Deployments.

Es gibt keine Argumente gegen eine gedeihliche Koexistenz von X.509 und OpenPGP. Certificate Authorities (CAs), die beide Paradigmen unterstützen, sind sicher der sinnvollste Weg. Wünschenswert wäre die Einigung der führenden Keyserver-Betreiber auf ein Abgleichprotokoll, einen einheitlicher Keyserververbund zumindest unter den OpenSource-Keyservern sowie eine gemeinsame Sichtweise des „Housekeepings“ (abgelaufene und widerrufene Zertifikate) und der Verifikation per E-Mail. Insbesondere wäre ein bidirektionaler Abgleich des PGP Open Directory mit nicht-kommerziellen PGP-Keyservern vorteilhaft.

Die rechtliche Erörterung bezog sich auf die Anforderungen und Möglichkeiten der Teilnahme am Rechtsleben mittels OpenPGP, der daraus resultierenden Rechtsfolgen und Rechts(un)sicherheiten und des Status‘ solchermaßen digital unterschriebener Dokumente (Beweiswert, Beweiskraft, Einstufung in der Begriffswelt des SigG). Eng damit verbunden war eine Diskussion der ZDA (nebst sicheren Signaturerstellungseinheiten) und der Frage, ob und wann man im OpenPGP-Kontext als solcher anzusehen ist oder durch Gebarung ein solcher wird. Daraus resultierte die Frage, ob Aussteller und Beglaubiger (*Notary Services, Key-signing Parties*) von PGP-Zertifikaten Zertifizierungsdiensteanbieter (ZDA) sind. Letzendlich wurde die Frage beantwortet, ob sich PGP für die Erstellung qualifizierter Zertifikate und Signaturen eignet bzw. woran es ggw. scheitert.

Eine wesentliche Schlussfolgerung der Betrachtung war, dass eine Grundvorausetzung der Qualifikation von OpenPGP als qualifiziertes Signaturverfahren die Einbindung von Special Introducern in das *PGP Trust Model* sein dürfte, ebenso die Erzeugung des Schlüsselmaterials *„On Chip“* ohne Exportmöglichkeit des private Key-Materials.

Ein wichtiger Unsicherheitspunkt bei der Einstufung und damit rechtlichen Anerkennung jeder Art von PGP-Signaturen als fortgeschrittene Signaturen wurde im Zusammenhang mit der nach Ansicht des Autors unzutreffenden Interpretation der SigRL-Forderung nach „alleiniger Kontrolle des Signators“ über die Mittel zur Signaturerstellung aufgezeigt. Aus den Materialien zum SigG geht hervor, dass dieses Kriterium zum einen an zusätzliche technische und/oder betriebliche Vorkehrungen gebunden sei und dass diese zum anderen der Auslegung offenstünden. Insbesondere für die am weitest verbreiteten PGP-Zertifikate – nämlich diejenigen, die nicht von einem ZDA ausgestellt bzw. beglaubigt wurden – könnte diese Sichtweise in der konkreten Rechtsanwendung eine ungerechtfertige Benachteiligung bedeuten.

Anmerkung: *Eine eingehendere Erörterung der Rechtswirkungen elektronischer Signaturen bedürfte nicht nur der zusätzlichen Auseinandersetzung mit formalrechtlichen Normen (z.B. Verfahrens- & Prozessordnungen) im Speziellen, sondern auch eine grundlegende Betrachtung der elektronischen Willens- bzw.*

5 Pluggable Authentication Modules

Wissenserklärung und der Besonderheiten der eigenhändigen Unterschrift im Allgemeinen. Dies würde allerdings den Rahmen dieser Studie bei weitem sprengen.

10. Literatur, Links und Quellen

- „Der Beweiswert elektronischer Signaturen“, Sebastian Jungermann, Dissertation
- „PGP Keys – des Signaturrechts vergessene Kinder?“, Präsentation Gernot Schmied & Wolfgang Fabics anlässlich des ADV-Signaturtages 2007
- SigRL, SigG, SigV, EGovG, VerwSigV, BVergG, ABGB, ZPO sowie Materialien dazu (http://www.ris.bka.gv.at)
- „Grundlagen der elektronischen Signatur“, BSI Bonn/DE, 2006
- „Die Bedeutung digitaler Signaturen für den elektronischen Geschäftsverkehr “, http://www.zbb.de
- http://www.bundesnetzagentur.de
- http://www.rtr.at
- http://www.openpgp.org
- http://www.gnupg.org
- http://www.pgpi.org
- http://philzimmermann.com
- http://www.nongnu.org/sks/
- http://www.hushmail.com
- RFC3156 MIME Security with OpenPGP - "PGP/MIME"
- RFC2538 Storing Certificates in the Domain Name System (DNS)
- RFC4880 OpenPGP Message Format
- OpenPGP Card http://www.g10code.com/p-card.html
- OpenPGP PAM (Poldi) – PAM for the OpenPGP smartcard
- draft-josefsson-cert-openpgp "OpenPGP data in the CERT RR"

11. Glossar

PKI	Public Key Infrastructure = ein System zur Validierung, Verteilung und Administration von Zertifikaten ***Zitat Phil Zimmermann:*** *„What we call a PKI in the OpenPGP world is actually an emergent property of the sum total of all the keys in the user population, all the signatures on all those keys, the individual opinions of each OpenPGP user as to who they*

	choose as introducers, all the OpenPGP client software which runs the OpenPGP trust model and performs trust calculations for each client user, and the key servers which fluidly disseminate this collective knowledge.“
WoT	„Web of Trust” = das PGP/GnuPG Trust Model – ein verteiltes Trust Model auf Basis von vertrauenswürdigen „Vorstellern” (Introducern) und kumulativem Gesamt-Trust-Level
TM	Trust Model = eine Abbildung der Vertrauensverhältnisse zwischen Zertifikat und unterzeichnenden bzw. einführenden Dritten
CA	Certificate Authority = eine vertrauenswürdige organisatorische/technische Einrichtung zum Management von Zertifikaten
CRL	eine on-line Liste zurückgezogener Zertifikate
OCSP	Online Certificate Status Protocol - ist ein Internet-Protokoll, das es Clients ermöglicht, den Status von X.509-Zertifikaten bei einem Validierungsdienst abzufragen, somit eine skalierbarere Alternative zu CRLs
SCVP	Server-based Certificate Validation Protocol (neu und bisher kaum verwendet)
SKS	ein moderner OpenSource Keyserver-Verbund
TC	Trust Center (eine vertrauenswürdige Einrichtung, die eine PKI bzw. CA betreibt)
ZDA	Zertifizierungsdiensteanbieter (aus SigRL bzw. SigG)
SSEE	sichere Signaturerstellungseinheit (aus SigRL bzw. SigG)
key-ID	die letzten acht Stellen des hexadezimal notierten PGP fingerprints (z.B. CA57AD7C)
fingerprint	ein eindeutiger Hashwert über den öffentlichen (Haupt-)Schlüssel eines PGP Keypairs bzw. -Zertifikats
keypair	besteht aus einen öffentlichen Schlüssel und seinem komplementären privaten Schlüssel
keyring	Schlüsselbund = Summe mehrerer Schlüssel (es gibt einen *Public* und einen *Private Keyring*)
private key	der Teil eines Schlüsselpaares, der geheim gehalten wird bzw. auf einem Chip generiert wird oder verbleibt
public key	der öffentliche Teil eines Schlüsselpaares

Keyserver	ein Repository öffentlicher Schlüssel; dient der öffentlichen Bereitstellung und gleicht sich mit anderen Keyservern ab
X.509	eine Gruppe von ITU-T- und IETF-Standards für digitale Zertifikate
Introducer	im PGP-Sinne eine vertrauenswürdige (mir bekannte) Person die einen i.d.R. unbekannten oder weniger bekannten Teilnehmer am WoT vorstellt (diesen einführt)
PKCS	„Public Key Crypto Standards“ – eine Gruppe von Implementierungsstandards für Public Key Cryptography
LDAP	Lightweight Directory Access Protocol – eine schlankere Version des X.500-Standards für den Zugriff auf elektronische Verzeichnisdienste
S/MIME	= Secure / Multipurpose Internet Mail Extensions) ist ein Standard für die Verschlüsselung und Signatur von MIME-gekapselter E-Mail durch ein asymmetrisches Kryptosystem (Wikipedia)
(Open)PGP/MIME	RFC3156: MIME Security with OpenPGP - „PGP/MIME“
PGP	“Pretty Good Privacy” – ggw. ein “Registered Trademark” der PGP Corporation, wird aus historischen Gründen oft synonym für GnuPG- oder PGP.COM-Implementierungen verwendet.
OpenPGP	IETF-Spezifikation von Messages und Implementierungsgrundlagen (RFC 4880)
GnuPG	die führende OpenSource OpenPGP-Implementierung
PGP.COM	die PGP Corporation, der führende kommerzielle Anbieter von OpenPGP-Lösungen und Rechtsnachfolger der Marke „PGP“ bzw. „Pretty Good Privacy“