

ZIK / SF•FS / simsa

## Public Key Infrastrukturen im Rahmen von ICT Rechtspraxis

ADRIAN GAUTSCHI \*

- I. Public Key Infrastrukturen (PKI) – Neuland für manch gestandenen Rechtsgelehrten**
  - 1. Zukunftsbewusste Gruppe in traditionellem Rahmen
  - 2. Einleitende Bemerkungen zum rechtlichen Umfeld
- II. Audit und Zertifizierung einer PKI aus Sicht der Anerkennungsstelle**
  - 1. Bedeutung von Audit und Zertifizierung sowie Rolle des Rechts
  - 2. Der (lange) Weg der Zertifizierung
- III. Rechtsstruktur einer PKI**
  - 1. Standort- und Begriffsbestimmung
  - 2. Gesetzliche Regelungen und Normierungen
  - 3. Rechtsverhältnisse der Teilnehmer einer PKI und Bedeutung der CP/CPS
- IV. Elektronischer Geschäftsverkehr mit den Gerichten**
- V. Kein BG über den elektronischen Geschäftsverkehr – quid iuris?**
  - 1. Anfängliche Analyse der Verwaltung und Entwurf eines BG über den elektronischen Geschäftsverkehr
  - 2. Entscheide des Bundesrates in den Jahren 2002–2005
  - 3. Ausblick mit Konzentration auf den Konsumentenschutz
- VI. Abschliessende Diskussion im Plenum**

So wie es in technischer Hinsicht um die E-Mail vor einigen Jahren stand, sieht es derzeit bezüglich Public Key Infrastrukturen (PKI) aus. Aber auch die rechtlichen Fragestellungen betreffend PKI sind nicht fern. Daher bedarf es der Aufklärung – sogar gestandener Juristen – nicht nur in Bezug auf die einer PKI zugrunde liegende Technologie, sondern auch in Bezug auf die rechtlichen Aspekte.

An der Tagung «Public Key Infrastrukturen im Rahmen von ICT Rechtspraxis» wurden beide Themenkomplexe untersucht. Behandelt wurden u.a. die Bedeutung des ZertES, der VzertES, der TAV und der technischen Spezifikationen (TS) des European Telecommunications Standards Institute (ETSI) sowie die Rechtsbeziehungen der an einer PKI beteiligten Stellen.

Hiernach ging es um den elektronischen Geschäftsverkehr mit den Gerichten, insbesondere um die seit dem 1. Januar 2007 mit dem Inkrafttreten des BGG mögliche Einreichung von Rechtsschriften in elektronischer Form. Im Sinne einer Bedienungsanleitung und mit der Hoffnung auf rege Benutzung wurde die neue Übermittlungsmethode präsentiert.

Abgerundet wurde die Tagung mit einem retrospektiven Bericht über das im Jahr 2005 vom Bundesrat fallen gelassene BG über den elektronischen Geschäftsverkehr (= Teilrevision von OR und UWG [Verbesserung des Konsumentenschutzes]). Bei diesem Programmpunkt kam der teilweise wacklige Stand des Konsumentenschutzes in der Schweiz generell und aktualitätsbezogen zur Sprache.

### I. Public Key Infrastrukturen (PKI) – Neuland für manch gestandenen Rechtsgelehrten

#### 1. Zukunftsbewusste Gruppe in traditionellem Rahmen

Ist dieser Tage jemand bekümmert um die Rechtslage im elektronischen Geschäftsverkehr? – In der Tat: RA Dr. Mathis Berger, LL.M., Geschäftsführer des Schweizer Forums für Kommunikationsrecht, begrüsst die Wissbegierigen im Namen des Organisationskomitees<sup>1</sup> hinter der gemäss Berger nicht mit einem elektronischen Schlüssel verriegelten Tür des Saales der Zürcher Zunft zur Zimmerleuten. Er zeigte sich erfreut über die Anwesenheit der auf dem zur Diskussion stehenden Gebiet qualifizierten Exponenten. Zurzeit noch nicht Interessierte dürfen das Ganze aufgrund verschiedener Sachzwänge wohl in absehbarer Zeit nacharbeiten. Zu begeistern vermochte Berger ausserdem das rege

<sup>1</sup> RA Prof. Dr. Rolf H. Weber, RA Dr. Rolf auf der Maur, RA Dr. Mathis Berger, LL.M.

Interesse an der ICT Landsgemeinde 2006<sup>2</sup>, deren Nachfolgerin im Jahr 2007 ebenfalls Ende August am selben Ort, d.h. an der ETH Zürich, mit anschliessendem Aperitif auf der Terrasse dieser Hochschule stattfinden wird<sup>3</sup>.

## 2. Einleitende Bemerkungen zum rechtlichen Umfeld

Da Zweck des ZertES<sup>4</sup> u.a. ist, «die Verwendung qualifizierter elektronischer Signaturen zu begünstigen» (Art. 1 Abs. 1 lit. b ZertES<sup>5</sup>), werde im Zunftsaal zur Zimmerleuten in Bezug auf ein wirtschaftlich bedeutendes – nach Berger würden im Jahr 2006 in der Schweiz Geschäfte im Gesamtwert von etwa CHF 2 Mrd. über den elektronischen Geschäftsverkehr abgewickelt –, aber rechtlich teilweise vernachlässigtes Gebiet gewissermassen sogar «Entwicklungshilfe» geleistet. Die Spezialität der Veranstaltung sei – so Berger – die Verbindung bzw. «Zwangsehe» des Themenbereiches der elektronischen Signatur mit demjenigen des E-Commerce und damit mit dem vom Bundesrat im November 2005 fallen gelassenen Entwurf betreffend ein BG über den elektronischen Geschäftsverkehr. Die Zwangs-Eheleute gehen nach anfänglicher gleichlaufender Behandlung durch den Gesetzgeber mittlerweile in Trennung ihre Wege, wobei der Bereich der elektronischen Signatur mit dem ZertES und den entsprechenden Bestimmungen, z.B. im OR mit Art. 14 Abs. 2bis und Art. 59a, eigenständig ein Etappenziel erreicht hat.

Im Anschluss an diese neugierig machenden Sätze gewährte Berger eine Kurzvorschau auf das System einer PKI. Zentrales Element einer solchen ist die qualifizierte elektronische Signatur. Ein Schaubild zeigte das Zusammenwirken der an einer PKI beteiligten Stellen, nämlich von Sender und Empfänger einer Datei sowie der Aufsicht. Letztere setzt sich zusammen aus einer Anbieterin von Zertifizierungsdiensten (Certificate Services Provider [CSP] bzw. Certification Authority [CA]) und einer dieser übergeordneten Anerkennungsstelle (Certification Body [CB]) und der Akkreditierungsstelle, wobei die Reihenfolge in der Aufzählung die Hierarchie widerspiegelt.

Wie jedem angehenden Juristen schon frühzeitig gelehrt wird, sind bei Drei- und Mehrecks-Verhältnissen rechtliche Risiken nicht fern; man ist demzufolge um anwendbare Bestimmungen froh. Bei einer PKI sind die von Berger gewählten Beispiele die in Art. 59a OR geregelte Haftung eines Inhabers eines Signaturschlüssels, die Haftung des Anbieters von Zertifizierungsdiensten gemäss Art. 16 ZertES (mit der Besonderheit einer Beweislastumkehr in Art. 16 Abs. 2 ZertES) und diejenige der Anerkennungsstelle gemäss Art. 17 ZertES.

## II. Audit und Zertifizierung einer PKI aus Sicht der Anerkennungsstelle

Nicht-Jurist, aber Experte im technologischen Sektor, Reto P. Grubenmann, Leiter der Zertifizierungsstelle Schweiz (KPMG)<sup>6</sup>, setzte die von Berger angekurbelte Entwicklungshilfe fort mit der Analyse des Prozesses der Evaluierung, Verifizierung und Zertifizierung einer PKI durch eine akkreditierte Anerkennungsstelle. Diese Analyse aus dem Blickwinkel eines Vertreters der technischen Ecke löste seitens des Publikums eine positive Reaktion aus.

### 1. Bedeutung von Audit und Zertifizierung sowie Rolle des Rechts

Verschiedene Regelwerke sind für den europäischen und schweizerischen Markt in Bezug auf die qualifizierte digitale Signatur bedeutsam<sup>7</sup>. Nach Grubenmann müsse auf internationaler Ebene aller-

<sup>2</sup> ICT Landsgemeinde. Rechtspraxis der ICT Infrastruktur, Inhalte und Verträge, 30. August 2006, organisiert durch: Zentrum für Informations- und Kommunikationsrecht der Universität Zürich (ZIK); Schweizer Forum für Kommunikationsrecht (SF•FS); Schweizer Branchenverband für Neue Medien, Internet und Software (simsa).

<sup>3</sup> Der Termin für die nächste ICT Landsgemeinde ist auf den 29. August 2007 angesetzt.

<sup>4</sup> BG über Zertifizierungsdienste im Bereich der elektronischen Signatur (BG über die elektronische Signatur, ZertES) vom 19. Dezember 2003 (SR 943.03).

<sup>5</sup> Zur Begriffsbestimmung der qualifizierten elektronischen Signatur s. Art. 2 lit. c ZertES.

<sup>6</sup> KPMG ist derzeit in der Schweiz die einzige akkreditierte Anerkennungsstelle nach Art. 2 lit. h ZertES.

<sup>7</sup> Aus nationaler Sicht sind das ZertES, die VZertES (VO über Zertifizierungsdienste im Bereich der elektronischen Signatur [VO über die elektronische Signatur, VZertES] vom 3. Dezember 2004 [SR 943.032] und die TAV (VO des BAKOM über Zertifizierungsdienste im Bereich der elektronischen Signatur vom 6. Dezember 2004 [SR 943.032.1]), aus derjenigen Europas verschiedene Technische Spezifikationen (TS) des European Telecommunications Standards Institute (ETSI) zu nennen (ETSI TS 101.456, ETSI TS 101.862, ETSI TS 102.023, ETSI TS 101.861). Sämtliche Unternehmungen in der Schweiz, die Zertifikate ausstellen, genügen diesen Standards; zurzeit sind dies lediglich Swisscom Solutions AG, QuoVadis Limited, die Schweizerische Post PostMail und SwissSign AG ([http://www.sas.ch/de/pki\\_isms/pki.html](http://www.sas.ch/de/pki_isms/pki.html)), besucht am 12. Dezember 2006).

dings noch eine gewisse Validierung stattfinden, wobei die Standards der Schweiz, der EU und der USA sich bereits jetzt weitgehend gleich seien. Nicht zuletzt die Europa-Orientierung der Schweiz habe bewirkt, dass die einschlägigen schweizerischen Erlasse die entsprechenden europäischen Anforderungen erfüllen würden. Von den möglichen elektronischen Signaturen<sup>8</sup> schaffe selbstverständlich die qualifizierte und von einem zertifizierten Anbieter gewährte am meisten Rechtssicherheit. Dies äussere sich etwa in den Haftungsbestimmungen von Art. 59a OR und Art. 16 f. ZertES<sup>9</sup>.

Unabhängig von den existierenden Regelungen zeige sich, dass eine PKI höhere Hürden bei (Ablauf-) Prozessfragen aufwerfe als herkömmliche Übermittlungsmethoden. Nur knapp die Hälfte der zu meistern den Herausforderungen sei rechtlicher oder technischer Art.

Die Frage ist gestattet, worin die Vorteile einer Zertifizierung lägen. Neben der Ausstellung des Zertifikats umfasse nach Grubenmann die Leistung der Anerkennungsstelle einerseits die Schaffung qualitativ hochstehender Standards und betriebswirtschaftlicher Vorzüge wie Kundenzufriedenheit und andererseits längeres Geleit durch KPMG als zurzeit einzige schweizerische Anerkennungsstelle.

In der Folge erklärte Grubenmann den schon von Berger<sup>10</sup> gestreiften Aufbau der für den Einsatz der qualifizierten elektronischen Signatur notwendigen Beziehungen innerhalb einer PKI. Der Anbieter solcher Signaturen würde von der Anerkennungsstelle, d.h. von KPMG, zertifiziert. Über dieser stünde die Schweizerische Akkreditierungsstelle (SECO-SAS). Auf internationaler Ebene fänden sich sodann die European co-operation for Accreditation (EA) und entsprechende Organisationen auf anderen Kontinenten sowie das International Accreditation Forum (IAF).

## 2. Der (lange) Weg der Zertifizierung

Grubenmann zeigte das Verfahren der Zertifizierung auf, wie es bei einer Zusammenarbeit mit KPMG angewendet wird. Der relativ aufwendige Prozess mit einer Dauer von bis zu acht Monaten werde in mehrere Stufen unterteilt, wobei im sog. Pre-Audit vorab zu evaluieren sei, ob ein Kandidat überhaupt zum Audit zugelassen werden könne. Das Main-Audit sei alle drei Jahre zu wiederholen. Das ganze Verfahren habe neben einem externen auch einen betriebsinternen Fokus, und viel Gewicht werde auf die Sicherheit gelegt.

## III. Rechtsstruktur einer PKI

### 1. Standort- und Begriffsbestimmung

«Können Sie sich an Ihre erste E-Mail erinnern?», fragte RA Ralph Gramigna von KPMG Legal, Zürich, seine Zuhörer. Seiner Einschätzung nach sei die heutige Sachlage betreffend die elektronische Signatur vergleichbar mit derjenigen der E-Mail vor 25 Jahren. Die Schwelle zur digitalen Signatur werde in wenigen Jahren oder sogar Monaten überschritten; ein vollkommen papierloses Unternehmen sei denkbar.

Gramigna verlieh verschiedenen Begriffen, wie etwa demjenigen der Signatur, Inhalt. Wesentlich seien die Unterschiede von elektronischer Signatur (Art. 2 lit. a ZertES), fortgeschrittener elektronischer Signatur (Art. 2 lit. b ZertES) und qualifizierter elektronischer Signatur (Art. 2 lit. c ZertES) sowie die Definition eines qualifizierten Zertifikates (Art. 2 lit. f i.V.m. Art. 7 ZertES). Bedeutsamste Feststellung ist, dass die qualifizierte elektronische Signatur gemäss Art. 2 lit. c ZertES i.V.m. Art. 14 Abs. 2 bis OR der eigenhändigen Unterschrift gleichgestellt ist. Authentizität wird u.a. gewährleistet durch ein sog. Schlüsselpaar, das eine Verknüpfung des Private Key (Signaturschlüssel i.S.v. Art. 2 lit. d ZertES), des Senders und des Public Key (Signaturprüf Schlüssel i.S.v. Art. 2 lit. e ZertES) des Zertifizierungsdienste-Anbieters ist.

### 2. Gesetzliche Regelungen und Normierungen

<sup>8</sup> Diese sind die einfache elektronische Signatur, die qualifizierte elektronische Signatur und die von einem zertifizierten Anbieter gewährte elektronische Signatur (s. dazu hiernach III.1.). Ab dem Sicherheitsniveau der qualifizierten Signatur sind weitere Abstufungen möglich, wie das Verbinden der Signatur mit einer Seriennummer, einer bestimmten Währung oder einem bestimmten Höchstbetrag.

<sup>9</sup> Hiervor I.2.

<sup>10</sup> Hiervor I.2.

Auf schweizerischer Ebene würden sich das ZertES, die VZertES, die TAV und die entsprechenden Bestimmungen in anderen Gesetzen auf Art. 95 Abs. 1 und Art. 122 Abs. 1 BV, auf das THG<sup>11</sup> und die AkkBV<sup>12</sup> stützen, so Gramigna. Das ZertES, die VZertES und die TAV ihrerseits würden auf bestimmte v.a. technische Normen<sup>13</sup> verweisen. Auf europäischer Ebene sei die RL 1999/ 93/EG<sup>14</sup> zu erwähnen.

Nach wie vor offen sei, wie sich die Lösung im Bereich der MwSt präsentieren würde – dabei legte Gramigna dar, dass das Marktbedürfnis nach einer Massensignatur wohl bald durch eine Revision der TAV<sup>15</sup>, durch einen Alleingang der ESTV mit Zulassung fortgeschrittener Signaturen oder gar durch eine Kombination dieser beiden Möglichkeiten gestillt würde.

### 3. Rechtsverhältnisse der Teilnehmer einer PKI und Bedeutung der CP/CPS

Die Rechtsverhältnisse wurden aus der Sicht der Teilnehmer der PKI dargestellt. Zu Letzteren würden nach Gramigna der Certification Services Provider (CSP, Anbieter von Zertifizierungsdiensten, Art. 2 lit. g ZertES) bzw. Certification Authority (CA), die Registration Authority (RA, Registrierungsstelle, Art. 8 Abs. 4 ZertES), der Certificate Holder und die Relying Party (Dritte, z.B. Privatpersonen, Ämter, Gerichte) und der Certification Body (CB, Anerkennungsstelle, Art. 2 lit. h ZertES) zählen. Deren Beziehungen würden sich – ganz traditionell – in öffentliches und privates Rechts unterteilen. Sodann seien ausservertragliche und vertragliche Anspruchsgrundlagen zu unterscheiden. Certification Policy (CP, Art. 9 Abs. 1 ZertES), Certification Policy Statement (CPS), Time Stamp Authority-Policy (TSA-P) und das Time Stamp Authority-Policy-Statement (TSA-PS) seien die zentralen Dokumente einer PKI. Zweck der CP und TSA-P sei, die Rechte und Pflichten zu regeln; derjenige der CPS und TSA-PS seien die Festlegung von Organisation und Abläufen. Dass mittels CP und CPS erheblich Einfluss auf die Rechtsbeziehungen der Teilnehmer einer PKI genommen werden könne, wurde eingehend am Dreieck CSP-Certificate Holder-Relying Party dargestellt. Eine der zentralen Fragen sei diejenige nach Umfang und Grenzen des berechtigten Vertrauens nach Art. 59a OR und Art. 16 ZertES in die Gültigkeit des qualifizierten Zertifikats, da konkrete Pflichten der Relying Party zur Prüfung der Gültigkeit eines Zertifikats gesetzlich nicht vorgesehen seien. Nicht a priori, sondern erst nach Prüfung des Einzelfalls sei, so Gramigna, eine Qualifikation der Beziehungen der Relying Party zu den übrigen Teilnehmern als vertragliche oder ausservertragliche möglich. Bezüglich der Rechtsnatur von CP und CPS sei nach Erachten Gramignas jeweils fraglich, ob es sich um einen Vertrag, um AGB oder um Regelwerke sui generis handle. Bezüglich empfohlener Themen und innerer Strukturierung gebe RFC<sup>16</sup> 3647 eine Empfehlung ab.

### IV. Elektronischer Geschäftsverkehr mit den Gerichten

Nach einem kurzen Unterbruch ging die Entwicklungshilfe weiter: Dr. Jacques Bühler vom Schweizerischen Bundesgericht, Lausanne, ergänzte das gewonnene Wissen über PKI mit einem Referat über den elektronischen Geschäftsverkehr mit dem Schweizerischen Bundesgericht. Bislang sei bekanntlich die Schweizerische Post<sup>17</sup> mit dem physischen Transport von Dokumenten im Mittelpunkt des Übermittlungsvorgangs von Rechtsschriften gestanden. Ab 1. Januar 2007 sei die Übermittlung endlich elektronisch möglich. Dies ergibt sich auch aus Art. 42 Abs. 4, Art. 48 Abs. 2 und Art. 60 Abs. 3 BGG. Das Bundesgericht sodann treffe eine Pflicht, elektronische Beschwerden entgegenzunehmen.

<sup>11</sup> BG über die technischen Handelshemmnisse (THG) vom 6. Oktober 1995 (SR 946.51).

<sup>12</sup> VO über das schweizerische Akkreditierungssystem und die Bezeichnung von Prüf-, Konformitätsbewertungs-, Anmelde- und Zulassungsstellen (Akkreditierungs- und Bezeichnungsverordnung, AkkBV) vom 17. Juni 1996 (SR 946.512).

<sup>13</sup> Diese sind: Technical Specifications des European Telecommunication Standards Institute (ETSI TS; s. Fn. 7); Request for Comments oder Internet Engineering Task Force (RFC); Federal Information Processing Standards des U.S. DEPARTEMENT OF COMMERCE/National Institute of Standards on Technology (FIPS); CEN Workshop Agreements (CWAs) in the ICT domain des CEN (Europäisches Komitee für Normung) u.a.

<sup>14</sup> RL 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen.

<sup>15</sup> TAV (s. Fn. 7), Anhang. In der Zwischenzeit wurde die TAV revidiert und per 1. Dezember 2006 in Kraft gesetzt (<<http://www.bakom.ch/themen/internet/00467/index.html>>, besucht am 14. Dezember 2006, s. dort: Technische und administrative Vorschriften über Zertifizierungsdienste im Bereich der elektronischen Signatur, Ausgabe 3 vom 13. November 2006). Es wird nun die Möglichkeit des Einsatzes einer «nach FIPS [Federal Information Processing Standards] 140-2 Level 3 (oder höher) zertifizierte[n] Signaturerstellungseinheit (...) als sichere Signaturerstellungseinheit» vorgesehen, «um qualifizierte elektronische Signaturen gemäss ZertES zu erstellen» (TAV, Anhang, 12).

<sup>16</sup> Request for Comments, s. Fn. 13.

<sup>17</sup> Oder eine schweizerische diplomatische oder konsularische Vertretung im Ausland (Art. 32 Abs. 3 OG bzw. Art. 48 Abs. 1 BGG).

Bühler zeigte die Funktionsweise der Übermittlung einer elektronisch eingeschriebenen Meldung am Beispiel eines Urteils. Im Mittelpunkt stehe hier die virtuelle Zustellplattform der Schweizerischen Post. Das Gericht lade das Urteil auf diese Zustellplattform (Upload). Der Partei werde dieser Upload mit einer elektronischen Einladung zur Abholung angezeigt. Während einer Dauer von sieben Tagen stehe das Urteil zum Download ab dem zugewiesenen elektronischen Postfach bereit. Bei Abholung bzw. Nicht-Abholung werde dem Gericht eine Quittung ausgestellt. Bei einem Download des Urteils durch die Partei beginne, so Bühler weiter, die Beschwerdefrist von 30 Tagen zu laufen. Da bestimmte Informationen betreffend das Urteil schon in der Einladung zur Abholung enthalten seien, könne nach Bühler mit dem Fristbeginn für die Beschwerde mit einem zeitlichen Spielraum von sieben Tagen handiert werden. Sämtliche Sende- und Empfangsvorgänge würden OSCI-Übermittlungen<sup>18</sup> darstellen, nur die Einladung zur Abholung geschehe durch traditionelle Mail-Übermittlung (SMTP<sup>19</sup>).

Es müssten auch hier gewisse Rahmenbedingungen erfüllt sein. Die Rechtsgrundlage sei mit dem BGG geschaffen worden. Wie Bühler feststellte, sei auch die elektronische Signierung möglich<sup>20</sup> und mit der Zustellplattform der Schweizerischen Post sei eine virtuelle Poststelle eingerichtet. Die notwendige Software stehe mit den Clients eGovLink bzw. JusLink und Trinity-Outlook zur Verfügung. Die betriebliche Organisation sei dabei nicht zu unterschätzen. Um das Angebot zu nutzen, müsse sich der Anwender Zertifikate für die elektronische Signierung besorgen, sich auf der Zustellplattform registrieren<sup>21</sup> und einen geeigneten Client installieren<sup>22</sup>. Als Belohnung würde man dafür einen vorteilhaften Preis im Vergleich mit dem physischen eingeschriebenen Versand der Dokumente durch die Post<sup>23</sup> erhalten.

Mit Screenshots von JusLink 2.0 zeigte Bühler die Perspektiven von Absender und Empfänger, wobei durch den Klick auf den Button «Senden» das Dokument elektronisch signiert und die Rechtsschriften im Dateiformat PDF und XML versendet würden – unabhängig vom Aufenthaltsort und von Schalteröffnungszeiten der Schweizerischen Post. Ein neues Mass an Flexibilität sei gewonnen. Beim Bundesgericht hoffe man daher auf ein Massengeschäft, liess Bühler verlauten. In Bälde seien auch weitere Anwendungen möglich. Schon jetzt würden kantonale Gerichtssoftware-Produkte wie Juris oder Tribuna miteinbezogen. Auch in anderen Bereichen wie dem SchKG, dem Grundbuch- und Handelsregisterwesen sollten entsprechende Lösungen gefunden werden.

## V. Kein BG über den elektronischen Geschäftsverkehr – quid iuris?

### 1. Anfängliche Analyse der Verwaltung und Entwurf eines BG über den elektronischen Geschäftsverkehr

Peter Schöbi vom Bundesamt für Justiz beurteilte das Unterfangen, über ein nicht in Kraft getretenes Gesetz zu sprechen, als schwierig. Niemand möge ihn als «Leichenschänder» bezeichnen!

Die Verwaltung habe zum Zeitpunkt, als sich die Regelung der elektronischen Signierung aufdrängte, diesbezügliche Defizite betreffend Konsumentenschutz festgestellt<sup>24</sup>, so Schöbi. Sie habe die Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift nicht gewollt ohne eine Verbesserung des Konsumentenschutzes. Der Erlass des ZertES sollte also im Anhang entsprechende Teilrevisionen des OR und des UWG enthalten. Die damals zuständige Bundesrätin, Ruth Metzler, habe freilich die Revision nicht mit dem Konsumentenschutz verbinden wollen. Nach Metzler habe das ZertES vorgehen sollen. Daher seien die beiden Vorlagen in einer «Nacht- und Nebelaktion», wie Schöbi es nannte, zweigeteilt worden. 2001 wurden demzufolge zwei Vorlagen in die Vernehmlassung geschickt, diejenige betreffend die Belange der elektronischen Signatur und diejenige

<sup>18</sup> Online Services Computer Interface-Übermittlung.

<sup>19</sup> Simple Mail Transfer Protocol.

<sup>20</sup> Diese ist nach Art. 42 Abs. 4 BGG erforderlich.

<sup>21</sup> Registration auf <http://www.incamail.ch>, besucht am 14. Dezember 2006.

<sup>22</sup> JusLink steht zum Download bereit auf <http://www.juslink.ch>, eGovLink auf <http://www.incamail.ch>, beide Websites besucht am 14. Dezember 2006. Bei JusLink handelt es sich um einen von einer bestimmten Plattform unabhängigen Open-Source Client.

<sup>23</sup> Nachricht bis 1 MB: CHF 2.50, pro zusätzliches MB CHF 0.80, wobei der Preis ab 1 MB auf KB genau berechnet wird. (<http://www.incamail.ch>), besucht am 14. Dezember 2006.)

<sup>24</sup> Diese Defizite seien nach Schöbi im Vergleich mit dem europäischen Recht zu erkennen (RL 1997/7/EG des Europäischen Parlaments und des Rates vom 20. Mai 1997 über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz; RL 1999/44/EG des Europäischen Parlaments und des Rates vom 25. Mai 1999 zu bestimmten Aspekten des Verbrauchsgüterkaufs und der Garantien für Verbrauchsgüter).

betreffend den elektronischen Geschäftsverkehr mit einer Gewichtung im Bereich des Konsumentenschutzes. Änderungen im OR und im UWG seien vorgesehen gewesen<sup>25</sup>. Das ZertES und die VZertES traten bekanntlich am 1. Januar 2005 in Kraft, gemeinsam mit einer Teilrevision des OR mit den entsprechenden Art. 14 Abs. 2bis und Art. 59a, und haben auf diese Weise ein eigenständiges Etappenziel erreicht.

Der vom ZertES losgelöste Entwurf des BG über den elektronischen Geschäftsverkehr sei positiv aufgenommen worden, auch von den – allerdings wenig betroffenen – Kantonen. Die wissenschaftliche Seite habe dagegen die vorgeschlagenen neuen Artikel des OR in Frage gestellt. Auch seitens der Anbieter sei Kritik zu vernehmen gewesen. Man habe Handlungsbedarf an anderen Orten gesehen – z.B. die Klärung der Providerhaftung, fasste Schöbi zusammen.

## 2. Entscheide des Bundesrates in den Jahren 2002–2005

Trotz Kritik habe der Bundesrat an der Vorlage festgehalten, jedoch ohne Revision des OR und ohne die Idee des Mantelerlass-Konzeptes, fuhr Schöbi fort. Die Vorlage sei in BG über die Teilrevision des OR und des UWG (Verbesserung des Konsumentenschutzes) umbenannt worden, was sich nach Schöbis Ansicht als Fehler erwies, den er – zumindest teilweise – sich selber zuschreiben will. Durch die Abkoppelung der Vorlage von derjenigen betreffend die elektronische Signatur sei die Vorlage ohnehin nicht mehr mehrheitsfähig gewesen, und ihr neuer Name habe es den Gegnern zu einfach gemacht.

Im Jahr 2005 sei ein autonomer Nachvollzug des europäischen Rechts für Bundesrat Christoph Blocher nicht mehr in Frage gekommen ohne eine gleichzeitige Stärkung des Wirtschaftsstandortes Schweiz. Im November 2005 sei die Vorlage betreffend BG über die Teilrevision des OR und des UWG (Verbesserung des Konsumentenschutzes) vom Bundesrat fallen gelassen worden. Im Dezember desselben Jahres habe der Bundesrat weiter auf eine gesetzliche AGB-Regelung verzichtet.

Konsumentenschutz habe nach Schöbis Empfinden in der Schweiz einen schweren Stand und nur Aussicht auf Erfolg, wenn auch die Anbieter profitieren würden. Verhängnisvoll für das gescheiterte Gesetz war die Abkoppelung der Vorlage von derjenigen betreffend das ZertES.

## 3. Ausblick mit Konzentration auf den Konsumentenschutz

Nach Schöbis Interpretation seien die Signale des Parlamentes nicht widerspruchsfrei. So folge es grösstenteils den Anträgen des Bundesrates: Vorstösse betreffend Konsumentenschutz würden abgelehnt. Gleichzeitig aber reiche die Geschäftsprüfungskommission des Nationalrates beispielsweise eine parlamentarische Initiative<sup>26</sup> ein, mit der sie den Entscheid des Bundesrates, auf eine Teilrevision von OR und UWG im Sinne des Konsumentenschutzes zu verzichten, kritisiere.

Die ewige Problematik betreffend Regelungen in Bezug auf AGB solle im Anhang zur Revision des Versicherungsgesetzes wieder neu aufgegriffen werden. Schöbi zeigte sich gespannt, ob man es wage, dieses Projekt überhaupt in die Vernehmlassung zu schicken.

## VI. Abschliessende Diskussion im Plenum

Wie bei Tagungen dieser Art üblich, bot sich als abschliessender Höhepunkt die Möglichkeit, der Podiumsdiskussion unter Beteiligung aller Referenten beizuwohnen und den Spezialisten Fragen zu stellen.

Auf die ans Panel gerichtete Frage bezüglich Sicherheit und potentielltem Missbrauch der jungfräulichen Technologie wies Schöbi auf Art. 59a OR hin. Diese Norm sei ausserdem sehr konsumentenfreundlich und im Vergleich etwa zu entsprechenden Bestimmungen in den AGB von Bankinstituten sehr zurückhaltend.

<sup>25</sup> So Änderungen im OR AT (Art. 4, 6a, 74 und 107), Informationspflicht und die Einführung eines Widerrufsrechts bei Fernabsatzgeschäften und Verbesserungen der Rechtsstellung des Käufers.

<sup>26</sup> Parlamentarische Initiative 06.457 vom 18. September 2006, «Verbesserung des Konsumentenschutzes im elektronischen Geschäftsverkehr». Vgl. auch die aktuelle parlamentarische Initiative 05.458 vom 15. Dezember 2005 von Simonetta Sommaruga. Im Dezember beschäftigte sich die Rechtskommission des Ständerates mit dieser Initiative. Eine Prognose wagte Schöbi nicht.

Betreffend die Wirkungen einer PKI auf Dritte wollte Berger wissen, ob durch Art. 59a OR diesen Dritten nicht ein Vertrag aufgezwungen würde. Schöbi verwies auf die ausservertragliche Natur dieser Bestimmung und fand die Diskussion hierüber allgemein zu abstrakt, er wolle konkrete Beispiele sehen. Gramigna verwies einerseits auf das Modell des Verhandlungsvertrags und die im Vorfeld getroffene Formabrede und bezüglich der Relying Party Agreements auf die internationale Praxis und das Beispiel eines in der Schweiz anerkannten CSP. Über den Anwendungsbereich und die Rechtsnatur von Art. 59a OR waren sich Schöbi und Gramigna in der Folge uneinig, wobei seitens Gramigna mit Hinweis auf die Botschaft zum ZertES und die Rechtsprechung zu Art. 41 OR argumentiert wurde, dass Art. 59a OR im Bereich einer vertraglichen Regelung unter Umständen nicht oder modifiziert zur Anwendung komme.

Berger wollte von Bühler hören, wie er die Problematik sehe, dass die Anwaltschaft sich eher schwer tue mit (technischen) Neuerungen. Bühler wies darauf hin, dass die Initiative für den elektronischen Geschäftsverkehr mit den Gerichten von Seiten des Schweizerischen Anwaltsverbandes (SAV) gekommen sei und das Bundesgericht durch das BGG<sup>27</sup> zu entsprechendem Handeln verpflichtet gewesen sei. In Österreich würden 85% des Geschäftsverkehrs mit den Gerichten elektronisch abgewickelt<sup>28</sup>. Dort sei daher eine Senkung der Kosten möglich gewesen. Aus dem Publikum wurde darauf hingewiesen, dass zuweilen Markenmeldungen aus haftpflichtrechtlichen Gründen nicht elektronisch vorgenommen würden, obwohl dies CHF 100 billiger sei. Die Votantin zeigte mit ihrer Äusserung die allgemein vorhandene Skepsis in der Anwaltschaft mustergültig auf. Daraufhin stellte Berger die Frage betreffend das Risiko einer allfälligen Haftung eines Anwaltes bei einem Stromausfall in den Raum. Aus dem Publikum wurde sodann die Möglichkeit eines Stromausfalles bei der Post in Erwägung gezogen, worauf auch Bühler nicht wusste, wer in diesem Fall haften würde – auf jeden Fall sei dies nicht das Bundesgericht; es seien wohl die AGB der Post beizuziehen. Einen Ratschlag hatte Bühler schliesslich doch noch: Die elektronische Nachricht sei mit Vorteil nicht erst um 23:59 Uhr des letzten Tages der ablaufenden Frist zu senden, da der Sendevorgang mit Verschlüsselung etwa zehn Minuten dauere.

Aus dem Publikum wollte man weiter wissen, ob die CHF 2.50 für den Versand über IncaMail pro 1 MB verhandelbar seien. Bühler wies auf die publizierten Preise der Post auf dem Internet hin<sup>29</sup>, schloss jedoch eventuelle Voluminaprozente nicht aus. Bei nachfragestarken Kunden könnte überdies ein gewisser Verhandlungsspielraum bestehen.

Zum Abschluss kam aus dem Publikum die Bitte um Umschreibung der Open Source-Software für den elektronischen Geschäftsverkehr mit dem Schweizerischen Bundesgericht. Gemeint war damit wohl der Client JusLink<sup>30</sup>. Nach Angaben Bühlers sei diese Software unter LGPL<sup>31</sup> entwickelt und an die Post weitergegeben worden. Weiterentwicklungen, die verbreitet würden, müssten zur Verfügung gestellt werden, ausser diese seien nur für den Eigengebrauch bestimmt.

Mit dem Ende der Diskussion war die Entwicklungshilfe für diesen Tag abgeschlossen. Der virtuelle Wissensdurst war für diesen Nachmittag gestillt, der physische wurde am anschliessenden Aperitif gelöscht. Es bleibt die Erkenntnis, dass trotz hoher Entwicklung hierzulande Entwicklungshilfe noch immer möglich ist.

\* lic. iur., Assistent am Lehrstuhl für Immaterialgüterrecht an der Universität Zürich.

<sup>27</sup> Nach Art. 42 Abs. 4 BGG bestimmt z.B. das Bundesgericht «in einem Reglement, in welchem Format die elektronische Zustellung erfolgen kann».

<sup>28</sup> Allerdings sei zu beachten, dass in Österreich Betreuungssachen in die Kompetenz der Gerichte fielen, was die Anzahl der zu behandelnden Fälle erhöhe.

<sup>29</sup> Dazu s. Fn. 23.

<sup>30</sup> Dazu hiervor IV.

<sup>31</sup> GNU Lesser General Public License.