

# Rechtsverbindliche Telekooperation im gewerblichen Rechtsschutz

— Technische und organisatorische Aspekte —

PA Axel H. Horns

[horns@ipjur.com](mailto:horns@ipjur.com)

Ursprünglich veröffentlicht im Juni 1999 in:

Mitteilungen der deutschen Patentanwälte **90** (1999), Heft 6, Seiten 201-213

## 1. Inhaltsübersicht

1.	Inhaltsübersicht .....	1
2.	Ansatzpunkte für zukünftige Formen der Telekooperation .....	1
3.	Bisherige Erfahrungen .....	2
3.1.	Deutschland .....	2
3.2.	EPA und WIPO .....	2
3.3.	Japan .....	3
3.4.	Fazit .....	3
4.	Rechtliche Probleme und technische Lösungsansätze .....	4
4.1.	Elektronisch vermittelte Willenserklärungen .....	4
4.2.	Äußerer Tatbestand und Erklärungsbewußtsein .....	5
4.3.	Geschäftswille und objektiver Erklärungsinhalt .....	6
4.4.	Verbindlichkeit .....	9
4.4.1.	Digitale Signaturen .....	9
4.4.2.	Zertifizierungsstellen .....	9
4.4.3.	Konkrete Ansätze und mögliche Globalisierung .....	11
4.4.4.	Zur Beweiskraft digitaler Signaturen .....	12
4.5.	Vertraulichkeit .....	12
5.	Der Versagensfall .....	14
6.	Schlußfolgerungen .....	16
gen	2	
3.1.	Deutschland .....	2
3.2.	EPA .....	2

3.3.	Japan .....	3
3.4.	Fazit .....	3
4.	Rechtliche Probleme und technische Lösungsansätze .....	4
4.1.	Elektronisch vermittelte Willenserklärungen .....	4
4.2.	Äußerer Tatbestand und Erklärungsbewußtsein .....	5
4.3.	Geschäftswille und objektiver Erklärungsinhalt .....	6
4.4.	Verbindlichkeit .....	9
4.4.1.	Digitale Signaturen .....	9
4.4.2.	Zertifizierungsstellen .....	9
4.4.3.	Konkrete Ansätze und mögliche Globalisierung .....	11
4.4.4.	Zur Beweiskraft digitaler Signaturen .....	12
4.5.	Vertraulichkeit .....	12
5.	Der Versagensfall .....	14
6.	Schlußfolgerungen .....	16

## 2. Ansatzpunkte für zukünftige Formen der Telekooperation

Das System gewerblicher Schutzrechte trifft in vielen Staaten auf eine steigende Nachfrage, wie die von den Patent- und Markenämtern veröffentlichten Fallzahlen zeigen<sup>1,2,3</sup>. Dies darf jedoch

<sup>1</sup>Konrad Faust: "Internationale Patentanmeldungen: Globale Positionen und strukturelle Anpassungsreaktionen", ifo-Schnelldienst **50** (1997) Nr. 11, S. 7 bis 14, zeigt eine Statistik, nach der sich weltweit die Zahl der mindestens in zwei Staaten zum Patent angemeldeten Erfindungen von ca. 50.000 im Jahre 1970 auf ca. 109.000 im Jahr 1994 erhöht hat.

<sup>2</sup>vgl. dazu z.B. auch die Angaben in: WIPO Gazette of International Marks - Statistical Supplement - **2** (1997)

<sup>3</sup>Eine Pressemitteilung des DPA vom 13. August 1998

nicht darüber hinwegtäuschen, daß die im Zusammenhang mit dem gewerblichen Rechtsschutz seitens der Ämter, der Anmelder und der Anwaltschaft erbrachten Leistungen unter Kostengesichtspunkten kritischer als je zuvor betrachtet werden<sup>4</sup>. Ein wichtiger, jegliche Rationalisierung bremsender Hemmfaktor bei der Kostensenkung ist die durch gesetzliche Schriftformerfordernisse erzwungene Papiergebundenheit aller an den einschlägigen Arbeitsabläufen beteiligten Organisationen.<sup>5</sup> Die heute in Gestalt global vernetzter Rechner zur Verfügung stehenden datenverarbeitungstechnischen Mittel versprechen hier Abhilfe, doch ist ihr erfolgreicher Einsatz an eine Reihe rechtlicher und tatsächlicher Voraussetzungen gebunden.

Die Zeichen der Zeit sind auch in Deutschland nicht zu übersehen: Durch das zweite Gesetz zur Änderung des Patentgesetzes und anderer Gesetze vom 16. Juli 1998 (2. PatÄndG)<sup>6</sup> ist das Schriftformerfordernis aus dem § 35 PatG vom Gesetzgeber mit der Begründung gestrichen worden, es sollen damit rechtliche Möglichkeiten für eine zukünftige elektronische Einreichung von Patentanmeldungen eröffnet werden. Diese Reform weist in eine Zukunft, die im kommenden Jahrhundert durch eine *rechtsverbindliche Telekooperation* zwischen Amt und Anmelderschaft geprägt sein wird. Es gibt auch keinen Grund, die rechtsverbindliche Telekooperation lediglich auf die Interaktion zwischen Ämtern und Anmelderschaft beschränkt zu sehen. Ein wichtiger Teil des internationalen Rechtsbesorgungsgeschäftes wird durch Kooperation von Anwaltskanzleien abgewickelt, die ebenso wie die Interaktion mit den Ämtern einer durchgreifenden Modernisierung durch Telekooperation zugänglich sein sollte. Auch die Patentanwälte werden sich dieser Entwicklung langfristig nicht entziehen können. Es ist daher an der Zeit, über eine akzeptable Ausgestaltung dieser kommenden Technik nachzudenken.

### 3. Bisherige Erfahrungen

#### 3.1. Deutschland

Das Deutsche Patent- und Markenamt läßt durch die Bundesdruckerei eine Zusatzsoftware<sup>7</sup> für ein

gängiges Textverarbeitungsprogramm<sup>8</sup> herstellen, mit der die Anmelder die Anmeldungsangaben einschließlich Anmeldungstext und Figuren in maschinenlesbarer Form auf eine Diskette kopieren und dem Amt zur Verfügung stellen können<sup>9</sup>. Technisch ist die DEPAEASY-Software als Formatvorlagendatei implementiert. Die Möglichkeit, Programmbefehle der "Word Basic"-Programmiersprache in Word-Textdateien zu integrieren, hat dem DPMA die Verwirklichung einer rudimentären Strukturierung der bibliographischen Angaben sowie des Anmeldungstextes gestattet. Zeichnungen können als Grafikdateien in die Textdatei eingebettet werden. Für die Zukunft kündigt das DPMA einen Feldversuch im Rahmen des MIPEX-Projektes an.<sup>10</sup>

#### 3.2. EPA und WIPO

Seit Ende 1992 wird im Europäischen Patentamt (EPA) an einer Software zum elektronischen Einreichen von Patentanmeldungen gearbeitet<sup>11</sup>. Das EPA hat kürzlich eine entsprechende Software<sup>12</sup> in der Version 2 vorgestellt<sup>13</sup>. Dabei bildet die EASY-Software eine gemeinsame Plattform für einzelne Module, die die Besonderheiten der jeweiligen Patentämter berücksichtigen. Die Plattform ermöglicht eine komfortable Verwaltung von Dateien im Zusammenhang mit einer Vielzahl von Patentanmeldungen. Der Benutzer kann leicht verfolgen, welche Dateien bereits einreichungsreif oder sogar schon eingereicht sind und welche noch wesentlicher Angaben entbehren. Sogar eventuell von einem Patentamt zurückübermittelte Einreichungsbestätigungen können der entsprechenden Patentanmeldungsdatei zugeordnet verwaltet werden. Eine kleine Datenbank enthält länderspezifische Daten und unterstützt den Benutzer bei der Erstellung der Anmeldungen. Der Vorgang des Erfassens der Daten sowie des Erzeugens einer einreichungsfähigen Diskette ist ebenso wie ein zukünftig geplanter on-line-Einreichungsvorgang den länderspezifischen Modulen zugeordnet, in denen gewisse grobe Plausibilitätsüberprüfungen der eingegebenen Daten vorgenommen werden. Fehlt beispielsweise der Name des Anmelders oder eine andere obligatorische Angabe, warnt die Software den Benutzer. Bisher stehen spezifische Module für das Europäische Patentamt sowie für das Internationale Büro der WIPO zur Verfügung<sup>14,15</sup>. Der besondere

vermeldet im I. Halbjahr 1998 einen Anstieg der Anmeldezahlen für Patente von 17,4 % und für Marken von 20,7%.

<sup>4</sup>Siehe z.B. Joachim Beier: "Die tatsächlichen Patentkosten - eine FICPI Studie"; FICPI Revue et Bulletin Nr. 39 (1997), S. 82 bis 102

<sup>5</sup>Zum Rationalisierungspotential siehe zum Beispiel: "Draft Concept of Operations for Electronic Filing Version 0.1", US-PTO April 17, 1997. Erhältlich online über <http://www.uspto.gov/web/offices/cio/conops/cdr1007c.htm>

<sup>6</sup>Bl. f. PMZ **100** (1998), S. 382 bis 419

<sup>7</sup>DEutsches PAtentamt ELektronisches AAnmelde SYstem - "DEPAEASY"

<sup>8</sup>Microsoft Word Version 6

<sup>9</sup><http://www.bundesdruckerei.de/ep/depaeasy.htm>

<sup>10</sup>Zum MIPEX-Projekt vgl. u.a.

<http://www.tagish.co.uk/nip/236a.htm> und

[http://www.gresh.com/solutions/case/cas\\_cs3.htm](http://www.gresh.com/solutions/case/cas_cs3.htm)

<sup>11</sup>John R. S. Orange: "Legal Aspects of EASY"; FICPI Revue et Bulletin Nr. 39 (1997), S. 109 bis 121

<sup>12</sup>EASY Version 2.0

<sup>13</sup><http://www.epo.co.at/easy/index.htm>

<sup>14</sup>Das belgische Office de la Propriété Industrielle stellt eine entsprechende Softwarekomponente zur Verfügung, mit der ab dem 01. Januar 1999 Anmeldungen auch elektronisch angenommen werden; ABl. EPA 1998, S. 555. Wie zu erfahren war, arbeiten weitere nationale

Clou der EASY-Software besteht jedoch darin, daß beabsichtigt ist, sie in Gestalt eines Windows-API<sup>16</sup> an solche Unternehmen abzugeben, die Administrationssoftware für Patentanwaltskanzleien und Patentabteilungen erstellen und vermarkten. Hier ist also im Kern der Ansatz einer internationalen de-facto-Standardisierung einer Schnittstelle zur Telekooperation zwischen Ämtern und Anmeldern beziehungsweise deren Vertretern zu erkennen. Die WIPO hat unlängst einen ambitionierten IT-Gesamtplan veröffentlicht, der unter anderem auch Aspekte der rechtsverbindlichen Telekooperation umfaßt.<sup>17</sup>

### 3.3. Japan

Das älteste System zur elektronischen Einreichung von Patentanmeldungen ist jedoch bereits im Dezember 1990 in Japan in Betrieb genommen worden<sup>18</sup>. Mittlerweile können nicht nur Anmeldungen per Diskette oder on-line eingereicht werden; es ist auch möglich, Amtsbescheide elektronisch zuzustellen, Prüfungsanträge zu stellen und Einzahlungen von Jahresgebühren vorzunehmen. Das System basiert auf einer speziellen relativ kostspieligen Hardware, die von Anmeldern und Kanzleien beschafft werden muß, wenn die Teilnahme gewünscht wird. Beim herkömmlichen Einreichen von Papierdokumenten anstelle digitaler Dokumente werden die Kosten der Datenerfassung dem Anmelder auferlegt. Die online-Datenübermittlung erfolgt unverschlüsselt über ISDN- oder DDX-P-Netze. An Sicherheitsmaßnahmen sind als "digitale Ausweise" verwendete Magnetkarten vorgesehen. Da über die konkreten Erfahrungen mit diesem System nur sehr wenige Texte in vorliegen, ist es nicht leicht, einen Überblick über damit zusammenhängende Akzeptanz- und Sicherheitsprobleme zu gewinnen. Einige Andeutungen<sup>19</sup> lassen aber die Vermutung aufkommen, daß in der Einführungsphase Unstimmigkeiten an der Tagesordnung waren.

---

Patentämter bereits an eigenen Modulen.

<sup>15</sup> Da zwischen den PCT-Anmeldeämtern noch keine Einigung über zulässige Dateiformate erzielt worden ist, kann der Anmeldungstext mit Beschreibung und Patentansprüchen derzeit ebensowenig elektronisch eingereicht werden wie die Patentzeichnung.

<sup>16</sup> **A**pplication **P**rogramming **I**nterface

<sup>17</sup> WIPO-Dokument SCIT/3/2 vom 05. mai 1999: "SCIT Strategic Information Technology Plan into the twenty-first century"

<sup>18</sup> Kazuaki Takami: "The Japanese Experience", FICPI Revue et Bulletin Nr. 39 (1997), S. 122 bis 126

<sup>19</sup> WIPO-Dokument ITIP/WG/I/6 vom 14. Juli 1997: "[...] An electronic application filing system was also introduced in 1990 to allow applicants to file their applications by means of on-line data transmission or by mailing a flexible disk. Legal and technical hurdles were required to be cleared for the introduction of the electronic filing system. These included prevention of transmission errors, identification of applicants and payment of fees as well as development of the specific software designed for the electronic filing. The JPO's experience is full of successes and failures, both of which will provide the WIPO with good lessons.[...]"

### 3.4. Fazit

Die bisherigen Ansätze des DPMA, des EPA und der WIPO haben gemeinsam, daß sie in ihrer derzeitigen Ausprägung das klassische Schriftformerfordernis vorerst noch unangetastet lassen. Im deutschen Patentrecht verpflichtet § 2 der Patentanmeldeverordnung den Anmelder weiterhin, eine Papierfassung als allein rechtsverbindliche Anmeldungsunterlage einzureichen. Die Praxis des EPA wird durch Regel 24 EPÜ festgelegt und sieht gemäß den bisher vom Präsidenten des Amtes vorgelegten Regelungen noch keine papierlose Einreichung von Patentanmeldungen vor. Im Rahmen des PCT erfordert Regel 3.1 der Ausführungsordnung noch einen schriftlichen Antrag, der "auf einem gedruckten Formblatt zu stellen oder als Computerausdruck einzureichen" ist. Mit Wirkung zum 1. Januar 1999 ist nunmehr eine Regel 89ter in die Ausführungsordnung zum PCT aufgenommen worden, die es den Anmeldeämtern fakultativ ermöglicht, neben dem Papierexemplar ein Anmeldeexemplar in elektronischer Form entgegenzunehmen<sup>20</sup>. Der Vorteil der Entgegennahme maschinenlesbarer Unterlagen für die jeweiligen Ämter liegt auf der Hand: Dadurch, daß der Anmelder angehalten wird, die Anmeldungsunterlagen in maschinenlesbarer Form abzuliefern, entfällt der kostenintensive und fehlerträchtige Schritt des datenverarbeitungstechnischen Neuerfassens der Anmeldungsunterlagen im Amt. Der Ansatz der WIPO honoriert den dabei seitens des Anmelders entstehenden Mehraufwand mit einem Gebührenerlaß<sup>21,22</sup>; weitere Vorteile sind auf der Anmelderseite nicht erkennbar. Diese Parallelität von traditionellem Schriftformerfordernis und dem an die Anmelderschaft herangetragenen Ansinnen der Ämter, maschinenlesbare Anmeldungsunterlagen eingeliefert zu bekommen, kann wegen der Asymmetrie im Genuß der damit verbundenen Vorteile nur als Übergangszustand hin zu einer vollständig vom Papier abgelösten rechtsverbindlichen Telekooperation zwischen dem Anmelder und dem Amt zeitlich begrenzt Bestand haben.

Die japanische Erfahrung geht insofern weit über die noch eher konservativen Ansätze des DPMA, des EPA und der WIPO hinaus, als hier zu einem sehr frühen Zeitpunkt der "Sprung in das kalte Wasser" einer rechtsverbindlichen elektronischen Einreichung gewagt wurde, allerdings ohne Sicherheitsnetz. Es scheint nicht der landesspezifischen Mentalität zu entsprechen, die hierbei aufgetretenen Probleme im Detail vor einem internationalem Fachpublikum offenzulegen<sup>23</sup>. Gewiß

---

<sup>20</sup> Siehe WIPO-Dokument PCT/A/26/1 vom 17.07.1998 in Verbindung mit WIPO-Dokument PCT/A/26/2 vom 15. September 1998

<sup>21</sup> WIPO-Dokumente PCT/A/26/1 und PCT/A/26/2 a.a.O.

<sup>22</sup> PCT-EASY - vgl. die diesbezügliche Ankündigung in PCT-Newsletter 10/1998, Seite 2

<sup>23</sup> Weder in Printmedien noch im Internet läßt sich sonderlich viel hierüber herausfinden.

wäre es unvernünftig, in den sehr viel weniger korporatistisch verfaßten westlichen Staaten mit einer offeneren Streitkultur ein im technischen Sinne mangels wirksamer Schutzvorkehrungen gegen Betrug und Übermittlungsfehler unsicheres System einzuführen.

Ein typisches Szenario für eine zukünftige rechtsverbindliche Telekooperation wird beispielsweise darin bestehen, daß die Patentabteilung im Unternehmen oder der externe Patentanwalt eine mit dafür geeigneten Programmen ausgestattete Datenverarbeitungsanlage heranzieht, um eine Datei zu erstellen, die alle eine Patentanmeldung konstituierenden Angaben einschließlich Patentbeschreibung, Ansprüche und Zeichnung enthält. Wenn die Arbeiten zur Erstellung dieser Datei beendet sind, wird diese Datei in einem der Unterschriftenleistung vergleichbaren besonderen Vorgang von einer verantwortlichen Person für abgeschlossen erklärt und per Datenfernübertragung direkt auf einen Rechner des Patentamtes übertragen. Dabei sind die technischen Mittel derart ausgestaltet, daß sich der Anmelder rechtsverbindlich an dem Erklärungsgehalt der von ihm übertragenen Datei festhalten lassen muß. Andererseits stellt das Amt unverzüglich eine ebenso rechtsverbindliche digitale Einreichungsbestätigung aus, die binnen kürzester Zeit nach der Vollendung des Einreichungsvorganges auf den Rechner beim Anmelder beziehungsweise beim Anwalt übermittelt wird. Der Unterschied dieses Szenarios zu einer herkömmlichen elektronisch gestützten Kooperation per Telefax<sup>24</sup> besteht darin, daß bei dieser Telekooperation im engeren Sinne Willenserklärungen ohne körperlichen Ausdruck auf Papier<sup>25</sup> und ohne Bezugnahme auf eine vorbestimmte potentielle oder vollkommen fiktive körperliche Ausgabe auf Papier<sup>26</sup> direkt zwischen Datenverarbeitungsanlagen der Kooperationspartner ausgetauscht werden. Die durch den in der Rechts- und Verwaltungssprache gebräuchlichen Begriff "Fernkopie" eingeführte gedankliche Brücke von einer elektronisch vermittelten Darstellung einer Willenserklärung zu der althergebrachten Schriftform wird durch die Telekooperation im engeren Sinne aufgehoben.

Nun ist diese Telekooperation auch in ihrer rechtsverbindlichen Ausprägung als solche keinesfalls neu. In bestimmten Wirtschaftsbereichen, beispielsweise bei der Zusammenarbeit zwischen

<sup>24</sup> Die Dogmatik herkömmlicher Telekooperation per Telefax faßt der Vorlagebeschluß des BGH vom 29. September 1998 - XI ZR 367/97 - anschaulich zusammen; NJW 51 (1998), Heft 49, S. 3649 bis 3650.

<sup>25</sup>d.h. Ausdruck eines mit einem Textverarbeitungsprogramm erzeugten Dokumentes auf Papier und nachfolgendes Übertragen durch Einlegen des körperlichen Dokumentes in ein Telefaxgerät.

<sup>26</sup>d.h. Erzeugen einer rechnerinternen Darstellung einer fiktiven Papierseite mit dem Abbild eines mit einem Textverarbeitungsprogramm erzeugten Dokumentes, die dann durch ein zum Telefaxdienst befähigtes Modem unmittelbar an den Empfänger übertragen wird.

Automobilindustrie und Zulieferindustrie, ist sie in Gestalt von UN/EDIFACT<sup>27</sup> langjährig erprobte Wirklichkeit<sup>28</sup>. Dessenungeachtet ist zu beachten, daß Konzepte aus anderen Bereichen der Wirtschaft infolge der Besonderheiten des Rechtsbesorgungsgeschäftes im Bereich des Gewerblichen Rechtsschutzes nicht ohne weiteres einfach kopiert werden können<sup>29</sup>.

## 4. Rechtliche Probleme und technische Lösungsansätze

### 4.1. Elektronisch vermittelte Willenserklärungen<sup>30</sup>

Bei der rechtsverbindlichen Telekooperation kommt es darauf an, Willenserklärungen mit Hilfe vernetzter Datenverarbeitungsanlagen zu realisieren. Eine Willenserklärung ist eine auf einen Rechtserfolg gerichtete private Willensäußerung, deren Wirkungen von der Rechtsordnung entsprechend diesem Erfolgswillen bestimmt werden<sup>31</sup>. Der *äußere Tatbestand* einer Willenserklärung ist ein äußeres Verhalten, das nach Verkehrssitte oder Vereinbarung den Schluß auf einen bestimmten Geschäftswillen zuläßt und dazu bestimmt erscheint, einen derartigen Geschäftswillen anderen kundzugeben und wird im Falle der Telekooperation durch eine in einem System vernetzter Datenverarbeitungseinrichtungen<sup>32</sup> ablaufende Kausalkette verkörpert, die vom Erklärenden angestoßen werden kann und deren Wirkungen im Bereich des Erklärungsempfängers technisch wahrnehmbar sind. Von diesem äußeren Tatbestand ist der *innere Tatbestand* zu unterscheiden, der mit dem Erklärungsbewußtsein desjenigen, der die Willenserklärung abgibt, in Zusammenhang steht. Das Erklärungsbewußtsein setzt beim Handelnden die Vorstellung voraus, sich am Rechtsverkehr zu beteiligen, d.h. eine Erklärung für rechtliche Zwecke abzugeben<sup>33</sup>. Bei einer gelingenden Willenserklärung wird das äußere Verhalten, d.h. die die Kausalkette auslösende Handlung des Erklärenden, von einem ent-

<sup>27</sup>UN/EDIFACT (United Nations / Electronic Data Interchange For Administration, Commerce and Transport) ist der Name für das definierte Regelwerk der Vereinten Nationen für den elektronischen Datenaustausch in Verwaltung, Wirtschaft und Transport.

<sup>28</sup>Zu den Anwendungsbereichen siehe auch: UN/EDIFACT: Funktionale Beschreibungen ausgewählter UN/EDIFACT Nachrichtentypen. Berlin: Normenausschuß Bürowesen im DIN e.V., 4. Auflage, 1997

<sup>29</sup>zur Diskussion der Problematik der rechtsverbindlichen Telekooperation außerhalb des gewerblichen Rechtsschutzes vgl. auch Bundesnotarkammer [Hg.] "Elektronischer Rechtsverkehr - Digitale Signaturverfahren und Rahmenbedingungen", Köln: Verlag Dr. Otto Schmidt, 1995.

<sup>30</sup>Siehe dazu Heinz Hübner: Allgemeiner Teil des Bürgerlichen Gesetzbuches. Walter de Gruyter: Berlin, 1984, Rdn. 376ff.

<sup>31</sup>Hübner, a.a.O.

<sup>32</sup>beispielsweise dem Internet

<sup>33</sup>Hübner, a.a.O.

sprechenden *Erklärungsbewußtsein* getragen. Bei einem gestörten Ablauf findet zwar ein schlüssiges äußeres Handeln statt, es fehlt jedoch das Bewußtsein, sich am Rechtsverkehr zu beteiligen. Ist eine Willenserklärung zustandegekommen, erhebt sich die Frage nach ihrem Gegenstand. Der *Geschäftswille* ist die auf einen bestimmten rechtlich gesicherten Erfolg gerichtete Absicht. Die ohne technische Hilfsmittel mit den Sinnen nicht erkennbare Qualität eines digitalen Dokumentes kann besonders leicht dazu führen, daß der Geschäftswille vom objektiven Erklärungsinhalt abweicht.

Die Erörterung der Ursachen möglicher Störungen bei der Abgabe und dem Empfang elektronisch vermittelter Willenserklärungen kann nicht abstrakt ohne Bezugnahme auf die konkrete Ausgestaltung der hierfür herangezogenen technischen Systeme vorgenommen werden, da die agierenden Subjekte de facto in ihren Handlungsmöglichkeiten von vornherein auf bestimmte, durch das System vorbestimmte Handlungsoptionen beschränkt und diesen vollständig unterworfen sind<sup>34</sup>. Die technische Implementation von Systemen zur rechtsverbindlichen Telekooperation muß sich daher hinsichtlich zweier Aspekte befragen lassen:

a) Welche Hilfestellung leistet die konkrete Implementation bei der Unterscheidung solcher Abläufe, bei denen äußerer Tatbestand und Erklärungsbewußtsein einander entsprechen, von gestörten Abläufen, bei denen äußerer Tatbestand und Erklärungsbewußtsein möglicherweise auseinanderfallen?

b) Welche Hilfestellung leistet die konkrete Implementation bei der Unterscheidung solcher Abläufe, bei denen Geschäftswille und objektiver Erklärungsinhalt einander entsprechen, von gestörten Abläufen, bei denen der Geschäftswille möglicherweise nicht mit dem objektiven Erklärungsinhalt übereinstimmt?

#### **4.2. Äußerer Tatbestand und Erklärungsbewußtsein**

Die technische Entwicklung von Software für Datenverarbeitungsanlagen im Bürobereich in den vergangenen Jahren hat generell zu einer erheblichen *Vereinfachung* von Bedienungsabläufen geführt. So erforderten beispielsweise bestimmte Texteditoren auf Großrechnern der frühen 70er Jahre noch, daß bei einer Verschiebung einer

<sup>34</sup>An dieser Stelle wird vorausgesetzt, daß elektronische Einrichtungen ohne weiteres ein geeignetes Mittel zur Vermittlung von Willenserklärungen sein können. Für den bürgerlich-rechtlichen Bereich siehe z.B. Josef Mehrings: "Vertragsabschluß im Internet", MMR **1** (1998), Nr. 1, S. 30-33 m.w.N. Es ist nicht ersichtlich, daß diese Erwägungen nicht auch auf prozessuale Erklärungen übertragbar sind, wenn und soweit der Gesetzgeber dies zuläßt, was beispielsweise hinsichtlich bestimmter gegenüber dem DPMA abzugebender Verfahrenserklärungen in absehbarer Zukunft geschehen dürfte.

Zeile in einer Textdatei ein komplizierter Befehl in einer formalen Sprache abzufassen und vom Benutzer einzutippen war, der unter anderem die Zeilennummern des betreffenden Textbereiches enthielt, wohingegen moderne Bürosoftware mit einer graphischen Bedienoberfläche ausgestattet ist und eine entsprechende Textverschiebung unter Umständen mit einer einzigen Mausaktion ermöglicht. Was bei der Erstellung von Textdokumenten als vorteilhaft erkannt wird, erweist sich in solchen Programmteilen, die die Bedienoberfläche zur Abgabe elektronisch vermittelter Willenserklärungen herstellen, als Gefahrenquelle. Die prosaische Ausgestaltung der Abgabe einer Willenserklärung durch einen einzigen Mausklick auf eine Schaltfläche ließe Zweifel am Weitblick der hierfür verantwortlichen Softwarearchitekten aufkommen. Auch eine um Bestätigung bittende Rückfrage wie etwa "Wollen Sie diese Willenserklärung wirklich so abgeben?" hülfe nur bedingt, denn der Gewöhnungseffekt wird im Laufe der Zeit unweigerlich dazu führen, daß die Bestätigungsschaltfläche dieser Rückfrage mit einem Mausklick reflexartig betätigt wird, ohne auch nur einen einzigen weiteren Gedanken zu verschwenden. Unter den heutigen Gegebenheiten kann zwar die Notwendigkeit, eine Diskette in das Diskettenlaufwerk einzulegen oder - im Fall einer on-line Einreichung über das Internet mit einem Dial-Up-Zugang - der Einwählvorgang in den Zugangsrechner erlebbare Zäsurpunkte konstituieren, doch ist mittelfristig damit zu rechnen, daß diese Umstände mit der weiteren Verbreitung von Internet-Standleitungsanschlüssen mehr und mehr verschwinden werden.

Im Gegensatz zu der allgemeinen Maxime bei der Verbesserung von Software muß es bei der Bedienoberfläche für die Abgabe von Willenserklärungen nicht um eine Vereinfachung der Bedienung, sondern im Gegenteil geradezu um den Einbau von Schikanen gehen, die den die Willenserklärung abgebenden Benutzer zwingen, einen Augenblick innezuhalten und sich über die Tragweite seines Tuns klar zu werden. Dieses Problem ist weder rechtlicher noch technischer Natur, sondern hat seinen Kern im eingeübten Sozialverhalten des Benutzers. So darf man beispielsweise durchaus grundsätzlich unterstellen, daß den allermeisten Individuen die dessen Handlungsmöglichkeiten festlegende Rolle des Geldes ohne weiteres intuitiv klar ist. Dies führt dazu, daß bei Transaktionen an geldbetätigten Automaten, an EC-Geldautomaten oder bei Eingabe der Kreditkartennummer bei on-line-Bestellungen an Versandhäuser eher davon ausgegangen werden kann, daß der Handelnde in dem Augenblick, in dem er von diesen Zahlungsmitteln Gebrauch macht, sich der Tragweite seiner Handlung bewußt wird.

Bei der Abgabe von bestimmten Arten von Willenserklärungen gegenüber Zentralbehörden des gewerblichen Rechtsschutzes, die Kraft anderweitiger gesetzlicher Bestimmungen bei Ausbleiben einer dazugehörigen Gebührenentrichtung

als nicht abgegeben gelten, könnte somit daran gedacht werden, den Akt der Abgabe der Willenserklärung mit dem Benutzen einer Kreditkarte zur Gebührenentrichtung unmittelbar zu koppeln. Da in Patentabteilungen und Anwaltskanzleien Gebührenzahlungen jedoch aus betrieblichen Gründen anderweitig organisiert werden und überdies die Entrichtung der Gebühr in befristeten Grenzen zeitversetzt zur Abgabe der Willenserklärung erfolgen darf, kommt diese Ausgestaltung in der Praxis wohl kaum in Betracht.

Die weiter unten unter dem Gesichtspunkt der Beweisbarkeit von Willenserklärungen eingeführten und näher erläuterten *digitalen Signaturen* können in der Praxis so ausgestaltet werden, daß hierzu das Einführen einer Chipkarte in einen Kartenleser und das Entsperren dieser Karte durch Eingabe einer persönlichen und geheimen PIN erforderlich ist. Fortgeschrittenere Konzepte erkennen die Schwächen des PIN-Konzeptes und setzen auf biometrische Techniken zur Identifikation des rechtmäßigen Chipkartenbesitzers. Dies führt dazu, daß der Handelnde beispielsweise seinen Daumen auf einen Fingerabdruckabstastensensor pressen oder mit einem Auge in eine Iriserkennungsvorrichtung blicken muß. Neben dem primären Zweck der Fixierung des Erklärungsinhaltes kann ein System zur Generierung von digitalen Signaturen somit technisch derart ausgestaltet werden, daß der die Willenserklärung abgebende Bediener eine Reihe von ungewöhnlichen und ein wenig umständlichen Handlungen vornehmen muß. Diese Ritualisierung kann dazu herangezogen werden, um eine Zäsurwirkung zu erzielen, bei der dem Benutzer die rechtliche Tragweite seines Handelns bewußt wird.

Die bisherigen Ansätze des DPMA, des EPA und der WIPO lassen nicht erkennen, daß über das Betätigen von bestimmten eindeutig beschrifteten Schaltflächen hinaus Zäsurpunkte implementiert sind, die dem Benutzer Gelegenheit geben, die rechtliche Tragweite seines Handelns auch nach einer langjährigen Gewöhnung deutlich erlebbar werden zu lassen. Da diese Programme bislang noch nicht von digitalen Signaturen Gebrauch machen, kann dieser Aspekt derzeit auch noch nicht sinnvoll beurteilt werden.

#### **4.3. Geschäftswille und objektiver Erklärungsinhalt**

Bei der Beurteilung einer technischen Implementation eines Systems zur rechtsverbindlichen Telekooperation ist nach der technischen Ausgestaltung der Zuordnung zwischen einer digitalen Darstellung eines Dokumentes einerseits und dessen rechtsbedeutsamem Erklärungsinhalt andererseits zu fragen. Da der digital dargestellte Inhalt des Dokumentes als solcher nicht unmittelbar wahrnehmbar ist, bedarf es eines besonderen Anzeigeprogrammes, der sog. *Darstellungskomponente* eines Systems zur rechtsverbindlichen Telekooperation, das für eine Umsetzung des digitalen Dokumentes in eine sinnlich wahr-

nehmbare Form, beispielsweise als Zeichenfolge auf einem Bildschirm oder auf einem Papierausdruck, sorgt. Bei einer gelungenen Implementation eines solchen Programmes, durch das die Zuordnung zu dem sich des Systems bedienenden handelnden Akteur stets störungsfrei erfahrbar ist, kann die Gefahr eines Auseinanderfallens von Geschäftswille und objektivem Erklärungsinhalt reduziert werden. Andererseits wird eine mißlungene Implementation, die dem Handelnden eine fehlerhafte Zuordnung zuleitet, selbst zu einer Ursache für Störungen im Verlauf des Vorganges der Abgabe einer elektronisch vermittelten Willenserklärung. Hier stellt sich die Frage, wie die Qualität einer Darstellungskomponente beurteilt werden kann.

Eine denkbare und besonders einfache Form einer Festlegung dieser Zuordnung besteht darin, den Erklärungsgehalt eines digitalen Dokumentes an der sprachlichen Bedeutung der Aneinanderreihung von in dem digitalen Dokument dargestellten Schriftzeichen festzumachen. So ist es beispielsweise möglich, hinsichtlich des Erklärungsgehaltes eines digitalen Dokumentes eine Vereinbarung zu treffen, wonach jeweils acht aufeinanderfolgende Bit zusammenzufassen und gemäß der ASCII-Tabelle einem Schriftzeichen zuzuordnen sind, wobei die nach dieser Zuordnungsvorschrift gewonnenene Folge von Schriftzeichen nach überkommenen Regeln sprachlich auf ihren Erklärungsgehalt hin zu interpretieren ist. Programme, die ASCII-Zeichen auf einem Bildschirm darstellen oder auf einem Drucker ausgeben können, gibt es zuhauf. Es leuchtet jedoch unmittelbar ein, daß diese einfache Zuordnungsvorschrift schon für eine einfache Patentanmeldung mit mindestens einer Figur unzureichend ist, denn die flächige Schwärzungsverteilung einer Zeichnung ist nicht ohne weiteres durch eine Folge von Schriftzeichen darstellbar.

Erfreulicherweise stellt die moderne Datenverarbeitungstechnik eine ganze Palette leistungsfähiger und auf Rechnern implementierbarer Zuordnungsvorschriften von einzelnen Bits zu der menschlichen Verstandeswahrnehmung zugänglichen Objekten wie Texten und Bildern zur Verfügung. Dabei scheint es auf den ersten Blick eine triviale Forderung zu sein, daß die im Rahmen eines Telekooperationsverhältnisses jeweils vereinbarten Zuordnungsvorschriften genormt und vollständig veröffentlicht sind, damit verschiedene Anbieter Darstellungskomponenten erstellen können und jeder Anwender im Bedarfsfalle den gültigen Erklärungsgehalt der von ihm produzierten oder empfangenen digitalen Dokumente eigenständig mit einer oder mehreren Darstellungskomponenten seiner Wahl verifizieren kann. Außerdem sollte die Zuordnungsvorschrift so einfach wie möglich sein, da die Fehleranfälligkeit der Darstellungskomponenten mit der Komplexität der Zuordnungsvorschrift zunimmt.

In diesem Zusammenhang ist festzuhalten, daß bereits diese Minimalforderung bei den heute

eingesetzten Vorstufen von Systemen zum digitalen Einreichen von Patentanmeldungen nicht oder jedenfalls nur höchst unzureichend erfüllt ist. Die Verfahren von DEPAEASY und EPA-EASY setzen nämlich in wesentlichen Teilen auf proprietäre Datenformate von Herstellern von Textverarbeitungsprogrammen auf, die nicht oder nur unzureichend offengelegt sind. Beispielsweise erfordert der Gebrauch von DEPAEASY zwingend den Einsatz der von Microsoft erstellten und vermarkteten Textverarbeitungssoftware "WORD 6". Das originäre Datenformat, mit dem dieses Programm Dokumente als Bitfolgen darstellt, ist nie offengelegt worden. Demzufolge gibt es auch keine von Microsoft unabhängige Software, mit der der Erklärungsgehalt eines mit "WORD 6" erstellten Dokumentes dargestellt werden könnte. Da die Mächtigkeit des Dokumentenformates von "WORD 6" so weit geht, daß sogar Programme ("Makros") in das Dokument eingewoben werden können, die zum einen den Erklärungsgehalt völlig verdunkeln können und die zum anderen Störungen in der Datenverarbeitungsanlage des Amtes verursachen könnten ("Makroviren") haben sich die Verantwortlichen des DPAEASY-Projektes dazu entschlossen, die Übermittlung des Textes der Patentanmeldung auf der Grundlage eines zweiten proprietären Dokumentenformates von Microsoft, dem "**R**ich **T**ext **F**ormat" (RTF) vorzunehmen, welches keinerlei Makrofunktionalitäten unterstützt. Immerhin ist die Spezifikation dieses Dokumentenformates wenigstens im Prinzip veröffentlicht<sup>35</sup>; allerdings verfügt allein Microsoft über die Kontrolle über dieses Datenformat und behält sich vor, nach eigenen Erfordernissen die Spezifikation auch kurzfristig zu ändern<sup>36</sup>. Es er mangelt der RTF-Spezifikation also an der erforderlichen Persistenz, um als rechtlich bindende Norm zur Zuordnung von Bitfolgen zu Erklärungsinhalten angesehen zu werden. Außerdem erfolgt die Transformation des Anmeldungstextes aus dem WORD 6 - Format in das RTF und die Anzeige des RTF-Textes nur durch das einschlägige Programm der Firma Microsoft. Es ist bekannt, daß bei Verwendung unterschiedlicher Versionen für unterschiedliche Betriebssystemplattformen bei ein und derselben Textdatei unterschiedliche Anzeigen erhalten werden können.<sup>37</sup>

<sup>35</sup>Die RTF-Spezifikation kann aus einem kennwortgeschützten Bereich der Website der Firma Microsoft unter <http://www.microsoft.com> heruntergeladen werden, wenn und sofern ein Kennwort von Microsoft zugeteilt worden ist.

<sup>36</sup>In der Tat wird seitens Microsoft darauf geachtet, daß alle wesentlichen Dokumentendarstellungsoptionen im primären Word-Dokumentenformat auch über ein Abbild in der RTF-Spezifikation verfügen. Wenn eine neue Version von Word mit erweiterter Funktionalität erscheint, führt dies häufig zu einer entsprechenden Erweiterung der RTF-Spezifikation.

<sup>37</sup>Dirk Fox: "Zu einem prinzipiellen Problem digitaler Signaturen", DuD 22 (1998), Nr. 7, S. 386 bis 388. Fox bringt in seinem Beitrag ein Beispiel für einen Text, der

Im übrigen ist die RTF-Textdarstellung dazu bestimmt, eine bestimmte *äußerliche* Textformatierung zu beschreiben, etwa ein bestimmtes Layout oder die Verwendung bestimmter Schriftarten. Bei einer nicht auf die Papierform abstellenden Form von Telekooperation spielen aber gerade diese Parameter überhaupt keine Rolle mehr, d.h. beispielsweise legt das Patentamt das Layout der Offenlegungs- und Patentschriften nach eigenen Kriterien unabhängig von den Vorgaben des Anmelders fest. Bei der herkömmlichen Papiereinreichung ist die Festlegung des äußeren Erscheinungsbildes wichtig, da die Handhabbarkeit des Dokumentes im Amt unmittelbar davon abhängt<sup>38</sup>. Beim Übergang in die papierlose Telekooperation gilt es, sich von diesen überkommenen Vorstellungen zu lösen. Im Gegensatz zur Beschreibung des äußeren Erscheinungsbildes eines Textes durch Textverarbeitungsdateien ist die Beschreibung der inhaltlichen *Struktur* von Dokumenten erforderlich. Dasselbe Argument wendet sich in diesem Zusammenhang auch gegen den Einsatz anderer Layoutbeschreibungsmate wie das bekannte und weitverbreitete PDF-Format von Adobe.

Auch die EASY Version 2 Software greift auf proprietäre Datenformate namhafter Hersteller von Bürosoftware zurück. Im einzelnen können mit EASY Patentanmeldungen als RTF-Datei, als Microsoft Word 6.0 und als Corel Word Perfect 6.x-Datei verwendet werden<sup>39</sup>. Die hinsichtlich DEPAEASY dargelegten Aussagen gelten daher *mutatis mutandis* auch für EASY Version 2.0.

Nach alledem dürfte ersichtlich sein, daß ein Datenverarbeitungssystem zur rechtsverbindlichen Telekooperation nicht auf proprietären Dateiformaten bestimmter Hersteller von Bürosoftware aufbauen sollte. Die Versuchung, diesen Weg zu gehen, ist allerdings sehr groß, denn durch eine Festlegung auf eine begrenzte Auswahl von wenigen weitverbreiteten Softwaresystemen wird es leicht möglich sein, die Gegebenheiten einer überwältigenden Mehrheit von Unternehmen und Anwaltskanzleien abzudecken und dadurch eine hohe anfängliche Akzeptanz zu wecken. Ein bitteres Erwachen kann jedoch folgen, wenn es zum Streit um den wahren Erklärungsgehalt einer in Form einer Textdatei mit proprietärem Format abgegebenen Willenserklärung kommt.

Welche besseren Alternativen stehen zur Verfügung? Einerseits wäre es vorstellbar, sich an den EDIFACT-Normen zu orientieren, die sich in bestimmten Bereichen der Wirtschaft außerordentlich bewährt haben. Dazu ist aber anzumerken, daß die im Bereich des gewerblichen Rechts-

von der Word-Version für Windows-Rechner anders dargestellt wird als von einer Word-Version für einen Apple Macintosh.

<sup>38</sup>etwa Größe der Aktenordner, Eignung zum OCR-Einlesen des Inhaltes usw. usf.

<sup>39</sup>EASY Version 2 User Manual, EPA, September 1998, S. 133

schutzes elektronisch auszutauschenden Dokumente eine im Vergleich zu EDIFACT-Dokumenten komplexe Struktur aufweisen können. Zum anderen gilt das international festgelegte Procedere bei der Einführung neuer EDIFACT-Dokumente als sehr kompliziert und zeitraubend. Schließlich ist nicht absehbar, daß EDIFACT-gerechte Software kostengünstig und ohne Spezialpersonal beispielsweise in Anwaltskanzleien eingeführt werden könnte. Aus diesen Gründen entsteht der Eindruck, daß EDIFACT, obwohl prinzipiell geeignet, nicht das Mittel der Wahl darstellen dürfte.

Die im Rahmen des Systems des gewerblichen Rechtsschutzes auszutauschenden Willenserklärungen weisen — etwa im Gegensatz zu Willenserklärungen im Zusammenhang mit formalisierten Finanztransaktionen im Bankenbereich — die Besonderheit auf, zu einem großen Volumenanteil aus Folgen von Schriftzeichen zu bestehen, die einen in einer natürlichen Sprache niedergelegten komplexen Erklärungsgehalt verkörpern. Beispiele hierfür sind bei einer Patentanmeldung die Patentbeschreibung und die Patentansprüche. Diese komplexen natürlichsprachlichen Bestandteile entziehen sich als solche einer datenverarbeitungstechnischen Erfassung ihres Erklärungsgehaltes und richten sich ausschließlich an menschliche Rezipienten, d.h. keine Datenverarbeitungsanlage "verstehet" eine Patentbeschreibung oder einen Patentanspruch. Demgegenüber gibt es andere Angaben wie etwa eine Prioritätsbeanspruchung, deren Semantik ohne weiteres durch Datenverarbeitungsprogramme wenigstens teilweise erfaßt werden kann. Beispielsweise könnte bei einer Prioritätsbeanspruchung programmgesteuert ein Datenbankzugriff initiiert werden, um zu prüfen, ob eine Ersthinterlegung mit den vorliegenden Angaben überhaupt existiert. Daher macht es Sinn, die einzelnen Bestandteile eines digitalen Dokumentes, das eine Patentanmeldung darstellt, in einer zweckmäßigen Art und Weise so auszuzeichnen, daß ein Datenverarbeitungsprogramm sich bei der Verarbeitung von Einzelangaben in diesem Dokument auf eine Strukturbeschreibung stützen kann, die die einzelnen Bestandteile des Dokumentes maschinell voneinander unterscheidbar macht. Was benötigt wird, ist eine metasprachliche Ebene, auf der es möglich ist, daß der Ersteller eines komplexen digitalen Dokumentes dessen einzelne Teile jeweils als zu einem bestimmten Strukturelement gehörig auszeichnet. Derartige Techniken stehen in Gestalt der sogenannten Auszeichnungssprachen<sup>40</sup> seit einiger Zeit zur Verfügung und werden in Bereichen<sup>41</sup>, in denen komplexe digitale Dokumente mit hoher Zuverlässigkeit erstellt und gepflegt werden müssen, regelmäßig eingesetzt. Eine in diesem Bereich zentrale

<sup>40</sup>Gebräuchlicher ist der englische Ausdruck "Markup Languages"

<sup>41</sup>insbesondere das U.S.-Militär und die Flugzeugindustrie

Norm<sup>42</sup> schreibt die Spezifikation einer auch für den Bereich des gewerblichen Rechtsschutzes geeigneten universellen Auszeichnungssprache<sup>43</sup> SGML fest.

Der Gebrauch von SGML ist im Bereich des gewerblichen Rechtsschutzes für amtsinterne Zwecke seit langem bekannt; die WIPO verfügt über einen Standard ST.32<sup>44</sup> für eine SGML-DTD<sup>45</sup> zur Beschreibung von Patentdokumenten. Auch ist in den Vereinigten Staaten im Rahmen des aus öffentlichen Mitteln finanzierten Forschungsvorhabens DOCT<sup>46</sup> die Eignung von SGML als Auszeichnungssprache für Patentdokumente weiter eingehend untersucht worden<sup>47</sup>. Der 1997 von den Vereinigten Staaten der WIPO vorgeschlagene Generalplan<sup>48</sup> zur datenverarbeitungstechnischen Modernisierung des PCT-Verfahrens, der weitgehend akzeptiert worden ist und sich bereits in der Implementationsphase befindet, bezieht in seiner Beschreibung eines Konzeptes für eine "elektronische Patentakte" den auf SGML basierenden Standard ST.32 ausdrücklich ein. Es erscheint daher nicht abwegig, den Einsatz von SGML auch in Patentabteilungen und Anwaltskanzleien<sup>49</sup> zu bedenken. Dabei mag zunächst der hohe Preis von SGML-Autorenwerkzeugen abschrecken; dabei ist aber zu bedenken, daß aufgrund zunehmender Verbreitung von SGML und Untermengen<sup>50</sup> von SGML in anderen Bereichen mittlerweile Ergänzungen zu populären Textverarbeitungssystemen<sup>51</sup> zu moderaten Preisen auf den Markt kommen.

Eine weitsichtige Vorgehensweise bei der Ausgestaltung der elektronischen Einreichung von Patentanmeldungen im Rahmen weiterer zukünftiger Änderungen der Patentanmeldeverordnung sollte daher bei dem Standard ST.32 ansetzen

<sup>42</sup>ISO/IEC 8879:1986 - Deutsch als DIN EN 28879:1991 im Beuth Verlag, Berlin

<sup>43</sup>"Structured Generalized Markup Language" (SGML)

<sup>44</sup>WIPO Handbook on Industrial Property Information and Documentation. Ref.: Standards - ST.32 - Recommendation for the Markup of Patent Documents using SGML (Standard Generalized Markup Language), Seiten 3.32.0.1 bis 3.32.120

<sup>45</sup>Document Type Definition

<sup>46</sup>Distributed Object Computation Testbed (DOCT)

<sup>47</sup>Siehe insbesondere "Electronic File Wrapper Design Considerations with Input from the Distributed Object Computation Testbed (DOCT) Project", White Paper, <http://www.sdsc.edu/DOCT/Publications/efw/efw.html>

<sup>48</sup>Dokument WIPO ITIP/WG/I/3 vom 12.06.1997: "The Information Technologies Committee of the World Intellectual Property Organization" (Memorandum of the United States of America).

<sup>49</sup>Helmut Becker: "Aktuelle Trends in der EDV für Anwälte", BRAK-Mitt. 3/1998, S. 102 bis 104

<sup>50</sup>So sind die zur Beschreibung von Dokumenten im World Wide Web verwendeten Sprachen HTML und XML in der Tat nichts anderes als Untermengen von SGML

<sup>51</sup>So weist die Version 8 von Word Perfect (COREL) bereits einen SGML-Zusatz auf. Auch Microsoft bietet SGML-Zusätze für Word for Windows an.

und daraus eine Untermenge ableiten, die alle von Seiten des Anmelders oder Anwaltes einzureichenden Angaben umfaßt. Hierzu bedarf es einer engen Zusammenarbeit von Patentamt, Anmelderschaft und Patentanwälten.

#### 4.4. Verbindlichkeit

##### 4.4.1. Digitale Signaturen

Bei einer Telekooperationsbeziehung kann es vorkommen, daß sich ein daran beteiligter Partner Vorteile davon verspricht, die Abgabe eines eine Willenserklärung repräsentierenden digitalen Dokumentes wahrheitswidrig abzustreiten und statt dessen vorzutragen, es sei gar keine Erklärung oder eine solche anderen Inhaltes abgegeben worden. Eine rechtsverbindliche Telekooperation kann es daher nur dann geben, wenn technische Vorkehrungen getroffen werden, mit denen die Abläufe festlegbar sind, durch die das wahrheitswidrige Abstreiten von Willenserklärungen aufgedeckt werden kann. Das geeignete Mittel hierzu sind *digitale Signaturen*<sup>52</sup>. Mit ihrer Hilfe gelingt es, die *Authentizität*, d.h. die Zurechenbarkeit zu einer bestimmten Person, die *Integrität*, d.h. die Unverfälschtheit, und die *Nicht-Abstreitbarkeit* einer Willenserklärung sicherzustellen. Bei einer digitalen Signatur werden bestimmte kryptographische Algorithmen<sup>53</sup> verwendet, wobei derjenige, der für ein digitales Dokument eine dazu passende digitale Signatur generieren will, von einem nur ihm zur Verfügung stehenden Geheimnis — dem privaten *Signierschlüssel* — Gebrauch macht, um aus der Bitfolge des zu signierenden digitalen Dokumentes und aus dem Signierschlüssel unter Verwendung des kryptographischen Algorithmus eine weitere, die digitale Signatur darstellende Bitfolge zu ermitteln, die dem signierten digitalen Dokument beigefügt wird. Die Prüfung der Gültigkeit der digitalen Signatur durch Dritte beruht darauf, daß der Vorgang des Berechnens der Signatur mit einem dem Signierschlüssel mathematisch eindeutig zugeordneten komplementären *öffentlichen Schlüssel* auf der Grundlage desselben kryptographischen Algorithmus überprüft werden kann. Es ist mathematisch nicht möglich, aus dem öffentlichen Schlüssel den Signierschlüssel zu berechnen. Nur derjenige, der im Besitz des Signierschlüssels ist, kann die zu einem digitalen Dokument gehörende digitale Signatur erzeugen, aber die Veröffentlichung des zum Signierschlüssel komplementären öffentlichen Schlüssels ermöglicht es jedem Dritten, durch eine Art Umkehrung des Signiervorganges zu prüfen, ob die

<sup>52</sup>Zur Technik der digitalen Signatur siehe insbesondere Bruce Schneier: "Applied Cryptography", New York: John Wiley & Sons, Inc., 1. Aufl. 1994, S. 31 ff.

<sup>53</sup>Hier wird auf den Begriff der "digitalen Signatur" im Sinne des bundesdeutschen Signaturgesetzes abgestellt, der stets die Verwendung eines asymmetrischen Verschlüsselungsalgorithmus mit einem öffentlichen Schlüssel und einem privaten Schlüssel voraussetzt.

Signatur echt ist oder nicht.

Für einen praktischen Einsatzfall digitaler Signaturen könnte beispielsweise ein Anmelder dadurch im Alleinbesitz des Signierschlüssels sein, daß er — als einziger (!) — die Sachherrschaft über eine Diskette oder über eine Chipkarte ausübt, auf der bzw. in der die Bitfolge des Signierschlüssels abgespeichert ist. Der zu dem Signierschlüssel gehörende komplementäre öffentliche Schlüssel wird auf geeignete Weise<sup>54</sup> jedem interessierten Dritten zugänglich gemacht. Beim Signieren einer als digitales Dokument vorliegenden Patentanmeldung speist der Anmelder oder sein Vertreter *nach gehöriger Prüfung des digitalen Dokumentes und dem Willensentschluß, es nunmehr dem Patentamt verbindlich zu übermitteln*, den auf der Diskette beziehungsweise in der Chipkarte gespeicherten Signierschlüssel gemeinsam mit der digitalen Patentanmeldung einem kryptographischen Signierprogramm ein, um die digitale Signatur zu berechnen. Bevorzugterweise wird das Besitzmonopol hinsichtlich der Diskette oder der Chipkarte durch einen zusätzlichen Kennwortschutz ergänzt; bevor der geheime Signierschlüssel bereitgestellt wird, muß der Signierende die Signierkomponente durch Eingabe einer Paßphrase oder einer PIN freischalten. Die digitale Patentanmeldung wird dann zusammen mit der digitalen Signatur elektronisch an die Datenverarbeitungsanlage des Patentamtes übermittelt.

Das Patentamt kann nun mittels des allgemein zugänglichen öffentlichen Schlüssels ohne weiteres prüfen, ob die digitale Signatur einwandfrei ist. Ein positives Überprüfungsergebnis läßt zunächst den Schluß auf die *Integrität* zu, d.h. daß der Inhalt der als digitale Dokument eingereichten Patentanmeldung unverfälscht ist.

##### 4.4.2. Zertifizierungsstellen

In der Praxis ist dieser Befund jedoch nicht ausreichend, denn es kommt nicht nur darauf an, festzustellen, daß eine Einreichung unverfälscht ist, sondern auch, *wer* Einreicher ist. Ohne eine Prüfung der *Authentizität* einer Einreichung besteht die Gefahr, daß durch Dritte vom Berechtigten nicht autorisierte Verfahrenshandlungen mit schwerwiegenden Rechtsfolgen vorgenommen werden. Ihre rechtliche Qualität zum unabstreitbaren Sichern der Authentizität der Einreichung gewinnt die digitale Signatur jedoch erst dann, wenn im Patentamt keine Zweifel über die Zuordnung eines öffentlichen Schlüssels zu einer bestimmten Person bestehen. Dieses Ziel könnte im Prinzip am einfachsten dadurch erreicht werden, indem der Anmelder vor der Aufnahme der rechtsverbindlichen Telekooperation mit dem Amt persönlich dort erscheint, sich unter Vorlage seines Personalausweises legitimiert und eigenhändig einen Datenträger mit seinem persönli-

<sup>54</sup>beispielsweise über das Internet

chen öffentlichen Schlüssel dem Amt überreicht sowie im Gegenzug einen beglaubigten Datenträger mit dem öffentlichen Schlüssel des Patentamtes entgegennimmt. Die Beglaubigung des öffentlichen Schlüssels des Patentamtes ist von nicht zu unterschätzender Bedeutung. Technisch ist es nämlich durch sachkundige, aber rechtswidrige Eingriffe mit mehr oder weniger großem Aufwand stets möglich, das zur Datenübermittlung herangezogene Telekommunikationssystem derart zu manipulieren, daß der Einreicher den Eindruck hat, seine Einreichung an das Patentamt zu übermitteln, obwohl die Daten in Wirklichkeit von Dritten abgefangen werden. Daher müssen die von einem Patentamt als Empfangsbestätigung ausgestellten und an den Einreicher übermittelten digitalen Dokumente vom Patentamt mit einer digitalen Signatur versehen werden. Auch hierbei ist es erforderlich, daß die Zuordnung des entsprechenden öffentlichen Schlüssels zum Patentamt sicher verifizierbar ist: Aus der Sicht des Einreichers muß auch das Patentamt die Authentizität seiner Erklärungen wie etwa Empfangsbescheinigungen und Amtsbescheide, nachweisen<sup>55</sup>.

Freilich ist eine derartige Vorgehensweise in der Praxis absolut unpraktikabel; die Zuordnung von öffentlichem Schlüssel zu dessen Inhaber muß möglichst *dezentral* erfolgen können. Es bedarf somit einer Basis, um über geographische Entfernungen hinweg ein hinreichendes Vertrauen erwecken zu können, daß einerseits das Patentamt die Identität des Einreichers akzeptiert und andererseits der Einreicher genügend sicher ist, es am anderen Ende der Datenübertragungseinrichtungen tatsächlich mit dem Patentamt zu tun zu haben. Gleiches gilt, *mutatis mutandis*, für eine Telekooperationsbeziehung zwischen Anmelder und Anwalt oder unter Anwälten. Hierzu bedient man sich der *Zertifizierungsstellen*, die gegenüber allen beteiligten Telekooperationspartnern eine Vertrauensstellung genießen müssen, um die ihnen zugedachte Aufgabe erfüllen zu können. Eine Zertifizierungsstelle ist eine vertrauenswürdige Instanz, die die Zuordnung von öffentlichem Schlüssel und Schlüsselhaber mit hinreichender Zuverlässigkeit beglaubigt ("zertifiziert") und durch Ausgabe eines Zertifikates öffentlich verfügbar macht. Ein solches Zertifikat ist im Prinzip ein digitales Dokument, das diese Zuordnung aussagt und mittels des privaten Signierschlüssels der Zertifizierungsstelle mit einer digitalen Signatur versehen ist, die dann anhand des veröffentlichten zugehörigen öffentlichen Schlüssels von jedermann verifiziert werden kann. Die gewünschte Dezentralität kann durch eine formalisierte Übertragung von Vertrauen durch Verkettung von Vertrauensbeziehungen realisiert wer-

<sup>55</sup>Dieser Aspekt ist beispielsweise bei der Konstruktion der EC-Geldautomaten vernachlässigt worden. Daher ist es möglich, "gefälschte" EC-Geldautomaten aufzustellen, um ahnungslose Bankkunden zur Eingabe Ihrer PIN zu bewegen. Ein derartiger Fall ist z.B. 1997 in München vorgekommen.

den. Wenn beispielsweise einerseits eine erste Zertifizierungsstelle existiert, der zwar Vertrauen geschenkt wird, die aber die Zuordnung eines bestimmten öffentlichen Schlüssels zu dem Schlüsselhaber etwa wegen zu großer Entfernung zum Sitz des Inhabers nicht praktikabel beglaubigen kann, und andererseits eine zweite Zertifizierungsstelle in der Nähe des Schlüsselhabers besteht, über deren digitale Identität aber zunächst nichts bekannt ist, kann ein mehrstufiges Schlüsselzertifikat dadurch generiert werden, indem zunächst die zweite Zertifizierungsstelle die Zuordnung von öffentlichem Schlüssel und Inhaber zertifiziert und die erste Zertifizierungsstelle aufgrund eigener Sachverhaltskenntnis die Zuordnung des öffentlichen Schlüssels der zweiten Zertifizierungsstelle zu deren Rechtspersönlichkeit beglaubigt. Diese Verkettungen können einerseits benutzt werden, um ein *Netzwerk* von Zertifikaten<sup>56</sup> zu generieren; andererseits ist es aber auch möglich, eine Beschränkung auf eine *hierarchische Baumstruktur* von Zertifizierungsstellen herbeizuführen. Im letztgenannten Fall gibt es eine einzige Wurzelinstanz, die den öffentlichen Schlüssel von untergeordneten Zertifizierungsstellen erster Ordnung zertifiziert. Jede Zertifizierungsstelle erster Ordnung kann nun im Prinzip wiederum Schlüsselzertifikate für Zertifizierungsstellen zweiter Ordnung ausgeben u.s.w. u.s.f. Ein vernetztes System von Schlüsselzertifikaten eignet sich offensichtlich besser für informelle Gruppen von Telekooperationspartnern, bei denen jeder Teilnehmer potentiell auch Zertifizierungsstelle sein kann. Bei stärker regulierten und verrechtlichten Gruppen wird wegen der besseren Kontrollierbarkeit aufgrund einer klaren Zuordnung von Zertifizierungskompetenzen häufig auf das hierarchische Zertifizierungsmodell zurückgegriffen.

Eine Einführung digitaler Signaturen als Ersatz für die bisherige eigenhändige Unterschrift trifft mancherorts auf Bedenken. Es ist zu erwarten, daß auch in Kreisen der Anmelder und Anwälte im Bereich des gewerblichen Rechtsschutzes Vorbehalte bestehen. Eine wichtige Kritik geht davon aus, daß die Überprüfung einer digitalen Signatur nur beweisen könne, daß zum Zeitpunkt des Signierens der korrekte geheime Signierschlüssel verwendet worden sei, nicht aber, daß eine *bestimme* Person mit Erklärungsbewußtsein und Geschäftswillen gehandelt habe. Es könne vielmehr auch ein Fall von unechter Stellvertretung vorliegen, bei der der Zeichnungsberechtigte eine Signierchipkarte mit dem Signierschlüssel aus Bequemlichkeit oder vor einer längeren Abwesenheit einer Hilfsperson zum Gebrauch überlassen habe. Dieses Argument vermag aber nicht zu überzeugen, denn dieses Problem kann auch bei der eigenhändigen Unterschrift auftreten. Es

<sup>56</sup>zum "Web of Trust"-Zertifizierungsmodell von PGP siehe z.B. Simson Garfinkel: "PGP - Pretty Good Privacy", Sebastopol, USA: O'Reilly & Associates, Inc., 1995, S. 233-262

wäre weltfremd, abzustreiten, daß manche mit Unterschrift versehene Schriftstücke in Wirklichkeit durch Hilfspersonal auf blanko unterschriebenen Bögen per unechter Stellvertretung erzeugt worden sind. Es kommt vielmehr darauf an, daß der zeichnungsberechtigte Inhaber der Signierchipkarte die Verfügung über die Abgabe einer digitalen Signatur ganz und gar bei sich behalten kann, wenn er nur will. Begibt er sich leichtfertig der Sachherrschaft über die Chipkarte, muß er die rechtlichen Folgen ebenso tragen wie derjenige, der unterschriebene Blankobögen Dritten überläßt. Möglicherweise wird die Bindung der Signierchipkarte an den Inhaber zukünftig durch *biometrische Techniken* verbessert werden, d.h. die Freischaltung des in der Chipkarte abgelegten Signierschlüssels erfolgt dann nicht mehr durch Eingabe einer Geheimnummer (PIN), sondern durch Messung bestimmter Parameter (Fingerabdruck, Irisstruktur usw.) und Vergleich mit einem ebenfalls in der Chipkarte gespeicherten Bezugswert, der bei der Personalisierung der Signierchipkarte durch Messung beim rechtmäßigen Inhaber gewonnen wurde<sup>57</sup>. Der Mechanismus des Erzeugens der digitalen Signatur bleibt derselbe, lediglich die Freischaltung der Chipkarte erfolgt nach anderen Regeln. Die effektive Nicht-Abstreitbarkeit der durch eine digitale Signatur abgesicherten Willenserklärung steht und fällt mit der Beachtung dieser Zusammenhänge.

Die Integration von Verfahren zur digitalen Signatur bildet eine notwendige Voraussetzung für eine objektive begründbare Akzeptanzentwicklung für eine rechtsverbindliche elektronische Telekooperation in den westlichen Industrieländern, denn es ist nicht erkennbar, daß hier – wie offensichtlich in Japan – ein tradierte Zurückhaltung der Akteure bei Unstimmigkeiten im Zusammenhang mit dem Austausch digitaler Dokumente eine Prozeßflut verhindert. Wichtig ist, daß die betreffenden Zentralbehörden bei der Auswahl der zu verwendenden Verfahren und Geräte nicht hinter den technischen Möglichkeiten zurückbleiben, die die einschlägige Industrie derzeit schon bereithält.

#### 4.4.3. Konkrete Ansätze und mögliche Globalisierung

Das zum 1. August 1997 in Kraft getretene Signaturgesetz<sup>58</sup> (SigG) schafft in Deutschland die Grundlage für eine besonders privilegierte<sup>59</sup> Klasse von Zertifizierungsstellen, die im Rahmen einer flachen Hierarchie mit nur zwei Ebenen von einer staatlichen Wurzelinstanz zertifiziert werden. Es erscheint daher naheliegend, für den Geschäftsbereich des Deutschen Patentamtes die Zertifizierung der öffentlichen Schlüssel von Patentäm-

tern, Anmeldern und Patentanwälten den nach dem SigG evaluierten und genehmigten Stellen zu übertragen. Schon für das EPA stellt diese rein nationale Infrastruktur keine Lösung dar. Immerhin gibt es erkennbare Ansätze<sup>60</sup> auf der Ebene der EU, die Kriterien für die Zertifizierungsinfrastruktur zu harmonisieren<sup>61,62,63</sup>. Für den PCT wie auch für EPÜ-Länder, die wie die Schweiz kein Mitglied der EU bzw. des EWR sind, hilft auch dieser Ansatz nicht<sup>64</sup>. Es wäre daher durchaus sinnvoll, dieses Problem auf globaler Ebene anzugehen. Dabei steht einerseits die Entscheidung an, ob die Errichtung dieser Zertifizierungsinfrastruktur der Privatwirtschaft überlassen werden soll oder aber im Rahmen einer öffentlich-rechtlichen Körperschaft besser aufgehoben ist, und andererseits, ob ein Netzwerk von Zertifikaten oder eine hierarchische Struktur zu bevorzugen ist. Die von einigen Großbanken zur Gründung vorgesehene Zertifizierungsfirma *Global Trust* zeigt ein Beispiel für den privatwirtschaftlichen Weg auf<sup>65</sup>. Auch die DATEV e.G. bemüht sich offenbar, Zugang zum Zertifizierungsmarkt zu bekommen, besonders bei den rechtsberatenden Berufen.<sup>66</sup> Das Hauptproblem hierbei ist die Sicherstellung eines vorgegebenen Qualitätsstandards und die Garantie einer konsequenten Gleichbehandlung aller Kunden<sup>67</sup>. Die Errichtung einer globalen Zertifizierungsstelle für den gewerblichen Rechtsschutz könnte öffentlich-rechtlich unter dem Dach der WIPO<sup>68</sup> geschehen; möglicherweise bietet sich für eine Institutionali-

<sup>60</sup>Proposal for a European Parliament and Council Directive on a common framework for electronic signatures (98/C 325/04) COM(1998) 297 final - 09/0191(COD) in ABl. C 325 (1998), Seiten 5-11, inzwischen modifiziert durch Änderungen des EU-Parlamentes und des Rates. Der modifizierte Richtlinienentwurf stellt einen Kompromiß dar und unterscheidet "Zertifikate" im allgemeinen von "qualifizierten Zertifikaten" im Sinne des SigG.

<sup>61</sup>Zur Position der (vorherigen) Bundesregierung siehe: [http://www.kuner.com/data/sig/gov\\_ger\\_eu-draft.htm](http://www.kuner.com/data/sig/gov_ger_eu-draft.htm)

<sup>62</sup>Siehe dazu auch Klaus M. Brisch: "Gemeinsame Rahmenbedingungen für elektronische Signaturen - Richtlinienentwurf der Europäischen Kommission", CR Nr. 8/1998, S. 492 bis 499

<sup>63</sup>Dabei soll hier nicht – wie im Entwurf der EU-Richtlinie – einer Erweiterung des Konzeptes der stets auf asymmetrischer Kryptographie gegründeten *digitalen Signatur* auf eine technologisch völlig offene und beispielsweise auf rein biometrische Techniken abstellenden *elektronischen Signatur* das Wort geredet werden.

<sup>64</sup>Vgl. Anja Miedbrodt: "Regelungsansätze und -strukturen US-amerikanischer Signaturgesetzgebung"; DuD 22 (1998), S. 389 bis 394"

<sup>65</sup><http://www.certco.com/enterprise/press.htm>

<sup>66</sup>F.A.Z. vom 29.04.99, Seite 22: "Markt für Zertifizierungsstellen digitaler Signaturen formiert sich"

<sup>67</sup>Würde bestimmten Gruppen der Zugang zu Schlüsselzertifikaten durch höhere Preise oder auf andere Art und Weise erschwert, entstünden zwangsläufig Wettbewerbsverzerrungen auf dem Rechtsbesorgungsmarkt im Bereich des gewerblichen Rechtsschutzes.

<sup>68</sup>Ein derartiger Schritt wäre durch Art. 4 des Übereinkommens zur Errichtung der Weltorganisation für geistiges Eigentum abgedeckt.

<sup>57</sup>siehe dazu z.B. O. Fries: "Biometrische Verfahren"; in: O. Fries et al. [Hg.]: "Sicherheitsmechanismen", München: Oldenbourg, 1993, S. 49 bis 56

<sup>58</sup>BGBI. I 1997, Nr. 52, S. 1870 bis 1880

<sup>59</sup>Alexander Roßnagel: "Die Sicherheitsvermutung des Signaturgesetzes", NJW, Nr. 45 (1998), S. 3312 bis 3320

sierung das Internationale Büro in Genf an. Das Problem hierbei ist jedoch die erforderliche Unabhängigkeit gegenüber der WIPO, denn die Zertifikate müssen gegebenenfalls in Rechtsstreitigkeiten auch gegen das Vorbringen von Dienststellen der WIPO eingebracht werden können. Hinsichtlich der Strukturfrage scheinen die Argumente zugunsten der hierarchischen Struktur zu überwiegen, da sowohl die Anmelder als auch die Anwälte unter sich jeweils als Wettbewerber auftreten und schon deshalb eine hinreichend kooperative Gruppe gleichgestellter Telekooperationspartner nicht werden bilden können. Es bleibt daher wohl bei einem hierarchischen Ansatz, wobei sich die Frage stellt, wo die Wurzelinstanz organisatorisch anzusiedeln wäre.

Die technische Arbeit der Identitätsprüfung und des Ausstellens der Zertifikate sollte dezentral<sup>69</sup> erfolgen; die öffentlichen Schlüssel der dezentralen Zertifizierungsstellen sollten durch Zertifikate der "Root Certification Authority" beglaubigt werden. Für Deutschland wäre es vorstellbar, den öffentlichen Schlüssel der als Wurzelinstanz für die unter dem SigG arbeitenden Zertifizierungsstellen arbeitenden Regierungsbehörde<sup>70</sup> durch die globale Zertifizierungsinstanz für den gewerblichen Rechtsschutz zu zertifizieren, so daß die hier bereits im Aufbau befindliche Infrastruktur nahtlos mitbenutzt werden kann. Auf diese Weise könnte für den Bereich des gewerblichen Rechtsschutzes eine weltumspannende Hierarchie von Zertifizierungsinstanzen geschaffen werden, die nicht nur der Identifizierung der Anmelder und Anwälte den Ämtern gegenüber verwendbar ist, sondern die selbstverständlich auch gleichermaßen für eine weltweite rechtsverbindliche Telekooperation zwischen Anmeldern und Anwaltskanzleien bzw. der Anwaltskanzleien untereinander eingesetzt werden kann.

#### 4.4.4. Zur Beweiskraft digitaler Signaturen

Der technisch inspirierte Begriff der Nicht-Abstreitbarkeit einer digitalen Signatur ist streng zu trennen von den Regeln des Beweisrechtes, denen die Verwertung einer digitalen Signatur im Prozeß unterfällt. Da die diesbezügliche Entwicklung international noch sehr im Fluß ist, sollen im folgenden lediglich einige Hinweise auf die Rechtslage in Deutschland gegeben werden. Digital signierte Daten sind keine Urkunden im Sinne des Urkundsbeweises nach §§ 415ff. ZPO, denn die dem Urkundenbeweis zugrundeliegenden Beweisvermutungen basieren auf dem Umstand, daß Urkunden Gedankenerklärungen verkörpern und aus sich heraus verständlich sind. Digitale Dokumente sind aber weder verkörpert noch aus sich heraus, sondern nur mit Hilfe technischer

Geräte und Programme verständlich<sup>71</sup>. Dessen ungeachtet können digitale Signaturen in Form des Augenscheinsbeweises nach §§ 371ff. ZPO oder des Sachverständigenbeweises nach §§ 402 ff. ZPO als Beweis für Willenserklärungen in den Prozeß eingebracht werden. Nach § 1 SigG gelten nach diesem Gesetz zustandegekommene digitale Signaturen als sicher, solange der Vermutungstatbestand nicht qualifiziert bestritten wird.

#### 4.5. Vertraulichkeit

Die Vertraulichkeit von digitalen Dokumenten, die auf öffentlichen Telekommunikationsleitungen ausgetauscht werden, ist auf zwei Ebenen gefährdet: Zum einen können beliebige Dritte versuchen, durch rechtswidrige technische Manipulationen<sup>72</sup> in den Besitz einer Kopie des übermittelten digitalen Dokumentes zu gelangen. Besonders bei der Benutzung des Internet sind die technischen Hürden gegen ein unbefugtes Kopieren von Datenströmen faktisch überaus niedrig anzusetzen. Andererseits verdichten sich die Anzeichen, daß Geheimdienste der USA und anderer Staaten sich mit mehr oder weniger expliziter Legitimation durch den zuständigen Gesetzgeber in erheblichem Umfang damit befassen, Telekommunikationseinrichtungen im jeweiligen Ausland zu Zwecken der Wirtschaftsspionage umfassend zu überwachen<sup>73</sup>. Diese Zugriffe durch finanziell überaus gutgestellte Organisationen betreffen nicht nur das als notorisch unsicher geltende Internet, sondern alle Arten öffentlicher Telekommunikationsverbindungen einschließlich Sprache und Telefax, also insbesondere auch geschlossene Telekommunikationsnetzwerke, sofern diese auf öffentlicher Telekommunikationsinfrastruktur aufsetzen. Es versteht sich, daß noch nicht offengelegte Patentanmeldungen ein besonders attraktives Ziel für die Wirtschaftsspionage sein können. Aber auch andere Dokumente, beispielsweise im Zusammenhang mit hochrangigen Verletzungsstreitigkeiten, deren Ausgang von politischer Signifikanz sein kann, könnten in das Visier entsprechender Zugriffe gelangen. Wenn eine der beteiligten Streitparteien durch den Geheimdienst des Sitzlandes ein besonderes "Briefing" über die Strategie der Ge-

<sup>71</sup>Roßnagel a.a.O., S. 3314

<sup>72</sup>Manfred Fink: "Lauschziel Wirtschaft - Abhörgefahren und -techniken / Vorbeugung und Abwehr", Stuttgart: Richard Boorberg Verlag, 1996

<sup>73</sup>zum sog. ECHELON-System siehe u.a.:

Ingo Ruhmann, Christiane Schulzki-Haddouti: "Abhör-Dschungel - Geheimdienste lesen ungeniert mit" in c't Nr. 5 (1988), S. 82 bis 93;

<http://www.europarl.eu.int/dg4/stoa/en/publi/166499/execsum.htm>, die Debatte am 14. September 1998 im Europäischen Parlament (vgl. ABl. EU Nr. C-313 vom 12.10.1998, S. 14 und S. 53) sowie der STOA-Arbeitsbericht PE 168.184 "Development of Surveillance Technology and Risk of Abuse of Economic Information" vom April 1999 unter [http://www.gn.apc.org/duncan/interception\\_capabilities\\_2000.htm](http://www.gn.apc.org/duncan/interception_capabilities_2000.htm)

<sup>69</sup>beispielsweise bei den Zentralbehörden für den gewerblichen Rechtsschutz oder bei vertrauenswürdigen Privatfirmen, die diese Aufgabe übernehmen.

<sup>70</sup>Regierungsbehörde Telekommunikation und Post (RegTP) mit Sitz in Mainz

genseite bei Vergleichsverhandlungen erhalte, könnte dies die Symmetrie des Verfahrens empfindlich stören.

Die Sicherung der Vertraulichkeit bei der Übermittlung digitaler Dokumente kann daher allein schon wegen des Zugriffes der Geheimdienstapparate faktisch nicht bei der Verhinderung des Zugriffes Dritter auf die übertragenen Dokumente ansetzen. Statt zu verhindern, daß Dritte in den Besitz von Kopien übermittelter digitaler Dokumente gelangen, muß durch *Verschlüsselung* ihrer Inhalte dafür gesorgt werden, daß eine unbefugte Nutzung der darin übertragenen Information praktisch ausgeschlossen ist. Dabei wird der originale *Klartext* des digitalen Dokumentes unter Verwendung eines kryptographischen Algorithmus und eines Parameters, des öffentlichen Schlüssels, in ein unverständliches *Chiffrat* transformiert. Der Klartext kann aus dem Chiffrat unter Verwendung des kryptographischen Algorithmus und eines geheimgehaltenen privaten Schlüssels wieder zurückgewonnen werden. Der private Schlüssel hängt mit dem öffentlichen Schlüssel mathematisch eindeutig zusammen, kann aber nicht durch Berechnung aus diesem abgeleitet werden.

Bei der Konzeption von hinreichend sicheren Verschlüsselungssystemen sind zwei zentrale Gesichtspunkte zu beachten. Erstens können Verschlüsselungsalgorithmen an sich mangelhaft konstruiert sein und einem fachlich überlegenen Kryptologen Ansätze bieten, durch relativ kurze Rechenprozesse das Verfahren zu brechen. Es ist leicht, einen Algorithmus festzulegen, der dem ersten Anschein nach den Klartext eines digitalen Dokumentes derart verwirft, daß selbst dessen Autor keinen Weg weiß, ihn zu brechen. Erfahrene Kryptologen kennen jedoch Verfahren, mit denen sich viele derartige Algorithmen ohne weiteres aushebeln lassen. Sehr schwer ist es dagegen, einen Algorithmus zu finden, der auch nach Jahren intensiver Analyse durch erfahrene Kryptologen nicht verwundbar ist. Aus diesem Grunde ist die öffentliche Analyse von Kryptoalgorithmen durch die nicht an Geheimhaltungsverpflichtungen gebundene Fachöffentlichkeit an den Universitäten und Firmen ein wichtiger Eckpfeiler für die Sicherheit von Produkten zur Datenverschlüsselung. Hersteller, die sich weigern, den in ihren Produkten verwendeten Verschlüsselungsalgorithmus offenzulegen und damit der kritischen Fachöffentlichkeit zugänglich zu machen, arbeiten unseriös und sind abzulehnen. *Die Sicherheit ernstzunehmender Verschlüsselungstechnik hängt stets ausschließlich an der Geheimhaltung des Schlüssels, nie an der Geheimhaltung des Algorithmus*<sup>74,75</sup>.

Jedoch nützt auch ein an sich brauchbarer Verschlüsselungsalgorithmus nichts, wenn die theo-

retisch mögliche maximale Zahl der durch ihn verarbeitbaren Schlüssel zu gering ist, da dann ein enumeratives Ausprobieren aller möglichen Schlüssel stets zum Auffinden des Klartextes führt. Offensichtlich hängt die erforderliche Mindestanzahl verschiedener Schlüssel von der Geschwindigkeit ab, mit der der Algorithmus ausgeführt werden kann. Je weiter die Rechnertechnik fortgeschritten ist, desto mehr Schlüssel können pro Zeiteinheit ausprobiert werden. Da die kryptographischen Schlüssel durch Bitfolgen dargestellt werden, ist die Anzahl  $n$  der Bits, die den Schlüssel ausmachen, ein Maß für die Anzahl überhaupt möglicher Schlüssel  $Z$ ;

$$Z = 2^n$$

Die Schlüssellänge erlaubt jedoch stets nur im Zusammenhang mit der Angabe des jeweiligen Algorithmus eine Beurteilung der Sicherheit. Damit ein Algorithmus bei einer bestimmten Schlüssellänge als praktisch sicher gelten kann, muß die unter Zugrundelegung der am weitesten entwickelten Rechnertechnik abgeschätzte Zeitdauer zum enumerativen Absuchen der überhaupt möglichen Schlüssel den Zeitraum, innerhalb dessen das verschlüsselte Geheimnis überhaupt interessant ist, um sehr viele Größenordnungen übersteigen. So gelten derzeit der sog. IDEA-Algorithmus<sup>76</sup> mit 128 Bit Schlüssellänge oder der RSA-Algorithmus<sup>77</sup> bei 2048 Bit Schlüssellänge noch als ausreichend sicher. Demgegenüber ist unlängst gezeigt worden, daß der DES-Algorithmus<sup>78</sup> mit 56 Bit effektiver Schlüssellänge bei der heute zur Verfügung stehenden Rechnerleistung ohne weiteres durch enumeratives Ausprobieren aller möglichen Schlüssel gebrochen werden kann<sup>79</sup>.

Die Gelegenheit zur Beobachtung der Kommunikation nichtstaatlicher Stellen durch besonders beauftragte Behörden wird traditionell als Ausfluß der staatlichen Souveränität begriffen. Da starke Kryptographie auf der Grundlage guter Algorithmen und bei Verwendung ausreichend langer Schlüssel auch den Zugriff staatlicher Stellen auf die Inhalte privater Telekommunikation wirksam vereitelt, ist eine politische Debatte über die Legitimität des Einsatzes von solchen kryptographischen Techniken außerhalb staatlicher Stellen entstanden<sup>80,81</sup>. Es gibt daher Ansät-

<sup>76</sup>Schneier a.a.O., S. 260 bis 266

<sup>77</sup>Schneier a.a.O. S. 281 bis 288

<sup>78</sup>Schneier a.a.O. S. 219 bis 243

<sup>79</sup>Siehe Electronic Frontier Foundation: "Cracking DES" <http://www.jya.com/cracking-des.htm>

<sup>80</sup>Conor Ward: "Governmental Policies on Encryption", CTRLR Nr. 5 (1996), S. 171-173 m.w.N.

F.A.Z. Nr. 58 (1998) vom 10.03.1998 - Standpunkte: Siegmund Mosdorf

F.A.Z. Nr. 69 (1998) vom 23.03.1998, S. 28 - "Verschlüsselung soll den elektronischen Handel beflügeln"

<sup>74</sup>sog. "Kerckhoffsches Prinzip"

<sup>75</sup>siehe dazu auch "Snake Oil FAQ 1.0" unter <http://www.njh.com/latest/9609/960927-03.html>

ze, die außerhalb staatlicher Stellen zum Gebrauch zugelassene Schlüssellänge derart zu beschränken, daß besonders gut ausgestattete staatliche Agenturen mit speziellen Rechnerkonstruktionen in der Lage sind, durch enumeratives Ausprobieren aller möglichen Schlüssel binnen kürzester Zeit Zugriff auf die Inhalte zu erhalten. Andere Forderungen beinhalten eine Hinterlegungspflicht für Schlüssel bei staatlichen Stellen. Es gilt, hier zwei Fallkonstellationen zu unterscheiden. Im Hinblick auf den Austausch von digitalen Dokumenten mit den Patent- und Markenämtern ist festzuhalten, daß der Empfänger oder Absender sensibler digitaler Dokumente in aller Regel zunächst eine *Zentralbehörde* ist, die mit den Sicherheitsbehörden in jeder erforderlichen Weise zusammenarbeitet. Eine mutwillige Schwächung der bei der Einlieferung an die Patentämter zugelassenen Verschlüsselungssysteme durch willkürliche Beschränkungen der Schlüssellänge oder durch Schlüsselhinterlegungspflichten ist daher widersinnig und nützt nur der von Drittstaaten möglicherweise ausgehenden Wirtschaftsspionage. Von dieser Konstellation zu unterscheiden ist der Austausch von digitalen Dokumenten zwischen Anwaltskanzleien, die an ihre Berufsverschwiegenheit gebunden sind. Ein sehr häufiger Fall wird die Übermittlung von digitalen Dokumenten über Staatsgrenzen hinweg sein, da im Regelfall im Bereich jeder Jurisdiktion ein dort zugelassener Kollege mit der Vertretung beauftragt werden muß. Es ist nicht erkennbar, wie Verschlüsselungssysteme in praktikabler Weise technisch zu gestalten sind, die den reibungslosen Zugriff auf die verschlüsselt übertragenen Inhalte nur derjenigen Behörden gestatten, die zu der Jurisdiktion einer der beiden Kommunikationspartner gehören. Im Endeffekt würde eine pauschale Schwächung der Verschlüsselungsverfahren beispielsweise durch eine Begrenzung der höchstzulässigen Schlüssellänge wiederum nur die Wirtschaftsspionage befördern. Auch der Zwang zur Hinterlegung geheimer Schlüssel bei bestimmten staatlichen privatrechtlich verfaßten Stellen birgt nicht beherrschbare Risiken<sup>82</sup>. Man

---

DER SPIEGEL Nr. 12 (1997) S. 80 - "Schlüssel für den Staat - Zum Schutz vor Datenklau sollen elektronische Nachrichten codiert werden aber Polizei und Geheimdienste wollen mitlesen"

COMPUTERWOCHE Nr. 14 (1997) S. 9 bis 12 - "Siegen die liberalen Kräfte im Streit ums Kryptogesetz?"

COMPUTERWOCHE Nr. 15 (1997) S. 20 - Cristoph Ruland: "Kryptoregulierung : Eine Bedrohung für die Bürger und die Wirtschaft - Regierung umgeht Datenschutz: Orwell durch die Hintertür?"

<sup>81</sup>Simson Garfinkel: "PGP - Pretty Good Privacy", Sebastopol, CA, USA: O'Reilly & Associates, 1995, Kapitel 5: "Privacy and Public Policy", S. 117 bis 134

<sup>82</sup>Hal Abelson et al: "The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption"  
[http://www.crypto.com/key\\_study/report.shtml](http://www.crypto.com/key_study/report.shtml)  
<http://www.cdt.org/crypto/risks98/>

darf also gespannt sein, wie sich die einzelnen Patentämter zukünftig in der politisch verminten Schlangengrube der Kryptographiepolitik verhalten werden, d.h. ob sie die ureigensten Interessen ihrer Anmelderschaft oder übergeordnete, von außen auferlegte politische Zwänge zur Maxime ihres Handelns erwählen werden.

Die im Zusammenhang mit der digitalen Signatur eingeführte Zertifikationsinfrastruktur wird auch bei der Verschlüsselung der über unsichere Kanäle zu übermittelnden digitalen Dokumente benötigt. Im Prinzip bedient man sich bevorzugterweise ebenfalls asymmetrischer Verschlüsselungsalgorithmen mit einem der Allgemeinheit, mindestens aber allen potentiellen Absendern, zugänglich gemachten *öffentlichen Schlüssel*, mit dem der Klartext eines digitalen Dokumentes verschlüsselt wird, um ein Chifftrat zu erhalten, sowie mit einem streng geheimgehaltenen *privaten Schlüssel*, den nur der Empfänger besitzt und mit dem aus dem Chifftrat der Klartext zurückgewonnen wird. Ohne die Assistenz der Zertifizierungsinfrastruktur wären dann Angriffszenarien denkbar, bei denen einem Absender eines vertraulichen digitalen Dokumentes ein nicht zu dem intendierten Empfänger gehörender öffentlicher Schlüssel untergeschoben wird, dessen zugehöriger privater Schlüssel folgerichtig nicht in den Händen des zgedachten Empfängers, sondern eines Dritten liegt, der dann in den Besitz des Klartextes des vertraulichen digitalen Dokumentes gelangen könnte, sofern er Kenntnis von dem Chifftrat erlangt hat. Bei der Verwendung asymmetrischer Kryptographie zur Nachrichtenverschlüsselung gehört es daher zu den gewöhnlichen Sorgfaltspflichten aller Absender von vertraulichen Nachrichten, sich vor dem Verschlüsselungsvorgang auf geeignete Weise davon zu überzeugen, daß der vorliegende öffentliche Schlüssel des intendierten Empfängers authentisch ist. Dies kann — bevorzugterweise automatisiert — dadurch geschehen, indem zum Verschlüsseln mittels einer Prüfroutine nur solche öffentlichen Schlüssel zugelassen werden, deren Authentizität durch ein Zertifikat einer vertrauenswürdigen Zertifizierungsstelle beglaubigt ist.

## 5. Der Versagensfall

Wie alle technischen Systeme können auch Einrichtungen zur rechtsverbindlichen Telekooperation versagen. In einem solchen Versagensfall stellen sich insbesondere drei Fragen: (a) Wie ist ein Versagensfall objektiv erkennbar und von anderen Störungen im Zuge des Erstellens oder der Übermittlung einer Willenserklärung abgrenzbar; (b) wie kann das Reparaturinstrument der Wiedereinsetzung in versäumte Fristen eingesetzt

---

[http://www.crypto.com/key\\_study/](http://www.crypto.com/key_study/)

werden, und (c) wie ist mit Haftungsfragen umzugehen.

Ein typischer Störfallsachverhalt ist beispielsweise dann gegeben, wenn ein Einreicher vorträgt, eine bestimmte Patentanmeldung zu einem bestimmten Zeitpunkt elektronisch eingereicht zu haben, dies auf der Empfängerseite vom Patentamt jedoch bestritten wird. Einerseits kann es sich um eine technische Störung in einem überaus komplexen System handeln, die den Zugang einer tatsächlich abgegebenen Erklärung vereitelt hat; andererseits ist nicht ausgeschlossen, daß tatsächlich überhaupt keine Patentanmeldung eingereicht worden ist und daß das Vorbringen auf der (vermeintlichen) Absenderseite nur eine Schutzbehauptung darstellt. Bei der Zuweisung von Beweislasten ist hier die konzeptionelle Asymmetrie bei der Errichtung des technischen Gesamtsystems zu berücksichtigen. Die technische Ausgestaltung wird nämlich de facto fast ganz ausschließlich von der Seite der Zentralbehörden des gewerblichen Rechtsschutzes festgelegt, und der einzelne Anmelder oder Anwalt wird auf die vorgegebene Interaktionsschnittstelle verwiesen. Es wäre unbillig, wenn bei der anstehenden Ausgestaltung von Ausführungsbestimmungen für die Telekooperation mit Zentralbehörden des gewerblichen Rechtsschutzes Regelungen getroffen würden, nach denen der Anmelder oder sein Vertreter de facto Risiken tragen muß, deren Vermeidung ganz überwiegend oder sogar ausschließlich in der Sphäre des Amtes betrieben werden kann und muß. Andererseits ist es auch der Rechtssicherheit insgesamt nicht förderlich, wenn das Amt über keinerlei Instrumente verfügt, um seine tatsächlichen Feststellungen über den Zugang oder Nicht-Zugang bestimmter Willenserklärungen bei Auseinandersetzungen verteidigen zu können. Der erste Ansatz zur Überwindung dieses Problemes ist die förmliche *Evaluierung* des Gesamtsystems aller Einrichtungen zur Telekooperation, die zwischen Amt und Anmeldern bzw. deren Vertretern eingesetzt werden. Das SigG und die sich auf § 16 SigG gründende Signaturverordnung<sup>83</sup> - SigV - zeigen exemplarisch, wie eine Prüfungspflicht für komplexe, im Rechtsleben relevante Systeme der Informationstechnik gesetzlich gestaltet werden kann. § 17 (1) SigV legt beispielsweise fest, daß die Prüfung der technischen Komponenten im Zusammenhang mit unter das SigG fallenden digitalen Signaturen nach den "Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik"<sup>84</sup> zu erfolgen hat. Es erscheint sinnvoll, vor der Einführung von Optionen zur rechtsverbindlichen Telekooperation hinsichtlich der hierfür bei dem Deutschen Patent- und Mar-

kenamt und den Anmeldern beziehungsweise deren Vertretern zum Einsatz gelangenden Datenverarbeitungsanlagen - soweit diese für den Vollzug der rechtsverbindlichen Telekooperation wesentlich sind - einer ähnliche förmlichen Prüfung zu unterziehen, wobei für den durch die Prüfung festzustellenden Mindeststandard vorab sinnvolle Prüfstufen festzulegen sind<sup>85</sup>. Abweichend von den Festlegungen des SigG sollte im Bereich des gewerblichen Rechtsschutzes daran gedacht werden, den Beteiligten eine Pflicht zur Veröffentlichung des Prüfberichtes aufzuerlegen, so daß die Zertifikation sowohl der amtsseitig installierten Einrichtungen als auch der bei den Anmeldern und in den Kanzleien zum Einsatz gelangenden Geräte für die (Fach-)Öffentlichkeit nachvollziehbar wird. Dies erleichtert die notwendige öffentliche Erörterung des Sicherheitsstandards der verwendeten technischen Systeme. Bei einer vor Gericht ausgetragenen Auseinandersetzung zwischen Anmelder und Patentamt über einen Störfall im Zusammenhang mit den informationstechnischen Systemen zur Telekooperation kann dann der strittige technische Kausalablauf anhand des Sachvortrages beider Seiten auf der Grundlage der dem Prüfbericht zu entnehmenden Angaben gegebenenfalls auch unter Hinzuziehung von Sachverständigen erörtert und schließlich geklärt werden.

Die Betrachtung der Risiken darf jedoch nicht bei einem Szenario stehenbleiben, bei dem eine abgegebene Willenserklärung ihren Empfänger nicht erreicht. Auch der komplementäre Fall, bei dem trotz zweckmäßiger Einrichtung der Softwarekomponenten eine Willenserklärung abgesandt worden ist, die entweder überhaupt nicht oder zumindest nicht mit ihrem tatsächlichen Erklärungsinhalt hätte übertragen werden sollen, sollte betrachtet werden. Es erscheint unbillig, die Risiken einer Fehlbedienung einseitig den Anmeldern und deren Vertretern aufzubürden. Die herkömmlichen Instrumente zur Anfechtung irrtümlich abgegebener Willenserklärungen sollten durch eine zusätzliche gesetzliche Regelung für den Geschäftskreis des Deutschen Patent- und Markenamtes ergänzt werden, die beispielsweise vorsehen könnte, daß eine elektronisch übertragene Willenserklärung bis zum Ablauf eines Tages nach ihrer Übermittlung auf herkömmliche Weise, also schriftlich, ohne Angabe von Gründen widerrufen werden kann. Diese Regelung würde gegenüber dem Amt und der Öffentlichkeit für maximal 48 Stunden eine Rechtsunsicherheit hinsichtlich

<sup>83</sup>BGBl. I 1997, Nr. 70, S. 2498 bis 2502

<sup>84</sup>GMBL. 1992, S. 545ff.

<sup>85</sup>Damit sei keinesfalls gesagt, daß die von den Einrichtungen zur Telekooperation im Rahmen des gewerblichen Rechtsschutzes zu erreichenden Prüfstufen mit denen des § 17 SigV identisch sein müssen. Es ist zu erwarten, daß hier an manchen Stellen Abstriche vorgenommen werden können.

der abgegebenen Erklärungen nach sich ziehen. Dies erscheint hinnehmbar, zumal sich im Bereich des gewerblichen Rechtsschutzes einfach zu handhabende Reparaturmechanismen für Verfahrensmängel wie etwa das Instrument der Weiterbehandlung nach Art. 121 EPÜ trotz wesentlich länger andauernder Unsicherheit über den Verfahrensstand insgesamt hervorragend bewährt haben. Um Mißbrauch der vorgeschlagenen Widerrufsregelung einzuschränken, kann an eine zu entrichtende Amtsgebühr in der Größenordnung der Weiterbehandlungsgebühr des EPÜ gedacht werden.

Wird die Übermittlung einer fehlerhaften Willenserklärung erst nach Fristablauf erkannt, nützt auch die Widerrufsregelung nichts. In diesem Fall stellt sich die Frage nach der Möglichkeit der Wiedereinsetzung in die versäumte Frist oder sogar - wenn ein Vertreter eingeschaltet war - nach haftungsrechtlichen Ansprüchen. Beide Fragen stehen über den Verschuldensbegriff in engem Zusammenhang mit den dem Anmelder oder dessen Vertreter aufzubürenden *Sorgfaltspflichten*. Hier gilt es, eine Inflation überspannter Anforderungen an Anmelder und Anwälte abzuwehren. Die vorstehend unter dem Gesichtspunkt der objektiven Sachverhaltsklärung vorgeschlagene Evaluierungspflicht der für Zwecke der rechtsverbindlichen Telekooperation eingesetzten Datenverarbeitungseinrichtungen kann auch in diesem Zusammenhang hilfreich sein, indem eine (widerlegbare) gesetzliche (*prima facie*-)Vermutung eingeführt wird, die Anmelder und Vertreter bei bestimmungsgemäßem Gebrauch evaluierter DV-Komponenten von Folgen interner Störungen dieser Komponenten exkulpiert, es sei denn, es hätte aufgrund erkennbarer objektiver Anzeichen Anlaß bestanden, an der Einsatzbereitschaft dieser Komponenten zu zweifeln.

## 6. Schlußfolgerungen

Zahlreiche Patentabteilungen und Anwaltskanzleien sind hinsichtlich ihrer DV-Infrastruktur denkbar schlecht für die Einführung einer rechtsverbindlichen Telekooperation vorbereitet. Das primäre und im Büroalltag verbindliche Datenspeichermedium ist die Papierakte. Korrekte und zeitnah gepflegte Abbilder der in der Papierakte niedergelegten Daten in einer DV-Anlage werden oft nur insoweit geführt, als dies durch DV-gestützte Teile des Geschäftsprozesses erzwungen wird. Datenfelder, die zwar in der Bürosoftware vorgesehen sind, deren Inhalt jedoch an keiner Stelle entscheidend in den Geschäftsprozeß einfließt, werden erst gar nicht erfaßt oder aber nach einer gewohnheitsmäßigen Ersterfassung nie wieder aktualisiert. Der Geschäftsprozeß aber orientiert sich grundsätzlich an der Papierakte. Da die Wechselwirkung mit der Außenwelt durch

Austausch papierener Dokumente stattfindet, kann die Papierakte den tatsächlichen Status einer Angelegenheit widerspiegeln. Bei einer verbindlichen Beauskunftung wird daher stets die Papierakte, nicht die von ihr abgeleitete Schutzrechtsdatenbank herangezogen. Der Übergang zur Telekooperation erzwingt hier einen Wandel. Da die Interaktion mit der Außenwelt dann durch die DV-Anlage vermittelt wird, beinhaltet die Datenbank automatisch den korrekten Zustand einer Angelegenheit; eventuell erstellte Papierausdrucke sind demgegenüber sekundär. Die Sorgfalt, die bislang der Papierakte und der Aktenregistratur galt, muß sich nun der DV-Infrastruktur zuwenden.

Dadurch stehen Patentabteilungen und Anwaltskanzleien vor DV-Sicherheits- und Verfügbarkeitsproblemen, die für diese Kreise zuvor weitgehend unbekannt waren. Andere Zweige der Wirtschaft, beispielsweise die Banken und Versicherungen, haben diesen Anpassungsprozeß vor Jahrzehnten abgeschlossen und verfügen heute über einen breiten Erfahrungsschatz im Umgang mit unternehmenskritischen DV-Anwendungen. Diese Lernprozesse stehen im Bereich des gewerblichen Rechtsschutzes erst noch bevor. Die Anbieter von Software für Kanzleien und Patentabteilungen treffen bislang noch nicht auf einen Markt, der diese Anforderungen ernstlich stellt. Die von ihnen angebotenen Lösungen bieten wenig mehr als bloßen Paßwortschutz. Ausgefeilte Sicherheitskonzepte gegen Angriffe auf die DV-Infrastruktur von innen oder außen sind nicht verfügbar.

Die im Rahmen wirksamer Sicherheitskonzepte unerläßliche Kryptographietechnik hat weder auf der Seite der Ämter noch bei den Anmeldern oder ihren Vertretern bislang nennenswert Einzug gehalten. Für ihren Erfolg ist zunächst die Errichtung einer Infrastruktur für die Verwaltung und Zertifizierung der öffentlichen Schlüssel erforderlich<sup>86</sup>. Es bedarf vor allem eines politischen Entschlusses, den Einsatz der Kryptographie zu fördern und nicht unter dem Leitstern der Verteidigung staatlicher Souveränitätsrechte durch Auflagen wie Begrenzung der Schlüssellänge oder zwangsweise Hinterlegung der privaten Schlüssel bei staatlichen Stellen zu behindern.

Schließlich sind auch die Zentralbehörden des gewerblichen Rechtsschutzes gefordert. Ihre DV-Abteilungen standen bislang abseits des öffentlichen Interesses. Mit der Einführung von Verfahren rechtsverbindlicher Telekooperation rücken die dortigen internen Abläufe stärker in den Fokus des Interesses und werden auf ihre Angemessenheit und Sicherheit hin befragt werden.

\* \* \* \* \*

---

<sup>86</sup>PKI = **P**ublic **K**ey **I**nfrastructure

