



GMD Report 68

GMD –
Forschungszentrum
Informationstechnik
GmbH

Ulrich Pordesch

Nachweis der Präsentation signierter Daten

November 1999

© GMD 1999

GMD –
Forschungszentrum Informationstechnik GmbH
Schloß Birlinghoven
D-53754 Sankt Augustin
Germany
Telefon +49 -2241 -14 -0
Telefax +49 -2241 -14 -2618
<http://www.gmd.de>

In der Reihe GMD Report werden Forschungs- und Entwicklungsergebnisse aus der GMD zum wissenschaftlichen, nicht-kommerziellen Gebrauch veröffentlicht. Jegliche Inhaltsänderung des Dokuments sowie die entgeltliche Weitergabe sind verboten.

The purpose of the GMD Report is the dissemination of research work for scientific non-commercial use. The commercial distribution of this document is prohibited, as is any modification of its content.

Anschrift des Verfassers/Address of the author:

Ulrich Pordesch
Institut für Sichere Telekooperationstechnik
GMD – Forschungszentrum Informationstechnik GmbH
Rheinstraße 75
D-64295 Darmstadt
E-mail: ulrich.pordesch@gmd.de

ISSN 1435-2702

Kurzfassung

Um mit signierten Dokumenten Beweise führen zu können, ist nicht nur die Urheberschaft und Unversehrtheit der Daten, sondern auch deren Inhalt anhand einer Präsentation nachzuweisen. Unterschiede in der Hardware, in der Software, in unsignierten Zusatzdaten, sowie in Bedienweisen und in der Umgebung können jedoch zu sehr unterschiedlichen Präsentationen signierter Daten führen (Mehrdeutigkeit). Hinzu kommt das Risiko lokaler Manipulationen oder Fehler (Falschpräsentation). Signaturgesetz und -verordnung behandeln die Mehrdeutigkeitsrisiken bislang kaum, die technischen Spezifikationen sehen nur die Eintragung eines Datentyps zu signierten Daten in der Signatur vor. In Gerichtsprozessen kann schon die Behauptung der Existenz einer anderen Präsentation Beweisprobleme verursachen, weil die Sicherheitsvermutung des Signaturgesetzes keinen Anscheinsbeweis rechtfertigt. Sachverständige können durch Untersuchung der Dokumente und der Anwenderinfrastruktur zusätzliche Erkenntnisse gewinnen und Aussagen zur Wahrscheinlichkeit bestimmter Präsentationen treffen, aber nur eingeschränkt und in bestimmten Fällen. Als technischer Lösungsansatz wird das Konzept der zurechenbaren Standardpräsentation hergeleitet und beispielhaft dargestellt. Die Berücksichtigung der Präsentation und der Systemherrschaft über die Anwenderinfrastruktur im Signaturgesetz werden angeregt.

Abstract

If anyone wants to prove a declaratory act on court he not only has to prove integrity and authorship of signed data but also their content by a presentation. Unfortunately the presentation of data may depend on the hardware platform, the used software, on additional unsigned data, on the users behaviour and the environment, so that presentation can be ambiguous in legally relevant aspects. Additionally we have to face the risk of manipulation and faults of the used presentation system and its usage. The digital signature act does not treat the problem of ambiguity sufficiently, and technical specifications only contain a data field "content type" of data as part of the signature, which does not solve the problems. On court, the oponent of the proof can argue sucessfully that a different presentation could exist. The assumption of security of the signature act is no basis for a prima facie proof against such objections. Experts can get additional findings and likelihood statements, if they investigate the document and the presentation system of the signer, but only in some cases. As a technical solution the concept of the "ascribable standard presentation of signed data" is derived in an requirements analysis and elaborated exemplarily. It will be necessary to take the presentation into consideration, when the the digital signature act and other legal codes will be revised.

Schlagworte

Digitale Signaturen, rechtliche Aspekte, Darstellung.

Key words

Digital Signatures, legal aspects, presentation.

Vorwort

Nach der Verabschiedung des Signaturgesetzes und der bevorstehenden Verabschiedung der EG-Richtlinie über gemeinsame Rahmenbedingungen für elektronische Signaturen ist damit zu rechnen, dass digital signierte Dokumente Papierdokumente auch in schadensträchtigen Vorgängen ersetzen werden. Deshalb werden Signaturverfahren bald auch Mittel und Ziel krimineller Aktivitäten und als Folge davon Beweismittel in Gerichtsverfahren werden. Dabei werden sich für Richter und Prozessbeteiligte eine Reihe von Beweisfragen stellen, die aus der bislang vorherrschenden Welt papiergebundener Urkunden und der Schriftbegutachtung unbekannt sind. Und ebenso werden Techniker als Entwickler und Sachverständige mit Fragen aus einer für sie bis dato weitgehend unbekannten Denkwelt konfrontiert werden.

Diese Arbeit versucht, einen Teil dieser Entwicklung gedanklich vorwegzunehmen, zu erwartende Fragestellungen und Probleme zu identifizieren und technische Lösungsmöglichkeiten aufzuzeigen. Thema ist das Teilproblem des Nachweises der Präsentation digital signierter Daten auf Bildschirmen und anderen Ausgabegeräten. Hierbei handelt es sich um eine zentrale Fragestellung, weil eine Präsentation von Daten die Grundlage der Interpretation und Auslegung von Willenserklärungen sein wird und nicht die signierten Daten selbst. Gleichwohl findet dieser Aspekt in der juristischen und technischen Diskussion über Signaturverfahren bislang noch kaum Beachtung.

Die Arbeit gliedert sich in drei Hauptteile. Den ersten Teil bildet eine ausführliche Problemanalyse, in der das Konzept der Arbeit an einem fiktiven Beispiel erläutert, Grundbegriffe eingeführt und vor allem die technischen Risiken detailliert untersucht werden. Im zweiten Teil wird untersucht, wie mit diesen Problemen auf dem gegenwärtigen Stand der juristischen und technischen Diskussion umgegangen werden könnte, durch technische Anpassungen, im Rahmen des Gerichtsprozesses und der Sachverständigenbegutachtung. Das liefert den Kern schwer handhabbarer Probleme, deren Lösung der Inhalt des dritten Teils ist. Mit Hilfe der Methode der Konkretisierung rechtlicher Anforderungen (KORA) werden technische Anforderungen und Gestaltungsvorschläge systematisch hergeleitet.

Für anregende Diskussionen und wertvolle Hinweise zu diesem Arbeitspapier danke ich recht herzlich Peter von Ondarza, Berlin, Dr. Andreas Schmitt und Rüdiger Grimm, beide GMD-SIT. Über weitere Anregungen, Hinweise und Kritik seitens der Leser würde ich mich sehr freuen.

Darmstadt, 19.10.99

Inhaltsverzeichnis

Teil I: Problemanalyse

9

1. Einleitung	9
1.1 Der Fall Zange	9
1.2 Fragestellung: Nachweis der Präsentation	12
1.3 Einordnung der Fragestellung	13
1.4 Diese Arbeit	13
1.5 Vorarbeiten und Umfeld	14
1.6 Schwerpunktsetzung	16
1.7 Vorgehensweise	17
2. Präsentation	19
2.1 Inhalt und Bedeutung signierter Daten	19
2.2 Technischer Ablauf einer Präsentation	21
2.3 Präsentationskomponenten	23
2.4 Nachweis vermittelt einer Präsentation	23
2.5 Nachweis der Präsentation	27
3. Risiken	29
3.1 Präsentationsrisiken	29
3.2 Mehrdeutigkeiten	30
3.3 Falschpräsentation	37
3.4 Mögliche Effekte	43

Teil II: Möglicher Umgang mit dem Präsentationsproblem

53

4. Sicherheitsvorgaben und Schutzmöglichkeiten	53
4.1 Gesetze und Ausführungsbestimmungen	53
4.2 Technische Anforderungen und Spezifikationen	58
4.3 Individuelle Schutzmöglichkeiten	60
5. Gerichtliche Beweisführung	67
5.1 Beweisrechtliche Grundlagen	67
5.2 Einwendungsmöglichkeiten	75
5.3 Indiztatsachen und Beweiserleichterungen	81
5.4 Verbleibende Beweisprobleme	87
6. Sachverständigenbegutachtung	89
6.1 Aufgaben der Begutachtung	89
6.2 Untersuchungsmöglichkeiten	90
6.3 Bewertung	93
6.4 Werkzeuge	95
6.5 Probleme	96

Teil III: Problemlösung

97

<u>7. Rechtliche Gestaltungsanforderungen</u>	97
<u>7.1 Konkretisierung rechtlicher Anforderungen</u>	97
<u>7.2 Rechtliche Anforderungen</u>	98
<u>7.3 Rechtliche Kriterien</u>	101
<u>8. Gestaltungsziele</u>	105
<u>8.1 Datenformate mit Präsentationsvorschriften</u>	105
<u>8.2 Standardpräsentation</u>	109
<u>8.3 Kontrolle der physischen Präsentation</u>	110
<u>8.4 Nachweis der Sicherheit der Anwenderinfrastruktur</u>	112
<u>8.5 Hinweise auf die tatsächliche Präsentation</u>	114
<u>8.6 Systemarchitektur</u>	116
<u>8.7 Evaluierung und organisatorische Aspekte</u>	118
<u>9. Beispielhafte Lösungsvorschläge</u>	121
<u>9.1 Elektronisches Rezept</u>	121
<u>9.2 Elektronische Urlaubskarte</u>	123
<u>10. Anregungen für rechtliche Regelungen</u>	127
<u>10.1 Berücksichtigung der Präsentation</u>	127
<u>10.2 Berücksichtigung der Systemherrschaft</u>	129
<u>Ausblick</u>	133
<u>Literatur</u>	135

Teil I: Problemanalyse

1. Einleitung

1.1 Der Fall Zange

Nachdem im vorangegangenen Zivilverfahren festgestellt wurde, dass die elektronische Urlaubskarte von Frau Karin Zange Manipulationen aufwies und Anhaltspunkte für eine Fälschung bestehen, hat die GMD Forschungszentrum Informationstechnik Darmstadt Strafanzeige wegen aller in Frage kommenden Straftatbestände (insbesondere Datenmanipulation) erstattet. Der Anzeigeersteller, der Institutsleiter GMD Herr Mantil, legt der Anzeige mehrere Farbausdrucke der elektronischen Urlaubskarte bei, auf der die mutmaßlich gefälschten Anträge verzeichnet sind und den schriftlichen Bericht des technischen Leiters. Nach Eingang der Unterlagen leitet die Staatsanwaltschaft wegen des öffentlichen Interesses an dieser neuen Fragestellung das Ermittlungsverfahren ein und beauftragt die Polizei mit den weiteren Ermittlungen. Diese vernimmt die Beschuldigte Zange und befragt den Organisationsleiter und teilt das vorläufige Ergebnis an den Staatsanwalt mit. Aufgrund der Ermittlungsergebnisse sieht der Staatsanwalt eine ausreichende Grundlage für eine Anklage als gegeben an.

Im Prozess bestreitet Frau Zange einen bereits gestellten Urlaubsantrag vom 1.2 bis zum 5.2. später elektronisch storniert zu haben. Sie bestreite nicht die Echtheit der Daten und Signaturen, wisse aber ganz genau, in *so* einem elektronischen Urlaubsformular, wie dem abgebildeten keine Anträge gestellt zu haben, insbesondere nicht die in Frage stehenden. Ihr Anwalt wirft die Frage auf, ob die signierten Daten nicht zu einem anderen elektronischen Formular gehören könnten. Hierzu ergänzt Frau Zange auf Nachfrage, dass es - soweit sie sich erinnern könne - damals durchaus verschiedene ähnlich aussehende Formulare gegeben habe, so etwa Beschaffungsformulare und auch einmal eine Teststudie mit Vorläufern. Der als Zeuge geladene Organisationsleiter der GMD bestätigt, dass es tatsächlich verschiedene andere elektronische Formulare gegeben habe, dies habe aber nichts mit diesem Fall zu tun.

Da die Frage prozessentscheidend sein kann, beauftragt das Gericht einen Sachverständigen. Er soll klären, inwieweit der Ausdruck der Urlaubskarte der tatsächlichen elektronischen Urlaubskarte der GMD entspricht, und ob auszuschließen ist, dass sie Anträge in einem anderen Formular signiert hat.

Der Sachverständige sucht die GMD Darmstadt auf und wird dort an den zuständigen Programmierer der Urlaubskarten-Anwendung Herrn Dr. Tergün verwiesen. Auf Nachfrage erklärt dieser, dass zu der Urlaubskartenanwendung des Vorgangssteuerungssystems keine Übersichtsdocumentation erstellt worden sei, u.a. weil zunächst gar nicht geplant worden sei, den Testbetrieb in Regelbetrieb zu überführen. Er habe sich auch seit langem nicht mehr mit dem System beschäftigt. Auf eine für den Gutachter undurchsichtige Weise gelingt es ihm nach etwa 15 Minuten über einen entfernten Rechner das Vorgangssystem zu starten und dort ein Formular aufzurufen:

X Listen:Listen
Hilfen

Disponieren

GMD-DA-Urlaubskarte, Jahr: 1993

Name.....: Zange Verg.Gr.: Tarifurlaub.....: 30
Vorname.: Karin Alter....: Zusatz Schwerbeh.: 
Geb.Jahr: Abt.....: Urlaub gesamt.....: 30
Pers.Nr.: Dienstzt.: Resturlaub v. VJ.: 10

Letzter Eintritt: 90 Gesamt.....: 40

Tarifl.Freizeit...: 2

Sign: **KGue**

Vermerk: UK-Simulationsstudie Sign: 
OE des Antragstellers: /DEMO/MITARB/Zange
Mailadresse des Antragstellers: zange
OE des 1. Genehmigers: /DEMO/MITARB/Hammer
OE des 2. Genehmigers: /DEMO/MITARB/Hammer
Mailadresse des Sekretariats: usauer
OE der Verwaltung: /DEMO/VA/Urlaubsstelle

Antragsteller				Genehmiger			Verwaltung			
Erster	letzter	Arb.		Einverständnis			Rest-			
Urlaubstag	Bem.	Sign	Tage	Bem.	Sign1	Sign2	urlb.	Bem.	Sign	
28.1.	29.1.	Bi>	KZan	2		VHam		38		JRue
1.2.	5.2.	Li>	KZan	5	Da>	ARos		35		JRue
28.1.	29.1.			2				37	Gu>	JRue
1.2.	5.2.	Bi>	KZan	5		ARos		40	Da>	JRue
1.2.	5.2.	Ur>	KZan	3		ARos		35	Si>	
8.2.	12.2.	>	KZan	5	We>	VHam		30		
1111	1111		KZan	4				26		

Abbildung 1: Abbild der Bildschirmdarstellung der Urlaubskarte von Frau Zange

Die elektronischen Urlaubskarten lägen wie früher auf einer der mittlerweile nur noch als Server verwendeten SUN-Workstations im Keller. Einer dieser Rechner fungiere auch als X-Server, der einem X-Client auf dem PC den Zugang zu den Daten ermögliche.

Zur Frage, ob denn das Formularabbild, das 1999 zu sehen sei, dem von 1993 entspreche, ergab die Nachforschung des Sachverständigen folgende Erkenntnisse: 1993 seien überwiegend SUN-Workstations mit größeren und Macintosh-Rechner mit zum Teil sehr viel kleineren Bildschirmen gebräuchlich gewesen wären, teilweise auch nur mit schwarz/weiß-Bildschirmen. Welchen Rechner Frau Zange benutzt habe, könne er nicht mehr feststellen. Die kleinen MACs seien überdies auch kürzlich alle ausgemustert und verschrottet worden.

Die Darstellung auf dem PC entspreche sicher im Wesentlichen der damaligen Darstellung. Allerdings könne er dies auch nicht mit Bestimmtheit sagen. Nicht alle Einstellungen der

Bildschirmelemente - Farben, Größen und Positionen von Buttons und Teilfenstern - würden im Urlaubskarten-Anwendungsprogramm festgelegt. Viele dieser Festlegungen seien auch in so genannten resource-files des X-Windows-Systems getroffen, die sich auf den Client-Systemen der Endbenutzer befänden. Diese hätten zwar Default-Einstellungen, könnten im Prinzip aber durch die Benutzer oder die Administratoren der lokalen Systeme geändert werden. Die Einstellungen von 1993 auf dem Rechner von Frau Zange ließen sich nicht mehr rekonstruieren. Hinsichtlich der Zeichensätze merkte Dr. Tergün an, dass die X-Clients eigene Zeichensätze auf den Endbenutzersystemen gespeichert hätten. Diese würden dann durch das Anwendungsprogramm angesteuert. Auf den kleinen MAC-Rechnern seien durch das Anwendungsprogramm wegen der niedrigen Bildschirmauflösung kleinere Fonts ausgewählt worden. Letztlich könne der Benutzer bzw. Administrator der lokalen Systeme aber Fonts installieren und umbenennen wie er wolle, so dass von Seiten des Anwendungsprogramms keine Kontrolle über das tatsächliche Erscheinungsbild am Endsystem bestehe.

Die Besprechung der Dokumentstruktur ergab, dass Signaturen der Antragsteller immer nur Datenfelder mit als Zeitangaben interpretierbaren Zeichen (z.B. "1.2." und "5.2.") umfassten und dazu die Signatur der Verwaltung im Formulkopf.¹ Alle Daten sind ASN.1-codiert, so dass die Codierung nicht die Feldnamen und sonstige die Bedeutung der Daten und ihrer Struktur beschreibende Elemente enthält. Alle für die Präsentation der Daten wichtigen Aspekte werden durch das auf dem Server liegende Anwendungsprogramm bzw. durch das lokale System der Benutzer festgelegt. Diese sind nicht Teil der signierten Daten und mithin von Frau Zanges Signatur nicht umfasst.

Die Analyse der per Diskette übergebenen Daten ergibt, dass es sich um ein ASN.1-codiertes Dokument handelt, das denen der Urlaubskartenanwendung entspricht. Aus den signierten Daten ist nicht ersichtlich, um welche Anwendung es sich handelt und wie die Daten vor dem Signiervorgang präsentiert wurden. Die Bezeichnung des zugehörigen Anwendungsprogramms und dessen Version ist nicht Teil der signierten Daten, ebenso wenig wie Feldbezeichnungen, Überschriften und eine Darstellung als Formular. Einige Indizien sprechen allerdings mit gewisser Wahrscheinlichkeit für eine Urlaubskarten-Anwendung. Der signierte Bitstring enthält Daten, die einer Signatur der Verwaltungskraft Frau Hürl entsprechen. Diese Signatur wiederum bezieht sich auf unter anderem auf Textfelder mit den Werten "Urlaubskarte" und "K. Zange". Das spricht dafür, dass es sich um Daten handelt, die mit einer Urlaubskarten-Anwendung erzeugt wurden. Es ist aber auch nicht auszuschließen, dass die Daten in einem anderen Formular präsentiert wurden. Allerdings steht dann eine Erklärung dafür aus, warum darin Daten enthalten waren, die Signaturen der Verwaltung unter Personendaten von Frau Zange und dem Text "Urlaubskarte" entsprechen. Die Frage kann in Ermangelung der mittlerweile gelöschten alten Testanwendungen aus jener Zeit nicht mehr geklärt werden.

In seinem Gutachten schildert der Sachverständige die genannten Überlegungen und Untersuchungen und fasst seine Ergebnisse zusammen: In der GMD gibt es eine Datei, die Daten enthält, die dem Format nach einer elektronischen Urlaubskarte der vorgefundenen GMD-internen Urlaubskarten-Anwendung entsprechen. Sie enthält Daten, die mit dem von der GMD angegebenen Anwendungssystem als Urlaubsantrag bzw. Rücknahme eines Antrags dargestellt werden können. Diese Daten sind mit an Sicherheit grenzender Wahrscheinlichkeit

¹ In Abbildung 1, S. 10 gelb unterlegt, wie in einer Bildschirmpräsentation dieses Dokumentes zu erkennen ist, allerdings nicht im Ausdruck :-). Damals noch ohne das Bemerkungsfeld.

unverfälscht und mit einem auf Frau Zange zertifizierten Schlüssel signiert worden. Es spricht einiges dafür, dass Frau Zange diese Daten in der Urlaubskarten-Anwendung weitgehend so gesehen hat, wie der Richter auf dem Ausdruck. Es ist aber auch keineswegs auszuschließen, dass die Daten Frau Zange bei ihren Signiervorgängen teilweise oder sogar völlig anders als auf dem Ausdruck präsentiert dargestellt wurden, aus technischen Fehlern oder um sie zu täuschen. Vorstellbar ist, dass ein anderes Formularlayout mit anderen Feldbezeichnungen geladen wurde oder Fenster verdeckt blieben, aus denen die Urlaubskarten-Anwendung und Antragsdaten zu erkennen gewesen wäre. Diese Frage lässt sich heute nicht mehr klären. Denn aus den Signaturdaten ist auch nicht ersichtlich, auf welchem System die Signatur erzeugt wurde und es lässt sich nicht einschätzen, wer - Frau Zange, andere GMD-Mitarbeiter oder Dritte - Zugriff auf dieses System hatte.

Würden Sie Frau Zange bei dieser Beweislage verurteilen oder im Zweifel für die Angeklagte freisprechen?

1.2 Fragestellung: Nachweis der Präsentation

So oder so ähnlich wie im vorangegangenen fiktiven Beispiel könnte künftig ein gerichtlicher Streitfall verlaufen. Dabei wurde in der Konstruktion des hypothetischen Streitfalls eine der wenigen Signaturanwendungen aus der betrieblichen Praxis als Beispiel verwendet. Und der Autor hat tatsächlich den Versuch unternommen, in der Rolle eines Sachverständigen Aussagen zu treffen.²

Signaturverfahren sollen es ermöglichen, die Authentizität elektronischer Dokumente und Daten und deren Urheberschaft zweifelsfrei nachzuweisen. Auf diese Weise sollen elektronische Dokumente einen hohen Beweiswert erhalten und auch in Bereichen eingesetzt werden können, die bislang papiergebundenen Verfahren mit handschriftlichen Unterschriften vorbehalten blieben. Dabei wird jedoch zumeist übersehen, dass nicht Dokumente unterschrieben, sondern letztlich *nur Bitfolgen signiert* werden. Um die Bedeutung dieser Bitfolgen zu erschließen müssen sie von Programmen ausgewertet und - soweit sie nicht ausschließlich maschinell verarbeitet werden - über Ausgabegeräte, wie z.B. Bildschirm, Drucker, Lautsprecher ausgegeben werden (Präsentation). Je nach gewähltem Anwendungsprogramm, den Systemeinstellungen, der Hardwarekonstellation und der Bedienung durch den Benutzer können Auswertung und Ausgabe jedoch unterschiedlich verlaufen. Damit ergibt sich aber das Problem nachzuweisen, dass eine bestimmte Präsentation "richtig" erfolgt, d.h. insbesondere, dass diese der Intention des Signierers entspricht.

Zwar ist das Problem der Präsentation digitaler Daten nicht erst mit dem Einsatz elektronischer Signaturverfahren entstanden. Daten müssen ganz unabhängig davon, ob sie signiert wurden, durch Hard- und Software ausgewertet und ausgegeben werden, damit Menschen sie wahrnehmen können. Dass eine unmittelbare Wahrnehmung und Deutung von Daten nicht möglich ist, und dass Daten interpretiert werden müssen, ist ein generelles Problem der IT-Sicherheit.³ Bislang wirkte sich das Problem der potentiell mehrdeutigen Darstellung - sieht man vom täglichen Ärger mit Textverarbeitungssystemen unterschiedlicher Versionen und

² Die Anwendung elektronische Urlaubskarte ist nicht zitierfähig dokumentiert. Sie ist eine formularorientierte Anwendung des in der GMD entwickelten Vorgangssteuerungssystems DISCO (Günther 1989). Sie ist nach einer Testphase ca. seit 1993 im Regelbetrieb im Einsatz.

³ Dierstein 1995.

Ähnlichem einmal ab - jedoch kaum aus. Dies liegt vor allem daran, dass letztlich fast immer noch Papierdokumente erzeugt werden, auf die man sich in Zweifelsfällen bezieht. Außerdem haben unsignierte Dokumente aufgrund ihrer spurlosen Veränderbarkeit ohnedies nur geringen Beweiswert, so dass es wohl unsinnig wäre, rechtliche Auseinandersetzungen um deren richtige Präsentation führen zu wollen.

Diese Situation wird sich jedoch in den nächsten Jahren ändern: Gerade wenn Signaturverfahren die Unversehrtheit und Urheberschaft der Daten beweisbar machen und die Signaturgesetze sowie Änderungen in anderen Gesetzen Rahmenbedingungen für die Durchsetzung dieser Verfahren im Rechtsverkehr setzen, wird der Nachweis der richtigen Präsentation bedeutsam werden. Ohne einen solchen Nachweis könnten rechtsverbindliche Erklärungen und Handlungen erfolgreich abgestritten werden, auch wenn die Urheberschaft und Unversehrtheit der Daten aufgrund einer gültigen Signatur nicht mehr abstreitbar sein sollte.

1.3 Einordnung der Fragestellung

Ohne der noch zu leistenden Erörterung der Beweisfragen vorgreifen zu wollen, sei an dieser Stelle bereits eine Einordnung der Fragestellung und dieser Arbeit in die übergeordnete der Beweisführung und Begutachtung digital signierter Dokumente vorgenommen. Diese zerfällt in folgende Hauptfragestellungen:

- **Nachweis der Unversehrtheit und Urheberschaft der Rohdaten:** Zunächst ist immer der Nachweis zu führen, dass die vorliegenden (signierten) Daten unversehrt sind und von einem bestimmten Urheber stammen, unabhängig davon, welche Bedeutung sie haben. Ohne die Klärung dieser Frage ist es sinnlos, über die Präsentation zu streiten.
- **Nachweis der Präsentation:** Danach ist nachzuweisen, dass die signierten Daten nach Wunsch des Signierers oder aufgrund einer rechtsgültigen Vorschrift in einer bestimmten Art und Weise zu interpretieren sind.⁴ Dieser Nachweis erfolgt immer anhand einer Präsentation, deren Korrektheit in einem noch zu spezifizierenden Sinne wiederum nachzuweisen ist.

Daneben können eine Reihe weiterer Fragen eine Rolle spielen. Zu nennen ist zunächst die Frage der willentlichen Auslösung des Signiervorgangs durch den Signierer (Frage des Versehens, der Voreiligkeit, des Zwangs usw.). Auch der Nachweis der Signierzeit kann eine Rolle spielen, wenn man an den Ablauf von Fristen denkt.

Schließlich ist die Beweisbarkeit der Präsentation eines signierten Dokumentes Voraussetzung für die Beweisbarkeit von Transaktionen innerhalb von elektronischen Geschäftsprotokollen und damit die Verbindlichkeit der telekooperativen Geschäftsprozesse selbst.⁵

1.4 Diese Arbeit

In diesem Papier werden die mit dem Nachweis der Präsentation zusammenhängenden Fragen erstmals systematisch untersucht.

⁴ Entsprechend für die Signaturen, Zertifikate und anderen Bestandteile die zu den signierten Daten hinzugefügt werden.

Hier wird jedoch die allgemeinere Frage der Präsentation signierter Nutzdaten behandelt.

⁵ Grimm 1994 und Wichert GMD-Spiegel 1/98.

Im (überwiegenden) technischen Teil der Arbeit wird das Problem und seine Relevanz untersucht, d.h. die Frage, inwiefern die Präsentation zu substantiell unterschiedlichen Wahrnehmungen bzw. Interpretationen führen kann und welche Ursachen es für die Unterschiede gibt (Risikountersuchung). Außerdem wird untersucht, welche Rückschlüsse aus den signierten Daten aber auch aus anderen Informationsquellen auf die Präsentation geführt werden können (Begutachtung). Schließlich werden in einer Anforderungsanalyse ein Konzept und weitere Vorschläge entwickelt, mit denen der Nachweis der Präsentation verbessert werden kann (Technikgestaltung).

Die Beurteilung der Relevanz des Problems benötigt Relevanzkriterien, Gestaltungsvorschläge benötigen Gestaltungsanforderungen. Diese können, da die Technik sozialen Zwecken dienen soll, notwendigerweise nicht aus der Technik selbst heraus abgeleitet werden. In unserer rechtsstaatlich verfassten Gesellschaft ist vielmehr die Frage von entscheidender Bedeutung, inwiefern Nachweise in Gerichtsprozessen erfolgreich geführt werden können. Deshalb enthält die Untersuchung auch einen juristischen Anteil. Es werden wichtige gesetzliche Vorgaben - insbesondere aus dem Multimedia- und Beweisrecht zusammengestellt und auf die Themenstellung übertragen. Hinweise auf die Relevanz bestimmter Präsentationsunterschiede werden aus der Rechtsprechung gewonnen. Was in welcher Weise im Verfahren durch Richter, Parteien oder Sachverständige nachzuweisen ist, ergibt sich aus dem Beweisrecht. Für die Anforderungsanalyse werden grundrechtliche Vorgaben zusammentragen und technikbezogen konkretisiert. Hierbei handelt es sich um das Zusammentragen und Übertragen vorhandener rechtswissenschaftlicher Erkenntnisse auf die Technik, nicht um systematische rechtswissenschaftliche Untersuchungen. Letztere müssen Juristen vorbehalten bleiben.

1.5 Vorarbeiten und Umfeld

Bei papiergebundenen Verfahren ist durch die Verkörperung der Information und die untrennbare Verknüpfung mit dem Datenträger sichergestellt, dass in der Regel keine Frage dahingehend aufkommt, was die darauf präsentierte Information ist. Sie ist in der Regel ohne technische Mittel direkt und in ihrer Vollständigkeit wahrnehmbar. Allenfalls ist die Frage, ob man mit der Lupe und chemischen Mitteln irgendwelche Spuren oder Geheimschriften sichtbar machen kann, die nicht direkt sichtbar sind.⁶ Von daher verwundert es nicht, dass zur Frage der Präsentation in der Literatur zur wissenschaftlichen Schriftvergleichung⁷ und der kriminalistischen Urkundenuntersuchung⁸ keine Anknüpfungspunkte zu finden sind. Auch andere Fachleute aus dem Umfeld des Sachverständigenwesens, die sich bereits mit dem Signaturen befassen haben, sind der – wie zu zeigen sein wird viel zu optimistischen – Auffassung, dass es nach Einsatz von Signaturverfahren mit gesetzlichem Sicherheitsstandard keiner Sachverständigen mehr bedürfe.⁹

In der Informatik- und Informationstechnik-Literatur hat die Präsentation von Daten vor allem in der Diskussion um druckorientierte Dokumentformate eine Rolle gespielt. Bei der Entwicklung von Postscript und PDF geht es vornehmlich darum, einen Drucker-unabhängigen

⁶ In einem Fall gelang es einen Erpresser zu überführen, weil auf der Rückseite des Papiers Abdrücke anderer Briefe sichtbar gemacht werden konnten. Aber auch hier geht es nicht um verschiedene Darstellungsmöglichkeiten sondern höchstens verbesserter Darstellungsmöglichkeiten mittels technischer Analysehilfsmittel.

⁷ Michel 1982, Ries 1989.

⁸ Groß / Geerds 1979.

⁹ Bleutge 1997, 17.

einheitlichen Ausdruck elektronischer Dokumente zu ermöglichen. Bemühungen um Dokumentenstandards wie ODA¹⁰, später SGML und nun XML¹¹ zielen auf die plattform- und anwendungssystemunabhängige Austauschformate für Dokumente, die eine Weiterverarbeitung ermöglichen. In allen Fällen stand jedoch bislang die technische Interoperabilität der Verfahren der Dokumentverarbeitung im Vordergrund des Interesses, nicht jedoch die globale Eindeutigkeit. Zur Einbettung von Signaturverfahren gibt es jeweils erste Konzepte, dabei geht es jedoch um den Nachweis der Integrität von Daten, nicht um den eindeutigen Nachweis einer bestimmten Präsentation. Auch wenn das hier definierte Präsentationsproblem also nicht behandelt wird, finden sich doch bei der Lösung zu berücksichtigende Ansätze.

Dass die Frage der Präsentation im Kontext digital signierter Daten relevant sein könnte wurde, soweit bekannt, zunächst vom Autor als Konsequenz aus Verletzlichkeitsexperimenten zu digitalen Signaturen bemerkt und ansatzweise in Simulationsstudien zur telekommunikativen Rechtspflege und elektronischen Vorgangsbearbeitung untersucht, die die Projektgruppe verfassungsverträgliche Technikgestaltung provet und die GMD durchgeführt haben.¹² Im Kontext des Signaturgesetzes wies Fox auf das Problem uneindeutiger Darstellung mit einem Beispiel von Word-Dateien hin, bei dem auf unterschiedlichen Plattformen (PC und MAC) bestimmte Zahlenwerte unterschiedlich dargestellt werden.¹³ Erste Überlegungen, wie der Beweiswert von Signaturverfahren durch Technikgestaltung erhöht werden könnte, hat der Autor zusammen mit Bizer und Hammer untersucht.¹⁴ Die Untersuchung erfolgte noch nicht systematisch und zugespißt auf das Präsentationsproblem. Weitere Publikationen im Umfeld der Diskussion um Signaturverfahren zu diesem Thema sind nicht bekannt.

Als juristischer Autor erkannte Seidel frühzeitig offene Fragen hinsichtlich der Dokumentformate.¹⁵ Durch die Änderung des Dokumentausgabeformats ändere sich zwar nichts an der inhaltlichen Schriftauthentizität, wohl aber am Erscheinungsbild des Dokumentes. Leider berücksichtigt er dieses Problem jedoch nicht bei seinen Überlegungen zu rechtlichen Anerkennung der digitalen Signatur. Spätere Autoren griffen diese Überlegung nicht mehr auf. Zu Beweisführung bei EDV-gestützter Dokumentation (auch z.B. elektronische Buchführung) bemerken etwa Bergmann und Streitz, dass die für die Lesbarmachung erforderliche Hard- und Software durch die Partei zur Verfügung zu stellen ist, ohne allerdings bei der Analyse der Beweiskraft und möglicher Manipulationsrisiken auf Probleme der eindeutigen Interpretation von Daten einzugehen.¹⁶ Auch Ebbing, der entgegen der herrschenden Meinung bei elektronischen Dokumenten bereits die Schriftform nach dem Bürgerlichen Gesetzbuch (BGB) als erfüllbar sieht, ignoriert die Präsentation völlig. Die Nutzung eines Textverarbeitungs-PCs sei heute so selbstverständlich wie das Einschalten einer Schreibtischlampe oder das Aufsetzen einer Lesebrille, Datenträger sollten daher als Urkundsmaterial anerkennungsfähig sein.¹⁷ Dabeikennt er allerdings völlig, dass die Vielfalt von Hardwareplattformen, Anwendungssystemen, Schnittstellen, Konfigurationen und Einstellungen und ihre Auswirkungen auf die Darstellung mit den singulären Einstellmöglichkeiten einer Leselampe (Licht an/aus) nicht

¹⁰ Appelt 1991.

¹¹ Goldfarb 1998, Grimm / Wäsch 1999.

¹² Die Studien sind in provet / GMD 1994 und provet / GMD 1995 beschrieben. Zu Verletzlichkeitsexperimenten Pordesch, provet Arbeitspapier 81, 1992, Pordesch provet-Arbeitspapier Nr. 106, 1993, Pordesch DuD 1993.

¹³ Fox DuD 1998.

¹⁴ Bizer / Hammer / Pordesch 1995.

¹⁵ Seidel 1993.

¹⁶ Bergmann / Streitz 1994.

¹⁷ Ebbing 1996.

vergleichbar sind. Für Ernst ist bereits eine Mail oder die per Mail versendete Datei sogar bereits wie eine Papierurkunde "verkörpert" und es werden außer der Gültigkeit von allgemeinen Geschäftsbedingungen keine Probleme gesehen.¹⁸ Etwas mehr problematisierend wurden Fragestellungen im Zusammenhang mit der Präsentation in Bezug auf gespeicherte Informationen gemäß gesetzlicher Aufzeichnungspflichten (insbesondere bei der EDV-gestützten Buchführung) von Bohatiuk erörtert.¹⁹ Er weist darauf hin, dass bei EDV-Aufzeichnungen und -Speicherungen eine lückenlose Programm- und Verfahrensdokumentation notwendig ist und dass die EDV-Dokumentation gemäß der Grundsätze der ordnungsgemäßen Buchführung wie die Dokumente selbst 10 Jahre aufzubewahren ist. Bei nicht codierenden Bildaufzeichnungssystemen (Bildarchive) könne Aufzeichnungen nur dann ein Beweiswert zuerkannt werden, wenn es sich um eine - trotz der zahlreichen Editier-, Scalier-, Misch- und anderen Funktionen der Bildbearbeitung - unveränderte Aufzeichnung und Wiedergabe handele. Welche Anforderungen im Einzelnen zu stellen sind, stellt Bohatiuk nicht dar.

1.6 Schwerpunktsetzung

Risiken, rechtliche Bewertung und Gestaltungsmöglichkeiten hängen davon ab, um welche Medien (Text, Ton, Bild, ..), welche Inhalte und welche Rechtskontexte es bei den signierten Daten geht und welche rechtlichen Grundlagen dabei betrachtet werden. In dieser ersten systematischen Untersuchung wird folgende Schwerpunktsetzung gewählt:

Textdokumente

Texte spielen im Rechtsverkehr heute die größte Rolle. Obwohl es möglich wäre, verstärkt andere Medien zu nutzen - etwa Verträge mündlich abzuschließen und als Audiodokumente zu signieren - ist bereits erkennbar, dass der Gesetzgeber schriftliche Dokumente auch weiterhin bevorzugen wird. So liegt ein Entwurf eines Artikelgesetzes für umfangreiche Änderungen des Bürgerlichen Gesetzbuches (BGB) vor, in dem eine "elektronische Form" als Textform (lesbare Textzeichen) mit digitaler Signatur definiert werden soll. Nur diese elektronische (Text)Form soll in zahlreichen Rechtsbereichen zugelassen werden, in denen heute die herkömmlichen papiergebundene Schriftform vorgeschrieben ist.²⁰

In dieser Untersuchung werden die wichtigsten als Textform in Frage kommenden Dokumententypen, Freitextdokumente (wie Word), elektronische Formulare (wie die elektronische Urlaubskarte und das auch elektronische Rezept) und auch Hypertext (HTML) berücksichtigt.

Signaturgesetz und bundesdeutsches Recht

Gesetze und Richtlinien, die den Einsatz von digitalen Signaturverfahren und elektronischen Dokumenten regeln, gibt es in vielen Staaten und der EU. Hier soll die bundesdeutsche Gesetzeslage zur Grundlage genommen werden - weil diese für Gerichtsverfahren hierzulande entscheidend ist, aber auch, weil das bundesdeutsche Signaturgesetz als Vorläufer und Vorbild

¹⁸ Ernst 1997. Ähnlich optimistisch Deville / KaltheGener 1997.

¹⁹ Bohatiuk 1989.

²⁰ BMJ 1999.

von anderen Regelungen ist.²¹ An technischen Spezifikationen werden ebenfalls vor allem diejenigen berücksichtigt, die sich auf die bundesdeutschen gesetzlichen Grundlagen beziehen.

1.7 Vorgehensweise

Die Frage der Präsentation ist in der Diskussion um den Beweiswert von Signaturverfahren neu. Daher sind zunächst im folgenden Kapitel einige technische Begriffe zu klären. Danach ist im dritten Kapitel eingehend zu untersuchen, welche Risiken der Verfälschung durch die Präsentation bestehen und welche Aspekte der Präsentation relevant sein können. Für die Beurteilung der Relevanz werden hierbei Erkenntnisse aus der Rechtsprechung und juristischen Literatur - soweit vorhanden und bekannt - berücksichtigt.

Dieser ergeben Einwände gegen die Beweisführung mit digital signierten Dokumenten in Gerichtsverfahren, die zusammen mit den erforderlichen rechtlichen Grundlagen im fünften Kapitel dargestellt werden. Zu erkennen ist, welche Nachweise durch wen in welcher Form in Prozessen geführt werden müssen. Insbesondere ist die Frage zu klären, inwieweit Richter selbst mit Beweiserleichterungen bei Signaturgesetz-konformen Verfahren in der Lage sind, Beweismittel zu würdigen oder wo dies nicht möglich sein dürfte.

Die dabei identifizierten schwierigen Beweisfragen führen auf künftige Fragestellungen im sechsten Kapitel, mit denen sich Sachverständige zu beschäftigen haben werden. Technisch gesehen geht es dabei um die Frage, inwieweit unsignierte Daten und weitere Informationen ausgewertet werden können, um Aussagen über die Präsentation zum Signierzeitpunkt zu gewinnen. Dies gibt zum einen Hinweise auf eventuell zusätzlich zu signierende Daten - als auch als Bodensatz - bislang unlösbare Probleme, die durch technische und rechtliche Gestaltungsmaßnahmen zu lösen wären.

Im siebten und achten Kapitel werden dann technische Gestaltungsanforderungen entwickelt, die geeignet sein könnten, die Beweismöglichkeiten im Hinblick auf die Präsentation zu verbessern und den vorhandenen technischen Maßnahmenkatalog des Signaturgesetzes sinnvoll zu ergänzen. Dabei wird die von der Projektgruppe verfassungsverträgliche Technikgestaltung e.V. unter Mitarbeit des Autors entwickelte Methode der Konkretisierung rechtlicher Anforderungen (KORA) angewendet. Ansatzweise werden die Erkenntnisse im neunten Kapitel für zwei Anwendungsbeispiele konkretisiert.

Im zehnten Kapitel werden dann aus dieser technischen Sicht einige Anregungen für den Gesetzgebungsprozess formuliert.

²¹ SigG_97 und SigV_97.

2. Präsentation

In diesem Kapitel werden die technischen Abläufe der Präsentation grob skizziert und grundlegende Begriffe zur Präsentation definiert und es findet bereits eine grobe Einordnung in die Beweisführung mit signierten Dokumenten statt.

2.1 Inhalt und Bedeutung signierter Daten

2.1.1 Willens- und Wissenserklärungen

Rechtlich gesehen sind signierte und zu signierende Daten an sich, d.h. als rechnerinterne Bitfolge, bedeutungslos. Bedeutung erlangen sie, wenn mit ihnen rechtliche Ansprüche begründet, geändert, verworfen oder durchgesetzt werden. Der Terminus "Anspruch" bedeutet in diesem Zusammenhang, von jemandem ein Tun oder Unterlassen bzw. ein Dulden zu verlangen, also etwa eine Ware zu liefern oder eine öffentliche Behauptung zu unterlassen.²² Strafrechtlich ist ferner bedeutend, ob die Daten Mittel waren Straftaten zu begehen oder Mittel, solche nachzuweisen (z.B. Zeugenaussage). In diesen Zusammenhängen sind Daten relevant, wenn sie als Willens- und Wissenserklärungen interpretiert, oder solche mit ihnen nachgewiesen werden können:

Eine **Willenserklärung** ist eine Äußerung rechtlich erheblichen Willens einer natürlichen oder juristischen Person (etwas zu tun, zu unterlassen, zu fordern usw.), die auf einen rechtlichen Erfolg hinzielt.²³ Beispiele sind Kaufverträge und Bestellungen. Willenserklärungen können mündlich, schriftlich oder auch über elektronische Medien abgegeben werden. Signierte Daten können als elektronische Willenserklärung aufgefasst werden. Mit Blick auf die Präsentationsproblematik ist es jedoch besser, sie als Spur bzw. Abbild der Abgabe einer Willenserklärung an einem elektronischen Gerät aufzufassen.

Von der Willenserklärung wird bisweilen die **Wissenserklärung** unterschieden. Hierbei handelt es sich um eine rechtlich erhebliche Äußerung natürlicher Personen über Tatsachen, mit der - außer dem Willen zur der Äußerung selbst - kein Wille verbunden ist, insbesondere keiner zur Durchsetzung eines Anspruchs. Beispiele sind Aktennotizen über Gespräche, Sitzungsprotokolle oder Zeugenaussagen.

Neben den von Menschen abgegebenen Willens- und Wissenserklärungen können als Dritte zunehmend wichtige Kategorie noch **technische Vorgänge** als Quelle signierter Daten rechtserheblich werden. Beispiele sind automatisch erzeugte Zeitstempel oder Fehlerprotokolle eines technischen Systems. Diese Kategorie wird in dieser Arbeit nicht näher untersucht.

2.1.2 Dateninterpretation

Entscheidend ist also, dass elektronisch signierte Daten als ganz bestimmte Willens- und Wissenserklärungen sowie Ergebnisse bestimmter technischer Vorgänge oder zumindest Spuren

²² Creifelds 1996, 61.

²³ Creifelds 1996, 1484.

davon interpretiert werden können. Doch wie ist so eine solche Interpretation möglich? Hier ist sowohl technisch als auch rechtlich zwischen unformatierten von Menschen interpretierbaren Daten und formatierten maschinenauswertbaren Daten mit festgelegter Bedeutung zu unterscheiden:

Unformatierte Daten sind Daten, deren Bedeutung nicht exakt formalisiert ist, sondern durch den Menschen erschlossen werden muss. Beispiele für unformatierte Daten sind mit Word erzeugte Freitexte oder Corel-Draw-Grafiken. Es gibt in kein allgemeines Schema um aus solchen Daten eine Willens- oder Wissenserklärung abzuleiten. Festgelegt ist allenfalls, wie Programme solche Daten auswerten, um sie einem Benutzer gegenüber zu präsentieren. Damit ein Empfänger bzw. Prüfer die Bedeutung der Daten erkennen kann, die der Sender bzw. Signierende gemeint hat, muss er die Daten "richtig" wiedergeben. Erst auf der Grundlage einer solchen Wiedergabe können Menschen dann eine Willenserklärung wahrnehmen und den Versuch unternehmen, daraus den tatsächlichen Willen zu ermitteln. Dabei ist zu beachten, dass sich der Wille nicht nur aus dem Text bzw. dem abstrahierten Inhalt erschließen lässt, sondern auch aus allen scheinbar nebensächlichen Aspekten der äußerlichen Form.

Einfacher kann sich die Bedeutung aus **formatierten Daten** erschließen lassen. Hierbei handelt es sich um Daten mit, in einer technischen Spezifikation, einer anderen Willenserklärung oder vielleicht sogar in einem amtlichen Dokument festgelegter Bedeutung. Hier können die Datenbits etwa mittels eines Parsers logisch analysiert werden, um einen technischen Vorgang zu steuern, können selbst automatisch verarbeitet werden oder mit ihrer festgelegten Bedeutung in einer lesbaren Form ausgegeben werden. Im einfachsten Fall weist die signierte Nachricht ein Bit auf und das bedeutet die Wissensäußerung "Ereignis X hat stattgefunden". Dem Prinzip nach vergleichbar damit sind voll genormte Datenelemente in Kommunikationsprotokollen, bei denen die Bedeutung eines jeden Bit festgelegt ist und auf die ein Protokollanalytiker angesetzt werden kann. Auch bei formatierten Daten ist eine Ausgabe erforderlich, wenn der Mensch die maschinelle Dateninterpretation nachvollziehen will. Die Form der Wiedergabe ist jedoch für die Interpretation irrelevant, weil in den Daten keine verdeckten interpretationsbedürftigen Inhalte enthalten sein sollen.²⁴

Formatierte und unformatierte Daten im hier definierten Sinne sind Idealkategorien. Von technischen Protokollen einerseits und Freitext andererseits abgesehen hat man es häufig mit einer Kombination mehr oder weniger formatierter Daten zu tun. Insbesondere Daten für formularorientierte Anwendungen im Bankenbereich (z.B. HBCI-Standard), in Geschäftsprozessen (z.B. EDIFACT-Standard), in der Medizin (z.B. elektronisches Rezept) oder auch im in-house-Bereich (z.B. elektronische Urlaubskarte) enthalten neben stark formatierte Anteilen (z.B. Datumsfelder) und unformatierte Teile (z.B. Kommentarfelder), die durch Menschen interpretationsfähig und interpretationsbedürftig sind.

²⁴ Eine möglichst exakte Wiedergabe der Daten wie beim Signierer kann auch bei formatierten Daten erforderlich werden, wenn daran gezweifelt wird, dass der die Daten signierende Mensch die festgelegten Interpretationsregeln erkennen konnte und gelten lassen wollte und dass ihm nicht irgendwelche Daten zum Signieren untergeschoben wurden (Por-desch DuD 1993, 564). Dieses Teilproblem gilt jedoch gleichermaßen für formatierte und unformatierte Daten und erfordert den Nachweis der willentlichen Auslösung des Signiervorgangs (Zum Nachweis der Autorisierung des Signiervorgangs, siehe Bizer/Hammer DuD 1993).

2.1.3 Präsentation

Unabhängig von der später zu erörternden Frage, in welchen Fällen genau was nachzuweisen ist, lässt sich also bereits an dieser Stelle festhalten, dass es nicht ausreicht, mit einer Signaturprüfung nachzuweisen, dass Daten unverfälscht sind und von wem bzw. welchem technischen Gerät sie stammen. Vielmehr ist die Bedeutung der Daten anhand einer festgelegten Semantik nachzuweisen und soweit diese nicht existiert und in allen Zweifelsfällen die möglichst Wiedergabe einer bestimmten anderen.

Das Ergebnis eines Prozesses der Wieder- bzw. Ausgabe (signierter) Daten wird hier **Präsentation** genannt. Der Begriff "Präsentation" wird bewusst dem im Signaturgesetz²⁵ verwendeten Begriff der "Darstellung" vorgezogen, weil es anders als der letztgenannte Begriff suggeriert, nicht nur um Texte und deren Bildschirmausgabe geht. Signierte Daten können ebenso gut Tonaufnahmen, Bilder, Videos, Programme und Kombinationen davon sein. Es ist gut vorstellbar, dass ein Telefongespräch mit einem Callcenter abgespeichert und dann von beiden Partnern als Kaufvertrag behandelt und signiert wird, ohne jemals in einen Text umgesetzt worden zu sein. Außerdem vernachlässigt der Begriff "Darstellung" den wichtigen Aspekt der **Interaktion**. Bereits bei der Textbetrachtung tritt der Nutzer über Befehlsfunktionen in Interaktion mit dem signierten Dokument als Betrachtungsgegenstand und bestimmt diesen. Multimediale Dokumente können noch viel weitergehende Interaktionsmöglichkeiten beinhalten, vom interaktiv angepassten Formular bis zur parametergesteuerten nutzerabhängigen Textgenerierung und Modellsimulation.²⁶

Auch der **Ausdruck** signierter Daten ist im hier definierte Sinne eine Präsentation und im Prinzip nicht anders zu behandeln als etwa eine Bildschirmpräsentation.

Neben Daten wird häufig der Begriff des **elektronischen Dokumentes** verwendet. Unter einem elektronischen Dokument wird nach den o.g. Definitionen eine Einheit von Daten verstanden, die anhand einer formalen Bedeutungszuordnung (formatierte Daten) oder einer zugeordneten Präsentation (unformatierte Daten) interpretiert wird (elektronisches Dokument = Daten + Semantik| Präsentation. Ein elektronisches Dokument kann auch aus mehreren signierten Teildokumenten bestehen, die eine innere Struktur aufweisen. Dieser Aspekt wird hier noch nicht näher untersucht.

2.2 Technischer Ablauf einer Präsentation

Die Präsentation von signierten oder unsignierten Daten durch ein Computersystem auf einem Ausgabemedium verläuft im Wesentlichen in den folgenden Schritten:

1. Auswahl der Daten und Programmstart

Der Benutzer (Signierer, Prüfer) ruft das Präsentationsprogramm auf und wählt die zu präsentierenden Daten oder eine Datei aus, falls es nicht eine feste Bindung eines Programmes an Daten gibt. Alternativ dazu steuert der Nutzer über einen Dateimanager eine Datei an. In die-

²⁵ S. § 14 SigG.

²⁶ S. hierzu Beiträge in Roßnagel / Schröder 1999.

sem Fall entscheidet das Betriebssystem anhand seiner Konfigurationsdaten, welches Anwendungssystem zu starten ist (in Windows-basierten Systemen über die Dateierweiterung, ähnlich auch bei eingebetteten Dokumenten). Das Betriebssystem lädt das Programm, übergibt ihm die Daten und die Steuerung des weiteren Ablaufs.

2. Technische Interpretation der Daten

Das Anwendungsprogramm prüft das Format der Daten anhand von in der Datei vorhandenen Kennungen oder indem direkt ein Parser gestartet wird. Fremdformate gängiger Standardprodukte werden dabei unter Umständen automatisch erkannt und in das Format des Anwendungsprogramms konvertiert. Ein nicht erkanntes Format wird abgewiesen. Die so erhaltenen Daten werden in eine logische Datenstruktur, d.h. eine vom Anwendungsprogramm verarbeitbare Form umgesetzt. Für den Fall der ausschließlich programmierten Auswertung (etwa automatisierte Bearbeitung voll standardisierter Geschäftsdokumente) wird nun ein technischer Prozess der Weiterverarbeitung angestoßen. Für den hier interessierenden Fall der Verarbeitung durch Menschen folgen weitere Schritte.

3. Aufbereitung zur Ausgabe (Layouterstellung)

Aus der logischen Dokumentdatenstruktur erzeugt das Anwendungsprogramm wiederum Daten für eine bestimmte Form der Ausgabe (Druckerausgabe, Bildschirmausgabe, etc.). Neben den im Dokument vorhandenen Daten können weitere Daten und Benutzereingaben hierzu herangezogen werden. Das Ergebnis des Schritts kann logische Präsentationsdaten genannt werden.

4. Aufbereitung zur Geräteausgabe

Die Präsentationsdaten werden einem Gerätetreiber des Betriebssystems übergeben und von diesem für das Gerät aufbereitet. Hierbei kann es sich auch um virtuelle Gerätetreiber handeln, die die Daten nicht direkt ausgeben, sondern für die spätere Ausgabe speichern oder weiterverarbeiten.

5. Übergabe an die Hardware

Das Betriebssystem übergibt die Daten der internen Hardwaresteuerung (bei PCs das BIOS), die sie an die Hardware des Gerätes (z.B. Grafikkarte) weiterleitet, wo sie gegebenenfalls erneut zwischengespeichert werden (z.B. im Speicher der Grafikkarte). Dort erfolgt dann über Digital-/Analog-Wandler eine Aufbereitung der Daten in analoge Signale zur Endgerätesteuerung (z.B. der Kathodenstrahlröhre im Bildschirm).

6. Ausgabe

Schließlich erzeugt das Endgerät die analogen Reize (Bild, Ton, aber auch z.B. über Tastsinn erfahrbare Reize an einem Ausgabegerät für Braille-Schrift), die der Mensch wahrnehmen kann – oder auch nicht.

Die Schritte 2 und 3 können sich wiederholen, soweit die Präsentation - wie am Bildschirm, nicht aber z.B. beim Ausdrucken - ein **interaktiver Vorgang** ist. In diesem Fall erhält die Präsentation eine zeitliche Dimension. Im Falle von Text kann sie dann als zeitliche Abfolge von Einzelpräsentationen aufgefasst werden.

2.3 Präsentationskomponenten

Wie bereits aus dem Ablauf ersichtlich bestimmen folgende Komponenten eine Präsentation (in Klammern jeweils im engeren Sinne):

- **(Ausgabe)Geräte:** Dies sind die Ausgabegeräte (Drucker, Bildschirm,..), sowie die sonstige Hardware mit ihren physikalischen Eigenschaften.
- **(Präsentations)Programme:** Hierunter fallen die für die Präsentation verwendeten Programme, aber auch weitere zum Betrieb der Geräte erforderliche Programme, wie z.B. das Betriebssystem und Gerätetreiber.
- **Daten:** Dazu zählen die signierten Daten, aber auch weitere Dokumentdaten, etwa Links, sowie die Daten, die die Programme benötigen, insbesondere Konfigurationsdateien.
- **Benutzer:** Er bestimmt durch seine Interaktion, d.h. die Einstellung der Geräte, die Aktivierung von Programmen und Programmfunktionen, Scrollen usw. und die Auswahl von Daten die Präsentation.

Zu berücksichtigen ist ferner, dass das **Umfeld** die Präsentation und deren Wahrnehmung durch den Menschen bestimmt – etwa die Helligkeitsverhältnisse.

Ausgabegerät und Programme wären in der Terminologie des Signaturgesetzes bzw. der daraus abgeleiteten Maßnahmekataloge der sogenannten **Anwenderinfrastruktur** zuzuordnen.²⁷ Diese beinhaltet als zusätzliche Komponente dann noch ein Chipkartenlesegerät. Hingegen bezieht sich der in diesem Zusammenhang verwendete Begriff der "**Darstellungskomponente**"²⁸ zumeist nur auf eines der Programme, nämlich das Letzte, das der Nutzer startet, um Daten zu visualisieren. Die Darstellungskomponente wird hier Präsentationskomponente genannt, die Menge der technischen Komponenten, die die Präsentation bestimmen, Präsentationssystem.

2.4 Nachweis vermittelt einer Präsentation

Digital signierte Daten sollen Mittel zum Nachweis bestimmter Willens- und Wissenserklärungen vermittelt einer Präsentation sein. Bevor darauf näher eingegangen wird, inwieweit eine Präsentation selbst nachgewiesen werden muss, ist zunächst kurz darauf einzugehen, welche allgemeinen Beweisziele verfolgt werden, und wie sich die Präsentation hierin einordnet.

²⁷ Maßnahmekatalog nach § 16 (6) SigV Version 1.0, vom 12.2.98, Kapitel 1.6, BSI-Handbuch 1998, 199 ff.

²⁸ Gleichwohl ist eine Definition des Begriffs bislang nicht bekannt.

2.4.1 Allgemeine Nachweisziele

Werden signierte Dokumente als Beweismittel eingesetzt, um bestimmte Willens- und Wissenserklärungen nachzuweisen, so wird die Urkunde in der Praxis heute vornehmlich für den Nachweis folgender Aspekte verwendet:

- **Identifizierung des Urhebers**, anhand der Angaben im Dokument und der Unterschrift
- **Bestimmung des Inhalts** der Erklärung, durch lesen, und den interpretativen Rückschluss auf das "Gemeinte", den eigentlichen Willen also.
- **Erklärungswille**: In einigen Fällen interessieren die inneren physischen Umstände (mit vollem Bewusstsein, unter Drogeneinwirkung) sowie die inneren psychischen Umstände (freiwillig, voreilig, unter Zwang).

Neben den genannten Hauptnachweisfragen interessieren weitere Umstände z.B. Zeit bzw. Altersbestimmung, die hier nicht näher betrachtet werden. Es gibt auch Dinge, an die man nicht im Voraus denkt, und die sich einfach aus den medienspezifischen Möglichkeiten, der Existenz des Beweismittels und den Interessen der Beteiligten ergeben (z.B. Nachweis der äußeren Umstände, dass auf einem Autodach unterzeichnet wurde, um ein Alibi zu widerlegen, man sei zu hause gewesen)

Nachweis bei Papierurkunden

Zunächst lohnt ein kurzer vergleichender Blick auf Papierurkunden. Der Nachweis, dass eine bestimmte Willenserklärung vorliegt, erfolgt bei Papierurkunden zunächst schlicht dadurch, dass man

- die Urkunde liest bzw. sich ansieht und den Inhalt mitsamt seiner äußerlichen Form ganzheitlich intuitiv bewertet,
- aus dem Text oder der Unterschrift den Verfasser entnimmt.

Forensische Methoden der Urkundenuntersuchung und der Schriftvergleichung²⁹ liefern die Mittel, um Verfälschungen des Inhaltes und Fälschungen der Unterschrift zu erkennen. Sie können auch in einigen Fällen Hinweise auf die Umstände der Erzeugung der Willenserklärung geben.³⁰ So lässt sich aus Veränderungen im Schriftbild auf Alkoholeinflüsse, Zwang oder sonstige den freien Willen beeinflussenden Umstände schließen. Zumindest um den Inhalt zu erschließen und zu interpretieren bedarf es in der Regel jedoch keines technischen Gerätes und auch keines Sachverständigen.

Der Nachweis von Willenserklärungen und Wissenserklärungen mit signierten Dokumenten verläuft jedoch aufgrund deren medienspezifischer Besonderheiten zwangsläufig anders. Kein einziger Nachweisschritt kann ohne die Zuhilfenahme technischer Leistungen und einer dahinterstehenden technisch-organisatorischen Infrastruktur geführt werden. Ondarza hat aus rechtlicher Sicht hierfür den wichtigen Begriff der **Fremdleistungen** im Gegensatz zu den bislang vorliegenden Eigenleistungen der handschriftlichen Unterschrift geprägt.³¹

²⁹ Michel 1982 und Rieß 1989.

³⁰ S. hierzu die vergleichende Untersuchung zur Begutachtung handschriftlicher und elektronisch signierter Dokumente Pordesch / Nissen CR 1995.

³¹ Ondarza 1999.

2.4.2 Unversehrtheit und Urheberschaft der Rohdaten

Die technische Prüfung des Authentikators der Signatur weist zunächst nach, dass die Daten seit dem Signiervorgang unverfälscht blieben. Die Prüfung der Zertifikate ermöglicht den Nachweis, dass eine bestimmte Person signiert hat. Diese Nachweise stehen unter zahlreichen Einschränkungen und Vorbehalten – etwa dem, dass die Verschlüsselungsverfahren sicher sind und dass Zertifikate richtig erstellt und rechtzeitig eingetragen und gesperrt wurden.³² Daraus können und werden sich durchaus Fragestellungen für eine Sachverständigenbegutachtung ergeben, die aber an dieser Stelle nicht erörtert werden sollen. Vielmehr soll für diese Untersuchung davon ausgegangen werden, dass die Unversehrtheit und Urheberschaft *der Daten* geprüft und für bestätigt befunden ist.

Denn wäre bereits die Unversehrtheit der Daten umstritten, so würde man sich um deren Interpretation in der Regel kaum streiten. Daten, bei denen eine Signaturprüfung nicht zum Erfolg führt, sind für den Nachweis von Willenserklärungen praktisch so wertlos wie unsignierte Daten und es macht keinen Sinn über ihre Interpretation zu streiten. Sinnlos wird der weitere Nachweis in der Regel auch sein, wenn lediglich die Urheberschaft der Daten nicht zu klären ist, weil mit einer abstrakten Erklärung ohne Erklärenden kaum etwas zu beweisen ist.³³

Steht fest, dass signierte Daten unverfälscht sind und von wem sie stammen, so steht damit allerdings noch nicht fest, welche Willenserklärung sie darstellen. Die Daten müssen erst aufbereitet und ausgegeben werden. Zur Verdeutlichung dieses Aspekts erscheint es sinnvoll, vom Nachweis der Unversehrtheit und Urheberschaft von **Rohdaten** zu sprechen. Nur dieser erste Schritt wird mit der Signaturprüfung bislang wirklich durchgeführt.

2.4.3 Interpretation vermittelt einer bestimmten Präsentation

Da die signierten Bitstrings unmittelbar nicht wahrnehmbar und mithin auch nicht interpretierbar sind, müssen sie präsentiert werden. Der Nachweis der Interpretation muss *immer* über eine physische Präsentation erfolgen - jedenfalls solange noch Menschen Nachweise führen und Menschen und Maschinen nicht direkt verdrahtet werden. Selbst im Falle vollformatierter Willenserklärungen (Beispiel 1-bit-Willenserklärung mit der vereinbarten Bedeutung "Ich schulde X 100000 DM") muss wenigstens dieses Bit noch erfahrbar gemacht werden, nachdem die Signaturprüfung erfolgreich verlief. Wie gesagt kommt es aber auf die Form der Darstellung hier in der Regel nicht an, ob also z.B. der Text "Ich schulde X 100000 DM" angezeigt wird oder nur "ja", ist unerheblich, solange die Bedeutungszuordnung dieser Präsentation geklärt ist.

Liegen aber unformatierte Daten vor, dann kommt es für die Ermittlung des Inhaltes der Willenserklärung durch Interpretation auf die exakte Präsentation von vielerlei Aspekten an. Zu klären ist hier aber, welche Aspekte dies sind und woran sich die Exaktheit bemessen soll.

³² Bertsch / Pordesch DuD 1999, Roßnagel / Pordesch Kommentar zu § 14 SigG, 1999 und Grimm / Pordesch Spektrum der Wissenschaft 1998.

³³ Hier kann man sich freilich Ausnahmen vorstellen, etwa wenn man die existenz anonymer Drohungen nachweisen möchte, um eigenes Verhalten (illegales Besorgen einer Schußwaffe) zu rechtfertigen.

Bestimmung der anzuwendenden Präsentation

In dieser Arbeit wird folgender zur Bestimmung der anzuwendenden Präsentation rechtlich nahe liegender Ansatz verfolgt (und später dann auch aufgegriffen):

- 1) **Geregelte, vereinbarte Präsentation:** Gibt es eine gesetzliche oder andersweitig rechtlich bindende Vorschrift, die bestimmten Daten eine bestimmte Präsentation zuordnet, so gilt in vielen Fällen diese.
- 2) **Vom Signierer intendierte Präsentation:** Hat der Signierer seinen Willen zu erkennen gegeben, dass er eine bestimmte Präsentation der signierten Daten durch den/die Erklärungsempfänger wünscht, so ist diese zu erzeugen.
- 3) **Vom Signierer vorgenommene Präsentation:** In einigen Fällen – insbesondere bei der Klärung der absichtlichen Abgabe einer Willenserklärung – dürfte es auf die tatsächliche Präsentation des Signierers im Rahmen des Signiervorgangs³⁴ ankommen. Diese ist dann zu rekonstruieren.

Gibt es nur Interpretationsvorschriften und keine Präsentationsvorschrift, so ist eine geeignete Präsentation abzuleiten. Unter welchen Umständen genau welche der drei Präsentationen die objektive Beweisgrundlage darstellt und bei Widersprüchen welche in welcher Reihenfolge, muss im Detail einer juristischen Untersuchung vorbehalten bleiben.

Logische und physische Präsentation

Die ersten beiden anzuwendenden Präsentationsbestimmungen unterscheiden sich von der dritten. Während in letzterem Fall eine in Realität stattgefundene, tatsächliche Präsentation an einem Ausgabegerät nachzuweisen ist, existiert in den anderen beiden Fällen nicht notwendigerweise eine solche Vergleichsgrundlage. So ist im Bestimmungsfall "intendierte Präsentation" nicht notwendigerweise eine Präsentation tatsächlich auch erfolgt. Der Signierer kann (z.B. aus Zeitgründen) auf eine Präsentation verzichten haben, die Präsentation existiert dann nur als gedankliche bzw. geäußerte Präsentationsvorschrift. Im Bestimmungsfall "geregelte Präsentation" darf man davon ausgehen, dass eine spezifizierte Präsentationsvorschrift vorliegt oder eine Interpretationsvorschrift, aus der sich eine mögliche Präsentation ableiten lässt. In den beiden Fällen existiert also eine gedankliche oder codifizierte Präsentationsvorschrift und es geht darum, daraus eine Präsentation zu erzeugen - nicht etwa eine bereits einmal existierende zu reproduzieren.

Zur Unterscheidung ist es zweckmäßig, die an einem bestimmten Gerät zu einem bestimmten Zeitpunkt tatsächlich erfolgte Präsentation **physische Präsentation** zu nennen. Das geäußerte oder informell beschriebene Gedankenkonstrukt wird **Präsentationsvorschrift** genannt. Insbesondere wenn es für ein Computersystem codifiziert ist, erscheint **logische Präsentation** ein zweckmäßiger Begriff zu sein. Informatisch ist nahe liegend, dass die logische Präsentation signierter Daten die physische möglichst genau bestimmen soll, da es sonst zu Mehrdeutigkeiten kommen kann – worauf später näher einzugehen ist.

³⁴ D.h. normalerweise i.S. des Signaturgesetzes (s.u.) unmittelbar vor dem Signiervorgang. Es kann auch längere Zeit vorher gewesen sein, wenn das Dokument erst erstellt und später signiert wird. Relevant ist der denklogische Zusammenhang im Sinne des Signierers.

Statische und dynamische Präsentation

Anders als bei herkömmlichen Dokumenten ist bei elektronischen immer auch die Interaktion des Nutzers mit dem Präsentationssystem während der Präsentation zu berücksichtigen. Schon mehrseitige Textdokumente erfordern wenigstens eine Funktion zum Blättern (z.B. scroll-Fenster oder Menübefehl "Nächste Seite"). Von inhaltsverändernden Funktionen zu schweigen. Auch die zur Verfügung stehenden Funktionen sind wichtig, wenn beurteilt werden soll, wie eine Willenserklärung verstanden werden kann. Neben dem Layout sind auch die zur Verfügung stehenden Funktionen also objektive Grundlage zur Bestimmung des Inhalts.

Daneben interagiert der Nutzer mit diesen Funktionen, um eine Präsentation zu erzeugen. Diese Interaktion ist geeignet, Aspekte der Autorisierung nachzuweisen (insbesondere die vollständige aktive Kenntnisnahme des Inhaltes durch den Signierer). In der Papierwelt ist ein solcher Nachweis nicht möglich und man bedient sich verschiedener "Hilfskrücken": Beim Testament ist z.B. die vollständige Handschriftlichkeit gefordert. Ein von Polizeibeamten aufgenommenes Geständnis muss verlesen werden, bevor es der Beschuldigte unterschreibt. In Formularverträgen finden sich häufig Erklärungen wie "ich bestätige hiermit die dass ich ... gelesen habe". Die Möglichkeit, die Interaktion im technischen Medium nachzuweisen könnte also (bedingt) geeignet sein, in solchen Fällen auch Aspekte der Autorisierung, wie die Kenntnisnahme nachzuweisen. Berücksichtigt man, dass in elektronischen Systemen ein viel höheres Risiko besteht, Dinge versehentlich zu "unterschreiben",³⁵ könnte ein Nachweis des tatsächlichen Dialogs rechtlich gefordert werden (zumindest im Bestimmungsfall Vom Signierer vorgenommene Präsentation). Wahrscheinlich ist es ausreichend gewisse Eigenschaften des tatsächlichen Dialogs festzulegen (z.B. Vollständigkeit), dies ist aber noch gesondert näher zu untersuchen.

Zur begrifflichen Unterscheidung dieser Präsentationsformen wird **statische Präsentation** (im Falle von Text: Layout und Funktionen) und **dynamische Präsentation** (Ablauf nach einer ganz bestimmten Benutzung der Funktionen) vorgeschlagen.

2.4.4 Weitere Kontexte und Auslegung

Desweiteren ist auch der Verfahrenskontext innerhalb eines Geschäftsprozesses und anderen Dokumenten zu berücksichtigen, in dem das präsentierte signierte Dokument steht.

Der Vollständigkeit halber sei erwähnt, dass auch der Nachweis einer Präsentation noch immer kein vollständiger Nachweis einer bestimmten Willens- oder Wissenserklärung ist. Vielmehr ist er die Voraussetzung dafür, zwischen Menschen eine gemeinsame Basis für einen möglichen Streit um die "richtige" Auslegung bzw. die inhaltliche Bedeutung überhaupt führen zu können, wie man es vom Papier her kennt. Sie ersetzt diesen Teil der Nachweisführung, mehr aber auch nicht.

2.5 Nachweis der Präsentation

Erst mit einer bestimmten Präsentation wird also möglich, was bei Papierurkunden mit der Verkörperung der darauf befindlichen Information per se gegeben ist: Dass sich nämlich nie-

³⁵ Siehe die Ergebnisse der Simulationsstudien provet / GMD 1994 sowie speziell Pordesch DuD 1993.

mand darüber streitet, was zu sehen ist, sondern nur, wie es zu bewerten und inhaltlich zu deuten ist.³⁶

Erhält die Präsentation diese zentrale Bedeutung innerhalb des Nachweises einer Willens- oder Wissenserklärung, so muss auch diese selbstverständlich in einem zu spezifizierenden Sinne korrekt sein. Neben dem Nachweis der Urheberschaft und Unversehrtheit der Rohdaten ist also auch die Korrektheit der Präsentation dieser Daten selbst nachzuweisen. Nach den o.g. Bestimmungsfällen bedeutet Korrektheit allgemein gesagt den Nachweis, dass eine bestimmte erzeugte Präsentation

- **einer zuzurechnenden logischen Präsentation** entspricht, in Fällen, in denen die tatsächliche Präsentation keine Rolle spielt, sondern statt dessen eine vereinbarte, gesetzlich geregelte oder aus anderen Gründen gültige.
- **der physischen Präsentation des Signierers**, um nachzuweisen, was dieser tatsächlich signieren wollte³⁷

³⁶ Frühestens wenn der Nachweis einer eindeutigen Präsentation gelingt, macht es wirklich Sinn wesentliche Beweiserleichterungen, insbesondere die Einführung eines elektronischen Urkundsbeweises, bzw. Beweisregelungen wie beim Umgang mit Papier, ernsthaft ins Auge zu fassen.

³⁷ Teilfragestellung für den Nachweis der Autorisierung, Bizer/Hammer 1993.

3. Risiken

In diesem Kapitel wird untersucht, in welcher Hinsicht Präsentationen verfälscht sein können, um die Notwendigkeit eines Nachweises der Präsentation und seine Zielrichtung aufzuzeigen. Dabei wird in Anlehnung an übliche Gefährdungsanalysen untersucht, welche der die Präsentation bestimmenden Komponenten (Daten, Software, Hardware, Nutzer, sowie das Umfeld) für solche Effekte verantwortlich sein können. Diese Untersuchung erfolgt getrennt für die beiden Hauptrisiken der Falschpräsentation und der Mehrdeutigkeit. Danach werden mögliche Effekte, die Ausgangspunkt rechtlicher Streitigkeiten sein könnten, anhand von Beispielen aus der Textkommunikation aufgezeigt.

3.1 Präsentationsrisiken

3.1.1 Teilrisiken

Als Risiko der Präsentation wird nach der obigen Definition also verstanden, dass zwei Präsentationen signierter Daten so voneinander abweichen, dass sie bei einem Menschen andere Interpretationen der präsentierten Willens- oder Wissenserklärung verursachen. Dieses Risiko kann hinsichtlich der Ursachen recht klar in **Teilrisiken** unterschieden werden:

- **Falschpräsentation** (der Daten): Signierte Daten werden aufgrund von Fehlern in oder Angriffen auf das zum Präsentieren verwendete System (Anwenderinfrastruktur) falsch präsentiert und in Folge dessen durch Menschen auch falsch interpretiert. Dies setzt ein Einverständnis darüber voraus, wie eine Präsentation richtig zu erfolgen hätte, also i.d.R. eine eindeutige soziale Regelung oder eine technische Interpretationsvorschrift.
- **Mehrdeutigkeit** (der Daten): Zwei Präsentationen weichen aufgrund von Unterschieden der verwendeten Präsentationssysteme und ihrer Bedienung voneinander ab, ohne dass es explizite technische oder soziale Regeln gibt, nach denen eine Präsentation als "richtig" und eine andere als "falsch" zu bezeichnen wäre.³⁸

Neben diesen beiden Risiken können weitere identifiziert werden, die die Inhalte der Präsentation und ihre Wahrnehmung betreffen. Der Fall kann eintreten, dass die physische Präsentation unumstritten ist, dass jedoch der Inhalt der Präsentation dennoch verschieden interpretiert werden kann oder überhaupt nicht interpretierbar ist. Ein solches Risiko ist bereits bei den Papiermedien bekannt – unklare Verträge sind häufig gerichtlicher Streitgegenstand –, durch elektronische Medien gibt es jedoch zusätzliche Probleme durch die Vervielfachung der elektronischen Ausdrucksmöglichkeiten und deren unqualifizierter Anwendung. Zum anderen können die spezifischen Wahrnehmungsmöglichkeiten des Menschen so eingeschränkt sein, dass er die Präsentation nicht richtig wahrnehmen kann. So kann es vorkom-

³⁸ Die Unterscheidung in Falschpräsentation und Mehrdeutigkeit ist nicht immer klar. Ob Regeln vorliegen oder nicht kann durchaus umstritten sein, vor allem wenn es sich um informelle Vereinbarungen handelt (siehe unten Teil II:5.2.4 Mehrdeutigkeit oder Falschpräsentation?). Die Unterscheidung basiert also letztlich auf einem sozialen und keinem rein technischen Kriterium. Der Rückgriff auf soziale Kategorien ist in der IT-Sicherheit unvermeidlich, wenn man sich nicht nur mit Ausfallwahrscheinlichkeiten u.ä. befassen möchte.

men, dass ein Mensch behindert ist, etwa dass er schlecht sieht, oder dass seine Wahrnehmung temporär z.B. Alkoholkonsum eingeschränkt ist.

Solche Risiken sind weitestgehend unabhängig vom Medium existent (Papier oder Computer), die Computertechnologie verändert jedoch die Risiken und schafft z.T. auch Möglichkeiten zur Problemlösung z.B. über nutzerangepasste Präsentationen. Wahrnehmungsfragen und inhaltliche Aspekte betreffen nicht direkt den Nachweis der Präsentation. Sie sind aber bei der Gestaltung von Präsentationssystemen oder –komponenten zu berücksichtigen, die nicht nur an der Nachweismöglichkeit orientiert werden kann.

3.1.2 Wesentliche Aspekte

Schon die grobe Beschreibung der Abläufe macht deutlich, dass das was letztlich am Ausgabegerät präsentiert wird, nur zu einem kleinen Teil von den eigentlich signierten Daten abhängt, sondern auch von der Wirkungsweise der Programme, den Systemeinstellungen, der Systembedienung durch den Benutzer, den technischen Eigenschaften der Ausgabegeräte bis hin zu deren äußerem Zustand ist. Eine Präsentation ist deshalb ein orts- und zeitgebundener Vorgang, der niemals in allen Details wiederholbar und auch nicht vollständig formal beschreibbar ist.

Wenn aber alle Präsentationen bestimmter Daten per se unterschiedlich verlaufen, so erhebt sich die Frage, wie man überhaupt sinnvoll von einem "Risiko unterschiedlicher Präsentation" sprechen und wie man eine Präsentation nachweisen soll. Die Antwort ist, dass nicht die völlige Gleichheit von Präsentationen interessiert, sondern deren Gleichheit bzw. Ungleichheit in wesentlichen Aspekten.

Wesentlich ist eine Abweichung, wenn sich zwei Vergleichspräsentationen so stark unterscheiden, dass sie bei einem Menschen zu anderen Interpretationen und in Folge zu Missverständnissen und Schäden führen. Besonders relevant sind solche Abweichungen, die zu unterschiedlichen Auslegungen des Inhaltes der Daten im Gerichtsprozess führen.

3.2 Mehrdeutigkeiten

Mögliche Ursachen für Präsentationsunterschiede sind nicht nur beabsichtigte oder unbeabsichtigte menschliche Fehlhandlungen. Vielmehr ist auch an "normale" Unterschiede der von den Nutzern ausgewählten Programme oder Geräte, sowie deren Konfiguration und Benutzung zu denken. Hier handelt es sich weder um menschliche Fehler noch um höhere Gewalt oder gar Angriffe, sondern um Unterschiede, die aufgrund fehlender konkreter Vorgaben als zulässig bzw. normal zu betrachten sind.³⁹

³⁹ Das Risiko der Mehrdeutigkeit paßt nicht gut in gängige Klassifikationssysteme für Ursachen technischer oder sozialer Schäden (wie z.B. Roßnagel / Wedde / Hammer / Pordesch 1979). Am ehesten könnte man sie in eine Kategorie "organisatorische Mängel" (BSI 1996) einordnen, was allerdings eine Organisation voraussetzt, die in der offenen Telekooperation vielfach fehlt.

3.2.1 Hardware

i) Andere Ausgabegerätekonfiguration

Eine mögliche Ursache für Mehrdeutigkeiten signierter Daten kann darin liegen, dass für die Präsentation Ausgabegeräte mit unterschiedlichen Eigenschaften eingesetzt werden oder deren Ausgabeigenschaften unterschiedlich voreingestellt sind.

Die Geräte können zum einen unterschiedliche **Leistungsmerkmale** aufweisen. Bei Bildschirmgeräten ist zunächst an die Verwendung von Geräten mit unterschiedlichen **Farbeeigenschaften** zu denken. Je nach Gerät können eingefärbte Text- und Bildteile unleserlich werden, Hervorhebungen verlorengehen oder verstärkt werden. Auch die **Bildschirmauflösung** kann im Einzelfall eine Rolle spielen, etwa wenn das Dokument hochauflösende Grafiken enthält, weil z.B. davon abhängt, ob Linien noch sichtbar sind oder nicht (man denke z.B. an Durchstreichungen). Ein wichtiger Faktor ist die **Bildschirmgröße**. Ein Dokument ist auf einem kleinen Palmtop- oder gar Handy-Bildschirm trotz möglicherweise hoher Auflösung völlig anders wahrnehmbar als etwa auf einem 21 Zoll-Monitor. Bei Tondokumenten wäre an Geräte mit einem unterschiedlich leistungsfähigem Soundsystem zu denken, die bestimmte Tonlagen unterschiedlich deutlich wiedergeben, bei Bewegtbildern kann z.B. die Bildwiederholfrequenz eine Rolle spielen.

Wichtig sind schließlich die **Einstellungen**. Je nach **Helligkeit, Farbmischung und Kontrast** können farbliche und konturmäßige Hervorhebungen verstärkt oder abgeschwächt bzw. ausgeblendet erscheinen. Auch **Größe** und **Größenverhältnis** des Bildes, sowie seine Ausrichtung können sich auf die Wahrnehmbarkeit des Inhaltes auswirken.

Ursache der unterschiedlichen Einstellungen können neben den Hardwareeigenschaften der Geräte, die Verwendung unterschiedlicher Treiber, sowie deren Konfiguration und die Regelung über Schalter am Endgerät sein. Diese können in Abhängigkeit von den Vorlieben der Benutzer beträchtlich abweichen.

ii) Andere Eingabegerätekonfiguration

Bei interaktiven Medien (insbesondere hypermedialen Dokumenten) entscheiden auch die Eingabemöglichkeiten darüber, wie eine Präsentation erfolgt.

Eine Mouse mit Rollrad ermöglicht ein schnelles Durchblättern und zielgenaues Ansteuern großer Textdokumente. Fehlt umgekehrt eine Mouse, kann nur umständlich mit Tasten navigiert werden und Software-Buttons sind eventuell überhaupt nicht ansteuerbar. In einem solchen Fall können u.U. im Präsentationsprogramm vorgesehene Navigationsmöglichkeiten nicht genutzt werden und Teile eines Dokumentes sind deshalb nicht zugänglich.

Auch hier liegen die möglichen Ursachen nicht nur in der Hardware, sondern auch in der Softwarekonfiguration (Treiber, Einstellung, etc.).

iii) Andere Hardwareleistung

Dokumente, die besonders groß sind oder komplizierte Berechnungen beinhalten, stellen hohe Anforderungen an die Rechnerleistung. In solchen Fällen hängt die Präsentation von der für den Prozess verfügbaren Rechenzeit und dem verfügbaren Speicherplatz des verwendeten

Rechners ab, sowie gegebenenfalls weiteren Faktoren, wie der Datenübertragungsrate zum Netz (externe Dateien, Serveranwendung).

Je nach Rechner, Einstellung und gerade parallel laufenden Prozessen kann die Ausgabe unterschiedlich stark verzögert werden. Im Fall von Textdokumenten können insbesondere bei langen Texten, komplexen Verweisstrukturen und umfangreichen Grafiken Probleme beim Bildaufbau eintreten. Die Darstellung erfolgt dann zunächst unvollständig. Fehlende Teile können beim "schnellen Durchgehen" möglicherweise nicht bemerkt werden.

3.2.2 Software

i) (Daten)Formatkollision

Die Präsentation hängt davon ab, mit welchem Programm signierte Daten interpretiert und ausgegeben werden. Programme haben für gewöhnlich ihre eigenen Datei- und Datenformate, die, da sie von den Herstellern bzw. ihren Programmierern frei gewählt wurden, völlig voneinander abweichen. Der Versuch, die mit einem Programm erzeugten Daten durch ein anderes zu laden, wird dann scheitern. Schlimmstenfalls stürzt das Programm ab. Ist das Dokument jedoch so aufgebaut, dass seine Daten mehreren Formaten entsprechen (Formatkollision), so können sie auch von mehreren Programmen verarbeitet und dann völlig unterschiedlich präsentiert werden.

Eine Kollision liegt immer zu "primitiven" Datenformaten vor, d.h. Programmen, die alle Bitfolgen als zulässige Daten akzeptieren, wie ASCII – oder einfachen HEX-Editoren, beide Teil vieler Betriebssysteme. Im Regelfall ist dann ein unsinnig erscheinender "Text" zu sehen. Sinnvoll erscheinende Kollisionen und insbesondere "höherwertige" Formatkollisionen zwischen gängigen Datenformaten sind unwahrscheinlich, können aber (mühsam) konstruiert werden. Bei proprietären Anwendungen, etwa unternehmensinternen Anwendungen, die vielleicht auf gängigen Formaten aufbauen oder bei kurzen wenig redundanten Bitstrings sind sie aber nicht auszuschließen.

Die Daten einer Urlaubskarte liegen auf einem UNIX-Server in einer Datei in einer ASN.1 codierten Form vor. Sie sind nicht direkt, bzw. nur von einem ASN.1-Viewer oder einem Hex-Editor lesbar. Der ASN.1-Viewer stellt dann die Inhalte sichtbarer und unsichtbarer Felder dar, nicht jedoch die im Formular angezeigten Feldbezeichnungen. Diese werden durch das Anwendungsprogramm vorgegeben.

Bei dem Netscape-Messenger werden alle eingehenden Nachrichten in spezielle Folderdateien in komprimierter Form abgespeichert. Nur dieses Programm kann die Daten interpretieren.

Word zeigt ein Format, das es nicht erkennt als ASCII-String (nur Text) an oder weist es ab. Bestimmte Word-Viewer akzeptieren jedoch jeden Bitstring.

ii) Andere Präsentationsprogramme

Auch wenn das Datenformat feststeht, so noch nicht notwendigerweise das zu verwendende Programm. Die gängigen Standardprogramme, wie Word, WordPerfect, StarOffice usw. können von anderen gängigen Programmen erzeugten Daten wechselseitig lesen und auch Daten in diesen Fremdformaten abspeichern.

Außer umfangreichen Verarbeitungsprogrammen können jeweils noch abgespeckte "Viewer"-Programme der Hersteller eingesetzt werden, die nur wenige Funktionen und ausschließlich zur Betrachtung anbieten (z.B. der Word-Viewer statt des Anwendungsprogramms Word). Schließlich unterscheiden sich die Versionen ein und desselben Programmes beträchtlich.

Je nachdem welches Programm welcher Version als Präsentationssystem eingesetzt wird, können sich große Unterschiede ergeben. Ursache für die Abweichungen zwischen verschiedenen Programmen sind zum einen, dass einige Aspekte der Präsentation in technischen Spezifikationen von Datenformaten **nicht festgelegt** werden. Im Allgemeinen nicht festgelegt werden beispielsweise Funktionen zur Navigation, zur Inhalterschließung mittels Suchfunktionen, sowie Detail- und Überblicksansichten. Große Unterschiede bestehen beispielsweise zwischen dem komplexen Textverarbeitungsprogramm Word mit seinen zahlreichen Ansichtsmöglichkeiten und dem vergleichsweise sehr abgespeckteren Wordviewer. Zum anderen gibt es - beabsichtigt oder unbeabsichtigt – **Spezifikationslücken** oder -unklarheiten, die die Hersteller unterschiedlich interpretieren und ausfüllen. Auf diese Weise werden bestimmte Elemente nicht oder anders dargestellt. So gibt es zwischen dem Netscape Navigator und im Internet Explorer beispielsweise feine Unterschiede in der Darstellung von Zeilenabständen und den Inhalten von Formularauswahlfenstern.⁴⁰ Schließlich ist die oft **fehlende Dokumentation** der proprietären Dateiformate wohl Ursache für Abweichungen, weil die Bedeutung bestimmter Formateile dann unbekannt ist und deshalb ignoriert oder falsch interpretiert wird.

iii) Andere Programmbedienung

Über **Optionen** des Anwendungssystems beeinflusst der Anwender die Ausgabe signierter Daten. So kann z.B. im Word-Viewer eingestellt werden, ob Zeichnungen und nicht druckbare Zeichen angezeigt werden sollen, ob Grafiken oder nur Platzhalter angezeigt werden, und ob Feldfunktionen angezeigt werden sollen. Es macht bereits einen großen Unterschied, ob eine Skizze in einem zu signierenden Vertragsentwurf angezeigt wird, oder nur als, möglicherweise stark verkleinerter, Platzhalter.

Alle Standardprogramme bieten verschiedene Möglichkeiten Dokumente in verschiedenen **Überblicks- oder Ausschnittsdarstellungen** auszugeben und Einzelaspekte gezielt zu zoomen. Am weitestgehenden ist hier Word, das von der druckerorientierten Seitenansicht, über Normal-, Online-, Gliederungs- und Seitenlayoutsansicht etc. eine auch für Experten kaum mehr verständliche Fülle von Ansichtsmöglichkeiten der Daten bietet.⁴¹

Im Falle der GMD-Urlaubskarte wird der Hintergrund von der Anwendung vorgegeben und soweit sie dort als transparent gekennzeichnet sind von der grafischen Benutzeroberfläche des Windows-Betriebssystems.

Beim Netscape-Messenger kann der Sender einer HTML-Mail die Hintergrundfarbe vorgeben, wenn er möchte, sie ist dann Teil des gesendeten Dokumentes (ist allerdings beim Einsatz von PGP nicht mitsigniert, da hier nur der ASCII-Text signiert wird). Wird die Seitenfarbe nicht vorgegeben, so werden die Einstellungen des Browsers wirksam. Diese kann der Nutzer ändern, er kann auch angeben, die Einstellungen des Windows-Systems zu verwenden.

Word97 weist wiederum die meisten Einstellmöglichkeiten auf. Ohne Anspruch auf Vollständigkeit seien folgende genannt. Zum einen kann der Nutzer Schriftfarben für einzelne Zeichen im Dokument angeben, was mit der Dokumentdatei signiert würde. Desweiteren ist eine Angabe in der Dokumentvorlage möglich, wobei Änderungen in der Formatvorlage merkwürdigerweise nicht aktualisiert werden (dies mag bei der nächsten Version anders werden..) Darüber hinaus kann der Nutzer in den Optionen noch angeben, dass weiße Schrift auf blauem Hintergrund dargestellt werden soll. Werden Farben für Schriftzeichen und Hintergründe transparent eingestellt, so werden die Standardeinstellungen des Betriebssystems wirksam. Dies kann aber wiederum in den Optionen von Word überlagert werden. Die Anwendungsoption "weiß auf blauem Hintergrund" ändert Zeichenfarben in weiß und Hintergründe in blau, aber nur wenn beides jeweils transparent gefärbt ist, und auch nicht in allen Ansichtsmodi. Im Übrigen wird diese Einstellung nicht mit dem Dokument gespeichert, sondern gilt für die jeweilige Word-Session.

⁴⁰ Musciano / Kennedy 1997, 122.

⁴¹ Wobei es aber in eigenen Tests nicht gelang, von der Größe dem Druckbild entsprechende Bildschirmansicht zu finden.

iv) **Anderes Betriebssystem oder andere Konfiguration**

Büro- und Grafikprogramme (alle untersuchten Programme) greifen vielfach auf gemeinsam genutzte Zeichensätze zurück, die sich in den **Font-Verzeichnissen** des Betriebssystems befinden. Die signierten Daten bzw. Dateien enthalten zumeist nicht die Zeichensätze selbst⁴², sondern verweisen lediglich auf deren Bezeichnung (z.B. "Times New Roman"), so dass die Bildschirmpräsentation unter Verwendung der lokal gespeicherten Zeichensätze berechnet wird. Ist die Bezeichnung von zwei unterschiedlichen Zeichensätzen auf zwei unterschiedlichen Systemen gleich, so kann das Schriftbild dort, wo dieser Font verwendet wird, beträchtlich abweichen: Schrift erscheint kleiner oder größer, Sonderzeichen werden völlig anders dargestellt, Symbole oder Leerzeichen erscheinen, wo vorher ein lesbares Zeichen zu sehen war.⁴³ Ist ein im Dokument verwendeter Font nicht vorhanden, wird oft ohne Rückmeldung an den Benutzer ein Standardfont eingesetzt, wobei ähnliche Effekte auftreten können.

Im Falle der GMD-Urlaubskarte werden von der Anwendung der einzusetzenden Fonts angegeben. Die Fonts selbst sind (z.T.) lokal in Verzeichnissen des X-Window-Clients abgelegt und durch den Benutzer änderbar.

Bei HTML-Mail können einzusetzende Fonts vom Ersteller der Mail vorgegeben werden, ansonsten werden die Fonts verwendet, die der Empfänger für seinen Browsers eingestellt hat. Bei der Präsentation wird auf die in Windows-Verzeichnissen gespeicherten Fontdateien zurückgegriffen.

Bei Word können die verwendeten Zeichensätze im Dokument gespeichert (eingebettet) werden und wären dann mit der Datei signiert. Gewöhnliche Nutzer wissen nicht um diese Möglichkeit oder vermeiden dies (Fonts sind z.T. urheberrechtlich geschützt). Word und auch andere Textverarbeitungsprogramme und Grafikprogramme greifen deshalb unbemerkt auf die in den Windows-Verzeichnissen gespeicherten Zeichensätze zurück.

Bereits auf der Betriebssystemebene (bzw. für die grafische Benutzeroberfläche oder auch ein X-Windows-Fenster) lassen sich durch den Benutzer **Standardeinstellungen für Hintergrund und Textfarben** in Anwendungsfenstern festlegen. Solche werden als Standardeinstellung übernommen, wenn in der jeweiligen Dokumentdatei oder dem Anwendungsprogramm keine speziellen Einstellungen vorgenommen werden (bei Word).⁴⁴ Ein schwarzer Hintergrund lässt die gewöhnlich schwarze Schrift verschwinden, weiße Standardfarbe für Textzeichen erweckt den Eindruck einer leeren Datei. Auch die Größe, Form und Farbe von Fenstern, in denen das Dokument präsentiert wird, beeinflusst die Wahrnehmbarkeit des Dokumentinhaltes. Grenzen des Dokumentes und seines Inhaltes könnten dadurch verwischen, der Nutzer sieht möglicherweise nicht, was wirklich Dokumentinhalt ist und was eigentlich Teil der (nicht signierten) Dokumentumgebung zu sehen ist.

Im Falle der GMD-Urlaubskarte wird der Hintergrund von der Anwendung vorgegeben und, wenn dort als transparent gekennzeichnet, von der grafischen Benutzeroberfläche des Windows-Betriebssystems.

Beim Netscape-Messenger kann der Sender einer HTML-Mail die Hintergrundfarbe vorgeben, wenn er möchte, sie ist dann Teil des gesendeten Dokumentes (ist allerdings beim Einsatz von PGP nicht mitsigniert, da hier nur der ASCII-Text signiert wird). Wird die Seitenfarbe nicht vorgegeben, so werden die Einstellungen des Browsers wirksam. Diese kann der Nutzer ändern, er kann auch angeben, die Einstellungen des Windows-Systems zu verwenden.

Word weist wiederum die meisten Einstellmöglichkeiten auf. Ohne Anspruch auf Vollständigkeit seien folgende genannt. Zum einen kann der Nutzer Schriftfarben für einzelne Zeichen im Dokument angeben, was mit dem Dokument signiert würde. Desweiteren ist eine Angabe in der Dokumentvorlage möglich, wobei Änderungen in der Formatvorlage merkwürdigerweise nicht aktualisiert werden (dies mag bei der nächsten Version anders werden..). Darüber hinaus kann der Nutzer in den Optionen noch angeben, dass weiße Schrift auf blauem Hintergrund dargestellt werden soll. Werden Farben für Schriftzeichen und Hintergründe transparent eingestellt, so werden die Standardeinstellungen des Betriebssystems wirksam. Dies kann aber wiederum in den Optionen von Word überlagert werden. Die Anwendungsoption "weiß auf blauem Hintergrund" ändert Zeichenfarben in weiß und Hintergründe in blau, aber nur wenn beides jeweils transparent gefärbt ist, und auch nicht in allen Ansichtsmodi. Im Übrigen wird diese Einstellung nicht mit dem Dokument gespeichert, sondern gilt für die jeweilige Word-Session.

⁴² Dies hat auch vertrags- und urheberrechtliche Gründe.

⁴³ Funktionierte im Experiment gleichermaßen bei CORELDRAW und WORD97.

⁴⁴ Z.B. Schriftfarbe "Automatisch" bei Schriftfarbe oder "kein Füllbereich" beim Hintergrund in WORD 97. CORELDRAW 7.0 verfügt nicht über entsprechende Einstellmöglichkeiten.

3.2.3 Daten

i) Andere Vorlagen

Erfahrene Nutzer moderner Textverarbeitungssysteme benutzen selten die direkte Formatierung von Zeichen, Absätzen oder anderen Dokumentelementen, sondern symbolische Formatierungen, um ein einheitliches Layout zu erzeugen. Solche Layoutvorlagen können extern gespeichert werden (bei Word Dokumentvorlagen, bei HTML Cascading Stylesheets⁴⁵), um in mehreren Dokumenten stets ein gleichartiges Layout zu erzeugen. Bei entsprechender Einstellung werden die Layoutdaten für die Bildschirmpräsentation entsprechend der Vorlagen zur Laufzeit (d.h. beim Laden des Dokumentes) generiert. Das Erscheinungsbild hängt dann von der angebundenen Vorlagendatei oder auch mehreren solcher Vorlagendateien ab, die sich irgendwo im lokalen System oder im Netz befinden können. Benutzen Signierer und Prüfer unterschiedliche Vorlagen oder werden gemeinsam genutzte Vorlagen zwischenzeitlich geändert, so kann sich das Erscheinungsbild erheblich ändern.

Bei der GMD-Urlaubskarte werden nur die Inhalte des Formulars tatsächlich in einem ASN.1/BER-codierten Bitstring in der Datei Urlaubskarte gespeichert. Feldnamen, Grafiken und Feldbezeichnungen, die die Bedeutung der Felder wiedergeben, werden hingegen vom Anwendungsprogramm vorgegeben (und befinden sich wohl in einer Formatlayoutdatei). Sie werden bei der Präsentation automatisch ergänzt.

Im Falle von HTML-Mail (Netscape) sind keine automatischen Ergänzungen bekannt. Beim Netscape-Messenger gibt es im Composer neben der direkten Formatierung nur einige symbolische Absatz und Zeichenformate. Werden solche verwendet, so richtet sich die Formatierung nach den Einstellungen des Messenger (ladbare HTML-Stylesheets gibt es hier nicht).

Bei Word gibt es eingeschränkte Möglichkeiten Texte und andere inhaltsrelevante Bestandteile in der Präsentation automatisch zu ergänzen. So können Absatzformate, wie z.B. Überschriften, nicht nur um Nummern ergänzt werden, sondern auch um ganze Textpassagen. Solche Absatzformate können im Dokument selbst, aber auch in einer mit dem Dokument verknüpften Vorlage gespeichert werden, von wo aus die Dokumentpräsentation dann automatisch aktualisiert wird. Es ist einstellbar, ob das Dokument stets entsprechend der Vorlage aktualisiert wird. In den Layoutvorlagen kann auch eingestellt werden, welche Größe Absätze haben, welche Position auf einer Seite, welche Abstände von anderen und vieles mehr.

ii) Unklare externe Verweise

Dokumente können Links auf WWW-Seiten, extern abgespeicherte Grafiken und andere externe Objekte enthalten, die sich irgendwo auf dem lokalen System, einem angeschlossenen Rechnernetz oder im weltweiten Internet befinden. Sie können dann jederzeit gelöscht oder ausgetauscht werden, um eine Präsentation zu beeinflussen. Relative Verweise (etwa auf bestimmte Dateien in Verzeichnissen) können je nachdem, auf welchem System das Dokument präsentiert wird, zu unterschiedlichen Dateien führen und dann in einer Präsentation auch unterschiedlich dargestellt werden.

Word bietet umfangreiche (und bei jedem Versionswechsel und Service-Pack stets neue) Möglichkeiten, externe Objekte in die Präsentation einzubinden. Üblich sind Grafiken, Kalkulationstabellen oder Daten aus einer Datenbank, die sich lokal oder auf einem anderen Rechner innerhalb eines lokalen Netzes befinden. Auch WWW-Seiten irgendwo aus dem weltweiten Netz können hinzugeladen werden. Gewöhnlich wird ein Platzhalter für das Objekt vorgesehen oder eine Vorschaugrafik mit dem Dokument abgespeichert. In der Seitenlayoutansicht oder Seitenansicht kann das externe Objekt dann aktuell geladen werden.

Der Netscape-Messenger bietet die Möglichkeit, in einer Mail Links anzugeben, die dann beim Aufruf der Mail automatisch angesteuert und in der Präsentation als Teil des Dokumentes erscheinen. Der Inhalt der externen Quelle kann sich zwischen Signier- und Prüfzeitpunkt geändert haben.

⁴⁵ Musciano / Kennedy 1997, 251.

iii) Berechnungen

Je nach Anwendungssystem können Dokumente auch Datenelemente beeinhaltend, deren Inhalt erst mit dem Öffnen des Dokumentes in Abhängigkeit von Umgebungsbedingungen oder Benutzereingaben festgelegt wird. Beispiele hierfür sind aktualisierbare Felder, wie Seitenangaben, Datumsangaben, Makros und Programme und ereignisgesteuerte Buttons. Im Anwendungssystem Word können aktualisierbare Felder bei Wahl einer entsprechenden Optionen erkennbar gemacht werden, jedoch ist dies nicht Standardeinstellung und dem normalen Benutzer häufig unbekannt.

Word bietet u.a. die Möglichkeit, Datumsangaben (bei PDF unbekannt?) als aktualisierbar zu kennzeichnen. In diesem Fall wird ein entsprechendes Feld beim Aufruf des Dokumentes mit dem aktuellen Systemdatum des Betriebssystems gefüllt. Auch Seitenzahlen werden erst mit der Generierung des Layouts festgelegt. Ob ein Feld aktualisierbar ist, lässt sich hingegen nicht sofort erkennen. Eine spezielle Anzeigeoption ist dafür vorgesehen.

HTML-Mail kennt diese Möglichkeit nicht.

In der elektronischen Urlaubskarte sind ebenfalls keine berechneten Felder enthalten.

iv) Scripts

Durch in den Dokumenten enthaltene Makros, Scripts, Applets und andere Programmarten ergibt sich eine weitere Fülle von Quellen für Mehrdeutigkeit. Abhängig von Ereignissen (etwa Zeitgeber) oder Benutzereingaben können Formularteile ein- und ausgeblendet, Menüauswahlen neu zusammengestellt und die Präsentation dynamisch nahezu beliebig geändert werden.

3.2.4 Nutzer und Umgebung

Da die Präsentation wie oben beschrieben ein interaktiver Vorgang ist, ist das Verhalten des Nutzers während der Präsentation als Ursache von Mehrdeutigkeiten zu berücksichtigen.

Der Nutzer stellt Geräte ein, wählt Programme und Daten aus und soweit es mehrere Einstellungsmöglichkeiten gibt. Je nach der Art, wie er durch das Dokument navigiert und welche Eingaben er vornimmt kann sich die Präsentation ändern.

Die Umgebung kommt ebenfalls als Quelle von Mehrdeutigkeiten in Frage. Menschliche Wahrnehmung ist letztlich die Unterscheidung bestimmter Signale von einem Rauschpegel (Helligkeit, Hintergrundgeräusche, etc.). Was über ein Ausgabegerät für Menschen wahrnehmbar ist, hängt also von der Differenz zwischen Rauschpegel der Umgebung und den Signalen des Ausgabegerät ab. Ein mehrfarbiges Schriftdokument wird auf einem LCD-Bildschirm in einem passiv beleuchteten Raum anders wahrgenommen, als auf einem im freien stehenden Gerät abends im Laternenlicht, eine sprachliche Textannotation im ruhigen Zimmer anders als im Bahnhofsgebäude. Nicht immer gibt es ausgesprochene oder unausgesprochene Regeln unter welchen äußeren Bedingungen die Wahrnehmung zu erfolgen hat, so dass auch hier eine Mehrdeutigkeit vorliegen kann.

3.2.5 Schadensursachen

Die zuvor benannten potentiellen Mehrdeutigkeiten können unbemerkt bleiben, wenn die verwendeten Präsentationssysteme und die Bedienungsweisen hinreichend übereinstimmen. Aufgrund der häufigen Verwendung von (Quasi)-Standardsoftware - vor allem Microsoft - mit überwiegend ähnlichen Einstellungen und Benutzungsweisen ist dies auch häufig der Fall.

Tatsächliche Abweichungen in der Präsentation können aber aufgrund folgender Ursachen auftreten:

i) Zufälle

Mehrdeutigkeiten können zufällig auftreten. Mögliche Ursachen sind u.a. neuartige unerwartete Anwendungszusammenhänge (z.B. E-Mail auf Handy-Bildschirm), unterschiedlichen Traditionen (z.B. verschiedene Länder mit unterschiedlichen Zeichensätzen), eigentümlichen Vorlieben und Verhaltensweisen der Benutzer (z.B. Experte, "Freak", Anfänger).

ii) Angriffe

Am wahrscheinlichsten dürfte sein, dass mögliche Mehrdeutigkeiten von einem Angreifer gesucht, erkannt und dann gezielt ausgenutzt werden, um getätigte Willens- und Wissenserklärungen im Nachhinein abstreiten zu können und die Existenz nicht getätigter zu behaupten.

iii) Fehler

Eines lokales Präsentationssystem kann technische Fehler aufweisen oder sein Benutzer macht Fehler. Es ist eher unwahrscheinlich, dass ein zufälliger Fehler zusammen mit bestimmten Mehrdeutigkeiten auftritt.

3.3 Falschpräsentation

Die Ursachen voneinander abweichender Präsentationen sind nicht nur Mehrdeutigkeiten von Daten. Ebenso ist es möglich, dass bei Klärung der Umstände kein Zweifel daran besteht, wie die Daten richtig zu präsentieren gewesen wären und dass lokale Fehler oder Manipulationen der genutzten Anwenderinfrastruktur Ursache für die falsche Präsentation sind. Sicherheitstechnisch entspricht dieses Risiko weitgehend dem klassischen Risiko der Verwundbarkeit von IT-Systemen durch Manipulation und der Gefährdung der Integrität.⁴⁶

Eine Falschpräsentation führt dazu, dass der Signierer nicht das signiert, was er signieren möchte oder zu signieren glaubt, sondern etwas in Teilen oder völlig anderes. Er erzeugt damit nicht die von ihm gewünschte Willens- oder Wissenserklärung, sondern eine andere. Auf der Seite des Prüfers führt eine Falschpräsentation dazu, dass der Prüfende nicht die Willens- oder Wissenserklärung des Signierenden wahrnimmt, sondern ebenfalls eine ganz oder teilweise andere.

Erfahrungen aus Verletzlichkeitsexperimenten und Beobachtungen in Simulationsstudien, an denen der Autor als Angreifer mitgewirkt hat, zeigen die vielfältigen Angriffs- und Fehlermöglichkeiten.⁴⁷

3.3.1 Angriffe

Das zur Präsentation verwendete System kann manipuliert werden, so dass es die signierten Daten nicht korrekt präsentiert.

⁴⁶ Roßnagel / Wedde / Hammer / Pordesch 1989.

⁴⁷ Pordesch provet-Arbeitspapier Nr. 81, 1992 und Pordesch provet Arbeitspapier Nr. 106, 1993.

i) Untergeschobene Daten

Im einfachsten Fall werden gar nicht die signierten Daten, sondern andere präsentiert, die dem Nutzer beim Prüfen oder beim Signieren untergeschoben werden. Präsentation bezieht sich dann ganz oder teilweise auf andere Daten als der Nutzer denkt. Täuschungen sind beispielsweise dadurch möglich, dass ein Angreifer Dateinamen bzw. Dokumentbezeichnungen oder -symbole so wählt, dass sie verwechselt werden. So signierte in der Simulationsstudie "Rechtspflege" ein Rechtsanwalt eine per Diskette überbrachte fingierte Warenbestellung statt wie gewünscht eine Quittung über einen gezahlten Gebührenvorschuss. Der Angreifer hatte dazu nur zwei Dateien ähnlich benannt und eine davon im Dateiverwaltungsprogramm als "versteckt" gekennzeichnet. Der Anwalt rief ohne es zu merken eine andere Datei zum ansehen auf, als er danach signierte.⁴⁸

ii) Gerätemanipulation/-vertauschung

In der Vergangenheit wurden verschiedene Fälle der äußerlichen Manipulation von Geldautomaten bekannt – vom Anbringen von Folientastaturen oder zusätzlicher Kästen zum Auslesen der Magnetkarten.⁴⁹ Hardwaremanipulationen könnten aber auch an der für die Präsentation der Daten genutzten Komponenten ansetzen.

Subtile Manipulationen, wie die Verstellung von Reglern oder die Abkopplung oder Störung wirken sich wie bei Fehlern auf die globale Wahrnehmbarkeit des ganzen Dokumentes aus. Komplexere Effekte können erzielt werden, wenn zwischen Ausgabegerät und Computer ein Angreifersystem geschaltet wird, der Signale auffängt und umwandelt. In diesem Fall wäre man nicht an die begrenzten Programmiermöglichkeiten der Hardwarekomponenten gebunden. Derartige Manipulationen dürften andererseits aber auch so schwierig durchzuführen sein, dass der gewünschte Effekt anders leichter erreichbar ist. Möglich ist es aber auch, das Ausgabegerät schlicht an einen anderen Computer anzuschließen.

Eingabegeräte eignen sich möglicherweise auch für subtile aber wirkungsvolle Manipulationen. Schon die Umpolung einer Maus oder die Vertauschung von Tasten könnte beispielsweise dazu führen, dass in einem Dokument nicht vor-, sondern zurückgeblättert wird. Einem unbedarften Nutzer muss dies nicht auffallen.

iii) Programmanipulationen

Softwarefehler oder auch Hardwarefehler basieren z.T., auch darauf, dass die von diesen Programmen verwendeten Daten über Standardeinstellungen und Objekte manipuliert werden. Hinzu kommen als Ursache unsignierte Daten, die Teil des Dokumentes werden.

Über Bildschirmtreiber oder den Treiber der Grafikkarte lassen sich allgemeine auf alle Bildelemente auswirkende Aspekte der Darstellung manipulieren. Als Effekt derartiger Einstellungen können abhängig vom Anwendungssystem Teile eines Textes unleserlich werden (Größe, Auflösung) oder farbliche Nuancierungen und Hervorhebungen verschwinden (Farbpalette), was sich indirekt auch auf Passagen oder Elemente des Dokumentes auswirken kann. Allerdings ist es wohl kaum möglich, dass aufgrund eines Treibers der Inhalt eines Dokumentes grob entstellt wird. Dazu müssten die Treiberprogramme selbst manipuliert werden,

⁴⁸ Pordes, provet-Arbeitspapier Nr. 81, 1992, 14.

⁴⁹ Siehe z.B. Fall in der Frankfurter Rundschau 2.3.1991.

etwa so, dass sie einzelne Farben ausblenden oder bestimmte Bildpunktanordnungen in einem ganz bestimmten Kontext verfälschen (bis hin zum Ausblenden einzelner Buchstaben eines Textes). Der Aufwand für solche Manipulationen dürfte sehr hoch sein.

iv) Manipulierte Systemkonfiguration

Manipulationen der Programmverknüpfung können dazu führen, dass nicht das vorgesehene Präsentationsprogramm, sondern ein anderes gestartet wird. Dies gilt auch für den Aufruf von Präsentationsprogrammen aus einer bereits laufenden Präsentation, etwa wenn eingebettete Objekte (z.B. Kalkulationstabellen, Sounddateien) präsentiert werden sollen. Weist das andere Präsentationsprogramm nicht alle Funktionen und Elemente des Programmes auf, mit dem die Daten erzeugt bzw. zum Signierzeitpunkt präsentiert wurden, so gehen Elemente verloren (etwa Makros) oder werden umgewandelt, das präsentierte Dokument weist aber sonst keine Auffälligkeiten auf. Ist das Datenformat unbekannt, so wird es möglicherweise nicht abgewiesen, sondern in ein "primitives" Format umgewandelt und angezeigt.

Büro- und Grafikprogramme (alle untersuchten Programme) greifen vielfach auf gemeinsam genutzte Zeichensätze zurück, d.h. graphische Abbilder der einzelnen Zeichen, die sich jeweils für ein Alphabet sortiert in Font-Dateien des Betriebssystems befinden. Besonders heimtückisch dürfte die **Manipulation eines Fonts** sein, z.B. indem die graphische Darstellung einer Zahl durch die einer anderen ersetzt wird. So können z.B. Zahlenangaben in Verträgen unmerklich verändert werden, ohne die Signaturprüfung zu beeinträchtigen. Grobe inhaltliche Entstellungen ergeben sich auch bei der falschen Zuordnung von Bitfolgen zu Zeichen (Codierung). Textverarbeitungssysteme wie Word arbeiten normalerweise mit ASCII-Codetabelle, bei Email-Systemen wie Netscapes Messenger kann die Codierung jedoch eingestellt werden. Eine falsche Codierung bewirkt, dass einige (deutsche) Textzeichen durch andere ersetzt werden – bei menschlichen Sprachen mit sehr vielen Schriftzeichen (z.B. chinesisch) eine völlige Verquerung des Inhalts.

Bereits auf der Betriebssystemebene (bzw. für die grafische Benutzeroberfläche oder auch ein X-Windows-Fenster) lassen sich **Standardeinstellungen** für Hintergrund und Textfarben in Anwendungsfenstern festlegen. Solche werden als Standardeinstellung übernommen, wenn in der jeweiligen Dokumentdatei oder dem Anwendungsprogramm keine speziellen Einstellungen vorgenommen werden (bei Word, nicht jedoch z.B. bei Adobe PDF-Dateien).⁵⁰ Ein schwarzer Hintergrund lässt die gewöhnlich schwarze Schrift verschwinden, weiße Standardfarbe für Textzeichen erweckt den Eindruck einer leeren Datei. Mit "intelligenteren" Manipulationen lassen sich Textteile ausblenden: Ist der größte Teil des Dokumentes direkt schwarz eingefärbt und werden nur einige Zahlenangaben transparent gefärbt, so wird dies bei normaler Einstellung des Betriebssystems nicht erkannt werden können, alle Schriftzeichen erscheinen normal schwarz. Erst wenn die Standardfarbe für Schriftzeichen in Anwendungsfenstern "weiß" statt wie üblich "schwarz" eingestellt wird, werden bestimmte Zeichen plötzlich unsichtbar.

Auch die Größe, Form und Farbe von Fenstern, in denen das Dokument präsentiert wird, entscheidet mit über die Wahrnehmbarkeit des Dokumentinhaltes. Standardeinstellungen werden im Betriebssystem festgelegt und können dort eingestellt werden. Hier ist ein Angriff vorstell-

⁵⁰ Z.B. Schriftfarbe "Automatisch" bei Schriftfarbe oder "kein Füllbereich" beim Hintergrund in WORD 97. CORELDRAW 7.0 verfügt nicht über entsprechende Einstellmöglichkeiten.

bar, bei dem Fensterrahmen und Titelzeilen durch gezielte Farbwahl ausgeblendet werden, um ein dahinter liegendes Dokument oder Bild (auf dem Desktop-Hintergrund oder eines anderen Fensters als Teil des signierten Dokumentes anzusehen. Grenzen des Dokumentes und seines Inhaltes könnten dadurch verwischen, der Nutzer sieht möglicherweise nicht mehr, was wirklich Dokumentinhalt ist und was eigentlich Teil der (nicht signierten) Dokumentumgebung.

v) Datenmanipulationen

Je nach Anwendungssystem und Datenformat kann ein Dokument unsignierte Datenelemente beinhalten, die den Inhalt des Dokumentes erst mit dem Öffnen des Dokumentes in Abhängigkeit von Umgebungsbedingungen und Benutzereingaben festlegen. Beispiele hierfür sind aktualisierbare Felder, wie Seitenangaben, Datumsangaben, Makros und ereignisgesteuerte Buttons. Raffinierte Manipulationen können ein angezeigtes Dokumentdatum oder einen berechneten Zahlenwert abhängig machen, auf welchem Rechner das Dokument präsentiert wird.

Dokumente können Links auf WWW-Seiten, extern abgespeicherte Grafiken und andere externe Objekte enthalten, die sich irgendwo auf dem lokalen System, einem angeschlossenen Rechnernetz oder im weltweiten Internet befinden. Sie können dann jederzeit gelöscht oder ausgetauscht werden, um eine Präsentation gezielt zu verändern. Relative Verweise, etwa auf bestimmte Dateien in lokalen Verzeichnissen, können je nachdem, auf welchem System das Dokument präsentiert wird, zu unterschiedlichen Inhalten führen.

Wahrscheinlichkeit von Angriffen

Die Wahrscheinlichkeit von erfolgreichen Angriffen hängt neben der konkret zu beurteilenden Motivlage davon ab, welcher Aufwand damit verbunden ist und wie hoch das Entdeckungsrisiko ist.

Verhältnismäßig leicht sind Angriffe durchzuführen, wenn sich Systeme in einer allgemein zugänglichen Umgebung (z.B. öffentliches Terminal) befinden, wenn es sich um frei programmierbare Systeme (PCs) und unsichere Betriebssysteme mit Netzanbindung handelt. Besonders groß ist das Risiko, wenn das zur Präsentation verwendete System vom Angreifer selbst kontrolliert wird. Hier hat der Angreifer im Prinzip alle Möglichkeiten und genügend Zeit zur Vorbereitung.

Verhältnismäßig schwer sind Angriffe hingegen dann, wenn die Systeme sich in einer geschützten Umgebung befinden, nur von einem Nutzer (dem Signierer oder Prüfer) gepflegt werden, nur eine oder wenige Funktion dauerhaft erfüllen (z.B. Geldautomat), mit sicheren Zugriffskontroll- und Betriebssystemen ausgestattet und vom Netz abgekoppelt sind. Schwer ist ein Angriff, wenn das zur Präsentation verwendete System unter ausschließlicher Kontrolle des Signierenden oder Prüfenden steht, d.h. von diesem konfiguriert und betrieben wird. Jedoch kann auch dann ein Unterschieben von Daten gelingen. In der Simulationsstudie Rechtspflege gelang dies mit Hilfe einer zugesendeten Diskette, auf der sich ein trojanisches Pferd in einer Dokumentvorlage befand.⁵¹ Deshalb sind neben der Kontrolle über das lokale System auch die anderen Sicherheitsfaktoren und der Benutzer von erheblicher Bedeutung – und besonders wie im vorliegenden Fall, ob der Signierer das Dokument erstellt hat oder ein anderer.

⁵¹ Pordesch, provet-Arbeitspapier 81, 1992, 29.

3.3.2 Technische Fehler

i) Hardwarefehler und Gerätedefekte

Ausgabegeräte oder auch Eingabegeräte können technische Fehler aufweisen. Sie können vom Computersystem unbeabsichtigt abgekoppelt, falsch angeschlossen oder durch äußere Ursachen gestört werden. Ist der Gerätetreiber geladen und eventuell noch die Hardware (z.B. Audiokarte) vorhanden, so wird weder das Anwendungssystem noch das Betriebssystem das Fehlen oder die Störung des Endgerätes erkennen.

Im Falle der Textkommunikation würde der Defekt des **Ausgabegerätes** Bildschirms sofort bemerkt. Hingegen muss das Fehlen eines funktionsfähigen Lautsprechers nicht unbedingt auffallen, weil der Benutzer lediglich Dokumentteile nicht wahrnehmen kann. Außerdem können sich - insbesondere bei audiovisuellen Medien (Bewegtbild) - vorübergehende Störungen (Bildschirmflackern) auf die Wahrnehmbarkeit auswirken. Funktioniert das **Eingabegerät** nicht richtig, etwa ein Teil der Tastatur, die Mouse oder ihre Tasten, können u.U. im Präsentationsprogramm vorgesehene Navigationsmöglichkeiten nicht genutzt werden und Teile eines Dokumentes sind deshalb nicht wahrnehmbar. Falsch konfigurierte oder gestörte Systeme können auch die **Rechnerleistung** reduzieren. In einem solchen Fall kann die Ausgabe stark verzögert werden, unvollständig werden oder gänzlich unterbleiben.

ii) Fehlerhafte Betriebssystemkonfiguration

Auf Betriebssystemebene wird mit der Installation von Programmen bereits die Verknüpfung von Dateien und Programmen festgelegt. Fehler bei der Installation können dazu führen, dass nicht das vorgesehene Präsentationsprogramm, sondern ein **falsches Programm** gestartet wird - etwa eine zugleich installierte ältere Programmversion oder gar ein ganz andere Anwendung. Dies gilt auch für den Aufruf von Präsentationsprogrammen aus einer bereits laufenden Präsentation, etwa wenn eingebettete Grafiken, Teildokumente oder Sounddateien präsentiert werden sollen.

Falsche installierte oder falsch eingestellte **Gerätetreiber** wirken sich auf Farben und die Schriftgrößen (Bildelementgröße) aus. Hierdurch können Teile eines Textes unleserlich werden (Größe, Auflösung) oder farbliche Nuancierungen und Hervorhebungen verloren gehen (Farbpalette), was sich indirekt auch auf Passagen oder Elemente des Dokumentes auswirken kann. Allerdings ist es wohl kaum möglich, dass aufgrund eines Treibers der Inhalt eines Dokumentes grob entstellt wird. Fehler bei der Installation von Programmen - in Windows-Systemen leicht möglich - können dazu führen, dass **Zeichensätze überschrieben** oder gelöscht werden, wodurch sich das Aussehen eines Textdokumentes wesentlich verändern kann. Möglich ist auch die fehlerhafte Einstellungen für Hintergründe und Textfarben in Anwendungsfenstern, die sich auch auf die Darstellung von Dokumenten in Anwendungsfenstern auswirken und die Wahrnehmbarkeit des Dokumentinhaltes einschränken.

iii) Programmfehler

Die zur Präsentation eingesetzten Programme können die Daten fehlerhaft interpretieren. Erfahrungen beim fehlerhaften Konvertieren von Dokumentformaten (etwa Word) auf Programme anderer Hersteller oder neuere Versionen desselben Herstellers hat jeder Nutzer von Büroprogrammen schon gemacht. Berühmt-berüchtigt ist die Entstellung lesbarer Zeichen zu

Sonderzeichen bei Word: So konnte bereits eine fehlerhafte Microsoft Word 97-Version Dokumente einer Microsoft Word 95-Version nicht mehr richtig konvertieren und stellte einige Textzeichen als Sonderzeichen dar.

3.3.3 Benutzungsfehler

Wenn es um die Wahrnehmung geht, sind als bedeutende Ursache fehlerhafte menschliche Handlungen zu berücksichtigen. Benutzer können abgelenkt, gestresst sein, so dass sie die Systeme falsch bedienen. Ein weiterer Faktor ist die Unerfahrenheit vieler Nutzer.⁵²

i) Unterlassene Präsentation

Anwender sind häufig gestresst. Da ist es nahe liegend, den mit der Prüfung und Erzeugung von signierten Dokumenten verbundenen Aufwand möglichst gering zu halten. In solchen Fällen kann es passieren, dass auf die Präsentation teilweise oder ganz verzichtet und Daten "blind" signiert werden. Ein solches Verhalten war beispielsweise in der Simulationsstudie Rechtspflege zu beobachten, wo Anwälte aus Gründen der Zeitersparnis Dokumente en bloc signierten (oder sogar mit ihrer eigenen Chipkarte durch die Sekretärin signieren ließen), ohne sie jeweils zuvor noch einmal anzusehen.⁵³ Versehentlich falsche Signiervorgänge unter falsche Dokumente oder auch z.B. Entwürfe wären möglich gewesen.

ii) Fehlbedienung

Die Softwaresysteme können vom Benutzer fehlerhaft konfiguriert werden, so dass bestimmte Teile nicht wahrnehmbar sind. Der Benutzer kann versehentlich das falsche Programm auswählen, um Daten zu präsentieren. Regler am Ausgabegerät können versehentlich falsch eingestellt werden - etwa indem Farben ausgeblendet werden, oder indem bei einem Audiodokument die Lautstärke stark reduziert wird. Die Software ist im Allgemeinen nur sehr begrenzt in der Lage, den tatsächlichen Zustand eines Endgerätes festzustellen und Fehlermeldungen zu liefern. Den Status eines Kontrastreglers oder das Einlegen zu kleinen Papiers in einen Drucker wird sie nicht verhindern und bemerken können.

Eine weitere wichtige Fehlerquelle ist die falsche Wahl eines Präsentationsmodus. Alle Standardprogramme bieten verschiedene Möglichkeiten Dokumente in verschiedenen Überblicks- oder Ausschnittsdarstellungen und Einzelaspekte gezielt zu zoomen auszugeben. Am weitestgehenden ist hier Word, das von der druckerorientierten Seitenansicht, über Normal-, Online-, Gliederungs- und Seitenlayoutsansicht etc. eine auch für Experten kaum mehr verständliche Fülle von Ansichtsmöglichkeiten bietet - wobei es im Übrigen auf einem PC aber kaum gelingt, auch nur eine von der Größe dem Druckbild entsprechende Ansicht zu finden. Zu allem Überfluss ist dann bei Word 97 ausgerechnet die mit "Normal" gekennzeichnete Ansicht diejenigen, bei der ein Teil des Dokumentes (die Textfelder) ausgeblendet werden. Insbesondere Laien kann es also leicht passieren, zu einem Dokument die falsche Ansicht zu wählen, so dass Teile eines Dokumentes nicht richtig wahrgenommen werden können.

⁵² Kumbruck DuD 1994.

⁵³ Pordesch DuD 1993.

3.4 Mögliche Effekte

Wie bereits eingangs ausgeführt, ist eine physische Präsentation ein orts- und zeitgebundener Vorgang, der letztlich nie vollständig reproduzierbar ist. Wenn also vom Risiko abweichender Präsentation gesprochen wird, bezieht sich dieses auf rechtserhebliche Abweichungen, also solche, die in rechtlichen Auseinandersetzungen eine Rolle spielen.

Aus der Tatsache, dass das Präsentationsproblem unabhängig vom Einsatz der Signaturverfahren ein prinzipielles Problem des elektronischen Rechtsverkehrs ist, ließe sich vielleicht erwarten, einschlägige Gerichtsentscheidungen zur Wesentlichkeit bestimmter Abweichungen zu finden. Dies ist jedoch nicht der Fall. Aus eigenen Recherchen in juristischen Datenbanken (JURIS) zu schließen spielten nur zu einigen Gerichtsprozessen mit der Präsentation zusammenhängende Fragen eine Rolle. Dies mag u.a. daran liegen, dass die bislang unsigned elektronischen Willenserklärungen erfolgreich abgestritten werden können, indem Authentizität und Urheberschaft der Daten bestritten werden, so dass der kompliziertere Weg, das Bestreiten der Interpretation und Präsentation, schlicht unnötig ist. Wo Fälle und Urteile fehlen, wird im Folgenden daher versucht, solche mit plausiblen Argumenten gedanklich vorwegzunehmen.

3.4.1 Inhaltsart

Bei elektronischen Dokumenten handelt es sich nicht nur um druckbare bzw. am Bildschirm lesbare Schriftzeichen, sondern auch um Bilder, Tondokumente und Bewegbilddokumente oder Kombinationen verschiedener Medien. Da die Daten unabhängig von der Präsentationsform dennoch letztlich immer Bitfolgen sind, ist nicht auszuschließen, dass sie in verschiedenen Medien präsentiert werden können. Ist ein Dokument zugleich in verschiedenen Medien präsentierbar, stellt sich die Frage, welche Präsentation eigentlich die gültige Willens- oder Wissenserklärung enthält bzw. ob überhaupt eine bestimmte Erklärung existiert. Werden - wie beabsichtigt - mit SigG-Signatur signierte elektronische Schriftdokumente in vielen Rechtsbereichen als Ersatz für Papierurkunden zugelassen und beweisrechtlich privilegiert⁵⁴, so dürfte bereits vorab die Frage relevant werden, ob es sich bei den signierten Daten denn überhaupt um ein Schriftdokument im Sinne der dann gesetzlich definierten "elektronischen Form" handelt.

Der Aspekt der Inhaltsart ist medienspezifisch und neu. Bei Papierdokumenten konnte kein Streit bezüglich der Inhaltsart aufkommen. Bei den auf Papier verkörperten Zeichen handelt es sich stets um ganz bestimmte eindeutig wahrnehmbare Schriftzeichen und Bilder, nie um Ton oder etwas anderes. Bei unsigned elektronischen Dokumenten hätte bereits Streit aufkommen können, es sind bislang aber keine Auseinandersetzungen um diese Frage bekannt geworden.

Sofern nicht eine höherwertige Formatkollision vorliegt, wird bei einer solchen Kollision aus dem Bitstring eine Präsentation erzeugt werden, die dem Menschen nicht "sinnvoll" erscheint, d.h. durch den Menschen nicht interpretierbar ist. Eine Grafik erzeugt in einem Editor eine Folge unverständlicher Zeichen. Umgekehrt würde ein Textdokument – soweit technisch interpretierbar – ein „unsinniges“ Punktmuster ergeben. Fehler dürften daher auffallen. Angriffe unter Ausnutzung dieser Primitivkollision sind aber sehr wohl möglich:

⁵⁴ BMJ 1999.

Fallbeispiel 1: Testtext oder Beleidigungsgrafik?

Mallet ist Vorgesetzter von Alice und möchte diese loswerden. Er schreibt mit Corel-Draw ein Plakat, auf dem die Geschäftsleitung in einer Karikatur als ein unfähiger Haufen von Idioten und der Geschäftsführer als Schwein dargestellt und in einer Bildunterschrift auch so bezeichnet wird. Er benennt die Datei "Test.txt", sendet sie an Alice und äußert telefonisch die Bitte, diesen angeblichen "Testtext" zu signieren und zurückzusenden. Es handele sich um einen kryptographischen Funktionstest der Chipkarte an einer speziellen Testdatei. Alice klickt die Datei an, um zu sehen, was sie da "unterschreiben" soll. Es wird automatisch der Editor geöffnet, der eine bedeutungslose Folge von Zeichen anzeigt. Sie signiert diese und sendet die Datei mitsamt Signaturdatei an Mallet zurück. Mallet ändert den Namen der Datei in "Karrik.cdr" und sendet sie anonym an den Unternehmensverteiler und Personalchef Bob. Bob prüft die Signatur, klickt die Datei an und sieht die beleidigende Karikatur in CORELDRAW. Daraufhin wird Alice fristlos gekündigt und ein Strafverfahren wegen Beleidigung in Gang gesetzt. Alice zeigt die Geschäftsleitung an wegen Verleumdung und Datenfälschung und klagt außerdem vor dem Arbeitsgericht auf Kündigungsschutz.

"Höherwertige" Datenformatkollisionen, d.h. Daten, die in zwei verschiedenartigen Standardprogrammen eine sinnvolle Ausgabe erzeugen dürften extrem selten sein. Sie werden kaum zufällig und in Verbindung mit Fehlern, wie dem Start eines falschen Programmes auftreten.⁵⁵ Ein Angreifer könnte jedoch versuchen - insbesondere bei Datenformaten mit kürzeren Bistings - gezielt Daten zu suchen, die Formatkollisionen erzeugen.⁵⁶ Einfacher dürfte es sein, ein Anwendungsprogramm selbst zu schreiben, das die Kollision erzeugt.

Fallbeispiel 2: Das selbst geschriebene Anwendungsprogramm

Mallet hat die Verwaltungsleiterin Alice bestochen, um an einen Großauftrag heranzukommen. In Notizen hat er die Zahlungen (wg. Al. 50000) notiert und vom Archivierungsprogramm wurden sie zur Sicherheit signiert. Als ihm im Strafprozess die signierten Notizen vorgehalten werden, gibt er an, es handele sich um Testdaten eines betriebsinternen wissenschaftlichen Programmes. Zwei Wochen später präsentiert er dieses Programm.

Mögliche Ursachen

- Mehrdeutigkeit
 - Formatkollision
- Falschpräsentation:
 - Falsche Datenauswahl/Unterschieben
 - Falsche Programmauswahl, falsche Daten/Programmverknüpfung
 - Endgerätevertauschung

3.4.2 Inhaltsbestandteile

Auch wenn digitale Signaturen es ermöglichen, die Verfälschung von Daten zu erkennen, können am Ausgabegerät unterschiedliche Inhalte dargestellt werden. So können sich bei Schriftdokumenten Zeichen, bei Tondokumenten Töne und bei Bildern grafische Bildelemente eventuell unterscheiden.

Bei Papierdokumenten stellte sich die Frage nach Inhaltsbestandteilen bislang nur als Frage der Verfälschung oder Fälschung von Urkunden. Als Frage der Präsentation tauchte sie im Zusammenhang mit der elektronischen Reproduktion von Textdokumenten durch Fotokopien und Telefax auf. Aufgrund der Verfälschungsmöglichkeiten gelten elektronische Reproduktionen nicht als Originalurkunden.⁵⁷ Bei unsignierten elektronischen Dokumenten sind bislang

⁵⁵ Obwohl sie bei universellen Datenformaten wie ASN.1 (reine Syntax) und XML auf "höherer Ebene" wiederum auftreten können (insbesondere durch schlecht gewählte Feldbezeichnungen zu einfache Dokumentstrukturen). Darauf wird später näher eingegangen, S.61.

⁵⁶ Echte Formatkollisionen sind dem Autor gleichwohl bislang nicht bekannt.

⁵⁷ Zieleinski 1995, 286 ff.

keine Fälle bekanntgeworden, wohl weil es hier bedeutend einfacher ist, die Daten selbst, als deren Präsentation zu bestreiten.

Inhaltliche Änderungen können sich durch die Wahl unterschiedlicher **Zeichencodierungen** oder **Schriftzeichensätzen**. Von Schriftzeichensätzen haben für gewöhnlich den Effekt, dass sich das Schriftbild verändert, eine Schrift kleiner oder größer wird und sich eventuell dann auch der Umbruch ändert. Der Inhalt ändert sich jedoch, wenn ein Schriftzeichensatz Sonderzeichen verwendet werden, die einer anderer nicht enthält und wenn Bitfolgen aufgrund einer falschen Codierungstabelle anderen Textzeichen zugeordnet werden. Zufällige Veränderungen dürften in der Regel erkannt werden können: Im Text verändern sich viele Zeichen, einige fehlen, die Inhalte von Textfeldern sind nicht mehr richtig zu erkennen, z.B. weil Buchstaben zu groß sind. Angreifer können jedoch Zeichensätze durch die Manipulation einzelner Zeichen gezielt verändern, um die Präsentation unerkennbar zu verfälschen:

Fallbeispiel 3: Ein anderer Zeichensatz

Mallet beschließt mit Alice eine Gütertrennung nach der Scheidung. Auf dem PC zu Hause ändert er den Font Arial mit einem Fontbearbeitungsprogramm, so, dass feste Leerzeichen als "0" am Bildschirm dargestellt werden. Mit Alice zusammen schreibt er dann am PC einen Text "Mallet zahlt 50000 DM und erhält dafür den Porsche ...", wobei er aber unmerklich die letzte Null als festes Leerzeichen eingibt. Beide signieren den Vertrag kopieren ihn sich auf Diskette und trennen sich. Später macht er die Fontänderung rückgängig. Der Fahrzeugbrief des Porsche wird von Alice übergeben, Mallet überweist jedoch nur 5000 DM. Als Alice sich beschwert, sagt Bob, sie hätten nichts anderes vereinbart und verweist auf das signierte Schreiben. Alice öffnet das Dokument auf ihrem PC im neuen zu Hause, überprüft die Signatur und stellt bei der anschließenden Präsentation überrascht fest, da steht nur "Mallet zahlt 5000 DM und erhält dafür den Porsche"

Durch das Anwendungssystem können auch **Inhaltsergänzungen** vorgenommen werden. Dies ist besonders bei Formularen üblich, um den Feldinhalten eine Bedeutung zuzuweisen, jedoch auch bei gewöhnlichen Freitexten möglich. Werden nun solche automatischen Ergänzungen (soweit nicht Teil des Dokumentes) geändert, so kann sich dadurch die Bedeutung des Inhalts grundlegend ändern. Die Änderung einer Layoutvorlage kann dann aus einem "Vertrag" einen "Vertragsentwurf" und aus einem "Preis" eine "unverbindliche Preisempfehlung" werden lassen, was keinen Einfluss auf den Erfolg der Signaturprüfung hat. Es gibt jedoch speziell bei Word noch andere Möglichkeiten. Die Farbe von Schrift- bzw. Bildhintergründen und ihr Unterschied entscheidet darüber, ob Textpassagen hervorgehoben, abgeschwächt oder gänzlich unsichtbar werden.

Fallbeispiel 4: Eine merkwürdige Farbeinstellung

Bob ist Personalchef in einem Unternehmen und überlegt Alice einzustellen. Nach dem Vorstellungsgespräch sendet er Alice per Mail ein Word-Dokument mit dem Text. Im Wort "Arbeitsvertragsentwurf" hat er den Wortteil "entwurf" durch gelbe Farbe besonders hervorgehoben. Er signiert die Mail mitsamt dem Dokument und sendet beides an Alice. Alice hat auf ihrem Bildschirm die Hintergrundfarbe gelb eingestellt - sie hatte auch noch nie Dokumente und Mails mit gelbem Text erhalten. Sie freut sich über den elektronischen Arbeitsvertrag und kommt am vereinbarten ersten Arbeitstag. Da teilt ihr Bob mit, dass er leider einer anderen Bewerberin zugesagt habe, nachdem Alice auf seinen Entwurf nicht reagiert habe. Alice klagt auf Einstellung, da sie der Meinung ist, das Missverständnis, sei nur zustandegekommen, weil Bob den Hintergrund der des Dokumentes "transparent" eingestellt habe, statt, wie "für Papier üblich weiß".

Ein Dokument kann **berechnete Felder** enthalten, deren Inhalt erst mit dem Öffnen des Dokumentes festgelegt werden. An der Präsentation ändert dies dann etwas, wenn sich die Berechnungen nicht nur auf die Daten selbst, sondern Umgebungsbedingungen oder die Zeit beziehen. Der Einsatz aktualisierbarer bzw. berechnet Felder kann zu Fehlinterpretationen führen oder gezielt zu Angriffen genutzt werden.

Fallbeispiel 5: Tatzeit "Aktualisierbares Datum"

Bob war Zeuge eines Autounfalls, bei dem Alice die Geschädigte und Mallet der Verursacher war. Er schreibt "Ich war Zeuge eines Autounfalls am heutigen 11.12.99 ... und sah, dass Mallet Alice die Vorfahrt nahm, weshalb Alice ausweichen musste und gegen den Baum fuhr." Da er sich Datumsangaben nie merken kann, hat er das Datum mit der Hilfe von Word mit dem Befehl Einfügen Datum Uhrzeit eingefügt, leider aber übersehen, dass dort die Option "Aktualisierbar (als

Feld einfügen)" ausgewählt war. Am Bildschirm und auf dem Ausdruck hat er das nicht erkannt. Als Alice die signierte Zeugenaussage zwei Wochen später an die ermittelnde Staatsanwaltschaft sendet, wundert sich diese, denn da steht: Ich war Zeuge eines Autounfalls am heutigen 25.12.99 ... und sah ..". Die signierte Zeugenaussage ist von fraglichem Wert.

Mögliche Ursachen

- Mehrdeutigkeit
 - Andere Zeichensätze
 - Unklare externe Verweise
 - Berechnete Felder
- Falschpräsentation
 - Zeichensatzmanipulation
 - Vorlagenmanipulation/-vertauschung
 - Verfälschung eingebundener externer Daten/Dateien

3.4.3 Präsentationskontext

Neben den Inhaltsbestandteilen einer Präsentation, die auf die signierten Daten zurückgehen, sind auch diejenigen zu berücksichtigen, die durch andere signierte und unsignierte Daten bestimmt werden. In der elektronischen Urlaubskarte - dem Eingangsbeispiel - stehen einzelne Antragszeilen in Zusammenhang mit anderen Zeilen und dem Kopf der Urlaubskarte, die für sich signiert sind. Dieser Zusammenhang wird jedoch teilweise nur durch die Präsentation erzeugt. Die Daten selbst müssen nicht notwendigerweise in einer Datei gespeichert sein, sie könnten genauso gut zusammen in verschiedenen Tabellen einer Datenbank oder als Einzeldokument in verschiedenen Dateien gespeichert werden. Es ist auch nicht gesagt, dass der Zusammenhang zum Signierzeitpunkt dem des Prüfzeitpunktes entspricht.⁵⁸

Der Kontext von Inhaltselementen ergibt sich bei Papierdokumenten durch die Verkörperung auf dem Papierträger. Allerdings ist bei Dokumenten mit mehreren Teilen bisweilen umstritten, inwieweit diese durch die Unterschrift auf einem Dokumentteil oder einem Begleitschreiben umfasst sind. In einem Fall vor dem Bundesgerichtshof (BGH) ging es um die Frage, inwieweit Regelungen in Anlagen eines Mietvertrages gültig sind, die nicht direkt (körperlich) mit dem unterschriebenen Text zusammenhängen. Der BGH hält eine körperliche Verbindung zwischen Urkunde und Anlagen im vorliegenden Fall nicht für erforderlich, weil sich die Einheit von Vertragstext und Anlagen aus Verweisungen des Vertragstextes auf die Anlagen ergebe.⁵⁹

Dokumente können Links auf WWW-Seiten, externe Grafiken und andere externe Objekte enthalten, die sich irgendwo auf dem Computer, dem lokalen Rechnernetz oder im weltweiten Internet befinden. Auch wenn die externen Daten nicht Teil des (signierten) Dokumentes selbst sind, werden sie in der Präsentation teils unterschiedslos mit jenen angezeigt. Anders als die signierten Daten können sie dann aber ausgetauscht oder gelöscht werden, ohne die Signaturprüfung zu beeinflussen. Werden dann die externen Objekte gelöscht oder geändert, so kann dies auch den Inhalt des präsentierten Dokumentes wesentlich ändern.

Fallbeispiel 6: Externer Link auf die Preisliste

⁵⁸ Zum Problem der Kontextverfälschung: Pordesch DuD 1993, 565.

⁵⁹ BGH, Urteil vom 21.1.1999 - VII ZR 93/97 zitiert nach Betriebsberater 10/99, 495 ff.

Mallet versendet ein günstiges Angebote über eine Computer-Komplettsystem an Alice und andere per HTML-E-Mail. Das Angebot enthält einen ausführbaren Link auf die Preisliste mit Artikelnummern im Internet (850 DM für dieses Gerät). Alice liest die Mail, sieht die Preisangabe und bestellt sofort per signierter Rückantwort 3 Komplettsysteme für ihre Firma. Aufgrund der großen Nachfrage ändert Mallet die Preisliste, der Rechner kostet jetzt 1300 DM. Alice, die sich die Mail am nächsten Tag anschaut, wundert sich, dass sie den Preis offenbar falsch gelesen hat, denn die Signatur ist ja in Ordnung.

Mögliche Ursachen

- Mehrdeutigkeit
 - Andere Vorlagen
- Falschpräsentation
 - Vertauschung, Manipulation von Vorlagen
 - Verfälschung eingebundener externer Daten/Dateien

3.4.4 Anordnung

Ein wesentlicher Aspekt der Präsentation ist sicher die Anordnung der Inhaltselemente, d.h. Zeilenumbrüche und Absatzpositionen bei Schriftdokumenten. Die Anordnung bestimmt die inhaltliche Logik. Bei Papierdokumenten war sie durch das Medium vorgegeben und insofern kaum ein möglicher Streitgegenstand. Denkbar sind Auseinandersetzungen über die Reihenfolge von Seiten größerer Dokumente wie loser Blattsammlungen. Hierzu ist aber nichts bekannt geworden.

Bei elektronischen Dokumenten kann die Anordnung der Elemente durch eine Formatvorlage oder durch die Wahl von Ansichtsmodi durch den Benutzer bestimmt werden. Darüber hinaus bestimmen Buchstabenformate und Zeilenumbrüche sowie Fenstergrößen bisweilen auch (in allerdings geringerem Umfang) die Anordnung. Formatvorlagen werden jedoch nicht ohne weiteres mitsigniert, der Laie kennt deren lokalen Speicherort nicht einmal. Aspekte wie Fenstergrößen und Ansichtsmodi werden weder im Dokument noch in Vorlagen gespeichert und können deshalb garnicht signiert werden.

Fallbeispiel 7: Preisangaben-Position in Dokumentvorlage

Mallet versendet ein günstiges Angebote über eine Computer-Komplettsystem (Pentium VIII mit Extras) an Alice als Word-Dokument. Das Angebot enthält den Computer, plus Zubehör, Software und Handbücher und am unteren Ende der Seite den Preis (1150 DM für dieses Gerät). Alice liest die Mail, sieht die Preisangabe und bestellt sofort per signierter Rückantwort. Sie erhält eine Rechnung über 1500 DM. Mallet verweist darauf, dass bei ihm der Preis rechts oben stehe und sich nur auf den Computer beziehe, wohingegen Zubehör, Software und Handbücher das Pluspaket seien, das extra zu bezahlen sei.

Mögliche Ursachen

- Mehrdeutigkeit
 - Andere Vorlagen
 - Ansichtsmodi, Fenstergrößen, Umbrüche
- Falschpräsentation
 - Vertauschung, Manipulation von Vorlagen
 - Verfälschung eingebundener externer Daten/Dateien

3.4.5 Äußere Form / Gewichtung

Ein wesentlicher Aspekt der Präsentation ist auch die äußere wahrnehmbare Form der Inhalte und ihrer Relationen zueinander (Hervorhebungen, Abschwächungen, usw.), was im engeren Sinne als "Darstellung" bezeichnet werden könnte. Gemeint sind hier Aspekte wie Zeichenart, Linienarten und Zeichen bei Grafiken und Farben bei Fotos. Auch hierbei gehen teils unsignierte Daten in die Präsentation ein. Teils handelt es sich auch um nicht signierbare analoge Informationen.

Die äußere Form und Gestalt von Dokumenten ist insbesondere bei nicht formatierten Daten in vielen Fällen hoch relevant. Zu nennen sind hier die Fälle bei Papierurkunden, in denen wichtige Vertragsklauseln im "Kleingedruckten" enthalten sind. In einem Prozess vor dem Landgericht Osnabrück ging es um die Frage, inwieweit die Teilnahmebedingungen im Bildschirmtextsystem der deutschen Bundespost ausreichend lesbar gewesen seien. Als Einwand gegen die Gültigkeit der Verträge wurde unter anderem vorgebracht, bei den von der Beklagten - einem Anbieter von Sexgesprächen - seien die Formate "zu klein" gewesen. Das Gericht entschied in diesem Falle auf der Basis eines vom Kläger vorgelegten Ausdrucks der Bildschirmseite, dass es sich um eine größere Schrift als Schreibmaschinenschrift handle, was den Einwand entkräfte.⁶⁰ In diesem Fall war die Präsentation selbst also nicht umstritten, sondern nur deren Auslegung. Hätte der Kläger einen kleineren Ausdruck vorgelegt und wäre umstritten gewesen, ob der Ausdruck dem Bildschirmabbild in Größe und Form zum Zeitpunkt des Vertragsabschlusses dem entsprochen habe, was der Kläger sah, wäre der Fall u.U. schwieriger zu behandeln gewesen.

Die Formatierung wirkt sich - neben den bereits genannten Effekten bei den Zeichensätzen - dort aus, wo Hervorhebungen und Gewichtungen in Dokumenten von Bedeutung sind. Die Veränderung der Formatierung (Buchstaben fett, kursiv, normal, kleingedruckt, etc..) kann daher wesentlichen Einfluss darauf haben, wie der Inhalt einer Willenserklärung wahrgenommen wird.

Fallbeispiel 8: Schriftgröße für Provisionsklausel in Dokumentvorlage

Mallet schickt Alice ein Angebot über einen Bausparvertrag als signiertes Word-Dokument mit unsignierter Dokumentvorlage. Sie überliest, dass eine Provision für Mallet in Höhe von 10% und eine Bearbeitungsgebühr in Höhe von 3% der Vertragssumme fällig sind. Später wendet sie ein, diese wichtigen Klauseln seien "kleingedruckt" gewesen und mithin ungültig. Mallet wendet ein, dies sei nicht der Fall, und zeigt eine Präsentation, in der die Klausel sogar besonders fett gedruckt herausgehoben sind. Alices Einwand sei unbegründet, sie habe eine falsche Formatvorlage verwendet.

Mögliche Ursachen

- Mehrdeutigkeit
 - Andere Vorlagen
 - Andere Endgeräte/Endgerätekonfiguration
- Falschpräsentation
 - Endgerätemanipulation

⁶⁰ LG Osnabrück: Sexgespräche über BTX, Urteil vom 10. November 1995 - 2 O 60/94, zit. Nach CR 4/1996, 227.

3.4.6 Wahrnehmbarkeit

Von der Frage der Wahrnehmung einer konkreten Form lässt sich allgemein die Frage unterscheiden, ob ein bestimmter Mensch die von einem Ausgabegerät (Medium) ausgegebenen Analogreize mit seinen Wahrnehmungsorganen erfassen konnte oder ob es sich um Reize unterhalb seiner Wahrnehmungsmöglichkeiten handelte.

Die Frage der Wahrnehmbarkeit war auch bei herkömmlichen Papierdokumenten bereits Gegenstand gerichtlicher Auseinandersetzungen. Der im vorangegangenen Abschnitt genannte Fall kann auch als Frage der Wahrnehmbarkeit verstanden werden. Wegen der im Wesentlichen unveränderbaren Verkörperung der Information auf Papierdokumenten ist hierbei jedoch nicht die Beurteilungsgrundlage bestreitbar (also etwa die tatsächliche Größe von Buchstaben und deren Lesbarkeit) sondern nur ihr Verhältnis zum Wahrnehmungsvermögen eines Menschen. Denkbar ist allenfalls, dass bei älteren vergilbten oder zwischenzeitlich verschmutzten Dokumenten über das Aussehen zu einem früheren Zeitpunkt gestritten wird.

Bei Präsentationssystemen gibt es zahlreiche Möglichkeiten, wie durch Einstellungen der Geräte und Konfiguration der Software die Wahrnehmbarkeit beeinträchtigt sein kann.

Fallbeispiel 9: Schlecht lesbares öffentliches Signierterminal

Alice hat zu Hause keinen Internetanschluss mit Signierkartenlesegerät, möchte aber doch gerne die Möglichkeiten des Internet nutzen, um an einer Auktion teilzunehmen. Sie geht an eines der öffentlichen Terminals im Kaufcenter-Cafe. Alice kann nicht gut sehen und im Bildschirm blendet die Kneipenbeleuchtung. Dummerweise sind die Regler zur Helligkeits- oder Kontrasteinstellung vom Betreiber abgedeckt worden. Alice übersieht eine Null in der Preisangabe für den von ihr favorisierten Teppich, als sie die Kauforder signiert.

Mögliche Ursachen

- Mehrdeutigkeit
 - Andere Endgeräteeinstellung
- Falschpräsentation
 - Manipulierte Endgeräteeinstellung
 - Umgebungsbedingungen!!

3.4.7 Zugänglichkeit und Kontrolle

Wesentlicher Aspekt der Präsentation ist auch, inwieweit die Inhalte dem Rezipienten zugänglich sind und insbesondere, inwieweit es dem Signierer zumutbar war, den mit der Inhaltserschließung verbundenen Aufwand zu treiben. Aspekte der Zugänglichkeit sind, inwieweit Funktionen zur Inhaltserschließung vorhanden sind und wie lange die Ansteuerung dauert.

Die Frage der Zugänglichkeit stellt sich bei Papierurkunden vielleicht in Zusammenhang mit deren Dicke oder äußeren Form (verschmutzt). Bei unsignierten elektronischen Dokumenten spielte die Frage der Zugänglichkeit eine wichtige Rolle bei zahlreichen Auseinandersetzungen um Verträge im Bildschirmtextsystem. Hier wurde zunächst in mehreren Entscheidungen die Frage behandelt, inwieweit Klauseln der allgemeinen Geschäftsbedingungen, die im System z.T. nur recht schwierig zugänglich waren, gültig sind. In einem Prozess vor dem Landgericht Freiburg ging es um die Frage, inwieweit die allgemeinen Geschäftsbedingungen des Anbieters, als Vertragsbestandteil anzusehen sind. In seinem Leitsatz stellt das Gericht fest, dass eine zumutbare Kenntnisnahme bei Bildschirmtext nur dann möglich ist, wenn es sich

um relativ kurze Texte handelt, die klar gegliedert sind und sich problemlos abrufen lassen. Bereits von der gedruckten Form sei zu verlangen, dass sie für einen Durchschnittskunden mühelos lesbar seien, ein Mindestmaß an Übersichtlichkeit sowie einen im Verhältnis zur Bedeutung des Geschäfts vertretbaren Umfang aufweisen. Im Falle von BTX seien aufgrund der erschwerten sinnlichen Wahrnehmung noch strengere Anforderungen zu stellen. Der angezeigte Text bleibe in jedem Fall flüchtig, der Durchschnittskunde könne allenfalls wenige Sätze in zumutbarer Weise aufnehmen und nach kurzer Einblendung in ihrer Bedeutung erfassen. Erschwerend wirke ferner, dass nur etwa 1/7 bis 1/8 des Umfangs einer DIN A4-Seite abgebildet werden könne. Da die AGBs etwa 14 Bildschirmtextseiten umfassten stelle dies überdurchschnittliche Anforderungen, um sich einen Überblick zu verschaffen. Dies gelte in weit höherem Umfang auch dadurch, dass der BTX-Nutzer, der Bildschirmseite für Bildschirmseite lesen müsse und keine Möglichkeit habe, durch einen schnellen Blick nach oben oder unten wie bei einer ausgedruckten Seite zu vergleichen oder wiederholen zu können.⁶¹

Bei einer Präsentation sind auch die Interaktionsmöglichkeiten für den Benutzer entscheidend dafür, ob er den Dokumentinhalt in zumutbarer Weise oder überhaupt zur Kenntnis nehmen kann. Die Programme bieten dazu verschiedene Ansichten, Funktionen und Buttons zum Blättern, Scrollen und Anzeigen. Durch fehlerhafte oder manipulative Einstellungen im Betriebssystem können Fensterleisten und Schaltflächen verkleinert oder unsichtbar werden, so dass der Benutzer nicht erkennt, dass das Dokument noch weitere Teile enthält. Eine fehlerhafte Tastatur oder Mouse kann dazu führen, dass bestimmte Teile nicht angezeigt werden können. Es kann jedoch bereits problematisch sein, dass bestimmte Teile einer Präsentation nur schwer erschließbar sind:

Fallbeispiel 10: Unerwartet kleiner Bildschirm

Bob ist auf Geschäftsreise unterwegs und möchte mit seinem Palmtop noch einen Kaufvertrag mit Alice per Internet abschließen. Er lädt den langen Vertragstext von Alice herunter und liest die ersten Seiten. Alles OK, er signiert die Order. Die allgemeinen Geschäftsbedingungen mit den besonderen Einschränkungen der Garantieleistungen und Rücktrittsklauseln hat er nicht gelesen, sie befanden sich auf den Bildschirmseiten 35-40 seines kleinen Palmtops. Als er das Gerät später zurückgeben möchte, verweist ihn Alice mit Bedauern auf die AGBs. Als er darauf hinweist, es sei ihm nicht zumutbar gewesen, diese soweit hinten zu lesen, führt ihn Alice an ihren 21 Zoll-Monitor. Dort wird der Text anders umgebrochen, die AGBs sind auf Seite 3.

Mögliche Ursachen

- Mehrdeutigkeit
 - Anderes Ausgabegerät
- Falschpräsentation
 - Falsches, manipuliertes Ausgabegerät

⁶¹ LG Freiburg: Einbeziehung von AGB über Bildschirm, Urteil vom 7. April 1992 - 9 S 138/140, zit. Nach CR 7/1993, 433f. Entsprechende Beschlüsse faßten auch bereits das Landgericht Duisburg in einem Prozeß über einen Partnervermittlungsvertrag über BTX und das Landgericht Aachen. In letzterem Falle wurde bemängelt, dass eine strittige Klausel erst auf den Bildschirmseiten 10-12 der AGBs zu lesen gewesen seien. Dies sei unzumutbar. Zur Anwendung des § 656 BGB auf Partnervermittlung mittels Bildschirmtextes, LG Duisburg, Urt. V. 22.11.1990 - 2 S 161/90 und "Zur Einbeziehung von Allgemeinen Geschäftsbedingungen bei Vertragsabschluß mittels Bildschirmtext", LG Aachen, Urt. V. 31.1.1991 - 6 S 192/90. Ähnlich entschied das Arbeitsgericht Ansbach in einem Fall der Lieferung von Software über BTX. Die vom Kläger angebotene Möglichkeit, "Bedingungen im öffentlichen System" über Bildschirmtext abzurufen, genüge dem AGB-Gesetz nicht. Hier war anscheinend die Zugänglichkeit der AGBs als zu schlecht / zu indirekt bewertet worden (AG Ansbach: Lieferung von Software über BTX, CR 5/1995, 278f.)

3.4.8 Tatsächliche Navigation

Elektronische Dokumente sind anders als Papierdokumente nicht immer linear aufgebaut. Sie können Verweise enthalten, die auf verschiedene Art und Weise durchlaufen werden können. Besonders bei hypertextuellen Dokumenten ist z.T. überhaupt keine einheitliche Reihenfolge festgelegt, sondern das Programm und der Nutzer legen die Reihenfolge selbst fest. In Abhängigkeit von der Reihenfolge des Durchlaufens kann sich jedoch auch ein anderer Inhalt des Dokumentes oder eine andere inhaltliche Deutung ergeben.⁶²

Der Aspekt der Navigation ist bei Papierdokumenten unbekannt. Die für eine Inhaltserschließung zu wählende Reihenfolge ergibt sich sozusagen natürlich (im westlichen Kulturkreis: links nach rechts, oben nach unten, vorne nach hinten). Eine gewisse Analogie kann man zur Frage der Eigenhändigkeit der Erstellung papiergebundener Urkunden herstellen. So ist für Testamente gesetzlich die vollständige eigene (handschriftliche) Erstellung erforderlich, um sicherzustellen, dass der Testamentersteller jeden Aspekt des Dokumentes und seinen inhaltlichen Bezug willentlich erzeugt hat. Ein Maschinen geschriebener Text mit Unterschrift ist hingegen kein gültiges Testament. Hier ist die Eigenhändigkeit bisweilen umstritten (etwa lag eine Handreichung vor).

Fallbeispiel 11: Navigationsreihenfolge in HTML-Vertrag

Alice übernimmt für Bobs Firma einen großen Werkvertrag über die Erstellung eines EDV-Sicherheitskonzeptes und einer Hinweisbroschüre für die Mitarbeiter. Bob hat den Vertragsentwurf als Sammlung mehrerer untereinander verknüpfter HTML-Dokumente erstellt. Die Übersichtsseite enthält u.a. folgende Verweise:

...
Beschreibung der zu leistenden Aufgaben
Hochglanz-Kundenbroschüre, Bericht für die Geschäftsleitung
Druckkosten
 ...

Beim Durchgehen durch die Einzeldokumente liest sie "Kundenbroschüre", dass eine Kundenbroschüre erstellt und 10000 Exemplare gedruckt werden sollen. Im Dokument "Bericht für die Geschäftsleitung" steht, dass der Bericht in fünffacher Ausfertigung zu erstellen ist. Im Abschnitt Druckkosten liest Sie, dass der Vertragsnehmer den zuletzt genannten Druckauftrag in eigener Regie und auf eigene Kosten übernimmt, was sie bei fünf Exemplaren nicht weiter stört. Sie komprimiert das komplette Verzeichnis der Dokumente und signiert die Datei. Nach dreimonatiger Arbeit übergibt Alice Bob fünf Exemplare des Berichts und eine Druckvorlage für die Broschüre. Bob freut sich, dass Alice für ihn den Geschäftsbericht gedruckt habe, muss aber leider dennoch vertragsgemäße Lieferung der 10000 Hochglanz-Kundenbroschüren bestehen.

Mögliche Ursachen

- Mehrdeutigkeit
 - Anderes Programm
- Falschpräsentation
 - Falsches Programm
 - Betriebssystemmanipulation/anderes Betriebssystem

3.4.9 Weitere Aspekte

Die zuvor genannten Aspekte wurden aus vorhandenen Rechtsfällen und Tests des Autors mit existierenden Textverarbeitungssystemen abgeleitet. Es dürfte die wesentlichen in der Praxis

⁶²Idecke/Pordes/Roßnagel ebda., 143.

der Textkommunikation relevanten Aspekte abdecken. Gleichwohl kann die Liste nicht vollständig sein: Die Eigenschaften der Systeme ändern sich ebenso wie das Recht:

In Einzelfällen mag die **Qualität** (Exaktheit, Feinheit,..) einer Ausgabe – unabhängig von deren interpretierbarem Inhalt – eine Rolle spielen. Man denke an Grafiken oder Audiodaten, bei denen die Qualität der Ausgabe von den Endgeräten, Treibern und Programmen abhängt. Man kann sich Fälle denken, wo etwa signierte Fotos, Filme oder Tonaufnahmen aus dem Internet kostenpflichtig erworben werden und man sich anschließend über deren Qualität streitet.

Wird es ein System geben, das Texte in Form eines Filmabspanns abspult, dann mag die **Zeitdauer** der Präsentation einzelner Sequenzen einen rechtserheblichen Aspekt der Präsentation ergeben. Ein dauerhaft vollständiges kanonisches System wesentlicher Aspekte der Präsentation, das mehr als abstrakte Kategorien bietet dürfte leider unmöglich sein.

Teil II: Möglicher Umgang mit dem Präsentationsproblem

4. Sicherheitsvorgaben und Schutzmöglichkeiten

Im Folgenden wird untersucht, welche gesetzlichen Vorgaben zum Präsentationsproblem und seiner Lösung existieren und welche technischen Maßnahmenvorschläge daraus abgeleitet wurden. Schließlich interessieren die individuellen Schutzmöglichkeiten. Es werden jeweils nur die allgemeinen Anforderungen an die Darstellung der signierten Daten untersucht, nicht hingegen an die für Zertifikate, Zeitstempel, Prüfergebnisse und anderer Aspekte.⁶³

4.1 Gesetze und Ausführungsbestimmungen

Interessanterweise enthalten weder das Signaturgesetz noch die Signaturverordnung direkte Vorgaben zur Präsentation signierter Daten.

4.1.1 Signaturgesetz

Das Signaturgesetz⁶⁴ stellt in § 14 SigG (2) Forderungen für die Darstellung zu signierender Daten auf:

Für die Darstellung zu signierender Daten sind technische Komponenten mit Sicherheitsvorkehrungen erforderlich, die die Erzeugung einer digitalen Signatur vorher eindeutig anzeigen und feststellen lassen, auf welche Daten die digitale Signatur sich bezieht. Für die Überprüfung signierter Daten sind technische Komponenten mit Sicherheitsvorkehrungen erforderlich, die feststellen lassen, .. auf welche Daten sich die digitale Signatur bezieht und welchem Signaturschlüsselinhaber die digitale Signatur zuzuordnen ist“.

Auf "welche Daten" sich eine Signatur bezieht, kann auf die Datei, die zu signieren ist, bezogen werden und auf signierte Teile eines elektronischen Dokumentes. Eine enge Auslegung könnte daran ansetzen, dass der Gesetzestext den Begriff „Daten“ verwendet und nicht etwa „Inhalte“. Auf welche Daten sich eine Signatur bezieht, wäre in einer solchen engen Auslegung die Darstellung des Dateinamens, was allerdings nicht die Darstellung zu signierender Daten selbst ist. Eine Darstellung der Daten als Bitfolge oder Hexcode wäre zwar eine Darstellung der signierten Daten, aber eine ziemlich unnütze Form, die nicht dem Zweck des Gesetzes und der Regelung entspräche. Notwendig erscheint daher zumindest eine anwendungsbezogene Aufbereitung, aus der der Dateninhalt erkennbar ist, auch wenn dies das Gesetz nicht explizit fordert. Keine detaillierten Vorgaben lassen sich hingegen hinsichtlich der genauen Form der Präsentation und den anzubietenden Funktionen der Darstellungskomponente ableiten.

⁶³ Solche Aspekte müssen berücksichtigt werden, wenn die Gestaltung von Darstellungskomponenten nach SigG das Thema ist.

⁶⁴ SigG 1997.

Das Gesetz betrachtet den Signiervorgang und den Prüfvorgang jeweils für sich. Die geforderten Maßnahmen beziehen sich auf die Verminderung bzw. Verhinderung der Falschpräsentation durch Fehler und Angriffe. Gefordert wird nicht explizit eine gleichartige Darstellung beim Signierer und beim Prüfer. Die Forderung „die Erzeugung .. eindeutig anzeigen“ könnte als Forderung nach einer festgelegten oder festlegbaren Form der Präsentation verstanden werden. Sie wird jedoch nur im Zusammenhang mit dem Signiervorgang und nicht mit dem Prüfvorgang verwendet und bezieht sich daher wohl nur auf den Vorgang der Signaturerzeugung zu Daten. Auch wenn man im Zuge der Auslegung dieser Rechtsvorschriften unter Berücksichtigung der tatsächlichen Risiken und der Zweckbestimmung des Gesetzes dazu kommen kann, Forderungen an eine intersubjektiv eindeutige und rekonstruierbare Präsentation von Daten aus dem Gesetz abzuleiten, dürften diese umstritten sein. Denn der Gesetzestext selbst und die Begründungen dazu enthält keine klaren Bezüge zum Problem der Mehrdeutigkeit, sondern nur solche zur Falschpräsentation.

4.1.2 Signaturverordnung

Die Signaturverordnung (SigV)⁶⁵ greift die Forderungen des Signaturgesetzes in § 16 SigV Abs. 3 zunächst fast wörtlich auf.

Die zum Darstellen zu signierender Daten erforderlichen technischen Komponenten müssen so beschaffen sein, dass die signierende Person die Daten, auf die sich die Signatur erstrecken soll, eindeutig bestimmen kann, ..“

Im Unterschied zum Gesetzestext stellt die Verordnung eine **Verknüpfung der Darstellung mit der Datenauswahl zum Signieren** her. Dies dürfte so zu verstehen sein, dass einen Start des Signiervorgangs aus der Präsentationskomponente erfolgen muss und Handhabungsbrüche (erneute Dateiauswahl o.Ä.) zu vermeiden sind. Jedenfalls kann nur so eine sichere Anwendung von Signaturverfahren gewährleistet werden.⁶⁶ Interessanterweise spricht § 16 der Signaturverordnung auch nicht nur von „Daten“, sondern auch von „Inhalten“:

*Die technischen Komponenten müssen nach Bedarf den **Inhalt** der zu signierenden oder signierten Daten hinreichend erkennen lassen“*

Was unter "Inhalt" zu verstehen ist, lediglich das Medium (Sprache, Text, Daten) oder auch die konkrete Bedeutung der Daten und die genaue Darstellungsform geht aus dem Text allerdings nicht hervor. Hier gilt das bereits zum Signaturgesetz gesagte: Eine Darstellung der Daten als visualisierte Bitfolge oder Hexcode wäre eine unnütze Form der Darstellung, die dem Zweck des Gesetzes widerspräche. Notwendig erscheint zumindest eine anwendungsbezogene Aufbereitung, aus der der Dateninhalt erkennbar ist, ohne dass allerdings die genaue Form der Präsentation und den anzubietenden Funktionen der Darstellungskomponente vorge-schrieben wäre. Schwieriger ist die Antwort auf die Frage, wonach ein „Bedarf“ zu bemessen sei. Bedarf wird anwendungsbezogen im Zusammenhang mit „hinreichend“ zu verstehen sein: Steht der Inhalt genau fest und kennt der Nutzer diesen genau – etwa weil es sich immer um dieselbe Nachricht handelt (ein Zeitstempel etwa) kann auf die Darstellung der Inhalte verzichtet werden, andernfalls ist eine solche Darstellung erforderlich, aus denen die Inhalte er-

⁶⁵ SigV 1997.

⁶⁶ Siehe hierzu die Experimente zur Verletzlichkeit in den Simulationsstudien, bei denen ein Unterschieben u.a. wegen solcher Handhabungsbrüche mehrfach gelang, Pordesch provet-Arbeitspapier 81, 1992, Pordesch provet-Arbeitspapier 106, 1993 und Pordesch DuD 1993.

kannt werden können (bei einem routinemäßigen Geschäftsvorgang wie der Ausstellung einer Quittung nur die Summe, bei einer formlosen Bestellung via E-Mail der gesamte signierte Text). Nicht gefordert wird jedoch, dass die signierten Dokumententeile in ihrer Darstellung - etwa vom Layout - exakt der entsprechen, die zum Signierzeitpunkt beim Signierer gegeben war oder irgendeiner anderweitig vorgegebenen.

Eine intersubjektive Eindeutigkeit der Präsentation wird nicht explizit gefordert. Lediglich für technische Komponenten, die geschäftsmäßig Dritten zur Nutzung angeboten werden, enthält der Verordnungstext die zusätzliche Forderungen nach einer **eindeutigen Interpretation**:

Werden technische Komponenten nach den Sätzen 1 bis 4 geschäftsmäßig zur Nutzung angeboten, muss die eindeutige Interpretation der Daten sichergestellt sein und müssen die technischen Komponenten bei der Nutzung automatisch auf ihre Echtheit überprüft werden.

Unklar ist zunächst, ob „Interpretation“ als menschliche Interpretation im Sinne von „Verstehen“ und „Auslegen“ einer Erklärung oder als eindeutig zuzuordnender technischer Vorgang (automatisches Erkennen des richtigen Anwendungsprogrammes oder Dateiformates) zu verstehen ist. Da sich das gesamte Signaturgesetz nicht mit den Inhalten der Daten als rechtsverbindliche Erklärungen befasst, ist Letzteres anzunehmen. Die Forderung nach „Eindeutigkeit“ bezieht sich somit auf die Zuweisung des richtigen Datenformates oder Programmes zur Präsentation (Ersteres in enger, Letzteres in weiter Auslegung). „Sicherstellung“ heißt zunächst nur, dass es ein System zur eindeutigen Zuordnung von signierten Daten zu Formaten bzw. Programmen geben muss und in der Signatur oder den signierten Daten ein solcher Hinweis enthalten sein muss. Dem Zweck des Gesetzes würde es aber widersprechen, wenn der Benutzer nicht erkennen könnte, welche Zuweisung vorgenommen wird bzw. wurde, was also implizit gefordert ist.

Allerdings beziehen sich die Forderungen nach eindeutiger Interpretation auch nur auf Komponenten, die **geschäftsmäßig zur Nutzung angeboten** werden: Damit dürften Komponenten gemeint sein, bei denen ein Unternehmen oder eine Privatperson die zur Präsentation (Darstellung) benötigten Systeme einem Nutzer zur Verfügung stellt, um damit Gewinn zu erzielen. Nicht notwendig ist die explizite Entrichtung eines Entgelts, kostenlos angebotene Komponenten werden auch geschäftsmäßig angeboten, wenn ein Unternehmen oder eine Privatperson dies zum Zwecke der Erzielung von Werbeeinnahmen, zur Kundenbindung etc. macht. Entscheidend ist die Gewinnerzielungsabsicht und ein Gewerbe. Zu denken ist also an z.B. öffentliche Internet-Terminals privater Anbieter, an Bankcomputer, Fahrkartenautomaten, öffentlich zugängliche Bestellsysteme im Reisebüro etc.. Hingegen dürften Systeme eines Arbeitgebers, der seinen Mitarbeitern Systeme zur Nutzung zur Verfügung stellt, Systeme, die die Verwaltung ihren Klienten anbietet, privat genutzte oder einem Geschäftspartner kostenlos mal zur Nutzung angebotene Systeme keine geschäftsmäßige Nutzung i.S. des Gesetzes sein.

Zu klären ist noch, was unter „**Darstellungskomponente**“ hier zu verstehen ist: Der lokal genutzte Computer mit Bildschirm oder die von einem Internet-Server herunterzuladende Software (etwa ein Java-Applet eines elektronischen Bestellscheins, das ein Internet-Mall-Betreiber zur Verfügung stellt). Dem Zweck der Regelung – erkennen zu können, welche Daten signiert wurden und bei geschäftsmäßiger Nutzung, wie diese zu interpretieren sind, würde eine Einschränkung auf das lokale (Hardware) System widersprechen. Vom Risiko her ge-

meint sein müssten alle die Darstellung in den genannten Aspekten beeinflussenden Teilkomponenten.

Die Signaturverordnung enthält in § 17 Abs. 1 Vorgaben zur **Evaluierung**, die auch die Präsentationskomponente betreffen

Die Prüfung der technischen Komponenten ... hat die Prüfung der technischen Komponenten nach den „Kriterien für die Bewertung der Sicherheit in der Informationstechnik“ zu erfolgen. Die Prüfung muss bei technischen Komponenten zum Erzeugen und Anwenden privater Signaturschlüssel und bei technischen Komponenten, die geschäftsmäßig zur Nutzung angeboten werden, mindestens die Prüfstufe „E4“ und im Übrigen die Prüfstufe „E2“ umfassen. Die Stärke der Sicherheitsmechanismen muss mit „hoch“ .. bewertet werden sein.

Wenn man nicht in sehr weiter Auslegung eine Darstellungskomponente i.S. des SigG als Komponente zum Anwenden privater Signaturschlüssel bezeichnen will, gilt als Regelprüfstufe für diese Komponenten damit die Prüfstufe „E2“. Lediglich in den Fällen des Anbietens zur geschäftsmäßigen Nutzung (Bankcomputer, Internet-Terminal) wäre „E4“ anzunehmen. Mit hin ist ein elektronisches Bestellformular mit Software, das Kunden zur Anzeige der zu signierenden Bestelldaten von ihrem Diensteanbieter herunterladen eine nach „E4“ zu prüfende Komponente. Das zur Darstellung im Browser verwendete Teilsystem (etwa Browser-Plug-In), das der Kunde unabhängig vom Hersteller irgendwo käuflich erworben hat, ist hingegen keine geschäftsmäßig zur Nutzung angebotene Komponente und wäre demnach mit „E2“ zu prüfen – wenn nicht wiederum ein geschäftsmäßig zur Nutzung angebotenes öffentliches Terminal verwendet wird.

4.1.3 Gesetzesvorhaben

Weder das Signaturgesetz noch die Signaturverordnung regeln die Verwendung digital signierter Dokumente im Rechtsverkehr. Sollen digital signierte Dokumente auch in den Bereichen Anwendung finden, in denen dies bislang nicht zulässig ist, müssen zuvor - etwa durch Änderungen im Bürgerlichen Gesetzbuch (BGB) - die rechtlichen Grundlagen geschaffen werden. Das Bundesministerium des Inneren bereitet derzeit solche gesetzlichen Änderungen vor.⁶⁷

Im Entwurf eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts an den modernen Rechtsgeschäftsverkehr⁶⁸ wird im § 126a eine **elektronische Form** eingeführt, auf die dann an verschiedenen anderen Stellen des geänderten BGBs Bezug genommen werden soll.

Soll die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden, so muss der Aussteller der Erklärung dem Text seinen Namen hinzufügen und das elektronische Dokument mit einer digitalen Signatur nach dem Signaturgesetz versehen.

Der Verweis auf "Text" bestimmt, dass die Erklärung aus Text bestehen muss, andere neue Medien (Audio/Video) werden damit ausgeschlossen. Weitere Anforderungen an die Präsentation gibt es nicht - mit Ausnahme derjenigen, die aus dem Signaturgesetz abgeleitet werden können.

⁶⁷ Siehe auch die ursprünglichen Vorschläge der Bundesnotarkammer Erber-Faller 1996.

⁶⁸ BMJ 1999.

Zusätzlich führt § 126b eine **Textform** ein:

Ist durch Gesetz Textform vorgeschrieben, so muss die Erklärung einem anderen gegenüber so abgegeben werden, dass sie in Schriftzeichen lesbar und die Person des Erklärenden angegeben ist

Damit würde die Textform als Übermenge definiert, die sowohl die elektronischen Dokumente mit Signatur, solche ohne und auch herkömmliche papiergebundene Dokumente umfasst.⁶⁹ Auch gibt es außer der "Lesbarkeit als Schriftzeichen" keine Vorgaben zur Präsentation.

Der elektronischen Form scheint also ein elektronisches Dokument dann zu entsprechen, wenn es so ausgegeben werden kann, dass am Bildschirm Schriftzeichen erkennbar sind. Vorgaben, welche Art Schriftzeichen und wie diese darzustellen sind enthalten die Gesetzesvorschläge nicht.

4.1.4 Europäische und amerikanische Reglungsansätze

Der Richtlinienentwurf der Europäischen Kommission ist technisch wesentlich unbestimmter gefasst als die bundesdeutschen Regelungen.⁷⁰ Er legt keinerlei verbindliche Forderungen an die Präsentation digitaler Daten fest. Dementsprechend enthält das erste darauf basierende nationalen Regelwerk Österreichs offenbar keine diesbezüglichen Regelungen.⁷¹

Es ist nicht ersichtlich, dass in der Gesetzgebung amerikanischer Bundesstaaten Regelungen zur Frage der eindeutigen Präsentation enthalten wären.⁷² Über alternative Regelungsmodelle in anderen Staaten ist nichts bekannt.

4.1.5 Zusammenfassung

Nach der o.g. Auslegung enthalten die bestehenden rechtlichen Bestimmungen des Signaturgesetzes und der Signaturverordnung also folgende **inhaltliche Vorgaben**

- Der Nutzer soll eine sichere Datenauswahl beim Signieren und Prüfen einsetzen um das lokale Risiko der Falschpräsentation zu reduzieren. Die Darstellung selbst hat hinreichend eindeutig zu erfolgen, um den Inhalt der Daten anwendungsbezogen zu erkennen, wobei der Nutzer selbst den Anwendungsbezug herzustellen hat und für die Modalitäten der Präsentation und Funktionen des Präsentationssystems zu sorgen hat.
- Bei geschäftsmäßig zur Nutzung angebotenen Komponenten wird ferner ein eindeutigen Bezug auf ein zu verwendendes Datenformat gefordert.

Diese (nicht näher spezifizierten und deshalb jeweils konkretisierungsbedürftigen) Vorgaben sind mit folgenden **Prüfstufen** nach ITSEC zu evaluieren:

- bei Komponenten mit geschäftsmäßig zur Nutzung „E4“ hoch
- „E2“ hoch sonst

Geschäftsmäßig zur Nutzung angebotene Komponente bedeutet in diesen Vorschriften

⁶⁹ Es ist aber fraglich, ob die einfache Form ohne Signatur auch umfaßt sein soll, da die Textform an vielen Stellen eingeführt wird, wo bislang schriftliche Erklärungen erforderlich waren (und da waren Unterschriften erforderlich).

⁷⁰ Brisch CR 1998, 492ff.

⁷¹ Menzel / Schweighofer, DuD 1999, 503 ff.

⁷² Miedbrodt DuD 1998.

- jede Teilkomponente, die die Darstellung bestimmt (Hardware und Software, auf Server oder lokal)
- mit der Absicht der Gewinnerzielung angeboten wird,
- und bezogen auf einen Vorgang zur Verfügung gestellt wird.

Das Gesetz fordert also eine anwendungsbezogene Aufbereitung, aus der der Signierer und der Prüfer den Inhalt der zu signierenden Daten und signierter erkennen können. Die richtige Auswahl des Anwendungskontextes und des richtigen Präsentationsprogramms und die Modalitäten der Darstellung im Einzelnen obliegen demnach dem Signierer und Prüfer. Nur bei geschäftsmäßig angebotenen Komponenten ist eine eindeutige Interpretationsvorschrift (i.S. Datenformat, Programm) aus den signierten Daten abzuleiten.

4.2 Technische Anforderungen und Spezifikationen

Auf der Basis des Signaturgesetzes und der Signaturverordnung hat das Bundesamt für die Sicherheit in der Informationstechnik (BSI) Maßnahmekataloge und ein Handbuch erstellt, mit denen auch die genannten Vorschriften zu den technischen Komponenten konkretisiert werden sollen. Auch wenn diese Maßnahmekataloge keinen Gesetzescharakter haben können, ist die Behörde zumindest nach § 16 Abs. 6 zur Veröffentlichung solcher Kataloge geeigneter Maßnahmen ermächtigt. Man kann also zumindest davon ausgehen, dass diese Frage bei der Beweiswürdigung digital signierter Dokumente zu berücksichtigen wäre. Dies gilt m.E. nicht für die gegenwärtig in Entwicklung befindlichen Signaturinteroperabilitätsspezifikationen⁷³, die nur *mögliche* Lösungen und Vorschläge für interoperable Verfahren enthalten und weder im Gesetz noch in der Verordnung erwähnt werden.

4.2.1 Maßnahmekataloge

Die von der Regulierungsbehörde für Post und Telekommunikation herausgegebenen Maßnahmekataloge gemäß § 12 und § 16 der Signaturverordnung konkretisieren die unscharfen Anforderungen des Signaturgesetzes und der Signaturverordnung an die Präsentation nicht weiter. In Abschnitt 1.6. Anwenderinfrastruktur finden sich lediglich die Anforderungen,

- dass die Anwenderinfrastruktur "die Daten, die dem Signierer dargestellt werden, zuverlässig, eindeutig und unverfälscht signieren muss" (A-SHIF1), sowie dass sie "nur die Daten signieren" darf, "die dem Schlüsselinhaber dargestellt wurden" und
- dass sie "die Daten, die dem Verifizierer dargestellt werden, zuverlässig, eindeutig und unverfälschbar verifizieren" muss.

Die Vorschriften nehmen Bezug auf die gesamte Anwenderinfrastruktur, nicht eine Darstellungs- bzw. Präsentationskomponente. Sie sind insoweit sogar einschränkend, weil sie Anwenderinfrastruktur als das lokale Präsentationssystem verstehen, nicht aber z.B. herunterladbare Programme eines Servers. Auf Komponenten zur geschäftsmäßigen Nutzung werden Vorschriften zur Darstellung nicht weiter konkretisiert. Somit gehen die Maßnahmekataloge sogar im Konkretisierungsniveau eher noch einen Schritt hinter die Signaturverordnung zurück und sind hier nicht weiter behandlungsbedürftig.

⁷³ SigI 1999.

Die um konkrete Lösungsvorschläge angereicherten **Maßnahmenkataloge** des Bundesamtes für die Sicherheit in der Informationstechnik⁷⁴ (das so genannte BSI-Handbuch) enthalten auch einige Vorschläge zu Darstellungskomponenten. So fordert M-SHIF 3.2 die "Verwendung einer sicheren Visualisierungskomponente beim Signiervorgang" und "dass die Anzeige der Daten und der zugehörigen Signierinformationen eindeutig und vollständig erfolgt". Dem Anwender müsse "eine Funktion zur Verfügung (ZOOM, Scroll) gestellt" werden, "mit der er alle Teile der Darstellung auswählen kann und in ausreichender Genauigkeit anzeigen lassen kann." Entsprechendes fordert M-SHIF 3.3 für den Prüfvorgang merkwürdigerweise nicht. Die Vorschriften bzw. Umsetzungsvorschläge spezifizieren nicht näher, was mit "Eindeutigkeit" gemeint ist und sind ausschließlich auf am Bildschirm darstellbare Informationen (Texte und Bilder) ausgerichtet.

4.2.2 Spezifikationen

Zu Signatur- und Datenformaten sowie Darstellungskomponenten gibt es eine Fülle von Spezifikationen, die hier nicht im Einzelnen darzustellen sind. Interessant sind die Spezifikationen, die auf der Basis der genannten rechtlichen Anforderungen des Signaturgesetzes entstanden sind, die vom Bundesamt für die Sicherheit in der Informationstechnik herausgegebenen Signaturinteroperabilitätsspezifikationen (SigI).⁷⁵ Diese sollen den rechtlichen Vorgaben entsprechen und beanspruchen damit das gesetzliche Privileg als "sicher zu gelten" mit den möglicherweise daraus folgenden Beweiserleichterungen.⁷⁶ Außerdem wurden sie auf der Basis vorhandener Internet-Standards und Drafts entwickelt. Die Signaturgesetzanforderungen sind generell schärfer als sonst diskutierte Anforderungen, so dass sich die zumindest die Kritik an unzureichender Regelung auch auf anderen Spezifikationen wie z.B. Mailtrust⁷⁷ übertragen lässt.

i) Signaturinteroperabilitätsspezifikationen (SigI)

Die Signaturinteroperabilitätsspezifikationen enthalten keinen eigenen Abschnitt zur Gestaltung von Präsentationssystemen, vermutlich weil die Präsentation letztlich als Angelegenheit des lokalen Systems betrachtet wird und nicht als Kooperationsproblem, das einer interoperablen Lösung bedarf. Konsequenterweise enthält Abschnitt A2 der SigI⁷⁸ Vorschläge für die Datenformate von Signaturen und auszutauschenden Nachrichten, die aus den signierten Nutzdaten, Signaturen, Zertifikaten und anderen Datenelementen bestehen (sogenannte Signaturaustauschobjekte).

Als Teil des Signaturblocks ist neben Zeit- und anderen wahlfreien Angaben ein Feld **Contenttype** vorgesehen. Dieses obligatorische und mitzusignierende Feld soll einen Object-Identifier (OID) enthalten, der einen „Datentyp“ bezeichnet und auf den Inhalt und Typ der Nutzdaten verweist. Im Anhang des Abschnitts ist dann noch eine Liste von Datentypen zu finden, die Bezeichner gängiger Datenformate von Textverarbeitungs- und Grafikprogrammen sowie universeller Formate wie ASCII und „binären Daten“ enthält. OIDs sind dabei angegeben - soweit diese existieren bzw. als noch fehlend markiert.

⁷⁴BSI 1998

⁷⁵Berger DuD 1999

⁷⁶Auf das Privileg wird später noch näher eingegangen (Teil II:5.3.3i) Sicherheitsvermutung des Signaturgesetzes.

⁷⁷Biester DuD 1999.

⁷⁸SigI 1999.

Mit dem Rückgriff auf die von verschiedenen internationalen Organisationen verwalteten weltweit eindeutigen OIDs könnte ein stets eindeutiger Bezug zu einem Datenformat hergestellt werden. Die Auswahl ist jedoch noch willkürlich, es fehlt eine die Formate registrierende Instanz. Universelle Formate, wie „ASCII-Text“ und „binäre Daten“ sind ebenso mehrdeutig wie die Rohdaten, aus ihnen läßt sich per se nicht auf irgendeine Interpretation schließen. Und generell enthält das Datenformat kein Bezug zu speziellen Darstellungsprogrammen und Hardwarekomponenten. Letteres wird von den Autoren bewusst abgelehnt, weil es eine "unüberschaubare Vielzahl von Darstellungskomponenten mit einer Vielzahl von Parametern gibt, die für die Darstellung von Bedeutung sind".⁷⁹ Diese Beschränkung entspricht den vagen Vorgaben des Signaturgesetzes und der Signaturverordnung zur Präsentation.⁸⁰ Etwas verwunderlich ist nur, warum die Autoren den Datentyp als obligatorisch anzugeben ansehen, wo dies nach den obigen rechtlichen Ausführungen wohl nur für Komponenten zur geschäftsmäßigen Nutzung anzunehmen wäre.

Weitere Spezifikationen zur Darstellungskomponente enthalten die SigI nicht. Abschnitt A3 zur Anwenderinfrastruktur enthält lediglich noch Vorschläge für Ausgabetexte bei Signaturprüfungen.⁸¹

ii) European Electronic Signature Standardisation Initiative (EESSI)

Auf europäischer Ebene soll mit der "European Electronic Signature Standardisation Initiative"⁸² den SigI entsprechend Interoperabilitätsspezifikationen entwickelt werden. Zu Präsentationskomponenten oder auch nur Datentypen in Signaturformaten enthalten diese Vorgaben bislang jedoch keine Vorgaben.

4.2.3 Zwischenfazit

Weder das Signaturgesetz und Signaturverordnung, noch die Maßnahmekataloge, BSI-Handbuch und die SigI gehen systematisch auf das Problem der Präsentation oder bieten Lösungen an. Sie enthalten lediglich einzelne Hinweise auf das Problem und partielle Lösungsvorschläge - vor allem eine OID für den Contenttype als Teil der zu signierenden Daten.

Für den allgemeinen Fall ist daher davon auszugehen, dass zur Interpretation und Präsentation signierter Daten keine Vorgaben existieren. Die Daten enthalten im Allgemeinen also insbesondere keine Angabe des zu verwendenden Programms, der Hardwarebasis, des Betriebssystems oder irgendwelcher Einstellungen. Solche Angaben und Rückschlussmöglichkeiten darauf sind abhängig vom jeweiligen Datenformat und somit dem Anwendungskontext.

4.3 Individuelle Schutzmöglichkeiten

Bevor die Frage erörtert wird, welche Beweismöglichkeiten und Fragestellungen sich für die Sachverständigendenbegutachtung aus den genannten Risiken ergeben, soll zunächst kurz erörtert werden, welche Möglichkeiten die Beteiligten haben, sich auf der Basis der vorhande-

⁷⁹ SigI 1999A2, S.19.

⁸⁰ Siehe oben die Anmerkungen zum Signaturgesetz, S. 53.

⁸¹ SigI 1999A3.

⁸² EESS_99.

nen Technik zu schützen. Dabei wird wiederum zwischen dem lokalen Risiko falscher Präsentation und dem Kooperationsrisiko der Mehrdeutigkeit unterschieden.

4.3.1 Verringerung des Mehrdeutigkeitsrisikos

i) Geeignete Austauschformate

Für den rechtsverbindlichen Austausch von Dokumenten können Austauschformate gewählt werden, bei denen die Präsentation der Daten möglichst wenig von externen Daten oder benutzerdefinierten Einstellungen des Betriebs- oder Anwendungssystems abhängt und plattformunabhängig möglichst eindeutig erfolgt. Verbleibende Mehrdeutigkeitsrisiken sind dann durch Einschränkungen dieser Formate bzw. ergänzende Vereinbarungen zu lösen.⁸³ Für die Textkommunikation kommen insbesondere folgende Formate in Frage:

Postscript und PDF

Aufbauend auf dem Postscript-Standard für die Druckausgabe von Daten hat die amerikanische Firma Adobe mit PDF⁸⁴ ein plattformunabhängiges Format für den Dokumente definiert. Das PDF-Format soll auch beim Transfer zwischen unterschiedlichen Hardware- und Betriebssystemen „zuverlässig jede Schrift, jedes Bild und jede Farbe des Originals bewahren“. Das Format ist vor allem für die Präsentation und Archivierung von Dokumenten vorgesehen: Dokumente, die mit irgendeinem Bürosystem erzeugt wurden (z.B. MacWord), werden in PDF konvertiert, wobei ein Großteil der Strukturinformationen (z.B. symbolische Absatzformatierung) ignoriert wird, und stattdessen eine Konvertierung in Vektorgrafiken und ASCII-Text erfolgt und damit verbunden eine erhebliche Komprimierung. Über den kostenlosen Acrobat-Reader kann jeder Empfänger eines Dokumentes dessen Inhalt darstellen. Eine Weiterverarbeitung ist jedoch aufgrund der verlorenen Strukturinformationen nur über kostenpflichtige Bearbeitungsprogramme und auch nur eingeschränkt möglich. So können einzelne Zeichen geändert werden, nicht aber der Zeilen- und Seitenumbruch. PDF ist somit ein „finals Format“, es ist ein zur Archivierung vorgesehener Endzustand elektronischer Dokumente und beansprucht in dieser Hinsicht (nach den Vorstellungen von Adobe) zu einem quasi Weltstandard zu werden. Mittlerweile wird auch die Signiermöglichkeit angeboten, wobei jeweils ganze Dokumente signiert werden und die Signatur in der Dokumentdatei abgespeichert wird.⁸⁵

Im Ansatz entschärft der PDF-Standard einige Probleme der Mehrdeutigkeit, weil die wichtigsten Formatierungsinformationen untrennbar Teil des Dokumentes sind. Der Standard alleine garantiert jedoch noch nicht, dass keine Mehrdeutigkeiten entstehen können. Vielmehr hängt es davon ab, in welcher Weise PDF-Dokumente aus Anwendungssystemen heraus erstellt werden. So muss der Nutzer, der ein PDF-Dokument – etwa mittels des Adobe-Konvertierungstools aus einem Word-Dokument erzeugt- auch tatsächlich die verwendeten Zeichensätze einbetten, auf Links und berechnete Felder bei der Dokumenterstellung verzichten, u.v.m.. Dies kann er durch die Auswahl bzw. Konfigurierung eines geeigneten „Profils“ für die Konvertierung und Vorsichtsregeln bei der Dokumenterstellung. Keine Lösung bietet

⁸³ Siehe Abschnitt Teil II:4.3.1ii).

⁸⁴ Aktuelle Spezifikation unter <http://www.adobe.com>.

⁸⁵ Angaben aus der Präsentation von Adobe bei der GMD am 12.10.99.

das Format hinsichtlich der Überprüfung geeigneter Endgeräte. Der Hauptnachteil von PDF besteht jedoch auch darin, dass es sich um ein finales Format handelt. Eine automatische Weiterverarbeitung ist kaum möglich und für formularorientierte Anwendungen eignet sich das Format nicht.

XML

Große Hoffnungen für die Lösung aller Kompatibilitätsprobleme bei Dateiformaten werden mit der Datendefinitionssprache XML verbunden. XML ist eine Sprache zur Definition und zum Austausch von Daten, die man als Weiterentwicklung des HTML-Standards und eine Einschränkung des zu komplexen SGML-Standards für Daten- und Dokumentformate auffassen kann.⁸⁶ XML gibt eine allgemeine, durch Menschen lesbare Syntax vor (ASCII-codiert und auszeichnungsbasiert wie HTML mit Tags), in der die unterschiedlichsten Datenformate definiert werden können. Sie können mit Stylesheets versehen werden, die die Daten in eine bestimmte darstellbare Form umsetzen (etwa in HTML).

Die Frage ist nahe liegend, ob nicht XML geeignet sein könnte, die Probleme möglicher Mehrdeutigkeiten zu lösen. XML weist tatsächlich gewisse Vorteile für die Präsentation auf. Zu nennen ist die klare Gliederung zwischen Datendefinition, den eigentlichen Daten und dem Stylesheet (bzw. XSL), was die Möglichkeit zur vollständigen Offenlegung der Datendefinition im Dokument und der Darstellungsvorschriften bietet. Durch die Möglichkeit, den XML-Quelltext als ASCII-Text zu lesen, können auch normalerweise nicht sichtbare Markierungen und vom jeweiligen Browser nicht auswertbare Informationen sichtbar gemacht werden. Enthalten die Tags verständliche Namen etwa "</kontonummer>", so kann bereits mit einem ASCII-Editor als Präsentationsprogramm der Rückschluss auf den Präsentationskontext der Daten (Bankanwendung, sicher keine Urlaubskarte) möglich werden.

Andererseits ist XML zunächst auch "nur" eine universelle Datendefinitionssprache, die richtig angewendet werden muss. XML erzwingt nicht die Vergabe verständlicher Tag-Namen, ein Feld mit einer Kontonummer kann statt "</kontonummer>" ebenso gut den nichts sagenden Namen "</Datenfeld1>" erhalten. Analog zu PDF und Word müssen Stylesheets (bzw. XSL-Dateien) mitsigniert, Grafiken in die Dokumente eingebunden und andere Maßnahmen ergriffen werden. Die Beschreibungssprache XML enthält per se auch keine Vorgaben zum Vorhandensein bestimmter Ausgabegeräte, zur Verwendung bestimmter Browser, zur Navigation durch ein XML-Dokumente usw.. XML stellt aber Sprachelemente zur Verfügung stellen, solche Anforderungen in das Dokument geeignet zu integrieren und dann mit geeigneten Auswertungsprogrammen auszuwerten.

XML löst also das Präsentationsproblem nicht, es ermöglicht durch seine Offenlegung der Datendefinition und die Ausdrucksmittel aber sinnvolle Lösungen.⁸⁷

ii) Vereinbarungen zur Nutzung

Alleine die Verwendung geeigneter Formate löst also nicht das Mehrdeutigkeitsproblem, die Verwendung muss um Vorgaben zur Nutzung ergänzt werden (s.u.) die verbleibende Probleme (etwa Einbindung von Schriften, zu verwendenden Viewer etc.) behandeln.

⁸⁶ S. hierzu Möhr / Schmidt 1998, Goldfarb 1998, Grimm/Wäsch 1999.

⁸⁷ Entsprechend Schmitt 1999.

Soweit Signierer und Prüfer in einer dauerhaften Kooperationsbeziehung stehen, können die die Interpretation und Präsentation von Daten betreffenden Aspekte vertraglich vereinbart werden. Die Beteiligten wären dann an die Vorgaben dieser Vereinbarung gebunden.

Solche Vorgaben können in Rahmenverträgen zwischen Geschäftspartnern festgelegt werden, wie dies heute z.B. bei der Bucherstellung in Autorenverträgen teilweise bereits geschieht. Sie könnten auch in Allgemeinen Geschäftsbedingungen (AGBs) festgelegt werden: "Für an uns gesendete signierte Dokumente und von uns gesendete signierte Dokumente gilt grundsätzlich folgende Präsentationsform...". Inwieweit dies rechtlich zulässig ist, wäre in einer juristischen Arbeit zu untersuchen. In den Vereinbarungen können die zu nutzenden Präsentationsprogramme, Mindestanforderungen an die Hardware, ausschließlich zu nutzende Layoutvorlagen und Zeichensätze und die als maßgeblich für den Inhalt anzusehende Ansicht (bei Word etwa Datei.Seitenansicht mit einem bestimmten Postscriptdrucker-Treiber).

4.3.2 Verringerung des Risikos der Falschpräsentation

i) Schutzvorkehrungen des Signierers

Für einen Signierer ist es grundsätzlich problematisch zum Signieren eine Anwenderinfrastruktur zu verwenden, die er selbst nicht kontrolliert. Besonders riskant ist es, wenn Komponenten genutzt werden, die nicht von jemandem kontrolliert werden, der aus Fehlern oder Manipulationen des Signierers Nutzen ziehen kann, etwa ein Vertrags- oder Geschäftspartner. Statt dessen sollte der Signierer stets eine von ihm selbst kontrollierte Umgebung zu nutzen. Selbst kontrolliert bedeutet, dass der Nutzer selbst die Software ausgewählt und die Konfiguration selbst bestimmt, die Wartungsarbeiten selbst durchführt oder überwacht und zu dem nur er selbst Zugang hat.

Dieses Vorgehen gewährleistet keineswegs absoluten Schutz - Viren können nach wie vor z.B. über Netzzugänge eingeschleust werden, Programme können fehlerhaft sein usw.. Der Schutz hat aber eine hohe praktische Wirkung, da ein Kooperationspartner in der Regel keine Zugangsmöglichkeiten hat und Manipulationen vornehmen kann. Diejenigen, die dies könnten - etwa Systembetreuer – haben hingegen in der Regel keinen unmittelbaren Nutzen aus Fehlern oder Manipulation (können sich aber leicht ihren Ruf ruinieren). Außerdem kennt der Nutzer ein von ihm genutztes System und seine Konfiguration genau, so dass auch Fehler seltener auftreten.

Einen Vertragsentwurf sollte man also nicht auf dem Computer des Vertragspartners präsentieren. Man kann ihn sich per E-Mail zusenden lassen und dann auf dem PC zu Hause präsentieren und signieren. Eine solche Strategie wird freilich in vielen Fällen nicht realisierbar sein: Unterwegs - etwa beim Einkauf oder auf Reise - steht das eigene Präsentationssystem nicht zur Verfügung. Hier können langfristig portable Benutzerendgeräte eine Lösung sein, auf die die zu signierenden Dokumente zur Präsentation und zum Signieren und Prüfen transferiert werden.⁸⁸ Im beruflichen Alltag ist jeder Arbeitnehmer gezwungen, die Anwenderinfrastruktur seines Arbeitgebers zu nutzen, so dass möglicherweise nicht einmal diese Strategie nutzt.

⁸⁸ Pfitzmann u.a. Computer 1997, Pordesch 1995.

Externe Bezüge meiden oder mitsignieren

Wer als Signierer eine mögliche Missinterpretation des von ihm zu signierenden Dokumentes vermeiden will, sollte versuchen, möglichst viele der in die Präsentation eingehenden Daten mitzusignieren und unsignierte externe Daten zu vermeiden. Zeichensätze sind einzubinden, Grafiken einzubetten, Links und aktualisierbare Dokumentvorlagen sind zu vermeiden. Soweit sie sich nicht vermeiden lassen sind eindeutige Bezüge herzustellen (etwa relative Dateipfade zu Grafikdateien) und die entsprechenden Dateien sind mitzusignieren – etwa indem man Dokument, Dokumentvorlage und Grafiken zuvor in eine Datei komprimiert erst dann signiert.

Dokumente selbst erzeugen

Wer Dokumente signiert, die von anderen erzeugt wurden, geht ein gewisses Risiko ein, dass diese einen anderen Inhalt haben, als er sich am Bildschirm präsentieren lässt. Konfigurationsunterschiede und Nachlässigkeiten, etwa ein vorgelegtes Dokument nicht vollständig betrachtet zu haben, sind auch in der eigenen sicheren Systemumgebung immer möglich. Hingegen wird man bei Dokumenten, deren Inhalt man selbst erzeugt, d.h. durchdacht und aufgeschrieben hat, kaum etwas "blind" signieren. Es ist sicherer, eine Vertragsbestätigung per E-Mail kurz und formlos selbst zu erstellen und zu signieren, als eine vom Vertragspartner vorgelegte Dokumentvorlage auszufüllen und zu signieren.

Zweckgebundene Signierschlüssel

Damit signierte Dokumente nicht in einem anderen Zusammenhang durch ein anderes Präsentationsprogramm völlig anders dargestellt werden, hilft es über Zusicherung im Zertifikat zweckgebundene Signierschlüssel zu verwenden. Sie binden die Schlüsselerwendung für jeden Empfänger prüfbar an einen bestimmten Zweck (etwa Zahlungsverkehr), ein bestimmtes Anwendungsfeld (etwa unternehmensinterne Anwendung) oder einen maximalen Transaktionswert (etwa bis 1000 DM). Eine Zweckentfremdung signierter Dokumentteile und eine grobe Verfälschung des Präsentationskontextes kann dann erkannt werden.

ii) Schutzvorkehrungen des Prüfers

Eigene Anwenderinfrastruktur nutzen

Die Präsentation eines signierten Dokumentes auf einer Anwenderinfrastruktur, die anderen kontrolliert wird, ist unsicher. Man sollte statt dessen eine eigene Anwenderinfrastruktur verwenden. Eine solche Strategie wird freilich in vielen Fällen nicht realisierbar sein (Arbeitsverhältnis s.o.). Hier helfen aber noch andere Strategien.

Formale Prüfung des Dokumentinhaltes

Grundsätzlich ist einer Präsentation zu misstrauen. Es ist zu versuchen genau festzustellen, was wirklich signiert wurde und welche in die Präsentation eingehenden Daten unsigniert und mithin abstreitbar sind. Durch Wahl verschiedener Ansichten kann man versuchen, Mehrdeutigkeiten zu erkennen. Erkannt werden muss insbesondere, inwieweit ein Dokument Bezüge auf externe Daten enthält (Dokumentvorlagen, Links, Grafiken, aktualisierbare Felder).

Unterschiedliche Präsentationssysteme nutzen

Ein Prüfer, der signierte Dokumente erhält, kann versuchen, verschiedene Möglichkeiten der Präsentation zu erproben, um mögliche Änderungen wesentlicher Aspekte erkennen zu können. Zu denken ist an wiederholte Präsentationsvorgänge unter Verwendung unterschiedlicher Programme und unterschiedlicher Einstelloptionen. Da der normale Benutzer nicht einmal alle möglichen Einstellungen kennt, kann es sinnvoll sein, Computer unterschiedlicher Benutzer zu verwenden, um zumindest Absonderlichkeiten der eigenen Infrastruktur zu erkennen.

5. Gerichtliche Beweisführung

Für die Frage, wie mit Hilfe signierter Dokumente künftig etwas bewiesen werden kann, sind die Risiken der Mehrdeutigkeit oder Falschpräsentation nicht unmittelbar relevant. Die Notwendigkeit bestimmte Beweise zu führen ergibt sich vielmehr erst aus den Prozessen, in denen die Echtheit oder Gültigkeit signierter Dokumente umstritten ist. Sachverständige werden dann beauftragt werden, wenn eine unmittelbare Beweismittelwürdigung durch die Gerichte wegen des fehlenden Sachverständnisses oder des hohen Aufwands der Prüfung nicht möglich ist.⁸⁹ Zu untersuchen ist daher, inwieweit digital signierte Dokumente als Beweismittel in Gerichtsprozessen künftig eine Rolle spielen könnten und welche Beweisfragen Richter mit allgemeinen Erfahrungssätzen und gesetzlichen Beweiserleichterungen lösen können.

5.1 Beweisrechtliche Grundlagen

5.1.1 Verfahrenstypen

Die Nachweispflichten und beweisrechtliche Bestimmungen unterscheiden sich abhängig vom Typ des Gerichtsverfahrens etwas:

- **Strafverfahren:** In diesen Verfahren treffen Staat und Bürger aufeinander und es geht um den Nachweis begangener Straftaten. Für die Beweisführung gelten die Regeln der Strafprozessordnung (StPO).
- **Zivilverfahren:** Hier treffen streitende Parteien aufeinander und es geht darum nachzuweisen, dass der Kläger einen Anspruch gegen den Beklagten durchsetzen möchte. Für die Beweisführung gelten die Regeln der Zivilprozessordnung (ZPO).
- **Verwaltungsverfahren:** In diesen Verfahren treffen Bürger und Verwaltung aufeinander und es geht darum, über die Rechtmäßigkeit oder Unrechtmäßigkeit eines Verwaltungshandelns zu entscheiden. Für die Beweisführung gelten die Regeln der Verwaltungsgerichtsordnung (VwGO).

Neben diesen Haupttypen, die im Folgenden hinsichtlich einiger Abweichungen beachtet werden, gibt es noch Arbeitsgerichtsverfahren, Sozialgerichtsverfahren, Schiedsgerichtsverfahren usw., deren beweisrechtliche Vorgaben jedenfalls hinsichtlich des interessierenden Gegenstands den zivilrechtlichen ähneln und die hier nicht betrachtet werden.

5.1.2 Signierte Dokumente als Beweismittel

Mögliche Beweismittel im Zivil- und im Strafprozess sind der Augenschein, Zeugen, Urkunden, Sachverständige und amtliche Auskünfte. Im Zivilrecht kommt noch die Parteivernehmung hinzu, im Verwaltungsverfahren ist dies die Beteiligtenvernehmung.⁹⁰

⁸⁹ Sicher können Signatursachverständige auch unabhängig von Gerichtsverfahren im Rahmen polizeilicher Ermittlungen oder auch in privatem Auftrag tätig werden. Doch auch in diesen Fällen werden sich die Fragestellungen vorwiegend an möglichen späteren Gerichtsprozessen orientieren, schon alleine wegen der Kosten und dem Wunsch diese dann auch einzutreiben.

⁹⁰ Creifelds 1996, 216. Folter und Weissagungen wären andere – im Mittelalter übliche – Mittel zur "Wahrheitsfindung", die damit ausgeschlossen sind.

Es ist heute weitestgehend unumstritten, dass signierte Dokumente nicht als Urkunden im Sinne des Zivilrechts gelten. Ihnen fehlt die dauerhafte Verkörperung auf einem Träger und die unmittelbare Wahrnehmbarkeit von Papierdokumenten.⁹¹ Digital signierte Dokumente können jedoch als Objekte des Augenscheins Verwendung finden. Beim richterlichen Augenschein erhebt das Gericht Beweis durch unmittelbare sinnliche Wahrnehmung, neben dem „Sehen“ auch durch Hören, Fühlen und Schmecken.⁹² Mit dieser rechtlichen Festlegung wird bereits klar, dass nicht die Daten selbst sondern ihre Präsentation dann das durch den Richter wahrnehmbare Augenscheinsobjekt sind. Denn die signierten Daten (Bits) selbst sind nicht wahrnehmbar, und würden ohne eine Präsentation unter keine der genannten Kategorien zulässiger Beweismittel fallen. Dies erklärt die bislang zu Unrecht vernachlässigte zentrale Bedeutung der physischen Präsentation für die Beweiswürdigung signierter Dokumente.

Das Strafrecht kennt daneben auch die elektronische Urkunde: Ein "EDV-Dokument ist eine mit einem technischen Mittel verkörperte, jedoch nicht schriftlich niedergelegte Erklärung, die allgemein oder für Eingeweihte verständlich ist, den Aussteller (Erklärenden) erkennen lässt und die zum Beweis einer rechtlich erheblichen Tatsache bestimmt ist."⁹³ Dies hat jedoch keine Bedeutung für die Beweiswürdigung als Augenscheinsobjekt, sondern führt dazu, dass bei Fälschung oder Verfälschung eines elektronischen Dokumentes die mit der Urkundenfälschung zusammenhängenden Straftatbestände Anwendung finden können.⁹⁴

5.1.3 Formen elektronischer Beweismittel

Nachdem geklärt ist, dass signierte Dokumente mittels einer physischen Präsentation zulässiges Beweismittel werden, erhebt sich noch die Frage, ob irgendwelche Aussagen hinsichtlich der Art zu erwartender Beweismittel (Medium, Format,...) getroffen werden können.

Im zivilen Rechtsverkehr gilt für Willenserklärungen der Grundsatz der Formfreiheit. Dies bedeutet, dass die Menschen bei dem Erklären ihres Willens und dem Abschluss von Verträgen untereinander nicht bestimmte Medien in einer bestimmten Art und Weise nutzen müssen. Ein Vertrag kann grundsätzlich per Handschlag, nach telefonischer Absprache, über ein unterschriebenes Papierdokument oder auf elektronischem Weg z.B. per Fax abgeschlossen werden. Ausnahmen von der Formfreiheit sind nur die Fälle, für die im bürgerlichen Gesetzbuch Schriftlichkeit vorgeschrieben ist (Schriftformerfordernis). In diesen Fällen wird ein handschriftlich unterschriebenes Dokument (etwa Mietverträge) oder eine ganz handschriftlich gefertigte Urkunde (Testament) vorgeschrieben.⁹⁵ Derzeit ist nicht erkennbar, dass sich an der grundsätzlichen Formfreiheit mit der Einführung digital signierter Dokumente etwas ändern wird. Beabsichtigt wird die Einführung einer "elektronischen Form", bei der digital signierte Dokumente in den Fällen zugelassen werden sollen, in denen heute die (papiergebundene) Schriftform vorgeschrieben ist.⁹⁶ Die elektronische Form enthält die Anforderung der Lesbarkeit als Schriftzeichen, jedoch keine darüber hinausgehenden formalen Anforderungen an die Präsentation. Es sind also aus rechtlicher Sicht in jeder Hinsicht beliebige signierte Do-

⁹¹ S. z.B. Bizer / Hammer DuD 1993, 620.

⁹² Creifelds 1996, 102.

⁹³ Seidel CR 1993.

⁹⁴ S. hierzu Zielinski CR 1995 für die elektronische Übermittlung per Telefax.

⁹⁵ In einigen Fällen geht's auch ohne Unterschrift und faksimilierte oder automatisch erstellte Namenskennzeichen werden akzeptiert.

⁹⁶ BMJ 1999.

kumente als Beweismittel zu erwarten, wobei der Schwerpunkt bei Textdokumenten liegen dürfte.

Im Strafprozess kann die vage Einschränkung auf schriftliche elektronische Dokumente nicht getroffen werden. Digital signierte Dokumente beliebiger Medienarten können

- als Mittel verwendet worden sein, um Straftaten zu begehen (z.B. Erpressungsschreiben),
- ihre Erzeugung und Verwendung kann selbst eine Straftat darstellen (z.B. Urkundenfälschung) und
- sie können aufgrund ihres Inhalts geeignet sein, eine Straftat nachzuweisen (z.B. Bekennerschreiben).

In all diesen Fällen ist eine bestimmte Form des Dokumentes nicht vorgeschrieben und auch nicht zu erwarten.

Auch im Verwaltungsverfahren gilt der dem Zivilrecht vergleichbare Grundsatz der "Nichtförmlichkeit des Verwaltungsverfahrens".⁹⁷ Demzufolge besteht im Allgemeinen kein Zwang, für Anträge, Entscheidungen und deren Bekanntgabe eine bestimmte nicht-elektronische oder elektronische Form einzuhalten. Ausnahme von dieser Formfreiheit sind allerdings Bereiche, in denen besondere Rechtsvorschriften gelten, wie im Planfeststellungsverfahren, beim Melde- und Passrecht. Darüber hinaus unterliegt die Durchführung des Verwaltungsverfahrens und mit ihm auch die Festlegung einer konkreter elektronischen Form dem pflichtgemäßen Ermessen der Behörde, d.h. die Behörde legt - innerhalb gewisser Spielräume und Grenzen - Formvorgaben fest. Heute muss ein Widerspruch etwa schriftlich - unterschrieben und mit Datum versehen - vorgebracht werden, wohingegen etwa ein Telefonanruf oder ein bekritzelter Bierdeckel ignoriert werden kann. Künftig wird die Verwaltung die Art der elektronischen Dokumente, mit denen Anträge gestellt oder Widersprüche begründet werden, innerhalb gewisser rechtlicher Grenzen vorschreiben können (etwa Zulassung von Audiodokumenten, Verwendung bestimmter Datenformate wie PDF etc.).⁹⁸

5.1.4 Beweismittelbeschaffung

Im Zivilverfahren müssen die Beweismittel von der Partei als Beweismittel vorgebracht werden, die daraus für sie günstige Umstände beweisen will (in der Regel der Anspruchsteller). Beweismittel sind nicht nur die Daten, sondern auch die für deren "richtige" Präsentation erforderlichen Systeme. Je nach Anwendung wird sie hierzu das Programm benennen, Programme und Systeme dem Gericht zur Verfügung stellen oder eine vor-Ort-Präsentation auf einem bestimmten System organisieren müssen. Keine Partei kann eine andere dazu zwingen, Beweismittel herauszugeben oder neu zu erzeugen, selbst wenn dies den Rechtsstreit klären könnte. Insoweit kann keine Partei ihren Gegner auf der Basis des geltenden Rechts künftig dazu zwingen, signierte Dokumente vorzulegen, Zugang zu Präsentationssystemen zu gewähren und eine Präsentation durchzuführen. Wenn eine Partei die Herausgabe von Beweismitteln verweigert, kann ihr dies bei der Urteilsfindung nachteilig ausgelegt werden. Dies ist jedoch nur möglich, wenn es offenkundig (und im Streitfall wiederum beweisbar ist), dass sie die Beweismittel aus rein prozeßtaktischen Gründen nicht herausgibt. Im Zivilverfahren gibt es für die Parteien auch keine Möglichkeit, Dritte zu zwingen, Beweismittel zur Verfügung zu stellen oder zu erzeugen, selbst wenn dies eine strittige Tatsache belegen könnte. So kann ein

⁹⁷ Deutscher Städtetag 1999, 43 ff.

⁹⁸ Z.B. im Genehmigungsverfahren Roßnagel / Schroeder 1999.

Softwareunternehmen im Zivilprozess nicht gezwungen werden, den Quellcode eines Präsentationssystems herauszugeben. Nur wenn es offenkundig (und im Zweifelsfall wiederum nachweisbar) ist, dass die eine Prozesspartei für das Handeln des Dritten verantwortlich ist - etwa weil sie als Kunde die Herausgabe untersagt hat - kann ihr dies bei der Urteilsfindung nachteilig ausgelegt werden. Die Verfügungsmacht über Beweismittel ist zivilrechtlich also von großer Bedeutung. Wer - wie im Falle des Antragstellers der GMD - Urlaubskarte - nicht über solche verfügt, hat möglicherweise schlechte Karten.

Günstiger gestaltet sich die Beweismittelbeschaffung für den Ankläger im Strafrecht. Zwar muss die Staatsanwaltschaft alle für die Anklage und die Beweisführung nötigen Beweismittel selbst beschaffen (Amtsermittlungsgrundsatz) und der Angeklagte muss keine Beweismittel zur Verfügung stellen - er muss sich nicht selbst belasten, sondern kann Beweismittel zu seiner Entlastung in das Verfahren einbringen. Allerdings kann die Staatsanwaltschaft Beweismittel, die sich im Verfügungsbereich des Angeklagten befinden, im Ermittlungsverfahren und auch danach durch die Polizei beschaffen lassen, wenn sie klare Anhaltspunkte dafür hat, dass es solche zur Aufklärung des Falls nötigen Beweismittel gibt. Dazu hat sie das Recht, Wohnungen durchsuchen und Beweismittel beschlagnahmen zu lassen.⁹⁹ Die Staatsanwaltschaft kann also Geräte, Zubehör und Programme oder die gesamte EDV-Anlage, auf denen digital signierte Daten präsentiert wurden durch die Polizei sicherstellen lassen, um einen Nachweis führen zu können - wobei die Schwere der Straftat für die Eingriffstiefe zu berücksichtigen ist. Eine Beweisführung ist daher (zumindest theoretisch) auch lange nach dem Signiervorgang noch auf dem Originalsystem möglich. Gelingt die Beschlagnahme jedoch nicht, kann, auch wenn es offenkundig ist, dass der Angeklagte Beweismittel besitzt, ihm dies nicht unbedingt nachteilig bei der Urteilsfindung ausgelegt werden. Er muss auch nicht mitwirken, etwa durch die Herausgabe eines Programmes, da er sich als Beschuldigter nicht selbst belasten muss. Die Staatsanwaltschaft kann aber Dritte zwingen, Informationen über oder Gegenständen des Angeklagten herauszugeben. Voraussetzung ist aber, dass dies zur Klärung einer Straftat erforderlich und nicht anders möglich ist. Die Staatsanwaltschaft kann Dritte auch als Zeugen vorladen, wenn dies zur Aufklärung des Sachverhaltes notwendig ist, allerdings unter Berücksichtigung der Zeugnisverweigerungsrechte (z.B. für Angehörige).

5.1.5 Beweisfragen

Die Art des bezüglich der Präsentation zu erbringenden Nachweises hängt davon ab, ob nachzuweisen ist, dass der Signierende eine bestimmte Erklärung willentlich abgegeben hat oder ob lediglich nachzuweisen ist, welche Erklärung er sich zurechnen lassen muss.

Der Nachweis der willentlichen Abgabe einer bestimmten Willenserklärung (**Nachweis der Autorisierung**¹⁰⁰) ist zu führen, wo es auf den (freien) Willen und die Absicht der Erklärungsabgabe ankommt und wo die fehlerhafte, fahrlässige oder erzwungene Abgabe der Erklärung ausgeschlossen werden muss. Der Nachweis der Absicht der Abgabe wird regelmäßig im Strafprozess zu führen sein. Denn hier ist das Strafmaß in der Regel bei fahrlässigem Handeln erheblich geringer als bei absichtlichem. Bestimmte Straftatbestände knüpfen sogar direkt an der Ursache an. Aber auch im Zivilrecht kann Fälle geben, in denen die Autorisierung eine Rolle spielen könnte. Beispielsweise ist zu klären, ob eine mutwilliges oder ein fahrlässiges

⁹⁹ Siehe hierzu Bär CR 1995, Bär CR 1996 und Bär CR 1998, sowie Jäger 1998, 182 ff.

¹⁰⁰ Bizer/Hammer DuD 1993, 619ff.

Verhalten Ursache eines Schadens war, wenn nur Fahrlässigkeit durch eine Versicherungspolice abgedeckt ist. Der Nachweis der willentlichen Abgabe wird in der Regel darüber zu führen sein, dass dem Signierer die signierten Daten in einer bestimmten Art und Weise präsentiert wurden, bevor er den Signiervorgang auslöste (Nachweis der physischen Präsentation).¹⁰¹ Dieser Nachweis ist zweifellos besonders schwierig zu führen.

Glücklicherweise ist der schwere Nachweis einer Präsentation zum Signierzeitpunkt vielfach unnötig. Dies ist dann der Fall, wenn dem Signierer eine bestimmte Präsentation als Willenserklärung zugerechnet werden kann, und er die Konsequenzen einer versehentlichen oder absichtlichen Abgabe zu tragen hat (**Nachweis der zurechenbaren Präsentation**). Heute ist im zivilen papiergebundenen Rechtsverkehr allgemein anerkannt, dass für die Interpretation einer Willens- oder Wissenserklärung das relevant ist, von dem der Empfänger ausgehen musste, dass es dem Willen des Erklärenden entsprach (Empfängerhorizont). So muss sich der Erklärende heute z.B. die Folgen des Missbrauchs von selbst erteilten Blankounterschriften zurechnen lassen, weil der Empfänger einer unterschriebenen Erklärung davon ausgehen darf, dass der Erklärende gesehen hat, was er unterschrieb. Es ist anzunehmen, dass dieses Prinzip auch für das "Ob" und "Wie" der Präsentation digital signierter Daten gelten wird: Die Frage, ob der Signierende bei der Präsentation einen Fehler gemacht hat (Falschpräsentation), oder ob er die Daten überhaupt präsentiert hat, dürfte häufig keine Rolle spielen. Dies dürfte zumindest dann der Fall sein, wenn eventuelle Fehler durch ihn oder einen in seinem Auftrag handelnden Gehilfen verursacht wurde, wenn er oder der Gehilfe in der Lage war, den Fehler zu erkennen und zu vermeiden oder das spezifische EDV-Betriebsrisiko oder sich ein sonstiges erhöhtes, abstrakt beherrschbares Risiko aus der Sphäre des Erklärenden verwirklicht hat.¹⁰²

Es wird ihm eine bestimmte Präsentation zuzurechnen sein, von der der Empfänger ausgehen musste, dass dies "die Richtige" ist. Liegen Regelungen vor, nach denen Daten zu interpretieren und zu präsentieren sind, vor - seien es gesetzliche Vorgaben, vertragliche Regelungen oder vielleicht auch nicht-kodifizierte aber allgemein übliche Verhaltensregeln - so dürften diese für die Frage, wie Daten aus der Sicht des Empfängers zu präsentieren wären, zugrundegelegt werden.

Schwierigkeiten dürften sich allerdings dann ergeben, wenn solche Regeln fehlen oder wenn sie nicht hinreichend eindeutig sind, so dass kein eindeutiger Empfängerhorizont zu bilden ist (Risiko der Mehrdeutigkeit). Problematisch ist es, wenn Techniksysteme bei Abgabe der Erklärung zum Einsatz kommen, die der Signierer nicht durchschauen kann und die ein erhebliches Risikopotential übereilter oder versehentlicher Abgabe von Willenserklärungen mit sich bringen. Rechtlich sehr fraglich und daher unwahrscheinlich erscheint die Zuordnung einer Präsentation schließlich, wenn der Beweisführer die Präsentation bestimmen konnte, weil er selbst dem Signierer das Präsentationssystem zur Verfügung stellte und mithin selbst für

¹⁰¹ Abweichend mag im Einzelfall der Nachweis zu führen sein, dass der Signierende das Dokument selbst erstellt hat oder dass irgendwann vor oder nach dem dem Signierzeitpunkt einmal eine Präsentation erfolgte. Aber auch dann dürfte nachzuweisen sein, dass der Signierer die Daten signieren wollte und dass er mit diesen Daten eine bestimmte Präsentation assoziierte.

¹⁰² Entsprechend Kuhn 1991, 307 ff bereits für unsignierte elektronische Willenserklärungen mit dem Blick noch auf zentralisierte Telekommunikationssysteme wie BTX und ohne Berücksichtigung des dezentralen Internetprinzips. Der Risikospärendanke läßt sich aber übertragen. Ist der Signierer Betreiber der Anwenderinfrastruktur, so dürften Fehler und Mißbräuche in seine Risikosphäre fallen und die abgegebene Erklärung ist ihm zuzurechnen. Auch wenn Kuhn nur Daten berücksichtigt, sind seine Überlegungen direkt auf die Präsentation und Interpretation der Daten übertragbar – denn Daten, signiert oder unsigniert, sind ja keine Willenserklärungen, sondern eben nur ihre Präsentation!

eventuelle Fehler oder Manipulationen verantwortlich ist. In all solchen Fällen wird auch für den Nachweis der zurechenbaren Präsentation der Nachweis der tatsächlichen Präsentation (zum Signierzeitpunkt oder zum Zeitpunkt der Dokumenterstellung) geführt werden müssen.

Auch ohne einer genauen juristischen Analyse vorgreifen zu wollen, lässt sich also stark annehmen, dass eine festgelegte geregelte Präsentation und Interpretation signierter Daten nachzuweisen ist, wo es um die Verantwortlichkeit für deren Zustandekommen und Folgen geht und wo der Signierer die Präsentation selbst kontrollieren konnte. Hingegen wird die Präsentation der signierten Daten zum Signierzeitpunkt nachzuweisen sein, wenn eine absichtliche Abgabe der Erklärung nachgewiesen werden muss - vor allem im Strafrecht -, wenn Mehrdeutigkeiten in der Präsentation vorliegen und wenn ein vom Anspruchsteller als möglichem Prozessbegünstigten kontrolliertes Präsentationssystem zum Einsatz kam.

5.1.6 Beweislast

Im Zivilprozess geht es allgemein um die Durchsetzung von Ansprüchen (auf Schadensersatz, auf Unterlassung einer Handlung, auf Duldung, auf Herausgabe, auf Vornahme einer Handlung, u.s.w.). Es trifft ein klagender Anspruchsteller auf einen beklagten Anspruchgegner. Soweit keine besonderen gesetzlich geregelten oder vertraglich vereinbarten Beweisregeln gelten, hat der Anspruchsteller die volle Beweispflicht. Diese Beweispflicht gilt allerdings nur für strittige Tatsachen. Behauptungen, denen nicht widersprochen wird, kann der Richter im Regelfall als "wahr" unterstellen. Soweit signierte Dokumente als Beweismittel vorgelegt werden, hat der Anspruchsteller nachzuweisen, dass eine bestimmte Präsentation auf irgendeinem System in Gegenwart des Richters der des Signierers zum Signierzeitpunkt entspricht oder dem Signierer als Willenserklärung zuzurechnen ist.

Im Strafprozess hat die Staatsanwältin eine dem Anspruchsteller im Zivilprozess vergleichbare Position. Sie hat nachzuweisen, dass der Angeklagte bestimmte Straftaten begangen hat. Das Gericht kann allerdings nicht so leicht davon ausgehen, dass unbestrittene Behauptungen wahr sind, sondern die Staatsanwaltschaft hat in der Regel für alles volle Beweispflicht.

Soweit sie signierte Daten als Beweismittel verwendet - seien sie Mittel zur Begehung der Straftat gewesen, z.B. Beleidigungsschreiben, oder Nachweismittel, z.B. signierte Zeugenaussage - hat sie auch deren "richtige" Präsentation nachzuweisen. Im Regelfall dürfte dies - wegen der zumeist wichtigen Schuldfrage - die Präsentation zum Signierzeitpunkt sein.

5.1.7 Beweisregeln

Beweisrechtlich gesehen gilt die Präsentation digital signierter Daten bei der heutigen Rechtslage sowohl im Zivil- als auch im Strafrecht als „Augenscheinsobjekt“. Für den Richter bedeutet dies, dass er sich durch persönliche Wahrnehmung eine substantiierte Meinung bilden muss. Das Beweismittel unterliegt der freien Beweiswürdigung: Besondere Beweisregeln, die den Richter an eine bestimmte Aussage in Abhängigkeit von einem bestimmten Sachverhalt binden, gibt es nicht. Insbesondere gilt nicht die nach dem Urkundsbeweis für unterschriebene Papierdokumente geltende Vermutung der Echtheit eines über einer Unterschrift stehenden Textes bei nachgewiesener bzw. unbestrittener Echtheit der Unterschrift.

Frei bedeutet nicht willkürlich: Das Gericht muss die Eignung der Beweismittel prüfen und seine Überzeugungen und Schlussfolgerungen nachvollziehbar begründen. Eine Behauptung

über die Aussagekraft des Beweismittels kann sie wie jede andere Behauptung als Tatsache ansehen, wenn diese nicht bestritten wird (insbesondere Zivilprozess) oder auf andere Art bewiesen werden. Dabei wird regelmäßig auch der Umweg über andere Tatsachen, so genannte Hilfstatsachen oder Indiztatsachen (auch Indizien) geführt. So besteht die Hoffnung auch bei signierten Dokumenten den Beweis der Korrektheit der Präsentation eines Präsentationssystems über den Hinweis auf den Einsatz zertifizierter Systeme (zu beweisende Indiztatsache) führen zu können.

Die im Recht verankerte weitestgehend freie Beweiswürdigung lässt sich nicht umgehen: Gerichtliche Beweisregeln lassen sich nicht durch Vereinbarungen zwischen Vertragsparteien einführen.

Neben der unmittelbaren Wahrnehmung durch den Richter im Rahmen des Augenscheinsbeweises kann die Präsentation auch Gegenstand eines Sachverständigenbeweises sein. Der Sachverständige analysiert dann die Präsentation und berichtet über die Ergebnisse. Daneben ist auch noch ein Zeugenbeweis denkbar – ein Zeuge berichtet über die Präsentation im Rahmen eines Signiervorganges, bei den er zugegen war. Der Beweiswert solcher Zeugenaussagen dürfte jedoch vergleichsweise gering sein.

Das Gericht muss ein Beweismittel nicht würdigen, wenn es der Auffassung ist, dass dies für die Wahrheitsfindung nicht erforderlich ist. Wird es berücksichtigt, so muss das Gericht normalerweise sämtliche für die Bewertung des Beweismittels im konkreten Fall relevanten Umstände und die in diesem Zusammenhang von den Parteien vorgebrachten Argumente würdigen. Es kann nicht einfach die Echtheit einer Präsentation annehmen, sondern muss von einer Partei den Korrektheit des Präsentationssystems verlangen, wenn dies von der gegnerischen Partei in Frage gestellt wird.

Nur wenn in der Rechtsprechung über längere Zeit bestimmte Fälle immer wieder in derselben Art bewiesen und entschieden werden, kann bei einer strittigen Frage von der Allgemeinheit auf den besonderen Fall geschlossen werden (Deduktion), so dass alleine der Augenschein die Echtheit vermutet lässt (**Anscheinsbeweis**). So wird im Verkehrsrecht bei einem Auffahrunfall in der Regel auf die Schuld des Auffahrenden geschlossen, ohne dass die Umstände des Unfalls im Einzelnen geklärt werden. Bei Signaturverfahren, wo eine solche lange Rechtsprechung und Erfahrungstatsachen noch nicht zur Verfügung stehen, ist hingegen eine solche Vereinfachung der Beweisführung zunächst nicht zu erwarten.¹⁰³

Eine Tatsache gilt juristisch als bewiesen, wenn ein Gericht von dem Vorliegen oder Nichtvorliegen der streitigen Tatsache überzeugt ist. Absolute Sicherheit wird hierfür nicht verlangt. Von einer Überzeugung ist vielmehr bereits dann auszugehen, wenn für das Beweisergebnis ein so hoher Grad von Wahrscheinlichkeit spricht, dass vernünftiger Weise in Betracht kommende Zweifel ausgeschlossen sind. In freier Beweiswürdigung muss das Gericht seine Wertungs- und Entscheidungsprozesse ausführlich, nachvollziehbar und revisionstauglich begründen.

¹⁰³ Sie soll aber durch die vorbeugenden Sicherungsvorkehrungen des Signaturgesetzes quasi vorweggenommen werden können. Dies wird später im Abschnitt "Sicherheitsvermutung des Signaturgesetzes", S. 84 näher erläutert.

5.1.8 Rollen und Ablaufmodell

Vor dem Hintergrund der vorangegangenen prozessrechtlichen Überlegungen und der Risiken ist es aus informatischer Sicht naheliegend, das Prozedere der Beweisführung zusammenfassend etwas abstrakter zu modellieren.

Zunächst ist es wegen der Unterschiede in der Beweisführung zweckmäßig die beweisführenden Akteure und die das Beweismittel erzeugenden voneinander zu unterscheiden:

Der Beweisführer: Hiermit ist derjenige gemeint, der eine Behauptung mit Hilfe einer Präsentation beweisen will. Im Strafprozess ist dies zumeist der Staatsanwalt für die belastenden Behauptungen, jedoch kann auch der Angeklagte eine entlastende Behauptung beweisen. Im Zivilprozess ist Beweisführer in erster Linie der Anspruchsteller, jedoch kann auch der Anspruchsgegner den Anspruch negierende Behauptungen vorbringen.

Der Beweisgegner: Hiermit ist derjenige gemeint, dem das Beweismittel zum Nachteil gereicht und der es deshalb anzweifelt und dem Beweisgegner widerspricht. Die Realakteure sind die jeweiligen Widerparts der als Beweisführer genannten.

Der Signierer: Hier ist derjenige gemeint, der das als Beweismittel verwendete Dokumentes signiert hat. Sehr oft sind Signierer und Beweisgegner eine Person: Der Beweisführer will die für ihn günstige Tatsache mit einem vom Beweisgegner signierten Dokument nachweisen. Der Signierer kann aber auch ein am Prozess Unbeteiligter sein und der möglicherweise nicht befragt und im Prozess für seine Handlungen zur Verantwortung gezogen werden kann - man denke z.B. an eine signierte Zeugenaussage, deren Urheber verzogen ist.¹⁰⁴

Der Dokumentersteller: Hier ist derjenige gemeint, der das als Beweismittel verwendete und vom Signierer signierte Dokumentes erstellt hat. Oft hat der Signierer selbst nicht das Dokument erstellt, das er signiert, sondern er hat von einem anderen eine Vorlage erhalten, diese präsentiert und vielleicht um ein paar Angaben ergänzt und dann signiert. Oft ist der Dokumentersteller gerade der Beweisführer und er profitiert u.U. von Fehlern und voreiligen Signiervorgängen des Beweisgegners. Das muss berücksichtigt, die Rolle deshalb unterschieden werden.

Der Betreiber des Präsentationssystems: Unter dem Gesichtspunkt der Risikosphäre ist besonders wichtig, wer das Präsentationssystem verwaltet und wartet und somit die Möglichkeit hatte, Fehler oder Missbräuche durchzuführen bzw. zu entdecken oder zu verhindern. Beweiserfordernisse, insbesondere die Zurechenbarkeit, hängen stark davon ab, ob Signierer, Beweisgegner, Beweisführer oder eine andere Person der bzw. einer der Betreiber ist.

Ablaufmodell

Gegenstand der Beweisführung sind **Behauptungen** über das Vorliegen bestimmter Tatsachen, die die Akteure zur Durchsetzung ihrer Prozessziele zu beweisen haben. Die Präsentation ist erstes Mittel zum Beweis der Behauptung, dass ein Anspruch besteht oder eine Straftat begangen wurde. Die Behauptung wird bei Überzeugung des Richters zur (bewiesenen) Tatsache werden. Andererseits können durch den Beweisgegner Einwände gegen das Beweismittel bzw. seine Beweiskraft vorgebracht werden. Diese können wiederum durch Gegenbehauptun-

¹⁰⁴ Wie z.B. im Fallbeispiel 5: Tatzeit "Aktualisierbares Datum", S. 45.

gen und deren Beweis, sog. **Indiztatsachen** entkräftet werden. Beim Indizien oder Anzeichenbeweis wird aus einer mittelbar bedeutsamen auf die Haupttatsache zurückgeschlossen. Auch gegen diese können wiederum Einwände vorgebracht werden, so dass sich die Beweisführung in dieser abstrakten Sichtweise baumartig weiter verzweigen kann. Dabei kann in einigen Fällen, bei rechtlich geregelter Beweislastumkehr, derjenige, der den Einwand vorbringt, für diesen beweispflichtig werden, wodurch sich die Rollen von Beweisführer und Beweisgegner im Teilbaum verkehren. Informatisch gesehen wird bei der Beweisführung ein Baum aufgespannt, dessen Knoten die Behauptungen und dessen Kanten die Einwände darstellen. Das theoretisch unendliche Spiel der Verzweigung in Indizienbehauptungen terminiert (in der Regel rasch) durch folgende Umstände:

- **Fehlender Widerspruch:** Einer Behauptung wird nicht widersprochen (im Zivilrecht). Sie gilt dann als bewiesene Indiztatsache.
- **Anderes Beweismittel:** Eine Behauptung wird durch ein anderes zulässiges Beweismittel bewiesen, wie etwa eine Zeugenaussage, eine amtliche Auskunft, Sachverständigengutachten, eine (Papier)Urkunde. Die Papierurkunde hat den Vorteil, dass der über der Unterschrift stehende Text bei nachgewiesener bzw. unwidersprochener Echtheit der Unterschrift als abgegebene Willenserklärung gilt. Eine ähnliche Echtheitsvermutung gilt auch für die amtliche Auskunft. Trotzdem können auch hier Einwände vorgebracht werden, die allerdings dann zu einer faktischen Umkehrung der Beweislast (und damit der Rollen) führen.
- **Abweisung:** Der Richter kommt zur Ansicht, dass es sich um eine offensichtliche Schutzbehauptung handelt und lässt das Beweismittel nicht zu.
- **Anscheinsbeweis:** In Ermangelung eines anderen induktiven Beweises wird deduktiv nach den Regeln der menschlichen Lebenserfahrung von anderen Fällen (dem allgemeinen Fall) auf den speziellen vorliegenden geschlossen.
- **Kosten:** Ein wichtiger Begrenzungsfaktor ist schließlich auch das Kostenrisiko, das eine Prozesspartei in der Lage ist einzugehen.

Die Beweisführung als abstrakter Prozeß kann also in einem baumartigen Modell dargestellt werden, der einem technischen Verifikationsschema ähnelt. Allerdings ist die Analogie nur vordergründig, weil es die gerichtliche Beweisführung bei freier Beweiswürdigung ein dynamischer und durch Überzeugungskraft, Strategie und Taktik bestimmter Prozess ist und kein Abarbeiten einer im Voraus feststehenden Liste von Behauptungen. Im Folgenden werden wesentliche Aspekte dieses Verhandlungsprozesses bezogen auf die Präsentation signierter Daten dargestellt.

5.2 Einwendungsmöglichkeiten

Die im Kapitel 3 dargestellten Risiken einer fehlerhaften oder echt mehrdeutigen Präsentation signierter Daten ermöglichen - berechtigt oder unberechtigt – dem Beweisgegner nun Einwendungen gegen die Behauptung des Beweisführers, eine bestimmte Willens- oder Willenserklärung sei durch den Signierer abgegeben worden.

Wahrscheinlich wird der Beweisgegner, sofern er kein Experte ist, sondern "Normalbürger", zunächst nur einwenden, "dieses Dokument ist nicht echt" oder "... stimmt nicht". Es ist deshalb bereits Aufgabe des Richters - eventuell unter Hinzuziehung eines Sachverständigen - zu klären, inwieweit überhaupt die Präsentation angezweifelt wird und nicht etwa die Urheberchaft und Unversehrtheit der signierten Rohdaten. Dies ist im Beweisverfahren anhand einer Signaturprüfung und der Erörterung möglicher Einwände zuvor zu klären: Denn wäre bereits die Frage der Urheberchaft und Unversehrtheit der Rohdaten nicht beweisbar, so dürfte die Frage der Präsentation im Regelfall unerheblich sein.

Ist also die Urheberschaft und Unversehrtheit der Daten geklärt, so bleiben gegen das Beweismittel der Präsentation signierter Daten noch eine Reihe von Einwendungsmöglichkeiten.

5.2.1 Falschpräsentation auf Prüfsystem

Der Beweisgegner könnte einwenden, dass das Präsentationssystem, welches das Gericht oder der Beweisgegner nutze, fehlerhaft arbeite oder gar manipuliert sei. Es präsentiere möglicherweise überhaupt nicht die in Frage stehenden signierten Daten, sondern irgendetwas anderes, vielleicht sogar untergeschobene Daten. Oder es wird argumentiert, die Hard- oder Software weise Fehler auf, sei falsch konfiguriert oder werde durch den Richter bzw. den Beweisführer falsch bedient, so dass die Präsentation teilweise falsch sei.

Sofern die Prüfung auf einem Computersystem des Gerichtes stattfindet, so würde das Gericht den Präsentationsvorgang zunächst auf einem anderen gerichtsinternen Computer wiederholen können. Eine gleichartige Präsentation wäre ein Indiz dafür, dass die Präsentation doch richtig erfolgte. Dazu ist allerdings auszuschließen wäre, dass das zweite System dieselben fehlerhaften oder manipulierten Komponenten oder Einstellungen verwendet - etwa eine fehlerhafte Präsentationssoftware. Die Wiederholung einer Prüfung ist also umso aussagekräftiger, je unterschiedlicher die verwendeten Systeme sind. Indizien für die Korrektheit können evaluierte Darstellungskomponenten und Betriebssysteme sein, für die richtige Konfiguration eine regelmäßige gerichtsinterne Prüfung.¹⁰⁵ Das Gericht wird in diesem Fall vom Beweisgegner den Gegenbeweis - etwa durch eine Alternativpräsentation auf einem anderen System verlangen können.¹⁰⁶

Probleme ergeben sich, wenn die genannten Voraussetzungen bei gerichtsinternen Präsentationssystemen nicht vorliegen und Kontrollpräsentationen tatsächlich unterschiedlich verlaufen, oder wenn die Brauchbarkeit der Evaluierung angezweifelt wird. In einem solchen Fall dürfte eine Sachverständigenprüfung erforderlich werden.

Wesentlich schwieriger ist die Beweisführung, wenn ein externes System zur Präsentation genutzt wird, etwa das Rechnersystem eines Dritten oder gar das des Beweisführers. Ohne Beweiserleichterungen könnte der Beweisführer gezwungen sein, die Sicherheit der verwendeten Anwenderinfrastruktur zum Signierzeitpunkt nachzuweisen, zumindest wenn dieser Aspekt umstritten ist. Handelt es sich um ein Dokument in einer komplexen vernetzten Anwendung (etwa die "GMD-Urlaubskarte"), so kann eine retrospektive Begutachtung des gesamten vernetzten Systems erforderlich werden. In dieser müssen dann alle die Präsentation möglicherweise beeinflussenden Komponenten identifiziert und dann auf ihre ordnungsgemäße Funktion untersucht werden. Dieser Beweis dürfte äußerst aufwendig und in vielen Fällen undurchführbar sein.

5.2.2 Falschpräsentation durch den Signierer

Der Beweisgegner könnte einwenden, der Signierende habe die Erklärung von anderen vorgelegt bekommen und vor dem Signiervorgang nicht richtig wahrgenommen. Beispielsweise

¹⁰⁵ Und das hier im Prinzip bereits ohne die beweiserleichternden Vorgaben des Signaturgesetzes, die im folgenden Kapitel erörtert werden, alleine aufgrund der Glaubwürdigkeit der Evaluierung.

¹⁰⁶ Formell könnte man diesen Vorgang als die Vorlage eines anderen Beweismittels auffassen, da ja ein anderes Präsentations- bzw. Augenscheinsobjekt erzeugt wird.

habe er den Text nicht vollständig durchgesehen und einfach so, vielleicht versehentlich, signiert.¹⁰⁷ Er könnte einwenden, der Signierer habe Fehler gemacht, etwa ein falsches Programm benutzt oder ein richtiges falsch konfiguriert, so dass er etwas anderes wahrgenommen habe als das was man nun wahrnehmen könne. Schließlich könnte er einwenden, der Signierer habe nicht über die notwendigen zur Wahrnehmung erforderlichen Geräte verfügt oder diese nicht seinen Bedürfnissen entsprechend einstellen können.

Ist der Beweisgegner selbst der Signierer des fraglichen Dokumentes und geht es nicht um den Nachweis der Vorsätzlichkeit fehlerhaften Handelns (Schuldfrage), so könnte ein solcher Einwand fehlender Autorisierung der Willenserklärung im Zivilprozess regelmäßig zu seinen Lasten gehen. Die Erklärung gilt als abgegeben, sie kann lediglich noch als Inhalts- oder Erklärungsirrtum angefochten werden (vgl. §§ 119 ff. BGB), der Signierer (hier auch zugleich Beweisgegner) haftet dann aber zumindest für den entstandenen Vertrauensschaden.¹⁰⁸ Es zählt dann die "richtige" Präsentation als abgegebene Willens- bzw. Wissenserklärung - natürlich nur insoweit, als unbestritten ist, was "richtig" gewesen wäre.

Ist das zum Signieren verwendete System dasjenige des Beweisführers, so ist allerdings fraglich, ob das Gericht den Einwand so einfach abweisen kann. Denn in einem solchen Fall ist der Beweisführer als Begünstigter zugleich derjenige, der für eine, eventuell sogar beabsichtigte Falschpräsentationen verantwortlich sein kann. In einem solchen Fall könnte das Gericht daher den Beweisführer dazu verpflichten, die Präsentation zum Signierzeitpunkt nachzuweisen oder zumindest auszuschließen, dass er für mögliche Fehler- und Manipulationen die Verantwortung tragen kann.¹⁰⁹

Ist eine tatsächliche aktive Kenntnisnahme des Erklärungsinhalts nachzuweisen, insbesondere für den Nachweis einer vorsätzlichen Handlung im Strafrecht, so wird regelmäßig der Nachweis erforderlich sein, dass eine Präsentation beim Signierer stattgefunden hat. Abhängig vom Fall kann es auch erforderlich sein, genau nachzuweisen, dass diese in einer bestimmten Art und Weise erfolgt ist. Dies könnte beispielsweise bei einem von einem Polizeibeamten erstellten und zum Signieren vorgelegten Geständnis eines Angeklagten einmal der Fall sein, bei dem eventuell die komplette Kenntnisnahme vor dem Signiervorgang nachzuweisen wäre.

Für den Nachweis einer erfolgten Präsentation sind zusätzliche Beweismittel wie Zeugen etc. erforderlich. Die heutigen Präsentationssysteme bieten keine Möglichkeit zu Protokollierung der Kenntnisnahme. Unter Umständen gibt es im Betriebssystem oder verwendeten Vorgangssystem Protokollierungen, aus denen die Nutzung bestimmter Anwendungen ermittelt werden könnte. Nachzuweisen wäre z.B. anhand von Sicherheitskopien das Vorliegen von Entwürfen, aus denen hervorgeht, dass das Dokument vom Signierer selbst erstellt wurde. Wo dies möglich erscheint, könnte es Aufgabe eines Sachverständigen sein, solche Informationen zu suchen und auszuwerten.

¹⁰⁷ Es ist nicht ganz optimal, diesen Aspekt der Übereilung hier in den Nachweis der Präsentation bzw. das Risiko der Falschpräsentation der Rohdaten zu behandeln. Es handelt sich vielmehr um das Problem des Dialogs bei der Auslösung eines Signiervorgangs – auch ein Teil der zu gestaltenden "Darstellungskomponente" - der in diesem Papier noch nicht systematisch berücksichtigt wird.

¹⁰⁸ Entsprechend Kuhn 1992. Voraussetzung könnte eventuell noch sein, dass er sich aufgrund einer vertraglichen Verpflichtung mit der Zertifizierungsstelle die Folgen fahrlässigen Signierens zurechnen lassen muss, sonst haftet vielleicht die Zertifizierungsstelle. Die Erörterung muss einer juristischen Arbeit vorbehalten bleiben.

¹⁰⁹ Rechtspolitisch wäre dies jedenfalls unbedingt zu fordern. Eine andere Vorgehensweise wäre aber auch eine "schreiende Ungerechtigkeit" und dürfte eventuell spätestens durch das Verfassungsgericht "kassiert" werden.

5.2.3 Mehrdeutigkeit

Der Beweisgegner kann mit den oben skizzierten Möglichkeiten der Mehrdeutigkeit signierten Daten argumentieren.¹¹⁰

Er kann den fundamentalen Einwand vorbringen, die Daten stellten etwas völlig anderes dar, als das, was da auf dem vom Gericht verwendeten System wahrnehmbar sei. Insbesondere könnte er die Einhaltung der elektronische Form bestreiten (sobald diese eingeführt ist) und damit die Zulässigkeit des signierten Dokumentes für den in Frage stehenden Vorgang, sowie etwaige Beweiserleichterungen. Oder es wird argumentiert, die beobachtete physische Präsentation weiche in Teilen des Inhaltes oder der Form von der tatsächlichen oder intendierten des Signierers ab, wobei kein Fehler oder Missbrauch Ursache sei, sondern zulässiges Verhalten. Die signierten Daten stellten also eine andere Erklärung dar, als der Beweisführer behaupte und nun auf einem Präsentationssystem vorführe.

Von einem Laien kann nicht erwartet werden, dass er die Abweichung im Detail benennt. Der Beweisgegner kann seine Einwendung deshalb zunächst einmal schlicht mit dem Verweis auf die unbestreitbar vorhandene Möglichkeit einer anderen Präsentation der Daten begründen. Inwieweit das Gericht einen solchen Einwand würdigen muss, hängt von dem Wissensstand über die Wahrscheinlichkeit einer solchen Mehrdeutigkeit ab. Wird etwa das Vorliegen einer signierten Textdatei und die damit die elektronische Form bestritten, und handelt es sich um einen mehrere hundert Kilobyte langen Bitstring, der durch das Textverarbeitungssystem Word als Text präsentiert werden kann, so spricht schon die "Lebenserfahrung"¹¹¹ dafür, dass es sich um ein Dokument mit Word-Text handeln muss. Bei einem kürzeren Bitstring oder einem wenig redundanten Codierungsverfahren (etwa ASN.1-codierten Formulardaten) kann ein solcher Einwand hingegen nicht ohne weiteres zurückgewiesen werden. Es wird bereits zur Klärung dieser Frage ein Sachverständiger hinzuzuziehen sein.

Akzeptiert das Gericht den Pauschaleinwand nicht, so muss der Beweisgegner den Nachweis der Existenz einer anderen Präsentation bringen. Dies ist insbesondere dann anzunehmen, wenn die Möglichkeit zur Vorführung technisch möglich ist, weil die Programme noch existieren, die Konfiguration und Systembedienung noch nachstellbar ist. Zum Nachweis muss er ein anderes Programm benennen, mit dem das Gericht eine neuerliche Prüfung durchführt, kann Parametereinstellungen nennen, die anzusetzen sind, oder einen Sachverständigen beibringen, der ein Prüfsystem so konfiguriert, dass die unterschiedliche Präsentation wesentlicher Aspekte gezeigt wird.

Gelingt der Nachweis einer anderen Präsentation, so hat das Gericht per Inaugenscheinnahme zunächst einmal zu prüfen, ob die Abweichungen für den Prozessgegenstand erheblich sind. So ist es unerheblich, ob signierte Daten in einem Textverarbeitungssystem oder einer Urlaubskarte dargestellt werden, wenn aus ihnen in beiden Präsentationssystemen eindeutig hervorgeht, dass der Signierer einen Urlaubsantrag vom "1.1.-31.1.99" gestellt hat. Wenn hingegen eine rechtserhebliche Abweichung vorliegt - etwa andere Zahlen oder eine Grafik statt einem Text, wird der Beweisführer zu beweisen haben, welche Präsentation die "richtige" ist, also den Inhalt der Willenserklärung so wiedergibt, wie sie der Signierende angegeben hat. So

¹¹⁰ Siehe Kapitel Teil I:3.1

¹¹¹ Informationstheoretisch die übergroße Redundanz so formatierter Daten. Die fachliche Begründung hierfür erfolgt im Kapitel Möglichkeiten exakter Wahrscheinlichkeitsaussagen 6.3.1.

hat der Beweisführer im Fallbeispiel 6:¹¹² (Externer Link auf die Preisliste) zu beweisen, wie die Preisliste aussah, auf die der externe Link zum Signierzeitpunkt zeigte und im Fallbeispiel 7: (Preisangaben-Position in Dokumentvorlage)¹¹³, welche Positionsangaben zu einem bestimmten Absatzformat die seinerzeit gültige Dokumentvorlage enthielt.

Gelingt dem Beweisgegner die andere Präsentation nicht - weil das Programm nicht mehr vorhanden ist, oder weil ein Dritten es in seinem Herrschaftsbereich hat und nicht mitwirkt, so ist ein Gegenbeweis unmöglich. Es dürfte von der Würdigung des Einzelfalles abhängen - Plausibilität der Argumente - ob das Gericht in diesem Falle den positiven Nachweis des genutzten Präsentationssystems von Anspruchsteller verlangt oder den Einwand des Beweisgegners zurückweist.

Im Strafprozess dürfte die Nachweisführung prinzipiell ähnlich verlaufen. Allerdings hat die Staatsanwaltschaft hier die Möglichkeit und die Pflicht, Dritte zur Herausgabe des fraglichen Präsentationsprogrammes oder zu einer Prüfung vor Ort zu zwingen, wenn es den Angeklagten be- oder entlasten könnte.

5.2.4 Mehrdeutigkeit oder Falschpräsentation?

Während also (im Zivilrecht und unter den o.g. Bedingungen) eine Falschpräsentation des Signierers regelmäßig zu Lasten des Beweisgegners gehen könnte – die Erklärung wird trotzdem als abgegeben anerkannt - könnte eine Mehrdeutigkeit regelmäßig zu Lasten des Beweisführers gehen – er muss beweisen, dass die von ihm favorisierte Präsentation tatsächlich die vom Signierer intendierte ist – sonst wird sie als seine eigene Falschpräsentation angesehen. Diese Konstellation dürfte dazu führen, dass die Zuordnung, ob ein Fehler oder eine Mehrdeutigkeit vorliegt, in technisch nicht eindeutigen Fällen heftig umstritten sein dürfte.

Wie im Fallbeispiel 1: "Testtext oder Beleidigungsgrafik?"¹¹⁴ gezeigt kann ein Signierer eine Datei signieren, die bei seiner Präsentation keinen sinnvollen Inhalt ergibt, weil er nicht das vom Dokumentersteller intendierte Medium bzw. Programm nutzt. Der Beweisführer könnte argumentieren, es handele sich um einen Fehler des Signierers (Falschpräsentation). Es sei eine grobe Fahrlässigkeit, Zeichenfolgen zu signieren, deren Bedeutung man nicht ermitteln könne. Die Erklärung sei ihm zuzurechnen, zumindest hafte er für die entstandenen Vertrauensschäden. Der Beweisgegner könnte hingegen darauf hinweisen, dass es keine Vereinbarung zum zu nutzenden Programm gab – im Beispielfall zusätzlich darauf, dass eine Täuschung vorlag.¹¹⁵

Wie im Fallbeispiel 4: "Eine merkwürdige Farbeinstellung"¹¹⁶ kann eine außergewöhnliche Systemkonfiguration Ursache dafür sein, dass der Signierer etwas nicht sieht, was der Dokumentersteller und / oder der Dokumentempfänger Prüfer sieht. Der Beweisführer wird argumentieren, es handele sich um einen Fehler des Signierers, da er eine Fehler geradezu provozierende Einstellung gewählt habe, die kein vernünftiger Nutzer jemals verwende. Der Beweisgegner wird argumentieren, dass es keine Regelung zwischen Dokumentersteller und Signierer zur Bildschirmhintergründen gab, es handele sich deshalb um eine Mehrdeutigkeit.

¹¹² Siehe S. 46.

¹¹³ Siehe S. 47.

¹¹⁴ Siehe S. 44.

¹¹⁵ Im konkreten Beispielfall würde er die Manipulation behaupten, aber die kann er vielleicht ja nicht nachweisen.

¹¹⁶ Siehe S. 45.

In solchen Zweifelsfällen der "Grauzone" dürfte eine Rolle spielen, ob der Beweisführer selbst der Dokumentersteller ist.¹¹⁷ Es könnte argumentiert werden, dass der Beweisführer als Dokumentersteller auch dafür Sorge zu tragen hatte, dass es erst gar nicht zu Mehrdeutigkeiten kommen konnte. Einen Dokumenthintergrund hätte er demzufolge nicht transparent einstellen dürfen, mögliche Missdeutungen gingen demzufolge zu seinen Lasten. Wäre hingegen der Dokumentersteller eine andere Person, etwa ein Mitarbeiter des Signierers, so könnte dem Signierer vielleicht eine Verletzung von Sorgfaltspflichten vorgeworfen werden: Er alleine wäre in der Lage gewesen, problematische Einstellungen seines lokalen Präsentationssystems zu berücksichtigen und hätte dies tun müssen.

Der Richter hat im Rahmen der freien Beweiswürdigung zu entscheiden, ob ein bestimmtes ungewöhnliches Verhalten (etwa eine Konfiguration) als Fehler oder normales Verhalten zu werten ist. Voraussetzung dürfte in jedem Falle eine möglichst genaue Klärung des Sachverhalts und der Umstände des Signiervorgangs (in Bezug auf Systemherrschaft, Konfiguration, Dokumenterstellung) durch einen Sachverständigen sein.

5.2.5 Nichtwissen

Der Beweisgegner könnte die Willens- oder Wissenserklärung, die als physische Präsentation vom Gericht erzeugt wird auch pauschal abstreiten, mit dem Hinweis, er wisse auch nicht, wieso die Daten ausgerechnet so eine Präsentation erzeugten, es sei aber einfach nicht die Richtige.

Allgemein hat der Beweisführer nach § 138 ZPO das Recht, sich auf sein Nichtwissen zu berufen, wenn der Beweisgegenstand nicht seiner eigenen Wahrnehmung unterlag. Eine Wahrnehmung ist sicher dann nicht möglich gewesen, wenn nicht der Beweisgegner, sondern ein Dritter das Beweisdokument signiert hat.

Ist der Beweisgegner selbst Signierer, so spricht gegen die Möglichkeit eines solchen Pauschaleinwandes, dass Daten vorliegen, deren Urheber er ist, weil die mit dem ihm zugeordneten Schlüssel signiert wurden (dies ist die zuvor prüfende Annahme¹¹⁸). Andererseits kann der Beweisgegner die Erzeugung der Daten tatsächlich nicht direkt wahrnehmen, sondern höchstens mittelbar einen diesbezüglichen technischen Vorgang, so dass zumindest für Laien ein solcher Pauschaleinwand zulässig sein dürfte.

Soweit das Gericht einen solchen Pauschaleinwand gelten lässt, hat der Beweisführer den vollen Beweis zu erbringen. Er muss dann alle relevanten Umstände der Präsentation positiv nachweisen, nicht nur Einwände widerlegen. Nachzuweisen wäre dann in allen prozessrelevanten Aspekten der Willenserklärung, ob und wie eine Präsentation der Daten genau erfolgte und dass es tatsächlich nur in einer genau beschriebenen Weise möglich war. Aufgrund des möglichen Umfangs eines solchen Beweises dürfte der Beweisführer dann regelmäßig eines Sachverständigengutachtens bedürfen, das alle Aspekte der Präsentation eingehend untersucht und alle erdenklichen Einwände vorwegnimmt.

¹¹⁷ Deshalb wurde die Rollenunterscheidung in Teil II:5.1.8 getroffen.

¹¹⁸ Unter Berücksichtigung der Möglichkeit, dass bei einem Pin-basierten Verfahren auch ein anderer Urheber sein könnte, der die Chipkarte erhalten hat und die PIN genannt bekam.

5.3 Indiztatsachen und Beweiserleichterungen

5.3.1 Zu beweisende Indiztatsachen

Aus den vorangegangenen Darlegungen ergibt sich, dass eine Präsentation im Streitfall nur dann als Beweismittel erfolgreich verwendet werden kann, wenn folgende Hilfstatsachen bewiesen werden:

- **Korrektheit des Prüfsystems:** Es ist nachzuweisen, dass das bei der Augenscheinsprüfung verwendete System korrekt funktioniert.
- **Korrektheit des Signiersystems:** Es ist nachzuweisen, dass das vom Signierer verwendete System zum Signierzeitpunkt bzw. zum Präsentationszeitpunkt korrekt funktioniert hat und alle für eine ordnungsgemäße Präsentation erforderlichen Komponenten aufwies. Damit verbunden sind die beiden folgenden Nachweise.
- **Verwendete Anwenderinfrastruktur:** Um die Korrektheit des Signiersystems nachzuweisen, ist es in der Regel erforderlich, das zum Signieren verwendete System zu identifizieren. Zivilrechtlich bedeutsam dürfte insbesondere der Nachweis sein, in wessen Risikosphäre diese Anwenderinfrastruktur (Beweisgegner, Beweisführer, Begünstigter, ..) liegt.
- **Zeitpunkts des Signiervorgangs / der Präsentation:** Der Nachweis der Korrektheit ist in der Regel nur bezogen auf einen bestimmte Zeit möglich. Es ist nachzuweisen, wann die Daten zuletzt präsentiert wurden, für den Nachweis der Autorisierung bzw. wann signiert wurde, für die Zurechenbarkeit der Verantwortung – wann signiert wurde.
- **Tatsächliche Präsentation:** Bei einer feststellbaren Mehrdeutigkeit ist die tatsächliche Präsentation zum Signierzeitpunkt / Präsentationszeitpunkt nachzuweisen.
- **Ausschluß der Möglichkeit von Mehrdeutigkeiten:** Ist der Beweisgegner nicht der Signierer, oder kann er nicht mit Nichtwissen abstreiten, muss der Beweisführer nachweisen, dass Mehrdeutigkeiten der Präsentation ausgeschlossen sind.

Gelingen die Nachweise dieser Behauptungen (mit Hilfe weiterer Indiztatsachen) nicht, so kann der Beweisführer den Prozess verlieren.

5.3.2 Technisch-organisatorische Hilfsmittel

i) Datentyp

Nach den Signaturinteroperabilitätsspezifikationen soll die Signatur als zusätzliches Datenlement einen Objektbezeichner für den Datentyp (entspricht Dokumentformat) enthalten. Daraus kann geschlossen werden, dass ein Präsentationsprogramm zu verwenden ist, das diesen Datentyp auswerten kann. Aus einem Objektbezeichner für Word kann also wenigstens geschlossen werden, dass wohl ein Programm zu verwenden sein wird, das Word-Dokumente lesen kann. Darauf ist dieser Nachweis aber auch begrenzt. Der Rückschluss auf das vom Signierer verwendete Programm ist nicht möglich (zumindest jedes Programm ist möglich, das dieses Format exportieren kann). Eine ganz bestimmte Präsentationsform, also Konfiguration, Endgeräte, Einstellung und Benutzung lässt sich per se nicht ableiten. Sind Aspekte der Prä-

sensation jenseits des Datenformats umstritten, so wird der Beweisführer alle diese Einwände voll entkräften und die tatsächliche Präsentation des Signierers beweisen müssen.

Als Einwendungsmöglichkeit bleibt ferner bestehen, dass die Eintragung der Typbezeichnung falsch erfolgt ist – was der Beweisführer zu widerlegen hat, wenn auf seinem System signiert wurde oder wenn im Prozess die Autorisierung nachzuweisen ist.

Ein weiteres Argument gegen den Dateityp ist schließlich, dass die Objektbezeichnungen nicht korrekt vergeben wurden. Für Objektbezeichner wurde zwar ein einfaches baumartiges Verfahren der dezentralen Nummernvergabe festgelegt, dass die Doppelvergabe ausschließt.¹¹⁹ Auch sind die Objektbezeichner bestimmter viel genutzter Formate dauerhaft feststehend und bekannt. Im Massenverfahren könnte eine Instanz aber aufgrund eines Fehlers oder einer Manipulation eine Nummer mehrfach vergeben. Der Einwand, es handele sich bei einem bestimmten Format also nicht um das dem Objektbezeichner zugeordnete, sondern ein anderes wäre nicht von vorneherein unsinnig, sondern zu untersuchen.

ii) Zeitangabe und Zeitstempel

Zum Nachweis der Präsentationszeit kann eine Angabe aus der Signatur oder aus dem signierten Dokument herangezogen werden. Allerdings ist dies nur möglich, wenn lediglich eine zurechenbare Präsentationszeit nachgewiesen werden muss, wofür dieselben Voraussetzungen gelten dürften, wie für die Präsentation des Dokumentinhaltes: Zurechenbar ist diese Zeitangabe allenfalls dann, wenn nachgewiesen werden kann, dass mögliche Fehler oder Manipulationen (etwa das Verstellen der Rechnerzeit) in der Risikosphäre des Signierers lagen. Mehrdeutigkeiten, etwa widersprechende Zeitangaben im Dokument und der Signatur hat der Beweisführer aufzuklären. Ist dies nicht der Fall oder muss gar die Autorisierung nachgewiesen werden, so sind andere Beweismittel erforderlich.

Im Streitfall könnte der Signierzeitpunkt aber anhand eines von einer "vertrauenswürdigen Stelle" erstellten Zeitstempels zu den Daten nachgewiesen werden. Die Einwendungsmöglichkeiten gegen dieses Beweismittel und die zu deren Entkräftung erforderlichen Nachweise (insbesondere die kryptographische Sicherheit der Verfahren) sollen an dieser Stelle nicht vertiefend erörtert werden. Aber zwei Anmerkungen hierzu:

Soweit ein Zeitstempel einem Dokument nach dem Signierzeitpunkt hinzugefügt wurde, kann eingewendet werden, der Zeitstempel sei nachträglich erstellt worden. Er gebe also nicht den Signierzeitpunkt und auch nicht den der Präsentation an, sondern lediglich einen Zeitpunkt an, *vor* dem die Präsentation und der Signiervorgang erfolgt sei. Sofern ein Zertifikat vorhanden und nicht angezweifelt wird, kann dann z.B. der Zeitpunkt der Schlüsselerstellung oder Chipkartenausgabe als frühestmöglicher Zeitpunkt erkannt werden.¹²⁰ Die Korrektheit des Präsentationssystems des Signierers muss dann innerhalb dieses Zeitraumes nachgewiesen werden. Soweit ein Zeitstempel Teil der signierten Daten ist, gibt er umgekehrt den frühest möglichen Signierzeitpunkt an. Die Korrektheit des Präsentationssystems des Signierers muss dann nach diesem Zeitraum bis zum Zeitpunkt der Prüfung (bzw. der Klageerhebung) nachgewiesen werden. Erst eine Kombination aus internem und externem Zeitstempel ist also geeignet, den Signierzeitpunkt gut einzugrenzen.

¹¹⁹ Steedman 1990 und ISO/IEC 9834-1.

¹²⁰ Hier ist dann auf die zum Nachweis der Urheberschaft erforderlichen Indizbeweise zu verweisen, die hier ebenfalls noch nicht näher erörtert werden können.

Für den Nachweis der Autorisierung ist aber selbst dann im Streitfall noch nachzuweisen, dass der Zeitpunkt der Präsentation auch dem Zeitpunkt des Signierens entspricht. Denn es kann ja der Fall sein, dass ein Dokument auf einem System erstellt wurde und zu einem späteren Zeitpunkt ohne Präsentation nur noch signiert wurde.

iii) Zertifizierung von Systemen

Der Nachweis der Korrektheit eines Präsentationssystems zum Prüfzeitpunkt kann darüber geführt werden, dass qualitätsgeprüfte Hard- und Software zum Einsatz kommt. Zu denken ist hier insbesondere an nach nationalen und internationalen Sicherheitskriterien orientierte Prüfungen (ITSEC, Common Criteria). Die Prüfung erlaubt allerdings nicht ohne weiteres den Rückschluss, dass tatsächlich keine Fehler vorkommen. Prüfungen auf einem niedrigen Sicherheitslevel (E2 nach ITSEC oder EAL3 nach CC) sind auch in erster Linie Dokumentprüfungen, d.h. der Hersteller wird gezwungen, Programme und Herstellungsverfahren ausführlich zu beschreiben, wohingehend Code-Inspektionen nur stichprobenartig stattfinden. Fehler können auch unerkannt bleiben. Schließlich ist nachzuweisen, dass ein bestimmtes zertifiziertes System tatsächlich eingesetzt wird. Dies ist aber mit Hilfe der Prüfung digitaler Signaturen zu Programmen oder durch Neuinstallation eines Systems mit Software aus vertrauenswürdiger Quelle leicht möglich. Problem ist aber, dass nur wenige Programme bislang zertifiziert sind, von den vielfältigen Komponenten, die die Präsentation beeinflussen, sicher nur wenige.

Ist also ein System evaluiert und zertifiziert, so kann der Richter dies als Beweis der Indiztatsache der Korrektheit im Rahmen freier Beweiswürdigung akzeptieren. Er muss dann seine Überzeugung aber begründen und die Beurteilung ist eventuell leicht angreifbar.

iv) Vorbeugende Prüfungen der Anwenderinfrastruktur

Die Korrektheit des Signiersystems zum Signierzeitpunkt lässt sich, da dieser ja vergangen ist, nicht mehr unmittelbar technisch nachweisen. Allenfalls bei einem System, das nicht frei programmierbar ist und bei dem Veränderungsversuche äußerlich erkennbar sind, mag man von einer aktuellen Prüfung auf einen vergangenen Zustand schließen können.¹²¹

Einen Rückschluss auf einen früheren Zustand könnte man aber dann ziehen, wenn in dem fraglichen Zeitraum Revisionen stattfanden.¹²² Der Nachweis regelmäßiger Revisionen der Anwenderinfrastruktur kann als Indiz für die Abwesenheit grober Fehler gewertet werden. Der Nachweis anlassbezogener Kontrollen (etwa beim Wechsel von Software) können den Einwand von Konfigurations- und Installationsfehlern entkräften.

Schwieriger ist der Nachweis der Abwesenheit von Manipulationen, da solche jederzeit erfolgen können, wobei der korrekte Zustand sofort nach einer Falschpräsentation wiederhergestellt worden sein kann. Hier können aber – wie bei der Datenschutzkontrolle – unangekündigte Kontrollen in Frage kommen. Ein Anbieter von Anwenderinfrastrukturen, der mit solchen Kontrollen rechnen muss wird aus eigenem wirtschaftlichem Interesse Vorkehrungen gegen Fehler und Manipulationen treffen. Der Nachweis, dass solche Kontrollen stattfanden oder mit ihnen zu rechnen war, könnte als Beweis der Indiztatsache gelten, dass das bei Signieren verwendete System mit seiner Präsentationskomponente korrekt war.

¹²¹ Siehe Chipkarten.

¹²² Pordesch / Hammer / Roßnagel 1991.

Allerdings dürfte ein solcher Nachweis dann kaum akzeptabel sein, wenn der Beweisführer Betreiber der Anwenderinfrastruktur ist, weil er gezielt und jederzeit Manipulationen durchführen und leicht vertuschen kann.

5.3.3 Rechtliche Beweiserleichterungen

i) Sicherheitsvermutung des Signaturgesetzes

Zweck des Signaturgesetzes ist es nach § 1 SigG, "Rahmenbedingungen zu schaffen, unter denen Signaturen als sicher gelten..". Von Roßnagel wird dies als eine Art vorgezogener „Anscheinsbeweis“ interpretiert:¹²³ Signaturen die mit Verfahren und unter Berücksichtigung der Bedingungen des Signaturgesetzes erzeugt worden sind, haben nach Roßnagel zunächst den Anschein nicht gefälscht oder verfälscht zu sein. Dies impliziert keinen unwiderlegbaren Beweis und auch keine Umkehrung der Beweislast, also dass der Beweisgegner nun beweisen müsste, nicht signiert zu haben. Vielmehr handelt es sich um eine sich mittelbar auswirkende **Sicherheitsvermutung**. Der Beweisgegner habe in diesem Falle substantiierte Einwendungen vorzubringen, um den Anschein zu erschüttern. Insbesondere habe er das Gericht davon zu überzeugen, dass die Rahmenbedingungen des Signaturgesetzes beim Zustandekommen der Signatur nicht eingehalten wurden. Gelingt ihm das, so muss der Beweisführer die konkreten Bedingungen des Einzelfalls nachweisen. Ansonsten kann das Gericht Einwände als unbegründet verwerfen. Entscheidend bleibt aber letztlich die freie Beweiswürdigung durch das Gericht.

Wie jedoch bereits oben erörtert, enthält das Signaturgesetz nur wenige die Präsentation und Interpretation von Daten betreffenden Anforderungen, sondern fast ausschließlich solche zur Unversehrtheit und Urheberschaft der Rohdaten.¹²⁴ Die Vorschriften nach § 14 SigG, dass Komponenten erforderlich sind, die feststellen lassen, auf welche Daten sich eine Signatur bezieht, betreffen auch nur das lokale Risiko der Falschpräsentation. Dass der Inhalt "nach Bedarf" angezeigt werden soll, enthält keinen Zwang zur Eindeutigkeit und bezieht sich nur allgemein auf die Inhaltsart. Risiken der Mehrdeutigkeit werden nur durch die Forderung nach Eindeutigkeit der Interpretation der Daten bei geschäftsmäßig Dritten zur Nutzung angebotenen Komponenten angesprochen.

Das Signaturgesetz enthält auch keine Vorgaben zur Kontrolle des Betriebs von Anwenderinfrastrukturen. Kontrollrechte und Pflichten sind bislang ausschließlich für Zertifizierungsstellen festgelegt.

Anwendbarkeit der Sicherheitsvermutung auf die Präsentation?

Inwiefern kann das Signaturgesetz nun die Beweisführung erleichtern? Dies hängt letztlich von den nach Signaturgesetz getroffenen Maßnahmen ab. Ist, wie in den Signaturinteroperabilitätsspezifikationen vorgeschlagen, der Datentyp (als Verweis auf ein Programm-Dateiformat) Teil der signierten Daten, so könnte zunächst der Anschein gelten, dass diese Eintragung richtig erfolgt ist. Daraus könnte dann gefolgert werden, dass irgendein Programm, das diesen Datentyp erzeugen kann, für die Präsentation zu verwenden ist. Voraussetzung

¹²³ Roßnagel, NJW 1998, 3312 ff.

¹²⁴ Siehe Kapitel Teil II:4.1 Gesetze und Ausführungsbestimmungen.

dafür ist allerdings, dass die Eintragung des Dateityps bei dessen bestimmungsgemäßen Gebrauch richtig erfolgt ist, mithin, dass ein entsprechend sicheres nach ITSEC evaluiertes Programm eingesetzt wurde. Dass ein solches Programm durch den Signierer zu verwenden war, könnte das Gericht aus der Unterrichtungspflicht der Zertifizierungsstelle nach § 6 SigG über vom Teilnehmer einzuhaltende Sicherheitsmaßnahmen folgern.¹²⁵ Wird diese bestritten, ist wiederum ein Beweis etwa anhand einer Unterschrift unter ein ausreichendes Unterrichtungsdokument erforderlich und natürlich auch die tatsächliche Existenz entsprechend evaluierter Programme.

Diese Nachweisführung hat Haken. Zum einen kann das Gericht aus den Unterrichtungspflichten und den genannten Maßnahmen nicht den Anschein ableiten, dass tatsächlich ein entsprechendes Programm verwendet wurde. Eine versehentliche Missachtung der einzuhaltenden Sicherheitsvorkehrungen, etwa die Verwendung eines ungeprüften fehlerhaften oder manipulierten Programms, ist durchaus möglich. Der Nachweis der tatsächlichen Präsentation - für den vor allem strafrechtlich bedeutsamen Nachweis der Autorisierung - ist alleine hiermit nicht führbar. Allenfalls gilt dies für den besonders zivilrechtlich bedeutsamen Nachweis der zurechenbaren Präsentation. Zum Zweiten sind selbst für den Nachweis eines zurechenbaren Präsentation der Nachweis der Einhaltung der durch das Signaturgesetz gegebenen Rahmenbedingungen erforderlich: Es müssen die Programme zertifiziert sein, die dem Benutzer vor dem Signiervorgang anzeigen, welche Eintragung vorgenommen wird und die sie dann durchführen, sowie alle dazwischen liegenden und die Eintragung möglicherweise noch beeinflussenden Prozesse sein. Selbst wenn alle Teilprozesse (Anzeige, Eintragung) in einem zu evaluierenden Prüfprogramm vereinigt sind, müssen zumindest diejenigen Funktionen des Betriebssystems, die von dem Prüfprogramm genutzt werden, auch sicher angesteuert werden. Ohne entsprechendes zertifiziertes Betriebssystem dürfte auch dieser Nachweis schwer fallen.

Zum Dritten ist der Nachweis des zurechenbaren Datentyps bei weitem noch kein Nachweis einer bestimmten zurechenbaren Präsentation. Weder das Signaturgesetz noch die Signaturverordnung enthalten Regelungen für die Organisation des Vergabeverfahrens der dazu erforderlichen Objektbezeichner und die Überprüfung der Tätigkeit diesbezüglich tätiger Organisationen. Wie dargelegt können sich auch verschiedene Aspekte der Präsentation aufgrund von gewähltem Programm, Konfiguration, Endgeräten, Einstellung, Benutzung und Umfeld voneinander stark unterscheiden. Da Signaturgesetz und -verordnung hierzu keine (zumindest keine klaren) rechtlichen Vorgaben und die Maßnahmekataloge keine technischen enthalten, schafft in diesem Falle die Sicherheitsvermutung des Signaturgesetzes keine Beweiserleichterung. Sind Aspekte der Präsentation jenseits des Datenformats umstritten, so wird der Beweisführer alle diese Einwände voll entkräften und die tatsächliche Präsentation des Signierers beweisen müssen.

ii) Beweisvermutung des § 126 a BGB (Entwurf)

Nach §126a soll die Abgabe der Erklärung vermutet werden, soweit ein Dokument Textform und eine Signatur nach Signaturgesetz aufweist und soweit die Rahmenbedingungen des Signaturgesetzes, außer den Obliegenheiten des Schlüsselinhabers zuverlässig festgestellt werden können. Damit wird versucht, an die Sicherheitsvermutung des Signaturgesetzes explizit die Rechtsfolge zu knüpfen, dass die empfangene signierte Willenserklärung dann zivilrecht-

¹²⁵ Wenn diese hinreichend konkret wären, was sie z.Zt. noch nicht sind.

lich auch als abgegebene Willenserklärung zu gelten hat.¹²⁶ Ein die Signatur Prüfender soll aus einer erfolgreichen Prüfung einer SigG-konformen Signatur auf die Zurechenbarkeit der Willenserklärung schließen dürfen. Der Signierende soll sich nicht auf in seinem Verantwortungsbereich liegende Fehler berufen können, sondern zumindest für den entstandenen Schaden beim Vertrauen auf die Signatur haften.

Zusätzliche über die Sicherheitsvermutung des Signaturgesetzes hinausgehende beweis erleichternde Vorschriften enthält der Entwurf nicht. Der Verweis auf die "Obliegenheiten des Schlüsselinhabers" verweist lediglich auf die Vorsichtspflichten, über die die Zertifizierungsstelle den Signierer zu unterrichten hat.

Allerdings kann der BGB-Entwurf seinem beweis erleichternden Anspruch wohl kaum gerecht werden. Er bezieht sich nur auf das Signaturgesetz, das wie ausgeführt höchstens den Anschein der Echtheit des Datentyps begründen kann. Zwar schließt der Verweis auf die Obliegenheiten möglicherweise den Einwand einer fehlerhaften Präsentation des Signierers aus - wobei rechtlich und technisch gesehen höchst problematisch wäre, dass der Aspekt der Verfügungsmacht über die Anwenderinfrastruktur (die Risikosphäre) nicht berücksichtigt wird. Um die Willenserklärung nachzuweisen, müßte jedoch auch das Risiko der Mehrdeutigkeit durch das Signaturgesetz mit der Sicherheitsvermutung des SigG abgedeckt werden. Das wird es jedoch nicht.

Die BGB-Änderung dürfte daher zumindest hinsichtlich der beweisrechtlichen Folgen für den Nachweis der Präsentation ins Leere laufen. Der „elektronische Form“ fehlte folglich die verfassungsmäßig notwendige „Beweisfunktion“ als eine von vielen Schutzfunktionen einer gesetzlichen Form.

5.3.4 Vertragliche Beweiserleichterungen

Mit vertraglichen Regelungen kann Beweisrecht nicht verändert werden und die freie Beweiswürdigung des Richters einschränkende Regelungen wären nichtig. Auch einseitige Willenserklärungen, auf bestimmte Einwendungen in einem eventuellen Prozeß freiwillig zu verzichten, wären im Zweifelsfall unwirksam. Hingegen ist es sehr wohl möglich, Regelungen zur Interpretation und Präsentation signierter Daten zu treffen, die mögliche Mehrdeutigkeiten ausschließen sollen.¹²⁷ Liegen solche Willenserklärungen vor, so kann sich der Beweisgegner jedenfalls nicht mehr auf die Mehrdeutigkeiten berufen, die nach konsequenter Befolgung der Vereinbarung nicht aufgetreten wären. So könnten - wie dies bei Autorenverträgen heute bisweilen ja auch geschieht - Regelungen über den Gebrauch von Word-Dokumenten zwischen Geschäftspartnern getroffen werden - etwa über den ausschließlichen Gebrauch bestimmter Dokumentvorlagen und die Bedeutung der darin definierten Formate. Der Beweisgegner kann dann nicht erfolgreich einwenden, der Signierer habe nicht gewusst, welche Dokumentvorlage zu verwenden ist und zulässigerweise eine andere verwendet.

Die Schwierigkeit solcher Vereinbarungen liegt zum einen darin, dass sie inhaltlich recht umfangreich sein müssten, um Probleme der Mehrdeutigkeit zuverlässig zu vermeiden. Sie müssten detaillierte Vorgaben enthalten zu:

- Mindesteigenschaften der Ausgabegeräte,

¹²⁶ Siehe hierzu Bundesministerium der Justiz 1999 (Stand 19.Mai 1999).

¹²⁷ Etwa über Papierverträge, die dann als Urkunden im Prozeß verwertet werden können (In eine solche Richtung gehen wohl die EDIFACT-Rahmenvereinbarungen).

- Vorgeschriebene, zulässige und unzulässige Features,
- Systemkonfiguration, zu verwendenden Programme,
- Bedienung und Einstellungen durch die Nutzer.

Eine Schwierigkeit solcher Vereinbarungen liegt auch darin, dass sie zwischen einander unbekannten Partnern über das Internet im Voraus schwerlich getroffen werden können, vor allem nicht in beweisbarer Form. Denkbar wäre, dass einer der Kooperationspartner etwa über die Integration in allgemeine Geschäftsbedingungen (AGBs) bekannt gibt, wie andere seine Willenserklärungen interpretieren und präsentieren lassen sollen und wie er selbst ankommende signierte Daten zu interpretieren und präsentieren gedenkt. Allerdings müssen solche Bedingungen sicher zumutbar und auch zugänglich sein, was bei ihrem Umfang und ihrer Komplexität problematisch erscheint. Unter welchen Bedingungen solche Verpflichtungen bindend wären, müsste daher in einer juristischen Untersuchung geklärt werden.

5.4 Verbleibende Beweisprobleme

Die Untersuchung hat gezeigt, dass bei der absehbaren Rechtslage und unter Berücksichtigung der technischen Möglichkeiten Einwendungsmöglichkeiten gegen die Präsentation signierter Daten verbleiben. Dabei ist die Sicherheitsvermutung des Signaturgesetzes allenfalls in Bezug auf den Dateityp anwendbar. Ein Anschein einer Richtigkeit der Präsentation (Zurechenbarkeit oder gar Autorisierung) wird aus den signierten Daten oft nicht ableitbar sein. Wird die Präsentation bestritten, so müssen jeweils die Bedingungen des Einzelfalls berücksichtigt werden, wobei eine Kette von Indiztatsachen zu entwickeln und eingehend zu prüfen ist. Dafür dürfte es regelmäßig der Konsultation von Sachverständigen bedürfen.¹²⁸

Jeder Partei im Zivilverfahren steht es grundsätzlich frei, als Beweismittel auch Sachverständige zu beauftragen und als Zeugen zu laden. Über die Art des Sachverständigen, seine Qualifikation und seine Fragestellungen entscheidet in diesem Falle die Partei selbst, es gibt keine gesetzlichen Vorgaben. Die Würdigung der Ergebnisse solcher von einer Partei beauftragten und somit auch oft parteiischen Sachverständigen steht dem Gericht aber völlig frei.

Etwas anders ist die Lage, wenn das Gericht selbst den Parteien im Falle strittiger Tatsachen die Hinzuziehung eines (neutralen) Sachverständigen vorschlägt. Weil bei gerichtlich beauftragten Sachverständigen die Fragestellungen vom Gericht vorgegeben werden, wird den Aussagen dieser Sachverständigen in der Regel mehr Beweiswert zugemessen werden. Die Kosten hat in diesem Fall die Partei zu tragen, die den Prozess verliert. Sachverständige werden gerichtlich beauftragt, wenn eine Inaugenscheinnahme nicht möglich oder eine Tatsache mangels Fachkenntnis des Gerichtes von diesem nicht für bewertbar gehalten wird. Im Falle von Papierdokumenten ist die Schriftvergleichung als Sachverständigentätigkeit in der deutschen Zivil- und Prozessordnung fest verankert (§§ 441 f ZPO). Außerdem gibt es in der Praxis die allgemeine Vorgabe, in der Regel nur öffentlich bestellte und vereidigte Sachverständige hinzuzuziehen. Die Begutachtung signierter Dokumente ist bislang nicht geregelt und öffentlich bestellte Signatursachverständige sind selbstverständlich bislang unbekannt. Unabhängig davon hat das Gericht jedoch in solchen neuen Fällen das Recht, die Sachverständigen zu beauftragen, die es in diesen neuartigen Fällen für geeignet hält. Möglicherweise wird man

¹²⁸ Also im Gegensatz zur Annahme von Bleutge 1997. Ob es freilich dazu kommt, ist eine soziale Frage, da der Prozeßverlierer die Kosten für Sachverständige tragen muss. Es kann also ohne weiteres sein, dass sich die wirtschaftlich schwache Seite, weil sie das finanzielle Risiko, dass der Sachverständige keinen Erfolg hat, nicht eingehen will.

sich zunächst an vereidigte EDV-Sachverständige halten und soweit diese die Fragen nicht beantworten können, an mit Signaturfragen beschäftigte Praktiker und Wissenschaftler.

Der gerichtlich beauftragte Sachverständige hat vom Gericht vorgegebene streitige Tatsachen zu untersuchen.¹²⁹ Wenn eine Unterschrift fraglich ist, hat er die Unterschrift auf Echtheit zu untersuchen, und nicht etwa (zusätzlich) das Alter des Dokumentes. Nur in Ausnahmefällen darf der Sachverständige streitige Tatsachen selbst ermitteln, wenn bereits hierfür dem Gericht die erforderliche Sachkunde fehlt. Dies wird bei digital signierten Dokumenten zumindest in der Anfangsphase gerichtlicher Auseinandersetzungen der Fall sein, wenn das Gericht die Echtheitsfragen (Präsentation, Signatur, Zeitstempel, Zertifikat,...) mangels Sachkenntnis erst gar nicht richtig stellen kann.

¹²⁹ Zur Rolle des Sachverständigen Rudolph 1980.

6. Sachverständigenbegutachtung

Nachdem zuvor Beweisfragen herausgearbeitet wurden, deren Klärung die Prozessbeteiligten und den Richter überfordern dürfte, ist nun zu untersuchen, inwieweit Sachverständige zusätzliche Erkenntnisse gewinnen können. Wissenschaftlich gesehen geht es dabei um die Möglichkeit analytischer und empirischer Methoden, wie sie im Bereich der Handschriftenanalyse mit der wissenschaftlichen Schriftvergleichen entwickelt wurden.¹³⁰

6.1 Aufgaben der Begutachtung

Aus der vorangegangenen Prospektion einer wahrscheinlichen Beweisführung lassen sich im Zusammenhang mit der Präsentation einige Fragestellungen isolieren, die Prozessparteien alleine kaum beweisen können oder bei denen einem Richter die fachliche Grundlage zur Bewertung fehlen dürfte:

Existenz alternativer Präsentationen

Hierbei geht es vor allem um das Erkennen möglicher Schutzbehauptungen. Der Beweisgegner verweist – etwa anhand dieses Papiers – auf die Möglichkeit der Mehrdeutigkeit und schließt daraus auf die Möglichkeit einer substantiell anderen Willenserklärung im vorliegenden Fall. Kann der Signierer nicht befragt werden, so wird das Gericht oder der Beweisführer einen Sachverständigen mit der Klärung der Frage beauftragen müssen, ob im konkreten Fall für den Prozessgegenstand wesentliche Mehrdeutigkeiten nicht doch ausgeschlossen werden können.

Die Möglichkeit von Falschpräsentationen ist immer gegeben, deshalb ist die pauschale Frage nach deren Existenz stets mit "ja" zu beantworten. Sinnvoll ist die Frage aber unter bestimmten technischen Randbedingungen oder bestimmten Ursachen (etwa: Ist es möglich, dass der Signierer mit korrekt installiertem Word einen Fehler beging, bei dem bestimmte Zahlenangaben verfälscht wurden?).

Wahrscheinlichkeit gegebener Alternativpräsentationen

Soweit Mehrdeutigkeiten oder Falschpräsentationen nicht ausgeschlossen werden können oder sogar konkret vorgeführt werden, sind vergleichende Aussagen über deren Wahrscheinlichkeit im konkreten Fall gefragt, um die vom Signierer wahrscheinlich intendierte Präsentation zu ermitteln.¹³¹

¹³⁰ Michel 1982, Ries 1989.

¹³¹ Da der tatsächliche Vorgang abgeschlossen und niemals wiederholbar / rekonstruierbar ist, handelt es sich um die Wahrscheinlichkeit von Vermutungen (Hypothesen).

Umstände einer Präsentation

Konkrete Aussagen zu den Ursachen interessieren für die Klärung der Schuldfrage, ob also eine Manipulation durch Externe oder ein Benutzerfehler Ursache der Falschpräsentation gewesen sein kann. Für die Zurechenbarkeit ist wichtig, in wessen Verantwortungsbereich mögliche Fehler lagen, weshalb es Aufgabe eines Sachverständigen sein kann, alle Komponenten der Anwenderinfrastruktur und den Dokumentersteller zu identifizieren.

6.2 Untersuchungsmöglichkeiten

Für die Frage, ob und wie eine Sachverständigenbegutachtung möglich ist, sind zunächst die möglichen zusätzlichen fallbezogenen (empirischen) Erkenntnisquellen zu untersuchen.

6.2.1 Signierte Daten

Dies sind zunächst die Daten aus der Signatur und dem signierten Dokument selbst u.U. in Verbindung mit weiteren Erkenntnisquellen.

Signatur

Nach den Signaturinteroperabilitätsspezifikationen soll ein eindeutiger Objektbezeichner Teil der signierten Daten werden, der einen Verweis auf den Datentyp bzw. das Dokumentformat darstellt.¹³² Die Angabe ist optional, also nicht zwangsweise Bestandteil der Signatur, enthält z.T. keinen Versionsbezug und verweist nicht auf das genutzte bzw. zu nutzende Programm.¹³³ Dennoch kann bei einigen Angaben wenigstens auf eine Klasse vorgesehener Programme zurückgeschlossen werden, mit denen die Daten präsentiert worden sind bzw. werden sollen. So gibt es nur wenige Programme, die CORELDRAW-Grafiken erzeugen können, außer dem gleichnamigen Programmen selbst. In Verbindung mit der Signaturzeit kann z.B. bei einem neueren Dokument und dem Microsoft-Word für DOS-Format geschlossen werden, dass wahrscheinlich ein altes Word-Programm eingesetzt wurde.

Einen Hinweis auf das vom Signierer intendierte Programm kann auch die Angabe Dateibezeichner liefern, insbesondere bei Windows-basierten Systemen die Dateiendung. So könnte im Fall Fallbeispiel 1: "Testtext oder Beleidigungsgrafik?" aus der Angabe des Dateibezeichners mit der Endung ".TXT" ein Indiz dafür gesehen werden, dass die Signiererin tatsächlich glaubte eine Textdatei zu signieren anstatt einer beleidigenden Grafik.

Auch alle anderen optionalen Angaben in der Signatur nach den SigI (Ortsangabe, Mitzeichnung, Speicherdatum und -zeit und Signaturnummer) mögen im Einzelfall im Zusammenhang mit anderen Daten (etwa Ortsangaben im Dokument, Datum der letzten Änderung der Datei) Indizien für den tatsächlichen Verlauf der Präsentation liefern. Allerdings ist ihre Authentizität nicht nachweisbar, sondern muss aus den Umständen des Falles eingeschätzt werden.

¹³² SigI 1998 Abschnitt A2: Signatur, Version 4.0, S. 27.

¹³³ SigI 1998 Abschnitt A2: Signatur, Version 4.0, S. 76.

Zertifikate

Eine weitere Erkenntnisquelle sind die Zertifikate. Profile für Zertifikate und Sperrlisten enthalten nach der SigI-Spezifikation das Feld "Key usage", das der Unterscheidung verschiedener Verwendungszwecke öffentlicher Schlüssel dient.¹³⁴ Auch die Verweise auf die Zertifizierungsrichtlinien (CertificatePolicies) und die Angabe äquivalenter Policies (PolicyMappings) können Hinweise auf den Anwendungszweck liefern. Auf diese Weise können z.B. Hinweise auf eine Falschpräsentation oder Fehler und Versehen bei der Autorisierung gewonnen werden.

Signierte Nutzdaten

Ist das Dateiformat bekannt oder wird dies vermutet, so können die signierten Daten ausgewertet werden.¹³⁵ Je nach Datentyp können diese eine Reihe von Daten enthalten, die Rückschlüsse auf das verwendete Programm oder die verwendete Anwenderinfrastruktur zulassen. Beispiele für diese je nach Dateityp höchst unterschiedlichen Angaben sind beispielsweise:

- Rechnerkennung
- Programm und Programmversion
- Plattform (MAC oder Word) bei Winword-Format
- Druckertreiber (z.B. Word)
- Ersteller
- Versionsinfos
- Änderungsdatum
- Letzte Ansicht
- Überarbeitungen, Vorversionen, gelöschte Textteile
- Fontdateien, alternativer Font
- Autornamen, Name des letzten Überarbeiters
- Datum der Dokumenterzeugung, der letzten Änderung
- Namen von Druckformatvorlagen bzw. Dokumentvorlagen
- Dateinamen für Grafiken, Hintergrundmuster, WWW-Links

Viele dieser Daten sind zumindest Laien unbekannt, so dass je nach Fallkonstellation darauf geschlossen werden kann, dass diese nicht bewusst verfälscht wurden. Dies gilt besonders für Features, die durch Anwendungsprogramme nicht geändert werden können.

6.2.2 Anwenderinfrastruktur

Kann die Anwenderinfrastruktur oder können Teilkomponenten davon aus den signierten Daten oder fallbezogenen Quellen (etwa den Ermittlungsakten) ermittelt werden, sind weitere Untersuchungen möglich:

Hardware

Die Funktionsfähigkeit der Geräte, deren Einstellung und die Zugänglichkeit der Regler kann ermittelt werden. Tests wären durchzuführen (im Regelbetrieb ist dies allerdings schwierig).

¹³⁴ Siehe hierzu Biester / Bauspieß / Fox 1999b, 15.

¹³⁵ Zu Dateiformaten siehe Born 1997.

Präsentations- bzw. Anwendungsprogramm

Ist das Anwendungsprogramm bekannt (oder wird es vermutet) so sind die verschiedenen Präsentationsmöglichkeiten hinsichtlich der für den Prozessgegenstand wesentlichen und umstrittenen Aspekte durchzutesten. Ist etwa umstritten, um in einem Word-Dokument ein als Preisangabe vorgesehener Textrahmen für den Signierer sichtbar war und gegebenenfalls wo, so wären bezogen auf das konkrete in Frage stehende Dokument systematisch alle Ansichtsmöglichkeiten durchzutesten. Bei Word sind dies dann u.a.:

- Optionen.Ansicht: Konzeptschriftart
- Optionen.allgemein
 - Weiß auf blauem Hintergrund
 - Prüfungen während der Dateieingabe
 - Optionen.überarbeiten
 - Änderungen markieren
- Ansichten
 - Datei.Seitenansicht
 - Ansicht.Zentraldokument
 - Ansicht.Gliederung
 - Ansicht.online-Gliederung
 - Ansicht.Seitenlayout
 - Ansicht.Zoom
 - Ansicht.Ganzer Bildschirm
 - Grafiken, Objekte
- Fenster
 - Teilen (wird nicht gespeichert)

Betriebssystem

Die Korrektheit der Programme und die Abwesenheit von Manipulationen und Fehlern läßt sich durch Neuinstallation des Systems überprüfen. Daneben ist die Konfiguration des Betriebssystems zu untersuchen. Notwendige Untersuchungen im Betriebssystem sind

- Fontbibliotheken: Soweit die Zeichensätze nicht Teil des Dokumentes sind, wird auf lokale Zeichensätze der Maschine zurückgegriffen. Diese werden anhand des Fontnamens identifiziert. Das Anwendungsprogramm kann auch Ersatzfonts auswählen, wenn lokal bestimmte Fonts nicht vorhanden sind.
- Bildschirmeinstellungen des Gerätetreibers:
- Bildschirmeinstellungen: Hintergrundfarbe des Fensters
- Ausgewählter Bildschirmtreiber

6.2.3 Umstände des Falls

Weitere mögliche Informationsquellen sind die Akten. Zwar ist es umstritten, inwieweit auch fallbezogene Aspekte aus der Vernehmung oder den Ermittlungsakten in die Sachverständigenbegutachtung eingehen dürfen. Im Falle der Klärung der die Präsentation betreffenden Fragen dürfte dies jedoch unumgänglich sein. Denn schon die Frage, welcher Aspekt denn eigentlich umstritten ist, bestimmt die Untersuchung der Möglichkeit bestimmter Abweichungen und kann durch den Richter wahrscheinlich nicht beurteilt werden..

Eine weitere Informationsquelle ist der Signierer. Die Untersuchung seiner Verhaltensweisen kann Rückschlüsse auf bevorzugte Konfigurationen, Vorwissen und die Wahrscheinlichkeit von Fehlverhalten, die Befähigung zu komplexen Manipulationen erlauben.

6.3 Bewertung

Aus dem Fachwissen über Dokumentformate und Untersuchungen der Anwenderinfrastruktur können Sachverständige also zumindest Hinweise auf die Umstände der Präsentation des Signierers gewinnen. Daraus lassen sich in einer fehlerbaumartigen Analyse die möglichen abweichenden Präsentationen und ihre Ursachen ermitteln.

Bisweilen mögen solche Erkenntnisse bereits ausreichen. In einigen Fällen, wie etwa bei der Frage, ob ein Bitstring Ergebnis eines bestimmten Programmes sein *kann*, ist es z.B. durch eine Analyse der Datenstruktur oder einen Test festzustellen, ob eine Hypothese über die Möglichkeit einer bestimmten Präsentation verneint werden kann (wenn die Korrektheit der programme nicht angezweifelt wird). Sobald jedoch verschiedene Möglichkeiten gezeigt sind, interessiert weitergehend, wie wahrscheinlich die Hypothese einer bestimmten Präsentation ist. Ziel einer wissenschaftlichen Begutachtung sollte es dabei sein, möglichst fundierte Wahrscheinlichkeitsaussagen über verschiedene Präsentationsmöglichkeiten zu gewinnen.

6.3.1 Möglichkeiten exakter Wahrscheinlichkeitsaussagen

Angesichts der vielen weichen Faktoren fragt man sich, ob es überhaupt möglich ist, im Zusammenhang mit der Präsentation zu irgendwelchen exakten Wahrscheinlichkeitsaussagen zu kommen. Das folgende Beispiel zeigt zunächst, dass dies in Einzelfällen durchaus möglich sein kann:

Beispiel: Hypothese des zufälligen Bitstrings

Der Beweisgegner im Prozess könnte behaupten, von einem Anwendungsprogramm interpretierbare signierte Daten seien nicht mit diesem erzeugt worden, sondern in Wirklichkeit rein zufällig. Er habe diese Daten mit einem Testprogramm erzeugt, das Zufallswerte für wissenschaftliche Experimente erzeuge und diese dann signiert. Handelt es sich um einen kurzen Bitstring, wird das Gericht diese Behauptung nicht ohne nähere fachliche Einlassung als Schutzbehauptung abweisen können, sondern einen Sachverständigen beauftragen.

Ein Sachverständiger kann diese Behauptung des Beweisgegners auf folgende abstrakte Fragestellung zurückführen:

Wie groß ist die Wahrscheinlichkeit, dass ein Zufallszahlengenerator einen Bitstring der Länge N erzeugt, der einem Code des Codierungsverfahrens C entspricht?

Sei $\#C(n)$ = Anzahl der gültigen Nachrichten des Codes C der Länge n
und $\#M(n)$ die Anzahl möglicher Nachrichten der Länge n
 i eine bestimmte Nachricht (Bitfolge, Datei).

In einem solchen Fall ist leicht einzusehen, dass für die Wahrscheinlichkeit $p(i)$, dass die Nachricht (bei einmaligem Versuch) zufällig erzeugt wird gilt

$$p(i) = \#C(n) / \#M(n) = \#C(n) / 2^n$$

Dies ist zugleich die Redundanz (oder der Informationsgehalt) des Codierungsverfahrens.

In der Praxis ist es zumeist unmöglich $\#C(n)$ zu bestimmen. Andererseits dürfte es in den allermeisten Fällen genügen, $\#C(n)$ nach oben abzuschätzen, um eine brauchbare Abschätzung der Wahrscheinlichkeit zu erhalten. $\#C(n)$ kann nach oben abgeschätzt werden, indem die Mächtigkeit einer Übermenge $\ddot{U}C(n)$ des Codes bestimmt, über die man besser Aussagen treffen kann.

$$\text{Mit } C(n) \quad \ddot{U}C(n) \text{ gilt } \#C(n) \leq \#\ddot{U}C(n)$$

$$p(i) = \#C(n) / 2^n \leq \#\ddot{U}C(n) / 2^n$$

Oft wird man nicht einen einzelnen Code haben, der in Frage kommt, sondern mehrere. In diesem Fall wäre die Gesamtmenge der nach diesen Codes möglichen Ergebnisse zu berechnen ist $\#C^*(n) = \# \cup (C_1..C_n)$ zu berechnen. Dies dürfte freilich noch schwieriger sein, als bei einem einzigen Code, weshalb auch hier eine grobe Abschätzung nötig ist. Die Aufgabe besteht dann darin, möglichst eine Übermenge aller in Frage kommenden Codes zu finden.

Beispiel Lesbare ASCII-Zeichen

Da jedes Byte einem ASCII-Zeichen entspricht, ist jeder Bitstring auch ein ASCII-String (dessen Länge durch 8 teilbar ist), der durch einen ASCII-Editor erzeugt worden sein kann. Die Frage ist also nur für Teilmengen beantwortbar: Dasselbe gilt für andere nicht-redundante Codierungsverfahren.

Sinnvoll ist aber die Frage nach lesbaren ASCII-Zeichenfolgen (z.B. mittels eines ASCII-Editors erzeugter Text, z.B. eine Ziffernfolge für einen Zugangscode, aber auch HTML oder XML-Code). Dies lässt sich folgendermaßen einfach abschätzen: Sonderzeichen eingeschlossen sind 194 von 256 ASCII-Zeichen lesbar, hingegen 62 unlesbar. Mithin ist $p(i) < (194/256)^n$, was bereits bei einer 17 Zeichen langen lesbaren Nachricht unter 1% liegt.

Beispiel: Word 8

Gilt etwa $C(n)$ = Menge aller Word 8.0-Dateien der Länge n Bit. Über die Mächtigkeit dieser Menge ist nichts bekannt. Aber es hilft schon die (durch Nachfragen bei Microsoft gegebenenfalls zu verifizierende) Beobachtung, dass jede solche Datei stets mit einem bestimmten String aus 6 Byte anzufangen beginnt (6 Byte = 48 bit), um bereits eine aussagekräftige Abschätzung zu erhalten. Es kann dann nämlich grob vereinfachend davon ausgegangen werden, dass ansonsten jeder Bitstring Word-Dokument wäre, um die Hypothese zu bewerten. Für einen Bitstring der Länge n , der mit einem konstanten Bitstring der Länge k beginnt, gilt

$$\ddot{U}TC(n) = 2^{n-k} \text{ woraus banalerweise folgt}$$

$$p(i) < 2^{n-k} / 2^n = 1/2^k = 2^{-48} \approx 10^{-45}$$

Die Hypothese, ein Zufallszahlengenerator könne durch einmalige Berechnung eine solche Bitfolge erzeugt haben, wäre demnach - wenig verwunderlich - mit an Sicherheit grenzender Wahrscheinlichkeit auszuschließen. Das Ergebnis bliebe übrigens ähnlich eindeutig, wenn der Zufallszahlengenerator mehrfach rechnen würde.

Ähnlich konkrete, allerdings kompliziertere Berechnungen der Wahrscheinlichkeit sind bei Behauptungen der zufälligen Kollision zwischen Datenformaten möglich – etwa für die Behauptung ein zufällig gewähltes Datenformat habe einige Codes gemeinsam mit einem vorhandenen.

Auch die Wahrscheinlichkeit mit einem Codierungsschema ein Dokument zu erzeugen, das zufällig mehrdeutig ist, d.h zu einem anderen Codierungsschema entspricht, ist prinzipiell berechenbar. Hiermit lassen sich dann Einwände des Beweisgegners bewerten (und i.d.R. sicher widerlegen), wie etwa der im Fallbeispiel 2: Das selbst geschriebene Anwendungsprogramm¹³⁶, er habe ein Programm geschrieben, das rein zufällig eben eine bestimmte Datenformatkollision mit einem anderen Programm erzeuge.

¹³⁶ S. 44.

6.3.2 Grenzen

Leicht berechenbare Fragestellungen wie die zuletzt genannte dürften die Ausnahme bilden – gerade weil es verhältnismäßig leicht ist, entsprechende Behauptungen zu widerlegen. Bedeutend schwieriger ist die Wahrscheinlichkeit bestimmter Ursachen zu bewerten, die in genutzten Systemen, deren Konfigurationen und menschlichem Verhalten begründet sind.

Eine solche Frage ist im eingangs erwähnten Beispiel der elektronischen Urlaubskarte etwa, ob Frau Zange einen MacIntosh-Rechner mit kleinem 12 " schwarz-weiß-Bildschirm oder einen PC mit größerem Farbbildschirm genutzt hat. Weiß sie dies selbst nicht mehr oder kann sie nicht befragt werden, so könnte man versucht sein, eine Wahrscheinlichkeit für die Nutzung eines bestimmten Gerätes aus Beschaffungslisten der entsprechenden Jahrgänge zu berechnen. Allgemein ließen sich Wahrscheinlichkeiten für Kombinationen von Endgeräten und die Häufigkeit der Nutzung bestimmter Endgeräte aus Verkaufsstatistiken ermitteln. Allerdings führen solche Abschätzungen allerhöchstens dann zu verwertbaren Ergebnissen, wenn die Ereignisse "Nutzung/Besorgung einer Anwenderinfrastruktur " und "Präsentation des signierten Objekts" unabhängig voneinander sind – was in der Regel nicht der Fall ist, weil man sich große Bildschirme eben zur besseren Betrachtung bewusst anschafft und eben nicht rein zufällig irgendwelche Bildschirme zur Betrachtung nutzt.

Auf die Systemkonfiguration könnte man aus Statistiken über die Konfigurationsänderungen schließen. Wird etwa in einem konkreten Fall behauptet, der Bildschirmhintergrund eines Gerätes sei auf "schwarz" anstatt "weiß" eingestellt gewesen, so könnte man versuchen, diese Wahrscheinlichkeit über eine Statistik der Abweichungen von der Standardkonfiguration eines Betriebssystems zu ermitteln. Vermutung ist, dass die weitaus meisten Nutzer die Hintergrundfarbe ihres Bildschirms niemals schwarz einstellen. Auch die Wahrscheinlichkeit eines bestimmten Nutzerverhaltens (z.B. vollständiges Durchgehen durch einen zu signierenden Text) und Verständlichkeit bestimmter Buttons bzw. Menübefehle, aus denen auf die Autorisierung zurückgeschlossen werden kann, könnte man versuchen experimentell zu erheben.

Statistiken über die Abweichung von der Standardkonfiguration beim Betriebssystem (anderer Hintergrund, andere Farben) müsste man allerdings für bestimmte Nutzergruppen erstmal erstellen. Untersuchungen zu solch speziellen Fragen aus der Software- und Hardwareergonomie sind bislang nicht bekannt.¹³⁷ Ob es sich angesichts des rasanten Wandels der Technik und ihrer Anwendung lohnt, solche Fragestellungen überhaupt zu untersuchen und Statistiken zu erstellen, muss die Rechtspraxis zeigen.

6.4 Werkzeuge

Gutachter müssen soweit als möglich unabhängig von Systembetreibern und –herstellern arbeiten. Deren Interessen können darin liegen, erkannte Fehler oder Manipulationen bzw. entsprechende erkannte Fehler- und Manipulationsmöglichkeiten zu verschweigen. Deshalb sollten sie nicht auf Herstellerauskünfte angewiesen sein, sondern auf verfügbare Dokumentationen über Dokumentformate und Programmbeschreibungen (möglichst auch mit Quellcode) zugreifen können.

¹³⁷ Die Softwareergonomie interessiert sich auch mit Recht nicht für diese bloße Erbsenzählerei, sondern für Verbesserungen der Systemgestaltung. (Eberlein / Oberquelle / Oppermann 1995).

Heute haben Urkundensachverständige umfangreiche Sammlungen von Maschinenschriften, Schreibmitteleigenschaften und Handschriften, teilweise datenbankgestützt.¹³⁸ Die Menge der auf dem Markt angebotenen und genutzten Programme und Versionen ändert sich wahrscheinlich schneller, als die der Schreibmittel. Für Signatur-Sachverständige wäre längerfristig ein **Archiv** der unterschiedlichen im Rechtsverkehr genutzten Programme und Hardwaresysteme von Vorteil, um Präsentationsfragen langfristig klären zu können. Da auch die Hardware Beurteilungsgrundlage sein kann, wird man zentrale Einrichtungen benötigen (ähnlich der Handschriftensammlung im BKA).

Für die experimentelle Analyse sind universelle Dokument-Editoren erforderlich.¹³⁹

6.5 Probleme

Zusammenfassend läßt sich feststellen, dass eine Sachverständigenbegutachtung zwar zusätzliche Beweismöglichkeiten eröffnet, sicher aber keine Lösung für Beweisprobleme im Zusammenhang mit der Präsentation darstellt. Zusätzliche Angaben sind zwar in signierten Dokumenten oder Zertifikaten vorhanden, zuverlässige Rückschlüsse erlauben sie jedoch nur sehr eingeschränkt.

Besondere Probleme bereiten bei der Begutachtung:

- Undokumentierte, proprietäre Dateiformate: Viele Dokumentformate wurden von den Herstellern der entsprechenden Programme nicht dokumentiert. Informationen sind nicht verfügbar oder unsicher.
- Unvollständige Daten: Daten über das verwendete Programm, die verwendeten oder vorgesehenen Ausgabegeräte, Einstellungen des Benutzers, Betriebssystem und sonstige Systemkonfigurationen sind in den Dokumentformaten nicht durchgängig vorhanden, sondern differieren stark zwischen Datenformaten und sogar einzelnen Versionen. Viele für die Präsentation wesentlichen Aspekte der Systembenutzung, etwa die zuletzt gewählte Ansicht sind bislang nicht Gegenstand der Dateiformate.
- Nicht beweisbare Authentizität: Wichtige Daten über die genutzte Anwenderinfrastruktur und den Dokumentersteller (Namen, Dokumenterstellungsdatum,...) stammen aus unsicheren Quellen der Systemumgebung und können vom Nutzer jederzeit geändert werden.
- Fehlende Zugangs- und Prüfmöglichkeiten: Soweit die Klärung von Präsentationsproblemen nur auf einer in Betrieb befindlichen Anwenderinfrastruktur möglich ist (etwa der elektronischen Urlaubskarte), sind Test- und Untersuchungsmöglichkeiten stark eingeschränkt. Zeitlich zurückliegende Präsentationsvorgänge lassen sich kaum noch rekonstruieren.

¹³⁸ Kuckuck / Philipp 1989

¹³⁹ S. auch Hammer 1993, 269.

Teil III: Problemlösung

7. Rechtliche Gestaltungsanforderungen

In den vorangegangenen Kapiteln wurde gezeigt, dass sich hinsichtlich der Präsentation bei signierten Daten nach Signaturgesetz auch durch Sachverständige nur eingeschränkt Aussagen treffen lassen. Der Beweiswert digital signierter Daten ist deshalb eingeschränkt. Angesichts der großen Bedeutung der Signaturverfahren für die Entwicklung rechtsverbindlicher Telekooperation ist dies ein unbefriedigender Zustand. Deshalb soll im Folgenden untersucht werden, welche Möglichkeiten es gibt, den Beweiswert von Signaturverfahren im Hinblick auf die Präsentation elektronischer Daten und Dokumente zu verbessern und insbesondere die Sicherheitsvermutung des SigG auf die Präsentation auszudehnen. Dabei erfolgt eine Beschränkung auf Maßnahmen zur Verminderung des Mehrdeutigkeitsproblems. Maßnahmen zur Sicherung einer Anwenderinfrastruktur missbräuchlicher Verwendung werden noch nicht näher betrachtet.¹⁴⁰

7.1 Konkretisierung rechtlicher Anforderungen

Die für eine rechtliche Anforderungsanalyse notwendigen konkreten rechtlichen Vorgaben zumindest fehlen zurzeit weitgehend, die wenigen zur Präsentation vorliegenden wurden in Kapitel bereits dargestellt. Vorgaben müssen deshalb auch aus anderen, vor allem grundlegenden rechtlichen Regelungen abgeleitet werden. Für die rechtliche Anforderungsanalyse hat die Projektgruppe Verfassungsverträgliche Technikgestaltung (provet) unter Mitwirkung des Autors die Methode KORA - Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen - entwickelt.¹⁴¹ Diese soll hier dargestellt und angewendet werden.

¹⁴⁰ Sie entsprechen auch eher den allgemeinen Vorkehrungen zum Schutz von IT-Systemen. S. z.B. BSI, IT-Grundschutzhandbuch, 1996, sowie dessen aktuelle Nachauflagen unter <http://www.bsi.de>.

¹⁴¹ Zur Methode siehe Hammer/Pordesch/Roßnagel 1993, Pordesch 1994. Eine Verallgemeinerung zur normativen Anforderungsanalyse findet sich in Hammer 1998.

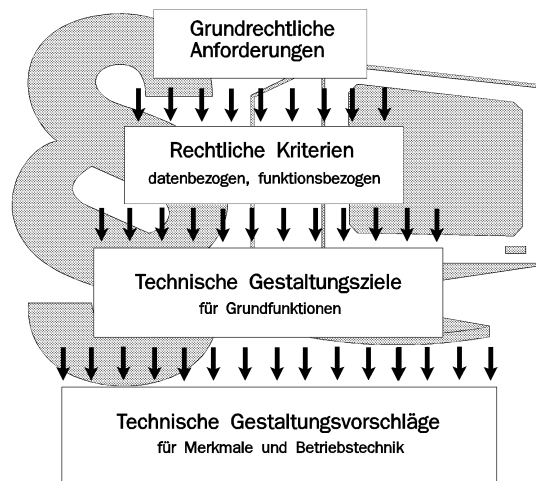


Abbildung 1: Vorgehensweise bei der Konkretisierung rechtlicher Anforderungen

Mit KORA werden rechtliche Normen in vier Schritten zu technischen Gestaltungsmaßnahmen konkretisiert (siehe Abbildung 2). In einem ersten Schritt werden aus rechtlichen Vorgaben des Grundgesetzes und der Rechtsprechung des Bundesverfassungsgerichtes **(grund)rechtliche Anforderungen** abgeleitet. Aus diesen Anforderungen und den Konkretisierungen, die diese im einfachen Gesetzesrecht und der Rechtsprechung bereits erfahren haben, können in einem zweiten Konkretisierungsschritt **rechtliche Kriterien** zur Bewertung und Gestaltung von Informations- und Kommunikationssystemen abgeleitet werden. In einem dritten Zwischenschritt werden dann Grundfunktionen des Techniksystems identifiziert und für diese mit Hilfe der rechtlichen Anforderungen und Kriterien **technische Gestaltungsziele** festgelegt. Schließlich werden in einem vierten Schritt komplexe Merkmale auf die darin enthaltenen Grundfunktionen analysiert, um durch geeignete Kombination der relevanten Gestaltungsziele **technische Gestaltungsmaßnahmen** abzuleiten. Diese stellen dann eine mögliche Realisierungsform rechtlich erforderlicher oder wünschenswerter Maßnahmen dar. Die beiden eher rechtlichen Schritte werden in diesem, die beiden eher technischen im folgenden behandelt.¹⁴²

7.2 Rechtliche Anforderungen

Grundrechtliche Anforderungen an die Gestaltung von Signaturverfahren hat der Autor zusammen mit den Juristen von provet bereits in anderen Publikationen erarbeitet.¹⁴³ Die Grundgedanken sollen hier im Hinblick auf das Präsentationsproblem zusammengestellt werden.

7.2.1 Rechtssicherheit¹⁴⁴

Mit der Entfaltungsfreiheit ist die Freiheit verbunden, in rechtlich verbindlicher Weise durch Austausch von Willenserklärungen Rechte und Pflichten zu begründen. Diese Vertragsfreiheit

¹⁴² Es handelt sich um eine erste Zusammenstellung, die im weiteren Verlauf der Untersuchungen noch überarbeitet werden wird.

¹⁴³ Pordesch/Roßnagel 1994, Idecke / Pordesch / Roßnagel 1999, 131ff.

¹⁴⁴ Pordesch / Roßnagel DuD 1994; 84, Idecke / Pordesch / Roßnagel 1999, 138.

setzt voraus, dass deren Rechtsfolgen auch eingefordert werden können. Dazu muss es ermöglicht werden, über alle rechtlich relevanten Aspekte von Willenserklärungen Beweise zu führen.

Der Einsatz elektronischer - auch multimedialer Dokumente führt zu gravierenden Änderungen. Elektronische Dokumente können auf verschiedene Art und Weise präsentiert und wahrgenommen werden, wobei auch der Empfänger selbst auf die Präsentation Einfluss nehmen kann. Mit der Anforderung Rechtssicherheit wird zum Ausdruck gebracht, dass Unbestimmtheiten zu vermeiden und möglichst Nachvollziehbarkeit und Beweiskraft der Verfahren und Dokumente herzustellen sind.

Rechtssicherheit bedeutet, dass über alle für den jeweiligen Rechtskontext relevanten Aspekte der Präsentation Beweis geführt werden kann. Der Interpretations- und Präsentationswille des Signierers muss eindeutig ermittelbar sein. Gelten Regeln der Zurechnung einer Interpretation, so müssen diese für alle eindeutig ermittelbar sein.

7.2.2 Willenserklärungsfreiheit¹⁴⁵

Aus Grundrechten folgt, dass jeder grundsätzlich das Recht hat, seinen Willen frei zu äußern. Diese Erklärungsfreiheit gilt im Rahmen des Beschäftigungsverhältnisses grundsätzlich auch für Mitarbeiter in Betrieben und Verwaltungen. Jedem steht es grundsätzlich frei, rechtlich verbindliche Erklärungen abzugeben und dadurch rechtliche Bindungen einzugehen oder aufzuheben und Ansprüche zu begründen, geltend zu machen und diese aufzugeben oder zu erfüllen. Zwar können Organisationen aufgrund gesetzlicher Vorschriften, betrieblicher Regelungen zwischen Arbeitgebern und Arbeitnehmern oder durch Weisung des Arbeitgebers bestimmte Formen für Willenserklärungen - wie etwa die Verwendung eines Formulars - vorschreiben (Formgebundenheit). Im Rahmen dieser Regelungen müssen jedoch Form, Inhalte und Umstände einer Willenserklärung frei bestimmbar sein. Insbesondere muss der Nutzer die Möglichkeit haben, alle im Rahmen des Vorgangs zulässigen Willenserklärungen mit den vorhandenen Mitteln klar zum Ausdruck zu bringen.

Der Einsatz elektronischer Verfahren erweitert die prinzipiellen Möglichkeiten seinen zum Ausdruck zu bringen gegenüber papiergebundenen Verfahren ganz erheblich. Verschiedene Medien können kombiniert eingesetzt werden, die unterschiedlichen stilistischen Elemente genutzt werden. Auf der anderen Seite können die Möglichkeiten aber auch sehr stark eingeschränkt werden, etwa indem Bearbeitungsschritte und Eingabemöglichkeiten exakt vorgegeben werden.

In bezug auf die Präsentation signierter Daten bedeutet Willenserklärungsfreiheit, dass der Signierende erkennen und bestimmen können muss, welche Interpretation bzw. Präsentation von Daten er sich zurechnen lassen möchte. Diese Willensbekundung darf durch die Technik (Programme und Dateiformate) nicht zu stark eingeschränkt werden.

¹⁴⁵ Pordesch / Roßnagel DuD 1994; 84.

7.2.3 Fairness¹⁴⁶

In Gerichtsverfahren sind bei der Beweisführung die Interessen aller Beteiligten (der streitenden Parteien) abzuwägen zu berücksichtigen. Eine einseitige Benachteiligung eines Akteurs, des Beweisführers oder Beweisgegners zu Lasten des jeweils anderen muss – auch im Interesse der Wahrheitsfindung – vermieden werden. Ein gerechter Interessenausgleich zwischen den streitenden Parteien soll möglich sein.

Elektronische Dokumente können die Beweismöglichkeiten gegenüber herkömmlichen Verfahren bedeutend erhöhen, etwa wenn in elektronischen Geschäftsprozessen automatisch Beweismittel erzeugt werden. Sie schaffen aber auch zusätzliche Probleme und verstärken vorhandene, wie das der Verfügungsmacht über Beweismittel. Außerdem kann die Schwierigkeit Nachweise zu führen und das Risiko des Prozessverlustes dazu führen, dass die wirtschaftliche schwächere Partei ihre Rechte noch schlechter durchsetzen kann.

Unter der Anforderung der Fairness wird verstanden, dass die Beweismittel so gestaltet werden müssen, dass die am Prozess Beteiligten gleichermaßen in die Lage versetzt werden, die für sie günstigen Tatsachen zu beweisen und nicht durch Zugangshürden, sowie komplexe und teure Beweisführungen gegenüber dem jeweils anderen beeinträchtigt werden.

7.2.4 Informationelle Selbstbestimmung¹⁴⁷

Hinsichtlich der Risiken der elektronischen Datenverarbeitung für die freie Entfaltung und den Schutz der Persönlichkeit ist das Grundrecht aus Art. 2 Abs.1 GG zu einem Recht auf informationelle Selbstbestimmung zu konkretisieren. Dieses "Grundrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen". Beschränkungen dieses Rechts sind nur "im überwiegenden Allgemeininteresse" zulässig und dürfen nur soweit reichen, "als es zum Schutz öffentlicher Interessen unerlässlich ist". Um zu verhindern, dass die "Bürger nicht mehr wissen können, wer was wann bei welcher Gelegenheit über sie weiß, wird der Betroffene mit der Verfügungsbefugnis über 'seine' Daten ausgestattet, muss die Datenverarbeitung bei ihm ihren Ausgang nehmen, ist ihm gegenüber legitimationsbedürftig und muss ihm gegenüber transparent sein.

Mit digitalen Signaturverfahren und in digitalen Signaturen werden auch personenbezogene Daten gespeichert, wie etwa die der Signaturzeit. Um den Beweiswert zu erhöhen, liegt es nahe weitere Daten zu speichern, auch in Bezug auf das ob und wie der Präsentation. Im Extremfall würde die Anwendungsumgebung des Signierers Teil der signierten Daten.

In Bezug auf die Präsentation bedeutet informationelle Selbstbestimmung, nach Lösungen zu suchen, die die Erfassung personenbezogener Daten möglichst vermeiden und die Zustimmung zur Verarbeitung sicherstellen. Dazu ist soweit möglich auf den vollen Nachweis der tatsächlichen Präsentation zu verzichten und statt dessen als Lösungsweg die Zurechenbarkeit einer Präsentation zu verbessern.

¹⁴⁶ Idecke / Pordesch / Roßnagel 1999, 135 (fairer Interessenausgleich) und 137 (Chancengleichheit) jeweils mwN. Man kann dies auch als Teil der Anforderung nach Rechtssicherheit auffassen, die Betonung liegt hier jedoch auf der Chancengleichheit und nicht einem abstrakten Gerechtigkeitsbegriff.

¹⁴⁷ Pordesch / Roßnagel DuD 1994; 84, Hammer / Pordesch / Roßnagel 1993, 56.

7.3 Rechtliche Kriterien

Aus den grundrechtlichen Anforderungen und anderen rechtlichen Überlegungen können im nächsten Schritt der Konkretisierung Kriterien zur Bewertung und Gestaltung von Präsentationssystemen und diesbezüglichen Verfahren abgeleitet werden.

7.3.1 Transparenz¹⁴⁸

Um Rechtssicherheit zu gewährleisten, müssen Signierer und Prüfer erkennen können, welche Bedeutung signierte und zu signierende Daten haben sollen und wie der jeweils andere diese Bedeutungszuordnung vorgenommen hat. Soweit sich die Bedeutung durch eine Präsentation ermitteln lässt, muss auch klar sein, in welcher Weise die Daten zu präsentieren sind (Programme, Parameter,...), um die Bedeutung authentisch zu erschließen. Transparenz ist auch in Bezug auf die gespeicherten Daten gefordert. Der Signierer muss wissen, welche ihn betreffenden Daten in der Signatur und im signierten Dokument gespeichert werden. Schließlich müssen die Funktionen und ihre Bedienung verständlich sein.

7.3.2 Entscheidungsfreiheit¹⁴⁹

Willenserklärungsfreiheit erfordert, dass der Signierer über die Bedeutungszuweisung von Daten entscheiden können muss. Er muss in der Lage sein, über die Vorgabe einer Präsentation die Interpretation der Daten zu bestimmen. Bedeutungszuweisung heißt nicht, dass der das signierte Dokument Prüfende die Daten nur auf eine exakt vorgegebene Art und Weise präsentieren lassen darf. Vielmehr sollte der Prüfer im durch die Tätigkeit vorgegebenen Rahmen auch selbst über die Modalitäten der konkreten Präsentation entscheiden können. Prüfungen sollten vom Benutzer gezielt bezogen auf die von ihm gewünschten Aspekte durchgeführt werden können. Zur Entscheidungsfreiheit gehört auch die Auswahl der einzusetzenden Präsentationsprogramme.

7.3.3 Erforderlichkeit¹⁵⁰

Jede Beeinträchtigung von Grundrechten ist auf das unbedingt erforderliche Mindestmaß zu beschränken, das zur Erfüllung der gesetzlich oder vertraglich geregelten Aufgabe und zur Erreichung des konkreten Zwecks notwendig ist. Sichergestellt werden muss also insbesondere, dass die Willenserklärungsfreiheit und die informationelle Selbstbestimmung nur im unbedingt erforderlichen Maße eingeschränkt wird.

Hinsichtlich personenbezogener Daten korrespondiert das Kriterium mit der Forderung nach Datensparsamkeit.¹⁵¹ Daten, die nicht unbedingt erforderlich sind, sollten erst gar nicht erzeugt, und ansonsten möglichst nicht gespeichert und so wenig wie möglich zugänglich gemacht werden. Funktional bedeutet Erforderlichkeit, dass sicherheitskritische Funktionen nur angeboten werden, wo nicht anders möglich, und Freiheitsgrade des Nutzers bei der Systembedienung nur soweit eingeschränkt werden, wie unbedingt nötig.

¹⁴⁸ Pordesch / Roßnagel DuD 1994; 86 und Hammer / Roßnagel / Pordesch 1993, 71.

¹⁴⁹ Pordesch / Roßnagel DuD 1994; 86 und Hammer / Roßnagel / Pordesch 1993, 72.

¹⁵⁰ Hammer / Roßnagel / Pordesch 1993, 74.

¹⁵¹ Z.B. Köhntopp 1977.

7.3.4 Anpassbarkeit¹⁵²

Rechtssicherheit ist nur dann zu gewährleisten, wenn die Rechtsfolgen erkannt und durchgesetzt werden können, die elektronische Willenserklärungen haben sollen. Die Rechtsfolgen sind vom jeweiligen Anwendungskontext des signierten Dokumentes abhängig. Je nach diesem Kontext sind bestimmte Inhalte und bestimmte Aspekte der Präsentation entscheidend dafür, ob ein Dokument rechtsgültig ist oder nicht und ob daraufhin etwas zu tun oder zu unterlassen ist.

Rechtliche Anpassbarkeit erfordert, dass die Prüfung und mit ihr die Präsentation von Daten an die Regeln rechtlicher Gültigkeit angepaßt werden kann, die in dem Verwendungszusammenhang des signierten Dokumentes gelten. Festlegbar muss jeweils sein, welche medialen Bestandteile (Ton, Video, Text, Bilder usw.) ein Dokument enthalten darf oder muss und wie diese beim Signiervorgang und beim Prüfvorgang zu präsentieren sind. Die rechtlichen Vorgaben im Anwendungsfeld und die möglichen Rechtsfolgen sind dabei entscheidend, die technische Prüfung ist nur Hilfsmittel! Wird ein Prüfprogramm für mehrere Anwendungen genutzt, so muss es verschiedene mögliche rechtliche Gültigkeitsmodelle abbilden können.

7.3.5 Reproduzierbarkeit¹⁵³

Um Rechtssicherheit bei elektronischen Dokumentenaustausch zu gewährleisten, muss es möglich sein, Rechtsfolgen notfalls vor Gericht einzuklagen. Da die Präsentation eines Dokumentes über das Handeln oder Unterlassen von Handlungen entscheidet, was gegebenenfalls rechtlich zu bewerten ist, muss über diese Beweis erhoben werden können. Daraus folgt nicht, dass die Präsentation eines Dokumentes beim Signierenden und beim Prüfenden zu jedem Zeitpunkt absolut identisch sein muss und es ist nicht einmal zu fordern, dass vor jedem Signiervorgang überhaupt eine Präsentation erfolgt. Es muss aber möglich sein eindeutig und ohne jeden Zweifel festzustellen, aus welcher Form der Präsentation der Daten sich die dem Signierenden zuzurechnende Erklärung ergibt.¹⁵⁴

Die Forderung nach Reproduzierbarkeit ist eine "schwächere" (d.h. weniger reglementierende) Forderung als "Eindeutigkeit" durch ein einheitliches Gültigkeitsmodell und Prüfverfahren, die rechtlich gesehen weder notwendig noch geboten ist.

¹⁵² Berger / Pordesch 1999, 229 und Bertsch / Pordesch 1999, 516. Siehe auch Kriterium "Anpassungsfähigkeit" in Hammer / Roßnagel / Pordesch 1993, 80.

¹⁵³ Berger / Pordesch 1999, 229 und Bertsch / Pordesch 1999, 516.

¹⁵⁴ Dies ist nur im zivilrechtlichen Sinne möglich. Im strafrechtlichen Sinne könnte theoretisch die Möglichkeit zur vollständigen Nachstellung des Signiervorgangs gefordert werden, um auch die Absicht beim Signieren nachzuweisen. Eine solche allgemeine Forderung wäre aber nicht sonderlich geeignet – ein technischer Protokollierungsvorgang beweist ja noch nicht die tatsächliche menschliche Wahrnehmung am Bildschirm, man muss ja nicht hinschauen. Außerdem wäre die regelmäßige Erhebung personenbezogener Daten der Benutzung eines Präsentationssystems alleine für das extrem seltene Ereignis eines erleichterten Nachweises einer strafrechtlich relevanten Absicht grob unverhältnismäßig. Die informationelle Selbstbestimmung geht hier vor. Gleichwohl lassen sich Anwendungsfälle denken – wie ein elektronisches Testament in ferner Zukunft –, in denen die tatsächliche Wahrnehmung und mit ihr die Autorisierung nachgewiesen werden sollten.

7.3.6 Bestimmtheit¹⁵⁵

Elektronische Dokumente eröffnen neue Möglichkeiten Sachverhalte auf verschiedene Weise darzustellen (Grafik, Schrift, Bild). Präsentationen können abhängig von den Wünschen des Nutzers generiert werden. Dazu wird zusätzliches Datenmaterial in Bezug auf die Formen, Zeichen, Oberflächen, Farbe, Hintergrundgeräusche etc. benötigt. Damit wird die Präsentation stark von den Eigenschaften der verwendeten Präsentationsmedien abhängen. Es können sich sogar Fragen dahingehend ergeben, was Inhalt des jeweiligen Dokumentes und was nicht.

Bestimmtheit bedeutet, dass trotz aller variablen Möglichkeiten der Präsentation jedem Benutzer klar sein muss, was Gegenstand ist. Bezogen auf Modelle muss klar sein, welchen Wirklichkeitsbereich und welche Beziehungen das Modell abbildet. Dabei muss klar sein, was zum Modell gehört, und was nur schmückendes Beiwerk ist.

7.3.7 Verkehrsfähigkeit

Von entscheidender Bedeutung für die Beweiswürdigung elektronischer Dokumente, Rechtssicherheit und Fairness des Verfahrens, ist, dass diese in das Gerichtsverfahren eingebracht werden können. Elektronische Willenserklärungen, die als Beweismittel verwendet werden sollen, müssen zwischen den Parteien und dem Gericht ausgetauscht werden können. Ungeeignet in dieser Hinsicht sind proprietäre Verfahren, die an ein bestimmtes Programm oder Hardwaresystem gebunden eines Herstellers oder Betreibers sind, weil sie die Beweisführung sehr erschweren. Die signierten Daten müssen bei allen Beteiligten richtig präsentiert werden können. Und die Dokumente müssen bei den Teilnehmern und in den elektronischen Gerichtsakten auch archiviert werden können.

7.3.8 Konsistenz¹⁵⁶

Wenn Informationen über denselben Gegenstand in unterschiedlichen Arten repräsentiert werden als Text, Grafik, Animation, Simulation und darüber hinaus in Überblicks-, Detail-, Schnell-, Gliederungs- oder sonstigen Ansichten - muss klar sein welche Information Geltung beansprucht (Konsistenz¹⁵⁷). Dies ergibt sich direkt aus der Anforderung nach Rechtssicherheit. Sichergestellt sein muss, dass zwischen den verschiedenen Präsentationsformen keine Widersprüche auftreten

Konsistenz erfordert inhaltliche Widerspruchsfreiheit und Übereinstimmung in Bewertungen, nicht jedoch einen identischen Informationsgehalt verschiedener Präsentationen. Bestimmte Informationen können in unterschiedlichen Präsentationen und Sichten durchaus weggelassen werden, wenn dies nicht zu inhaltlicher Widersprüchlichkeit führt.

¹⁵⁵ Idecke / Pordesch / Roßnagel 1999, 143.

¹⁵⁶ Idecke / Pordesch / Roßnagel 1999, 143.

¹⁵⁷ Der im Zusammenhang der Informatik gebrauchte Begriff stellt eine unvollständige Übersetzung des englischen Wortes consistency, das eigentlich Widerspruchsfreiheit bedeutet dar (Schröder 1995, 10); In Schneider (1997, 473) wie folgt definiert: Synonym Widerspruchslosigkeit: Die Aussagenmenge, die keinen logischen Widerspruch beinhaltet, heißt konsistent.

7.3.9 Techniksicherung¹⁵⁸

Unabhängig von der Verbesserung der Zurechenbarkeit einer Präsentation erfordert Rechtssicherheit auch, dass die Gefahren der absichtlichen und unbeabsichtigten Falschpräsentation eingeschränkt werden. Signierer und Prüfer sollten vor Manipulationen und Fehlern eines lokalen Präsentationssystems soweit möglich geschützt werden. Sie müssen sicher sein können, dass eine Präsentation ihrer Vorgabe oder der gewählten Norm entspricht. Der Signierer muss sichergehen können, dass die von ihm ausgewählte und den Daten zuzurechnende Präsentationsform auch korrekt in die zu signierenden Daten bzw. die Signatur übernommen wird.

¹⁵⁸ Pordesch/Roßnagel 1994, 87 und Hammer / Roßnagel / Pordesch 1993, 84.

8. Gestaltungsziele

Die im vorangegangenen Kapitel vorgestellten rechtlich motivierten Kriterien lassen bereits technische Anforderungen erkennen. Nun werden im dritten KORA-Schritt technische Grundfunktionen und Konzepte entwickelt, die die Nachweismöglichkeiten verbessern könnten und für diese werden dann technische Gestaltungsziele abgeleitet. Im Mittelpunkt steht dabei die Konzeptidee einer zurechenbaren Standardpräsentation, die einen Anscheinsbeweis für die Präsentation und Interpretation der Daten ermöglichen soll.

8.1 Datenformate mit Präsentationsvorschriften

8.1.1 Konzeptansatz

Damit der Signierer und der Prüfer (und im Zweifelsfall ein Gericht) aus den signierten Daten dieselbe Willenserklärung ermitteln können, müssen die Präsentationen aller Beteiligten in allen wesentlichen Aspekten übereinstimmen. Möglich wird dies, wenn der Signierer den zu signierenden Daten im Signiervorgang eine Präsentationsvorschrift explizit zuweist. Das Prüfprogramm muss dann in der Lage sein, diese zu erkennen und eine Präsentationskomponente anzusteuern, die diese Vorschrift erfüllt und eine entsprechende Präsentation erzeugt.

Eine Vorschrift zur Interpretation der Daten als Teil der Signatur wird bereits in den Signatur-Interoperabilitässpezifikationen (SigI) vorgeschlagen. Hierbei handelt es sich jedoch bislang um Datenformate, die vorwiegend die syntaktische Datenstruktur festlegen, mit denen aber keine Vorschriften zur Interpretation und Präsentation verknüpft sind. Zumindest ist dies nicht durchgehend, eindeutig und ausreichend der Fall, wie die Risikoanalyse an den Beispielen von Word, ASCII und Coreldraw gezeigt wurde. Anstatt beliebiger Datenformate werden also solche benötigt, zu denen eindeutige Interpretations- und Präsentationsvorschriften festgelegt wurde. In der Evaluierung ist dann u.a. zu prüfen, ob die Beschreibung des Datenformates hinreichend eindeutig ist und ob die Präsentationskomponente wenigstens eine Präsentation entsprechend dieser Vorgaben erzeugen kann (normgerechte Präsentation). Der Signierer und der Prüfer haben dafür Sorge zu tragen, dass sie eine normgerechte Präsentation erzeugen und dazu evaluierte Komponenten einzusetzen. Soweit der Signierer die Verantwortung für die genutzte Anwenderinfrastruktur trägt, sollte er sich eine (im Beweisverfahren an einem Gerichtscomputer erzeugte) normgerechte Präsentation zurechnen lassen, unabhängig davon, ob und wie er sich das Dokument tatsächlich präsentieren ließ. Für ein Gericht ergibt eine so erzeugte Präsentation dann in allen Streitfällen den dem nachgewiesenen Urheber der Erklärung zurechenbaren Inhalt der signierten Daten, also die Willenserklärung.¹⁵⁹

¹⁵⁹ Natürlich nur, insoweit es nicht um die Schuldfrage im engeren Sinne geht also die Frage der Autorisierung. Aber auch in diesen Fällen wäre eine solche Standardpräsentation ein Indiz für den Willen des Signierers und die Signierabsicht, alleine allerdings zum Nachweis oft nicht ausreichend.

8.1.2 Präsentationsbeschreibung

Zu jedem Datenformat ist in einer Formatbeschreibung die syntaktische Datenstruktur zu spezifizieren und um eine Beschreibung der Interpretation sowie um eine Beschreibung der Präsentation zu ergänzen.¹⁶⁰ Eine Präsentationsbeschreibung für Textdokumente muss Festlegungen enthalten hinsichtlich:

- aller Aspekte des Layouts (Anordnung, Zeichenformate,...)
- zur Fenstergröße, sowie anderen äußeren Aspekten der Darstellung, die das wahrnehmbare Layout beeinflussen,
- allen Funktionen (insbesondere zur Navigation / Inhaltserschließung),¹⁶¹

Da letztlich die physikalische Ausgabe die Wahrnehmung bestimmt und nicht die Daten, sind auch hinsichtlich der Ausgabegeräte Mindestanforderungen festzulegen (soweit diese nicht aus den anderen Angaben ableitbar sind). Solche sind bei Bilddokumenten die Auflösung des Bildschirms, die Farbtauglichkeit und die Farbtiefe, soweit diese nicht unmittelbar aus den Layoutangaben ableitbar sind.

Ein Problem liegt in der Definition und dem Nachweis der Vollständigkeit einer Präsentationsbeschreibung. Es ist möglich, zu Elementen einer Präsentation neue Eigenschaften und Ereignisse zu definieren und dennoch konform zur Präsentationsbeschreibung zu bleiben. Man denke an die Präsentation eines alten Word-Dokuments in einem neuen Präsentationssystem, das die Eigenschaft „blinkend“ kennt. Die Eigenschaft „blinkend“ ist neu – in einer alten Präsentationsbeschreibung zu Word würde nicht die Eigenschaftsfestlegung „nicht blinkend“ zu finden sein. Eine Präsentation im neuen System, die den Text standardmäßig blinkend darstellt, könnte also als konform zur Beschreibung angesehen werden. Gleichwohl dürfte eine Willenserklärung durch ständiges Blinken verfälscht werden, zumindest würde die Wahrnehmung empfindlich beeinträchtigt. Prinzipiell ist das Problem der Vollständigkeit unlösbar. Praktisch ist damit so umzugehen, dass ergänzend informelle und interpretationsoffene Anforderungen an die Präsentation formuliert werden (wesentliche Aspekte, Sicherheitsziele und was zu vermeiden ist).

8.1.3 Gestaltungsziele

i) Eindeutigkeit in allen wesentlichen Aspekten

Die Festlegungen müssen umso genauer sein, je mehr die Form der Präsentation Grundlage der Interpretation durch Menschen ist und je weniger die Präsentation durch die Dokumentdaten und die Interpretationsvorschriften vorgegeben ist. Mehr Festlegungen sollten aber nicht unbedingt getroffen werden (Erforderlichkeit).

¹⁶⁰ Es könnte sinnvoll sein, mehrere Präsentationsbeschreibungen zu einem Datenformat festlegen zu können (etwa WORD als Datenformat und Dateiseitenansicht mit bestimmten Drucker und Layout-Seitenansicht als zwei verschiedene Präsentationsformate. Auch eine Kaskadierung von Formaten ist denkbar: Codierung in XML, Datenformat Word und Präsentationsformat Seitenansicht. Dies ändert nichts an dem Ziel, zu jedem Format eine eindeutige Präsentation festzulegen, sondern führt zu einer Aufschlüsselung des Formatkennzeichens in mehrere Teilbestandteile (Codierung, Programmformat, Präsentation), die dann alle Bestandteil der Signatur bzw. des signierten Dokumentes sein müssen.

¹⁶¹ Prinzipiell natürlich allen Funktionen, also auch zur Aufbereitung des Inhalts (Makros, etc.), die aber wegen des Mehrdeutigkeitsrisikos nicht unbedingt in eine Standardpräsentation eingehen sollten.

Die Präsentation für allgemein verwendbare Freitextdokumente muss exakt festgelegt werden, weil anwendungsunabhängig im Voraus nicht beurteilt werden kann, welche Aspekte der Präsentation die Interpretation künftiger Willens- oder Wissenserklärungen beeinflussen und es mithin auf den Nachweis eines jeden Aspekts ankommen kann. Einfache Datenformate, wie ASCII enthalten keine Vorgaben zur Präsentation. Es sind deshalb keine Formate im hier geforderten Sinne. Allerdings können geeignete ASCII-Formate definiert werden, wenn Festlegungen zum Layout, zur Fenstergröße und zu Funktionen getroffen werden. Komplexe Datenformate wie PDF können detaillierte Vorgaben enthalten, so dass sie nicht festgelegt werden müssen. Aber auch bei solchen Formaten müssen noch Teile ergänzt werden, wie z.B. Defaulteinstellungen für die Fenstergröße und die zur Verfügung zu stellenden Funktionen.

Bei formatierten Daten ist die Interpretation von der Form der Präsentation größtenteils unabhängig. Die Präsentation muss nicht in allen Aspekten nachgewiesen und folgedessen auch nicht vorgegeben werden. Vielmehr reicht es hier aus, allgemeine Anforderungen hinsichtlich der Zugänglichkeit und Wahrnehmbarkeit zu formulieren, die jede normgerechte Präsentation erfüllen muss. Ein Zeitstempel muss nur geeignet lesbar gemacht werden können, es kommt aber nicht auf den verwendeten Zeichensatz an, weil in diesem kein Wille zum Ausdruck kommen soll.¹⁶² In einer Präsentationsbeschreibung sind deshalb lediglich allgemeine Anforderungen zur Codierung, zur Zugänglichkeit und Wahrnehmbarkeit der Inhalte festzulegen, nicht aber z.B. der Zeichensatz.

ii) Vollständigkeit hinsichtlich der signierten Daten

In einer Präsentation müssen alle Teile der signierten Daten zugänglich sein (Transparenz). Wahrnehmbar gemacht werden müssen also auch in Textdokumenten enthaltene Dokumenteigenschaften (Verfasser, Seriennummer,...) und Programmcode. Der Nutzer darf nicht gezwungen werden, Dokumentteile „blind“ zu signieren, mit denen er aber später – etwa über ein Sachverständigengutachten im Gerichtsprozeß – konfrontiert wird.

Um die Probleme der Mehrdeutigkeit zu verringern, wäre es ein Weg, von signierten Dokumenten im Präsentationssystem diejenigen Teile nicht zu präsentieren, die Probleme bereiten können. So werden ja auch beim Word-Viewer in das Dokument eingebettete Makros und ältere Versionen ignoriert. Diese Methode der Ausblendung und Definition einer normgerechten Präsentation als eines reduzierten rechtsverbindlichen Views hätte den Vorteil, dass existierende Dokumentenstandards und Dateiformate nicht geändert werden müssen. Dies widerspricht jedoch dem Ziel der Vollständigkeit.

Eine Lösung besteht darin, Signaturen so in die Dokumente einzubetten, dass potentiell Mehrdeutigkeiten produzierende kritische Bestandteile erst gar nicht mitsigniert werden. Demzufolge wäre also, um im Beispiel zu bleiben, keine Word-Datei zu signieren, sondern die Signatur in Word so einzubetten, dass Makros nicht mitsigniert werden. Ein anderer Weg besteht darin, vor dem Signiervorgang die Daten über einen Konverter auf ein anderes reduziertes Format umzusetzen und nur den so konvertierten Bitstring dann zu signieren.¹⁶³

¹⁶² Freilich *kann* darin ein Wille zum Ausdruck kommen, etwa wenn der Signierer mit der gegebenen Möglichkeit etwas zum Ausdruck bringen will. So kann man sich vorstellen, dass ein Signierer mit der Wahl des Zeichensatzes "MS Serif" verdeckt zum Ausdruck bringen möchte, dass er zur Unterzeichnung einer elektronischen Überweisung gezwungen wurde. Nur erscheint es unsinnig, einen verdeckten Kanal für solche Informationen einzuplanen, besonders an so einer Stelle.

¹⁶³ Darauf wird später näher eingegangen, S.116.

iii) **Abgeschlossenheit hinsichtlich der signierten Daten**

Der Nutzer muss klar erkennen können, welche Elemente der Präsentation zu den signierten Daten gehören und welche nicht (Transparenz). Am besten erscheint eine Lösung, die externe Bezüge verzichtet, also möglichst sogar die Zeichensätze in das Dokument einbettet. Das wird nicht immer möglich sein und kann dann durch einen eindeutigen Verweis auf den einzusetzenden Zeichensatz in der Präsentationsbeschreibung ersetzt werden. Eine Präsentationskomponente sollte aber keinesfalls Links zu externen nicht signierten Objekten automatisch auflösen und das Objekt direkt innerhalb des Kontextes der präsentierten Daten anzeigen (etwa im selben Fenster). Auch ein manuelles Auflösen der Verknüpfung– etwa durch Anklicken und Start eines zusätzlichen Fensters ist problematisch, weil der Laie den Überblick über das, was signierte Willenserklärung ist und was nicht, verliert. Man sollte auf solchen „Komfort“ innerhalb einer normgerechten Präsentation verzichten, es reicht ihn im Anwendungsprogramm verfügbar zu haben, mit dem die Dokumente erstellt werden.

iv) **Einfache Formate (Vermeidung von Komplexität)**

Heutige komplexe Dateiformate der gebräuchlichen Bürosoftware eignen sich nur bedingt für die Präsentation digital signierter Daten. Sie sind zu mächtig, die Dokumentstrukturen zu komplex. Dies erfordert zum einen komplexe Präsentationskomponenten und Ausgabegeräte, bei denen der Signierer nicht davon ausgehen kann, ob sie auf der Seite des Prüfers vorhanden sind. Zudem enthalten sie Bestandteile wie aktualisierbare Felder und Makros, die für die Abgabe von Willenserklärungen überflüssig sind, aber in rechtsverbindlichen Dokumenten zu Mehrdeutigkeiten führen können.

In Einschränkung zu üblichen komplexen Dokumentformaten sind deshalb einfachere, inhaltlich klare auf die Kenntnisaufnahme und den Signaturvorgang ausgerichtete Datenformate zu definieren. Beispiele für vorstellbare Formate sind:

- ASCII, 20 Zeichen pro Zeile und maximal 10 Zeilen auf 5 Zoll-Fenster: Ein solches Primitivformat (mit der Festlegung eines bestimmten einfachen Zeichensatzes und Funktionen zum fensterbezogenen Vor- und Zurückblättern) kann auf praktisch jedem Bildschirm, sogar dem eines tragbaren Telefongerätes, präsentiert werden, ohne dass Funktionen für das Blättern angeboten werden müssen. Es eignet sich gleichwohl für viele einfache standardisierte Anwendungen, wie etwa Medikamentierungen im Krankenhaus, Abhebungen am Geldautomat, Überweisungen etc..
- HTML, ohne Frames, Java-Applets, Links und Bilder mit direkter Formatierung und 3 Standardschriftarten, DIN A5-Seitenfestlegung und Begrenzung auf 5 Seiten. Für electronic Mail am PC und die meisten Vertragsabschlüsse im Internet dürfte dieses an fast allen in Betrieb befindlichen PCs darstellbare Format ausreichen.

Es ist möglich, für komplexere Dokumentformate (etwa Websites mit Java, für Word) Konverter zu schreiben, die die Dokumente vor dem Signiervorgang auf einfachere, für viele Ausgabegeräte und Plattformen geeignete Präsentationsformate umsetzen. Dies schränkt die Gestaltungsvielfalt etwa von Websites nicht ein, reduziert aber den zurechenbaren Willenserklärungsakt auf ein notwendiges per Anscheinsbeweis nachweisbares Maß.

v) Universelle Formate

Müssen Datenformate wie oben gefordert mit Interpretations- und Präsentationsvorschriften versehen werden, so kann dies leicht zu einer unübersichtlichen Fülle von Formaten führen. So kann man sich zu ASCII viele sinnvolle Festlegungen hinsichtlich des Layouts für die unterschiedlichsten Anwendungskontexte denken. Für alle diese Formate müssten dann Präsentationskomponenten erstellt und evaluiert werden, was sehr aufwendig wäre. Deshalb kommt es darauf an geeignete universelle Datenformate zu finden, in denen die Präsentationsvorschriften in den Daten enthalten sind. Vorstellbar wäre ein ASCII-Format, das zu den unformatierten Inhaltsdaten ergänzend Daten zur Präsentation enthalten, die in codierter Form die Vorgaben zum Layout, zur Fenstergröße und den Navigationsfunktionen enthalten. Ein Kandidat für ein geeignetes universelles Datenformat ist XML, dessen Eignung im Hinblick auf die hier formulierten Ziele aber noch eingehend zu untersuchen ist.

vi) Zusätzliche Präsentations- aber keine Bearbeitungsfunktionen

Wahrnehmungsmöglichkeiten und –gewohnheiten von Menschen unterscheiden sich erheblich. Eine Präsentationskomponente sollte dem Nutzer deshalb die Möglichkeit bieten, eine seinen Wünschen entsprechende Präsentation zu wählen (Anpassbarkeit, Entscheidungsfreiheit). Wichtig ist zumindest die Anpassung auf die Wahrnehmungsmöglichkeiten der Person und eventuelle Handicaps (Zoomfunktionen für eingeschränktes Sehvermögen).

Um Fehlbedienungen auszuschließen und die Evaluierung möglichst einfach zu halten sollte mit zusätzlichen Funktionen aber sparsam umgegangen werden. Problematisch und in der Regel auch unnötig sind Bearbeitungsfunktionen. Die Bearbeitung kann im Anwendungsprogramm erfolgen.

vii) Anwendungsvorgaben

Das zur Dokumenterstellung verwendete Anwendungsprogramm des Signierers sollte eine Präsentation vorgeben können, die vor dem Signiervorgang gewählt wird, um dem Signierenden die zu signierende Erklärung noch einmal abschließend zu vergegenwärtigen. Die Festlegung der zu wählenden Präsentation sollte anhand des jeweiligen Dokumentes oder auch Vorgangs und der geltenden Rechtsregeln erfolgen können (Anpassbarkeit). Es sollte auch vorgegeben werden können, ob die Präsentation über eine Präsentationskomponente im Rahmen des Signiervorgangs erfolgen muss.¹⁶⁴

8.2 Standardpräsentation

8.2.1 Grundfunktion

Unter Berücksichtigung der Kriterien Erforderlichkeit und Entscheidungsfreiheit sind die Festlegungen der Präsentation zu minimieren, so dass es mehrere beschreibungskonforme (äquivalente) Präsentationen geben kann.

¹⁶⁴ Ein erster Vorschlag für eine Systemarchitektur, die solche Vorgaben beim Prüfprozeß ermöglicht, findet sich in Por-desch / Berger 1999.

Ein solches Vorgehen hat jedoch auch Nachteile. Die wesentlichen Aspekte der Präsentation, die in allen Präsentationen übereinstimmen müssen, sind genau zu identifizieren, die Präsentationsvorschriften müssen allgemeingültig gefasst werden. Dies ist möglich, wenn der Anwendungskontext und die dort geltenden rechtlichen Regeln bekannt sind, also z.B. bei Signaturobjekten wie Zertifikaten und Zeitstempeln.

Praktikabler erscheint es, auch in Fällen, in denen eine bestimmte exakte festgelegte Präsentation nicht notwendig erscheint, trotzdem eine solche exakt festzulegen (Standardpräsentation). Denn dann können Präsentationskomponenten ohne eine anwendungsbezogene Analyse von Wesentlichkeitsaspekten anwendungsunabhängig evaluiert werden und die rechtlichen Beweiserleichterungen könnten eher zur Geltung kommen.

Eine Standardpräsentation ist aber auch aus anderen Gründen sinnvoll. Selbst wenn verschiedene Präsentationen vom Anwendungskontext her und rechtlich gesehen in allen wesentlichen Aspekten übereinstimmen, kann insbesondere der Computer-Laie durch unterschiedliche Präsentationen verwirrt werden. Schon wenn die Namensangabe in einem Zertifikat einmal mit dem Font „Times“ und ein anderes mal mit dem Font „Kids“ dargestellt wird, kann dies von unerfahrenen Nutzern auch unterschiedlich interpretiert werden (bezüglich der Seriosität dieser Angabe). Eine einfache Standardpräsentation, die am kleinsten gemeinsamen Nenner möglicher Systemkonfigurationen orientiert ist, und deshalb plattform- und endgeräteunabhängig gleich verläuft („aussieht“) ist deshalb zumindest als ergänzende Funktion sinnvoll.

8.2.2 Gestaltungsziele

Zusätzliche Funktionen müssen eindeutig von der Standardpräsentation unterschieden werden können, damit keine Unklarheit aufkommen kann. Möglich ist dies z.B. durch farbliche Kennzeichnung, separate Menüs oder dadurch, dass zusätzliche Funktionen nur im Menü erscheinen und die Funktionen der Standardpräsentation nur im Dokumentfenster (Transparenz).

8.3 Kontrolle der physischen Präsentation

8.3.1 Grundfunktion

i) Automatischer Gerätecheck

Aus den Festlegungen zu den einzelnen Formaten sollte die Präsentationskomponente ableiten können, welche Mindestanforderungen an die Eigenschaften des Ausgabemediums ein zu präsentierendes Dokument hat. Die Präsentationskomponente sollte dann auch sicherstellen, dass das Computersystem, auf dem seine Teilkomponenten laufen, über die für das jeweilige Dokument erforderlichen Ausgabegerät mit genügender Ausgabequalität verfügt und dass diese zum Zeitpunkt der Präsentation auch richtig funktionieren. Solche Informationen können bei Windows-Systemen z.B. aus der Registry entnommen werden.

Soweit dies nicht automatisch möglich ist, muss die automatische Kontrolle durch eine interaktive Kontrolle mit dem Benutzer ergänzt werden.

ii) Interaktive Nutzer-Kontrolle

Software ist in jedem Falle nur eingeschränkt in der Lage, das tatsächliche Vorhandensein und die Einstellungen der Hardware zu überprüfen. Ob ein geeigneter Bildschirm konfiguriert ist, lässt sich noch automatisch überprüfen, ob er funktioniert, ob die Regler richtig eingestellt sind und ob Blendeffekte vorliegen nicht. Deshalb ist ergänzend immer ein interaktiver Testmodus erforderlich. Hierzu können durch das Präsentationssystem Testpräsentationen (Töne, Farbbilder, Druckseiten) erzeugt werden, anhand derer der Nutzer die Funktionsfähigkeit des Präsentationssystems prüfen und z.B. mit einer gedruckten Vorlage vergleichen kann. Das zeitabhängige Verhalten des genutzten Systems lässt sich dadurch testen, dass der Nutzer den Hinweis erhält, dass nach Drücken eines Buttons in maximal einer bestimmten Zeitspanne eine bestimmte Reaktion des Systems erfolgen sollte (etwa: "Nach Drücken des nebenstehenden Buttons muss in einer maximal 1 Sekunde das bekannte Testbild vollständig aufgebaut sein").

Hier stellt sich die Frage, wie aufwendig ein Interaktionstest sein muss und wann er durchzuführen ist. Handelt es sich immer wieder um dasselbe Dokument und das der Nutzer kennt und ändert sich die Konfiguration der Anwenderinfrastruktur selten, so ist einmaliger Test zu Beginn der Installation oder Neuansmeldung eines Nutzers ausreichend. Der Nutzer kennt das ihn erwartende Dokument und wird fehlerhafte Einstellungen der Endgeräte auch im Gebrauch erkennen. Kann sich die Art der Dokumente jedoch stark ändern und weiß der Nutzer nicht, was ihn erwartet, so ist ein aufwendigerer Test erforderlich, der auch häufiger – im Extremfall bei jedem Signiervorgang - durchzuführen ist.

iii) Präsentations- und Rezeptionsüberwachung

Soweit der Benutzer über Funktionen auf die Präsentation Einfluß nehmen kann, sollte eine Komponente des Präsentationssystems überwachen, ob der Benutzer alle für die Wahrnehmung des Inhaltes erforderlichen Interaktionen durchgeführt hat. Eine Präsentationsüberwachung hat insbesondere sicherzustellen, dass alle Dokumententeile tatsächlich präsentiert wurden. Der Benutzer ist bei einer unzureichenden Präsentation zumindest zu warnen, es sollte aber auch die Möglichkeit gegeben sein, die Funktionen zum Signieren und Prüfen der Signatur zu deaktivieren, bis eine vollständige Wahrnehmung erfolgt ist.

8.3.2 Gestaltungsziele**i) Freiwilligkeit**

Unter dem Kriterium der Entscheidungsfreiheit sollte die Nutzung der Kontrollmittel möglichst freiwillig erfolgen. Insbesondere ist ein Zwang zur Präsentation und zu einer bestimmten Präsentation (etwa vollständige Kenntnisnahme) zu vermeiden, wo dies im Anwendungskontext nicht unbedingt erforderlich ist. Systemtechnisch gesehen ist also konfigurierbar zu halten, ob die erfolgreiche Kontrolle Vorbedingung für die Auslösung eines Signiervorgangs ist.

ii) Einbettung in den Signiervorgang

Die Akzeptanz einer Selbstkontrolle dürfte eingeschränkt sein, wenn zusätzlicher Interaktionsaufwand damit verbunden ist. Deshalb ist nach Möglichkeiten zu suchen, die Prüfung mit

dem Signiervorgang zu verbinden wird und so erfolgen zu lassen, dass der Benutzer das Vorhandensein und die richtige Einstellung von Ausgabegeräten durch seine Reaktionen implizit bestätigt. So läßt sich die ausreichende Größe eines Bildschirms für das Anwendungsfenster dadurch prüfen, dass zunächst ein Button in der unteren rechten Ecke des Dokumentes den Signiervorgang startet und dann später im oberen linken Eck dann aber ein Fenster eingeblendet wird, um den Vorgang zu bestätigen.

Wenn ein Präsentationssystem vor erfolgreicher Bestätigung von Selbsttestfunktionen die Signierfunktion erst gar nicht aktiviert und über das Formatkennzeichen vermutet werden kann, dass ein solches System eingesetzt wurde, dann kann auch auf tatsächliche Funktionsfähigkeit des Endgerätes zum Signierzeitpunkt zurückgeschlossen werden!

8.4 Nachweis der Sicherheit der Anwenderinfrastruktur

8.4.1 Ansatz

Eine bestimmte Präsentation kann einem Signierer nur dann als Willenserklärung zugerechnet werden, wenn die Anwenderinfrastruktur in seine Risikosphäre fällt, wenn er selbst Maßnahmen zum Ausschluß und zum Erkennen von Fehlern und Manipulationen ergreifen kann. Ist dies nicht der Fall, so kann der Signierer stets den Einwand der Falschpräsentation vorbringen: Ein Fehler oder eine Manipulation der Präsentationskomponente habe vorgelegen, es sei z.B. falsches Kennzeichen für das Datenformat eingetragen worden oder eine nicht evaluierte fehlerhafte Präsentationskomponente sei zum Einsatz gekommen. Eine aus der Formatkennzeichnung in der Signatur ableitbare normgerechte Präsentation habe er also ohne sein Verschulden nicht erzeugen können. Wie bereits geschildert wird dieser Einwand im Rahmen der freien Beweiswürdigung insbesondere dann zu gewichten sein, wenn der Beweisführer zugleich Betreiber der Anwenderinfrastruktur ist, auf der die Präsentationskomponente zum Signierzeitpunkt lief.¹⁶⁵ Ist der Signierer Betreiber gewesen, so kann hingegen davon ausgegangen werden, dass er die erforderlichen Sicherheitsvorkehrungen traf.¹⁶⁶ Es ist also der Nachweis erforderlich, wer die Anwenderinfrastruktur betrieb, auf der das Dokument präsentiert wurde.

8.4.2 Grundfunktionen

i) Bestätigung der Systemherrschaft des Signierers

Für den vereinfachten Nachweis der Präsentation ist es lediglich erforderlich, nachweisen zu können, dass der Signierer eine von ihm selbst betriebene Anwenderinfrastruktur benutzt hat bzw. dass dies nicht der Fall war. Eine Indiztatsache hierfür wäre es, wenn der Nutzer selbst dies in mit seiner Signatur bestätigen würde –in einer Form, die den Nachweis der Urheberschaft einer solchen Bestätigung zweifelsfrei ermöglicht.

¹⁶⁵ Ist ein Dritter Betreiber, so wird es eher auf den Nachweis der Sicherheitsvorkehrungen ankommen, aber es können geringere Anforderungen an den Nachweis gestellt werden.

¹⁶⁶ Rechtlich setzt dies alles aber entsprechende Erklärungen voraus, sich Willenserklärungen unter den genannten Bedingungen auch zuordnen lassen zu wollen. Siehe hierzu Ondarza 1999.

Eine einfache und zugleich sichere Lösung besteht in der Verwendung **Unterschiedlicher Signierschlüssel**. Der Signierer könnte verschiedene Signierschlüssel für das Signieren in eigener (potentiell sicherer) und in fremder (potentiell unsicherer) Signierumgebung verwenden. Die Verwendung des Signierschlüssels kann vom Betreiber der Anwenderinfrastruktur nicht manipuliert werden, soweit der Signiervorgang selbst in einer sicheren Komponente erfolgt (z.B. Chipkarte oder verkapseltem Lesegerät). Der Signierer muss dann zuvor an geeigneter Stelle, z.B. der Zertifizierungsstelle, nachweisbar eine Willenserklärung abgeben, welchen Schlüssel er wie zu nutzen gedenkt.

Mehr Nachweismöglichkeiten eröffnet eine **Gerätesignatur**. Die Anwenderinfrastruktur signiert zeitlich vor dem Signierer selbsttätig die zu signierenden Daten und ihre Signatur wird Teil des vom Erklärer signierten Dokumentes. Dies ist zuverlässiger für den Nachweis der tatsächlichen Präsentation – der Signierer selbst kann dann nicht einfach eine falsche Bestätigung ausstellen, es liegt nicht in seiner Hand. Es ist aber auch eine aufwendigere Lösung, weil dann auch die Signaturkomponenten für die Geräte und ihre Zurodnung zu bestimmten Geräten und Betreibern registriert werden muß. Für öffentlich betriebene Systeme erscheint eine solche Lösung aber durchaus angemessen.

ii) Sichere Systeme

Auf die verschiedenen Möglichkeiten zur Erhöhung der Systemsicherheit bei Anwenderinfrastrukturen (sichere Betriebssysteme, Firewalls, Programmverifikation etc.) soll hier nicht eingegangen werden. Die Frage ist, wie im Gerichtsverfahren der Nachweis zu verbessern ist, dass diese zum Signierzeitpunkt wirksam waren.

Denkbar ist ein solcher Nachweis bei nicht frei programmierbaren und konfigurierbaren Systemen, der Funktion fest vorgegeben und im Betrieb nicht änderbar ist. Solche Systeme (wie der Bankautomat, der elektronische Fahrkartenschalter, ...) könnten nach einer Revision durch eine autorisierte Stelle überprüft und dann in geeigneter Weise verplombt werden. Kann der Nutzer die Plombe überprüfen, tut dies aber nicht, kann ihm die Verantwortung für eventuelle Missbräuche oder Fehler zugewiesen werden. Die Indiztatsache der ordnungsgemäßen Funktion des Systems gilt – jedenfalls bis zum Beweis des Gegenteils – als bewiesen.

Bei Systemen, die im Betrieb frei programmierbar sind, ist dieser Nachweis im Nachhinein kaum möglich. Der Betreiber hat jederzeit die Möglichkeit, die Software komplett auszutauschen und später wieder den ordnungsgemäßen Zustand herzustellen (primitiv z.B. über den Austausch der Festplatte). Auch regelmäßige Kontrollen helfen wenig. Ist der Betreiber der Anwenderinfrastruktur der Beweisführer und der Signierer Beweisgegner, so muss er mit Hilfe anderer Beweismittel (etwa Zeugen) versuchen nachzuweisen, dass die Anwenderinfrastruktur sicher war, wenn dies umstritten ist. Dieser Nachweis kann sehr schwer sein und vielleicht auch misslingen, aber jede andere Lösung würde den Signierer benachteiligen und würde der Anforderung nach Fairness grob zuwiderlaufen.

Werden die freiprogrammierbaren Systeme nicht vom Beweisführer sondern einem Dritten betrieben, der kein Nutznießer einer möglichen Manipulation ist, ist eine andere Beweislastverteilung möglich. Hier besteht allenfalls das Risiko der Schlamperei und des Vertuschens von Fehlern durch den Betreiber, weil er Interesse am Betrieb hat. In einem solchen

Fall könnten regelmäßige Revisionen der Anwenderinfrastruktur durch eine autorisierte Stelle ein sicheres Indiz dafür sein, dass keine Manipulation erfolgt ist.¹⁶⁷

8.4.3 Gestaltungsziele

i) Einfache Lösungen

Wenn die Kennzeichnung der Systemherrschaft einen so großen Stellenwert für die Beweisführung erhält, müssen Benutzerfehler auf jeden Fall vermieden werden. Vorstellbar ist der Einsatz unterschiedlicher Chipkarten und einer Kenntlichmachung des Zwecks (z.B. "Nur zur Nutzung in selbstkontrollierter Umgebung") sichtbar auf der Chipkarte. Oder man kann eine Chipkarte mit zwei Chips und einer roten und einer grünen Seite einsetzen: Grüne Seite in den Kartenleser einschieben nur zu Hause, rote überall sonst.

ii) Erkennen der Zuordnung

Der Kooperationspartner muss die Zuordnung der Risikosphäre erkennen können, um entscheiden zu können, ob er das Risiko erschwerter Beweisführung im Falle fremder Infrastruktur eingehen und die Willenserklärung akzeptieren möchte. Am besten wäre deshalb ein Attribut im Schlüsselzertifikat dafür vorzusehen, so dass die Zuordnung bei der Signaturprüfung erkennbar ist.

iii) Nutzerkontrollierte Signierumgebungen

Die Verwendung selbstkontrollierter Signierumgebungen ermöglicht also indirekt und mit Hilfe der anderen genannten Maßnahmen den Nachweis einer zurechenbaren Präsentation. Bislang ist allerdings nur ein Teil der Transaktionen in der elektronischen Welt an einem nutzerkontrollierten System möglich. Am Arbeitsplatz nutzt man das System des Arbeitgebers zum Signieren, beim Außendienstbesuch das des Vertragspartners, in der Bankfiliale das der Bank, im Cafe das öffentliche Internetterminal eines Internetproviders. Eine notwendige Forderung ist deshalb die Entwicklung und der verstärkte Einsatz nutzerkontrollierter mobiler Endgeräte.¹⁶⁸

8.5 Hinweise auf die tatsächliche Präsentation

8.5.1 Ansatz

Neben der Verbesserung des Nachweises einer zurechenbaren Präsentation ist auch darüber nachzudenken, wie der Nachweis der tatsächlichen Präsentation erleichtert werden könnte. Dazu sind die genutzten Hard- und Softwarekomponenten zu identifizieren, um eine Präsentation später wiederholen oder das Originalsystem durch Sachverständige untersuchen lassen zu können.

¹⁶⁷ Zu den technischen Möglichkeiten und Verfahrensweisen der Revision am Beispiel von ISDN-Telekommunikationsanlagen siehe Pordesch / Hammer / Roßnagel 1991.

¹⁶⁸ Siehe hierzu die Entwicklung eines Prototypen eines nutzerkontrollierten Signiergerätes auf einem Newton PDA im Gesundheitswesen: Grimm / Gattung / Pordesch / Schneider 1997 und Gattung / Pordesch / Schneider 1998, sowie erste Erfahrungen im Rahmen einer Simulationsstudie im Gesundheitswesen in Pordesch 1999.

In den Signaturinteroperabilitätsspezifikationen ist der Verweis auf das Nutzdatenformat als Datenfeld vorgesehen, wobei diese Eintragung obligatorisch erfolgen soll.¹⁶⁹ Diese Angabe lässt bisher jedoch allenfalls einen Rückschluss auf eine Klasse möglicher Programme zu.

8.5.2 Grundfunktionen

i) Erkennung der Präsentationsprogramme

Neben dem Datenformat wären als Teil der Signatur ein Kennzeichen für das Präsentationsprogramm vorzusehen, das vom Signierer verwendet wurde. Probleme, die sich aus der Verwendung nicht evaluierter Präsentationsprogramme ergeben oder die Behauptung von trotz Evaluierung vorhandenen Fehlern liessen sich so besser aufklären.

Hier ist zunächst an ein Kennzeichen zu denken, das auf das genutzte Programm und dessen Version verweist. In einzelnen Anwendungsfällen, insbesondere bei öffentlich zur Nutzung angebotenen Systemen, könnte eine individuelle Programmkennzeichnung (der Installation) von Vorteil sein, um nachprüfen zu können, ob bei einem Präsentationssystem noch das zum Signieren verwendete Programm installiert ist – um dessen Konfiguration überprüfen zu können.¹⁷⁰ Da auch das Betriebssystem die Präsentation wesentlich beeinflussen kann, könnte schließlich ein Feld für die entsprechende Eintragung vorgesehen werden.

Kennzeichen für Programme sollten für den Signierer und den Prüfer lesbar sein. Als Programmkennzeichen sollten deshalb nicht nur Objekt-Identifiern (OIDs, sofern vorhanden) verwendet werden, sondern eine von Menschen lesbare und interpretierbare Angabe von Programmnamen.

ii) Hardwareerkennung

Neben den Programmen ist auch die verwendete Hardware wichtig für die Rekonstruktion der Präsentation.

Zu denken ist zunächst an Typkennungen der verwendeten Hardware, insbesondere die Ausgabegeräte. Solche könnten bei WINDOWS-basierten Systemen aus der Registry entnommen werden (z.B. verwendeter Bildschirm).

Neben einer Typkennung ist jedoch auch an eine individuelle Erkennung der verwendeten Anwenderinfrastruktur sinnvoll. Eine eindeutige individuelle Kennung des verwendeten Rechners könnte die Aufklärung behaupteter oder tatsächlicher Falschpräsentationen wesentlich erleichtern, was insbesondere bei öffentlich genutzten Systemen erforderlich ist (öffentliche Bankterminals, Internetterminals). Die signierten Daten enthielten dann eine Art Fingerabdruck des Rechners, der auch im Nachhinein noch identifiziert und auf mögliche Fehler, Manipulationen oder äußerliche Störeinflüsse untersucht werden kann.¹⁷¹

Eine Kennung in der Signatur kann durch den Signierer oder den Betreiber der zum Signieren verwendeten Anwenderinfrastruktur falsch eingetragen werden, man kann z.B. Kennungen aus anderen Dokumenten in ein neues übernehmen. Eine solche Kennung kann daher nur als

¹⁶⁹ Das Feld selbst ist aber nicht obligatorisch.

¹⁷⁰ Entsprechend der GUID, die in Microsoft-office-Dokumenten teilweise abgespeichert wird (Persson/Siering 1999).

¹⁷¹ Cornelius DuD 1999, 532 nennt die Prozessor-Seriennummer als möglichen Bestandteil signierter Daten

Indiz insbesondere zur Aufklärung von Fehlern verwendet werden. Eine verbesserte Nachweismöglichkeit wäre bereits oben gefordert eine Gerätesignatur durch eine in das Signiersystem fest eingebaute Hardwarekomponente, die zusätzlich zu der des Nutzers zu einem Dokument erzeugt würde.

8.5.3 Gestaltungsziele

i) Zustimmung des Nutzers

Um die Transparenz und Entscheidungsfreiheit über die Preisgabe personenbezogener Daten zu wahren, sollte die Eintragung nicht automatisch und ohne Einflussmöglichkeit des Signierers erfolgen, sondern nur mit dessen ausdrücklichem Einverständnis (Entscheidungsfreiheit). Der Nutzer muss die Eintragungen erkennen können. Er muss aber über Einstellmenüs oder Rückfragen entscheiden können, ob er die Daten in die Signatur übernehmen lassen möchte. Wo dies aus Sicherheitsgründen nicht möglich sein soll und rechtlich bzw. vertraglich geregelt ist, muss zumindest die Möglichkeit bestehen, den Signiervorgang abubrechen. Defaultoptionen müssen die datensparsame Varianten sein.

ii) Unverkettbarkeit der Daten

Individuelle Gerätekennungen in Dokumenten bergen die Gefahr in sich, dass ein Bewegungsprofil des Signierers aus den von ihm signierten Daten erstellt werden kann. Deshalb ist möglichst zu verhindern, dass aus den Gerätekennungen auf die verwendeten Geräte zurückgeschlossen werden kann, zugleich dabei aber die Nachweiseigenschaft zu erhalten (Erforderlichkeit).

Eine datensparsame Lösung für Gerätekennungen könnte darin bestehen, statt der Kennung einen Hashwert aus dieser und dokumentspezifischen Daten, etwa dem Hashwert des Dokumentes, in die Signatur zu übernehmen. Bei einer solchen Lösung könnte nachgewiesen werden, dass die Signatur an einem bestimmten Gerät erfolgt ist, wenn das Gerät und seine Hardwarekennung bekannt ist. Die Hardwarekennung könnte jedoch aus dem Hashwert nicht direkt abgeleitet werden, der Empfänger signierter Dokumente könnte die verwendete Anwenderinfrastruktur nicht alleine aus der Hardwarekennung ableiten.

8.6 Systemarchitektur

8.6.1 Ansatz

Die Realisierung der genannten Gestaltungsziele erfordert eine passende Systemarchitektur. Diese soll nun noch grob skizziert werden.

In der Diskussion um die Umsetzung des Signaturgesetzes wird die "Darstellungskomponente" vielfach als Teil des Anwendungssystems angesehen, zumindest wird diesbezüglich keine klare Unterscheidung getroffen. Wären Präsentationskomponenten Teil des Anwendungssystems, so müssten nachteilige Wechselwirkungen aller anderen Komponenten des Anwendungssystems auf diese Teilkomponente bedacht und ausgeschlossen werden. Faktisch müsste dann das gesamte Programm evaluiert werden, als Voraussetzung für eine Sicherheitsvermu-

tung und die damit verbundene Beweiserleichterungen wäre. Programme wie Microsoft Word können aber wohl niemals mit einer brauchbaren Sicherheitsstufe evaluiert werden.

Die Präsentationskomponente mit den genannten Funktionen ist also als möglichst einfaches, separates System zu konstruieren.

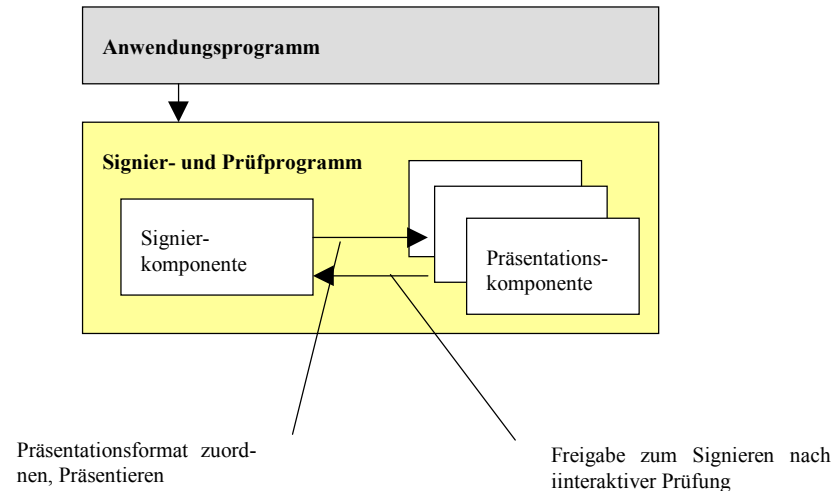


Abbildung 1: Systemarchitektur, funktionale Einbindung von Präsentationskomponenten

8.6.2 Ideallösung

Der einfachere Weg besteht darin, Präsentationskomponenten zu normen, die nur wenige Funktionen (etwa lediglich die Standardpräsentation) aufweisen und einfach gestaltet sind. Dokumente werden dann mit dem Anwendungssystem erstellt und bearbeitet und vor dem Signiervorgang mit einer sicheren Präsentationskomponente hinsichtlich ihres rechtsverbindlichen zurechenbaren Inhalts präsentiert.

Folgende funktionale Einbettung und folgenden Ablauf kann man sich vorstellen:

1. Der Signierer ruft über das Anwendungsprogramm die Signierkomponente auf.
2. Innerhalb der Signierkomponente bestimmt er die Bedeutungszuordnung durch Auswahl eines passenden Präsentationsprogrammes (bzw. Akzeptanz eines Vorschlages entsprechend dem Vorschlag des aufrufenden Anwendungsprogrammes).
3. Über die gestartete Präsentationskomponente wird dann der Signiervorgang ausgelöst und die zugehörige Funktion der Signierkomponente angesteuert. Die Präsentationskomponente kann dann auch die Kontrolle darüber behalten, ab wann ein Signiervorgang überhaupt freigegeben wird, etwa nach interaktivem Selbsttest, oder nachdem tatsächlich alles „gesehen“ wurde.
4. Die Signierkomponente trägt das übergebene Kennzeichen des verwendeten Datenformats ein und führt den Signiervorgang durch.

Entsprechend würde der Ablauf beim Prüfvorgang erfolgen.

8.6.3 Konverterlösung

Diese angestrebte Ziellösung hat den Nachteil, dass Anwendungssysteme auf ein existierendes Datenformat hin umkonzipiert werden müssten oder dass komplexe und potentiell mehrdeutige Standardpräsentationen für die existierenden Formate definiert werden müssten. Eine Lösung könnte darin bestehen zwischen die Standardpräsentationskomponente und das Anwendungsprogramm einen Konverter zu schalten, der die Anwendungsdaten in das Datenformat der Standardpräsentation umsetzt.

Dabei ist jedoch das o.g. Gestaltungsziel der Vollständigkeit zu beachten. Die Signatur darf sich nur auf die im Format der Standardpräsentation vorliegenden Daten beziehen. Signiert wird der konvertierte Bitstring, nicht die Originaldaten des Anwendungsprogramms. Dies ergibt folgenden Ablauf:

- (1) Der Signierer ruft über das Anwendungsprogramm die Signierkomponente auf.
- (2) Das Anwendungsprogramm startet einen Konverter und übergibt dem Signier- und Prüfprogramm die konvertierten Daten zusammen mit dem Formatkennzeichen des Präsentationsformates.
- (3) Das Signier- und Prüfprogramm startet eine zugeordnete Präsentationskomponente, die dann die Standardpräsentation erzeugt.
- (4) Über die gestartete Präsentationskomponente wird dann wie oben der Signiervorgang ausgelöst.
- (5) Die Signaturdaten werden an das aufrufende Anwendungsprogramm zurückübergeben und von diesem in das Dokument eingetragen.

Entsprechend könnte der Ablauf beim Prüfvorgang erfolgen.

8.7 Evaluierung und organisatorische Aspekte

Es muss eine Prüfung von Präsentationsprogrammen geben, ob diese die Präsentationsbeschreibungen korrekt umsetzen. Außerdem müssen die Datenformate mit den Präsentationsbeschreibungen selbst auf Eignung (Vermeidung jeglicher Mehrdeutigkeiten, Vollständigkeit und Abgeschlossenheit) überprüft werden.

Für die Prüfung könnten Evaluierungsverfahren nach ITSEC und Prüfinstanzen nach SigG mit Aufsicht durch Regulierungsbehörde analog zur Evaluierung der anderen technischen Komponenten angewendet werden.¹⁷² Es muss aber eine Stelle geben, die zumindest – ähnlich der Maßnahmekataloge und der Signaturinteroperabilitätsspezifikationen – Anforderungskataloge an Datenformate und Präsentationskomponenten erstellt, die Prüfgrundlage wären (also medien- und gegebenenfalls auch anwendungsspezifische Konkretisierungen der o.g. Ziele).

Schließlich muss es noch eine Stelle geben, die ein zentrales Register führt für

- Formatkennzeichen: D.h. die den Daten zuzuordnenden Kennzeichen der Standardpräsentationen und die zugehörigen beschreibungen

¹⁷² Sinnvoll wäre es auch, bereits Präsentationsformate selbst evaluieren zu können (Bestimmtheit). Dafür sind die CC und die ITSEC jedoch nicht vorgesehen, die Norm gilt für „in Hardware, Firmware oder Software implementierte Sicherheitsmaßnahmen“, nicht für Konzepte.

- Verzeichnis der evaluierten Präsentationskomponenten, die diese erfüllen.¹⁷³

Im Kontext des Signaturgesetzes ist es naheliegend die Regulierungsbehörde die Verantwortung für die beiden letztgenannten Aufgaben zu überantworten.

¹⁷³ Dazu könnten weitere Angaben kommen, etwa der Zeitpunkt, ab wann die entsprechenden Programme und Formate nach einer Prüfung freigegeben wurden und auch ein Sperrzeitpunkt, z.B. für den Fall neuer Erkenntnisse über Unsicherheit.

9. Beispielhafte Lösungsvorschläge

Auf der vierten Ebene der Gestaltung sollen die Gestaltungsziele nun an zwei Beispielen, dem elektronischen Rezept und der elektronischen Urlaubskarte weiter konkretisiert werden. Diese folgenden Gestaltungsvorschläge verstehen sich als erste Diskussionsvorschläge.

9.1 Elektronisches Rezept

9.1.1 Beschreibung

Das elektronische Rezept ist eine prototypische Signaturanwendung für das Gesundheitswesen. Das Dokument ist ein an das herkömmliche Papierrezept angelehntes elektronisches Formular. Mit Hilfe dieses Dokumentes können Medikamente verschrieben, bei der Apotheke ausgegeben und schließlich bei der Abrechnungsstelle geprüft und zahlungstechnisch verarbeitet werden.¹⁷⁴ Der Arzt stellt in seinem Praxissystem ein Rezept aus, signiert es mit seiner Health Professional Card und überträgt es auf eine Patientenchipkarte. In einer Apotheke kann das Rezept aus der Karte ausgelesen und nach Einlösung als Datensatz an die Abrechnungsstelle weitergesendet werden. Die Rezeptdaten sind stark formatiert. Es gibt nur Eingabefelder mit Vorauswahlwerten und Textfelder definierten Inhalts, wie z.B. Name oder Medikamentenbezeichnung, nicht jedoch größere Freitextfelder für Kommentare o.ä.. Das Rezept weist neben einem Formularkopf mit den Daten des Patienten¹⁷⁵ und den Daten des Arztes auch mehrere Eintragszeilen für Medikamente auf. Im Formular ist nur eine Signatur des Arztes für das gesamte Rezeptdokument vorgesehen. Signiert wird wie in der elektronischen Urlaubskarte der GMD eine ASN.1-Codierung der Feldinhalte, nicht jedoch die Feldbezeichnungen oder andere Strukturinformationen. Diese werden durch das Programm vorgegeben.

9.1.2 Einbindung der Präsentationskomponente

Die Erfassung der Rezeptdaten erfolgt am besten weiterhin in den Praxissystemen. Dort ist eine Weiterverarbeitung der Daten jederzeit möglich. Die Praxissysteme sind allerdings wegen ihrer Komplexität nicht evaluierbar. Deshalb wird eine Umsetzung der oben skizzierten Architektur vorgeschlagen. Für verschiedene Plattformen wären Viewer zu entwickeln, die die Daten entsprechend der zu erstellenden Präsentationsbeschreibung anzeigen. Sie müssen vom ärztlichen Anwendungsprogramm aus, aber genauso vom Signier- und Prüftool aktiviert werden können.

Das verwendete Signier- und Prüftoolkit muss in der Lage sein selbsttätig die Darstellungskomponente aufzurufen, wenn eine Signatur erzeugt wird oder Daten mit einer Signatur gefunden werden. Das Anwendungssystem des Arztes sollte nicht Signiervorgänge ohne Umweg über diese Darstellungskomponente ansteuern können – zumindest muss dieser Aspekt konfigurierbar sein.

¹⁷⁴ S. Engelmann / Struif / Wohlmacher 1995.

¹⁷⁵ Eckstein / Paule 1999, 57. Ursprünglich sollte auch ein Pseudonym möglich sein (Engelmann / Struif / Wohlmacher 1995, 27).

9.1.3 Präsentationsbeschreibung

Die wesentlichen Aspekte der Präsentation sind zu untersuchen, die Vorgaben für Layout und Funktionen in einer Präsentationsbeschreibung festzulegen. Im vorliegenden Beispiel ist es am vielleicht ausreichend nur eine einzige Standardpräsentation festzulegen, weil es auf Aspekte der „Schönheit der Darstellung“ nicht ankommt.

Die Beschreibung der Standardpräsentation muss an dem kleinsten gemeinsamen Nenner von Geräteausstattungen der Anwender (Ärzte, Apotheken) bei Hardware / Ausgabegeräten orientiert sein. Hinsichtlich der Geräteausstattung dürfte dies ein 14 Zoll-Monochrome-Bildschirm sein.

i) Layout

Überschriften und Formulartexte sind festzulegen. Zusätzliche Inhaltsbestandteile durch eingebettete Objekte, Grafiken sind zu vermeiden.

Die Anordnung der Inhaltselemente ist festzulegen, wozu eine Grafik ausreichen kann. Die Reihenfolge der Medikamentierungseinträge muss vorgegeben werden, z.B. entsprechend der internen Numerierung der Einträge.

Nutzereingaben, Formularinhalte und Feldbezeichner müssen auf jeden Fall klar erkennbar und voneinander unterscheidbar sein. Dementsprechend sind Fonts, Fontgrößen und Farben auszuwählen und vorzugeben. Das Minimum der zu erwartenden Endgeräteausstattung ist Monochrome, deshalb ist auf Farbe bei der Standardpräsentation zu verzichten. Der Schriftgrad ist an der Bildschirmauflösung zu orientieren (z.B. 14 pt). Fonts sind vorzugeben (plattformübergreifend z.B. Times) und es muss auf die Beschreibung dieser Fonts verwiesen werden. Auch die verwendeten Zeichensätze müssen Evaluierungsgegenstand sein und mit den Präsentationskomponenten mitgeliefert werden.

Die Größen von Textfeldern sollten so gewählt werden, dass sie stets vollständig lesbar sind, z.B. auch bei langen Namen (die Buchstabenanzahl ist vorzugeben, soweit sie sich nicht aus Feldgröße und Zeichensatz ableitet). Eine sinnvolle zusätzliche Konvention ist, dass führende Leerzeichen bei Eingabe zu löschen sind.

Standardeinstellung des Anwendungsfensters beim Aufruf ist ein Fenster, dessen Größe am Minimum zu erwartender Bildschirmgrößen orientiert ist. Auf ihm sollten alle Daten im Zusammenhang zu sehen sein. Erforderlichenfalls ist eine Navigationsfunktion (1./2. Seite) vorzusehen und zu beschreiben.

ii) Funktionen

Die Anzeigefunktionen der Standardpräsentation sind zu spezifizieren. Je weniger Funktionen, desto besser. Ist die Vollständigkeit der Anzeige im Feld nicht zu garantieren, so sind die Funktionen zur Erschliessung des Feldes zu spezifizieren (z.B. Pfeil wird sichtbar am rechten Feldrand, wenn Feldinhalt größer als Feld), paßt das Dokument nicht in das Fenster oder wird eine Fensterverkleinerung zugelassen, sind auch die Blätterfunktionen zu beschreiben.

Die Signierfunktion sollte aus der Standardpräsentation heraus angesteuert werden können. Ein Signieren sollte erst möglich sein, wenn sichergestellt ist, dass alle Formulareinträge gesehen werden konnten. Es muss erkennbar sein, worauf sich die Signatur bezieht - und worauf

nicht (§ 14 Abs. 2 SigG). Entsprechend der westeuropäischen Lesegewohnheiten wäre der zu empfehlende Standort für einen Signierbutton im Dokument rechts unten.

Die Erzeugung einer Signatur muss vorher eindeutig angezeigt werden (§ 14 Abs. 2 SigG). Ein zufälliges Auslösen des Signiervorgangs sollte in allen Situationen verhindert werden, ein einfaches „Return“ bei eingestellter Mehrfachnutzung der PIN sollte nicht zur Auslösung des Signiervorgangs führen können.

9.1.4 Formatkennzeichen

Entsprechend der SigI- muss eine OID für den Datentyp (elektronisches Rezept) in der Signatur eingetragen sein. Da es kein allgemein zugängliches und gepflegtes Verzeichnis der OIDs gibt und sich die Datentyp-Spezifikationen möglicherweise einmal ändern, könnte zusätzlich eine lesbare Bezeichnung des Formates erwogen werden (Textfeld, z.B. "Elektronisches Rezept nach DIN xyz V1.0").

9.1.5 Selbstkontrolle

Für die Überprüfung der Korrektheit der Installation, aber auch für Zweifel beim Signiervorgang ist ein jederzeitig zugänglicher Selbsttestmodus vorzusehen, in dem die Funktionsfähigkeit und richtige Einstellung der Komponenten also die physischen und logischen Aspekte interaktiv überprüft werden können.

Als "Testpatient" kann Datensatz vorgesehen werden, dessen Attribute alle Formularfelder maximal ausfüllen, der alle (fünf) Medikamentierungszeilen belegt und bei dem sämtliche lesbaren alphanumerischen Zeichen des Zeichensatzes verwendet werden. Die Sichtbarkeit kann der Nutzer dann z.B. mit einer Vergleichsschablone (z.B. auf der Rückseite der Dokumentation) vergleichen.

9.1.6 Nachweis der physischen Präsentation

In Arztpraxen werden z.T. mehrere Rechner für die Rezeptanwendung genutzt werden, z.T. nutzen auch mehrere Ärzte einen Rechner gemeinsam. Um Fehler oder Mißbräuche besser aufklären und Nachweise über die tatsächliche Präsentation führen zu können, könnten zusätzliche Informationen über die genutzte Anwenderinfrastruktur in das signierte Rezept übernommen werden– optional und konfigurierbar. Zu denken ist an

- **Programmbezeichnung:** Ein eindeutige lesbare Bezeichnung des verwendeten Präsentationsprogramms, der Betriebssystemplattform und der Version.
- **Rechnerkennung:** Zur Identifizierung des beim signieren genutzten Rechners. Damit die Kennung nicht einfach aus einem elektronischen Rezept ausgelesen werden kann, ist die Bildung eines Hashwertes aus der Prozessorkennung und einem weiteren veränderlichen Wert (Zufallszahl, Dokumentauthentikator) möglich.

9.2 Elektronische Urlaubskarte

Die elektronische Urlaubskarte wurde bereits im fiktiven Eingangsbeispiel beschrieben und abgebildet. Diese Pilotanwendung ist lange in Betrieb und wird akzeptiert, größere Fehler und Mißbräuche sind nicht bekanntgeworden. Dennoch gibt es im Lichte der obigen Ausführungen einige Schwachpunkte.

9.2.1 Problematische Aspekte

Unter den in diesem Papier genannten Kriterien ist diese Anwendung in einiger Hinsicht problematisch:

- Nicht reproduzierbare Präsentation: Änderungen an den Formularen und den Datenstrukturen und den Anwendungsbedingungen sind nicht mehr, zumindest nicht ohne den verantwortlichen Entwickler nachvollziehbar. Aussagen über das Aussehen und den Inhalt einer Urlaubskarte sind im nachhinein (insbesondere nach längerer Zeit wie im Beispiel) kaum mehr möglich. Eine Präsentationsbeschreibung existiert nicht.
- Ungleiche Beweismittelverteilung: Der Signierer hat keine Verfügungsgewalt über Beweismittel. Er hat keinen Zugriff auf die Daten, kann von ihm signierte Dokumente nicht archivieren und verfügt er über keine Programme, um eine Präsentation seiner früher signierter Dokumente durchzuführen.
- Mißbrauchsmöglichkeiten: Dokumenterstellung, Präsentation (Visualisierung), Signiervorgang und Prüfvorgang werden nicht vom Signierer kontrolliert, die Anwenderinfrastruktur steht vollständig unter Fremdkontrolle.
- Verkehrsfähigkeit: Eine eventuelle Prüfung kann nur am Gerät in der GMD erfolgen, nicht aber an einem neutralen Ort auf einer geprüften Anwenderinfrastruktur.

Unter diesen Bedingungen ist ein wie auch immer gearteter Anscheinsbeweis unmöglich. Beweisführung wäre grundsätzlich nur durch einen Sachverständigen möglich.¹⁷⁶

9.2.2 Denkbare Lösung

Es ist wenig sinnvoll, für interne Einzelanwendungen wie die Urlaubskarte spezielle Präsentationsformate zu definieren und Präsentationskomponenten zu entwickeln. Der Aufwand wäre hoch, die Komponente würde von denselben Programmierern entwickelt, wie das komplexe Programm, eine Evaluierung wäre zu teuer. Eine Lösung ist hier nur im größeren Rahmen vorstellbar, indem Viewer für verschiedene formularorientierte Anwendungen in verschiedenen Unternehmen entwickelt und dann gemeinsam genutzt werden.

Es sind jedoch unterhalb dieser Schwelle praktische Verbesserungen möglich: Die Urlaubskartenanwendung könnte um ein Konvertierungsprogramm ergänzt werden, das die signierten oder zu signierenden Teildokumente der Karte (Kartenkopf, Antragszeilen) in ein spezielles HTML-File konvertiert und das dann diese Daten dem vom Nutzer installierten HTML-Browser zur Anzeige übergeben kann. Die Präsentationskomponente wäre dann der (vom Signierer, Prüfer) frei ausgewählte Browser, der zudem auch Speichermöglichkeiten bietet. Damit auch signiert wird, was angezeigt wird, wäre dann dieses HTML-Dokument zu signieren, lokal beim Signierer an dessen Anwenderinfrastruktur, und an den Server zur Eintragung in den Datensatz zurückzübermitteln.

Das HTML-Dokument selbst muss so aufgebaut werden, dass Mehrdeutigkeiten möglichst ausgeschlossen werden. Dies bedeutet dann u.a.: Nur direkte Formatierung mit einem auf allen Plattformen vorhandenen Font, festgelegte Hintergrundfarbe, usw. dabei keine Links, Grafiken und andere problematischen Elemente.

¹⁷⁶ Zu den Problemen dabei siehe das Eingangsbeispiel. Teil I:1.1, Der Fall Zange, S. 9. Glücklicherweise kommt es auf die Elektronik in der Regel nicht an, Beweise um Urlaub werden in der Regel mit Zeugen geführt werden können.

Die Präsentation, der Signier- und der Prüfvorgang wird so aus dem Netz heraus in die Anwenderinfrastruktur des Signierers verlegt. Beweismittel sind besser verteilt (Einzelanträge und Signaturen können lokal gespeichert werden) und bedingt verkehrsfähig.

10. Anregungen für rechtliche Regelungen

Das Problem der Eindeutigkeit der Interpretation und Darstellung signierter Daten wurde in den geltenden und geplanten Gesetzen bislang unzureichend berücksichtigt. Im Folgenden werden aus technischer Sicht einige Anregungen gegeben, wie eine Berücksichtigung denkbar wäre. Dabei werden Ergänzungen zum Signaturgesetz vorgeschlagen und nicht (was auch vorstellbar wäre) der Aspekt der Präsentation aus dem Signaturgesetz herausgenommen und gesondert behandelt.

10.1 Berücksichtigung der Präsentation

10.1.1 Vorschläge zum SigG und zur SigV

Ohne Eindeutigkeit der Interpretation und Präsentation digitaler Rohdaten haben digitale Signaturen nur eingeschränkte Beweiskraft. Im Signaturgesetz fehlen bislang klare Vorschriften zur Interpretation signierter Daten. Um diese nicht in die vorhandenen Vorschriften "hineininterpretieren" zu müssen – soweit das überhaupt ginge – sollte eine Änderung/Anpassung der Vorschriften erfolgen. Als Änderung böte sich folgende Ergänzung von § 14 Absatz 2 an, die zunächst einmal klarstellt, **dass** eine eindeutige Präsentation erforderlich ist (noch nicht allerdings wie dies zu bewerkstelligen ist).

*Für die Darstellung zu signierender Daten sind technische Komponenten mit Sicherheitsmerkmalen erforderlich, **die eine eindeutige Interpretation der Daten sicherstellen und die Erzeugung einer digitalen Signatur sowie die Interpretation vorher eindeutig anzeigen** ...*

Die Formulierung ändert nichts an der Selbstverantwortung des Nutzers für die Sicherheit der Anwenderinfrastruktur, wie sie im Signaturgesetz insgesamt angelegt ist. Die Forderung nach eindeutiger Interpretation impliziert wie in diesem Papier dargelegt eine Präsentation, eindeutig zumindest bezogen auf den Anwendungszweck. Die Formulierung als "kann"-Vorschrift würde keinen Zwang zur Präsentation von Daten bei jedem Signiervorgang nahe legen – was zumindest bei automatischen Massensigniervorgängen unsinnig und unrealisierbar wäre.

Einen Bezug zur Interpretation und Präsentation enthält bereits § 16 Abs. 3 SigV, der fordert, dass "die technischen Komponenten .. nach Bedarf den Inhalt der zu signierenden oder signierten Daten hinreichend erkennen lassen" müssen. Diese Formulierung ist etwas unscharf (Bedarf besteht grundsätzlich immer) vor allem vor, weil Satz 5 die viel deutlichere Forderung nach „eindeutiger Interpretation der Daten“ enthält. Diese ist wiederum jedoch nur abstrakt, beinhaltet nicht die Forderung nach der eindeutigen Wahrnehmbarkeit für den Signierer und klärt nicht das wie. Außerdem gilt sie nur für technische Komponenten, die "geschäftsmäßig zur Nutzung angeboten" werden: Ein nicht geschäftsmäßig signiertes Dokument könnte dann immer noch als ein geschäftsmäßiges interpretiert werden, die Forderung so unterhöhlt werden. In § 16 Abs. 3 Satz 5 könnte der Bezug zur Interpretation bei geschäftsmäßig genutzten Komponenten gestrichen und als Folgesatz eingefügt werden:

Eine eindeutige Interpretation muss sichergestellt sein, eine eindeutige Präsentation muss festgelegt sein.

Hier vermeidet "Festlegung" einen Zwang zur Präsentation und deren ausschließlicher Nutzung, erzwingt aber die Festlegung einer hinreichend eindeutigen Präsentation und eindeutigen Interpretation für alle signaturgesetzkonformen Anwendungen.

Erweiterungsbedürftig wären auch die Bestimmungen zur Prüfung technischer Komponenten. Aus § 17 Satz 1 in Verbindung mit § 16 (3) Satz 5 kann gefolgert werden, dass als Prüfstufe für eine Präsentationskomponente „E2-hoch“ und in Fällen des Anbietens zur geschäftsmäßigen Nutzung wäre „E4-hoch“ anzunehmen. Dabei ist auch schon heute nicht klar festgelegt, was inhaltlicher Gegenstand der Prüfung sein soll bzw. wer diesen eigentlich spezifiziert.¹⁷⁷ Im Lichte dieses Papiers sollte klar sein, dass die Prüfung der Präsentationskomponente (genauer des Präsentationsprogrammes) die Offenlegung des Dokumentformates mit der Festlegung einer Standardpräsentation in einer Datentyp-Dokumentation erfordert, wobei die Einhaltung dieser Vorgaben dann Gegenstand der Programmprüfung ist. Aus den obigen Änderungsvorschlägen des SigG und der SigV könnte dies in Verbindung mit § 17 dann auch ohne weitere Gesetzesänderung abgeleitet werden.

Da die Vorgaben des Gesetzes und der Verordnung nur sehr allgemein sind, ist dann aber noch eine technische Konkretisierung erforderlich. Notwendig erscheint eine Ergänzung der Maßnahmekataloge der Behörde nach § 16(6) in denen schon bisher die Vorgabe für die Präsentationskomponente weitestgehend fehlen. Hier wären allgemeinen Gestaltungsziele für Präsentationssysteme und Dokumentformate aufzunehmen. Das BSI sollte als konkretere Maßnahmenempfehlungen auch Prüfrichtlinien (oder gar protection profiles i.S. der Common Criteria) für Präsentationskomponenten herausgeben, die in der Evaluierung zu berücksichtigen wären.

Die Lösung hat noch die Eigenschaft, dass Dokumentformate nicht unabhängig von Präsentationsprogrammen geprüft werden können. Im Interesse der Offenheit wäre es allerdings vorteilhaft, wenn Dokumentformate (ähnlich wie technische Kommunikationsprotokolle) auf ihre Eignung für den Rechtsverkehr geprüft werden könnten, damit Hersteller Produkte gezielt für diese als geeignet beurteilten und veröffentlichten Formate entwickeln und zertifizieren könnten. Grundlage sollte ein zentrales Register aller Dokumentformate sein, die mit Signaturen nach SigG signiert werden. Für jedes Format sollten im Register neben der Beschreibung des Dateiformates, Standardpräsentationen für einzusetzende Präsentationsprogramme und Minimalanforderungen an die zu verwendenden Ausgabemedien festgelegt werden (§17-Ergänzung):

(2a) Die zuständige Behörde führt ein allgemein zugängliches Register von für das Signieren und Prüfen von Signaturen geeigneten Dokumentformaten und für diese zertifizierten Präsentationsprogrammen.

Ein solcher Regelungsansatz entspräche dem der Eignungsprüfung von Algorithmen, für die allerdings mangels Menge kein Register erforderlich ist sondern eine Veröffentlichung im Bundesanzeiger ausreicht. Problematisch wäre, dass die Regulierungsbehörde die Eignungsprüfung durchführen müsste. Im Unterschied zu Algorithmen gibt sehr viele Dokumentformate und die Fragen der Präsentation und Interpretation sind teilweise anwendungsabhängig

¹⁷⁷ Bislang müssen solche aus den allgemeinen Vorgaben in Signaturgesetz und -verordnung abgeleitet werden (z.B. dass die Daten, die signiert werden vorher kenntlich zu machen sind).

und ihre Prüfung dürfte die Regulierungsbehörde überfordern. Eine Lösung könnte darin bestehen, dass die Regulierungsbehörde allgemeine Anforderungen an eine Standardpräsentation und die Dokumentation aufstellt – und dass dann die für Komponenten vorgesehenen Prüfstellen die Prüfung übernehmen.¹⁷⁸

10.1.2 Anregungen zur BGB-Änderung

Erst mit den klarstellenden Änderungen im Signaturgesetz und Signaturverordnung lässt sich eine elektronische Form über § 126 BGB sinnvoll einführen. In der bisherigen Fassung des Vorschlags von § 126a wird darauf verwiesen, dass der Erklärende das elektronische Dokument mit einer Signatur nach SigG versehen muss. Mit den klarstellenden Änderungen im Signaturgesetz und Signaturverordnung lässt möglicherweise bereits daraus folgern - was anzustreben wäre - dass sich nämlich der Erklärende die eindeutige Interpretation und Präsentation der signierten Daten zurechnen lassen muss, wenn er nicht den Gegenbeweis führt bzw. substantiierte Einreden vorbringt (Vermutung der Abgabe der Erklärung in § 126a Abs.3). Eine ergänzende Klarstellung erscheint aber auf jeden Fall sinnvoll:

*Liegt eine Erklärung in der Form des Absatzes 1 vor und ergibt eine Prüfung mit dem öffentlichen Signaturschlüssel, das das Dokument nachträglich nicht verändert worden ist, so wird vermutet, dass die Erklärung **in der mit dem Signaturgesetz vorgegebenen eindeutigen Interpretation und Präsentation** vom Schlüssel-Inhaber abgegeben worden ist...*

10.2 Berücksichtigung der Systemherrschaft

Nach den Ausführungen in diesem Papier kann der (zivilrechtliche) Nachweis einer bestimmten Willens- und Wissenserklärung aus signierten Daten über die Zurechenbarkeit einer normierten Standardpräsentation gelingen, ohne dass der sehr schwierige Nachweis der tatsächlichen Präsentation geführt werden muss. Allerdings muss zumindest die Korrektheit eines tatsächlichen Vorgangs, nämlich die richtige Eintragung des Präsentationsformates in der Signatur, nachgewiesen werden. Was hierzu als Indiztatsache nachzuweisen ist dürfte von der Verantwortung und Kontrolle der Anwenderinfrastruktur abhängen.

Kontrolliert der Signierer die Anwenderinfrastruktur selbst, dann ist er für deren Korrektheit (und z.B. die Installation evaluierter Teilkomponenten) verantwortlich – und die Folgen möglicher Versäumnisse. Der Beweisführer sollte dann aber nachweisen müssen, dass der Signierer wirklich auf seinem eigenen System signiert hat.

Wird auf einem anderen System signiert, ist die Korrektheit des Systems zum Signierzeitpunkt nachzuweisen. Die Korrektheit kann vermutet werden, wenn der Betreiber des genutzten Systems nicht möglicher Nutznießer einer Manipulation ist. Damit aber ein solches vereinfachtes Beweisverfahren möglich ist, müssen Anwenderinfrastrukturen, die von Dritten betrieben werden, regelmäßig und stichprobenartig überprüft werden.¹⁷⁹ Dazu muss anhand des signierten Dokumentes auf die Systemherrschaft (eines bestimmten Anbieters) und die Signierzeit zurückgeschlossen werden können.

¹⁷⁸ Hier ist noch zu klären: Kann ein Datenformat nach ITSEC eigenständig geprüft werden

¹⁷⁹ Bedenkt man, dass selbst Jahrmarktswaagen regelmäßig überprüft werden, so sollte die Forderung nach Kontrolle eines öffentlich zugänglichen Signiersystems nicht als Überregulierung verstanden werden!

Schließlich muss der Beweisführer in die Lage versetzt werden, zu beweisen, dass nicht auf einer von ihm kontrollierten Anwenderinfrastruktur signiert wurde, damit er nicht den sehr schwierigen Nachweis der tatsächlichen Präsentation zum Signierzeitpunkt antreten muss und auf den (praktisch undurchführbaren) Indizienbeweis der Sicherheit und Korrektheit der Anwenderinfrastruktur zum Signierzeitpunkt verzichten kann.

Bisher findet sich von alledem nichts im Signaturgesetz und in den vorgeschlagenen Änderungen des BGB. Nachfolgend einige Anregungen für denkbare Ergänzungen:

Die Forderung nach dem Erkennen der Anwenderinfrastruktur könnte recht einfach in § 14 Abs. 2 integriert werden.

*.. Für die Überprüfung signierter Daten sind technische Komponenten mit Sicherheitsvorkehrungen erforderlich, die feststellen lassen, ob die signierten Daten unverändert sind, auf welche Daten sich die digitale Signatur bezieht, **wer die zum Signieren verwendete Anwenderinfrastruktur betreibt** und welchem Signaturschlüssel-Inhaber die digitale Signatur zuzuordnen ist.*

Das "wer" könnte dann in der Signaturverordnung oder in Maßnahmekatalogen insoweit eingeschränkt werden, dass insbesondere festzustellen ist, ob der Signierer oder ein öffentlicher Anbieter Betreiber der Anwenderinfrastruktur ist.

Die Forderung nach Kontrolle der Betreiber öffentlich zur Nutzung angebotener Anwenderinfrastrukturen gibt es nicht im Signaturgesetz, dessen Adressat bislang Zertifizierungsinstanzen und mittelbar ihre Kunden und die Hersteller sind. Eine Forderung lässt sich deshalb nur schwer in das vorhandene Gerüst des Signaturgesetzes einsortieren und erfordert wohl die Ergänzung des SigG um wenigstens einen zusätzlichen Paragraphen. Dies ist in einer juristischen Arbeit eingehend zu untersuchen. Notwendige Bestandteile einer solchen zusätzlichen Regelung wären:

- **Zweck:** Betreiber öffentlich zum Signieren angebotener Systeme haben Maßnahmen zu treffen, die jederzeitige Korrektheit der Funktion ihrer Systeme sicherstellen und nur Komponenten nach SigG § 14 einzusetzen. Mit einer solchen Regelung wären ebenso wie bei Zertifizierungsstellen nicht alle Betreiber zwangszuverpflichten, sondern nur bestimmte kontrollierte Betriebsweisen zu privilegieren, weil die Beweisführung vereinfacht werden könnte - im Sinne einer Beweisvermutung auf der Basis einer Sicherheitsvermutung für die öffentliche Anwenderinfrastruktur zum Signierzeitpunkt oder auch im Sinne eines gewöhnlichen Anscheinsbeweises.
- **Prüfungspflicht:** Betreiber solcher Anwenderinfrastrukturen haben regelmäßige Prüfungen dieser Systeme durch berechnigte Prüfstellen durchführen zu lassen und die Bestätigung ihren Nutzern in einer nicht verfälschbaren Art und Weise anzuzeigen (keine Festlegung auf ein bestimmtes elektronisches oder nicht-elektronisches Verfahren). Die berechtigten Stellen haben jederzeit das Recht, stichprobenartig zusätzliche Prüfungen durchzuführen.
- **Prüfstellen:** Die Regulierungsbehörde bestimmt das Prüfverfahren und den Prüfturnus und genehmigt und überwacht Prüfstellen.
- **Maßnahmekataloge:** Die Regulierungsbehörde kann die technischen Sicherheitsanforderungen an solche Systeme im Einzelnen regeln.

In § 126 BGB könnte dann die Vereinfachung des Nachweises der Zurechenbarkeit von der Systemherrschaft abhängig gemacht werden.

Ausblick

In dieser Arbeit wurde der Nachweis der Präsentation digital signierter Daten untersucht und es wurde mit dem Konzept der zurechenbaren Präsentation ein Lösungsansatz für die dabei auftretenden Beweisprobleme vorgestellt. Gleichwohl dieses Papier noch einige Fragen offen bzw. und eröffnet eine Reihe neue Fragestellungen.

Für Standardpräsentationen wurde die Definition von Mindesteigenschaften an Ausgabegeräte festzulegen. Auch wenn die zu definierenden Eigenschaften nahe liegen, sind noch einige Fragen zu klären. Qualitätseigenschaften heutiger Ausgabegeräte (Bildschirmauflösung, Bildwiederholungsfrequenz, ..) sind an der Technik selbst orientiert. Die für die Wahrnehmung erforderlichen biometrischen Kriterien wären noch zu bestimmen und mit den technischen Qualitätskriterien abzugleichen.

Die Risiken und auch Lösungen wurden am Beispiel der Textkommunikation dargestellt. Wegen der heutigen Bedeutung dieser Kommunikationsform und ihrer absehbaren Privilegierung durch Änderungen im BGB war dies sinnvoll. Gleichwohl werden andere Medien wie Audio- und Videodaten, interaktive Modelle und Virtual Reality, sowie deren Kombination in Multimediadokumenten eine zunehmende Bedeutung erlangen. Auch für diese Medien ist zu untersuchen, was wesentliche Aspekte der Präsentation sein könnten, welche Risiken sich ergeben und wie Standardpräsentationen festzulegen wären.

Für Fälle, in denen der Nachweis einer Standardpräsentation nicht ausreicht, sondern die tatsächliche Präsentation nachzuweisen ist – insbesondere Schuldnachweis in Strafprozessen – ist die Wahrscheinlichkeit bestimmter alternativer Präsentationen gutachterlich abzuschätzen. Hierzu sind, wie dargelegt, Wahrscheinlichkeiten der Ursachen für Abweichungen zu bestimmen. Um solche zu ermitteln, wären empirische Erkenntnisse über das Nutzerverhalten, z.B. zur Häufigkeit bestimmter Systemkonfigurationen erforderlich. Ein Feld für Untersuchungen, deren Notwendigkeit und Richtung sich aber erst mit der Rechtspraxis und Sachverständigenbegutachtung ergeben dürfte.

In dieser Arbeit konnten in den juristischen Datenbanken und der Literatur nur einige Fälle (vor allem im Zusammenhang mit BTX) gefunden und ausgewertet werden. Es wäre sicher sinnvoll, die Präsentationsproblematik auch aus juristischer Sicht noch einmal systematisch zu untersuchen.

Schließlich sei noch darauf hingewiesen, dass hier nur die Präsentation der Dokumentdaten untersucht wurde und nicht die der Sicherheitsmerkmale (Signaturen, Zertifikate,..) und die Dialogfelder beim Signiervorgang. Für die Gestaltung der Darstellungskomponente sind auch solche Aspekte wichtig und wären entsprechend zu untersuchen.

Literatur

- [Adob_89] Adobe Systems Inc.: Postscript Handbuch, Bonn u.a., 1999.
- [Appe_91] Appelt, W.: Document Achitecture in Open Systems The ODA Standard, Berlin u.a. 1991.
- [Bär_98] Bär, J.: EDV-Beweissicherung im Strafverfahrensrecht, CR 7/1998, 434 - 439.
- [Bär_96] Bär, J.: Beschlagnahme von Computerdaten, CR 11/1996, 675 - 683 und CR 12/1996, 744-752.
- [Bär_95] Bär, J.: Durchsuchungen im EDV-Bereich, CR 3/1995 158-169 und CR 4/1995, 227-234.
- [Berg_99] Berger, A.: Signatur-Interoperabilitätsspezifikation: Zertifikate und Dokumentenformate, DuD 4/1999, 206 - 212.
- [BPor_99] Bertsch, A. / Pordesch, U.: Zur Problematik von Prozeßlaufzeiten bei der Sperrung von Zertifikaten, DuD 9/1999, 514 - 519.
- [BePo_99] Berger, A. / Pordesch, U.: Kontextabhängige Gültigkeitsprüfung digitaler Signaturen, in: Baumgart, R. / Rannenber, K. / Wähler, D. / Weck, G. (Hrsg.): Verlässliche Informationssysteme IT-Sicherheit an der Schwelle des neuen Jahrtausends (VIS 99), Essen 22.-24.9.1999, Braunschweig 1999, 225 - 242.
- [Berg_99] Berger, A.: Signatur-Interoperabilitätsspezifikation: Zertifikate und Dokumentenformate, DuD 4/1999, 206 - 212.
- [BeSt_94] Bergmann, M. / Streitz, S.: Beweisführung durch EDV-gestützte Dokumentation, CR 2/1994.
- [BiHa_93] Bizer, J. / Hammer, V.: Elektronisch signierte Dokumente als Beweismittel, DuD 11/1993, 619 - 628.
- [BiHP_95] Bizer, J. / Hammer, V. / Pordesch, U.: Gestaltungsvorschläge zur Verbesserung des Beweiswertes digital signierter Dokumente, in: Pohl, H. / Weck, G., Beiträge zur Informationssicherheit: Strategische Aspekte der Informationssicherheit und staatliche Reglementierung, München Wien 1995, 99 - 144.
- [Bies_99] Biester, J.: MailTrust-PKI-Spezifikation MailTust Version2, DuD 4/1999, 218 - 221.
- [BiBF_99a] Biester, J. / Bauspieß, F. / Fox, D.: MailTrusT Version 2 Austauschformat, in: TeleTrusT: Biester, J. / Bauspieß, F. / Fox, D. (Secorvo Security Consulting GmbH): MailTrust Version 2 Gesamtkonzeption, Aufbau und Komponenten einer PKI, Stand 16.März 1999.
- [BiBF_99b] Biester, J. / Bauspieß, F. / Fox, D.: MailTrusT Version 2 Profile für Zertifikate und Sperrlisten, in: TeleTrusT: Biester, J. / Bauspieß, F. / Fox, D. (Secorvo Security Consulting GmbH): MailTrust Version 2 Gesamtkonzeption, Aufbau und Komponenten einer PKI, Stand 16.März 1999.
- [Bleu_97] Bleutge, P.: Digitale Unterschrift schützt Daten, Der Sachverständige Jan./Feb. 1997, 16 - 17.
- [BMJ_1999] Bundesministerium der Justiz (BMJ): Entwurf eines Gesetzes zur Anpassung der Formvorschriften des Privatrechts an den modernen Rechtsgeschäftsverkehr, Stand 19.Mai 1999.
- [Boha_89] Bohatiuk, E.: Beweiswert gespeicherter Informationen, CR 6/1989, 535 - 539.

- [Born_97] Born, G.: Referenzhandbuch der Dateiformate: Datenbanken, Tabellenkalkulation, Text, Grafik. Multimedia, Sound und Internet, Bonn / Reading, Massachusetts u. a., 1997.
- [Bris_98] Brisch, K.: Gemeinsame Rahmenbedingungen für elektronische Signaturen Richtlinienentwurf der Europäischen Union, CR 8/1998, 492 - 499.
- [BSI_96] Bundesamt für die Sicherheit in der Informationstechnik (BSI): IT-Grundschutzhandbuch, Bonn, 1996.
- [BSI_98] Bundesamt für die Sicherheit in der Informationstechnik (BSI): Maßnahmekataloge für digitale Signaturen - auf Grundlage von SigG und SigV, Stand 18.11.1997, Version 1.0, Bonn 1998.
- [Corn_99] Cornelius, H.: Die Intel Pentium III Prozessor-Seriennummer, DuD 9/1999, 529 - 532.
- [Crei_96] Creifelds, C.: Rechtswörterbuch, 13. Auflage, München, 1996.
- [DeKa_97] Deville, R. / Kalthegeener, R.: Wege zum Handelsverkehr mit elektronischer Unterschrift, NJW-CoR 3/1997, 168 - 172.
- [DeSt_99] Deutscher Städtetag: Digitale Signatur auf der Basis multifunktionaler Chipkarten Ein Leitfaden, Köln, 1999.
- [Dier_97] Dierstein, R.: Duale Sicherheit - IT-Sicherheit und ihre Besonderheiten, in: Müller, G. / Pfitzmann, A.: Mehrseitige Sicherheit in der Kommunikationstechnik Verfahren, Komponenten, Integration, Bonn u.a., 1997, 31 - 60.
- [Ebbs_96] Ebbing, F.: Schriftform und E-Mail, CR 5/1996, 271 - 278.
- [Eber_95] Eberlein, E. / Oberquelle, H. / Oppermann, R.: Einführung in die Software-Ergonomie, Berlin New York 1995.
- [EcPa_99] Eckstein, L. / Paule, C.: AM-Card Spezifikation der Applikations-Programmier-Schnittstelle, Version 1.0, 30. August 1999, GMD-Forschungszentrum Informationstechnik GmbH 1999.
- [EESS_99] European Electronic Signature Standardization Initiative (EESSI), Final Draft of the EESSI Expert Team Report, June 18, 1999
- [EnSW_95] Engelmann, W. / Struif, B. / Wohlmacher, P.: Anwendungsbeispiele der digitalen Signatur: elektronisches Rezept, elektronischer Notfallausweis und elektronischer Führerschein, in: Glade, A. / Reimer, H. / Schneider, W. / Struif, B.: Digitale Signaturen, Braunschweig / Wiesbaden, 1995, 25 - 35.
- [Erbe_96] Erber-Faller, S.: Gesetzgebungsvorschläge der Bundesnotarkammer zur Einführung elektronischer Unterschriften, CR 6/1996, 375 - 663.
- [Erns_97] Ernst, S.: Der Mausclick als Rechtsproblem, NJW-CoR 3/1997, 165 - 167.
- [Fox_98] Fox, D.: Zu einem prinzipiellen Problem digitaler Signaturen, DuD 7/1998, 386 - 388.
- [GaPS_98] Gattung, G. / Pordes, U. / Schneider, M.J.: Der mobile persönliche Sicherheitsmanager, GMD-report 24, St. Augustin, Juli 1998.
- [GLI_oD] Mehnen, H. (GLI): EDIFACT ohne Geheimnisse, Haar, o.D..
- [Gold_98] Goldfarb, C.F.: Future Directions in SGML/XML, in: Mumm, W. / Sommer, I.: SGML und XML Anwendungen und Perspektiven, 1998, 3 - 25.
- [GrPo_98] Grimm, R. / Pordes, U.: Wie sicher ist die digitale Signatur, Spektrum der Wissenschaft Dossier 1/1998, 60 - 62.
- [GrWä_99] Grimm, R. / Wäsch, J.: Projekt "XML-Strategiestudie" zur Positionierung des Einsatzes von XML in der Sparkassenorganisation, Darmstadt, 9.2.1999.
- [GrGe_79] Groß, G / Geerds, F.: Handbuch der Kriminalistik, 10. Aufl., Berlin 1978.

- [Grim_94] Grimm, R. Sicherheit für offene Kommunikation, Mannheim u.a. 1994.
- [Günt_89] Günther, K.: Programmierung verteilter Bürovorgänge in DISCO, Sonderdruck aus GMD-Jahresbericht 1989.
- [HaBi_93] Hammer, V. / Bizer, J.: Beweiswert elektronisch signierter Dokumente, DuD 12/1993, 689 - 699.
- [Hamm_93] Hammer, V.: Beweiswert elektronischer Signaturen, in: Weck, G. / Horster, P. (Hrsg.), Verlässliche Informationssysteme, Proceedings der GI-Fachtagung VIS '93, 269 - 291.
- [Hamm_95] Hammer, V.: Sicherungsinfrastrukturen Gestaltungsvorschläge für Technik, Organisation und Recht, Berlin u.a. 1995.
- [Hamm_99] Hammer, V.: Die 2. Dimension der IT-Sicherheit, DuD-Fachbeiträge Braunschweig/Wiesbaden 1999.
- [HaPR_93] Hammer, V. / Pordesch, U. / Roßnagel, A.: Betriebliche Telefon- und ISDN-Anlagen rechtsgemäß gestaltet, Berlin u.a. 1993.
- [Hets_99] Hetschold, T.: PKI-Interoperabilität: PKIX und SigI im Vergleich, DuD 4/1999, 213 - 217.
- [IPRo_99] Idecke, S. / Pordesch, U. / Roßnagel, A.: Rechtsgemäße Technikgestaltung, in: Roßnagel, A. / Schroeder, U.: Multimedia in technischrechtlichen Genehmigungsverfahren, Köln u. a., 1999, 131 - 166.
- [ITSE_93] Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik - Information Technology Security Evaluation Criteria (ITSEC), Version 1.2, in: Kersten, H. (Hrsg.), Internationale Sicherheitskriterien, München u.a. 1993, 427 ff.
- [Keus_98] Keus, K.J.: European Electronic Signature Standardisation Initiative (EESSI) - die europäische Standardisierungsinitiative für elektronische Signaturen, in: DIN - Deutsches Institut für Normung e.V.: Branchenübergreifende digitale Identität, Berlin, 1999.
- [Köhn_97] Köhntopp, M.: Datenschutz durch Technik ?!, FIFF-Kommunikation 2/1997, 53 - 56.
- [Kuhn_91] Kuhn, M.: Rechtshandlungen mittels EDV und Telekommunikation, München 1991.
- [Kumb_94] Kumbruck, C.: Der "unsichere" Anwender - vom Umgang mit Signaturverfahren, Datenschutz und Datensicherung 1/1994, 20 - 29.
- [KuPh_89] Kuckuck, W. / Philipp, M.: FISH - Das Forensische Informations-System Handschriften, in: Conrad, W. / Stier, B.: Grundlagen, Methoden und Ergebnisse der forensischen Schriftuntersuchung, Lübeck, 1989, 159 - 188.
- [MeSc_99] Menzel, T. / Schweighofer, E.: Das österreichische Signaturgesetz, DuD 9/1999, 503 - 507.
- [Mich_82] Michel, L.: Gerichtliche Schriftvergleichung, Berlin, New York, 1982.
- [Mied_98] Miedbrodt, A.: Regelungsansätze und -strukturen US-amerikanischer Signaturgesetzgebung, DuD 7/1998, 389 - 394.
- [MöSc_98] Möhr, W. / Schmidt, I.: SGML und XML Anwendungen und Perspektiven, Berlin Heidelberg 1998.
- [MuKe_97] Musciano, C. / Kennedy, B.: HTML The Definitive Guide 2nd Edition, Maryland, 1997.
- [Niss_91] Nissen, K.: Befunderhebung und Befundbewertung, Der Sachverständige 11/1991, 283 - 290.
- [Niss_83] Nissen, K.: Theorie der Begutachtung, Archiv für Kriminologie 172 / 1983, 143 - 152.

- [Onda_99] Ondarza, P.: Digitale Signaturen und staatliche Kontrolle, Manuskript zum (juristischen) Dissertationsvorhaben, Berlin 1999.
- [PeSi_99] Persson, C. / Siering, P.: Big Brother Bill, C't 6/1999, 16 - 20.
- [PPSW_97] Pfitzmann, A. / Pfitzmann, B. / Schunter, M. / Waidner, M.: Trusting Mobile User Devices and Security Modules, Computer 30/2 1997, 61 - 68.
- [PoHR_91] Pordesch, U. / Hammer, V. / Roßnagel, A.: Prüfung des rechtsgemäßen Betriebs von ISDN-Anlagen, Braunschweig 1991.
- [Pord_92] Pordesch, U.: Experimente zur Verletzlichkeit im Rahmen der Simulationsstudie Rechtspflege, provet-Arbeitspapier Nr. 81, Darmstadt 1992.
- [Pord_93a] Pordesch, U.: Experimente zur Verletzlichkeit im Rahmen der Simulationsstudie formularorientierte Vorgangssysteme, provet-Arbeitspapier Nr. 106, Darmstadt 1993.
- [Pord_93b] Pordesch, U.: Risiken elektronischer Signaturverfahren, DuD 10/93, 561 - 569.
- [Pord_94] Pordesch, U.: Rechtliche und software-ergonomische Gestaltungsanforderungen an Groupware, in: Hartmann, A. / Herrmann, T. / Rohde, M. / Wulf, V. (Hrsg.), Menschengerechte Groupware - Software-ergonomische Gestaltung und partizipative Umsetzung, Stuttgart 1994.
- [Pord_95] Pordesch, U.: Sekretär oder Aufpasser? Zur möglichen Rolle von Personal Digital Assistants in der Dienstleistungsgesellschaft, in: Kubicek, H. / Müller, G. / Neumann, K.H. / Raubold, E. / Roßnagel, A. (Hrsg.), Jahrbuch Telekommunikation und Gesellschaft 1995 Multimedia - Technik sucht Anwendung, Heidelberg 1995.
- [Pord_99] Pordesch, U.: Sicherheitsmanagement, in: Roßnagel, A. / Haux, R. / Herzog, W. (Hrsg.): Mobile und sichere Kommunikation im Gesundheitswesen, Braunschweig 1999, 153 - 170.
- [PoBe_99] Pordesch, U. / Berger, A.: Context-Sensitive Verification of the Validity of Digital Signatures, in: Müller, G. / Rannenber, K.: Multilateral Security in Communications Technology, Infrastructure, Economy, München u.a., 1999, 251 - 267.
- [PoNi_95] Pordesch, U. / Nissen, K.: Fälschungsrisiken elektronisch signierter Dokumente, CR 9/1995, 562 - 568.
- [PoRo_94] Pordesch, U. / Roßnagel, A.: Elektronische Signaturverfahren rechtsgemäß gestaltet, DuD 2/94, 82 - 91.
- [prGM_94] provet / GMD: Die Simulationsstudie Rechtspflege - Eine neue Methode zur Technikgestaltung für Telekooperation, Berlin 1994.
- [pr_GM_95] provet / GMD: Rechtsverbindliche Telekooperation in der elektronischen Vorgangsbearbeitung, GMD-Studien Nr. 261, St. Augustin 1995.
- [Rann_95] Rannenber, K.: Evaluationskriterien zur IT-Sicherheit - Entwicklungen und Perspektiven der Normung, in: Brüggemann, H.H. / Gerhardt-Häckl, W.: Verlässliche IT-Systeme, Braunschweig 1995, 45 - 68.
- [RegT_98a] Regulierungsbehörde für Telekommunikation und Post (REGTP): Maßnahmenkatalog nach § 12 Abs. 2 der Verordnung zur digitalen Signatur, Entwurf, nach Angaben des Bundesamt für die Sicherheit in der Informationstechnik, Stand: 25.3.1998, Version 2.0a, 1998.
- [RegT_98b] Regulierungsbehörde für Telekommunikation und Post (REGTP): Maßnahmenkatalog nach § 16 Abs. 6 der Verordnung zur digitalen Signatur, Entwurf, nach Angaben des Bundesamt für die Sicherheit in der Informationstechnik, Stand: 12.2.1998, Version 1.0, 1998.
- [Ries_89] Riess, M.: Beweismittel Schriftvergleichung, Lübeck, 1989.
- [Roßn_98] Roßnagel, A.: Die Sicherheitsvermutung des Signaturgesetzes, NJW 1998, 3312.

- [Roßn_99] Roßnagel, A.: Die digitale Signatur in der öffentlichen Verwaltung, in: Kubicek, H. / Braczyk, H.J. / Klump, D. / Müller, G. / Neu, W. / Raubold, E. / Roßnagel, A.: Multimedia @Verwaltung Jahrbuch Telekommunikation und Gesellschaft, Heidelberg, 1999, 158.
- [RoPo_99] Roßnagel, A. / Pordesch, U.: Kommentare zu § 14 SigG, sowie den §§ 16 und 17 SigV, in: Roßnagel, A.: Recht der Multimedia-Dienste Kommentar, Heidelberg, 1999.
- [RoSc_99] Roßnagel, A. / Schroeder, U.: Multimedia in technikalrechtlichen Genehmigungsverfahren, Köln u. a., 1999.
- [Rudo_80] Rudolph, K.: Die Formulierung der Beweisfrage beim richterlichen Sachverständigenbeweis, Zeitschrift für das gesamte Sachverständigenwesen 1980, 208 - 211.
- [RWHP_90] Roßnagel, A. / Wedde, P. / Hammer, V. / Pordesch, U.: Die Verletzlichkeit der Informationsgesellschaft, 2. Auflage, Opladen 1990.
- [Schm_99] Schmidt, A.: XML und das Präsentationsproblem, Manuskript, GMD-SIT, Darmstadt 1999.
- [Seid_93] Seidel, U.: Dokumentenschutz im elektronischen Rechtsverkehr Bestandsaufnahme und Regelungsperspektiven, CR 7/1993 409 - 413 und CR 8/1993, 485-490.
- [SigG_97] Deutscher Bundestag: Gesetz zur digitalen Signatur (Signaturgesetz - SigG), in: Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie: Iukdg Informations- und Kommunikationsdienste-Gesetz - Umsetzung und Evaluierung - Chancen für Wirtschaft, Erwartungen an Verwaltung und Gesetzgebung, Bonn, 1998,
- [SigI_99A2] Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.): Spezifikation zur Entwicklung Interoperabler Verfahren und Komponenten nach SigG/SigV - Signaturinteroperabilitätsspezifikation, SigI, Abschnitt A2, Signatur, Stand: 31.3.1999, Version 4.0, Bonn 1999.
- [SigI_99A3] Bundesamt für die Sicherheit in der Informationstechnik (Hrsg.): Spezifikation zur Entwicklung Interoperabler Verfahren und Komponenten nach SigG/SigV - Signaturinteroperabilitätsspezifikation, SigI, Abschnitt A3, Anwenderinfrastruktur, Stand: 30.4.1999, Version 3.0, Bonn 1999.
- [SigI_99] Bundesamt für die Sicherheit in der Informationstechnik: Spezifikation zur Entwicklung Interoperabler Verfahren und Komponenten nach SigG/SigV - Signaturinteroperabilitätsspezifikation, SigI, Bonn 1999.
- [SigV_97] Deutscher Bundestag: Verordnung zur digitalen Signatur (Signaturverordnung - SigV), in: Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie: Iukdg Informations- und Kommunikationsdienste-Gesetz - Umsetzung und Evaluierung - Chancen für Wirtschaft, Erwartungen an Verwaltung und Gesetzgebung, Bonn
- [Stee_90] Steedman, D.: Abstract Syntax Notation One ASN.1 The Tutorial & Reference, Wiltshire, 1990.
- [TTT_99] TeleTrust: Biester, J. / Bauspieß, F. / Fox, D. (Secorvo Security Consulting GmbH): MailTrust Version 2 Gesamtkonzeption, Aufbau und Komponenten einer PKI, Stand 16.März 1999.
- [W3C_99] W3C: Extensible Forms Description Language (XFDL) 4.0, WWW.W3.org/TK/NOTE-XFDL.
- [Wich_98] Wichert, Michael: BOPD/BAKO - Sicheres Geschäftsprotokoll, GMD-Spiegel 1/98. März 1998.
- [Ziel_95] Zielinski, D.: Urkundenfälschung durch Telefax, CR 5/1995, 286 - 297.