Ludwig-Maximilians-Universität München
Juristische Fakultät
Institut für Politik und Öffentliches Recht

Staatsrechtliches Grundlagenseminar „Verfassungsfragen von Multimedia“ im Wintersemester 1997/98

bei Prof. Dr. Rupert Scholz und Prof. Dr. Peter Lerche

Seminararbeit

Rechtsfragen der Kryptographie und der digitalen Signatur

13. Januar 1998

stud. iur. Wolfgang Kopp

E-Mail: wk@wolfgang-kopp.de

WWW: http://www.wolfgang-kopp.de/

Inhaltsverzeichnis

Rechtsfragen der Kryptographie und der digitalen Signatur

A. Problematik

Die sogenannte Informationsgesellschaft hat neue Formen des menschlichen Handelns hervorgebracht. Wo man früher vertrauliche geschäftliche Verhandlungen „unter vier Augen“ geführt hat, besteht heute die Möglichkeit – und wegen der zunehmenden Globalisierung oft auch die Notwendigkeit –, sich per Telefon oder Videokonferenz zu besprechen. Der persönlich unterschriebene Brief, den man in einen Umschlag steckt und von der Post zu seinem Empfänger befördern läßt, wird von den schnelleren und billigeren Medien Telefax und E-Mail abgelöst. An die Stelle von Bargeld treten andere Zahlungsformen wie Kredit- oder ec-Karte sowie „elektronisches Geld“. Der Mensch in der industrialisierten Welt hat die Reichweite seiner Gestaltungsmöglichkeiten dadurch beträchtlich erhöht.

Doch sind diese neuen Handlungsformen auch mit einem Verlust an persönlicher Unmittelbarkeit verbunden, aus dem sich neue Gefahren ergeben[1]. Technisch übertragene Nachrichten und Gespräche lassen sich viel leichter abhören als persönlich geführte, so daß Geheimnisse leicht an Unbefugte gelangen können[2]. Elektronische Dokumente lassen sich verändern, ohne daß der Inhalt oder überhaupt die Tatsache der Veränderung sich später feststellen ließen. Vielmals ist der Verfasser eines Dokuments, der Absender einer Mitteilung oder sogar der Gesprächspartner gar nicht identifizierbar, weil auch hier Fälschungen mit teilweise geringem Aufwand machbar sind[3]. All dies erzeugt gewaltige Vertrauens- und Beweisprobleme, die ein Hindernis bei der sicheren privaten und kommerziellen Nutzung neuer Kommunikationsformen wie des **Internet**[4] darstellen.

---

[1] so auch *Heuser*; *Huhn/Pfitzmann* in DANA 6/1996, 4, 4, unter 1; *Schmidt/Ungerer* in iX 4/1997, 128, 128; spezifische Gefahren durch Vernetzung beschreibt *Grimm* in DuD 1996, 27, 27 f., unter 1

[2] *Bizer* in KritJ 1995, 450, 450 f., unter 1

[3] *Bizer* in DuD 1997, 203, 203, vor 1.1; *Bizer/Fox* in DuD 1997, 66, 66; BT-Drs. 13/7385 vom 9. April 1997, im Internet: http://www.fitug.de/ulf/politik/iukdg.html , Begründung zu Art. 3, unter B II; *Engel-Flechsig/Maennel/Tettenborn* in NJW 1997, 2981, 2988, unter V 1; *Roßnagel* in DuD 1997, 75, 75, unter „Entstehungsgeschichte“

[4] vgl. dazu *Beyer/Katzenschwanz*; *Köhntopp* in Rost, 20 ff.; *Schwarz*

Eine technische Möglichkeit zur Lösung solcher Probleme stellt die wissenschaftliche Disziplin der **Kryptographie** dar. Da Kryptographie und die damit zusammenhängenden Fragen derzeit weitgehend eine Domäne der Mathematiker und Informatiker sind, soll zunächst versucht werden, einen Überblick über Grundlagen und Anwendungsmöglichkeiten der Kryptographie zu geben (B), bevor dann darauf aufbauend auf einige aktuelle Probleme eingegangen wird und bestehende und denkbare rechtliche Lösungen untersucht werden (C).

B. Grundlagen und Anwendungen der Kryptographie

I. Einführung

1. Terminologie

Kryptographie ist die wissenschaftliche Disziplin, die sich damit beschäftigt, wie man den Inhalt von Nachrichten verheimlicht, sie also vor unbefugter Kenntnisnahme absichert[5]. Unter **Kryptanalyse** versteht man dagegen die Kunst, eine Verschlüsselung zu brechen, also den geheimen Inhalt einer abgesicherten Nachricht unbefugt lesbar zu machen[6]. Der Oberbegriff für beide Disziplinen ist **Kryptologie**[7]; diese Wissenschaft gilt als Teilgebiet der (angewandten) Mathematik[8].

Eine nicht abgesicherte Nachricht bezeichnet man als **Klartext**, eine abgesicherte Nachricht als **Chiffretext**. Die **Verschlüsselung** (Chiffrierung) überführt Klartext in Chiffretext, die **Entschlüsselung** (Dechiffrierung) erzeugt aus dem Chiffretext wieder den ursprünglichen Klartext[9].

2. Historischer Überblick

Seit es Menschen gibt, gibt es Geheimnisse. Man verbarg sie, indem man sie für sich behielt oder Aufzeichnungen darüber an geheimen oder sicheren Orten versteckte und ihre Existenz geheimhielt. War dies jedoch nicht möglich, zum Beispiel weil eine geheime Botschaft über unsicheres Gebiet transportiert werden sollte, so benutzte man schon im Altertum kryptographische Verfahren[10].

Die berühmteste Verschlüsselung überhaupt dürfte die von *Gaius Iulius Caesar* ersonnene Methode sein, mit der er geheime Nachrichten vor neugierigen Augen schützte: Jeder Buchstabe wurde zum Verschlüsseln um drei Positionen im Alphabet verschoben, so daß aus einem A im Klartext ein D im Chiffretext, aus einem B ein E wurde und so weiter[11].

---

[5] *Bauer*, unter 1.1, S. 5; *Beutelspacher*, vor 1.1, S. 10; *Schneier*, unter 1.1, S. 1

[6] *Bauer*, vor 1, S. 4; *Beutelspacher*, vor 1.1, S. 10; *Schneier*, unter 1.1, S. 1

[7] vgl. die Nachw. bei Fn. 6

[8] *Bauer*, vor 1, S. 2; *Schneier*, unter 1.1, S. 1

[9] *Schneier*, unter 1.1, S. 1; „Geheimtext“ statt „Chiffretext“: *Bauer*, unter 2.2, S. 26; *Beutelspacher*, vor 1.1, S. 11

[10] *Grimm* in DuD 1996, 27, 28, unter 2

[11] *Beutelspacher*, unter 1.2, S. 13; *Schneier*, unter 1.3, S. 12

Die älteste heute bekannte Verschlüsselung stellt jedoch die **Skytale** von Sparta (5. Jhdt. v. Chr.) dar: Ein Holzstab wurde mit einem Pergamentstreifen umwickelt, der dann der Länge nach mit einer geheimen Nachricht der spartanischen Regierung beschrieben wurde. Den Text auf dem abgewickelten Pergamentstreifen sollten nur die Generäle lesen können, die über Stäbe von gleichem Durchmesser verfügten[12].

Im Laufe der folgenden Jahrhunderte bildete sich langsam die kryptologische Wissenschaft heraus. Während sie ihre Anwendungen lange Zeit hauptsächlich im militärischen, diplomatischen und geheimdienstlichen Bereich fand, haben sich mit dem Aufkommen zunächst der Telegraphen- und dann der Computertechnologie sowohl Möglichkeiten als auch Bedürfnisse zur privaten und vor allem kommerziellen Anwendung gezeigt[13].

In der Zeit nach dem ersten Weltkrieg hatte sich die kryptographische Forschung zwar immer stärker in den nichtöffentlichen militärischen Bereich verlagert, doch erschienen seit 1967 wieder viele kryptographische Arbeiten in öffentlich zugänglichen Publikationen[14]. Den endgültigen Durchbruch zum Einsatz kryptographischer Verfahren auf breiter Front dürften die Entdeckung der sogenannten **asymmetrischen Kryptographie** durch *Diffie* und *Hellman* im Jahre 1976[15] und die Einführung des amerikanischen **Data Encryption Standard** (DES)[16] im folgenden Jahr gebracht haben.

3. Ziele der Kryptographie

An moderne kryptographische Verfahren werden im wesentlichen vier Anforderungen gestellt[17]. Sie müssen nicht bei jeder Anwendung gleichzeitig erfüllt werden.

- **Vertraulichkeit:** Der Inhalt eines Dokuments soll nur von dazu befugten Personen gelesen werden können.
- **Integrität:** Der Inhalt eines Dokuments soll nicht unbemerkt verändert werden können.

[12] *Bauer*, unter 6.3, S. 86; *Beutelspacher*, unter 1.1, S. 11 f.; *Schmidt/Ungerer* in iX 4/1997, 128, 128 und 130

[13] näher *Beutelspacher*, S. 2 f.; *Bauer*, vor 1, S. 4

[14] Schneier–*Diffie*, S. xiii

[15] *Diffie/Hellman* in Trans. IEEE Inform. Theory 1976, 644

[16] s.u. B IV 1

[17] vgl. dazu *Schneier*, unter 1.1, S. 2

- **Authentikation:** Der Urheber eines Dokuments soll feststellbar sein; kein anderer soll sich als Urheber ausgeben können.
- **Verbindlichkeit:** Der Urheber eines Dokuments soll seine Urheberschaft nicht abstreiten können.

Ein weiteres Ziel kann in manchen Situationen **Anonymität** sein. Damit ist die Vertraulichkeit nicht des Nachrichteninhalts, sondern sogar des Kommunikationsvorgangs als solchem gemeint[18].

II. Kryptographische Theorie

1. Grundbegriffe

a) Algorithmen und Schlüssel

Um Kryptographie tatsächlich anwenden zu können, müssen sich Sender und Empfänger auf ein bestimmtes Verfahren einigen, das sie verwenden wollen, z. B. die oben erwähnte Caesar-Chiffre oder die Skytale[19]; das ist der **Algorithmus**. Wäre das Wissen um den verwendeten Algorithmus aber alles, was zur Entschlüsselung notwendig ist, so ließe sich Kryptographie praktisch nicht verwenden, da etwa bei einer Implementierung in Software jedermann Einsicht in das Verfahren nehmen und somit abgesicherte Nachrichten unbefugt mitlesen könnte. Dem Verfahren wird deshalb ein variabler Parameter hinzugefügt, der sogenannte **Schlüssel**. Auch auf diesen müssen die Beteiligten sich einigen, er bleibt jedoch ihr Geheimnis und ist auch innerhalb eines Algorithmus veränderlich.

Bei der Caesar-Chiffre etwa wäre der Schlüssel die Anzahl der Zeichen, um die der Klartext verschoben wird, bei der Skytale der Durchmesser des Stabes. Selbst wenn nun jemand das verwendete Verfahren kennt, kann er verschlüsselte Nachrichten nicht ohne weiteres lesen. Es liegt natürlich auf der Hand, daß sich bei den beiden als Beispiel dienenden Algorithmen durch Testen aller möglichen Schlüssel die Nachricht letztlich entziffern läßt; dagegen hilft nur eine Erweiterung der Auswahl an möglichen Schlüsseln, des sogenannten **Schlüsselraums**, durch Verwendung eines besseren Algorithmus. Die

[18] *Beutelspacher*, unter 6.1, S. 149

[19] s.o. B I 2

Gesamtheit eines Algorithmus und aller zu ihm kompatiblen Schlüssel, Klartexte und Chiffretexte nennt man ein **Kryptosystem**[20].

b) Die Maxime von Kerckhoffs

Aus der Tatsache, daß stets die Möglichkeit – und oft sogar die Gewißheit – besteht, daß der verwendete Algorithmus einem möglichen Angreifer bekannt wird, folgt eine der wichtigsten Grundregeln der kryptologischen Wissenschaft, die sogenannte **Maxime von Kerckhoffs**[21]:

Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung des Algorithmus, sondern ausschließlich von der Geheimhaltung des Schlüssels abhängen.

Da es also ohnehin keinen Sinn macht, einen Algorithmus geheimzuhalten, wird in der kryptologischen Wissenschaft die Veröffentlichung eines Algorithmus als wichtigste Voraussetzung angesehen, um ihn als sicher einschätzen zu können. Denn nur eine Überprüfung durch die gesamte wissenschaftliche Gemeinschaft und insbesondere durch ausgiebige Kryptanalyse kann Schwächen eines Algorithmus hinreichend zuverlässig aufdecken[22].

c) Funktionsprinzipien moderner Chiffrieralgorithmen

Es gibt grundsätzlich zwei Möglichkeiten, eine Nachricht zu chiffrieren: Bei der **Substitution** wird ein Zeichen im Klartext durch ein anderes Zeichen im Chiffretext ersetzt (wie bei der Caesar-Chiffre), während bei der **Transposition** alle Klartextzeichen erhalten bleiben und lediglich eine neue Anordnung im Chiffretext erhalten (wie bei der Skytale)[23]. Gute Algorithmen arbeiten zumeist mit einer Kombination dieser beiden Verfahren[24].

Man unterscheidet außerdem zwischen **Block- und Stromchiffren**. Stromchiffren eignen sich gut für die Implementierung in Hardware und zum Verschlüsseln von Echtzeit-

[20] *Schneier*, unter 1.1, S. 4; eine mathematische Definition findet sich bei *Bauer*, unter 2.3, S. 27 f.

[21] *Bauer*, unter 10.2.3, S. 149 f.; *Beutelspacher*, unter 1.6, S. 23; *Schneier*, unter 1.1, S. 6 und 8

[22] *Bauer*, unter 10.2.2, S. 148 f.; *Schneier*, unter 1.1, S. 8

[23] *Beutelspacher*, unter 1.1, S. 12; *Schneier*, unter 1.3, S. 11 ff.; mathematisch *Bauer*, unter 3 ff., S. 36 ff.

[24] *Schneier*, unter 1.3, S. 11

Kommunikation, Blockchiffren dagegen lassen sich gut in Software implementieren und zum Verschlüsseln großer Datenmengen auf einmal einsetzen[25].

Wichtige Kenngrößen für Algorithmen sind die **Schlüssellänge** und – bei Blockchiffren – die Größe der Datenblöcke, die jeweils pro Durchlauf bearbeitet werden. Sowohl Schlüssellänge als auch **Blocklänge** werden in Bit angegeben.

2. Symmetrische und asymmetrische Algorithmen

a) Symmetrische Algorithmen

Symmetrische Kryptographie ist gleichsam die Grundform der Verschlüsselung. Sender und Empfänger haben sich dabei meist auf einen Schlüssel geeinigt, den der Sender zur Verschlüsselung und der Empfänger zur Entschlüsselung der Nachricht verwendet[26].

Dieses Prinzip wirft folgende Frage auf[27]: Wenn Sender und Empfänger über einen sicheren Kommunikationskanal verfügen, den sie ja zur Schlüsselvereinbarung benötigen, wozu brauchen sie dann Kryptographie? Darauf gibt es mehrere Antworten. Zum einen ist der Schlüssel oft nur eine sehr kurze Information, die leichter sicher zu übermitteln ist als viele, vergleichsweise lange Nachrichten. Und zum anderen können die Beteiligten den Zeitpunkt für den Schlüsselaustausch frei wählen und später sicher kommunizieren, auch wenn ihnen *dann* kein sicherer Kanal mehr zur Verfügung steht. Die Notwendigkeit eines sicheren Kanals bleibt jedoch ein Manko symmetrischer Kryptographie.

b) Asymmetrische Algorithmen

Asymmetrische Kryptographie schafft hier (teilweise) Abhilfe. Bei asymmetrischen Algorithmen verfügt jeder Beteiligte über *zwei* zusammengehörige Schlüssel: einen, mit dem Nachrichten an ihn verschlüsselt werden können, und einen, mit dem er derart verschlüsselte Nachrichten entschlüsseln kann. Es ist nicht möglich, mit dem Verschlüsselungsschlüssel Nachrichten zu entschlüsseln, die mit diesem erzeugt wurden; nur der Besitzer des Entschlüsselungsschlüssels kann dies. Auch ist es nicht möglich, den Entschlüsselungsschlüssel aus dem Verschlüsselungsschlüssel herzuleiten. Letzterer

[25] *Schneier*, unter 9.13, S. 249 f.

[26] *Bauer*, unter 11.1.1, S. 154; *Beutelspacher*, vor 1.1, S. 10; *Gerling* in DuD 1997, 197, 198, unter 3; *Grimm* in DuD 1996, 27, 28, unter 3; *Huhn/Pfitzmann* in DANA 6/1996, 4, 5, unter 2.1; *Ohst*, unter 5; *Schneier*, unter 1.1, S. 4 f. Möglich ist auch, daß zwei Schlüssel verwendet werden, wobei sich aber jeder aus dem anderen berechnen läßt, vgl. *Schneier*, aaO.

[27] vgl. *Beutelspacher*, unter 1.2, S. 15 f.; *Ohst*, unter 5; *Schmidt/Ungerer* in iX 4/1997, 128, 130

kann daher veröffentlicht werden und wird auch als **öffentlicher Schlüssel** (*public key*) bezeichnet. Geheimgehalten werden muß nur der Entschlüsselungsschlüssel, der daher **privater Schlüssel** (*private key*) heißt[28].

Der Vorteil dieses Systems liegt auf der Hand: Eine Person, die die Möglichkeit schaffen will, ihr verschlüsselte Nachrichten zu senden, braucht nur ein Schlüsselpaar zu erzeugen und den öffentlichen Schlüssel möglichst vielen anderen Personen zugänglich zu machen, etwa durch Hinterlegung in einer frei einsehbaren Datenbank (*Keyserver*). Jeder, der nun eine verschlüsselte Nachricht an diese Person schicken will, besorgt sich den öffentlichen Schlüssel, verschlüsselt seine Nachricht damit und verschickt den Chiffretext. Die Nachricht kann dann nur vom Empfänger mit dessen privatem Schlüssel wieder entschlüsselt werden[29].

Es ist zwar nicht möglich, durch Kenntnis des öffentlichen Schlüssels die Nachricht zu entschlüsseln. Doch ist ohne weitere Absicherung des Systems ein anderer Angriff möglich: Jemand könnte sich als ein anderer ausgeben und unter dessen Namen einen öffentlichen Schlüssel verbreiten, den er selbst zusammen mit dem zugehörigen privaten Schlüssel erzeugt hat. Werden Nachrichten mit diesem falschen öffentlichen Schlüssel verschlüsselt und an den vermeintlichen Empfänger geschickt, so braucht der Angreifer nur die Möglichkeit zu haben, diese Nachrichten abzufangen. Er ist dann in der Lage, mit Hilfe des ihm bekannten (weil ebenfalls von ihm erzeugten) privaten Schlüssels die Nachricht lesbar zu machen[30]. Dieses Problem ist allerdings lösbar[31].

c) Hybridsysteme

Asymmetrische Algorithmen haben wie gesehen den Vorteil, daß vor der Kommunikation kein Schlüsselaustausch stattfinden muß. Auch wird ein Problem vermieden, das bei der Verwendung symmetrischer Kryptographie in größeren Personengruppen entsteht: Soll jeder Teilnehmer wirklich nur an ihn gerichtete Nachrichten lesen können, so ist für jedes mögliche Sender-Empfänger-Paar innerhalb einer Gruppe ein eigener Schlüssel nötig, das sind bei 1000 Teilnehmern bereits 499.500 Schlüssel. Bei der Verwendung

---

[28] *Bauer*, unter 11.1.2, S. 154 f.; *Beutelspacher*, unter 5.1, S. 114; *Gerling* in DuD 1997, 197, 198, unter 4; *Grimm* in DuD 1996, 27, 29 f., unter 4; *Schneier*, unter 1.1, S. 5. Manchmal wird der private Schlüssel auch als geheimer Schlüssel (*secret key*) bezeichnet, was jedoch, um Verwechslungen mit symmetrischen Algorithmen auszuschließen, vermieden werden sollte, vgl. *Schneier*, aaO.

[29] *Bauer*, unter 11.1.2, S. 155; *Beutelspacher*, unter 5.1, S. 115 f.; *Grimm* in DuD 1996, 27, 28, unter 2; *Huhn/Pfitzmann* in DANA 6/1996, 4, 6, unter 2.1; *Ohst*, unter 6; *Schmidt/Ungerer* in iX 4/1997, 128, 130

[30] vgl. *Grimm* in DuD 1996, 27, 30 f., unter 6; *Schneier*, unter 3.1, S. 58 f.

[31] s.u. B II 3 c

asymmetrischer Kryptographie dagegen braucht man für jede Person nur zwei Schlüssel, um diese Voraussetzung zu erfüllen, also im Beispielfall 2000 Schlüssel[32].

Es gibt jedoch auch einen wichtigen Nachteil asymmetrischer Algorithmen: Alle heute bekannten Implementierungen sind wesentlich langsamer als symmetrische Verschlüsselung[33]. Dies ist der Hauptgrund[34] dafür, daß in der Praxis ganz überwiegend eine Kombination aus symmetrischer und asymmetrischer Verschlüsselung angewendet wird, die sogenannten **Hybridsysteme**[35].

Dabei erzeugt der Sender einen zufälligen **Sitzungsschlüssel** für den symmetrischen Algorithmus, den er dann mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Nun schickt er dem Empfänger den Sitzungsschlüssel und die damit verschlüsselte Nachricht zu. Der Empfänger kann mit seinem privaten Schlüssel den chiffrierten Sitzungsschlüssel dechiffrieren und mit diesem dann die eigentliche Nachricht lesen. Die durch den Sitzungsschlüssel entstehenden Zwischenschritte werden normalerweise von der Software für den Benutzer unbemerkt vorgenommen, so daß sich für diesen kein Mehraufwand ergibt. Er kommt mit dem Sitzungsschlüssel nie in Kontakt; für ihn stellt sich das ganze Verfahren wie die normale Kommunikation mit asymmetrischer Kryptographie dar.

Der Vorteil liegt darin, daß der Sitzungsschlüssel normalerweise viel kleiner ist als die Nachricht, so daß die geringe Geschwindigkeit asymmetrischer Algorithmen kaum ins Gewicht fällt. Mit Hybridsystemen läßt sich asymmetrische Kryptographie sogar für sehr zeitkritische Anwendungen wie die Verschlüsselung von Echtzeit-Datenströmen (ISDN- oder Internet-Telefonie, Videokonferenzen usw.) einsetzen.

3. Authentikationssysteme

Bisher war nur von Kryptosystemen die Rede, mit deren Hilfe man Nachrichten vor unbefugtem Mitlesen absichern kann. Solche Systeme dienen dem Ziel der Vertraulichkeit[36]

---

[32] *Bauer*, unter 11.1.1 f., S. 154 f.; *Beutelspacher*, unter 5.1, S. 118; *Ohst*, unter 5 f.

[33] *Beutelspacher*, unter 5.1, S. 118; *Grimm* in DuD 1996, 27, 30, unter 4; Faktor 100 bis 1000 höherer Rechenaufwand: *Huhn/Pfitzmann* in DANA 6/1996, 4, 6, unter 2.1; symmetrische Algorithmen mindestens um den Faktor 1000 schneller: *Schneier*, unter 2.5, S. 39

[34] vgl. daneben *Schneier*, unter 2.5, S. 39

[35] *Beutelspacher*, unter 5.4, S. 136 ff.; *Gerling* in DuD 1997, 197, 199, unter 4; *Grimm* in DuD 1996, 27, 30, unter 4; *Huhn/Pfitzmann* in DANA 6/1996, 4, 6, unter 2.1; *Schmidt/Ungerer* in iX 4/1997, 128, 131; *Schneier*, unter 2.5, S. 38 ff.

[36] s.o. B I 3

und heißen **Konzelationssysteme** (lat. *celare*: verbergen, verheimlichen). Moderne kryptographische Verfahren lassen sich aber auch einsetzen, um die anderen drei Ziele – Integrität, Authentikation und Verbindlichkeit – zu erreichen. Man spricht dabei von **Authentikationssystemen**[37].

a) Symmetrische Authentikationssysteme

Ein symmetrisches Authentikationssystem funktioniert wie folgt[38]: Der Sender berechnet aus der Nachricht mit Hilfe einer sogenannten **Einwegfunktion** einen vergleichsweise kleinen Datenblock, den man **Hashwert** nennt[39]. Es ist nicht möglich, ohne Kenntnis der Nachricht eine zu einem solchen Hashwert passende Nachricht zu finden. Auch ist es praktisch nicht möglich, zwei Nachrichten zu finden, die denselben Hashwert haben[40]. Nun verschlüsselt der Sender den Hashwert mit dem vereinbarten Schlüssel und sendet Nachricht und verschlüsselten Hashwert an den Empfänger. Der Empfänger kann dann den Hashwert durch Dechiffrierung wieder herstellen. Durch erneute Anwendung der (öffentlichen) Einweg-Hashfunktion auf die Nachricht und Vergleich des Ergebnisses mit dem entschlüsselten Hashwert kann er feststellen, ob die Nachricht während der Übertragung verändert wurde. Denn ein Angreifer könnte zwar die Nachricht verändern und aus der neuen Nachricht den zugehörigen Hashwert berechnen. Er ist jedoch nicht dazu in der Lage, diesen neuen Hashwert korrekt zu verschlüsseln, da er den zwischen Sender und Empfänger vereinbarten Schlüssel nicht kennt. Jede Veränderung der Nachricht muß dem Empfänger also auffallen, weil die Nachricht dann nicht mehr zum Hashwert paßt.

Ein solches System hat einige Nachteile. Zum einen kann nur eine Person, die den geheimen Schlüssel kennt, eine solche Überprüfung vornehmen; wünschenswert wäre aber in vielen Situationen, daß jeder Beliebige die Echtheit einer Nachricht überprüfen kann. Zum anderen kann jeder, der über den zur Überprüfung nötigen Schlüssel verfügt, auch authentifizierte Nachrichten erstellen. Das bedeutet, daß das System in Gruppen von mehr als zwei Teilnehmern dem Empfänger keine Auskunft mehr darüber gibt, von *wem* eine bestimmte Nachricht eigentlich stammt, und daß es auch bei nur zwei Teilnehmern stets möglich ist, das Erstellen einer bestimmten Nachricht abzustreiten: Den Hashwert

---

[37] *Huhn/Pfitzmann* in DANA 6/1996, 4, 7, unter 2.2

[38] *Beutelspacher*, unter 4.2.1, S. 82 ff.; *Huhn/Pfitzmann* in DANA 6/1996, 4, 7, unter 2.2

[39] vgl. zu Hashfunktionen und ihrer Sicherheit *Dobbertin* in DuD 1997, 82 ff.

[40] *Bauer*, unter 11.2, S. 156 ff.; *Beutelspacher*, unter 4.2.1, S. 85; *Schneier*, unter 2.3, S. 34 f.

könnte genau so gut der Kommunikationspartner verschlüsselt haben, denn auch er hat den Schlüssel[41]. Integrität und Authentizität einer Nachricht werden also nur gegen Angriffe von außenstehenden Personen gesichert, Verbindlichkeit dagegen wird überhaupt nicht erreicht.

b) Asymmetrische Authentikationssysteme

Asymmetrische Systeme umgehen diese Schwierigkeiten. Solchermaßen authentifizierte Nachrichten ähneln in ihren Eigenschaften unterschriebenen Schriftstücken, weshalb in diesem Zusammenhang auch von **digitalen Signaturen** die Rede ist[42].

Bei einem asymmetrischen Authentikationssystem besitzt jeder Teilnehmer – wie auch beim asymmetrischen Konzelationssystem – zwei Schlüssel: einen privaten Signaturschlüssel und einen öffentlichen Prüfschlüssel. Will jemand eine Nachricht als von ihm erstellt ausweisen („unterzeichnen"), so berechnet er den Hashwert einer Nachricht und verschlüsselt diesen mit seinem Signaturschlüssel. Jeder, der im Besitz des zugehörigen öffentlichen Prüfschlüssels ist, kann nun die Echtheit der Nachricht überprüfen, sie **verifizieren**. Unterzeichnen kann die Nachricht allerdings nur der Besitzer des privaten Signaturschlüssels, so daß Integrität, Authentikation und Verbindlichkeit realisiert werden können.

c) Zertifizierungsstrukturen

Noch bleibt das bei den Konzelationssystemen bereits angesprochene[43] Problem zu lösen, daß kein nachvollziehbarer Zusammenhang zwischen einem öffentlichen Schlüssel und der vorgeblich zu ihm gehörenden Person besteht. Jemand kann sich als eine andere Person ausgeben, indem er unter deren Namen einen selbst erzeugten öffentlichen Schlüssel – sei es einen Authentikations- oder einen Konzelationsschlüssel – in Umlauf bringt. In anderen sozialen Strukturen wird das Problem des Vortäuschens einer anderen Identität dadurch gelöst, daß ein **vertrauenswürdiger Dritter** eingeschaltet wird, der sich für die Identität einer Person verbürgt. Dies kann z. B. ein Freund oder Bekannter, eine Organisation, ein Wirtschaftsunternehmen oder eine staatliche Stelle sein. Dadurch wird

[41] *Grimm* in DuD 1996, 27, 28, unter 3

[42] vgl. dazu *Bauer*, unter 11.1.2, S. 155 f.; *Beutelspacher*, unter 5.2, S. 119; *Grimm* in DuD 1996, 27, 29 f., unter 4; *Huhn/Pfitzmann* in DANA 6/1996, 4, 7, unter 2.2; *Schmidt/Ungerer* in iX 4/1997, 128, 131; *Schneier*, unter 2.6, S. 41 ff.

[43] s.o. B II 2 b a.E.

eine Beziehung zum sozialen Umfeld hergestellt, die es erst ermöglicht, von Identität zu sprechen[44].

Dieses Verbürgen läßt sich mit Hilfe digitaler Signaturen auch im Rahmen kryptographischer Systeme realisieren[45]. Der vertrauenswürdige Dritte unterzeichnet eine Nachricht, in der er zusichert, daß ein bestimmter öffentlicher Schlüssel zu einer bestimmten sozialen Person gehört. Jeder, der dem Dritten vertraut und diese Nachricht liest, kann sich sicher sein, daß er seine Nachrichten an eine bestimmte Person tatsächlich mit deren öffentlichem Schlüssel verschlüsselt bzw. daß eine zu dem genannten Prüfschlüssel passende Nachricht tatsächlich von dieser Person unterzeichnet wurde. Die Zusicherung des Dritten wird **Zertifikat** genannt; das Format solcher Zertifikate läßt sich standardisieren, so daß sie automatisch auswertbar sind. Bei dem vertrauenswürdigen Dritten spricht man oft auch von einer **Zertifizierungsinstanz**.

Das Problem wird also darauf reduziert, daß ein Benutzer vertrauenswürdige Zertifizierungsinstanzen finden und deren Schlüssel ihnen zweifelsfrei zuordnen können muß. Dazu ist zumindest anfangs persönlicher Kontakt oder ein sonstiger sicherer Kommunikationskanal nötig.

III. Kryptanalyse

Auch und gerade für den Juristen besonders interessant ist die Frage, wie verläßlich und sicher kryptographische Algorithmen, insbesondere für digitale Signaturen verwendete, eigentlich sind. Diese Frage läßt sich nur beantworten, wenn man sich mit den Grundlagen der Kryptanalyse vertraut macht.

1. Ziele der Kryptanalyse

Kryptanalyse kann auf eines oder mehrere der folgenden Ziele gerichtet sein[46].

- **Vollständiges Aufbrechen:** Der geheime Schlüssel wird ermittelt, so daß jede mit diesem Algorithmus und Schlüssel chiffrierte Nachricht lesbar wird.
- **Globale Deduktion:** Der Kryptanalytiker findet ohne Ermittlung des Schlüssels ein Verfahren, mit dem sich aus jedem Chiffretext der zugehörige Klartext ermitteln läßt.

[44] *Grimm* in DuD 1996, 27, 30 f., unter 6

[45] vgl. dazu BT-Drs. 13/7385 (s.o. Fn. 3), Begründung zu Art. 3, unter B I; *Fox* in DuD 1997, 106, 106; *Grimm* in DuD 1996, 27, 31, unter 6; *Schneier*, unter 8.12, S. 219 ff.

[46] *Schneier*, unter 1.1, S. 9

- **Lokale Deduktion:** Der Klartext zu einem bestimmten Chiffretext wird ermittelt.
- **Informationsdeduktion:** Informationen über den Schlüssel oder den Klartext werden dem Kryptanalytiker bekannt.

2. Mögliche Angriffe

a) Angriffsformen

Einem Angreifer, der versucht, ein kryptographisches System zu brechen, stehen je nach seiner Situation verschiedene Informationen zur Verfügung. Danach werden auch verschiedene Angriffsarten unterschieden[47].

- **Ciphertext-only-Angriff:** Dies ist geradezu der klassische Angriff. Der Kryptanalytiker verfügt nur über eine bestimmte Menge von jeweils mit demselben Algorithmus erzeugtem Chiffretext.
- **Known-plaintext-Angriff:** Neben dem Chiffretext verschiedener Nachrichten ist auch dazugehörender Klartext vorhanden.
- **Chosen-plaintext-Angriff:** Der Angreifer hat die Möglichkeit, von ihm gewählte Klartextblöcke mit dem zu analysierenden Algorithmus und Schlüssel chiffrieren zu lassen. Einen Unterfall stellt der *adaptive-chosen-plaintext*-Angriff dar: Der Kryptanalytiker kann bei der Auswahl der zu verschlüsselnden Klartexte auch die Ergebnisse vorangehender *chosen-plaintext*-Angriffe berücksichtigen.
- **Chosen-ciphertext-Angriff:** Hier kann der Analytiker Chiffretexte zur Dechiffrierung auswählen und er hat auch Zugriff auf den entschlüsselten Klartext. Sein Ziel ist es, den Schlüssel zu ermitteln.

Gute kryptographische Verfahren müssen all diesen Angriffsarten möglichst viel Widerstand entgegensetzen.

Daneben kommt die Ermittlung von Schlüssel oder Klartext durch Bedrohung, Erpressung, Folter oder Bestechung in Frage. Doch hängt der Erfolg solcher Angriffe natürlich nicht von der Sicherheit des verwendeten Kryptosystems ab.

[47] *Schneier*, unter 1.1, S. 6 ff.; zur speziellen Terminologie für Authentikationssysteme vgl. *Fox* in DuD 1997, 69, 70, unter 2

b) Brute-force-Angriff und sichere Schlüssellängen

Von dieser Form der „Kryptanalyse mit Gewalt“ ist der sogenannte **brute-force-Angriff** („Angriff mit roher Gewalt“) zu unterscheiden, der der wissenschaftlichen Kryptanalyse zuzuordnen ist. Er stellt einen Unterfall des *ciphertext-only*-Angriffs dar und wird durch Entschlüsselung des Chiffretextes mit allen in Frage kommenden Schlüsseln (exhaustive Suche) realisiert[48]. Sobald sich bei der Entschlüsselung ein Klartext ergibt, der „Sinn macht“, ist der richtige Schlüssel gefunden.

Dieser Angriff ist zwar der schwächste denkbare, läßt sich aber theoretisch gegen jedes kryptographische Verfahren anwenden. Je höher die Anzahl der möglichen Schlüssel jedoch ist, desto länger dauert die Suche nach dem richtigen Schlüssel. Daher ist die Schlüssellänge ein wichtiges Maß für die Beurteilung der Sicherheit eines Verfahrens. Obwohl es vielleicht nicht möglich ist, einen besseren als den *brute-force*-Angriff durchzuführen, verbleibt immer die Restwahrscheinlichkeit, daß ein solcher erfolgreich sein wird. Sie kann durch die Wahl eines hinreichend langen Schlüssels minimiert werden.

Schätzungen, wie lange ein *brute-force*-Angriff auf einen Schlüssel bestimmter Länge dauern würde, werden dadurch erheblich erschwert, daß zukünftige Fortschritte in der Rechnertechnologie heute noch nicht absehbar sind. Im Bereich der symmetrischen Algorithmen gibt es bereits erfolgreiche *brute-force*-Angriffe gegen 40- und 48-Bit-Schlüssel durch Kooperation vieler Rechner über das Internet[49]. *Schneier* schätzt, daß das Brechen von 56-Bit-Schlüsseln bereits heute innerhalb des Budgets großer Unternehmen und krimineller Vereinigungen liegt und 64-Bit-Schlüssel von großen Industrienationen gebrochen werden können. 80-Bit-Schlüssel könnten innerhalb der nächsten 30 Jahre in diesen Bereich geraten, während 112- und erst recht 128-Bit-Schlüssel auf nicht absehbare Zeit als sicher gelten müßten[50]. 256-Bit-Schlüssel schließlich sind aufgrund der Gesetze der Thermodynamik wohl nicht von Computern zu brechen, die aus Materie bestehen und eine räumliche Ausdehnung besitzen[51]. Für asymmetrische Algorithmen, also vor allem auch im Bereich der digitalen Signaturen, gelten andere Werte[52].

---

[48] *Bauer*, unter 12.5, S. 178 ff.; *Schneier*, unter 1.1, S. 9

[49] vgl. http://www.klammeraffe.org/challenge/text.html

[50] *Schneier*, unter 7.1, S. 179 ff.

[51] *Schneier*, unter 7.1, S. 185

[52] für RSA s.u. B IV 3

3. One-Time-Pads

Es gibt ein Verfahren, das sogar gegen den *brute-force*-Angriff vollständig immun ist. Jedes Zeichen im Klartext wird dabei mit einem zufällig erzeugten Zeichen verknüpft[53]. Das Ergebnis dieser Verknüpfungen ist der Chiffretext, die Folge der Zufallszeichen ist der Schlüssel. Der Schlüssel ist dabei genau so lang wie der Klartext bzw. der Chiffretext.

Aus diesem Prinzip ergibt sich, daß ein Chiffretext einer bestimmten Länge *jeden beliebigen* Klartext der gleichen Länge repräsentieren kann. Selbst bei Ermittlung aller möglichen Klartexte – das sind alle nur möglichen Zeichenfolgen dieser Länge, einschließlich aller sinnvollen – weiß der Angreifer also nicht, wie der wirkliche Klartext lautet. Dieser sogenannte One-Time-Pad-Algorithmus ist nicht nur praktisch, sondern auch theoretisch sicher. Ohne Ermittlung des Klartextes oder des Schlüssels ist es *unmöglich*, aus dem Chiffretext auf den Klartext zu schließen, selbst mit beliebigem technischem Aufwand[54].

Dieser Algorithmus hat jedoch auch einen so gravierenden Nachteil, daß er in der Praxis fast nicht eingesetzt wird: Für jedes übertragene Zeichen Klartext muß auch ein Zeichen des Schlüssels zwischen Sender und Empfänger auf einem sicheren Kanal übertragen werden. Damit liegt der einzige Vorteil, den die Verschlüsselung noch bietet, in der freien Wahl des Zeitpunkts zum Schlüsselaustausch. One-Time-Pads werden nur da eingesetzt, wo möglichst perfekte Sicherheit verlangt wird und ausreichende Möglichkeiten zum sicheren Schlüsselaustausch zur Verfügung stehen[55]. Sie eignen sich deshalb auch nur schlecht für Übertragungen großer Datenmengen.

IV. Einzelne bedeutende Algorithmen

Im folgenden werden einige ausgewählte symmetrische und asymmetrische Algorithmen vorgestellt, die heute in der Praxis von besonderer Bedeutung sind.

1. DES

Der amerikanische **Data Encryption Standard (DES)** von 1977 beruht auf einem von IBM seit Beginn der 70er Jahre entwickelten Algorithmus[56]. Er wurde im Rahmen einer

[53] vgl. dazu *Bauer*, unter 8.6, S. 117 ff.; *Beutelspacher*, unter 3.3, S. 63 ff.; *Schneier*, unter 1.5, S. 17 ff.

[54] sehr anschaulich *Schneier*, unter 1.5, S. 20

[55] *Beutelspacher*, unter 8.6, S. 65 f.; *Schneier*, unter 1.5, S. 19

[56] zu DES ausführlich *Schneier*, unter 12, S. 309 ff.

öffentlichen Ausschreibung des National Bureau of Standards (NBS, heute NIST) ausgewählt und von dem mit der Überwachung der internationalen Nachrichtenstrecken betrauten und kryptologisch überragend kompetenten Geheimdienst **NSA** (National Security Agency)[57] untersucht und teilweise verändert. Es handelt sich um eine symmetrische Blockchiffre mit einer Blocklänge von 64 und einer Schlüssellänge von 56 Bit.

DES hat sich in Amerika als Standard zur Verschlüsselung von Daten durchgesetzt, obwohl es stets Kritik an der Herabsetzung der Schlüssellänge von 128 auf nur 56 Bit durch die NSA und der Geheimhaltung der Designkriterien für die von der NSA vorgenommenen Veränderungen gab[58]. Es dürfte sich um den meist analysierten kryptographischen Algorithmus überhaupt handeln, und er gilt heute noch als recht sicher. Allerdings muß mittlerweile bei pessimistischer Betrachtung davon ausgegangen werden, daß DES keinen Schutz vor Angriffen durch große Regierungen bietet[59].

2. IDEA

Der **International Data Encryption Algorithm (IDEA)** stammt aus dem Jahr 1991[60]. Er wurde trotz seines geringen Alters bereits vielen Analysen unterzogen und gilt als einer der sichersten verfügbaren Algorithmen. IDEA ist eine symmetrische Blockchiffre mit einer Blocklänge von 64 und einer Schlüssellänge von 128 Bit.

3. RSA

Der 1978 von ***R**ivest*, ***S**hamir* und ***A**dleman* vorgestellte Algorithmus setzt die Idee von *Diffie* und *Hellman* aus dem Jahr 1976[61] um. Es ist ein asymmetrischer Algorithmus mit variabler Schlüssellänge[62].

---

[57] http://www.nsa.gov:8080/

[58] Anfang der 90er Jahre stellte sich der Grund für die Geheimhaltung heraus. Die NSA hatte DES gegen einen Angriff, die sog. differentielle Kryptanalyse, abgesichert, der damals nur ihr bekannt war. Man beschloß, die Designkriterien geheimzuhalten, um den amerikanischen Vorsprung auf diesem Gebiet nicht zu gefährden. Die differentielle Kryptanalyse wurde von der öffentlichen Forschung erst 1990 entdeckt. Dies zeigt, wie weit die NSA den veröffentlichten Erkenntnissen der Kryptologie voraus war (und vielleicht noch ist), vgl. *Schneier*, unter 12.4, S. 337.

[59] *Bizer* in KritJ 1995, 450, 453, unter 3; *Schneier*, unter 14.12, S. 409. Durch Zusammenarbeit vieler Rechner über das Internet wurde bereits ein DES-Schlüssel (56 Bit) gebrochen, vgl. *Hortmann* in DuD 1997, 532, 533, unter 3, wo in Fn. 4 auf http://www.frii.com/~rcv/deschall.htm verwiesen wird. *Hortmann* geht auch davon aus, daß Nachrichtendienste und kriminelle Organisationen über spezielle Hardware zum Brechen von DES verfügen könnten.

[60] zu IDEA ausführlich *Schneier*, unter 13.9, S. 370 ff.

[61] s.o. B I 2 a.E.

Die Sicherheit von RSA beruht darauf, daß es kein Problem darstellt, zwei große Primzahlen miteinander zu multiplizieren, es aber praktisch nicht möglich ist, aus dem Produkt wieder die beiden Primfaktoren zu ermitteln. Die Rekonstruktion des Klartextes oder des privaten Schlüssels aus Chiffretext und öffentlichem Schlüssel ist nach heutigem Erkenntnisstand genauso schwierig, wie die Lösung dieses **Problems der Faktorisierung großer Zahlen**, allerdings gibt es dafür keinen Beweis. Für die Beurteilung der praktischen Sicherheit kommt es vor allem darauf an, wie groß die Zahlen sind, die in der Praxis gerade noch faktorisierbar sind. 512 Bit gelten mittlerweile als unsicher, und auch 768 Bit genügen nicht den höchsten Sicherheitsansprüchen. 1024-Bit-Schlüssel werden im Lauf der nächsten Jahrzehnte möglicherweise zu brechen sein, erst ab 2048 Bit kann man von guter Sicherheit ausgehen[63].

Der Algorithmus läßt sich nicht nur zur Verschlüsselung, sondern auch zum Erzeugen und Überprüfen digitaler Signaturen einsetzen[64]. Dabei kann der private Konzelationsschlüssel gleichzeitig als privater Signaturschlüssel und der öffentliche Konzelationsschlüssel zur Überprüfung von Signaturen eingesetzt werden. Signiert wird durch Verschlüsseln des Hashwerts mit dem privaten Schlüssel.

4. ElGamal und DSA

Das auf der Idee von *Diffie* und *Hellman* aufbauende, 1985 von *Taher ElGamal* entwikkelte Schema ist ebenfalls ein asymmetrischer Konzelationsalgorithmus[65]. Es beruht auf dem sogenannten Problem des **diskreten Logarithmus**, das von manchen Mathematikern für noch schwieriger als das Problem der Faktorisierung großer Zahlen gehalten wird[66].

Es gibt auch ein ElGamal-Signaturschema, dessen Variante **DSA (Digital Signature Algorithm)** 1994 vom NIST zum **Digital Signature Standard (DSS)** der USA erklärt wurde[67]. DSA wurde von der NSA entwickelt und arbeitet mit einer variablen Schlüssel-

---

[62] ausführlich *Schneier*, unter 19.3, S. 531 ff.; *Beutelspacher*, unter 5.3, S. 122 ff.; daneben *Bauer*, unter 11.3 f., S. 160 ff.; *Gerling* in DuD 1997, 197, 198 f., unter 4; *Grimm* in DuD 1996, 27, 35 f., Anhang; *Ohst*, unter 7

[63] *Schneier*, unter 7.2, S. 190; ebenso, doch 1024 Bit für die nächsten 20 bis 30 Jahre ausreichend: *Fox* in DuD 1997, 69, 71, unter 3.3

[64] vgl. dazu *Fox* in DuD 1997, 69, 70 ff., unter 3; sowie die Nachw. bei Fn. 62

[65] vgl. dazu *Beutelspacher*, unter 5.5, S. 141 f.; *Schneier*, unter 19.6, S. 543 ff.

[66] *Beutelspacher*, unter 5.4, S. 139

[67] vgl. zu DSA *Fox* in DuD 1997, 69, 72 f., unter 4; *Schneier*, unter 20.1, S. 553 ff.

länge zwischen 512 und höchstens 1024 Bit, was beides einige Kritik ausgelöst hat. Jedoch werden schon 512-Bit-DSA-Schlüssel für die nächsten 20 bis 30 Jahre für sicher gehalten[68].

V. Anwendungen

1. Schutz von im Netz übertragenen Daten

Fast alle Daten bewegen sich in kleinen Datenpaketen durchs Netz und durchlaufen dabei konzeptbedingt eine unüberschaubare Anzahl von Rechnern, oft sogar in verschiedenen Ländern[69]. Jeder, der auf einem solchen Rechner über ausreichende lokale Zugriffsmöglichkeiten verfügt, kann die übers Netz übertragenen Daten mitlesen oder verändern; die Möglichkeit dazu kann sogar durch einen „Einbruch" in das entsprechende Rechnersystem erlangt werden[70]. Bei diesen Daten kann es sich um elektronische Post (E-Mail), um Telefongespräche, Videokonferenzen, Banktransaktionen, medizinische Daten, Firmendaten und vieles mehr handeln. Schon an diesem Punkt wird klar, daß sich die verschlüsselte und signierte Übertragung solcher Daten zum Verhindern unbefugten Ausspähens und Verfälschens anbietet.

Software dafür ist bereits erhältlich oder in Entwicklung. Zum Verschlüsseln und digitalen Signieren von E-Mail (wie auch von anderen Dokumenten) hat sich weltweit zumindest im privaten Bereich das Programm **PGP** (Pretty Good Privacy) durchgesetzt, das auf den Algorithmen IDEA und RSA basiert[71]. Es ist für Privatanwender kostenlos und steht im Internet jedermann zum Download zur Verfügung[72]; auch existiert eine Variante zum Verschlüsseln von über das Internet geführten Telefongesprächen. WWW-Verbindungen können mit Hilfe des **Secure Socket Layer (SSL)**, das mittlerweile in den verbreitetsten Browsern eingebaut ist, verschlüsselt und authentisch durchgeführt werden[73]. Und für die nächste Generation des grundlegenden Internet-Übertragungsprotokolls **IP** ist die Inte-

---

[68] *Fox* in DuD 1997, 69, 72, unter 4.3

[69] *Köhntopp* in Rost, 63, 63 f.; *Schwarz*, unter V 6

[70] *Bizer* in KritJ 1995, 450, 450, unter 1; *Gerling* in DuD 1997, 197, 197, unter 2

[71] *Grimm* in DuD 1996, 27, 33, unter 8; *Huhn/Pfitzmann* in DANA 6/1996, 4, 8, unter 3. Neuere Versionen von PGP arbeiten wahlweise auch mit anderen Algorithmen wie CAST (einer relativ neuen, symmetrischen Blockchiffre), Triple-DES, ElGamal und DSA.

[72] http://www.pgpi.com

[73] *Gerling* in DuD 1997, 197, 200, unter 7; es gibt allerdings Einschränkungen aufgrund der restriktiven amerikanischen Exportrichtlinien für kryptographische Produkte, vgl. *Gerling*, aaO.

gration kryptographischer Authentikations- und Konzelationssysteme für idealiter sämtliche transportierte Datenpakete im Internet bereits vorgesehen[74].

2. Digitale Signatur als „elektronische Unterschrift“

Für den „elektronischen Handel“ wie überhaupt für jede rechtsverbindliche Kommunikation über das Netz wird es von entscheidender Bedeutung sein, die Abgabe von Willenserklärungen beweisen zu können[75]. Verbindliche digitale Signaturen werden hier eines ihrer wichtigsten Einsatzfelder finden. Über ausgeprägte Zertifizierungsstrukturen wird es möglich sein, jedem digital signierten Dokument einen Urheber zuzuordnen, so daß Verträge auch übers Netz ohne Einbuße an Beweissicherheit geschlossen werden können.

3. Digitales Geld

Mit **digitalem** (oder auch „elektronischem“) **Geld** ist im Gegensatz zum elektronischen Zahlungsverkehr (Scheckkarten, Kreditkarten, Überweisungen etc.) ein System gemeint, in dem digital symbolisierte Zahlungsmittel („Münzen“ oder *Tokens*) *ohne* Einschaltung Dritter (wie etwa einer Bank) von einer Person an eine andere transferiert werden können[76]. Das Funktionieren eines solchen Systems wäre eine weitere wichtige Voraussetzung für die Etablierung einer echten Handelsinfrastruktur im Internet[77].

Ideales digitales Geld sollte einige Voraussetzungen erfüllen[78]: Das Geld kann über Computernetze transferiert, es kann nicht kopiert und dann wiederverwendet werden, niemand kann grundsätzlich die Geschäfte eines Benutzers nachvollziehen (Anonymität), zur Bezahlung muß keine Verbindung zu einem Zentralrechner bestehen, das Geld kann zu anderen Benutzern übertragen werden und eine Einheit über einen bestimmten Betrag läßt sich in kleinere Einheiten zerlegen. Daneben ist für die Durchsetzung von digitalem Geld auch wichtig, daß es einfach zu benutzen, kostengünstig, überall einsetzbar und auf einem robusten System basierend realisiert ist[79]. Sogenannte **elektronische Geldbörsen**,

---

[74] *Jaeger* in Rost, 180, 190

[75] so auch *Bizer/Fox* in DuD 1997, 66, 66; *Roßnagel* in DuD 1997, 75, 75, unter „Entstehungsgeschichte“

[76] vgl. dazu *Beutelspacher*, unter 6.3, S. 155 ff.; *Gramlich* in DuD 1997, 383 ff.; *Petersen* in DuD 1997, 403 ff.; *Schneier*, unter 6.4, S. 165 ff.; zu Datenschutzaspekten *Knorr/Schläger* in DuD 1997, 396 ff.; zur volkswirtschaftlichen Bedeutung *Herreiner* in DuD 1997, 390 ff.

[77] *Petersen* in DuD 1997, 403, 403, unter 1

[78] *Schneier*, unter 6.4, S. 173 f.

[79] *Petersen* in DuD 1997, 403, 404, unter 2

die ihr Einsatzgebiet außerhalb des Netzes im alltäglichen Leben finden sollen, müssen daneben auch über Vorteile gegenüber normalem Bargeld verfügen, damit sie von den Kunden akzeptiert werden. Hier sind vor allem die bereits erwähnte Teilbarkeit von Münzen, Verlusttoleranz, Quittierung und Stornierung von Zahlungen sowie Geldwechsel zwischen verschiedenen Währungen zu nennen[80].

Es existieren mittlerweile sehr komplexe **kryptographische Protokolle**[81], die viele oder alle dieser Anforderungen erfüllen und sich somit prinzipiell zur Umsetzung in die Praxis eignen[82]. Einige Firmen bieten digitales Geld auch schon zur Bezahlung im Internet an[83].

4. Sonstiges

Kryptographische Protokolle können zur Lösung vieler Probleme eingesetzt werden, von denen man auf den ersten Blick nie denken würde, daß sie in der Umgebung eines Computernetzes überhaupt lösbar sind. Einige Beispiele für solche Protokolle sind: Verteilen eines Geheimnisses auf mehrere Personen, datierte Stempel, faire Simulation eines Münzwurfs, Beweis von Geheimniskenntnis ohne Geheimnisenthüllung, gleichzeitige Vertragsunterzeichnung, gleichzeitiger Geheimnisaustausch, sichere Wahlen[84] und Anonymität[85]. Es dürfte nicht übertrieben sein, die Kryptographie als absolute Schlüsseltechnologie für die Entwicklung des Internet und der Informationsgesellschaft überhaupt zu bezeichnen[86].

---

[80] *Petersen*, aaO

[81] vgl. zum Begriff Protokoll *Schneier*, unter 2.1, S. 25 ff.

[82] vgl. *Petersen* in DuD 1997, 403, 406 f., unter 4 f.; *Schneier*, unter 6.4, S. 174

[83] vgl. etwa *Schneier*, unter 6.4, S. 172 f.

[84] In Costa Rica sollen 2002 die nationalen Wahlen über das Internet durchgeführt werden, vgl. http://www.intern.de/97/22/29.shtml

[85] näher zu allen genannten Protokollen *Schneier*, unter 3 ff., S. 83 ff.; zur Anonymität näher *Beutelspacher*, unter 6, S. 149 ff.

[86] in diesem Sinne auch *Heuser*; aus Sicht des Datenschutzes ähnlich *Bizer* in KritJ 1995, 450, 451, unter 2; *Gerling* in DuD 1996, 197, 197 f., unter 2

C. Bestehende und denkbare rechtliche Regelungen

Aufbauend auf die Darstellung der tatsächlichen Rahmenbedingungen sollen nun rechtliche Fragen der Kryptographie, wie sie sich in Deutschland derzeit stellen, untersucht werden.

I. Aktuelle Rechtslage

Der deutsche Gesetzgeber behandelt Authentikations- und Konzelationssystemen getrennt, obwohl beides kryptographische Verfahren sind. Während erste mittlerweile eine recht ausführliche gesetzliche Regelung erfahren haben (1), verbleiben letztere weitgehend ungeregelt (2). Die Differenzierung zwischen Signatur- und Verschlüsselungsverfahren erscheint gerechtfertigt, da sie aus juristischer Sicht völlig unterschiedlichen Zwecken dienen, die Erwartungen der Benutzer an die Systeme verschieden sind und sich auch jeweils andere Probleme ergeben.

1. Das Signaturgesetz

Das Gesetz zur Regelung der Rahmenbedingungen für Informations- und Kommunikationsdienste (Informations- und Kommunikationsdienste-Gesetz, IuKDG) vom 22. Juli 1997[87] enthält in seinem Art. 3 das **Gesetz zur digitalen Signatur (Signaturgesetz, SigG)**. Dieses ist nach Art. 11 IuKDG am 1. August 1997 in Kraft getreten[88].

a) Gesetzgebungskompetenz

Die Gesetzgebungszuständigkeit des Bundes ergibt sich aus seiner Kompetenz zur konkurrierenden Gesetzgebung für das **Recht der Wirtschaft** (Art. 74 Abs. 1 Nr. 11 GG). Damit überall im Bundesgebiet die gleichen Sicherheitsbedingungen und -anforderungen herrschen und die Wirtschaftsunternehmen die notwendige technische Infrastruktur ökonomisch sinnvoll zur Verfügung stellen können, ist zur Wahrung der Rechts- und Wirtschaftseinheit eine bundesgesetzliche Regelung im gesamtstaatlichen Interesse erforderlich (Art. 72 Abs. 2 GG)[89].

[87] BGBl. I S. 1870; im Internet: http://www.iid.de/rahmen/iukdg.html

[88] vgl. zum SigG (BGBl. I S. 1870, 1872; FNA 9020-8) auch *Engel-Flechsig/Maennel/Tettenborn* in NJW 1997, 2981, 2988, unter V; *Geis* in NJW 1997, 3000; *Roßnagel* in DuD 1997, 75

[89] so auch BT-Drs. 13/7385 (s.o. Fn. 3), Begründung zu Art. 3, unter B VI

b) Gesetzeszweck

Zweck des SigG ist es, „Rahmenbedingungen für digitale Signaturen zu schaffen, unter denen diese als sicher gelten und Fälschungen digitaler Signaturen oder Verfälschungen von signierten Daten zuverlässig festgestellt werden können“ (§ 1 Abs. 1 SigG).

Änderungen an Formvorschriften oder dem Beweisrecht wurden nicht vorgenommen, insbesondere wurde die digitale Signatur **nicht der gesetzlichen Schriftform** (§ 126 BGB) **gleichgestellt**. Es soll zunächst durch tatsächliche Sicherheit Vertrauen in die gesetzliche digitale Signatur geschaffen werden[90], so daß sie vom Rechtsverkehr akzeptiert wird und Gerichte ihr im Rahmen der freien Beweiswürdigung die nötige Beweiskraft zuerkennen können. Später wird dann möglicherweise in bestimmten Fällen, in denen heute Schriftform verlangt wird, auch die digitale Signatur zugelassen werden; außerdem könnte es dann auch Änderungen im Beweisrecht geben[91].

Das SigG stellt die Anwendung anderer Verfahren in § 1 Abs. 2 ausdrücklich frei; es besteht also **kein Zwang**, nur Authentikationssysteme nach dem SigG zu verwenden.

c) Zertifizierungsstellen

Das SigG regelt im wesentlichen die Rahmenbedingungen für die Arbeit von Zertifizierungsinstanzen[92], die es **Zertifizierungsstellen** nennt. Nach § 2 Abs. 2 SigG sind dies Personen, die die Zuordnung von öffentlichen Prüfschlüsseln[93] zu natürlichen Personen bescheinigen und dafür eine Lizenz nach § 4 SigG besitzen. Die Prüfschlüssel der Zertifizierungsstellen werden nach § 4 Abs. 5 SigG ihrerseits von der zuständigen Behörde zertifiziert, so daß sich eine **zweistufige Zertifizierungshierarchie** mit der Behörde an der Spitze ergibt.

Mit der Festlegung, daß alle Zertifizierungsstellen von der zuständigen Behörde zu zertifizieren sind, wird ein zentrales Sicherheitsrisiko geschaffen. Sollte der Schlüssel der Behörde kompromittiert werden, so ist die gesamte Zertifizierungshierarchie und damit der gesamte elektronische Rechtsverkehr gefährdet. Daneben wird aber auch verhindert,

---

[90] vgl. *Roßnagel* in DuD 1997, 75, 76, unter „Entstehungsgeschichte“; *Timm* in DuD 1997, 525, 528, unter 3.1

[91] BT-Drs. 13/7385 (s.o. Fn. 3), Begründung zu Art. 3, unter B III

[92] s.o. B II 3 c a.E.

[93] Das SigG spricht von „Signaturschlüsseln“, was jedoch falsch ist, vgl. *Roßnagel* in DuD 1997, 75, 78, unter „Korrekte Gesetzessprache“.

daß Zertifizierungsstellen „Dependancen“ gründen können und sich somit eine mehrstufige Zertifizierungshierarchie ausbilden kann. Es ist fraglich, ob dies zweckmäßig ist[94].

d) Lizenzierung

Nach § 4 SigG bedarf der Betrieb einer Zertifizierungsstelle einer Lizenz. Es besteht ein Rechtsanspruch auf Erteilung einer Lizenz durch die Behörde, wenn der Antragsteller die für den Betrieb einer Zertifizierungsstelle nötige Zuverlässigkeit und die dort tätigen Personen die nötige Fachkunde besitzen und außerdem in einem Sicherheitskonzept und bei einer Vorortprüfung die Erfüllung der technischen und organisatorischen Sicherheitsanforderungen des SigG nachgewiesen werden. Die Lizenz kann mit erforderlichen Nebenbestimmungen versehen werden (§ 4 Abs. 4 SigG).

Aufgrund eines Zirkelschlusses zwischen § 2 Abs. 2 SigG, der in die Legaldefinition einer „Zertifizierungsstelle“ als Voraussetzung den Besitz einer Lizenz nach § 4 SigG aufnimmt, und § 4 Abs. 1 SigG, der für den Betrieb einer *Zertifizierungsstelle* eine Lizenzierungspflicht aufstellt, ist unklar, ob eine Lizenz für den Betrieb jeder Zertifizierungsinstanz erforderlich ist, oder ob sich nur diejenigen lizenzieren lassen müssen, die Zertifikate nach dem SigG ausstellen und damit an der gesetzlichen Sicherheitsfiktion des § 1 Abs. 1 SigG teilhaben wollen[95]. Der Wortlaut von § 4 Abs. 1 SigG, der sich eines im selben Gesetz legaldefinierten Begriffs bedient, und die grundsätzliche Freistellung alternativer Verfahren für die digitale Signatur in § 1 Abs. 2 SigG sprechen für die liberalere Auslegung. Die Bundesregierung wollte jedoch offenbar jegliche Ausstellung von Zertifikaten für Signaturprüfschlüssel einer Lizenzierungspflicht unterwerfen[96]. Dieser Wunsch hat im maßgeblichen Gesetzestext allerdings keinen Ausdruck gefunden. Nimmt man die Legaldefinition in § 2 Abs. 2 SigG ernst, so ergibt sich, daß die Lizenzierung eine freiwillige Unterwerfung unter die Bestimmungen des SigG darstellt und keine Pflicht dazu besteht, wenn eine Zertifizierungsinstanz die Vorteile des SigG (wie etwa die Fiktion in § 1 Abs. 1 SigG) nicht in Anspruch nehmen möchte. Diese Auslegung allein ist auch in der Lage, den durch § 1 Abs. 2 SigG angestrebten Wettbewerb[97] des gesetzlichen Modells mit anderen Sicherungsinfrastrukturen zu gewährleisten, da ein Authentikationssystem ohne Zertifizierungsstruktur im großen Maßstab nicht ein-

[94] *Roßnagel* in DuD 1997, 75, 78 f., unter „Rigide Zertifizierungsstruktur“

[95] vgl. auch *Roßnagel* in DuD 1997, 75, 79, unter „Unklare Lizenzierungspflicht“

[96] BT-Drs. 13/7385 (s.o. Fn. 3), Begründung zu Art. 3 § 4 Abs. 1 bis 4

[97] vgl. auch BT-Drs. 13/7385 (s.o. Fn. 3), Begründung zu Art. 3 § 1 Abs. 1; Roßnagel in DuD 1997, 75, 76, unter „Freiheit der Signaturverfahren“

setzbar ist[98]. Die dem experimentellen Charakter des SigG[99] entsprechende Erprobung von Technologien, von denen noch nicht bekannt ist, ob sie den Sicherheitsanforderungen des SigG entsprechen, wird nur so ermöglicht. Auch wird damit die absurde Konsequenz vermieden, daß praktisch jeder Benutzer des im Internet gebräuchlichen Verschlüsselungsprogramms PGP als „Zertifizierungsstelle" eine Lizenz nach § 4 SigG benötigte[100]. Und schließlich verlangt das rechtsstaatliche Erfordernis der Klarheit und Bestimmtheit eine Regelung, die für den Einzelnen erkennen läßt, was von ihm verlangt wird und inwiefern seine Grundrechte eingeschränkt werden[101]. Eine Gesetzesauslegung, die einen Eingriff in die Berufsfreiheit (Art. 12 Abs. 1 GG) oder die allgemeine Handlungsfreiheit (Art. 2 Abs. 1 GG) darauf stützen wollte, daß sie eine durch das selbe Gesetz aufgestellte Legaldefinition für unbeachtlich hält, müßte sich vorwerfen lassen, dieses Erfordernis aufzugeben.

Demnach ist der Auslegung der Vorzug zu geben, nach der **keine Lizenzierungspflicht** besteht.

e) Aufgaben der Zertifizierungsstellen

Durch das SigG und die aufgrund von § 16 SigG durch die Bundesregierung erlassene **Verordnung zur digitalen Signatur (Signaturverordnung, SigV)** vom 22. Oktober 1997[102], die Detailfragen regelt und gemäß § 19 SigV am 1. November 1997 in Kraft getreten ist, werden den Zertifizierungsstellen eine Reihe von Pflichtaufgaben übertragen.

Die Zertifizierungsstelle muß die Identität einer Person, die ein Zertifikat beantragt, durch Überprüfung des Personalausweises feststellen (§§ 5 Abs. 1 SigG, 3 Abs. 1 SigV). Sie muß für den Antragsteller ein Schlüsselpaar erzeugen und es ihm zuordnen oder aber sich davon überzeugen, daß der Antragsteller zur Erzeugung des Schlüsselpaars geeignete technische Komponenten eingesetzt hat (§ 5 SigV). Hat sie das Schlüsselpaar erstellt, muß sie es dem Antragsteller persönlich übergeben (§ 6 SigV). Sie stellt ein Prüfschlüssel-Zertifikat aus (§ 5 Abs. 1 Satz 2 SigG), das auch zusätzliche Daten wie Angaben über Vertretungsmacht oder Berufszulassungen (Ärzte, Anwälte etc.) enthalten

---

[98] s.o. B II 3 c

[99] *Timm* in DuD 1997, 525, 528, unter 3.1

[100] zum dezentralen Zertifizierungsmodell von PGP *Grimm* in DuD 1996, 27, 33 f., unter 8; daneben Huhn/Pfitzmann in DANA 6/1996, 4, 8, unter 4 a.E.

[101] vgl. *Pieroth/Schlink*, Rdnr. 339; zu diesem Gebot auch *Görisch* in JuS 1997, 988, 989 f., unter 4

[102] BGBl. I S. 2498; FNA 9020-8-1; im Internet: http://www.iid.de/rahmen/sigv.html

kann (§ 5 Abs. 2 SigG), und belehrt den Antragsteller über Sicherheitsfragen (§§ 6 SigG, 4 SigV).

Daneben muß die Zertifizierungsstelle einen immer erreichbaren Sperrdienst (§§ 8 SigG, 9 SigV), einen 10 Jahre lang über öffentlich zugängliche Telekommunikationsverbindungen erreichbaren Verzeichnisdienst für Zertifikate und Sperrungen (§§ 5 Abs. 1 Satz 2 SigG, 8 SigV) sowie einen Service zum „Zeitstempeln" digital signierter Daten[103] (§ 9 SigG) unterhalten.

f) Datenschutzaspekte

Personenbezogene Daten, die die Zertifizierungsstelle nach § 12 Abs. 1 SigG erhoben hat, unterliegen einer **Zweckbindung**. Der Antragsteller ist nicht einmal gezwungen, sein Zertifikat veröffentlichen zu lassen; es genügt nach § 5 Abs. 1 Satz 2 SigG, wenn eine Online-*Überprüfung* bei der Zertifizierungsstelle möglich ist.

Nach § 5 Abs. 3 SigG sind auch Zertifikate, die anstelle eines Namens mit einem **Pseudonym** versehen sind, zulässig, wobei dieser Umstand im Zertifikat kenntlich zu machen ist; auf Wunsch des Kunden *muß* ein solches Zertifikat sogar ausgestellt werden. Jedoch ermächtigt § 12 Abs. 2 SigG Sicherheits- und Geheimdienstbehörden, die wahre Identität eines Zertifikat-Inhabers bei der Zertifizierungsstelle zu ermitteln, soweit das zur Erfüllung ihrer Aufgaben notwendig ist. Diese Regelung ist in zweierlei Hinsicht zu kritisieren.

Zum einen ist keine Möglichkeit für Privatpersonen vorgesehen, um eine Aufdeckung der pseudonymen Identität zu erreichen. Dies wird die tatsächlichen Einsatzmöglichkeiten von pseudonymen digitalen Signaturen erheblich behindern, da sich ein Vertragspartner normalerweise auf einen Abschluß mit einem unter Pseudonym agierenden Partner nur einlassen wird, wenn er bei Leistungsverweigerung die wahre Identität in Erfahrung bringen und auf dem Rechtsweg gegen seinen Vertragspartner vorgehen kann[104].

Zum anderen ist die Regelung aber auch zu weitgehend. Die Aufdeckung der pseudonymen Identität durch eine Behörde stellt einen Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen aus Art. 1 Abs. 1, 2 Abs. 1 GG[105] dar. Die Eingriffsvoraussetzungen in § 12 Abs. 2 SigG sind allerdings zu unbestimmt und es gibt auch keine

[103] vgl. dazu *Schneier*, unter 4.1, S. 91 ff.

[104] *Roßnagel* in DuD 1997, 75, 79, unter „Unvollständige Regelungen"

[105] vgl. BVerfGE 65, 1; *Pieroth/Schlink*, Rdnr. 412 und konkret insbes. 418

besonderen verfahrensmäßigen Sicherungen, was beides den von BVerfG vorgegebenen Bedingungen widerspricht[106]. Insbesondere ist nicht einmal eine Unterrichtung des Betroffenen nach Ende der Ermittlungen vorgesehen[107], so daß dieser möglicherweise noch lange auf die Geheimhaltung seiner pseudonymen Identität vertraut, während der Staat weiterhin in der Lage ist, seine Aktionen zu verfolgen. Dadurch geht der Eingriff in zeitlicher Hinsicht weiter als erforderlich und wird damit unverhältnismäßig. In seiner jetzigen Fassung ist § 12 Abs. 2 SigG aus diesen Gründen verfassungswidrig[108].

g) Sicherheit und Überprüfungen

§§ 5 Abs. 4, 5 Abs. 5 SigG, 10 f., 14 ff. SigV enthalten Regelungen, die organisatorische, personelle und technische Sicherheit garantieren sollen. Besondere Bedeutung hat das Verbot der Speicherung des privaten Signaturschlüssels bei der Zertifizierungsstelle in § 5 Abs. 4 Satz 3 SigG, denn wer über diesen Schlüssel verfügt, kann theoretisch beliebige Dokumente mit der digitalen Signatur des legitimen Schlüsselinhabers versehen; diese Möglichkeit würde dem Vertrauen in die digitale Signatur schweren Schaden zufügen. Die Maßnahmen, die eine Zertifizierungsstelle zur Einhaltung der Sicherheitsanforderungen durchführt, sind in einem **Sicherheitskonzept** niederzulegen (§§ 4 Abs. 3 Satz 3 SigG, 12 SigV).

Dieses Konzept wird bei der Lizenzierung und danach jeweils im Abstand von zwei Jahren überprüft (§ 15 SigV). Außerdem hat die zuständige Behörde zur Überwachung der Zertifizierungsstelle Durchsuchungs-, Einsichts- und Auskunftsrechte. Sie kann Maßnahmen gegen die Zertifizierungsstelle verhängen und die Lizenz zurücknehmen oder widerrufen (§ 13 SigG). Daneben hat die Datenschutzbehörde gemäß § 12 Abs. 3 das Recht zu verdachtsunabhängigen Kontrollen.

§ 13 Abs. 2 SigG sieht zwar vor, daß die Kontrollbehörde bei einer Überprüfung Einsicht in die schriftlichen Unterlagen der Zertifizierungsinstanz nehmen kann, doch fehlt eine Ermächtigung zum Zugriff auf Datensammlungen und technische Anlagen. Eine umfassende Überprüfung scheint ohne diese Möglichkeit nahezu ausgeschlossen[109].

---

[106] vgl. BVerfGE 65, 1, 1; *Pieroth/Schlink*, Rdnr. 108

[107] kritisch dazu auch *Bizer* in DuD 1997, 203, 204, unter 2.2

[108] so auch *Roßnagel*, Kritische Anmerkung, unter 2 „Informationelle Selbstbestimmung durch Pseudonyme“

[109] *Roßnagel* in DuD 1997, 75, 80, unter „Unzureichende Kontrollbefugnisse“

h) Haftungsfragen

Das SigG enthält **keine eigene Haftungsregelung** und überläßt die Beantwortung von Haftungsfragen den allgemeinen Regeln[110]. Danach haftet die Zertifizierungsstelle gegenüber dem Schlüsselinhaber gemäß § 278 BGB ohne Exkulpationsmöglichkeit für ein Verschulden ihrer Mitarbeiter und sonstigen Erfüllungsgehilfen aus positiver Forderungsverletzung des Zertifizierungsvertrags, wobei dem Schlüsselinhaber die übliche Beweislastverteilung nach Verantwortungsbereichen[111] (Rechtsgedanke des § 282 BGB) zugute kommt: er muß nur die Pflichtverletzung und deren Kausalität für den Schaden beweisen[112]. Gegenüber Dritten haftet die Zertifizierungsstelle für primäre Vermögensschäden jedoch nur bei vorsätzlichen Manipulationen durch einen ihrer Mitarbeiter (§ 831 BGB iVm § 826 BGB bzw. §§ 823 Abs. 2 BGB, 263 StGB)[113], und dies mit Exkulpationsmöglichkeit.

Damit ergibt sich eine **Haftungslücke** zumindest für Fälle, in denen fahrlässiges Verhalten von Mitarbeitern oder Handlungen Dritter einen Vermögensschaden bei einem anderen als dem Schlüsselinhaber verursacht haben[114]. Es wurde vorgeschlagen, zur Behebung dieser Lücke eine Gefährdungshaftung mit Haftungshöchstgrenze, Deckungsvorsorge und Ursachenvermutung einzuführen[115]. Dies würde jedoch für Zertifizierungsstellen eine schärfere Haftung als für Notare bedeuten, obwohl die von letzteren ausgestellten Beglaubigungen und Beurkundungen im Gegensatz zu digitalen Signaturen und Zertifikaten öffentlichen Glauben besitzen[116]. Auch wegen einiger weiterer dogmatischer und Wertungswidersprüche[117] sollte auf die Einführung einer solchen Gefährdungshaftung deshalb verzichtet werden[118].

---

[110] BT-Drs. 13/7385 (s.o. Fn. 3), Begründung zu Art. 3, unter B V „Haftungsfragen“; *Engel-Flechsig/Maennel/Tettenborn* in NJW 1997, 2981, 2989, unter V 3 e; *Roßnagel* in DuD 1997, 75, 79, unter „Fehlende Haftungsregelungen“

[111] vgl. *Kropholler/Berenbrok*, § 276 Rdnr. 33; *Medicus* SchR AT, Rdnr. 420

[112] *Timm* in DuD 1997, 525, 526, unter 2.1

[113] *Timm* in DuD 1997, 525, 526 f., unter 2.2

[114] vgl. *Engel-Flechsig/Maennel/Tettenborn* in NJW 1997, 2981, 2989, unter V 3 e; *Timm* in DuD 1997, 525, 527, vor 3.1

[115] so etwa *Roßnagel* in DuD 1997, 75, 79, unter „Fehlende Haftungsregelungen“

[116] *Timm* in DuD 1997, 525, 528, unter 3.2

[117] *Timm* in DuD 1997, 525, 527 f., unter 3.1 f.

[118] so auch *Timm* in DuD 1997, 525, 528, unter 4

2. Rechtsvorschriften zu Konzelationssystemen

a) Benutzungs- und Ausfuhrbeschränkungen

Im Gegensatz zu einigen anderen Staaten gibt es in Deutschland keine rechtlichen Beschränkungen des Einsatzes von Verschlüsselungsverfahren[119]. Allerdings unterliegt der Export der meisten kryptographischen und kryptanalytischen Technologien nach §§ 7 Abs. 1, 5 Abs. 1 AWG einem Genehmigungsvorbehalt[120].

b) § 8 Abs. 4 Satz 2 FÜV

§ 8 Abs. 4 Satz 2 der Fernmeldeüberwachungsverordnung (FÜV) vom 18. Mai 1995[121] lautet: „Falls der Betreiber dem Teilnehmer Verschlüsselungsmöglichkeiten für die Nachrichten bereitstellt, hat er […] dem Bedarfsträger die für eine Entschlüsselung erforderlichen Informationen zeitgerecht zur Verfügung zu stellen." Die FÜV wurde aufgrund einer Ermächtigung in § 10b FAG erlassen, der seit dem 1. August 1996 durch § 99 Abs. 1 Nr. 3 TKG außer Kraft gesetzt ist.

Es fragt sich, ob diese Vorschrift vom Betreiber einer Telekommunikationsanlage auch verlangt, sich die von seinen Benutzern verwendeten geheimen Schlüssel aushändigen zu lassen und diese den Behörden im Bedarfsfall zur Verfügung zu stellen, oder ob sich die Verpflichtung auf vom Betreiber mit eigenen Schlüsseln vorgenommene Verschlüsselung beschränkt. Dazu ist zunächst zu untersuchen, ob § 8 Abs. 4 Satz 2 FÜV von einer ausreichenden gesetzlichen Ermächtigung getragen wird (Art. 80 GG). Die Verordnung könnte nach dem Wegfall von § 10b FAG unwirksam geworden sein[122]. Dies ist jedoch nicht der Fall, da die alte Ermächtigungsgrundlage in § 10b FAG durch eine neue in § 88 Abs. 2 Satz 2 TKG ersetzt wurde, die ihrerseits § 8 Abs. 4 Satz 2 FÜV trägt[123].

Die Ermächtigung im TKG erlaubt allerdings nur eine Verordnung, die „die technische und organisatorische Umsetzung von Überwachungsmaßnahmen in diesen Telekommunikationsanlagen" regelt. Eine solche Verordnung kann also keine Verpflichtungen ent-

---

[119] vgl. dazu *Bizer* in DuD 1997, 203, 206, unter 3.4; *Hortmann* in DuD 1997, 214; *Kuner* in NJW-CoR 1997, 221; *Möller*

[120] *Bizer* in KritJ 1995, 450, 453, unter 3; die aktuelle Ausfuhrliste der EU für Kryptographie findet sich im Beschluß des Rates vom 22. Oktober 1996, EGABl. C 295/34 vom 30. Oktober 1996, auszugsweise abgedruckt in DuD 1997, 229 ff.

[121] BGBl. I S. 722

[122] so *Bizer* in DuD 1997, 203, 207, unter 5.1

[123] vgl. *Maurer*, § 13 Rdnr. 7

halten, die sich auf Bereiche außerhalb der Telekommunikation beziehen. Nun ist aber teilnehmerautonome Kryptographie kein Bestandteil der Nachrichtenübertragung, sondern Gestaltung des Nachrichteninhalts. Außerdem können die Benutzer ihre eigenen Schlüssel auch zu anderen Zwecken als zur Verschlüsselung von zu übertragenden Nachrichten benutzen, so daß insgesamt festzustellen ist, daß die oben dargestellte weitgehende Auslegung des § 8 Abs. 4 Satz 2 FÜV von der Ermächtigung im TKG nicht mehr getragen und damit verfassungswidrig wäre[124].

II. Potentielle zukünftige Regelungen

Die unbeschränkte Zulassung kryptographischer Verfahren zur Konzelation stellt vor allem die Sicherheits- und Strafverfolgungsbehörden vor das Problem, daß (organisierte) Kriminelle moderne Kommunikationstechnik zur Koordination einsetzen können, ohne daß der Staat eine Möglichkeit hat, vom Inhalt der Kommunikation Kenntnis zu erlangen und präventiv oder repressiv tätig zu werden[125]. Es gibt verschiedene Regelungsmodelle, die diesen Nachteil eines weitverbreiteten Einsatzes von kryptographischen Verfahren beseitigen sollen[126]. Es soll daher untersucht werden, inwiefern solche Regelungen mit dem Grundgesetz vereinbar wären. Dazu wird zunächst geklärt, welchen grundrechtlichen Schutz die Verwendung kryptographischer Konzelationssysteme genießt (1), um dann auf die einzelnen Vorschläge und ihre Verfassungskonformität einzugehen (2).

1. Grundrechtliche Gewährleistung der Verschlüsselungsfreiheit

a) Fernmeldegeheimnis (Art. 10 Abs. 1 Fall 3 GG)

Den Schutzbereich des **Fernmeldegeheimnisses (Art. 10 Abs. 1 Fall 3 GG)** bildet die Vertraulichkeit der unkörperlich vermittelten Individualkommunikation[127]. Neben dem Nachrichteninhalt selbst ist aber auch die Befugnis der Kommunikationspartner geschützt, selbst darüber zu bestimmen, wem der Inhalt der Nachricht zugänglich werden

---

[124] so auch *Bizer* in DuD 1997, 203, 207 f., unter 5.1; *Telesec*, a.E., auch abgedruckt bei *Huhn/Pfitzmann* in DANA 6/1996, 4, 8, Box 1

[125] *Bizer* in KritJ 1995, 450, 452 f., unter 3, und 456 f., unter 5; *Hamm* in DuD 1997, 186, 186, unter 1; *Huhn/Pfitzmann* in DANA 6/1996, 4, 8 f., unter 5 a.E.; *Schmidt/Ungerer* in iX 4/1997, 128, 128

[126] Es darf natürlich spekuliert werden, ob es in Wirklichkeit nicht viel eher um die Ermöglichung geheimdienstlicher Tätigkeit – insbesondere zur Industriespionage – geht, vgl. etwa bei *Huhn/Pfitzmann* in DANA 6/1996, 4, 13, Box 6. Doch ist die subjektive Motivation, die zu solchen Vorschlägen geführt hat, für die *juristische* Bewertung der Modelle nicht von Betracht.

[127] BVerfGE 67, 157, 172; Dreier–*Hermes*, Art. 10 Rdnr. 13; v. Münch/Kunig–*Löwer*, Art. 10 Rdnr. 9 und 12; *Pieroth/Schlink*, Rdnr. 837; *Bizer* in KritJ 1995, 450, 454, unter 4

soll[128]. Es muß ihnen daher auch offenstehen, den Inhalt durch technische Maßnahmen vor unbefugter Kenntnisnahme zu schützen, wie etwa im Bereich des Brief- und Postgeheimnisses durch die Verwendung von Briefumschlägen[129]. Die Verwendung kryptographischer Verfahren zur Konzelation des Nachrichteninhalts durch die Kommunikationsteilnehmer ist daher ebenfalls vom Schutzbereich des Art. 10 GG erfaßt[130].

b) Weitere Grundrechte

Neben Art. 10 GG kommen als Prüfungsmaßstab für mögliche Kryptographieregelungen auch – nämlich in Bezug auf kommerzielle Anbieter – die **Berufsfreiheit** (Art. 12 Abs. 1 GG) und, soweit nicht eines der spezielleren Grundrechte einschlägig ist, das Auffanggrundrecht der **allgemeinen Handlungsfreiheit** (Art. 2 Abs. 1 GG) in Betracht. Außerdem muß wie bei jeder Regelung der **Gleichheitssatz** (Art. 3 Abs. 1 GG) beachtet werden. Gegenüber dem **Recht auf informationelle Selbstbestimmung** (Art. 1 Abs. 1, 2 Abs. 1 GG) ist das Fernmeldegeheimnis allerdings das speziellere Grundrecht[131], so daß insoweit nur am Maßstab des Art. 10 GG zu prüfen ist[132].

2. Mögliche Eingriffe und ihre Rechtfertigung

a) Gemeinsamer verfassungslegitimer Zweck

Das Fernmeldegeheimnis (Art. 10 Abs. 1 Fall 3 GG) kann nach Art. 10 Abs. 2 Satz 1 GG, die Berufsfreiheit (Art. 12 Abs. 1 Satz 1 GG) nach Art. 12 Abs. 1 Satz 2 GG auf Grund eines Gesetzes eingeschränkt werden[133]. Jedoch sind stets nur solche Einschränkungen zulässig, die einem von der Verfassung anerkannten Zweck dienen[134]. Der Zweck, der allen im folgenden besprochenen Eingriffen gemeinsam ist, liegt darin, zum einen die Benutzung moderner Kommunikationstechnik zur Koordination oder Ausübung illegaler Aktivitäten durch die abschreckende Wirkung potentieller Überwachung zu er-

---

[128] BVerfGE 67, 157, 172; 85, 386, 396; *Bizer* in KritJ 1995, 450, 454, unter 4; Dreier–*Hermes*, Art. 10 Rdnr. 13

[129] *Bizer*, aaO

[130] so ausdrücklich auch Dreier–*Hermes*, Art. 10 Rdnr. 13; *Bizer* in KritJ 1995, 450, 454, unter 4; *Hamm* in DuD 1997, 186, 186, unter 1, der den passenden Vergleich von Kryptographie mit der Verwendung einer für Dritte unverständlichen Sprache aufstellt

[131] Dreier–*Hermes*, Art. 10 Rdnr. 82

[132] vgl. dazu *Pieroth/Schlink*, Rdnr. 367

[133] zu den bestehenden Einschränkungen des Fernmeldegeheimnisses vgl. *Bizer* in KritJ 1995, 450, 455 f., unter 5

[134] vgl. *Pieroth/Schlink*, Rdnr. 300 f.

schweren; zum anderen sollen der Strafrechtspflege und anderen Behörden Beweis- und Hinweisquellen erschlossen werden[135]. Sowohl die öffentliche Sicherheit als auch die Effektivität der Strafverfolgung sind verfassungslegitime Zwecke. An diesen Zwecken werden die im folgenden vorgestellten Regelungsmöglichkeiten zu messen sein[136].

b) Kryptographieverbot mit Erlaubnisvorbehalt

(1) Regelungsinhalt

Einer der weitestgehenden Eingriffe in die Verschlüsselungsfreiheit[137] wäre ein strafbewehrtes gesetzliches Verbot der Herstellung, des Vertriebs, des Besitzes und der Verwendung kryptographischer Produkte ohne behördliche Erlaubnis, wobei die Erlaubnis nur unter engen Voraussetzungen und in der Regel nur staatlichen Stellen und großen Wirtschaftsunternehmen – etwa Kreditinstituten oder Unternehmen der Rüstungsindustrie – erteilt wird[138].

(2) Eignung

Bei der Prüfung der Verhältnismäßigkeit einer Regelung ist nach der Feststellung ihres Zwecks[139] zunächst danach zu fragen, ob sie geeignet ist, diesen Zweck zu erreichen. Damit eine Regelung als geeignet angesehen werden kann, ist allerdings nicht nötig, daß sie ihren Zweck in jedem Fall voll erreicht, denn ansonsten wäre nahezu jedes Gesetz – vor allem im Bereich des Strafrechts – als ungeeignet und damit unverhältnismäßig anzusehen; normativer Anspruch und faktischer Zustand können sich nie völlig decken. Es genügt vielmehr, daß die Regelung den Zweck *fördert*; insofern ist oft auch von einer **Einschätzungsprärogative** des Gesetzgebers die Rede[140].

Die vorgestellte Regelung würde dazu führen, daß Privatpersonen und die meisten Organisationen keinen legalen Zugang mehr zu kryptographischen Anwendungen hätten und deren Einsatz auch wegen der Strafandrohung unterlassen würden.

---

[135] s.o. C II vor 1

[136] so auch *Bizer* in KritJ 1995, 450, 461, unter 7.2.1

[137] s.o. C II 1

[138] Ein ähnliches Modell wurde von 1990 bis 1996 in Frankreich praktiziert, vgl. *Hortmann* in DuD 1997, 214, 214 f., unter 3.

[139] s.o. C II 2 a

[140] *Pieroth/Schlink*, Rdnr. 304 und 308

Sie könnte freilich nicht verhindern, daß in kriminellen Kreisen, vor allem im Bereich der organisierten Kriminalität, des Terrorismus und der Spionage, weiterhin Kryptographie – wenngleich illegal – zum Einsatz käme[141]. Denn starke kryptographische Software ist für jeden, der Zugriff auf das Internet hat, verfügbar[142]. Und auch die Gefahr, beim Einsatz solcher Software „erwischt" zu werden, läßt sich ausschalten: Eine Technik namens **Steganographie** erlaubt es, in völlig unverdächtigen Nachrichten wie Bildern, Musikdateien, ISDN-Telefongesprächen oder auch einfachen Texten andere, gegebenenfalls verschlüsselte Nachrichten zu verbergen[143]; auch hierfür steht geeignete Software im Internet zur Verfügung[144]. Der Empfänger kann die geheime Botschaft lesen, für Außenstehende ist deren Existenz nicht zu erahnen und erst recht nicht nachweisbar.

Dazu kommt noch ein weiteres Problem: Es ist aufgrund der Eigenschaft kryptographischer Verfahren, Nachrichten beim Verschlüsseln in möglichst zufällig erscheinende Zeichenfolgen zu überführen, nicht möglich zu beweisen, ob eine solche Zeichenfolge eine verschlüsselte Nachricht ist oder nicht. Ebenso könnte es sich um durch einen technischen Fehler entstandenen „Datenmüll", absichtlich erzeugte Zufallszahlen, Meßergebnisse, Daten in einem exotischen Datenformat etc. handeln. Nur wenn die Kommunikationspartner sich bekannter Standardsoftware bedient haben, kann es möglich sein, einen entsprechenden **Nachweis** zu führen[145].

Wenn sich also die Möglichkeit des Einsatzes von Kryptographie durch diese Regelung nicht ausschalten ließe, so läge darin trotzdem – insbesondere für „Kleinkriminelle" – eine nicht unerhebliche Erschwernis. Es ist nicht auszuschließen, daß die Verwendung kryptographischer Methoden zu kriminellen Zwecken bei einer solchen Regelung zurückginge und die Strafverfolgungsbehörden deshalb mehr Straftäter überführen könnten. Unter Berücksichtigung der Einschätzungsprärogative müßte die Regelung deshalb als den angestrebten Zweck fördernd und damit als geeignet angesehen werden.

---

[141] so auch *Bizer* in KritJ 1995, 450, 462, unter 7.2.1, und 464, unter 7.2.2; *Hamm* in DuD 1997, 186, 189, unter 4.3

[142] s.o. B V 1

[143] *Gerling* in DuD 1997, 197, 200, unter 6; *Hamm* in DuD 1997, 186, 189, unter 4.2; *Huhn/Pfitzmann* in DuD 1996, 23, 25

[144] *Hamm* in DuD 1997, 186, 189, unter 4.2

[145] vgl. *Hamm* in DuD 1997, 186, 190 f., unter 5.5

(3) Erforderlichkeit

Eine Regelung ist dann erforderlich und somit nur dann verhältnismäßig, wenn es kein gleich geeignetes, aber weniger belastendes Mittel gibt, um den angestrebten Zweck zu erreichen[146].

Wegen der dargestellten Umgehungsmöglichkeiten ist auch von anderen Mitteln keine besonders hohe Wirksamkeit zu verlangen, um sie als gleich geeignet ansehen zu können. Daß es solche ebenso geeigneten Mittel gibt, wird im folgenden gezeigt werden[147].

Diese müßten aber auch weniger belastend wirken. Die besprochene Regelung führte dazu, daß insbesondere Privatpersonen ihre im Netz übertragenen Daten nicht mehr vor unbefugtem Zugriff schützen könnten. Diese wären somit dem Zugriff nicht nur des Staates, sondern auch von anderen Personen ausgesetzt, die sie in krimineller Absicht abfangen und zum Schaden des Absenders oder Empfängers mißbrauchen könnten. Diese Gefahr ist gerade in einem offenen Netz wie dem Internet nicht zu unterschätzen; ihr kann ohne Einsatz kryptographischer Protokolle nicht wirksam begegnet werden[148]. Da es, wie noch zu zeigen ist[149], aber Mittel gibt, die zumindest dieses Problem nicht aufwerfen, muß die vorgestellte Regelung mangels Erforderlichkeit als unverhältnismäßig verworfen werden.

c) Verbot starker Kryptographie

(1) Regelungsinhalt

Schon weniger einschneidend wäre ein Verbot nur solcher kryptographischer Methoden, die vom Staat nicht mehr in vertretbarer Zeit entschlüsselt werden können, etwa durch Begrenzung der zulässigen Schlüssellänge[150]. Auch hier wäre wahrscheinlich ein Erlaubnisvorbehalt vorgesehen, so daß in besonders sensiblen Bereichen im Einzelfall doch starke Kryptographie zur Anwendung kommen könnte.

---

[146] *Pieroth/Schlink*, Rdnr. 306

[147] s.u. C II 2 c und C II 2 d

[148] *Bizer* in KritJ 1995, 450, 451, unter 2; *Gerling* in DuD 1997, 197, 197 f., unter 2

[149] s.o. Fn. 147

[150] s.o. B III 2 b

(2) Eignung

Die Eignung einer solchen Regelung ist ähnlich zu beurteilen wie die des Totalverbotes[151]. Zwar ist bei diesem Modell im Fall einer Überwachung die gesamte Kommunikation zunächst zu entschlüsseln, doch ist dies bei entsprechender finanzieller Ausstattung und Festlegung von niedrigen Schlüsselhöchstlängen kein besonderes Problem[152]. Eine solche Regelung wäre also (gerade noch) geeignet, um den angestrebten Zweck zu erreichen.

(3) Erforderlichkeit

Auch dieses Modell ist mit dem Problem behaftet, daß Unbefugte – hier allerdings nur finanziell leistungsfähige wie z. B. organisierte Kriminelle – Zugriff auf zu schützende Daten erlangen können. Es ist also ebenfalls unzulässig, wenn es ein anderes Mittel gibt, das zu einer insgesamt milderen Belastung führt[153].

d) Key Recovery

(1) Regelungsinhalt

Eine weitere denkbare Beschränkung wäre es, kryptographische Anwendungen nur dann zu erlauben, wenn die Benutzer (bzw. ihre Software) die verwendeten Schlüssel oder wesentliche Teile davon so hinterlegen, daß staatliche Stellen darauf Zugriff haben und somit im Bedarfsfall von den Benutzern unbemerkt Nachrichten entschlüsseln können (sog. Key Recovery)[154]. Es sind hier verschiedene Varianten denkbar. Um das Risiko zu minimieren, könnte der Schlüssel etwa mittels *secret sharing* auf mehrere Hinterlegungsstellen verteilt werden, so daß keine davon alleine Zugriff auf den Schlüssel hat. Auch könnte das System möglicherweise so eingerichtet werden, daß die Hinterlegungsstellen keine Schlüssel an Behörden herausgeben müßten, sondern lediglich einzelne Nachrichten damit zu entschlüsseln bräuchten.

(2) Eignung

Geeignet ist eine solche Regelung freilich nur, wenn sie auch technisch durchführbar ist. Schon die bloße Konzeption und Ausführung eines umfassenden Key-Recovery-Systems

[151] s.o. C II 2 b

[152] s.o. B III 2 b

[153] s.o. C II 2 b

[154] vgl. dazu im einzelnen *Fox* in DuD 1997, 227; *Abelson u.a.*, unter 1.2

könnte sich als technisch nicht machbar erweisen[155]. Doch scheitert an der bloßen Möglichkeit der Undurchführbarkeit die Eignung einer Regelung noch nicht; im Lichte des gesetzgeberischen Einschätzungsspielraums ist vielmehr erst von fehlender Eignung auszugehen, wenn die Durchführbarkeit mit hoher Wahrscheinlichkeit ausgeschlossen werden kann.

Geht man also davon aus, daß ein solches System machbar ist, so ergibt sich zur Eignung ein ähnliches Bild wie schon beim Totalverbot und beim Verbot starker Kryptographie[156]: Große Erfolge sind nicht zu erwarten, weil die Einschränkungen zu leicht unterlaufen werden können. Ein Unterlaufen ist durch die Anwendung sogenannter *Überschlüsselung* sogar noch einfacher als bei den anderen Modellen[157]. Dabei wird im Prinzip eine mit einem nicht hinterlegten Schlüssel chiffrierte Nachricht zusätzlich mit einem hinterlegten Schlüssel verschlüsselt. „Von außen" kann dieser Nachricht nun nicht mehr angesehen werden, daß sie mit verbotener Kryptographie behandelt wurde. Auch der Austausch solcher „verbotener" Schlüssel läßt sich ohne größere Probleme durchführen, und zwar unter Ausnutzung der staatlichen Infrastruktur für Signaturschlüssel oder sogar des Key-Recovery-Systems selbst.

Doch fördert die Regelung immerhin den angestrebten Zweck. Auch sie kann daher nicht als ganz untauglich angesehen werden.

(3) Erforderlichkeit

Eine geeignete Maßnahme ist dann nicht erforderlich, wenn es ein anderes, gleich geeignetes Mittel gibt, das weniger belastend wirkt. Beim derzeitigen technischen Stand ist ein solches Mittel jedoch nicht ersichtlich, will man nicht gänzlich auf das Erreichen des Zwecks verzichten. Von allen derzeit diskutierten Kryptographiebeschränkungen ist Key Recovery noch mit den geringsten Gefahren verbunden, weil das spezifischen Risiko des Totalverbots und des Verbots starker Kryptographie – relativ unproblematische Kenntnisnahme Dritter von Nachrichteninhalten – hier wegfällt. Da also ein milderes Mittel nicht ersichtlich ist, muß die Regelung auch als zum Erreichen des angestrebten Zwecks erforderlich angesehen werden.

---

[155] vgl. *Abelson u.a.*, unter 4

[156] s.o. C II 2 b und C II 2 c

[157] *Hamm* in DuD 1997, 186, 189, unter 4.2; *Huhn/Pfitzmann* in DuD 1996, 23, 24 f.

(4) Angemessenheit

(a) Maßstab

Nach der Rechtsprechung des BVerfG und der im Schrifttum ganz herrschenden Ansicht ist allerdings nicht jeder zur Erreichung eines verfassungslegitimen Zwecks geeignete und erforderliche Grundrechtseingriff auch als verhältnismäßig anzusehen. Als weiteres Kriterium – Verhältnismäßigkeit im engeren Sinn oder Angemessenheit – wird eine stimmige Zweck-Mittel-Relation verlangt; besteht ein krasses Mißverhältnis zwischen den durch die Zweckförderung erreichten Vorteilen und den durch die Maßnahme ausgelösten Nachteilen für die Grundrechtsträger, so ist sie unverhältnismäßig und damit verfassungswidrig[158].

(b) Vorteile

Der Vorteil des Key-Recovery-Modells liegt wie beschrieben darin, daß es dazu beiträgt, die Verwendung moderner Kommunikationsmedien zur Begehung von Straftaten zu unterbinden und den Behörden durch die Möglichkeit zur Beobachtung dennoch stattfindender Kommunikation Beweis- und Hinweisquellen zu erschließen.

Die Beobachtung kann freilich auf vielfältige Weise unterlaufen und die Verwendung solcher Verfahren nur äußerst schwer nachgewiesen werden[159]. Es ist davon auszugehen, daß dies in immer stärkerem Umfang geschehen würde und die Key-Recovery-Regelung daher nur sehr begrenzte Wirksamkeit – hauptsächlich im Bereich der Kleinkriminalität, wo Beschränkungen des Fernmeldegeheimnisses oft gar nicht zulässig sind (§ 100a StPO) – entfalten würde.

(c) Nachteile

Ein Key-Recovery-System würde in einen sowohl finanziell als auch unter Gesichtspunkten des Persönlichkeits- und Datenschutzes hoch sensiblen Bereich eingreifen. Wie bereits erwähnt, ist es äußerst **schwierig**, ein Key-Recovery-System zu entwerfen, das keine Schwächen aufweist; nicht einmal der 1993 von der NSA, der weltweit auf dem Gebiet der Kryptologie wohl kompetentesten Gruppe, entwickelte *U.S. Escrowed Encryption Standard* (sog. *Clipper*), hat sich als brauchbar erwiesen[160].

---

[158] vgl. etwa *Maurer*, § 10 Rdnr. 17; aA *Pieroth/Schlink*, Rdnr. 314 f.

[159] s.o. C II 2 b 2

[160] *Abelson u.a.*, unter 3.2; *Fox* in DuD 1997, 227, unter „Probleme“

Zu bewältigen wäre eine Dimension mit Tausenden von Produkten und Hinterlegungsstellen, Zehntausenden von Behörden, Millionen von Benutzern, mehreren Zehnmillionen Schlüsselpaaren und Hunderten von Milliarden von Sitzungsschlüsseln, die immer weiter wachsen wird und deshalb letztlich nicht sicher zu überwachen sein dürfte[161]. Es bestünden konzeptionsbedingt sehr hohe Anforderungen an die Sicherheit und *gleichzeitig* an Geschwindigkeit und Leistungsmenge der Hinterlegungsstellen, wodurch **Fehlleistungen** nach aller menschlichen Erfahrung völlig unvermeidlich wären[162].

Auch die **Angriffsanfälligkeit** stiege stark an. Durch die Konzentrationen sehr sensitiver Daten bei der Hinterlegungsstelle bestünde neben anderen Angriffsmöglichkeiten auch Anreiz und Gelegenheit zur Benutzung von Insidern – Verführung, Bestechung, Erpressung, Bedrohung, Gewalt usw. –, um unberechtigt Schlüssel zu erlangen; eine Methode, die erfahrungsgemäß häufig zum Erfolg führen wird und daher eine enorme Steigerung der Risiken bewirkt[163]. Auch die Gefährdung durch fremde Nachrichtendienste ist in diesem Zusammenhang zu bedenken. Dieser besonderen Gefährdung durch Konzentration, die auch kostenintensive und riskante Angriffe lohnend erscheinen lassen würde, ließe sich durch Verteilung der geheimen Schlüssel auf möglichst viele Hinterlegungsstellen entgegenwirken, doch würde dies die Kosten für das System enorm erhöhen und im Gegenzug die Risiken durch technische Fehler steigern oder die Brauchbarkeit für den verfolgten Zweck beeinträchtigen.

Die durch die Realisierung dieser Gefahren angerichteten **Schäden** könnten vom Umfang her den eigentlich zu verhindernden Schäden durchaus entsprechen oder sie übersteigen. All diese Gefahren müßten auch dazu führen, daß das **Vertrauen** der Benutzer in die Verwendung kryptographischer Verfahren und in moderne Netze überhaupt erschüttert würde.

(d) Abwägung

Mithin stehen einem kaum spürbaren Vorteil für das Gemeinschaftsinteresse zahlreiche und schwerwiegende Nachteile für die Grundrechtsträger gegenüber. In Anbetracht dessen, daß auch das Key-Recovery-Modell nur von sehr zweifelhafter und jedenfalls geringer Eignung ist, den Interessen der Strafverfolgung und der öffentlichen Sicherheit kein genereller Vorrang vor dem Fernmeldegeheimnis zukommt (vgl. § 100a StPO) und die

[161] *Abelson u.a.*, unter 3.2.1

[162] *Abelson u.a.*, unter 3.2.2

[163] *Abelson u.a.*, unter 3.1.2; *Bizer* in KritJ 1995, 450, 463, unter 7.2.2

Nachteile die Grundrechtsträger in ihren geschützten Positionen schwer beeinträchtigen würden, muß die Regelung daher als unverhältnismäßig verworfen werden[164].

Auch das Totalverbot und das Verbot starker Kryptographie[165] können deshalb als noch einschneidendere Maßnahmen vor dem Grundsatz der Verhältnismäßigkeit keinen Bestand haben.

[164] so im Ergebnis auch *Bizer* in KritJ 1995, 450, 464, unter 7.2.2; *Hamm* in DuD 1997, 186, 191, unter 6; *Telesec*

[165] s.o. C II 2 b und C II 2 c

D. Zusammenfassung

In den offenen Netzen, die das Bild der Kommunikation im 21. Jahrhundert bestimmen werden, sind Daten dem unbefugten Mitlesen und Verändern schutzlos ausgeliefert. Starke Kryptographie erlaubt zuverlässig das technische Schützen von übermittelten oder gespeicherten Daten vor unbefugter Kenntnisnahme durch Verschlüsselung und bietet die Voraussetzungen für die digitale Signatur, mit deren Hilfe elektronische Dokumente einem bestimmten Urheber zugerechnet und vor unbemerkten Veränderungen geschützt werden können.

Die organisatorischen Anforderungen an sichere digitale Signaturen sind im Signaturgesetz (SigG) vom 22. Juli 1997 (BGBl. I S. 1870, 1872; FNA 9020-8) und der Signaturverordnung (SigV) vom 22. Oktober 1997 (BGBl. I S. 2498; FNA 9020-8-1) geregelt, die unter anderem eine Lizenzierungspflicht vorsehen für solche Personen, die die Zuordnung anderer Personen zu ihren Signaturschlüsseln verbindlich bescheinigen wollen (Zertifizierungsstellen). Daneben werden Aspekte des Datenschutzes und der Sicherheitsüberprüfung geregelt, aber keine spezielle Haftungsgrundlage und keine Form- oder Beweisfragen im Zusammenhang mit der digitalen Signatur.

Für den Bereich der Verschlüsselung bestehen in Deutschland nur vereinzelte Vorschriften im Recht der Telekommunikation, wobei § 8 Abs. 4 Satz 2 FÜV nicht so ausgelegt werden darf, daß er Betreiber von Telekommunikationsanlagen zwingen würde, Schlüssel der Kommunikationsteilnehmer an die Behörden auszuhändigen; es besteht lediglich eine Verpflichtung zum Aufheben nicht-teilnehmerautonomer Verschlüsselung im Einzelfall. Beschränkungen des Einsatzes teilnehmerautonomer Kryptographie wie ein totales Verbot, ein Verbot starker Kryptographie oder ein obligatorisches Schlüsselhinterlegungsmodell (Key Recovery) wären verfassungswidrig.

Literaturverzeichnis

- **Abelson, Harold; Anderson, Ross; Bellovin, Steven M.; Benaloh, Josh; Blaze, Matt; Diffie, Whitfield; Gilmore, John; Neumann, Peter G.; Rivest, Ronald L.; Schiller, Jeffrey I.; Schneier, Bruce:** „The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption“, 27. Mai 1997, http://www.crypto.com/key_study
- **Bauer, Friedrich L.:** Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie, 1. Auflage, Berlin u.a. 1995
- **Beutelspacher, Albrecht:** Kryptologie, 5. Auflage, Braunschweig/Wiesbaden 1996; im Internet: http://www.uni-giessen.de/~gcb6/krypto.html (Einleitung, S. 1 - 7)
- **Beyer, Wolfgang; Katzenschwanz, Ulrich:** Internetdienste im Münchner Hochschulnetz, 25. Februar 1997, http://www.lrz-muenchen.de/services/netzdienste/internet/
- **Bizer, Johann:** Schutz der Vertraulichkeit in der Telekommunikation, in: Kritische Justiz (KritJ) 1995, S. 450 - 465; auch erschienen als: Kryptokontroverse – Der Schutz der Vertraulichkeit in der Telekommunikation, in: Datenschutz und Datensicherheit (DuD) 1996, S. 5 - 14
- **Bizer, Johann:** Rechtliche Bedeutung der Kryptographie, in: Datenschutz und Datensicherheit (DuD) 1997, S. 203 - 208
- **Bizer, Johann; Fox, Dirk:** „Digital signierte Zukunft?“, in: Datenschutz und Datensicherheit (DuD) 1997, S. 66
- **Diffie, Whitfield; Hellman, Martin E.:** New Directions in Cryptography, in: IEEE Transactions on Information Theory 1976, Vol. IT-22, S. 644 - 654
- **Dobbertin, Hans:** Digitale Fingerabdrücke. Sichere Hashfunktionen für digitale Signaturen, in: Datenschutz und Datensicherheit (DuD) 1997, S. 82 - 87
- **Dreier, Horst (Hrsg.):** Grundgesetz. Kommentar, 1. Auflage, Tübingen 1996
- **Engel-Flechsig, Stefan; Maennel, Frithjof A.; Tettenborn, Alexander:** Das neue Informations- und Kommunikationsdienste-Gesetz, in: Neue Juristische Wochenschrift (NJW) 1997, S. 2981 - 2992

- **Fox, Dirk:** Fälschungssicherheit digitaler Signaturen. Eine Übersicht, in: Datenschutz und Datensicherheit (DuD) 1997, S. 69 - 74
- **Fox, Dirk:** „Gateway: Signaturschlüssel-Zertifikat“, in: Datenschutz und Datensicherheit (DuD) 1997, S. 106
- **Fox, Dirk:** „Gateway: Key Recovery“, in: Datenschutz und Datensicherheit (DuD) 1997, S. 227
- **Geis, Ivo:** Die digitale Signatur, in: Neue Juristische Wochenschrift (NJW) 1997, S. 3000 - 3004
- **Gerling, Rainer W.:** Verschlüsselungsverfahren. Eine Kurzübersicht, in: Datenschutz und Datensicherheit (DuD) 1997, S. 197 - 202
- **Görisch, Christoph:** Die Inhalte des Rechtsstaatsprinzips, in: Juristische Schulung (JuS) 1997, S. 988 - 992
- **Gramlich, Ludwig:** „Elektronisches Geld“ im Recht, in: Datenschutz und Datensicherheit (DuD) 1997, S. 383 - 389
- **Grimm, Rüdiger:** Kryptoverfahren und Zertifizierungsinstanzen, in: Datenschutz und Datensicherheit (DuD) 1996, S. 27 - 36
- **Hamm, Rainer:** Kryptokontroverse, in: Datenschutz und Datensicherheit (DuD) 1997, S. 186 - 191
- **Herreiner, Dorothea K.:** Die volkswirtschaftliche Bedeutung elektronischen Geldes, in: Datenschutz und Datensicherheit (DuD) 1997, S. 390 - 395
- **Heuser, Ansgar:** „Kryptographie: der Schlüssel zu den Netzen“, in: Bundesministerium für Wirtschaft, Referat Öffentlichkeitsarbeit (Hrsg.): Die Informationsgesellschaft. Fakten. Analysen. Trends, November 1996, Kapitel 3, http://www.bmwi-info2000.de/gip/fakten/zeitbild/kapitel3.html#3.4
- **Hortmann, Michael:** „Kryptoregulierung weltweit – Überblick“, in: Datenschutz und Datensicherheit (DuD) 1997, S. 214 - 215
- **Hortmann, Michael:** „Wie sicher ist die PIN? Zum Scheckkarten-Urteil des OLG Hamm“, in: Datenschutz und Datensicherheit (DuD) 1997, S. 532 - 533
- **Huhn, Michaela; Pfitzmann, Andreas:** Technische Randbedingungen jeder Kryptoregulierung, in: Datenschutz und Datensicherheit (DuD) 1996, S. 23 - 26

- **Huhn, Michaela; Pfitzmann, Andreas:** Krypto(de)regulierung, in: Datenschutz-Nachrichten (DANA) 1996, Heft 6, S. 4 - 13; im Internet: http://www.informatik.uni-hildesheim.de/FB4/Projekte/sirene/lit/abstr96.html#HuPf2_96
- **Jaeger, Kurt:** Anmerkungen zur zukünftigen Technik des Internet, in: Rost, Martin (Hrsg.): Die Netz-Revolution. Auf dem Weg in die Weltgesellschaft, 1. Auflage, Frankfurt (Main) 1996, S. 180 - 193
- **Knorr, Michael; Schläger, Uwe:** „Datenschutz bei elektronischem Geld. Ist das Bezahlen im Internet anonym?“, in: Datenschutz und Datensicherheit (DuD) 1997, S. 396 - 402
- **Köhntopp, Kristian:** „Was ist das Internet? Ein Überblick“, in: Rost, Martin (Hrsg.): Die Netz-Revolution. Auf dem Weg in die Weltgesellschaft, 1. Auflage, Frankfurt (Main) 1996, S. 20 - 36
- **Köhntopp, Kristian:** „Wer beherrscht das Internet?“, in: Rost, Martin (Hrsg.): Die Netz-Revolution. Auf dem Weg in die Weltgesellschaft, 1. Auflage, Frankfurt (Main) 1996, S. 63 - 69
- **Kropholler, Jan; Berenbrok, Marius:** Studienkommentar BGB. Erläutert für Studium und Examen, 2. Auflage, München 1995
- **Kuner, Christopher:** Die neuen „Crypto Regulations“ der USA und die deutsche „Kryptopolitik“, in: Neue Juristische Wochenschrift – Computerreport (NJW-CoR) 1997, S. 221 - 223; im Internet: http://www.beck.de/njw-cor/download/pdf-docs/kuner497.pdf
- **Maurer, Hartmut:** Allgemeines Verwaltungsrecht, 10. Auflage, München 1995
- **Medicus, Dieter:** Schuldrecht I. Allgemeiner Teil, 8. Auflage, München 1995
- **Möller, Ulf:** „Kryptographie: Rechtliche Situation, politische Diskussion“, 5. August 1997, http://www.thur.de/ulf/krypto/verbot.html
- **von Münch, Ingo (Begr.); Kunig, Philip (Hrsg.):** Grundgesetz-Kommentar. Band 1 (Präambel bis Art. 20), 4. Auflage, München 1992
- **Ohst, Daniel:** Vertrauliche Kommunikation, 9. Mai 1996, http://www2.rz.hu-berlin.de/~h0444saa/rdi/

- **Petersen, Holger:** Anonymes elektronisches Geld. Der Einfluß der blinden Signatur, in: Datenschutz und Datensicherheit (DuD) 1997, S. 403 - 410
- **Pieroth, Bodo; Schlink, Bernhard:** Grundrechte. Staatsrecht II, 11. Auflage, Heidelberg 1995
- **Roßnagel, Alexander:** Das Signaturgesetz. Eine kritische Bewertung des Gesetzentwurfs der Bundesregierung, in: Datenschutz und Datensicherheit (DuD) 1997, S. 75 - 81
- **Roßnagel, Alexander:** Kritische Anmerkungen zum Entwurf eines Signaturgesetzes, 12. Februar 1997, http://www.uni-kassel.de/fb6/oeff_recht/publikationen/kritanmerkung.html
- **Schmidt, Jens-Uwe; Ungerer, Bert:** Al dente, in: iX 1997, Heft 4, S. 128 - 131; im Internet: http://www.heise.de/ix/artikel/1997/04/128/artikel.shtml
- **Schneier, Bruce:** „Angewandte Kryptographie. Protokolle, Algorithmen und Sourcecode in C“, 1. Auflage der deutschen Übersetzung, Bonn u.a. 1996
- **Schwarz, Mathias:** „Merkmale, Entwicklungstendenzen und Problemstellungen des Internet“, 19. Juni 1996, http://www.jura.uni-muenchen.de/Institute/internet_I.html
- **Telesec:** Kryptokontroverse, 9. August 1996, http://www.telesec.de/recht3.htm
- **Timm, Birte:** Signaturgesetz und Haftungsrecht, in: Datenschutz und Datensicherheit (DuD) 1997, S. 525 - 528