DANA, Datenschutz-Nachrichten; Deutsche Vereinigung für Datenschutz, Reuterstr. 44, 53113 Bonn; 19/6 (1996) 4-13

Krypto(de)regulierung

Michaela Huhn
Univ. Hildesheim, Inst. für Informatik
Marienburger Platz 22, D-31141 Hildesheim
Tel. 05121 / 883-742, Fax -768
e-mail: huhn@informatik.uni-hildesheim.de

Andreas Pfitzmann
TU Dresden, Fakultät Informatik
D-01062 Dresden
Tel. 0351 / 463-8277, Fax -8255
e-mail: pfitza@inf.tu-dresden.de

Zusammenfassung

Durch die Verbreitung der Telekommunikation haben die Möglichkeiten zugenommen, unbeobachtet Informationen auszuspähen oder zu manipulieren, während das Schützen von Informationen gegen diese Gefahren erschwert wurde. Durch den Einsatz kryptographischer und steganographischer Verfahren verschieben sich die Kosten wieder zugunsten des Schützens. Diese Entwicklung wird von politischer Seite unterstützt, soweit sie nicht mit den Sicherheitsinteressen der jeweiligen Staaten kollidiert.

Als Hauptargument für eine rechtliche Regulierung von Kryptographie wird auf nationaler und internationaler Ebene die Bekämpfung der (organisierten) Kriminalität ins Feld geführt. Eine Regulierung kryptographischer Verfahren – besonders von Verschlüsselung zum Schutz der Vertraulichkeit – muß aber schon aus technischen Gründen ins Leere laufen. Insbesondere das organisierte Verbrechen kann jede Kryptoregulierung problemlos unterlaufen, während sie den Schutz aller anderen Anwender erheblich verringert und der Wirtschaft durch Wettbewerbsnachteile schadet. Vertreter der Wissenschaft und der deutschen Wirtschaft plädieren daher gegen eine Regulierung von Verschlüsselung.

Über politische Einflußnahme, insbesondere der USA, wird z.Z. versucht, Key-Recovery-Systemen zu einer marktbeherrschenden Position zu verhelfen. Key-Recovery-Systeme sollen den Sicherheitsdiensten den Zugriff auf Informationen gewährleisten, ihre technische Sicherheit wird aber zu Recht angezweifelt.

1 Die Informationsgesellschaft

Elektronische Datenverarbeitung und Telekommunikation sind heutzutage ein unverzichtbarer Teil des Alltags für Verwaltung, Wirtschaft und Privatpersonen. Zukunftsperspektive der "Informationsgesellschaft" ist es, durch neue Angebote im Bereich der Medien und der Telekommunikations-Dienstleistungen immer mehr Abläufe des Alltags zum Gegenstand der Datenverarbeitung zu machen. Die Verlagerung von unmittelbarer "Handlung" auf mittelbare Handlung unter Zuhilfenahme der elektronischen Datenübermittlung erzeugt bei Benutzern ein neues Schutzbedürfnis ihrer elektronisch übermittelten[1] Daten. Andererseits weckt die Perspektive, daß mehr relevante Informationen über Personen, Firmen oder politische Verbände elektronisch vergleichsweise einfach zugreifbar sein werden, natürlich die Begehrlichkeit der verschiedensten Interessenten, angefangen von neugierigen Nachbarn über Geschäftspartner und Marktforschungsinstitute, bis hin zu Kriminellen, Wirtschaftsspionen, in- und ausländischen Geheimdiensten, aber auch Strafverfolgungsbehörden.

Zur Zeit ist der technische und organisatorische Schutz der Daten bei Telediensten in keiner Weise mit dem Schutz der Daten bei "traditionell abgewickelten" Dienstleistungen zu vergleichen, da insbesondere das systematische Ausspähen und Manipulieren großer Datenmengen bei traditionellen

[1] Im folgenden wird Datenübermittlung als Oberbegriff für Datenübermittlung und -verarbeitung verwendet.

Dienstleistungen ungleich aufwendiger ist. Außerdem gilt für die traditionelle "Datenverarbeitung" etwa im persönlichen Gespräch oft ein besonderer rechtlicher Schutz (Betriebs-, Dienst-, Bank-, Arztgeheimnis). Ihm steht bei der Telekommunikation zwar der Schutz des Fernmeldegeheimnisses gegenüber. Das Fernmeldegeheimnis ist aber wesentlich unspezifischer, d.h. nicht den Schutzbedürfnissen der speziellen Handlung angepaßt, und auf Grundlage des G10 Gesetzes durch mehrere Gesetzen (§§100a, 100b StPO, §39 AWG) eingeschränkt.

Die moderne Kryptographie bietet verschiedene *technische*, inzwischen auch praktisch einsatzfähige Schutzmaßnahmen an, um die Integrität[2] und die Vertraulichkeit[3] elektronischer Datenübermittlung zu sichern. Der wirksame Schutz elektronisch übermittelter Informationen ist eine wesentliche Voraussetzung für eine breite Akzeptanz und Anwendbarkeit der neuen Teledienste und Medien. Mit Hilfe der Kryptographie können Benutzer, Teledienstanbieter und auch Betreiber der Übertragungsnetze erstmals einen technisch wirksamen, *autonom gestaltbaren* Schutz gegen unerwünschte Kenntnisnahme und Manipulation der übermittelten Daten durch Dritte realisieren.

2 Kryptographische und steganographische Systeme

Zunächst wird ein Überblick über die informationstechnische Struktur kryptographischer und steganographischer Systeme gegeben. Unterschieden wird zwischen Systemen zur vertraulichen Übermittlung von Information (Konzelationssysteme) und Systemen zur Sicherstellung der Integrität übermittelter Information (Authentikationssysteme). Darüber hinaus gibt es eine technische Unterscheidung zwischen sogenannten *symmetrischen* Verfahren, die nur einen – beiden Teilnehmern und sonst hoffentlich niemandem bekannten – Schlüssel verwenden, und *asymmetrischen* Verfahren, bei denen der Schlüssel in einen nur einem Teilnehmer bekannten geheimen Teil und einen öffentlichen Teil zerfällt *(public key cryptography).*

Allen beschriebenen Systemen ist gemein, daß sie jeweils ein festes (i.a. öffentlich bekanntes) Verfahren verwenden, der Schutz hingegen durch individuelle Schlüssel erreicht wird. Alle beschriebenen Systemtypen können sowohl in Hardware als auch in Software realisiert werden.

Für die Bewertung der Sicherheit kryptographischer Systeme wird eine Unterteilung in Bereiche vorgenommen, in denen das Verfahren vor äußeren Angriffen schützen kann – im folgenden **Angriffsbereich** genannt – und in Bereiche, die mit Hilfe *anderer* Maßnahmen geschützt sein müssen, im folgenden **Vertrauensbereiche** der jeweiligen Teilnehmer genannt.

Versagt der Schutz des Vertrauensbereichs, so kann das beste kryptographische System dem Teilnehmer keinerlei Sicherheit bieten. In einer Anwendung wird ein Vertrauensbereich häufig über ein dem Teilnehmer individuell zugeordnetes vertrauenswürdiges Benutzerendgerät (Chipkarte, Personal Organizer, PDA, Laptop, ...) realisiert. Es muß nicht nur gewährleistet sein, daß in Benutzerendgeräten keine die Sicherheit unterlaufende Soft- oder Hardware eingebaut ist, sondern auch, daß normale Nebeneffekte der Gerätefunktion nicht ausgenutzt werden können. Falls beispielsweise in Kryptogeräten transiente Fehlfunktionen ausgelöst oder auch nur beobachtet werden können, können mit gezielter Kryptoanalyse geheimzuhaltende Schlüssel ermittelt werden.[4] Zu erwarten ist, daß Strahlung (etwa Mikrowellen oder Wärme) in Chipkarten solche transienten Fehl-

---

2 Daten können nicht unerkannt unbefugt geändert werden.

3 Daten können nicht unbefugt verstanden werden.

4 D. Boneh, R. A. DeMillo, R. J. Lipton: On the Importance of Checking Computations (Extended abstract), Sept. 1996, E. Biham, A. Shamir: A New Cryptanalytic Attack on DES (Research Announcement, 18. Okt. 1996), The next Stage of Differential Fault Analysis: How to break completely unknown cryptosystems (Draft, 30. Okt. 1996), sowie popularisiert: Heiße Chipkarten geben Code Preis, Computer Zeitung 31. Okt. 1996, Seite 1.

funktionen induziert. Ross Anderson und Markus Kuhn berichten von praktischen Experimenten, bei denen durch kurzfristige Erhöhung des an Chipkarten angelegten Taktes ähnliche Fehlfunktionen gezielt herbeigeführt und aus einer einstelligen Zahl von manipulierten Transaktionen große Teile des geheimzuhaltenden Schlüssels bestimmt werden konnten.[5]

Dem kreativen, kriminellen Ausnutzen weiterer Funktionscharakteristika ist natürlich insbesondere bei Geräten, die schon beim regulären Betrieb in den Wirkungsbereich anderer übergehen, nur schwer eine Grenze zu setzen.

2.1 Konzelationssysteme

Die bekannteste, älteste und nach wie vor gebräuchlichste Sorte kryptographischer Systeme ist das **symmetrische Konzelationssystem**, s. Bild 1. Bekannte Vertreter sind DES und IDEA. Für symmetrische Konzelation sind effiziente Implementierungen verfügbar, die für hohe Übertragungsraten geeignet sind, und daher auch die Verschlüsselung von Sprache oder Videokonferenzdaten zulassen.

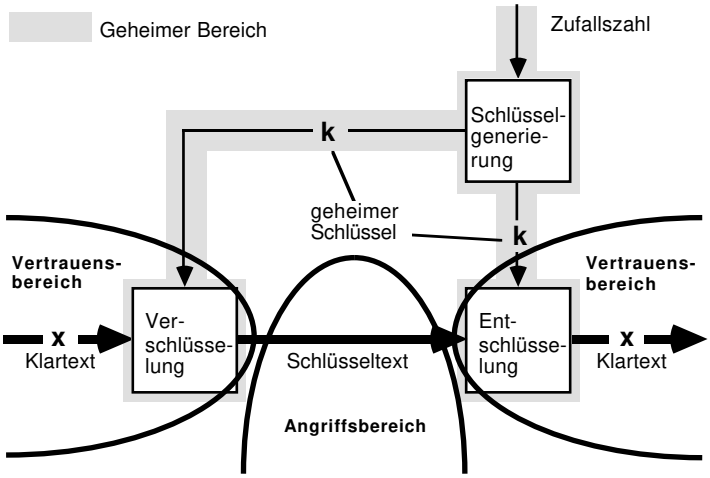

Bild 1: Symmetrisches Konzelationssystem

Bei symmetrischen Konzelationssystemen müssen Sender und Empfänger den gleichen geheimzuhaltenden Schlüssel kennen. Für eine sichere Schlüsselverteilung müssen sich die Teilnehmer daher treffen oder sich einer vertrauenswürdigen „**Schlüsselverteilzentrale**“ bedienen, die für Paare von Teilnehmern Schlüssel generiert und verschickt[6]. Die Schlüsselverteilzentrale kann dann natürlich die zwischen den Teilnehmern verschickten Nachrichten auch entschlüsseln und bildet, falls sie die Schlüssel auch speichert, ein wesentliches Sicherheitsrisiko im System. Eine dritte, sehr gebräuchliche Methode ist der Schlüsselaustausch mit Hilfe eines asymmetrischen Konzelationssystems.

---

5 Ross J. Anderson, Markus G. Kuhn: Improved Differential Fault Analysis (Ankündigung 15. Nov. 1996)

6 Vorausgesetzt, daß jeder Teilnehmer über einen Schlüssel verfügt, mit dem er sicher mit der Schlüsselverteilzentrale kommunizieren kann.

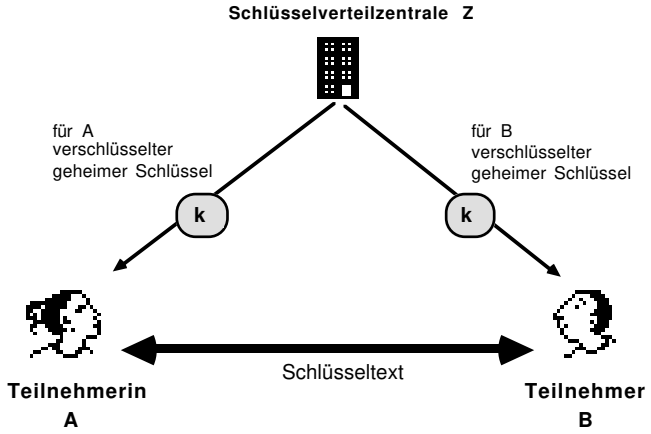

Bild 2: Schlüsselverteilung bei symmetrischen Konzelationssystemen

Asymmetrische Konzelationssysteme beruhen auf einfach zu berechnenden mathematischen Funktionen, die zur Zeit nur unter extrem hohen Rechenaufwand umkehrbar sind[7]. Bekannte Vertreter sind RSA und ElGamal. Heutige asymmetrische Konzelationssysteme verursachen einen um den Faktor 10^2 bis 10^3 höheren Rechenaufwand als symmetrische. Deshalb ist die Kombination mit symmetrischen Verfahren geschickt: Zu Beginn einer Sitzung wird über ein asymmetrisches Konzelationssystem ein Schlüssel vereinbart, mit dem dann die eigentliche Kommunikation über ein symmetrisches Verfahren verschlüsselt wird.

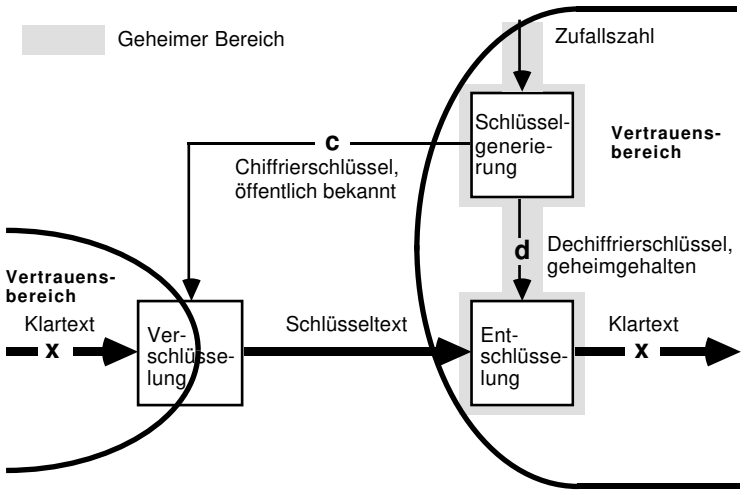

Bild 3: Asymmetrisches Konzelationssystem

Zum asymmetrischen Ver- und Entschlüsseln sind verschiedene Schlüssel c und d erforderlich, und nur d muß geheimgehalten werden. Das Verfahren steht und fällt mit der Annahme, daß d nicht mit vertretbarem Rechenaufwand (und damit Kapitaleinsatz) aus c oder dem Abhören verschlüsselter Nachrichten zu ermitteln ist. Asymmetrische Verfahren ermöglichen eine sehr einfache Schlüsselverteilung: Jeder Teilnehmer A kann sich selbst ein Schlüsselpaar (c_A, d_A) generieren und muß d_A nie

---

7 Das bekannteste Beispiel ist die Multiplikation: Während es vergleichsweise einfach ist, das Produkt zweier großer Primzahlen (>150 Stellen) zu bilden, gibt es nur sehr rechenaufwendige Algorithmen, um aus einem Produkt die Faktoren zu ermitteln. Daher können solche Funktionen zum Verschlüsseln verwendet werden.

jemand anderem mitteilen.[8] Der sogenannte *öffentliche* Schlüssel c_A muß nur noch in einem öffentlich zugreifbaren Schlüsselregister (Online-Datenbank) eingetragen werden, aus dem andere Teilnehmer c_A abrufen können, um damit Nachrichten an A zu verschlüsseln. Mit c_A verschlüsselte Nachrichten kann ausschließlich A (und nicht das Schlüsselregister) entschlüsseln.

Während bei der Verwendung von Kryptographie – sofern keine weiteren Schutzmaßnahmen ergriffen werden – im Kommunikationsnetz erkennbar ist, ob gerade vertraulich oder authentisiert kommuniziert wird, ist dies bei **Steganographie** nicht der Fall. Steganographische Konzelationssysteme betten geheimzuhaltende Nachrichten in harmlos wirkende Hüllnachrichten ein (vgl. Bild 4), so daß für Außenstehende, die nur den Stegotext beobachten, nicht einmal die Existenz der geheimen Nachricht erkennbar ist – und damit auch nicht ihr Inhalt. Insbesondere Multimedia-Kommunikation[9], aber auch bereits das normale ISDN-Telefon bieten geeignete Hüllnachrichten in Hülle und Fülle.

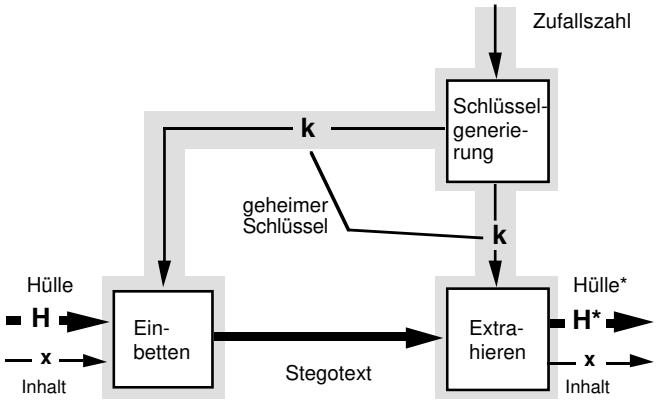

Bild 4: Symmetrisches steganographisches Konzelationssystem

2.2 Authentikationssysteme

Authentikationssysteme stellen die Integrität einer Nachricht sicher, während die Vertraulichkeit in der Regel nicht geschützt wird. Sie sollen gewährleisten, daß der Inhalt eines elektronischen Dokuments nicht unbemerkt manipuliert werden kann. Auch hier werden wieder symmetrische und asymmetrische Verfahren unterschieden.

Ein **symmetrisches Authentikationssystem** ist in Bild 5 dargestellt. An eine Nachricht wird ein Prüfteil (englisch: Message Authentication Code oder MAC) angehängt. Der Empfänger kann aus der Nachricht x und dem Schlüssel k ebenfalls den MAC bilden und prüfen, ob dieser mit dem empfangenen übereinstimmt.

Die Schlüsselverteilung kann – mit analogen Schwierigkeiten – wie bei symmetrischen Konzelationssystemen erfolgen. Die Integrität einer Nachricht kann nur insoweit gewährleistet werden, wie ausgeschlossen werden kann, daß unter (unerlaubter) Zuhilfenahme der Schlüsselverteilzentrale gefälschte Nachrichten in Umlauf gebracht werden.

---

8 Am sichersten geschieht die Schlüsselgenerierung in dem Gerät, das den geheimen Schlüssel später verwenden soll. Dann muß er dieses Gerät nie verlassen. Da Geräte, die asymmetrische Entschlüsselung durchführen können, auch zur Schlüsselgenerierung in der Lage sind, sollte der Vertrauensbereich wie in Bild 3 dargestellt realisiert werden.

9 Andreas Westfeld: Implementierung eines steganographischen Systems am Beispiel einer Videokonferenz; Belegarbeit, TU Dresden, 1. Nov. 1996; Elke Franz: Untersuchung von Bewertungsmöglichkeiten für Bilder bezüglich eingebetteter steganographischer Daten; Belegarbeit, TU Dresden, Nov. 1996

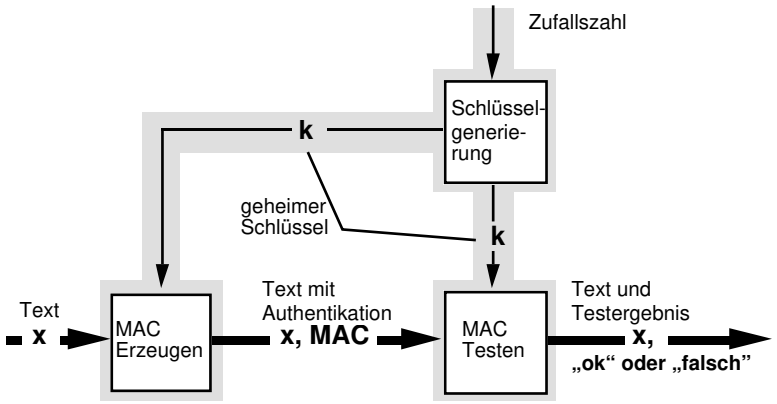

Bild 5: Symmetrisches Authentikationssystem

Asymmetrische Authentikationssysteme, auch als **digitale Signatursysteme** bekannt, vereinfachen zunächst die Schlüsselverteilung analog zu asymmetrischen Konzelationssystemen (s. Bild 6). Ihr Hauptvorteil ist aber ein anderer: Der Empfänger einer Nachricht kann gegenüber Dritten beweisen, daß die Nachricht von dem ausgewiesenen Absender *A* kam, sofern *A*'s Testschlüssel t_A öffentlich bekannt ist, was z.B. von einem Schlüsselregister gerichtsverwertbar beglaubigt werden könnte. Dies ist bei symmetrischen Authentikationssystemen nicht möglich: Selbst wenn die Schlüsselverteilzentrale bestätigt, daß *A* und *B* den gemeinsamen Schlüssel *k* hatten, kann *B* den MAC genausogut selbst erzeugt haben. Bei digitalen Signatursystemen ist jedoch *A* der einzige, der die Signatur erzeugen kann. Daher sind digitale Signatursysteme eine Voraussetzung für Rechtsverbindlichkeit elektronisch abgewickelter Handlungen.

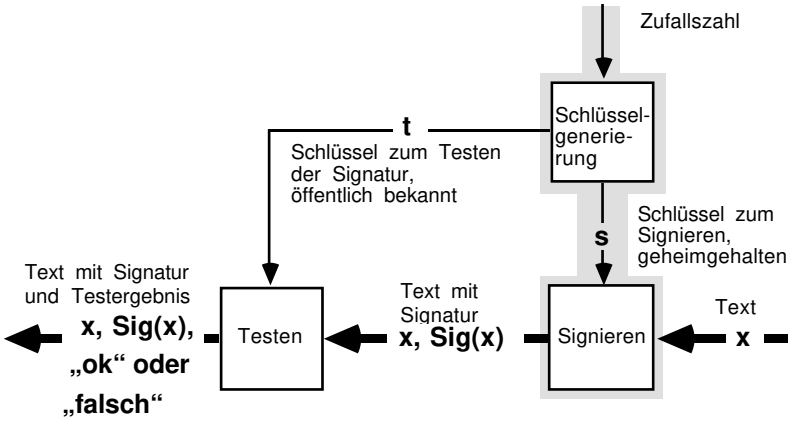

Bild 6: Signatursystem

Im Gegensatz zur symmetrischen Authentikation wird allerdings ein eigener Testalgorithmus benötigt, weil dem Empfänger der geheime Schlüssel *s* nicht vorliegt. Für Signatursysteme sind Schlüsselregister notwendig, um den *Zusammenhang* zwischen Schlüssel und Teilnehmer zu beglaubigen. Selbsterzeugte und privat ausgetauschte Signaturschlüssel können zwar zur Authentikation zwischen den Partnern benutzt werden, sind aber im Streitfall nicht zum Beweis geeignet.

Steganographische Authentikationssysteme sind unter dem Namen Watermarking bekannt – sie werden für die Wahrnehmung von Urheberrechten an digitaler Information eine wichtige Rolle spielen.

3 Praktischer Einsatz krypto- und steganographischer Systeme

Kryptographie wurde bisher im wesentlichen in der Geldwirtschaft und im staatlichen, insbesondere militärischen Bereich eingesetzt. Mit der Ausbreitung des Internets schützen aber immer mehr Privatpersonen und Interessengruppen ihre Nachrichten durch Verschlüsselung. Auf dem Internet und insbesondere durch seinen interaktiven multimedialen Informationsdienst www verbreiten sich kryptographische Freewarepakete wie *pretty good privacy* (*pgp*) von Philip Zimmermann bei interessierten privaten Benutzern. Damit stehen für nahezu alle Rechner lauffähige Implementierungen symmetrischer wie asymmetrischer Kryptographie für die Datenverschlüsselung zur Benutzung bereit. Ähnlich arbeitende Systeme gibt es inzwischen auch für die Sprachübertragung. Auch kommerzielle Verschlüsselungsgeräte für alle Arten von Kommunikationsanwendungen sind in den letzten Monaten auf den Markt gekommen.[10]

Bei steganographischen Systemen hat sich noch kein Quasi-Standard herausgebildet. Doch stehen auch hier im Internet zahlreiche Freeware-Programme zur Benutzung bereit[11], die laufend verbessert werden.

Natürlich können kryptographische und steganographische Systeme kombiniert werden[12].

4 Problembewußtsein ?!

Mit Ausnahme der Geldwirtschaft scheint Vertraulichkeitsverlust bei elektronisch übermittelten Daten in der Wirtschaft *noch* nicht als größere Gefahr wahrgenommen zu werden: In einer Umfrage der Zeitschrift KES[13] wird Manipulation, Spionage und Sabotage insgesamt nur von 7% der befragten Unternehmen als eine Hauptgefahr ihrer internen Informationssicherheit genannt, während Nachlässigkeit und Irrtum einen Anteil von 62% einnimmt. Fälle von krimineller Datenmanipulation oder -ausspähung kommen eher selten an die Öffentlichkeit, da sie natürlich auch immer dem Ansehen der betroffenen Unternehmen schaden.

Es häufen sich allerdings die Meldungen über Wirtschafts- und Politspionage. CIA-Chef William Webster gab bereits 1990 unumwunden zu, daß seine Behörde künftig selbst stärker in die Wirtschaftsspionage einsteigen werde – um zu garantieren, daß die Vereinigten Staaten wettbewerbsfähig blieben[14]. Die Sunday Times[15] meldete Anfang August 1996, daß der Verdacht bestünde, daß amerikanische Nachrichtendienste in das Computernetz des Europäischen Parlaments und der Europäischen Kommission eingebrochen wären, mit dem Ziel, die Verhandlungsstrategie der Europäer bei den GATT-Verhandlungen auszuspionieren, um sie an die US-Delegation weiterzuleiten. Ähnliche Vorwürfe gegen die CIA wurden von der französischen und japanischen Regierung erhoben. Andersherum wurde der französische Geheimdienst auch schon vom FBI beschuldigt, die europäischen Ableger der Computerkonzerne IBM und Texas Instruments auszuspionieren.

In den letzten Jahren ist das Problembewußtsein der InternetnutzerInnen deutlich gestiegen. Das Verschlüsseln und/oder Signieren wichtiger Nachrichten wird immer üblicher, wobei hierzu fast

---

10 z.B. Jürgen Axland: Fax- und Sprachverschlüsselung für jedermann; Siemens-Zeitschrift Special FuE, Frühjahr 1995, Seite 18-20

11 Einen Überblick findet man unter: Steganography http://www.cs.hut.fi/ssh/crypto/software.html#stego

12 Z.B. ist Stealth ein Filter für pgp, der alle Headerinformation abstreift und nur die verschlüsselten Daten für die steganographische Einbettung übrigläßt. Stealth ist erhältlich unter http://dcs.ex.ac.uk/~aba/stealth/.

13 Computerzeitung 43/96

14 ZEIT 51/1990 G. Freese: "Geheimdienste: Andere Ziele"

15 siehe auch Hamburger Abendblatt vom 5.8.1996

ausschließlich *pgp* verwendet und über die gegenseitige Zertifizierung öffentlicher Schlüssel durch die Teilnehmer selbst ein Vertrauensnetz aufgebaut wird.

5 Gesetzliche Maßnahmen und Gesetzesvorhaben

In den letzten Jahren traten mehrere Gesetze und Verordnungen in Kraft, die das Thema Kryptographie berühren[16]: Im Verbrechensbekämpfungsgesetz (1994) wurde der Bundesnachrichtendienst ermächtigt, den elektronischen Datenverkehr systematisch nach Schlüsselwörtern zu durchsuchen. 1995 trat die Fernmeldeverkehr-Überwachungs-Verordnung (FÜV) in Kraft, die insbesondere die Abhörbarkeit von Mobiltelefonen für die Sicherheitsbehörden sichern sollte. Daneben wurde §8 aber auch schon als "Kryptoverbot durch die Hintertür" diskutiert, doch bestehen erhebliche Zweifel an der Rechtmäßigkeit einer derartig weiten Auslegung (siehe Stellungnahme des Projektzentrums Telesec der Deutschen Telekom in Box 1).

Box 1: **Telesec: Das Fernmeldeanlagengesetz (FAG), ein heimliches Kryptogesetz?**
(am 14.11.96 kopiert von http://www.telesec.de/recht3.htm)
Als 1995 die auf Basis der Verordnungsermächtigung des § 10b FAG (Fernmeldeanlagengesetz) erlassene FÜV (Fernmeldeverkehr-Überwachungs-Verordnung) in Kraft trat, herrschte in Fachkreisen zunächst Verwirrung über eine zu Spekulationen Anlaß gebende Formulierung in § 8 Absatz 4 FÜV. Dort heißt es in Satz 2:

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.

Weil sich diese Formulierung so oder so ähnlich in einem Kryptogesetz wiederfinden könnte, herrschte anfänglich Streit darüber, ob § 8 Absatz 4 Satz 2 FÜV das "Kryptogesetz durch die Hintertür" sei. Der Streit war jedoch schnell beigelegt, da diese Verpflichtung als Kryptogesetz offensichtlich verfassungswidrig wäre. Die FÜV findet, wie erwähnt, ihre rechtliche Grundlage im FAG. Damit ist klar, daß sich sämtliche Verpflichtungen ausschließlich auf Fernmeldeanlagen und nicht auf davon unabhängige Dienstleistungen beziehen können. Jede weitergehende Verpflichtung würde den Rahmen der Verordnungsermächtigung des § 10b FAG sprengen und wäre bereits deswegen als verfassungswidrig einzustufen (Art. 80 GG). Darüber hinaus würde eine nur auf Betreiber von Fernmeldeanlagen beschränkte Verpflichtung, Schlüsselduplikate vorzuhalten und im Bedarfsfall zur Verfügung zu stellen, gegen den Gleichbehandlungsgrundsatz gemäß Art. 3 Absatz 1 GG verstoßen und müßte sich zudem allgemein an Art. 12 Absatz 1 GG messen lassen. Als eine weitere verfassungsrechtliche Schranke einer Auslegung des § 8 Absatz 4 Satz 2 FÜV im Sinne eines Kryptogesetzes wird in der juristischen Literatur die Verletzung des Fernmeldegeheimnisses der Teilnehmer genannt, da diese zwar eine Überwachung ihres Fernmeldeverkehrs, nicht aber die Preisgabe von auch zu anderen als zu Fernmeldezwecken nutzbaren Verschlüsselungsschlüsseln dulden müssen.

Im Sommer 1996 wurde das Telekommunikationsgesetz TKG beschlossen, das das Fernmeldeanlagengesetz FAG ablöst und bzgl. Überwachungsbefugnissen der FÜV weitgehend entspricht.

Zur Zeit arbeiten das Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie, das Wirtschafts-, Innen- und das Justizministerium an einem Gesetzentwurf, der die Rechtsgültigkeit elektronisch vorliegender Dokumente regeln soll, sofern sie bei der Übermittlung oder Speicherung

16 vgl. Ulf Möller: Kryptographie: Rechtliche Situation; http://www.thur.de/ulf/krypto/verbot.html sowie Bert-Jaap Koops: Crypto Law Survey; http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm

durch kryptographische Verfahren vor Verfälschung geschützt sind. Grundlage ist das "Signaturgesetz", das als Teil des sogenannten Multimediagesetzes[17] 1997 in Kraft treten soll und das Voraussetzungen bestimmt, unter denen eine digitale Signatur als fälschungssicher anzusehen ist, bzw. wann signierte Daten als unverfälscht anerkannt werden. Es sollen weitere Gesetze folgen, die die digitale Signatur der handschriftlichen Unterschrift (in Teilen) gleichstellen und signierten Dokumenten unter bestimmten Umständen Urkundencharakter verleihen. Die Anwendungen des "elektronischen" Rechtsverkehrs sind vielfältig: Geschäfte im Internet, die rechtsverbindliche elektronische Kommunikation zwischen Firmen und Behörden, sowie die elektronische Archivierung.

Neben der rechtlichen Regelung von Authentikationsverfahren prüft die Bundesregierung z.Z. auch die Regelung von Konzelationsverfahren[18]: Dazu wurde unter der gemeinsamen Federführung von Wirtschafts- und Innenministerium eine "Task Force Kryptopolitik" eingerichtet, die bis Ende 1996 "konkrete Vorschläge für eine umfassende politische Strategie im Bereich IT-Sicherheit vorlegen soll." In Äußerungen der Bundesregierung oder einzelner Minister wird stets der Konflikt zwischen dem verbesserten Schutz des Fernmeldegeheimnisses sowie der Notwendigkeit teilnehmerautonomer Verschlüsselungsverfahren zur Sicherung der Vertraulichkeit und "der Gefahr, daß durch den Einsatz der Verschlüsselungstechnik der Strafverfolgung künftig ein erheblicher Teil des Sachbeweises verloren geht."[19] gesehen. Beispielhaft ist die Erklärung von Wirtschaftsminister Rexrodt zur Einrichtung der Task Force Kryptopolitik am 7.10. 1996 (siehe Box 2).

Box 2: **Rexrodt: "Task Force Kryptopolitik" für mehr Sicherheit im Bereich Informationstechnologie** (7. Oktober 1996)

"Die Sicherheit der Kommunikation in offenen Netzwerken, wie dem Internet, ist von zentraler Bedeutung für die Entwicklung der Informationsgesellschaft insgesamt. Die Nutzer müssen sich darauf verlassen können, daß ihre Daten, die sich auf einem unkontrollierbaren Weg durch die globalen Datenlabyrinthe befinden, von keiner fremden Seite manipuliert, zerstört oder ausgespäht werden, damit sie das notwendige Vertrauen in die neuen Techniken gewinnen. (...)

Eine zentrale Frage ist hier, wie wir den Einsatz leistungsfähiger Verschlüsselungsverfahren auf breiter Front unterstützen können, damit für deutsche Nutzer ein wirksamer Schutz in weltweiten Datennetzen gewährleistet ist. Gerade für mittelständische Betriebe und private Haushalte, die große Mehrzahl der privaten Nutzer, ist es schwierig, den tatsächlichen Schutzwert von komplexen Verschlüsselungsverfahren zu beurteilen. Gerade sie sind darauf angewiesen, daß ein Ordnungsrahmen geschaffen wird, der ihren Sicherheitsbedürfnissen Rechnung trägt. Gerade diese Nutzer brauchen eine Infrastruktur unabhängiger und vertrauenswürdiger Instanzen, die Verschlüsselungsdienstleistungen auf öffentlich anerkanntem hohen Niveau anbieten.

(...)wichtig ist, daß jeder Nutzer die Freiheit hat zu wählen, welches Kryptographieverfahren er im Einzelfall einsetzen will. Und ebenso wichtig ist es zu verhindern, daß Kriminelle diese Instanzen mißbrauchen, um die dort angebotenen leistungsfähigen Verschlüsselungsverfahren zur Begehung von Straftaten zu nutzen. Hier muß ein sachgerechter und wirtschaftlich vertretbarer Ausgleich gefunden werden."

17 Der überarbeitete 2. Referentenentwurf des "Informations- und Kommunikationsdienste-Gesetzes – IuKDG" vom 8. Nov. 1996 wurde von Dr. Rüttgers inzwischen der Öffentlichkeit vorgestellt.

18 J. Bizer, Kryptokontroverse - Der Schutz der Vertraulichkeit in der Telekommunikation, DuD 1996, 1-14

19 Bundesinnenminister Kanther in der Computerzeitung 21/95.

6 Nationale Interessenvertreter

Wissenschaftler, die deutschen Kommunikationsnetzbetreiber und die Telekommunikationswirtschaft lehnen eine gesetzliche Kryptoregulierung zu großen Teilen ab. Verschiedene Verbände begrüßen die Initiative zu einem Signaturgesetz, äußern sich aber kritisch zu einer Kryptoregulierung. Häufig werden praktische Wirkungslosigkeit und potentielle Wettbewerbsnachteile genannt (siehe Box 4 und Kapitel 9), aber z.B. Telesec sieht auch verfassungsrechtliche Bedenken (siehe Box 5). Dagegen bestätigte BND-Chef Hansjörg Geiger, daß die Geheimdienste in Bonn auf ein Gesetz gegen das Verschlüsseln drängen:

Box 3: **BND-Chef Hansjörg Geiger** im Spiegel 34/1996, S. 25-29:
"Es ist zwingend erforderlich, den Privat-, den Banken-, den Geschäftsverkehr verstärkt durch Kryptierung gegen Angriffe von außen zu schützen. Gerade als Datenschützer sage ich das. Selbstverständlich aber muss es wie auf allen Gebieten, wo wir geschützte Bereiche haben, in besonderen Ausnahmefällen für staatliche Stellen möglich sein, gleichwohl an Informationen heranzukommen".

Box 4: Fachverband Informationstechnik im VDMA und ZVEI (25. September 1996)

Position zur Einführung des "Gesetzes zur digitalen Signatur" und zur Regulierung von Verschlüsselungsverfahren

(...) In den Zusammenhang mit der digitalen Signatur wird auch immer wieder die Diskussion um eine Kryptoregulierung gestellt, da die zugrunde liegenden Verfahren auch für Verschlüsselung nutzbar sind. Hier sind die berechtigten Interessen von Wirtschaft, Privatpersonen und Sicherheitsbehörden angemessen zu berücksichtigen. Unternehmen und Privatpersonen müssen sicher und vertraulich kommunizieren können, für die Sicherheitsbehörden geht es letztendlich darum, die gesetzlichen Abhörmöglichkeiten zu erhalten. Dabei ist zu berücksichtigen, daß aufgrund der technischen Entwicklung gegenwärtig keine realistische und wirtschaftlich tragbare Möglichkeit zu sehen ist, diese Zielsetzung aufrecht zu erhalten. Die früher geheime Kryptologie wird heute weltweit an Universitäten gelehrt und nicht zu überwindende Verschlüsselungsverfahren können z.B. über das Internet bezogen werden. Dazu kommen noch weitere Umgehungsmöglichkeiten wie die Steganographie. Vor diesem Hintergrund wird jede Regulierung der Verschlüsselung zwecks Aufrechterhaltung der Abhörmöglichkeiten von Sicherheitsbehörden zwangsläufig ins Leere laufen.

Die Verwendung sicherer Verschlüsselungsverfahren ist im Hinblick auf die Bedeutung der Ressource Information und die gleichzeitige Bedrohung durch Wirtschaftsspionage für die deutsche Wirtschaft unerläßlich. Eine Regulierung schafft nur unnötigen Verwaltungs- und Kostenaufwand in beträchtlicher Höhe und mindert die Exportchancen deutscher Sicherheitsprodukte. Sie trifft im Ergebnis nur gesetzestreue Unternehmen und Bürger, deren Verfahren darüber hinaus auch unsicherer werden (jede legale Zugriffsmöglichkeit kann auch mißbraucht werden, z.B. durch ausländische Dienste).

Deshalb sollte von einer Regulierung von Verschlüsselung zwecks Aufrechterhaltung der Abhörmöglichkeiten von Sicherheitsbehörden Abstand genommen werden.

Box 5: **Telesec (Deutsche Telekom AG): Kryptokontroverse**
(am 14.11.96 kopiert von http://www.telesec.de/recht3.htm)

Mit dem wachsenden Einsatz kryptographischer Verfahren im privaten und kommerziellen Umfeld werden auch die Forderungen nach einer staatlichen Kontrolle solcher Verfahren lauter. Die Diskussion bewegt sich dabei im Spannungsfeld zwischen staatlichen Sicherheits- und privaten Geheim-

haltungsinteressen. Beide Interessen sind grundsätzlich im Normengefüge verankert und lassen sich auch prinzipiell mit vertretbaren Argumenten in ihrer praktischen Relevanz begründen. Dennoch: Eine gesetzliche Beschränkung oder gar ein Verbot des nationalen Einsatzes kryptographischer Verfahren im privaten oder kommerziellen Umfeld gibt es in der Bundesrepublik nicht und jeder Versuch, solche Restriktionen durchzusetzen, muß sich sowohl einer verfassungsrechtlichen als auch einer praktischen Überprüfung unterziehen.

***Verfassungsrechtlich** ist in der Hauptsache das durch Art. 10 Abs. 1 GG (Grundgesetz) umfassend geschützte Fernmeldegeheimnis relevant. Einschränkungen dieses Rechts sind nur durch Regelungen möglich, die auf Basis der strengen Voraussetzungen des Art. 10 Abs. 2 GG erlassen wurden.*

Die bisher existenten Regelungen dieser Art lassen im wesentlichen nur ein Abhören (Überwachen und Aufzeichnen) der Kommunikation durch die dazu berechtigten Stellen (die sogenannten Bedarfsträger) zu. Ein diesem Vorgang nachgeschaltetes Dechiffrieren individuell verschlüsselter Kommunikation ist gesetzlich nicht geregelt und darf folglich nicht zu einer weiteren Einschränkung des Fernmeldegeheimnisses führen. Anders gesagt: Wenn im Rahmen einer Abhörmaßnahme nur kryptographisches Wirrwarr aufgezeichnet werden konnte, muß es die abhörende Stelle aus eigener Kraft leisten, dem Wirrwarr Klartext zu entlocken. Ein Anspruch beispielsweise darauf, daß die Deutsche Telekom AG als Anbieter von Verschlüsselungsverfahren Schlüsselduplikate ohne Einverständnis des Schlüsselinhabers vorhalten und bei Bedarf zur Verfügung stellen muß, besteht nicht. Im Gegenteil, schon ein nicht mit dem Schlüsselinhaber abgestimmtes Vorhalten von Schlüsselduplikaten würde gegen geltendes Datenschutzrecht verstoßen. Im Telekom Trust Center werden daher auch keine geheimen Verschlüsselungsschlüssel aufbewahrt. Diese werden vielmehr unmittelbar nach der Personalisierung einer Chipkarte unwiderruflich gelöscht. Anders wird nur auf ausdrücklichen Wunsch eines Kunden verfahren.

Auf der Suche nach Möglichkeiten, das Fernmeldegeheimnis über den Abhörvorgang hinaus weiter einzuschränken, werden aktuell zwei Optionen diskutiert. Das Verbot jeglicher privater oder kommerzieller Kryptographie und das Verbot nur der autonomen Kryptographie bei gleichzeitiger Zulassung von Diensteanbietern, die dann aber zur Aufbewahrung und Vorlage der Schlüsselduplikate verpflichtet sein sollen. Verfassungsrechtlich unbedenklich wären beide Optionen nur dann, wenn sie als verhältnismäßig gewertet werden könnten. Dies ist jedoch angesichts der nachfolgend aufgeführten praktischen Auswirkungen eines totalen oder eingeschränkten Kryptoverbots nicht der Fall, so daß beiden Optionen eine verfassungsrechtliche Unbedenklichkeit nicht bescheinigt werden kann. (...)

7 USA: Die "Clipper"-Initiative

Die Initiative zur derzeitigen Kryptoregulierungsdebatte kam aus den USA. Dort war das vielbenutzte symmetrische Konzelationssystem DES 1976 unter Mitarbeit von Sicherheitsbehörden entwickelt worden. Der Verdacht konnte nie ausgeräumt werden, daß den US-Geheimdiensten Methoden bekannt sind, DES-verschlüsselte Daten zu entschlüsseln. Auch Public-key-Verfahren gerieten bereits früh ins Interesse der Nachrichtendienste[20]. Ende der 80ziger Jahre hatte die National Security Agency (NSA) ein geheimgehaltenes Key-Escrow-Verfahren entwickelt, das im sogenannten Clipper-Chip implementiert und zum verbindlichen Standard für Konzelation in den USA erklärt werden sollte. Im Laufe einer heftigen politischen Debatte wurde die 1993 eingebrachte Clipper-Initiative in

20 Der RSA-Algorithmus ist in den USA patentiert und die Benutzung nur unter Verwendung von Bibliotheken zulässig, die von der patenthaltenden Firma RSA bereitgestellt werden und die Schlüssellänge auf 1024 Bit beschränken.

entscheidenden Punkten modifiziert: So sollte anfangs in jedem Clipper-Chip bei der Produktion ein "Universalschlüssel" eingespeichert werden, mit dessen Kenntnis jede über diesen Chip abgewickelte Verschlüsselung entschlüsselt werden könnte. Die ausschließlich amerikanischen Produzenten des Clipper-Chips sollten die Schlüssel dann in zwei Teile zerlegen, um sie dann bei zwei verschiedenen staatlichen Institutionen (den sogenannten **key escrow agents**) zu hinterlegen.

Nach anhaltender Kritik von Seiten der Internetnutzer und der Computerindustrie sollten auch unabhängige und privatwirtschaftliche Institutionen für die Schlüsselhinterlegung zugelassen werden, unter denen die Benutzer auswählen könnten (als "Clipper II" bekannt). Im nächsten Entwurf ("Clipper III", 5/96) sollten dann beliebige kryptographische Verfahren sowie beliebig lange Schlüssel zur Konzelation verwendet werden dürfen. Die Regierung schlug den Aufbau einer Schlüsselmanagement-Infrastruktur vor, die eine Hinterlegung der geheimen Schlüssel umfassen sollte. Die Teilnahme daran bzw. die Hinterlegung des Schlüssels bei einem unabhängigen Key Escrow Agent sollte "nur" für die Benutzer verpflichtend sein, die ein Public-Key-Zertifikat erwerben wollen. Seit Oktober 1996 gibt es eine weitere Variante, nach der die US-Regierung keine rechtsverbindliche Kryptoregulierung innerhalb der USA anstrebt, sich aber die Förderung von Key-Escrow-Produkten durch Marktbeeinflussung zum Ziel setzt: So sollen staatliche Institutionen bevorzugt Key-Escrow-Produkte kaufen und die Entwicklung weiterer Key-Escrow-Produkte unterstützt werden, sowie auf internationaler Ebene Key-Escrow gefördert werden. Des weiteren wird seit einiger Zeit nicht mehr von Key-Escrow-, sondern vielmehr von **Key-Recovery**-Systemen gesprochen.

Bezüglich der restriktiven US-Exportbeschränkungen für Kryptoprodukte scheint sich inzwischen die Erkenntnis durchzusetzen, daß der Verbreitung kryptographischer und steganographischer Verfahren über die großen Datennetze nicht wirksam Einhalt zu gebieten ist[21].

8 EU und OECD: "Trusted Third Parties"

In der EU wird zur Zeit auf die regulierende Wirkung des Marktes gesetzt. Die Europäische Kommission arbeitet an einem Vorschlag für eine europaweite Regelung, die den Sicherheitsbehörden den Zugriff auf verschlüsselte Daten ermöglichen soll. Die europäischen Varianten von Key-Recovery-Systemen firmieren unter der Bezeichnung **Trusted Third Party (TTP)-**Verfahren. Die Trusted Third Parties, staatliche oder privatwirtschaftliche Institutionen, haben auch eine im elektronischen Rechtsverkehr notwendige Funktion: Sie sollen die öffentlichen Testschlüssel digitaler Signaturen zertifizieren, also den Zusammenhang zwischen einem Teilnehmer und seinen digitalen Signaturen beglaubigen. Gleichzeitig sollen sie die Erzeugung und Speicherung von Schlüsseln für die Konzelation übernehmen[22], entsprechen also den amerikanischen Key Escrow Agents. Diese Lösung wird auch von der Senior Officials Group on Information Security (SOG-IS) favorisiert, die beratend an der europäischen Regelung mitarbeitet. Ein erster britischer Vorschlag für ein TTP-Verfahren liegt vor, ist aber noch technisch fehlerhaft.

Aus dem Europarat wurde im September 1995 eine restriktivere Empfehlung bekannt, die nahelegt, starke Kryptographie ohne Schlüsselhinterlegung einzuschränken[23], was in der Europäischen Kommission mit "Verwunderung und Empörung" aufgenommen wurde.

---

21 So wurde gegen Philip Zimmermann zwar wegen Verstoß gegen die Exportbeschränkungen im Zusammenhang mit der Bereitstellung von *pgp* auf international zugänglichen ftp-Servern ermittelt, aber dieses Verfahren ist inzwischen eingestellt.

22 Was zu einem deutlichen Verlust an Sicherheit führt, vgl. Kap. 2.1 FN 8.

23 Recommendation No. R (95) 13 of the Committee of Ministers to Member States.

In der OECD (Organisation for Economic Co-operation and Development) wird auf Betreiben der USA seit Ende 1995 an einer Richtlinie "Guidelines For Cryptography Policy" gearbeitet, die Anfang 1997 vom Council der OECD verabschiedet werden soll. Die geplante Richtlinie soll nichtverbindliche Empfehlungen für die IT-Sicherheitspolitik der Mitgliedsstaaten und auf internationaler Ebene enthalten.

Teilnehmer an den Verhandlungen sehen als Gründe[24] für die Anstrengungen der USA die praktische Wirkungslosigkeit der US-Exportbeschränkungen sowie den Druck der US-Telekommunikationsindustrie auf die Regierung. In der OECD scheint sich die vertrauenerweckendere Bezeichnung "Trusted Third Party" durchzusetzen. Während die USA, aber auch Frankreich und Großbritannien, auf eine verpflichtende Schlüsselhinterlegung drängen, favorisiert die EU eine auf Freiwilligkeit basierende Schlüsselhinterlegung, u.a. weil eine verbindliche Regulierung technisch nicht durchsetzbar ist; die skandinavischen Länder und Japan stehen jeder Kryptoregulierung sehr kritisch gegenüber. Für eine Mehrzahl der Regierungen ist eine zentrale (in den USA gelegene?) Schlüsselhinterlegung inakzeptabel. Die USA sind aber inzwischen bereit, sich an einer internationalen Schlüsselmanagement-Infrastruktur zu beteiligen und TTPs außerhalb der USA zuzulassen, sofern bilaterale Verträge zur Herausgabe der Schlüssel bestehen.

9 Technische Randbedingungen jeder Kryptoregulierung

Aus den technischen Eigenschaften krypto- und steganographischer Systeme ergeben sich bereits einige Randbedingungen für jede Regulierung ihres Einsatzes, sofern die Einhaltung der Regulierung überprüfbar sein soll (und ohne Überprüfbarkeit macht Strafandrohung wenig Sinn) und man nicht den Besitz frei programmierbarer Rechner allgemein einschränken will:[25]

Jede Sicherheitsinfrastruktur für digitale Signatursysteme ermöglicht den sicheren Austausch von Schlüsseln für Konzelationssysteme (Vertraulichkeitsschutz).

Jedes Konzelationssystem kann zum zunächst nicht bemerkbaren Austausch von Schlüsseln für weitere aufgesetzte Konzelationssysteme verwendet werden. Dies relativiert insbesondere den Nutzen von Key-Escrow-Systemen für die Verbrechensbekämpfung.

Mittels steganographischer Verfahren können Benutzer jede Einschränkung der Verwendung von kryptographischen Konzelationssystemen unterlaufen, sofern sie nur einen Bruchteil der vom Kommunikationssystem bereitgestellten Bandbreite benötigen. Auch steganographische Systeme können mit Schlüsseln parametrisiert und so in offenen Benutzergruppen sicher eingesetzt werden.

Außerdem sollte zwischen Schlüsseln zum Schutz von Kommunikation und solchen zum Schutz langfristig zu speichernder Daten unterschieden werden: Key-Escrow-Systeme zur Rekonstruktion verlorengegangener Schlüssel sind nur für die letztere Anwendung dem Nutzer dienlich, während sie für erstere vornehmlich den Sicherheitsbehörden die Überwachung der Kommunikation ermöglichen.

---

24 Summary Report on the OECD Ad Hoc Meeting of Experts on Cryptography by Stewart A. Baker, http://www.us.net/~steptoe/276908.htm

25 Entnommen M. Huhn, A. Pfitzmann: Technische Randbedingungen jeder Kryptoregulierung, DuD, Datenschutz und Datensicherheit, Vieweg-Verlag 20/1 (1996) 23-26 sowie unter http://www.informatik.uni-hildesheim.de/FB4/Projekte/sirene/lit/sirene.lit.html

10 Beurteilung von Key Recovery

Eine TTP-Variante, die auf nationalen Infrastrukturen beruht und privatwirtschaftliche TTPs zuläßt, erscheint vielen wesentlich akzeptabler. Eine Diskussion, wer *de facto* auf die Schlüssel zugreifen kann, muß aber nicht nur die Organisationsform berücksichtigen. Auch die TTPs werden beim Schutz der bei ihnen hinterlegten Schlüssel auf kryptographische Verfahren zurückgreifen. Da es praktisch unmöglich ist, kryptographische Verfahren gegen das systemeigene Betriebssystem und die Hardware abzuschirmen, muß davon ausgegangen werden, daß auch ein rechtlich/organisatorisch unabhängiges TTP eher wenig Vertraulichkeitsschutz gegen den Hersteller und Sicherheitszertifizierer seiner Systeme bietet. Bei der technischen Ausstattung der TTPs werden sich vermutlich einige wenige oder ein einziger Systemhersteller durchsetzen. Amerikanische Firmen sind bei Betriebssystemen und Prozessoren nahezu unangefochten Marktführer und sie lassen ihre Produkte bevorzugt vom National Computer Security Center (NCSC), betrieben von der NSA, sicherheitszertifizieren.

Nach wie vor sind sogar Key-Recovery-Systeme in der Diskussion, deren zugrundeliegende Algorithmen geheimgehalten werden mit dem Argument, daß dadurch die Sicherheit der Verfahren erhöht würde. In der Vergangenheit hat sich gezeigt, daß Geheimhaltung der Verfahren auf längere Zeiträume nicht mal für reine Hardwarerealisierungen gelingt, wenn die Systeme für die Massenbenutzung vorgesehen sind.[26] Inzwischen sind auch Softwareimplementierungen von Key-Recovery-Systemen mit geheimgehaltenen Algorithmen im Gespräch, die noch weniger gegen Reverse Engineering zu schützen sind.

Befürworter von TTP-Systemen argumentieren, daß ein Hinterlegen der Schlüssel an fremder Stelle auch im Interesse der Benutzer sei, da ihnen so bei Verlust ihres geheimen Schlüssels geholfen werden könne. Dies trifft allenfalls für Schlüssel zum Schutz langfristig zu speichernder Daten zu, nicht aber bei kryptographischem Schutz der Telekommunikation. Dort ist es im Falle eines Schlüsselverlustes nicht aufwendig, neue Schlüssel zu erzeugen und damit eine Datenübertragung zu wiederholen.

Bei der Authentikation langfristig zu speichernder Daten ist zusätzlich noch zwischen symmetrischen und asymmetrischen Verfahren zu unterscheiden, d.h. zwischen sogenannten Message Authentication Codes (MACs) und digitalen Signaturen: Während bei ersteren ein Hinterlegen des geheimen Schlüssels sinnvoll sein kann, da bei seinem Verlust die Authentikation der langfristig gespeicherten Daten nicht mehr zu überprüfen ist, ist bei letzteren ein Hinterlegen des geheimen Signierschlüssels unnötig, da digitale Signaturen auch bei Verlust des geheimen Signierschlüssels weiterhin mit dem öffentlichen Testschlüssel geprüft werden können. Bild 7 veranschaulicht die Situation.

---

[26] So wurden z.B. "wiederaufladbare" Telefonkarten in Umlauf gebracht, nachdem Konstruktionsdetails von Mitarbeitern verraten wurden.

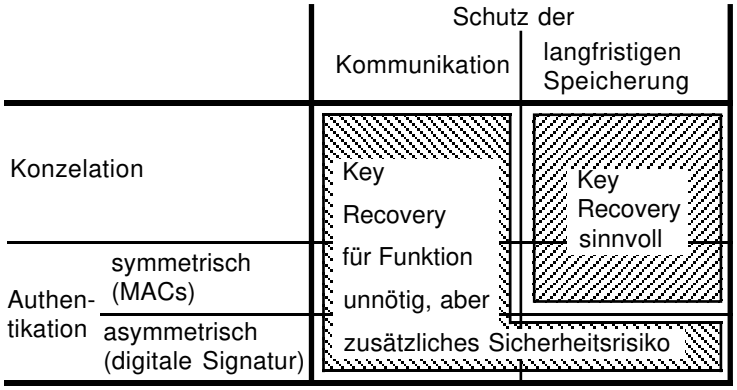

Bild 7: Wo ist Key Recovery sinnvoll, wo unnötig und ein zusätzliches Sicherheitsrisiko

Neben der Diskussion um die technischen Details werden auch zunehmend rechtliche Bedenken gegen Key-Recovery-Systeme laut. Einerseits werden – nicht nur in der Internetgemeinde – grundsätzliche Probleme benannt: So hat der dänische Technologierat festgestellt, daß eine Einschränkung der Verschlüsselungstechniken gegen Artikel 8 und 10 der europäischen Menschenrechtskonvention verstieße. Ein weiterer Kritikpunkt, der in mehreren Ländern aufkam, ist die Einschränkung der Kommunikationsfreiheit[27] durch eine Kryptoregulierung.

Andererseits sind aber auch Rechtsprobleme in der Strafverfolgung absehbar: Während in der Vergangenheit eine Abhörmaßnahme de facto mit der Installation eines Abhörgerätes begann und mit seinem Abbau beendet war, ist die Übergabe eines geheimen Schlüssels an die Sicherheitsbehörden zeitlich nicht eingrenzbar. Sowohl Nachrichten, die *vor* einer richterlichen Genehmigung einer Abhörmaßnahme verschickt wurden, aber noch gespeichert sind, als auch Nachrichten, die gesendet werden, *nachdem* die richterliche Genehmigung aufgehoben wurde, können entschlüsselt werden.

Auch auf internationaler Ebene sind sich die Experten einig, daß eine Kryptoregulierung und damit auch TTP-Verfahren von organisierten Kriminellen umgangen werden können. Trotz der bekannten technischen Risiken wird auf verschiedenen politischen Ebenen auf eine Sicherheitsinfrastruktur basierend auf TTP-Systemen hingearbeitet.

Wenn der Einsatz moderner krypto- und steganographischer Verfahren zunimmt, wird die Entschlüsselung von übermittelten Daten auch für Länder und Institutionen mit gut ausgebautem Zugriff auf nationale und internationale Telekommunikationsverbindungen zu einem weitgehend aussichtslosen Geschäft. Gleichzeitig wird die Entwicklung von Kryptogeräten, die bisher zu den Aufgaben der Sicherheitsbehörden gehörte, also staatlich kontrolliert war, von der Telekommunikations- und Computerindustrie übernommen. Die Initiative, TTP-Systeme zum (Quasi-)Standard für eine Sicherheitsinfrastruktur zu machen, sichert langfristig den Zugriff zumindest auf Teile der vertraulichen Telekommunikation und die Marktübersicht bei Verschlüsselungsprodukten für diejenigen, die beides heute haben (siehe Box 6).

Box 6: **Interview with David Herson** – Head of SOG-IS (25. September 1996)
(conducted by K. Westh Nielson, Engineering Weekly, Denmark)
(…)
Nielson: What do you think about the fact that the crypto debate focuses on privacy versus law enforcement?

27 Es ist auch zulässig, Telefonate in einem der 300 Hindi-Dialekte zu führen, ohne sich vorher zu versichern, daß die Sicherheitsdienste über einen kundigen Übersetzer verfügen.

D. Herson: Law Enforcement is a protective shield for all the other governmental activities. You should use the right word – we're talking about foreign intelligence, that's what we're talking about – that's what all this is about. There is no question – that's what it is about. The Law enforcement is a smoke screen, because we all understand law enforcement, policemen, courts, this is something we see everyday in our life. And it's an important element, I'm not suggesting it's not relevant but it is a protective shield for what goes on behind that. Countries like France and the United States, as you well know, are active. So at the OECD meeting at least half the people round the table understand that – not everybody but half of them do. And no solution will be acceptable unless it keeps that in balance as well.
In principle we want the government to protect us from terrorism and drug dealers, paedophilia or whatever bothers you today. And I think you can put a package around those interests – some of which you understand – some of which you don't. But you can identify them as something which is the public good as against the private good, and all we're trying to do is keep the public and private interest in balance. (...)

Falls sich die europäische Linie einer Kryptoregulierung über Marktbeeinflussung durchsetzen sollte, bleibt die Frage, wie sich der Markt entwickelt. Gerade im Kernbereich der Informationstechnik gibt es einige Beispiele[28] von Freeware-Systemen, die erfolgreich mit kommerziellen Produkten konkurrieren. Derartige Freeware-Systeme sind oft sogar besser gewartet und schneller bei der Anpassung an neue Systemarchitekturen, was sie nicht nur für private PC-Besitzer und Universitäten, sondern auch für kommerzielle Anwender interessant macht. Voraussetzung ist allerdings, daß eine vertrauenswürdige Organisation die Freeware-Systeme betreut, und daß ein hinreichend großer Interessentenkreis an ihrer Verbesserung mitarbeitet. Mit der Gründung einer Firma hat Philip Zimmermann hoffentlich die erste Voraussetzung erfüllt.

28 z.B. Emacs, Linux, GNU C-Compiler,...