Beitrag zum Buch "Internet & Politik – Von der Zuschauer- zur Beteiligungsdemokratie", Claus Leggewie, Christa Maar (Hrsg.), Bollmann-Verlag, Köln 1998, Seite 438-456

Verschlüsselungstechniken für das Netz*

Wie schützt man Vertraulichkeit und Integrität?

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

Einleitung

Weltweite Vernetzung, verbesserter Benutzerkomfort und Preisverfall haben von isolierten DV-Anwendungen zu offenen Systemen geführt und die wissenschaftliche Diskutierstube "Internet" in einen globalen, virtuellen Marktplatz verwandelt. Damit hat sich die elektronische Kommunikation, Verarbeitung und Archivierung von Informationen von einem Arbeitsmittel im Hintergrund zu einem in der öffentlichen Verwaltung, der Wirtschaft und bei Privatleuten akzeptierten Medium entwickelt, das herkömmliche Übertragungswege und Speicherungsformen zu verdrängen beginnt. Die einsetzende Verrechtlichung versucht einerseits als Reaktion auf diese Entwicklung Charakteristika herkömmlicher Verfahren auf die elektronische Kommunikation und Archivierung zu übertragen; andererseits beseitigt die Verrechtlichung eine der letzten Hürden beim Übergang zu einer integrierten elektronischen Archivierung, Verarbeitung und Übermittlung von Informationen, bei der auf eine dem Augenschein direkt zugängliche Darstellung wie etwa der Ausdruck eines Vertrages verzichtet werden kann.

Zu den wichtigsten Charakteristika jedweder Telekommunikations- und Archivierungsformen gehört der Schutz der *Integrität* und *Vertraulichkeit* von Informationen. Die moderne *Kryptographie* ist eines der wesentlichen technischen Hilfsmittel, um elektronisch vorliegende Informationen vor unbefugter Kenntnisnahme sowie unerwünschter Veränderung zu schützen. Die technische Sicherung von Integrität und Vertraulichkeit ist eine grundlegende Voraussetzung, um den Übergang zu rechtsverbindlicher elektronischer Kommunikation zu ermöglichen[1]. Im Internet weit verbreitete Programme wie PGP beweisen, daß der breite Einsatz kryptographischer Techniken heute einfach und ohne größere Leistungseinbußen möglich ist.

Allerdings unterscheidet sich der durch Kryptographie gewährleistete technische Schutz insbesondere bei der Informationsübermittlung von traditionellen Schutzmaßnahmen: In Zeiten des Postmonopols wurden Integrität und Vertraulichkeit von Briefen und Telefonaten geschützt, indem das Übermittlungsnetz von Unbefugten organisatorisch und physikalisch abgeschirmt wurde und die mit der Übermittlung beschäftigten, die Postangestellten, besonderen Pflichten zur Wahrung des Fernmeldegeheimnisses unterworfen waren. Schutzmaßnahmen waren also in erster Linie dem

---

* Teile dieses Artikels sind Überarbeitungen aus den früheren Artikeln "Krypto(de)regulierung; DANA, Datenschutz-Nachrichten; Deutsche Vereinigung für Datenschutz 19/6 (1996) 4-13 und "Technische Randbedingungen jeder Kryptoregulierung" in DuD, Datenschutz und Datensicherheit, Vieweg 20/1 (1996) 23-26.

1 So wird etwa in dem im August 1997 in Kraft getretenen Signaturgesetz auf als sicher bewertete kryptographische Verfahren Bezug genommen.

Netzanbieter Post anvertraut, und dieser staatlich organisierte Schutz konnte durch gesetzlich geregelte Eingriffe ins Fernmeldegeheimnis für die staatlichen Sicherheitsdienste aufgehoben werden. Im Gegensatz dazu liegt der Schutz durch kryptographische Techniken in den Händen des Benutzers. Vorausgesetzt die verwendeten Programme und Endgeräte sind sicher, steht und fällt der Schutz in den neuen Kommunikationsnetzen mit dem Zugang zu den geheim zu haltenden kryptographischen Schlüssel des einzelnen Benutzers. Einerseits ist die Verlagerung der Schutzmaßnahmen auf den Benutzer notwendig, da in Zeiten eines liberalisierten Telekommunikationsmarktes und technisch offener Systeme der organisatorische und physikalische Schutz eines staatlichen Fernmeldewesens nicht aufrecht gehalten werden kann. Andererseits werden die technischen Möglichkeiten der Sicherheitsdienste, das Fernmeldegeheimnis aufzuheben, damit erheblich beschränkt.

Der sinkende staatliche Schutz der Kommunikation kann also durch die wachsenden Möglichkeiten des eigenverantwortlichen Schutzes kompensiert werden, allerdings um den Preis verringerter staatlicher Kontrollmöglichkeiten. Zentrale Bedeutung für die Gestaltung kryptographischer Schutzmaßnahmen in einer Sicherheitsinfrastruktur eines Telekommunikationssystems hat die Erzeugung und Verwaltung der kryptographischen Schlüssel, deren Kenntnis für den Zugang zu den geschützten Informationen entscheidend ist. Die politischen Diskussionen darum sind entsprechend kontrovers.

Die Verfechter staatlicher Kontrollmöglichkeiten – Teile des Innenministeriums und der Sicherheitsdienste – fordern, die Organisation der Schlüsselverwaltung gesetzlich so zu regeln, daß den Sicherheitsdiensten die privaten Schlüssel der Benutzer für Überwachungsmaßnahmen zugänglich bleiben. Diese Hintertür für den Staat soll zumindest in alle verkäuflichen Produkte und Dienstleistungen eingebaut werden. Manche Hardliner treten sogar für die Strafbarkeit der Verwendung von Kryptographie ein, sofern sie keine derartige Hintertür enthält. Die Entwicklung in den USA geht bereits in diese Richtung: Mittels Standards für den öffentlichen Bereich und Exportkontrolle auf Hersteller wird starker Druck ausgeübt, in kryptographische Produkte Hintertüren einzubauen – wesentliche Schlagworte dort waren seit 1993 Clipper-Chip, Key-Escrow und neuerdings Key-Recovery. Seit Sommer 1997 wird ein Verbot von starker Kryptographie ohne Hintertür auch für den Einsatz innerhalb der USA vom FBI nun auch offiziell angestrebt.

Wirtschaft, das deutsche Wirtschafts- sowie Forschungsministerium und Bürgerrechtsbewegungen fordern dagegen den freien Einsatz starker Kryptographie ohne eine Hintertür. Diese Gruppen befürchten, daß jedwede Hintertür, die ein für den Benutzer unbemerkbares Entschlüsseln seiner Informationen erlaubt, zum Einfallstor für Datensammler aller Art wird und den notwendigen Integritäts- und Vertraulichkeitsschutz erheblich gefährdet. Zusätzlich ist zu erwarten, daß eine für die Verbrechensbekämpfung geschaffene Hintertür gerade im Fall strafrechtlicher Ermittlungen nicht weiter als bis zu einer nächsten kryptographisch verschlossenen Tür führt.

In diesem Artikel wird der Zusammenhang technischer Aspekte kryptographischer Systeme mit den Benutzeranforderungen an elektronische Telekommunikations- und Archivierungssysteme diskutiert. Nach einer Darstellung der mathematisch-technischen Grundmuster kryptographischer Verfahren werden Gestaltungs- und Regulierungsmöglichkeiten aufgezeigt und mit den Benutzeranforderungen in Beziehung gesetzt. Daraus ergibt sich eine Bewertung der zur Zeit in der politischen Diskussion geforderten Maßnahmen zur Kryptoreglementierung aus technischer Sicht.

Als Resümee ergibt sich: Eine gesetzliche Reglementierung von Kryptographie zum Zwecke der Verbrechensbekämpfung muß ihr Ziel verfehlen, hat aber gravierende Nachteile für die informationelle Selbstbestimmung und Sicherheit der Bürger wie auch für die Schutzinteressen der Wirtschaft.

1 Kryptographische und steganographische Systeme

Neben der Grundforderung, daß ein Kommunikationssystem die angebotenen Kommunikationsmöglichkeiten zuverlässig zur Verfügung stellt, haben Benutzer häufig zwei weitere Interessen:

1. Die Kommunikation, zumindest aber die Kommunikationsinhalte, sollen Unbefugten nicht bekannt werden (Vertraulichkeit).
2. Es soll nachprüfbar sein, ob die empfangene Information unverfälscht die ist, die abgeschickt wurde (Integrität). Für manche Anwendungen ist es sogar notwendig, daß der Empfänger die Unverfälschtheit gegenüber Dritten beweisen kann.

Nur wenn diesen Anforderungen in den neuen Kommunikationsnetzen Rechnung getragen wird, ist der Übergang von Briefpost auf e-mail oder der Abwicklung von Bestell- und Zahlungsvorgängen über das Internet verantwortbar.
Aufbauend auf vertrauenswürdigen Endgeräten sind Kryptographie und Steganographie wesentliche technische Hilfsmittel, um Vertraulichkeit und Integrität auch bei Kommunikation über offene Netze zu gewährleisten. Während mit Hilfe der Kryptographie Nachrichten so verschlüsselt werden können, daß Unbefugte zwar ihre Existenz wahrnehmen, nicht aber ihren Bedeutungsinhalt verstehen oder gezielt ändern können, versteckt die Steganographie geheimzuhaltende Nachrichten, so daß Unbefugte nicht einmal die Existenz einer Nachricht wahrnehmen können und damit weder den Bedeutungsinhalt verstehen noch gezielt ändern können.

In diesem Absatz 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 beiden Teilnehmern und sonst hoffentlich niemandem bekannte Schlüssel verwenden, und *asymmetrischen* Verfahren, bei denen jeder 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 oder steganographische 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.[2] Werden die Geräte schon beim regulären Betrieb in den Wirkungsbereich anderer übergeben, bieten sich

[2] In praktischen Experimenten konnten beispielsweise durch kurzfristige Erhöhung des an Chipkarten angelegten Taktes Fehlfunktionen gezielt herbeigeführt und aus einer einstelligen Zahl von manipulierten Transaktionen große Teile des geheimzuhaltenden Schlüssels bestimmt werden. Ross J. Anderson, Markus G. Kuhn: Improved Differential Fault Analysis (Ankündigung 15. Nov. 1996).

naturgegeben eine noch größere Anzahl von Möglichkeiten zur kriminellen Verwendung von Funktionscharakteristika.

1.1 Systeme zur vertraulichen Übermittlung von Information (Konzelationssysteme)

Das älteste, bekannteste und nach wie vor gebräuchlichste kryptographische System ist das **symmetrische Konzelationssystem**, s. Bild 1. Wie alle kryptographischen Systeme besteht es aus drei Algorithmen, die öffentlich bekannt sein sollten. Grau hinterlegt sind die Bereiche, wo Parameter der Algorithmen geheim gehalten werden müssen, etwa die Zufallszahl, die die Schlüsselerzeugung parametrisiert und der Schlüssel, der Ver- und Entschlüsselung steuert.[3] Bekannte Vertreter symmetrischer kryptographischer Konzelationssysteme sind DES und IDEA [Schn_96]. Für symmetrische Konzelation sind effiziente Implementierungen verfügbar, die für hohe Übertragungsraten geeignet sind, und daher auch die Verschlüsselung von Sprache oder Videokonferenzdaten zulassen.

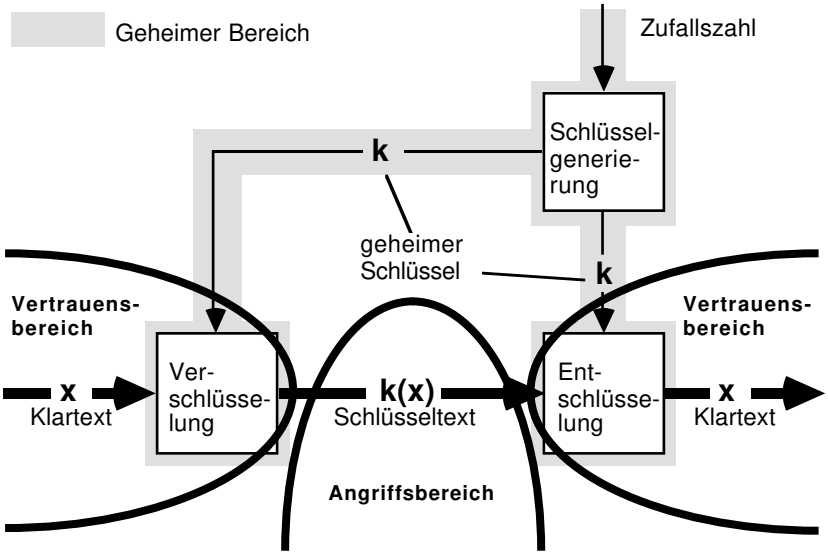

Bild 1: Symmetrisches kryptographisches Konzelationssystem

Jeder Teilnehmer *A* tauscht bei der Anmeldung zum offenen System einen Schlüssel mit einer zentralen Instanz *Z* aus, etwa k_{AZ}. Wenn nun *A* mit *B* kommunizieren will und noch keinen gemeinsamen Schlüssel mit *B* hat, so fragt er bei *Z* an. *Z* generiert einen Schlüssel *k* und schickt ihn sowohl an *A* als auch an *B*, und zwar mit k_{AZ} bzw. k_{BZ} verschlüsselt (Bild 2). Von da an können *A* und *B* den Schlüssel *k* benutzen, um in beide Richtungen verschlüsselte Nachrichten zu schicken. Vertraulichkeit gegenüber der zentralen Instanz kann mit diesem Verfahren nicht gewährleistet werden, außer *A* und *B* kann auch *Z* alle Nachrichten entschlüsseln.

---

3 Da geheime Parameter bei der Ausführung geheimzuhalten sind, sind die betreffenden Algorithmen ebenfalls grau hinterlegt.

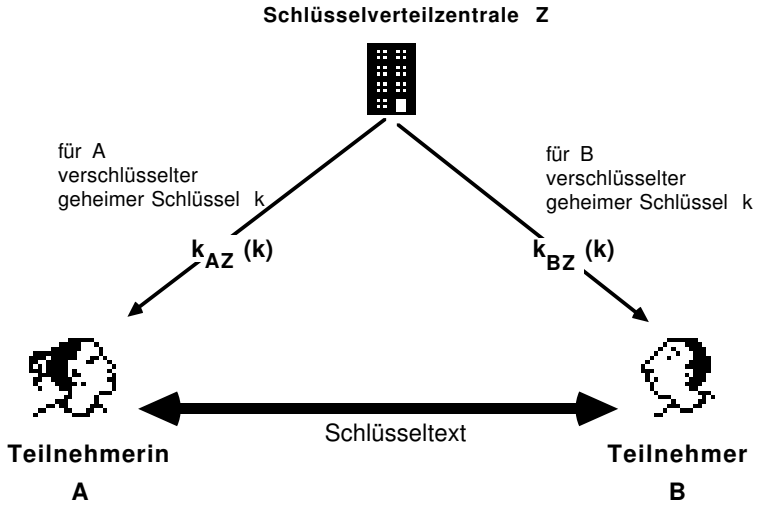

Bild 2: Schlüsselverteilung bei symmetrischen Konzelationssystemen

Asymmetrische Konzelationssysteme beruhen auf einfach zu berechnenden mathematischen Funktionen, die zur Zeit nur unter extrem hohen Rechenaufwand umkehrbar sind[4]. Bekannte Vertreter sind RSA und ElGamal [Schn_96]. 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.

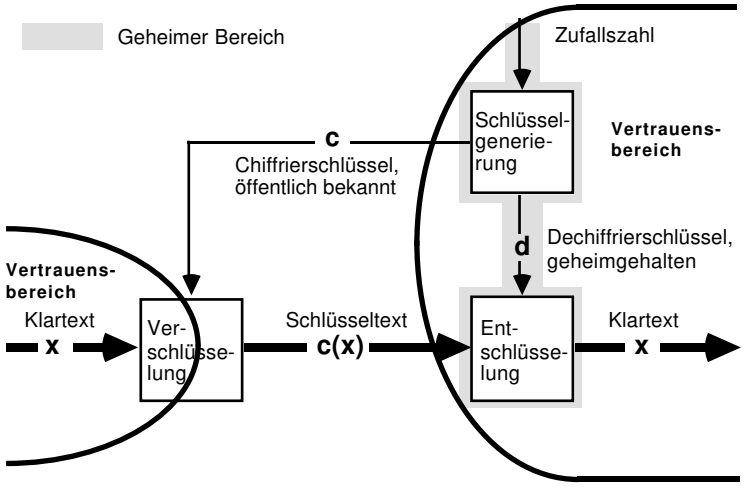

Bild 3: Asymmetrisches kryptographisches Konzelationssystem

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 Schlüsselver-

4 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.

teilung: Jeder Teilnehmer A kann sich selbst ein Schlüsselpaar (c_A, d_A) generieren und muß den geheimen Dechiffrierschlüssel d_A nie anderen mitteilen.[5] Der sogenannte *öffentliche* Schlüssel c_A muß nur noch in einem öffentlich zugreifbaren Schlüsselregister, etwa einer Online-Datenbank, eingetragen werden, aus dem andere Teilnehmer ihn abrufen können, um damit Nachrichten an A zu verschlüsseln. Mit c_A verschlüsselte Nachrichten kann ausschließlich A (nicht aber das Schlüsselregister) entschlüsseln.

Während bei der Verwendung von Kryptographie in der Regel 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 (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 (siehe etwa [West_97]), aber auch bereits das normale ISDN-Telefon [MöPS_94] bieten geeignete Hüllnachrichten in Hülle und Fülle.

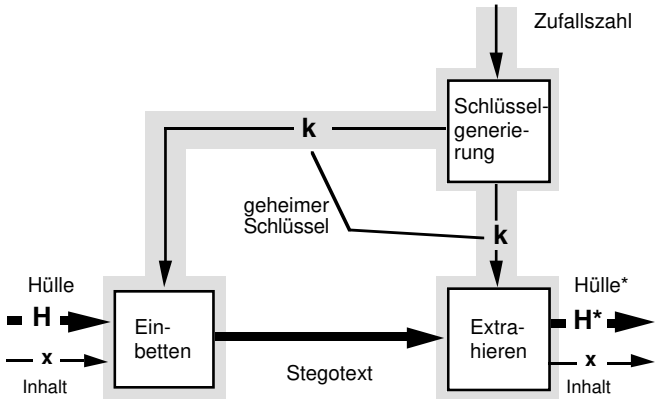

Bild 4: Symmetrisches steganographisches Konzelationssystem

1.2 Systeme zur Sicherstellung der Integrität übermittelter Information (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 kryptographisches 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 Problemen – 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.

---

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

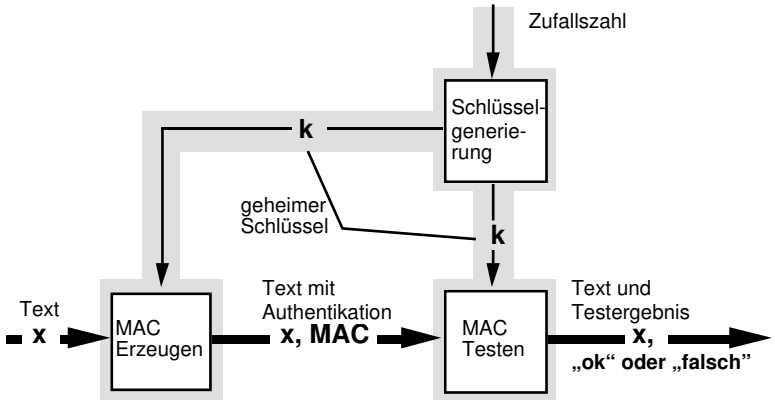

Bild 5: Symmetrisches kryptographisches Authentikationssystem

Asymmetrische kryptographische Authentikationssysteme, auch als **digitale Signatursysteme** bekannt, vereinfachen zunächst die Schlüsselverteilung analog zu asymmetrischen Konzelationssystemen (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 etwa 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 auch selbst erzeugt haben. Bei digitalen Signatursystemen ist jedoch *A* die einzige, die die Signatur erzeugen kann. Daher sind digitale Signatursysteme eine Voraussetzung für Rechtsverbindlichkeit elektronisch abgewickelter Handlungen.

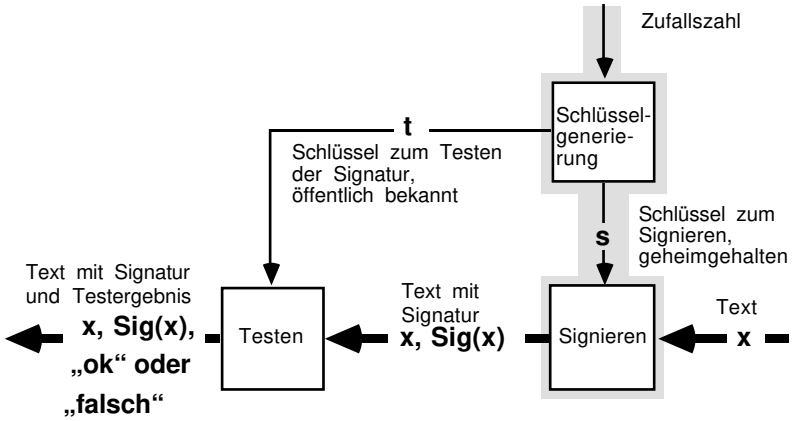

Bild 6: Digitales Signatursystem

Im Gegensatz zur symmetrischen Authentikation wird allerdings ein zusätzlicher Testalgorithmus benötigt, weil dem Empfänger der geheime Schlüssel *s* nicht vorliegt. Für Signatursysteme sind Schlüsselregister (engl. Certification Authorities) notwendig, um den *Zusammenhang* zwischen Schlüssel und Teilnehmer zu beglaubigen. Schlüsselregister, Schlüssel und zugehörige rechtsverbindliche Beglaubigungen bilden zusammen die *Sicherheitsinfrastruktur* des elektronischen Rechtsverkehrs – und wie wir sehen werden, der Sicherheit in offenen Netzen schlechthin. Die technisch/organisatorische Realisierung dieser Sicherheitsinfrastruktur steht im Zentrum der politischen Diskussion über die gesetzliche Regelung kryptographischer Anwendungen. Selbsterzeugte und lediglich 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.

2 Technische Randbedingungen kryptographischer Verfahren

Auf Grundlage der Funktionsprinzipien kryptographischer und steganographischer Verfahren werden nun die wichtigsten Anforderungen und technischen Gestaltungsmöglichkeiten diskutiert, die für die aktuelle Diskussion um eine Kryptoregulierung von Bedeutung sind.

2.1 Benutzeranforderungen an Signatur- und Konzelationsschlüssel

Digitale Signatursysteme werden zur Zeit für den elektronischen Rechtsverkehr[6] und die elektronische Archivierung eingeführt. Für beide Anwendungsbereiche ergeben sich Zertifizierungsanforderungen an Signaturschlüssel, die neben den kryptographischen Eigenschaften des Signatursystems Voraussetzung für die Rechtsverbindlichkeit digital signierter Dokumente sind. So muß der Empfänger einer signierten Nachricht nicht nur prüfen können, daß Nachricht und Signatur zum öffentlichen Testschlüssel passen, sondern er muß den öffentlichen Testschlüssel auch nachweisbar einer Person zuordnen können[7]. Hierfür sollen sogenannte TrustCenter – technisch-organisatorische Einheiten, die verschiedene vertrauenswürdige, der Sicherheit dienliche Dienstleistungen erbringen sollen –, auch die Funktion einer Certification Authority wahrnehmen. Die Erzeugung der Signaturschlüsselpaare in TrustCentern[8] kann zur Voraussetzung zur Teilnahme am elektronischen Rechtsverkehr gemacht werden, und damit besteht nun die Möglichkeit, alle geheimen Signierschlüssel dort zu speichern. Die Verwendbarkeit von Signatursystemen im elektronischen Rechtsverkehr beruht aber auf der Zusicherung, daß außer dem Besitzer eines geheimen Signaturschlüssels niemand eine entsprechende Signatur erzeugen kann. Eine Zugriffsmöglichkeit auf geheime Signaturschlüssel erlaubt das Fälschen von Beweismitteln und entwertet damit die ganze Sicherheitsinfrastruktur, auf der der elektronische Rechtsverkehr beruht.

Schlüsselpaare für Konzelation, also zum Vertraulichkeitsschutz, brauchen nicht in einem rechtlich bindenden Sinne zertifiziert zu werden. Es mag sinnvoll sein, beim Aufbau einer Infrastruktur Schlüsselzertifizierungen einzusetzen, um die Authentizität der verwalteten Schlüssel zu sichern. Damit kann verhindert werden, daß in einer Sicherheitsinfrastruktur Personen unter falschen Namen öffentliche Konzelationsschlüssel bereitstellen und auf diese Weise in den Besitz vertraulicher Nachrichten gelangen. Aber die Anforderung der Benutzer an Konzelationssysteme besteht darin, daß *sie* sich *gegenseitig* der Authentizität der öffentlichen Konzelationsschlüssel sicher sind, nicht daß sie diese vor Gericht nachweisen können. Daher können Kommunikationspartner, sobald es ihnen

---

6 Das Gesetz zur digitalen Signatur (Art. 3 des Informations- und Kommunikationsdienste-Gesetzes (IuKDG)) trat zum 1. Aug. 1997 in Kraft.

7 Daher werden der öffentliche Testschlüssel und die Identität der inhabenden Person von einer *Certification Authority* digital signiert, was als *Zertifizierung* des öffentlichen Schlüssels bezeichnet wird. Um solche Zertifikate überprüfen zu können, muß der Empfänger einer signierten Nachricht eventuell weitere Zertifikate einholen. Der entstehende Zertifizierungsbaum ist beispielsweise in X.509 und in eingeschränkter Form im Gesetz zur digitalen Signatur (bzw. der zugehörigen Verordnung) beschrieben.

8 Dies ist allerdings nicht empfehlenswert, da zentrale Systemkomponenten, auf denen die Ausführung verschiedener voneinander unabhängiger Teilaufgaben konzentriert wird, immer auch Schwachpunkte einer Sicherheitsarchitektur bilden, vgl. [FJPP_95], und es vereinfacht die Zertifizierung auch nicht.

gelungen ist, einmal Schlüssel auszutauschen[9], deren Authentizität sie vertrauen, jedes beliebige Konzelationssystem zur weiteren vertraulichen Kommunikation verwenden. Die Erzeugung von Schlüsselpaaren in sogenannten TrustCentern kann also für Konzelation nicht erzwungen werden, denn niemand ist beim Gebrauch der Konzelationsschlüssel auf Zertifikate von TrustCentern angewiesen.

Im folgenden argumentieren wir, daß Benutzer einen Schlüsselaustausch für eine gegenüber jedwedem Dritten vertrauliche Konzelation unter Verwendung der Sicherheitsinfrastruktur für den elektronischen Rechtsverkehr bzw. von Konzelationssystemen, bei denen die Hinterlegung der geheimen Konzelationsschlüssel vorgesehen ist, eigenständig realisieren können, ohne eine Einschränkung in ihren Anforderungen in Kauf nehmen zu müssen.

2.2 Digitale Signaturen ermöglichen den Austausch von Konzelationsschlüsseln

Jede Sicherheitsinfrastruktur für digitale Signaturen ermöglicht den sicheren Austausch von Schlüsseln für Konzelation: Nach bekannten Algorithmen [Schn_96], die bereits in allgemein verfügbaren Programmen implementiert sind (z.B. Pretty Good Privacy – PGP), kann jeder für Konzelation geeignete Schlüsselpaare generieren. Danach kann jeder seine öffentlichen Konzelationsschlüssel selbst zertifizieren, d.h. die Authentizität des Konzelationsschlüssels für andere überprüfbar machen, indem er etwa folgende Nachricht digital signiert: „Der öffentliche Schlüssel ... gehört ...“ (in Bild 7 die Nachricht $s_A(A,c_A)$). Eine Sicherheitsinfrastruktur für digitale Signaturen erlaubt nun jedem, die Unverfälschtheit dieser Nachricht zu prüfen[10] und sich so zu vergewissern, daß alles, was mit diesem öffentlichen Schlüssel verschlüsselt wird, nur vom Inhaber des Schlüsselpaares wieder entschlüsselt werden kann. Soll diese Verwendung eines Signatursystems ausgeschlossen werden, so besteht die einzige Möglichkeit darin, die Sicherheit der Signaturen zu untergraben, indem digital signierte Nachrichten in Umlauf gebracht werden, bei denen der Unterzeichner eben nicht der Eigentümer des Signierschlüssels ist. Damit ist natürlich jede Rechtsverbindlichkeit von Dokumenten, die in diesem System signiert wurden, hinfällig.

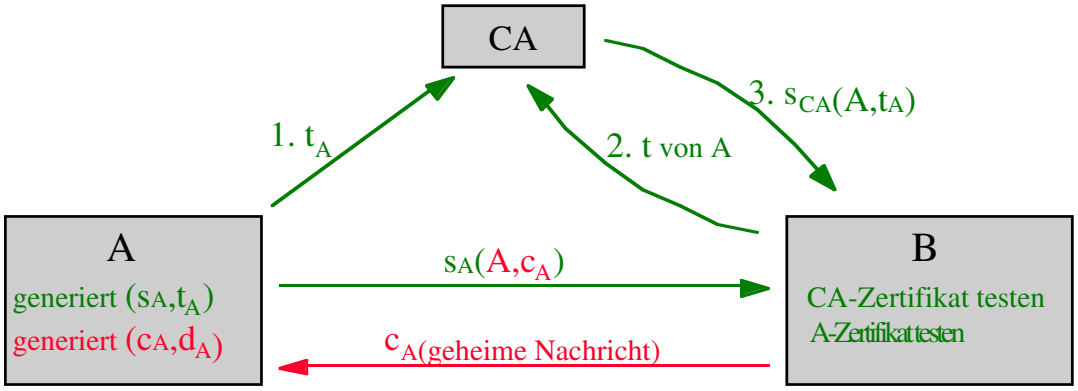

Bild 7: Sichere digitale Signaturen ermöglichen teilnehmerautonome sichere Konzelation

---

9 z.B. mit Hilfe der staatlich bereitgestellten Sicherheitsinfrastruktur, aber auch durch persönlichen Austausch von Schlüsseln.

10 indem er sowohl das Zertifikat $s_{CA}(A,t_A)$ der Certification Authority testet wie auch das Zertifikat, das sich Teilnehmer A selbst ausgestellt hat.

Konzelationsschlüssel, die mit Hilfe einer Sicherheitsinfrastruktur für digitale Signaturen verbreitet wurden, ermöglichen sowohl, Nachrichten vertraulich auszutauschen als auch Schlüssel für symmetrische Konzelationssysteme. Mit diesen kann dann effizienter konzeliert werden.

2.3 Key-Escrow-Systeme können zum zunächst unerkennbaren Schlüsselaustausch verwendet werden

Ähnlich wie sichere digitale Signaturen zum sicheren Austausch von Schlüsseln für Konzelation verwendet werden können, kann auch jedes Konzelationssystem, also insbesondere auch jedes Key-Escrow- und Key-Recovery-System, bei dem den Sicherheitsdiensten der Zugang zu den geheimen Schlüsseln ermöglicht werden kann, dazu benutzt werden, um Schlüssel für zusätzlich zu verwendende Konzelationssysteme zu vereinbaren (Bild 8). Statt einem Konzelationssystem direkt die vertraulich zu haltenden Nachrichten zu übergeben, wird zunächst ein öffentlicher Konzelationsschlüssel redundant kodiert übertragen. Der Empfänger überprüft den Schlüssel, ähnlich dem Prüfen des Zertifikates bei Verwendung digitaler Signaturen. Sofern er keine Verfälschung des öffentlichen Schlüssels feststellt, verwendet er den öffentlichen Schlüssel entweder, um geheim zu haltende Nachrichten zu verschlüsseln (Bild 8, 2. Pfeil) oder aber zum Austausch eines weiteren Schlüssels für ein symmetrisches Konzelationssystem, mit dem dann effizienter verschlüsselt werden kann (Bild 8, 4. Pfeil). Bei der weiteren Kommunikation werden dann die mit dem aufgesetzten Konzelationssystem bereits verschlüsselten Nachrichten mit dem zugrundeliegenden Key-Escrow-Konzelationssystem ein weiteres Mal verschlüsselt, wie dies in Bild mit Pfeil 3 und 4 angedeutet wird.

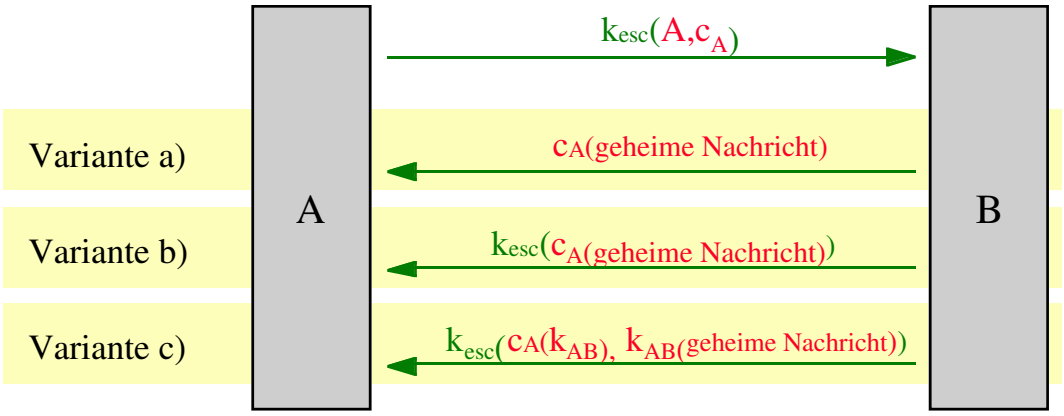

Bild 8: Key-Escrow-Konzelation ohne Dauerüberwachung ermöglicht Schlüsselaustausch und damit a) "normale" Konzelation, b) asym. Konzelation ohne Key-Escrow und c) sym. Konzelation ohne Key-Escrow

Die Verwendung zusätzlicher Verschlüsselungsmaßnahmen kann erst dann entdeckt werden, wenn die Schlüssel eines Key-Escrow-Systems herausgegeben und zum Entschlüsseln des Fernmeldeverkehrs benutzt wurden, was nach geltendem Recht eine Erlaubnis zur Überwachung des Fernmeldeverkehrs voraussetzt. Key-Escrow ist – wenn die Schlüsselherausgabe tatsächlich so zurückhaltend gehandhabt wird, wie in der öffentlichen Diskussion immer wieder betont wird – für die Ermittlungen der Sicherheitsbehörden, des Verfassungsschutzes, des Bundesnachrichtendienstes und MADs vermutlich kaum hilfreich, da gerade in den Fällen, wo Key-Escrow die Entschlüsselung von Nachrichten ermöglichen soll, höchstens die Verwendung zusätzlicher Verschlüsselungssysteme festgestellt werden kann. Daher wird neben der Einführung von Key-Escrow auch das Verbot anderer Verschlüsselungsverfahren diskutiert, was die Problematik allerdings in keiner Weise löst: Wird die

Überwachung des Fernmeldeverkehrs zurückhaltend gehandhabt, so wird ein Übertreten des Kryptoverbots häufig „zu spät“ bemerkt werden. Ein ernsthafter Durchsetzungsversuch des Kryptoverbots setzt also eine weitgehende Aushöhlung des Fernmeldegeheimnisses voraus. Doch selbst dann können sich Teilnehmer steganographischer Techniken bedienen (siehe unten), bei denen die Verwendung eines Verschlüsselungssystems praktisch nicht nachweisbar ist.

Daneben ist zu berücksichtigen, daß alle Stellen und Personen, die Kenntnis von dem geheimen Konzelationsschlüssel eines Benutzers erhalten haben, alle zu diesem Schlüssel gehörigen Nachrichten entschlüsseln können. Im Unterschied zu traditionellen Überwachungstechniken gerät damit das Ende einer Abhöraktion diffus, da die Kenntnis eines Schlüssels nicht rückholbar ist. Die zentrale Speicherung dieser sensiblen Informationen bei Key-Escrow-Agencies und Bedarfsträgern macht diese ggf. zu einem vielversprechenden Angriffspunkt für Wirtschaftsspionage und andere kriminelle Aktivitäten.

Kurzum: Key-Escrow zur Verbrechensbekämpfung wird weitestgehend wirkungslos bleiben – erfordert aber kaum realisierbaren technischen[11] und erheblichen organisatorischen[12] Aufwand, um die Aushöhlung der Rechte der Bürger und eine Steigerung der informationellen Verletzbarkeit von Wirtschaft und Gesellschaft in vertretbaren Grenzen zu halten.

2.4 Steganographie: Vertrauliche Nachrichten zu finden, ist unmöglich

Wie in Absatz 1.1 erläutert, können Nachrichten nicht nur durch kryptographische Konzelationssysteme vor unerwünschter Kenntnisnahme geschützt werden, sondern auch durch Steganographie. Dabei wird die zu schützende Nachricht in einer anderen längeren Nachricht versteckt. Selbst wenn Kryptographie – oder noch wesentlich allgemeiner: jede Form unüberwachbarer Kommunikation oder Speicherung – verboten würde, ist dem Anwender nichts zu beweisen, wenn die verwendete steganographische Technik gut ist.
Steganographie macht sich eine Grundtatsache der menschlichen Kommunikation zunutze, nämlich daß die gleiche Nachricht für unterschiedliche Empfänger eine unterschiedliche Bedeutung haben kann. In den modernen digitalen Kommunikationsnetzen können hocheffiziente Verfahren realisiert werden, mit denen Benutzer, ohne sich persönlich zu treffen und ohne daß es von Dritten nachgewiesen werden kann, Nachrichten austauschen können oder vereinbaren, wie sie zukünftig auszutauschende Nachrichten interpretieren wollen. Natürlich ist es möglich und zur Erhöhung der Sicherheit empfehlenswert, die zu schützende Nachricht vor dem steganographischen Verstecken noch zu verschlüsseln.

Die bereits verfügbaren und geplanten datenintensiven interaktiven Telekommunikationsanwendungen aus dem Multi-Media-Bereich bieten sich als Trägersysteme für steganographische Techniken geradezu an.

---

11 Wie soll eine Zugriffskontrolle in den Datenbanken der Key-Escrow-Agencies fehlerfrei realisiert werden, und gleichzeitig ein kurzfristiger Zugriff auf die Schlüssel möglich bleiben? Die Erfahrung, daß bisher *jedes* größere technische System Fehler enthielt, lehrt, daß derartige Risikozusammenballungen vermieden werden sollten.

12 Es ist erstaunlich, daß gerade die Bedarfsträger Key-Escrow fordern, deren Erfolge und Skandale doch häufig auf der Erfahrung „Jeder Mensch hat seinen Preis“ beruhen.

2.5 Maßnahmen bei Schlüsselverlust

Der Verlust[13] von Schlüsseln, die zum Schutz der Vertraulichkeit oder zur Integritätssicherung bei der *Übertragung* von Nachrichten verwendet werden, stellt für den Benutzer kein ernstliches Problem dar: Können etwa die mit Hilfe eines Konzelationssystems geschützten Daten nicht entschlüsselt werden, so generiert der Empfänger ein neues Schlüsselpaar und teilt dem Sender seinen neuen öffentlichen Konzelationsschlüssel authentisiert mit. Danach verschlüsselt der Sender die Daten unter Zuhilfenahme des neuen Schlüssels noch einmal und überträgt sie erneut. Diese Methode ist weit weniger aufwendig als jede sichere Form des Schlüsselbackups[14] und weitaus sicherer als Key-Escrow- und Key-Recovery-Systeme. Key-Escrow- und Key-Recovery-Systeme halten die geheimen Schlüssel für gesetzlich festgelegte Bedarfsträger, Sicherheitsbehörden und Nachrichtendienste vor, um ggf. eine Überwachung des Fernmeldeverkehrs zu ermöglichen, als technische Hilfe bei Schlüsselverlust sind sie überflüssig.

Gleiches gilt hinsichtlich Schlüsseln für Signaturen, vgl. Bild 9. Verliert der Inhaber seinen geheimen Signierschlüssel, kann er nicht mehr passend zu seinem öffentlichen Schlüssel signieren. Er kann sich aber jederzeit ein neues Schlüsselpaar generieren und den neuen öffentlichen Schlüssel zertifizieren lassen. Dieser muß den Empfängern von zukünftig signierten Nachrichten samt Zertifikat mitgeteilt werden.

Der Verlust öffentlicher Schlüssel ist praktisch nicht relevant, da ihre Öffentlichkeit beliebig weit verbreitete Speicherung gewährleistet.

Bei Schlüsseln für den Schutz der Vertraulichkeit oder der symmetrischen Authentikation längerfristig gespeicherter Daten[15] führt ein Verlust des geheimen Entschlüsselungs- bzw. Prüfschlüssels in der Regel zum Verlust der Daten bzw. ihrer Prüfbarkeit. Hier muß der Schlüsselinhaber also ggf. Vorsorgemaßnahmen wie Schlüsselbackup oder Key-Escrow einplanen.

Schlüsselbackup und Key-Escrow sind nur für Anwendungen sinnvoll, bei denen Daten nicht auf anderem Wege wiederbeschafft werden können, da die Sicherheit der geheimen Schlüssel in jedem Falle sinkt, wenn außer dem Schlüsseleigentümer noch weitere Personen oder Institutionen im Besitz (von Teilen) des geheimen Schlüssels sind.

---

13 Relevant für unsere Betrachtungen ist die Situation, daß Schlüssel vollständig verloren sind. Falls die Schlüssel in ungefugte Hände geraten können, sind weitere geeignete Maßnahmen zu ergreifen, etwa das Führen von Sperrlisten durch die Stellen, die Schlüssel zertifiziert haben. Bevor Teilnehmer Schlüssel verwenden, müssen sie bei der Stelle, die sie zertifiziert hat, nachfragen, ob der Schlüssel nicht gesperrt ist.

14 Hierzu kann jeder seine eigenen geheimen Schlüssel mit einem Schwellwertschema in Teile zerlegen und einzelne Teile an ihm vertrauenswürdig scheinende Freunde, Organisationen etc. weitergeben. Zur Rekonstruktion ist dann eine vom Teilnehmer vor der Zerlegung gewählte Mindestzahl an Teilen nötig. Bei geschickter Wahl dieser Mindestzahl können einerseits wenige doch nicht vertrauenswürdige Teilverwahrer den geheimen Schlüssel nicht rekonstruieren, andererseits verhindert der Verlust einzelner Teile nicht die Rekonstruktion.

15 etwa für Archivierungszwecke, z.B. in Grundbuchämtern oder im Gesundheitswesen.

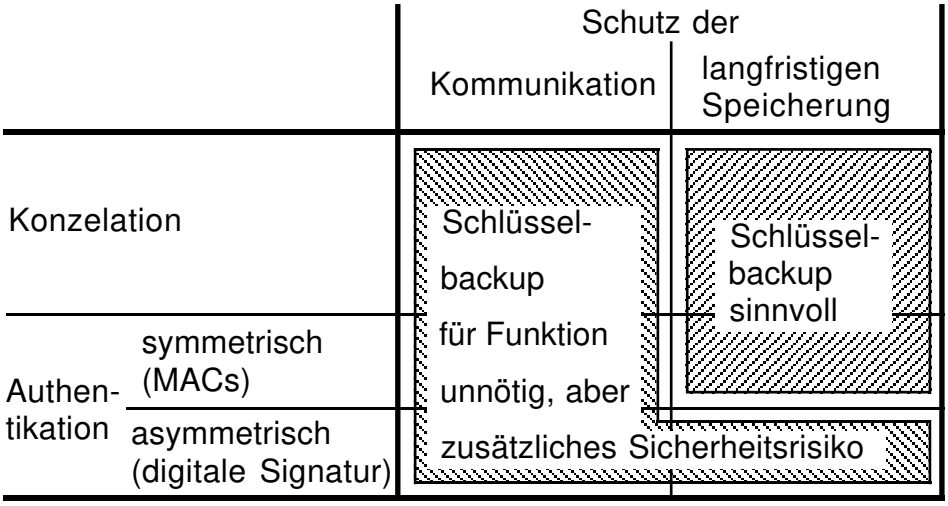

Bild 9: Wo ist Schlüsselbackup sinnvoll, wo unnötig und ein zusätzliches Sicherheitsrisiko

Für die Archivierung längerfristig gespeicherter Daten können also Schlüsselbackupmechanismen sinnvoll sein, die allerdings den Bedürfnissen der Benutzer Rechnung tragen sollten. So sollte jedes Schlüsselbackup technisch und organisatorisch so gestaltet werden, daß der Inhaber des Schlüssels von der Rekonstruktion des Schlüssels zumindest sofort erfährt, wenn nicht an ihr mitwirken muß. Nur so bleibt er über die Sicherheit seiner Daten im Bilde. Dies ist eine wichtige erste Verteidigunglinie gegen Mißbrauch [AABB_97 Kap. 2.3]. Gerade diese Forderung erfüllen Key-Escrow-Systeme nicht.

Benutzern von Verschlüsselung Key-Escrow-Systeme mit dem Argument nahe bringen zu wollen, damit sei auch ihr Schlüsselbackup-Problem gelöst, ist also unseriös: Zwei unabhängige Probleme, denen unterschiedliche Schutzinteressen zugrunde liegen, müssen auseinandergehalten und einzeln gelöst werden.

3 Schlußfolgerungen

Kryptographie ermöglicht jedem, Einzelnen wie Organisationen, Vertraulichkeit und Integrität seiner Informationen auch in Räumen ohne physische Kontrolle effizient selbst zu schützen. Geschieht dies nicht, so können beispielsweise beim Internet weiterhin Tausende neugieriger Systemverwalter den e-mail-Verkehr mitlesen und Geheimdienste die elektronische Kommunikation weiterhin sehr bequem für Zwecke der Wirtschaftsspionage auswerten. Ohne sichere Kryptographie kann Information im Netz beliebig manipuliert werden.

Die dezentrale Natur globaler digitaler Kommunikationsnetze hat den Nationalstaaten Kontroll- und Schutzmöglichkeiten entzogen. Kryptographie gibt den Einzelnen die Möglichkeit zurück, ihre Informationen selbst zu schützen. In einer Informationsgesellschaft geht Kryptographie deshalb alle an, da alle von ihrer (Un)Sicherheit betroffen sind!

Der Einsatz von Kryptographie wird deutlich sicherer, wenn Benutzer die für Kryptographie nötigen Schlüssel von ihren Geräten selbst erzeugen lassen. Das oft gehörte Argument, die Schlüsselerzeugung gehöre zum Zwecke der Verbrechensbekämpfung zusammen mit einer Aufbewahrung auch der geheimen Schlüssel zu den Aufgaben von staatlich autorisierten TrustCentern, ist aus den dargelegten technischen Gründen nicht haltbar. Das Argument, dies diene

sogar den Interessen des Nutzers, entpuppt sich bei genauer Betrachtung als unzutreffend. Entsprechendes gilt auch für Key-Escrow.

Eine Regulierung kryptographischer Techniken zur Konzelation mit dem Ziel der Verbrechensbekämpfung ist nicht sinnvoll, da eine Kryptoreglementierung nicht wirksam durchsetzbar ist, aber die Sicherheitsinteressen von Bürgern, Wirtschaft und Gesellschaft empfindlich beeinträchtigt. Die im Signaturgesetz vorgenommene fördernde Regulierung von Kryptographie zur Integritätssicherung und Beweiseignung digitaler Dokumente ist zu begrüßen.

Literatur

AABB_97 Hal Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Peter G. Neumann, Ronald L. Rivest, Jeffery I. Schiller, Bruce Schneier: The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption; Final Report – 27 May 1997; http://theory.lcs.mit.edu/~rivest/publications.html

FJPP_95 Hannes Federrath, Anja Jerichow, Andreas Pfitzmann, Birgit Pfitzmann: Mehrseitig sichere Schlüsselerzeugung; in: P. Horster (Hrsg.); Trust Center; Proc. der Arbeitskonferenz Trust Center 95; DuD Fachbeiträge, Vieweg, Wiesbaden 1995, 117-131

HuPf_96 Michaela Huhn, Andreas Pfitzmann: Krypto(de)regulierung; DANA, Datenschutz-Nachrichten; Deutsche Vereinigung für Datenschutz 19/6 (1996) 4-13

MöPS_94 Steffen Möller, Andreas Pfitzmann, Ingo Stierand: Rechnergestützte Steganographie: Wie sie funktioniert und warum folglich jede Reglementierung von Verschlüsselung unsinnig ist; Datenschutz und Datensicherung DuD 18/6 (1994) 318-326

Schn_96 Bruce Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C; John Wiley & Sons, (2nd ed.) New York 1996

West_97 Andreas Westfeld: Steganographie am Beispiel einer Videokonferenz; in: G. Müller, A. Pfitzmann (Hrsg.); Mehrseitige Sicherheit in der Kommunikationstechnik; Addison-Wesley, 1997, 507-525

Stichwörter

Kryptographie, Kryptoregulierung, Kryptographiegesetz, Verschlüsselung, digitale Signatur, Key-Escrow, Key-Recovery, Schlüsselbackup, TrustCenter, Konzelation, Vertraulichkeit, Steganographie