Beitrag zum IBM-Symposium "Internet und Security", 25.-26.09.1997 in Herrenberg

Kryptographie und Internet – Stand der Diskussion*

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

Kryptographie ist ein wesentliches Hilfsmittel, mit dem Information auch in Räumen ohne zentrale physische Kontrolle wie etwa dem Internet effizient gegen unbefugte Kenntnisnahme und/oder unbefugte unerkannte Änderung geschützt werden kann. Die dezentrale Natur globaler digitaler Kommunikationsnetze entzieht den Nationalstaaten Kontroll- und Schutzmöglichkeiten. Einerseits verstärkt Kryptographie diese Entwicklung, ermöglicht andererseits aber einen Selbstschutz der betroffenen Bürger und der Wirtschaft. Der sinkende staatliche Schutz der Kommunikation kann daher durch die wachsenden Möglichkeiten des eigenverantwortlichen Schutzes kompensiert werden, was allerdings die staatlichen Kontrollmöglichkeiten weiter verringert. Die politischen Diskussionen dieses Paradigmenwechsels sind entsprechend kontrovers.

In der Diskussion über Einsatz und Reglementierung kryptographischer Verfahren tritt häufig eine grundlegende Verwirrung über die technischen Zusammenhänge zutage. Oft sind die in ihnen aufgestellten Forderungen an die technische Gestaltung unerfüllbar oder den angestrebten Zielen nicht dienlich. Hauptthema der politischen Diskussion sind Erzeugung und Verwaltung kryptographischer Schlüssel. Dabei wird davon ausgegangen, daß kryptographische Systeme eine fest vorgegebene Systemarchitektur und einen bestimmten Verwendungsmodus (Integritätssicherung oder Vertraulichkeitsschutz) besitzen. Beide Annahmen sind falsch:

Jede Sicherheitsinfrastruktur für digitale Signatursysteme, die technisch zuverlässige Signierschlüssel bereitstellt, ermöglicht auch 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[1], also von Kryptosystemen mit zwangsweiser Hinterlegung von „geheimen“ Schlüsseln, die der Verbrechensbekämpfung dienen soll.

Außerdem kann jede datenintensive Anwendung mittels steganographischer Verfahren zum Konzelationssystem ausgebaut werden. Damit 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.

---

* Die Einführung in die Krypto- und Steganographie ist unserem Artikel "Krypto(de)regulierung; DANA, Datenschutz-Nachrichten; Deutsche Vereinigung für Datenschutz 19/6 (1996) 4-13 entnommen. Die Diskussion von (Un)Möglichkeiten zur Reglementierung von Kryptographie ist eine ergänzte Fassung unseres Artikels "Technische Randbedingungen jeder Kryptoregulierung" in DuD, Datenschutz und Datensicherheit, Vieweg 20/1 (1996) 23-26.

+ Teile dieses Artikels wurden während eines Gastaufenthalts bei INRIA Sophia Antipolis, Frankreich, erstellt.

1 Inzwischen wegen des freundlicheren Wortklangs häufig *key-recovery (crypto)system* genannt.

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

Resümee: Eine gesetzliche Reglementierung von Konzelationssystemen zum Zwecke der Verbrechensbekämpfung muß ihr Ziel verfehlen und sollte daher unterbleiben, da sie gravierende Nachteile für informationelle Selbstbestimmung und Sicherheit der Bürger wie auch für die Schutzinteressen der Wirtschaft hat.

1 Einleitung

Seitdem Rechner klein, billig und leistungsfähig geworden sind, ist der breite Einsatz kryptographischer Techniken problemlos möglich. Damit sind diese Techniken in das Zentrum politischer Diskussionen gerückt, ohne daß allen Beteiligten die technischen Randbedingungen bekannt sind. Deshalb gehen viele dieser Diskussionen – insbesondere solche über eine Kryptoregulierung zum Zwecke der Bekämpfung der sogenannten „Organisierten Kriminalität“ – in die Irre.

Dieser Beitrag führt in Kap. 2 die kryptographischen und steganographischen Systeme auf der geeigneten Abstraktionsebene ein. In Kap. 3 nennt er mathematisch-technische Grundzusammenhänge kryptographischer Systeme und zeigt Gestaltungs- und Regulierungsmöglichkeiten sowie Regulierungsgrenzen auf, die sich daraus ergeben. Anforderungen von politischer Seite, die dem nicht Rechnung tragen, sind *technisch* nicht realisierbar.

Eine breitere gesellschaftspolitische Diskussion über Krypto(de)regulierung ist in [HuPf_96] zu finden.

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 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. Ross Anderson und Markus Kuhn berichten von praktischen Experimenten, bei denen 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 konnten.[2]

Dem kreativen, kriminellen Ausnutzen weiterer Funktionscharakteristika ist 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 [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.

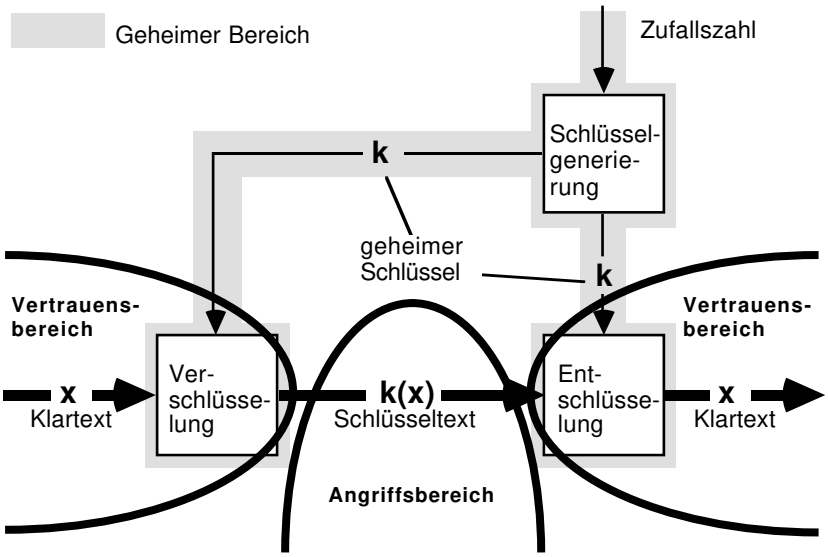

Bild 1: Symmetrisches kryptographisches Konzelationssystem

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 (vgl. 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.

---

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

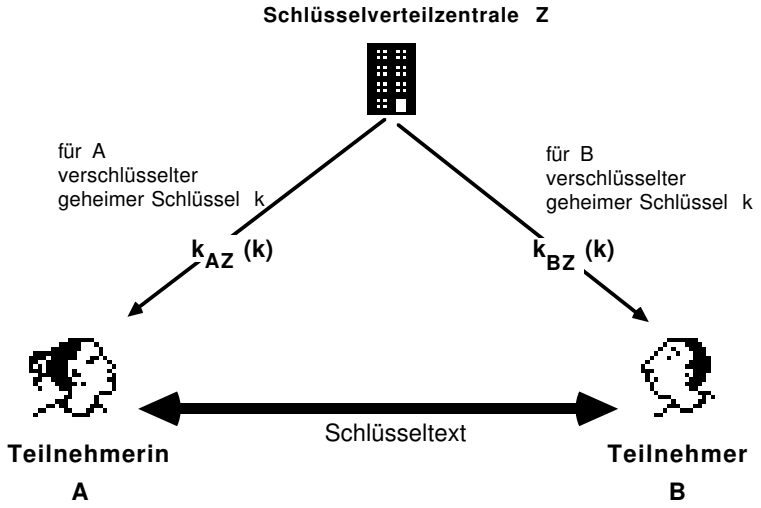

Bild 2: Schlüsselverteilung bei symmetrischen Konzelationssystemen

Asymmetrische Konzelationssysteme beruhen auf einfach zu berechnenden mathematischen Funktionen, die zur Zeit nur unter extrem hohen Rechenaufwand umkehrbar sind[3]. 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.

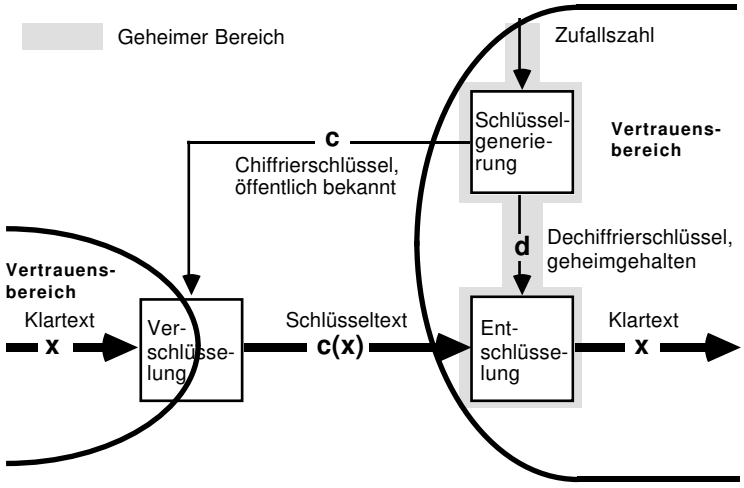

Bild 3: Asymmetrisches kryptographisches Konzelationssystem

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-

[3] 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.[4] Der sogenannte *öffentliche* Schlüssel c_A muß nur noch in einem öffentlich zugreifbaren Schlüsselregister (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 (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[5], aber auch bereits das normale ISDN-Telefon [MöPS_94] bieten geeignete Hüllnachrichten in Hülle und Fülle.

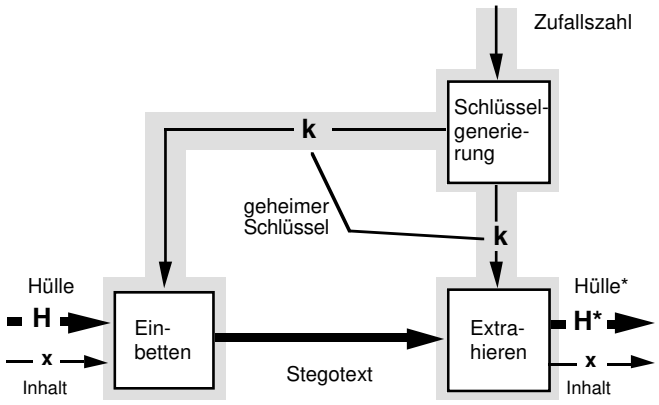

Bild 4: Symmetrisches steganographisches Konzelationssystem

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 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.

---

4 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.

5 Andreas Westfeld: Implementierung eines steganographischen Systems am Beispiel einer Videokonferenz; Belegarbeit, TU Dresden, 1. Nov. 1996 (gekürzt in [West_97]); Steganographie in komprimierten Videosignalen; Diplomarbeit, TU Dresden, 1. Juli 1997; Elke Franz: Untersuchung von Bewertungsmöglichkeiten für Bilder bezüglich eingebetteter steganographischer Daten; Belegarbeit, TU Dresden, Nov. 1996.

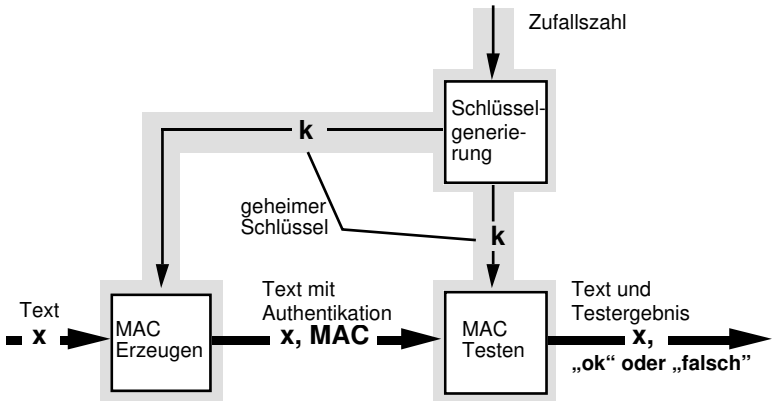

Bild 5: Symmetrisches kryptographisches Authentikationssystem

Asymmetrische kryptographische 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.

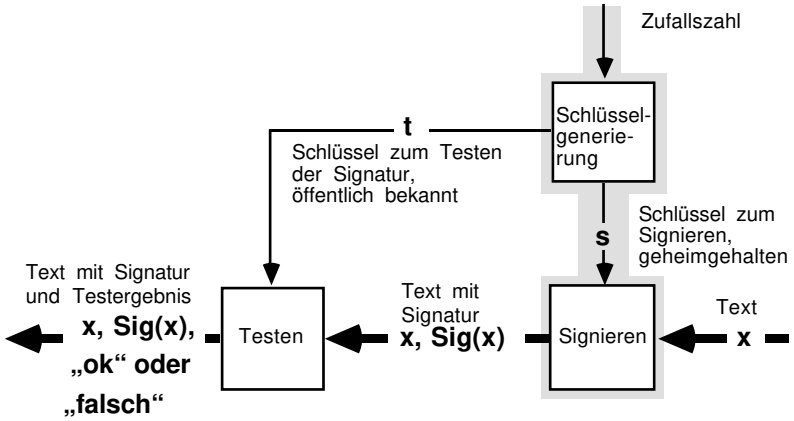

Bild 6: Digitales Signatursystem

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, CAs) 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.

3 Technische Randbedingungen jeder Kryptoregulierung

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

3.1 Benutzeranforderungen an Signaturschlüssel 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 auch die Funktion einer CA 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. Es wurde allerdings noch an keiner Stelle argumentiert, daß der Zugriff auf geheime Signierschlüssel hilfreich sei zum Zwecke der Strafverfolgung oder Verbrechensverhinderung. Ein solcher Zugriff ermöglicht im Gegenteil das Fälschen von Beweismitteln und entwertet sie damit.

Schlüsselpaare für Konzelation, also das Verschlüsseln von Daten zum Schutz vor unerwünschter Kenntnisnahme, 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 gelungen ist, einmal Schlüssel auszutauschen[9], deren Authentizität sie vertrauen, jedes beliebige Konzelationssystem zur weiteren vertraulichen Kommuni-

---

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*, CA, digital signiert, was allgemein als *Zertifizierung* des öffentlichen Schlüssels bezeichnet wird. Um derartige Zertifikate überprüfen zu können, muß der Empfänger einer signierten Nachricht den öffentlichen Schlüssel der zertifizierenden Stelle kennen. Ist dies nicht der Fall, so benötigt er wiederum ein Zertifikat für diesen Schlüssel. Es entsteht ein Zertifizierungsbaum, wie er beispielsweise in X.509 und in sehr eingeschränkter Form im Gesetz zur digitalen Signatur (bzw. der zugehörigen Verordnung) beschrieben ist.

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.

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

kation 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 zeigen wir, daß Benutzer einen Schlüsselaustausch für Konzelation unter Benutzung der Sicherheitsinfrastruktur für den elektronischen Rechtsverkehr bzw. von Konzelationssystemen mit Key-Escrow eigenständig realisieren können, ohne irgendeine Einschränkung in ihren Anforderungen in Kauf nehmen zu müssen.

3.2 Digitale Signaturen ermöglichen Austausch von Konzelationsschlüsseln

Jede Sicherheitsinfrastruktur für digitale Signaturen erlaubt 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 eine Nachricht unterschreibt: „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 Gewißheit zu verschaffen, 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, daß die Sicherheit der Signaturen untergraben wird, 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.

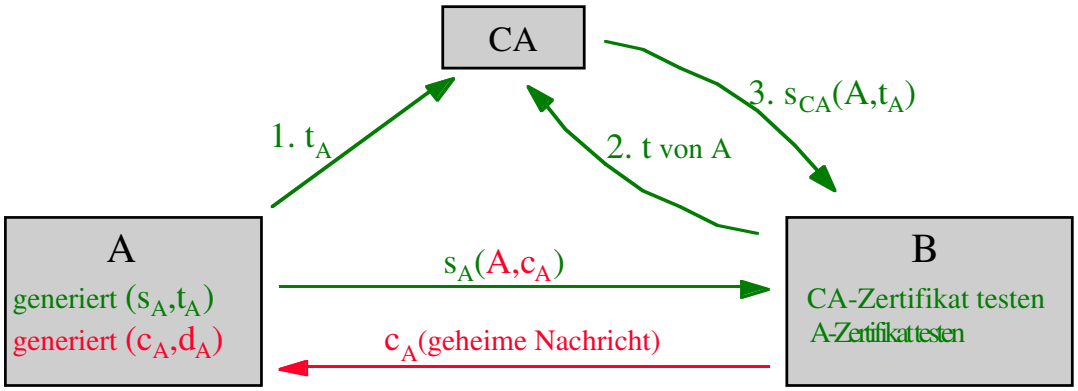

Bild 7: Sichere digitale Signaturen ermöglichen teilnehmerautonome sichere Konzelation

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.

---

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

3.3 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-System, benutzt werden, um Schlüssel für zusätzliche zu verwendende Konzelationssysteme zu vereinbaren (Bild 8). Statt einem Konzelationssystem direkt die vertraulich zu haltenden Nachrichten zu übergeben, wird zunächst ein öffentlicher Konzelationsschlüssel redundant codiert übertragen. Der Empfänger prüft die Redundanz (was dem Prüfen des Zertifikates bei Verwendung digitaler Signaturen entspricht). Sofern er keine Verfälschung des öffentlichen Schlüssels feststellt, verwendet er den öffentlichen Schlüssel entweder, um wirklich vertraulich zu haltende Nachrichten zu verschlüsseln (Bild 8 a) und b)) oder aber zum Austausch eines weiteren Schlüssels für ein symmetrisches Konzelationssystem, mit dem dann effizienter verschlüsselt werden kann (Bild 8 c)). 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 8 b) und c) gezeigt ist.

Ist das Key-Escrow-System so gestaltet, daß eine Entschlüsselung früherer Nachrichten nicht möglich oder nicht erlaubt ist, so braucht nicht einmal der Umweg über den öffentlichen Konzelationsschlüssel gegangen zu werden. Wie in Bild 9 gezeigt, kann dann direkt ein symmetrischer Schlüssel ausgetauscht werden – dies muß nur rechtzeitig geschehen.

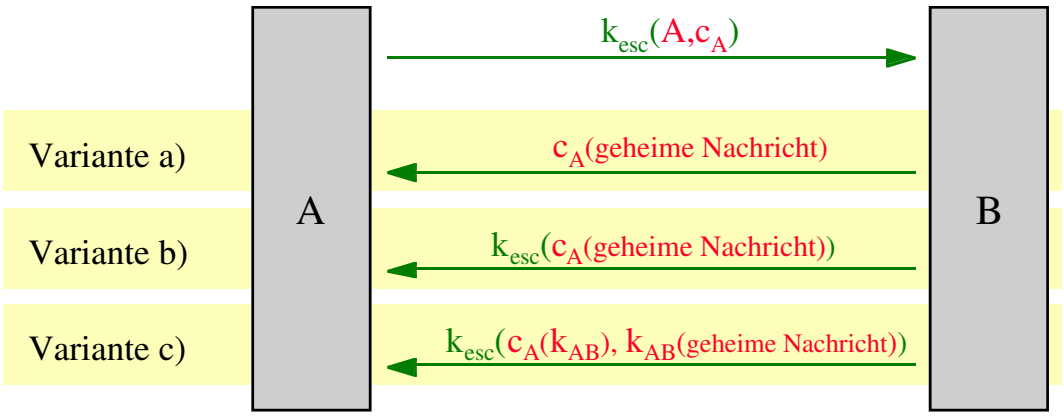

Bild 8: Key-Escrow-Konzelation ohne Dauerüberwachung ermöglicht Schlüsselaustausch und damit a) "normale" Konzelation, b) asym. Konzelation ohne Key-Escrow und c) sym. Konzelation ohne Key-Escrow

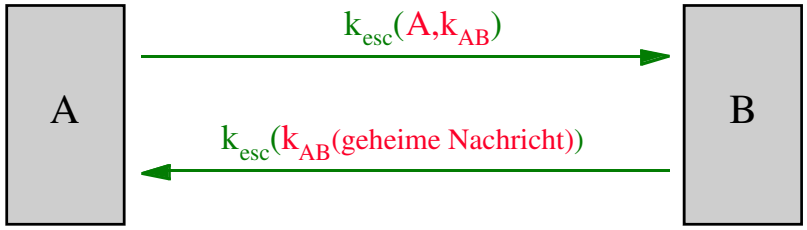

Bild 9: Key-Escrow-Konzelation ohne rückwirkende Entschlüsselung ermöglicht direkt symmetrische Konzelation ohne Key-Escrow

Die Verwendung zusätzlicher Verschlüsselungsmaßnahmen gemäß Bild 8 b) und c) oder Bild 9 kann erst dann entdeckt werden, wenn die Schlüssel des Key-Escrow-Systems von den Key-Escrow-Agencies 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 (den sogenannten Bedarfsträgern) 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. Diese einfache Beobachtung macht Key-Escrow-Agencies und Bedarfsträger ggf. zu einem vielversprechenden Angriffspunkt für Wirtschaftsspionage und andere kriminelle Aktivitäten. Gerade in Ländern, in denen die organisierte Kriminalität eine wichtigere Rolle spielt, zeigt sich immer wieder, daß der „Erfolg“ der organisierten Kriminalität und Korruption der Sicherheitsbehörden zwei Seiten derselben Medaille sind.

Kurzum: Key-Escrow zur Verbrechensbekämpfung wird weitestgehend wirkungslos sein – 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.

3.4 Steganographie: Vertrauliche Nachrichten zu finden ist unmöglich

Nachrichten können nicht nur durch kryptographische Konzelationssysteme vor unerwünschter Kenntnisnahme geschützt werden, sondern auch durch Steganographie: Die zu schützende Nachricht wird in einer anderen Nachricht, die notwendigerweise wesentlich länger ist, geeignet versteckt, vgl. Kap. 2.1. 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. Natürlich ist es möglich und zur Erhöhung der Sicherheit empfehlenswert, die zu schützende Nachricht vor dem steganographischen Verstecken noch zu verschlüsseln.

In [MöPS_94 Kap. 3.3] ist beschrieben, wie ein steganographisches Verfahren mit einem zufällig gewählten Schlüssel parametrisiert werden kann: Der Schlüssel gibt beispielsweise die Abstände

---

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 lehrt, daß bisher *jedes* größere technische System Fehler enthielt. Also müssen Risikozusammenballungen vermieden werden.

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.

zwischen den Bitpositionen an, an denen die zu schützende Nachricht versteckt wird. Steganographische Algorithmen, die mit einem frei wählbaren Schlüssel parametrisiert sind, entsprechen in der Funktionalität Konzelationssystemen, bei denen die Algorithmen allgemein bekannt sind und die Sicherheit nur über geheimgehaltene Schlüssel gewährleistet wird. Sie sind wie solche Konzelationssysteme auch in *offenen* Benutzergruppen verwendbar, da das zugrundeliegende Verfahren nicht geheimgehalten werden muß. Damit sind alle beschriebenen Möglichkeiten zum Schlüsselaustausch nicht nur beim Einsatz von ausgewiesenen kryptographischen Verfahren, sondern auch beim Einsatz von Steganographie verwendbar.

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

3.5 Sinnvolle Wahl der Sicherheitsparameter und Maßnahmen bei Schlüsselverlust berücksichtigen den gewünschten Schutzzeitraum

Es ist sowohl bei Signatursystemen als auch bei Konzelationssystemen danach zu unterscheiden, für welchen Zeitraum die Sicherheit der verwendeten Systeme gewährleistet sein muß. So müssen Sicherheitsparameter wie die Schlüssellänge danach eingestellt werden, ob es dem Benutzer wichtiger ist, in kurzer Zeit große Datenmengen zu verarbeiten, deren Vertraulichkeit oder Integrität nur kurzfristig garantiert werden muß, oder ob die Daten über Jahrzehnte geschützt werden sollen, so daß auch Angriffe mit erheblich gesteigerter Rechenleistung berücksichtigt werden müssen.

Auch für Maßnahmen im Falle eines Schlüsselverlustes[13] ist die Zeitkomponente zu berücksichtigen. Der Verlust 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, d.h. die zwangsweise Hinterlegung von „geheimen“ Schlüsseln bei sogenannten Key-Escrow-Agencies. Key-Escrow Systeme sollen die geheimen Schlüssel für gesetzlich festgelegte Bedarfsträger, Sicherheitsbehörden und Nachrichtendienste vorhalten, um ggf. eine Überwachung des Fernmeldeverkehrs zu ermöglichen.

---

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.

Gleiches gilt hinsichtlich Schlüsseln für Signaturen, vgl. Bild 10. 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.

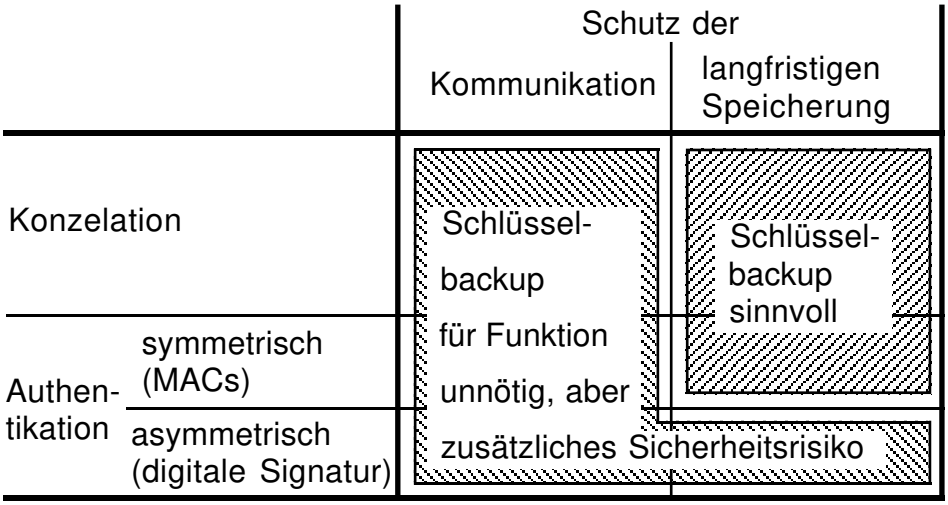

Bild 10: Wo ist Schlüsselbackup sinnvoll, wo unnötig und ein zusätzliches Sicherheitsrisiko

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. Dies ist eine wichtige erste Verteidigunglinie gegen Mißbrauch [AABB_97 Kap. 2.3].

Key-Escrow-Systeme werden dagegen für Entschlüsselung von vertraulicher Kommunikation vorgeschlagen, von der die Schlüsselinhaber gerade nichts erfahren sollen.

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.

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

4 Schlußfolgerungen

Kryptographie ermöglicht jedem, Einzelnen wie Organisationen, Vertraulichkeit und Integrität seiner Informationen auch in Räumen ohne physische Kontrolle selbst zu schützen.

Das oft gehörte Argument, die Schlüsselerzeugung gehöre aus Gründen der Verbrechensbekämpfung zusammen mit einer Aufbewahrung auch der geheimen Schlüssel zu den Aufgaben von staatlich autorisierten TrustCentern, ist aus den dargelegten Gründen vollständig falsch. 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.

5 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; erhältlich via 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

Stichwörter

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