in: Uwe Schneider, Dieter Werner (Hrsg.): Taschenbuch der Informatik; 3. Auflage, Fachbuchverlag Leipzig im Carl Hanser Verlag, München 2000, 586-604.Taschenbuch der Informatik (3., neub. Auflage)

17 Datenschutz und Datensicherheit

Hannes Federrath, Andreas Pfitzmann

17.1 Grundbegriffe

17.1.1 Schutzziele

IT-Systeme (einschließlich der Übertragungsstrecken) müssen gegen unbeabsichtigte Fehler und Ereignisse (z.B. höhere Gewalt, technische Fehler, Fahrlässigkeit, Programmierfehler, Verschleiß, Havarien) und beabsichtigte Angriffe (z.B. Abhören, Manipulation und Zerstören von Informationen, aber auch von Software und Hardware) von außen (Outsider, z.B. Hacker oder Terroristen mit Sprengstoff) und innen (Insider, z.B. Administratoren, Programmierer) gesichert werden.

Im Englischen werden die Begriffe **Security** für Schutz vor beabsichtigten und **Safety** für Schutz vor unbeabsichtigten Ereignissen verwendet (→ Tabelle 17.1). Der Bereich Datenschutz und Datensicherheit befaßt sich insbesondere mit dem Schutz vor beabsichtigten Angriffen (Security). Hier unterscheidet man die drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit.

Tabelle 17.1: Abgrenzung von Security und Safety

Security Schutz gegen beabsichtige Angriffe		**Safety** Schutz gegen unbeabsichtigte Ereignisse	
Vertraulichkeit:	Anonymität Unbeobachtbarkeit Unverkettbarkeit Pseudonymität Abhörsicherheit Sicherheit gegen unbefugten Gerätezugriff	Verfügbarkeit:	Funktionssicherheit Technische Sicherheit
Integrität:	Zurechenbarkeit Übertragungsintegrität Abrechnungssicherheit	Sonstige Schutzziele:	Maßnahmen gegen hohe Gesundheitsbelastung
Verfügbarkeit:	Ermöglichen von Kommunikation		

Schutzinteressen können sich nicht nur auf die über die Netze ausgetauschten Nachrichteninhalte (Vertraulichkeit, Integrität) beziehen, sondern gelten ebenfalls für den Schutz von Kommunikationsumständen: In manchen Anwendungen ist zu schützen, wer wann mit wem kommuniziert hat (Anonymität und Unbeobachtbarkeit), in anderen Anwendungen ist vor allem sicherzustellen, daß eine Nachricht nachprüfbar und beweisbar von einem bestimmten Absender stammt (Zurechenbarkeit).

17.1.2 Angreifermodell

Ein Angreifermodell definiert die Stärke eines Angreifers, gegen den ein bestimmter Schutzmechanismus (z.B. ein ganz bestimmtes Verschlüsselungsverfahren) gerade noch sicher ist.

Dabei berücksichtigt es folgende Aspekte:

1. Aktive oder passive Rolle des Angreifers:
   - Was kann der Angreifer maximal passiv beobachten?
   - Was kann der Angreifer maximal aktiv kontrollieren (steuern, verhindern) bzw. verändern?
2. Mächtigkeit des Angreifers:
   - Wieviel Rechenkapazität besitzt der Angreifer?
   - Wieviel finanzielle Mittel besitzt der Angreifer?
   - Wieviel Zeit besitzt der Angreifer?
   - Welche Verbreitung hat der Angreifer? Oder spezieller: Welche Leitungen, Kanäle, Stationen kann der Angreifer beherrschen?

Als potentielle Angreifer können Außenstehende, Teilnehmer, Betreiber, Hersteller, Entwickler und Wartungstechniker betrachtet werden, die natürlich auch kombiniert auftreten können. Außerdem kann man nach Angreifern innerhalb des betrachteten IT-Systems (Insider) und außerhalb (Outsider) unterscheiden. Die Feststellung, daß eine Instanz angreifen kann, ist nicht gleichzusetzen damit, daß sie wirklich angreift.

17.1.3 Sicherheitsmanagement

Je mehr Funktionen eine Organisation mit Hilfe von IT-Systemen erledigt, umso abhängiger wird sie von der fehlerfreien und verläßlichen Funktion der Systeme. Im Rahmen des Sicherheitsmanagements sind folglich entsprechende Maßnahmen zu treffen:

1. Entwicklung einer IT-Sicherheitspolitik und eines IT-Sicherheitskonzeptes,
2. Realisierung der IT-Sicherheitsmaßnahmen,
3. Schulung und Sensibilisierung der Benutzer,
4. Erhaltung der IT-Sicherheit im laufenden Betrieb.

Im Rahmen des IT-Sicherheitskonzeptes werden Maßnahmen festgelegt, die auf weite Teile der Organisation Einfluß haben. Beispiele sind:

- Infrastruktur: Physische Zugangs- und Zutrittskontrolle, Stromversorgung, Feuerschutz, Klimatisierung;
- Organisation: Überwachung, Kontrolle, Dokumentation, permanente Anpassung des Sicherheitskonzeptes an veränderte Gegebenheiten;
- Personal: Maßnahmen bei Auswahl, Einstellung, Ausscheiden; fortlaufende Schulung;

- Hardware und Software: Hardware-, Betriebssystem- und Softwareauswahl, Passwort- und Virenschutz;
- Kommunikation: Netztopologie, Netzverwaltung, -administration, Übertragungssicherung, Protokollierung von Zugriffen;
- Notfallvorsorge: Datensicherungskonzept (Backup), Versicherungen, Notfallrechenzentrum.

▸ Informationen zum IT-Grundschutz, konkrete Maßnahmen- und Gefährdungskataloge, aktuelle Informationen: http://www.bsi.de/gshb/

17.2 Sicherheit einzelner Rechner

Um sichere Kommunikation zu erreichen, werden Geräte (Hardware) und Programme (Software) benötigt, die für denjenigen, der sie benutzt, sicher sind. Diese persönliche Rechenumgebung (typischerweise der PC) ist der Vertrauensbereich des Benutzers. Er ist vor Zugang und Zugriff durch Unberechtigte zu schützen. Dies muß zunächst durch physische Schutzmaßnahmen erfolgen, bevor weitere Maßnahmen, wie Zugangskontrolle und Zugriffskontrolle sinnvoll sind.

17.2.1 Physische Sicherheit

Alle technischen Schutzmaßnahmen benötigen eine physische „Verankerung“ in Form eines Systemteils, auf den der Angreifer keinen physischen Zugriff hat.

Beispielsweise ist es unmöglich, den Inhalt einer zu verschlüsselnden Nachricht vor dem Verschlüsselungsbaustein zu verbergen. Dies gilt analog für die eingesetzten kryptographischen Schlüssel. Die Größe physisch sicherer Geräte muß skalierbar sein (→ Bild 17.1).

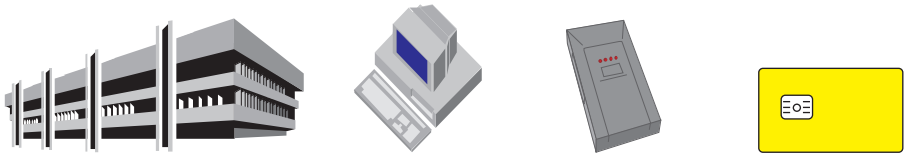

Bild 17.1: Die Größe physisch sicherer Geräte muß skalierbar sein

☐ Beispiel: Es soll der Inhalt einer Festplatte vor unbefugtem Zugriff geschützt werden. Um zu verhindern, daß die Festplatte aus dem Rechner ausgebaut wird, muß der Rechner physisch sicher sein. Alternativ kann die Festplatte verschlüsselt werden. Die Ver- und Entschlüsselung der Festplatte erfolgt über ein Sicherheitsmodul, das während des Betriebs im Rechner steckt. Nun genügt es, daß das Sicherheitsmodul physisch geschützt wird. Wird der Rechner bzw. die Festplatte gestohlen, bleiben die gespeicherten Inhalte trotzdem vertraulich.

Angriffe auf die physische Sicherheit werden, unabhängig von der jeweiligen Größe des physischen Gerätes, durch Schirmung (z.B. gegen elektromagnetische Abstrahlung), Erkennen und Bewerten (z.B. durch entsprechende Sensoren) sowie Verzögern des Angriffs (z.B. durch hartes Material) realisiert. Bei Angriffen können als letzte Maßnahme die gespeicherten Geheimnisse gelöscht werden.

17.2.2 Zugangskontrolle und Identifikation von Menschen durch IT-Systeme

Unter **Zugangskontrolle** versteht man, daß ein IT-System die Identitäten seiner Kommunikationspartner erfragt, prüft und nur mit berechtigten Partnern weiter kommuniziert.

Die Zugangskontrolle verhindert so mindestens die unbefugte Inanspruchnahme seiner Betriebsmittel. Ein IT-System kann einen Menschen daran erkennen (**Identifikation**), was er ist, hat oder weiß (→ Tabelle 17.2).

Tabelle 17.2: Identifikation von Menschen durch IT-Systeme

Was man	**ist:**	Handgeometrie Fingerabdruck Aussehen eigenhändige Unterschrift Retina-Muster Stimme Tipp-Charakteristik (Tastenanschlag)
	hat:	Papierdokument Metallschlüssel Magnetstreifenkarte Chipkarte Taschenrechner
	weiß:	Passwort Antworten auf Fragen

☐ Beispiele: 1. Ein (maschinenlesbarer) Personalausweis ist eine Kombination aus Foto („Aussehen“), eigenhändiger Unterschrift und Papierdokument. 2. Die in IT-Systemen derzeit noch am häufigsten vorkommende Form der Identifizierung ist das Passwort.

17.2.3 Zugriffskontrolle und Rechtevergabe

Unter **Zugriffskontrolle** versteht man, daß ein IT-System auch berechtigten Partnern nicht alles erlaubt: Jedes *Subjekt* (Mensch, IT-System, Prozeß) hat nur bestimmte *Rechte*, Operationen auf *Objekten* (Prozesse, Daten, Peripherie-Geräte, etc.) auszuführen.

Ein möglichst kleiner und gut abgegrenzter Teil des IT-Systems kontrolliert vor Ausführung aller Operationen, ob ihr Urheber die dafür nötigen Rechte hat. Dieser Teil des IT-Systems wird **Zugriffsmonitor** genannt (→ Bild 17.2). Der Zugriffsmonitor merkt sich ihm vorgelegte oder implizit entstehende Rechte und muß auch deren Ungültigwerden erkennen.

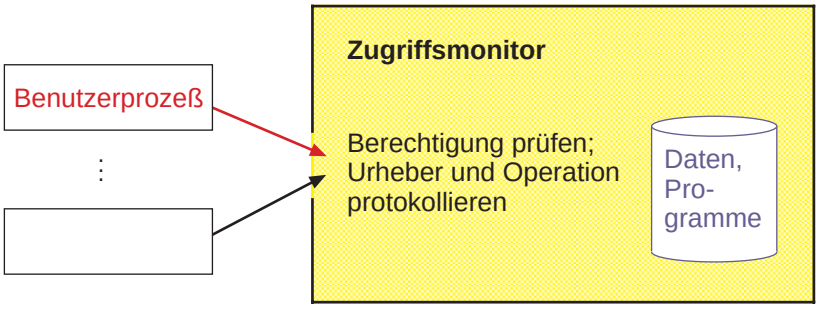

Bild 17.2: Gewährung von Rechten über einen Zugriffsmonitor

- Beispiel: Rechte werden z.B. in einer Zugriffskontrollmatrix gespeichert. Typische Rechte sind Schreiben, Lesen, Verändern, Löschen, Ausführen.

Die Rechtevergabe selbst wird **Autorisierung** (*authorization*) genannt.

17.2.4 Schutz vor Computerviren durch geringstmögliche Privilegierung

In vielen der heute verbreiteten PC-Betriebssystemen (DOS, Windows 95/98, MacOS) fehlt die Zugriffskontrolle. Dies begünstigt die Ausbreitung von Computerviren und Trojanischen Pferden erheblich.

Ein **Computervirus** ist ausführbarer Code, der sich in fremde Programme einpflanzt, dort ausgeführt wird und ggf. eine sog. **Schadenfunktion** ausführt. Ein **Trojanisches Pferd** ist ein Computerprogramm, das neben einer bekannten (vom Anwender gewünschten) Funktion eine (nicht gewünschte) Schadenfunktion ausführt.

Viren und Trojanische Pferde können nicht nur die Integrität und Verfügbarkeit von Daten und Programmen verletzen, sondern alle Schutzziele, also auch die Vertraulichkeit von Daten. Im schlimmsten Fall können Viren und Trojanische Pferde ihre Schadenfunktion modifizieren und sogar sich selbst zerstören, nachdem sie ihre „Aufgabe“ erfüllt haben, um die hinterlassenen Spuren zu vernichten.

In IT-Systemen mit Zugriffskontrolle kann die Ausbreitung von Viren durch das **Prinzip der geringstmöglichen Privilegierung** (*principle of least privilege*) verhindert werden. Das bedeutet, jedes Programm bekommt nur die minimal notwendigen (Schreib-)-Rechte. Bei Trojanischen Pferden kann der Schaden zumindest auf die autorisierten Ressourcen begrenzt werden.

17.3 Sicherheit in verteilten Systemen

17.3.1 Kryptographie

Kryptographische Systeme lassen sich sowohl zum Schutz der Vertraulichkeit (Konzelations- oder Verschlüsselungssysteme) als auch zum Schutz der Integrität (Authentikationssysteme) einsetzen.

Wenn sowohl Sender als auch Empfänger über den gleichen kryptographischen Schlüssel verfügen, spricht man von symmetrischen Systemen, andernfalls von asymmetrischen.

17.3.1.1 Symmetrisches kryptographisches Konzelationssystem

Die bekanntesten und ältesten kryptographischen Systeme sind symmetrische Konzelationssysteme (→ Bild 17.3). Ihre bekanntesten modernen Vertreter sind DES (Data Encryption Standard) und IDEA (International Data Encryption Algorithm).

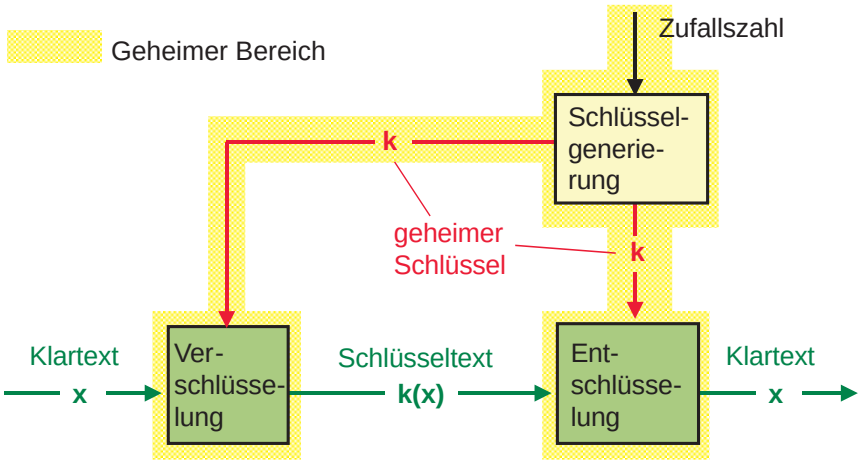

Bild 17.3: Symmetrisches kryptographisches Konzelationssystem

Wenn eine Nachricht x verschlüsselt über einen unsicheren Kanal gesendet werden soll, muß zuvor der Schlüssel k bei Sender und Empfänger vorliegen. Wenn sich Sender und Empfänger vorher getroffen haben, können sie k bei der Gelegenheit austauschen. Andernfalls muß k über eine vertrauenswürdige „Schlüsselverteilzentrale“ Z ausgetauscht werden (→ Bild 17.4): Hierzu melden sich die Teilnehmer A und B bei Z an und tauschen jeweils Schlüssel mit Z aus. A und Z tauschen k_{AZ} aus und B und Z tauschen k_{BZ} aus. Wenn A mit B kommunizieren will und noch keinen Schlüssel mit B gemeinsam 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 (Abbildung 4). Ab jetzt können A und B den Schlüssel k benutzen, um in beide Richtungen verschlüsselte Nachrichten N zu schicken. Die Vertraulichkeit ist allerdings nicht sehr groß: Außer A und B kann auch Z alle Nachrichten entschlüsseln.

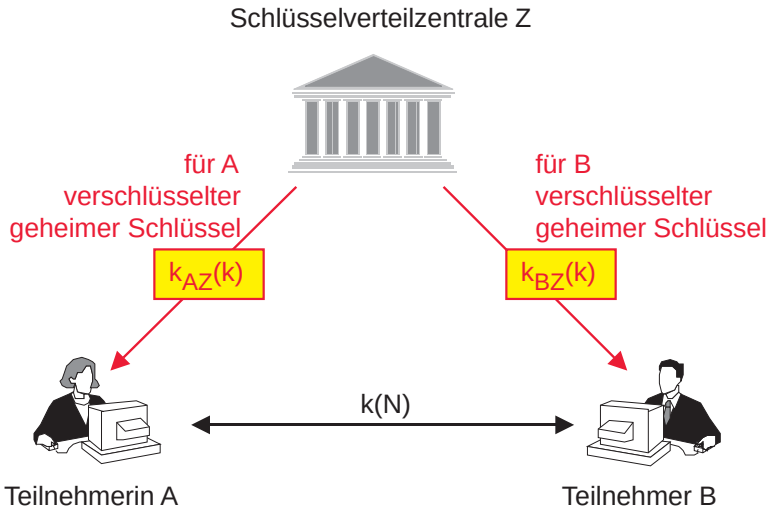

Bild 17.4: Schlüsselverteilung bei symmetrischen Konzelationssystemen

17.3.1.2 Asymmetrisches kryptographisches Konzelationssystem

Die bekanntesten Vertreter asymmetrischer kryptographischer Konzelationssysteme sind RSA und ElGamal (jeweils benannt nach ihren Erfindern Rivest, Shamir, Adleman bzw. ElGamal). Im Vergleich zu symmetrischen Konzelationssystemen sind sie deutlich rechenaufwendiger (etwa Faktor 100 bis 1000).

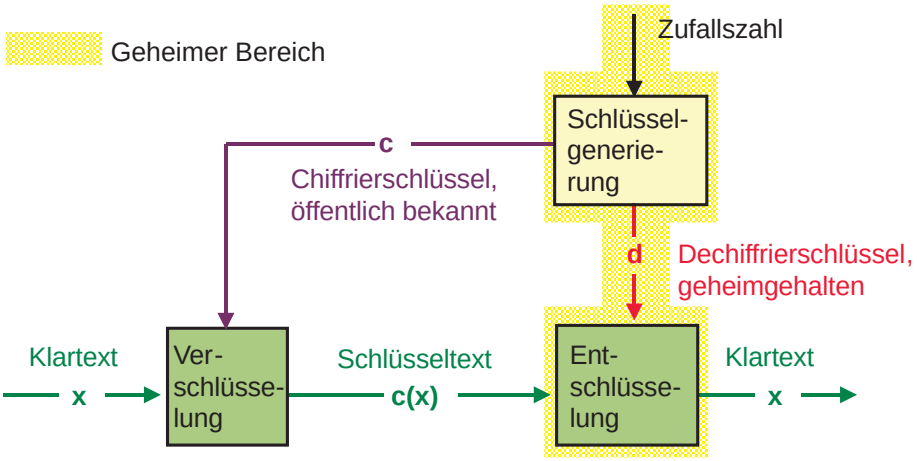

Bild 17.5: Asymmetrisches kryptographisches Konzelationssystem

Asymmetrische Konzelationssysteme (→ Bild 17.5) wurden erfunden, um die Schlüsselverteilung zu vereinfachen. Hier sind zum Ver- und Entschlüsseln verschiedene Schlüssel c und d erforderlich, und nur d muß geheimgehalten werden. Damit man c tatsächlich nicht geheimhalten muß, darf d nicht mit vernünftigem Aufwand aus c zu bestimmen sein.

Nun kann jeder Benutzer A sich selbst ein Schlüsselpaar (c_A, d_A) generieren und muß d_A nie jemand anderem mitteilen. Der öffentliche Schlüssel c_A kann in einem öffentlichen Schlüsselregister R gespeichert sein.

17.3.1.3 Symmetrisches kryptographisches Authentikationssystem

Bei symmetrischen kryptographischen Authentikationssystemen (→ Bild 17.6) wird die Nachricht durch den kryptographischen Algorithmus links nicht verschlüsselt, sondern es wird ein Prüfteil **MAC** (**Message Authentication Code**) an *x* angehängt. Der Empfänger kann anhand von *x* auch den richtigen MAC bilden und prüfen, ob der mit der Nachricht mitgekommene damit übereinstimmt.

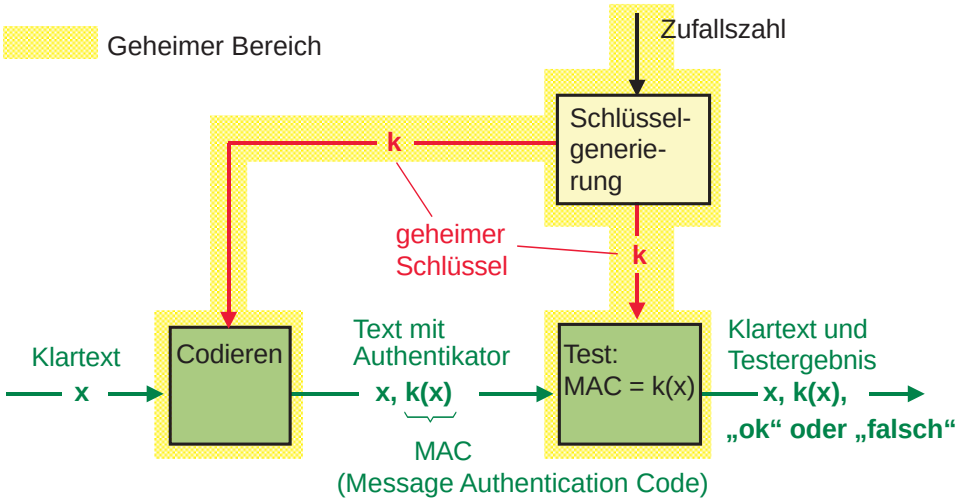

Bild 17.6: Symmetrisches kryptographisches Authentikationssystem

Die Schlüsselverteilung kann wie bei symmetrischen Konzelationssystemen erfolgen. Entsprechend könnte die Schlüsselverteilzentrale diesmal gefälschte Nachrichten unterschieben.

17.3.1.4 Asymmetrisches kryptographisches Authentikationssystem

Asymmetrische kryptographische Authentikationssysteme (→ Bild 17.7) werden **digitale Signatursysteme** genannt und vereinfachen zunächst die Schlüsselverteilung analog zu asymmetrischen Konzelationssystemen. Ihr Hauptvorteil ist aber ein anderer: Der Empfänger *B* einer signierten Nachricht von *A* kann jedem, der *A*s öffentlichen Schlüssel t_A kennt, beweisen, daß diese Nachricht von *A* stammt. Dies geht bei einem symmetrischen Authentikationssystem nicht: Selbst wenn z.B. vor Gericht die Schlüsselverteilzentrale bestätigen würde, welchen Schlüssel *A* und *B* hatten, kann *B* den *MAC* genausogut selbst erzeugt haben. Bei digitalen Signatursystemen ist jedoch *A* der einzige, der die Signatur erzeugen kann. Deswegen sind digitale Signatursysteme unumgänglich, wenn man rechtlich relevante Dinge digital in *zurechenbarer* Weise abwickeln will, z.B. bei Electronic-Commerce und digitalen Zahlungssystemen. Digitale Signaturen haben dort die Funktion der eigenhändigen Unterschrift in heutigen Rechtsgeschäften.

Bekannte Signaturverfahren sind RSA (ebenfalls für asymmetrische Konzelation einsetzbar) und DSS (Digital Signature Standard).

Im Gegensatz zur symmetrischen Authentikation wird bei der digitalen Signatur ein eigener Testalgorithmus benötigt, der mit dem öffentlichen Schlüssel *t* arbeitet.

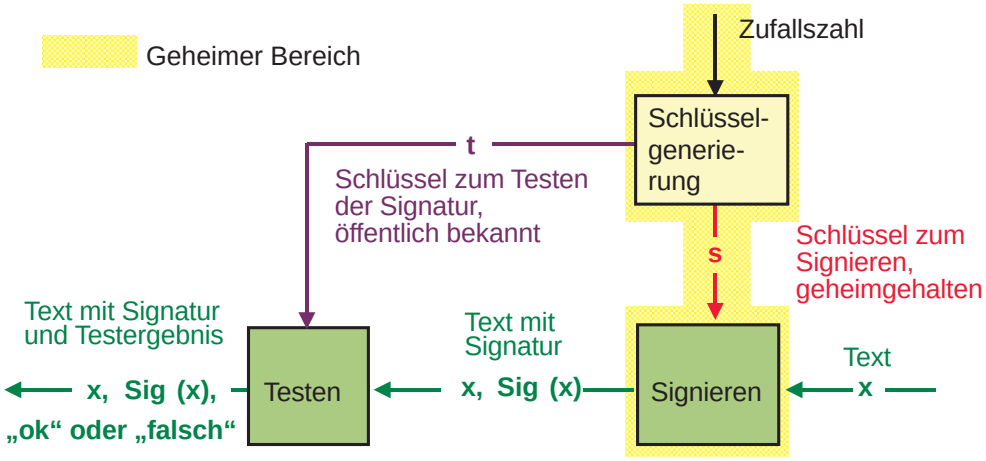

Bild 17.7: Digitales Signatursystem

Will man sicher sein, daß eine Signatur später ggf. vor Gericht anerkannt wird, muß man sich versichern, daß man den richtigen bzw. authentischen Testschlüssel hat. Die Authentizität eines öffentlichen Schlüssels kann durch die Prüfung eines Zertifikats festgestellt werden.

Die **Zertifizierung** (Beglaubigung) **des öffentlichen Testschlüssels** bezieht sich nicht auf den Schlüssel allein, sondern auf den *Zusammenhang* zwischen Schlüssel und Teilnehmer. Bei der Zertifizierung überprüft die Zertifizierungsstelle (auch vertrauenswürdiger Dritter oder Trust Center genannt) die Identität des Teilnehmers (beispielsweise anhand seines Personalausweises) und erstellt ein **Zertifikat**, d.h. eine digitale Signatur über der Identität und dem öffentlichen Schlüssel des Teilnehmers.

- Weiterführende Literatur zur Kryptographie: [Schn_96]

17.3.2 Steganographie

17.3.2.1 Symmetrisches steganographisches Konzelationssystem

Bei Verwendung von Kryptographie ist im Kommunikationsnetz erkennbar, ob gerade vertraulich oder authentisiert kommuniziert wird, sofern keine weiteren Schutzmaßnahmen ergriffen werden. Bei Steganographie ist das nicht der Fall.

Steganographische Konzelationssysteme betten geheimzuhaltende Nachrichten in harmlos wirkende Hüllnachrichten (z.B. digitalisierte Fotos oder Sound-Dateien) ein, so daß für Außenstehende, die nur den Stegotext (→ Bild 17.8) beobachten, nicht einmal die Existenz der geheimen Nachricht erkennbar ist und damit auch nicht ihr Inhalt.

Politische Diskussionen um ein Kryptoverbot führten zu einer verstärkten Beachtung der Steganographie, da mit Steganographie Verschlüsselungsverbote unterlaufen werden können.

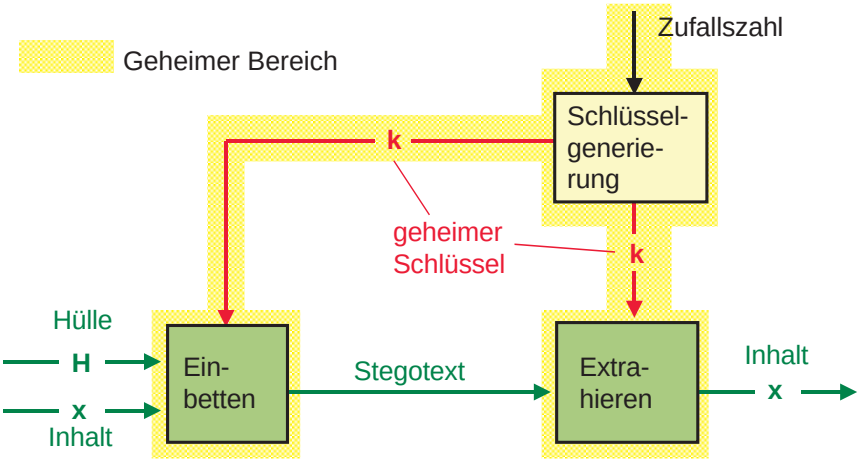

Bild 17.8: Symmetrisches steganographisches Konzelationssystem

Ein Nachteil der steganographischen Konzelation ist, daß zum Übertragen einer bestimmten Informationsmenge ein Vielfaches an Stegotext benötigt wird. Der Grund liegt darin, daß *x* meist nur in manchen niederwertigsten Bits der Hüllinformation *H* untergebracht werden kann, da nur diese Bits je nach Hüllinformation derart indeterministisch sind, daß ihre Veränderung für den Außenstehenden zu keiner beobachtbaren Beeinträchtigung der Hüllinformation führt.

Bisher sind nur *symmetrische* steganographische Konzelationssysteme bekannt. Die selbstverständlich mögliche Hintereinanderschaltung eines asymmetrischen Konzelationssystems und symmetrischen Stegosystems führt nicht zu einem asymmetrischen Stegosystem.

17.3.2.2 Steganographisches Authentikationssystem

Steganographische Authentikationssysteme werden **Watermarking-Systeme** genannt. Durch die zunehmende Bedeutung von Multimedia und dem damit verbundenen Wunsch, die Urheberrechte bei der Verbreitung digitaler Objekte (Daten, Programme, Computerkunst etc.) über CD-ROM und Internet zu sichern, gewinnen Watermarking-Verfahren an Bedeutung. Die Hülle (siehe steganographisches Konzelationssystem) stellt dabei die urheberrechtlich zu schützende Information dar. Die Urheberinformation sei *x*. Nun kommt es nicht darauf an, eine möglichst große Menge an Informationen *x* in die Hülle einzubetten. Vielmehr soll die Urheberinformation möglichst *robust* eingebettet werden. Am Beispiel digitaler Bilder wird dies deutlicher: Trotz einer Veränderung von Bildparametern (Größe, Farbe, Helligkeit etc.) oder Ausschneiden von Bildteilen zum Zwecke der eigenen Nutzung soll die Urheberinformation erhalten bleiben.

Das Einbetten von Daten über den Käufer eines digitalen Objektes nennt man **Fingerprinting**.

- Weiterführende Literatur zur Steganographie: [IHW_96, IHW_98]

17.3.3 Diversität als Verfügbarkeitsmaßnahme

Kryptographische Systeme allein können das Schutzziel Verfügbarkeit nicht realisieren. Die Verfügbarkeit von Daten, Programmen und Diensten kann jedoch durch die adäquate technische Gestaltung der Kommunikationsinfrastruktur sichergestellt werden. Dabei spielen der Grad an **Diversität** und **Entwurfskomplexität** eine entscheidende Rolle.

So sollte im Interesse der Durchschaubarkeit eine Kommunikationsinfrastruktur mit geringstmöglicher Entwurfskomplexität gewählt werden, damit sie keine, zumindest keine schweren, verborgenen Entwurfsfehler enthält.

Ein diversitäres Kommunikationsnetz mit mehrfach redundanter und unterschiedlicher Leitungsführung kann z.B. den Totalausfall bei Ausfall von Teilen des Netzes vermeiden. Bei Funknetzen könnte auf unterschiedliche Frequenzbänder ausgewichen werden, sobald Störungen auftreten. Besonders problematisch sind evtl. vorhandene Kommunikationsengpässe, z.B. Netzübergänge.

17.4 Datenschutzfreundliche Technologien

Es ist nicht das primäre Interesse eines Betreibers, beispielsweise Daten über seine Nutzer zu sammeln, um diese anschließend mißbräuchlich zu verwenden. Im Gegenteil: Je weniger Daten ein Betreiber zur Diensterbringung benötigt, umso weniger Kosten fallen für deren Verarbeitung und Schutz an. Außerdem reduzieren sich die Mißbrauchsmöglichkeiten. Bekannte Schutzmechanismen für **Anonymität** und **Unbeobachtbarkeit** sind

- Schutz des Empfängers durch Verteilung (Broadcast) und implizite Adressierung,
- Schutz des Senders durch Dummy Traffic, DC-Netze (überlagerndes Senden, [Chau_88]) und Ring-Netze [Pfit_90],
- Schutz der Kommunikationsbeziehung zwischen Sender und Empfänger durch Proxies und Mixe [Chau_81],
- Schutz von Datenbankzugriffen durch „Blindes Lesen“ (Blinded Message Service, [CoBi_95]),
- Schutz des Senders gegen Peilbarkeit (in Funknetzen) durch Bandspreiztechniken (Spread Spectrum Systems, siehe z.B. [Torr_92, PiSM_82]) und
- Schutz von Aufenthaltsorten (in Funknetzen und mobilen Festnetzen) durch spezielle Pseudonyme sowie anonyme und unbeobachtbare Verfahren zum Location Management (siehe z.B. [Fede_99]).

17.4.1 Schutz des Empfängers durch Verteilung (Broadcast)

Einer der einfachsten und wirkungsvollsten Schutzmechanismen ist **Verteilung** (**Broadcast**). Jeder Nutzer eines Kommunikationsnetzes erhält alle Nachrichten aller Teilnehmer. Handelt es sich um vertrauliche Daten, können sie problemlos verschlüsselt werden. Ebenso ist eine Integritätssicherung mit Authentikationssystemen möglich.

Die Adressierung eines Nutzers erfolgt über implizite Adressen, damit die Nachrichten nur vom intendierten Adressaten erkannt werden können. **Implizite Adressen** kennzeichnen im Gegensatz zu *expliziten* weder einen Ort im Netz noch einen Teilnehmer. Sie

sind ein für Außenstehende mit nichts in Beziehung zu setzendes Merkmal. Der Empfänger kann daran erkennen, ob eine Nachricht für ihn bestimmt ist.

Offene implizite Adressen können von Unbeteiligten auf Gleichheit getestet werden. Die einfachste Implementierung von offenen impliziten Adressen sind Zufallszahlen: Ein Teilnehmer wählt sich eine Menge solcher Zufallszahlen (seine Adressen), die er in einem lokalen Speicher hält. Die Nachricht wird mit einer dieser Zufallszahlen adressiert. Durch Vergleich der verteilten Zufallszahl mit denen im lokalen Speicher kann der Empfänger erkennen, ob eine Nachricht für ihn bestimmt ist.

Verdeckte implizite Adressen können nur vom Adressaten auf Gleichheit getestet werden. Der Test auf Gleichheit durch den Adressaten stellt eine kryptographische Operation dar und ist deshalb auch für den Adressaten deutlich aufwendiger als bei offenen impliziten Adressen.

17.4.2 Proxies

Proxies (Stellvertreter) verbergen den Ursprung einer Verbindung im Internet. Hierzu bauen die Programme eines Benutzers zunächst eine Verbindung zu einem Proxy-Server auf, der seinerseits (stellvertretend) die vom Benutzer gewünschte Verbindung zum Zielrechner (z.B. einem WWW-Server) aufbaut (→ Bild 17.9). Proxy-Server werden häufig zusammen mit Cache-Servern und **Firewalls** an der Übergangsstelle vom (firmeninternen) Intranet zum Internet betrieben. Beobachtern im Internet bleiben damit die (firmeninternen) Netzstrukturen und Adressen verborgen. Dies erschwert Hackern das Eindringen in das Intranet. Darüber hinaus verhindern sie die Beobachtung einzelner Nutzer, da die Ursprungsadresse einer Verbindung vor dem Internet verborgen wird.

Proxies schützen nicht vor einem Beobachter, der im Intranet verbreitet ist. Ebenso schützen sie nicht, wenn der Proxy selber der Beobachter ist. Ein Verfahren, das selbst gegen Beobachtung durch den Betreiber des Proxys sicher ist, ist das Mix-Netz (→ 17.4.3).

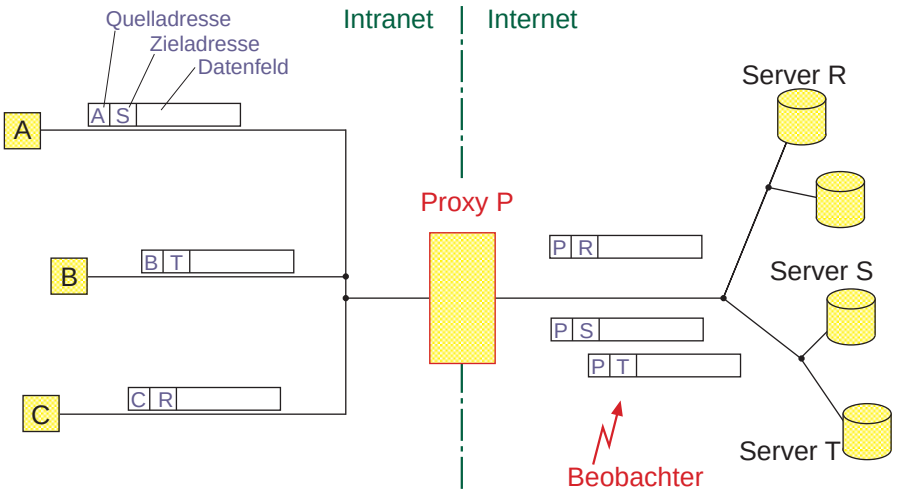

Bild 17.9: Proxies als Schutz vor Beobachtern im Internet

17.4.3 Das Mix-Netz

Das **Mix-Netz** [Chau_81] verbirgt die Kommunikationsbeziehung zwischen Sender und Empfänger einer Nachricht. Dabei darf ein Angreifer alle Leitungen des Kommunikationsnetzes beobachten, und trotzdem bleibt die Kommunikationsbeziehung unbeobachtbar. Hierzu wird die Nachricht über sog. Mixe geschickt. Ein Mix verbirgt dabei die Verkettung zwischen eingehenden und ausgehenden Nachrichten.

Von seiner Grundfunktion ist der Mix einem Proxy ähnlich. Allerdings schützt das Mix-Netz auch vor Beobachtung durch die Mixe selber. Hierzu wird eine Nachricht über mehrere Mixe zum Empfänger transportiert. Das Ziel des Mix-Netzes ist, daß alle Mixe, die von einer Nachricht durchlaufen wurden, zusammenarbeiten müssen, um die Kommunikationsbeziehung zwischen Sender und Empfänger aufzudecken. Die durchlaufenen Mixe sollten bzgl. ihres Entwurfs, ihrer Herstellung und insbesondere bzgl. ihres Betreibers möglichst unabhängig sein. Andernfalls könnten Mixe (oder gar ganze Mix-Ketten) überbrückt und so die Kommunikationsbeziehung aufgedeckt werden.

Ein Mix muß eingehende Nachrichten speichern, bis genügend viele Nachrichten von genügend vielen Absendern vorhanden sind, ihr Aussehen verändern, d.h. sie umkodieren, und die Reihenfolge der ausgehenden Nachrichten verändern, d.h. sie umsortieren und in einem Schub ausgeben.

Die Kernfunktion eines Mixes ist das Umkodieren der Nachrichten. Das Umkodieren erfolgt mit einem asymmetrischen Konzelationssystem.

- Weiterführende Literatur zum Mix-Netz: [PfPW_88, Pfit_90, PfPf_90, PfPW_91]

17.4.4 Das DC-Netz: Schutz des Senders

Beim **DC-Netz** (die Abkürzung steht für die Initialen des Erfinders David Chaum, [Chau_88]) wird durch sog. überlagerndes Senden aller Teilnehmer des Netzes der Schutz des Senders erreicht: Teilnehmer können Nachrichten ins Netz senden, ohne daß beobachtbar ist, wer der Absender der Nachricht ist.

Die Teilnehmer haben paarweise miteinander Schlüssel ausgetauscht, die sie vor den anderen Teilnehmern geheim halten. Das Netz ist getaktet und das Funktionsprinzip jedes Taktes (auch Runde genannt) ist folgendes: Alle Teilnehmer, die nichts zu senden haben, senden eine kodierte Leerbotschaft (Null-Bits). Derjenige, der etwas zu senden hat, sendet seine Botschaft kodiert. Leernachrichten bzw. echte Botschaften werden dabei mit allen symmetrischen Schlüsseln, die ein Teilnehmer mit anderen Teilnehmern paarweise ausgetauscht hat, lokal bitweise XOR verknüpft und als sog. lokale Summe auf das Netz gegeben. Durch die lokale XOR-Verknüpfung der (Leer-)Botschaft mit den Schlüsseln sieht eine lokale Summe für denjenigen, der nicht alle lokalen Schlüssel kennt, wie eine Zufallszahl aus. Durch die globale Überlagerung (globale Summe) aller lokalen Summen heben sich die paarweisen Schlüssel weg, die Leerbotschaften liefern keinen Beitrag und es entsteht so die Summe der (Leer-)Botschaften, die ihrerseits alle Teilnehmer erhalten.

- Beispiel: (→ Bild 17.10) Es kooperieren drei Teilnehmer A, B und C in einem DC-Netz. Sie haben vorher *paarweise* miteinander Schlüssel ausgetauscht. Teilnehmer A sendet die Botschaft "00110101". B und C senden Leerbotschaften.

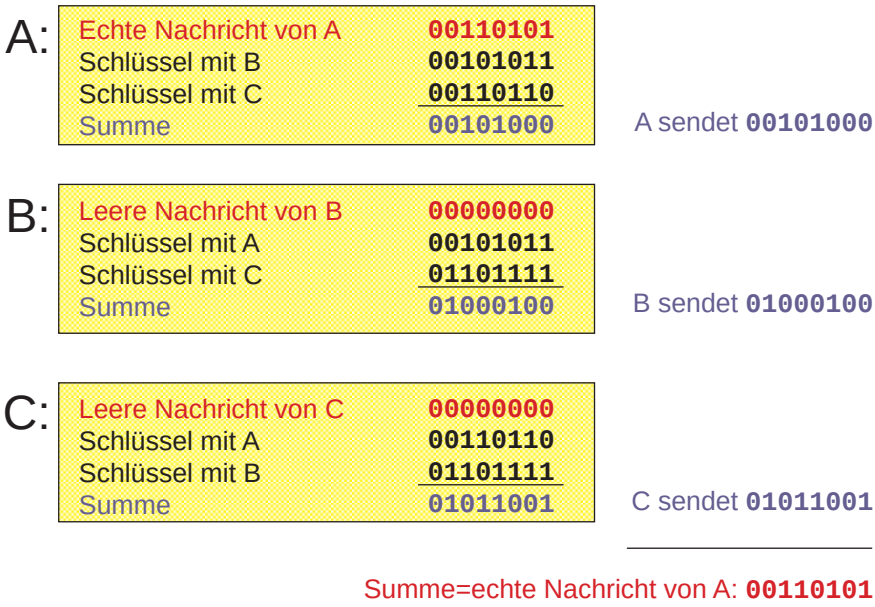

Bild 17.10: Bitweises Überlagerndes Senden im DC-Netz

17.4.5 Pseudonymität

Manche Anwendung erfordert trotz anonymer und unbeobachtbarer Kommunikation auch die Zurechenbarkeit von Aktionen (z.B. Bestellungen) zu ihrem Akteur. **Pseudonymität** gestattet die Verknüpfung von Anonymität und Zurechenbarkeit. Das bedeutet, Transaktionen werden nicht unter der Identität des Akteurs durchgeführt, sondern unter einem Kennzeichen (Pseudonym), das ggf. (z.B. im Streitfall) aufgedeckt werden kann, d.h. mit der Identität verknüpft wird. Einfache Pseudonymitätskonzepte arbeiten mit einem vertrauenswürdigen Dritten (hier Treuhänder genannt), der die Identität des Teilnehmers kennt und im Bedarfsfall aufdeckt. Kompliziertere Pseudonymitätskonzepte bilden die Funktion des Treuhänders mit Hilfe kryptographischer Verfahren nach und lassen sich so auch ohne aktive Beteiligung vertrauenswürdiger Dritter Instanzen realisieren [Chau_85].

Man unterscheidet Personen- und Rollenpseudonyme, die bezüglich ihrer Anonymität skalierbar sind. In [PWP_90] wurden die verschiedenen Arten von Pseudonymen grob eingeteilt (→ Bild 17.11).

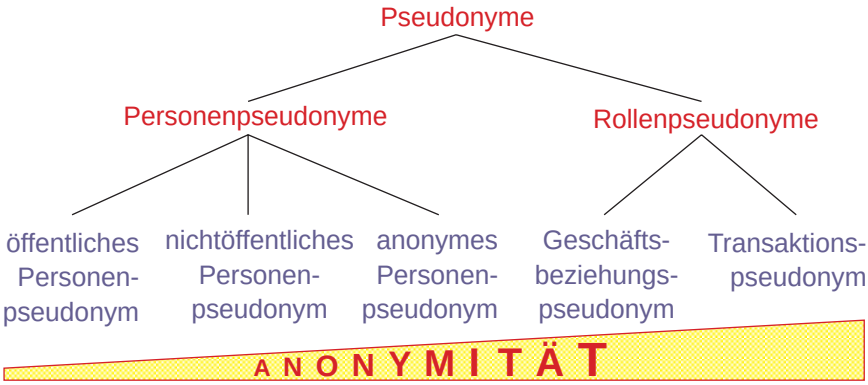

Bild 17.11. Pseudonyme sind skalierbar in ihrem Personenbezug

Ein **Personenpseudonym** wird für viele verschiedene Geschäftsbeziehungen über lange Zeit hinweg verwendet. Es stellt somit einen Namensersatz dar. Bei *öffentlichen* Personenpseudonymen ist die Zuordnung zu einer Person allgemein bekannt (z.B. Telefonnummern), bei *nichtöffentlichen* Personenpseudonymen ist diese Zuordnung nur wenigen Stellen bekannt (z.B. nicht im Teilnehmerverzeichnis aufgeführte Telefonnummern) und bei anonymen Personenpseudonymen ist diese Zuordnung nur dem Besitzer bekannt (z.B. biometrische Merkmale des Teilnehmers oder gar seine DNA).

Im Streitfall ist man bei den öffentlichen und nichtöffentlichen Personenpseudonymen in der Lage, die Verkettung zwischen der Identität und dem Pseudonym herzustellen. Damit kann eine Person trotz Pseudonymverwendung verfolgt werden, falls dies erforderlich ist.

Bei anonymen Personenpseudonymen besteht innerhalb des Kommunikationsnetzes keine direkte Möglichkeit zur Verkettung mit einer Identität. Da sich jedoch bei jeder Pseudonymbenutzung personenbezogene Daten ansammeln, besitzt man nach einer gewissen Zeit genug Informationen zur Deanonymisierung des anonymen Personenpseudonyms. Über Kontextinformationen, z.B. die zeitlich oder örtlich verkettete Beobachtung einer verdächtigen Person bei nicht anonymen Handlungen (u.U. auch außerhalb des Kommunikationsnetzes) kann ein Bezug zur Identität der Person hergestellt werden.

Rollenpseudonyme sind im Gegensatz zu Personenpseudonymen nicht einer Person, sondern *nur* ihrer momentan ausgeübten Rolle zugeordnet. Geschäftsbeziehungspseudonyme werden für viele Transaktionen verwendet, z.B. eine Kontonummer bei den vielen Buchungen eines Kontos. Transaktionspseudonyme hingegen werden nur für eine Transaktion verwendet, z.B. Kennwörter bei anonym aufgegebenen Chiffreanzeigen. Bei Verwendung von Rollenpseudonymen können verschiedene Parteien über den Pseudonymträger gesammelte Information zumindest nicht einfach über die Gleichheit von Pseudonymen, sondern allenfalls über Korrelation von Zeiten, Geldbeträgen etc. verketten. Trotzdem besteht bei Geschäftsbeziehungspseudonymen die Gefahr, daß bei intensiv genutzten Beziehungen der Partner genügend pseudonymbezogene Information zur Deanonymisierung erhält. Aus Sicht des Datenschutzes sollten daher, wenn immer möglich, Transaktionspseudonyme verwendet werden.

17.5 Rechtsaspekte

Datenschutz ist in unterschiedlichen Rechtsnormen verankert. Er umfaßt allgemeine und bereichsspezifische Regelungen. **Allgemeine Regelungen** sind das Bundesdatenschutzgesetz (BDSG) und die Landesdatenschutzgesetze. Das BDSG definiert u.a. einige Grundsätze des Datenschutzes, z.B. Zweckbindung, Verhältnismäßigkeit, Einwilligung,

sowie Rechte der Betroffenen, z.B. Recht auf Auskunft, Benachrichtigung, Berichtigung, Sperrung, Löschung und Schadensersatz. In den **bereichsspezifischen Regelungen** wird versucht, bereichsspezifischen Aspekten des Datenschutzes gerecht zu werden. Solche Bereiche sind z.B. das Gesundheits- und Sozialwesen, Polizei/Verfassungsschutz und die Telekommunikation. Bereichsspezifische Regeln gehen den allgemeinen vor. Die wichtigsten bereichsspezifischen Regelungen für den Bereich Telekommunikation sind:

- Artikel 10 Grundgesetz
- Telekommunikationsgesetz (TKG),
- Telekommunikations-Dienstunternehmen-Datenschutzverordnung (TDSV),
- EG-Telekommunikations-Datenschutzrichtlinie,
- Informations- und Kommunikationsdienste-Gesetz (IuKDG), bestehend aus:
  - Teledienstegesetz (TDG),
  - Teledienstedatenschutzgesetz (TDDSG),
  - Signaturgesetz (SigG),
- Telekommunikations-Überwachungsverordnung (TKÜV).

In diesen Vorschriften sind u.a. Regeln zum Fernmeldegeheimnis, zur datenschutzgerechten Abrechnung von Telekommunikationsleistungen, Rufnummernanzeige, Gestaltung von Teilnehmerverzeichnissen und staatlichen Überwachungsmaßnahmen enthalten.

- Gesetzestexte, Hinweise und aktuelle Informationen: http://www.datenschutz.de, [BfD_99, GeRo]

Literatur

BfD_99 Der Bundesbeauftragte für den Datenschutz: BfD-Info 5 - Datenschutz und Telekommunikation. 3. Auflage, September 1999.

Chau_81 David Chaum: Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. Communications of the ACM 24/2 (1981) 84-88.

Chau_85 David Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM 28/10 (1985) 1030-1044.

Chau_88 David Chaum: The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. Journal of Cryptology 1/1 (1988) 65-75.

CoBi_95 David A. Cooper, Kenneth P. Birman: Preserving Privacy in a Network of Mobile Computers. 1995 IEEE Symposium on Research in Security and Privacy, IEEE Computer Society Press, Los Alamitos 1995, 26-38.

Fede_99 Hannes Federrath: Sicherheit mobiler Kommunikation. DuD Fachbeiträge, Vieweg, Wiesbaden 1999.

GeRo Martin Geppert, Alexander Rossnagel: TeleMediaRecht - Telekommunikations- und Multimediarecht. Beck-Texte im dtv.

IHW_96 Proc. 1st Workshop on Information Hiding, LNCS 1174, Springer-Verlag, Berlin 1996.

IHW_98 Proc. 2nd Workshop on Information Hiding, LNCS 1525, Springer-Verlag, Berlin 1998.

Pfit_90 Andreas Pfitzmann: Diensteintegrierende Kommunikationsnetze mit teilnehmerüberprüfbarem Datenschutz. IFB 234, Springer-Verlag, Berlin 1990.

PfPf_90 Birgit Pfitzmann, Andreas Pfitzmann: How to Break the Direct RSA-Implementation of MIXes. Eurocrypt '89, LNCS 434, Springer-Verlag, Berlin 1990, 373-381.

PfPW_88 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: Datenschutz garantierende offene Kommunikationsnetze. Informatik-Spektrum 11/3 (1988) 118-142.

PfPW_91 Andreas Pfitzmann, Birgit Pfitzmann, Michael Waidner: ISDN-MIXes – Untraceable Communication with Very Small Bandwidth Overhead. Proc. Kommunikation in verteilten Systemen, IFB 267, Springer-Verlag, Berlin 1991, 451-463.

PiSM_82 R.L. Pickholtz, D.L. Schilling, L.B. Milstein: Theory of Spread-Spectrum-Communications – A Tutorial. IEEE Transactions on Communications 30/5 (1982) 855-878.

PWP_90 Birgit Pfitzmann, Michael Waidner, Andreas Pfitzmann: Rechtssicherheit trotz Anonymität in offenen digitalen Systemen. Datenschutz und Datensicherung DuD 14/5-6 (1990) 243-253, 305-315.

Schn_96 Bruce Schneier: Applied Cryptography: Protocols, Algorithms, and Source Code in C. John Wiley & Sons, (2nd ed.) New York 1996. (Die deutsche Übersetzung ist bei Addison-Wesley-Longman erschienen.)

Torr_92 Don J. Torrieri: Principles of Secure Communication Systems. 2nd ed., Artech House Books, 1992.

Ausgewählte Standards im Bereich Datenschutz und Datensicherheit

Internet Engineering Task Force (IETF)

RFC 1421 Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures

RFC 1422 Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management

RFC 1423 Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers

RFC 1424 Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services

RFC 2015 MIME Security with Pretty Good Privacy (PGP)

RFC 2246 The TLS Protocol Version 1.0

RFC 2401 Security Architecture for the Internet Protocol

RFC 2402 IP Authentication Header

RFC 2406 IP Encapsulating Security Payload (ESP)

RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP)

RFC 2409 The Internet Key Exchange (IKE)

RFC 2440 OpenPGP Message Format

RFC 2632 S/MIME Version 3 Certificate Handling

RFC 2633 S/MIME Version 3 Message Specification

RFC 2659 Security Extensions For HTML

RFC 2660 The Secure HyperText Transfer Protocol

International Organization for Standardization (ISO)

ISO 7498-2:1989 Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture

ISO 8372:1987 Information processing – Modes of operation for a 64-bit block cipher algorithm

ISO 9160:1988 Information processing – Data encipherment – Physical layer interoperability requirements

ISO/IEC 10116:1991 Information technology – Modes of operation for an n-bit block cipher algorithm

ISO/IEC 10164-7:1992 Information technology – Open Systems Interconnection – Systems Management: Security alarm reporting function

ISO/IEC 10164-8:1993 Information technology – Open Systems Interconnection – Systems Management: Security audit trail function

ISO/IEC DIS 10181-1 Information technology – Open Systems Interconnection – Security Frameworks for Open Systems: Overview

ISO/IEC DIS 10181-2 Information technology – Open Systems Interconnection – Security Frameworks for Open Systems – Part 2: Authentication Framework

ISO/IEC DIS 10181-3 Information technology – Open Systems Interconnection – Security frameworks in open systems – Part 3: Access control

ISO/IEC DIS 10181-4 Information technology – Open Systems Interconnection – Security frameworks in Open Systems – Part 4: Non-repudiation

ISO/IEC DIS 10181-5 Information technology – Security frameworks in open systems – Part 5: Confidentiality

ISO/IEC DIS 10181-6 Information technology – Security frameworks in open systems – Part 6: Integrity

ISO/IEC DIS 10181-7 Information technology – Open Systems Interconnection – Security Frameworks for Open Systems: Security Audit Framework

International Telecommunication Union (ITU)

[X.273] Recommendation X.273 - Information technology - Open Systems Interconnection - Network layer security protocol (9)

[X.274] Recommendation X.274 - Information technology - Telecommunication and information exchange between systems - transport layer security protocol (6)

[X.509] Recommendation X.509 - Information technology - Open Systems Interconnection - The directory: Authentication framework (4)

[X.736] Recommendation X.736 - Information technology - Open Systems Interconnection - Systems management: Security alarm reporting function (6)

[X.740] Recommendation X.740 - Information technology - Open Systems Interconnection - systems management: security audit trail function (6)

[X.800] ITU-T Recommendation X.800 - Security architecture for Open Systems Interconnection for CCITT applications (6)

[X.802] Recommendation X.802 - Information technology - Lower layers security model (2)

[X.803] Recommendation X.803 - Information Technology - Open Systems Interconnection - Upper layers security model (2)

[X.810] ITU-T Recommendation X.810 – Security Frameworks For Open Systems: Overview