46.239.32

Orientierungshilfe zum Einsatz kryptografischer Verfahren

Version 1.0
Stand September 2003

Gliederung

Abschnitt 1 **Einleitung**

Abschnitt 2 **Datenschutzrechtliche Grundlagen**

2.1 Schutzziele

2.2 Datenkategorien mit besonderem Schutzbedarf
2.2.1 Gesundheitsdaten
2.2.2 Daten über Dienst- und Arbeitsverhältnisse (Personaldaten)
2.2.3 Sozial- und Steuerdaten

Abschnitt 3 **Technische Grundlagen der Kryptographie**

3.1 Was kryptographische Verfahren leisten
3.2 Klassen von Verschlüsselungsverfahren
3.3 Schlüssellängen und ihre Bedeutung
3.4 Schlüsselverwaltung
3.5 Attacken
3.6 Recovery
3.7 Filterung und Virenschutz beim Einsatz von Verschlüsselung
3.8 Verschlüsselung durch Auftragnehmer
3.9 Kryptokontroverse und Exportkontrolle

Abschnitt 4 **Grundszenarien der Nutzung der Informationstechnik im Zusammenhang mit ihrer Absicherung mit kryptographischen Verfahren**

4.1 Die Verschlüsselung bei der Speicherung von Daten
4.1.1 Verschlüsselung für die Zugriffskontrolle
4.1.2 Verschlüsselung für die Weitergabekontrolle beim Datenträgeraustausch
4.1.3 Merkmale für das Verschlüsselungsverfahren bei der Speicherverschlüsselung

4.2 Die Verschlüsselung bei der Übertragung von Daten
4.3 Die Verschlüsselung für Zwecke der Authentisierung

Abschnitt 5 **Allgemeine Lösungsansätze**

5.1 Tunneling
5.2 Elektronische Signaturen
5.3 Challenge Response-Verfahren

5.4 Leitungs- und Ende-zu-Ende-Verschlüsselung
5.5 Kryptoboxen
5.6 Verschlüsselungskomponenten von Standardsoftware

Abschnitt 6 Szenarien – Infrastrukturen

6.1 Internet
6.2 Landesnetze
6.3 Corporate und Virtual Private Networks (VPN)
6.4 Lokale Netze
6.5 Sprachkommunikation und Telefax

Abschnitt 7 Szenarien - ausgesuchte Anwendungsfälle

7.1 Abschottung der Systemadministration
7.2 Anbindung von Außenstellen
7.3 E-Commerce - Elektronischer Handel
7.4 Elektronische Bürgerdienste
7.5. Elektronische Post
7.6 Externe Archivierung
7.7 Fernwartung
7.8 Mobile Geräte und Datenträger
7.9 Outsourcing
7.10 Außendienst und Telearbeit

Anhang 1 Glossar
Anhang 2 Abkürzungsverzeichnis
Anhang 3 Literaturverzeichnis

Hinweis:

Verweise auf einen Abschnitt X.Y werden durch das Symbol (-->X.Y), Verweise auf das Glossar durch das Symbol (-->G) dargestellt.

Abschnitt 1 Einleitung

Geheimschriften und ihre Entzifferung haben Menschen seit Alters her mit breitem Spektrum fasziniert:

- Kindliche Fantasie wird angeregt mit dem Abenteuer, etwas aufschreiben zu können, was kein anderer (vor allem nicht die Eltern oder Lehrer), nur man selbst lesen und verstehen kann.

- Militärische, diplomatische oder geschäftliche Geheimnisse sollen in einer Form weitergegeben werden, dass sie auf dem Weg zum Empfänger nicht gegenüber den Falschen offenbart werden können.

Das Raum zwischen Spiel und Ernst wird gefüllt von der

- Kryptologie, die sich mit den Methoden befasst, wie man den Inhalt von Nachrichten Dritten gegenüber unter Anwendung von Regeln und Schlüsseln verbirgt (Kryptografie), und umgekehrt mit den Methoden, wie man den verborgenen Inhalt als Dritter dennoch aufspüren kann (Kryptoanalyse), und der

- Steganografie, die sich mit den Methoden befasst, eine geheime Nachricht in einer nicht geheimen Nachricht so unter Anwendung von Regeln zu verstecken, dass sie niemand finden kann, der die Regeln nicht kennt.

Bis vor nicht allzu langer Zeit hatte die Beschäftigung mit Kryptologie und Steganografie die Aura einer Geheimwissenschaft. Das Problem, vertrauliche Nachrichten über weite Entfernungen zu übermitteln, spielte im alltäglichen Leben keine Rolle, war vielmehr eine Angelegenheit des Staates und großer Unternehmen, die darüber kein Aufsehen erwecken wollten.

Lesenswerte Ausführungen zu den historischen Hintergründen der Kryptografie findet man z. B. in [Bauer91].

Mit dem Siegeszug der Computer und ihrer weltweiten Vernetzung, an dem die meisten Haushalte in den entwickelten Ländern bereits teilnehmen, also mit dem Aufkommen der Informationsgesellschaft, sind auch die Bedürfnisse zur technisch vermittelten Kommunikation immens gestiegen. Gleichzeitig steigen die Bedürfnisse, die Kommunikation vertraulich zu gestalten. Ob die Unternehmen (B2B) oder Behörden (G2G) untereinander oder miteinander (B2G) oder mit ihren Kunden (B2C) oder Bürgern (G2C) kommunizieren wollen, fast immer besteht ein Bedarf ein Vertraulichkeit, manchmal auch, wenn Menschen privat kommunizieren.

Die Anwendung kryptografischer Verfahren findet heute gesamtgesellschaftliche Verbreitung und hat damit die Sphäre des Geheimnisvollen verlassen. Der Versuch, die Anwendung zu reglementieren, weil ja auch Straftäter die Kryptografie nutzen können, hat sich als untauglich erwiesen, weil er dem hohen Bedarf der Ehrlichen entgegen steht, mit garantierter Vertraulichkeit zu kommunizieren. Damit steht er auch der Entwicklung der Informationsgesellschaft entgegen.

Den öffentlichen Stellen des Bundes, der Länder und der Kommunen, stellt sich damit ebenfalls die Frage, welchen kryptografischen Methoden, Verfahren und Produkten in unterschiedlichen Szenarien der Informationsverarbeitung und Kommunikation unter den Aspekten der Wirksamkeit und der Wirtschaftlichkeit der Vorzug zu geben ist. Diese Frage richten sie auch an die Datenschutzbeauftragten in Bund und Ländern, die gesetzlich zur Beratung der öffentlichen Stellen berufen sind.

Zur Unterstützung dieser Beratungstätigkeit wurde die vorliegende Orientierungshilfe zum Einsatz kryptografischer Verfahren von einer Arbeitgruppe des Arbeitskreises für technische und organisato-

rische Fragen des Datenschutzes der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet.

Selbstverständlich bestehen keine Einwände, wenn auch Unternehmen der Privatwirtschaft oder Privatleute Nutzen aus der Orientierungshilfe zielen wollen.

Die Orientierungshilfe beschreibt in **Abschnitt 2** die Schutzziele des Datenschutzes, die mit technischen Methoden anzustreben sind und macht auf Datenkategorien mit besonderem Schutzbedarf aufmerksam. An den Beispielen Gesundheits-, Personal-, Sozial- und Steuerdaten wird deutlich, dass Daten mit besonderem Schutzbedarf keineswegs eine Ausnahme darstellen.

Abschnitt 3 führt in die technischen Grundlagen der Kryptografie ein, differenziert zwischen den unterschiedlichen mathematischen Prinzipien und befasst sich mit wichtigen Rahmenbedingungen für sichere kryptografische Verfahren wie die Länge der zu verwendenden Schlüssel, ihre Verwaltung und vertrauliche Verbreitung, Risiken der Kryptoanalyse, ggf. notwendiges Key Recovery, Zielkonflikte mit Filterungsverfahren und Verfahren des Virenschutzes, Verschlüsselung beim Outsourcing und befasst sich mit der wirtschafts- und sicherheitspolitischen Diskussion um den Einsatz kryptografischer Werkzeuge.

Abschnitt 4 beschreibt die Grundszenarien der Nutzung der Informationstechnik, für die der Einsatz kryptografischer Verfahren in Betracht kommt: Bei der Speicherung von Daten, bei der Übertragung von Daten und zur Authentisierung von Daten, also der Zuordnung von Daten zu ihrem Ursprung, u. A. mittels digitaler Signatur.

Allgemeine Lösungsansätze werden in **Abschnitt 5** gezeigt. Dazu zählen das Tunneling, die digitale Signatur, das Challenge Response-Verfahren zur gegenseitigen Authentisierung technischer Systeme, Leitungs- und Ende-zu-Ende-Verschlüsselung, Hardwareverschlüsselung mit Kryptoboxen und die in verschiedenen Software-Standardprodukten einbezogenen Verschlüsselungskomponenten.

Die **Abschnitte 6 und 7** beschreiben in schematisierter Weise Szenarien, die dort auftretenden Sicherheitsprobleme, die Lösungswege für diese Probleme unter Anwendung der Kryptografie und geben in Einzelfällen Hinweise auf Besonderheiten. Zunächst befassen sich die Szenarien mit Infrastrukturen (Abschnitt 6), dann mit ausgesuchten Anwendungsfällen (Abschnitt 7), wobei bei der Auswahl der Anwendungsfälle die Erfahrungen aus der Beratungspraxis der Datenschutzbeauftragten ausschlaggebend waren.

Im **Glossar** im **Anhang 1** finden sich nicht nur Erklärungen verschiedener Begriffe, sondern auch eine nähere technische Beschreibung von Protokollen und Produkten, die nach Auffassung der Autoren bei der Lösung der in den Abschnitten 6 und 7 aufgeworfenen Sicherheitsprobleme eine besondere Rolle spielen.

Als weitere Anhänge finden sich ein **Abkürzungsverzeichnis** (Anhang 2), ein **Literaturverzeichnis** (Anhang 3) und eine **Linkliste** relevanter Fundstellen im Internet (Anhang 4).

Abschnitt 2

Datenschutzrechtliche Grundlagen

2.1 Schutzziele

Ausgehend von der Erkenntnis, dass eine absolute Datensicherheit in der Praxis nicht zu erreichen ist, sind in den Datenschutzgesetzen die Prinzipien der „Angemessenheit“ und „Erforderlichkeit“ festgeschrieben worden. Dies bedeutet, dass in Abhängigkeit von dem Schutzbedürfnis der betreffenden personenbezogenen Daten (Angemessenheit) entsprechend wirksame (erforderliche) Sicherheitsmaßnahmen zu treffen sind. In einigen Gesetzen wird explizit verlangt, dass die Maßnahmen dem Stand der Technik zu entsprechen haben. Ferner gibt es Datenschutzgesetze, die ausdrücklich Risikoanalysen und Sicherheitskonzepte verlangen, um näher zu konkretisieren, was warum als angemessen und erforderlich anzusehen ist.

Dabei ist zu berücksichtigen, dass es völlig „schutzlose“ personenbezogene Daten nicht gibt. Der Grad ihrer Schutzbedürftigkeit ergibt sich aus dem Rechtsverhältnis des Betroffenen zur Daten verarbeitenden Stelle und dem Zweck der Datennutzung. In der Praxis lassen sich „normale“ und besonders zu sichernde Verwaltungsdaten unterscheiden. Diesen Aspekt hat das BSI auch in seinem Grundschutzhandbuch, das sich nur auf die Kategorie der „normalen“ Daten bezieht, aufgegriffen.

2.2 Datenkategorien mit besonderem Schutzbedarf

Die Daten, die einer besonders gesicherten Behandlung bedürfen, sind im Wesentlichen solche über

- die rassische oder ethnische Herkunft,
- politische Meinungen,
- religiöse oder philosophische Überzeugungen,
- die Gewerkschaftszugehörigkeit,
- die Gesundheit,
- das Sexualleben,
- Dienst- und Arbeitsverhältnisse sowie
- steuerliche und soziale Verhältnisse.

Nachfolgend werden an einigen Beispielen die sicherheitstechnischen Konsequenzen aus diesen rechtlichen Gegebenheiten erläutert.

2.2.1 Gesundheitsdaten

Gesundheitsdaten zählen nach der EG-Datenschutzrichtlinie vom 24.10.1995 zu der Kategorie von Informationen, die im höchsten Maße vertraulich zu behandeln sind. Dies spiegelt sich auch im nationalen Rechtssystem wieder. Die ärztlichen Berufsordnungen, das Strafgesetzbuch (§ 203 StGB), das Sozialgesetzbuch (§ 76 SGB X) und die Datenschutzgesetze verpflichten die Daten verarbeitenden Stellen (Ärzte, Krankenkassen, Arbeitgeber, Versicherungsunternehmen usw.) zu einem besonders abgesicherten Umgang mit derartigen Datenbeständen.

Es ist dabei zu unterscheiden zwischen den umfassenden Anamnese-, Diagnose- und Therapiedaten in den ärztlichen Dokumentationen (Patientenkarteien/-dateien) und den daraus selektierten Sekundärdatenbeständen (Abrechnungsdaten, Bescheinigungen, Atteste usw.). Die gesetzlichen Anforderungen an die Datensicherheitsmaßnahmen differieren insoweit auf einem allerdings hohen Niveau. Logischerweise sind sie am anspruchsvollsten in Bezug auf die ärztlichen Datenbestände. Die Bundesärztekammer hat daher in ihren „Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis“ [BÄK96] u.a. festgestellt:

- Die Wartung einer EDV-Anlage oder jegliche Fehlerbeseitigung vor Ort darf grundsätzlich nur mit Testdaten erfolgen. Im Notfall, z. B. beim Systemstillstand in einer spezifischen Patientendatenkonstellation, muss der Einblick Dritter in Originaldaten auf besondere Ausnahmefälle eingeschränkt bleiben. Das Wartungspersonal ist zu beaufsichtigen und schriftlich auf die Verschwiegenheit zu verpflichten. Die durchgeführten Maßnahmen sowie der Name der Wartungsperson sind zu protokollieren.
- Die Fernwartung von EDV-Systemen in Arztpraxen ist unzulässig, wenn nicht auszuschließen ist, dass dabei auf patientenbezogene Daten zugegriffen werden kann.
- Bei einem Datenträgeraustausch mit befugten Dritten ist ein sicherer Transport zu gewährleisten.
- Die Datenfernübertragung personenbezogener Daten per Leitung muss chiffriert erfolgen.
- Auszumusternde Datenträger müssen unter Aufsicht des Arztes (z. B. durch mehrfaches Überschreiben mittels geeigneter Software) unbrauchbar gemacht werden.

2.2.2 Daten über Dienst- und Arbeitsverhältnisse (Personaldaten)

Als Personaldaten werden alle personenbezogenen Informationen bezeichnet, die in einem unmittelbaren Zusammenhang mit dem Inhalt und dem Verlauf eines Beschäftigungsverhältnisses stehen. Typischerweise sind dies: Bewerbungsunterlagen, Personalfragebogen, Nachweise für Vor-, Aus- und Fortbildung, Zeugnisse, Arbeitsverträge oder Ernennungsurkunden, Beurteilungen, Abmahnungen usw. sowie der Schriftwechsel zwischen dem Arbeitgeber und dem Arbeitnehmer. Diese Daten sind sowohl innerhalb der Dienststelle als auch gegenüber außenstehenden Dritten vertraulich zu behandeln. Daher muss der Arbeitgeber den Kreis der mit Personaldaten befassten Mitarbeiter möglichst klein halten. EDV-Personal, Service-Techniker usw. zählen grundsätzlich nicht zur Personalverwaltung, daher ist ihnen die Kenntnisnahme der Inhalte der Personaldateien bzw. der Personalinformationssysteme unmöglich zu machen.

2.2.3 Sozial- und Steuerdaten

Beide Datengruppen unterliegen einem „klassischen“ besonderen Amtsgeheimnis. Die gesetzlichen Regelungen in § 35 SGB I und § 30 AO erzwingen eine Abschottung auf der Bearbeiterebene („Die Wahrung des Sozialgeheimnisses umfasst die Pflicht, auch innerhalb des Leistungsträgers sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind oder nur an diese weitergegeben werden. Sozialdaten der Beschäftigten und ihrer Angehörigen dürfen Personen, die Personalentscheidungen treffen oder daran mitwirken können, weder zugänglich sein noch von Zugriffsberechtigten weitergegeben werden.“).

Befugt, im Einzelfall Sozial- bzw. Steuerdaten zur Kenntnis zu nehmen, sind also nur diejenigen Mitarbeiter, die im Rahmen ihrer Aufgabenstellung an dem konkreten Sozialleistungs- bzw. Besteuerungsverfahren mitwirken. Häufig wird die Abschottung in den Finanzämtern, Krankenkassen, Sozialämtern usw. über differenzierte Zugriffsbefugnisse realisiert. Diese Verfahrensweise stößt dann an ihre Grenzen, wenn eigenes oder fremdes technisches Personal bei seiner Aufgabenerledigung notwendigerweise in Kontakt mit gespeicherten Datenbeständen bzw. zu übertragenden Daten kommen würde (System- und Netzwerkadministratoren, Leitungstechniker, Softwareentwickler usw.). Ihnen gegenüber kann das Sozial- und Steuergeheimnis effektiv nur durch entsprechende Verschlüsselungen der Dateien bzw. Datenströme gewahrt werden.

Abschnitt 3

Grundlagen der Kryptografie

3.1 Was kryptografische Verfahren leisten – und nicht leisten können

Kryptografische Verfahren sind Realisierungen von mathematischen Rechenvorgängen, sog. Algorithmen (-->G). Sie sind im Prinzip geeignet, die folgende Ziele zu erreichen:

- Unbefugte Personen können die Daten nicht zur Kenntnis nehmen. (**Vertraulichkeit**)
- Unbefugte Änderungen von Daten können erkannt werden. (**Integrität**)
- Es kann nachgewiesen werden, wer der Kommunikationspartner ist (Identitätsnachweis), und es kann nachgewiesen werden, von wem eine Nachricht stammt (Nachrichtenauthentisierung). (**Authentizität**)
- Dritten gegenüber kann nachgewiesen werden, dass eine Kommunikation zwischen bestimmten Partnern stattgefunden hat. (**Nichtabstreitbarkeit**)

Die Vertraulichkeit wird durch Verschlüsselung erreicht. Eine Verschlüsselung basiert auf einem Algorithmus, der unter Verwendung eines Schlüssels die Ursprungsdaten so "verquirlt", dass es für jeden, ausgenommen die autorisierten Empfänger, extrem schwierig ist, die Ursprungsdaten wieder herzustellen. Die Methoden, die der Gewährleistung von Integrität, Authentizität und Nichtabstreitbarkeit zugrunde liegen, sind Message Authentication Codes (-->G), Hashfunktionen (-->G), digitale Signaturen (-->G) und kryptografische Protokolle. Digitale Signaturen verbinden Hashfunktionen mit asymmetrischen Verschlüsselungsverfahren (-->G). Sie erlauben es festzustellen, wer eine Nachricht erzeugt hat und es ist überprüfbar, ob die signierte Datei mit der vorliegenden Datei übereinstimmt.

Verschlüsselungsverfahren und digitale Signaturen haben, auch wenn sie gleiche oder ähnliche Algorithmen verwenden, stark differierende Eigenschaften. Verschlüsselte Daten können nur die Kommunikationsteilnehmer entschlüsseln, die den geheimen Schlüssel kennen. Eine gesicherte Aussage, wer Urheber einer Nachricht ist, kann – zumindest bei asymmetrischen Verschlüsselungsverfahren – jedoch nicht getroffen werden. Demgegenüber kann eine digitale Signatur nur vom Inhaber des passenden geheimen Schlüssels erzeugt worden sein, aber jeder kann sie lesen und verifizieren.

Kryptografische Verfahren können nicht verhindern, dass Nachrichten unterdrückt oder verändert werden; sie können jedoch helfen, solche (gezielten oder ungezielten) Störungen zu erkennen. Sie sind ebenfalls nicht geeignet, eine Verkehrsanalyse („wer kommuniziert wann mit wem?“) zu verhindern, können jedoch dazu beitragen, deren Aussagekraft zu minimieren.

Kryptografie ist kein Allheilmittel für alle Probleme des Datenschutzes und der Datensicherheit. Doch in einer Reihe von Situationen gibt es aus heutiger Sicht keine Alternative.

3.2 Klassen von Verschlüsselungsverfahren

Es gibt drei Klassen von Verschlüsselungsverfahren: symmetrische (-->G), asymmetrische (-->G) und, als Kombination beider, hybride Verfahren (-->G).

Symmetrische Verschlüsselungsverfahren benutzen denselben Schlüssel für die Ver- und die Entschlüsselung. Beispiele sind DES (-->G), IDEA (-->G), Triple-DES (-->G), RC5 und der derzeitige Verschlüsselungsstandard AES (Advanced Encryption Standard) (-->G).

Asymmetrische Verschlüsselungsverfahren arbeiten im Unterschied zu symmetrischen Verfahren mit einem Schlüsselpaar. Das Schlüsselpaar besteht aus einem allgemein zugänglichen öffentlichen Schlüssel (Public-Key) (-->G) und einem geheimen Schlüssel (Private-Key) (-->G). Wird eine Nachricht mit dem öffentlichen Schlüssel verschlüsselt, so kann die Nachricht nur mit dem passenden geheimen Schlüssel entschlüsselt werden. Bekannte Verfahren sind RSA (-->G), ElGamal und ECC.

Symmetrische und asymmetrische Verfahren haben spezifische Vor- und Nachteile. Symmetrische Verfahren erreichen einen hohen Durchsatz und sind daher besser geeignet, Daten zu verschlüsseln, wenn die Anwendung, wie im Fall der Kommunikation über Netze, zeitkritisch ist. Demgegenüber ist die Schlüsselverteilung bei asymmetrischen Verfahren einfacher. Die öffentlichen Schlüssel können auf allgemein zugänglichen Servern vorgehalten werden, während bei symmetrischen Verfahren die Schlüssel so ausgetauscht werden müssen, dass sie kein Unbefugter zur Kenntnis nehmen kann. Auch müssen bei symmetrischen Verfahren sämtliche Schlüssel geheim gehalten werden, während bei asymmetrischen Verfahren jeder Teilnehmer nur seinen eigenen Schlüssel geheim halten muss (siehe 3.4).

Um die Vorteile beider Klassen zu kombinieren, wurden Hybridverfahren entwickelt. Dabei wird für jede Sitzung ein Schlüssel (Session-Key) zufällig generiert und asymmetrisch verschlüsselt ausgetauscht. Die Daten selbst werden dann durch einen schnellen symmetrischen Algorithmus mit dem Session-Key verschlüsselt.

3.3 Schlüssellängen und ihre Bedeutung

Im Zusammenhang mit der Qualität kryptografischer Verfahren ist immer wieder von der Länge der verwendeten Schlüssel die Rede, wobei je nach Zusammenhang sehr unterschiedliche Werte genannt werden. Einer Analyse aus Sicht des Datenschutzes muss vorausgeschickt werden, dass eine zu geringe Schlüssellänge zu einer nicht ausreichenden Sicherheit führt, die Frage der Schlüssellänge aber nicht als alleiniges Kriterium zur Bewertung eines Verschlüsselungsverfahrens dienen kann. Letztlich dient sie zur Ermittlung der Obergrenze für den Aufwand, der erforderlich ist, um ein Verfahren zu brechen (siehe 3.5). Sofern ein Verfahren jedoch auf andere Weise angegriffen werden kann, spielt die Schlüssellänge u.U. eine unwesentliche Rolle.

Schlüssellängen bei symmetrischen und asymmetrischen Verfahren
Zwischen beiden Verfahren muss bei der Betrachtung der Schlüssellänge unterschieden werden. Da es bei der Betrachtung der Schlüssellänge um den Aufwand geht, der für ein Brechen des Verfahrens höchstens erforderlich ist, müssen die jeweiligen mathematischen Methoden, die den Verfahren zu Grunde liegen, berücksichtigt werden. Dabei ergibt sich folgende Gegenüberstellung in etwa aufwandsäquivalenter Schlüssellängen [Schneier96, S. 194):

symmetrisch	asymmetrisch (Beispiel RSA)
56 Bit	384 Bit
64 Bit	512 Bit
80 Bit	768 Bit
128 Bit	2304 Bit

Zeitliche Relativität der Schlüssellängen
Aussagen zur (ausreichenden) Länge von kryptografischen Schlüsseln sind immer im Zusammenhang mit dem angenommenen Aufwand zu betrachten, der einem potenziellen Angreifer unterstellt wird. Dieser ist vom Stand der Technik und von dessen finanziellen und zeitlichen Ressourcen abhängig. Allein durch die Weiterentwicklung der Computertechnik werden daher die Anforderungen an Schlüssellängen immer größer. Dabei spielt nicht nur die durch ein einzelnes Gerät zur Verfügung gestellte Leistung eine Rolle, sondern in zunehmendem Maße auch die Vernetzung, die es ermöglicht, eine umfangreiche Entschlüsselungsaufgabe durch viele Geräte arbeitsteilig in kurzer Zeit zu lösen.

Theoretische Obergrenzen
Gleichwohl sind auch bei weiterhin steigenden Rechenkapazitäten den Möglichkeiten der Entschlüsselung physikalische Grenzen gesetzt. Aus Erwägungen der Thermodynamik heraus lässt sich folgern, dass symmetrische Verfahren ab ca. 256 Bit Schlüssellänge in konventioneller Technik nicht mehr mit Brute-Force-Methoden (-->G) attackierbar sind, da hierfür schlichtweg die Energie des gesamten Universums nicht ausreichen würde [Schneier96, S. 185]. Neuartige Computertechniken (Stichwort: Quantencomputer) könnten diese Aussage allerdings relativieren.

Verwendungsspezifische Erwägungen
Bei der Überlegung, mit welchem Aufwand durch einen Angreifer zu rechnen ist, spielt es u.a. eine Rolle, für welche Zeitdauer die Daten geheim bleiben müssen. Daten mit kurzem Geheimhaltungsbedarf können schwächer (mit kürzeren Schlüssellängen) verschlüsselt werden als Daten mit langem Schutzbedarf (z.B. im Rahmen der Archivierung). Eine unberechtigte Entschlüsselung kann hingenommen werden, wenn die Daten bereits nicht mehr schützenswert oder aus anderen Gründen uninteressant geworden sind.

Allerdings kommt dieser Unterschiedung im Datenschutzumfeld eine geringe Bedeutung zu, da bei personenbezogenen Daten generell von einem Langzeitschutzbedarf auszugehen ist. Daher kommt es hier in der Hauptsache auf die Sensibilität der Daten an.

Empfehlungen aus Datenschutzsicht
Unter Berücksichtigung der datenschutzrechtlichen Hintergründe ist die Wahl der Verschlüsselungsverfahren und deren Parameter unter dem Aspekt des angemessenen Aufwands zu betrachten. Dabei liegt der wesentliche Faktor nicht so sehr im Aspekt des Rechenaufwandes bei einer Verschlüsselung, der für höhere Schlüssellängen zu leisten ist (dieser ist vergleichsweise gering), sondern aufgrund der Marktsituation vielmehr in der Beschaffung von Produkten, die mit geeigneten Schlüssellängen operieren können (siehe hierzu 3.9). Für den symmetrischen Bereich lässt sich beim jetzigen Stand der Technik folgende Bewertung vornehmen:

Effektive Schlüssellänge	**datenschutzrechtliche Bewertung**	**datenschutzrechtliche Empfehlung**
40 bis 55 Bit	Schutz gegen zufällige Kenntnisnahme	Einsatz bei nicht sensiblen personenbezogenen Daten, wenn ein gezielter Angriff unwahrscheinlich ist.
ab 56 Bit	Schutz von Daten mit niedrigem bis mittlerem Schutzbedarf	Einsatz bei nicht sensiblen personenbezogenen Daten oder in solchen Fällen, in denen ein Angriff mit hohem Aufwand aus anderen Gründen unwahrscheinlich ist (z.B. geschlossenes Netz). Zukünftige Sicherheitsprobleme sind jedoch zu erwarten.
ab 80 Bit	Schutz von Daten mit mittlerem bis hohem Schutzbedarf	Einsatz uneingeschränkt außer bei Daten mit sehr hohem Schutzbedarf; bei Archivierung generell höhere Schlüssellängen
ab 112 Bit	Schutz von Daten mit sehr hohem Schutzbedarf	Einsatz uneingeschränkt

In jedem Fall sollten möglichst hohe Schlüssellängen eingesetzt werden, um einen ausreichenden Schutz gegen Brute-Force-Angriffe (siehe 3.5) zu erhalten. Da ein einmal installiertes Verschlüsselungssystem sich in der Regel nicht ohne erheblichen Aufwand mit anderen Schlüssellängen oder Algorithmen versehen lässt, sollten für neue Anwendungen nur Algorithmen mit Schlüssellängen ab 112 Bit zum Einsatz kommen. Dieses entspricht auch dem aktuellen Stand der Technik: Aktuelle Produkte erreichen diesen Mindeststandard in jedem Falle.

Die empfohlenen Schlüssellängen bei asymmetrischen Algorithmen differieren in Abhängigkeit vom gewählten Algorithmus. Der bekannteste und auch verbreitetste Algorithmus ist derzeit der RSA-Algorithmus (-->G). Da er gleichzeitig Objekt intensiver und erfolgreicher Forschung zur Kryptoanalyse ist, kann er heute nicht mehr als hinreichend angesehen werden, wenn die Schlüssellänge 1024 Bit verwendet wird. Es sollten daher RSA-Schlüssel von mindestens der Länge von 2048 Bit eingesetzt werden [Weis/Lucks/Bogk03].

3.4 Schlüsselverwaltung

Erfolgt die Verschlüsselung nur zwischen zwei oder wenigen Beteiligten, bereitet die Verwaltung der Schlüssel keine nennenswerten Probleme. Bei der Verwendung symmetrischer Verfahren (-->G) steigt die Komplexität jedoch mit höherer Benutzerzahl rasch an. Um eine jeweils bilateral sichere Kommunikation zu ermöglichen, sind bei n Teilnehmern ca. $n^2/2$ Schlüssel zu verwalten, d.h. zu erzeugen, zu verteilen, zu verifizieren und nach gewisser Zeit wieder zu ersetzen. Daher wird auf zwei- oder mehrstufige Verfahren ausgewichen, bei denen die eigentlichen Schlüssel – durch besondere Schlüssel (key-encryption keys) verschlüsselt – sicher elektronisch übermittelt werden können. Nur die Schlüssel höherer Ordnung müssen dann aufwändig auf besonderem Weg verteilt werden (vgl. X9.17-Standard).

Die asymmetrische Verschlüsselung (-->G) hingegen erfordert zum einen weniger Schlüssel (n Schlüssel bei n Teilnehmern), zum anderen ist deren Versand selbst weniger sicherheitskritisch. Gleichwohl stellen sich auch hier Fragen der Schlüsselverwaltung. Das wesentliche Sicherheitsproblem bei öffentlichen Schlüsseln liegt in der korrekten Zuordnung eines öffentlichen Schlüssels zu dem zugehörigen Eigentümer. Diese Aufgabe übernehmen typischerweise besondere Stellen, für die sich im deutschen Sprachraum der Begriff „Trust Center“ (TC) (-->G)etabliert hat. Im Englischen wird dabei von „Certification Authority“ (CA) gesprochen.

TC bzw. CA stellen öffentliche Schlüssel zur Verfügung und belegen zugleich mit Hilfe eines kryptografischen Zertifikats (-->G) die Korrektheit des Schlüssels sowie dessen Zugehörigkeit zu dem angegebenen Eigentümer. Als technisches Rahmenwerk für solche Zertifikate hat sich der X.509-Standard etabliert (siehe hierzu die Orientierungshilfe Verzeichnisdienste des AK Technik). Die Verwendung eines solchen Schlüssels setzt also das Vertrauen in diese Stelle voraus. Durch eine baumartige Hierarchie von CA kann das Vertrauen jedoch auf eine höhere Instanz gestützt werden, wobei am oberen Ende im Idealfall eine Stelle angesiedelt ist, denen alle Beteiligten vertrauen. In diesem Zusammenhang wird von einer PKI (Public Key Infrastructure) (-->G) gesprochen.

Neben diesem hierarchischen Modell hat sich durch das weit verbreitete E-Mail-Verschlüsselungsprogramm PGP (-->G) ein vermaschtes Vertrauensmodell (sog. „web of trust“) etabliert. Bei diesem bestimmt jeder Benutzer selbst, in welchem Maße er oder sie einem Zertifikat traut, wobei sowohl die eigene Einschätzung eines Ausstellers als auch das Vertrauen Dritter einfließen können. Das Vertrauen in einen PGP-Schlüssel hängt dabei nicht nur vom Aussteller allein ab, sondern vom Distributionsweg und von der Korrektheit des zugehörigen Hashwerts (sog. Fingerprint) (-->G).

3.5 Attacken

Als Gegenpart zur Kryptografie ist die Kryptanalyse zu sehen. Hierbei handelt es sich um die Kunst, ohne Kenntnis des geheimen Schlüssels möglichst viele Informationen über den Klartext zu gewinnen, der einer Verschlüsselung zugrunde lag. Es gibt eine Reihe von Angriffsmöglichkeiten auf einen Algorithmus, die Kryptologen zur Verfügung stehen [Wobst97, Kapitel 3]

Ein häufiger Angriff ist die sog. Brute-Force-Attacke (-->G), bei der alle möglichen Schlüssel ausprobiert werden. Die Empfehlungen zur Schlüssellänge von symmetrischen Verfahren in 3.3 sind Einschätzungen, inwieweit dieser Angriff derzeit eine realistische Gefahr darstellt. Dabei muss man sich vor Augen halten, in welcher zeitlichen Relation ein Brechen der Schlüssel steht. Wenn man hypo-

thetisch annimmt, ein 56-Bit-Schlüssel könnte in einer Stunde ausgeforscht werden, so benötigt man für einen 80-Bit Schlüssel mehr als 1.900 Jahre. Bei einem 112-Bit Schlüssel kommt man auf die nicht mehr vorstellbare Dauer von mehr als 8.000 Milliarden Jahren; ein Vielfaches der Existenzdauer des Universums. Um auch in der überschaubaren Zukunft gegen diesen Angriff gesichert zu sein, insbesondere wenn es darum geht, archivierte Daten gegen unberechtigte Kenntnisnahme zu schützen, sind Schlüssellängen ab 112 Bit als ausreichend sicher anzusehen. Da die meisten heute verfügbaren Algorithmen Schlüssellängen von mindestens 112 Bit haben, können sie nicht mit Brute-Force-Attacken allein, sondern nur zusammen mit anderen Methoden geknackt werden.

Die Ansatzpunkte für Angriffe auf Verschlüsselungsverfahren sind daher weniger in unzureichenden Schlüssellängen zu suchen, als in Schwächen des Algorithmus (-->G) und bei der Implementierung.

Es könnten in einen Algorithmus mathematische Schwachstellen vorhanden sein, die ihn gegenüber bestimmten Analysemethoden angreifbar machen. Um derartige Schwachstellen aufzuzeigen und ev. Gegenmaßnahmen zu treffen, bietet sich eine öffentliche Diskussion unter Experten an. Der FEAL-Algorithmus bietet ein gutes Beispiel für Analysen und eine offene Diskussion darüber [Wobst97, S. 228]. Bei asymmetrischen Verfahren tritt ein vergleichbares Problem auf. Die Sicherheit beruht auf mathematischen Problemen, beim RSA (-->G) z.B. die Faktorisierung großer Zahlen, die schwer zu lösen sind. Wenn die mathematische Forschung Fortschritte macht, die bestimmte Algorithmen unsicher werden lässt, kann das nur bei offengelegten Algorithmen publik werden. Für diesen Fall müssen Ersatzalgorithmen vorhanden sein, die auf anderen mathematischen Fragestellungen beruhen. Anderenfalls profitieren zwar die Stellen, die den Algorithmus kennen, der Bürger wiegt sich aber in einer nicht vorhandenen Sicherheit. Aus diesem Grund bewirkt die Geheimhaltung von Kryptoalgorithmen in der Regel keine Verbesserung der Sicherheit.

Ein großes Problem stellt die sichere Implementierung dar. Dazu gehören Details wie Passworteingabe, Verwaltung geheimer Daten, Größe des Schlüsselraums oder Betriebsart. Zwei Beispiele sollen das illustrieren:

Bei der Implementierung eines Verschlüsselungsverfahrens in Hard- oder Software kann eine Hintertür eingebaut werden, die beispielsweise Teile des Schlüssels im Geheimtext oder im Kommunikationsprotokoll versteckt. Ein kundiger Angreifer kann den Text sofort entziffern oder muss nur noch einen kleinen Teil der möglichen Schlüssel testen. In Exportversionen vieler Produkte amerikanischer Hersteller ist für denjenigen eine effektive Schlüssellänge von 40-Bit implementiert, der die Hintertür kennt. Alle anderen Angreifer sehen sich einer Schlüssellänge von 56 und mehr Bit gegenüber.

Eine weitere wichtige Komponente in einem Verschlüsselungssystem ist ein Zufallszahlengenerator. Er ist unverzichtbar, wenn Schlüssel erzeugt werden. Wenn der Generator aber, absichtlich oder irrtümlich, nicht alle möglichen Schlüssel generiert, reduziert das die Zahl der möglichen Schlüssel. Eine Brute-Force-Attacke kann dann trotz eigentlich ausreichender Schlüssellänge machbar sein. Ein Beispiel hierzu lieferte Netscape, das in alten Version des Navigator Zufallszahlen in Abhängigkeit von der Systemzeit und anderen Informationen des Rechners erzeugte [Wobst97, S. 187]. Mit diesen Informationen wurde die Zahl der möglichen Schlüssel stark reduziert.

Neben Versuchen, den Algorithmus selbst zu knacken oder Schlüssel auszuforschen gibt es Angriffe auf die Kommunikation und den Schlüsselaustausch. So sind Angriffe denkbar, bei denen keine Daten entschlüsselt werden, sondern Daten eingefügt oder Nachrichten wiederholt werden. Der bekannteste Angriff auf den Schlüsselaustausch wird "Mann in der Mitte" (Man in the middle) (-->G) genannt. Dabei gibt sich der Angreifer M gegenüber dem Teilnehmer A als Teilnehmer B aus und umgekehrt. Wenn nun A an B verschlüsselte Daten senden will, schickt A sie tatsächlich an M. Der entschlüsselt die Daten und schickt sie dann an B weiter, wobei er sich als A ausgibt. Durch ein entsprechendes Design der Kommunikation können diese Angriffe unterbunden werden.

In vielen Fällen werden solche Lücken nicht vorsätzlich eingebaut, sondern sind durch Fehler im Entwurf oder der Umsetzung entstanden.

3.6 Recovery

Wenn Daten verschlüsselt gespeichert oder übertragen werden, gibt es zwei Szenarien, die eine Entschlüsselung durch Dritte erforderlich machen können. Es kann der geheime Schlüssel verloren gegangen sein oder es soll (ohne Mitwirkung des Schlüsselinhabers) Dritten ein Zugriff auf die Originaldaten ermöglicht werden. Dritter kann beispielsweise der Arbeitgeber oder eine staatliche Stelle sein.

Um einen Zugang zu den Originaldaten zu ermöglichen, sind verschiedene Lösungen denkbar. Es könnte der geheime Schlüssel bereitgestellt werden, der zur Entschlüsselung benötigt wird (Key-Recovery) (-->G). Die Konsequenz wäre dann, dass auch alle anderen Daten entschlüsselt werden könnten, die mit diesem Schlüssel gesichert wurden oder zukünftig gesichert werden. Bei einer anderen Lösung werden die Daten mit einem zufälligen Schlüssel verschlüsselt. Der Zufallsschlüssel wird dann für jeden potentiellen Zugriffsberechtigten getrennt verschlüsselt und den Daten hinzugefügt. Dadurch können mehrere Benutzer die Originaldaten erhalten, ohne geheime Schlüssel anderer Beteiligter kennen zu müssen (Data-Recovery).

Bei den Überlegungen, welche Lösung sinnvoll sein kann, lassen sich folgende Fälle unterscheiden.

Verschlüsselte Kommunikation
Um Übertragungsfehler zu korrigieren, ist in der Regel kein Zugriff auf Schlüssel nötig, weil die Übertragung wiederholt werden kann. Als Privatperson sollte man in der jetzigen Situation keine Zugriffsmöglichkeit durch Dritte akzeptieren. Das gilt nicht für Arbeitnehmer. Der Arbeitgeber hat das Recht zu wissen, welche Daten in seinem Namen übertragen wurden. Er darf die Daten lesen, die ein Mitarbeiter verschlüsselt hat, soweit dabei die rechtlichen Vorgaben eingehalten werden.

Verschlüsselte Speicherung
Es ergeben sich enorme Risiken für die Verfügbarkeit, wenn auf verschlüsselt gespeicherte Daten nicht mehr zugegriffen werden kann. Daher muss eine Möglichkeit vorgesehen werden, die Originaldaten zu rekonstruieren. Als Privatperson kann man den Schlüssel an einer sicheren Stelle hinterlegen. Im beruflichen Umfeld sollten Regelungen existieren, die eine Rekonstruktion unabhängig von bestimmten Personen erlauben. Es muss aber ein unkontrollierter Zugriff verhindert werden. Dem kann zum Beispiel durch "Data-Recovery" oder das Hinterlegen von Schlüsseln nach einem "Secret Splitting" (Das Geheimnis, mit dessen Kenntnis der Schlüssel rekonstruiert werden kann, wird so auf mehrere Personen oder Institutionen verteilt, dass nur alle zusammen den Schlüssel rekonstruieren können.) oder "Secret Sharing" (Das Geheimnis wird auf mehrere Personen oder Institutionen so verteilt, dass mehrere, die Zahl kann vorgegeben werden, kooperieren müssen, um den Schlüssel rekonstruieren zu können.) Rechnung getragen werden. Auf keinen Fall darf ein Hersteller oder ein anderer Dritter einen Generalschlüssel haben, der es erlaubt auf die Daten zuzugreifen.

Digitale Signatur
Es gibt keinen Grund, einen Signierschlüssel zu hinterlegen oder einer anderen Person zugänglich zu machen. Wenn der Schlüssel verloren geht, können keine Dokumente mehr signiert werden, aber alle bereits signierten Dokumente können weiterhin verifiziert werden. Der einzige Schaden kann darin bestehen, dass bis zum Erhalt des neuen Schlüssels keine Signaturen erfolgen können. Er ist aber nicht vergleichbar mit dem Schaden, der entstehen würde, wenn unberechtigte Personen mit einem hinterlegten Schlüssel statt des Eigentümers Dokumente signieren können.

3.7 Filterung und Virenschutz beim Einsatz von Verschlüsselung

Durch den Einsatz von Verschlüsselungsverfahren kann sich hinsichtlich der Datensicherheit ein Zielkonflikt ergeben. Denn nicht nur die unberechtigte Kenntnisnahme von Inhalts- und Verbindungsdaten wird dadurch unmöglich gemacht, sondern ebenso eine mitunter erwünschte zentrale Kontrolle auf enthaltene Schadensprogramme (Viren etc.) und u.U. auch eine Adress- und Port-

Filterung durch Firewalls (-->G). Inwieweit ein solcher Konflikt besteht, hängt von der eingesetzten Technik wesentlich ab; dies sollte daher im Rahmen eines Einsatzkonzeptes berücksichtigt werden. Grundsätzlich lässt sich das Problem dadurch vermeiden, dass die Verschlüsselung erst jenseits der in Frage stehenden zentralen Komponenten (Firewall, Virenscanner) ansetzt, z.B. durch Einsatz einer Verbindungsverschlüsselung am Übergang zum Internet (-->6.1) oder Corporate Network (-->6.3). Allerdings kann das Problem auch in diesem Szenario durch eine zusätzliche Ende-zu-Ende-Verschlüsselung (-->G) (z.B. im E-Mail-Verkehr oder beim Dateiversand) auftreten.

Da sich die Verschlüsselung in der Regel auf die Inhaltsdaten bezieht, ergeben sich für die Filterung nur dann Probleme, wenn diese auch inhaltliche Teile einbezieht (z.B. Webadressen oder Elemente von Protokollen auf Anwendungsebene). TCP/IP-Adressen und -Ports hingegen sind auch bei verschlüsselten Daten (z.B. beim Einsatz von SSL (-->G)) auswertbar, sofern nicht besondere Tunnelungsverfahren eingesetzt werden, die (etwa bei IPSec (-->G)) die eigentlichen Adressdaten verbergen. In diesem Fall allerdings läuft eine Filterung nahezu vollkommen ins Leere.

Mehr Probleme entstehen für den Fall einer zentralen inhaltlichen Überprüfung. Hier scheitert u.U. bereits die Feststellung, ob z.B. eine verschlüsselte E-Mail Anhänge enthält, die aus Sicht einer Virenkontrolle von Bedeutung sind. Sofern nicht durch eine entsprechende Schlüsselinfrastruktur eine zentrale Entschlüsselungsmöglichkeit (mit all ihren Problemen, (-->3.6)) eröffnet werden soll, ist mit dieser Einschränkung zu leben. Dies bedeutet, dass neben einer zentralen auch eine dezentrale Virenkontrolle (die sich auch aus anderen Gründen empfiehlt) erfolgen muss. Der Versuch, den Zielkonflikt dadurch zu vermeiden, dass die Verschlüsselung unterdrückt wird (z.B. durch Nichtweiterleitung eingehender verschlüsselter E-Mails), ist aus Sicht des Datenschutzes jedenfalls keine sinnvolle Lösung.

3.8 Verschlüsselung durch Auftragnehmer

Während die Verschlüsselung typischerweise eingesetzt wird, um Dritte von der Kenntnisnahme und der Manipulation von Daten auszuschließen, ist gleichwohl eine Übertragung der Kryptografie auf einen Dienstleister denkbar. Insbesondere im Zusammenhang mit der Bereitstellung von Netzwerkdiensten bietet sich als zusätzlicher Dienst die kryptografisch gesicherte Übertragung an.
Typischer Fall einer solchen Konstruktion wäre die Bereitstellung eines VPN (Virtuellen Privaten Netzwerks, (-->6.3)) durch einen Provider, mit dessen Hilfe verteilte Standorte über offene Netze wie das Internet sicher miteinander verbunden werden können.

Da der Sicherheits-Dienstleister bei einer solchen Konstruktion prinzipiell über die Möglichkeit verfügt, die Daten im Klartext zur Kenntnis zu nehmen, muss diesem ausreichendes Vertrauen entgegengebracht werden, und die Dienstleistungsverträge sind so zu gestalten, dass ein Missbrauch weitgehend ausgeschlossen ist.

Eine solche Verschlüsselungsinfrastruktur kann zudem als Grundschutz eingesetzt werden, um ein ausreichendes Schutzniveau bei der Übermittlung nicht sensibler Daten zu gewährleisten. Die im Einzelfall übertragenen sensiblen Daten können dann mit zusätzlichen Verschlüsselungsverfahren, ggf. anwendungsbezogen, auch gegen eine Kenntnisnahme durch den Provider geschützt werden.

3.9 Kryptokontroverse und Exportkontrolle

Seit einigen Jahren gibt es immer wieder Bestrebungen, den Einsatz von Verschlüsselungssystem zu reglementieren, weil die Verfahren immer schwerer zu brechen sind. Dabei wird auf kriminelle Organisationen verwiesen, die sich durch Verschlüsselung einer staatlichen Überwachung entziehen können. Die Diskussion, inwieweit ein Zugriff staatlicher Stellen auf eine verschlüsselte Kommunikation zulässig und sinnvoll ist, ist als Kryptokontroverse bekannt.

Befürworter einer Überwachung schlagen als technische Lösung Key-Recovery-Systeme vor, wie sie erstmals als Reaktion auf die Clipper-Initiative der US-Regierung 1993 öffentlich diskutiert wurden. Demgegenüber weisen Gegner darauf hin, dass es Möglichkeiten gibt, sich der Überwachung

zu entziehen. Außerdem halten sie die vorgeschlagenen Systeme für unbeherrschbar, sowohl vom Betrieb her, als auch hinsichtlich der Gefahren für die Bürger [Abelson98]. Die Datenschutzbeauftragten teilen die Vorbehalte. In ihrem Eckpunktepapier zur Kryptopolitik vom 2. Juni 1999 hat die Bundesregierung einen vorläufigen Schlussstrich gezogen. Sie stellt fest, dass solche Eingriffe zur Zeit nicht geplant sind. Abhängig von zukünftigen Erfahrungen behält man sich jedoch vor, diese Aussage zu revidieren.

Mit dem Ziel, starke Verschlüsselungsverfahren nur kontrolliert zu verbreiten, haben praktisch alle Staaten Regelungen zum Export und Import getroffen ([Beucher/Schmoll99], [Roth98]) Am bekanntesten sind die Exportrestriktionen der USA, weil sie wegen der Dominanz amerikanischer Software die größten Auswirkungen haben. Die Beschränkungen waren früher sehr restriktiv und führen teilweise noch immer dazu, dass exportierte Produkte nur unzureichende Verschlüsselungsmöglichkeiten bieten (vgl. 3.5). Inzwischen sind die Restriktionen deutlich gelockert, so dass heute aus diesem Grund bei keinem Hersteller bzw. Produkt auf eine starke Verschlüsselung verzichtet werden muss.

Abschnitt 4

Grundszenarien der Nutzung der Informationstechnik im Zusammenhang mit ihrer Absicherung mit kryptografischen Verfahren

Die Verwendung kryptografischer Verfahren deckt einen erheblichen Teil der Maßnahmen ab, die zur Eindämmung der Risiken für die informationstechnische Sicherheit herangezogen werden. Die Kryptografie in all ihren Anwendungsformen ist in so weit als eine der „Grundtechniken" für die IT-Sicherheit anzusehen. Sie dient vor allem der Abwehr von Bedrohungen der Vertraulichkeit und der Integrität bei der Speicherung und Übertragung von Daten sowie der Authentizität von Dateien (speziell: Dokumenten) beim bi- oder multilateralen Austausch in offenen Kommunikationsnetzen (speziell: Internet). Die Lösungen im Einzelfall sind stark abhängig von den Anwendungen und technischen Rahmenbedingungen, unter denen Sicherheitsanforderungen erfüllt werden sollen. In den Abschnitten 6 und 7 werden daher solche Einzelfallszenarien näher behandelt.

Grundsätzlich ergeben sich jedoch kryptografische Lösungen für Probleme der informationstechnischen Sicherheit in drei Grundsituationen: Bei der Speicherung schutzbedürftiger Daten in elektronischen Speichermedien zum Schutz vor Kenntnisnahme bei unbefugtem Zugriff, bei der Übertragung schutzbedürftiger Daten auf Übertragungsmedien (Leitungen, Funk) zum Schutz vor unbefugter Kenntnisnahme und Verfälschung sowie zum Nachweis der authentischen Herkunft empfangener Daten, vor allem Dokumente.

4.1 Die Verschlüsselung bei der Speicherung von Daten

4.1.1 Verschlüsselung für die Zugriffskontrolle

Nach Nr. 3 der Anlage zu § 9 Satz 1 Bundesdatenschutzgesetz und gleich oder ähnlich lautenden Vorschriften der Landesdatenschutzgesetze ist zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle).

Es geht also u.a. darum, organisatorisch festgelegte differenzierte Zugriffsprofile möglichst genau so differenziert in Zugriffsrechte auf die Dateien und Programme umzusetzen. Für diese Realisierung stehen unterschiedliche Verfahrensweisen zur Verfügung, eine von ihnen ist die Verschlüsselung der zugriffsbeschränkten Dateien auf dem Speicher. Die Zugriffsberechtigung auf eine Datei wird dann durch die Kenntnis des zum Entschlüsseln erforderlichen Schlüssels vergeben.

In der Praxis spielt die Zugriffsdifferenzierung durch Verschlüsselung jedoch nur eine untergeordnete Rolle, weil die anderen Umsetzungsmöglichkeiten an Wirksamkeit oft nicht nachstehen, aber leichter zu realisieren sind.

Vor allem dann, wenn aufgrund der Sensibilität der Daten oder der besonderen Einsatzbedingungen der IT-Systeme mit anderen Maßnahmen den Risiken bei der Gewährleistung der Vertraulichkeit und Integrität nicht hinreichend entgegen gewirkt werden kann, kommt auch die kryptografische Verschlüsselung des Speicherinhalts oder einzelner Dateien als Maßnahme in Frage.

Dabei geht es sowohl um die Abschottung sensibler Daten gegen den unbefugten Zugriff Außenstehender als auch um den Schutz schutzwürdiger Dateien vor dem Zugriff anderer Systemnutzer:

- Die IT-Einheit (Rechner, externes Speichermedium) kann vollständig oder längerfristig/endgültig in die Hände Unbefugter geraten (z.B. durch Diebstahl, Einbruchdiebstahl, Verlust).

Ein solches Risiko muss für tragbare Systeme (Laptops, Notebooks, Organizer etc.) grundsätzlich als gegeben angesehen werden. In diesem Falle ist die Speicherverschlüsselung schutzbedürftiger Daten daher obligatorisch.

Aber auch dann, wenn für nicht tragbare Systeme aufgrund deren Abmessungen und geringem Einbruchsschutz die Entwendung solcher Systeme nicht ausgeschlossen werden kann, ist die Speicherverschlüsselung zu empfehlen.

Man beachte in diesem Zusammenhang speziell die Ausführungen unter 7.8 (Mobile Geräte und Datenträger).

- Privilegierte Benutzer (Systemverwalter, Wartungspersonal, Administratoren verschiedener Art) erhalten lesenden und ändernden Zugriff auf sensible Datenbestände.

  Wenn es wegen der Sensibilität der Daten also nicht ausreicht, auf die vorauszusetzende besondere Vertrauenswürdigkeit der privilegierten Benutzer zu bauen, ist die kryptografische Verschlüsselung vorzusehen. Dabei ist selbstverständlich darauf zu achten, dass die privilegierten Benutzer auch keinen Zugriff auf die verwendeten Schlüssel haben dürfen.

  Man beachte in diesem Zusammenhang die Ausführungen unter 7.1 (Abschottung der Systemadministration) und 7.7 (Fernwartung).

- Bei der Datenverarbeitung im Auftrag (Outsourcing) erhalten Mitarbeiter des Auftragnehmers lesenden und ändernden Zugriff auf Datenbestände, für die ein Offenbarungsverbot besteht (z.B. medizinische Daten).

  Die Regelungen der Datenschutzgesetze für die Datenverarbeitung im Auftrag setzen zwar formaljuristische Schranken für den Umgang des Auftraggebers mit den bereitgestellten Daten. In besonderen Fällen ist es jedoch opportun, den Auftragnehmer an der Kenntnisnahme der Daten zu hindern. Dies gilt vor allem dann, wenn die Verhinderung einer Offenbarung der Daten gegenüber Dritten als höheres Rechtsgut anzusehen ist. Dies gilt etwa für patientenbezogene medizinische Daten, die dem Arztgeheimnis unterliegen.

  Auch in solchen Fällen ist der Einsatz der Speicherverschlüsselung vorzusehen.

  Man beachte in diesem Zusammenhang die Ausführungen unter 7.6 (Externe Archivierung) und 7.9 (Outsourcing)

4.1.2 Verschlüsselung für die Weitergabekontrolle beim Datenträgeraustausch

Nach Nr. 4 der Anlage zu § 9 Satz 1 Bundesdatenschutzgesetz und gleich oder ähnlich lautenden Vorschriften der Landesdatenschutzgesetze ist u.a. zu gewährleisten, dass personenbezogene Daten während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Aspekte der Weitergabekontrolle).

Erfolgt der Transport mittels elektronischen Datenträgern (z.B. Disketten, Bandkassetten, Bänder, CD-ROM, DVD etc.), so stellt die kryptografische Verschlüsselung der Daten auf diesen Datenträgern den effizientesten Weg dar, die Weitergabekontrolle beim Transport zu realisieren, weil es dann auf die weiteren Umstände des Transports nicht mehr ankommt. Hohe Kosten und organisatorische Aufwände für den sicheren Versand können dann entfallen.

In diesem Zusammenhang wird besonders auf die Ausführungen unter 7.8 (Mobile Geräte und Datenträger) verwiesen.

4.1.3 Merkmale für das Verschlüsselungsverfahren bei der Speicherverschlüsselung

Abgesehen von der Verschlüsselung beim Transport elektronischer Datenträger, die zur Umsetzung der Weitergabekontrolle nach Nr. 4 der Anlage zu § 9 Satz 1 BDSG geboten ist und bei der der rechtmäßige Empfänger über einen anderen und sicheren Kanal den Schlüssel zum Entschlüsseln der Daten erhalten muss, entfallen bei der Speicherverschlüsselung die Probleme der Schlüsselverteilung. Die Ver- und Entschlüsselung kann durch die gleichen Personen erfolgen.

Dies hat folgende Konsequenzen:

- Für die Speicherverschlüsselung reicht der Einsatz symmetrischer Verschlüsselungsverfahren (-->G) aus. Die Stärke des Verfahrens, gemessen an der Schlüssellänge, ist vom Schutzbedarf abhängig. Die Aussage gilt auch für den Transport von Datenträgern, denn die Kommunikationsbeziehung ist dabei bilateral mit feststehendem Partner. Der Schlüsselaustausch kann daher einfach vollzogen werden.

- Wenn die verschlüsselten Daten entschlüsselt werden müssen, ohne dass die Schlüsselinhaber daran mitwirken können, müssen organisatorische und/oder technische Maßnahmen für eine Wiedererlangung des Schlüssels (Key Recovery) (-->G) getroffen werden. Dabei können je nach Bedarf einfache organisatorische Maßnahmen (Bekanntgabe des Schlüssels an Vertreter, gesicherte schriftliche Hinterlegung) oder aufwendige technische Lösungen (z.B. automatische Hinterlegung der Session Keys (-->G) in einem organisationsinternen Trust Center (-->G)) gefunden werden.

4.2 Die Verschlüsselung bei der Übertragung von Daten

Verschlüsselung für die Transportkontrolle bei der Datenübertragung

Nach Nr. 4 der Anlage zu § 9 Abs. 1 Bundesdatenschutzgesetz ist außerdem (siehe 4.1.2 - Verschlüsselung für die Weitergabe beim Datenträgeraustausch) zu verhindern, dass bei der elektronischen Übertragung personenbezogener Daten diese u.a. nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Diese Anforderungen stellen sich unabhängig vom Übertragungsmedium (Kupfer- oder Glasfaserkabel, Funk) oder Übertragungsart (Interaktion, File Transfer). Daher sind hier nur Maßnahmen sinnvoll, die davon unabhängig sind und am Zustand der Daten selbst ansetzen:

Die kryptografische Verschlüsselung ist daher die einzige sinnvolle Maßnahme zur Umsetzung der gesetzlich gebotenen Transportkontrolle auf Übertragungswegen, weil sie von Überlegungen zur Sicherung der Übertragungswege entbindet.

Eine Verschlüsselung hat auf allen Übertragungswegen zu erfolgen, die von Abhörangriffen bedroht werden können. Ob eine Ende-zu-Ende-Verschlüsselung (-->G) von Client zu Client erforderlich ist oder ob Server-zu-Server-Verschlüsselung ausreicht, muss den Risikobetrachtungen für die Client-Server-Verbindungen überlassen bleiben. Da speziell die Netzübergänge zwischen lokalen und nicht-lokalen Netzen bzw. die Übertragungsstrecken zwischen Netzabschluss und dem ersten Netzknoten des öffentlichen Netzes abhörgefährdet sind, genügt die Verschlüsselung zwischen dem ersten und dem letzte Netzknoten im öffentlichen Netz nicht.

Geeignete Verschlüsselungsverfahren sind symmetrische Verfahren oder hybride Verfahren, bei denen die Wirkdaten symmetrisch und der dabei verwendete Sitzungsschlüssel asymmetrisch verschlüsselt übertragen wird.

Symmetrische Verfahren (-->G) eignen sich bei Übertragungen in kleinen geschlossenen Benutzergruppen, die auf anderen sicheren Kanälen Schlüssel vereinbaren können. Meist gilt dies auch für File-Transfers, da diese in der Regel in einem vorgegebenen organisatorischen Rahmen erfolgen. Bei größeren Gruppen steigt die Gefahr, dass der Schlüssel unbemerkt entwendet oder widerrechtlich weitergegeben wird. Außerdem steigt der Aufwand zu Schlüsselerneuerung bei einem kompromittierten Schlüssel stark an.

Asymmetrische Verfahren (-->G) sind jedoch erforderlich, wenn ein Austausch von Schlüsseln auf sicheren Kanälen nicht möglich ist, also bei der Kommunikation zwischen beliebigen Kommunikationspartnern in öffentlichen Kommunikationsnetzen.

Anstelle von rein asymmetrischen Verfahren, die wegen des extremen Rechenaufwandes zu Performanzproblemen bei den beteiligten Systemen führen würden, werden allerdings hybride (-->G) Produkte eingesetzt (z.B. PGP, (-->G)), die jedoch nach außen wie asymmetrische Verfahren funktionieren. Wichtigstes Beispiel ist dabei der E-Mail-Verkehr auf dem Internet (siehe 7.5 E-Mail).

4.3 Die Verschlüsselung für Zwecke der Authentisierung

Im Zusammenhang mit dem technisch-organisatorischen Datenschutz und der informationstechnischen Sicherheit kommt es in verschiedenen Zusammenhängen darauf an, dass zwei oder mehrere miteinander kommunizierende Menschen und/oder technische Systeme sich gegenseitig den Beweis liefern müssen, dass sie jene sind, die tatsächlich miteinander kommunizieren wollen oder sollen. Neben der Authentisierung von Mensch zu Mensch (z.B. bei der Zutrittskontrolle durch Pförtner) oder des Menschen gegenüber dem technischen System (z.B. zur Zugangs- und Zugriffskontrolle), die durch Authentisierung mittels Besitz (z.B. eines. maschinenlesbaren Ausweises) oder Wissen (z.B. Passwort, PIN) erfolgen, besteht Authentisierungsbedarf

- zwischen zwei technischen Systemen untereinander durch eine Challenge Response-Verfahren (-->5.3),

- zwischen einem Benutzer und einem technischen System, welches aus der Ferne über ein Netz erreicht werden soll, durch eine Variante des Challenge Response-Verfahrens,

- des rechtmäßigen Absenders von elektronisch übertragenen Daten (vor allem als Dokumente) gegenüber dem Empfänger durch die digitale Unterschrift (-->5.2).

Im Unterschied zur Speicherverschlüsselung muss bei der elektronischen Signatur ein Key Recovery (-->G) ausgeschlossen sein, da es hier um den Nachweis einer Identität geht und dieser kompromittiert werden kann, wenn anderen der private Schlüssel bekannt wird.

Abschnitt 5

Allgemeine Lösungsansätze

5.1 Tunneling

Der häufigste Lösungsansatz für die Bildung kryptografiebasierter Corporate Networks (--> 6.3) besteht darin, den Datenstrom zwischen den einzelnen Niederlassungen oder Teilnehmer zu "tunneln". Die Datenpakete der eigentlichen Kommunikation werden hierzu kryptografisch verpackt und mit einem zusätzlichen Header versehen. Die Adressierung innerhalb des logischen Unternehmensnetzes oder das intern verwendete Übertragungsprotokoll spielen dabei keine Rolle. Auf diese Weise ist es möglich, lokale Netze zu koppeln, ohne dass Inhalt und Endteilnehmer der Kommunikation auf den WAN-Verbindungen erkennbar sind.

Das Tunneling erfolgt in der Regel transparent für die Benutzer, d.h. das Aushandeln der kryptografischen Algorithmen (-->G), das Ver- und Entpacken der Datenpakete sowie die Verschlüsselung werden von entsprechenden Komponenten selbständig übernommen. Die Teilnehmer des Corporate Networks arbeiten, als ob sie an einem einheitlichen Netz angeschlossen wären. Neben der Verschlüsselung zur Wahrung der Vertraulichkeit werden im Rahmen des Tunnelings meist auch kryptografische Mechanismen zur Authentisierung der Komponenten (Tunnel-Inititiator, Tunnel-Switch/Tunnel-Terminator) oder zur Integritätssicherung (Hashwerte (-->G)) verwendet.

Je nach Art der beteiligten Stellen können folgende Lösungen unterschieden werden:

Site-to-Site Tunneling

Hier wird der Tunnel lediglich zwischen den beteiligten Gateways (z.B. Router(-->G)) gebildet. Die erforderliche Hard- und Software ist nur an den WAN-Übergängen - vor dem Zugangsrouter des Providers - erforderlich.

End-to-Site Tunneling

In diesem Fall wird der Tunnel zwischen einer Arbeitsstation und dem Tunnel-Gateway des Zielnetzes gebildet. Diese Lösung dient meist dazu, mobile Außendienstmitarbeiter (-->7.8) oder Tele- bzw. Heimarbeitsplätze (-->7.10) anzubinden. Die erforderliche Hard- und Software muss dabei sowohl an der Arbeitsstation (DFÜ-Karte) als auch am Tunnel-Server des Zielnetzes (Router) vorhanden sein.

Ende-to-End Tunneling

Hierbei wird der Tunnel über die komplette Strecke zwischen den beteiligten Arbeitsstationen aufgebaut. Beide müssen damit über die erforderlichen Komponenten verfügen. Diese Lösung kommt vor allem dann in Betracht, wenn die gewünschte Sicherheit auch innerhalb des jeweiligen lokalen Netze (-->6.4) benötigt wird. Werden innerhalb eines Netzes mehrere End-to-End-Tunnel betrieben, reicht meist ein sog. Tunnel-Switch die Verbindungen zum jeweiligen Endgerät weiter.

Die für das Tunneling verwendeten Protokolle sind in der Regel auf den Schichten 2 und 3 des OSI-Refernzmodells angesiedelt. Für die Protokolle gibt es verschiedene Modelle und Industriestandards, wie z.B. GRE (-->G), Ipsec (-->G), PPTP (-->G), L2TP (-->G).

Die genannten Protokolle werden in vielen Fällen von den Netzwerkkomponenten gängiger Hersteller unterstützt. Entsprechende Client-Software ist häufig bereits in den Betriebssystemen enthalten. Je nach Anforderung sollte darauf geachtet werden, dass die verwendeten kryptografischen Algorithmen und Schlüssellängen den Empfehlungen der Datenschutzbeauftragten entsprechen.

5.2 Elektronische Signaturen (digitale Signaturen)

Der wichtigste Anwendungsbereich kryptografischer Verfahren ist neben der Verschlüsselung die elektronische oder digitale Signatur. Eine digitale Signatur kann die handschriftliche Unterschrift unter einer E-Mail (-->7.5), unter einem Antrag bei der Behörde oder unter einem Vertragsentwurf ersetzen. Sie kann auch zum Signieren von Zertifikaten (-->G) genutzt werden und Warenbestellungen oder Bezahlvorgänge mit elektronischem Geld absichern (-->7.3, 7.4).

Die bisher im Rechts- und Geschäftsverkehr bekannten digitalen Signaturen sind im technologieoffenen Begriff "elektronische Signatur" (-->G) integriert. Nach dem Signaturgesetz (SigG) (-->G) wird zwischen elektronischen Signaturen, fortgeschrittenen und qualifizierten elektronischen Signaturen unterschieden.

Einfache elektronische Signaturen sind elektronische Daten, die elektronischen Dokumenten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentisierung des Unterzeichners dienen. Als elektronische Signatur gilt bereits das Anfügen eines Namens oder einer eingescannten Unterschrift unter ein elektronisches Dokument. Allerdings ist damit keine Sicherheit gegeben, weil diese "Unterschrift" beliebig oft kopiert und unter andere Dokumente gesetzt werden kann.

Eine fortgeschrittene elektronische Signatur (z. B. bei der Nutzung von PGP (-->G)) kann die Identität des Unterzeichners bestätigen und außerdem prüfen, ob die Daten nachträglich verändert wurden.

Die gesetzlichen Anforderungen an die Schriftform erfüllt jedoch nur die qualifizierte elektronische Signatur. Sie muss gegenüber der fortgeschrittenen elektronischen Signatur zusätzlich auf einem gültigen qualifizierten Zertifikat (-->G) beruhen und gesetzlich festgelegten Sicherheitsanforderungen genügen. Sie ist der handschriftlichen Unterschrift gleichgestellt. Die Rahmenbedingungen für ihren Einsatz und die Pflichten der Zertifizierungsdiensteanbieter regelt das Signaturgesetz (-->G). Beim Einsatz qualifizierter elektronischer Signaturen für öffentlich-rechtliche Verwaltungstätigkeit können Rechtsvorschriften zusätzliche Anforderungen anordnen.

Im allgemeinen ist die Verwendung aller elektronischer Signaturen freigestellt, soweit nicht durch Rechtsvorschriften etwas anderes vorgeschrieben ist.

Kryptografisch basieren fortgeschrittene und qualifizierte elektronische Signaturen auf asymmetrischen Verschlüsselungsverfahren (-->4.2) (-->G) und Hash-Funktionen (-->G).

Beim Signieren wird ein Hashwert (-->G) wie ein "digitaler Fingerabdruck" für die elektronischen Daten (z. B. Dokumente) berechnet. Dieser wird mit dem Signaturschlüssel (privater Schlüsseln des Unterzeichners) verschlüsselt und den elektronischen Daten hinzugefügt. Eine Hash-Funktion berechnet für ein Dokument immer den gleichen Hashwert (Prüfsumme), solange der Inhalt des Dokuments nicht verändert wird.

Beim Prüfen wird die Signatur (verschlüsselter Hashwert) mit dem Signaturprüfschlüssel (öffentlicher Schlüssel des Unterzeichners) entschlüsselt. Zugleich wird ein aktueller Hashwert für die elektronischen Daten berechnet, der mit dem entschlüsselten Hashwert verglichen wird. Bei Gleichheit wird bestätigt, dass die elektronischen Daten nachträglich nicht verändert wurden und dass die signierten Daten vom Unterzeicher stammen. Bei Ungleichheit wird die Signatur als ungültig abgelehnt.

Zur Sicherheit des Signatur- bzw. Prüfverfahrens ist der Signaturprüfschlüssel durch eine vertrauenswürdige Stelle (Zertifizierungsdiensteanbieter) mit einem elektronischen Zertifikat einer Person zuzuordnen. Außerdem ist der Signaturschlüssel, der z. B. auf einer Chipkarte gespeichert ist, geheim zu halten und vor unbefugter Nutzung zu schützen. Die Anwendungskomponenten (z. B. Spezialsoftware), die zur Erzeugung bzw. Prüfung elektronischer Signaturen eingesetzt werden, dürfen nur auf vertrauenswürdigen IT-Systemen betrieben werden. Geeignete Kryptoalgorithmen werden im

Bundesanzeiger mindestens für die kommenden sechs Jahre veröffentlicht, gegebenenfalls aktualisiert und ergänzt.

5.3 Challenge Response-Verfahren

In vielen Anwendungszusammenhängen ist es für die informationstechnische Sicherheit bedeutsam, dass zwei technische Systeme sich gegenseitig oder nur einseitig die Berechtigung beweisen, miteinander in Interaktion treten zu dürfen (Maschine-Maschine-Authentisierung).

Ein herausragendes Beispiel ist dabei die gegenseitige Authentisierung von Chipkarten und chipkartenbasierten Dienstleistungssystemen (CDLS). Der Betreiber des CDLS will dabei sicherstellen, dass nur die Inhaber berechtigter Chipkarten die Dienstleistungen in Anspruch nehmen können. Umgekehrt will der Besitzer einer Chipkarte sicherstellen, dass das CDLS nicht ohne die versprochene Gegenleistung die dafür erforderlichen Daten aus der Karte herausliest.

Ein gängiges Verfahren ist dabei das Challenge Response-Verfahren (-->G), welches der Einfachheit halber hier nur einseitig und vom Prinzip her beschrieben werden soll:

Wenn zwei Systeme im Rahmen eines Dienstleistungs- oder Anwendungsverfahrens miteinander interagieren sollen, dann müssen sie über einen gemeinsamen Systemschlüssel verfügen. Das authentisierende System generiert eine Zufallszahlenfolge, überträgt diese an das zu authentisierende System. Dann verschlüsseln beide Systeme unabhängig voneinander diese Zahlenfolge mit dem gleichen, in der Regel symmetrischen Verschlüsselungsverfahren, z. B. DES (-->G). Das zu authentisierende System überträgt sein Ergebnis an das authentisierende System. Dieses vergleicht das übertragene mit dem eigenen Ergebnis und stellt bei Gleichheit das Gelingen der Authentisierung fest.

Eine Variante des Challenge Response-Verfahrens dient der Authentisierung eines menschlichen Benutzers gegenüber einem informationstechnischen System, welches über ein unsicheres Netz (z.B. Internet) erreicht werden soll, ohne dass ein Passwort über das Netz geschickt werden muss.

Dabei verwendet der Benutzer ein ihm zur Verfügung stehendes IT-System, dem gegenüber er sich auf übliche Weise (oder gar nicht) authentifiziert. In dieses IT-System gibt er seine Benutzerkennung für das entfernte System und ein (u.U. weiteres) Passwort ein. Sein System führt eine Einwegverschlüsselung dieses Passworts durch und überträgt die Benutzerkennung zum entfernten System.

Dieses stößt dann eine Challenge Response-Authentisierung mit dem Benutzer-System an, wobei zur Verschlüsselung der Zufallszahlenfolge das Einweg-Chiffrat (-->G) des vom Benutzer eingegebenen Passworts als Schlüssel verwendet wird.

5.4 Leitungs- und Ende-zu-Ende-Verschlüsselung

Kryptografischer Schutz kann in Form einer Verbindungs- oder einer Ende-zu-Ende-Verschlüsselung realisiert werden:

Eine Verbindungsverschlüsselung wird durch solche Verfahren realisiert, die den Datenstrom nur zwischen bestimmten Netzknoten chiffrieren - ungeachtet der an einer Kommunikation beteiligten Endgeräte. Ende-zu-Ende-Verschlüsselungen dagegen schützen die Daten auf der gesamten Strecke zwischen Absender und Empfänger.

Dabei wird die Verbindungsverschlüsselung auf den unteren Schichten des OSI-Referenzmodells (Schicht 1-4), die Ende-zu-Ende-Verschlüsselung auf den oberen Schichten (Schicht 3-7) realisiert.

Der Vorteil der Verschlüsselung auf unteren Netzwerkschichten liegt darin, dass der bereitgestellte Schutz für sämtliche darüber liegenden Dienste und Anwendungen wirkt und somit Anforderungen einer Verschlüsselungsinfrastruktur erfüllt. Allerdings liegen die Daten in Vermittlungsstationen entsprechend höherer Schichten dann unverschlüsselt vor, was – je nach administrativer Kontrolle über diese Stationen – unerwünscht sein kann.

Die Verschlüsselung auf höheren Schichten vermeidet diese Unterbrechungen im kryptografischen Schutz, setzt jedoch die Einbindung von Verschlüsselungsfunktionalität in jeden Dienst bzw. jede Anwendung voraus, mit der schützenswerte Daten übermittelt werden. Die Verschlüsselung rückt damit auch näher zum Benutzer, was Vorteile (z.B. Möglichkeit persönlicher Schlüssel) und Nachteile (z.B. zusätzlicher Aufwand) mit sich bringt.

5.5 Kryptoboxen

Bei dem Austausch von hochsensiblen Informationen, beispielsweise personenbezogenen Daten gemäß § 3 Abs. 9 BDSG, reicht die Sicherheit einer digitalen Telefonleitung für Sprach- und Datenkommunikation nicht aus. Hier können nur kryptografische Verschlüsselungssysteme den Sicherheits- und Datenschutzanforderungen gerecht werden.

Zur Bereitstellung eines sicheren Übertragungsweges wurden Komponenten entwickelt, die zwischen das öffentliche Telefonnetz und Telefon bzw. Rechner geschaltet werden. Diese Verschlüsselungskomponente kann je nach Anwendung und Bauart z.B. direkt in einen Rechner eingebaut oder als separate Komponente in das Netz integriert werden. Besonders kleine Verschlüsselungseinheiten eignen sich sogar für den mobilen Einsatz z.B. zum Einbau in Notebooks oder zur Nutzung in Verbindung mit einem Notebook.

Die Verschlüsselungskomponente arbeitet wie ein gesicherter Zugang (Security Gateway) , indem sie Datenpakete (IP Pakete) verschlüsselt sendet bzw. ankommende Datenpakete entschlüsselt. Die derzeit eingesetzten Komponenten arbeiten mit dem DES (-->G) oder Triple DES (-->G) Verschlüsselungs-Algorithmus; Komponenten der neueren Generation z.T. schon mit dem Advanced Encryption Standard (AES (-->G)).

Einsatzbereich dieser Einheiten ist neben der Verschlüsselung der Sprache (Telefon) die Datenkommunikation in Netzwerken, insbesondere bei der Absicherung von IT-Systemen, die über ein Wide Area Network kommunizieren.

Für den Einsatzbereich in der öffentlichen Verwaltung hat das Bundesamtes für Sicherheit in der Informationstechnik (BSI) Geräte entwickeln lassen, die bis zur Vertraulichkeitsstufe "Geheim" zugelassen sind. Hier sei das ELCRODAT 6-2 (-->G) beispielhaft genannt.

5.6 Verschlüsselungskomponenten von Standardsoftware

Eine Reihe von Software-Produkten für die Bürokommunikation (Textverarbeitung, Tabellenkalkulation etc.) und für das Dateimanagement (Archivierung etc.) enthält Funktionen, mit denen Daten verschlüsselt abgelegt werden können. Hierbei handelt es sich häufig um eigene Verfahren des jeweiligen Herstellers, die nur von den entsprechenden Programmen selbst beherrscht werden. Zudem ist die Dokumentation über die benutzten Algorithmen und die Qualität der Verschlüsselung vielfach wenig aussagekräftig.

Viele dieser Schutzmaßnahmen genügen nicht den Anforderungen, die aus datenschutzrechtlicher Sicht zum Schutz der Vertraulichkeit zu stellen sind. Insbesondere die Überwindungssicherheit ist häufig mangelhaft, wie entsprechende "Knackprogramme", die aus dem Internet bezogen werden können, belegen. Verschlüsselungskomponenten in Standardsoftware zielen insofern eher auf den Schutz vor zufälliger Kenntnisnahme Dritter, was aus Datenschutzsicht regelmäßig nicht ausreicht.

Sofern es sich allerdings bei solchen Verschlüsselungskomponenten um die Implementation bekannt hochwertiger Standards handelt, ist gegen deren Verwendung nichts einzuwenden. Es sollte jedoch beachtet werden, dass die Verschlüsselung jeweils nur auf Dateiebene wirkt, und der Schutz bei der Verwendung in Netzwerken daher eingeschränkt sein kann.

Abschnitt 6

Szenarien – Infrastrukturen

6.1 Internet

Situationsbeschreibung	Das Internet hat sich in den letzten Jahren zum wichtigsten Kommunikationsmedium entwickelt. Bei vielen wächst daher der Wunsch, dem Internet auch sensible persönliche oder geschäftliche Angaben anzuvertrauen, um etwa per E-Mail (--> 7.5) mit Partnern weltweit zu korrespondieren oder elektronische Angebote des World Wide Web in Anspruch zu nehmen.
Auftretende IT-Sicherheitsprobleme	Mit der Nutzung des Internet sind jedoch erhebliche Gefährdungen für die Vertraulichkeit, die Integrität und die Zurechenbarkeit der Daten verbunden: - Im Internet werden Daten grundsätzlich unverschlüsselt im Klartext übertragen. Sie können daher von Personen mitgelesen oder verändert werden, für die die Daten gar nicht bestimmt sind. - Die Kommunikation eines berechtigten Nutzers lässt sich mitschneiden und später wieder einspielen (sog. Replay Attack (--> G)). Dadurch kann sich der Angreifer bei vielen Diensten die Rechte des berechtigten Nutzers verschaffen, indem er zur Authentisierung eines berechtigten Nutzers benutzte Daten, wie dessen Benutzerkennung und Passwort, die sogar verschlüsselt sein können, zu einem späteren Zeitpunkt wieder einspielt. - Der Empfänger hat nicht die Gewähr, dass die Daten wirklich von dem angegebenen Absender stammen und nicht etwa von jemandem, der sich als dieser Absender ausgibt. So lässt sich etwa elektronische Post auch unter einer falschen Absenderangabe versenden.
Lösungswege unter Anwendung kryptografischer Verfahren	Den genannten Risiken lässt sich durch Einsatz kryptografischer Verfahren wirksam begegnen. Personenbezogene Daten sollten generell nur verschlüsselt und digital signiert über das Internet übertragen werden. Welche Sicherheitslösung einzusetzen ist, richtet sich nach der vorgesehenen Art der Nutzung: **Elektronische Post** Es existieren zahlreiche marktgerechte Lösungen, die ermöglichen, E-Mails verschlüsselt und digital signiert zu übertragen (-->7.5). Im Internet kommt PGP (--> G) und S/MIME (--> G) besondere Bedeutung zu. **Interaktive Dienste** Auch für interaktive Internet-Dienste wie World Wide Web (WWW),

	FTP oder Telnet sind kryptografische Lösungen verfügbar. Am meisten wird das SSL-Verfahren (--> G) eingesetzt. Weitere Verfahren sind S-HTTP ((--> G)) und SSH ((--> G)).

6.2 Landesnetze

Situationsbeschreibung	In den letzten Jahren wurden in den verschiedenen Bundesländern die einzelnen verfahrensspezifischen Kommunikationsinfrastrukturen immer mehr zusammengefasst und sog. Landesnetze gebildet. Ausschlaggebend hierfür war u.a. der Durchbruch des Internet und die damit verbundene kostengünstige Übertragung der Internet-Technologie auf kleinere örtlich begrenzte Bereiche, den Intranets. Auch wenn nicht von einem Landesnetz oder einem Metropolitan Area Network (MAN) ausgegangen werden soll, sondern es nur um die Anbindung von Außenstellen oder anderen Behörden (-->7.2), geht, sind die folgenden Ausführungen relevant.
Auftretende IT-Sicherheitsprobleme	Auch wenn man davon ausgeht, dass nur öffentliche Stellen eines Landes an ein Landesnetz angeschlossen sind, muss wegen der Nutzung der Internet-Technologie, der großen Anzahl angeschlossener Stellen und berechtigter Benutzer sowie wegen der meist erfolgenden Anbindung an das Internet prinzipiell von den gleichen Gefahren und Risiken wie im Internet ausgegangen werden. Die Kommunikationsleitungen sind entweder im Landesbesitz und oftmals in für Angreifer zugänglichen Trassen und Wegen verlegt oder es handelt sich um bei kommerziellen Telekommunikationsanbietern angemietete Leitungen. Im letzten Falle kann der Zugriff von Mitarbeitern der Anbieter nicht ausgeschlossen werden. Aber auch innerhalb eines Landesnetzes muss durch geeignete technisch-organisatorische Maßnahmen sichergestellt werden, dass die informationelle Gewaltenteilung eingehalten werden kann. Eine Landesverwaltung darf nicht als informatorisches Ganzes betrachtet werden. Daher besteht unabhängig von möglicherweise von außen drohenden Gefahren die Notwendigkeit, schutzbedürftige Daten während der Übertragung vor unbefugter, auch unabsichtlicher Kenntnisnahme, Veränderungen oder Löschungen durch Angehörige der Verwaltung zu bewahren.
Lösungswege unter Anwendung kryptografischer Verfahren	In all diesen Fällen kann nur eine entsprechend starke Verschlüsselung gegen Abhörangriffe bei der Übertragung über die physikalischen Leitungen schützen. Grundsätzlich werden zwei Möglichkeiten zur Nutzung kryptografischer Verfahren in Landesnetzen gesehen: 1. Die kryptografischen Verfahren werden **verfahrensspezifisch** von den jeweiligen Verfahrensbetreiber installiert. Damit wird auch die datenschutzrechtliche Verantwortung bei der Verarbeitung personenbezogener Daten nach § 9 BDSG untermauert, wonach die Daten verarbeitende Stelle die technischen und organisatorischen Maßnahmen treffen muss, die erforderlich sind, um die in der Anlage zu § 9 BDSG genannten Anforderungen, z.B. der Weitergabekontrolle, zu gewährleisten. Für die technische Realisierung kommen sowohl hardware- als auch

	software-basierte Verfahren in Betracht. Bei hardware-basierten Verfahren können Kryptoboxen (-->5.5), die die gesamte Kommunikation zwischen den Beteiligten verschlüsseln, zum Einsatz kommen. Diese Variante beeinträchtigt den Datendurchsatz im Normalfall nicht, ist jedoch, da alle beteiligten Kommunikationspartner mit einer Kryptobox ausgestattet werden müssen, kostenintensiv. Software-basierte Lösungen sind im Einzelfall im allgemeinen kostengünstiger und können direkt auf die zum Einsatz kommende Hard- und Software abgestimmt werden. Problematisch ist jedoch oftmals die Integration in ein vorhandenes Netzwerk. Zum einen kann der Einsatz verschiedener Verschlüsselungsprodukte innerhalb eines Netzwerkes erhebliche Probleme verursachen und andererseits ist die Beschaffung verschiedener verfahrensabhängiger Verschlüsselungsprodukte in der Summe sehr kosten- und pflegeintensiv, insbesondere vor dem Hintergrund, dass alle Verfahren das gleiche Ziel, nämlich eine sichere Verschlüsselung der Daten, haben. 2. Wünschenswert ist daher ein **zentraler landesweiter Infrastrukturdienst** (Verschlüsselungsdienst), der z.B. vom Landesnetzbetreiber angeboten wird. Auch hier kommen für die technische Realisierung sowohl hardware- als auch software-basierte Verfahren in Betracht. Bei hardware-basierten Lösungen können z.B. im gesamten Landesnetz an den Übergangspunkten der lokalen Netze (dezentrale Infrastruktur) in das Landesnetz (zentrale Infrastruktur) Krypto-Gateways zum Einsatz kommen, die den gesamten Datenverkehr verschlüsseln. Die Daten werden im Landesnetz verschlüsselt übertragen und an den Übergangspunkten in die jeweiligen lokalen Netze wieder entschlüsselt zur Verfügung gestellt. Dieses Verschlüsselungssystem realisiert zwar keine Ende-zu-Ende Verschlüsselung (-->5.4) der beteiligten Kommunikationspartner, garantiert aber eine Verschlüsselung außerhalb des Einwirkungsbereichs der Betreiber der jeweiligen lokalen Netze. Innerhalb der lokalen Netze (-->6.4) müssen natürlich Sicherheitsmaßnahmen realisiert werden, die die Vertraulichkeit im lokalen Netz gewährleisten. Diese Lösung ist völlig anwendungsunabhängig und funktioniert mit allen Arten von lokalen Netzen. Für software-basierte Lösungen bieten sich z.B. anwendungsunabhängige Verschlüsselungs-Gateways an. Diese werden an strategisch günstigen Punkten in die lokalen Netze der angeschlossenen Verwaltungen installiert. Die Kommunikation zwischen Client und Server wird immer über einen vor dem Server platzierten Gateway geleitet, der für eine Ver- bzw. Entschlüsselung der übertragenen Daten sorgt. Die Kommunikation zwischen dem Server und dem Gateway erfolgt unverschlüsselt. Die Kommunikation zwischen Gateway und Client bzw. zwischen Gateway und Gateway bei einer Server-Server-Kommunikation erfolgt jedoch immer verschlüsselt. Diese Lösung bietet zwar eine nahezu vollständige Ende-zu-Ende Verschlüsselung, kann aber erhebliche Probleme bei der Integration in die verschiedenen Plattformen der lokalen Netze mit sich bringen. Das zum Einsatz kommende Verschlüsselungsprodukt sollte auch eine Authentisierung auf der Grundlage einer Public Key Infrastructure (PKI) (--> G) mittels Schlüsselzertifikaten unterstützen. Die Nutzung eines Verschlüsselungs-Gateways kann parallel für verschiedene Anwen-

	dungen und Server erfolgen. Hierbei werden dann verschiedene Virtuell Private Networks (VPNs, -->6.3) gebildet.
Besondere Hinweise:	Die generelle Verschlüsselung von personenbezogenen Daten in einem Landesnetz stellt wegen der Vielfalt der Informationsbeziehungen und angeschlossenen Systeme ein erhebliches Problem dar. Es existieren eine Vielzahl von großen und kleineren Verwaltungsverfahren mit jeweils unterschiedlich vielen festen oder variablen Kommunikationspartnern. Die zum Einsatz kommende heterogene Hard- und Software betrifft alle Bereiche, vom Großrechner über UNIX-, Windows-NT-, Novell-basierte Server bis zu PCs der unterschiedlichsten Generationen und auch X-Terminals. Einerseits geht die Entwicklung eindeutig von proprietären zu allgemeinen Client-Server-Anwendungen, andererseits jedoch führt die Entwicklung des Preis-/Leistungsverhältnisses bei Servern wieder zu einer zunehmenden Zentralisierung von Server-Leistungen. Nach derzeitigen Erfahrungen bieten sich deshalb die oben erwähnten anwendungsunabhängigen Verschlüsselungs-Gateways an.

6.3 Corporate und Virtual Private Networks (VPN)

Situationsbeschreibung:	Firmen, Organisationen und Verwaltungen besitzen häufig eine Organisationsstruktur, die sie in Haupt- und Außenstellen oder einzelne Niederlassungen gliedert. Werden deren lokale Netze über WAN-Verbindungen zusammengeschaltet, so dass sie eine logische Einheit bilden, spricht man von einem "Corporate Network". Die Unterschiede zu Virtuellen Privaten Netzen (VPN) sind fließend, beide Begriffe nicht trennscharf abzugrenzen. Corporate Networks beschränken sich zumeist auf Teilnehmer der gleichen Organisation, während VPNs häufig einen logischen Zusammenschluss von Teilnehmern verschiedener Stellen abbilden. Auch stützen sich Corporate Networks häufig auf feste Leitungswege, zumindest jedoch auf festgelegte Zugangsknoten.
Auftretende IT-Sicherheitsprobleme:	Wie immer bei der Nutzung von Übertragungswegen, die nicht unter der Kontrolle der beteiligten Kommunikationspartner stehen, ist die Vetrauenswürdigkeits des Transportwegs und die Sicherheit der Kommunikation nur bedingt verlässlich abzuschätzen. Vertraulichkeit und Integrität basieren in der Regel auf Vertrauen gegenüber dem jeweiligen Netzbetreiber oder Kommunikationsdienstleister. Soweit das Internet genutzt wird, gelten die dort genannten Risiken (vgl. 6.1 Internet). Mit Corporate Networks oder VPNs können geschlossene Benutzergruppen (Closed User Group - CUG) (--> G) innerhalb von Netzen gebildet werden, um deren Kommunikation gegenüber den übrigen Netzteilnehmern - und gegeüber dem Netzbetreiber - abzuschotten. Die Sicherheit gegenüber unbefugter Kenntnisnahme oder Manipulation der Kommunikation basiert auch hier auf dem Einsatz kryptografischer Lösungen.
Lösungswege unter Anwendung kryptografischer Verfahren:	Der häufigste Lösungsansatz für die Bildung kryptografiebasierter Corporate Networks oder VPNs besteht darin, den Datenstrom zwischen den einzelnen Niederlassungen oder Teilnehmer zu "tunneln“ (-->5.1)
Besondere Hinweise:	VPN-Lösungen können direkt am Endgerät ansetzen, indem, als Hard- oder Softwarelösung, entsprechende Funktionen in die Kommunikationskomponenten integriert werden. Der VPN-Tunnel endet dabei am jeweiligen Endgerät. Alternativ dazu ist eine VPN-Bildung auf Router-Ebene möglich, der VPN-Tunnel endet damit am LAN bzw LAN-Segment. Da VPNs häufig dazu verwendet werden, um verteilte Standorte mit jeweils mehreren Endgeräten über unsichere Netze geschützt miteinander zu verbinden, ist die Router-Integration i.a. von Vorteil. Verschiedene Router-Hersteller bieten dazu spezielle Geräte bzw. Ergänzungen zu ihren Standardprodukten an. In Corporate Networks oder VPNs erfolgt eine Verschlüsselung der Inhalte auf Verbindungs- nicht auf der Anwendungsebene. Bei Router-basierten VPNs verwendem die Endgeräte den gleichen Schlüssel. Insofern ist eine Kenntnisnahme ggf. auch für andere als den eigentlichen Empfänger Pakets möglich. Die für die Bildung des VPN verwendeten Schlüssel sind jedoch so aufzubewahren, dass sie auch bei Verlust wiederhergestellt werden können, da sonst der gesamte Zugang zum VPN unterbrochen ist.

6.4 Lokale Netze

Situationsbeschreibung:	Ein lokales Netz ist ein Computernetz, das sich in einem Gebäude (Hausnetz) oder in mehreren Gebäuden innerhalb einer geschlossen Liegenschaft (Campusnetz) befindet und über das der Nutzer das alleinige Verfügungsrecht besitzt. Es gibt kleine lokale Netze wie etwa in einer Amtsverwaltung, einer Arztpraxis oder einem Handwerksbetrieb und große lokale Netze wie etwa in Kreisverwaltungen, größeren Rathäusern, in Ministerien, Landesämtern oder Hochschulen. Lokale Netze sind überwiegend Client-Server-Systeme, seltener größere Rechner mit Terminalbetrieb. Zunehmend werden lokale Netze eingesetzt, die ohne Kabelverbindungen drahtlos über Funkverbindungen kommunizieren. Solche Wireless LANs (--> G) sparen Verkabelungskosten und tragen z.B. zum Denkmalschutz bei, weil auf bauliche Veränderungen verzichtet werden kann.
Auftretende IT-Sicherheitsprobleme:	Auch bei der Übertragung schutzbedürftiger Daten in lokalen Netzen kann das Risiko des unbefugten Zugriffs auf die übertragenen Daten auf dem Übertragungsweg nicht auszuschließen. Dabei spielt natürlich die Größe, die Konfiguration und die räumliche Ausdehnung der lokalen Netze eine Rolle. Auf lokalen Netzen sind aus verschiedenen Gründen unterschiedliche Zugriffsprofile der Benutzer umzusetzen. Die datenschutzrechtliche Zweckbindung personenbezogener Daten und der unterschiedliche Schutzbedarf der verschiedenen Verfahren und Dateien machen eine differenzierte Zugriffskontrolle erforderlich, damit die Benutzer daran gehindert werden, Zugriff auf andere Verfahren und Dateien zu erhalten, zu deren Verwendung sie nicht befugt sind. Die Zugriffskontrolle wird meist dadurch realisiert, dass einem Benutzer nach einer zuverlässigen Authentisierung (z.B. Passwortverfahren und/oder maschinenlesbarer Benutzerausweis) vorgegebene Benutzerrechte zugewiesen werden, deren Einhaltung vom System kontrolliert wird. Diese Abschottungen erreichen aber nicht immer die angemessene Sicherheit. Privilegierte Benutzer, etwa die Systemverwalter, können normalerweise nicht durch solche Maßnahmen in ihren Zugriffsrechten beschränkt werden. Wenn also Daten auf Grund ihres Schutzbedarfs auch vor dem Zugriff privilegierter Benutzer geschützt werden müssen, sind weiter gehende Maßnahmen erforderlich. Häufig werden lokale Netze an öffentliche Netze angeschlossen. Dann muss der Gefahr begegnet werden, dass aus diesen Netzen unbefugt auf schutzbedürftige Daten zugegriffen werden kann. Die Abschottungen mit Firewalls (--> G) bieten auch bei sorgfältiger Administrierung nicht immer angemessenen Schutz. Bei Wireless LANs liegen die Risiken unbefugten Abhörens oder Mitschneidens der Kommunikation auf der Hand. Was mit Funk gesendet wird, kann von jedem mitgeschnitten werden, der sich mit entsprechenden Empfängern im Sendebereich aufhält. Hinzu kommt die Gefahr, dass zusätzliche Clients unbefugt in das LAN

	eingebunden werden – bei entsprechender Einstellung der sog. Access Points (--> G)werden sogar alle aktiven Systeme im Sendebereich, die mit der entsprechenden Funknetzkarte ausgestattet sind automatisch in das LAN einbezogen. Aber auch, wenn der Access Point durch Filterung der Netzkarten-Adressen (MAC-Adresse) (--> G) nur eingetragene Netzkarten akzeptiert, bestehen große Risiken, da die MAC-Adressen manipulierbar sind.
Lösungswege unter Anwendung kryptografischer Verfahren:	Wenn also der unbefugte Zugriff auf schutzwürdige Daten nicht mit hinreichender Sicherheit ausgeschlossen werden kann, dann müssen Maßnahmen ergriffen werden, die sicherstellen, dass trotz der Zugriffsmöglichkeiten Unbefugter ein Missbrauch der Daten ausgeschlossen werden kann. Dies kann zum Teil mit einer **Speicherverschlüsselung** erreicht werden. Für die **Datenübertragung** in lokalen Netzen bieten sich zur Verschlüsselung je nach Größe des Netzes und der Komplexität der Schlüsselverteilung symmetrische oder hybride kryptografische Verfahren an. Für die **Speicherverschlüsselung** der Datenbank des Servers werden sinnvollerweise symmetrische Verschlüsselungsverfahren eingesetzt, da Probleme der Schlüsselverteilung in diesem Falle nicht auftreten. Die Verschlüsselung der Daten erfolgt bei **Wireless LAN**s des Standards IEEE 802.11b mit dem symmetrischen Verschlüsselungsverfahren WEP (Wired Equivalent Privacy) (--> G), welches auf 40 Bit oder 104 Bit Verschlüsselungstiefe eingestellt werden kann. Das Verfahren enthält jedoch mathematische Schwächen und ist daher wiederholt erfolgreich kryptoanalytisch angegriffen worden. Daher ist es vorzuziehen, auch bei Wireless LANs auf die als sicher erkannten symmetrischen oder hybriden Verfahren zurückzugreifen, beispielsweise mit kryptografisch gesicherten VPNs (-->6.3). Für die sichere Authentisierung von Clients im Wireless LAN sind Challenge-Response-Verfahren (-->5.3) angemessen.
Besondere Hinweise:	Eine vollständig oder teilweise verschlüsselte Festplatte ist über das Netzwerk angreifbar, wenn sie gerade durch einen Berechtigten genutzt wird und damit der Zugriff auf die Daten freigegeben ist. In diesem Falle wird nur die für einen Angriff zur verfügbare Zeit verringert.

6.5 Sprachkommunikation und Telefax

Situationsbeschreibung:	Das Telefonieren ist nach wie vor die am meisten verwendete Kommunikationsform im privaten und im beruflichen Bereich. Dabei verlassen sich die Gesprächsteilnehmer in der Regel darauf, dass die Gesprächsinhalte vertraulich bleiben und deshalb Inhalte ausgetauscht werden, die aus privaten und geschäftlichen Interessen für vertraulich gehalten werden. Was für das Telefon gilt, betrifft die Telefax-Nutzung in gleicher Weise. In der Zwischenzeit ergänzt die Mobilfunktelefonie die gewohnte Nutzung des Festnetzes.
Auftretende IT-Sicherheitsprobleme:	Das Abhören von Telefongesprächen war in der Vergangenheit möglich und wird auch künftig – trotz neuer Technologien – ein immer währendes Problem sein. Rechtlich ist die Sprachkommunikation zwar durch das Fernmeldegeheimnis (§10 GG und § 85 TKG) geschützt; in der Praxis fehlen jedoch immer noch geeignete technische Instrumente, um diesen Schutz auch in allen Fällen zu gewährleisten. Insbesondere in Wirtschaft und Politik sind Gesprächsinhalte oft sehr vertraulich. Wenn es um Wettbewerbsvorteile geht, wächst das Interesse daran, Kenntnis von Gesprächsinhalten der Konkurrenz zu erlangen. Analoge Anschlüsse können mit einfachen Mitteln abgehört werden, sofern der Abhörende sich Zugang zu der Telefonleitung verschaffen kann. ISDN-Anschlüsse und digitale Endgeräte in TK-Anlagen erfordern dafür einen deutlich höheren Aufwand, z. B. sind hierzu spezielle teure Messgeräte notwendig. Das Abhören von ISDN-Anschlüssen ist daher eher eine Maßnahme der Wirtschaftsspionage oder der Strafverfolgung als eine zur Befriedigung privater Neugier. Ein wirksamer Schutz gegen Abhörgefahren kann nur durch ein Zusammenspiel von baulichen (Gebäude- bzw. Raumsicherung), organisatorischen (Zugangsregelungen) und technischen Maßnahmen realisiert werden. Zu den technischen Maßnahmen gehören die Protokollierung von Eingriffen in die TK-Infrastruktur einschl. der Wartungsaktivitäten, die Überwachung der Signale auf dem Steuerungskanal (D-Kanal) sowie die Verschlüsselung der Kommunikationsinhalte. Eine weitere Gefährdung besteht bei Richtfunkverbindungen. Diese sind im allgemeinen unverschlüsselt. Hier besteht die Möglichkeit, die Funksignale mittels Antennen und Spezialempfängern unbemerkt aufzufangen und abzuhören.
Lösungswege unter Anwendung kryptografischer Verfahren:	Der bisher einzig wirksame Schutz vor dem Abhören von Telefongesprächen ist die kryptografische Verschlüsselung. Dies gilt nicht nur für die Sprachkommunikation mittels Telefone, sondern auch für Funkdienste, Betriebsfunk oder BOS-Netze (z.B. Polizeifunk). Beim GSM-Mobilfunk wird die Luft-Übertragungsstrecke zwischen dem Handy und der Basisstation verschlüsselt. Diese Verschlüsselung kann noch als relativ sicher gelten. Es gibt jedoch spezielle Angriffsgeräte (sog. IMSI-Catcher), die die Sicherheitsdefizite des GSM-Standards ausnutzen und den Mobiltelefonen eine Basisstation vortäuschen, die Verschlüsselung des Dienstes unbemerkt abschalten und Klarbetrieb vorgeben. Dadurch

	wird ein Abhören möglich. Dies gilt jedoch nur bei abgehenden Gesprächen. Der effektivste Schutz gegen das Abhören ist die Anwendung einer starken “Ende-zu-Ende – Verschlüsselung” (--> G). Hierbei wird jedem Telefon eine Verschlüsselungs- und Authentisierungseinheit vorgeschaltet, so dass beim Aufbau der Verbindung die Authentizität der Gesprächsteilnehmer sichergestellt und während der Verbindung alle Daten verschlüsselt übertragen werden. Hierzu ist es jedoch notwendig, dass der Gesprächspartner ebenfalls ein entsprechendes Gerät besitzt. Aus wirtschaftlichen Gesichtspunkten kommt eine Ende-zu-Ende Verschlüsselung nur für Anschlüsse mit hohem Sicherheitsbedarf in Frage. Auch für GSM sind Endgeräte verfügbar, die eine Ende-zu-Ende Verschlüsselung für Sprache bieten. Dabei wird die verschlüsselte Sprache über den “Datenkanal” übertragen. Ein Beispiel für den Einsatz kryptografischer Verfahren ist die Verschlüsselung von Standleitungen zwischen TK-Anlagen.

Abschnitt 7

Szenarien - ausgesuchte Anwendungsfälle

7.1 Abschottung der Systemadministration

Situationsbeschreibung:	Systemadministratoren benötigen zur Erfüllung ihrer Aufgaben privilegierte und sehr weitreichende Zugriffsberechtigungen. Gängige Betriebssysteme gewähren ihnen sogar unbeschränkten Dateizugriff auf sämtliche gespeicherten Daten. In der Regel benötigen Administratoren aber nur zur Behebung von Fehlerfällen Zugriff auf gespeicherte personenbezogene Daten
Auftretende IT-Sicherheitsprobleme:	Bedingt durch die weitgehenden Zugriffsberechtigungen oder Zugriffsberechtigungserteilung haben Systemadministratoren die Möglichkeit, Daten missbräuchlich zu lesen oder gar zu manipulieren. Eine nachträgliche Überprüfung, ob der Systemadministrator tatsächlich nur in berechtigten Einzelfällen, wenn die Notwendigkeit des Zugriffs gegeben war, auf gespeicherte personenbezogene Daten zugegriffen hat, ist in der Praxis schwierig oder gar unmöglich: Marktgängige Systeme verfügen oft über keine aussagekräftige und revisionssichere Protokollierung der durchgeführten Administrationstätigkeiten oder die Implementierung derartiger Protokollierungsmechanismen vermindert die Leistung eines Rechners in nicht tragbarer Weise. Daneben entsteht bei der extensiven Protokollierung das Problem, dass die Menge an gewonnenen Protokollierungsdaten so umfangreich sind, dass eine visuelle Auswertung nicht praktikabel ist. Software zur Auswertung der Datenmengen hingegen birgt das Risiko, dass bestimmte Aktionen nicht bemerkt werden. Angesichts dieser faktisch uneingeschränkten und weitgehend unkontrollierbaren Zugriffsmöglichkeiten ist es notwendig, schutzbedürftige personenbezogene Daten auf wirksame Weise vor dem missbräuchlichen Zugriff durch Systemadministratoren zu schützen. Insbesondere gilt dies bei besonders sensiblen personenbezogenen Daten wie z.B. medizinischen Angaben, Steuer-, Sozial- oder Personaldaten.
Lösungswege unter Anwendung kryptografischer Verfahren:	Lösungsmöglichkeiten ergeben sich durch eine Verschlüsselung der gespeicherten Daten. Die Verschlüsselung von Datenspeichern lässt sich durch marktgängige Produkte auf der Grundlage symmetrischer Verschlüsselungsalgorithmen (--> G) realisieren, mit denen vollständige Verzeichnisse oder Laufwerke eines Computernetzwerks verschlüsselt werden können. Im Rahmen des Schlüsselmanagements wird festgelegt, welche Benutzer welche Daten verschlüsseln und entschlüsseln können. Die Entschlüsselung von Daten sollte dabei nur auf dem Client des Benutzers erfolgen; auf dem Server sollten die Daten auch während der Bearbeitung verschlüsselt gespeichert sein. Auch sollten temporäre Dateien verschlüsselt werden, wenn sie während der Bearbeitung auf dem Client oder Server erstellt werden. Wird die Entschlüsselung auf dem Client durchgeführt, dann ist der übertragene Datenstrom zwischen Client und Server ebenfalls verschlüsselt. Damit die beabsichtigte Schutzwirkung eintritt, darf mit dem Schlüsselmanagement nicht die Systemadministration betraut werden. Ansonsten könnte sie sich selbst berechtigen, gespeicherte Dateien auch wieder zu ent-

	schlüsseln. Sofern Daten mit Hilfe eines Datenbanksystems verarbeitet werden, lässt sich die Vertraulichkeit der Daten gegenüber dem Systemadministrator durch eine Datenbank-Verschlüsselung sicherstellen. Um die beabsichtigte Schutzwirkung zu erzielen, darf auch hier das Schlüsselmanagement nicht der Systemadministration übertragen werden.

7.2 Anbindung von Außenstellen

Situationsbeschreibung:	In vielen Fällen verteilen sich Behörden über mehrere Standorte. Dabei muss im Normalfall sowohl eine Kommunikation zwischen den verschiedenen Standorten einer Behörde als auch von jedem Standort aus mit anderen Behörden möglich sein. Eine Verbindung mehrerer Standorte erfolgt meist über die direkte, meist sternförmige Anbindung von Außenstellen an einen Hauptstandort oder über den direkten Zugang aller beteiligten Außenstellen und Hauptstandorte an ein Landesnetz (-->6.2) und Anbindung über dieses Landesnetz. Bei mehreren Außenstellen sind natürlich Mischformen der genannten Wege möglich. Bei einer direkten Vernetzung kommen normalerweise gemietete gewidmete Leitungen, aber auch eigene Kommunikationsleitungen zum Einsatz.
Auftretende IT-Sicherheitsprobleme:	Obwohl an ein Landesnetz in der Regel nur öffentliche Stellen des Landes angeschlossen sind, muss man wegen der Nutzung der Internet-Technologie, der großen Anzahl angeschlossener Stellen und berechtigter Benutzer sowie wegen der meist bestehenden Anbindung an das Internet (-->6.1) prinzipiell von den gleichen Gefahren und Risiken wie im Internet ausgehen. Das Landesnetz ist somit aus Sicht der zu verbindenden Standorte einer Landesverwaltung wie ein öffentliches Kommunikationsnetz anzusehen. Daher eine Verschlüsselung bei der Übertragung personenbezogener oder anderweitig schutzwürdiger Daten erforderlich. (-->6.2).
Lösungswege unter Anwendung kryptografischer Verfahren:	Prinzipiell bieten sich folgende Möglichkeiten der Verschlüsselung an: Bei einer direkten Verbindung von Außenstellen und Hauptstandort mit einer begrenzte Zahl von feststehenden Kommunikationsbeteiligten, können Kryptoboxen, die die gesamte Kommunikation zwischen den Beteiligten verschlüsseln, zum Einsatz kommen. Dieses hat den Vorteil, dass man keine Unterscheidung nach personenbezogenen oder anderen schutzbedürftigen Daten machen muss und keine Eingriffe in existierende Verfahren notwendig sind. Kryptoboxen können auch bei einer Verbindung über das Landesnetz zum Einsatz kommen, sind hier jedoch, wie in 6.2 beschrieben, wenig flexibel. Bei einer direkten Kommunikation von Außenstellen mit anderen Landesverwaltungen über ein Landesnetz müssen dann u.U. andere - in diesem Fall zusätzliche - Verschlüsselungsmechanismen implementiert werden. Die Errichtung von Virtuell Private Networks (VPNs) (-->6.3) bietet sich sowohl für eine direkte Verbindung von Außenstellen und Hauptstandort als auch einer Verbindung über ein Landesnetz an. Diese Variante wird ausführlicher in den Kapiteln 6.2 und 6.3 beschrieben.
Besondere Hinweise:	Auch bei der Anbindung über eigene oder angemietete und gewidmete Leitungen ist eine Verschlüsselung zu empfehlen. Einerseits sind Kommunikationsleitungen u.U. physikalisch angreifbar und andererseits muss mit dem Zugriff von Mitarbeitern des Telekommunikationsanbieters bei gemieteten Leitungen gerechnet werden.

7.3 E-Commerce - Elektronischer Handel

Situationsbeschreibung:	Mit E-Commerce werden Rechtsgeschäfte bezeichnet, die weitgehend über elektronische Medien abgewickelt werden. Dazu gehören Vorgänge wie Warenbestellung, Versteigerung, Softwarelizensierung, aber auch vorgelagerte Tätigkeiten wie Produktauswahl und Blättern in elektronischen Katalogen. Davon begrifflich abgegrenzt, aber mit vergleichbaren Problemen behaftet, ist der Bereich des Electronic Banking (E-Banking). E-Commerce wird überwiegend über das Internet (-->6.1), speziell das WWW, abgewickelt.
Auftretende IT-Sicherheitsprobleme:	Besondere Bedeutung kommt beim E-Commerce der **Vertraulichkeit** der personenbezogenen Daten bei der Übertragung zu, insbesondere der Daten für den Bezahlvorgang. Die heute üblichen Methoden der Online-Bezahlung (per Kreditkarte oder per Einzugsermächtigung) bergen ein hohes Missbrauchsrisiko, wenn die dabei übermittelten Daten Unbefugten in die Hände fallen. Aber auch andere personenbezogene Daten (Bestelldaten, Daten über besondere Produktinteressen) sind vor einer unberechtigten Kenntnisnahme zu schützen. Dabei ist bereits bei der Ausgestaltung der Verfahren darauf zu achten, dass Nutzungsdaten, soweit möglich, nicht personenbezogen (sondern anonym bzw. pseudonym) verarbeitet werden, so dass die Missbrauchsmöglichkeiten Dritter verringert werden. Besonders gefährdet sind auch die Stammdaten, Zertifikate, Zugangscodes, TAN-Listen (beim E-Banking) etc., die lokal gespeichert werden. Diese Daten sowie die über die Tastatur eingegebenen Passwörter sind außerdem bevorzugte Ziele von verbreiteten Trojanischen Pferden wie BackOrifice oder NetBus. Neben der Frage der Vertraulichkeit spielt bei E-Commerce der Aspekt der Authentizität und Integrität der übermittelten Daten eine wesentliche Rolle. Für den Kunden muss erkennbar sein, dass ein Angebot, das auf elektronischem Wege unterbreitet wird, tatsächlich von dem Anbieter stammt, der dabei genannt wird. Gerade im Internet bestehen jedoch eine Reihe von technischen Möglichkeiten, um (zumindest zeitweilig) ganze Websites oder einzelne Seiten zu manipulieren. Umgekehrt müssen Kundendaten unverfälscht beim Empfänger ankommen. Beide Vertragsseiten müssen ihre Rechtsgeschäfte nachweisen können.
Lösungswege unter Anwendung kryptografischer Verfahren:	Bei der Übertragung der Daten im Rahmen des E-Commerce ist eine Transportverschlüsselung in jedem Fall geboten. Zur Gewährleistung von Authentizität und Integrität ist vor allem das Mittel der digitalen Signatur (--> 5.2) geeignet, bei der ebenfalls kryptografische Verfahren verwendet werden. Im E-Commerce ist vor allem der Standard SSL (--> G)von Bedeutung, da dies das im WWW vorherrschende Sicherheitsprotokoll darstellt. Für das E-Banking ist der Standard HBCI (--> G).
Besondere Hinweise:	Im Bereich E-Commerce ist die Verwendung einer mittleren bis hohen Verschlüsselungsqualität zu empfehlen. Zwar sind die einzelnen Nutzungsdaten i.A. nur in einem engen zeitlichen Rahmen von Interesse, allerdings

	werden auch länger gültige Stammdaten (wie z.B. Kreditkartennummern) übertragen, bei denen zudem ein wirtschaftliches Interesse Dritter angenommen werden kann. Die Verschlüsselung muss daher ausreichend stark sein, damit ein sicherer Schutz gewährt wird. Für private, im Rahmen des E-Commerce lokal gespeicherte Daten ist in jedem Fall eine Recovery-Option durch den Benutzer sinnvoll, etwa durch eine sichere Aufbewahrung der unverschlüsselten Daten auf Diskette.

7.4 Elektronische Bürgerdienste

Situationsbeschreibung:	Zunehmend nutzt die öffentliche Verwaltung das Internet dazu, ihr Dienstleistungsangebot zu verbessern. Sie hält nicht nur eine Vielzahl von Informationen zum Abruf bereit, sondern bietet verstärkt auch elektronische Dienstleistungen an. Musste der Bürger bisher eine Behörde mitunter mehrfach persönlich aufsuchen und war strikt an deren Öffnungszeiten gebunden, so soll er künftig mehr und mehr die Möglichkeit haben, von Zuhause aus und wann immer es ihm gerade passt, Behördengänge via Datennetz zu erledigen. Denkbar wäre, dass der Nutzer auf diese Weise seinen Wohnsitz an- oder ummeldet, ein Wunschkennzeichen oder die Zulassung seines KfZ beantragt, einen Anwohnerparkausweis anfordert oder seine Steuererklärung elektronisch abgibt. Die Übersendung des beantragten amtlichen Dokuments, der angeforderten Bescheinigung oder der gewünschten Auskunft sowie der Bezahlvorgang könnten wie bislang oder in weiteren Ausbauschritten auch zunehmend elektronisch erfolgen. Die Gesamtheit dieser über das Internet angebotenen Dienstleistungen wird mit eGovernment bezeichnet.
Auftretende IT-Sicherheitsprobleme:	Weil grundlegende Anforderungen an Vertraulichkeit, Integrität und Authentizität ohne die Ergreifung zusätzlicher Maßnahmen im Internet nicht erfüllt sind, müssen an die Realisierung von eGovernment-Diensten folgende Anforderungen gestellt werden: Die Behörde muss zweifelsfrei feststellen können, wer ihr einen elektronischen Antrag zugeleitet hat. Wenn Daten über das Internet übertragen werden, dann ist im allgemeinen nicht sichergestellt, dass sie tatsächlich von demjenigen herrühren, der als Absender der Daten angegeben ist. Umgekehrt muss sichergestellt sein, dass der Nutzer tatsächlich die elektronische Dienstleistung der Behörde und nicht etwa ein gefälschtes Angebot nutzt, das ihm ein Angreifer vorspiegelt, um ihn zur Preisgabe sensibler Daten zu verleiten (Gewährleistung der Authentizität). Es muss weiter sichergestellt sein, dass Unberechtigte von den zwischen der Behörde und dem Nutzer ausgetauschten Daten keine Kenntnis erlangen können. Ohne entsprechende Maßnahmen ergriffen zu haben, können über das Internet im Klartext übertragene Daten an einer Vielzahl von Stellen des Übertragungswegs abgehört werden (Gewährleistung der Vertraulichkeit). Es muss außerdem sichergestellt sein, dass die zwischen der Behörde und dem Nutzer ausgetauschten Daten den Empfänger auch so erreichen wie sie abgesandt wurden. Ohne dass dies für den Empfänger erkennbar wäre, können über das Internet im Klartext übertragene Daten inhaltlich verändert werden (Gewährleistung der Integrität).
Lösungswege unter Anwendung kryptografischer Verfahren:	Den beschriebenen Risiken lässt sich derzeit nur durch Einsatz kryptografischer Methoden der Verschlüsselung und der digitalen Signatur wirksam begegnen. Der Einsatz kryptografischer Verfahren ist daher unverzichtbar, um eine ausreichende Sicherheit und damit auch eine Akzeptanz elektronischer Bürgerdienste zu erzielen. Mit den Diensten der Elektronische Post und des WWW stehen die benötigten technischen Hilfsmittel zur Verfügung, um elektronische Bürgerdiens-

	te zu realisieren. Folgendes Realisierungsmodell kommt beispielsweise in Frage: - Die Behörde stellt ihre Antragsformulare auf einem WWW-Server für den Bürger bereit. - Der Bürger kann mit einem herkömmlichen WWW-Browser die Antragsformulare abrufen, sie ausfüllen und die Daten entweder per E-Mail oder im Rahmen einer WWW-Kommunikation verschlüsselt und digital signiert an die Behörde senden. - Die Behörde entschlüsselt den eingegangenen elektronischen Antrag, prüft die digitale Signatur, sendet dem Bürger eine Quittung zu und bearbeitet den Antrag. Um in diesen Verfahrensschritten die Vertraulichkeit, Integrität und Authentizität der Daten zu gewährleisten, stehen sowohl für den Austausch von Daten via E-Mail als auch für eine WWW-Kommunikation geeignete Methoden zur Verfügung. Sofern zur Absicherung einer WWW-Kommunikation SSL (-->G) eingesetzt werden soll, ist allerdings zu beachten, dass SSL ein verbindungsorientiertes, nicht dagegen ein dokumentenorientiertes Sicherheitsprotokoll ist. Dem Nutzer ist es nicht möglich, einzelne Dokumente digital zu signieren. Die digitale Signierung einzelner Dokumente kann durch den Einsatz eines auf dem Client des Nutzers installierten lokalen http-Sicherheits-Proxy ermöglicht werden. Der Web-Browser auf dem Client des Nutzers wird so konfiguriert, dass er stets den lokalen Sicherheits-Proxy anspricht, der wiederum die externe Verbindung zum WWW-Server der Behörde herstellt. Der Sicherheits-Proxy verfügt über eine Signierkomponente, die es ermöglicht, einzelne Dokumente mit einer digitalen Signatur zu versehen, bevor sie an den WWW-Server der Behörde übertragen werden. Schließlich gilt es, die technischen und organisatorischen Rahmenbedingungen für den Einsatz der digitalen Signatur festzulegen. In Deutschland wurden mit dem Signaturgesetz und der Signaturverordnung bereits die gesetzlichen Rahmenbedingungen geschaffen, die ein hohes Maß an Sicherheit bieten. Der Gesetzgeber hat mit der Überarbeitung einer Fülle von Gesetzen die Grundlagen geschaffen, um rechtsverbindliches Handeln innerhalb von eGovernment-Diensten in Verwaltungsverfahren zu ermöglichen. Es empfiehlt sich deshalb, diese Vorgaben zu übernehmen. Sofern von diesen Standards abgewichen wird, muss im Einzelfall unter Berücksichtigung der Art des vorgesehenen Dienstes und der davon berührten personenbezogenen Daten genau geprüft werden, welche Auswirkungen dies auf die Sicherheit und Rechtsverbindlichkeit hat und ob das erzielte Sicherheitsniveau akzeptabel ist.
Besondere Hinweise:	Weitere Anforderungen an die Gestaltung von eGovernment-Diensten können der Broschüre "Datenschutzgerechtes eGovernment" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder entnommen werden.

7.5. Elektronische Post

Situationsbeschreibung:	Die elektronische Post hat sich als Kommunikationsform in den Verwaltungen etabliert. Die Möglichkeit, multimediale Daten ohne Medienbruch und nahezu verzögerungsfrei auszutauschen sowie die Integration in die IT-Lösungen am Arbeitsplatz haben dazu geführt, dass die E-Mail-Kommunikation binnen kurzer Zeit den papiergebundenen Schriftverkehr und das Telefax ergänzt, in Teilbereichen bereits ersetzt hat. Es ist absehbar, dass in Zukunft mit Hilfe elektronischer Mitteilungssysteme rechtsverbindliche Informationen ausgetauscht und Verwaltungsleistungen erbracht werden.
Auftretende IT-Sicherheitsprobleme:	Den klaren Vorteilen der E-Mail-Kommunikation stehen Sicherheits- und Datenschutzbedenken gegenüber. Die Übertragungswege sind durch die Nutzer i.d.R. nicht kontrollierbar. Welchen Weg eine Nachricht nimmt oder in welchem Vermittlungsrechner die Nachricht bearbeitet wird, ist nicht transparent. Beim E-Mail-Dienst werden die Inhaltsdaten standardmäßig meist im Klartext übertragen. Mit entsprechenden Programmen kann daher der Datenverkehr im Netz bzw. auf den Netzknoten abgehört, nach relevanten Informationen durchsucht oder manipuliert werden. Nach den Anforderungen der Datenschutzgesetze sind für personenbezogene Daten bei der Übertragung via E-Mail Maßnahmen zu treffen, die gewährleisten, dass Nachrichten nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können. Die Vertraulichkeit der übertragenen Daten, ihre Vollständigkeit und ihr Schutz vor unerlaubten Veränderungen sind damit durch geeignete Maßnahmen sicher zu stellen. Hinzu kommt vielfach die Notwendigkeit die verlässliche Zurechenbarkeit zu einem bestimmten Absender zu gewährleisten. Risikoszenarien beim Einsatz von E-Mail sind u.a.: - Vortäuschen einer falschen Absenderadresse, - Aufzeichnen von Nachrichten während der Übertragung und Weiterleitung über Vermittlungseinrichtungen - Zugriff auf Nachrichten in Postfächern - Manipulation von Verteilerlisten - Verändern von Nachrichteninhalten
Lösungswege unter Anwendung kryptografischer Verfahren:	Für die Wahrung der Vertraulichkeit und Integrität sowie die verlässliche Identifizierung von Kommunikationspartnern kommen damit vor allem kryptografische Verfahren zur Verschlüsselung (= Wahrung der Vertraulichkeit) und Elektronischen Signatur (= Nachweis der Integrität und Authentizität) in Betracht. Mit ihrer Hilfe lassen sich Manipulationen und Übertragungsfehler erkennen und die unberechtigte Kenntnisnahme unterbinden. Entsprechende Lösungen sind Stand der Technik und können mit vertretbarem Aufwand eingesetzt werden, beispielsweise mit dem Programm PGP (-->G) oder dem Protokoll S/MIME (-->G).

7.6 Externe Archivierung

Situationsbeschreibung:	Wenn datenverarbeitende Stellen vor der Frage stehen, ob und welche Funktionen im Rahmen eines Outsourcings durch externe Stellen übernommen werden können, drängt sich die Archivierung auf. Gründe für eine externe Archivierung sind beispielsweise Raumprobleme oder der Zwang, für die Dauer der meist langjährigen Archivierung die Technik bereit zu halten, um alle Datenträger zu lesen.
Auftretende IT-Sicherheitsprobleme:	Den Vorteilen der externen Archivierung steht als ein Nachteil gegenüber, dass der Auftragnehmer Zugriff auf die Daten hat und sie zur Kenntnis nimmt. Das kann insbesondere bei sensiblen Daten untragbar sein.
Lösungswege unter Anwendung kryptografischer Verfahren:	Mit einer Datenverschlüsselung ist es möglich, die Kenntnisnahme durch den Auftragnehmer zu verhindern, und gleichzeitig dessen Sicherheitsmaßnahmen gegen Dritte zu unterstützen. In diesem Falle dürften in der Hauptsache symmetrische Verfahren in Frage kommen. Damit die Verschlüsselung der Daten als wesentliche Maßnahme gegen unberechtigte Zugriffe während der Archivierung greift, sind einige grundsätzliche Forderungen umzusetzen. 1. Das Verschlüsselungsverfahren muss hinreichend sicher sein (-->3). 2. Die für eine Entschlüsselung nötigen geheimen Schlüssel dürfen nur der datenverarbeitenden Stelle zur Verfügung stehen. Der Auftragnehmer darf keinen Zugriff auf unverschlüsselte Daten oder die geheimen Schlüssel haben. Die Verschlüsselung sollte daher bei der datenverarbeitenden Stelle erfolgen, was den weiteren Vorteil hat, dass damit auch eine Kenntnisnahme der Daten durch Dritte während der Übertragung oder auf dem Transport verhindert wird. Bei der Abschottung der Kryptokomponenten sollte auch versucht werden, den Zugriff auf die Schlüssel für Personal des Auftraggebers zu unterbinden. Die gesicherte Speicherung in Chipkarten oder Kryptomodulen kann dazu dienen. Soweit möglich und sinnvoll sollte die datenverarbeitende Stelle die Schlüssel selbst erzeugen. Wenn ein Trust-Center (--> G) die Schlüssel generiert, sollte es vom Auftragnehmer für die externe Archivierung unabhängig sein. 3. Das Verfahren muss an geänderte Rahmenbedingungen angepasst werden können. Die Archivierungsdauer bemisst sich in Jahrzehnten. Angesichts der technischen Entwicklung und der Forschung im Bereich der Kryptografie können Verschlüsselungsverfahren in dieser Zeit unsicher werden oder überholt sein, von denen heute keine Schwachstellen bekannt sind. Es muss daher möglich sein, das Verfahren zu ändern oder zu ersetzen und auch bereits archivierte Daten mit der neuen Technik zu sichern. 4. Der Auftraggeber muss für die gesamte Dauer der Archivierung auf die Daten zugreifen können. Damit der Auftraggeber bei Bedarf auf die Daten zugreifen kann, muss über Jahrzehnte sichergestellt sein, dass die geheimen Schlüssel zusammen mit einer funktionsfähigen Hard- und Software zur Verfügung stehen. Werden beispielsweise die geheimen Schlüssel ausschließlich auf wenigen Chipkarten gespeichert, so müssten diese Chipkarten für die ganze Dauer

	der Archivierung funktionsfähig bleiben. Abhängig von der Einsatzumgebung kann das schwierig sein. Es muss ein Verfahren gefunden werden, wie ein geheimer Schlüssel im Fall seines Verlusts, z.B. durch technisches Versagen der Chipkarten, rekonstruiert werden kann (Key-Recovery (--> G)). Wenn der geheime Schlüssel an mehreren Stellen hinterlegt wird, sind damit mehrere potentielle Angriffspunkte für einen Angreifer vorhanden, der die Daten entschlüsseln will. Dies kann ein Sicherheitsproblem darstellen. Wird das Geheimnis, mit dessen Kenntnis der Schlüssel rekonstruiert werden kann, so auf mehrere Personen oder Institutionen verteilt, dass nur alle zusammen den Schlüssel rekonstruieren können, spricht man von „Secret Splitting“. (siehe Wobst Ziff. 6.2.1.; ein Beispiel wäre das Aufteilen des Schlüssels in 3 Teile, die von 3 verschiedenen Personen verwahrt werden.) Problematisch ist in diesem Fall, dass nach dem Ausfall eines Geheimnisträgers der Schlüssel nicht mehr rekonstruiert werden kann. Eine dritte mögliche Lösung ist das "Secret Sharing" (zu Details siehe Wobst Ziff. 6.2.2), bei dem das Geheimnis ebenfalls auf mehrere Personen oder Institutionen verteilt wird. Im Unterschied zum „Secret Splitting“ kann aber ein Teil der Geheimnisträger, die Anzahl kann vorgegeben werden, den Schlüssel rekonstruieren, ohne dass einzelne oder einige wenige, wie bei der Hinterlegung des Schlüssels, dazu in Lage sind. Diese Lösung entschärft die Probleme der beiden anderen „Key-Recovery“-Varianten. Neben den Schlüsseln muss für die Dauer der Archivierung auch die Hard- und Software auf einen Stand wiederherstellbar sein, der eine Entschlüsselung zulässt.

7.7 Fernwartung

Situationsbeschreibung:	Fernwartungs- und Fernadministrationsprozeduren sind dadurch gekennzeichnet, dass Veränderungen an den Betriebssystemen, der systemnahen Software, der Applikationssoftware oder den Datenbeständen nicht an dem Ort vorgenommen werden, an dem sich das Rechnersystem befindet. Dieser Umstand erlangt insbesondere dann eine sicherheitstechnische Bedeutung, wenn das Wartungspersonal von einem externen Dienstleister und nicht von der Daten verarbeitenden Stelle gestellt wird. Häufig ist in diesen Fällen nämlich die verantwortliche Stelle mangels eigener System- und Administrationskenntnisse nicht oder nur begrenzt in der Lage, die Ordnungsmäßigkeit der Arbeiten des externen Dienstleisters zu überwachen. Ob eine derartige Situation unter datenschutzrechtlichen Aspekten zu verantworten ist, muss im Einzelfall entschieden werden.
Auftretende IT-Sicherheitsprobleme:	Der Fernwartende erhält in der Regel die volle Verfügungsgewalt über die Administrationsebene des Systems (Super-User). Damit besteht die Möglichkeit, durch Softwaremodifikationen aber auch durch einen Direktzugriff die Inhalte der gespeicherten Datenbestände unbefugt zur Kenntnis zu nehmen. Generell wird dieser Gefahr dadurch begegnet, dass zwischen das zu wartende System und dem Rechner des Wartungsunternehmens ein „Schattenterminal“ zwischengeschaltet wird, auf dem alle übertragenen Informationen dargestellt werden. Ist das systemtechnische Wissen in der Stelle, deren System gewartet wird, ausreichend, sind durchaus wirksame Kontrollen möglich. Filetransfers sind aber z. B. nur sehr schwer zu entdecken, außerdem ist die Wirkung von Dienstprogrammen für nicht professionelle Systemadministratoren in der Regel nicht zu beurteilen. Für sehr sensible Datenbestände (vgl. 2.2) ist das Schattenterminal-Konzept daher nicht „angemessen“.
Lösungswege unter Anwendung kryptografischer Verfahren:	Die Gewährleistung der Vertraulichkeit besonders sensibler Datenbeständen auch gegenüber Wartungsunternehmen kann nur durch ihre Verschlüsselung erreicht werden. Eine solche Verschlüsselung kann auch bei einer Administration der Systeme durch eigene Mitarbeiter erforderlich sein (z. B. für Datenbestände der Personalabteilungen, Personalräte und Betriebsärzte, -->7.1). Zu beachten ist, dass die verwendeten Schlüssel den Administratoren nicht verfügbar sein dürfen. Bei einem Datentransport über offene Netze (z. B. Internet) sind die übertragenen Systemdaten grundsätzlich zu verschlüsseln. In diesem Fall geht es nicht um die Vertraulichkeit gegenüber dem Wartungsunternehmen, sondern um den Schutz vor Angriffen aus dem Netz. Bei beiden Konstellationen ist eine symmetrische Verschlüsselungsmethode ausreichend und praktikabel.

7.8 Mobile Geräte und Datenträger

Situationsbeschreibung:	Der typische Einsatzbereich für mobile Geräte ist die Ausstattung von Außendienstmitarbeitern mit Laptops (siehe auch 7.10 Außendienst und Telearbeit). Mit ihrer Hilfe werden außerhalb der Räumlichkeiten der datenverarbeitenden Stelle Daten automatisiert verarbeitet. Auf maschinell lesbaren Datenträgern (z. B. Magnetband, Diskette) tauschen Behörden elektronisch gespeicherte, personenbezogene Daten aus.
Auftretende IT-Sicherheitsprobleme:	Während des Transportes und der Lagerung sind die mobilen Geräte einem wesentlich höheren Diebstahl- und Missbrauchsrisiko ausgesetzt als stationäre Geräte in der gesicherten Umgebung einer Behörde. Die unbefugte Aktivierung der Software (insbesondere der Applikationssoftware) der mobilen Geräte kann zwar durch Authentisierungsmethoden recht wirksam unterbunden werden, jedoch sind die Datenbestände beim Diebstahl oder Festplattenaustausch ungeschützt. Beim Transport von Datenträgern ist eine unbefugte Kenntnisnahme, Verändern, Löschen und Kopieren der gespeicherten Daten oder ein Verlust bzw. Diebstahl der Datenträger möglich, weil die verantwortlichen Stellen häufig weder die Transportwege noch die übermittelnden Personen auswählen können. Je mehr Personen mit der Beförderung befasst und je länger die Zeiten sind, in denen der Datenträger unbeaufsichtigt bleibt, desto weniger kann die Vertraulichkeit und Integrität der Daten garantiert werden. Der Versand der Datenträger per Einschreiben oder Wertbrief kann dieses Risiko nicht wesentlich verkleinern.
Lösungswege unter Anwendung kryptografischer Verfahren:	Der erforderliche Schutz ist nur durch eine Verschlüsselung des Platteninhaltes (bzw. einer Partition) der Datenträger oder einzelner Dateien zu gewährleisten. Dies ist in einigen Datenschutzgesetzen zwingend vorgeschrieben (vgl. § 6 Abs. 3 LDSG SH vom 26.01.2000). Die Integrität der Daten kann durch Erzeugen eines „digitalen Fingerabdrucks (Message Authentification Code (--> G), Elektronische Signatur (--> 5.2), Checksummen-Verfahren), der mit den in elektronischer Form gespeicherten Daten verknüpft ist, jederzeit erneut überprüft werden.
Besondere Hinweise:	Bei der Verschlüsselung von Datenträgern ist der kryptografische Schlüssel auf sicherem Weg (per Kurier, Brief, persönlich, telefonisch – letzteres jedoch nicht bei sensiblen Daten) getrennt vom Datenträger zu übermitteln.

7.9 Outsourcing

Situationsbeschreibung:	Auf der Suche nach finanziellen Einsparmöglichkeiten versprechen sich manche einen Vorteil, indem sie ihre Datenverarbeitung ganz oder teilweise an einen Auftragnehmer, meist ein externes Unternehmen, auslagern, auf neudeutsch outsourcen. Typische Unterstützungsleistungen des externen Partners können sein: - Datenerfassung - Mikroverfilmung - Vernichtung von Datenträgern - Wartung und Fernwartung (-->7.7) - Betrieb eines Netzwerks (LAN oder WAN) - Erbringung von Rechenzentrumsdienstleistungen - externe Archivierung (-->7.6) Wer ein Outsourcing beabsichtigt, muss zunächst einmal sehr genau prüfen, ob eine Verarbeitung personenbezogener Daten durch einen Auftragnehmer rechtlich überhaupt zulässig ist. Insbesondere sind die besonderen Berufs- und Amtsgeheimnisse und die daran geknüpften Verschwiegenheitspflichten zu berücksichtigen und zu wahren (z. B. ärztliche Schweigepflicht, Sozial-, Statistik- und Steuergeheimnis). Sofern die rechtlichen Voraussetzungen für das Outsourcing vorliegen, gehört zu einer datenschutzgerechten Realisierung, dass dem Auftragnehmer personenbezogene Daten nur in dem Umfang bekannt werden sollen, wie dies zur Erfüllung des Auftrags unerlässlich ist. Die Zugriffsmöglichkeiten des Auftragnehmers sind also auf das notwendige Minimum zu beschränken. Klassische Methoden der Zugriffsbeschränkung stoßen mitunter aber sehr rasch an ihre Grenzen, insbesondere dann, wenn dem Auftragnehmer weit reichende Administrationsberechtigungen übertragen werden müssen, weil er z.B. das lokale Computernetzwerk des Auftraggebers betreibt. Vor diesem Hintergrund kommt der Verschlüsselung von Daten eine wachsende Bedeutung zu, um Daten auf wirksame Weise vor Zugriffen des Auftragnehmers abzuschotten.
Auftretende IT-Sicherheitsprobleme:	Wegen der strengen vertraglichen Verpflichtungen, die ein Auftragnehmer gegen über dem Auftraggeber bei der Verarbeitung sensibler Daten eingehen muss, ist es meist entbehrlich, die Daten vor der Offenbarung gegenüber den Auftragnehmer zu schützen. Bei manchen besonderen Beruf- und Amtsgeheimnissen kommt es jedoch darauf an, die Daten auch vor Offenbarung an Dritte – dazu gehören auch externe Auftragnehmer - zu schützen. Außerdem kann in Betracht kommen, dass man dem Auftragnehmer nicht zutraut, für einen hinreichenden Schutz besonders sensibler Daten zu sorgen, so dass eine Verschlüsselung der Daten in Betracht zu ziehen ist, wenn der Auftragnehmer keinen Zugriff aus den Inhalt der Daten benötigt.
Lösungswege unter Anwendung kryptografischer Verfahren:	Inwieweit eine Verschlüsselung der Daten zum Schutz vor Zugriffen des Auftragnehmers in Betracht kommt, hängt also maßgeblich von der Art des erteilten Auftrags ab. Benötigt der Auftragnehmer keinen Zugriff auf den Inhalt der Daten, fungiert er typischerweise als Netzbetreiber (eines LAN oder WAN), als Vermittlungsstelle, die Daten annimmt und weiterverteilt oder als Archivbetrei-

	ber, der Daten aufbewahrt und bei Bedarf übermittelt. In diesen Fällen ist eine Verschlüsselung der Daten sowohl auf dem Übertragungsweg als auch bei der Speicherung möglich, z.B.: - Verschlüsselung des gesamten, zu übertragenden Datenstroms durch eine Hardware-Verschlüsselungsbox (-->5.5), die zwischen den Computer und den Netzanschluss geschaltet wird; - Ende-Ende-Verschlüsselung bei elektronischer Post (-->7.5), deren Inhalt der Auftragnehmer nicht kennen muss, um sie weiterzuverteilen; - Einsatz eines Verschlüsselungsprodukts, welches die verschlüsselte Speicherung von Daten auf dem Server ermöglicht; die Entschlüsselung von Daten erfolgt nur kurzzeitig auf dem Client während der Bearbeitung. Um den mit der Verschlüsselung beabsichtigten Schutz zu erzielen, darf das Schlüsselmanagement nicht dem Auftragnehmer übertragen werden. Sofern der Auftragnehmer Daten zu bearbeiten, zu verändern oder auszuwerten hat, benötigt er zumindest kurzzeitig Zugriff auf deren Inhalt. In Fällen, in denen der Auftragnehmer zur Erfüllung seiner Aufgaben keinen Personenbezug benötigt, ist eine Pseudonymisierung des gespeicherten Datenbestands angezeigt. Dieselbe Person soll dabei immer dasselbe Pseudonym erhalten, damit beispielsweise statistische Auswertungen korrekte Ergebnisse liefern und Daten, die zu unterschiedlichen Zeitpunkten zu einer Person anfallen, zusammengeführt werden können. Unterschiedliche Personen müssen dagegen auf unterschiedliche Pseudonyme abgebildet werden. Für die Generierung von Pseudonymen spielen kryptografische Funktionen, beispielsweise asymmetrische Verschlüsselungsverfahren, eine wichtige Rolle. Die Zusammenführung der pseudonymisierten mit den getrennt gespeicherten personenidentifizierenden Angaben darf dem Auftragnehmer nicht möglich sein, um den mit der Pseudonymisierung verfolgten Zweck nicht zu konterkarieren.

7.10 Außendienst und Telearbeit

Situationsbeschreibung:	Außendienst- und Telearbeitsplätze sind u.a. dadurch gekennzeichnet, dass die im jeweiligen Arbeitsumfeld benutzten IT-Systeme bzw. die darauf gespeicherten Daten der unmittelbaren Verfügungsgewalt des Arbeitgebers entzogen sind. In der häufig privaten Umgebung von Telearbeitsplätzen und im Außendienst entfällt die beaufsichtigende Wirkung des üblichen Büroumfeldes. Organisatorische Vorgaben des Arbeitgebers und Sicherheitsmaßnahmen sind u.U. nicht oder nur zum Teil umsetzbar.
Auftretende IT-Sicherheitsprobleme:	Der Zugang von Außendienst- und Telearbeitsplätzen zu IT-Systemen des Arbeitgebers erfolgt in der Regel über öffentliche Kommunikationsverbindungen (z.B. ISDN, Internet), deren Nutzung grundsätzlich nicht auf einen festgelegten Teilnehmerkreis beschränkt ist, sondern einer Vielzahl von Teilnehmern offen steht. Welche Übertragungswege genutzt werden und welches Sicherheitsniveau dabei gewährleistet ist, entzieht sich in der Regel der Kenntnis und der Einflussmöglichkeiten der Nutzer. Im Klartext übertragene Inhalte sowie Zugangskennungen und Passworte stehen damit potentiell im Zugriff Unbefugter. Darüber hinaus unterliegen Kommunikationsanschlüsse im Privatbereich potentiell größeren Gefährdungen.
Lösungswege unter Anwendung kryptografischer Verfahren:	Der Sicherheitsstandard ausgelagerter Arbeitsplätze muss hinsichtlich der Verarbeitetung personenbezogener Daten mindestens dem der regulären Büroarbeitsplätze des Arbeitgebers entsprechen. Schutz vor unbefugter Kenntnisnahme gewährleisten dabei insbesondere kryptografische Verfahren. Je nach genutztem Kommunikationsdienst kommen Ende-zu-Ende-Lösungen auf Anwendungsebene oder eine Leitungsverschlüsselung auf der Ebene der Netzwerk- oder Kommunikationsprotokolle in Betracht. Soweit die Kommunikation via E-Mail vorgesehen ist, sind die hierzu genannten Empfehlungen zu Grunde zu legen (--> 7.5). Bei Client-Server-Lösungen auf der Basis von Internetprotokollen stehen für die Einrichtung vertrauenswürdiger Kommunikationsverbindungen Protokollerweiterungen wie S-HTTP (--> G), SSH (--> G) oder insbesondere SSL(--> G) zur Verfügung. Diese ermöglichen die Nutzung von Standardsoftware und -diensten bei gleichzeitiger Verschlüsselung der Kommunikation zwischen Client und Server. Alternativ, oder soweit die Anbindung ausgelagerter Arbeitsplätze über proprietäre Protokolle erfolgt, kann die notwendige Vertraulichkeit und Integrität mit Tunneling-Lösungen (-->5.1) bzw. den Aufbau Virtueller Privater Netze (-->6.3) sichergestellt werden. Der Einsatz kryptografischer Verfahren erlaubt je nach gewählter Lösung zudem eine verlässliche Authentisierung der an der Kommunikation beteiligten Komponenten.
Besondere Hinweise:	Bei Telearbeit und Außendienst im Rahmen eines Arbeits- oder Dienstverhältnisses handelt es sich um Datenverarbeitung des jeweiligen Arbeitgebers. Dieser bleibt weisungsbefugt und bestimmt die Art und Weise der Aufgabenerfüllung. Die Entscheidung über die erforderlichen Maßnahmen liegt nicht im Ermessen oder der Verantwortung des jeweiligen Arbeitnehmers. Für die Ausstattung, Konfiguration und Nutzung von Außendienst- und Telearbeitsplätzen sollten daher explizite Festlegungen im Rahmen

	einer Dienstanweisung getroffen werden. Neben den kryptografischen Aspekten andere technische sowie organisatorische Maßnahmen von Bedeutung. Die Datenschutzbeauftragten des Bundes und der Länder haben hierzu entsprechende Empfehlungen ausgesprochen.

Anhang 1 Glossar

Access Point Gerät, mit dem die Distanz der Funknetze erweitert werden kann. Über Access Points (AP) werden Funk-LANs mit einem drahtgebundenen Ethernet verknüpft.

AES *Advanced Encryption Standard*

AES tritt als Verschlüsselungsstandard die Nachfolge des wegen der kurzen Schlüssellänge nicht mehr zeitgemäßen *DES*-Verfahrens (-->G) an.

Algorithmus Beschreibung einer Verfahrensweise zur Lösung eines (mathematischen) Problems. Im Zusammenhang mit der *kryptografischen Verschlüsselung* steht der Begriff für die Art und Weise in der ein Klartext in ein *Chiffrat* umgewandelt wird und umgekehrt. Bekannte Algorithmen sind *DES*, *RSA*, oder *IDEA.*

Asymmetrische Verschlüsselung Kryptografisches Verfahren, bei der zwei Schlüssel, ein öffentlicher und ein *geheimer Schlüssel*, verwendet werden. Der öffentliche Schlüssel ist jedem zugänglich, der geheime nur dem jeweiligen Empfänger einer Nachricht. Die Verschlüsselung folgt dabei folgendem Konzept: Wird mit dem *öffentlichen Schlüssel* des Empfängers verschlüsselt, kann die Nachricht nur mit dem geheimen Schlüssel des Empfängers entschlüsselt werden. Mit umgekehrter Verwendung der Schlüssel lässt sich die elektronische Signatur realisieren. Wird dabei mit dem geheimen Schlüssel des Absenders signiert, kann die Signatur anhand des öffentlichen Schlüssel des Absenders überprüft werden. Beispiele für asymmetrische Verfahren sind *RSA* und *DSS*.

Authentisierung Formeller Nachweis der Berechtigung zur Benutzung eines IT-Systems oder von dessen Ressourcen. Die Authentisierung erfolgt in Verbindung mit der *Identifikation* zumeist im Rahmen der Anmeldung an einem IT-System. Die Eingabe eines gültigen Passwortes ist ein Beispiel für eine Authentisierung.

Authentizität Verlässliche Zurechenbarkeit einer elektronischen Nachricht zu einem bestimmten Absender.

BOS Behörden und Organisationen mit Sicherheitsaufgaben

Brute-Force-Angriff Versuch, verschlüsselten Text durch das Durchprobieren des gesamten Schlüsselraums zu entschlüsseln.

Challenge Response-Verfahren Verfahren zur gegenseitigen Authentisierung von IT-Systemen (siehe 5.3)

CHAP Challenge Handshake Authentication Protocol. Automatisches Verfahren zur *Authentisierung* bei welchem dem rufenden Anschluss eine binäre Zufallszahl (challenge) zur Verfügung gestellt wird. Diese wird mit einem vorgegebenen *Algorithmus* verarbeitet und das Ergebnis dem gerufenen Anschluss übermittelt. Entspricht das Zurückgelieferte dem erwarteten Ergebnis, wird die Verbindung hergestellt.

Chiffrat Ergebnis einer *kryptografischen Verschlüsselung*, d.h die mittels *Algorithmus* und Schlüssel verschlüsselten Daten.

CUG Closed User Group (Geschlossene Benutzergruppe). Leistungsmerkmal von Kommunikationsdiensten, bei welchem die zugelassenen Anschlüsse in ei-

ner Berechtigungstabelle eingetragen werden. Kommunikationsanforderungen von in dieser Tabelle nicht enthaltenen Anschlüssen werden zurückgewiesen.

DES Data Encryption Standard. Von IBM in den 70er Jahren entwickeltes symmetrisches Verschlüsselungsverfahren. Bei DES werden Datenblöcke zu je 64 Bits mit einem 56-Bit-Schlüssel codiert. DES ist weit verbreitet und wurde mit der Standardschlüssellänge bereits kompromittiert, d.h. innerhalb überschaubarer Zeit entschlüsselt. Höhere Sicherheit bietet Triple DES (DES 3) bei welchem drei Verschlüsselungsrunden aufeinander folgen.

Digitale Signatur = Elektronische Signatur (-->G)

DSS Digital Signature Standard. Ein kryptografisches Verfahren für die d*igitale Signatur*.

ELCRODAT 6-2 Das Gerät ELCRODAT 6-2, mit dem Telefonate, Faxe, Daten und Videokonferenzen verschlüsselt und somit sicher übertragen werden können, ist mit einem hochmodernen Schlüssel- und Zertifikatsmanagement ausgestattet und erlaubt die unabhängige Verschlüsselung von bis zu 30 ISDN-Kanälen. Zwischen ISDN-Netz und Endgerät geschaltet, dechiffrieren diese Verschlüsselungsgeräte die zu übermittelnden Daten transparent und somit nicht als verschlüsselt erkennbar für die anderen ISDN-Komponenten.

Elektronische Signatur "Elektronische Unterschrift". Verfahren bei welchem durch die Verwendung *asymmetrischer Verschlüsselungsverfahren,* meist in Kombination mit *Hash-Verfahren* die *Integrität* und *Authentizität* einer elektronischen Nachricht sichergestellt werden kann. Eine gesetzliche Sicherheitsvermutung besteht für qualifizierte Signaturen nach dem Signaturgesetz.

Ende-zu-Ende-Verschlüsselung Verschlüsselung des Datenverkehrs zwischen den Kommunikationsteilnehmern. Die Ende-zu-Ende-Verschlüsselung erfolgt im Gegensatz zur *Leitungsverschlüsselung* auf der Anwendungsebene, d.h. bei der Nutzung von Programmen. So muss z.B. eine e-Mail-Nachricht als solche explizit verschlüsselt werden.

Firewall Sicherheitssystem zum Schutz von sicheren Netzdomänen gegenüber Angriffen aus unsicheren Netzdomänen (i.d.R. Absicherung von lokalen Netzen gegenüber dem Internet bzw. anderer Wide Area Networks). Firewalls setzen die Sicherheitspolitik des Betreibers der sicheren Domäne technisch um, in dem sie nur solche Dienste für die Kommunikation an der Schnittstelle zulassen, die ausdrücklich gewünscht sind.

Geheimer Schlüssel siehe *Private Key.*

Geschlossene Benutzergruppe siehe *CUG.*

GRE *Generic Routing Encapsulation*

Der Aufbau von Tunnelpaketen ist u.a. in der von der Firma 3COM entwickelten Generic Routing Encapsulation-Definition(GRE, RFC 1701, RFC 1702) beschrieben. In GRE werden drei Abschnitte unterschieden:

- die *Payload*, d.h. das ursprüngliche Datenpaket einschließlich der Quell- und Zieladresse als Nutzlast,

- den *GRE-Header* mit Informationen über das verwendete Tunneling-Protokoll und die kryptografischen Informationen sowie,

- den *Network-Header* mit den Adressangaben der Tunnel-Komponenten.

Bei GRE handelt es sich weniger um eine konkretes Kommunikationsprotokoll, als vielmehr um einen Vorschlag für den logischen Aufbau eines Tunnels. Die gängigen Protokolle berücksichtigen jedoch die GRE-Empfehlungen.

Hash-Verfahren/ Hashfunktion Mathematisches Verfahren mit dem ein (langes) elektronisches Dokument auf eine (kurze) Prüfsumme abgebildet wird. Änderungen am Dokument, auch geringste, führen bei erneutem "hashen" zu einer anderen Prüfsumme. Hashverfahren werden im Rahmen der d*igitalen Signatur* für den Nachweis der Integrität einer Nachricht benötigt.

Hashwert Prüfsumme als Ergebnis eines Hash-Vorgangs.

HBCI *Homebanking Computer Interface*

Sicherheitsstandrad für das elektronische Banking der deutschen Kreditwirtschaft unter Verwendung kryptografischer Funktionen (-->www.hbci.de)

Hybrides Verschlüsselungsverfahren Hybride Verschlüsselungsverfahren kombinieren die Vorteile symmetrischer und asymmetrischer Verschlüsselungsverfahren. Dabei wird für jede Sitzung ein Schlüssel (Session-Key) zufällig generiert und asymmetrisch verschlüsselt ausgetauscht. Die Daten selbst werden dann durch einen schnellen symmetrischen Algorithmus mit dem Session-Key verschlüsselt (-->3.2).

IDEA International Data Encryption Algorithm. *Ein symmetrisches Verschlüsselungsverfahren* mit einer Schlüssellänge von 64 bzw. 128 Bit.

Identifikation Nachweis über die Identität eines Benutzers eines IT-Systems, z.B. anhand einer Benutzerkennung (User-ID). Die Identifikation erfolgt in Verbindung mit der *Authentisierung* zumeist im Rahmen der Anmeldung an einem IT-System.

Integrität Unversehrtheit und Vollständigkeit der in elektronischer Form gespeicherten oder übermittelten Daten. Der Nachweis der Integrität einer elektronischen Nachricht, z.B. mittels *Hash-Verfahren*, stellt sicher, dass diese während der Übertragung nicht verändert wurde.

IPSec Bei *IPSec* handelt es sich um einen von der IETF vorgeschlagenen Internet-Standard. Es besteht aus einem Paket von Protokollen (RFC 1825-1829) die die Aspekte Authentisierung, Integrität und Vertraulichkeit abdecken und arbeitet auf der Netzwerkschicht - Schicht 3 - des OSI-Referenzmodells. IPSec basiert auf dem IP-Protokoll Version 4 (IPv4) und ist Bestandteil von IPv6. Der IPSec-Standard wird ergänzt durch zwei Substandards, SKIP (Simple Key Management for Internet Protocol) und ISAKMP (Internet Security Association and Key Management Protocol).

IPSec deckt verschiedene Anwendungsbereiche ab; u.a. stellt es einen sog. Tunnelmodus zur Verfügung. Dabei wird das komplette ursprüngliche IP-Paket verschlüsselt und mit einem neuen IP-Header sowie einem IPSec-Header für die kryptografischen Verfahren (*Authentication Header* und *En-*

capsulation Payload Header) versehen. Im Zielnetz werden der neue IP-Header entfernt, die Authentisierungsangaben geprüft, das ursprüngliche IP-Paket wiederhergestellt und zur eigentlichen Zieladresse weitergeleitet.

Die Informationen zu den jeweils verwendeten kryptografischen Algorithmen sind in den IPSec-Headern enthalten und implentierungabhängig. Grundsätzlich stehen zur Verschlüsselung DES (56 Bit), Triple-DES (168 Bit) und IDEA (128 Bit) und zur Prüfsummenbildung MD 5 zur Verfügung.

Key Recovery Verfahren zur Rekonstruktion von Schlüsseln ohne Mitwirkung des Schlüsselbesitzers.

Krypto-Box Komponente, die entsprechend voreingestellter Parameter für eine Kommunikationsverbindung eine kryptografische Absicherung gewährleistet. Sie erfordert empfängerseitig eine entsprechende Gegenstelle. Kryptoboxen machen benutzerseitige Eingriffe für eine Verschlüsselung oder Integritätssicherung i.d.R. entbehrlich.

Kryptografische Verschlüsselung Verfahren, bei welchem mit Hilfe eines kryptografischen Algorithmus (-->G) Klartexte in ein Chiffrat (-->G) umgewandelt, d.h. verschlüsselt werden. Die Wiederherstellung des ursprünglichen Klartextes ist nur mit Kenntnis des jeweiligen Schlüssels möglich.

L2TP *Layer 2 Tunneling Protocol*

L2TP vereint PPTP und das von Cisco entwickelte Layer 2 Forwarding Protocol (L2F) und unterscheidet sich nur wenig von PPTP. So unterstützt es u.a. mehrere Tunnel gleichzeitig. Das Protokoll bietet starke Authentisierung sowohl für SLIP- als auch PPP-Verbindungen, indem es das zur Übertragung von ISDN- und Modem-Daten verwendete HDLC-Protokoll (High Level Data Link Control) tunnelt. L2TP eignet sich damit im Gegensatz zu PPTP nur für Wählverbindungen. Zur Datenverschlüsselung greift L2TP optional auf IPSEC-Mechanismen (ESP) zurück.

Die genannten Protokolle werden in vielen Fällen von den Netzwerkkomponenten gängiger Hersteller unterstützt. Entsprechende Client-Software ist häufig bereits in den Betriebssystemen enthalten. Je nach Anforderung sollte darauf geachtet werden, dass die verwendeten kryptografischen Algorithmen und Schlüssellängen den Empfehlungen der Datenschutzbeauftragten entsprechen.

Leitungsverschlüsselung Verschlüsselung des Datenverkehrs auf der physikalischen Ebene zwischen den Anschlusskomponenten einer Kommunikationsverbindung (Leitung oder Funkstrecke). Die Leitungsverschlüsselung erfolgt im Gegensatz zur *Ende-zu-Ende-Verschlüsselung* unabhängig von der jeweiligen Anwendung (z.B. e-Mail). Sie wird i.d.R. über technische Komponenten (Verschlüsselungsboxen, Router) realisiert und erfasst alle Datenübertragungen auf der betroffenen Kommunikationsverbindung. Ein Zutun des Benutzers ist anders als bei der Ende-zu-Ende-Verschlüsselung nicht erforderlich.

MAC-Adresse *Media Access Control-Adresse*

Adresse für den Netzwerkzugang von Rechnern (Adresse der Netzkarte)

MailTrusT Siehe SPHINX/MailTrusT

Man-in-the-Middle Attack Bezeichnung für alle Formen der Angriffe auf die Sicherheit der Kommunikation zwischen Sender und Empfänger durch Zwischenschaltung des Angreifers während der Kommunikation

Message Authentication Code Angabe anhand derer die *Authentizität* einer Nachricht überprüft werden kann.

Öffentlicher Schlüssel siehe *Public Key*.

PAP *Password Authentication Protocol*

Kommunikationsprotokoll bei dem die *Authentisierung* über Passworte erfolgt. Das Passwort wird allerdings unverschlüsselt übertragen.

PGP *Pretty Good Privacy*

Bei Pretty Good Privacy - PGP - handelt es sich um ein für die nicht kommerzielle Nutzung lizenzfreies Produkt. Als solches ist es im privaten Bereich häufig vorhanden und im Internet frei verfügbar. Für die kommerzielle Nutzung ist eine Lizenzierung erforderlich, diese ist jedoch nur mit geringen Gebühren verbunden. Aufgrund dessen ist PGP für die gesicherte E-Mail-Kommunikation im Internet derzeit eine der am weitesten verbreiteten Lösungen. PGP ermöglicht sowohl eine Verschlüsselung zur Wahrung der Vertraulichkeit als auch die Digitale Signatur als Nachweis der Authentizität einer Nachricht. Die Anwendung ist auf einer Reihe von Plattformen Verfügbar (u.a. Windows 95/98/NT/XP, MacOS, UNIX) und kann in eine Vielzahl gängiger E-Mail Lösungen eingebunden werden. Zusätzlich kann PGP für die verschlüsselte Speicherung von Dateien verwendet werden.

PGP ist in verschiedenen Versionen verfügbar, die sich in der Handhabung und den eingesetzten Algorithmen unterscheiden. Ältere Versionen verwendeten ausschließlich das RSA-Verfahren (-->G), später - ab Version 5 - kamen der Digital Signature Standard (DSS) (-->G) und der Schlüsselaustausch nach dem Diffie-Hellmann-Verfahren (DH) hinzu. Die mit zurückliegenden Versionen (z.B. 2.6.3i) erzeugten RSA-Schlüssel sind jedoch auch in höheren Versionen (ab 5.xx) verwendbar, umgekehrt gilt dies jedoch nicht. Detaillierte Hinweise zur Interoperabilität können der PGP-Homepage *www.pgpi.com* entnommen werden. Auch PGP arbeitet als Hybridverfahren (-->G), bei welchem die eigentliche Verschlüsselung mit symmetrischen Algorithmen erfolgt (z.B. IDEA (-->G) oder Triple DES (-->G)).

Die von PGP verwendeten Algorithmen sind die gleichen wie in vielen kommerziellen Produkte; sie gelten bei Wahl einer ausreichenden Schlüssellänge (mind. 1.024 Bit) gegenwärtig als ausreichend sicher. Voraussetzung hierfür ist, das eine international verfügbare PGP-Version eingesetzt wird, die keinen Exportbeschränkungen unterliegt; bei anderen Versionen ist u.U. die nutzbare Schlüssellänge beschränkt.

PKI ***Public Key Infrastructure***

Gesamtheit der für die Verwendung von *Public Key*-Verfahren erforderlichen Komponenten und Dienste (u.a. Schlüsselerzeugung, Zertifizierungs-, Verzeichnis-, Sperr- und Zeitstempeldienste)

PPTP *Point to Point Tunneling Protocol*

PPTP ist eine federführend von Microsoft entwickelte Erweiterung des Point-to-Point Protokolls PPP und arbeitet auf der Verbindungsschicht - Schicht 2 - des OSI-Referenzmodells. PPTP kapselt, ähnlich wie IPSec, PPP-Pakete. Auf diese Weise können Netzwerkprotokolle wie IP, IPX und NetBEUI getunnelt werden. Für die Zugangskontrolle stehen das Password Authentication Protocol (PAP) sowie das Challenge Handshake Protocol (CHAP) zur Verfügung. Als kryptografische Algorithmen werden RC4 und DES mit, implementierungsabhängig, Schlüsseln zwischen 40 und 128 Bit Länge verwendet.

PPTP setzt sich aus vier Schichten zusammen. Die oberste Schicht bildet ein Zustellungskopf, der aus dem Netzwerkprotokoll des WAN besteht, über den das Corporate Network aufgebaut wird. Der darunter liegende Aufbau basiert auf den GRE- Empfehlungen und entspricht logisch der IPSec-Struktur.

Pretty Good Privacy siehe *PGP.*

Private Key Geheimer Schlüssel. Der Teil eines Schlüsselpaares im Rahmen eines *asymmetrischen Verschlüsselungsverfahrens*, der nur dem Empfänger einer verschlüsselten Nachricht bzw. dem digital Signierenden bekannt sein darf. Der geheime Schlüssel dient der Entschlüsselung einer mit dem *öffentlichen Schlüssel* des Empfängers verschlüsselten Nachricht. Eine mit einem geheimen Schlüssel erzeugte Signatur kann nur mit dem öffentlichen Schlüssel des Erzeugers der Signatur verifiziert werden.

Protokoll Technische Regelung über den Aufbau und die Größe von Datenpaketen und die Art und Weise, wie diese im Rahmen einer Kommunikation übertragen werden.

Public Key Öffentlicher Schlüssel. Der Teil eines Schlüsselpaares im Rahmen eines *asymmetrischen Verschlüsselungsverfahrens* der allen Teilnehmern bekannt sein muss. Zum Verschlüsseln wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Die Entschlüsselung erfolgt durch den Empfänger mit dessen *geheimen Schlüssel*. Bei der digitalen Signatur wird durch den Absender mit dessen geheimen Schlüssel signiert, und die Signatur beim Empfänger mit dem öffentlichen Schlüssel des Absenders verifiziert.

Replay Attack Variante des Man-in-the-Middle-Angriffs, bei der die Kommunikation eines Nutzers, insbesondere seine Authentisierungsdaten (Kennung, Passwort) mitgeschnitten und später wieder eingespielt werden, so dass sich der Angreifer die Rechte des Nutzers verschaffen kann.

Router Technische Komponente, die die Wegefindung (routing) und Übermittlung in einem Netzwerk steuert. Mit routing bezeichnet man den Weg der Datenpakete innerhalb von Netzen. Das Internet kennt keine Direktverbindungen zwischen Rechnern. Statt dessen erfolgt der Versand von Daten in kleinen Paketen und nach Bedarf über verschiedene Zwischensysteme auf dem zum Übermittlungszeitpunkt günstigsten Weg. Diese Form des Datenverkehrs ermöglicht die hohe Flexibilität und Ausfallsicherheit des Internet.

RSA Aus den Anfangsbuchstaben der Erfinder (Rivest, Shamir und Adleman) zusammengesetzte Bezeichnung für ein *asymmetrisches Verschlüsselungsver-*

fahren.

Schlüsselpaar Das Paar aus geheimem und öffentlichem Schlüssel bei *asymmetrischen Verschlüsselungsverfahren*.

Session Key Kryptografischer Schlüssel, der nur für eine bestimmte Zeit (Session) verwendet wird und danach seine Gültigkeit verliert.

S-HTTP ***Secure Hypertext Transfer Protocol***

Das Protokoll S-HTTP, das von der Firma Enterprise Integration Technologies entwickelt und im RFC 2660 spezifiziert wurde, stellt eine Erweiterung des http-Protokolls dar und wird nur für http-Verbindungen verwendet. Es bietet folgende Funktionalität:

- Verwendung eines symmetrischen Verschlüsselungsverfahrens zur Verschlüsselung des Datenstroms
- Schlüsselaustausch des Schlüssel für das symmetrische Verfahren durch das Verfahren nach Rivest-Shamir-Adleman (RSA)
- Die Verschlüsselung wird dadurch erreicht, dass die Dokumentbeschreibung einer URL mit der Endung "shtml" spezifiziert wird
- Im Gegensatz zu SSL wird bei S-HTTP jede Nachricht (http-request) einzeln verschlüsselt

Durch die letztgenannte Funktionalität ist es mit dem Protokoll S-HTTP zwar möglich, jede Nachricht einzeln digital zu signieren. Andererseits ergibt sich als Konsequenz, dass das Verfahren für den jeweiligen Schlüsselaustausch erheblichen Zusatzaufwand auf der Protokollebene gegenüber dem Protokoll SSL mit sich bringt.

Signaturgesetz Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16. Mai 2001, BGBl. I, S. 876

S/MIME ***Secure Multipurpose Internet Mail Extension***

Verbreiteter Standard für die Verschlüsselung von E-Mails.

Das S/MIME-Protokoll erweitert den vorhandenen Internet-Standard MIME (RFC 2045ff) um kryptografische Funktionen zur Verschlüsselung und zur digitalen Signatur. S/MIME verfolgt dabei einen weitgehend produkt- und plattformunabhängigen Ansatz und basiert auf dem Nachrichtenformat CMS des Public Key Cryptography Standard Teil 7 (PKCS#7, RFC 2315).

Bei PKCS handelt es sich um eine Reihe von Spezifikationen, die von der Firma RSA Data Security herausgegeben wurden. Sie befassen sich mit der Erzeugung und Verwendung von digitalen Signaturen und den zugehörigen Zertifikaten. Wesentliche Spezifikationen sind

PKCS #1	RSA Encryption Standard (Definition RSA Algorithmus)
PKCS #3	Diffie-Hellman Key-Agreement Standard (Schlüsselaustausch)
PKCS #7	Cryptografic Message Syntax Standard (Nachrichtenformat)
PKCS #11	Cryptografic Token Interface Standard (Schnittstelle Schlüs-

selverarbeitung)

Für die Verschlüsselung von Nachrichten erlaubt S/MIME den Einsatz verschiedener Algorithmen, u.a. Triple DES (--> G) und RC2, letzteren allerdings mit lediglich 40 Bit Schlüssellänge. Die Erweiterung um zusätzliche Algorithmen ist möglich, sofern Sender und Empfänger diese unterstützen. S/MIME erlaubt wahlweise jeweils die Verschlüsselung oder Signatur eine Nachricht bzw. beides gemeinsam. S/MIME- Erweiterungen sind für diverse E-Mail Clients und -Server verfügbar. Die aktuellen Versionen der Browser Netscape Communicator und Microsoft Internet Explorer unterstützen ebenfalls S/MIME.

Die Signaturzertifikate entsprechen dem Standard ITU-X.509.

SPHINX/MailTrusT

In dem vom Bundesamt für Sicherheit in der Informationstechnik (BSI) betreut Pilotversuch SPHINX (beendet Ende 2000) wurden Produkte verschiedener Hersteller zur Realisierung einer Ende-zu-Ende-Sicherheit im Bereich der öffe lichen Verwaltung erprobt. Die Sicherheit wird durch den Einsatz marktgängige Softwareprodukte realisiert. Diese basieren auf der MailTrusT-Spezifikation de TeleTrusT e.V., eines Zusammenschlusses von Vertretern aus Forschung und Industrie. Die MTT-Spezifikation ist ein deutsche Entwicklung, die bislang auf dem Standard Privacy Enhanced Mail (PEM) beruht. Die Spezifikation definier ein interoperables Datenaustauschformat für signierte und verschlüsselte Date Insbesondere berücksichtigt sie die Verarbeitung binärer Daten, so dass beliel ge Dateien als E-Mail Anlagen gesichert übertragen werden können.

Über die in der Spezifikation festgelegten gemeinsamen Anforderungen soll di Interoperabilität der Produkte hinsichtlich Verschlüsselung und Digitaler Signat sichergestellt werden. Im Wesentlichen handelt es sich dabei um Festlegunge hinsichtlich der Zertifikats- und Nachrichtenformate, der verwendeten Algorithmen, der Zertifikatsverwaltung sowie der Anforderungen an die Komponenten einer Private Key Infrastruktur (PKI (-->G)).

Gegenwärtig wird die Bundesverwaltung (Grundlage: Regierungsbeschluss vo 16. Januar 2002) und teilweise bereits auch Landesverwaltungen mit diesen Technologien ausgestattet.

Die Einhaltung der MailTrusT-Spezifikationen wird durch eine SPHINX-Freigab bestätigt.

SSH

Secure Shell Remote Login

SSH ist ein Software-Paket, das anstelle der Dienste Telnet und FTP sowie anstelle der Kommandos rlogin, rsh und rcp verwendet werden kann und mit dem man durch kryptografische Verfahren eine zuverlässige gegenseitige Authentisierung und eine Verschlüsselung des gesamten Datenstroms auf der Transportschicht erreichen kann. Dabei werden statt rlogin, rsh und rcp die Programme slogin, ssh und scp eingesetzt.

Mit SSH wird die

- automatische und transparente Verschlüsselung der Verbindungen,
- entfernte Terminalsitzung und Kommandoausführung sowie Datei-

übertragung über verschlüsselte Kommunikationskanäle,

- transparente Verschlüsselung beliebiger TCP/IP-Kommunikationsendpunkte (sog. ports) und für beliebige Protokolle wie beispielsweise X11, DNS über sichere Kommunikationskanäle sowie die

- starke Authentifizierung der Kommunikationspartner

realisiert.

Zur Authentifizierung wie auch zum Austausch der Schlüssel für die symmetrischen Verschlüsselungsverfahren verwendet SSH RSA (--> G).

Als symmetrische Verschlüsselungsverfahren unterstützt das Protokoll SSH Verschlüsselungsalgorithmen wie beispielsweise DES (--> G), Triple DES (--> G), IDEA (--> G), RC4. Neben einer Open-Source-Implementierung bietet die Firma SSH Communications Security eine kommerzielle Implementierung des Protokolls und Support an. Für alle gängigen Plattformen (Windows, Apple, Unix) werden kommerzielle Client- und Server-Implementierung angeboten.

SSL ***Secure Socket Layer***

SSL ist ein von der Fa. Netscape entwickeltes Sicherheitsprotokoll, dass insbesondere im Zusammenhang mit finanziellen Transaktionen Bedeutung erlangt hat. Mit dem von der Firma Netscape entwickelten SSL und seiner Weiterentwicklung Transport Layer Security (TLS) (--> G), sind transportorientierte Sicherheitsprotokolle entwickelt worden, die in gängigen WWW-Browsern unterstützt werden.. Das SSL-Protokoll realisiert folgende Funktionalität:

- eine verschlüsselte Übertragung von Daten zwischen einem WWW-Browser und einem WWW-Server,

- eine Überprüfung, ob die übermittelten Daten vollständig und korrekt übertragen wurden

- eine Authentifikation des Servers gegenüber dem Client anhand eines Server-Zertifikats

- eine Authentifikation des Clients gegenüber dem Server, sofern auch der Client über ein Zertifikat verfügt.

Das Protokoll SSL kommt vorwiegend bei der Nutzung des WWW zum Einsatz. Grund dafür ist, dass sowohl marktgängige WWW-Browser als auch marktgängige Software für WWW-Server SSL standardmäßig unterstützen. Der Nutzer erkennt die Verwendung von SSL innerhalb einer WWW-Sitzung daran, dass anstelle der Zugriffsmethode http die Methode https verwendet wird. Das Protokoll SSL ist, da es zwischen der Transportschicht (TCP/IP) und der Anwendungsschicht eingebettet ist, für Anwendungen transparent. Lediglich beim Zertifikataustausch muss der Nutzer die Akzeptanz bestätigen. Der Einsatz von SSL ist damit nicht auf http-Clients und -Server beschränkt. Auch Anwendungen wie Telnet oder FTP können per SSL gesichert werden. Dies erfordert allerdings eine Anpassung der verwendeten Clients und Server.

SSL basiert auf einem hybriden kryptographischen Verfahren: Die Verschlüsselung der Daten erfolgt mit Hilfe eines symmetrischen Verfahrens; der für jede Sitzung zwischen Server und Client neu ausgehandelte symmetrische Schlüssel wird asymmetrisch mit Hilfe von RSA-Schlüsseln (--> G) verschlüsselt und zwischen Client und Server ausgetauscht. Als symmetrische Verschlüsselungsverfahren unterstützt der Standard verschiedene Verschlüsselungsalgorithmen wie IDEA (--> G), DES(--> G), Triple-DES (--> G) und RC4. Welcher Algorithmus verwendet wird, handeln Client und Server beim Verbindungsaufbau jeweils aus. Die Authentifikation beruht auf Zertifikaten nach dem Standard X.509.

Mit dem Protokoll SSL ist es nicht möglich, zu übertragende Dokumente einzeln mit einer digitalen Signatur zu versehen. Vielmehr wird die Verbindung zwischen Client und Server komplett gesichert. Während einer bestehenden Verbindung reicht SSL die übertragenen Daten unverschlüsselt und unsigniert an die Anwendung weiter. Die Prüfung, ob die übertragenen Daten authentisch sind, ist damit nur zum Zeitpunkt des Empfangs, nicht dagegen zu einem späteren Zeitpunkt, möglich.

Ein gravierender Nachteil von Protokolls SSL war, dass aufgrund US-amerikanischer Ausfuhrbeschränkungen Exportversionen der Browser lediglich eine 40-Bit-Verschlüsselung ermöglichten. Dieser Schwachpunkt ist mittlerweile entfallen. Allerdings unterstützten nur die neueren Versionen die 128-Bit-Verschlüsselung.

Standleitung

Kommunikationsverbindung die im Gegensatz zu einer *Wählleitungsverbindung* permanent und in der Regel exklusiv für bestimmte Teilnehmer geschaltet ist.

Symmetrische Verschlüsselung

Verschlüsselungsverfahren, bei welchem im Gegensatz zu *asymmetrischen Verfahren* für die Ver- und Entschlüsselung der gleiche Schlüssel verwendet wird. Dieser muss damit dem Empfänger einer Nachricht auf einem zweiten sicheren Kanal zugeleitet werden.

TLS

Transport Layer Security

Das TLS-Protokoll ist eine Weiterentwicklung von SSL (--> G) und hat mit dem RFC 2246 eine Standardisierung erfahren. Es ist abwärtskompatibel zu SSL.

Tunneling

Verfahren zur Absicherung einer Datenübertragung über unsichere oder nicht vertrauenswürdige Kommunikationsverbindungen mit Hilfe kryptografischer Verfahren.

Triple DES

Verfahren, bei welchem der Verschlüsselungsalgorithmus *DES* in drei aufeinanderfolgenden Durchgängen durchlaufen wird. Triple DES bietet eine höhere Sicherheit gegenüber Entschlüsselungsversuchen als der einfache *DES*.

Trust-Center

Stelle, die im Rahmen des Einsatzes von Verschlüsselungsverfahren zentrale Funktionen wahrnimmt. Beispiele hierfür sind die Erzeugung kryptografischer Schlüssel, die Erteilung und Verwaltung von *Zertifikaten* sowie der Betrieb von *Verzeichnisdiensten*

Verzeichnisdienst Serverdienst in welchem Personen und Ressourcen mitsamt zugehörigen Attributen katalogisiert werden. Verzeichnisdienste werden z.B. als Adressverzeichnisse für die elektronische Post oder im Rahmen des Einsatzes von Signatur und Verschlüsselungsverfahren für die Verwaltung von *Zertifikaten* eingesetzt.

VPN *Virtuelles Privates Netz*

Logisches Netz auf physikalischen Kommunikationsverbindungen. Die *VPN*-Technologie ermöglicht es, verschiedene, die gleiche Infrastruktur nutzenden Netze gegeneinander abzuschotten.

WEP *Wired Equivalent Privacy*

Speziell in Wireless LANs verwendetens Verschlüsselungsverfahren (mit inzwischen erkannten mathematischen Schwächen).

Wireless LAN Drahtloses lokales Netz. Es folgt in der Regel dem Standard IEEE 802.11b. Die Clients kommunizieren über Funk mit Access Points, die den Übergang zum festen Netzbereich mit den Servern darstellen.

Zertifikat Ein Zertifikat ist eine elektronische Bescheinigung, mit der ein Signaturprüfschlüssel (öffentlicher Schlüssel) einer Person zugeordnet und die Identität dieser Person bestätigt wird. Zertifikate werden von Zertifizierungsanbietern ausgestellt.

Anhang 2 Abkürzungsverzeichnis

Nicht aufgenommenen sind Abkürzungen, die nur in einem bestimmten Kapitel verwendet und dort erklärt werden, sowie allgemein bekannte Abkürzungen

Stand: 30. Mai 2003

AO	Abgabenordnung
B2B	Business to Business (Kommunikationsbeziehung unter Wirtschaftsunternehmen)
B2C	Business to Customer (Kommunikationsbeziehung zwischen Wirtschaftsunternehmen und ihren Kunden)
B2G	Business to Government (Kommunikationsbeziehung zwischen Wirtschaftsunternehmen und Behörden)
BDSG	Bundesdatenschutzgesetz
CA	Certificate Authority (Zertifizierungsstelle)
CAST	Carlisle Adams Stafford Tavares (symmetrischer Verschlüsselungsalgorithmus, benannt nach dem Erfinder)
CD-ROM	Compact Disc Read Only Memory (optischer Datenspeicher)
CMS	Cryptographic Message Syntax (Nachrichtenformat bei PKCS#7)
DES	Data Encryption Standard (symmetrisches Verschlüsselungsverfahren) (-->G)
DFÜ	Datenfernübertragung
DSS	Digital Signature Standard (-->G)
DUD	Datenschutz und Datensicherheit, Zeitschrift
DVD	Digital Versatile Disk (Nachfolger der CD)
E-Banking	Electronic Banking
ECC	Elliptic Curve Crytography, (Kryptografie auf der Basis elliptischer Kurven)
E-Commerce	Electronic Commerce
ElGamal	Asymmetrischer Verschlüsselungs-Algorithmus (auf der Basis diskreter Logarithmen, benannt nach seinem Erfinder)
E-Mail	Electronic Mail
ESP	Encapsulating Security Payload (Sicherheitseinkapselung)
FEAL	Fast Encryption Algorithm (Blockalgorithmus)
FTP	File Transfer Protocol
G2G	Government to Government (Kommunikationsbeziehung unter Behörden)
G2C	Government to Citizen (Kommunikationsbeziehung zwischen Behörden und Bürgern)
HTTP/http	HyperText Transfer Protocol (Protokoll zum Austausch von HTML-Dokumenten)
IDEA	International Data Encryption Algorithm (symmetrischer Verschlüsselungs-Algorithmus) (-->G)
IETF	Internet Engineering Task Force (Interessengemeinschaft für Internet-Standards)
IP	Internet Protocol
IPSEC/IPSec	IP Secure (Standard für Verschlüsselung und Authentifizierung) (-->G)
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IPX	Internetwork Packet Exchange (Übertragungsprotokoll für Novell-Netzwerk)
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
IT	Informationstechnik

ITU	International Telecommunication Union (Internationale Fernmeldeunion)
LAN	Local Area Network
LDSG	Landesdatenschutzgesetz
MD4, MD5	Message Digest, Hash-Algorithmen
MIME	Multipurpose Internet Mail Extensions (Erweiterung des E-Mail-Standards)
MTT	MailTrusT-Standard
NetBEUI	NetBIOS Extended User Interface (Netzwerkprotokoll)
NetBIOS	Network Basic Input/Output System (Schnittstelle für Netzwerkanwendungen)
OSI	Open Systems Interconnection (Referenzmodell der ISO für Netzwerke)
PGP	Pretty Good Privacy (-->G)
PIN	Personal Identification Number (personenbezogene Identifikationsnummer)
PKCS	Public-Key Cryptography Standard (Spezifikationen für Anwendung von asymmetrischen Verschlüsselungsverfahren)
PKI	Public Key Infrastructure (-->G)
RC2, RC4, RC5	Ron´s Code (symmetrische Verschlüsselungsalgorithmen)
RFC	Request For Comments (Richtlinien für das Internet)
RSA	Rivest Shamir Adleman (asymmetrischer Verschlüsselungs-Algorithmus) (-->G)
S/MIME	Secure Multipurpose Internet Mail Extensions (-->G)
SGB	Sozialgesetzbuch
S-HTTP	Secure HTTP (-->G)
SKIP	Simple Key Management for Internet Protocols (Schlüsselverwaltungsprotokoll für Internet-Protokolle)
SLIP	Serial Line Internet Protocol (Übertragungsprotokoll von IP-Paketen über serielle Leitungen)
SPHINX	Pilotprojekt zur Ende-zu-Ende-Sicherheit in der öffentlichen Verwaltung (-->G)
SSH	Secure Shell (Sicherheitsprotokoll für UNIX) (-->G)
SSL	Secure Socket Layer (Protokoll einer sicheren (verschlüsselten) Kommunikation im Internet) (-->G)
TAN	Transaktionsnummer für Online-Bankgeschäfte
TC	Trust Center (Zertifizierungsstelle)
TCP	Transmission Control Protocol (Übertragungsprotokoll)
VPN	Virtual Private Network (virtuelles privates Netzwerk)
WAN	Wide Area Network
WWW	World Wide Web
X.509	Standard für Directory-System/Verzeichnisdienste zur Authentisierung
X-Terminal	Terminal für simultanen Zugriff auf unterschiedliche Anwendungen und Ressourcen in heterogenen Hardwareumgebungen auf Basis von X-Windows

Anhang 3 Literaturverzeichnis

[Abelson98] Abelson, Anderson, Bellovin, et al.: Risiken von Key Recovery, Key Escrow und Trusted Third Party-Verschlüsselung, DuD 1/1998, S 14 ff

[Bauer91] F. L. Bauer: Kryptologie, 1991

[BÄK96] Bundesärztekammer: Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, in Deutsches Ärzteblatt 1996, Heft 43

[Beucher/Schmoll99] Beucher, Schmoll: Kryptotechnologie und Exportbeschränkung, CR 8/1999

[Blaze96] Blaze u.a.: Minimal Key Length for Symmetric Ciphers to Provide Adequate Commercial Security, 1996, http://www.counterpane.com/keylength.html

[Gerling00] R. W. Gerling: Verschlüsselung im betrieblichen Einsatz, 2000

[KoopAADV02] Kooperationsausschuss Automatisierte Datenverarbeitung des Bundes, der Länder und der Kommunen – KoopA ADV (Hrsg.): Handlungsleitfaden für die Einführung der elektronischen Signatur und Verschlüsselung in der Verwaltung, Version 1.1, Dezember 2002

[Rivest/Shamir/Adleman78] R. Rivest, A. Shamir, L. Adleman: A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21(2), Februar 1978, S. 120

[Roth98] Roth: Exportkontrollen für Verschlüsselungsprodukte, DuD 1/1998; S.8 ff, und 2/1998, S. 81 ff

[Schmidt 98] M. Schmidt, Virtual Private Networks - vertraulicher Datenaustausch über das Internet, c't 8/98

[Schreier96] B. Schneier: Angewandte Kryptografie, 1996

[Smith98] R. Smith: Internet-Kryptografie, 1998

[STOA99] European Parliament, STOA: Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues, 1999, http://cryptome.org/stoa-r3-5.htm

[Weis/Lucks98] R. Weis, S. Lucks: Sicherheitsprobleme bei Authentisierung und Verschlüsselung in GSM-Netzen, DuD 9/1998, S. 504

[Weis/Lucks/Bogk03] R. Weis, S. Lucks, A. Bogk: Sicherheit von 1024 bit RSA-Schlüsseln gefährdet; DuD 6/2003, S. 360

[Wobst97] R.Wobst: Abenteuer Kryptologie, 1997