Erschienen in: Fox, D.; Horster, P.: *Datenschutz und Datensicherheit – DuD*. Verlag Vieweg, Wiesbaden 1999, S. 283-304.

Realisierung von Public-Key-Infrastrukturen

Dirk Fox

Secorvo Security Consulting GmbH
fox@secorvo.de

Patrick Horster

Universität Klagenfurt
pho@ifi.uni-klu.ac.at

Zusammenfassung

Sicherheitsinfrastrukturen sind für die Nutzung von Sicherheitsdiensten in verteilten Informationstechnischen Systemen zwingend erforderlich. Sie können als der technische und organisatorische Unterbau aufgefaßt werden, und sie garantieren ein einheitliches, zuvor festgelegtes Sicherheitsniveau für die unterstütze Funktionalität. Sicherheitsinfrastrukturen spielen somit eine zentrale Rolle, insbesondere für Sicherheitsdienste in offenen Kommunikationssystemen, die in zunehmendem Maße öffentliche digitale Kommunikationsnetze nutzen. Für diese Sicherheitsdienste sind moderne kryptologische Techniken, sogenannte asymmetrische Public-Key-Verfahren von ausschlaggebender Bedeutung. Konzepte zur Realisierung unternehmensinterner sowie öffentlicher Public-Key-Infrastrukturen müssen dabei unterschiedliche Anforderungen genügen, die sich aus dem Stand der wissenschaftlichen und technischen Entwicklung, dem Signaturgesetz und dem Einsatz moderner Kommunikationsanwendungen ergeben. Als Sicherheitstoken nehmen dabei Smartcards mit ihren integrierten Crpytoprozessoren eine Schlüsselrolle ein. Der Beitrag gibt eine Übersicht über die wichtigsten Anforderungen und den Stand der Technik, bereichert um praktische Erfahrungen, die beim Aufbau von Public-Key-Infrastrukturen gewonnen werden konnten.

1 Einleitung

Zweifellos hat die verstärkte Nutzung des Internets zum erheblich gewachsenen Interesse an Sicherheitslösungen beigetragen. Denn wer seinem Unternehmen den Zugang zum Internet ebnen möchte, will natürlich nicht zugleich die Unternehmensinfrastruktur dem Internet öffnen. Moderne Kommunikationsinfrastrukturen können aber auf die zahlreichen Vorteile, die durch die intensive Nutzung des Internets möglich werden, nicht verzichten; dies darf allerdings nicht ohne geeignete Sicherheitsmaßnahmen geschehen.

Durch gut konfigurierte Firewalls können die entstehenden Probleme allerdings nicht alleine gelöst werden. Dies ist etwa dann der Fall, wenn geographisch auseinanderliegende Teile ei-

nes Unternehmens über das Internet in Virtual Private Networks (VPNs) integriert werden sollen. Dabei sollen Kommunikations- und sensible Unternehmensdaten weder im Klartext übertragen werden noch während der Übertragung (unerkannt) verfälscht werden können.

Die derzeitige Entwicklung und Verbreitung von Informations- und Kommunikationssystemen in Unternehmen macht allerdings bei VPNs nicht Halt:

- Zunehmend werden moderne Kommunikationstechniken auch in der Business-to-Business-Kommunikation eingesetzt. Für den Austausch sensibler Daten und Informationen zwischen Unternehmen sowie bei Verhandlungen wird in wachsendem Umfang E-Mail als Kommunikationsmedium verwendet. Die dabei übertragenen Daten sind meist nicht vor unberechtigtem Zugriff bzw. Verfälschung geschützt.
- Papierbasierte unternehmensinterne Abläufe werden aus Kosten- und Effizienzgründen durch elektronisch abgewickelte Vorgänge ersetzt. Mit Workflow-Messaging-Systemen wird dabei versucht, eingespielte Abläufe durch den Einsatz moderner Kommunikationstechniken zu vereinfachen und zu beschleunigen. Dabei muß nicht nur die Vertraulichkeit von Daten und Dokumenten gewährleistet werden, sondern ist meist auch sicherzustellen, daß einzelne Schritte des Vorgangs im Falle von Fehlern oder Unstimmigkeiten nachgeprüft werden können. Der Revisionsfähigkeit kommt somit auch eine elektronische Bedeutung zu.
- Auch ein Teil der Kundenbeziehung findet inzwischen vielfach und in wachsendem Umfang auf elektronischem Wege statt. Vorreiter waren dabei u.a. Banken mit der Entwicklung und dem Angebot von Home-Banking-Lösungen; inzwischen wurde das Internet von vielen Herstellern (und Kunden) als kostengünstiger Vertriebs-, Werbe- und Supportkanal entdeckt. Das vielschichtige Feld der E-Commerce-Techniken hat daher eines gemeinsam: einen hohen Bedarf an Sicherheitsmechanismen zum Schutz elektronischer Kundenbeziehungen und dabei verarbeiteter Daten.

Eine einfache Verschlüsselung der über das Internet übertragenen Daten (etwa durch Tunneling zwischen zwei Routern) genügt den durch diese neuen Entwicklungen entstehenden Anforderungen zumindest aus drei Gründen nicht:

- Erstens ist zumeist ein „personenbezogener“ Ende-zu-Ende-Schutz der Daten (z.B. im Fall von E-Mail-Nachrichten von Sender zu Empfänger) erforderlich, wenn die Kommunikationsinhalte oder Dokumente auch keinem unberechtigten Dritten im eigenen Unternehmen zur Kenntnis gelangen sollen.
- Zweitens müssen Bearbeitungsschritte einzelner Sachbearbeiter in einem Workflow-System dokumentiert und diesem Bearbeiter, analog der Zeichnung mit Namenszeichen oder einer eigenhändigen Unterschrift in herkömmlichen Abläufen, zugeordnet werden können.
- Drittens muß das System offen sein, d.h. eine sichere Kommunikation zwischen beliebigen, auch einander a priori unbekannten Netz-Teilnehmern erlauben.

Sicherheitsprotokolle und Lösungen auf der Grundlage asymmetrischer kryptographischer Verfahren, auch als Public-Key-Verfahren bezeichnet, können diese Anforderungen erfüllen. Durch die Verwendung öffentlicher Schlüssel erlauben sie die Erzeugung und Prüfung digitaler Signaturen sowie den Austausch (hybrid) verschlüsselter Daten (Dokumente). Sie benöti-

gen eine Schlüsselinfrastruktur zur authentischen Verteilung öffentlicher Schlüssel, auch Public-Key-Infrastruktur (PKI) genannt.

2 Begriffsbildung und Grundanforderungen

Public-Key-Infrastrukturen können als Bestandteil moderner Sicherheitsinfrastrukturen angesehen werden. Sie bilden den Kern nahezu aller sicherheitsrelevanten Neuentwicklungen im Umfeld heutiger Informations- und Kommunikationstechniken [HoKW99]. Die Anwendungsfelder umfassen Datenkommunikation, Electronic Banking, Electronic Commerce, Electronic Voting und zahlreiche weitere Dienste moderner Informations- und Kommunikationstechnik, wobei die meisten dieser Anwendungen erst durch PKIs realisierbar werden.

Unter einer Infrastruktur versteht man einen „notwendigen wirtschaftlichen und organisatorischen Unterbau einer hoch entwickelten Wirtschaft (etwa Verkehrsnetze und Arbeitskräfte)„ [Wiss97]. Überträgt man diesen Begriff auf eine „Sicherheits„-Infrastruktur, dann kann man darunter eine Infrastruktur verstehen, die einen notwendigen technischen und organisatorischen, möglicherweise auch gesetzlich geregelten Unterbau darstellt, mit dem ein festgelegtes Sicherheitsniveau erreicht werden kann.

Das für eine spezielle Sicherheitsinfrastruktur festgelegte Sicherheitsniveau wird in der Regel in Gestalt einer Security Policy oder eines Sicherheitskonzept dokumentiert, in dem neben den grundlegenden Zielen die zentralen Sicherheitsanforderungen, aber auch die Beziehungen der Beteiligten und die Leistungsmerkmale der Sicherheitsinfrastruktur festgeschrieben sind. Beteiligte in einer Sicherheitsinfrastruktur können neben den Betreibern der Infrastruktur und den Benutzern auch die Hersteller von Systemkomponenten und sogar staatliche Organe sein.

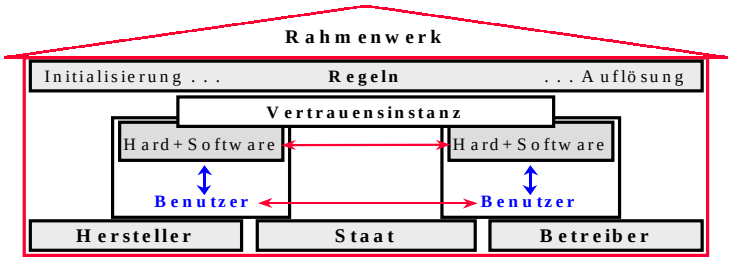

Abb. 1: Beteiligte und Komponenten einer Sicherheitsinfrastruktur

Alle Beteiligten stehen zueinander in organisatorischen, technischen und rechtlich relevanten Beziehungen. Gegenstand einer Security Policy sind daher nicht nur Aussagen zur Bereitstellung der Sicherheitsdienste, Gewährleistung deren Verfügbarkeit und ein Notfallmanagement, sondern oft auch Verträge, Lizenzen und die Klärung der Haftungsfragen. Insbesondere ist es wichtig, Anforderungen zu definieren, deren technische Umsetzung gewährleistet, daß das definierte Rahmenwerk eingehalten werden kann. Nur so kann eine hohe Akzeptanz der Infra-

struktur auf Seiten aller Beteiligten erreicht werden.

Hersteller müssen zuverlässige technische Komponenten liefern, die als vertrauenswürdig eingestuft werden können. Um hier das notwendige Vertrauen zu erhalten, können die Produkte durch unabhängige Dritte, etwa nach den Kriterien der ITSEC [ITSE91], geprüft werden. Eine solche Prüfung kann von akkreditierten Prüfstellen vorgenommen werden.

Die Betreiber sollten die Verfügbarkeit und Robustheit der Sicherheitsinfrastruktur gewährleisten, beispielsweise die Instandhaltung der technischen Geräte zusichern.

Die Sicherheitsinfrastruktur muß für ihre Benutzer in einer transparenten Art und Weise die erforderlichen Sicherheitsdienste wie Vertraulichkeit, Verbindlichkeit, Anonymität und Verfügbarkeit erbringen. Die Benutzer müssen hierzu den eingebundenen Instanzen ein gewisses Maß an Vertrauen entgegenbringen, wobei dieses Vertrauen je nach Dienstleistung unterschiedlich groß sein kann:

Erzeugt beispielsweise eine Instanz kryptographische Schlüssel, die in einem Verfahren für digitale Signaturen eingesetzt werden sollen, dann ist im Vergleich zur Veröffentlichung von Schlüsselzertifikaten ein weitaus höheres Maß an Vertrauen erforderlich, da Schlüsselzertifikate von jedem Benutzer auf Authentizität und Integrität geprüft werden können.

Operationelle Anforderungen an eine allgemeine Sicherheitsinfrastruktur können die folgenden Leistungsmerkmale betreffen:

- **Offenheit**: Die Sicherheitsdienste, die in einer Anwendung eingesetzt werden, müssen so konzipiert sein, daß sie mit unterschiedlichen Implementierungen auf verschiedenen Systemen und Plattformen interoperieren können (Interoperabilität, Standardkonformität und Kompatibilität).
- **Langlebigkeit**: Die Verfahren und Mechanismen, mit denen die Sicherheitsdienste realisiert werden, sollten als sicher eingestuft sein, entweder bewiesenermaßen oder dadurch, daß sie öffentlichen Untersuchungen über einen längeren Zeitraum standhalten konnten. Alle technischen Systemkomponenten sollten so angelegt sein, daß sie in einfacher Art und Weise verbessert werden können, etwa durch ein Upgrade der Software. Auch das Sicherheitskonzept sollte geeignet geprüft sein, um unverändert für eine lange Zeit bestehen zu können.
- **Stabilität**: Die Sicherheitsinfrastruktur muß so angelegt sein, daß der Ausfall einer Vertrauensinstanz nicht gleich die gesamte Infrastruktur lahmlegt. So muß sichergestellt sein, daß Vertrauensinstanzen die Aufgaben anderer, konkurrierender Vertrauensinstanzen einfach, schnell und sicher übernehmen können.
- **Erweiterbarkeit und Skalierbarkeit**: Eine Sicherheitsinfrastruktur unterliegt – bedingt durch technische, wissenschaftliche und rechtliche Veränderungen – einem ständigen Wandel. Sie sollte zum einen erweiterbar im Hinblick auf neue Verfahren sein, aber auch um neue Vertrauensinstanzen ergänzt werden können.

3 PKI-Technik

Asymmetrische Kryptoverfahren arbeiten mit Schlüsselpaaren (OS, GS), wobei der Schlüssel GS vom Schlüsselinhaber geheimgehalten werden muß, während der zweite Schlüssel als öffentlicher Schlüssel OS des Schlüsselinhabers bekanntgegeben wird. Für unterschiedliche Sicherheitsdienste kommen dabei in der Regel auch unterschiedliche Schlüsselpaare zur Anwendung. Zudem besitzen verschiedene Benutzer auch unterschiedliche Schlüssel.

Die Verschlüsselung eines für einen Schlüsselinhaber B bestimmten Dokuments m erfolgt dann mit dessen öffentlichen Verschlüssellungsschlüssel OSB. Mit seinem geheimgehaltenen Entschlüsselungsschlüssel GSB kann der Empfänger dann die Nachricht entschlüsseln. In der folgenden Abbildung bezeichnet E die Verschlüsselungsfunktion und D die zugehörige Entschlüsselungsfunktion.

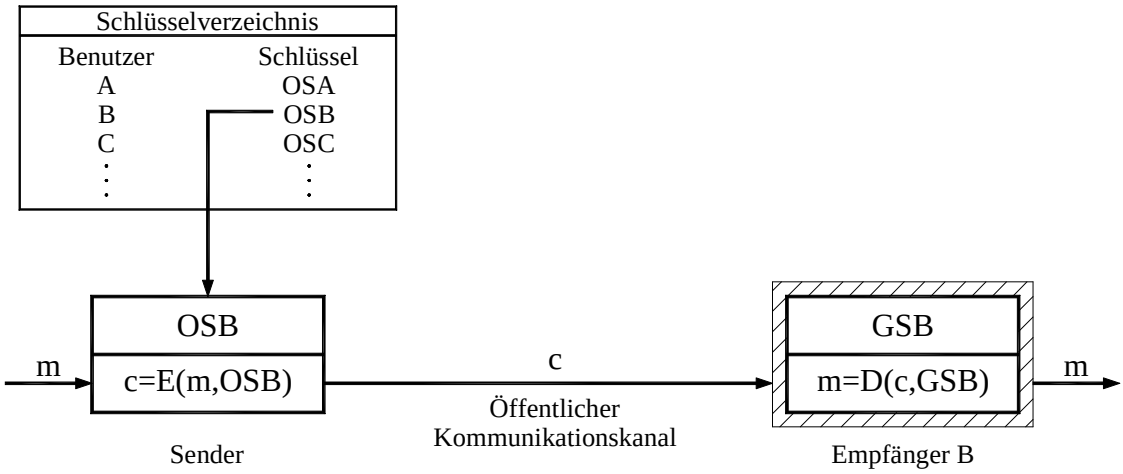

Abb. 2: Prinzip einer asymmetrischen Verschlüsselung

Üblicherweise wird dabei zudem ein hybrides Verfahren verwendet: Die Daten werden zunächst mit einem symmetrischen Standard-Verfahren mit hinreichender Schlüssellänge und einem zufällig gewählten Nachrichtenschlüssel verschlüsselt. Der Nachrichtenschlüssel wird dann mit dem öffentlichen Schlüssel des Empfängers asymmetrisch verschlüsselt.

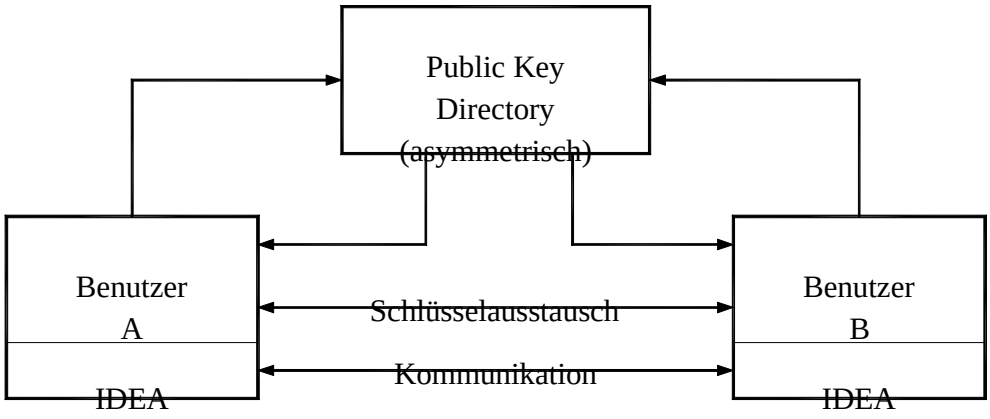

Abb. 3: Prinzip einer hybriden Verschlüsselung (mit IDEA als symmetrische Komponente)

Ähnlich der asymmetrischen Verschlüsselung können digitale Signaturen erzeugt und geprüft werden: Eine digitale Signatur s zu einer gegebenen Nachricht m berechnet der Schlüsselinhaber A mit seinem geheimen Signierschlüssel GSA und einer Signierfunktion S. Die Prüfung, ob eine digitale Signatur zu einer vorliegenden Nachricht gehört, kann anschließend jeder vornehmen, der die zugehörige Verifizierfunktion V und den öffentlichen Prüfschlüssel OSA des Signierers A kennt.

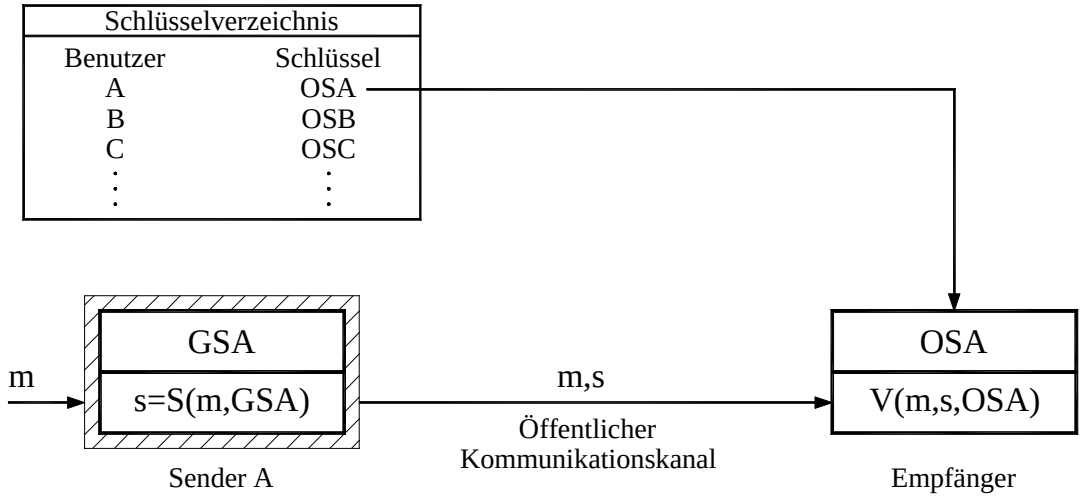

Abb. 4: Prinzip einer Digitalen Signatur

Asymmetrische Verfahren erlauben damit den Aufbau von Sicherheitsinfrastrukturen für offene Kommunikationssysteme: Die öffentlichen Schlüssel zur Verschlüsselung und zur Prüfung digitaler Signaturen können allgemein zugänglich gemacht werden und erfordern keine „geschlossene Benutzergruppe„ für eine sichere Kommunikation.

Eine wesentliche Forderung besteht allerdings: Die öffentlichen Schlüssel eines Teilnehmers müssen demjenigen, der ein Dokument an diesen verschlüsselt gesendet oder dessen digitale Signatur prüfen möchte, authentisch bekannt sein. Die Authentizität eines Schlüssels läßt sich dabei auf unterschiedliche Art und Weise gewährleisten:

- Das populäre Verschlüsselungsprogramm „Pretty Good Privacy„ von Phil Zimmermann geht dabei einen Weg, der am „wirklichen Leben„ angelehnt ist [Zimm95, Grim96]: Erhält jemand von einer Person, die er kennt und der er vertraut, deren öffentlichen Schlüssel (persönlich ausgehändigt oder digital übertragen und telefonisch überprüft anhand des schlüsseleigenen „Fingerprints„), so bestätigt er dies, indem er diesen öffentlichen Schlüssel digital signiert. Der Schlüsselinhaber erhält damit mit der Zeit mehr und mehr digitale Signaturen unter seinem Schlüssel, die bestätigen, daß dieser Schlüssel zu ihm gehört. Weitere Personen, die diesen Schlüssel erhalten, können damit die Authentizität des Schlüssels prüfen, wenn sie einer der Personen vertrauen, die mit einer digitalen Signatur unter diesem Schlüssel die Authentizität bestätigt haben. Auf diese Weise entsteht nach und nach ein „Web of Trust„.
- Die Standardisierung von Public-Key-Verfahren geht einen anderen Weg: Hier wird ein hierarchisches Vorgehen bevorzugt. Zu öffentlichen Schlüsseln werden von zentralen „Zertifizierungsstellen„ (Certification Authorities – CAs) digital signierte Bestätigungen ausgestellt, die den eindeutigen Namen des Schlüsselinhabers, den öffentlichen Schlüssel

und die Gültigkeit der Bestätigung sowie mögliche andere Informationen (z.B. über die Verwendung des Schlüssels) enthalten. Solche Bestätigungen, Schlüsselzertifikate genannt, werden über allgemein zugängliche Verzeichnisse publiziert. Dritte können sich damit anhand des Zertifikats davon überzeugen, daß ein ausgewählter Schlüssel zu einer bestimmten Person gehört. Die Authentizität der öffentlichen Schlüssel der Zertifizierungsstellen kann wiederum durch eine übergeordnete Instanz bestätigt werden. Auf diese Weise entsteht ein hierarchischer „Zertifizierungsbaum„. Alle Schlüsselinhaber, die ein Zertifikat von einer solchen Hierarchie zugehörigen Zertifizierungsstelle besitzen, müssen lediglich den öffentlichen Schlüssel der „Wurzel-Instanz„ (Root-CA) authentisch kennen, um die Authentizität aller anderen Schlüssel direkt prüfen zu können.

Der zentralisierte Ansatz wurde bereits in den frühen IETF-Spezifikationen für E-Mail-Sicherheit Ende der 80er Jahre verfolgt (Privacy Enhancement for Internet Electronic Mail, PEM) [HoPo94]. Er findet sich wieder bei S/MIME [DHR+98, DHRW98], MailTrusT [Baus96], und in der ITU- bzw. ISO/IEC-Standardisierung für Schlüsselzertifikate, X.509 [ITU 93]. Auch das deutsche Signaturgesetz hat sich für diesen Ansatz entschieden [SigG97].

4 PKIs nach deutschem Signaturgesetz

Mit der Verabschiedung des Signaturgesetzes (SigG) und der Signaturverordnung (SigV) haben Bundestag und Bundesregierung Mitte des vergangenen Jahres Neuland beschritten: Vor allen anderen europäischen Ländern und als zweites Land weltweit (nach dem US-Bundesstaat Utah) bekam Deutschland eine gesetzliche Regelung zu digitalen Signaturen [SigG97, SigV97].

4.1 Konzeption des Signaturgesetzes

Der von der Bundesregierung verfolgte Ansatz weicht – aus gutem Grund – von den Konzepten anderer Staaten und auch dem aktuellen Regulierungsvorschlag der EU-Kommission ab [EU-K98, GrFo98]: Die Rechtswirksamkeit digitaler Signaturen wurde angesichts der Tatsache, daß auch der Beweiswert von eigenhändigen Unterschriften sich erst in vielen Jahren Rechtsgeschichte schrittweise entwickelt hat, nicht gesetzlich festgeschrieben.

Statt dessen wurden Sicherheitsanforderungen an eine Infrastruktur für Schlüsselerzeugung, Schlüsselzertifizierung, Schlüsselverteilung und Schlüsselanwendung zusammengestellt, die für eine hohe Vertrauenswürdigkeit solcher digitaler Signaturen, die nach Signaturgesetz erzeugt wurden, sorgen sollen. Dazu zählen insbesondere:

- Ein Sicherheitskonzept sowie regelmäßige Prüfungen für alle nach dem Signaturgesetz anerkannten Zertifizierungsstellen.
- Die eingesetzten technischen Komponenten müssen hohen Sicherheitsstandards genügen (vorgeschrieben ist eine Sicherheitszertifizierung nach ITSEC, E2/E4 hoch).
- Die geforderten Mindestschlüssellängen für die kryptographischen Verfahren sind so gewählt, daß eine Kompromittierung der Schlüssel unter realistischen Annahmen in den nächsten zehn Jahren nicht zu erwarten ist. Dies muß allerdings für jeden einzelnen Schlüssel garantiert werden.
- Die geheimen Schlüssel werden in einer physisch geschützten Umgebung erzeugt und in

einem „Sicherheitstoken“ (etwa eine Smartcard) gespeichert – und den sie zu keinem Zeitpunkt verlassen. Aus Sicherheitsgründen ist es dabei sinnvoll, den Schlüssel direkt in der Smartcard zu erzeugen.

- Die Nutzung der Schlüssel ist nicht nur an den Besitz der Smartcard („Haben“), sondern an zusätzliche Parameter wie eine PIN („Wissen“) oder ein biometrisches Merkmal („Eigenschaft“) geknüpft.
- Die Wurzel-Instanz („Root-CA“) der Schlüsselinfrastruktur nach Signaturgesetz ist bei der Regulierungsbehörde für Post und Telekommunikation (RegTP) angesiedelt.

Der Beweiswert einer digitalen Signatur ist damit nicht präjudiziert, sondern muß sich erst vor Gericht erweisen. Bei Nutzung einer Zertifizierungsinfrastruktur nach Signaturgesetz sollte jedoch eine sehr hohe Wahrscheinlichkeit für die Anerkennung digitaler Signaturen als Beweismittel im Rahmen der freien Beweiswürdigung vor Gericht bestehen.

Es ist zu erwarten, daß der Beweiswert digitaler Signaturen sich auf der Grundlage der Einschätzungen von im Streitfall gerichtlich bestellten Gutachtern in den nächsten Jahren etablieren wird. Sollte es dazu kommen, so erscheint es sinnvoll, mit zunehmender Erfahrung im Umgang mit digitalen Signaturen (als Gegenstück der modernen Kommunikationsgesellschaft zur eigenhändigen Unterschrift) über eine gesetzliche Verankerung der Rechtswirkung digitaler Signaturen nachzudenken, wie sie heute bereits im Entwurf der EU-Richtlinie gefordert wird [EU-K 98].

4.2 Kritische Würdigung des Signaturgesetzes

Zweifellos hat allein die Verabschiedung des Signaturgesetzes zu einer erheblichen Marktentwicklung bei PKI-Produkten beigetragen. Denn Signaturgesetz und Signaturverordnung geben Orientierung und damit Investitionsschutz: Sowohl Hersteller als auch Unternehmen, die den Aufbau einer PKI planen, gewinnen Gewißheit, daß ihre Investitionen in PKI-Produkte nicht durch die Gesetzgebung Makulatur werden, wenn sie sie am Signaturgesetz orientieren. Die europäischen und internationalen Entwicklungen müssen aber dennoch mit der gebotenen Aufmerksamkeit verfolgt werden, um gegebenenfalls schnell eine entsprechende Interoperabilität zu erreichen.

Zudem legt das Signaturgesetz die „Sicherheitslatte“ hoch und betont damit die Bedeutung eines hohen Sicherheitsstandards in Sicherheitsinfrastrukturen für moderne Kommunikationssysteme. Auch die im Gesetz vorgesehene Kontrollinfrastruktur, die durch eine Bindung der Betriebsgenehmigung an regelmäßige unabhängige Prüfungen und Abnahmen für die Erhaltung eines hohen Sicherheitslevels sorgen soll, ist nicht nur für Zertifizierungsstellen nach Signaturgesetz eine wichtige Einrichtung. Nicht zuletzt macht der hohe Sicherheitsstandard des Signaturgesetzes die Anerkennung digitaler Signaturen als Beweismittel vor Gericht sehr wahrscheinlich.

Da das Signaturgesetz jedoch durch die vergleichsweise geringen Erfahrungen mit digitalen Signaturen im praktischen Einsatz eher im Bereich „experimentelle Gesetzgebung„ anzusiedeln ist, hat der Gesetzgeber beschlossen, es (als Artikel 3 des Informations- und Kommunikationsdienste-Gesetzes) in Zweijahresfrist einer Evaluation zu unterwerfen, um zu prüfen, ob Korrekturen oder Änderungen erforderlich sind. Im Juni 1999 soll das Ergebnis dieser Evaluation vorgelegt werden.

Aus praktischer Erfahrung und technischer Sicht gibt es an mehreren wichtigen Stellen Nacharbeits- und Korrekturbedarf:

- **Hierarchie**: Das Signaturgesetz arbeitet mit einer nur zweistufigen Hierarchie (Zertifizierungsstellen und Root-CA bei der Regulierungsbehörde). Obwohl eine solche flache Hierarchie die Konzeption vereinfacht und auch sicherheitstechnisch einfacher zu behandeln ist, ist dies für viele praktische Anwendungsfälle eine erhebliche Einschränkung. Exemplarisch seien hier das Gesundheitswesen und die verzweigten Strukturen global agierender Großkonzerne genannt.
- **Zertifikate für juristische Personen**: Das Signaturgesetz erlaubt die Ausstellung von Schlüsselzertifikaten ausschließlich für natürliche Personen. Das gilt auch für die Schlüssel von Zertifizierungsstellen, die zur Ausstellung von Schlüsselzertifikaten, Rückruflisten, Verzeichnisdiensten oder Zeitstempeln verwendet werden. Um bei Kündigung eines Mitarbeiters den Schlüssel der Zertifizierungsstelle nicht zurückrufen zu müssen, behilft man sich heute mit der Verwendung eines Pseudonyms: Der dem Pseudonym zugeordnete Mitarbeiter kann dabei wechseln. Grundsätzlich ist es jedoch auch in vielen praktischen Fällen sinnvoll, Schlüsselzertifikate für juristische Personen, z.B. ein Unternehmen auszustellen. Hinzu kommt, daß bisher keine einheitliche Regelung für die Struktur des „gesetzlichen Namens“ einer natürlichen oder juristischen Person existiert. Dies ist aber eine wichtige Voraussetzung für die Vergabe unverwechselbar eindeutiger Namen in einer Sicherheitsinfrastruktur.
- **Gültigkeitsprüfung**: Das derzeit dem Signaturgesetz zugrundeliegende Verständnis der Gültigkeit einer digitalen Signatur nimmt an, daß der Empfänger einer digitalen Signatur immer prüfen kann, ob ein Signaturschlüsselzertifikat gültig und nicht gesperrt ist (und damit der zugehörige Schlüssel akzeptiert werden kann). Technisch erfordert diese Annahme die Bereitstellung eines absolut zuverlässigen und hochverfügbaren Online-Dienstes, bei dem zu jeder Zeit die Gültigkeit eines Zertifikats geprüft werden kann. Offline-Benutzer sind damit von einer Gültigkeitsprüfung ausgeschlossen. Zudem entstehen ein erheblicher zusätzlicher Kommunikationsaufwand sowie erhöhte Sicherheitsanforderungen an den Auskunftsdienst. Der Mechanismus steht im Widerspruch zu den in internationalen Standards verfolgten Konzept der Sperrlisten [Fox 99]. Auch eine rückwirkende Sperrung von Zertifikaten bei Bekanntwerden einer Schlüsselkompromittierung, der in bestimmten Fällen in der Praxis sinnvoll sein kann, ist nicht konform zum Signaturgesetz.
- **Ansichtskomponente**: Die (zweifellos sinnvolle) Anforderung an Signier- und Prüfkomponenten, dem Signierer respektive Prüfer zu garantieren, daß er sieht, was er digital signiert bzw. was digital signiert wurde, stößt auf ein prinzipielles Problem: Eine digitale Signatur bezieht sich immer nur auf 0-1-Folgen oder Bitstrukturen (also die Syntax), nicht aber auf die Bedeutung eines Dokuments (seine Semantik) – selbst die Codierung der Dokumenteninhalte ist in der Regel nicht festgelegt. Verbreitete Produkte (etwa im Office-Bereich) bieten jedoch eine Vielzahl von Möglichkeiten, nicht-eindeutig darstellbare Dokumente zu erzeugen (versteckter Text, Notizen, Anmerkungen, Ausnutzung von Inkompatibilitäten zwischen verschiedenen Produktversionen etc.) [HoKr96, Fox 98]. Bisher gibt es kein geeignetes und verfügbares Produkt, das dieses Problem einer eindeutigen Ansichtskomponente zufriedenstellend löst. Eine strengen Sicherheitsanforderungen genügende Lösung wird zudem sowohl teuer als auch in der Funktionalität stark einge-

schränkt sein. Ideen wie der Einsatz eines Postscript-Viewers zeigen aber Wege auf, wie die vorhandenen Probleme zumindest partiell angegangen werden können.

- **Dienstleistung durch Dritte**: Nach Signaturgesetz werden alle Dienste, von der Registrierung über die Zertifizierung bis hin zu Verzeichnis- und Zeitstempeldienst, von einer Zertifizierungsstelle erbracht. Das kollidiert mit dem praktischen Erfordernis, insbesondere die Registrierung geographisch in Kundennähe zu plazieren, um Wegekosten zu reduzieren. Hier ist auch die Frage zu klären, wie Zertifizierungsstellen durch Kooperationsverträge organisiert werden können, wenn von ihnen verschiedene Dienstleistungen (etwa Registrierung, Identifizierung und Zertifizierung) in unterschiedlichen Institutionen angeboten werden [Reis98].

4.3 Öffentliche Zertifizierungsstellen

Signaturgesetzkonforme Zertifizierungsstellen müssen den hohen Sicherheitsanforderungen des Signaturgesetzes entsprechen – und unterliegen damit auch den angeführten technischen Restriktionen, die das Gesetz vorsieht.

Der Prozeß einer Anerkennung nach Signaturgesetz ist wegen der hohen Sicherheitsanforderungen zeit- und kostenintensiv. Nur wenige Unternehmen werden sich daher die Einrichtung einer signaturgesetzkonforme Zertifizierungsstelle leisten. Für kleine und mittelständische Unternehmen sowie für Privatpersonen könnte daher die Möglichkeit zur Nutzung von öffentlichen Zertifizierungsdiensten wichtig werden.

Mehrere Unternehmen haben bereits Anträge bei der Regulierungsbehörde für Telekommunikation und Post (RegTP) auf Anerkennung als Zertifizierungsstelle nach Signaturgesetz gestellt. Die Root-CA der RegTP hat am 23. September 1998 ihre Arbeit aufgenommen. Die erste digitale Signatur nach Signaturgesetz wurde am 23.09.1998 um 17:18:13 Uhr erzeugt, dabei wurde in der Zertifizierungsstelle der RegTP in Mainz der Root-Zertifizierungsschlüssel und das korrespondierende Zertifikat generiert.

Betriebsbereit ist seit Januar 1999 die Zertifizierungsstelle der deutschen Telekom AG (Produktzentrum TeleSec, Siegen). Sie ist, mehr als 18 Monate nach Verabschiedung des Signaturgesetzes, die bisher einzige Zertifizierungsstelle, die Zertifizierungsdienste nach Signaturgesetz anbieten kann. Das hat auch Gründe, denn der Betreiber einer öffentlichen Zertifizierungsstelle nach Signaturgesetz muß bei der Konzeption eine Vielzahl von Randbedingungen berücksichtigen:

- **Kundennähe**: Den größten Teil der Kosten bei der Ausstellung eines Zertifikats verursacht die Registrierung eines Schlüsselinhabers – sowohl für den Schlüsselinhaber selbst (Wegezeiten) als auch für den Anbieter (Identifizierung, Einweisung, Dokumentation). Für den Anbieter rechnet sich die Dienstleistung nur dann, wenn er bei der Registrierung ein existierendes eigenes oder externes Filialnetz nutzen kann.
- **Konkurrenzproblematik**: Der Betreiber einer Zertifizierungsstelle, der in anderen Geschäftsbereichen seines Unternehmens mit potentiellen Kunden konkurriert, kann ein Akzeptanzproblem haben, insbesondere dann, wenn er die Schlüssel in seiner Zertifizierungsstelle generiert.
- **Einsatzgebiet**: Zertifikate nach Signaturgesetz werden sicherlich zunächst nur in speziellen Anwendungen (z.B. Behördenkontakte, wie dem Finanzamt) eingesetzt werden

können. Da die Interoperabilitätsspezifikation (SigI) [Gies98, Berg99] noch nicht abgeschlossen ist, gibt es zur Zeit keine einzige nicht-proprietäre Anwendung, die die Verwendung von Signaturgesetz-Zertifikaten erlaubt.

- **Kosten (Business Case)**: Die Investitionen in eine Zertifizierungsstelle nach Signaturgesetz müssen sich in einem überschaubaren Zeitraum amortisieren. Der Markt für Zertifikate nach Signaturgesetz ist allerdings begrenzt: Es wird sicherlich noch weitere zehn Jahre dauern, bis sich das Konzept einer „Signaturschlüssel-Smartcard“ bundesweit durchgesetzt hat. Außerdem sind die derzeitigen Grenzen durch die Lebensdauer von fünf Jahren, die Tatsache, daß Zertifikate nur für natürliche Personen ausgestellt werden, und die Beschränkung auf den deutschen Markt vorgegeben. Schließlich werden sich mehrere Anbieter den Markt teilen müssen. Dazu kommen fixe Kosten (für die Smartcard, die Mitarbeiter in Registrierungsstellen und die Abwicklung von Antragstellung und Dokumentation), die je Zertifikat anfallen. Dadurch wird ein realistischer Preis eines Zertifikats nicht unter 50 DM liegen können – wiederum ein marktbegrenzender Faktor.
- **Weitere Signaturtypen**: Neben der originären digitalen Signatur finden bereits heute zahlreiche weitere Typen von digitalen Signaturen eine breite Anwendung. Hier sind etwa Beglaubigungsschemata, empfängerspezifische Signaturen, unleugbare Signaturen und blinde Signaturen zu nennen, womit das breite Spektrum allerdings nur angedeutet ist. Zukünftige Anwendungen im Bereich Electronic Commerce und weiterer innovativer Anwendungen (etwa Electronic Voting und Secure Multimedia) verlangen nach neuartigen Konzepten, an denen zumindest in der Forschung bereits seit mehreren Jahren gearbeitet wird [PeMH96].

Signaturen nach Signaturgesetz sind also nur eine spezielle Anwendung von PKI-basierten digitalen Signaturen. In der Praxis werden jedoch bereits heute PKIs genutzt, meist im Zusammenhang mit Anwendungen, in denen die Frage einer gerichtlichen Würdigung der erzeugten digitalen Signaturen irrelevant ist. Überwiegend genügen hier auch deutlich geringere Sicherheitsanforderungen als die in SigG bzw. SigV geforderten.

5 Unternehmensweite PKIs

Viele Großunternehmen, vor allem im Bankenbereich, in der Automobilindustrie und der Telekommunikationsbranche, haben PKIs als eine Sicherheitsinfrastruktur mit zentraler Bedeutung für die gesamte Unternehmenssicherheit erkannt und bereits mit der Konzeption, dem Aufbau und dem Betrieb firmeninterner Public-Key-Infrastrukturen begonnen.

Entscheidende Voraussetzung für die Nutzbarkeit der von PKIs bereitgestellten Schlüssel und Zertifikate ist dabei natürlich die Verfügbarkeit von Anwendungen, die auf Sicherheitsdiensten beruhen, die asymmetrischen Verfahren nutzen. In Gestalt von hybriden Kryptosystemen kommen dabei zumeist außerdem symmetrische Verfahren zum Einsatz.

5.1 PKI-Anwendungen

Es lassen sich zwei verschiedene Klassen von PKI-Anwendungen unterscheiden:

- **Kommunikationsinfrastruktur**: Anwendungen, die eine Kommunikationsstrecke zwischen zwei Endpunkten oder spezielle Dienste des Kommunikationsnetzes schützen. Beispiele dafür sind Protokolle wie DNSsec, IPsec, SSH und SSL/TLS. Asymmetrische Verfahren werden dabei zur Authentifikation und für den Integritätsschutz übertragener Daten eingesetzt. Diese Anwendungen haben die folgenden Eigenschaften gemein:
  - Die Sicherheitsmechanismen sind vollständig transparent für den Nutzer.
  - Die Ausstellung von Zertifikaten erfolgt nicht für natürliche Personen, sondern für Rechner (z.B. DN = IP-Adresse).
  - Die geheimen Schlüssel sind nur schwach geschützt, da sie in Software und in ungesicherter Umgebung gespeichert werden.
  - Zertifikats-Rückruflisten und Verzeichnisdienste sind nicht erforderlich.
  - In der PKI werden geschlossene Benutzergruppen verwaltet.
- **Nutzer-Anwendungen**: Auf der Ebene von Nachrichten (z.B. E-Mail-Messages) oder Dokumenten (z.B. Spreadsheets, Texte) wird ein „personenbezogener„ Ende-zu-Ende-Schutz benötigt. Dies geht über einen einfachen Ende-zu-Ende-Schutz auf Kommunikationsebene hinaus, denn hier soll mit digitalen Signaturen die Urheberschaft und Integrität einer Nachricht bzw. eines Dokuments bezogen auf eine Person sichergestellt werden. Verschlüsselte Daten sollen allein vom gewünschten Empfänger entschlüsselt werden können. Auch die Einrichtung von Remote Access-Zugängen zu einem Unternehmen und der Aufbau sicherer VPNs über Internet-Verbindungen oder öffentliche Leitungen fällt in diese Klasse, sofern der Schutz personenbezogen realisiert wird. Weitere Anwendungen sind Home-Banking, Bestell- und Bezahlsysteme im Umfeld von E-Commerce, Dokumentenarchivierung und Workflow-Systeme. Für diese Anwendungen sind die folgenden Punkte charakteristisch:
  - Verwendung separater (unterschiedlicher) Schlüsselpaare für verschiedene Dienste, etwa für Vertraulichkeit, Verbindlichkeit und Authentizität.
  - Die Aufbewahrung geheimer Schlüssel ist vor dem Zugriff Dritter gesichert, z.B. durch den Einsatz von Smartcards.
  - Die Mitwirkung des Nutzers ist nicht nur gewünscht, sondern explizit gefordert, etwa durch Verwendung einer Smartcard und Eingabe einer PIN oder die Anzeige von Integritätsprüfergebnissen und eine vom Nutzer kontrollierbare Zertifikatsverwaltung.
  - Die Problematik eines Key Backup oder Message Recovery für verschlüsselt archivierte Daten ist geeignet zu lösen.
  - Techniken für den Zertifikatsrückruf (z.B. durch regelmäßige Herausgabe von Certificate Revocation Lists – CRLs) sind zwingend erforderlich.

5.2 Interoperabilität

Die Investition in PKI-basierte Anwendungen lohnt in vielen Bereichen nur dann, wenn auch Aussicht darauf besteht, mit externen Geschäftspartnern und Kunden auf diese Weise sicher kommunizieren zu können. Dies hat jedoch die Erfüllung einiger Interoperabilitätsanforderungen zur Voraussetzung:

- **Standardkonformität**: Die Übereinstimmung der eingesetzten Lösungen mit Standards betrifft vor allem drei Bereiche: die Dokumentenaustauschformate, das Zertifikatsformat und das Zugriffsprotokoll auf den Verzeichnisdienst. Hier setzen sich derzeit S/MIME, X.509v3 und LDAPv2/3 durch.
- **Kommunikation mit Teilnehmern fremder PKIs**: Der Austausch von verschlüsselten E-Mails muß auch mit Teilnehmern von PKIs möglich sein, deren Sicherheitsinfrastruktur (aus welchen Gründen auch immer) weniger verläßlich und sicher erscheint. Auch muß eine Anwendung auf fremde Verzeichnisdienste zugreifen können (und dürfen).
- **Schlüsseltrennung**: Bei bestimmten Anwendungen (z.B. S/MIME-Nachrichten) gehen Hersteller sehr unterschiedlich mit der nach dem Standard prinzipiell möglichen Verwendung getrennter Schlüssel für digitale Signaturen und Verschlüsselung um. S/MIME-Anwendungen müssen jedoch in allen Fällen interoperabel sein.
- **Offenheit**: Die Erfahrungen der letzten Jahre haben aber auch gezeigt, daß eine völlige Interoperabilität selbst dann nicht garantiert werden kann, wenn sich unterschiedliche Hersteller an Standards halten. In solchen Fällen sind geeignete Filter- und Zusatzfunktionen erforderlich, um dennoch eine Interoperabilität zu gewährleisten. Diese zusätzlichen Funktionen verlangen aber, daß Hersteller ihre Produkte offen gestalten, damit die erforderlichen Erweiterungen möglich sind.

5.3 Kontrolle über die PKI

Eine PKI ist eine zentrale Sicherheitsinfrastruktur in einem Unternehmen. An sie werden sowohl hohe Sicherheits- als auch Verfügbarkeitsanforderungen gestellt. Eine solche Infrastruktur sollte daher nicht ohne Not an externe Dienstleister abgegeben werden. Das hat nicht nur Sicherheitsgründe:

- Eine PKI muß eng mit dem Verzeichnisdienst eines Unternehmens verzahnt werden. Zudem müssen Zertifikate und Rückruflisten in den Verzeichnisdienst integriert werden.
- Registrierungsstellen im eigenen Haus verkürzen die Wege der Mitarbeiter bei der Zertifikatsbeantragung und -aushändigung. Die Identitätsprüfung kann dabei in enger Koppelung mit den Personalstellen erfolgen.
- PKIs müssen sehr flexibel realisiert werden. Sie müssen sowohl skalierbar sein, als auch für zusätzliche Anwendungen (mit möglicherweise speziellen Zertifikatsformaten) erweitert werden können. Auch die Neuausstellung von Zertifikaten muß schnell und „unbürokratisch„ erfolgen können, ohne daß dabei die Sicherheit der Infrastruktur gefährdet wird.
- Der Revisionsfähigkeit kommt in zahlreichen Anwendungen eine besondere Bedeutung zu. Die realisierte PKI muß jederzeit auf Korrektheit überprüft werden können. Dies ist

bereits bei der Konzeption zu berücksichtigen.

- In vielen Unternehmen ist „Branding“, d.h. der Namenseintrag im Zertifikat (Name der Zertifizierungsstelle) ein Politikum: Mitarbeiter benötigen möglicherweise (analog verschiedenen Visitenkarten) mehrere Zertifikate mit unterschiedlichem Branding. Das macht gegebenenfalls den Betrieb mehrerer CAs in einer Hierarchie erforderlich.
- Eigene unternehmensweite Sicherheitsstategien (Security Policies) und Regelungen (z.B. „Vier-Augen-Prinzip“) lassen sich wesentlich kontrollierter und konsequenter in einer PKI im eigenen Haus durchsetzen.
- Das Know-how der Sicherheitsabteilung in bezug auf eine PKI sollte im Unternehmen gehalten werden, um auch zukünftig die Kompetenz zur Weiterentwicklung der eigenen Sicherheitsstrategien und Sicherheitskonzepte zu besitzen.

6 Sicherheitsanforderungen an PKIs

Sowohl an die von PKIs unterstützten Sicherheitsdienste als auch an die Abläufe und den Aufbau der Infrastruktur sind eine Reihe von Sicherheitsanforderungen zu stellen, die im folgenden übersichtsartig zusammengefaßt werden.

6.1 Starke Kryptographie

Für PKI-basierte Sicherheitsmechanismen, die in wachsendem Maße dazu eingesetzt werden, besonders sensible Abläufe in Unternehmen vor Verfälschung oder unberechtigter Kenntnisnahme zu schützen, sind kryptographische Verfahren, die aufgrund spezieller Exportregelungen einzelner Staaten (z.B. Großbritannien, Israel, USA) „schwach„ realisiert wurden, prinzipiell ungeeignet. Von einer PKI und den eingesetzten, PKI-basierten Anwendungen müssen daher unterstützt werden:

- ausschließlich veröffentlichte und gut untersuchte symmetrische und asymmetrische kryptographische Verfahren (Triple-DES, IDEA, RSA, DSS). Der Einsatz des DES (mit einem 56 bit langen Schlüssel) sollte vermieden werden. Zukünftig wird auch der als „DES-Nachfolger“ konzipierte amerikanische AES (Advanced Encryption Standard) [AES 98] zu berücksichtigen sein.
- eine Schlüssellänge von mindestens 75, besser mehr als 90 bit bei symmetrischen Verfahren [BDR+96] und mindestens 768 bis 2048 bit bei asymmetrischen Verfahren [Fox 97]. In aktuellen Anwendung kommen für symmetrische Verfahren Schlüssel der Länge 112, 128 und 168 bit, für asymmetrische Verfahren Schlüssel der Länge 512, 768 und 1024 bit zum Einsatz.
- kollisionsresistente kryptographische Hashverfahren, denn die Unfälschbarkeit digitaler Signaturen ist in der Regel eng gekoppelt mit der Kollisionsresistenz der eingesetzten Hashfunktionen. Hashfunktionen mit einem 160 bit langen Hashwert (SHS-1, RIPEMD-160) [Dobb97] sind dabei derzeit als geeignet zu erachten. Für Anwendungen mit besonderen Sicherheitsanforderungen können zudem mehrere Hashwerte parallel genutzt werden.
- ein geeignetes Padding, bei dem die zu verarbeitenden Daten auf die benötigte Länge erweitert werden. Diese Verlängerung muß nach wohldefinierten Regeln geschehen, da sich

ansonsten Angriffsmöglichkeiten und Inkompatibilitäten ergeben können.

- (Pseudo-) Zufallszahlengeneratoren und Schlüsselwahlverfahren, die nicht-vorhersagbar sind und eine geeignete Verteilung liefern. In vielen Anwendungen sind dabei auch Verfahren verlangt, durch die sichergestellt werden kann, daß die generierten Zufallswerte frisch sind, also (im betrachteten Kontext) noch niemals zuvor erzeugt bzw. genutzt wurden.

Insbesondere muß bei den eingesetzten Lösungen sichergestellt sein, daß die Implementierung auch der Spezifikation entspricht, und nicht etwa bei der Schlüsselgenerierung nur ein kleinerer Schlüsselraum genutzt wird – sei es aufgrund von Implementierungsfehlern oder aus politischen Gründen.

6.2 Sicheres Schlüsselmanagement

Sicherheitsinfrastrukturen müssen insbesondere ein sicheres Schlüsselmanagement gewährleisten [Heus97]. Die Schlüssel der Kryptosysteme, die zur Wahrung der Vertraulichkeit im Falle der Verschlüsselung, zur Feststellung der Authentizität und Integrität im Falle der Digitalen Signatur eingesetzt werden, müssen in jeder Phase ihres Lebenszyklusses für alle Beteiligten in einem vertrauenswürdigen Zustand sein. So darf es beispielsweise nicht möglich sein, Schlüssel zu kompromittieren, sei es durch Vorausberechnen oder Raten der Schlüssel vor ihrer Erzeugung oder dadurch, daß die Qualität der Schlüssel und ihrer erzeugenden Funktionen nicht genügend geprüft wurde und so ein einfaches Verfahren angewendet werden kann, um den Schlüssel zu brechen.

Die erzeugten Schlüssel müssen authentisch an ihre Besitzer gelangen und dürfen nicht auf dem Weg dorthin abgehört, ausgetauscht werden oder gar verloren gehen. Sind die Schlüssel einmal in Gebrauch, dann müssen sie ebenfalls diesen Anforderungen genügen. Gehen Schlüssel verloren, so muß eine Sperrmöglichkeit bestehen. Werden Schlüssel ungültig oder gar kompromittiert, so muß eine sichere Vorgehensweise vorgesehen sein, wie das Schlüsselpaar vernichtet werden kann. Ebenso muß eine Vorgehensweise für die Ausstellung neuer Schlüssel festgelegt sein, um dem Benutzer möglichst schnell wieder die Nutzung aller relevanten Dienstleistungen zu ermöglichen.

Um diesen Anforderungen zu genügen, müssen Technik und Organisation aller die Schlüssel betreffenden Belange, das sogenannte Schlüsselmanagement, in geeigneter Weise gestaltet werden. Im folgenden werden einige konzeptionelle Betrachtungen zu den wichtigsten dieser Abläufe angestellt.

Erzeugen der Schlüssel: Prinzipiell gibt es zwei Orte, an denen Schlüssel erzeugt werden können. Zum einen vor Ort beim Benutzer und zum anderen bei einer externen vertrauenswürdigen Instanz. Dabei kann man wiederum zwischen Instanzen unterscheiden, die Bestandteil der Sicherheitsinfrastruktur sind oder aber externe Diensteanbieter sind. In der Praxis überwiegt die Schlüsselerzeugung in einer zentralen Instanz, da die Schlüsselerzeugung beim Benutzer eine sichere Hard- und Software und meist auch ein Grundverständnis für die Funktionsweise und den Einsatz von Public-Key-Verfahren voraussetzt. Im allgemeinen besitzen die Benutzer einer Massenanwendungen kein entsprechendes Know-how; ebenso wird ihnen aus Kostengründen nicht das nötige technische Equipment wie eine abhörsichere Umgebung zur Verfügung stehen. Schlüssel können auf unterschiedliche Weisen erzeugt werden, beispielsweise durch physikalische Rauschgeneratoren, die für die Erzeugung „zufälliger„ Werte

besonders geeignet sind. Daneben existieren mathematische Methoden wie Quasi-Zufallsgeneratoren, die die Eigenschaft besitzen, schwer vorhersagbare Systemzustände zu erzeugen, bei denen es dem Benutzer ermöglicht wird, zu von ihm frei wählbaren Zeiten in den erzeugenden Prozeß einzugreifen und ihn zu beeinflussen. Zudem können Schlüssel mit Hilfe kryptographischer Verfahren aus einigen wenigen zufälligen Ausgangsdaten „pseudozufällig„ erzeugt werden.

Rücknahme und Vernichtung der Schlüssel: Bei Rücknahme der Schlüssel ist insbesondere darauf zu achten, daß die bereits verwendeten Schlüssel nicht nochmals vergeben werden. Außerdem muß gewährleistet werden, daß die zugrundeliegende Sicherheitsstrategie (Security Policy) eingehalten wird. Werden Schlüssel in geeigneten Token (z.B. Smartcards) gespeichert, so kann bei der Rücknahme sichergestellt werden, daß keine Kopien der Schlüssel existieren. Auch die Löschung kann durch eine Vernichtung des Datenträgers relativ leicht und unwiderruflich realisiert werden.

Überprüfen der Schlüssel: Bei der Erzeugung der Schlüssel muß sichergestellt sein, daß derselbe Schlüssel nur einmal erzeugt und kein weiteres Mal einem eventuell anderen Benutzer zugeordnet wird. Um dies zu gewährleisten, kann ein Schlüsselverzeichnis verwendet werden, in dem die öffentlichen Schlüssel (oder geeignete Hashwerte) aller Benutzer gespeichert sind. Durch einen Vergleich neu erzeugter Schlüssel mit den so gespeicherten Werten kann festgestellt werden, ob der Schlüssel (und damit etwa auch ein Schlüsselpaar) schon existiert. Schlüsseldubletten können somit zumindest lokal verhindert werden. Problematisch wird es jedoch dann, wenn Schlüssel an unterschiedlichen Stellen erzeugt werden sollen. Hier sind Konzepte gefragt, mit deren Hilfe eine dublettenfreie Schlüsselgenerierung realisiert werden kann [Hors98, HoSc99].

Beglaubigen der Schlüssel: Die Beglaubigung der Schlüssel dient dazu, um dem Kommunikationspartner zu versichern, daß seinem Gegenüber der Schlüssel, den er behauptet zu besitzen, auch nachweisbar gehört. In offenen Systemen werden Schlüssel im allgemeinen nicht von einer einzigen Instanz vergeben. Die Schlüssel aller Benutzer müssen beglaubigt sein, sonst wäre es möglich, daß ein nicht rechtmäßiger Dritter die Identität eines anderen annimmt und behauptet, der rechtmäßige Besitzer des Schlüssels zu sein. Hier sind vertrauenswürdige dritte Instanzen notwendig, die die Rolle einer Beglaubigungsinstanz übernehmen. Die Zusammengehörigkeit von Schlüssel und Besitzer kann durch Zertifikate (wie X.509 [ISO 93, ISO 96]) gewährleistet werden.

Verteilen der Schlüssel: Bei Verwendung asymmetrischer (Public-Key-) Verfahren genügt bei n Teilnehmern die Übermittlung von nur insgesamt n geheimen Schlüsseln und Schlüsselzertifikaten. Werden die Schlüssel vom Benutzer selbst (lokal) und nicht von einer Instanz (zentral) erzeugt, dann sind lediglich Zertifikate zu übermitteln. Die öffentlichen Schlüssel müssen authentisch bekanntgegeben werden, beispielsweise durch einen allgemein zugänglichen Verzeichnisdienst. Falls Schlüssel ihre Gültigkeit verlieren, muß es möglich sein, daß sie zurückgerufen werden, beispielsweise durch die Verteilung von Sperrlisten.

Aufteilen von PKI-Schlüsseln: Neben den technischen und organisatorischen Fragen müssen auch personelle Aspekte berücksichtigt werden. Wie die Erfahrung zeigt, ist die Schwachstelle in einem Sicherheitssystem oft die Vertrauenswürdigkeit der eingebundenen Personen. Um ein großes Vertrauen in das System zu erhalten, ist es sinnvoll, daß alle Geheimnisse von zentraler Bedeutung wie beispielsweise die geheimen Zertifizierungsschlüssel auf mehrere

Personen verteilt werden (Vier-Augen-Prinzip) und nicht an eine einzige gebunden sind. Bei geheimen kryptographischen Schlüsseln bieten sich Konzepte wie Schwellenwertschemata [BeKe95] an, bei denen die Schlüssel nur dann verwendet werden können, wenn mehrere Personen zum selben Zeitpunkt am selben Ort sind und den Besitz von Teilgeheimnissen nachweisen.

Speichern der Schlüssel: Geheime kryptographische Schlüssel müssen sicher aufbewahrt werden. Es darf nicht möglich sein, daß Unbefugte Kenntnis über solche Schlüssel erhalten. Um dies zu garantieren, können solche Schlüssel unauslesbar auf einer Smartcard gespeichert werden, die durch eine PIN oder biometrische Verfahren derart zugriffsgeschützt wird, daß nur der rechtmäßige Besitzer diese Schlüssel verwenden kann (siehe folgendes Kapitel).

Wechseln der PKI-Schlüssel: Die Sicherheit einer Anwendung hängt maßgeblich von der Sicherheit der verwendeten (geheimzuhaltenden) Schlüssel ab. Das gilt auch für eine PKI: Werden PKI-Schlüssel wie der einer Zertifizierungsinstanz kompromittiert, dann kann im schlimmsten Fall die gesamte Infrastruktur ihre Vertrauenswürdigkeit verlieren. Oder aber eine Zertifizierungsinstanz wird durch den Verlust eines geheimen Zertifizierungsschlüssels (z.B. durch einen Defekt im Sicherheitsmodul) aktionsunfähig. Daher sollten in einer PKI regelmäßige Wechsel der relevanten PKI-Schlüssel vorgesehen werden. Auch für die Schlüssel der Benutzer sollten Vorgehensweisen für einen effizienten Schlüsselwechsel Teil des Ablaufkonzepts sein, falls beispielsweise Fortschritte in der Kryptoanalyse einen Wechsel auf größere Schlüssellängen notwendig machen.

6.3 Dienste von Zertifizierungsinstanzen

Die Aufgaben einer Zertifizierungsstelle lassen sich wie folgt gliedern: (siehe Abb. 5)

- **Beglaubigungsleistungen** wie Personalisierung, Registrierung und Zertifizierung. Sie dienen dazu, um die Authentizität von Daten und die Vertrauenswürdigkeit von Instanzen zu bezeugen.
- **Schlüsselmanagement**: Hierzu zählen Erzeugen, Zurücknahme, Beglaubigen, Verteilen, Aufbewahren, Archivieren, Wechseln und Vernichten von Schlüsseln.
- **Serverfunktionen** in Form von öffentlichen Verzeichnissen, Authentication Servern oder Archivierungssystemen, mit denen Informationen innerhalb der Sicherheitsinfrastruktur bereitgestellt werden können.

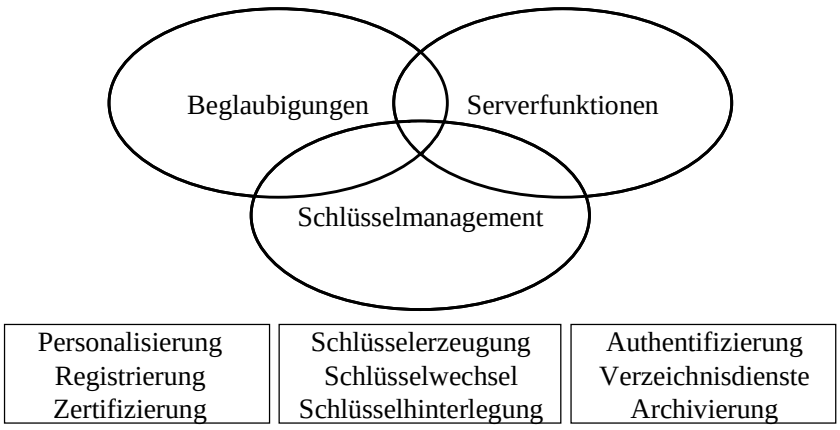

Abb. 5: Aufgaben von Zertifizierungsinstanzen

Diese Aufgaben sollten in PKIs auf unterschiedliche Instanzen verteilt werden, um eine Kontrolle der Abläufe (durch Protokollieren und Revision) zu ermöglichen („checks and balances„). Auch die personelle Zuständigkeit für die Administration der einzelnen Instanzen sollte verteilt sein, damit eine Kompromittierung von PKI-Diensten nur bei Zusammenarbeit mehrerer Personen und verteilter Komponenten möglich ist.

6.4 Smartcards als Sicherheitstoken

Moderne Smartcards mit integrierten Crypto-Chips sind nahezu ideale Medien, um die einer Person zugeordneten geheimen Schlüssel für Public-Key-Verfahren vor fremdem Zugriff geschützt aufzunehmen. Solche Smartcards werden zunehmend als Sicherheitstoken in modernen Public-Key-Infrastrukturen eingesetzt.

Dem Sicherheitstoken Smartcard kommt als Träger geheimer Schlüsselkomponenten dabei eine besondere Bedeutung zu. Im folgenden werden typische Merkmale der Einführung von Smartcards als Zertifikatsträger aufgezeigt. Dabei werden hier ausschließlich Aspekte der Personalisierung beleuchtet, daneben interessieren allerdings auch die weitere Lebensgeschichte einer solchen Smartcard – bis hin zur endgültigen Vernichtung nach Ablauf der regulären Gültigkeit. Das solchen Karten natürlich auch beliebte Sammlerstücke sind, gilt es zudem zu berücksichtigen.

Die Personalisierung einer Smartcard für den Einsatz in einer PKI kann grundsätzlich in vier Schritten geschehen. Die folgende Beschreibung gibt den prinzipiellen Ablauf wieder, spezielle Lösungen können sich dabei jedoch deutlich voneinander unterscheiden.

- In einem ersten Schritt werden die (Chipkarten-) Rohlinge **initialisiert**. Dies kann entweder beim Hersteller oder bei der zugrundeliegenden Zertifizierungsinstanz (CA) geschehen. Die Komponenten des Betriebssystems werden um die erforderlichen Filestrukturen erweitert. Diese müssen entsprechend den geplanten Anwendungen eingerichtet werden. Zudem ist die Festlegung einer Vorpersonalisierungs-PIN erforderlich, durch die insbesondere ein sicherer (manipulationsgeschützter) Transport gewährleistet werden kann. Werden die aufgeführten Prozesse durch einen Kartenhersteller ausgeführt, so erfolgt anschließend eine Lieferung der Chipkarten an die Zertifizierungsinstanz.
- In der Zertifizierungsinstanz findet eine **Vorpersonalisierung** statt. Hierzu werden entsprechend den vorgegebenen Sicherheitsanforderungen Schlüsselpaare generiert und auf der jeweiligen Karte gespeichert. Die Vertraulichkeit der geheimen Schlüsselkomponenten muß dabei gewährleistet sein, insbesondere dürfen geheime Schlüsselparameter nicht aus der Karte ausgelesen werden können. Zum Laden von Schlüsselkomponenten wird der Vorpersonalisierungs-PIN verwendet; so wird insbesondere eine unberechtigte „Fremdladung“ verhindert. Die zugehörigen öffentlichen Schlüssel werden (eventuell zusammen mit eindeutigen Kartendaten wie z.B. einer Seriennummer) in der CA gespeichert. Die so vorpersonalisierten Chipkarten werden an dafür vorgesehene Ausweisstellen (Registrierungsinstanzen – RAs) gesendet, die etwa in der Personalverwaltung angesiedelt sein können.
- Die eigentliche **Personalisierung** findet dann in einer Ausweisstelle statt. Liegt der Antrag eines Benutzers vor und ist dessen Identifikation zweifelsfrei durchgeführt, so werden eine User-PIN generiert und ein zugehöriger PIN-Brief erzeugt. Gegebenenfalls wird eine zusätzliche optische Personalisierung auf der Karte vorgenommen, etwa durch Drucken

von Name und Foto des zukünftigen Nutzers. Der Public Key wird aus der Karte gelesen und zusammen mit administrativen Daten an die CA gesendet. Die CA erzeugt das zugehörige Zertifikat. Neben dem Unique Name und dem zugehörigen Public Key enthält das (von der CA signierte) Zertifikat weitere Daten, deren Zusammensetzung sich nach der zugrundeliegenden Policy richtet. Die CA sendet das Zertifikat an die anfragende RA, die ihrerseits das Zertifikat in der Karte speichert. Anschließend werden die Karte und der PIN-Brief an den zukünftigen Nutzer ausgegeben.

- Die Personalisierung der Chipkarte wird durch die **erstmalige Nutzung** abgeschlossen. Dabei sollte der Nutzer seine initiale User-PIN ändern.

7 Praktische Schwierigkeiten

In der Praxis ergeben sich eine Reihe von Schwierigkeiten beim Aufbau und der Einführung unternehmensweiter Public-Key-Infrastrukturen. Einige der wichtigsten Aspekte, die entscheidenden Einfluß auf Erfolg und Mißerfolg eines PKI-Projekts haben, sollen hier zusammengefaßt werden.

- **Export-/Import-Beschränkungen**: Wird die PKI für eine weltweite Nutzung aufgebaut, können Export- und Importbeschränkungen einzelner Länder eine konsequente Umsetzung des Konzepts verhindern. Daher sollte eine Evaluation der zu erwartenden Hindernisse möglichst frühzeitig erfolgen, um nachträgliche Änderungen der Konzeption (z.B. Spezifikation der Smartcards, Anwendungen) zu vermeiden. Ist man jedoch auf eine Nutzung mit Partnern in anderen Geltungsbereichen angewiesen, so sind geeignete Maßnahmen zu ergreifen, damit zumindest eine eingeschränkte Anwendung ermöglicht werden kann.

- **Verfügbarkeit von Smartcards**: Smartcards mit Krypto-Chip, die hohen Sicherheitsanforderungen genügen und zugleich noch über ausreichend Speicherplatz verfügen, um eine ausreichende Anzahl verschiedener Zertifikate und Schlüssel aufzunehmen, existieren (trotz anderslautender Ankündigungen der Hersteller) bisher nur als Prototypen.

- **Implementierungsfehler**: Da das Gebiet PKI noch vergleichsweise jung ist, kämpft man bei den heute verfügbaren Produkten noch mit einer Vielzahl von Unzulänglichkeiten. Viele PKI-Produkte, das zeigt die Erfahrung mit der Evaluation aktueller Versionen, haben zudem konzeptionelle Sicherheitsmängel. Im Extremfall kann durch eine einfache Manipulation das Vertrauen in die gesamte Sicherheitsinfrastruktur gefährdet werden.

- **Proprietäre Lösungen**: Einige Hersteller haben in ihren Produkten proprietäre Erweiterungen von Zertifikaten (z.B. spezielle Extensionen) oder eigene Protokolle bzw. Protokollerweiterungen implementiert. Meist können diese Lösungen nur mit Anwendungen (oder Anwendungserweiterungen) von demselben Hersteller interoperieren oder erfordern Anpassungen bei Produkten anderer Hersteller. Eine solche Lösung ist nur dann akzeptabel, wenn es sich bei den zugrundeliegenden Anwendungen um geschlossene Systeme handelt, bei denen eine Kommunikation mit der „Außenwelt“ weder erforderlich noch gewünscht ist.

- **Standardisierungsprozesse**: Vier im Zusammenhang mit PKIs wichtige Standardisierungsvorhaben der IETF sind derzeit noch nicht abgeschlossen. Das sind die S/MIME-Spezifikation (Version 2 ist seit Juni 1998 als RFC verfügbar, Version 3 ist in Arbeit), die

PKIX-Protokolle (Kommunikation zwischen PKI-Komponenten, erste Teilspezifikation seit Januar 1999 als RFC verfügbar), das bisher noch nicht standardisierte Protokoll für den Schlüsselaustausch und die Authentifikation in IPsec sowie die Standardisierung von OpenPGP. In Deutschland spielt auch die derzeitige Weiterentwicklung des MailTrusT-Standards von TeleTrusT e.V. [Baus96] zu einer PKI-Spezifikation (MTTv2) eine wichtige Rolle. Möchte man proprietäre Lösungen vermeiden, so bleibt derzeit nur die Wahl von Produkten, die Vorversionen der Standards genügen.

- **Koordination verschiedener PKI-Aktivitäten**: Wegen der Rolle von PKIs als zentrale Sicherheitsinfrastruktur für unterschiedlichste Anwendungen ist es gerade in großen Unternehmen unvermeidlich, daß verschiedene Aktivitäten zum Aufbau einer PKI angestoßen werden. Werden diese Aktivitäten nicht rechtzeitig koordiniert, ist später eine Zusammenführung in eine strukturierte Hierarchie ohne größere Investitionen nicht mehr möglich.

8 Ausblick

Die Einführung von Public-Key-Infrastrukturen ist insbesondere in Großunternehmen unvermeidlich, sowohl zur Sicherung der unternehmensinternen Kommunikation als auch (kurzfristig) für Business-to-Business-Anwendung und (mittelfristig) für die Sicherung elektronischer Kundenbeziehungen.

Obwohl die Idee von Public-Key-Kryptoverfahren mehr als zwanzig Jahre alt ist, steckt die Entwicklung geeigneter Produkte, die den vielschichtigen praktischen Anforderungen aus heterogenen IT-Umgebungen genügen, noch in den Kinderschuhen. Dennoch ist zu erwarten, daß innerhalb der nächsten zwei bis drei Jahre die meisten Großunternehmen ihre Infrastruktur um eine PKI erweitern werden. Verwaltungen und größere mittelständische Unternehmen werden nachziehen. Die meisten dieser Infrastrukturen werden sich zwar an einigen Anforderungen des Signaturgesetzes orientieren, aber aus Kosten- und konzeptionellen Gründen keine vollständige Signaturgesetzkonformität anstreben.

Kleineren Unternehmen, Verwaltungen und Privatpersonen werden öffentliche Zertifizierungsstellen, möglicherweise konform zu einer weiterentwickelten Fassung des derzeitigen Signaturgesetzes, Zertifizierungsdienste anbieten.

Literatur

[AES 98] National Institute of Standards and Technology: Advanced Encryption Standard – AES, CD-1 Documentation, Round 1 Technical Evaluation (1998).

[Baus96] F. Bauspieß, (TeleTrusT): MailTrusT-Spezifikation, V 1.1, Stand: 18.12.1996.

[BDR+96] M. Blaze, W. Diffie, R. L. Rivest, B. Schneier, T. Shimomura, E. Thompson, M. Wiener: Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security, BSA Report, Januar 1996.

[BeKe95] A. Beutelspacher, A. G. Kersten: Verteiltes Vertrauen durch geteilte Geheimnisse, in P. Horster (Hrsg): Trust Center, DuD-Fachbeiträge, Vieweg (1995), 101-116.

[Berg99] A. Berger: Signatur-Interoperabilitätsspezifikation: Zertifikate und Dokumentenformate, Tagungsband des 9. GMD-SmartCard-Workshops, Darmstadt (1999) 15.1-15.10.

[DHR+98] S. Dusse, P. Hoffman, B. RamsdellL. Lundblade, L. Repka: S/MIME Version 2 Message Specification, IETF Network Working Group, RFC 2311, March 1998.

[DHRW98] S. Dusse, P. Hoffman, B. Ramsdell, J. Weinstein: S/MIME Version 2 Certificate Handling, IETF Network Working Group, RFC 2312, March 1998.

[Dobb97] H. Dobbertin: Digitale Fingerabdrücke – Sichere Hashfunktionen für digitale Signatursysteme, Datenschutz und Datensicherheit (DuD), 2/97, 82-87.

[EU-K98] EU-Kommission: Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingunen für elektronische Signaturen. 98/C 325/04, KOM(1998) 297, vorgelegt am 16. Juni 1998, Amtsblatt der Europäischen Gemeinschaften, 23.10.1998, 5-11.

[Fox 97] D. Fox: Fälschungssicherheit digitaler Signaturen, Datenschutz und Datensicherheit (DuD), 2/97, 69-74.

[Fox 98] D. Fox: Zu einem prinzipiellen Problem Digitaler Signaturen, Datenschutz und Datensicherheit (DuD), 7/98, 386-388.

[Fox 99] D. Fox: Zum Problem der Gültigkeitsprüfung von Schlüsselzertifikaten, in: Proceedings zum 6. Deutschen IT-Sicherheitskongreß 1999 des BSI, SecuMedia Verlag (1999) erscheint.

[Gies98] A. Giessler: Signatur-Interoperabilitätsspezifikation, in P. Horster (Hrsg.): Sicherheitsinfrastrukturen für Wirtschaft und Verwaltung – SiS-WV 98, COMPUTAS (1998) 14.1-14.10.

[GrFo98] R. Grimm, D. Fox: Entwurf einer EU-Richtlinie zu Rahmenbedingungen „elektronischer Signaturen„, Datenschutz und Datensicherheit (DuD), 7/98, 407-408.

[Grim96] R. Grimm: Kryptoverfahren und Zertifizierungsinstanzen, Datenschutz und Datensicherheit (DuD), 1/96, 27-36.

[Heus97] A. Heuser: Schlüsselversorgung von Kryptosystemen, in P. Horster (Hrsg.): Sicherheit in der Informations- und Kommunikationstechnik – SIUK 97, COMPUTAS 1997.

[Hors98] P. Horster: Dublettenfreie Schlüsselgenerierung durch isolierte Instanzen, in P. Horster (Hrsg.): Chipkarten, DuD-Fachbeiträge, Vieweg (1998) 104-119.

[HoKr96] P. Horster, P. Kraaibeek: Grundüberlegungen zu digitalen Signaturen, in P. Horster (Hrsg.): Digitale Signaturen, DuD-Fachbeiträge, Vieweg (1996) 1-14.

[HoPo94] P. Horster, M. Portz: Privacy Enhanced Mail: Ein Standard zur Sicherung des elektronischen Nachrichtenverkehrs im Internet, Datenschutz und Datensicherung (DuD), 8/94, 434-442.

[HoSc99] P. Horster, P. Schartner: Bemerkungen zur Erzeugung dublettenfreier Prim-

zahlen, in P. Horster (Hrsg.): Sicherheitsinfrastrukturen, DuD-Fachbeiträge, Vieweg (1999) 358-368.

[HoKW99] P. Horster, P. Kraaibeek, P. Wohlmacher: Sicherheitsinfrastrukturen – Basiskonzepte, in P.Horster (Hrsg.): Sicherheitsinfrastrukturen, DuD-Fachbeiträge, Vieweg (1999) 1-16.

[ITSE91] Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC), Kommission der Europäischen Gemeinschaft, EGKS-EWG-EAG (1991) ISBN 92-8263003-X.

[ITU 93] International Telecommunication Union: Information Technology – Open Systems Interconnection – The Directory: Authentication Framework. ITU-T Recommendation X.509 (1993 E).

[PeMH96] H. Petersen, M. Michels, P. Horster: Taxonomie digitaler Signaturkonzepte, in: P. Horster (Hrsg.): Digitale Signaturen, Proceedings der Arbeitskonferenz Digitale Signaturen 96, Vieweg (1996) 63-79.

[Reis98] A. Reisen: Juristische und technische Fragen bei der Umsetzung des Signaturgesetzes, in P. Horster (Hrsg.): Sicherheitsinfrastrukturen für Wirtschaft und Verwaltung – SiS-WV 98, COMPUTAS (1998) 13.1-13.9.

[SigG97] Gesetz zur digitalen Signatur (Signaturgesetz – SigG), Beschluß des Bundestages vom 13. Juni 1997 (BT-Drs. 13/7934 vom 11.06.97) und Bundesrates vom 4. Juli 1997; in Kraft seit 1. August 1997.

[SigV97] Verordnung zur digitalen Signatur (Signaturverordnung – SigV), Beschluß der Bundesregierung vom 8. Oktober 1997; in Kraft seit 1. November 1997.

[Wiss97] Wissenschaftlicher Rat der Dudenredaktion: Duden; Fremdwörterbuch, Dudenverlag, 1997.

[Zimm95] P. R. Zimmermann: The Official PGP User's Guide, MIT Press, 1995.