Erschienen in: Tagungsunterlagen zum 6. DFN-Workshop „Sicherheit in verteilten Systemen“, Hamburg, 17.-18. März 1999, S. G-1 bis G12.

Aufbau unternehmensweiter Public Key-Infrastrukturen

1 Zusammenfassung

Die Konzeption unternehmensinterner Public Key-Infrastrukturen (PKI) muß sehr unterschiedlichen Anforderungen genügen, die sich aus der technischen Entwicklung, dem Signaturgesetz (SigG) und dem Einsatz moderner Kommunikationsanwendungen ergibt. Der Beitrag gibt eine Übersicht über die wichtigsten Anforderungen und den Stand der Technik, bereichert um praktische Erfahrungen beim Aufbau von PKIs in Großunternehmen.

2 Einführung

Zweifellos hat der Boom des Internet seit 1994 für ein erheblich gewachsenes Interesse an Sicherheitslösungen gesorgt. Denn wer in seinem Unternehmen für Mitarbeiter den Zugang zum Internet ebnen möchte, will natürlich nicht zugleich umgekehrt die Unternehmensdaten für den Zugriff aus dem Internet freigeben.

Auch gut konfigurierte Firewalls lösen dieses Problem allerdings nicht vollständig. Denn wenn z. B. geographisch auseinanderliegende Teile eines Unternehmens über das Internet in Virtual Private Networks (VPN) integriert werden sollen, dann dürfen Kommunikations- und sensible Unternehmensdaten weder im Klartext übertragen werden noch während der Übertragung verfälscht werden können.

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

- Zunehmend werden moderne Kommunikationstechniken auch für Anwendungen im Business-to-Business-Bereich eingesetzt. Für den Austausch sensibler Daten und Informationen zwischen Unternehmen oder auch bei Verhandlungen dient in wachsendem Umfang E-Mail als Informationsträger. Dabei sind die übertragenen Daten meist nicht angemessen vor unberechtigtem Zugriff und Verfälschung geschützt.
- Papierbasierte unternehmensinterne Abläufe werden aus Kosten- und Effizienzgründen mehr und mehr durch elektronische Vorgänge ersetzt. Mit Workflow-Messaging-Systemen wird dabei versucht, eingespielte Abläufe durch den Einsatz moderner Kommunikationstechniken zu unterstützen, zu vereinfachen, zu vereinheitlichen und vor allem zu beschleunigen. Dabei muß jedoch nicht nur die Vertraulichkeit von Daten und Dokumenten gewährleistet werden, sondern ist meist auch sicherzustellen, daß einzelne Schritte eines Vorgangs im Falle von Fehlern oder Unstimmigkeiten nachvollzogen und im Streitfall dokumentiert und belegt werden können.
- Auch ein Teil der Kundenbeziehung wird inzwischen vielfach auf elektronischem Wege abgewickelt. 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. Dieses vielgesichtige Feld der E-Commerce-Techniken hat jedoch eines gemeinsam: einen hohen Bedarf an Sicherheitsmechanismen zum Schutz elektronischer Kundenbeziehungen.

Eine einfache Verschlüsselung der über das Internet übertragenen Daten (z. B. durch Tunneling zwischen zwei Routern oder den Einsatz von IPSec) genügt den durch diese neuen Entwicklungen entstehenden Anforderungen vor allem 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 unbekannten Netz-Teilnehmern erlauben.

Sicherheitsprotokolle und -lösungen auf der Grundlage asymmetrischer kryptographischer Verfahren, auch als Public Key-Verfahren bezeichnet, erfüllen diese Anforderungen. Durch die Verwendung öffentlicher Schlüssel erlauben sie die Erzeugung und Prüfung unfälschbarer digitaler Signaturen [Fox_97] sowie den Austausch (hybride) verschlüsselter Dokumente.

Für einen Einsatz in offenen Systemen benötigen Public Key-Verfahren eine Schlüsselinfrastruktur zur authentischen Verteilung öffentlicher Schlüssel, auch Public Key-Infrastruktur (PKI) genannt.

3 PKI-Technik

Asymmetrische Kryptoverfahren arbeiten mit Schlüsselpaaren, deren einer Schlüssel vom Schlüsselinhaber geheimgehalten werden muß, während der zweite Schlüssel als öffentlicher Schlüssel des Schlüsselinhabers bekanntgegeben wird.

Die Verschlüsselung von für einen Schlüsselinhaber bestimmten Dokumenten erfolgt mit dessen öffentlichem Verschlüssellungsschlüssel.[1] Mit seinem geheimgehaltenen Entschlüsselungsschlüssel kann der Empfänger dann die Nachricht wieder entschlüsseln.

Ähnlich können digitale Signaturen erzeugt und geprüft werden: Eine digitale Signatur zu einer gegebenen Nachricht berechnet der Schlüsselinhaber aus den Bits dieser Nachricht mit seinem geheimen Signierschlüssel. Die Prüfung, ob eine digitale Signatur zu einer vorliegenden Nachricht gehört, kann anschließend jeder vornehmen, der den öffentlichen Prüfschlüssel des Signierers kennt.

Asymmetrische Verfahren erlauben damit den Aufbau von vergleichsweise einfach strukturierten 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 einzige Einschränkung besteht allerdings: Die öffentlichen Schlüssel eines Teilnehmers müssen demjenigen, der ein Dokument an diesen verschlüsseln oder dessen digitale Signatur prüfen möchte, authentisch bekannt sein. Die Authentizität eines Schlüssels läßt sich dabei prinzipiell 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 [Zimm_95, Grim_96]: Erhält jemand von einer Person, die er kennt und der er vertraut, deren öffentlichen

---

[1] Üblicherweise wird dabei ein hybrides Verfahren verwendet: Die Daten werden zunächst mit einem symmetrischen Verschlüsselungsverfahren mit hinreichender Schlüssellänge (mind. 75, besser 90 bit) und einem zufällig gewählten Nachrichtenschlüssel verschlüsselt. Der Nachrichtenschlüssel wird dann mit dem öffentllichen Schlüssel des Empfängers asymmetrisch verschlüsselt und zusammen mit der verschlüsselten Nachricht an den Empfänger geschickt.

Schlüssel (persönlich ausgehändigt oder digital übertragen und telefonisch überprüft anhand des schlüsseleigenen „Fingerprints“), 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 ihrerseits 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 Verfahren bevorzugt. Zu öffentlichen Schlüsseln werden von zentralen, dazu speziell autorisierten und anerkannten „Zertifizierungsstellen“ (Certification Authorities, CA) 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 diesen übergeordnete Instanz bestätigt werden. Auf diese Weise entsteht ein hierarchischer „Zertifizierungsbaum“. Alle Nutzer einer solchen Infrastruktur müssen lediglich den öffentlichen Schlüssel der gemeinsamen „Wurzel-Instanz“ (Root-CA) authentisch kennen, um die Authentizität der Schlüssel aller anderen Nutzer 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) [HoPo_94]. Er findet sich wieder bei S/MIME [DHRL+_98, DHRW_98], MailTrusT [Baus_96], und in der ITU- bzw. ISO/IEC-Standardisierung für Schlüsselzertifikate, X.509 [ITU_93]. Auch das deutsche Signaturgesetz (SigG) hat sich für diesen Ansatz entschieden.

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 [SigG_97, SigV_97].

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_98, GrFo_98]: 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, -zertifizierung, -verteilung und -anwendung zusammengestellt, die für eine hohe Vertrauenswürdigkeit solcher digitaler Signaturen, die nach Signaturgesetz erzeugt wurden, sorgen sollen. Dazu zählen insbesondere:

- Für alle nach dem Signaturgesetz anerkannten Zertifizierungsstellen sind ein Sicherheitskonzept sowie regelmäßige Prüfungen vorgeschrieben.
- Die eingesetzten technischen Komponenten müssen hohen Sicherheits-Standards 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 wenigstens in den nächsten zehn Jahren nicht zu erwarten ist.
- Die geheimen Schlüssel werden in einem physisch geschützten „Sicherheits-Token“ (einer Smartcard) erzeugt und gespeichert, den sie zu keinem Zeitpunkt verlassen. 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 („Sein“) 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 zur eigenhändigen Unterschrift in der „Kommunikationsgesellschaft“) über eine gesetzliche Verankerung der Rechtswirkung digitaler Signaturen nachzudenken, wie sie heute bereits im Entwurf der EU-Kommission einer EU-Richtlinie zu digitalen Signaturen gefordert wird ([EU_98], auch zu finden unter „http://www.dud.de“).

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.

Zudem legt das Signaturgesetz die „Sicherheits-Latte“ hoch und betont damit die Bedeutung eines hohen Sicherheitsstandards in Sicherheitsinfrastrukturen für moderne Kommunikationssysteme. Auch die im Gesetz vorgesehene Kontroll-Infrastruktur, die durch eine Bindung der Betriebsgenehmigung einer Zertifizierungsstelle 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 be-

herrschen ist, ist dies für viele praktische Anwendungsfälle eine erhebliche Einschränkung.

- **Zertifikate für juristische Personen**: Das Signaturgesetz erlaubt die Ausstellung von Schlüsselzertifikaten nur 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 eigentlich aus Datenschutzgründen im Signaturgesetz vorgesehenen Mechanismus: einem Pseudonym. Der dem Pseudonym zugeordnete Mitarbeiter kann wechseln, der Schlüssel bleibt erhalten. Grundsätzlich ist es jedoch auch in vielen praktischen Fällen sinnvoll, wie bei Unterschriftsberechtigungen und Prokura in Unternehmen, Schlüsselzertifikate für juristische Personen auszustellen.
- **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 entsteht ein erheblicher zusätzlicher Kommunikationsaufwand. Auch eine rückwirkende Sperrung von Zertifikaten bei Bekanntwerden einer Schlüsselkompromittierung, der in bestimmten Fällen in der Praxis sinnvoll sein kann, ist nicht signaturgesetzkonform.
- **Ansichtskomponente**: Die (zweifellos sinnvolle) Anforderung an Signier- und Prüfkomponenten, dem Signierer resp. 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 Bits (also die Syntax), nicht aber auf den Inhalt eines Dokuments (seine Semantik) – selbst die Kodierung der Dokumenteninhalte ist nicht festgelegt. Verbreitete Office-Produkte bieten jedoch eine Vielzahl von Möglichkeiten, nichteindeutig darstellbare Dokumente zu erzeugen (versteckter Text, Notizen, Anmerkungen, Ausnutzung von Inkompatibilitäten zwischen verschiedenen Produktversionen etc.; siehe dazu [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 eingeschränkt sein.
- **Diensterbringung 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.

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 der Anerkennung einer Zertifizierungsstelle nach Signaturgesetz durch die Regulierungsbehörde ist wegen der zahlreichen und hohen Sicherheitsauflagen zeit- und kostenintensiv. Nur wenige Unternehmen werden sich daher die Einrichtung einer signaturgesetzkonformen Zertifizierungsstelle leisten wollen und können. 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 (RegTP) auf Anerkennung als Zertifizierungsstelle nach Signaturgesetz gestellt. Die Root-CA der RegTP hat am 23. September 1998 ihre Arbeit aufgenommen. Betriebsbereit ist allerdings bisher erst eine einzige Zertifizierungsstelle: Seit Januar 1999 kann in T-Punkten eine Signaturgesetzkonforme Smartcard bestellt werden, ausgegeben vom Produktzentrum Telesec der Deutschen Telekom AG.

Daß es eineinhalb Jahre nach Verabschiedung des Signaturgesetzes keine weiteren Zertifizierungsstellen gibt, hat durchaus Gründe: 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 mit Kundennähe nutzen kann.
- **Konkurrenzproblematik**: Ein Anbieter, 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, oder spezielle Business-to-Business-Applikationen) eingesetzt werden können. Da die Interoperabilitätsspezifikation (SigI) noch nicht abgeschlossen ist, gibt es zur Zeit keine einzige interoperable, d. h. nicht hersteller-spezifische (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 mindestens noch zehn Jahre dauern, bis sich das Konzept einer „Signaturschlüssel-Smartcard“ bundesweit durchgesetzt hat. Außerdem wirken die Lebensdauer von 5 Jahren, die Tatsache, daß Zertifikate nur für natürliche Pesonen ausgestellt werden, und die Beschränkung auf den deutschen Markt begrenzend. 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.

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

5 Unternehmens-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 dem Aufbau firmeninterner Public Key-Infrastrukturen begonnen.

Entscheidende Voraussetzung für die Nutzbarkeit der von PKIs bereitgestellten Schlüsseln und Zertifikaten ist dabei natürlich die Verfügbarkeit von Anwendungen, die auf asymmetrischen Verfahren beruhende Sicherheitsdienste nutzen.

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, für den Integritätsschutz übertragener Daten und die automatische Vereinbarung von symmetrischen *session keys* bei Verbindungsaufbau eingesetzt. Diese Anwendungen haben die folgenden Eigenschaften gemein:
  - vollständige Transparenz für den Nutzer, d. h. Schlüsselmanagement, Authentifikation, Integritätsschutz und Verschlüsselung erfolgen ohne aktives Eingreifen des Benutzers und im Normalfall von ihm unbemerkt
  - Ausstellung von Zertifikaten für Rechner erforderlich (z. B. *distinguished name* = IP-Adresse)
  - keine gesicherte Speicherung geheimer Schlüssel (meist in Software und ungesicherter Umgebung)
  - Zertifikats-Rückruflisten und Verzeichnisdienste sind oft nicht erforderlich, wenn die Zertifikate als Protokollelement bei Verbindungsaufbau mitgeschickt werden und eine zusätzliche Zugriffskontrolle die Berechtigungen verwaltet
  - Verwaltung geschlossener Benutzergruppen in der PKI
- **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 Originalität 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 Schlüsselpaare für unterschiedliche Dienste (zum Schutz vor aktiven Angriffen auf die Kryptosysteme, siehe [Denn_94])
  - vor dem Zugriff Dritter gesicherte Aufbewahrung geheimer Schlüssel in einem physisch geschützten Bereich (PSE, z. B. SmartCard)
  - Mitwirkung des Nutzers gewünscht und erforderlich (z. B. PIN-Eingabe, Smartcard)
  - Problematik des Key Backup/Message Recovery für verschlüsselt archivierte Daten
  - Techniken für den Zertifikatsrückruf (Sperrung von Zertifikaten im Falle des Verlustes oder der Kompromittierung des geheimen Schlüssels oder der PSE) sind erforderlich

5.2 Interoperabilität

Die Investition in PKI-basierte Anwendungen lohnt 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 (für E-Mail-Nachrichten und -Anhänge), X.509v3 und LDAPv2/v3 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. Aus Sicherheitsgründen ist eine Schlüsseltrennung zu befürworten, da sie aktive Angriffe wie den von Denning/Moore [Denn_84] grundsätzlich verhindert.

Auch die zentralen PKI-Komponenten wie Registrierungs-, Zertifizierungs- und Verzeichnisdienste sollten aus Gründen der Investitionssicherheit Interoperabilitätsanforderungen genügen:

- **Cross-Zertifizierung**: Um im Business-to-Business-Bereich unmittelbar gesichert kommunizieren zu können, kann es erforderlich sein, kurzfristig Wurzel-Zertifikate anderer Unternehmens-PKIs anzuerkennen, damit Zertifikate gegenseitig in den Anwendungen akzeptiert werden. Der PKIX-Standard bietet hierzu ein interoperables Protokoll, das inzwischen von vielen PKI-Produkten unterstützt wird. Die Infrastruktur muß außerdem intern die Verbreitung und Akzeptanz von Cross-Zertifikaten untersützen.
- **Zusammenführung existierender PKIs**: Unterschiedliche externe Anforderungen können die Zusammenführung von Teil-Infrastrukturen oder kompletten PKIs erforderlich machen – Unternehmensaquisitionen, die Unterstützung von Branchen-PKIs, Unternehmenspartnerschaften oder auch die Zusammenarbeit mit öffentlichen PKIs. Die PKI-Komponenten sollten daher die nachträgliche Einführung übergeordneter Zertifizierungsinstanzen unterstützen. Auch die authentische Integration übergeordneter Wurzel-Zertifikate in die Anwendungen muß dabei möglich sein.
- **Verzeichnisdienst**: Damit auf den Verzeichnisdienst einer PKI auch von Nutzern anderer Infrastrukturen zugegriffen werden kann, muß dieser nicht nur skalierbar sein und geeignet dimensioniert werden, sondern auch eine übliche interne Struktur aufweisen, sodaß Anwendungen beim LDAP-Zugriff Zertifikate, CRLs und ARLs an den erwarteten Stellen finden.

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 und Zertifikate sowie Rückruflisten in diesen 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.

- In vielen Unternehmen ist „Branding“, d. h. der Namenseintrag im Zertifikat (Name der Zertifizierungsstelle) ein Politikum: Mitarbeiter benötigen möglicherweise (analog verschiedenen Visitenkarten) mehrere Zertifikate von Zertifizierungsstellen mit unterschiedlichem Namen oder aus unterschiedlichen Zweigen einer Hierarchie (z. B. in internationalen Unternehmen). Das macht den Betrieb mehrerer CAs in einer Hierarchie erforderlich.
- Eigene unternehmensweite Sicherheitspolitiken 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, damit hinsichtlich der Pflege und Weiterentwicklung der eigenen Sicherheitsinfrastruktur keine Abhängigkeit des Unternehmens von externen PKI-Serviceanbietern entsteht.

5.4 Starke Kryptographie

PKI-basierte Sicherheitsmechanismen spielen zunehmend eine zentrale Rolle in Unternehmen. Sie werden in wachsendem Maße dazu eingesetzt, besonders sensible Abläufe vor Verfälschung oder unberechtigter Kenntnisnahme zu schützen.

Für solche Abläufe sind kryptographische Verfahren, die aufgrund spezieller Exportregelungen einzelner Staaten (z. B. den USA) häufig mit zu kurzen Schlüssellängen oder nicht ausreichend sicheren Verfahren 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)
- eine Schlüssellänge von mindestens 75, besser mehr als 90 bit bei symmetrischen Verfahren [BDRS+_96] und mindestens 768 bis 2048 bit bei asymmetrischen Verfahren [Fox_97]
- gut untersuchte Hashfunktionen mit einer Mindest-Ausgabelänge von 160 bit wie der SHS-1 und RIPEMD-160 [Dobb_97]
- (Pseudo-)Zufallszahlengeneratoren und Schlüsselwahlverfahren, die nicht-vorhersagbar sind und eine geeignete Verteilung liefern

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

6 Praktische Schwierigkeiten

In der Praxis stellen 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 eins 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 etc.) zu vermeiden.

- **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, sind zwar von mehreren Herstellern angekündigt, aber derzeit noch nicht erhältlich.
- **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 Mängel.
- **Proprietäre Lösungen**: Einige Hersteller haben in ihren Produkten proprietäre Erweiterungen von Zertifikaten (spezielle Extensionen, z.B. Netscape) 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.
- **Standardisierungsprozesse**: Drei 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, Status: Draft) und das bisher noch nicht standardisierte Protokoll für den Schlüsselaustausch und die Authentifikation in IPsec. In Deutschland spielt auch die derzeitige Weiterentwicklung des Mail-TrusT-Standards von TeleTrusT e.V. [Baus_96] zu einer PKI-Spezifikation (MTTv2) eine wichtige Rolle. Möchte man proprietäre Lösungen vermeinden, 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.

7 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-Anwendungen 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, z.T. 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 an den Anforderungen des Signaturgesetzes orientieren, aber aus Kosten- und konzeptionellen Gründen zunächst keine vollständige Signaturgesetzkonformität anstreben.

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

8 Abkürzungen

ARL	Authority Revocation List (Sperrliste für CA/PCA-Zertifikate)
CA	Certification Authority (Zertifizierungsstelle)

CRL	Certificate Revocation List (Sperrliste für Zertifikate)
DES	Data Encryption Standards (sym. Verschlüsselungsalgorithmus)
DNS	Domain Name Service
IDEA	International Data Encryption Algorithm (sym. Verschlüsselungsalgorithmus)
IETF	Internet Engineering Task Force
IPsec	Internet Security Protocol
IT	Informationstechnologie
LDAP	Lightweight Directory Access Protocol
MTT	MailTrusT
NIST	National Institute of Standards and Technology (USA)
PKI	Public Key Infrastructure
PKIX	Internet X.509 Public Key Infrastructure
PSE	Personal Secure Environment
RegTP	Regulierungsbehörde für Telekommunikation und Post
RIPEMD-160	Hashfunktion (Message Digest) mit einem 160 bit langen Output
RFC	Request For Comments
RSA	„Rivest, Shamir, Adleman“ – asymmetrisches Kryptoverfahren
SHS-1	Secure Hash Standard (in USA vom NIST standardisiert, 160 bit)
SigG	Deutsches Signaturgesetz
S/MIME	Secure/Multipurpose Internet Mail Extensions
SSH	Secure Shell Protocol
VPN	Virtual Private Networks
X.509v3	ISO/IEC/ITU-Standard für Schlüsselzertifikate

9 Literatur

Baus_96 Bauspieß, Fritz (TeleTrusT): *MailTrusT-Spezifikation*. Version 1.1, Stand: 18.12.1996.

BDRS+_96 Blaze, Matt; Diffie, Whitfield; Rivest, Ronald L.; Scheier, Bruce; Shimomura, Tsutomu; Thompson, Eric; Wiener, Michael: *Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security*. BSA Report, Januar 1996.

Denn_84 Denning, Dorothy E.: *Digital Signatures with RSA and Other Public-Key Cryptosystems*. Communications of the ACM, Vol. 27, No. 4, April 1984, S. 388-392.

DHRL+_98 Dusse, S.; Hoffman, P.; Ramsdell, B.; Lundblade, L.; Repka, L.: *S/MIME Version 2 Message Specification*. IETF Network Working Group, RFC 2311, March 1998.

DHRW_98 Dusse, S.; Hoffman, P.; Ramsdell, B.; Weinstein, J.: *S/MIME Version 2 Certificate Handling*. IETF Network Working Group, RFC 2312, March 1998.

Dobb_97 Dobbertin, Hans: *Digitale Fingerabdrücke. Sichere Hashfunktionen für digitale Signatursysteme*. Datenschutz und Datensicherheit (DuD), 2/97, S. 82-87.

EU_98 EU-Kommission: *Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über gemeinsame Rahmenbedingungen für elektronische Si-*

gnaturen. 98/C 325/04, KOM(1998) 297, vorgelegt am 16. Juni 1998, Amtsblatt der Europäischen Gemeinschaften, 23.10.1998, S. 5-11.

Fox_97 Fox, Dirk: *Fälschungssicherheit digitaler Signaturen*. Datenschutz und Datensicherheit (DuD), 2/97, S. 69-74.

Fox_98 Fox, Dirk: *Zu einem prinzipiellen Problem Digitaler Signaturen*. Datenschutz und Datensicherheit (DuD), 7/98, S. 386-388.

GrFo_98 Grimm, Rüdiger; Fox, Dirk: *Entwurf einer EU-Richtlinie zu Rahmenbedingungen „elektronischer Signaturen“*. Datenschutz und Datensicherheit (DuD), 7/98, S. 407-408.

Grim_96 Grimm, Rüdiger: *Kryptoverfahren und Zertifizierungsinstanzen*. Datenschutz und Datensicherheit (DuD), 1/96, S. 27-36.

HoPo_94 Horster, Patrick; Portz, Michael: *Privacy Enhanced Mail: Ein Standard zur Sicherung des elektronischen Nachrichtenverkehrs im Internet*. Datenschutz und Datensicherung (DuD), 8/94, S. 434-442.

ITU_93 International Telecommunication Union: *Information Technology – Open Systems Interconnection – The Directory: Authentication Framework*. ITU-T Recommendation X.509 (1993 E).

SigG_97 *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.

SigV_97 *Verordnung zur digitalen Signatur (Signaturverordnung – SigV)*. Beschluß der Bundesregierung vom 8. Oktober 1997; in Kraft seit 1. November 1997.

Zimm_95 Zimmermann, Philip R.: *The Official PGP User’s Guide*. MIT Press, 1995.