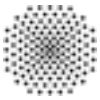


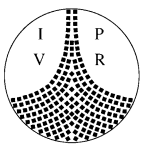
Universität Stuttgart
Fakultät Informatik

Studiengang:	Informatik
Prüfer:	Prof. Dr. rer. nat. Dr. h. c. Kurt Rothermel
Betreuer:	Dipl.-Inf. Michael Kinateder
begonnen am:	01.11.2000
beendet am:	30.04.2001
CR-Nummer:	C.2.0, E.3, K.4.4, K.6.5

Diplomarbeit-Nr. 1886

"Untersuchung aktueller Sicherheitsmodelle bezüglich ihrer Eignung für den elektronischen Handel"

Jens Musleh



Institut für Parallele und Verteilte
Höchstleistungsrechner (IPVR)
Breitwiesenstr. 20-22
70565 Stuttgart

Inhaltsverzeichnis

Kurzinhalt

Der klassische Handel verlagert sich mehr und mehr in das Internet. Immer mehr Händler entdecken es als Chance, ihre Produkte über ihren bisherigen Aktionsradius hinaus anzubieten. Beim Handel im Internet stehen einem Händler potentielle Kunden aus der ganzen Welt zur Verfügung.

Auch die Kunden nutzen die Vorteile des elektronischen Handels (E-Commerce) wie zum Beispiel den einfachen Preisvergleich und die Informationsbeschaffung über interessante Produkte.

In einem immer noch enorm wachsenden E-Commerce-Umfeld werden sowohl von Kunden- als auch von Händlerseite Anforderungen aufgestellt, die sie von den eingesetzten Sicherheitsmodellen erfüllt sehen wollen.

Eine Aufgabe dieser Diplomarbeit war es, Anforderungen an Sicherheitsmodelle, die von den Beteiligten im E-Commerce-Umfeld aufgestellt werden, zu ermitteln. Die Sicherheitsmodelle von Pretty Good Privacy, Public Key Infrastructure und Simple-PKI wurden auf die Erfüllung der Anforderungen hin getestet und die Ergebnisse dokumentiert.

Ein wichtiges Ziel beim Einsatz einer Sicherheitsarchitektur ist die Interoperabilität mit anderen Sicherheitsarchitekturen, so dass z.B. ein Kunde mit der Sicherheitsarchitektur A mit einem Händler, der die Sicherheitsarchitektur B einsetzt, zusammenarbeiten kann. Daher wurde die Anforderung nach Interoperabilität gesondert betrachtet.

Danksagung

An dieser Stelle möchte ich mich ganz herzlich bei allen Mitarbeitern der Abteilung e-Solutions-Division bei Hewlett-Packard in Böblingen für die unkomplizierte Aufnahme in ihrem Team bedanken. Besonderer Dank geht an Thomas Damrau für Betreuung der Diplomarbeit und an Udo Fink für die fachliche Unterstützung.

Mein herzlicher Dank geht vor allen Dingen an Michael Kinateder, der diese Diplomarbeit an der Universität Stuttgart betreute und mir durch unermüdliches Korrekturlesen und Abhalten von Reviews sehr geholfen hat.

Ich möchte mich auch bei meinen Kommilitonen Markus Reichart, Thomas Ziegler und Amin Hamdan für die Unterstützung während meines gesamten Studiums bedanken.

Des weiteren danke ich allen Freunden, Bekannten und den Mitarbeitern der Abteilung IT Solutions bei Agilent Technologies, die an meiner Befragung für die Anforderungsanalyse teilgenommen haben.

Nicht zuletzt möchte ich mich bei Prof. Rothermel bedanken, der es mir ermöglichte, meine Diplomarbeit in der Industrie bei Hewlett-Packard durchzuführen.

Kapitel 1 Einleitung

Das Internet ist in den letzten Jahren enorm gewachsen. War das Internet in seinen Anfangstagen noch ein kleines Netz aus Universitätsrechnern, in dem man sich gegenseitig vertrauen konnte, ist es heute (Anfang 2001) ein Netzwerk mit weit über 120 Millionen Rechnern und 440 Millionen Benutzern weltweit[1].

Selbst bei den heutigen Ausmaßen des Internets erfolgt der Großteil der Datenübertragung noch unverschlüsselt. Den meisten Benutzern ist dies nicht einmal bewusst. Erst Schlagzeilen über Hackerangriffe auf Web-Seiten oder andere Schäden durch Missbrauch oder Unachtsamkeit sorgen allmählich für ein Umdenken.

Vor allen Dingen im Bereich des elektronischen Handels ist die Datenverarbeitung besonders zu schützen. Zum Einen erwarten Kunden, dass ihre Daten bei einem Händler für Dritte unzugänglich gespeichert werden. Zum Anderen hat ein Händler ein Interesse daran, zu verhindern, dass Daten seiner Kunden und der jeweiligen bestellten Artikel beispielsweise von der Konkurrenz ausgespäht werden können.

Zur Steigerung der Sicherheit haben sich Verschlüsselungsverfahren etabliert, wie z.B. das asymmetrische Verschlüsselungsverfahren, das auf zwei mathematisch zusammenhängenden Schlüsseln basiert. Dabei kommen zwei Schlüssel zum Einsatz, von denen der eine geheim gehalten werden muss, der andere hingegen öffentlich verbreitet werden sollte. Werden Daten mit dem einen Schlüssel verschlüsselt, können sie nur mit dem passenden anderen Schlüssel wieder entschlüsselt werden. Damit entstehen zwei Anwendungsbereiche.

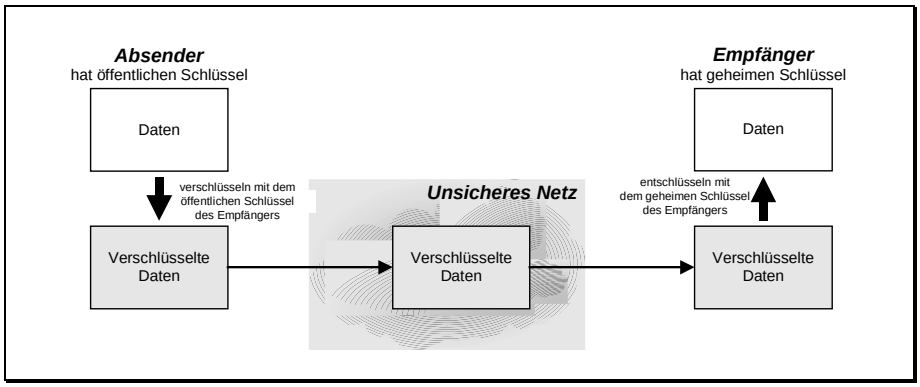


Abbildung 1.1: Übertragung von Daten mit asymmetrischen Verschlüsselungsverfahren

[1] Quelle: www.netsizer.com

Wird mit dem öffentlichen Schlüssel verschlüsselt, können die Daten nur vom Besitzer des passenden geheimen Schlüssels entschlüsselt werden. Somit kann jeder, der einen öffentlichen Schlüssel hat, dem Besitzer des dazu gehörenden geheimen Schlüssels eine verschlüsselte Nachricht schicken. Nur der Inhaber des geheimen Schlüssels kann die Nachricht entschlüsseln (siehe Abbildung 1.1).

Die andere Möglichkeit besteht darin, dass mit dem geheimen Schlüssel Daten verschlüsselt werden, die dann mit dem passenden öffentlichen Schlüssel von jedem entschlüsselt werden können. Dabei entsteht eine Art Unterschrift, denn die Daten konnten nur vom Besitzer des geheimen Schlüssels verschlüsselt werden.

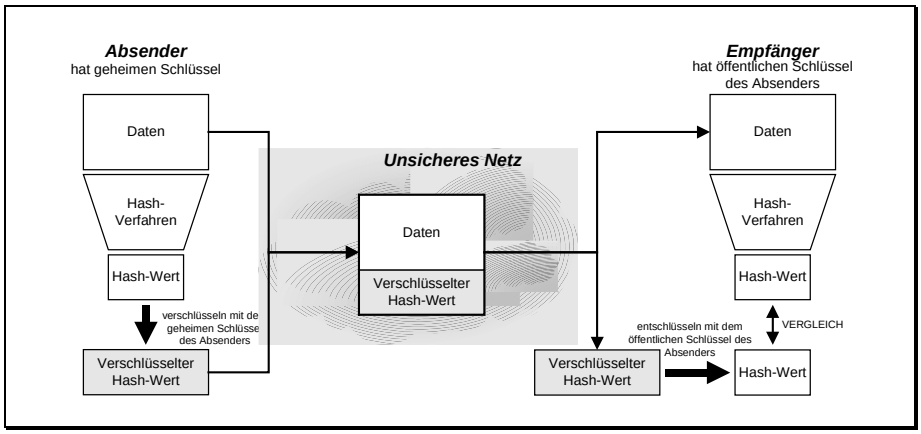


Abbildung 1.2: Prinzip der digitalen Signatur

Da die Verschlüsselung mit diesem Verfahren etwas aufwendig ist, werden die zu unterschreibenden Daten nicht komplett verschlüsselt. Es wird vielmehr aus den Daten eine Zahlenfolge gebildet, die eine Art Fingerabdruck der Daten darstellt. Diese Zahlenfolge wird Hash-Wert genannt. Würde man die Daten kopieren und auch nur ein Zeichen verändern, ergäbe sich ein anderer Hash-Wert. Somit ist es ausreichend, nur den Hash-Wert mit dem geheimen Schlüssel zu verschlüsseln. Der Empfänger der unterschriebenen Daten kann den Hash-Wert mit dem öffentlichen Schlüssel entschlüsseln und mit dem selbst ermittelten Hash-Wert vergleichen.

Dabei entsteht jedoch das Problem herauszufinden, ob ein gegebener öffentlicher Schlüssel tatsächlich von der fraglichen Person stammt. Abhilfe schaffen so genannte Zertifikate, die bestätigen, dass ein öffentlicher Schlüssel einer bestimmten Person gehört. Diese Bestätigung wird digital unterschrieben. Der öffentliche Schlüssel, der zur Validierung des Zertifikats benötigt wird, muss jedoch aus einer sicheren Quelle stammen.

Seit rund zehn Jahren steht der Internetgemeinde nun Pretty Good Privacy (PGP) von Philip Zimmermann kostenlos zur Verfügung. Dieses Produkt nutzt das vorgestellte asymmetrische Verschlüsselungsverfahren für die Sicherung des E-Mail-Verkehrs. Inzwischen sind etliche Zusatzfunktionen hinzugekommen, die über das einfache Verschlüsseln von E-Mails hinausgehen. So stellt sich die Frage, ob PGP nicht auch für E-Commerce-Lösungen geeignet sein könnte.

In PGP werden die Zertifikate von den Benutzern selbst erstellt. Öffentliche Schlüssel in Kombination mit einem Namen werden meist von Privatpersonen zertifiziert. Benutzer müssen daher für Zertifikate entscheiden, ob sie darauf vertrauen, dass der Zertifikatsersteller die Zuordnung zwischen öffentlichem Schlüssel und angegebenem Namen kontrolliert hat.

Alternativ dazu entwickelte sich das Konzept der Public Key Infrastructure (PKI). Im Gegensatz zu PGP werden öffentliche Schlüssel von einer zentralen Instanz zertifiziert. Der Benutzer muss somit (im Idealfall) nur einmal entscheiden, ob er dem Zertifikatsersteller vertraut.

Damit nicht alle Benutzer von einer einzelnen Zertifizierungsstelle abhängig sind, kann aus mehreren Zertifizierungsstellen eine Architektur gebildet werden. Die Zertifizierungsstellen zertifizieren sich gegenseitig, um dem Benutzer Arbeit zu ersparen.

Dadurch können jedoch umfangreiche Strukturen entstehen, die eine komplexe Administration erforderlich machen. Dem entgegenzuwirken ist das Ziel der Simple-PKI, in der versucht wird, den Ansatz der globalen Namensräume aufzugeben und durch lokale Namensräume zu ersetzen. Dadurch soll speziell die Authentifizierung mit Hilfe von Zertifikaten vereinfacht werden.

1.1 Aufgabenstellung

Ziel der Arbeit ist die Untersuchung bestehender Sicherheitsmodelle, insbesondere auf ihre Eignung im Bereich des E-Commerce hin.

Um eine Untersuchung durchführen zu können, muss eine möglichst umfassende Sammlung von Anforderungen an die Sicherheit aller beteiligten Parteien des E-Commerce angefertigt werden. Dazu werden drei Informationsquellen verwendet: Zunächst wird in Fachliteratur recherchiert, um die grundsätzlichen Anforderungen, wie zum Beispiel der Geheimhaltung, Wahrung der Integrität von Nachrichten und der Authentifizierung, festzuhalten. Anschließend werden im Internet verschiedene E-Commerce Lösungen begutachtet, um weitere Anforderungen zu ermitteln.

Auf der Grundlage der gefundenen Anforderungen werden mehrere Personengruppen befragt. Dazu gehören Personen der Abteilung e-Solutions-Division bei Hewlett-Packard, die in der Entwicklung von E-Commerce-Lösungen tätig sind, Personen der Abteilung IT-Solutions bei Agilent Technologies, die Intranet-Plattformen für Mitarbeiter der Agilent Technologies entwickeln, Informatik-Studenten der Universität Stuttgart und Personen, die nicht direkt mit dem Thema Sicherheit vertraut sind, um auch ein Bild aus der Sicht der Endanwender zu erhalten.

Anschließend erfolgt die Auswahl der zu untersuchenden Sicherheitsmodelle. Es werden in Abstimmung mit Hewlett-Packard die drei Sicherheitsmodelle PGP, PKI und Simple-PKI ausgewählt. Es folgt eine Einarbeitung in die Konzepte, die verwendeten Kryptoalgorithmen und die Art der Vertrauensbildung dieser Sicherheitsmodelle.

Für die Untersuchung der Sicherheitsmodelle werden jeweils Produkte ausgewählt, um die Erfüllung der Anforderungen an einem Beispiel zu testen. Für PGP wird das Produkt *PGP Desktop Security* der Firma Network Associates, Inc. verwendet. Als Beispiel für eine PKI wird die UniCERT-PKI der Firma Baltimore Technologies plc. ausgewählt. Im Bereich der Simple-PKI wird zurzeit noch geforscht, daher kann kein bestimmtes Produkt ausgewählt werden.

1.2 Gliederung der Arbeit

Die Arbeit gliedert sich in die drei Aufgabenpakete: *Anforderungsanalyse*, *Auswahl und Einarbeitung in verschiedene Sicherheitsmodelle*, *Test dieser Sicherheitsmodelle auf die Erfüllung der ermittelten Anforderungen*. Eine wichtige Anforderung im Umfeld des E-Commerce ist die Erfüllung der Interoperabilität zwischen den Sicherheitsmodellen. Diese zu testen, ist eine weitere Aufgabe dieser Diplomarbeit.

Nach einer kurzen Einleitung in Kapitel 1 erfolgt die Vorstellung der ermittelten Anforderungen in Kapitel 2. Die Anforderungsanalyse wird, wie beschrieben, zusammen mit verschiedenen Personengruppen, Internetrecherchen und dem Studium von Fachliteratur durchgeführt.

Danach werden Sicherheitsmodelle ausgewählt, die in dieser Arbeit zu behandeln sind. Diese werden in Kapitel 3 vorgestellt. Kapitel 3 enthält auch Informationen zu verschiedenen Kryptoverfahren, die in den Sicherheitsmodellen zum Einsatz kommen.

In Kapitel 4 werden die Ergebnisse der untersuchten Anforderungen für jedes Sicherheitsmodell aufgezeigt. Im letzten Abschnitt des 4. Kapitels werden die Sicherheitsmodelle gegenübergestellt und die herausragenden Eigenschaften vorgestellt.

Die Fähigkeit der Interoperabilität der vorgestellten Sicherheitsmodelle wird in Kapitel 5 gezeigt. Schließlich erfolgt im letzten Kapitel eine Zusammenfassung der Diplomarbeit.

Kapitel 2 Anforderungsanalyse

In diesem Kapitel werden Anforderungen an Sicherheitsmodelle ermittelt. Um ein möglichst umfassendes Ergebnis zu erzielen, wurde neben der Recherche in den jeweils genannten Büchern und Internetquellen eine Befragung verschiedener Personengruppen durchgeführt. Befragt wurden Mitarbeiter der Abteilung e-Solutions Division bei Hewlett-Packard, Mitarbeiter der Abteilung IT-Solutions bei Agilent Technologies und Studenten der Fachrichtung Informatik der Universität Stuttgart. Auch Personen, die nicht unmittelbar mit dem Thema Sicherheit vertraut sind, wurden befragt. Dadurch sollten Aspekte entdeckt werden, die Sicherheitsexperten als zu trivial eingestuft hätten.

Als Vorbereitung auf die Befragung wurden verschiedene Bereiche festgelegt, in denen Sicherheit erwünscht ist. Es wurden die Bereiche *E-Mail-Austausch*, *Internet*, *Geld* und *E-Commerce* bestimmt, deren Anforderungen in den folgenden Abschnitten vorgestellt werden.

Im vorletzten Abschnitt dieses Kapitels wird auf die Anforderungen an Sicherheitsarchitekturen eingegangen. In einer Sicherheitsarchitektur werden alle Komponenten, die jede eine spezielle Aufgabe im Netz übernimmt und einen bestimmten Bereich absichert, zu einer Architektur zusammengefasst. Diese Architektur muss ein einheitliches Management-System besitzen, das globale Regeln kontrolliert, sicherheitsrelevante Ereignisse protokolliert und alle Netzwerkkomponenten zentralisiert steuert.

Abschließend werden im letzten Abschnitt die Anforderungen in Bezug auf Interoperabilität aufgezeigt. Interoperabilität ist in Unternehmen ein wichtiges Thema, da nur durch eine gute Unterstützung der Interoperabilität ein Umstieg auf andere Produkte möglich wird. Dabei muss ein Umstieg nicht freiwillig sein, wenn z.B. der Hersteller des eingesetzten Produktes dieses nicht mehr weiterentwickelt.

2.1 Anforderungen an E-Mail Sicherheitsmodelle

Um Anforderungen im Bereich des sicheren E-Mail-Austauschs aufstellen zu können, muss zunächst bestimmt werden, was darunter zu verstehen ist. E-Mail-Austausch bezeichnet das Versenden von Nachrichten über ein Netzwerk an einen oder mehrere bestimmte Empfänger. Dazu müssen sich Absender und Empfänger im selben Netzwerk (z.B. das Internet) befinden, so dass eine einheitliche Adressierung möglich ist. Sollten sich Absender und Empfänger nicht im selben Netzwerk befinden, müssen E-Mails über ein oder mehrere Gateways von einem in das andere Netzwerk transferiert werden.

Standardmäßig betrifft der E-Mail-Versand das Verschicken von ASCII-Texten; E-Mails können jedoch auch digitale Daten beliebiger Art enthalten, die als Anhang mitgeschickt werden. Dazu wird der Anhang mit Hilfe des MIME-Systems (Multipurpose Internet Mail Exten-

sions, [RFC2045-49]) in ASCII Zeichen umgewandelt. Jedes Mail-System ist in der Lage, mit diesem reduzierten Zeichensatz umzugehen. Auf der Empfängerseite können die ASCII Zeichen dann wieder in ihre ursprüngliche Form gebracht werden.

Zu einem Mailsystem gehören Mail-Clients und Mail-Server. Die Mail-Server nehmen Nachrichten von den Mail-Clients entgegen und liefern sie über zwischengeschaltete Mail-Server bis an den Mail-Server des Empfängers aus. Das Simple Mail Transfer Protocol (SMTP), das hierfür zum Einsatz kommt, ist in [RFC821] spezifiziert. Der Mail-Client des Empfängers kann ankommende E-Mails beim Ziel-Mail-Server abholen, wobei entweder das Post Office Protocol (POP3, spezifiziert in [RFC1939]) oder das Internet Message Access Protocol (IMAP, spezifiziert in [RFC2060]) verwendet werden kann. Die Mail-Clients übernehmen die Kommunikation mit den Mail-Servern und bieten dem Benutzer vielfältige Funktionen zur Verwaltung von E-Mails.

Die gesamte Kommunikation zwischen Mail-Clients und Mail-Servern sowie zwischen den Mail-Servern untereinander läuft unverschlüsselt ab. Dadurch wird es potentiellen Angreifern sehr leicht gemacht, E-Mails mitzulesen, zu verändern, zu löschen oder umzuleiten. Die erste Version des SMTP erlaubt die Angabe eines beliebigen Absendernamens. Da diese noch sehr häufig verwendet wird, kann der Empfänger der Angabe des Absendernamens nicht vertrauen.

2.1.1 Grundlegende Sicherheitsanforderungen

Aufgrund der eben genannten Schwierigkeiten beim E-Mail-Austausch ergeben sich zunächst folgende Anforderungen:

- **Geheimhaltung**: Es muss sichergestellt sein, dass auf dem Weg zwischen dem Absender und dem gewünschten Empfänger niemand die Nachricht mitlesen kann.

  Die Geheimhaltung wird über die Verschlüsselung der Nachricht erreicht. Dabei können symmetrische oder asymmetrische Verschlüsselungsverfahren verwendet werden. Diese werden in Kapitel 3 näher beschrieben.

- **Integrität**: Die Integrität der Nachricht muss sichergestellt werden, d.h. der Absender kann sicher sein, dass seine Nachricht auf dem Weg zum Empfänger nicht verändert worden ist.

- **Authentifizierung**: Der Empfänger muss sicher sein können, dass es sich tatsächlich um den angegebenen Absender handelt.

  Integrität und Authentifizierung werden über digitale Signaturen erreicht. Dazu muss der Absender einen geheimen Signaturschlüssel besitzen, mit dem die digitale Signatur erzeugt wird. Der zum Signaturschlüssel gehörende öffentliche Prüfschlüssel muss dem Empfänger vorliegen. Mit dem Prüfschlüssel kann der Empfänger die Authentizität und die Integrität prüfen.

Eng verknüpft mit der Authentifizierung ist auch die Anforderung, dass der Absender einer E-Mail später die gesendete Nachricht nicht leugnen kann:

- **Unleugbarkeit**: Diese Eigenschaft ermöglicht dem Empfänger einer E-Mail den Nachweis darüber, dass der Absender die Nachricht tatsächlich abgeschickt hat. Der Absender hat also keine Möglichkeit, seine gesendete E-Mail später zu leugnen.

Um Unleugbarkeit zu erreichen muss der Absender eine signierte E-Mail verschicken. Da nur der Absender die digitale Unterschrift erstellt haben kann, hat der Empfänger damit einen Nachweis darüber, dass die E-Mail vom Absender stammt. Der Absender kann also nur sehr schwer abstreiten, dass er eine von ihm selbst signierte E-Mail abgesendet hat.

2.1.2 Sicherer E-Mail-Austausch

Die im vorigen Abschnitt genannten Anforderungen betreffen den Schutz der Information selbst. Man kann jedoch auch die Anforderung stellen, dass der gewünschte Mail-Server erreichbar ist. Um eine hohe Verfügbarkeit des Mail-Servers zu erreichen, muss er vor nicht autorisiertem Zugriff geschützt werden. Dies macht entsprechende Sicherheitsmaßnahmen erforderlich.

In [Stra98] heißt es folgendermaßen:

- **Verfügbarkeit**: Schutz der Systemressourcen vor nicht autorisiertem Zugriff, um Verfügbarkeit für autorisierte Benutzer garantieren zu können. Unter Systemressourcen versteht man u.a. Prozessoren, Speicher, Kommunikationskanäle, Programme.

Wird ein Mail-Server nicht ausreichend geschützt, sind beispielsweise so genannte Denial-of-Service-Attacken möglich. Diese zielen darauf ab, einen Server (dabei muss es sich nicht zwangsläufig um einen Mail-Server handeln) so zu überlasten, dass er für die eigentlich vorgesehenen Benutzer nicht mehr erreichbar ist. Meist sind diese Attacken gegen Implementierungsfehler in Betriebssystemen, Server-Programmen oder andere Dienste gerichtet, die auf dem selben Rechner laufen. Es werden auch grundsätzliche Entwurfsschwächen von Netzwerkprotokollen ausgenutzt, um einen Server zum Absturz zu bringen.

In [KPS98] werden noch weitere Anforderungen an den sicheren E-Mail Austausch genannt. Einige dieser Anforderungen (und auch der vorher genannten Anforderungen) wurden in der Befragung auch von E-Mail-Anwendern, die mit den Sicherheitstechnologien nicht so vertraut sind, immer wieder genannt.

- **Absendenachweis**: Der Absender erhält vom Mailsystem eine Bestätigung über die Entgegennahme der E-Mail. Diese Eigenschaft ist vergleichbar mit einem Brief, den man bei der Post als Einschreiben abgibt. Im Gegensatz zum Einschreiben wäre zudem möglich, die entgegengenommene E-Mail zu signieren. Dadurch erhält der Absender sogar eine Bestätigung über die Abgabe einer E-Mail inklusive des Inhalts.

- **Zustellungsnachweis**: Nach der Zustellung der E-Mail beim Empfänger durch das Mailsystem erhält der Absender eine Bestätigung hierüber. Auch in diesem Fall wäre es möglich, dass das Mailsystem, das dem Empfänger die E-Mail zustellt, die vom Absender gesendete Nachricht signiert.

- **Vertraulicher E-Mail-Fluss**: Als weitere Anforderung kann vom Absender oder Empfänger aufgestellt werden, dass ein Dritter nicht feststellen kann, ob überhaupt eine Nachricht versendet wurde.

- **Anonymität**: Beschreibt die Eigenschaft, dass ein Absender eine E-Mail versenden kann, ohne dass der Empfänger weiß, von wem die E-Mail stammt.

- **Eingrenzung**: Manche E-Mail-Anwendungen machen es erforderlich, dass Mails nur in Teilnetzen weitergeleitet werden, die den geforderten Sicherheitsstandards entsprechen. Dazu erhält jedes Teilnetz eine bestimmte Sicherheitseinstufung und Router schicken Mails, die jeweils durch eine Sicherheitsstufe gekennzeichnet sind, nur in die passenden Teilnetze weiter.

- **Audit**: Dabei handelt es sich um die Eigenschaft des Netzwerks, bestimmte Ereignisse aufzuzeichnen, z.B. dass jemand zu einem bestimmten Zeitpunkt eine Mail abgeschickt hat. Dadurch könnte auch ein Nachweis geführt werden, wenn jemand versucht, eine abgesandte E-Mail zu leugnen.

- **Selbstzerstörende Mails**: Ein Absender könnte die Anforderung haben, dass eine Mail nur genau einmal gelesen werden kann. Dazu müsste das Mailsystem ein Flag in der Mail einführen, das anzeigt, dass es sich um eine selbstzerstörende Mail handelt. Das Mailsystem beim Empfänger müsste sicherstellen, dass die Mail nicht weitergeleitet oder gespeichert werden kann. Ferner müssen alle zwischengeschalteten Mail-Server die Mail verwerfen, sobald sie weitergeleitet wurde.

- **Nachrichten-Reihenfolge**: Manche Anwendungen machen es erforderlich, dass Mails in der Reihenfolge ankommen, wie sie abgesendet wurden. Dabei dürfen auch keine Mails verloren gehen. Diese Anforderung ist für den sicheren E-Mail-Austausch nicht entscheidend, könnte aber durch ein Sicherheitsmodell erfüllt werden.

Die meisten dieser Anforderungen werden von Mailsystemen bereits erfüllt. Manche Anforderungen erfordern jedoch eine gute Zusammenarbeit zwischen verschiedenen Arten von Mailsystemen. Als Beispiel seien hier die selbstzerstörenden Mails genannt. Da nicht jedes Mailsystem dieses Merkmal unterstützt, kann der Absender nicht sicher sein, dass seine Anforderung, die Mail nach dem Lesen zu löschen, erfüllt wird. Der Empfänger hätte die Möglichkeit, diese Mail zu speichern oder weiterzuleiten, obwohl es vom Absender beim Versenden der E-Mail anders angegeben wurde.

Andere Anforderungen können erst durch Erweiterungen der vorhandenen Mailsysteme erfüllt werden. Selbst die naheliegendste Anforderung nach Datenschutz wird in den meisten Fällen nur durch eine Erweiterung der Mail-Clients erfüllt. Sehr problematisch ist jedoch, dass den meisten Benutzern nicht bekannt ist, dass E-Mails sehr leicht „abhörbar“ sind. Dies kann beispielsweise direkt an einer Leitung geschehen oder aber auch in zwischengeschalteten Mailsystemen.

Wird eine Sicherheitslösung für Mailsysteme in einem Unternehmen eingeführt, ist es wichtig, dass das zu erzielende Sicherheitsniveau möglichst hoch ist, um die mit der Einführung verbundenen Kosten zu rechtfertigen. Welche Faktoren das Sicherheitsniveau beeinflussen, wird im nächsten Abschnitt erläutert.

2.1.3 Anforderungen bezüglich geheimer Schlüssel

Da für die Entschlüsselung und das Signieren von Nachrichten geheime Schlüssel verwendet werden und diese naturgemäß geheim gehalten werden müssen, muss sie das System in einem geschützten Bereich ablegen. Zugriff auf diesen Bereich darf nur dem Besitzer der geheimen Schlüssel gewährt werden. Die Anforderungen in diesem und im folgenden Abschnitt wurden aus [Fox00] entnommen.

- **Sichere Verwahrung der Schlüssel**: Speicherung des geheimen Schlüssels in einem so genannten Personal Security Environment (PSE), z.B. auf einer Smartcard oder in einer Datei, die mit einem als sicher geltenden Verschlüsselungsverfahren geschützt wird.

Die beste Möglichkeit, diese Anforderung zu gewährleisten, ist es den geheimen Schlüssel auf einer Smartcard zu speichern. Der Vorteil dieser Lösung ist, dass der geheime Schlüssel die Smartcard nicht verlässt, da zu verschlüsselnde Daten direkt auf der Smartcard verschlüsselt werden.

Zusätzliche Sicherheit der geheimen Schlüssel bietet die so genannte Passphrase. Es handelt sich hierbei um ein Passwort, das bei jeder Verwendung des geheimen Schlüssels eingegeben werden muss. Somit kann ein geheimer Schlüssel nicht von unbefugten Personen verwendet werden. Die Passphrase sollte so gewählt werden, dass sie nicht durch systematische Rateangriffe in kurzer Zeit bestimmt werden kann. Im Zusammenhang mit Smartcards werden statt einer Passphrase normalerweise PINs (Personal Identification Number – besteht in der Regel nur aus Ziffern) verwendet.

Um sicherzustellen, dass es sich bei einem öffentlichen Schlüssel tatsächlich um den Schlüssel einer bestimmten Person handelt, wird er von einer Zertifizierungsstelle signiert und das Ergebnis als Zertifikat zurückgegeben. Dieses Zertifikat enthält u.a. den eindeutigen Namen des Inhabers des öffentlichen Schlüssels, den öffentlichen Schlüssel selbst und die Signatur der Zertifizierungsstelle. An das Zertifizierungssystem werden folgende zwei Anforderungen gestellt:

- **Verlässliche Identitätsprüfung**: Die Identität des Schlüsselinhabers muss in verlässlicher Weise von der Zertifizierungsstelle geprüft werden. Ferner sollte das erstellte Zertifikat eine beschränkte Gültigkeit haben.

- **Rücknahme ausgestellter Zertifikate**: Sollte die Passphrase oder die PIN verloren gehen oder der Verdacht auf Kompromittierung bestehen, muss das Zertifikat für ungültig erklärt werden. Dazu werden bei der Zertifizierungsstelle so genannte Certificate Revocation Lists (CRL) geführt, die periodisch von den Mail-Clients geladen werden oder online für ein bestimmtes Zertifikat abgefragt werden können.

Um das gewünschte Sicherheitsniveau einhalten zu können, ist es wichtig, dass die verwendeten Sicherheitsfunktionen keine Implementierungsfehler aufweisen.

- **Fehlerfreiheit der Implementierung**: Die Funktionen zum Ver- und Entschlüsseln von Nachrichten sowie des Schlüsselmanagements dürfen keine Implementierungsfehler aufweisen.

Ob ein System frei von Fehlern ist, könnte man z.B. von einem externen Unternehmen prüfen lassen.

2.1.4 Interoperabilität des Mail-Systems

Durch die hohe Verbreitung des Internets haben sich die Internet-Protokolle für E-Mail inzwischen als Standard durchgesetzt. Daher stellt auf dieser Ebene mangelnde Interoperabilität kein Hindernis dar. Selbst Netzwerke, die nicht auf Internet-Protokollen aufbauen, wie z.B. X.400, können vom Internet über Gateways erreicht werden. Die meisten proprietären E-Mail-Protokolle (z.B. Lotus Notes, Novell MHS) wurden inzwischen durch Internet-Protokolle abgelöst.

Die abgelösten Protokolle wurden hauptsächlich für den internen E-Mail Austausch innerhalb eines Unternehmens eingesetzt. In abgeschlossenen Netzwerken stellten die proprietären Lösungen kein Problem dar. Will man jedoch auch E-Mails mit Personen außerhalb des Unternehmens austauschen, müssen alle beteiligten Partner einen allgemeinen Standard verwenden.

Auch E-Mail Sicherheitslösungen sollten auf allgemein verwendeten Standards aufbauen, so dass eine sichere Kommunikation über das Unternehmensnetzwerk hinaus möglich ist. Verschiedene Sicherheitsmodelle müssen in folgenden Punkten interoperieren können:

- **Zertifikatsformat**: Es muss einen gemeinsamen Nenner der verwendeten Felder in den auszutauschenden Zertifikaten geben, die von allen Sicherheitsmodellen ausgewertet werden können.

- **Zertifikats-Austauschformat**: Zertifikate erhält man aus unterschiedlichen Quellen. Es muss möglich sein, Zertifikate über ein Medium austauschen zu können. Die erhaltenen Zertifikate werden vom Mail-Client in einer lokalen Datenbank abgespeichert. Daher muss ein Sicherheitsmodell in der Lage sein, Zertifikate importieren zu können.

- **Nachrichten-Austauschformat**: Verschlüsselte oder signierte Nachrichten werden in einem bestimmten Format versendet. Dieses Nachrichten-Austauschformat sollte einheitlich sein, so dass Mail-Clients mit verschiedenen installierten Sicherheitsmodellen Mails der jeweils anderen Implementierung verarbeiten können.

Aus diesen drei Punkten lässt sich die folgende Anforderung an eine E-Mail Sicherheitslösung ableiten:

- **Verbreitung des Protokolls**: Da zurzeit verschiedene Lösungen für den sicheren E-Mail-Austausch existieren (zum Beispiel PGP oder S/MIME – diese werden in Kapitel 3 vorgestellt) und eine sichere Kommunikation zwischen diesen nicht möglich ist, sollte ein Sicherheitsmodell gewählt werden, das entweder allgemein einen hohen Verbreitungsgrad hat oder das von den zu erwartenden Kommunikationspartnern eingesetzt wird.

2.1.5 Bedienungsfreundlichkeit

Damit sich eine Sicherheitslösung im E-Mail Bereich durchsetzen kann, muss sie von den Benutzern verwendet werden. Dies lässt sich jedoch nur durch eine intuitive und einfach zu benutzende Oberfläche realisieren. Komplizierte Systeme, auch wenn sie auf bestehenden und somit bekannten Mailprogrammen aufsetzen, werden von den Benutzern kaum akzeptiert werden.

- **Integration in das Mailprogramm**: Die gewählte Sicherheitslösung muss sich möglichst nahtlos in das Mailprogramm des Benutzers integrieren lassen.

- **Transparente Prüfung**: Entschlüsselung bzw. Prüfung einer digitalen Signatur sollten für den Benutzer transparent ablaufen. Lediglich das Prüfergebnis (korrekte oder falsche digitale Signatur) sollte dem Benutzer in klarer und verständlicher Weise angezeigt werden. Idealerweise werden dem Benutzer die weiteren Handlungsschritte dargestellt.

- **Durchsetzung einer Sicherheitspolicy**: Wird eine Sicherheitslösung unternehmensweit eingesetzt, sollte es möglich sein, eine Vorauswahl an Sicherheitseinstellungen als Standardeinstellungen in diesem Unternehmen vorgeben zu können.

- **Einfache Zertifikatsverwaltung**: Um die Integrität der Zertifikatsdatenbank zu gewährleisten, sollte es dem Benutzer nicht gestattet werden, manuell in die Datenbank einzugreifen. Die folgenden Funktionen sollten daher automatisch ablaufen:

    - automatische Zuordnung empfangener Zertifikate zur jeweiligen E-Mail Adresse.

    - automatischer Empfang und anschließende Auswertung von CRLs (dabei sollten gesperrte Zertifikate jedoch nicht aus dem lokalen Speicher gelöscht werden, sondern entsprechend markiert werden, so dass später bereits empfangene E-Mails noch geprüft werden können).

    - einfache bzw. automatische Suche nach Kontakten in Verzeichnisdiensten mit automatisiertem Import des dazugehörigen Zertifikats.

2.2 Sicherheit im Internet

In diesem Abschnitt werden die Anforderungen ermittelt, die beim Surfen im Internet aufkommen. Unter Surfen im Internet versteht man das Betrachten von Inhalten, die auf verschiedenen Servern im Internet verteilt sein können. Die einzelnen Dokumente sind über Links miteinander verbunden. Klickt man auf einen der Links, wird im Browser das zugeordnete Dokument angezeigt. Um dem Benutzer die Möglichkeit zu geben, Daten an den Server zu schicken, wurden Internet-Formulare eingeführt.

2.2.1 Anforderungen an Sicherheit im Internet

Für die Kommunikation zwischen zwei Rechnern über das Internet gelten ähnliche Anforderungen, wie bei E-Mails. Es können folgende Anforderungen ermittelt werden:

- **Geheimhaltung**: Kein Dritter darf den Inhalt des Datenflusses zwischen zwei Rechnern im Internet abhören können.

- **Integrität**: Mit dieser Anforderung soll sichergestellt werden, dass kein Dritter den Inhalt des Datenflusses zwischen zwei Rechnern im Internet verändern kann, ohne dass es von den Kommunikationspartnern bemerkt wird.

- **Verfügbarkeit**: Von Servern im Internet wird eine hohe Verfügbarkeit gefordert. Diese Forderung geht hauptsächlich von den Anbietern der Inhalte aus. Denn wenn eine Firma ihre Geschäfte über das Internet abwickelt und ein Server dieser Firma ausfällt, kann sie ihre Geschäfte nicht mehr tätigen. Denial-of-Service-Attacken auf Server haben einen Ausfall zur Folge. Es sollte also gewährleistet sein, dass ein Server nicht durch unberechtigte Angriffe ausfallen kann.

- **Authentifizierung**: Diese Anforderung soll sicherstellen, dass beispielsweise ein Benutzer eines Webshops korrekt identifiziert werden kann. Man könnte sich zum Beispiel vorstellen, dass bestimmte Kundengruppen Sonderpreise erhalten, die anderen Kundengruppen nicht zugänglich sein dürfen.

2.2.2 Anforderungen an Sicherheit in Intranets

Werden Inhalte nur innerhalb eines Unternehmens zur Verfügung gestellt, spricht man von einem Intranet. Die Mitarbeiter haben die Möglichkeit, Informationen, die nur für die Mitarbeiter bestimmt sind, über das Intranet abzurufen bzw. bereitzustellen. In einem Intranet-System gelten auch die oben genannten Anforderungen. Zusätzlich gilt folgende Anforderung:

- **Schutz des Netzwerks**: Ein Unternehmen hat die Anforderung, dass unternehmensrelevante Daten das eigene Netz nicht verlassen können und dass schädliche Inhalte aus dem Internet nicht in das eigene Netzwerk gelangen.

Zur Erfüllung der letztgenannten Anforderung werden Firewalls eingesetzt. Dabei handelt es sich um Systeme, die den Datenverkehr zwischen dem internen und dem externen Netzwerk (Intranet und Internet) kontrollieren und unter Umständen unterbinden.

Firewalls sollen verhindern, dass von außerhalb des Firmennetzes unbefugt auf Rechner innerhalb des Intranets zugegriffen werden kann. Sollte es dennoch gelingen, in das Intranet einzudringen, ist gewünscht, diesen Eindringling so schnell wie möglich aufzuspüren, um eventuell Gegenmaßnahmen einleiten zu können.

- **Erkennung von Eindringlingen (Intrusion Detection)**: Die Sicherheitsarchitektur eines Intranets sollte eine Komponente enthalten, die Eindringlinge schnellstmöglichst meldet, so dass Gegenmaßnahmen ergriffen werden können. Ist dies nicht mehr möglich, sollte diese Komponente zumindest die Verfolgung des Eindringlings erleichtern. Dies kann durch Anlegen von Logfiles erfolgen.

Sehr häufig erlangen Fremde Zugriff auf das Intranet durch Einschleusung von so genannten Trojanischen Pferden. Dabei handelt es sich um scheinbar nützliche Programme, die jedoch versteckt eine Hintertür für einen Eindringling offen halten. Es könnten auch durch Fremde gezielt Viren in ein Unternehmensnetz eingespeist werden, um die internen Rechner lahm zu legen. Daher wird noch folgende Anforderung an eine Sicherheitsarchitektur eines Intranets gestellt:

- **Einsatz von Virenscannern**: Auf allen Rechnern im Intranet sollte ein einheitlicher Virenscanner zum Einsatz kommen, so dass es auf einfache Weise möglich ist, aktuelle Virendefinitionsdateien über das eigene Netzwerk zu verteilen. Diese Verteilung sollte möglichst automatisiert ablaufen, so dass die Aktualität der Datei auf den einzelnen Rechnern nicht von der Sorgfalt des jeweiligen Benutzers abhängt. Die Virendefinitionsdatei enthält Informationen über Viren und Trojanische Pferde für den Virenscanner.

Der Einsatz von Virenscannern kann die zwei oben genannten Probleme minimieren, nämlich das Eindringen von Fremden über eine Hintertür innerhalb des Netzwerks und das Stilllegen von Rechnern über Viren.

Um Ausfallzeiten möglichst gering zu halten, bietet es sich an, zusätzlich zu den Backups der Server auch Backups von den Clients im Intranet durchzuführen. So kann im Notfall ein Rechner innerhalb kürzester Zeit wiederhergestellt werden und somit geht wenig produktive Arbeitszeit verloren.

- **Durchführen unternehmensweiter Backups**: Sollte durch ein Sicherheitsloch im System ein Rechner z.B. durch einen Virus unbrauchbar gemacht worden sein, ist es wünschenswert, ein Backup vom Vortag wieder einspielen zu können, um so den Rechner innerhalb kurzer Zeit wieder benutzbar zu machen.

Backupsysteme werden normalerweise unabhängig von Sicherheitssystemen angeboten. Ein Unternehmen, das eine Sicherheitsarchitektur aufbauen will, sollte sich jedoch aus den oben genannten Gründen auch Gedanken über ein durchdachtes Backupsystem machen.

2.3 Geld im Internet

Dieser Abschnitt beschäftigt sich mit Zahlungsmitteln im Internet. Diese können nach den folgenden Varianten unterschieden werden:

- **Kunde – Bank Transaktionen**: Hierbei handelt es sich um das so genannte Homebanking, das Banken ihren Kunden zur Verwaltung ihrer Konten über das Internet oder anderen Medien anbieten.

- **Kunde – Zahlungssystem – Händler Transaktionen**: In diesem Fall werden die Transaktionen von dem zwischengeschalteten Zahlungssystem kontrolliert. Das Zahlungssystem wird normalerweise von Kreditkarteninstituten oder Banken zur Verfügung gestellt.

Zur ersten Variante zählen Homebanking-Anwendungen (Verwaltung von Konten), die im nächsten Abschnitt behandelt werden. Die zweite Variante behandelt elektronisches Geld (z.B. Bezahlen im Internet), welches im übernächsten Abschnitt behandelt wird.

2.3.1 Homebanking

Beim Homebanking handelt es sich um Lösungen, die Banken ihren Kunden anbieten. Diese sollen den Kunden die Verwaltung ihrer Konten über automatisierte Systeme ermöglichen. Heutige Lösungen erlauben das Auslesen der Umsätze, Tätigen von Überweisungen, Anlegen, Ändern und Löschen von Daueraufträgen sowie vereinzelt auch die Verwaltung von Wertpapieren.

Varianten des Homebanking

Da in diesem Bereich sehr viele verschiedene Lösungen unter verschiedenen Namen von den Banken angeboten werden, werden in Anlehnung an [Münc99] zunächst die häufigsten Begriffe unterschieden:

- **Telefonbanking**: Im Fall des Telefonbankings erfolgt der Zugriff auf das Konto über das Telefon. Der Kunde ruft hierbei ein Call-Center der Bank an. In der Regel wird der Kunde über ein einfaches Passwort (meist ein einfacher Begriff) oder über die Eingabe einer PIN authentifiziert. Wenn der Kunde legitimiert wurde, hat er Zugriff auf sein Konto, d.h. er kann zum Beispiel Überweisungen ausführen und seinen Kontostand abfragen. In diesen Call-Centern können Routine-Transaktionen zur Entlastung der Mitarbeiter von Computern entgegengenommen werden.

- **Mobile Banking**: Hierbei handelt es sich um die Verwaltung des Kontos über ein mobiles Endgerät, wie zum Beispiel ein Handy. Die Kommunikation läuft dann über den SMS-Dienst (Short Message Service) oder WAP (Wireless Application Protocol) ab.

- **BTX-/HBCI-Banking**: Bisher wird computergestütztes Homebanking noch hauptsächlich über das alte BTX-System ermöglicht. Dem Kunden wird die Bedienung durch unabhängige Onlinebanking-Programme erleichtert, die die Kommunikation mit dem BTX-System übernehmen. Da die Banken inzwischen jedoch ihre Dienste auch über andere Systeme, wie z.B. das Internet, anbieten möchten, wurde ein neuer Standard entwickelt. Dieser Standard (HBCI – Home Banking Computer Interface, [HBCI00]) soll die Sicherheit im Homebankingbereich gewährleisten. Zur Abgrenzung wird in dieser Arbeit der Begriff BTX-Banking für das alte BTX-System verwendet. Für den neuen Standard HBCI wird im Folgenden der Begriff HBCI-Banking verwendet.

- **Internetbanking**: Wie im vorigen Punkt bereits festgestellt, streben die Banken ein unabhängiges System an, um darüber ihre Dienste anzubieten. Die meisten Banken sind schon vor der Etablierung des HBCI-Standards dazu übergegangen, die vom BTX-System her bekannten Leistungen auch im Internet anzubieten. Dazu wurden eigene Programme entwickelt, wie zum Beispiel Java-Applets. Das für das BTX-System eingeführte PIN/TAN-Verfahren (s.u.) ist auch hier noch häufig anzutreffen.

Wie in der folgenden Abbildung dargestellt, lassen sich die Homebanking-Anwendungen in computergestütztes Homebanking und telefongestütztes Homebanking einteilen.

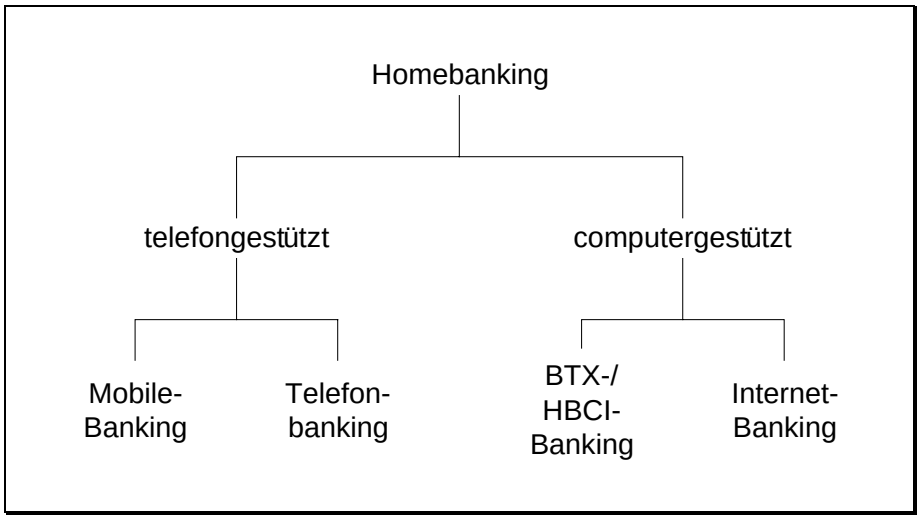


Abbildung 2.1: Einteilung der Homebanking-Anwendungen

Zugriffsschutzvarianten im Homebanking

In diesem Abschnitt wird zunächst kurz auf die verschiedenen Varianten des Zugriffsschutzes im Homebanking eingegangen, um anschließend die Anforderungen in diesem Zusammenhang aufstellen zu können.

Im Bereich des Telefonbanking hat der Kunde meistens nach Angabe eines einzelnen Passwortes Zugriff auf alle Leistungen, die sein Konto betreffen. Sollte dieses Passwort in falsche Hände geraten, kann der Schaden immens sein. Es obliegt also dem Kunden, das Passwort entsprechend sicher zu wählen und dafür zu sorgen, dass es nicht ausspioniert werden kann.

Es stellt sich auch die Frage, ob es dem Kunden ermöglicht werden darf, ein eigenes Passwort zu wählen. Denn in diesem Fall werden häufig einfach zu erratende Passwörter, wie zum Beispiel Namen von Personen, Städten oder Ländern gewählt. So sollte er zum Beispiel nicht in Telefonzellen Telefonbanking durchführen.

Ein weiteres Problem in diesem Zusammenhang stellen ältere Mobiltelefone dar, die ohne großen Aufwand abhörbar sind. Neuere Modelle basieren auf dem DECT-Standard (Digital Enhanced Cordless Telecommunications), der durch die digitale Übertragung einen wesentlich höheren Aufwand zum Abhören erfordert.

Das für das BTX-Banking eingeführte PIN/TAN-Verfahren gilt als relativ sicher. Dabei erhält der Kunde eine PIN, mit der er Zugang zu seinem Konto erhält. Mit diesem Zugang sind zunächst nur Informationen abrufbar, wie zum Beispiel die letzten Umsätze oder der Kontostand. Zusätzlich erhält der Kunde eine Liste mit mehreren TAN (TAN – Transaktionsnummer), die für Aufträge (z.B. Überweisungen, Wertpapierorder, Ändern, Anlegen oder Löschen von Daueraufträgen) verwendet werden. Dabei ist jede TAN nur für eine Transaktion gültig. Sollte sich also jemand durch Abhören der Leitung eine TAN beschafft haben, ist sie in der Regel bereits verbraucht und somit für den Betrüger wertlos.

Um dem Kunden eine einfache Bedienung zu bieten, werden von manchen Banken Onlinebanking-Programme angeboten, die entweder über das alte BTX-System oder über das Internet mit Hilfe des HBCI-Protokolls Kontakt zum Bankrechner aufnehmen. In diesen Programmen kann eine Speicherung der PIN und TAN-Nummern möglich sein. Da in der Regel im privaten Bereich keine sehr sicheren Betriebssysteme (z.B. Microsoft Windows 95, 98 oder ME) eingesetzt werden, könnte jemand durch den Zugriff auf eine bestimmte Datei des Onlinebanking-Programms die Nummern ausspionieren.

Die meisten Banken ermöglichen ihren Kunden den Zugang zum Konto mittels PIN/TAN-Verfahren über das Internet. Im Gegensatz zum BTX- oder HBCI-Banking unterstützen aufgrund der proprietären Benutzeroberflächen Onlinebanking-Programme diesen Zugang zum Konto nicht. Verwendet der Kunde nur Internetbanking, so besteht normalerweise nicht die Gefahr, dass er die PIN und TANs in einer Software abspeichern kann.

Es lassen sich also folgende Anforderungen den Zugriffsschutz im Homebanking betreffend aufstellen:

- **Passwort-Policy**: Es muss eine sinnvolle Policy erstellt werden, nach der Passwörter bzw. PINs erstellt werden.
    - Werden für das Telefonbanking Passwörter verwendet, ist es sinnvoll, dem Kunden ein Passwort vorzugeben, das hinreichend sicher ist. Es sollte aber dennoch so einfach zu merken sein, dass der Kunde es nicht notieren muss (zum Beispiel eine Zusammensetzung aus zwei deutschen Begriffen und einer Zahl, wie haus637nudel).
    - Beim PIN/TAN-Verfahren sollte es dem Kunden ermöglicht werden, die Zahlenkombination ändern zu können. Die Änderung sollte mit einer TAN bestätigt werden müssen.

- **Onlinebanking-Programme**: An diese Programme werden folgende sicherheitsrelevante Anforderungen gestellt:

  - Es darf dem Benutzer nicht ermöglicht werden, PINs oder TANs im Programm abzuspeichern. Sollte der Anbieter der Software aufgrund der Benutzerfreundlichkeit nicht darauf verzichten wollen, diese Funktion anzubieten, sollte zumindest eine eindringliche Warnung erscheinen, die den Benutzer auf die möglichen Gefahren hinweist.

  - Der Zugriff auf das Programm sollte durch ein Passwort geschützt werden, das der Benutzer selbst wählen kann.

  - Alle Dateien, die Daten des Benutzers enthalten, sollten verschlüsselt abgespeichert werden.

2.3.2 Elektronisches Geld

In diesem Bereich werden zurzeit verschiedene Verfahren angeboten, die es ermöglichen, elektronisches Geld über das Internet zu versenden. Die Verfahren können durch folgende Merkmale unterschieden werden:

Zeitpunkt, wann das Geld den Kunden verlässt	Es werden drei Arten unterschieden: pre-paid (dabei muss der Kunde zunächst ein Guthaben beim Betreiber anlegen), pay-now (es wird zeitnah abgerechnet) und post-paid (vergleichbar mit Schecks oder Kreditkarten).
Teilbarkeit der Beträge	Werden in dem angebotenen Verfahren elektronische Münzen verwendet, können diese meistens nicht geteilt werden. Daher erhält der Kunde bei einer Bezahlung den Restbetrag in neuen Münzen zurück.
Anonymität	Es gibt Verfahren mit kompletter Anonymität, teilweiser Anonymität und keiner Anonymität. Bei den Verfahren mit teilweiser Anonymität werden meistens mehrere Parteien oder Transaktionen benötigt, um die Identität eines Kunden herauszufinden.
Mobilität	Ist eine Bezahlung von mobilen Endgeräten möglich?
Online oder Offline	Bei Offline-Zahlungen ist kein Kontakt zu einem weiteren Server, wie zum Beispiel einem Authorisierungsserver, nötig. Bei Online-Zahlungen wird bei einem weiteren Server (z.B. im Falle von elektronischen Münzen, die ausgebende Bank) die Gültigkeit der Transaktion abgefragt.

Übertragbarkeit	Beschreibt die Eigenschaft, das Geld auch an andere Kunden direkt zu übertragen (wie es beim Bargeld auch möglich ist, z.B. einem Freund Geld zu geben) und nicht nur zwischen Händler und Kunde bzw. Kunde und Bank.
Geografische Nutzungsmöglichkeit	Online-Geschäfte können lokal, national und international getätigt werden. Ein System muss entsprechende geografische Nutzbarkeit unterstützen.
Eignung für kleine oder große Beträge	Manche Verfahren sind speziell für sehr kleine Beträge entwickelt worden. Andere Verfahren verursachen pro Transaktion Fixkosten, die kleine Beträge nicht rechtfertigen würden, bieten jedoch höhere Sicherheit, die bei kleinen Beträgen nicht nötig wäre.

Tabelle 2.1: Unterscheidungsmerkmale von elektronischen Zahlungsmitteln

Aufgrund der in der Tabelle genannten Kriterien kann ein Anwender selbst die für sich wichtigen Anforderungen aufstellen und anschließend die passende Lösung auswählen.

Ein wesentlicher Aspekt des elektronischen Geldes ist die Speicherung der Information darüber, wie hoch das Guthaben eines Kunden ist. Basiert das Verfahren beispielsweise auf elektronischen Münzen, könnten diese in Dateien auf dem Rechner des Kunden gespeichert sein. Auch hier sind, wie bereits beim PIN/TAN-Verfahren genannt, entsprechende Maßnahmen gegen den Diebstahl dieser Dateien zu treffen. Es wäre auch denkbar, die elektronischen Münzen auf einer Chipkarte zu speichern.

2.4 E-Commerce

In diesem Abschnitt werden die Anforderungen im E-Commerce ermittelt. Dazu werden zunächst die Rollen bestimmt, die in E-Commerce-Szenarien vorkommen können. Dann werden die möglichen Geschäftsbeziehungen der einzelnen Geschäftspartner vorgestellt und anschließend mögliche Aktionen aufgezeigt. Dabei handelt es sich um leicht abgewandelte Informationen aus [Gehm99].

Mit diesen Daten werden schließlich Anforderungen ermittelt, die in den folgenden vier Abschnitten vorgestellt werden. Es erfolgt dabei eine Einteilung in Anforderungen an die Kommunikation zwischen den Geschäftspartnern, Feststellen und Sicherstellen der Identität des jeweiligen Geschäftspartners, Anforderungen an die Sicherung der Komponenten und abschließend Anforderungen zum Schutz des Endbenutzers.

2.4.1 Rollen im E-Commerce

Im Bereich des E-Commerce schließen zwei Geschäftspartner, wie auch beim konventionellen Handel, einen Vertrag ab. Dabei wird in dieser Arbeit der Geschäftspartner, der die Leistung erbringt, als Händler bezeichnet. Der Leistungsempfänger wird als Kunde bezeichnet. Im Gegensatz zum konventionellen Handel müssen die Geschäftspartner zum Abschluss des

Vertrags nicht in einem physischen Kontakt miteinander stehen. Der Kauf bzw. Verkauf von Waren und Dienstleistungen erfolgt im E-Commerce auf elektronischem Wege, also über Computer oder andere Telekommunikationseinrichtungen (z.B. Telefon, Fax).

Durch die elektronische Integration werden Medienbrüche zwischen unternehmensübergreifenden Transaktionen vermieden. So kann es z.B. sein, dass ein Unternehmen Rechnungen und Lieferscheine, die intern noch in elektronischer Form verarbeitet werden, nach außen in Papierform weitergeben muss. Unter elektronischer Integration versteht man die Verwendung von vernetzten Computern und Telekommunikationseinrichtungen zur Vermeidung von Medienbrüchen.

2.4.2 Geschäftsbeziehungen

Kunden und Händler können verschiedenen Gruppen angehören. Diese sind Endverbraucher und Unternehmen. Dies soll das folgende Bild veranschaulichen.

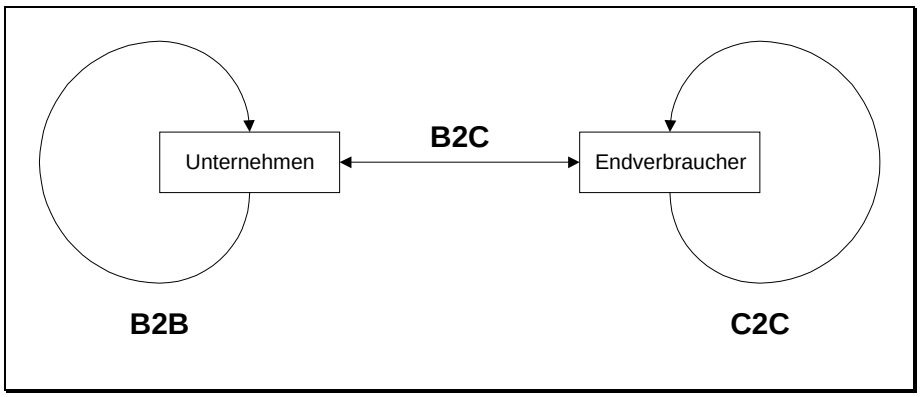


Abbildung 2.2: Geschäftsbeziehungen im E-Commerce

Handelt es sich beim E-Commerce um Geschäftsbeziehungen der Unternehmen untereinander, spricht man vom Business-to-Business Bereich (B2B). Ein Hersteller steht hierbei in Verbindung mit seinen direkten Zulieferern und Abnehmern. Dieser Bereich des E-Commerce macht den größten Anteil am Gesamt-E-Commerce aus.

Geschäftsbeziehungen zwischen Unternehmen und Endverbraucher tragen die Bezeichnung Business-to-Consumer (B2C) und gewinnen mehr und mehr an Bedeutung. Ein populäres Beispiel ist der Online-Bücherhändler Amazon.com.

Wenn Endverbraucher untereinander Geschäftsbeziehungen eingehen, spricht man von Consumer-to-Consumer (C2C). Dies ist bei Online-Auktionshäusern der Fall, wie zum Beispiel Ebay.com, in denen Endverbraucher selbst zu Gelegenheitshändlern werden. Sie nutzen dabei allerdings die Infrastruktur des Online-Auktionshauses, für die meistens bezahlt werden muss. Im Gegensatz dazu betreiben im B2C-Bereich die Händler einen eigenen Web-Shop.

In einem Web-Shop, das den virtuellen Laden des Händlers darstellt, lassen sich alle Waren vertreiben, die auch im konventionellen Handel verkauft werden. Dabei wird zwischen physi-

schen und digitalen Gütern unterschieden. Physische Güter sind Produkte (z.B. Bücher, CDs) oder Dienstleistungen (z.B. Malerarbeiten), die über einen Paketdienst oder auf andere geeignete Weise dem Empfänger zugestellt werden müssen. Dagegen lassen sich digitale Güter über das bestehende Netzwerk vertreiben. Zu den digitalen Gütern gehören z.B. Software, Bücher in digitaler Form, Statistiken und Nachrichten. Digitale Güter haben gegenüber den physischen den Vorteil, dass keinerlei Medienbruch mehr vorhanden ist.

Im E-Commerce werden die folgenden Aktionen in elektronischer Form durchgeführt:

- **Produktpräsentation**: Produktkataloge, Faltblätter und Prospekte können in elektronischer Form im Internet abgelegt werden. Vorteilhaft ist dabei, dass ein Kunde zum Beispiel nach bestimmten Artikeln im Produktkatalog eines Händlers nach Stichworten suchen kann.

- **Auswahl**: Der Kunde wählt die Artikel direkt am Computer im Web-Shop des Händlers aus.

- **Bestellung**: Der Kunde gibt seine Bestellung in elektronischer Form direkt im Web-Shop auf.

- **Bezahlung**: Die Bezahlung kann in elektronischer Form erfolgen. Die einfachste Möglichkeit besteht in der Angabe der Kreditkartennummer oder der Bankverbindung (für das Lastschriftverfahren, das allerdings national begrenzt ist), so dass der Händler den fälligen Betrag einziehen kann.

- **Lieferung**: Digitale Güter können anschließend über das Netzwerk in elektronischer Form geliefert werden.

- **Benutzung der Artikel**: Handelt es sich um digitale Güter, kann der Kunde die Artikel in elektronischer Form benutzen (z.B. Anzeigen eines Buches in digitaler Form auf dem Bildschirm).

- **Reklamationen/Support**: Sollten Probleme mit den gekauften Artikeln auftreten, hat der Kunde meist die Möglichkeit, seine Beschwerden direkt im Web-Shop zu formulieren. Sind sich beide Geschäftspartner über die Reklamation einig, wäre bei digitalen Gütern ein sofortiger Umtausch möglich.

In den folgenden Abschnitten werden nun die Anforderungen an E-Commerce-Lösungen ermittelt. Naheliegend sind zunächst die Anforderungen, die die Kommunikation betreffen.

2.4.3 Anforderungen an eine gesicherte Kommunikation

Um die Kommunikation zwischen den Geschäftspartnern abzusichern, werden folgende Anforderungen an die Kommunikationskomponenten einer E-Commerce-Lösung gestellt:

- **Aufdeckung von Manipulationen**: Beim Transfer von Daten über das Netzwerk, speziell bei der Bestellung, Bezahlung und der Lieferung, muss eine Manipulation verhindert werden. Sollte doch eine Manipulation vorgenommen worden sein, so muss diese vom Empfänger aufgedeckt werden können und die entsprechende Transaktion abgelehnt werden.

- **Geheimhaltung**: Daten, die über das Netzwerk versendet werden, müssen geheim gehalten werden. Dies ist besonders wichtig bei personenbezogenen Daten und Daten über die Bankverbindung bzw. Kreditkarteninformationen.

- **Verhindern von Duplikaten**: Transaktionen, die einmal durch das Netzwerk transferiert wurden, könnten nach einer unbefugten Aufzeichnung wieder verwendet werden. Es sollte daher verhindert werden, dass eine Transaktion doppelt ausgeführt werden kann.

- **Unleugbarkeit**: Erledigte Transaktionen, wie z.B. eine Bestellung, Bezahlung oder Lieferung, sollten nicht nachträglich abgelehnt werden können.

Im folgenden Abschnitt wird auf die Anforderungen im Zusammenhang mit der Authentifizierung der beteiligten Parteien eingegangen.

2.4.4 Überprüfung von Identitäten

Ein weiterer sehr wichtiger Punkt ist die Überprüfung der Identität der Kommunikationspartner. Gerade in unsicheren Netzwerken wie dem Internet kann man auf angegebene Namen nicht vertrauen.

Zum einen möchte der Kunde darauf vertrauen können, dass es sich beim im Internet ausgewählten Händler tatsächlich um den Händler handelt, bei dem er einkaufen möchte. So kann der Kunde z.B. nicht darauf vertrauen, dass die Firma XYZ AG der Firma unter der Internet-Adresse www.xyz.de entspricht.

Zum anderen möchte der Händler sicher sein, dass die Angaben eines Kunden korrekt sind. Verlässt sich beispielsweise ein Händler auf die Eingaben seiner Kunden und bietet als Zahlungsweise Bankeinzug an, könnte ein Kunde eine andere Bankverbindung angeben und sich somit die Leistungen des Händlers erschleichen.

Die Anforderung lautet wie folgt:

- **Sicherstellen der Identität**: Die Identität aller Beteiligten muss für alle Beteiligten überprüfbar sein.

Weitere Anforderungen können an die Komponenten der E-Commerce-Lösung gestellt werden. Diese werden im folgenden Abschnitt erläutert.

2.4.5 Anforderungen an die Sicherheit der Komponenten

Händler, die Produkte mittels E-Commerce anbieten, müssen sich der Risiken bewusst sein, denen die Komponenten der E-Commerce-Lösung ausgesetzt sind. Der Web-Server beispielsweise ist allgemein bekannt und für die Öffentlichkeit jederzeit verfügbar. Er stellt daher ein potentielles Angriffsziel für Hacker dar. Händler sollten daher eine E-Commerce-Lösung bevorzugen, die den folgenden Anforderungen genügt:

- **Verfügbarkeit**: Der Service und der Server, der den Service ermöglicht, sollten eine hohe Verfügbarkeit aufweisen. Ausfallzeiten sollten so kurz wie möglich sein.
- **Anlegen von Logfiles**: Alle Aktivitäten einer Komponente sollten in einem Logfile festgehalten werden, durch das später Transaktionen nachvollzogen werden können.
- **Kontrolle der Logfiles**: Die angelegten Logfiles sollten durch automatisierte Skripte regelmäßig auf verdächtige Aktionen überprüft werden und entsprechende Berichte generiert werden.
- **Schutz vor unberechtigter Benutzung**: Eine unberechtigte Benutzung einer Komponente, sei es durch externe oder interne Zugriffe, sollte ausgeschlossen werden.
- **Korrekte und sichere Datenverarbeitung**: Die Integrität und Geheimhaltung der zu verarbeitenden Daten muss gewährleistet werden.

2.4.6 Anforderungen zum Schutz des Endbenutzers

Man kann von den Benutzern (Kunden) von E-Commerce-Lösungen nicht erwarten, dass ihnen beim Einkaufen im Internet die Sicherheitsrisiken bekannt sind. Ein Benutzer möchte ohne Einschränkungen im Internet surfen können. Dabei wird er sich in der Regel wenig Gedanken über die Sicherheit machen.

Leider haben die Händler, die Web-Shops im Internet betreiben, sowie die Anbieter der E-Commerce-Lösungen nur einen sehr bedingten Einfluss auf die Systeme, die der Endverbraucher verwendet.

Wünschenswert ist die Erfüllung der folgenden Anforderungen:

- **Einfache Bedienung**: Das System sollte einfach zu bedienen sein, so dass Anrufe bei einer Hotline wegen Routineaufgaben nicht erforderlich sind.
- **Unleugbarkeit**: Alle Transaktionen (Bestellung, Bezahlung, Lieferung) sollten im nachhinein nachweisbar sein.
- **Unfälschbarkeit**: Transaktionen müssen so konzipiert sein, dass eine Fälschung nicht möglich ist oder zumindest erkannt und anschließend abgelehnt wird.

- **Fehlertoleranz**: Das System sollte dem Endbenutzer auch bei Systemausfällen keine Vermögensschäden verursachen.

- **Anonymität**: Die Daten des Benutzers sollten vom System geschützt werden. Transaktionen sollten größtenteils anonym möglich sein und nur die nötigste Information über den Benutzer beinhalten.

Außerdem lassen sich noch folgende Anforderungen an die Soft- und Hardware aufstellen, die beim Benutzer zum Einsatz kommen:

- **Verhindern ungewollter Transaktionen**: Es dürfen vom System keine Transaktionen durchgeführt werden, von denen der Benutzer nichts weiß. Dies kann z.B. durch Eingabe einer Passphrase oder Einstecken einer SmartCard bei Durchführung einer Transaktion geschehen.

- **Integrität der Transaktionen**: Das System muss so abgeschottet sein, dass es für Viren und Trojanische Pferde nicht möglich ist, Transaktionen vor dem Absenden zu ändern.

- **Verhindern irreführender Meldungen**: Das System sollte anstehende Transaktionen in verständlicher Weise anzeigen, so dass kein Zweifel darüber aufkommen kann, welche Folgen diese Transaktion für den Endbenutzer haben wird (z.B. Überweisung eines höheren Betrages).

2.5 Anforderungen an Sicherheitsarchitekturen

Abschließend seien noch drei Anforderungen genannt, die an eine Infrastruktur gestellt werden sollten:

- **Skalierbarkeit**: Wenn ein Web-Shop erfolgreich ist und die Zugriffszahlen steigen, wird immer wichtiger, dass die Zugriffszeiten gering bleiben und eine gute Performance gewährleistet bleibt. Daher müssen spätere Erweiterungen der Infrastruktur ermöglicht werden.

- **Verfügbarkeit**: Die Verfügbarkeit der einzelnen Komponenten der Infrastruktur sollte hoch sein, um lange Ausfallzeiten zu verhindern.

- **Offene Architektur**: Spätere Änderungen an der Infrastruktur oder das Wechseln des Produkts setzen eine offene Architektur voraus. Nur wenn alle Komponenten anerkannte Standards verwenden, können die bestehenden Daten wieder verwendet werden.

Eine weitere wichtige Anforderung an eine Infrastruktur ist Interoperabilität, auf die im nächsten Abschnitt eingegangen wird.

2.6 Interoperabilität von Sicherheitsarchitekturen

Zusätzlich zu den im vorigen Kapitel angegebenen Anforderungen an Sicherheitsarchitekturen können weitere Anforderungen an die Interoperabilität gestellt werden.

- **Migration**: Unter Migration versteht man die Weiterverwendung bisheriger Daten beim Wechsel von einem Produkt zu einem anderen oder einer neueren Version. Die einzelnen Komponenten einer Sicherheitsarchitektur sollten für eine spätere Migration sämtliche Daten in einem dafür geeigneten Format speichern können. Dadurch werden Mehrkosten bei einem Wechsel des Produkts oder der Version vermieden (z.B. für die Neueingabe der Daten oder das Neuausstellen aller bisher ausgestellten Zertifikate).

- **Daten-Export**: Jede eingesetzte Komponente der Sicherheitsarchitektur sollte eine Möglichkeit bieten, gespeicherte Daten und Einstellungen in einem bestimmten Format abzuspeichern. Als Formate sollten möglichst Standardformate verwendet werden. In einzelnen Fällen (wenn bereits bekannt ist, welches Zielsystem eingesetzt wird) könnte die Speicherung direkt in dem Format erfolgen, das das Zielsystem unterstützt.

- **Daten-Import**: Der Import von Daten sollte von den Komponenten der Sicherheitsarchitektur unterstützt werden. Dies ermöglicht dem Anwender die Übernahme bereits vorhandener Daten. Dabei sollte die Importfunktion unterscheiden können, ob die zu importierenden Daten dem bisherigen Datenstamm hinzugefügt werden sollen, oder ob die bisherigen Daten durch die neuen ersetzt werden sollen.

- **Unterstützung für heterogene Architekturen**: Bei umfangreicheren E-Commerce-Lösungen sind die Schnittstellen zu anderen Systemen wichtig. Zum Beispiel für den Import von Produktdaten oder die automatische Verarbeitung eingehender Bestellungen. Eine E-Commerce-Lösung sollte universelle Schnittstellen zur Anbindung an bestehende Systeme (z.B. Warenwirtschaft) besitzen.

- **Verbindung zwischen verschiedenen Architekturen**: Wenn Anwender zweier verschiedener Architekturen auf einem sicheren Weg kommunizieren möchten, können sie Zertifikate verwenden. Sicherheitsarchitekturen sollten daher Zertifikate erstellen, die von anderen Architekturen verarbeitet werden können. So sollte es z.B. möglich sein, das das Zertifikat eines Mitarbeiters einer Firma im Web-Shop einer anderen Firma akzeptiert werden kann.

Zusätzlich zu diesen Anforderungen muss untersucht werden, ob es möglich ist, Zertifikate über Sicherheitsmodelle hinaus verwenden zu können. Ist zum Beispiel ein Zertifikat, das im Format eines Sicherheitsmodells A vorliegt in einem Sicherheitsmodell B verwendbar?

Kapitel 3 Sicherheitsarchitekturen

In diesem Kapitel werden die Sicherheitsarchitekturen vorgestellt, die in dieser Arbeit untersucht werden. Ausgewählt wurden Pretty Good Privacy von Network Associates, exemplarisch die Public-Key-Infrastructure Lösung der Firma Baltimore Technologies und das noch in der theoretischen Ausarbeitung befindliche Simple-PKI, das von der gleichnamigen Arbeitsgruppe der IETF (Internet Engineering Task Force) erarbeitet wird.

Es wird eine Einführung zu jedem dieser Produkte gegeben, die verwendeten Kryptoalgorithmen erläutert und der Lieferumfang der jeweils getesteten Version vorgestellt.

3.1 Pretty Good Privacy

Pretty Good Privacy (PGP, übersetzt etwa "relativ gute Privatsphäre") wurde 1991 von Philip Zimmermann in den USA herausgegeben. PGP wurde für eine Vielzahl unterschiedlicher Betriebssysteme entwickelt (z.B. Unix, Windows-Systeme und Macintosh) und liegt der Öffentlichkeit als Quelltext vor. Dadurch ist es möglich, dass jeder selbst kontrollieren kann, ob das Programm seinen Anforderungen entspricht.

Inzwischen sind einige PGP-Versionen verfügbar, die von unterschiedlichen Entwicklern herausgegeben wurden. Zu den bekanntesten Versionen dürften die internationale Freeware-Version von PGP, der GNU Privacy Guard (GnuPG) sowie die für kommerziellen Einsatz gedachte PGP-Version der Network Associates, Inc. gehören. Diese drei genannten Versionen werden kurz im folgenden Abschnitt beschrieben

PGP wird – wie der Name schon sagt – zur Wahrung der Privatsphäre eingesetzt. Dazu werden E-Mails oder Dateien (um sie dann z.B. auf Diskette dem Empfänger zu geben) so verschlüsselt, dass nur der Empfänger sie wieder entschlüsseln kann – selbst der Absender hat nach dem Verschlüsseln keine Möglichkeit mehr, diese Nachricht zu entschlüsseln (ausgenommen sie wurde für ihn ebenso verschlüsselt). Außerdem bietet PGP die Möglichkeit, E-Mails zu unterschreiben, so dass der Empfänger sich auf die Absenderangabe verlassen kann. PGP verwendet eine Kombination mehrerer kryptografischer Verfahren, die in Abschnitt 3.1.2 erläutert werden.

In dieser Arbeit werden die Tests für die o.g. kommerzielle Lösung durchgeführt. Network Associates bietet dem Kunden verschiedene Pakete an, die für den Aufbau einer Sicherheitsinfrastruktur nötig sind. Wie die Pakete heißen und welche Komponenten sie enthalten, wird in Abschnitt 3.1.3 vorgestellt.

Wie eine Sicherheitsinfrastruktur mit Hilfe der Produkte von Network Associates aussehen kann und wie Zertifikate unter PGP aussehen und verwendet werden, wird im Abschnitt 3.1.4 gezeigt.

3.1.1 Erhältliche Versionen

1991 wurde in den USA ein Gesetz gegen die wachsende Kriminalität vorgeschlagen, das u.a. allen Herstellern von sicheren Kommunikationseinrichtungen vorschrieb, eine Hintertür in ihre Produkte einzubauen. Es sollte damit sichergestellt werden, dass die Regierung mit einer richterlichen Befugnis verschlüsselte Nachrichten oder Telefonate entschlüsseln kann. Obwohl diese Gesetzesvorlage nicht angenommen wurde, entschied sich Philip Zimmermann, ein Programm zu schreiben, mit dem eine starke Verschlüsselung möglich ist. Dies war die erste Version von PGP (PGP 1.0). Nähere Informationen zur Geschichte von PGP sind in [Garf94] und aktuellere Informationen in [Back99] zu finden.

PGP 1

Die erste Version von PGP verwendete u.a. das von Zimmermann selbst entwickelte Bass-O-Matic als symmetrische Verschlüsselung. Es stellte sich jedoch bald heraus, dass dieses verwendete Verschlüsselungsverfahren nicht sicher genug war. Daraufhin programmierte Philip Zimmermann eine neue Version, die auf dem IDEA-Algorithmus basierte. Dieser Algorithmus war von der Firma Ascom aus der Schweiz patentiert worden, die lediglich eine unkommerzielle Nutzung erlaubte. Dadurch mussten Firmen, die PGP kommerziell einsetzen wollten, eine Lizenz von Ascom einholen.

PGP 2

Das zum Einsatz kommende asymmetrische Verschlüsselungsverfahren basiert auf dem RSA-Algorithmus. Dieser wurde 1983 vom MIT (Massachusetts Institute of Technology) für die USA patentiert. Die von den RSA-Erfindern gegründete Firma RSA Data Security Inc. erhielt eine Exklusivlizenz vom MIT. Das Patent und somit die Lizenz liefen im Jahr 2000 aus [RSAP00].

In den USA stellte PGP eine Patentverletzung dar. Daher wurde mit der Version 2.5 zwischen Zimmermann und dem MIT in Zusammenarbeit eine freie Version von PGP entwickelt, die keine Patentrechte verletzen sollte. Jedoch sind diese 'MIT-Versionen' nicht kompatibel mit vorhergehenden Versionen (d.h. Schlüssel und Signaturen der MIT-Version sind mit alten Versionen nicht entschlüsselbar). Benutzer sollten dazu gebracht werden, zu der patentrechtlich ordnungsgemäßen MIT-Version zu wechseln. Sie benutzen statt der RSA-Implementierung von Zimmermann ein lizenziertes Softwarepaket namens RSAREF. Nach der dazugehörigen Lizenz ist die Verwendung für nichtkommerzielle Zwecke kostenfrei.

Die internationalen Versionen (die nicht dem RSA-Patent in den USA unterliegen) benutzen dagegen noch die alte RSA-Implementierung von Zimmermann. Darüber hinaus kann sie derart konfiguriert werden, dass sie Schlüssel und Signaturen aller Versionen lesen kann, d.h. sowohl von alten als auch von MIT-Versionen.

Daher gab es also ab der Version 2.5 zwei verschiedene, aber vollständig interoperable Versionen von PGP: eine US-Version, die lizenzgebundene Software verwendet und nicht rückwärtskompatibel ist, sowie eine internationale Version, die insbesondere die Kompatibilität zu allen Versionen von PGP aufweist.

Aktuelle PGP Versionen

Diese Trennung wurde bis zur Version 6.0 beibehalten, wobei die internationalen Versionen jeweils ein „i“ in der Versionsnummer trugen. Die USA-Versionen wurden zunächst von der Firma ViaCrypt vertrieben. Später wurde der Vertrieb von der Firma PGP Inc. übernommen, die Philip Zimmermann 1997 gründete. Nur kurze Zeit später wurde PGP Inc. von Network Associates aufgekauft. Dort arbeitete Zimmermann bis Anfang 2001.

Inzwischen wird lediglich zwischen einer kommerziellen und einer nicht kommerziellen Version von PGP unterschieden, die die Versionsnummer 7.0 erreicht haben. Diese haben einige Erweiterungen erhalten. Dazu gehören neben der von Anfang an gebotenen Verschlüsselungsfunktion für E-Mails und Dateien jetzt auch die Verschlüsselung ganzer Festplatten und die Verschlüsselung von Nachrichten über Instant Messaging Programme.

Außerdem bietet PGP seit der Version 6.5 die Funktion PGPnet, die die gesamte TCP/IP-Kommunikation zwischen PGPnet und sämtlichen anderen Rechnern, auf denen PGPnet ausgeführt wird, sichert. Dadurch wird es möglich, sichere entfernte Zugriffe auf einen Rechner über ein unsicheres Netzwerk zu leiten (Virtual Private Network – VPN).

GnuPG

Seit den Versionen 5.5/6.0 wird parallel zu PGP, das in der freien Version nicht den vollen Leistungsumfang aufwies, der GNU Privacy Guard (GnuPG) entwickelt. Dieser steht unter der so genannten GNU General Public License (GPL) der Free Software Foundation. Somit ist der Quelltext des Programms der Öffentlichkeit zugänglich und es ist jedem möglich, daran weiterzuentwickeln.

GnuPG besteht aus einem Kommandozeilenprogramm und einer grafischen Benutzeroberfläche. Dadurch wird die Bedienung wesentlich vereinfacht. Da GnuPG als Quelltext vorliegt, kann es auf jedem Betriebssystem zum Laufen gebracht werden. Für Windows ist ferner eine kompilierte Version erhältlich. Um die Interoperabilität zu PGP zu gewährleisten, können Schlüssel problemlos zwischen GnuPG und PGP ab Version 5 ausgetauscht werden.

Da GnuPG noch relativ neu ist, ist die Bedienung trotz grafischer Benutzeroberfläche bisher nur fortgeschrittenen Anwendern vorbehalten. Im Gegensatz zu PGP gliedert sich GnuPG nicht in Mail-Clients ein, sondern erfordert die Ver- und Entschlüsselung in Windows über die Zwischenablage bzw. in Unix-Systemen über Kommandozeilenparameter.

3.1.2 Verwendete Kryptoverfahren

In PGP kommen drei Klassen von Kryptoverfahren zum Einsatz: Zum einen sind das Verschlüsselungsverfahren, die auf symmetrischen Schlüsseln basieren, zum anderen werden

asymmetrische Verschlüsselungsverfahren verwendet, die einen sicheren Austausch des per Zufallsfunktion ermittelten symmetrischen Schlüssels vereinfachen. Ferner werden zur Signierung von Dateien oder E-Mails Hash-Algorithmen in Kombination mit den asymmetrischen Verschlüsselungsverfahren eingesetzt. Dadurch muss nicht die gesamte Nachricht mit dem geheimen Schlüssel verschlüsselt werden, sondern lediglich der Hash-Wert der Nachricht.

In den verschiedenen Versionen von PGP kommen als asymmetrische Verfahren RSA und ElGamal, als symmetrische Verfahren IDEA und 3DES zum Einsatz. Wie bereits erwähnt, wird vor dem Signieren ein Hash-Wert gebildet. Dazu wird das MD5- und das SHA1-Verfahren verwendet. In den folgenden Abschnitten werden die Verfahren kurz zusammengefasst. Eine ausführliche Beschreibung ist z.B. in [Schn96] enthalten.

RSA-Verfahren

Die Buchstaben RSA wurden nach ihren Entwicklern Rivest, Shamir und Adleman gewählt. RSA ist ein asymmetrisches Verschlüsselungsverfahren, das eine variable Schlüssellänge bietet. So kann gewählt werden, ob man einen langen Schlüssel für eine hohe Sicherheit verwendet oder einen kürzeren Schlüssel für eine höhere Effizienz.

Bei RSA werden die Nachrichten in einzelne zu verschlüsselnde Blöcke geteilt. Die Blockgröße der zu verschlüsselnden Nachricht ist dabei ebenso variabel, sie muss jedoch kleiner sein als die gewählte Schlüssellänge. Wurden diese Blöcke verschlüsselt, haben sie die selbe Länge wie der Schlüssel.

RSA ist wesentlich langsamer als symmetrische Verschlüsselungsverfahren, daher werden meist nicht ganze Nachrichten mit RSA verschlüsselt, sondern ein gemeinsamer Schlüssel für eine symmetrische Verschlüsselung generiert und dieser dann mit RSA verschlüsselt.

Die Schlüsselgenerierung basiert auf zwei sehr großen Primzahlen, die miteinander multipliziert werden. Aus diesem Multiplikator ist es mit heutigen Mitteln nicht möglich, die zwei Primzahlen in akzeptabler Zeit zu faktorisieren.

Der RSA-Algorithmus ist öffentlich zugänglich und daher eines der am besten untersuchten asymmetrischen Verfahren überhaupt. Probleme bereitete PGP allerdings die Tatsache, dass RSA in den USA patentiert wurde. Dadurch war es nicht möglich, RSA in einer für den kommerziellen Einsatz gedachten PGP-Version zu vertreiben. Inzwischen wird in PGP das neuere ElGamal-Verfahren verwendet, das frei verfügbar ist. Aus Kompatibilitätsgründen wird RSA auch in neueren Versionen wieder verwendet, seit das Patent im Jahr 2000 ausgelaufen ist [RSAP00].

DH / ElGamal / DSA / DSS

Das erste asymmetrische Verfahren wurde 1976 von W. Diffie und M. E. Hellman vorgestellt. Es stellt im strengen Sinn eigentlich kein Verschlüsselungsverfahren dar, sondern bietet die Möglichkeit, Schlüssel für symmetrische Verfahren zwischen zwei Kommunikationspartnern auszutauschen. Seine Sicherheit beruht auf der Schwierigkeit der Bestimmung diskreter Logarithmen.

Eine Variante des Diffie-Hellman-Verfahrens ist das ElGamal-Verfahren, das von Taher ElGamal 1985 entwickelt wurde. Im Gegensatz zu Diffie-Hellman kann ElGamal direkt für Verschlüsselung und für digitale Signaturen eingesetzt werden. Der Vorteil gegenüber RSA ist, dass ElGamal nicht patentiert ist. Zwar ist das Diffie-Hellman-Verfahren patentiert worden, dieses Patent ist jedoch 1993 ausgelaufen.

Als Abwandlung des ElGamal-Verfahrens existiert der Digital Signature Algorithm (DSA), der vom NIST (National Institute of Standards and Technology in USA) als Standard Digital Signature Standard (DSS) vorgeschlagen wurde.

In der aktuellen Version von PGP werden die drei Verfahren RSA, ElGamal und DSS unterstützt. Als symmetrische Verfahren werden CAST, Triple-DES, IDEA und seit Version 7 Twofish eingesetzt, die im Folgenden kurz beschrieben werden:

DES / Triple-DES

Das amerikanische National Bureau of Standards (Vorgänger des heutigen NIST) veröffentlichte 1977 bereits den Data Encryption Standard (DES). DES verwendet einen 56-Bit-Schlüssel und verschlüsselt 64-Bit-Blöcke, die im verschlüsselten Zustand die selbe Größe haben. DES wurde entwickelt, um als Hardwareimplementierung möglichst effizient abzulaufen. In einer Softwareimplementierung ist DES relativ langsam. Bei den heutigen Prozessorleistungen ist dieser Nachteil jedoch nicht relevant.

Es gab eine Menge Diskussionen darüber, ob DES bei Verwendung eines 56-Bit-Schlüssels sicher genug wäre. Und tatsächlich wurde 1997 nach einer Ausschreibung der RSA Data Security ein mit einem 56-Bit-Schlüssel verschlüsselter Text geknackt. Zwar wurden dazu mehrere tausend private Rechner im Internet zusammengeschaltet und diese rechneten über vier Monate, es zeigt jedoch, dass DES von jemandem, der sich die entsprechende Ausrüstung leisten könnte, gebrochen werden kann.

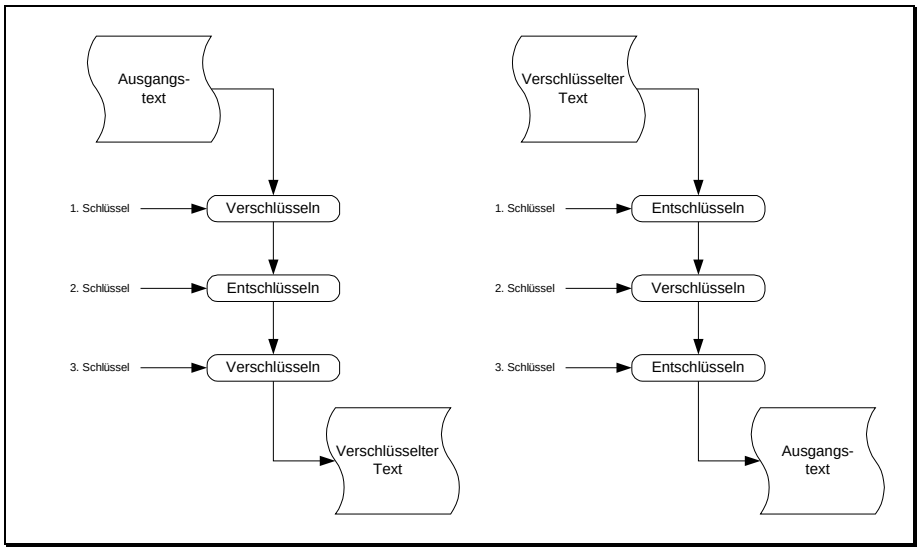


Abbildung 3.1: Ver- und Entschlüsselungsfolgen bei Triple-DES

Um eine Verbesserung zu erreichen, wurde Triple-DES eingeführt. In Triple-DES werden drei Schlüssel verwendet und drei DES-Operationen (Ver- und Entschlüsseln gemischt) durchgeführt. Zum Verschlüsseln wird zunächst mit dem ersten Schlüssel verschlüsselt, dann mit dem zweiten Schlüssel entschlüsselt und anschließend mit dem dritten Schlüssel wieder verschlüsselt. Der dadurch entstandene verschlüsselte Datenblock kann durch die Operationen Entschlüsseln mit erstem Schlüssel, Verschlüsseln mit zweitem Schlüssel und erneutem Entschlüsseln mit erstem Schlüssel wieder in den Ausgangstext entschlüsselt werden (siehe auch Bild). In einer Variation des Verfahrens aus [KPS95] sind der erste und dritte Schlüssel identisch.

IDEA

Der Blockverschlüsselungsalgorithmus IDEA (International Data Encryption Algorithm) wurde 1990 von James L. Massey und Xuejia Lai von der ETH Zürich entwickelt. Er wurde veröffentlicht, um ihn von der Öffentlichkeit auf mögliche Schwachstellen untersuchen und testen zu lassen. Bisher wurde jedoch noch keine Schwachstelle gefunden. IDEA ist zwar öffentlich verfügbar, allerdings hat die Firma Ascom aus der Schweiz ein Patent darauf. Im Gegensatz zu den anderen hier vorgestellten symmetrischen Verfahren hat die Firma Ascom den Algorithmus nicht für den privaten Gebrauch freigegeben.

CAST

CAST verdankt seinen Namen seinen zwei Entwicklern Carlisle Adams and Stafford Tavares von Northern Telecom (Nortel). Nortel hat zwar auf den CAST-Algorithmus ein Patent angemeldet, bietet dieses jedoch der Allgemeinheit zur freien Verfügung an. CAST wird im Detail im [RFC2144] beschrieben. Der CAST-Algorithmus kann Schlüssel der Länge 40 bis 128 Bit verarbeiten. Da er noch nicht sehr lange bekannt ist, ist er noch nicht so genau untersucht worden, wie z.B. der DES-Algorithmus. Dennoch gilt er als extrem sicher.

Twofish

Da die Sicherheit von DES angezweifelt wird (siehe auch in [EFF98]), wurde vom NIST ein neuer Standard ins Leben gerufen, der Advanced Encryption Standard (AES). Der Twofish-Algorithmus von Bruce Schneier der Counterpane Labs ist einer von fünf Kandidaten für AES. Obwohl Twofish nicht für AES ausgewählt wurde, wird dieser Algorithmus in PGP verwendet. Twofish hat den Vorteil, mit 128-Bit-Datenblöcken zu arbeiten, d.h. der Algorithmus ist für zum Zeitpunkt der Erstellung dieser Arbeit aktuell eingesetzte Prozessoren optimiert. Als Schlüssellängen können 128, 192 und 256 Bit verwendet werden. Er ist frei verfügbar, da er nicht patentiert wurde.

3.1.3 Lieferumfang PGP Corporate Desktop

Eine Version von PGP für den kommerziellen Einsatz bietet Network Associates unter dem Namen PGP Corporate Desktop an[2]. In dieser Arbeit wird die zum Zeitpunkt ihrer Erstellung aktuelle Version 7.0.3 untersucht. Diese beinhaltet folgende Komponenten: Personal IDS (Intrusion Detection System), Personal Firewall, VPN (Virtual Private Network), Verschlüsselungsmechanismen für E-Mail, Instant Messaging und Dateien bzw. ganze Festplatten sowie X.509- und PGP-Infrastruktur Verwaltung. Diese Komponenten werden im Folgenden kurz erläutert:

Personal Firewall

Die in dem PGP Corporate Desktop Paket enthaltene Personal Firewall hat die Funktion, einen einzelnen Rechner im Netzwerk vor Angriffen von außen zu schützen. Dazu überprüft sie jedes ein- bzw. ausgehende Datenpaket auf vordefinierte Regeln. Je nach Einstellung werden die Pakete dann entweder weitergeleitet oder, bei Ausgabe einer entsprechenden Meldung, verworfen. Die Personal Firewall bietet dem Anwender bereits sechs vorgefertigte Regelwerke. Somit muss ein Anwender kein Netzwerkspezialist sein, um die Personal Firewall zu konfigurieren. Ferner ist es möglich, eigene Regelwerke zu definieren.

Normalerweise werden in Unternehmen bereits Firewalls eingesetzt, so dass damit alle Rechner innerhalb dieses Netzwerks bereits geschützt sind. Network Associates begründet die Beilage eines Personal Firewalls mit der Gefahr von gezielten Angriffen aus dem firmeninternen Netzwerk. Außerdem bietet die Sicherung einzelner Rechner im internen Netzwerk eine Unterscheidung zwischen verschiedenen Sicherheitsstufen.

Personal IDS (Intrusion Detection System)

Firewalls bieten leider keinen umfassenden Schutz vor Eindringlingen. Sollte es vorkommen, dass sich jemand unerlaubterweise Zugang zu einem geschützten System verschafft, sollte es möglich sein, dies zu erkennen. Network Associates liefert daher die Komponente Personal IDS mit, die diese Aufgabe erfüllen soll.

Dazu überprüft sie den ein- und ausgehenden Verkehr auf verdächtige Aktivitäten und reagiert je nach Einstellung darauf. Es werden die Absenderdaten des Eindringlings, Datum und Uhrzeit sowie Grund des Alarms in einem Logfile festgehalten. Es wird versucht, durch eine Analyse der Aktivitäten des Eindringlings die Regeln der Personal Firewall dynamisch anzupassen, um weitere Aktionen des Eindringlings zu verhindern. Je nach Einstellung gibt das Personal IDS ein akustisches Signal von sich oder benachrichtigt den Administrator z.B. per Mail.

[2] Der Lieferumfang des PGP Corporate Desktop ist in [NAI00a] beschrieben.

Virtual Private Network

Ein VPN (Virtual Private Network) bietet eine sichere Verbindung zwischen zwei Rechnern über einen unsicheren Kommunikationskanal, in diesem Fall vornehmlich das Internet. Dazu werden die Daten zwischen den beiden Rechnern verschlüsselt übertragen. Diese Verbindung wird auch Tunnel genannt.

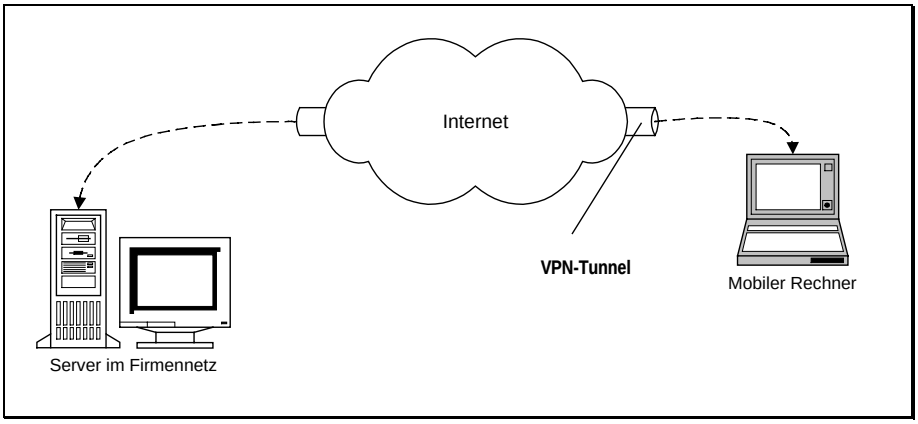


Abbildung 3.2: Sichere Verbindung über ein unsicheres Netz mittels VPN-Tunnel

Dadurch bieten sich verschiedene Möglichkeiten der Nutzung an:

- Ein mobiler Benutzer kann eine sichere Verbindung in das Firmennetzwerk aufbauen.
- Zwei getrennte Firmennetzwerke (z.B. zwei Filialen einer Firma) können über eine sichere Verbindung miteinander verbunden werden.
- Firmen können anderen Personen oder Firmen, denen sie vertrauen, Zugriff auf ihr internes Netzwerk gewähren, um bestimmte Daten auszutauschen.
- Für den Austausch von Daten über das Internet können Einzelpersonen eine sichere Verbindung aufbauen.

Verschlüsselungsmechanismen

Die bekannteste Anwendung von PGP ist das Verschlüsseln von E-Mails. Natürlich bietet auch PGP Corporate Desktop diese Funktion sowie die Verschlüsselung von Nachrichten über ein Instant Messaging System. Ferner ist es möglich, Dateien zu verschlüsseln. Diese können dann per E-Mail-Anhang versendet oder auf einen Datenträger kopiert und auf konventionellem Wege versandt werden.

Die auf diese Weise verschlüsselten Dateien können je nach Einstellung auch auf Systemen ohne installiertes PGP entschlüsselt werden. Dazu muss der Absender ein so genanntes Self Decypting Archive generieren. Dieses enthält die Entschlüsselungssoftware und nach Eingabe des richtigen Passworts werden die darin enthaltenen Daten entschlüsselt.

PGP Corporate Desktop bietet außerdem die Möglichkeit, ganze Festplatten zu sichern. Dazu wird eine Containerdatei angelegt, die im System wie eine eigene Festplatte angesprochen werden kann. Die Daten werden in dieser Containerdatei verschlüsselt abgespeichert. Die Komponente wird von Network Associates PGPdisk benannt.

Ein weiteres mitgeliefertes Sicherheitsmerkmal betrifft das Löschen von Dateien. Beim Löschen werden vom Betriebssystem in der Regel lediglich die Einträge der Datei im Inhaltsverzeichnis des Dateisystems gelöscht. Die eigentlichen Daten sind in diesem Fall noch auf der Festplatte vorhanden und könnten wiederhergestellt werden. PGP Corporate Desktop bietet eine Funktion zum permanenten Löschen von Dateien an. Dabei werden die betroffenen Datenblöcke auf der Festplatte mehrmals überschrieben und es wird sichergestellt, dass auch in der Auslagerungsdatei des Betriebssystems keine Spuren dieser Datei mehr vorhanden sind.

3.1.4 Zertifikate in PGP

Bei der Erstellung eines neuen Schlüsselpaares muss die eigene E-Mail-Adresse und der Name angegeben werden[3]. Außerdem kann zwischen dem RSA- und DH/DSS-Verfahren gewählt werden. Zusätzlich zur E-Mail-Adresse und dem Namen wird für einen eindeutigen Namen aus dem Schlüssel eine Benutzerkennung generiert. Nach dem Generieren des öffentlichen und privaten Schlüssels bietet PGP an, die Benutzerkennung mit dem öffentlichen Schlüssel auf einen so genannten Keyserver zu übertragen. Auf diesem Keyserver kann jeder nach dem öffentlichen Schlüssel und der Benutzerkennung einer Person suchen.

Da es prinzipiell jedem möglich ist, ein Schlüsselpaar zu generieren, in dem jeder beliebige Name angegeben wurde, besteht die Schwierigkeit, die Zugehörigkeit eines Schlüssels zu einer Person sicher festzustellen. Erhält man beispielsweise eine signierte Mail eines bisher unbekannten Absenders, kann man den öffentlichen Schlüssel über einen Keyserver vergleichen, man weiß jedoch nicht, ob der Schlüssel vom Keyserver nicht von jemandem anderen dorthin übertragen wurde.

Eine einfache Möglichkeit, die Authentizität eines Schlüssels zu überprüfen ist, den Inhaber anzurufen oder zu treffen und die Schlüssel zu vergleichen. Dabei sollte der Inhaber des Schlüssels den so genannten Fingerprint des Schlüssels vorlesen. Der Fingerprint ist eine Kontrollsumme des Schlüssels, die eine verbale Übertragung vereinfachen soll. Diese Option hilft jedoch im Beispiel eines unbekannten Absenders nicht, da die Stimme oder das Aussehen des Inhabers nicht bekannt sind.

[3] Die Informationen zu Zertifikaten in PGP wurden aus [Luck99a], [Luck99b], [Luck99c], [NAI00c] und [NAI00u] entnommen.

Damit nicht authentisierte Schlüssel nicht verwendet werden können, sind diese Schlüssel standardmäßig in PGP zunächst als ungültig markiert. Wurde der Schlüssel nach einer Kontrolle für gültig befunden (d.h. er wird vom Empfänger signiert), kann in PGP die Vertrauensstufe eingestellt werden. Es werden vier Vertrauensstufen angeboten:

- **unknown** (Eine Vertrauensstufe konnte bisher nicht ermittelt werden. Ein solcher Schlüssel wird wie ein untrusted Schlüssel behandelt),
- **untrusted** (Ein solcher Schlüssel wird nicht verwendet),
- **marginal** (Ein Schlüssel, der dieser Vertrauensstufe zugeordnet wurde, benötigt mindestens einen weiteren signierten Schlüssel, um als trusted zu gelten) und
- **trusted** (Jeder weitere durch einen trusted Schlüssel signierte Schlüssel gilt ebenfalls als trusted).

Ferner wird bei öffentlichen Schlüsseln, zu denen der geheime Schlüssel verfügbar ist, implizites Vertrauen eingestellt.

Diese Einstellung kann an den Keyserver gesendet werden, wenn der Schlüssel mit der Option *exportable* signiert wurde. Dort wird auf Anfrage ab diesem Zeitpunkt die Signatur des Empfängers mitgeschickt. Diese Signatur wird in der PGP-Architektur Zertifikat genannt. Im folgenden Bild ist ein Beispiel für Zertifikate zu sehen.

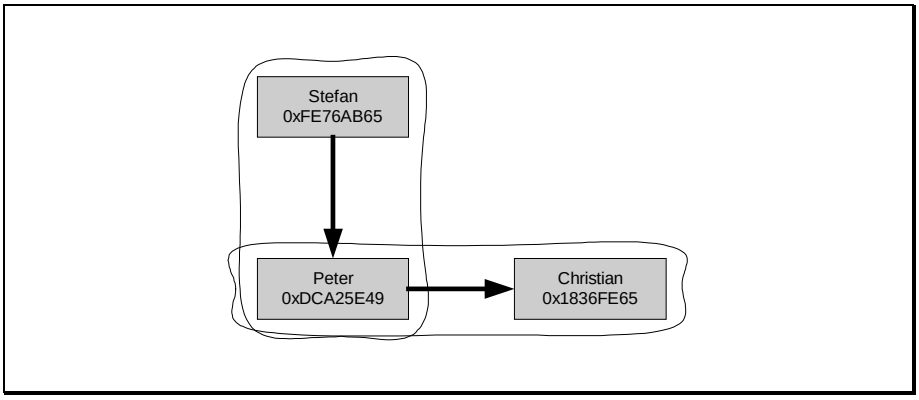


Abbildung 3.3: Beispiel für eine Vertrauensweitergabe in PGP

In dem Bild wird gezeigt, dass Peter dem Schlüssel von Christian vertraut, da sie sich persönlich kennen. Auch Stefan und Peter kennen sich persönlich (Bekanntheit durch Kreise markiert), Christian und Stefan jedoch nicht. Da Stefan weiß, dass Peter die Authentizität von Schlüsseln sorgfältig prüft, kann er darauf vertrauen, dass der Schlüssel von Christian gültig ist, auch wenn er ihn nicht von ihm persönlich erhalten hat.

Im nächsten Bild wird ein Beispiel für das teilweise Vertrauen gezeigt, das in PGP möglich ist.

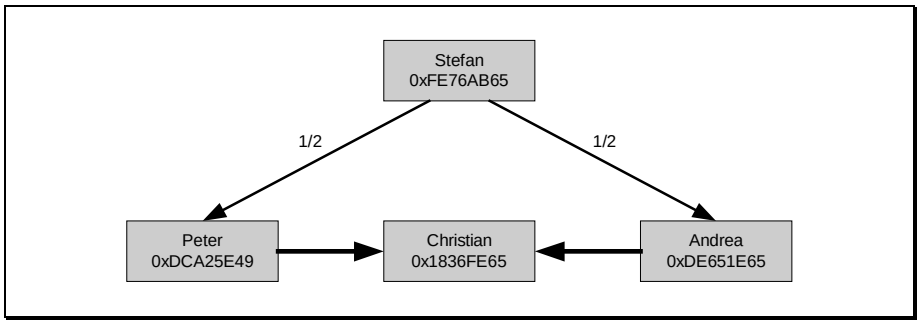


Abbildung 3.4: Beispiel für die Vertrauensstufe marginal in PGP

In diesem Beispiel weiß Stefan, dass Peter und Andrea zwar die Gültigkeit anderer Schlüssel überprüfen, ist sich jedoch nicht sicher, ob sie dies in jedem Fall zuverlässig durchführen. Daher setzt er die Vertrauensstufe der beiden auf marginal. Damit nun der Schlüssel von Christian als gültig angesehen werden kann, erwartet PGP, dass mindestens zwei Personen, denen Stefan marginal vertraut, dessen Schlüssel zertifiziert haben.

Durch die gegenseitige Zertifizierung von Personen entsteht ein Netz aus Gültigkeitspfaden, das als Web of Trust bekannt ist. Der Vorteil liegt im dezentralen Ansatz, d.h. jeder Benutzer hat die volle Kontrolle darüber, wem er wie weit vertraut.

Mit Hilfe einer Erweiterung, die seit der Version 5 in PGP implementiert ist, können ansatzweise hierarchische Infrastrukturen aufgebaut werden. In den erweiterten Einstellungen zur Signierung von Schlüsseln gibt es die Möglichkeit, einen Schlüssel als Meta Introducer zu signieren. Der Inhaber dieses Schlüssels, in der Regel eine Certification Authority (CA), kann so genannte Trusted Introducer Zertifikate erstellen. Diese werden in PGP als gültig aufgenommen und die Vertrauensstufe automatisch auf trusted gesetzt. Im folgenden Bild wurde das Zertifikat der c't PGP-CA von Stefan als Meta Introducer eingestuft. Daher werden die von der c't PGP-CA zertifizierten Schlüssel von Christian, Andrea, Bernd und Alexander automatisch als trusted eingestuft.

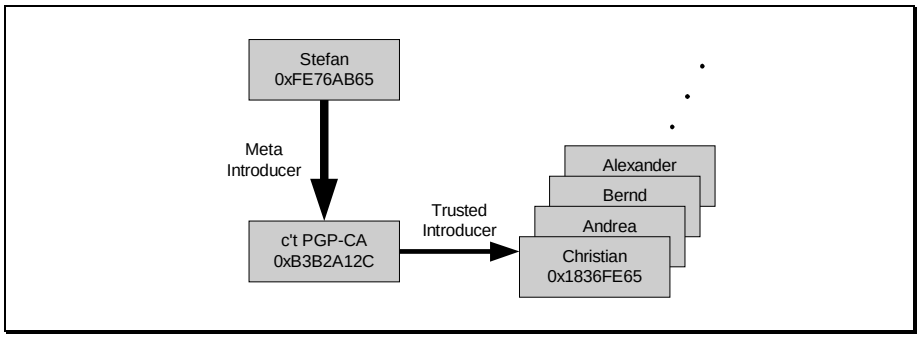


Abbildung 3.5: Beispiel für die Unterstützung von CAs in PGP

In einem Firmennetz bedeutet dies eine wesentliche Erleichterung für die einzelnen Benutzer. Sie müssen nun lediglich den Schlüssel der firmeneigenen CA zertifizieren. Damit erkennen sie alle Zertifikate, die von dieser CA erstellt wurden, automatisch als gültig und trusted ein. Welche Komponenten für den Aufbau einer Infrastruktur nötig sind, wird im Folgenden Abschnitt gezeigt:

3.1.5 Aufbau einer Infrastruktur mit PGP

Um mit PGP eine Infrastruktur in einem Firmennetzwerk aufzubauen, sind weitere Komponenten nötig. Diese sind in [NAI00a] beschrieben. Im folgenden Bild ist eine solche Infrastruktur schematisch dargestellt. Sie enthält PGP Keyserver (als LDAP-Server) und Net-Tools PKI (als CA). Es können jedoch auch entsprechende Lösungen anderer Hersteller verwendet werden.

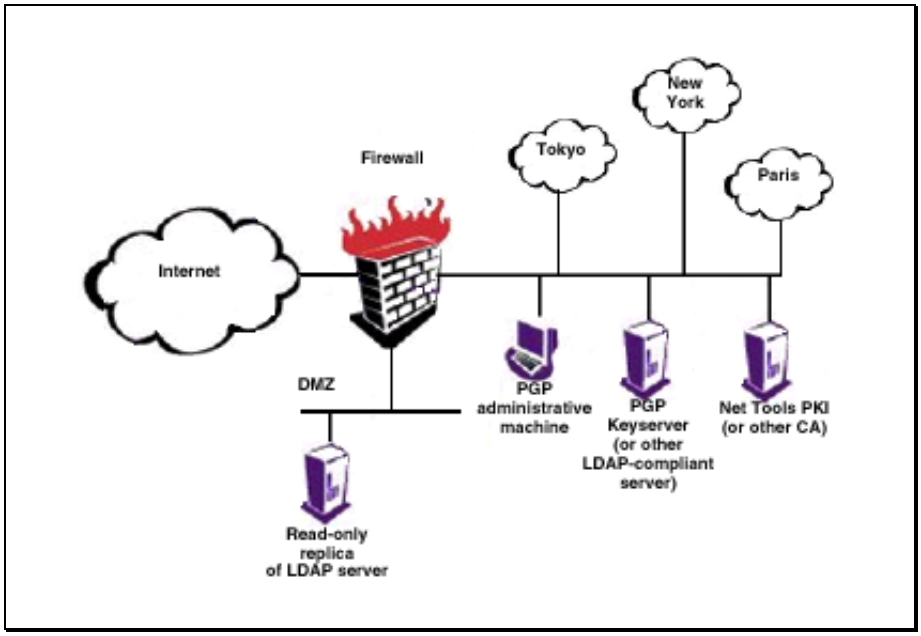


Abbildung 3.6: Beispiel einer einfachen Infrastruktur mit PGP Komponenten (Entnommen aus [NAI00a])

Die Administration der PGP Installationen (z.B. Festlegen der erlaubten Installationsoptionen) erfolgt über PGPadmin, das beim PGP Corporate Desktop mitgeliefert wird.

PGPadmin

Diese Software wird auf einem administrativen Rechner installiert und bietet dem Administrator die Möglichkeit auszuwählen, welche Optionen von PGP im Unternehmen erlaubt oder verboten sind. PGPadmin erlaubt das Vordefinieren der Installationsoptionen. Dabei gibt es zwei Möglichkeiten, diese Einstellungen im Unternehmen durchzusetzen:

- Erstellung eines neuen Installationspakets, das die Benutzer auf ihren Rechnern starten können. Dabei sind die vom Administrator gewählten Optionen bereits ausgewählt oder deaktiviert und können von den Benutzern je nach Voreinstellung des Administrators nicht verändert werden.

- Erstellung eines Optionen-Profils, das in einer Datei gespeichert wird und über den Keyserver, der im folgenden Abschnitt beschrieben wird, im Netzwerk von den Benutzern abrufbar ist.

Der Vorteil des Optionen-Profils ist, dass die Clients im Netzwerk in regelmäßigen Abständen den Keyserver kontaktieren, um z.B. ungültige Zertifikate zu aktualisieren. Dabei kann auch das Optionen-Profil geladen und Änderungen automatisch übernommen werden. So ist eine relativ schnelle Durchsetzung von Änderungen der Sicherheitspolicy möglich.

PGP Keyserver

Der PGP Keyserver implementiert einen LDAP-Server. Er verarbeitet Suchanfragen und unterstützt das Management von PGP-Zertifikaten. Es handelt sich in erster Linie um eine Datenbank für Zertifikate eines Unternehmens. Es werden regelmäßig Indizierungen der Datenbank durchgeführt, so dass Suchanfragen schnell beantwortet werden können.

PGP Keyserver sind skalierbar, d.h. durch ein Replikationsmanagement können die gespeicherten Daten zwischen mehreren im Unternehmen eingesetzten Keyservern ausgetauscht werden. Dies hat folgende Vorteile:

- **Fehlertoleranz**: Sollte ein Keyserver ausfallen, können andere Keyserver des Unternehmens für Anfragen verwendet werden.

- **Lastbalancierung**: Die Anfragen an die Keyserver können so verteilt werden, dass einzelne Keyserver nicht überlastet werden.

- **Kürzere Zugriffszeiten**: Setzt man in schnellen Teilnetzen jeweils eigene Keyserver ein, können diese über das schnelle Teilnetz erreicht werden und nicht über eine Zwischenverbindung. Dies reduziert Zugriffszeiten.

PGP Keyserver bieten ferner die Möglichkeit, verlorene Schlüssel wiederherzustellen. Bei der Generierung eines Schlüsselpaars wird der Benutzer aufgefordert, eine Frage mit Antwort einzugeben, die er leicht beantworten kann, auf deren Lösung andere jedoch nicht kommen.

Der PGP Keyserver wird mit einer abgespeckten Version des Apache-Webservers geliefert. Dadurch wird den Benutzern zusätzlich ein Web-Interface für Suchanfragen geboten. Auch die Konfiguration des Keyservers wird dem Administrator über das Web-Interface ermöglicht.

Net Tools PKI

Dieses Paket von Network Associates enthält einen Certification Authority Server (CA). Dieser ermöglicht einem Unternehmen, Zertifikate zu erstellen, für ungültig zu erklären, zu speichern und zu verwalten. Mit der CA von Network Associates können PGP-Zertifikate an Mitarbeiter im Unternehmen ausgestellt werden. Zertifikate nach dem X.509-Standard werden unterstützt, können jedoch nicht erstellt werden.

3.2 Baltimore PKI

Baltimore bietet drei PKI-Pakete unter dem Namen UniCERT an, die aufeinander aufbauen.

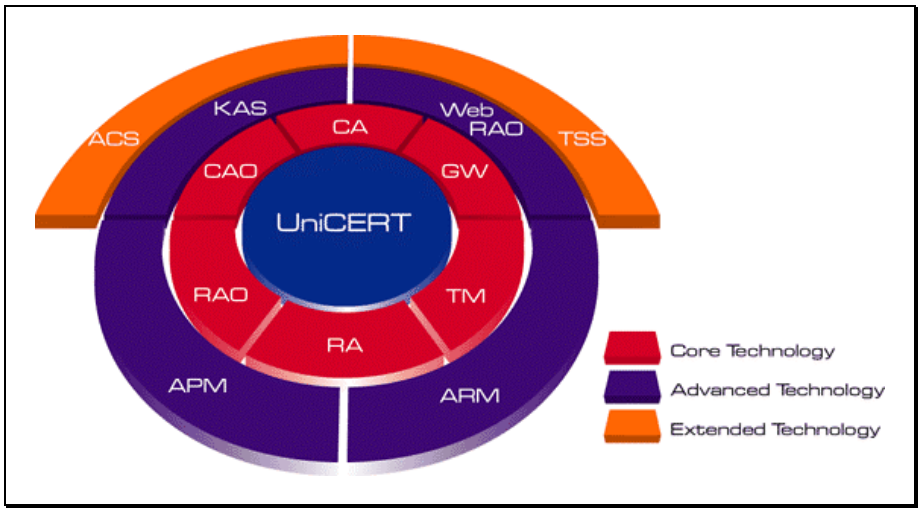


Abbildung 3.7: Lieferumfang der Baltimore UniCERT Suite
(Entnommen aus der Produktübersichtsseite der Baltimore Webseite[4])

In der Core-Technology-Version sind die Basiskomponenten enthalten, die für den Aufbau einer PKI notwendig sind. Die Erweiterungen Advanced-Technology und Extended-Technology werden in dieser Arbeit nicht behandelt, daher werden im Folgenden nur die einzelnen Komponenten des Core-Technology Pakets beschrieben, welches derzeit in der Version 3.1 vorliegt.

Im ersten Abschnitt wird zunächst allgemein auf den Aufbau einer Hierarchie mit Hilfe einer PKI eingegangen. Im darauffolgenden Abschnitt werden die Standards beschrieben, die für

[4] www.baltimore.com/unicert/unicert/details.html

Zertifikate innerhalb einer PKI verwendet werden. Im dritten Abschnitt werden die einzelnen Komponenten vorgestellt, die im Lieferumfang der Baltimore UniCERT-PKI enthalten sind.

3.2.1 Hierarchie einer PKI

Die Art, wie eine PKI aufgebaut werden kann, wurde in der Arbeitsgruppe PKIX (PKI unter Verwendung von X.509 Zertifikaten) der IETF in einer Roadmap vorgestellt [ArTu00]. Nach dieser Roadmap wird eine PKI folgendermaßen definiert:

> Eine PKI ist eine Menge von Hardware, Software, Personen, Richtlinien und Prozeduren, die für die Erstellung, Verwaltung, Verteilung und Rücknahme von Zertifikaten, die auf Public-Key-Kryptographie basieren, benötigt werden.

In einer PKI werden verschiedene Komponenten verwendet, die entsprechend dem folgenden Bild aus [ArTu00] miteinander verknüpft werden:

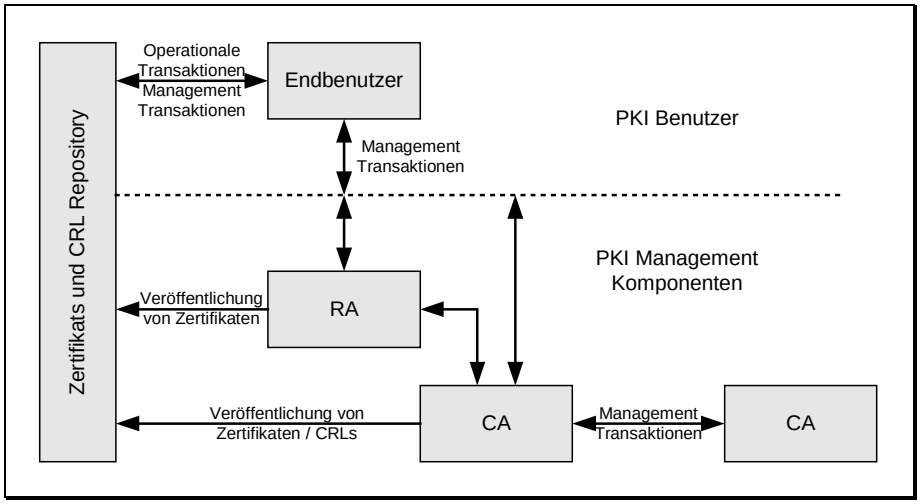


Abbildung 3.8: Komponenten in einer PKI nach der Roadmap der PKIX

Der *Certification Authority (CA)* wird von den Benutzern der PKI Vertrauen entgegengebracht. Die CA erstellt Zertifikate, dabei kann sie optional den geheimen Schlüssel der Benutzer erstellen und mitverwalten. Außerdem ist die CA für die Rücknahme von Zertifikaten zuständig.

Zwischen den Endbenutzern und der CA kann eine *Registration Authority (RA)* geschaltet werden, die administrative Aufgaben für die Ausstellung von Zertifikaten übernimmt. Dazu gehören beispielsweise die Überprüfung der Identität eines Antragstellers, die Überprüfung, ob die beantragten Eigenschaften eines Zertifikates dem Antragsteller zugewiesen werden dürfen, und die Überprüfung, ob der Antragsteller im Besitz des geheimen Schlüssels ist, der zum öffentlichen Schlüssel gehört, mit dem das Zertifikat beantragt wurde.

Die Komponenten der PKI müssen nach einem *Certificate Practice Statement (CPS)* handeln. Im CPS werden Regeln festgelegt, die den Endbenutzern eine Einschätzung der Vertrauens-

würdigkeit der einzelnen Komponenten ermöglichen soll. Es kann z.B. festgelegt sein, dass Zertifikate nur nach vorhergehender Prüfung des Personalausweises an Personen ausgegeben werden.

Die *Endbenutzer* sind Personen, Maschinen oder Teile einer Software, die ein Zertifikat erhalten und damit Daten digital signieren können. Ferner verwenden Endbenutzer Zertifikate, um die Authentizität von Daten zu überprüfen, die sie von anderen Endbenutzern erhalten haben.

Das *Zertifikats- und CRL-Repository* bietet eine zentrale Datenbank für alle beteiligten Komponenten, in der Zertifikate, CRLs sowie weitere Daten gespeichert werden können. So kann beispielsweise eine Sicherheitspolicy, die für die gesamte PKI gilt, in dieser Datenbank zur Verfügung gestellt werden.

Die möglichen Funktionen, die eine PKI erfüllen muss, werden im Folgenden vorgestellt:

Registrierung: Diese Aktion bezeichnet das erste Bekanntmachen eines Endbenutzers gegenüber der CA. Dies kann entweder direkt oder über eine RA geschehen. Vom Endbenutzer müssen die für die Registrierung benötigten Daten genannt werden können, wie z.B. ein einheitlicher Name und ein vollqualifizierter Domainname, die in das Zertifikat integriert werden sollen. Die CA (bzw. RA) muss vor der Ausstellung des Zertifikats die Angaben überprüfen und die Regeln des CPS beachten.

Zertifizierung: Die CA stellt dem Endbenutzer das beantragte Zertifikat aus und liefert es über einen der verfügbaren Wege dem Endbenutzer aus. Gleichzeitig wird das Zertifikat im Zertifikats- und CRL-Repository abgelegt.

Schlüssel-Wiederherstellung: In manchen PKI-Implementierungen kann erwünscht sein, dass jeglicher Schlüsselaustausch bzw. die Verwendung der Schlüssel registriert und gespeichert wird. Somit ist ein Wiederherstellen verschlüsselter Daten möglich, auch wenn der Endbenutzer seinen Schlüssel verloren haben sollte.

Wird eine solche Funktion angeboten, muss sichergestellt werden, dass der gespeicherte geheime Schlüssel nur autorisierten Personen zugänglich gemacht wird.

Schlüssel-Generierung: Schlüsselpaare können entweder vom Endbenutzer selbst oder von der CA erstellt werden. Die Verfahrensweise wird im CPS festgelegt. Werden die Schlüssel von der CA erstellt, müssen sie auf einem sicheren Weg den Endbenutzer erreichen. Die Übergabe könnte z.B. auf einer Smartcard erfolgen.

Schlüssel-Aktualisierung: Schlüsselpaare sollten von Zeit zu Zeit erneuert werden. Das folgende Ereignis veranlasst eine Erneuerung eines Schlüsselpaares:

- Das im Zertifikat angegebene Ablaufdatum wurde erreicht. Der Vorteil liegt in der Planbarkeit. Da im Voraus bereits das Ablaufdatum bekannt ist, können Vorkehrungen getroffen werden, so dass der Wechsel zwischen dem alten und neuen Zertifikat reibungslos durchgeführt werden kann.

Rücknahme von Zertifikaten: Ein Zertifikat kann durch bestimmte Ereignisse bereits vor seinem vorgesehenen Ablaufdatum für ungültig erklärt werden. Folgende Ereignisse sind denkbar:

- Der Endbenutzer ändert seinen Namen.
- Ein Mitarbeiter verlässt das Unternehmen, daher muss sein Zertifikat für ungültig erklärt werden.
- Dritte haben Zugriff zum geheimen Schlüssel erlangt, der zum Zertifikat gehört oder es wird vermutet, dass dies geschehen ist. Da es sich in diesem Fall um eine unvorhergesehene Neugenerierung des Schlüsselpaares handelt, kann der Wechsel nicht reibungslos verlaufen.

Die PKI muss in der Lage sein, ein Zertifikat für ungültig zu erklären und das neue zur Verfügung stellen.

Für die Rücknahme von Zertifikaten werden CRLs eingesetzt, in denen die für ungültig erklärten Zertifikate enthalten sind. Die CRL wird in regelmäßigen Abständen von der CA im Zertifikats- und CRL-Repository abgespeichert.

Cross-Zertifizierung: Bei der Cross-Zertifizierung wird ein Zertifikat von einer CA für eine andere CA ausgestellt. Dies ermöglicht Benutzern, die der PKI der ersten CA angehören, Zertifikaten zu trauen, die von der CA einer anderen PKI ausgestellt wurden. Dadurch wird z.B. der Austausch von Zertifikaten zweier verschiedener Unternehmen möglich.

Im folgenden Abschnitt werden die Standards, die Zertifikate betreffen, erläutert. Dazu gehört das Format für Zertifikate selbst und das Format zum Austauschen von Zertifikaten.

3.2.2 Zertifikatsformate

In der hier vorgestellten Baltimore UniCERT PKI werden Zertifikate nach dem IX.509v3 Standard generiert und verwaltet. In diesem Abschnitt wird auf den Standard der ISO und ITU eingegangen. Zum besseren Verständnis wird zunächst der X.500-Verzeichnisdienst vorgestellt (Informationen aus [Chad94]), danach der 1988 vorgeschlagene X.509 Standard und abschließend die Erweiterungen der 3. Version von X.509 (Informationen aus [Bran97]).

X.500

Das X.500 Verzeichnis ist vergleichbar mit einem Telefonbuch, in dem nach Angabe eines Namens zusätzliche Informationen (wie Telefonnummer und Adresse) ermittelt werden können. In einem X.500 Eintrag werden im Gegensatz zum Telefonbuch mehr Daten gespeichert, wie z.B. eine E-Mail-Adresse oder der Arbeitgeber. X.500 Einträge beziehen sich nicht nur auf Personen, sondern können auch für alle erdenklichen Objekte angelegt werden. Dazu gehören u.a. Computer, Drucker, Unternehmen, Länder und Regierungen.

Jedem X.500 Eintrag wird ein eindeutiger Name (engl. distinguished name – DN) zugewiesen. Um die Eindeutigkeit zu gewährleisten, werden DNs hierarchisch vergeben und in einem entsprechendem Baum (directory information tree – DIT) dargestellt. Im folgenden Bild wird ein solcher Baum gezeigt:

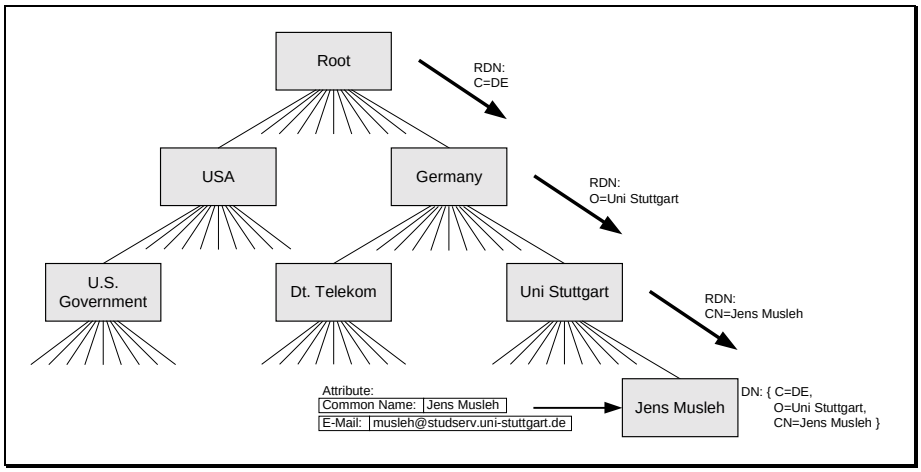


Abbildung 3.9: Hierarchischer Aufbau der Namensgebung in X.500

Jedem Knoten ist ein Mutterknoten (ausgenommen der Wurzelknoten) und mehrere Kindknoten zugeordnet. Bis auf den Wurzelknoten erhält jeder Knoten einen in der Hierarchie relativen Namen (relative distinguished name – RDN), der in der Hierarchie des übergeordneten Knotens eindeutig ist (z.B. darf der Common Name „Jens Musleh“ in der Uni Stuttgart nur einmal vorkommen).

X.509

Um eine Authentifizierung der Einträge in einem X.500 Verzeichnis zu ermöglichen, wurde X.509 entwickelt. In einem X.509 Zertifikat sind die folgenden Felder enthalten:

Version	Version des verwendeten X.509 Formats
Serial Number	Vergabe einer lfd. Nummer durch die ausstellende Instanz, z.B. eine CA
CA Signature Algorithm	Der von der ausstellenden Instanz verwendete Kryptoalgorithmus und seine Hash-Funktion
Issuer Name	Name der ausstellenden Instanz
Validity Period	Gültigkeitsdauer des Zertifikats
Subject Name	Name des Objekts bzw. des Zertifikatinhabers
Subject PK Information	Der öffentliche Schlüssel des Zertifikatinhabers und Angaben zum verwendeten Verschlüsselungsalgorithmus und zur Hash-Funktion.

Tabelle 3.1: Felder in einem X.509-Zertifikat

Durch die enge Verbindung von X.509 mit X.500 werden die CAs in einer streng hierarchischen Infrastruktur angeordnet. Es ist vorgesehen, eine Baumstruktur für eine weltweite Zertifizierungsarchitektur zu schaffen. Daher muss jedem X.509-Zertifikat ein global eindeutiger Name zugeordnet werden. An der Wurzel des Baumes steht eine weltweite Root-CA, die

untergeordnete Stellen zertifiziert, die wiederum für weitere kleinere Teilbereiche zuständig sind.

Um in dieser Hierarchie tatsächlich für eindeutige Namen sorgen zu können, wurden in der 2. Version von X.509 zwei weitere Felder hinzugefügt:

Issuer Unique ID	Bitstring, der den X.500-Namen der ausstellenden Instanz weltweit eindeutig machen soll
Subject Unique ID	Bitstring, der den X.500-Namen des Objekts bzw. des Zertifikatinhabers eindeutig machen soll

Tabelle 3.2: Zusätzliche Felder in einem X.509-Zertifikat der 2. Version

Ein Beispiel für die Notwendigkeit dieser Felder ist ein Mitarbeiter mit einem häufig vorkommenden Namen, der seinen Arbeitgeber verlässt. Nun kann es leicht vorkommen, dass ein neuer Mitarbeiter in diesem Unternehmen anfängt, der den selben Namen hat. Mit Hilfe der Subject Unique ID können die Zertifikate der beiden Personen unterschieden werden.

Um eine Verarbeitung in den Endsystemen gewährleisten zu können, müssen alle im Zertifikat verwendeten Bezeichner eindeutig definiert werden. Daher wird allen Bezeichnern eine globale Objektidentifikationsnummer (OID) zugewiesen. Diese wird aus mehreren ganzen Zahlen zusammengesetzt, die durch Punkte getrennt werden. Die OID wurde bereits im X.500 Verzeichnisdienst eingeführt und beschreibt die Semantik eines Attributs eines Verzeichniseintrags. Die OID wird zentral vergeben.

Problematisch an den beiden vorgestellten Versionen ist der geforderte streng hierarchische Aufbau der Infrastruktur. In der von der PKIX-Arbeitsgruppe vorgeschlagenen Infrastruktur werden X.509 Zertifikate der Version 3 verwendet, ohne jedoch die streng hierarchische Struktur von X.509 zu übernehmen.

X.509v3

Aufgrund der vorhergenannten und anderer aufgetretener Probleme in den Versionen 1 und 2 des X.509-Standards wurde das Format der X.509v3-Zertifikate und CRLs individuell erweiterbar gestaltet. Die bisher genannten Felder der vorhergehenden Versionen bleiben als Basisattribute erhalten. Zusätzliche Felder sollen dazu dienen, weitere Informationen im Zertifikat selbst zu speichern. Die Erweiterungen im Zertifikatsformat werden in der folgenden Tabelle beschrieben:

Certificate Policies / Policy Mapping	Die Richtlinien, die eine CA befolgt um Zertifikate auszustellen, können im Zertifikat untergebracht werden. Damit soll einem Benutzer des Zertifikats die Entscheidung erleichtert werden, ob er diesem bzw. dem übergeordneten CA-Zertifikat Vertrauen schenkt. Ferner können Einschränkungen bezüglich der Nutzung des Zertifikats festgelegt werden. So könnte im Zertifikat die Information enthalten sein, dass es nur zum Signieren von E-Mails gedacht ist.
Alternative Names	In diesem Feld können E-Mail Adressen oder Internet Adressen angegeben werden. Damit soll der Zugriff auf eine X.500-Struktur umgangen werden.
Subject Directory Attributes	Diese Erweiterung erlaubt die Aufnahme beliebiger Attribute für spezielle Anwendungen in das Zertifikat.
Certification Path Constraints	Mit dieser Erweiterung kann von einer CA vorgegeben werden, auf welche Weise (z.B. welcher Zertifizierungspfad verfolgt werden soll) die Gültigkeit des Zertifikats geprüft werden soll. Dadurch werden nicht hierarchische Strukturen möglich.

Tabelle 3.3: Zusätzliche Felder in einem X.509-Zertifikat der 3. Version

Im X.509v3-Standard wurden bereits einige Attribute definiert, die hier jedoch nicht näher beschrieben werden sollen. Weitere Attribute (wie z.B. Personalnummern innerhalb eines Unternehmens) können individuell definiert werden. Dazu muss vom PKI-Betreiber jedoch ein OID-Präfix beantragt werden, unter der die selbstdefinierten Attribute angesiedelt werden. So hat Netscape z.B. bereits anwendungsspezifische Attribute definiert, die alle mit der OID 2.16.840.1.113730 beginnen.

Bei der Verwendung selbstdefinierter Attribute entsteht jedoch das Problem, die selbst vergebenen OIDs bekannt zu machen. Der Benutzer eines Zertifikats muss die Bedeutung der darin enthaltenen Attribute vor der Benutzung kennen. Die Bedeutung einer OID kann nur ermittelt werden, wenn sie vom Ersteller veröffentlicht wurde. Dafür sind jedoch keine zentralen Stellen verfügbar, daher ist eine systematische Suche nach der Bedeutung einer OID nicht möglich.

Die Kommunikation zwischen den Komponenten einer PKI muss bestimmten Standards entsprechen, um Interoperabilität zu gewährleisten. Die Firma RSA Data Security Inc hat 1991 begonnen eine Reihe von Verfahren, die die Kommunikation für einzelne Aufgaben beschreiben, unter dem Namen Public-Key Cryptography Standards (PKCS) zu veröffentlichen. Die Standards sind PKCS#10, der die Zertifikatsanfrage eines Benutzers an eine CA beschreibt, und PKCS#7, der verwendet werden kann, um das angeforderte Zertifikat dem Benutzer zu schicken.

3.2.3 Lieferumfang der Baltimore UniCERT-PKI

Im Folgenden werden die Programme vorgestellt, die im Baltimore UniCERT-PKI Lieferumfang enthalten sind [Balt00a].

Certification Authority (CA)

Die Certification Authority steht in der Hierarchie der UniCERT-PKI an der Spitze. Sie ist in der Dokumentation [Balt00ca] beschrieben, deren Hauptaufgabe es ist, Zertifikate zu generieren und zu signieren. In großen Unternehmen können mehrere CAs eingesetzt werden, es wird dazu eine Root-CA aufgebaut, die die Verwaltung mehrerer Sub-CAs übernimmt.

Baltimore empfiehlt, den Rechner, der als CA fungiert, besonders zu schützen. Es muss verhindert werden, dass der geheime Schlüssel des CA-Schlüsselpaars in falsche Hände gerät, da sonst eigene Zertifikate im Namen des CA-Betreibers generiert werden könnten. Natürlich könnte man das CA-Schlüsselpaar für ungültig erklären, dann müssten jedoch ebenfalls alle bisher generierten Zertifikate erneuert werden. Dies bedeutet einen enormen Aufwand und verursacht entsprechend hohe Kosten.

Um diesem Fall vorzubeugen, werden von der UniCERT-CA mehrere Hardware-Lösungen zur Generierung und Speicherung des Schlüsselpaars unterstützt, darunter u.a. RACAL77 (Speicherung und Verwendung der Schlüssel auf einer Erweiterungskarte im ISA-Slot des CA-Rechners) und Smartcards. Baltimore rät jedoch von der Benutzung von Smartcards ab, da die Schlüssel einer CA nicht bestimmten Personen zugeordnet werden. Außerdem kann eine Smartcard leichter verloren gehen als eine eingebaute Hardware.

Bei der Installation der UniCERT-CA muss der Administrator wählen, ob ein Schlüsselpaar für alle Aktionen der CA verwendet wird oder ob für jede mögliche Aktion ein eigenes Schlüsselpaar generiert werden soll. Mögliche Aktionen sind:

- Datenverschlüsselung
- CRL Signierung
- Zertifikatssignierung
- Unleugbarkeit (dabei werden Einträge im Logfile signiert)
- Verschlüsselung symmetrischer Schlüssel

Nach der Installation einer CA auf einem Rechner wird außer dem Start und Beenden des Services keine weitere interaktive Aktion auf diesem Rechner ausgeführt. Als Interface zwischen dem Administrator und der CA dient die CA Operator Komponente von UniCERT.

CA Operator (CAO)

Die CA Operator Komponente wird zur Verwaltung der Daten der CA verwendet. Sie wird im Detail in [Balt00cao] beschrieben. Dem Benutzer dieser Komponente, der ebenfalls CA Operator genannt wird, stehen drei Funktionen zur Verfügung:

- Verwalten der PKI-Struktur
- Verwalten der Sicherheitspolicy
- Verwalten der gespeicherten Zertifikate

Zur Verwaltung der PKI-Struktur wird dem CA Operator ein so genannter PKI-Editor angeboten, der in einer grafischen Maske die folgenden Funktionen sehr intuitiv unterstützt:

- Abbilden des Layouts der verschiedenen Entitäten in der PKI
- Konfiguration der Attribute der verschiedenen Entitäten
- Festlegen der Kommunikationsprotokolle (z.B. E-Mail, PKIX oder TCP) zwischen den Entitäten
- Generierung von Schlüsseln und Zertifikaten für die Entitäten
- Weiterleiten von Änderungen an der Sicherheitspolicy an die Registration Authority Operator
- Exportieren von Zertifikaten und CRLs

Ein einfaches Beispiel einer PKI ist aus dem folgenden Bild ersichtlich. Sie enthält eine Root-CA, an der zwei Sub-CAs anschließen. Die eine Sub-CA wird von zwei RAs, die andere von einer RA verwendet. Die RAs werden von mehr als einem RA Operator administriert im Gegensatz zu den CAs, denen jeweils nur ein CA Operator zugeordnet wurde.

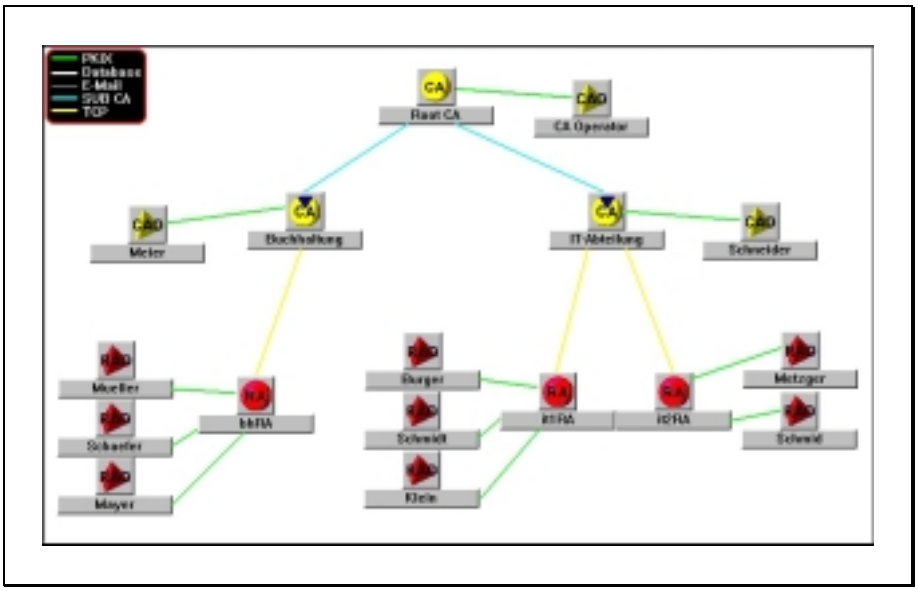


Abbildung 3.10: Beispiel für eine PKI, dargestellt im PKI Editor der Baltimore PKI

Im zweiten Modul, der Verwaltung der Sicherheitspolicy, können das Layout der einzelnen Registrierungsmasken und Vorgaben für die Erstellung von Zertifikaten festgelegt werden. In der Sicherheitspolicy werden eine Menge von Kriterien festgelegt, die vor der Erstellung eines Zertifikats erfüllt sein müssen.

Zertifikate können bei UniCERT über ein Web-Interface oder per E-Mail angefordert werden. Es ist auch möglich, Zertifikate nur nach persönlichem Erscheinen des Anfragenden auszustellen. Unter welchen Bedingungen ein Zertifikat ausgestellt wird, sollte im Certificate Practice Statement (CPS) festgelegt sein. Dies ist ein Dokument, das für jedermann einsehbar ist und in dem vom Betreiber der CA erklärt wird, welche Voraussetzungen von ihm und vom Anfragenden erfüllt werden müssen. Die Aussagen in diesem Dokument sollten sich in der Sicherheitspolicy widerspiegeln.

In der Verwaltung der gespeicherten Zertifikate ist es dem CA Operator möglich, eine Liste der gespeicherten Zertifikate ausgeben zu lassen, einzelne Zertifikate für ungültig zu erklären, zu exportieren, temporär für ungültig zu erklären und Details anzeigen zu lassen.

Registration Authority (RA)

Die Registration Authority stellt die ausgebende Stelle in der UniCERT-PKI dar. Die Beschreibung ist in [Balt00ra] zu finden. Sie verarbeitet Zertifikatsanfragen, die von Benutzern persönlich, per Web-Interface oder E-Mail an den RA Operator gestellt werden. Die Anfragen werden von der RA signiert und an die übergeordnete CA weitergeleitet. Die daraus resultierenden Nachrichten der CA werden von der RA überprüft und erst dann an den Benutzer weitergeleitet.

Anfragen der Benutzer werden, bevor sie an die CA weitergeleitet werden, zunächst auf die Einhaltung der Sicherheitspolicy hin überprüft. Die Sicherheitspolicy wird bei Änderungen vom CA Operator an alle RAs geschickt. Die RA verarbeitet Anfragen sequentiell, d.h. es wird eine Anfrage nach der anderen abgearbeitet. Alle Aktionen der RA werden in einem Logfile festgehalten.

RA Operator (RAO)

Der RA Operator ist eine Person, die Anfragen auf Zertifikate von Benutzern bearbeitet. Dazu überprüft sie je nach CPS die persönlichen Daten des Benutzers und verwendet das RA Operator Programm von UniCERT, um die Anfrage an die RA weiterzuleiten. Dieses ist in der Dokumentation [Balt00rao] beschrieben.

Das RA Operator Programm bietet dem RA Operator die Möglichkeit, Zertifikate zu beantragen, für ungültig zu erklären und die angeforderten Zertifikate von der RA abzurufen.

Web- bzw. Mail-Gateway (GW)

Das UniCERT Gateway Modul bietet den Benutzern die Möglichkeit, Zertifikatsanfragen über ein Web-Interface oder per E-Mail zu stellen. Es wird in [Balt00gw] beschrieben. Es bleibt dem Administrator überlassen zu entscheiden, ob beide Möglichkeiten auf einem Rech-

ner implementiert werden oder ob für die einzelnen Aufgaben eigene Rechner eingerichtet werden.

Beim Einsatz des UniCERT Gateways als Mail-Gateway werden Mail-Anfragen an eine festgelegte Mailadresse zunächst auf ihre Richtigkeit überprüft. Erfüllen sie die Anforderungen, werden sie an die RA über das Netzwerk weitergeleitet. Die RA speichert die Anfrage in ihrer Datenbank, aus der der RA Operator sie zur Bearbeitung ausliest. Wurde das Zertifikat erstellt, wird es von der RA über das Netzwerk an das Gateway geleitet, das es per Mail an den Anfragenden sendet.

Voraussetzung für den Betrieb des Gateways als Mail-Gateway ist die Einrichtung einer Mailbox auf einem Mailserver, der die Protokolle SMTP und POP3 unterstützt. Diese Voraussetzung wird von den meisten Mailservern erfüllt.

Wird UniCERT Gateway als Web-Interface verwendet, können Benutzer ihre Anfragen direkt von einer Webseite absenden. Dazu wurde von Baltimore ein Webserver in das Gateway integriert. Die Anfragen werden, wie beim Einsatz als Mail-Gateway, zunächst auf ihre Richtigkeit geprüft und anschließend von der RA verarbeitet. Im Gegensatz zum Mail-Gateway wird das erstellte Zertifikat nicht direkt an den Benutzer gesendet, sondern auf der Festplatte des Gateway-Rechners gespeichert. Der Benutzer erhält dann eine E-Mail, die einen Link auf die Zertifikatsdatei enthält.

Token Manager (TM)

Der Token Manager verwaltet Hardwarelösungen zur Speicherung von Schlüsseln. Informationen können in [Balt00tm] gefunden werden. Dazu werden DLLs (Dynamic Link Libraries – Funktionsbibliotheken in kompilierter Form) verwendet, die der Hersteller der Hardwarelösung mitgeliefert haben muss.

Die Schnittstelle zwischen dem Token Manager und der DLL muss dem PKCS#11 Standard entsprechen, damit er vom Token Manager unterstützt werden kann. In der Version 3.1 des Token Managers werden folgende Hardwarelösungen unterstützt: HSP4000 von Baltimore, LunaCA, Luna2 und LunaCA3 von Chrysalis, Datakey 310 und 320, GemPKCSv2 Smartcards von Gemplus und nCipher nForce. Wie bereits im Abschnitt über die Certification Authority (CA) erwähnt, erlaubt die CA den Einsatz von RACAL77; diese Hardwarelösung wird jedoch nicht vom Token Manager unterstützt.

Die Einrichtung der Hardwarelösungen in den einzelnen Komponenten der UniCERT-PKI erfolgt über den Token Manager. Baltimore verwendet den Begriff Token als eine logische Sicht auf eine kryptografische Hardware- oder Software-Speichermöglichkeit für Schlüssel. Daher werden vom Token Manager hauptsächlich Kopierfunktionen zwischen den Dateien, welche Schlüssel enthalten, und den Speichermöglichkeiten auf Hardwarebasis zur Verfügung gestellt.

3.3 SPKI/SDSI

SPKI (Simple Public Key Infrastructure) und SDSI (Simple Distributed Security Infrastructure) werden zum Zeitpunkt der Erstellung der Arbeit noch entwickelt. An der Entwicklung von SPKI ist im Wesentlichen Carl Ellison beteiligt. Die SDSI Entwicklung wird von Ronald L. Rivest geleitet.

Das Konzept der Authentifizierung, das hinter SPKI/SDSI steht, wird bereits in einigen Softwareprodukten verwendet. Dazu gehören E-Speak von HP und CDSA (Common Data Security Architecture) von Intel.

Der Großteil der folgenden Zusammenfassung über SPKI und SDSI wurde aus [Elie98] und [Mayw00] entnommen. Im ersten Abschnitt wird der Weg zur Kombination SPKI/SDSI, die in der Version 2.0 vorliegt, dargestellt und im darauffolgenden Abschnitt wird das Format der Zertifikate in SPKI/SDSI vorgestellt.

3.3.1 Versionsübersicht

SPKI

Die stärkste Motivation für die Entwicklung von SPKI war, die Spezifikation von X.509 durch ein einfacheres Modell zu ersetzen. Vor allen Dingen sollte der globale Namensraum durch eine einfachere Struktur ersetzt werden. Ein Problem des globalen Namensraums stellt das Finden von einheitlichen Namen dar. Selbst wenn eine hierarchische Struktur vorliegt und daher z.B. jedes Unternehmen selbst für das Finden einheitlicher Namen verantwortlich ist, ist es schwierig, für mehrere Personen, die den selben Namen haben, einheitliche Namen zu finden.

Ein weiteres Problem des globalen Namensraums stellt die Schwierigkeit bei Namensänderungen dar. In PKIs muss bei einer Namensänderung ein neues Zertifikat ausgestellt werden und das alte für ungültig erklärt werden.

SPKI setzt die Idee um, nicht Namen an einen Schlüssel zu binden, sondern Berechtigungen für bestimmte Aktionen auf Objekte einem Schlüssel zuzuordnen. Wie in klassischen PKIs kann als Zusatzfunktion trotzdem ein Name an einen Schlüssel gebunden werden.

SDSI

1996 stellten Ronald L. Rivest und Butler Lampson die erste Version von SDSI vor [RiLa96a]. Sie entwickelten unabhängig von der SPKI-Entwicklung von Ellison eine Infrastruktur, die ebenso Namen an den öffentlichen Schlüssel gebunden hat.

Schon einen Monat später wurden Teile von SPKI in die SDSI-Spezifikation aufgenommen, die dann die Version 1.1 darstellte [RiLa96b]. Eine wesentliche Verbesserung stellte die Definition lokaler Namensräume dar, die jeweils relativ zu einem bestimmten öffentlichen Schlüssel definiert werden. Diese können dann wieder von diesem Schlüssel entbunden oder einem anderen SDSI-Namen zugewiesen werden.

Ein SDSI-Name ist eine Sequenz aus einem öffentlichen Schlüssel und keinem bis mehreren darauffolgenden Bezeichnern. Daher ist auch jeder Schlüssel automatisch ein SDSI-Name.

SPKI/SDSI 2.0

Die beiden Entwicklungen werden inzwischen gemeinsam unter dem Namen SPKI/SDSI weitergeführt. Die zum Zeitpunkt der Arbeit aktuelle Version 2.0 soll im Gegensatz zu klassischen PKIs noch einfacher sein. Dazu werden die in SDSI eingeführte Namensgebung und die Möglichkeit der Delegation von Berechtigungen aus SPKI vereinigt.

3.3.2 Zertifikate in SPKI/SDSI 2.0

In SPKI/SDSI gibt es zwei Arten von Zertifikaten: Namenszertifikate und Berechtigungszertifikate. Namenszertifikate binden einen Namen an einen Schlüssel, wohingegen Berechtigungszertifikate einem Schlüssel die Befugnis für eine bestimmte Ressource zuordnen. Für beide Arten gibt es in SPKI/SDSI jeweils ein eigenes Format, um die Delegation von Berechtigungen besser darstellen zu können.

In SPKI/SDSI ist es ferner möglich, Gruppen von Bezeichnern in einem Namensraum zu bilden. Gruppen bieten eine komfortable Möglichkeit, auf eine Menge von Personen zu verweisen, anstatt sich auf jede einzelne Person zu beziehen.

In der folgenden Abbildung ist ein Beispiel für ein Namenszertifikat dargestellt:

```
(cert
  (issuer
    (name
      (public-key
         (rsa-pkcs1-md5
           (e #25#)
           (n
             |ANHJgjhgKhgkUZgkucvhcZTfuzGjvHigchg
             vckgVkhv  ...  hgH|)))
     Alice))
  (subject
    (name
      (public-key
         (rsa-pkcs1-md5
           (e #25#)
           (n
             |zgvzuTwyDPpiMNnbmKrCztrCztrCZrxreaw
             QwewvdVh  ...  Pun|)))
     Bob))
  (not-before ``2002-01-31_12:00:00´´)
)
```

Abbildung 3.11: Beispiel für ein Namenszertifikat in SPKI/SDSI

Die Syntax, der das Zertifikatsformat folgt, wird S-Expression genannt. Es handelt sich um eine Lisp-Notation, die es auch Menschen ermöglicht, das Zertifikat als Quelltext zu lesen.

Ein SPKI/SDSI-Zertifikat besteht aus den drei Elementen Issuer, Subject und der optionalen Gütligkeitsdauer. Der public-key Eintrag enthält außer dem öffentlichen Schlüssel Informationen über die verwendeten Algorithmen (in diesem Fall rsa-pkcs#1-md5: RSA als asymmetrischer Algorithmus, PKCS#1 für das Verschlüsselungsformat und MD5 als Hash-Funktion) und die Zahl des verwendeten Exponenten des Schlüssels in hexadezimaler Form (hier 25h, entspricht 37).

In SPKI/SDSI kann jede Entität, die ein Schlüsselpaar besitzt, Zertifikate generieren und auf diese Weise Berechtigungen, die sie inne hat, an andere weitergeben. Ein Problem besteht nun darin, auf eine Befugnisanfrage eines Servers mit der korrekten Zertifikatskette zu antworten. Das Problem kann etwas gemildert werden, indem einem Berechtigungszertifikat die Weitergabe der Berechtigung (Delegation) nicht gestattet wird. Dazu wurde ein Flag eingeführt, das anzeigt, ob eine Delegation ausgeschlossen ist oder nicht (in diesem Fall kann die max. Anzahl der Delegationen festgelegt werden).

Auf dem Server werden so genannte Access Control Lists (ACL) verwaltet, in denen gespeichert wird, mit welchen Tags, welche Aktionen durchgeführt werden können. Ein Beispiel für ein solches Tag ist aus der folgenden Abbildung ersichtlich:

```
(tag
  (telnet
    rupert.informatik.uni-stuttgart.de
    23
    |HghuzgBtzfFfffghfCFgftRfGHFGHf ... |))
```

Abbildung 3.12: Beispiel für ein Tag in SPKI/SDSI

In diesem Beispiel wird einem Schlüssel die Berechtigung erteilt, per Telnet auf den angegebenen Rechner über den Port 23 zuzugreifen. Das dazugehörige SPKI/SDSI-Zertifikat kann vom Zertifikatsersteller an die berechtigten Personen ausgegeben werden. In diesem Fall ist der angegebene Schlüssel der Bezeichner im lokalen Namensraum, der dem Zertifikatsersteller untersteht.

Kapitel 4 Analyse

In diesem Kapitel werden die drei vorgestellten Sicherheitsarchitekturen auf die Erfüllung der aufgestellten Anforderungen untersucht. Sollte eine Anforderung nicht oder nur teilweise erfüllt werden, wird versucht, eine Verbesserung vorzuschlagen.

Zunächst wird im ersten Abschnitt erläutert, inwieweit PGP die Anforderungen erfüllt. Im darauffolgenden Abschnitt wird die PKI der Baltimore Technologies Inc auf die Erfüllung der Anforderungen überprüft. Die als theoretische Lösung vorliegende SPKI/SDSI wird im letzten Abschnitt bearbeitet.

Die Anforderungen an die Interoperabilität von Sicherheitsarchitekturen werden im nächsten Kapitel separat behandelt und daher in den folgenden Abschnitten nicht aufgeführt.

4.1 Analyse von PGP Desktop Security

In diesem Abschnitt wird geprüft, inwieweit die Anforderungen aus dem 2. Kapitel von PGP Desktop Security erfüllt werden. Obwohl PGP ursprünglich für den Schutz von E-Mails konzipiert wurde, können auch Anforderungen, die nicht den E-Mail-Austausch betreffen, erfüllt werden. Dazu werden in Einzelfällen jedoch zusätzliche Komponenten von Network Associates benötigt und an den jeweiligen Stellen erwähnt. Nicht betrachtet werden in diesem Abschnitt Anforderungen, die im Zusammenhang mit Geld im Internet aufgestellt wurden.

4.1.1 E-Mail-Austausch

Im Folgenden wird untersucht, wie die Anforderungen, die für E-Mail Sicherheitsarchitekturen aufgestellt wurden, von PGP Desktop Security erfüllt werden.

Geheimhaltung

Die Erfüllung der Geheimhaltung im E-Mail-Verkehr war bei der Entwicklung von PGP das oberste Ziel. In PGP werden Kryptoalgorithmen verwendet, die allgemein zugänglich und daher von der Öffentlichkeit auf Lücken überprüft worden sind. Wird eine Sicherheitslücke bekannt, wird versucht, den entsprechenden Algorithmus möglichst schnell durch einen besseren zu ersetzen.

In [NAI00c] werden Angriffspunkte auf die Geheimhaltung genannt. Diese werden im Folgenden beschrieben und dazu jeweils die Maßnahmen erläutert, die in PGP Desktop Security vorgesehen sind, um sie zu schließen oder zu minimieren:

- **Entwenden des geheimen Schlüssels**: Der geheime Schlüssel ist in einer Personal Security Environment (PSE) gespeichert. Dies kann eine Datei auf der Festplatte oder einer Diskette sein. Wird der geheime Schlüssel auf der Festplatte gespeichert, besteht die Gefahr, dass jemand darauf Zugriff erhält (z.B. in einer Multiuser-Umgebung oder durch Trojanische Pferde). Bei der Speicherung auf einer Diskette besteht die Gefahr, dass diese gestohlen wird. Um zu verhindern, dass ein entwendeter geheimer Schlüssel verwendet werden kann, muss vom Benutzer eine Passphrase eingegeben werden. Nur mit der Passphrase ist eine Benutzung möglich.

  Der Administrator kann im Modul PGPadmin für die Passphrase eine Mindestlänge vorgeben, die die Benutzer von PGP Desktop Security bei Erstellung oder Änderung der Passphrase einhalten müssen. Ferner kann die Qualität der Passphrase vorgegeben werden. Die Qualität der Passphrase ist höher, wenn eine Mischung aus Groß- und Kleinbuchstaben, Ziffern und Satzzeichen verwendet wird. Die Mindestqualität kann vom Administrator in Prozent angegeben werden. (Siehe Seite 46f aus [NAI00a]).

- **Ausspähen der unverschlüsselten Daten**: Während die Daten vom Benutzer bearbeitet oder gelesen werden, sind sie unverschlüsselt. Es gibt mehrere Angriffspunkte, um an diese unverschlüsselten Daten zu gelangen:

  - **Abfangen kompromittierender Strahlung**: Computermonitore strahlen elektromagnetische Wellen aus, die in einem gewissen Radius mit Spezialgeräten empfangen werden können. So ist es möglich, den Bildschirminhalt eines Monitors abzufangen und unverschlüsselte Daten mitzulesen.

    PGP Desktop Security bietet dem Benutzer die Möglichkeit Nachrichten in einer speziellen Schriftart darzustellen. Sie soll die elektromagnetische Abstrahlung verringern und so ein Abfangen erschweren machen. (Siehe Seite 62f aus [NAI00c]).

  - **Zugriff auf den Arbeitsspeicher oder das Swap-File**: Bei der Bearbeitung von Daten werden diese im Arbeitsspeicher abgelegt. Über spezielle Programme wäre es einem Angreifer möglich, Zugriff auf den Arbeitsspeicher zu erlangen und die Daten daraus zu extrahieren. Dazu kann der Angreifer ein Trojanisches Pferd einsetzen oder in einer Multiuser-Umgebung versuchen, auf den Arbeitsspeicher zuzugreifen. Im Swap-File werden nicht benötigte Teile des Arbeitsspeichers temporär auf die Festplatte ausgelagert. Dies stellt einen weiteren Angriffspunkt dar.

    Die Zeiten, in denen sich unverschlüsselte Daten innerhalb von PGP im Arbeitsspeicher befinden, wurden weitgehend minimiert. So soll verhindert werden, dass gerade unverschlüsselte Daten vom Betriebssystem in das Swap-File ausgelagert werden. Damit ist diese Schwachstelle jedoch nicht vollständig beseitigt. In [NAI00c] werden noch weitere Maßnahmen empfohlen, falls befürchtet wird, jemand könnte die Schwachstelle ausnützen. (Siehe Seite 61f aus [NAI00c]).

- **Unverschlüsselte Weiterverarbeitung**: Als Weiterverarbeitung wird hier das Drucken einer E-Mail oder das unverschlüsselte Weiterleiten an andere Empfänger bezeichnet. Nach dem Ausdrucken könnten die Daten in Papierform in falsche Hände geraten.

  Das Ausdrucken oder die unverschlüsselte Weiterleitung an Dritte kann von PGP nicht ausgeschlossen werden. Dies liegt im Verantwortungsbereich des Benutzers. Um diese Aktionen verhindern zu können müssten von PGP im Mailprogramm grundlegende Funktionen deaktiviert werden. Dazu gehören die Druck- und Weiterleitungsfunktion, aber auch Funktionen, die es ermöglichen würden, einen Text über die Zwischenablage weiterzuverarbeiten oder den Text in eine Datei zu speichern. Dies würde jedoch den Funktionsumfang enorm einschränken und von den Benutzern wohl nicht akzeptiert werden. Es bleibt daher nur, das Verantwortungsbewusstsein der Benutzer durch entsprechende Anleitung zu erhöhen.

- **Hardware-Angriffe**: Darunter fallen alle direkten Eingriffe in das Computersystem des Benutzers. Beispiele könnten das Aufzeichnen des Monitorbildes oder die Eingaben über Tastatur sein. Beim Aufzeichnen des Monitorbildes kann von einem Angreifer der unverschlüsselte Text gelesen werden. Es ist zudem möglich, die Passphrase im Klartext zu sehen, wenn die entsprechende Option vom Benutzer gesetzt wurde. Die Passphrase kann auch beim Aufzeichnen der Tastatureingaben extrahiert werden.

  Da Angriffe, die Veränderungen an der Hardware bedeuten, nicht in den Kontrollbereich von PGP fallen, können keine Maßnahmen dagegen getroffen werden.

- **Temporäre Dateien der Anwendungen**: Bei der Erstellung oder Bearbeitung der zu verschlüsselnden Daten werden Programme verwendet, die u.U. temporäre Dateien anlegen, wie zum Beispiel Microsoft Word. Eine temporäre Datei wird nach der Bearbeitung der Daten normalerweise gelöscht, jedoch ist es in der Regel möglich, diese gelöschte Datei wiederherzustellen.

  PGP Desktop Security bietet eine Funktion, die den entsprechenden Speicherbereich der temporären Datei auf der Festplatte mehrmals mit verschiedenen Bitmustern überschreibt, um so eine Wiederherstellung unmöglich zu machen. Diese Funktion muss jedoch vom Benutzer explizit aufgerufen werden und der Pfad der temporären Datei muss dem Benutzer bekannt sein. (Siehe Seite 59f aus [NAI00c]).

Im Zusammenhang mit dem Schutz der unverschlüsselten Daten lässt sich die sichere Verwahrung der Originaldatei nennen. Der Benutzer sollte eine Datei, die verschlüsselt versandt wurde, nicht unverschlüsselt auf seiner Festplatte speichern. PGP Desktop Security bietet dem Benutzer daher die Möglichkeit, Dateien oder auch ganze Verzeichnisse zu verschlüsseln. Zum Löschen von solchen Dateien sollte der Benutzer ferner die o.g. Löschfunktion verwenden, die keine Spuren hinterlässt.

Zusammenfassend lässt sich feststellen, dass PGP Angriffe auf die unverschlüsselt vorliegenden Daten teilweise nicht gut abwehren kann. Dies kann jedoch durch Schulungen der Benutzer, Hinweise des Administrators oder durch geeignete Dokumentation kompensiert werden.

- **Lücken in den verwendeten Algorithmen**: Es sind vier Angriffspunkte denkbar, an denen versucht werden kann, eine Lücke in den verwendeten Algorithmen zu finden:
  - **Verschlüsselungsalgorithmus für den geheimen Schlüssel**: Der geheime Schlüssel wird mit der vom Benutzer angegebenen Passphrase mit einem symmetrischen Verfahren verschlüsselt.
  - **Verschlüsselungsalgorithmus für die Nachricht**: Von PGP wird ein Zufallsschlüssel erstellt, mit dem die Nachricht verschlüsselt wird (Message Key). Der Message Key wird mit dem öffentlichen Schlüssel des Empfängers verschlüsselt.
  - **Verschlüsselungsalgorithmus für den Message Key**: Bei diesem Algorithmus handelt es sich um das asymmetrische Verfahren von PGP, mit dem der per Zufallsfunktion erzeugte Message Key verschlüsselt wird.
  - **Zufallsfunktion zur Generierung des Message Keys**: Wird eine schwache Zufallsfunktion verwendet, wäre es vorstellbar, dass ein Angreifer die von der Funktion erzeugte Zufallsfolge rekonstruieren kann und somit den verwendeten Message Key selbst erzeugen kann.

  Leider gibt es für die Sicherheit von Kryptoalgorithmen keine Garantie. Die von PGP verwendeten Algorithmen liegen jedoch der Öffentlichkeit als Quelltext vor und sind einer ständigen Kontrolle unterworfen. Sie gelten gemeinhin als sicher.

Durch die Einhaltung der empfohlenen Maßnahmen wird die Geheimhaltung gewährleistet. Auf Grund der Komprimierung der E-Mails durch PGP wird sogar noch ein weiterer Aspekt der Geheimhaltung erfüllt. Sollte jemand eine E-Mail abfangen, die mit PGP verschlüsselt ist, kann er die exakte Länge der ursprünglichen Daten nicht feststellen. Somit bleibt die tatsächliche Größe der übermittelten Daten geheim.

Integrität

Die Wahrung der Integrität wird von PGP erfüllt. Die Integrität einer E-Mail wird mittels des verwendeten Hash-Algorithmus und der anschließenden Verschlüsselung des Hash-Wertes mit dem geheimen Schlüssel des Absenders gewährleistet.

Auch für die Wahrung der Integrität ist es wichtig, dass die verwendeten Algorithmen nicht geknackt werden können. Der Hash-Algorithmus muss so konzipiert sein, dass zu einem gegebenen Hash-Wert keine weitere passende Nachricht gefunden werden kann.

Authentifizierung

Um E-Mails einer Person authentifizieren zu können, muss der entsprechende öffentliche Schlüssel vorliegen. Die Authentizität ist jedoch nur gewährleistet, wenn tatsächlich der zu dieser Person gehörende öffentliche Schlüssel vorliegt und nicht etwa ein Schlüssel, der von einer dritten Person unter falschem Namen generiert wurde.

Es liegt in der Verantwortung des Benutzers, die Authentizität des öffentlichen Schlüssels zu überprüfen. Dazu kann der Besitzer des öffentlichen Schlüssels direkt kontaktiert werden, oder im Zertifizierungspfad wird überprüft, ob eine vertrauenswürdige Person den Schlüssel signiert hat.

Ob die Anforderung der Authentifizierung erfüllt wird, hängt also vom Verhalten des Benutzers ab. Es steht dem Benutzer frei, jeden beliebigen öffentlichen Schlüssel für gültig und vertrauenswürdig zu erklären. Damit wäre es einem Angreifer möglich den Benutzer dazu zu bringen ein selbst erstelltes, gefälschtes Zertifikat zu verwenden.

In PGP Desktop Security kann vom Administrator die Option vorgegeben werden, dass Benutzer die Schlüssel nicht signieren dürfen und damit selbst Schlüssel nicht für gültig erklären können (siehe [NAI00a], S. 59). Schlüssel wären somit nur von eigenen oder vertrauenswürdigen CAs oder Personen gültig. Herrscht jedoch hoher Mailverkehr mit vielen verschiedenen Personen, die nicht einer der vertrauenswürdigen CAs oder der eigenen CA unterstehen, kann der Benutzer diese Schlüssel nicht für gültig erklären. Das folgende Bild soll diese Situation verdeutlichen:

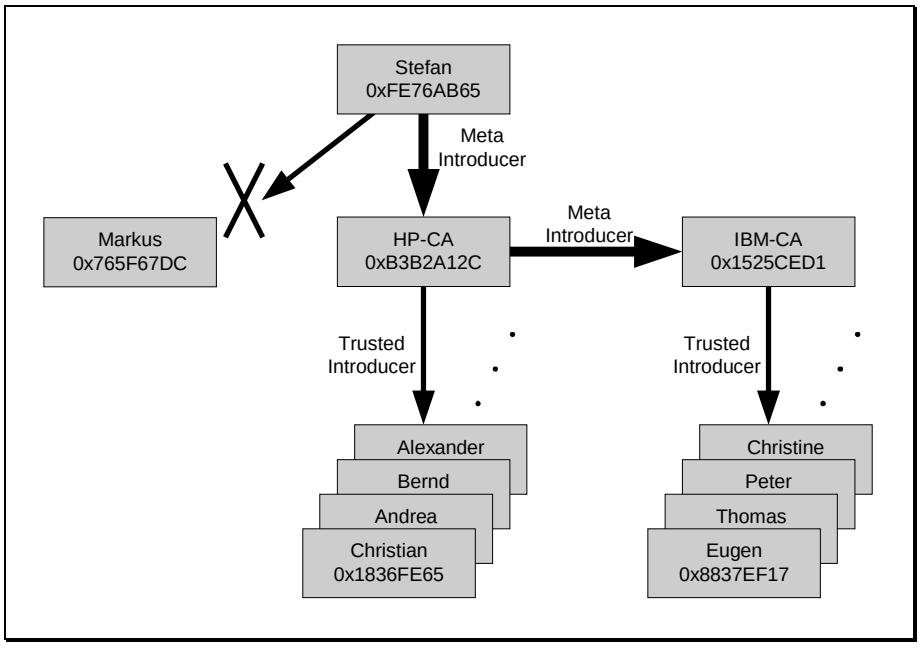


Abbildung 4.1: Vertrauen gegenüber anderen Unternehmen in PGP Desktop Security

In diesem Beispiel ist Stefan Mitarbeiter von HP. Das Zertifikat der HP-CA wird automatisch als Meta Introducer Zertifikat bei der Installation von PGP eingerichtet. Damit sind alle anderen Mitarbeiter von HP bereits als vertrauenswürdig eingestellt. Da im Beispiel die Mitarbei-

ter von HP mit den Mitarbeitern von IBM kommunizieren, wurde die IBM-CA von der HP-CA zertifiziert. Damit sind die Mitarbeiter von IBM ebenfalls als vertrauenswürdig eingestuft. Will nun Stefan jedoch mit einem Kunden (im Bild Markus) kommunizieren, kann er dieses Zertifikat nicht selbst als vertrauenswürdig einstufen.

Es wäre vorstellbar, dass er dazu die HP-CA beauftragen muss, um die Authentizität von Markus' öffentlichen Schlüssel zu überprüfen und diesen als vertrauenswürdig einzustellen. Diese Vorgehensweise würde zwar einen höheren Aufwand für die HP-CA bedeuten, sie stellt jedoch sicher, dass externe öffentliche Schlüssel durch ein geschultes Personal auf Authentizität geprüft werden.

Sinnvoll wäre es in diesem Fall zu prüfen, ob der Kunde (wie im Beispiel Markus) nicht bereits von einer CA zertifiziert wurde und diese ggf. anstatt des Kunden zu zertifizieren. Dadurch werden in einem Arbeitsgang größere Personengruppen zertifiziert.

Unleugbarkeit

Die Anforderung nach Unleugbarkeit kann von PGP nur teilweise erfüllt werden. Zwar kann eine Transaktion, die mit einem privaten Schlüssel signiert wurde nur von dessen Besitzer signiert worden sein. Es ist jedoch nicht auszuschließen, dass der private Schlüssel entwendet wurde. Dies kann geschehen, ohne dass es der Benutzer bemerkt. Daher wird der Schlüssel nicht für ungültig erklärt.

Auch wenn der private Schlüssel nicht entwendet wurde, könnte von einem Benutzer, der nicht mehr zu seiner Transaktion steht, die Transaktion mit der Begründung eines entwendeten Schlüssels geleugnet werden.

Es ist ferner möglich, dass von PGP etwas signiert wird, das der Benutzer nie gesehen hat. Dies wird durch die Funktion des Passphrase-Cache möglich, die nach der Eingabe der Passphrase diese innerhalb eines bestimmten Zeitraums speichert und ggf. wiederverwendet. Vergisst ein Benutzer zum Beispiel seinen Rechner zu sperren, wenn er diesen verlässt, könnte ein Angreifer die gespeicherte Passphrase verwenden. Daher sollte diese Funktion vom Administrator in der Sicherheitspolicy deaktiviert werden.

Verfügbarkeit

PGP Desktop Security bietet keine speziellen Funktionen um die Verfügbarkeit zu erhöhen. Die zusätzliche Komponente PGP Keyserver ist jedoch so ausgelegt, dass Backup-Server im Netzwerk aufgebaut werden können. Durch diese Redundanz wird die Verfügbarkeit der Keyserver erhöht.

Die Replikation der Keyserver ist für den Benutzer jedoch nicht transparent. Sollte ein Keyserver ausfallen, muss vom Benutzer explizit ein anderer gewählt werden. Es ist jedoch möglich, die Adressen aller Keyserver in die Konfiguration aufzunehmen. Der zu verwendende Keyserver kann dann aus einer Liste ausgewählt werden.

Um die Verfügbarkeit der anderen Komponenten einer PGP-Infrastruktur zu erhöhen, können lediglich Mittel eingesetzt werden, um diese gegen Ausfälle zu schützen. Ein solches Mittel

ist der Einsatz von Firewalls, um die Gefahr von Ausfällen durch Eingriffe Dritter zu minimieren.

Sichere Verwahrung der Schlüssel

Geheime Schlüssel werden bei PGP in einer Datei gespeichert, die mit der Passphrase verschlüsselt wurde. Für jeden Schlüssel wird eine eigene Datei angelegt, die jeweils eine eigene Passphrase besitzt. Es sind bereits Sicherheitslücken bekannt geworden, durch die ein Umgehen der Passphrase möglich ist. Diese wurden von Network Associates durch Patches behoben. Dies zeigt, dass die Schlüsseldateien zusätzlich geschützt werden sollten.

Für einen zusätzlichen Schutz könnte das mitgelieferte Modul PGPdisk eingesetzt werden. Dazu richtet man ein geschütztes Verzeichnis an, in das die Schlüsseldateien abgelegt werden.

Verlässliche Identitätsprüfung

Ein wichtiger Aspekt von PGP ist sein dezentraler Ansatz. Die Benutzer können selbst Zertifikate erstellen. Damit ist jedoch eine verlässliche Identitätsprüfung nicht immer gegeben. In einem Unternehmen könnte der dezentrale Ansatz aufgegeben werden und Schlüsselgenerierung und –zertifizierung nur durch eine zentrale Stelle durchgeführt werden.

Fehlerfreiheit der Implementierung

Zum Zeitpunkt der Erstellung dieser Arbeit ist der Quelltext der untersuchten Version 7.0.3 nicht verfügbar. Daher entzieht sich diese Version der Kontrolle der Öffentlichkeit. Network Associates bietet Zugriff auf den Quelltext der Version 6.5.8 über das Internet.

Selbst wenn der Quelltext von der Öffentlichkeit überprüft wird, kann nicht sicher davon ausgegangen werden, dass keine Fehler in der Implementierung vorhanden sind.

Unterstützte Zertifikatsformate / Zertifikats-Austauschformate

Zertifikate werden im eigenen PGP-Format verarbeitet. PGP Desktop Security kann darüber hinaus Zertifikate der X.509v3-Spezifikation verarbeiten. Erstellt werden können jedoch nur PGP-Zertifikate. In das Schlüsselverzeichnis können sowohl PGP- als auch X.509v3-Zertifikate aufgenommen werden.

Unterstützte Nachrichten-Austauschformate

Mit PGP verschlüsselte oder signierte E-Mails werden als ASCII-Text versendet. Innerhalb dieses ASCII-Textes wird der von PGP bearbeitete Abschnitt durch PGP-eigene Kopf- und Fußzeilen begrenzt. Ein Beispiel für die Kopf- und Fußzeilen ist aus Abbildung 4.2 im Abschnitt über transparente Prüfung ersichtlich.

Verbreitung des Protokolls

Da PGP auch in einer freien Version zur Verfügung steht, ist die Verbreitung relativ hoch. Leider sind keine offiziellen Untersuchungen über die Verbreitung von PGP erhältlich, somit ist dies eine subjektive Aussage.

Integration in das Mail-Programm

PGP Desktop Security unterstützt u.a. die folgenden Mail-Programme unter Verwendung von Plugins:

- Microsoft Outlook 97/98/2000
- Microsoft Outlook Express 4.x and 5.x
- Lotus Notes 4.5.x, 4.6.x and 5.0
- Qualcomm Eudora 4.x and 5.0

Vom Administrator kann über das Optionenprofil festgelegt werden, welche der Plugins bei einer Installation tatsächlich zur Verfügung stehen sollen.

Andere Mail-Programme, wie zum Beispiel Netscape Messenger, können über Plugins von Drittherstellern erweitert werden.

Die für die Verwendung von PGP benötigten Funktionen werden als Menüpunkte und als Symbole in der Symbolleiste des Mail-Programms eingefügt. Zu diesen Funktionen gehören das Verschlüsseln, das Entschlüsseln, das Signieren, das Prüfen von Signaturen und die Schlüsselverwaltung.

Wird ein Mail-Programm verwendet, das nicht zu den unterstützten Mail-Programmen gehört, muss über die Zwischenablage mit PGP gearbeitet werden. Dies stellt jedoch keine komfortable Lösung dar.

Transparente Prüfung

Mit den Standardeinstellungen werden eingegangene E-Mails mit dem PGP-Quelltext angezeigt. Bei verschlüsselten E-Mails sind daher nur kryptische Zeichen zu erkennen und bei signierten E-Mails ist nicht bekannt, ob die Signatur gültig ist. Dies soll das folgende Bild darstellen. Erst der explizite Aufruf der PGP-Funktion „decrypt/verify“ entschlüsselt die E-Mail und prüft die Signatur auf Gültigkeit.

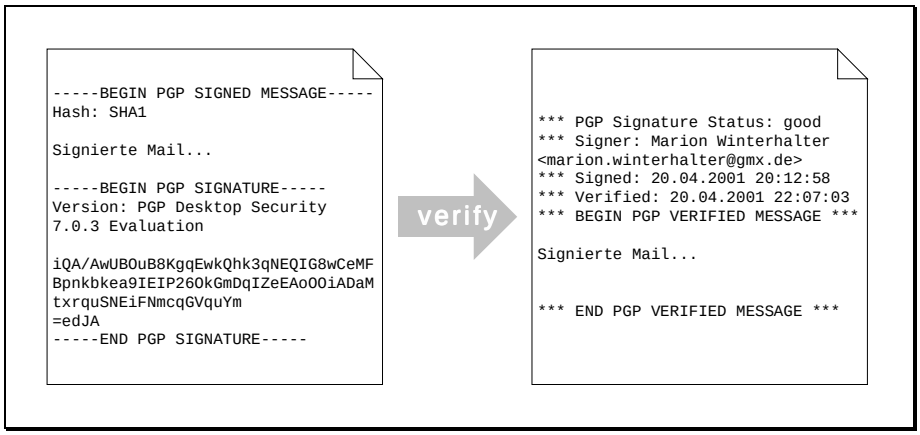


Abbildung 4.2: Darstellung signierter E-Mails in PGP

Mit dieser Standardeinstellung ist eine transparente Bedienung nicht gegeben. Abhilfe schafft das Aktivieren der E-Mail-Option „Automatically decrypt/verify when opening messages“. Damit werden die Entschlüsselung und Überprüfung automatisch durchgeführt.

Durchsetzen einer Sicherheitspolicy

In einem Unternehmen ist es sinnvoll, eine Sicherheitspolicy einzusetzen. Im mitgelieferten Programm PGPadmin kann der Administrator Einstellungen vorgeben, die bei der Installation von PGP Desktop Security bei den Benutzern entsprechend gesetzt werden.

Wurden nach der Installation der Software Änderungen an den Voreinstellungen durchgeführt, so werden diese über den unternehmenseigenen Keyserver verbreitet. In den Optionen kann festgelegt werden, wie häufig nach geänderten Einstellungen auf dem Keyserver nachgesehen werden soll.

Einfache Zertifikatsverwaltung

Zur Zertifikatsverwaltung kommt bei PGP die Schlüsselverwaltung (PGPkeys) zum Einsatz. Diese unterstützt außer den Verwaltungsfunktionen auch das Suchen nach Schlüsseln auf eingetragenen Keyservern.

Hat der Benutzer das grundsätzliche Konzept von PGP verstanden (Gültigkeit und Vertrauenswürdigkeit festlegen), ist die Bedienung der Schlüsselverwaltung intuitiv und wird durch eingängige Symbole unterstützt.

4.1.2 Internet- / Intranet-Anwendung

Im Folgenden wird untersucht, inwieweit die Anforderungen von Internet- und Intranet-Anwendungen an PGP Desktop Security erfüllt werden.

Geheimhaltung

Das Modul PGPnet bietet Virtual Private Network (VPN) Funktionalität. Es ist daher möglich, gesicherte Verbindungen über ein unsicheres Netzwerk aufzubauen. Diese Funktion ist nur verfügbar, wenn beide Kommunikationspartner PGPnet einsetzen.

Integrität

Wird PGPnet für eine gesicherte Verbindung zwischen zwei Rechnern verwendet, bleibt die Integrität gewahrt.

Verfügbarkeit

Mit PGP Desktop Security wird eine Personal Firewall installiert, die die Verfügbarkeit erhöhen kann. Durch das Setzen bestimmter Regeln, können Denial-of-Service Angriffe teilweise verhindert werden.

Authentifizierung

Bevor mittels PGPnet eine gesicherte Verbindung aufgenommen werden kann, müssen sich die beiden Kommunikationspartner gegenseitig mit ihren Schlüsseln authentifizieren. Dazu müssen als Vorbereitung die Schlüssel gegenseitig ausgetauscht und zertifiziert werden.

Schutz des Netzwerks

Die mit PGP Desktop Security gelieferte Firewall ist für den Betrieb als Desktop Firewall konzipiert. Daher ist sie für die Absicherung der einzelnen Rechner gedacht und nicht zur Absicherung eines gesamten Netzwerkes.

Die Absicherung einzelner Rechner ist über fünf vorgefertigte Konfigurationsschablonen einfach einzustellen. Detaillierte Regeln können darüber hinaus ebenfalls eingestellt werden. Die gesamte Konfiguration ist über die Sicherheitspolicy vom Administrator voreinstellbar.

Erkennung von Eindringlingen

In der Personal Firewall von PGP können Regeln eingestellt werden, nach denen Netzwerkverkehr erlaubt oder verboten wird. Ferner kann festgelegt werden, bei welchen Regeln ein Eindringlings-Alarm ausgelöst werden soll.

Die Konfiguration des PGP Intrusion Detection Systems erlaubt das Versenden einer E-Mail an eine vorgegebene Adresse. Hier kann vom Administrator in der Sicherheitspolicy eine Adresse vorgegeben werden.

Einsatz von Virenscannern

Im Lieferumfang von PGP Desktop Security ist kein Virenscanner enthalten. Der Einsatz eines Virenscanners wird jedoch dringend empfohlen, da ansonsten zum Beispiel über ein Trojanisches Pferd Tastatureingaben aufgezeichnet und an einen Angreifer gesendet werden könnten.

Durchführen von Backups

Eine eigene Backup-Funktion ist in PGP Desktop Security nicht implementiert. Es wird jedoch zum Beispiel in der Schlüsselverwaltung eine Sicherung der Schlüssel in einer zusätzlichen Datei empfohlen. Dieses Verhalten der Schlüsselverwaltung muss jedoch in den Optionen aktiviert werden und könnte vom Administrator in der Sicherheitspolicy vorgegeben werden. Die Sicherung einer eingerichteten PGPdisk erweist sich ebenfalls als einfach, da diese in einer einzigen Datei untergebracht wird.

4.1.3 Eigenschaften der Architektur

In diesem Abschnitt werden die Anforderungen, die für die Architektur aufgestellt wurden, geprüft. Die Anforderungen werden im Zusammenhang mit den zusätzlich lieferbaren Komponenten von Network Associates betrachtet.

Skalierbarkeit

Die Skalierbarkeit muss für jede einzelne Komponente einer PGP-Architektur geprüft werden. In der folgenden Tabelle sind diese Komponenten aufgezählt und die Möglichkeit der Skalierbarkeit aufgezeigt.

PGP Desktop Security	Diese Software wird auf jedem Rechner im Netzwerk installiert und kommuniziert lediglich mit dem PGP Keyserver, um Schlüssel auszutauschen. Daher ist sie unabhängig von den jeweils anderen installierten Programmen und kann beliebig skaliert werden.

PGP Keyserver	PGP Keyserver können beliebig viele eingesetzt werden. Dazu werden in [PGPKSAdmin] zwei mögliche Konfigurationen vorgestellt, die jedoch beide auf einem Master-/Slave-Konzept basieren. Die Daten werden zwischen Master und Slave periodisch repliziert. Ein Schwachpunkt dieses Ansatzes ist der Master-Server. Fällt dieser aus, werden keine Daten mehr zwischen den Slave-Servern repliziert.
PGP Net Tools PKI	Der Aufbau einer weiteren CA ist weitgehend unabhängig von bereits bestehenden CAs, daher stellt bei PGP Net Tools PKI die Skalierbarkeit kein Problem dar.

Tabelle 4.1: Skalierbarkeit der Komponenten einer PGP-PKI

Verfügbarkeit

Die Verfügbarkeit ist lediglich für die Komponenten zu untersuchen, die nicht direkt beim Benutzer auf dem Rechner installiert sind. Zu diesen Komponenten gehören der PGP Keyserver und mit PGP Net Tools PKI aufgebaute CAs.

Die PGP Keyserver können über die Sicherheitspolicy vom Administrator bei den Benutzern eingestellt werden. Sollte ein Keyserver ausfallen, wird von den Benutzern der nächste Keyserver in der Liste kontaktiert. Diese Lösung arbeitet zwar nicht transparent, bietet trotzdem eine Erhöhung der Verfügbarkeit.

Bei einer CA wiegt ein Ausfall meist schwerer. Wurde in einem Unternehmen für jede Abteilung eine eigene CA aufgebaut und eine fällt aus, ist es in der Regel nicht vorgesehen, dass Mitarbeiter Zertifikate bei CAs anderer Abteilungen erhalten können.

Sehr problematisch ist zudem der Ausfall des Servers, der die CRL verwaltet. Wenn nicht geprüft werden kann, ob ein Zertifikat ungültig ist, kann es missbräuchlich verwendet werden. Bis die Ungültigkeit eines Zertifikats festgestellt werden kann, entsteht unter Umständen ein sehr hoher Schaden.

4.1.4 E-Commerce-Anwendungen

In diesem Abschnitt wird geprüft, ob PGP für E-Commerce Anwendungen geeignet ist. Es wird gezeigt, inwieweit PGP die Anforderungen an eine gesicherte Kommunikation erfüllt, die Überprüfung von Identitäten unterstützt, die Sicherheit der Komponenten gewährleistet und die Anforderungen zum Schutz der Endbenutzer erfüllt.

Gesicherte Kommunikation

Eine gesicherte Kommunikation, wie sie in Abschnitt 2.4.3 gefordert wurde, kann von PGP nur teilweise erfüllt werden. So ist in PGP nicht vorgesehen, doppelte Nachrichten zu erkennen. Damit diese Anforderung erfüllt wird, können von der E-Commerce-Anwendung zum

Beispiel Sequenznummern in die Nachrichten eingefügt werden. Daran wäre eine erneute Übermittlung einer bereits verarbeiteten Nachricht zu erkennen.

Die Anforderungen nach Geheimhaltung und Aufdeckung von Manipulationen werden, wie bereits in den vorangegangenen Abschnitten beschrieben, je nach Anwendung (E-Mail-Kommunikation oder Internet-/Intranet-Verbindung) erfüllt.

Überprüfung von Identitäten

Da PGP lediglich die E-Mail-Adresse und den Namen in seinen Zertifikaten erfasst, können nur diese Informationen überprüft werden.

Es wäre denkbar, dass ein Händler eigene PGP-Zertifikate an seine Kunden vergibt. Diesen Zertifikaten wird der Händler entsprechendes Vertrauen entgegenbringen. Auch die Beauftragung einer externen Stelle mit dieser Aufgabe ist denkbar. So könnten sich mehrere Händler zusammenschließen, um einer solche PGP-CA zu vertrauen. Es stellt sich jedoch die Frage, ob Kunden diesen Aufwand auf sich nehmen würden. Vor allem im B2C-Bereich, in dem viele Kunden noch keine Geschäftsbeziehung mit dem Händler haben, wird sich solch eine Verfahrensweise nicht durchsetzen können.

Ferner können keine zusätzlichen Angaben in PGP-Zertifikate gespeichert werden. Ein Kunde könnte – selbst wenn er sich gegenüber dem Händler erfolgreich authentifiziert hat – falsche Angaben (wie zum Beispiel einer falschen Bankverbindung für Lastschriften) machen.

Sicherheit der Komponenten

Alle Komponenten von Network Associates beinhalten eine Personal Firewall, die über Regeln den Netzwerkverkehr überwacht. Bei der richtigen Wahl der Regeln können Angriffe gegen Rechner, auf denen einzelne Komponenten laufen, minimiert werden.

Die Kommunikation zwischen den Komponenten kann über PGPnet in verschlüsselter Form ablaufen und so ein Abhören oder Verändern verhindern.

Schutz des Endbenutzers

Die Anforderung nach einer einfachen Bedienung kann bei entsprechender Einstellung der Sicherheitspolicy und Verwendung eines unterstützten Mail-Clients erfüllt werden. Trotzdem muss der Benutzer in die Verwendung von PGP eingewiesen werden, da nicht jede Fehlbedienung der Benutzer abgefangen werden kann.

Die Unleugbarkeit, die Unfälschbarkeit der Transaktionen (Integrität), die Fehlertoleranz, das Verhindern ungewollter Transaktionen, die Integrität von Transaktionen und das Verhindern irreführender Meldungen werden im beschriebenem Rahmen erfüllt.

Die Anforderung nach Anonymität des Benutzers kann nur unter Angabe eines falschen Namens im Zertifikat erfüllt werden. Die Angabe einer E-Mail-Adresse ist optional.

4.2 Analyse der Baltimore PKI

In diesem Abschnitt wird geprüft, inwieweit die Anforderungen von der UniCERT PKI der Baltimore Technologies erfüllt werden können. Für die Analyse wurde angenommen, dass die Benutzer mit einem Windows Betriebssystem arbeiten, auf dem Internet Explorer und Outlook Express (mindestens Version 4) oder Outlook installiert sind.

Auch Netscape Messenger unterstützt die Verwaltung von Zertifikaten, diese werden jedoch von Netscape selbst verwaltet. In diesem Abschnitt wird jedoch nicht auf Netscape Messenger eingegangen.

4.2.1 E-Mail-Austausch

Die Anforderungen, die den E-Mail-Austausch betreffen, werden von der Baltimore PKI nicht direkt erfüllt. Es wird vielmehr die Funktionalität der Mail-Clients ausgenutzt, die über das S/MIME-Protokoll verschlüsselte Nachrichten verschicken.

Geheimhaltung

Die in [NAI00c] genannten Angriffspunkte auf die Geheimhaltung sollten von S/MIME ebenfalls berücksichtigt werden. Die Sicherung gegen diese Angriffspunkte werden im Folgenden erläutert.

- **Entwenden des geheimen Schlüssels**: Zertifikate werden in einem zentralen Zertifikatsspeicher unter Windows verwaltet. Die Zertifikate, die in dieser Zertifikatsverwaltung enthalten sind, werden verschlüsselt in der zentralen Windows-Datenbank (Registry) gespeichert. Da für den Zugriff auf die Registry besondere Zugriffsmechanismen notwendig sind und die Daten verschlüsselt gespeichert sind, wird das Entwenden von geheimen Schlüsseln erschwert. Manche Programme (zum Beispiel Netscape Messenger) verwenden jedoch eigene Zertifikatsspeicher. Daher kann für diese keine Aussage über die Sicherheit getroffen werden.

- **Ausspähen der unverschlüsselten Daten**: Die fünf Angriffspunkte, die im Abschnitt 4.1 zum Schutz unverschlüsselter Daten unter PGP genannt wurden, werden von der Baltimore PKI nicht erfüllt. Es bleibt dem Benutzer nur die Möglichkeit, Produkte von Drittherstellern zu verwenden. Außerdem werden von der Baltimore UniCERT-PKI Smartcard-Terminals unterstützt, die eine erhöhte Sicherheit bieten. Bei einer Signierung beispielweise werden die Daten an dieses Terminal geleitet und werden in der Smartcard selbst signiert. Wird die Smartcard aus dem Terminal entfernt, ist eine Signierung nicht möglich. Ferner kann vom Benutzer Hardware eingesetzt werden, die für eine schwache Abstrahlung elektronmagnetischer Wellen bekannt ist. Eine Liste mit abstrahlsicherer Hardware führt das Bundesamt für Sicherheit in der Informationstechnik in [BSI01].

- **Lücken in den verwendeten Algorithmen**: Die zum Einsatz kommenden Algorithmen bei S/MIME sind wie bei PGP im Quelltext verfügbar. Sie gelten gemeinhin als sicher.

Somit wird von der Baltimore – bis auf das Ausspähen der unverschlüsselten Daten – die Anforderung an die Geheimhaltung erfüllt. Gegenmaßnahmen gegen das Ausspähen der unverschlüsselten Daten zu ergreifen fällt in die Verantwortung des Benutzers.

Integrität

Wie bei PGP wird in S/MIME eine Hash-Funktion und die anschließende Verschlüsselung mit dem geheimen Schlüssel zur Wahrung der Integrität verwendet. In S/MIME sind zwei verschiedene Modi spezifiziert, die das Format zum Versand einer Signatur beschreiben. Diese sind:

- **clear-signed**: Die Signatur wird getrennt von der eigentlichen Nachricht als Anhang in der E-Mail versendet. Der Vorteil besteht darin, dass die ursprüngliche Nachricht auch in Mail-Programmen ohne S/MIME-Unterstützung gelesen werden kann. Nachteilig ist jedoch, dass die ursprüngliche Nachricht auf dem Weg zum Empfänger durch die zwischengeschalteten Mail-Server verändert werden kann. Dadurch wird die Signatur ungültig, obwohl keine böswillige Veränderung der E-Mail vorliegt.

- **opaque-signed**: Das Problem bei clear-signed-Nachrichten zu beseitigen, ist das Ziel der opaque-signed Nachrichten. Die Signatur einer opaque-signed Nachricht wird zusammen mit der Nachricht selbst in einen binären Anhang verpackt. Hier entsteht jedoch das Problem, dass Nachrichten in diesem Format nur von Mail-Programmen verarbeitet werden können, die dieses verstehen.

Authentifizierung

Im Gegensatz zu PGP werden in einer PKI strengere Vorgaben bezüglich des hierarchischen Aufbaus der Infrastruktur gemacht. Hat ein Benutzer ein Zertifikat eines Kommunikationspartners, kann er davon ausgehen, dass dieses von einer CA zertifiziert wurde. Zumeist ist diese CA selbst von einer Root-CA zertifiziert worden. Durch diese Struktur kann einem Zertifikat im Allgemeinen ein höheres Vertrauen entgegengebracht werden, das für eine Authentifizierung Voraussetzung ist.

In regelmäßigen Abständen oder jeweils beim Empfang einer E-Mail sollte das Mail-Programm in der zum Zertifikat gehörenden CRL überprüfen, ob es nicht vorzeitig für ungültig erklärt wurde. Hier tritt das Problem auf, herauszufinden, in welcher CRL ein solcher Eintrag zu finden wäre. In der Spezifikation zu X.509v3 sind Felder definiert, die das Auffinden der passenden CRL ermöglichen sollen, diese werden jedoch nicht von allen CAs ausgefüllt. Als Beispiel sei hier VeriSign genannt, die Anfang 2001 fälschlicherweise einem vermeintlichen Microsoft-Mitarbeiter ein Zertifikat auf den Namen „Microsoft Corporation“ ausgestellt haben. Nachdem der Fehler festgestellt wurde, wurde dieses Zertifikat in die CRL aufgenommen. Da jedoch in VeriSign-Zertifikaten das angesprochene Feld (CRL Distribution Points) nicht ausgefüllt wird, können Empfänger dieses Zertifikats nicht ohne weiteres feststellen, dass dieses für ungültig erklärt wurde [Veri01].

Unleugbarkeit

Wird eine E-Mail von einem Benutzer unterschrieben, wird er von Windows zur Eingabe der Passphrase aufgefordert. In diesem Eingabedialog ist angegeben, welches Zertifikat für die Signierung verwendet werden soll, so dass beim Einsatz mehrerer Zertifikate die dazu passende Passphrase eingegeben werden kann.

Leider ist diese Funktion vom Benutzer abschaltbar, so dass er im Zweifelsfall behaupten kann, nicht gesehen zu haben, was genau zu signieren war. Es erscheint zumindest jedoch immer eine Meldung, dass etwas zu signieren ist und welches Zertifikat verwendet wird.

Verfügbarkeit

Die Verfügbarkeit der Komponenten der Baltimore UniCERT-PKI kann durch Redundanz erhöht werden. Dazu sind entsprechende Mechanismen, wie zum Beispiel Replikation vorgesehen. Jede einzelne Komponente der Baltimore UniCERT-PKI kann im Netzwerk mehrfach vorkommen, wobei vom Administrator festgelegt werden kann inwieweit die Daten repliziert werden sollen.

Sichere Verwahrung der Schlüssel

Für die Verwahrung der Schlüssel sind zwei Möglichkeiten denkbar. Entweder werden sie in jedem Programm, das die Schlüssel verwendet gespeichert oder in einer zentralen Datenbank, auf die die Programme zugreifen können.

Das Mail-Programm Netscape Messenger speichert zum Beispiel Zertifikate in einer eigenen Datenbank, während Microsoft Programme, wie Outlook und Internet Explorer die zentrale Windows-Datenbank verwenden.

Wichtig bei der Verwendung einer zentralen Datenbank ist die Verschlüsselung von geheimen Schlüsseln, so dass Programme nicht ohne Erlaubnis des Benutzers darauf zugreifen können. In Windows werden Zertifikate in der Registry verschlüsselt gespeichert und können nur mit der passenden Passphrase verwendet werden. Trotzdem bleibt die Gefahr, dass zum Beispiel ein Trojanisches Pferd den Benutzer zur Eingabe seiner Passphrase auffordert und er diese eingibt und damit diese Sicherheitsfunktion umgangen wird.

In der Baltimore UniCERT-PKI ist eine Unterstützung für Smartcards integriert, so dass die sehr sichere Verwahrung auf einer Smartcard verwendet werden kann. Je nach verwendeter Hardware werden die Smartcards zusätzlich durch Eingabe einer PIN gegen unbefugte Benutzung geschützt.

Besonderer Schutz muss vorhanden sein, wenn die geheimen Schlüssel der Benutzer in der CA verwaltet werden. Die UniCERT-PKI bietet für diesen Fall die Verwendung geteilter Passphrases an. Dabei müssen für den Zugriff auf das Personal Security Environment (PSE) mehrere Passphrases eingegeben werden. Die verschiedenen Passphrases sollten von verschiedenen Personen verwaltet werden. Dann ist es einer einzelnen Person nicht möglich, Zugriff auf die geheimen Schlüssel zu erlangen.

Verlässliche Identitätsprüfung

Die Anforderung nach einer verlässlichen Identitätsprüfung lässt sich durch Software nur bedingt erfüllen. Der zentrale Ansatz einer PKI ermöglicht jedoch die Einrichtung einer eigenen Abteilung für die Erstellung von Zertifikaten. Die Zertifikatsanforderungsmasken in der CA und RA der Baltimore PKI können vom Administrator vorgegeben werden. Dabei kann er angeben, welche Informationen Pflichtangaben sind. Wird zum Beispiel eine Ausweisnummer bei der Zertifikatserstellung verlangt, kann man davon ausgehen, dass der Bearbeiter der Anfrage den Ausweis überprüft hat.

In einem Unternehmen wird den Mitarbeitern ein gewisses Vertrauen entgegengebracht und da auf ein Intranet normalerweise von außen nicht zugegriffen werden kann, können in diesem Fall Server im Intranet eines Unternehmens zur Verfügung gestellt werden, über den die Mitarbeiter Zertifikate bestellen können. Von Baltimore wird dies unterstützt.

Fehlerfreiheit der Implementierung

Da der Quelltext der mitgelieferten Programme der Baltimore UniCERT PKI der Öffentlichkeit nicht zugänglich ist, bleibt dem Benutzer nur die Möglichkeit, sich auf externe Gutachten zu verlassen. Die Baltimore UniCERT PKI wurde auf die Information Technology Security Evaluation Criteria (ITSEC) geprüft und in die Sicherheitsstufe E3 eingestuft [ITSEC00]. Im Verlauf der Untersuchungen wurden die Programme der UniCERT PKI auf Fehlerfreiheit überprüft.

Unterstützte Zertifikatsformate

Die Baltimore UniCERT-PKI ist für die Generierung und Verwaltung von X.509v3 Zertifikaten entwickelt worden. Sie unterstützt daher lediglich Zertifikate, die in der X.509v3-Spezifikation vorliegen.

Unterstützte Zertifikats-Austauschformate

Da die Zertifikate beim Benutzer zentral von Windows verwaltet werden, wird im Folgenden beschrieben, welche Formate von Windows verarbeitet werden können:

- **Personal Information Exchange**, mit der Dateiendung PFX, das im Standard PKCS#12 spezifiziert wurde;
- **Cryptographic Message Syntax Standard**, mit der Dateiendung P7B, das im Standard PKCS#7 spezifiziert wurde;
- **DER Encoded Binary X.509**, mit der Dateiendung CER und
- **Base64 Encoded X.509**, das ebenfalls die Dateiendung CER verwendet.

Die beiden letztgenannten Formate werden aus Gründen der Interoperabilität verwendet, da Dateien in diesen Formaten von PKIs anderer Hersteller verarbeitet werden können.

Zertifikate, die geheime Schlüssel enthalten, können nur im erstgenannten Format abgespeichert werden. In diesem Dateiformat werden die Information verschlüsselt gespeichert.

Unterstützte Nachrichten-Austauschformate

E-Mails werden, wie bereits im Abschnitt zur Integrität beschrieben, im S/MIME-Format versendet. Um verschlüsselte oder signierte Nachrichten verarbeiten zu können, muss der Empfänger ein Mail-Programm verwenden, das mit S/MIME-Nachrichten umgehen kann.

Wurde eine Signatur mit dem clear-signed Verfahren in die E-Mail integriert, kann jedes Mail-Programm zumindest den Inhalt der E-Mail anzeigen, ohne jedoch die Signatur überprüfen zu können.

Im Gegensatz dazu können E-Mails, die eine Signatur enthalten und mit dem opaque-signed Verfahren versendet wurden, von Mail-Programmen, die dieses Verfahren nicht unterstützen, nicht verarbeitet werden.

Verbreitung des Protokolls

Einige auf dem Markt befindliche Mail-Programme beinhalten eine Unterstützung für S/MIME-kodierte E-Mails. Dazu gehören unter anderem:

- Microsoft Outlook 97/98/2000
- Microsoft Outlook Express 4.x and 5.x
- Netscape Messenger
- Lotus Notes 4.5.x, 4.6.x and 5.0

Diese Mail-Programme sind jedoch untereinander nicht vollständig interoperabel. Die Hersteller begründen dies mit Mehrdeutigkeiten in der S/MIME-Spezifikation.

Durch die hohe Verbreitung der aufgeführten Mail-Programme ist das S/MIME-Protokoll ebenso weit verbreitet. Es besteht jedoch das Problem, dass diese Funktion nicht von allen Benutzern verwendet wird. Potentiell ist also eine hohe Verbreitung vorhanden – sie muss lediglich aktiviert werden.

Integration in das Mail-Programm

In den angesprochenen Mail-Programmen – insbesondere die verschiedenen Versionen von Microsoft Outlook – ist die S/MIME-Unterstützung bereits im Lieferumfang voll integriert. Daher muss vom Benutzer kein spezielles Plugin installiert werden.

Transparente Prüfung

Durch die vollständige Integration in das Mail-Programm kann die Prüfung einer Signatur und der Unverfälschtheit einer E-Mail transparent ablaufen. In den verschiedenen Versionen von Microsoft Outlook werden dem Benutzer zusätzlich Hinweise für den Umgang mit Sig-

naturen und verschlüsselten E-Mails gegeben. Im folgenden Bild handelt es sich um eine signierte Mail, die in Outlook Express beim ersten Öffnen zunächst eine Hinweisseite verursacht.

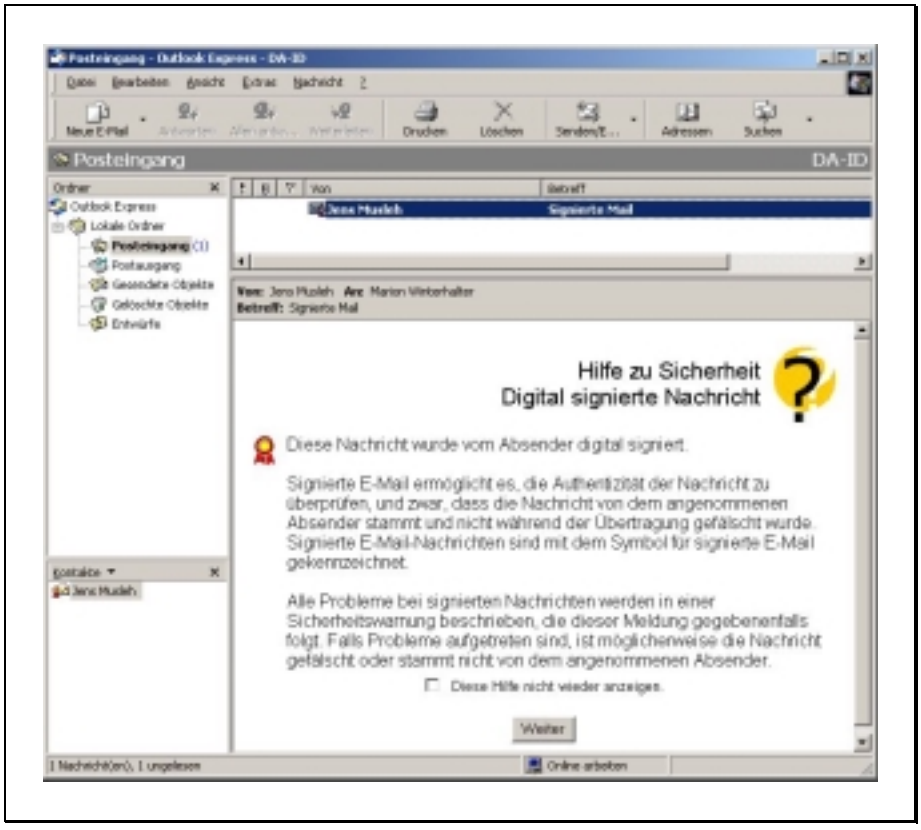


Abbildung 4.3: Benutzungs-Hinweise in Outlook Express bei signierten E-Mails

Wie im Bild ersichtlich, werden signierte Mails in Outlook Express mit einem kleinen, roten Siegel versehen, so dass der Benutzer bereits in der Übersicht der E-Mails erkennen kann, welche E-Mails eine digitale Signatur enthalten und welche nicht.

Verschlüsselte E-Mails werden in ähnlicher Weise dargestellt. Je nach Einstellung wird der Benutzer zur Eingabe der Passphrase aufgefordert. Verschlüsselte E-Mails werden in der Übersicht der E-Mails mit einem kleinen Vorhängeschloss gekennzeichnet.

Durchsetzen einer Sicherheitspolicy

In der Komponente „Certification Authority Operator“ können von einem Administrator Optionen festgelegt werden, die bestimmen, welche Daten zur Erstellung eines Zertifikats zwingend vorhanden sein sollen. Der Administrator generiert hierzu die Eingabemaske, die von einem Mitarbeiter der CA bei einem Auftrag eines Zertifikats ausgefüllt werden muss. Ferner kann die Eingabemaske für Zertifikatsanfragen im Intranet festgelegt werden.

Diese Einstellungen werden von Baltimore Customer Registration Policies (CRP) genannt und enthalten des weiteren Angaben über die erlaubten Schlüsselalgorithmen, Schlüsselläng-

gen, Verwendungszweck der Schlüssel und Hash-Algorithmen. Ferner können Default-Werte für einzelne Felder festgelegt werden und darüber hinaus zusätzliche Felder nach der X.509v3-Spezifikation angegeben werden.

Einfache Zertifikatsverwaltung

Zertifikate werden auf den Rechnern der Benutzer in einem zentralen Zertifikatsspeicher unter Windows verwaltet. Der Zugriff auf die Verwaltung des Zertifikatsspeichers ist in Windows in den Internetoptionen unter „Inhalt“ abgelegt. Diese Position dürfte nur den wenigsten Benutzern bekannt sein und die Zertifikatsverwaltung daher meist verborgen bleiben. Es sollten daher entsprechende Dokumentationen oder Schulungen angeboten werden, um den Benutzer auch mit dem Umgang von Zertifikaten vertraut zu machen.

Die Bedienung der Zertifikatsverwaltung ist einfach gehalten und wird durch gute Hilfetexte unterstützt. Bei der Installation von Windows werden Zertifikate verschiedener Root-CAs bereits als vertrauenswürdige Root-CAs eingestuft. Benutzer sollten daher die bereits installierten Zertifikate überprüfen und sich für jedes einzelne überlegen, ob diesem Vertrauen entgegengebracht werden kann.

4.2.2 Internet- / Intranet-Anwendung

Die Erfüllung der Anforderungen an die sichere Internet- bzw. Intranet-Kommunikation ist hauptsächlich von den eingesetzten Web-Servern und Web-Browsern abhängig. Daher wird im folgenden Abschnitt zunächst das Protokoll vorgestellt, das zur sicheren Kommunikation zwischen Web-Servern und Web-Browsern verwendet wird.

Geheimhaltung / Integrität

Diese Anforderungen werden über das Secure Sockets Layer (SSL) Protokoll erfüllt. Das folgende Bild, das aus [Götz99] entnommen wurde, zeigt wie das SSL-Protokoll logisch zwischen die Transport-Schicht (im Internet TCP) und die Anwendungsschicht gelegt wird.

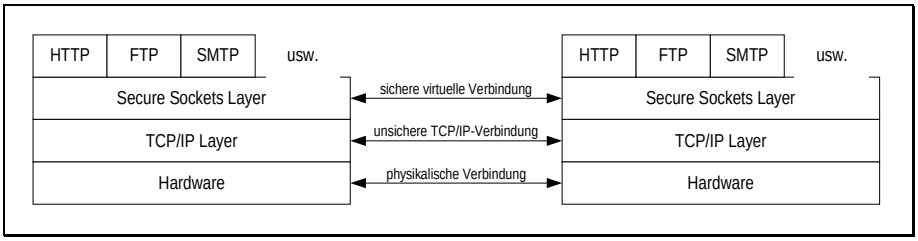


Abbildung 4.4: Secure Socket Layer Protokoll

In [Götz99] wird der Verbindungsaufbau in den folgenden vier Schritten vollzogen:

- Der Client baut eine Verbindung zum Server auf und teilt ihm die unterstützten Kryptoverfahren mit.

- Der Server wählt daraus die Verfahren für asymmetrische und symmetrische Verschlüsselung sowie den Hash-Algorithmus aus und sendet sein Zertifikat an den Client.

- Der Client generiert einen Schlüssel für die kommende symmetrische Verschlüsselung, verschlüsselt diesen mit dem öffentlichen Schlüssel des Servers und sendet diesen an den Server.

- Abschließend erfolgt eine Authentifizierungsphase, in der der Client dem Server eine Reihe – mit dem generierten symmetrischen Schlüssel verschlüsselter – zufälliger Testnachrichten schickt, die der Server nur dann entschlüsseln und bestätigen kann, wenn es sich um den echten Server handelt. Optional kann der Server auf vergleichbare Weise den Client authentifizieren, sofern dieser über ein Zertifikat verfügt, dem der Server Vertrauen entgegen bringt.

Nach dem erfolgreichen Verbindungsaufbau können die eigentlichen Daten verschlüsselt übertragen werden.

Verfügbarkeit

Da für eine gesicherte Kommunikation zwischen zwei Kommunikationspartnern über SSL lediglich bereits ausgestellte Zertifikate nötig sind, ist die Verfügbarkeit der PKI-Komponenten nicht zwingend erforderlich.

Eine Ausnahme bildet jedoch der Server, der die CRL zur Verfügung stellt. Dieser sollte bei einer Kommunikationsanforderung aktiv sein, so dass die eingesetzten Zertifikate auf ihre Gültigkeit überprüft werden können. Die CRL wird von der CA in einstellbaren Intervallen ausgegeben und mit einem Zeitstempel versehen. Diese kann als Datei gespeichert werden und auf beliebig viele Server verteilt werden. Die Datei wird von der CA digital signiert, so dass eine Manipulation der Datei ausgeschlossen ist.

Authentifizierung

Durch die Möglichkeit der Client-Authentifizierung in SSL kann die Authentifizierung transparent ablaufen. Der Benutzer wird beim Aufruf einer geschützten Seite lediglich zur Eingabe der Passphrase oder Bestätigung der Verwendung seines Zertifikats aufgefordert.

Außerdem besteht die Möglichkeit bei Zertifikaten der X.509v3-Spezifikation eigene Felder zu definieren. Ein Händler könnte selbst Zertifikate ausgeben, die einen Benutzer zu bestimmten Aktionen autorisiert. So könnte zum Beispiel ein Grenzbetrag festgelegt werden, bis zu dem der Kunde ohne weitere Rückfragen einkaufen kann. Allerdings müsste der Händler in diesem Fall eine eigene CA betreiben. Außerdem hätte der Kunde das Problem, die Zertifikate verschiedener Händler zu verwalten.

Schutz des Netzwerks

Im Lieferumfang der Baltimore UniCERT-PKI sind keine speziellen Programme für den Aufbau von Virtual Private Networks (VPNs) vorhanden. Die erstellten Zertifikate können jedoch für eine sichere Verbindung über das Internet Protocol Security (IPSec) verwendet werden.

In der CRP kann vom Administrator festgelegt werden, dass ein Zertifikat die Eigenschaft hat, für VPN-Verbindungen verwendet zu werden. Ferner bietet die UniCERT-PKI eine Unterstützung für VPN-Router der Firma Cisco.

Erkennung von Eindringlingen / Einsatz von Virenscannern

Diese Anforderungen werden von der Baltimore UniCERT-PKI nicht erfüllt. Diese Anforderungen zu erfüllen liegt in der Verantwortung der Benutzer. Diese können durch den Einsatz unternehmensweit einheitlicher Produkte unterstützt werden.

Durchführen von Backups

Die Komponenten der Baltimore UniCERT-PKI verwenden als Datenbank das Datenbanksystem von Oracle in der Version 8. Die Daten sollten möglichst mit den zum Oracle Datenbanksystem mitgelieferten Backup-Programmen gesichert werden.

4.2.3 Eigenschaften der Architektur

Die Erfüllung der Anforderungen an die Architektur der UniCERT-PKI werden im Folgenden gezeigt.

Skalierbarkeit

Im Gegensatz zu PGP wurde die UniCERT-PKI als kommerzielle Lösung entwickelt und soll vorrangig Großkunden bedienen. Daher wurde besonderer Wert auf die Möglichkeit der Skalierbarkeit gelegt. Durch die Aufteilung in CA und RA wird bereits die Skalierbarkeit erreicht. Durch die jeweilige Trennung zwischen CA und CAO bzw. RA und RAO kann auch auf Administratorebene skaliert werden.

Verfügbarkeit

Wie bereits im Abschnitt 4.2.2 beschrieben, ist die Verfügbarkeit des Servers, der die CRL zur Verfügung stellt, besonders kritisch. Es sollten daher Maßnahmen getroffen werden, die diesen Server vor Angriffen schützen. Auch Ausfälle, die nicht auf Angriffe zurückzuführen sind, sollten einkalkuliert werden. Es empfiehlt sich, diese Server redundant auszulegen. Auch der Rechner, auf dem der geheime Schlüssel einer CA gespeichert ist, bedarf besonderem Schutz. Er sollte zum Beispiel möglichst nicht im Netzwerk angeschlossen sein, um Angriffe zu verhindern.

4.2.4 E-Commerce Anwendung

Durch die transparente und benutzerfreundliche Authentifizierung mit Hilfe von X.509-Zertifikaten sind sie für E-Commerce Anwendungen gut geeignet. Die Erfüllung der speziellen Anforderungen im Zusammenhang mit E-Commerce Anwendungen wird in den folgenden vier Abschnitten behandelt.

Gesicherte Kommunikation

Es hat sich gezeigt, dass X.509-Zertifikate für eine gesicherte Kommunikation – sei es nun über E-Mail oder über eine SSL-Verbindung – sehr gut geeignet sind. Ein Problem, das noch weiter untersucht werden muss, ist jedoch die Problematik der vorzeitig zurückgezogenen Zertifikate. Zwar werden diese in einer CRL verwaltet, diese müsste jedoch vor jeder Verwendung eines Zertifikats abgefragt werden, um zurückgezogene Zertifikate zu erkennen. Hinzu kommt die Abhängigkeit vom Aktualisierungsintervall, das vom Administrator der CA vorgegeben wird.

Überprüfung von Identitäten

X.509-Zertifikate sind gut geeignet, die Identität der Kommunikationspartner über digitale Signaturen sicherzustellen. Ob jedoch tatsächlich die richtige Person hinter einem angegeben Namen steht, hängt von der Sorgfalt der jeweiligen CA ab. Der Vorteil von X.509-PKIs gegenüber PGP ist, dass CAs ein Certificate Practice Statement (CPS) veröffentlichen, in dem jeder nachschlagen kann, auf welche Weise die Identität der Zertifikats-Inhaber geprüft wurde.

Ein weiterer Vorteil ist der Einsatz von Zertifikaten in den Web-Servern, die es ermöglichen eine Kommunikation mit dem tatsächlich gewünschten Server aufzubauen. Der Benutzer erhält eine Warnmeldung, falls der Domainname im Zertifikat nicht dem tatsächlichen Domainnamen entspricht und kann die Kommunikation abbrechen.

Sicherheit der Komponenten

Die Verfügbarkeit kann durch Redundanzen erhöht werden. Es muss jedoch bei der Einrichtung einer CA oder RA darauf geachtet werden, dass die Systeme gegen Angriffe geschützt werden. Eine eigene Firewall, die solche Angriffe verhindern kann, ist im Lieferumfang der Baltimore UniCERT-PKI nicht enthalten.

Alle Komponenten der UniCERT-PKI können so konfiguriert werden, dass sie Ereignisse in ein Logfile schreiben. Es können spezielle Zertifikate erstellt werden, mit denen diese Logfiles signiert werden. Die Logfiles regelmäßig zu kontrollieren ist jedoch Aufgabe des Administrators. Er wird von der UniCERT-PKI unterstützt, indem bei bestimmten Ereignissen eine E-Mail an ihn versendet werden kann.

Die korrekte und sichere Verarbeitung von Daten hängt von der fehlerfreien Implementierung und der Abschottung der Systeme gegen Angriffe ab. Aufgrund des erteilten ITSEC-Zertifikats kann von einer sicheren und korrekten Datenverbeitung ausgegangen werden.

Schutz des Endbenutzers

Die einfache Bedienung unter Windows wird einer Etablierung von X.509-PKIs sehr entgegen kommen. Durch die hohe Integration der Zertifikatsbehandlung müssen von Benutzern keine speziellen Programme installiert werden.

Es wurde gezeigt, dass mit der UniCERT-PKI ein Sicherheitsmodell aufgebaut werden kann, das es den Kommunikationspartnern ermöglicht, Transaktionen nachzuweisen. Die Integrität der Transaktionen wird gewahrt.

4.3 Analyse von SPKI/SDSI

In diesem Abschnitt werden die Ansätze der theoretischen Lösung SPKI/SDSI 2.0 auf die Erfüllung der Anforderungen hin untersucht. Da es nicht bei allen Anforderungen eine Möglichkeit des Tests gibt, werden nur diese angeführt, die getestet werden können.

4.3.1 E-Mail-Austausch

Eine Implementierung im E-Mail-Bereich ist nicht bekannt. Vom Prinzip her ist es jedoch möglich, SPKI-Zertifikate für die Signierung und Verschlüsselung von E-Mails zu verwenden.

Geheimhaltung / Integrität

Da in der Spezifikation keine bestimmten Kryptoverfahren vorgeschrieben sind, kann keine definitive Aussage über die Erfüllung der Anforderungen nach Geheimhaltung und Integrität getroffen werden. Es können beliebige Kryptoverfahren zum Einsatz kommen und je nachdem, welches für die jeweilige Aufgabe (Verschlüsseln bzw. Signieren) verwendet wird, muss geprüft werden, ob dieses den Sicherheitsanforderungen entspricht. Man kann jedoch davon ausgehen, dass in einer tatsächlichen Implementierung Verfahren eingesetzt werden, die zu diesem Zeitpunkt die Anforderungen nach Geheimhaltung und Integrität hinreichend erfüllen.

Authentifizierung

Aufgrund der Verwendung von lokalen Namensräumen ist SPKI/SDSI für E-Mails über einen geschlossenen Benutzerkreis nur bedingt geeignet. Einzelne Benutzerkreise bilden jeweils einen Namensraum, die über die SPKI-Delegation miteinander verbunden werden müssen. Dabei entsteht das Problem, für die Authentifizierung die richtige Zertifikatskette zu finden. Dies soll das folgende Bild veranschaulichen, in dem die mit 1, 2 und 3 bezifferten Pfeile eine Zertifikatskette bilden.

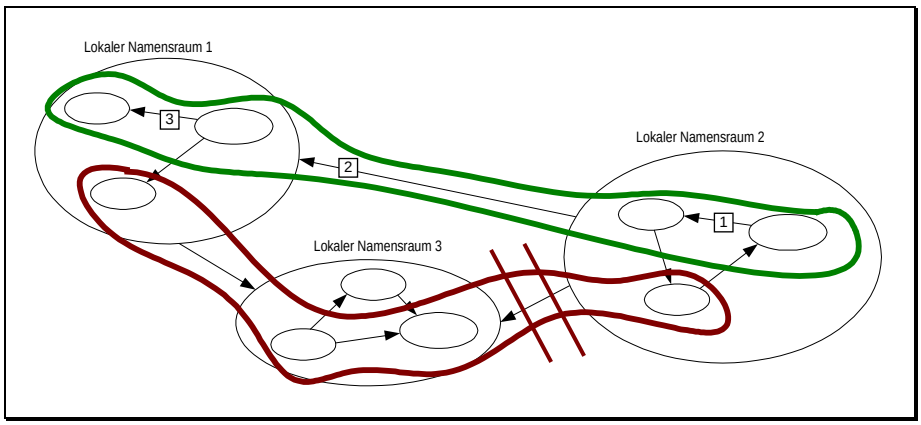


Abbildung 4.5: SPKI/SDSI-Zertifikate über lokale Namensräume hinaus

Wenn nicht alle Zertifikate vorliegen, kann es passieren, dass eine solche Kette nicht gefunden werden kann.

Darüber hinaus ist es das Ziel von SPKI, Namen aus den Zertifikaten zu entfernen und stattdessen den Personen Berechtigungen in Form von Zertifikaten zu geben. Diese Berechtigungszertifikate werden von dem Objekt, das die Berechtigung betrifft, direkt erstellt. Es müsste daher für den E-Mail-Austausch eine eigene Instanz geschaffen werden, die Zertifikate für die Authentifizierung in E-Mails ausgibt.

Verlässliche Identitätsprüfung

Da jedes Objekt (auch Personen) selbst Zertifikate erstellen kann, um so seine Berechtigungen zu delegieren, gibt es keine verlässliche Identitätsprüfung. Würde eine eigene Zertifizierungsinstanz geschaffen, die Zertifikate für den E-Mai-Austausch erstellt, so könnte von dieser eine verlässliche Identitätsprüfung vorgenommen werden. Jedoch ist in SPKI/SDSI kein Mechanismus vorgesehen, der wie beispielweise bei X.509 ein CPS vorschreibt. Jede dieser Instanzen könnte eigene Vorstellungen darüber haben, was sie unter einer verlässlichen Identitätsprüfung versteht.

Unterstützte Zertifikatsformate / Zertifikats-Austauschformate

Zertifikate werden in der S-Expression dargestellt und sind daher für Menschen lesbar. Damit können kundige Benutzer die Zertifikate im Quelltext anschauen und diese ohne zusätzliche Programme kontrollieren. Dies erhöht die Kontrollmöglichkeiten der erteilten Berechtigungen.

Die Zertifikate können optional in der Base64-Kodierung dargestellt werden. Soll ein solches Zertifikat kontrolliert werden, ist es jedoch mit einem Zusatzprogramm wieder in die ursprüngliche Form konvertierbar.

Verbreitung des Protokolls

Aufgrund der mangelnden Produkte, die SPKI/SDSI einsetzen, ist noch keine Verbreitung zu verzeichnen. In den wenigen Implementierungen werden SPKI/SDSI-Zertifikate nur intern verwendet, und zumeist leicht abgewandelt, so dass sie den Anforderungen der jeweiligen Implementierung entsprechen.

4.3.2 Internet- / Intranet-Anwendung

Im Bereich der Internet- und Intranet-Anwendung von SPKI/SDSI ist bereits eine prototypische Implementierung in der Arbeit von Maywah [Mayw00] vorgestellt worden. Dabei handelt es sich um ein Plugin für den Netscape Communicator. Theoretisch ist auch ein Plugin für den Microsoft Internet Explorer oder andere Browser möglich. Als Web-Server kommt in der vorgestellten Lösung der Apache-Webserver zum Einsatz. So kann vom Administrator relativ einfach in der Datei „.htaccess“ für jede Datei oder ganze Verzeichnisse festgelegt werden, welche Tags für den Zugriff benötigt werden. Der Vorteil ist hierbei, dass anstatt Namen lediglich die Befugnis selbst im Zertifikat als Tag angegeben wird.

Geheimhaltung / Integrität

Das in der Arbeit von Maywah vorgestellte Geronimo-Protokoll, das für die Authentifizierung mittels SPKI/SDSI-Zertifikaten zuständig ist, beinhaltet keine Schutzmechanismen gegen die Verletzung der Geheimhaltung oder Integrität. Er empfiehlt daher, eine eigene SSL-Implementierung zu entwickeln, die auf SPKI/SDSI-Zertifikaten basiert. Diese kann in das Geronimo-Protokoll integriert werden.

Authentifizierung

Das Geronimo-Protokoll sieht vor, dass bei einer Anfrage bei einem Web-Server dieser die für einen Zugriff auf das gewünschte Objekt benötigten Tags angibt. Das Plugin ermittelt aus den vorhandenen SPKI/SDSI-Zertifikaten die passende Zertifikatskette mit dem benötigten Tag und sendet diese an den Web-Server. Bei erfolgreicher Authentifizierung wird der Benutzer sogleich autorisiert.

4.3.3 Eigenschaften der Architektur

In der von Maywah vorgestellten Lösung kommen lediglich Web-Server und Web-Clients zum Einsatz. Daher wird die Untersuchung der Erfüllung der beiden Anforderungen nach Skalierbarkeit und Verfügbarkeit im Folgenden auf diese Komponenten beschränkt.

Skalierbarkeit

Die Skalierbarkeit der Web-Server wird von SPKI/SDSI-Zertifikaten oder dem Geronimo-Protokoll nicht beeinträchtigt oder begünstigt. Sie hängt vom eingesetzten Web-Server selbst ab.

Die Web-Clients beeinträchtigen sich nicht gegenseitig und sind nicht voneinander abhängig, daher sind keine Probleme bezüglich der Skalierbarkeit zu erwarten.

Verfügbarkeit

Auch die Anforderung nach der Verfügbarkeit wird durch den Einsatz von SPKI/SDSI-Zertifikaten nicht erhöht oder verringert. Sie hängt damit vom jeweils eingesetzten Produkt (in diesem Fall Netscape Communicator und Apache Webserver) selbst ab.

4.3.4 E-Commerce Anwendung

Die Anforderungen für E-Commerce Anwendungen können nicht alle geprüft werden. Die Erfüllung der Anforderungen, die mit der Authentifizierung in Zusammenhang stehen, wurden geprüft und werden im Folgenden beschrieben.

Gesicherte Kommunikation / Überprüfung von Identitäten

Die Anforderung nach einer gesicherten Kommunikation und der Überprüfung von Identitäten wird von SPKI/SDSI nicht erfüllt. Es müssen Produkte von Drittanbietern verwendet werden, wie zum Beispiel SSL von Netscape.

In der Arbeit von Maywah wurde vorgeschlagen, eine eigene Implementierung des SSL-Protokolls zu entwickeln, das mit SPKI/SDSI-Zertifikaten arbeitet. Dabei sollten die beiden Protokolle Geronimo und SSL in ein einzelnes Protokoll integriert werden.

Die Überprüfung von Identitäten kann nur erfolgen, wenn Namenszertifikate verwendet werden. Selbst dann ist zunächst eine entsprechende Vertrauenshierarchie aufzubauen. Dabei geht die besondere Eigenschaft einer *einfachen* PKI jedoch verloren, da das Ziel, den aufwendigen Betrieb einer Hierarchie mit CAs in SPKI zu vermeiden, nicht erfüllt werden kann.

Schutz des Endbenutzers

Die Anforderung nach einer einfachen Bedienung konnte sogar schon in der prototypischen Implementierung unter Netscape erfüllt werden. Die Bedienung ist sehr einfach gehalten: Der Benutzer wird beim Start von Netscape (genauer beim Start des SPKI/SDSI-Plugins) einmalig zur Eingabe seines Passwortes aufgefordert. Danach wird bei Verwendung eines Zertifikats ein „SPKI/SDSI Authentication Session Window“ angezeigt, das vom Benutzer zur Beendigung der Session geschlossen werden muss.

Allerdings sind noch Performance-Probleme zu lösen, denn eine Anmeldung an einem Server dauert laut Maywah im Durchschnitt ca. 20 Sekunden. Dies dürfte für die meisten Benutzer eine inakzeptable Reaktionszeit sein.

Die Anforderung nach Anonymität kann von SPKI/SDSI erfüllt werden, da Berechtigungen ohne die Angabe von Namen in den Zertifikaten untergebracht werden können. Die Angabe von Namen in SPKI/SDSI-Zertifikaten ist optional. Stattdessen können Berechtigungszertifikate auf die Angabe des öffentlichen Schlüssels beschränkt werden.

4.4 Gegenüberstellung der Sicherheitsmodelle

Da einige der Anforderungen der drei untersuchten Sicherheitsmodellen in gleichem Maße erfüllt werden, sollen in diesem abschließenden Abschnitt die Unterschiede und herausragenden Eigenschaften – auch im Hinblick auf die Eignung im E-Commerce – der Sicherheitsmodelle aufgezeigt werden.

4.4.1 Pretty Good Privacy

PGP verfolgt als Vertrauensmodell einen dezentralen Ansatz. Jeder Benutzer kann Zertifikate erstellen, dadurch entsteht keine Abhängigkeit von einer zentral verwalteten CA. Dadurch wird jedoch die Vertrauensbildung erschwert. Ein Empfänger eines Zertifikats muss selbst evaluieren, ob der Aussteller dieses Zertifikats entsprechende Sorgfalt bei der Prüfung der Identität des Zertifikatsinhabers walten ließ. Speziell für Zertifikatsersteller, denen ein nicht so hohes Vertrauen entgegengebracht wird, bietet PGP die Funktion, diesen nur marginales Vertrauen entgegenzubringen. Somit ist eine Abstufung des Vertrauens möglich.

Durch die Unabhängigkeit von zentralen Instanzen ist PGP besonders ausfallsicher. Meist werden öffentliche Schlüssel nicht nur von einem Zertifikatsersteller signiert. Es entsteht ein Netz aus Vertrauensbekundungen. So können meist redundante Vertrauensketten gefunden werden.

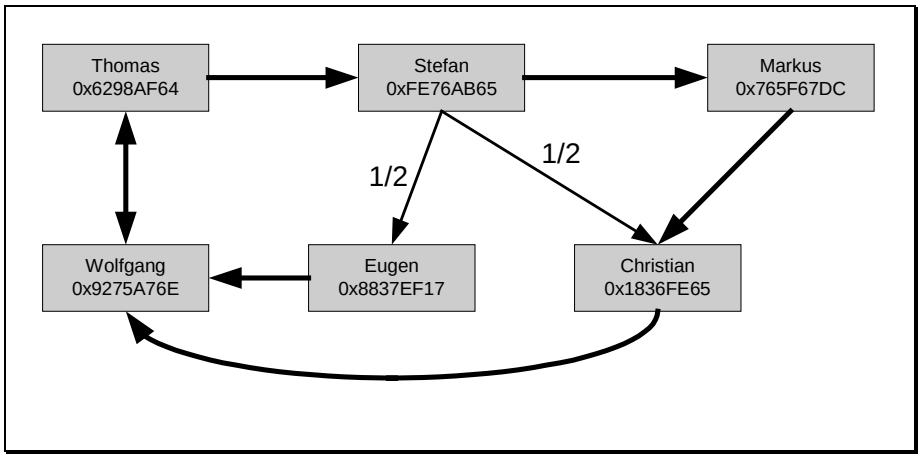


Abbildung 4.6: Beispiel für ein Vertrauensnetz in PGP

Allerdings ist PGP hauptsächlich für den Einsatz in der Verschlüsselung von E-Mails konzipiert. Da im Bereich des E-Commerce besonderes Augenmerk auf die Authentifizierung innerhalb eines Web-Shops liegt, ist PGP für E-Commerce nicht gut geeignet.

Im Zuge der Entwicklung des Transport Layer Security (TLS) Protokolls soll auch die Unterstützung für PGP-Zertifikate nach dem OpenPGP-Standard integriert werden [PrEl01]. Das TLS-Protokoll soll das zurzeit eingesetzte SSL-Protokoll ablösen und wird von den

meisten Browsern bereits jetzt unterstützt. Sollte dies implementiert werden, ist PGP über die proprietäre Lösung PGPnet hinaus für sichere Internet- bzw. Intranetverbindungen geeignet.

Des weiteren werden Schlüssel meist von Bekannten signiert, da die Überprüfung der Identität einer fremden Person mühsam ist. PGP wird daher hauptsächlich innerhalb des eigenen Bekanntenkreises eingesetzt. Im Bereich des E-Commerce wäre dies höchstenfalls mit einer B2B-Plattform vergleichbar, in der die Kunden in der Regel bekannt sind und nicht sehr häufig wechseln.

4.4.2 PKI mit X.509v3-Zertifikaten

Eine PKI basiert auf einem hierarchisch aufgebauten Vertrauensmodell. An oberster Stelle steht eine Root-CA, die mehrere Sub-CAs zertifiziert. Die Benutzer erhalten ihre Zertifikate in der Regel von diesen Sub-CAs.

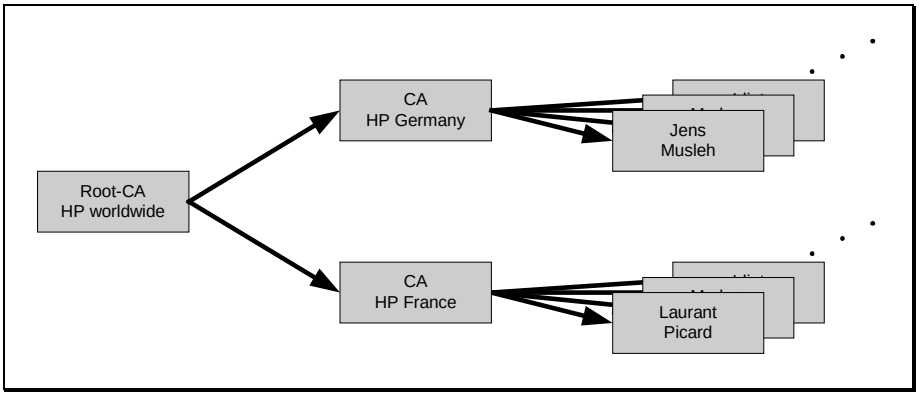


Abbildung 4.7: Beispiel für eine zweistufige Hierarchie in einer PKI

Auf diese Weise wird eine große Anzahl von Benutzern von einer Root-CA indirekt zertifiziert. Der Vorteil einer PKI liegt also darin, dass zur Evaluierung der Gültigkeit eines Zertifikats lediglich der Root-CA einmalig Vertrauen geschenkt werden muss und damit alle Benutzer dieser CA als vertrauenswürdig eingestuft werden.

Daher ist eine PKI für E-Commerce gut geeignet. Ein Händler könnte den Zertifikaten der verbreitetsten Root-CAs vertrauen und damit bereits einem sehr großen Kundenstamm vertrauen. Sollte ein Kunde noch kein Zertifikat einer der vertrauten Root-CAs haben, kann der Händler den Kunden an eine dieser Root-CAs verweisen und muss sich somit nicht selbst um die Zertifikatserstellung kümmern. Die Chance, dass der Kunde ein solches Zertifikat dann bei anderen Händlern einsetzen kann, ist relativ hoch.

In X.509v3-Zertifikaten sind zusätzliche Felder vorgesehen, die vom Zertifikatsersteller beliebig gefüllt werden können. Es macht jedoch keinen Sinn, besondere Berechtigungen (zum Beispiel eine bestimmte Kreditlinie, bis zu der der Kunde einen Einkauf tätigen kann), die ein Kunde gegenüber einem Händler hat, in ein solches Zertifikat zu speichern. Sonst müssten bei Änderungen der Berechtigungen neue Zertifikate ausgestellt und die alten für ungültig erklärt werden. Außerdem müsste der Kunde für jeden Händler ein eigenes Zertifikat erhalten und diese verwalten.

4.4.3 SPKI/SDSI

In SPKI/SDSI wird der Ansatz eines globalen Namensraums, wie er bei PGP und PKI besteht, aufgegeben. Auch in SPKI/SDSI kann jeder ein Zertifikat erstellen. Ein angegebener Name in einem Zertifikat gehört jedoch nur dem lokalen Namensraum des Zertifikaterstellers an. Namen sagen in SPKI/SDSI nichts über die Person aus, die das Zertifikat erhält, sondern repräsentieren einen Bezeichner, der auf eine Berechtigung hinweisen kann.

Diese Definition der Namensgebung bedeutet für den Zertifikatsersteller die volle Kontrolle über seinen eigenen Namensraum. Keine andere Instanz außerhalb des lokalen Namensraums kann eine Zuordnung in Frage stellen, da für sie das Zertifikat nicht gültig ist. Daher ist in SPKI/SDSI keine CRL notwendig.

Für E-Commerce-Anwendungen bedeutet dies, dass die Händler jeweils ihre eigenen Zertifikate ausgeben und diesen implizit vertrauen. Da als Namen beliebige Bezeichner verwendet werden, könnten zum Beispiel die selbst vergebenen Kundennummern des Händlers als Bezeichner gewählt werden.

Die Verwendung von Gruppenzertifikaten, von denen jedes Mitglied einer Gruppe das selbe Zertifikat erhält, ermöglicht die Unterstützung von anonymen Transaktionen.

Der Kunde muss allerdings eine größere Menge von Zertifikaten verwalten. In der Arbeit von Maywah [Mayw00] wurde jedoch gezeigt, dass die Verwendung von SPKI/SDSI-Zertifikaten in einer benutzerfreundlichen Weise ablaufen kann. Der Benutzer muss zum Schutz der gespeicherten geheimen Schlüssel lediglich einmal ein Passwort beim Start des Browsers angeben. Danach werden bei einer Anforderung eines Servers die passenden Zertifikate vom Plugin ausgewählt. Somit stellt die Verwaltung mehrerer Zertifikate bei SPKI/SDSI keinen Aufwand für den Kunden dar.

Kapitel 5 Interoperabilität

Für den Test der Sicherheitsmodelle auf Interoperabilität wird zunächst geprüft, ob die Anforderungen aus Abschnitt 2.6 erfüllt werden können. Die Ergebnisse werden für jedes Sicherheitsmodell in einem eigenen Abschnitt vorgestellt. Im darauf folgenden Abschnitt wird darauf eingegangen, wie Sicherheitsmodelle von PGP und PKI interoperieren.

5.1 Pretty Good Privacy

Nachstehend wird untersucht, ob die aufgestellten Anforderungen an die Interoperabilität durch PGP Desktop Security erfüllt werden.

Migration

Da PGP ständig an neue Sicherheitsanforderungen angepasst wird und somit immer wieder neue Versionen auf den Markt kommen, ist in PGP eine Migration zu einer neueren Version in der Regel unproblematisch. Lediglich beim Versionswechsel auf die Version 2.5 konnten die Daten älterer Versionen nicht mehr verarbeitet werden.

Daten-Export und –Import

In PGP sind Mechanismen vorgesehen, um Daten zu exportieren bzw. zu importieren. Allerdings werden vorrangig PGP-eigene Dateiformate verwendet. Der Import von X.509-Zertifikaten ist jedoch möglich.

Unterstützung für heterogene Architekturen

Die einzige Komponente, die eine automatische Verarbeitung ein- oder ausgehender Daten ermöglicht, ist der PGP eBusiness-Server der Firma Network Associates. Dieser erlaubt eine skriptbasierte Aufgabenverarbeitung, wie zum Beispiel das automatische Signieren.

Verbindungsmöglichkeiten zu anderen Architekturen

Die folgende Tabelle enthält die möglichen Komponenten in einer PGP-Infrastruktur und gibt Aufschluss darüber, welche dieser Komponenten durch Produkte anderer Hersteller ersetzt werden könnten. Sofern ein standardisiertes Protokoll für die Kommunikation verwendet wird, ist eine Ersetzung möglich.

PGP Clients	Die PGP Clients verwenden das PGP-eigene Format und können daher lediglich durch andere PGP-Produkte ausgetauscht werden. Dazu gehören die kostenlose Version von PGP sowie GnuPG. Allerdings werden dann Vorgaben der Sicherheitspolicy nicht erfüllt.
CA	Die Net Tools PKI von Network Associates können durch andere CAs ersetzt werden. Auch CAs, die nur X.509-Zertifikate erstellen, können zum Einsatz kommen.
Keyserver	Der PGP Keyserver von Network Associates kann durch einen beliebigen anderen LDAP-Server ersetzt werden.
Programm zur Verwaltung von Sicherheitspolicies	Das Programm zur Verwaltung der Optionenprofile kann nicht durch ein anderes Produkt ersetzt werden, da damit Installationspakete erstellt werden, in denen die vorgegebenen Optionen eingestellt sind.

Tabelle 5.1: Austauschmöglichkeiten der Komponenten einer PGP-Infrastruktur

5.2 Baltimore PKI

In diesem Abschnitt wird die Interoperabilität der UniCERT-PKI der Firma Baltimore untersucht. Inwieweit eine PKI, die auf X.509-Zertifikaten basiert, mit dem Sicherheitsmodellen von PGP interoperabel ist, wird im Abschnitt 5.4 vorgestellt.

Die Baltimore UniCERT-PKI basiert hauptsächlich auf offenen Standards und erfüllt daher die Anforderungen nach Migration, Import und Export von Daten und die Unterstützung von heterogenen Architekturen.

Die Anforderung nach Verbindungsmöglichkeiten zu anderen Architekturen wird durch Ersetzungsmöglichkeiten der einzelnen Komponenten gezeigt.

In der folgenden Tabelle sind die mitgelieferten Komponenten der UniCERT-PKI aufgelistet. Dazu wurde jeweils bemerkt, ob und in welcher Weise diese Komponente durch ein Produkt eines anderen Herstellers ersetzt werden kann:

CA	Da die von Baltimore gelieferte CA nur auf offenen Standards basiert, ist die Verwendung von CAs anderer Hersteller unproblematisch, sofern das Produkt des anderen Herstellers ebenfalls diese offenen Standards unterstützt.
CAO	Das CAO-Programm kann als Steuerungsprogramm für die UniCERT-CA angesehen werden und arbeitet nur mit dieser zusammen.
RA	Da auch die RA von Baltimore auf offenen Standards basiert, kann sie durch ein Produkt eines anderen Herstellers ersetzt werden.
RAO	Das RAO-Programm dient als Steuerprogramm für die RA von Baltimore. Es kann daher nicht ausgetauscht werden.
LDAP-Server	In der UniCERT-PKI kann ein beliebiger LDAP-Server zum Einsatz kommen. Lediglich zur Verbreitung der Sicherheitspolicy sollte der LDAP-Server der Firma Baltimore eingesetzt werden.
Gateway	Das Gateway stellt die Schnittstelle zwischen den Benutzern und den Komponenten CA und RA dar. Benutzer können damit Anfragen an die CA oder RA über ein Web-Formular oder per E-Mail stellen. Es kann durch ein anderes Produkt ersetzt werden, wenn dieses die beiden Schnittstellen (zwischen Benutzer und Gateway und zwischen Gateway und den Komponenten CA bzw. RA) unterstützt.
Token Manager	Der Token Manager muss bei der Verwendung einer fremden CA bzw. RA durch ein entsprechendes Produkt des anderen Herstellers ersetzt werden.

Tabelle 5.2: Austauschmöglichkeiten der Komponenten der UniCERT-PKI

5.3 SPKI/SDSI

Bei der Entwicklung eines neuen Modells steht zunächst die Beschreibung der internen Schnittstellen im Vordergrund. In SPKI/SDSI sind aufgrund des Entwicklungsstadiums noch keine Informationen über die Interoperabilität mit anderen Sicherheitsmodellen vorhanden. Daher wird im folgenden Abschnitt nur die Interoperabilität zwischen PGP und PKI untersucht.

5.4 Interoperabilität zwischen PGP und PKI

Da PGP und PKI auf der gleichen Technik basieren, ist es vorstellbar, dass diese beiden Sicherheitsmodelle miteinander gekoppelt werden können. Dazu ist zu untersuchen, ob Nachrichten und Zertifikate untereinander ausgetauscht und verarbeitet werden können. Es ergeben sich folgende Konstellationen:

Verschlüsselte Nachricht eines PGP-Absenders an einen PKI-Empfänger

Damit ein PGP-Benutzer an einen PKI-Empfänger eine verschlüsselte E-Mail versenden kann, muss ihm das X.509-Zertifikat des PKI-Empfängers vorliegen. In PGP können X.509-Zertifikate in die Schlüsselverwaltung aufgenommen werden und E-Mails an solche Empfänger generiert werden.

Signierte Nachricht eines PGP-Absenders an einen PKI-Empfänger

Da dem PKI-Empfänger die Möglichkeit fehlt, PGP-Zertifikate zu verarbeiten, kann er die Signatur des PGP-Absenders nicht überprüfen. Da eine von PGP signierte E-Mail jedoch als ASCII-Text übertragen wird, ist zumindest der Inhalt der E-Mail für den PKI-Empfänger lesbar.

Verschlüsselte Nachricht eines PKI-Absenders an einen PGP-Empfänger

Da der PGP-Empfänger lediglich ein PGP-Zertifikat hat, das der PKI-Benutzer nicht verarbeiten kann, ist es nicht möglich, eine verschlüsselte E-Mail aus einer PKI einem PGP-Empfänger zu schicken.

Signierte Nachricht eines PKI-Absenders an einen PGP-Empfänger

Liegt dem PGP-Empfänger das X.509-Zertifikat des PKI-Absenders vor, kann er die Signatur überprüfen.

Versand eines PGP-Zertifikats an einen PKI-Benutzer

PGP-Zertifikate können von PKI-Benutzern nicht verarbeitet werden. Ein PGP-Benutzer ist daher gezwungen selbst ein X.509-Zertifikat für die Kommunikation mit PKI-Benutzern anzulegen. Eine Möglichkeit, PGP-Zertifikate in X.509-Zertifikate zu konvertieren, würde ein so genannter Wrapper bieten, der die einzelnen Felder der unterschiedlichen Zertifikate umwandelt.

Versand eines X.509-Zertifikats an einen PGP-Benutzer

Da X.509-Zertifikate in die PGP-Schlüsselverwaltung aufgenommen werden können, stellt diese Richtung der Kommunikation kein Problem dar.

Kapitel 6 Zusammenfassung und Ausblick

Die Untersuchungen der Sicherheitsmodelle in dieser Arbeit zeigen, dass die Verwendung einer PKI für E-Commerce-Anwendungen besonders gut geeignet ist. Besonders die transparente Authentifizierung ist ein großer Vorteil bei der Verwendung von X.509-Zertifikaten. Durch die Integration in den verbreiteten Betriebssystemen Windows und Unix ist eine einfache Bedienung sowohl im Bereich des E-Mail-Austauschs als auch bei Internet- bzw. Intranet-Anwendungen bei den meisten potentiellen Kunden gegeben. Gerade die Verwendung von Zertifikaten für die sichere Kommunikation zwischen dem Web-Server bei einem Händler und dem Browser beim Kunden ist im E-Commerce besonders wichtig. Hier kommen Protokolle wie Secure Sockets Layer (SSL) und Transport Layer Security (TLS) zum Einsatz. Da von PGP diese Funktion bisher noch nicht erfüllt werden kann, wird es im E-Commerce noch nicht eingesetzt. Zum Zeitpunkt der Erstellung der Arbeit wird bereits an einer Integration von PGP in das TLS-Protokoll gearbeitet, damit könnte die Attraktivität von PGP für E-Commerce steigen.

Eine besonders elegante Lösung würde die Verwendung von SPKI/SDSI darstellen, bei der die Kunden von jedem Händler jeweils ein eigenes Zertifikat erhalten. Händler behalten die Entscheidungsgewalt darüber, ob sie einem Kunden Vertrauen schenken oder nicht, da sie die Zertifikate selbst erstellen. Im Gegensatz zu PKIs ist die Erstellung von Zertifikaten unter SPKI/SDSI wesentlich einfacher und somit günstiger. Vor allen Dingen Anwendungen, in denen anonyme Transaktionen verlangt werden, können mit Gruppenzertifikaten in SPKI/SDSI einfach implementiert werden.

SPKI/SDSI befindet sich allerdings noch im Forschungsstadium und daher ist eine Verwendung noch nicht möglich. Ziel sollte es sein, ein SPKI/SDSI-Plugin zu entwickeln, das in die gängigen Browser integriert werden kann. Dieses Plugin sollte die Verwaltung der SPKI/SDSI-Zertifikate transparent gestalten, so dass der Benutzer von einer einfachen Bedienung ausgehen kann. Auch für die gängigen Web-Server muss ein Plugin entwickelt werden, das dem Administrator eine einfache Verwaltung von Zugriffsrechten ermöglicht.

Die Verwendung von PGP ist aufgrund des etwas komplizierteren Schlüsselkonzepts bei Endkunden nicht so stark verbreitet. Im Gegensatz zu X.509-Zertifikaten müssen Schlüssel vom Benutzer meist einzeln für gültig und vertrauenswürdig erklärt werden. Daher wird PGP (noch) hauptsächlich von Computerkundigen verwendet, die sich die Zeit nehmen, sich mit dem Konzept der Schlüsselvalidierung und dem Aussprechen von Vertrauen in PGP zu beschäftigen. Abhilfe schaffen auch in PGP Zertifizierungsstellen (Certification Authority – CA), die seit der PGP-Version 6 unterstützt werden. Diese ermöglichen dem Benutzer mit dem Einstufen eines einzigen Zertifikates (dem der CA) den Zertifikaten einer großen Gruppe von Personen zu vertrauen.

Durch die steigende Anzahl von Meldungen über Sicherheitslücken im Internet sind immer mehr Personen bereit, das Schlüsselkonzept von PGP zu erlernen – zumal eine kostenlose Version von PGP angeboten wird.

Mit Hilfe der ausführlichen Liste der Anforderungen der beteiligten Parteien im E-Commerce, die in Kapitel 2 zu finden ist, können zukünftige Sicherheitsmodelle bzw. –architekturen untersucht und mit den Ergebnissen aus dieser Arbeit verglichen werden.

Literaturverzeichnis

[ArTu00] Aresenault, A., Turner, S.:
Internet X.509 Public Key Infrastructure – Internet Draft.
Reston, VA: Internet Engineering Task Force, PKIX Working Group 2000

[Back99] Back, Adam:
PGP timeline and brief history.
http://www.cypherspace.org/~adam/timeline 1999

[Balt00ca] Baltimore Technologies, plc.:
UniCERT Administrator's Guide – Version 3.1 – Certification Authority.
Dublin. Im Lieferumfang der UniCERT-PKI 2000

[Balt00cao] Baltimore Technologies, plc.:
UniCERT Administrator's Guide – Version 3.1 – Certification Authority Operator.
Dublin. Im Lieferumfang der UniCERT-PKI 2000

[Balt00gw] Baltimore Technologies, plc.:
UniCERT Administrator's Guide – Version 3.1 – Gateway.
Dublin. Im Lieferumfang der UniCERT-PKI 2000

[Balt00ra] Baltimore Technologies, plc.:
UniCERT Administrator's Guide – Version 3.1 – Registration Authority.
Dublin. Im Lieferumfang der UniCERT-PKI 2000

[Balt00rao] Baltimore Technologies, plc.:
UniCERT User's Guide – Version 3.1 – Registration Authority Operator.
Dublin. Im Lieferumfang der UniCERT-PKI 2000

[Balt00tm] Baltimore Technologies, plc.:
UniCERT Administrator's Guide – Version 3.1 – Token Manager.
Dublin. Im Lieferumfang der UniCERT-PKI 2000

[Bran97] Branchaud, Marc:
A SURVEY OF PUBLIC-KEY INFRASTRUCTURES.
Montreal: McGill University 1997

[BSI01] Bundesamt für Sicherheit in der Informationstechnik – BSI:
Für staatliche VS zugelassene abstrahlsichere/-arme Hardware.
(VS = Verschlusssachen)
Bonn. www.bsi.de BSI7206 2001

[Chad94] Chadwick, David:
Understanding X.500 – The Directory.
London: Chapman & Hall (ISBN 0-412-43020-7) 1994

[EFF98] Electronic Frontier Foundation:
Cracking DES: Secrets of Encryption Research,
Wiretap Politics & Chip Design.
Sebastopol, CA: O'Reilly & Associates (ISBN: 1-56592-520-3) 1998

[Elie98] Elien, Jean-Emile:
Certificate Discovery Using SPKI/SDSI 2.0 Certificates.
Cambridge, MA: Massachusatts Institute of Technology 1998

[Fox00] Fox, Dirk:
Gegenüberstellung von E-Mail-Sicherheitslösungen – White Paper.
Karlsruhe: Secorvo Security Consulting GmbH 2000

[Garf94] Garfinkel, Simson:
PGP – Pretty Good Privacy.
Sebastopol, CA: O'Reilly & Associates (ISBN: 1-56592-098-8); 1994;

[Gehm99] Gehmeyr, Andreas:
"Electronic Commerce" – Ein Überblick.
München: Siemens AG, Abt. SBS – E-Commerce 1999

[Götz99] Götz, Tobias:
Secure Socket Layer – Informationen zur Vorlesung.
Berlin: Technische Fachhochschule Berlin 1999

[HBCI00] Bundesverband deutscher Banken e. V. (u.a.):
HBCI – Homebanking-Computer-Interface
Schnittstellenspezifikation, Version 2.2.
www.hbci.de 2000

[ITSEC00] Defence Signals Directorate - Australasian Certification Authority:
Certification Report – Certificate Number: 2000/14
Baltimore Technologies Ltd – UniCERT – Version 3.1.2:
Russell, Canberra: Defence Signals Directorate 2000

[KPS98] Kaufman, Charlie; Perlman, Radia; Speciner, Mike:
Network Security: Private Communication in a Public World
Englewood Cliffs, NJ: Prentice Hall (ISBN: 0-13-061466-1) 1995

[Luck99a] Luckhardt, Norbert:
Pretty Good Privacy – Teil 1: Einstieg in das Web of Trust.
c't Magazin, Heft 12, 212 – 214 (1999)

[Luck99b] Luckhardt, Norbert:
Pretty Good Privacy – Teil 2: Schlüsselfragen und –antworten.
c't Magazin, Heft 13, 208 – 210 (1999)

[Luck99c] Luckhardt, Norbert:
Pretty Good Privacy – Teil 3: Dateibehandlung und geteilte Schlüssel.
c't Magazin, Heft 16, 172 – 175 (1999)

[Mayw00] Maywah, Andrew J.:
An Implementation of a Secure Web Client Using SPKI/SDSI Certificates.
Cambridge, MA: Massachusatts Institute of Technology 2000

[Münc99] Münch, Isabel:
Security Considerations with Electronic Commerce.
Series on IT Security; Volume 10.
Bonn: Bundesamt für Sicherheit in der Informationstechnik 1999

[NAI00a] Network Associates, Inc.:
PGP Desktop Security – Administrator's Guide – Version 7.01.
Santa Clara, CA. Im Lieferumfang des PGP Desktop Security Pakets 2000

[NAI00c] Network Associates, Inc.:
An Introduction to Cryptography.
Santa Clara, CA. Im Lieferumfang des PGP Desktop Security Pakets 2000

[NAI00u] Network Associates, Inc.:
PGP Desktop Security for Windows 95, Windows 98, Windows NT, Windows 2000 & Windows ME – User's Guide.
Santa Clara, CA. Im Lieferumfang des PGP Desktop Security Pakets 2000

[PrEl01] Price, W., Elkins, M.:
Extensions to TLS for OpenPGP keys – Internet Draft.
Reston, VA: Internet Engineering Task Force, TLS Working Group 2001

[RFC821] Postel, Jonathan B.:
RFC821: SIMPLE MAIL TRANSFER PROTOCOL.
Marina del Rey, CA: University of Southern California 1982

[RFC1939] Myers, J., Rose, M.:
RFC1939: Post Office Protocol - Version 3.
Reston, VA: Internet Engineering Task Force, Network Working Grp. 1996

[RFC2045] Freed, N., Borenstein, N.:
RFC2045: Multipurpose Internet Mail Extensions (MIME)
Part One: Format of Internet Message Bodies.
Reston, VA: Internet Engineering Task Force, Network Working Grp. 1996

[RFC2046] Freed, N., Borenstein, N.:
RFC2046: Multipurpose Internet Mail Extensions (MIME)
Part Two: Media Types.
Reston, VA: Internet Engineering Task Force, Network Working Grp. 1996

[RFC2047] Moore, K.:
RFC2047: Multipurpose Internet Mail Extensions (MIME)
Part Three: Message Header Extensions for Non-ASCII Text.
Reston, VA: Internet Engineering Task Force, Network Working Grp. 1996

[RFC2048] Freed, N., Klensin, J., Postel, J.:
RFC2048: Multipurpose Internet Mail Extensions (MIME)
Part Four: Registration Procedures.
Reston, VA: Internet Engineering Task Force, Network Working Grp. 1996

[RFC2049] Freed, N., Borenstein, N.:
RFC2049: Multipurpose Internet Mail Extensions (MIME)
Part Five: Conformance Criteria and Examples.
Reston, VA: Internet Engineering Task Force, Network Working Grp. 1996

[RFC2060] Crispin, M.:
RFC2060: INTERNET MESSAGE ACCESS PROTOCOL –
VERSION 4rev1.
Reston, VA: Internet Engineering Task Force, Network Working Grp. 1996

[RFC2144] Adams, C.:
RFC2144: The CAST-128 Encryption Algorithm.
Reston, VA: Internet Engineering Task Force, Network Working Grp. 1997

[RiLa96a] Rivest, Ronald L., Lampson, Butler:
SDSI - A Simple Distributed Security Infrastructure – Version 1.0.
Cambridge, MA: Massachusetts Institute of Technology 1996

[RiLa96b] Rivest, Ronald L., Lampson, Butler:
SDSI - A Simple Distributed Security Infrastructure – Version 1.1.
Cambridge, MA: Massachusetts Institute of Technology 1996

[RSAP00] RSA Security Inc:
Press Release on September 6, 2000 –
RSA Security Releases RSA Encryption Algorithm into Public Domain.
Bedford, MA. http://www.rsasecurity.com/news/pr/000906-1.html 2000

[Schn96] Schneier, Bruce:
Angewandte Kryptographie.
Bonn: Addison-Wesley (ISBN3-89319-854-7) 1996

[Stra98] Straßer, Markus:
Kapitel 6 – Sicherheit.
Vorlesung „Verteilte Systeme und Kommunikation WS98/99“.
Universität Stuttgart, Fakultät Informatik 1998

[Veri01] VeriSign, Inc.:
VeriSign Security Alert Fraud Detected in
Authenticode Code Signing Certificates.
Mountain View, CA.
http://www.verisign.com/developer/notice/authenticode/index.html 2001

Abbildungsverzeichnis

Tabellenverzeichnis

Index

Erklärung

Hiermit versichere ich, diese Arbeit selbständig verfasst und nur die angegebenen Hilfsmittel verwendet zu haben.

Stuttgart, 30.04.2001

(Jens Musleh)