Konzeption und Umsetzung einer VPN-Lösung mit PKI-Anbindung und Smartcards

Diplomarbeit

Jan Grell

Fachhochschule Bonn-Rhein-Sieg

Sommersemester 2002

Betreut durch

Prof. Dr. Martin Leischner,
Fachhochschule Bonn-Rhein-Sieg

und

Reinhard Ochsenkühn,
T-Systems ISS GmbH

Erklärung

Hiermit versichere ich, dass ich die vorliegende Diplomarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.

Bonn, 15. Juli 2002 _____

0 Inhalt

1 Aufgabenstellung

Gegenstand der Diplomarbeit ist die Umsetzung einer VPN-Lösung mit asymmetrischer Verschlüsselung und Authentifizierung. Dabei fällt ein besonderes Augenmerk auf die Anbindung an eine PKI sowie die Verwendung von Smartcards als Schlüssel- und Zertifikatsträger. Auch die Interoperabilität verschiedener Produkte soll untersucht werden.

Zunächst werden die zugrunde liegenden Techniken in der Theorie betrachtet und anhand einer Anforderungsanalyse sowie einer Marktsichtung ein technisches Konzept erarbeitet.

Der Schwerpunkt liegt bei der anschließenden praktischen Umsetzung des erarbeiteten Konzepts und der Durchführung von zuvor spezifizierten Testfällen.

Zwei Einsatzszenarien für VPN sollen dabei umgesetzt werden: Zum einen soll eine LAN-Strecke (z.B. Wireless LAN) abgesichert und zum anderen eine Wählverbindung (z.B. PPP over ISDN) geschützt werden. In der Praxis findet man diese Konfiguration z.B. bei Telearbeitsplätzen oder Außendienstmitarbeitern.

Für die praktische Umsetzung werden u.a. folgende Produkte in Betracht kommen:

- Netscape iPlanet Certificate Management System
- Baltimore UniCert
- Microsoft Windows 2000 VPN
- Checkpoint VPN-1
- SSH Sentinel VPN Client
- PGPvpn
- GemSAFE Workstation (PKCS#11-Interface zur GPK GemSAFE 8000 / 16000)
- Giesecke + Devrient StarcOS mit "SafeSign" Software
- SECUDE CSP (PSE-Managent als PKCS#11-Plugin / CSP)

2 Grundlagen / Begriffsklärungen

2.1 Verschlüsselung

Grundlage einer vertraulichen Kommunikation sind Verschlüsselungsalgorithmen. Davon gibt es grundsätzlich zwei Arten, die zu unterscheiden sind.

2.1.1 Symmetrische Verfahren

Hierbei wird der gleiche Schlüssel zum Ver- und Entschlüsseln benutzt. Es ist klar, dass dadurch jeder, der den Schlüssel kennt, die Nachricht entschlüsseln kann. Demnach muss der Schlüssel geheim gehalten werden, und darf nur berechtigten Empfängern bekannt sein.

Soll für eine gesicherte Kommunikation symmetrische Verschlüsselung eingesetzt werden, so wird für jede Kommunikationsbeziehung ein eigener Schlüssel benötigt. Die Anzahl der maximal nötigen verschiedenen Schlüssel beträgt bei n Kommunikationspartnern n*(n-1)/2 (= max. Anzahl an Kommunikationsbeziehungen).

2.1.2 Asymmetrische Verfahren

Hier kommen zwei Schlüssel zum Einsatz: Einer zum Verschlüsseln und einer zum Entschlüsseln. Ein Schlüssel wird veröffentlicht (öffentlicher Schlüssel, public key), der andere vom Eigentümer geheim gehalten (privater Schlüssel, private key). Die entsprechenden mathematischen gewährleisten, dass man bei alleinigem Besitz des öffentlichen Schlüssels den privaten Schlüssel nicht oder nur mit erheblichem Aufwand errechnen kann. Heute verfügbare asymmetrische Verfahren erfordern aufgrund ihrer mathematischen Komplexität und der verwendeten Schlüssellänge (z.B. RSA mit 1024 bit) im Vergleich zu den symmetrischen Verfahren (mit Schlüssellängen von z.B. 128 bit) erheblich mehr Rechenzeit.

2.1.3 Hybridverfahren

Aufgrund der benötigten Rechenzeit bei asymmetrischen Verfahren werden oft symmetrische und asymmetrische Verfahren kombiniert. Dies nennt man Hybridverfahren: Zur sicheren Übertragung des geheimen Schlüssels (für die symmetrische Verschlüsselung) wird dieser mittels asymmetrischer Verschlüsselung mit dem öffentlichen Schlüssel des Empfängers verschlüsselt. Nur der Empfänger kann, da nur er den privaten Schlüssel besitzt, den geheimen Schlüssel, und damit diese Nachricht entschlüsseln.

Aus Gründen der Arbeitsgeschwindigkeit wird die weitere Kommunikation symmetrisch mit dem zuvor sicher übertragenen Schlüssel verschlüsselt.

2.2 Virtual Private Networks (VPN)

Virtuelle private Netze (VPN) ermöglichen die sichere Übertragung von Daten über unsichere Netze. So kann ein Unternehmen beispielsweise seine verschiedenen Standorte über das Internet verbinden. Für die Rechner im Firmennetz erscheint das VPN dabei als ein eigenes Netzwerk, so als wären die jeweiligen Router der Standorte per Direktleitung verbunden (in Abbildung 2.1 ist dies der virtuelle Tunnel).

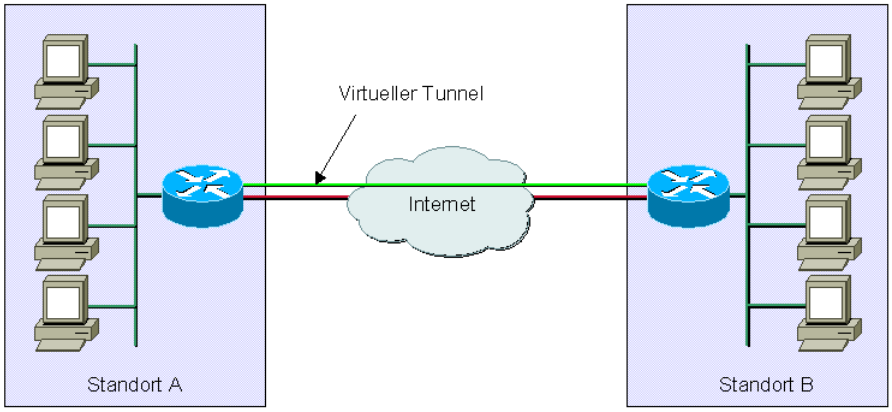

Abbildung 2.1: Verbindung zweier Firmennetze über das Internet

2.2.1 Layer 2 Tunneling-Protokolle

Eine gesicherte Verbindung durch ein unsicheres Netzwerk kann man sich bildlich als Tunnel vorstellen. Für VPN-Verbindungen kommen daher sogenannte Tunnel-Protokolle zum Einsatz.

Das Point-to-Point Tunneling Protocol (PPTP) wurde unter anderem von Microsoft entwickelt. Es stellt eine Erweiterung des Point-to-Point Protocol (PPP) dar, wie es beispielsweise bei Internet-Wählverbindungen zum Einsatz kommt. Eine Besonderheit des PPTP ist die Möglichkeit, neben IP auch nahezu jedes beliebige Layer 3 Protokoll (z.B. IPX) durch den "Tunnel" zu übertragen.

Parallel dazu hat Cisco Systems das Layer 2 Forwarding (L2F) entwickelt. Eine spätere Weiterentwicklung, das Layer Two Tunnel Protocol (L2TP), ähnelt dem PPTP. Die Protokolle L2TP und PPTP findet man beispielsweise bei den VPN-Diensten von Windows 2000.

2.2.2 IP Security (IPSec)

Im Gegensatz zu den eben vorgestellten Protokollen, ist IPSec, das Protokoll für IP Security, auf Schicht 3 im Referenzmodell angesiedelt. Das 1998 entwickelte Protokoll wird in mehreren RFC (Request for Comments) der IETF (Internet Engineering Task Force) definiert. Die drei zentralen Bestandteile des IPSec sind:

- Authentication Header (AH), definiert in [RFC2402]
  Sichert die Integrität der übertragenen Daten; es findet keine Verschlüsselung statt.

- Encapsulating Security Payload (ESP), definiert in [RFC2406]
  Bietet Vertraulichkeit, Integrität und eine Authentifizierung (= Nachweis der Echtheit) der Datenherkunft.

- Internet Security Association and Key Management Protocol (ISAKMP), definiert in [RFC2408] bzw. Internet Key Exchange (IKE), die aktuell verwendete Variante, definiert in [RFC2409]
  Stellt den ersten Schlüsselaustausch einer VPN-Verbindung her, bevor eine IPSec-Verbindung mit ESP oder AH ausgehandelt wird.

Einen Überblick über die Architektur von IPSec gibt [RFC2401].

2.2.2.1 Security Associations

Eine Sicherheitsbeziehung (Security Association, SA) beschreibt die Art der Anwendung von Sicherheitsdienstleistungen in einem Verhältnis zwischen zwei oder mehr Kommunikationspartnern, damit diese sicher kommunizieren können. Dieses Verhältnis wird durch einen Datensatz dargestellt. SA müssen zwischen allen beteiligten Kommunikationspartnern vereinbart werden, damit eine sichere Kommunikation möglich ist. Da SA unidirektional sind, erfordert eine bidirektionale Kommunikation die Einrichtung zweier SA.

Die möglichen Attribute einer SA sind:

- Adresse des Kommunikationspartners
- Authentifizierungsverfahren
- Verschlüsselungsparameter, wie z.B. Algorithmus, Modus der Verschlüsselung, Schlüssellänge, Initialisierungsvektor

Für ISAKMP bzw. IKE und IPSec werden jeweils separate SA etabliert.

2.2.2.2 Abläufe beim Verbindungsaufbau

Beim Verbindungsaufbau sendet der Initiator einer VPN-Verbindung ein ISAKMP-Paket mit Angabe der von ihm unterstützten Verschlüsselungs- und Hashalgorithmen (Proposal). Die Gegenstelle vergleicht nun diese Auflistung mit den eigenen Fähigkeiten und sendet eine Antwort mit dem aus ihrer Sicht besten Algorithmus, der von beiden unterstützt wird. Gibt es keine gemeinsam unterstützten Algorithmen, so wird eine Fehlermeldung versandt und die Einrichtung der Verbindung ist gescheitert.

Beim Einsatz von Zertifikaten für die Authentifizierung werden diese als nächstes übertragen. In einem Certificate Request kann jeder Kommunikationspartner angeben, von welchen Zertifizierungsstellen die zu verwendenden Zertifikate stammen müssen.

Die nachfolgenden Handshake-Pakete sind mit dem gemeinsam unterstützten Algorithmus verschlüsselt. Mit dem ersten verschlüsselten Datenaustausch ist die Phase 1, der sogenannte Main Mode abgeschlossen.

In Abbildung 2.2 ist ein solcher Verbindungsaufbau, der mittels des Netzwerkanalyseprogramms ethereal abgehört wurde, dargestellt. Abbildung 2.3 zeigt den Ablauf vom ersten Handshake bis zur Datenübertragung ins Zielnetz in einem Diagramm.

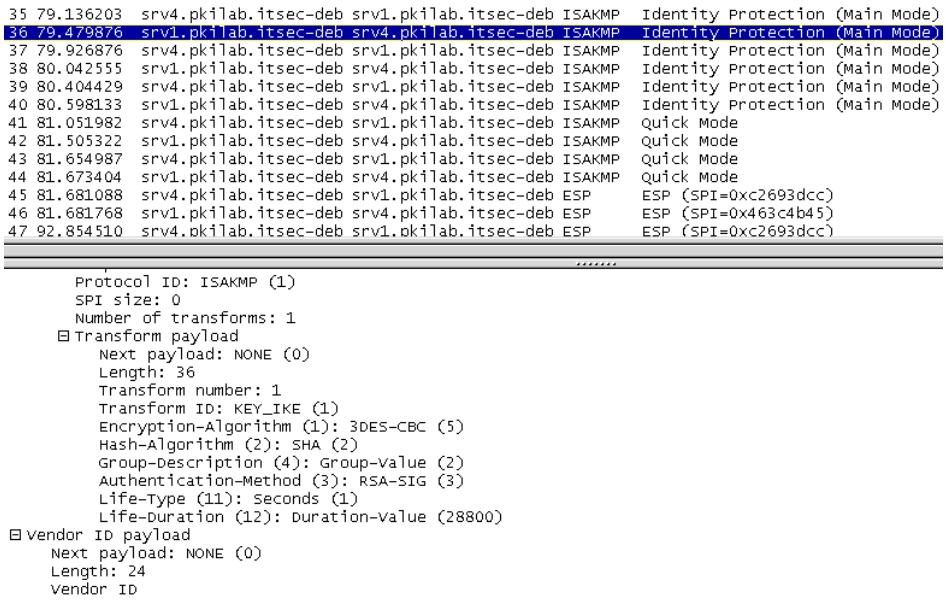

Abbildung 2.2: Mitschnitt eines Verbindungsaufbaus in ethereal

Es folgt mit Phase 2 der sogenannte Quick Mode, bei dem die nachfolgende IPSec Verbindung ausgehandelt wird. Im Anschluß an den Quick Mode folgen die zur IPSec-Verbindung gehörenden ESP- oder AH-Pakete.

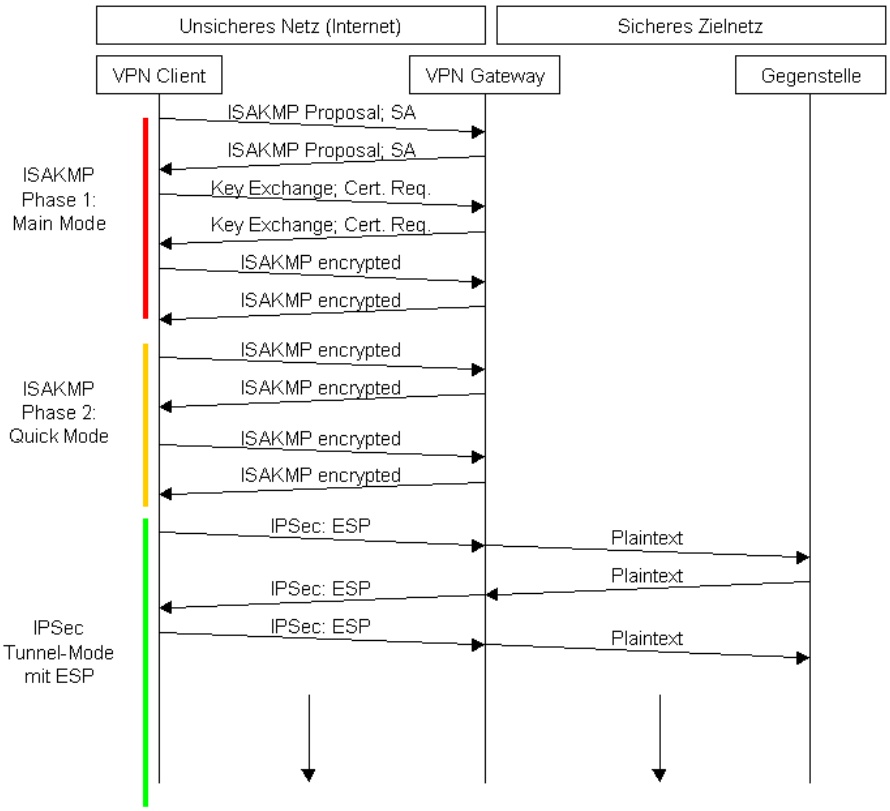

Abbildung 2.3: schematische Darstellung der Einrichtung einer IPSec-Verbindung

Ist die Gültigkeit einer IPSec SA abgelaufen oder eine IPSec SA gelöscht worden, so kann der nächste Handshake zum Aufbau einer IPSec SA über die noch gültige ISAKMP bzw. IKE SA ablaufen. Dadurch wird der neue Verbindungsaufbau erheblich beschleunigt, da nur noch etwa 4 Datenpakete im Quick Mode übertragen werden müssen, bis die SA etabliert ist.

2.2.2.3 Unterscheidung Transportmodus vs. Tunnelmodus

Beim Transportmodus bleiben die IP-Header der einzelnen Pakete erhalten. Lediglich ein IPSec-Header wird angefügt und der Datenteil verschlüsselt. Dadurch ist es einem Angreifer möglich, die Kommunikation auf die Kommunikationspartner und die Datenmenge hin zu untersuchen. Die Nutzdaten bleiben ihm allerdings verborgen. Ein typischer Anwendungsfall wäre die direkte, verschlüsselte Kommunikation zweier Rechner (End-to-End).

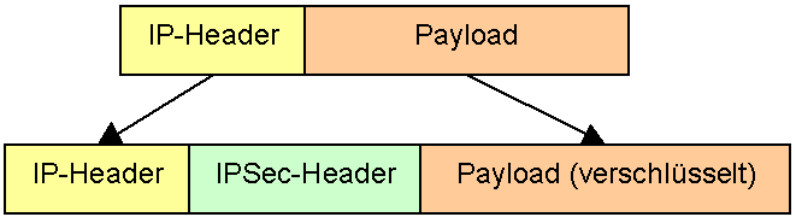

Abbildung 2.4: Kapselung von IP-Paketen beim IPSec-Transportmodus

Im Tunnelmodus wird jedes einzelne IP-Paket komplett verschlüsselt und bekommt einen neuen Header. So können auch die ursprünglichen Headerdaten nicht mehr ausspioniert werden. Es kann vom Angreifer nur festgestellt werden, welche VPN-Gateway Rechner kommunizieren. Die Kommunikationspartner hinter den Gateways bleiben jedoch von außen unerkannt.

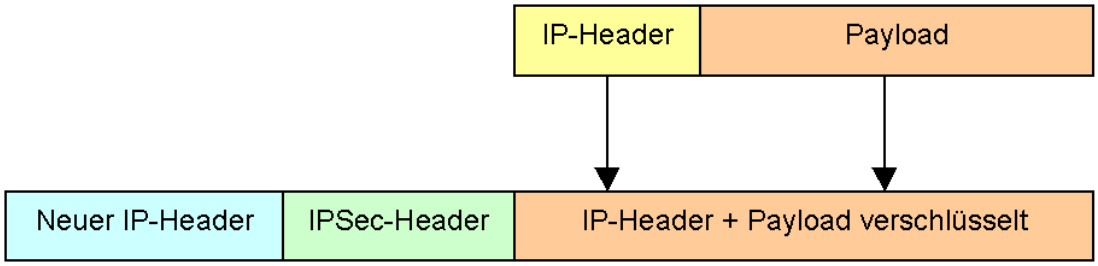

Abbildung 2.5: Kapselung von IP-Paketen beim IPSec-Tunnelmodus

Der in beiden Fällen eingefügte IPSec-Header enthält einen Authentication Header (AH) oder einen Encapsulating Security Payload (ESP) Header. In der Praxis kommt zumeist ESP zum Einsatz, da AH keine Verschlüsselung bietet. AH kann z.B. sinnvoll sein, wenn ein gesetzliches Verschlüsselungsverbot herrscht, aber die Integrität und Authentizität gesichert werden soll.

2.2.3 Einsatzmöglichkeiten

End-to-End (auch Host-to-Host genannt): direkte VPN-Verbindung zwischen den Kommunikationspartnern. Diese Konstellation erfordert den Transportmodus des IPSec. Der Tunnelmodus ergibt hier zum einen unnötigen Mehraufwand und zum anderen keinen Sicherheitsgewinn gegenüber dem Transportmodus.

Abbildung 2.6: End-to-End Verbindung

Gateway-to-Gateway: VPN-Verbindung mehrerer LAN über Gateway-Router. Bei dieser Lösung findet eine Verschlüsselung nur zwischen den Gateways statt, die Kommunikationspartner müssen selbst kein IPSec unterstützen. Hierbei wird der Tunnelmodus des IPSec angewendet.

Abbildung 2.7: Gateway-to-Gateway Verbindung

End-to-Gateway (auch Host-to-Gateway genannt): VPN-Verbindung zwischen einem Gateway und einem extern angesiedelten Kommunikationspartner. In der Praxis kann diese Konfiguration z.B. bei Firmen eingesetzt werden, deren Außendienstmitarbeiter sich in das Firmennetz einwählen oder über das Internet verbinden. Gemäß [RFC2401] ist hier ebenfalls der Tunnelmodus anzuwenden, da bei Anwendung des Transportmodus nur der direkte Verkehr vom externen Anwender zum Gateway und nicht der Verkehr vom Anwender ins Zielnetz gesichert wäre.

Abbildung 2.8: End-to-Gateway Verbindung

2.3 Public Key Infrastrukturen (PKI)

Für den Ablauf einer sicheren Kommunikation gibt es drei zentrale Sicherheitsziele:

- Integrität (Nachricht soll unverändert den Empfänger erreichen)
- Authentizität (Herkunft der Nachricht eindeutig sicher stellen)
- Vertraulichkeit (nur berechtigte Personen dürfen die Nachricht lesen können)

2.3.1 Digitale bzw. elektronische Signatur

Die Ziele Integrität und Authentizität werden mittels digitaler Signatur erreicht. Dazu erstellt der Sender eine Prüfsumme mittels einer sogenannten Hashfunktion (auch als *hashen* bezeichnet). Diese Prüfsumme signiert er dann mit seinem privaten Schlüssel (beim RSA-Verfahren entspricht dies einer Verschlüsselung). Zur Feststellung der Integrität der Nachricht entschlüsselt der Empfänger die Prüfsumme mit dem öffentlichen Schlüssel des Senders (Authentizität wird erreicht, da nur der Inhaber des privaten Schlüssels signiert haben kann) und vergleicht sie mit der Prüfsumme, die er selbst aus der Nachricht erstellt hat. Bei Übereinstimmung kann der Empfänger sicher sein, die Nachricht unverändert empfangen zu haben.

Die Begriffe "digitale Signatur", "elektronische Signatur", "elektronische Unterschrift" sind als Synonyme zu sehen. Mit der Inkraftsetzung der neuen Fassung des Signaturgesetzes wird im Signaturgesetz konformen Umfeld vor allem der Begriff "elektronische Signatur" verwendet.

2.3.2 Digitale Zertifikate

Zur Dokumentation einer Zuordnung von Person und öffentlichem Schlüssel werden sogenannte Zertifikate eingesetzt. Diese sind nach [X509] standardisiert und enthalten neben einigen weiteren Angaben einen öffentlichen Schlüssel und den Namen des Inhabers. Diese Informationen sind von einer Zertifizierungsstelle digital signiert. Abbildung 2.9 zeigt die Ansicht eines Zertifikats im Programm Netscape Communicator.

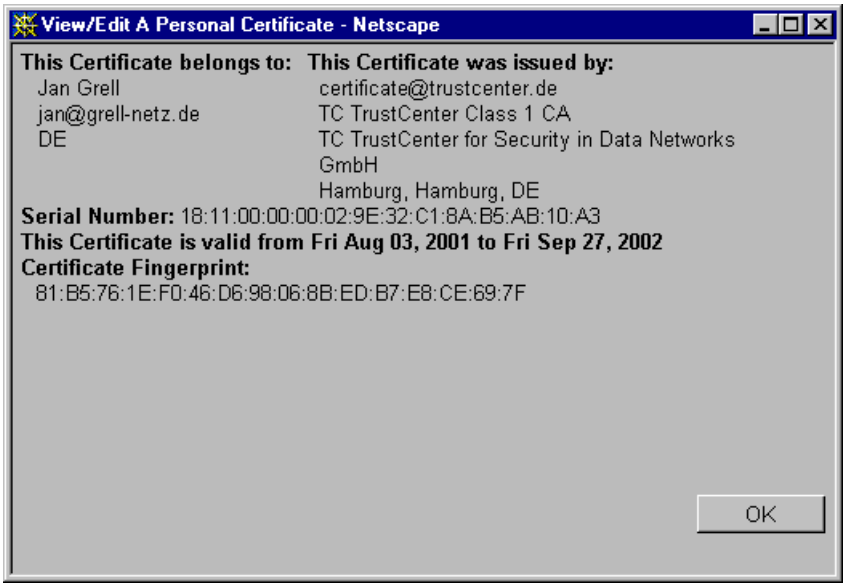

Abbildung 2.9: Ansicht eines Zertifikats im Netscape Communicator

2.3.3 Komponenten einer PKI

2.3.3.1 Certification Authority (CA)

Zentrales Organ einer PKI ist die Zertifizierungsstelle (engl.: Certification Authority, CA). Sie nimmt Zertifizierungsanfragen entgegen, überprüft diese, stellt ihren Benutzern digitale Zertifikate aus und verwaltet Statusinformationen aller Vorgänge.

2.3.3.2 Registration Authority (RA)

Für die Registrierung der Benutzer einer PKI sind die Registrierungsstellen (engl.: Registration Authorities, RA) zuständig. Die Registrierungsstelle ist verantwortlich für die korrekte Identifizierung des Antragstellers.

2.3.3.3 Verzeichnisdienst (Directory Service)

Meist direkt an die CA gekoppelt, beinhaltet eine PKI einen Verzeichnisdienst zur Veröffentlichung der Zertifikate und Sperrlisten. Im Normalfall ist dies ein X.500 kompatibler Server, der das LDAP (Leightweight Directory Access Protocol) bereit stellt. Nach [X500] werden Einträge im Verzeichnisdienst in einer Baumstruktur abgelegt. Die einzelnen Knoten bezeichnen einzelne Elemente, die jeweils durch einen eindeutigen Namen (Distinguished Name, DN) bezeichnet werden. Ein DN setzt sich aus allen Knotenbezeichnern zusammen, die zwischen der Wurzel und dem Element liegen, das er bezeichnet. Die einzelnen Bestandteile eines DN sind Informationen der Form "Attribut = Wert", wobei die Attribute im sogenannten LDAP-Schema definiert werden. Für LDAP Version 2 legt [RFC2587] ein Schema für die Benutzung mit Zertifikaten nach X.509 fest.

2.3.3.4 End-Entity

Als End-Entities einer CA werden die Anwender und Systeme bezeichnet, die von ihr Zertifikate erhalten.

2.3.4 Schlüsselverwaltung

2.3.4.1 Schlüsselverteilung

Um in der Lage zu sein, anderen Kommunikationspartnern eine verschlüsselte Nachricht zu senden, benötigt man von jedem Empfänger einer Nachricht dessen öffentlichen Schlüssel. Dem Sicherheitsziel der Authentizität entsprechend, muss jeder öffentliche Schlüssel von Zertifizierungsstelle unterzeichnet worden sein. Damit wird belegt, dass der vorliegende Schlüssel auch tatsächlich zu dem mutmaßlichen Empfänger gehört. Der öffentliche Schlüssel der Zertifizierungsstelle muss daher jedem Kommunikationspartner zur Überprüfung dieser Signaturen vorliegen. Dieser wird aus dem Zertifikat der CA entnommen, welches sicher an die Anwender zu verteilen ist. Somit ist jeder Schlüssel einem Zertifikat und damit auch einer End-Entity eindeutig zugeordnet.

Emailprogramme, wie z.B. Microsoft Outlook Express und Netscape Messenger liefern in ihrer Grundeinstellung schon einige Zertifikate von Certification Authorities mit. Bei Netscape sind dies unter anderem Digital Signature Trust Co., Entrust, GTE Cybertrust, GlobalSign, TC TrustCenter, ValiCert und VeriSign. Dieser Liste können weitere Zertifikate von Zertifizierungsstellen frei hinzugefügt werden. Ist das in der eigenen Infrastruktur verwendete Wurzelzertifikat nicht vorinstalliert, so muss es sicher an die End-Entities verteilt werden. Ob ein Zertifikat unverändert vorliegt, kann durch Vergleich der sogenannten Fingerprints (kryptografische Prüfsumme über das Zertifikat) festgestellt werden.

2.3.4.2 Revocation

Ähnlich wie bei Kreditkarten kann es auch bei digitalen Zertifikaten vorkommen, dass sie zurückgerufen (engl.: revoked) werden müssen. Dies ist immer dann nötig, wenn:

- Der private Schlüssel nicht mehr dem Eigentümer alleine bekannt (kompromittiert) ist (hier genügt bereits der Verdacht der Kompromittierung für eine Sperrung!)
- Der private Schlüssel verloren ging (Smart Card verloren oder defekt, Datei gelöscht etc.)
- Der Mitarbeiter das Unternehmen verlässt (weitere Signaturen im Namen der Firma verhindern)
- Angaben im Zertifikat nicht mehr korrekt sind (Name ändert sich etc.)

2.3.4.3 Revocation Checking

Damit nicht allen Benutzern einzeln mitgeteilt werden muss, dass ein Schlüssel bzw. Zertifikat zurückgerufen wurde, gibt es Sperrlisten (Certificate Revocation List, CRL), in denen sämtliche zurückgerufenen Schlüssel aufgeführt sind. Diese Listen werden bei jeder neuen Sperrung aktualisiert. Für die Praxis bedeutet dies, dass der Anwender selbst für die Überprüfung der Gültigkeit eines Zertifikats verantwortlich ist. Insbesondere bei Verschlüsselung und Signaturprüfung ist das betreffende Zertifikat auf Sperrung zu prüfen, da mit einem kompromittierten Schlüssel keine Sicherheit mehr gewährleistet ist.

Für eine verbesserte Aktualität der Statusprüfungen definiert [RFC2560] mit dem Online Certificate Status Protocol (OCSP) ein Verfahren, bei dem die Zertifikatsprüfung durch einen Server erledigt wird.

2.4 Standards & Protokolle

Die nachfolgende Auflistung stellt die für dieses Dokument relevanten Standards vor.

- **IPSec:** IP Security [RFC2401] - [RFC2411]
  Protokolle für die Sicherung von IP-Verbindungen, z. B. zwischen Routern und Workstations
- **ISO 7816:** Der maßgebliche Standard für Chipkarten
- **LDAP:** Leightweight Directory Access Protocol [RFC2559]
  Zugriffsprotokoll für Verzeichnisdienste nach [X500]
- **PKCS:** Public Key Cryptography Standards
  Standards und Protokolle bezüglich PKI von der Firma RSA Security.
  - **PKCS #1:** RSA Cryptography Standard [PKCS1]
  - **PKCS #10:** Certification Request Syntax Standard [PKCS10]
    Definiert das Format einer Zertifizierungsanfrage
  - **PKCS #11:** Cryptographic Token Interface Standard [PKCS11]
    In Windows-Umgebungen in Form eines DLL-Interface; Standard gibt C-Header für bereit zu stellenden Funktionen vor
  - **PKCS #12:** Personal Information Exchange Syntax Standard [PKCS12]
    Definiert ein Format für die Speicherung von Zertifikaten und Schlüsseln in einer Datei.
  - **PKCS #15:** Cryptographic Token Information Format Standard [PKCS15]
    Definiert ein Format zur Speicherung von Zertifikaten und Schlüsseln auf einer Chipkarte.
- **X.500:** Standard für Verzeichnisdienste [X500]
  Definiert eine Struktur für Verzeichnisdienste und die Adressierung von Informationen
- **X.509:** Standard für digitale Zertifikate [X509]
  Definiert die Struktur von digitalen Zertifikaten

2.5 Smartcards als Schlüssel- und Zertifikatsträger

Bei erhöhten Sicherheitsanforderungen empfiehlt sich der Einsatz von Smartcards als Schlüssel- und Zertifikatsträger. Besonders der Schutz von privaten Schlüsseln wird durch Smartcards im Vergleich zur Speicherung auf Festplatte deutlich verbessert. Smartcards mit kryptografischem Prozessor sind in der Lage, selbständig Schlüsselpaare zu generieren und anzuwenden. Durch eine entsprechende Architektur der Karte sind private Schlüssel derart gespeichert, dass sie nicht von außerhalb der Karte ausgelesen werden können, also nur die Anwendung auf der Karte Zugriff darauf hat. So kann, in Verbindung mit einer Eigentümerauthentifizierung (z.B. PIN-Eingabe), eine Nutzung der privaten Schlüssel durch Unbefugte sicher unterbunden werden.

Um das Leistungsvermögen moderner kryptografischer Karten zu verdeutlichen, sind hier zwei Produktbeispiele aufgeführt:

- Gemplus GPK8000
  - ISO 7816 kompatibel
  - Proprietäre Erweiterungen zur Administration der Karte
  - EMV kompatibel
  - DES, 3DES, RSA, DSA
  - RSA Schlüsselerzeugung bis 2048 bit
  - SHA-1 und MD-5 Hashes
  - 7,4 kByte EEPROM
- Giesecke + Devrient StarcOS
  - ISO 7816 kompatibel
  - DES, 3DES, RSA
  - RSA Schlüsselerzeugung bis 1024 bit
  - SHA-1
  - Signaturanwendung ITSEC E4 hoch evaluiert (SigG konform)
  - EMV kompatibel
  - Bis zu 16 kByte EEPROM

3 Konzept

3.1 Anforderungen

Als Beispiel aus der Praxis soll die Realisierung von Telearbeitsplätzen bzw. ans Firmennetz angeschlossene Außendienstmitarbeiter dienen. Für die Firma, die eine solche Lösung umsetzen möchte, ergeben sich eine Reihe von Anforderungen.

Da eine Einwählmöglichkeit oder eine Internetverbindung stets das Risiko der Spionage oder Sabotage der Infrastruktur und Daten einer Firma bergen, müssen diese Zugänge der Situation entsprechend abgesichert werden.

Zum einen muss die Übertragung sämtlicher Daten zwischen externem Endbenutzer und der Firma vertraulich ablaufen, was eine sichere Verschlüsselung voraussetzt. Zum anderen ist nur befugten Personen der Zugriff auf die Daten zu gestatten. Daher ist eine sichere Identifizierung und Authentifizierung vonnöten.

Außerdem ist das Firmennetz gegen Eindringen von außen sowie andere unberechtigte Zugriffe zu schützen. Da die meisten Firmen bereits über eine Internet-Anbindung und oft auch über ein Firewall-System verfügen, soll dies hier nicht ins Detail erörtert werden. Es darf aber nicht vergessen werden, dass ein Internet-Zugang ohne weitere Absicherung jeglichen Gefahren aus dem Internet schutzlos ausgesetzt ist. Zumal die einzusetzenden VPN-Lösungen nur in Kombination mit einer Firewall für das gewählte Szenario sinnvoll sind. Nach [RFC2401] ist in IPSec bereits eine einfache Paketfilterung anhand von Richtlinien (Policies) vorgesehen. Zur Vereinfachung des Beispielszenarios dieser Arbeit wird angenommen, dass das Firmennetz nach außen durch eine entsprechende Firewall geschützt wird und das interne Netz somit als sicher zu betrachten ist.

Natürlich spielen auch die Kosten der Lösung ein Rolle. Zur Einschätzung der zu erwartenden Kosten für eine der vorgestellten Lösungen erfolgt in Kapitel 5 eine Kostenbetrachtung. Ebenso ist das Thema Investitionssicherheit von großer Bedeutung. Daher wird bei der Auswahl der zu testenden Produkte auf die Verwendung von gängigen Standards Wert gelegt, um nicht von einem Hersteller abhängig zu sein.

Für den Anwender, also im angenommenen Fall für den externen Benutzer, steht unter anderem die Benutzerfreundlichkeit im Vordergrund. Im günstigsten Fall soll es für den Benutzer nicht wesentlich komplizierter sein, sich am Firmennetz anzumelden, als es innerhalb der Firma der Fall wäre.

Die hier festgestellten Anforderungen sind zur Übersicht in nachstehender Tabelle zusammengefasst.

Anforderung	**Technisches Hilfsmittel**
Absicherung nach außen	Firewall
Vertrauliche Datenübertragung	Verschlüsselung
Zugriff auf Daten nur für Befugte	Identifizierung + Authentifizierung
Geringe Investitionskosten	Open Source oder vorhandene Hard- / Software
Investitionssicherheit	Einsatz von Standards
Benutzerfreundlichkeit / Transparenz	Verwendung einfach zu bedienender Programme

Tabelle 3.1: Zusammenfassung allgemeiner Anforderungen

3.1.1 Anforderungen an die PKI-Software

Die eingesetzte PKI-Software sollte, um ein Höchstmaß an Interoperabilität zu gewährleisten, Schnittstellen nach gängigen Standards unterstützen. So ist es zwingend erforderlich, dass Zertifikate gemäß [X509] erstellt und verwendet werden. Sofern die End-Entities selbst die Zertifikate beantragen, ist es erforderlich, dass die Request-Syntax nach [PKCS10] verwendet werden kann. Bei zentraler Generierung der Zertifikate muss ein Export nach [PKCS12] möglich sein. Zur späteren Prüfung der Zertifikate wird ein Verzeichnisdienst gemäß [X500] benötigt, in dem die CA ihre Sperrlisten und ausgestellten Zertifikate veröffentlichen kann. Wünschenswert, aber nicht zwingend erforderlich, ist die Unterstützung des Simple Certificate Enrollment Protocol (SCEP), das VPN-Geräten eine automatisierte Beantragung und Installation von Zertifikaten ermöglicht.

Unumgänglich hingegen ist die Möglichkeit, Chipkarten mit Schlüsseln und Zertifikaten ausstellen zu können. Dazu ist vorzugsweise eine Schnittstelle nach [PKCS11], sofern vorhanden, zu verwenden. An diese Schnittstelle sollte die für die eingesetzte Karte passende Software gebunden werden. Steht keine solche Schnittstelle zur Verfügung, so sollte die PKI-Software eigene Treiber und Schnittstellen für Chipkarten und Lesegeräte besitzen. Besteht keine Möglichkeit, direkt von der CA eine Chipkarte ausstellen zu können, so ist der Umweg über die Benutzerschnittstelle eines Web-Browsers mit installierter Schnittstelle zur Chipkarte in Betracht zu ziehen.

Nicht zuletzt ist es erforderlich, dass die von der CA ausgestellten Zertifikate die nötigen Eigenschaften haben, um von den VPN-Geräten akzeptiert zu werden. Hierzu zählen die Arten der Schlüsselverwendung "digital signature" und "key encipherment" sowie die Erweiterungen

"SubjectAlternativeName:DNS", "SubjectAlternativeName:IP" und "ExtendedKeyUsage" in den Einstellungen "IPSec User" und "IPSec Tunnel".

3.1.2 Anforderungen an die VPN-Software

Aus Gründen der Interoperabilität und Flexibilität hat die VPN-Software aktuell gängige Standards zu verwenden:

Für die VPN-Verbindung zwischen Host und Gateway muss IPSec (gem. [RFC2401]-[RFC2411]) zur Anwendung kommen. Laut [RFC2401] ist hierbei die Betriebsart "Tunnel-Mode" zwingend, da die Endgeräte hinter dem Gateway (im abzusichernden Zielnetz) keine VPN-Funktionalität besitzen müssen.

Die Einbindung der Chipkarte als Schlüssel- und Zertifikatsträger soll über eine Schnittstelle nach [PKCS11] erfolgen.

Auch die PKI-Anbindung soll über Standardschnittstellen erfolgen. Es muss über einen Verzeichnisdienst oder ähnliches die Gültigkeit von Zertifikaten überprüfbar sein. Für die Einbindung von Zertifikaten und privaten Schlüsseln sollte neben der Schnittstelle zur Chipkarte eine Importmöglichkeit für Dateien im Format [PKCS12] verfügbar sein. Eine Unterstützung von SCEP zum automatischen beantragen von Zertifikaten ist nicht zwingend erforderlich, dennoch aber wünschenswert.

3.1.3 Anforderungen an die Smartcard

Für die einzusetzenden Chipkarten muss eine zu [PKCS11] konforme Schnittstelle erhältlich sein. Zur Erhöhung der Sicherheit, ist es wünschenswert, wenn alle nötigen Schlüssel von der Karte selbst erzeugt und private Schlüssel von außen nicht ausgelesen werden können. Ebenso sollte die Karte eine Schlüssellänge von 1024 bit für RSA oder länger unterstützen.

3.2 Beispielszenarien

In der Praxis können VPN in der Betriebsart End-to-Gateway beispielsweise für die gesicherte Anbindung von Telearbeitsplätzen oder Außendienstmitarbeitern ans Firmennetz eingesetzt werden. Ebenso ist denkbar, VPN für die Absicherung eines Wireless LAN zu nutzen, da die bei WLAN-Karten vorhandene Verschlüsselung WEP zu unsicher ist.

3.3 Marktsichtung

Zur Auswahl der zu testenden Produkte wurde eine Marktsichtung durchgeführt. Anhand der Produktbeschreibungen der Hersteller erfolgte eine Vorauswahl, die mittels einer Kriterienliste eingegrenzt wird. Diese Eingrenzung ist nötig, da aufgrund des zeitlichen Rahmens dieser Diplomarbeit nicht beliebig viele Testfälle durchführbar sind.

Die nachfolgenden Tabellen enthalten Argumente, die für oder gegen den Einsatz des jeweiligen Produkts sprechen.

Zwingend erforderlich für die einzusetzenden PKI-Produkte (Zertifizierungsinstanz und Registrierungsstelle) ist die Möglichkeit der Personalisierung von Chipkarten (vorzugsweise PKCS#11), sowie die Möglichkeit des Ausstellens von Zertifikaten für die Verwendungsart "IPSec".

Produkt	**Pro**	**Kontra**
Microsoft Windows 2000 Certificate Services		• PKCS#11 nur via Webbrowser
Baltimore UniCert	• PKCS#11; SCEP; Personalisierung von Chipkarten in der RA möglich	
RSA Keon		• PKCS#11 nur via Webbrowser
iPlanet Netscape Certificate Management System	• CEP	• PKCS#11 nur via Webbrowser
SmartTrust CA		• Nur Cardprinter unterstützt (zu teuer für den Test)

Tabelle 3.2: PKI-Systeme: Auswahlargumente

Die VPN-Produkte (Gateway sowie Client) müssen die Verwendung von Chipkarten als Schlüssel- und Zertifikatsträger unterstützen. Bei den Gateways ist dies nicht erforderlich, da diese in Firmenumgebung gesichert werden können. Weiterhin ist die Anbindung an die PKI zur Prüfung auf Gültigkeit eines Zertifikats wichtig. Absolut unverzichtbar ist die Unterstützung des IPSec-Protokolls.

Produkt	**Pro**	**Kontra**
RSA Keon VPN Client		
Cisco VPN-Concentrator		
Cisco VPN-Client		
SSH Sentinel VPN Client	• PCSC/PKCS#15 Unterstützung • Standardschnittstellen zur PKI • Testversion frei verfügbar	
Microsoft Windows 2000 VPN-Dienste	• Smartcard-Support in Windows integriert	
NCP VPN/PKI	• PC/SC Chipkartenleser • Speziell für PKI-Anbindung	• Nur bestimmte Chipkartentypen, keine Standardschnittstelle
PGPvpn (Bestandteil des Corporate Desktop)	• PKCS#11-Support • Testversion frei verfügbar	
FreeSWAN	• Frei verfügbar	• Zertifikate nach [X509] werden erst nach einem Patch unterstützt. • Keine Schnittstellen wie SCEP oder CMP
CheckPoint VPN-1		

Tabelle 3.3: VPN-Systeme: Auswahlargumente

Für die einzusetzenden Chipkarten muss eine PKCS#11-Schnittstelle verfügbar sein (alternativ direkte Unterstützung durch VPN + PKI).

Produkt	**Pro**	**Kontra**
Gemplus GPK8000-Full	• PKCS#11 via GemSAFE Workstation 3.0	• Müssen für GemSAFE vorpersonalisiert werden (teure Software erforderlich)
Gemplus GPK16000 GemSAFE	• PKCS#11 via GemSAFE	
Aladdin eToken (USB)		• Keine USB-Unterstützung bei Windows NT
TCOS (NetKey)	• PKCS#11 von T-TeleSec	
Giesecke + Devrient StarcOS	• PKCS#11 via SafeSign	

Tabelle 3.4: Smartcards: Auswahlargumente

3.3.1 Auswahl der einzusetzenden Produkte

Die Auswahl der zu verwendenden Produkte basiert rein auf den Angaben der Hersteller.

3.3.1.1 PKI-Systeme

Als Basissystem für die Public Key Infrastruktur wird zum einen das Produkt Baltimore UniCert zum Einsatz kommen, da es im Vergleich zu den übrigen betrachteten Systemen das Ausstellen, bzw. Personalisieren von Smartcards direkt in der RA gestattet und dabei gängige Standards unterstützt.

Als zweiter Kandidat wird das iPlanet Netscape Certificate Management System installiert werden.

3.3.1.2 VPN-Gateway Systeme

Für das VPN-Gateway soll die im Microsoft Windows 2000 Server enthaltene VPN-Funktion näher untersucht werden, da in der Praxis häufig bereits Windows 2000 in Unternehmen vorhanden ist, so dass dies eine relativ preiswerte Alternative darstellen könnte. Als eine andere, möglichst preisgünstige Lösung soll die IPSec-Implementation FreeSWAN unter Linux herangezogen werden.

3.3.1.3 VPN-Client Systeme

Bei den VPN Clients wurden die Produkte SSH Sentinel Internet Pilot in der Version 1.3, PGP Corporate Desktop 7.1.1, sowie die IPSec Komponente von Microsoft Windows 2000 ausgewählt.

3.4 Testspezifikation

3.4.1 Installation

Zu testen ist zuerst der Installationsvorgang der Produkte selbst. Hierbei sollte auf eventuelle Problemfälle bzw. Fehler geachtet werden. Die Installationen sind, wie in 4.1 beschrieben, durchzuführen. Besonderheiten wie "Workarounds" oder Fehlverhalten der Software sind zu dokumentieren.

Dieser Test ist für jedes Produkt separat aufzuführen.

3.4.2 Einrichtung der Testkonfigurationen

Die Einrichtung einer VPN-Testkonfiguration (nach Installation der Produkte) läuft wie folgt ab:

- In den PKI-Systemen werden Zertifikate für die VPN-Komponenten erzeugt:
  - Ein Zertifikat + Schlüsselpaar als PKCS#12 Datei (Alle VPN Gateways verwenden das gleiche Zertifikat, um den Test zu vereinfachen)
  - Je ein Zertifikat + Schlüsselpaar auf Smartcard und als PKCS#12 Datei (Alle VPN-Clients verwenden die gleichen Zertifikate, um den Test zu vereinfachen)
- Installation der CA-Zertifikate auf den VPN-Komponenten, damit diese den Zertifizierungspfad prüfen können
- Einbindung der zuvor erzeugten Zertifikate in den VPN-Komponenten
- Einrichten einer VPN-Verbindung von jedem Client zu jedem Gateway, zunächst mit Authentisierung durch "Shared Secret". Dadurch soll die Basisfunktionalität der VPN-Komponenten sicher gestellt werden. Client-Gateway-Kombinationen, die diesen Test nicht bestehen, werden im Weiteren nicht getestet, da dieser Test die Interoperabilität der Produkte aufzeigt. Funktioniert selbst diese einfachste Form der Authentisierung nicht, so ist davon auszugehen, dass es mit Zertifikaten auch nicht funktionieren wird.

Die nötigen Vorgänge sind kurz zu beschreiben, sowie Besonderheiten zu notieren.

3.4.3 Prüfung der erzeugten Zertifikate

Sind alle nötigen Zertifikate ausgestellt, so sind diese auf Korrektheit zu überprüfen. Dazu wird das Programm Certificate Explorer von fun communications eingesetzt. Es zeigt sämtliche Informationen eines Zertifikats an. Alle Zertifikate müssen dem aktuellen Standard [X509] in Version 3 entsprechen und sollten eine RSA Schlüssellänge von mindestens 1024 bit aufweisen. Die Aussteller- sowie Inhaberbezeichnungen müssen der ursprünglichen Eingabe bei der Registrierung entsprechen. Nach Möglichkeit sollten Erweiterungen wie SubjectAltName oder ExtendedKeyUsage für IPSec Anwendungen enthalten sein.

3.4.4 Prüfung von Verbindungseinrichtung und Verschlüsselung

Mit ethereal, einem Programm zur Netzwerkanalyse, ist zu prüfen, ob in Phase 1 die gewünschten Algorithmen ausgehandelt werden und anschließend eine Verschlüsselung stattfindet.

3.4.5 Prüfung auf Verwendung der Chipkarte

Findet eine Verschlüsselung statt, so muss geprüft werden, ob die Chipkarte auch daran beteiligt ist. Testweise ist eine Datenübertragung mit aktivierter Chipkarte sowie eine Datenübertragung ohne Chipkarte zu versuchen.

Ohne eingesteckte und aktivierte Chipkarte sollte die VPN-Software eine Fehlermeldung erzeugen und die Übertragung von Daten verweigern.

Die Prüfergebnisse sind in einer Tabelle darzustellen.

3.4.6 Prüfung auf Verifizierung der Zertifikate

Die VPN-Einheiten haben jedes zu verwendende Zertifikat mittels der PKI auf Gültigkeit zu überprüfen. Dazu sind verschiedene ungültige Zertifikate zu erzeugen bzw. gültige Zertifikate ungültig zu machen:

- Verwendung eines Zertifikats einer nicht bekannten oder ungültigen Zertifizierungsstelle (Überprüfung des Zertifizierungspfades)
- Verwendung eines noch nicht gültigen Zertifikats (Prüfung der Gültigkeitsdaten)
- Verwendung eines abgelaufenen Zertifikats (Prüfung der Gültigkeitsdaten)
- Verwendung eines zurückgerufenen Zertifikats (CRL-Prüfung)
- Verwendung eines Zertifikats, das nicht für den Verwendungszweck IPSec ausgestellt wurde

In jedem Fall sollte eine VPN-Instanz (Gateway oder Client, je nachdem, wer prüft) einen Fehler melden und den Aufbau einer verschlüsselten Verbindung verweigern.

3.4.7 Recherche nach Sicherheitslücken

Bekannte Sicherheitslücken der eingesetzten Produkte sollen dokumentiert werden. Dazu dienen verschiedene Dienste im Internet, wie z.B. [SecFoc] oder [dCERT].

3.5 Organisatorische Aspekte

Bei der Einführung einer neuen Infrastruktur muss auch immer ein Augenmerk auf die Organisation gelegt werden. Vor der Umsetzung der hier vorgestellten Lösung muss sich das Unternehmen unter anderem folgende Fragen beantworten:

- Wie muss ein bestehendes Sicherheitskonzept angepasst werden?
- Wer bekommt Zugriff von außen?
- Wer verwaltet und administriert die neuen Komponenten? (CA, VPN-Gateway, Clients)
- Wie sollen die Benutzer ihre Zertifikate erhalten? (zentrale Personalisierung der Karten oder jeweils beim Client?)
- Wie erfolgt die Verteilung von Karten und PIN?
- Wer installiert die einzelnen Komponenten?
- Wie werden Schulungen organisiert?

Diese Fragen dienen als grobe Orientierung, was bei der Planung und Konzepterstellung zu beachten ist. Die Auflistung erhebt keinen Anspruch auf Vollständigkeit.

3.6 Restrisiken

Da es nach heutigem Stand der Technik keine hundertprozentige Sicherheit gibt, bestehen auch bei der hier vorgestellten Lösung weiterhin Risiken.

So können z.B. in der Software enthaltene, bisher aber unentdeckte Schwachstellen enthalten sein. Die zuständigen Administratoren müssen also regelmäßig Updates der Hersteller installieren, wenn ein neues Problem bekannt geworden ist. Dies betrifft vor allem die Systeme im Firmennetz mit direktem Kontakt nach außen, wie z.B. Firewall und VPN-Gateway.

Die Firewall könnte beispielsweise so konfiguriert werden, dass Zugriffe von außen nur über eine authentifizierte, verschlüsselte Verbindung zugelassen werden.

Ebenso ist bei den eingesetzten Chipkarten wichtig, dass private Schlüssel nicht die Karte verlassen. Diese ermöglichen den Zugriff auf das Firmennetz und bergen ungeschützt das Risiko des unerlaubten Zugriffs. Bei Chipkartensystemen gibt es verschiedene Angriffsmöglichkeiten, wie das Dokument [Kömmer99] beschreibt. Demnach gibt es bei einigen Prozessoren die Möglichkeit, von

Schwankungen in der Stromaufnahme des Chips auf innere Strukturen bzw. Daten zu schließen. Aber auch einige deutlich aufwändigere Angriffe sind möglich, bis hin zur Zerlegung des Chips, um die inneren Strukturen direkt zu kontaktieren.

Ein weiteres Risiko stellen Computerviren, trojanische Pferde oder andere Schädlinge dar. Diese auch als Malware oder Malicious Code bezeichneten Programme oder Programmteile können beispielsweise Daten auf der Festplatte oder Passwörter ausspionieren. Auch bei Einsatz von Antiviren-Software bleibt hier ein Restrisiko, dass ein Schädling unerkannt bleibt.

4 Umsetzung in die Praxis

4.1 Aufbau der Testumgebung

Für den Aufbau der Testumgebung im Labor stehen 5 PC-Systeme zur Verfügung, auf die wahlweise die zur Verfügung stehenden Betriebssysteme Microsoft Windows NT 4 Workstation, Microsoft Windows 2000 Professional, Microsoft Windows 2000 Server oder SuSE Linux 7.3 Professional installiert werden können. Aus Gründen der Aktualität wird in den meisten Fällen Microsoft Windows 2000 Professional installiert. Die genaue Auflistung der installierten Betriebssysteme ist im Anhang (Kapitel 8) dieses Dokuments zu finden.

Außerdem sind für alle Rechner Chipkartenleser verschiedener Hersteller mit PC/SC Treibern für Microsoft Windows Betriebssysteme verfügbar.

Die Rechensysteme werden so miteinander vernetzt, dass die PKI-Komponenten und der VPN-Client im unsicheren Netz (in der Realität z.B. das Internet) untergebracht sind, und über ein VPN-Gateway (PC mit 2 Netzwerkkarten als Router) mit einem Rechner im sicheren Zielnetz in Verbindung treten können. Auf einem Rechner im unsicheren Netz wird das Programm ethereal zur Netzwerkanalyse installiert. So kann der IPSec Verbindungsaufbau überprüft werden.

In einem zweiten Szenario wird ein Client via ISDN Wählverbindung mit dem Gateway verbunden. So soll ein Telearbeitsplatz simuliert werden, der über eine direkte Wählverbindung mit dem Firmennetz verbunden wird. Der Test auf Absicherung der Wählverbindung erfolgt nur bei Produktkombinationen, bei denen die Verschlüsselung über das LAN funktioniert hat.

4.1.1 Aufteilung in Arbeitspakete

4.1.1.1 Aufbau PC-Systeme

Das erste Arbeitspaket besteht aus der Vernetzung aller Systeme mit Ausnahme eines PC in einem LAN-Segment. Der als Gateway vorgesehene PC wird mit einer zweiten Netzwerkkarte ausgerüstet, an die der verbliebene Rechner angeschlossen wird. Er simuliert das sichere Zielnetz.

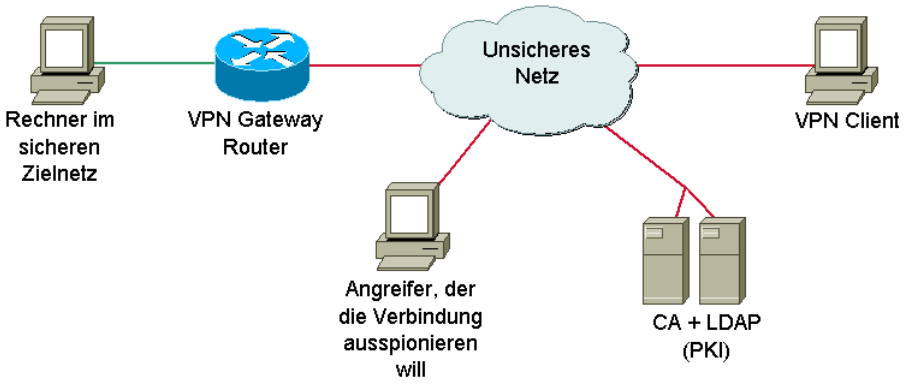

Abbildung 4.1: Vernetzung der Laborumgebung

Im Anschluß daran werden die benötigten Betriebssysteme installiert und mit aktuellen Service Packs bzw. Patches versehen.

4.1.1.2 Einrichtung PKI

Die Installation der PKI-Systeme hat gemäß Produktdokumentation zu erfolgen. Für die Testumgebung wird ein einfaches Namenskonzept gemäß Tabelle 4.1 zum Einsatz kommen.

DN-Bestandteil	**Inhalt**
CN (Common Name)	Bei PKI-Systemen: Produktname Bei VPN-Systemen: Hostname
O (Organization)	"Diploma-Factory" (willkürlich gewählt)
C (Country)	"DE" (Deutschland)

Tabelle 4.1: Namenskonzept für die Testumgebung

Als Schlüssellänge für Zertifikate sind, wenn möglich, 2048 bit zu wählen, ansonsten sollen 1024 bit den Anforderungen genügen.

Um eine Prüfung der Sperrlisten zu ermöglichen, müssen diese zugänglich sein. Eine verbreitete Möglichkeit ist die Veröffentlichung in einem LDAP-Verzeichnis.

Soweit die PKI-Systeme eine direkte Unterstützung für Chipkarten haben, so sind auch die erforderlichen Programme oder Treiber zu installieren.

4.1.1.3 Funktionstest PKI

Um die korrekte Installation der PKI zu testen, werden Testzertifikate ausgestellt. Je nach Möglichkeit der PKI-Systeme werden diese als Datei nach [PKCS12] oder direkt auf eine Smartcard gespeichert. Nach Ausstellen der Zertifikate ist die Veröffentlichung im LDAP-Verzeichnis mittels LDAP-Browser (von [Gawor]) prüfen. Neben den Testzertifikaten sollten sich auch das Wurzelzertifikat und eine Sperrliste im Verzeichnisdienst befinden.

In diesem Schritt können auch alle Zertifikate für die VPN-Komponenten erstellt werden.

4.1.1.4 Einrichtung VPN-Komponenten

Das VPN-Gateway wird ebenso gemäß Produktdokumentation eingerichtet. Es sollen grundlegende Einstellungen zur Realisierung einer IPSec-Verbindung im Tunnelmodus konfiguriert werden. Sofern es das zu installierende Produkt erfordert, sind auch die Wurzelzertifikate der PKI-Systeme zu installieren.

4.1.1.5 Durchführung der Tests

Die Tests werden, wie zuvor spezifiziert, für alle Produkte durchgeführt und samt Ergebnissen in den nachfolgenden Kapiteln dokumentiert.

4.2 Tests

Die Ergebnisse für die zuvor spezifizierten Tests werden im Folgenden zusammengefasst dargestellt.

4.2.1 Installation

Die aufgeführten Konfigurationen sind im Kapitel 8 (Anhang) im Detail einzusehen.

4.2.1.1 Baltimore UniCert

Vor der eigentlichen Installation der UniCert CA und RA muss das Oracle Datenbanksystem installiert werden. Das Administrator-Handbuch von Baltimore gibt hierfür jeden Schritt vor. Alle Schritte sind genau nach Anleitung durchzuführen. Für den Test kam der Oracle Enterprise Server in Version 8.1.6i zum Einsatz.

Da aus Platzgründen die Datenbank auf einem anderen System untergebracht wurde, muss auf dem Rechner für das CA-System der Oracle Client separat installiert werden. Auch diese Installation ist Schritt für Schritt im Handbuch erklärt. Ebenso werden kleinere Anpassungen der Datenbanksoftware an UniCert umfassend beschrieben.

Danach wurde noch der iPlanet Directory Server 4.1 installiert. Dieses Produkt stellt den LDAP Verzeichnisdienst für die UniCert CA zur Verfügung.

Bei der anschließenden Installation der UniCert Programmdateien wurden für den Test sämtliche Komponenten ausgewählt, um alle Funktionalitäten zur Verfügung zu haben.

Darauf folgend beginnt die Konfiguration der CA. Hierbei werden Parameter für das Wurzelzertifikat und Einstellungen für den CA-Dienst abgefragt. Ebenso wird der Pfad zur späteren CRL im Verzeichnisdienst angegeben.

Baltimore sieht bei UniCert eine strikte Rollentrennung vor, weshalb nach dem CA-Dienst noch ein CA-Operator (CAO) und mindestens eine RA mit je mindestens einem RA-Operator (RAO) eingerichtet werden muss. Der CAO definiert die eigentliche Struktur der PKI und lässt die Zertifikate für die PKI-Einheiten (RA, RAO) erstellen. Ebenso ist der CAO für die Einrichtung sogenannter Policies verantwortlich. Die Policies sind Eingabemasken mit speziellen Vorgaben, die bei der Beantragung eines Zertifikats zum Einsatz kommen. Diese werden vom RAO zur Erzeugung von Zertifikaten für die End-Entities verwendet.

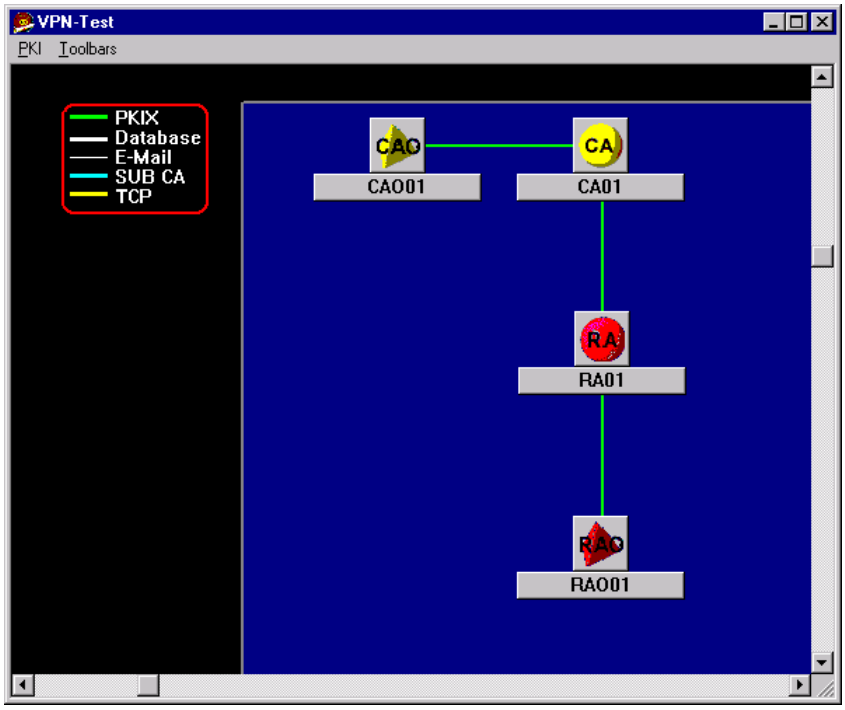

Abbildung 4.2: Definition der PKI-Struktur im UniCert CAO

Für den Zugriff auf Chipkarten enthält die Software von Baltimore einen sogenannten Token Manager. In diesen können mehrere [PKCS11] konforme Chipkartentreiber eingebunden werden, die zuvor eingerichtet sein müssen.

Um mittels RAO eine Chipkarte zu personalisieren, wird eine sogenannte "Customer Security Policy" angelegt, in der als Schlüsselherkunft die Option "PKCS#11 Smartcard" eingestellt wird. Wird diese Policy von einem RAO verwendet, so wird nach Eingabe der Benutzerdaten eine Chipkarte angefordert. Beim Versuch, ein erstes Testzertifikat auf eine Gemplus GemSAFE Karte zu schreiben, stürzte allerdings das RAO-Programm mit einer Fehlermeldung ab (Siehe Abbildung 4.3).

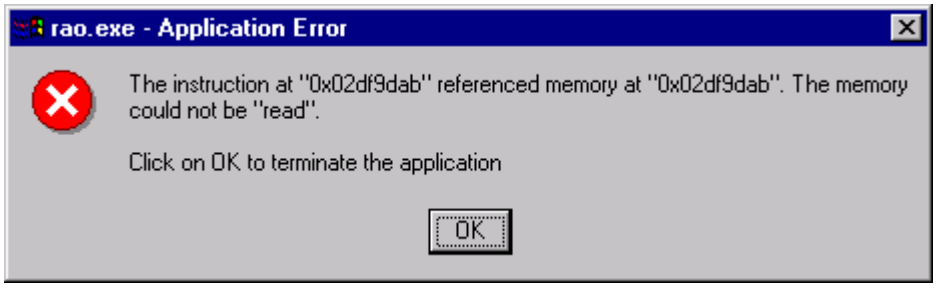

Abbildung 4.3: Fehlermeldung beim Versuch, eine GemSAFE Smartcard zu personalisieren

Da es sich hierbei um ein reproduzierbares Problem handelt, wurde ersatzweise die StarcOS Karte von Giesecke + Devrient mit der Anwendung SafeSign als PKCS#11 Schnittstelle installiert und in die RA eingebunden. Damit funktionierte die Ausstellung eines Zertifikats für die Chipkarte. Allerdings wurde

das Wurzelzertifikat nicht mit auf die Karte kopiert. Das wurde manuell mit dem UniCert Token Manager (im Lieferumfang enthalten) nachgeholt (Siehe Abbildung 4.4).

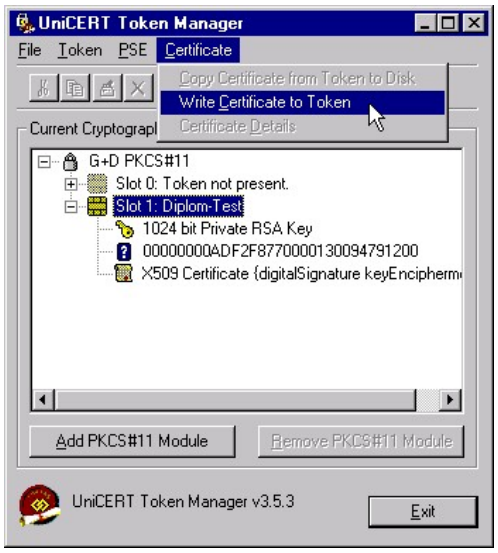

Abbildung 4.4: Ansicht einer StarcOS Smartcard im Baltimore UniCert Token Manager

4.2.1.2 iPlanet Netscape Certificate Management System 4.2

Die Installation des iPlanet Netscape Certificate Management System 4.2 (CMS) unter Linux läuft über ein mitgeliefertes Setup-Programm, das alle benötigten Informationen abfragt und Standardwerte vorgibt. Bei der Testinstallation unter SuSE Linux 7.3 musste lediglich das Paket "termcap" von der SuSE-CD nachinstalliert, sowie eine Datei im Verzeichnis `/usr/lib` kopiert werden.

Nachdem die Installationsdateien entpackt und das Setup-Programm durchlaufen wurden, wird eine CA definiert. Hierbei werden diverse Parameter für CA- und SSL-Server Zertifikat abgefragt. Anders als z.B. Baltimore UniCert ist das CMS komplett mit einem Web-Browser zu bedienen. Die einzige Ausnahme stellt die Konfiguration dar, die durch ein mitgeliefertes Programm namens "Netscape Console" geschieht.

Nach der Grundkonfiguration wird die Veröffentlichung von Zertifikaten in einen Verzeichnisdienst aktiviert. Bei der Einrichtung des sogenannten LDAP-Publishing wird festgelegt, in welchen Teilbaum des Verzeichnisses die Zertifikate abgelegt werden. Dazu können Bestandteile des DN im jeweiligen Zertifikat herangezogen, aber auch Teilpfade fest vorgegeben werden. Die im Test benutzte Konfiguration ist im Anhang dargestellt.

4.2.1.3 Windows 2000 Server (VPN-Dienste)

Da Windows 2000 im Auslieferungszustand, und auch nach Installation des aktuellen Service Pack 2, nur den einfachen DES mit 56 bit Schlüssellänge beherrscht, muss das von Microsoft separat angebotene High Encryption Pack (siehe [MSW2KHE]) installiert werden. Damit wird dann Triple-DES mit 128 bit Schlüsseln unterstützt.

Zur Unterstützung der Routing-Funktionalität wurde das Paket "Routing & RAS" vom Installationsmedium installiert. Zunächst wurde ein normales Routing ohne Verschlüsselung getestet, um die korrekte Installation sicher zu stellen.

Über die Microsoft Management Console kann man mit dem Snap-In "IP Sicherheitsrichtlinien" sämtliche IPSec relevanten Parameter einstellen.

Zunächst wurde eine Richtlinie hinzugefügt. Über einen IP-Filter wurde eingestellt, mit welchen Hosts verschlüsselt kommuniziert werden soll. Als Filteraktion wurde die Option "Sicherheit erforderlich" gewählt. Bei den Einstellungen für die Authentifizierung wurden die Möglichkeiten "Passwort" (Shared Secret) sowie "Zertifizierungsstelle" gewählt. Als gültige Zertifizierungsstellen wurden beide verwendeten Wurzelzertifikate angegeben.

4.2.1.4 FreeSWAN

Die offene IPSec Umsetzung FreeSWAN ist bei der Linux Distribution SuSE 7.3 im Lieferumfang enthalten. Dort vorhandene Version ist bereits mit der Erweiterung zur Unterstützung von Zertifikaten versehen. Für die Konfiguration musste lediglich das Routing aktiviert, sowie die Konfigurationsdateien an die Testumgebung angepasst werden. Diese finden sich im Anhang (Kapitel 8.3).

4.2.1.5 SSH Sentinel Internet Pilot

Die Installation des Internet Pilot erfolgt aus einem selbstextrahierenden Archiv, das der Hersteller im Internet zum Herunterladen anbietet.

Während des Installationsvorgangs werden im Dateisystem zu verwendenden Pfadnamen abgefragt, die Standardvorgabe wurde hier übernommen.

Nach Installation der Programmdateien wird der Anwender aufgefordert, die Maus beliebig zu bewegen. Auf diese Weise sammelt das Programm "echten" Zufall zur anschließenden Schlüsselgenerierung. Danach werden Daten zur Identifizierung des eigenen VPN-Client abgefragt.

Die Standardwerte werden hier auf Hostnamen und Domain der Windows-Installation eingestellt. Optional können weitere Datenfelder (je einmal ou, o, c) gemäß [X500] gefüllt werden.

Im weiteren Verlauf der Konfiguration kann gewählt werden, auf welche Weise ein Zertifikat erzeugt werden soll, wobei der Anwender zwischen "Self Signed" (selbstsigniertes Zertifikat), "CA Online" (mittels SCEP, wie in [Cisco00] beschrieben, oder mittels CMP nach [RFC2510]) und "CA Offline" (Zertifizierungsanforderung gemäß [PKCS10]) wählen kann. Zunächst wurde nur ein selbstsigniertes Zertifikat erzeugt, um unabhängig von den anderen Produkten das Programm in seinen Grundfunktionen zu überschauen.

Im Anschluß an die Zertifikatsanforderung bzw. -generierung führt das Programm selbständig einen Benchmark-Test für die ihm bekannten Verschlüsselungsalgorithmen durch. Hierbei fiel positiv auf, dass SSH bereits den Rijndael AES unterstützt, welcher vom Installationsprogramm automatisch als Standard eingestellt wurde.

Nach dem vom Programm verlangten Neustart des Systems stellte sich heraus, dass das Programm, anders als in der Dokumentation angegeben, im Labor nicht mit Windows NT 4 harmonierte. Es wurde ein virtueller Netzwerkadapter für die IPSec-Anbindung installiert, der nicht startete. Für die weiteren Tests wurde die Installation unter Windows 2000 Professional (Service Pack 2) erfolgreich wiederholt.

Zur Konfiguration stehen dem Anwender nun zwei Programme zur Verfügung: das Key Management Tool "Accession", mit dem sich neben Schlüsseldateien auch Smartcards direkt über PC/SC oder eine Schnittstelle nach [PKCS11] einbinden lassen. Mit dem "Policy Manager" werden Security Associations verwaltet, sowie ein einfacher Paketfilter konfiguriert.

4.2.1.6 PGPvpn

Beim Installationsprogramm des PGP Corporate Desktop 7.1.1 wurde nur die VPN-Komponente sowie weitere für PGP notwendige Bestandteile ausgewählt, um nur die wirklich benötigten Programme verfügbar zu haben.

Nach der Installation der PGP Software wurde im Konfigurationsdialog die DLL-Datei für die PKCS#11-Schnittstelle angegeben. Die Smartcard, bzw. die darauf enthaltenen Zertifikate und Schlüssel konnten sofort in PGPkeys eingebunden werden. Zertifikate, die auf einer Smartcard abgelegt sind, erhalten in der Schlüsselliste von PGPkeys den Zusatz "on Smartcard".

Die Einrichtung einer VPN-Verbindung für den Tunnelmodus erfolgt bei PGP in zwei Schritten: Erst wird das Gateway als "IPSec Gateway" eingerichtet, anschließend wird darunter das "Subnet" konfiguriert (nicht "IPSec Subnet", da die Rechner im "Subnet" keine VPN-Funktionalität besitzen),

das sich hinter dem Gateway verbirgt (Siehe Abbildung 4.5). Dadurch wird ein automatischer Verbindungsaufbau ermöglicht, wenn eines der genannten Subnetze angesprochen werden soll.

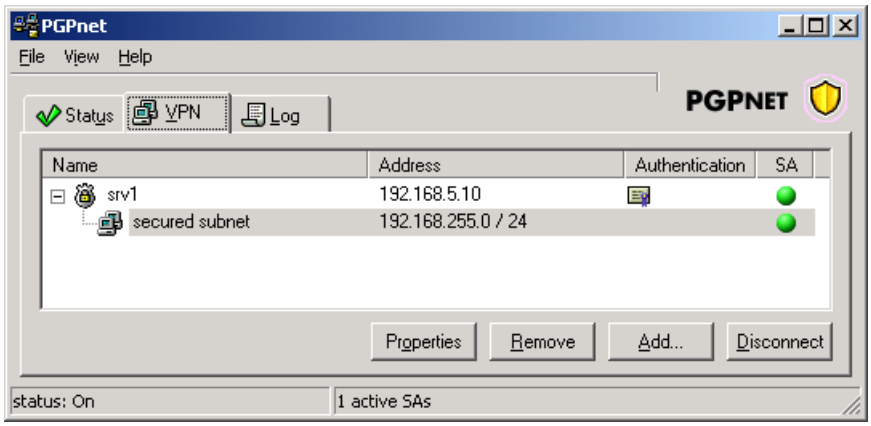

Abbildung 4.5: konfigurierte VPN-Verbindung in PGPnet

4.2.1.7 Windows 2000 Professional (VPN-Client)

Zunächst wurde die Funktion "Netzwerkverbindung hinzufügen" für eine VPN-Gateway Verbindung benutzt, dies schlug allerdings fehl. Wie sich herausstellte, sind VPN und IPSec für Microsoft zwei komplett verschiedene Dinge. Der VPN-Teil von Windows läuft nur mit L2TP oder PPTP, während die IPSec-Verbindungen ausschließlich über die "IP Sicherheitsrichtlinien" eingerichtet werden. Die Einrichtung des IPSec Tunnelmodus stellte sich als recht komplex im Vergleich zu den anderen Produkten heraus. Während für den Transportmodus nur jeweils eine IP Sicherheitsrichtlinie definiert werden muss, sind für den Tunnelmodus zwei Richtlinien je Tunnel nötig, da pro Regel nur ein Tunnelendpunkt definiert werden kann. Nach Konfiguration dieser Richtlinien stellt Windows eine IPSec Verbindung zu entsprechend konfigurierten Hosts bei Bedarf selbsttätig her (Abbildung 4.6). Dies kann mit dem Programm ipsecmon (Abbildung 4.7) überprüft werden. Es zeigt die aktuell etablierten SA mit Parametern an.

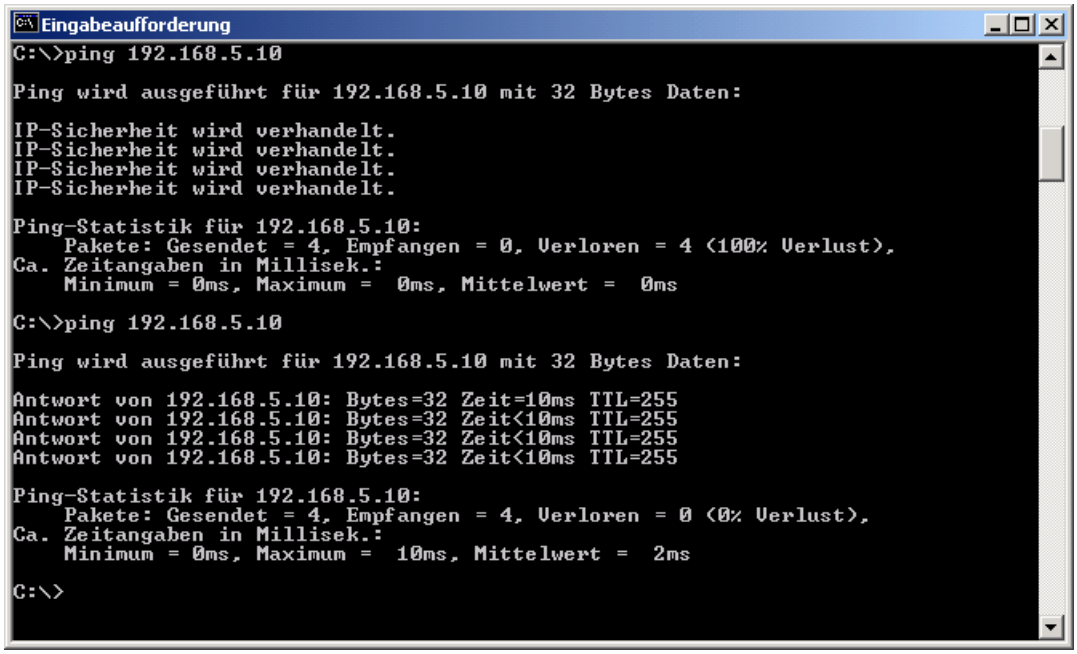

Abbildung 4.6: automatische Einrichtung einer IPSec-Verbindung, ausgelöst durch ping

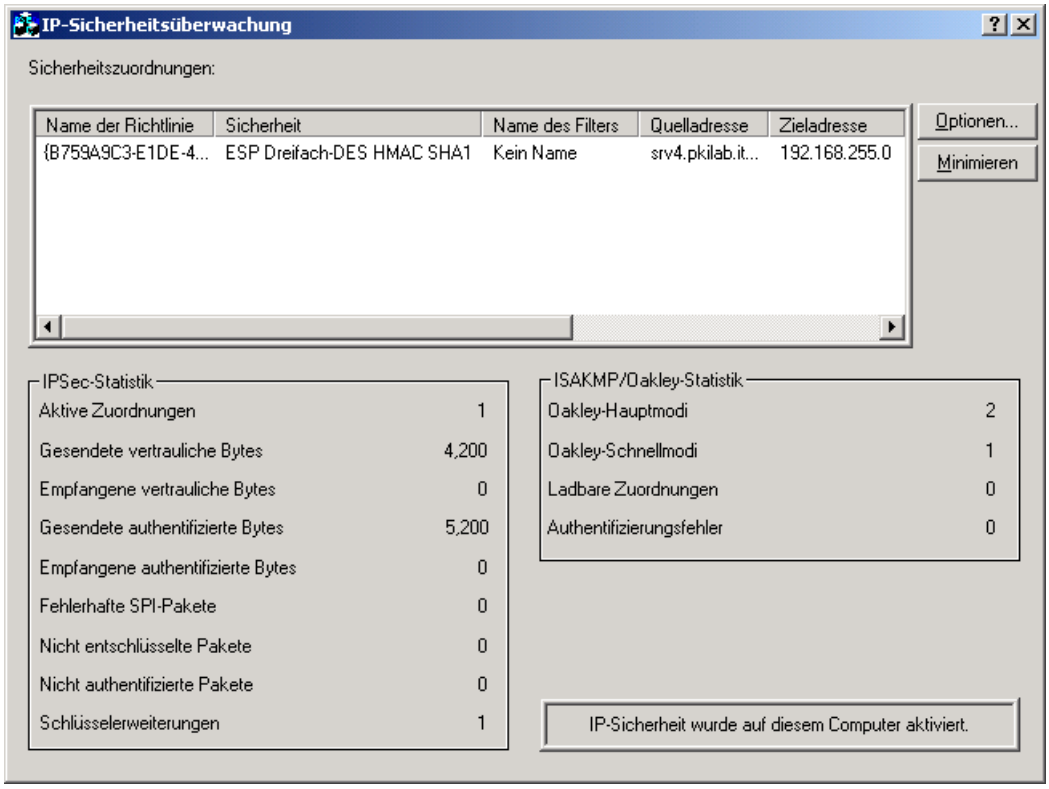

Abbildung 4.7: Darstellung der ausgehandelten SA mit dem Programm ipsecmon von Windows

4.2.2 Prüfung der Authentifizierung

In nachfolgender Tabelle 4.2 ist zusammengefasst dargestellt, welche Kombination von Produkten mit welcher Art der Authentifizierung eine Verbindung herstellen konnte. Die Eintragung "Erfolgreich" bedeutet hier, dass mit der gewählten Authentifizierung eine IPSec-Verbindung im Tunnelmodus aufgebaut werden konnte. Es ist dabei zu beachten, dass die Authentifizierung mittels Smartcard nur auf den Clients durchgeführt wurde. Auf eine Unterscheidung nach Zertifizierungsstellen konnte hier verzichtet werden, da diesbezüglich kein Unterschied festzustellen war.

Client	**Gateway**	**Pre-Shared Key**	**Zertifikat auf Festplatte**	**Zertifikat auf Smartcard**
Windows 2000	Windows 2000	Erfolgreich	Erfolgreich	Nicht unterstützt von Windows2000
Windows 2000	FreeSWAN	Erfolgreich	Erfolgreich	Nicht unterstützt von Windows2000
SSH Sentinel	Windows 2000	Erfolgreich	Erfolgreich	Erfolgreich mit G+D StarcOS GemSAFE erzeugte Absturz
SSH Sentinel	FreeSWAN	Erfolgreich	Erfolgreich	G+D StarcOS: nur "Diagnostics" GemSAFE erzeugte Absturz
PGPvpn	Windows 2000	Abbruch im Quick-Mode	Abbruch im Quick-Mode	Abbruch im Quick-Mode
PGPvpn	FreeSWAN	Erfolgreich	Erfolgreich	Erfolgreich mit G+D StarcOS Mit GemSAFE: "Bad Signature"

Tabelle 4.2: Prüfung: Authentifizierung der VPN Komponenten

4.2.3 Prüfung der Zertifikate

4.2.3.1 Baltimore UniCert

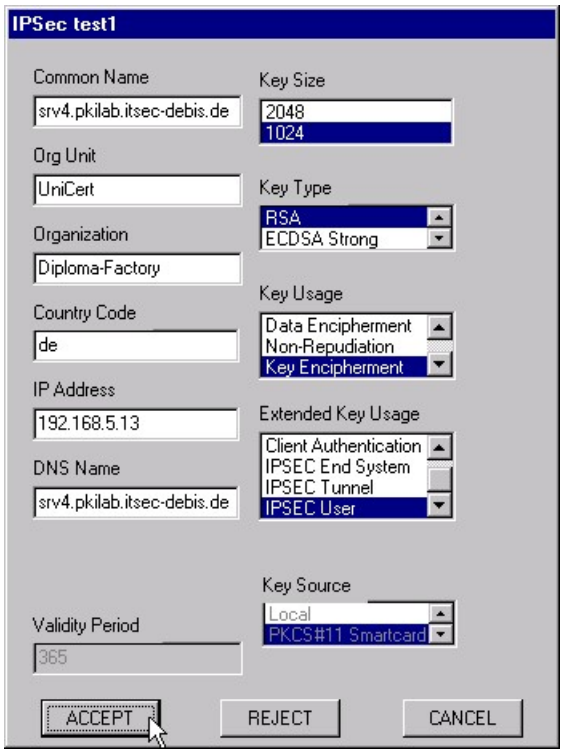

Abbildung 4.8: Beantragung eines IPSec-Zertifikats durch den UniCert RAO

Bei der Überprüfung der Gültigkeitszeiträume neu ausgestellter Zertifikate fiel auf, dass die ausgestellten Zertifikate Start- und Enddaten in einer anderen Zeitzone als der im System konfigurierten enthielten. So wurden neu ausgestellte Zertifikate erst nach zwei Stunden gültig.

Eine nähere Prüfung der Zertifikate mit dem Certificate Explorer von fun communications ergab, dass die aktuelle Systemzeit (nach Mitteleuropäischer Sommerzeit) von UniCert als Zeit nach Greenwich Mean Time (GMT) in das Zertifikat eingesetzt wurde. Statt 12:30 Uhr MESZ, also 10:30 Uhr GMT, stand 12:30 Uhr GMT im Zertifikat. Im Rahmen der Tests konnte die Ursache dieses Fehlers nicht geklärt werden.

Das erstellte Testzertifikat entsprach [X509] in Version 3 und war für ein 1024 bit RSA Schlüsselpaar ausgestellt. Der Gültigkeitszeitraum betrug 365 Tage. Folgende Erweiterungen (Extensions) waren enthalten:

- X509v3 Key Usage : Digital Signature, Key Encipherment
- X509v3 Extended Key Usage : 1.3.6.1.5.5.7.3.6 (OID für IPSec User)
- X509v3 Subject Alternative Name : <IP-Adresse>, <DNS-Name>

4.2.3.2 iPlanet CMS

Bei der Beantragung über das Web-Formular wird je nach Auswahl ein Email- oder SSL-Server-Zertifikat generiert. Das erzeugte Testzertifikat entsprach, wie erwartet, der Version 3 des [X509] Standards. Das für ein 1024 bit RSA Schlüsselpaar ausgestellte Zertifikat war 365 Tage gültig. Folgende Extensions waren gesetzt:

- Netscape Cert Type: <Länge=0>
- X509v3 Key Usage: Digital Signature, Non Repudiation, Key Encipherment
- X509v3 Subject Key Identifier
- X509v3 Authority Key Identifier

4.2.4 Prüfung der Verbindungseinrichtung und Verschlüsselung

Auch wenn einige Produkte bereits den neuen Advanced Encryption Standard AES Rijndael unterstützen, so ist der gemeinsam von allen unterstützte Verschlüsselungsalgorithmus immer noch der Triple-DES und damit das erwünschte Verfahren für die IPSec-Verbindungen. Bei den Hashverfahren wird SHA-1 im Allgemeinen als sicherer eingestuft als MD5, daher ist SHA-1 vorzuziehen. Die nachfolgende Tabelle 4.3 zeigt die jeweils ausgehandelten Algorithmen.

Client	**Gateway**	**Bemerkungen**
Windows 2000	Windows 2000	3DES-CBC; SHA1
Windows 2000	FreeSWAN	3DES-CBC; SHA1
SSH Sentinel	Windows 2000	3DES-CBC; SHA1
SSH Sentinel	FreeSWAN	3DES-CBC; SHA1
PGPvpn	Windows 2000	IKE mit 3DES-CBC; SHA-1 Abbruch im Quick Mode
PGPvpn	FreeSWAN	3DES-CBC; SHA1

Tabelle 4.3: Prüfung der Verbindungseinrichtung und Verschlüsselung

4.2.5 Verwendung der Chipkarte

4.2.5.1 SSH Sentinel Internet Pilot

Ist eine Smartcard via PKCS#11-Plugin im Keymanagement eingebunden und für eine VPN-Verbindung konfiguriert, so wird bei Verbindungseinrichtung nach der Smartcard-PIN gefragt. Nach Eingabe der PIN wird die eingesteckte Smartcard aktiv.

Bei Testverbindungen über einen längeren Zeitraum fiel negativ auf, dass nach ca. 4 Minuten die Verbindung unterbrochen, und erneut die Eingabe der Smartcard PIN verlangt wurde. In der Praxis ist dieses Verhalten nicht tragbar.

Ohne eingesteckte Smartcard versucht SSH Sentinel trotzdem eine Verbindung herzustellen, scheitert dann aber am Signieren während der Authentifizierung mit einer Fehlermeldung.

Wird die Smartcard während einer bestehenden Verbindung entfernt, so bricht die VPN-Verbindung wenige Sekunden später ab.

4.2.5.2 PGPvpn

Bei eingesteckter Smartcard wird der Inhalt der Karte im Schlüsselverwaltungsprogramm PGPkeys verknüpft und kann verwendet werden. Wird die Karte aus dem Lesegerät entfernt, so entfernt PGPkeys die verknüpften privaten Schlüssel aus seiner Liste. Bei einem Verbindungsversuch ergibt sich dann die Fehlermeldung, dass das für die Authentifizierung vorgesehene Zertifikat nicht verwendet werden kann, da kein passender privater Schlüssel gefunden wurde. Die Zertifikate bleiben aber weiterhin in PGPkeys gespeichert.

Soll ein privater Schlüssel der Smartcard z.B. für eine VPN-Verbindung verwendet werden, so fragt PGP nach der PIN der Karte. Anschließend wird die Karte aktiv. Entfernt man die Smartcard während einer bestehenden IPSec-Verbindung aus dem Lesegerät, so bleibt die Verbindung bestehen, bis die ausgehandelte IPSec SA abläuft.

4.2.5.3 Microsoft Windows 2000 Professional

Die Einbindung einer Smartcard in Windows 2000 erfolgt über einen zur Karte passenden Cryptographic Service Provider. Dieser ermöglicht es, Zertifikate der Karte genauso verwenden zu können, wie solche, die auf Festplatte abgelegt wurden. Die automatisch eingebundenen Zertifikate erscheinen im "personal certificate store" des aktuell angemeldeten Benutzers. Für die IPSec Verbindung sucht Windows 2000 seine Zertifikate und privaten Schlüssel jedoch im Zertifikatsspeicher des Computerkontos in der Systemregistrierung (Registry), und damit auf der Festplatte.

> aus [MS249125]: *"[...] The certificate and its private key are stored in the personal certificate store for the computer account.[...]".*

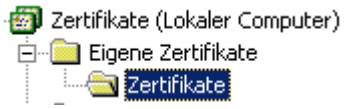

Abbildung 4.9: Zertifikatsspeicher in Windows 2000

Es ist also demnach nicht möglich, für Windows 2000 IPSec-Clients eine Smartcard zu verwenden. Tests im Labor haben dies bestätigt. Über die Management Console wurde das Zertifikat einer Smartcard manuell in diesen "certificate store" kopiert, Windows fand daraufhin den zugehörigen privaten Schlüssel nicht.

4.2.6 Verifizierung der Zertifikate

Für den Test auf ungültigen Zertifizierungspfad wurden jeweils die Wurzelzertifikate gelöscht. Für die vom Datum abhängigen Tests wurde jeweils die Systemzeit der Rechner auf einen Zeitpunkt vor bzw. nach der Gültigkeitsperiode der Zertifikate eingestellt. Dabei fiel auf, dass Zeitdifferenzen zwischen den Systemen nicht geprüft werden. So konnten sich die Uhren von Gateway und Client beispielsweise um ein Jahr unterscheiden und kein Programm hat dies bemängelt.

Für die Prüfung auf Sperrung der Zertifikate wurden die betreffenden Zertifikate nach Abschluß der anderen Tests in der CA gesperrt und eine Sperrliste im zugehörigen Verzeichnisdienst veröffentlicht.

Bei dem Produkt FreeSWAN musste die CRL manuell eingebunden werden, da keine LDAP-Schnittstelle dafür verfügbar ist. Dieses Manko lässt sich allerdings durch Einrichtung einer automatischen Abholung mittels LDAP-Client und dem Programm Cron beheben. Ein passendes Skript ist im Anhang dieses Dokuments zu finden.

Die einzelnen Ergebnisse dieses Tests sind in nachfolgender Tabelle 4.4 dokumentiert.

	FreeSWAN	**Windows 2000**	**PGPvpn**	**SSH Sentinel**
Ungültiger Zertifizierungs-pfad	CA-Zertifikate müssen installiert und gültig sein, sonst Zertifikat ungültig	Windows 2000 benötigt den kompletten Pfad im internen Speicher, sonst Zertifikat ungültig	Keine Pfadüber-prüfung, in PGPkeys muss das Vertrauen selbst konfiguriert werden	Wurzelzertifikat muss als vertrauenswürdig eingerichtet werden und gültig sein
Noch nicht gültiges Zertifikat	Protokolleintrag "Invalid X.509 Certificate" Verbindung kommt zustande	Es kommt keine Verbindung zustande. Aber auch keine Fehlermeldung	Zertifikat wird nicht als ungültig erkannt, es kann normal verwendet werden	Meldung "not trusted" kann übergangen werden, Verbindung kommt zustande
Abgelaufenes Zertifikat	Protokolleintrag "Invalid X.509 Certificate" Verbindung kommt trotzdem zustande	Es kommt keine Verbindung zustande. Aber auch keine Fehlermeldung	Zertifikat wird als abgelaufen angezeigt, kann aber normal verwendet werden	Meldung "not trusted" kann übergangen werden, Verbindung kommt zustande
Zurückgerufenes Zertifikat	CRL muss in FreeSWAN installiert sein, dann korrekte Prüfung. Gesperrte Zertifikate werden nicht verwendet.	Trotz manueller Installation der CRL wird ein gesperrtes IPSec-Zertifikat als gültig angezeigt	CRL-Prüfung konnte nicht aktiviert werden, da nur bestimmte CA-Systeme unterstützt werden.	CA-Zertifikat muss die Erweiterung "CRL Distribution Point" tragen; LDAP muss in SSH eingetragen sein
Kein IPSec-Zertifikat	Keine Prüfung auf IPSec Extensions, Email-Zertifikat genügt	Zweck "IPSec" kann nachträglich gesetzt werden; Email-Zertifikat genügt	Keine Prüfung auf IPSec Extensions, Email-Zertifikat genügt	Keine Prüfung auf IPSec Extensions, Email-Zertifikat genügt

Tabelle 4.4: Prüfung: Test auf Gültigkeit der Zertifikate

4.2.7 Bekannte Sicherheitslücken

4.2.7.1 Baltimore UniCert

In den durchsuchten Quellen wurden keine Sicherheitslücken gefunden.

4.2.7.2 iPlanet Netscape Certificate Management System 4.2

Auf [SecFoc] sind vier Sicherheitslücken in der Windows Version des CMS dokumentiert. Laut iPlanet wurden diese aber mit Erscheinen des Service-Pack 2 behoben.

4.2.7.3 FreeSWAN

In den durchsuchten Quellen wurden keine Sicherheitslücken gefunden.

4.2.7.4 Microsoft Windows 2000

Die Remote Access Services (RAS) von Windows 2000 bieten laut [MS318138] eine Angriffsmöglichkeit über die Telefonbucheinträge der Wählverbindungen. Abhilfe soll ein Update von Microsoft bieten. Relevant ist diese Schwäche nur bei der Verwendung von Wählverbindungen.

Ein weitaus größeres Problem dürfte die in [bug2001] dokumentierte Möglichkeit eines Denial-of-Service Angriffs darstellen. Demnach ist es möglich, durch kontinuierliches Senden von UDP-Paketen an Port 500 (IKE), die größer als 800 Byte sind, das betroffene System zu überlasten. Abhilfe schafft hier ein dem VPN-Gateway vorgeschalteter Paketfilter, der solche schädlichen Pakete verwirft.

4.2.7.5 PGPvpn

In den durchsuchten Quellen wurden keine Sicherheitslücken gefunden.

4.2.7.6 SSH Sentinel Internet Pilot

In den durchsuchten Quellen wurden keine Sicherheitslücken gefunden.

4.3 Test via ISDN

Die in 4.2.2 mit Smartcard erfolgreich verlaufenen Tests werden über eine ISDN Wählverbindung wiederholt. In der Theorie ist hierbei das gleiche Ergebnis zu erwarten, da die verwendeten Protokolle auf dem Internet Protokoll (IP) basieren und bei der Wählverbindung ebenfalls IP eingesetzt wird. Da aber die Erfahrung oft gezeigt hat, dass Theorie und Praxis nicht immer übereinstimmen, wird dies noch getestet.

Am vorhandenen Versuchsaufbau wird dazu im unsicheren Netz ein Rechner mit einer ISDN-Karte als Einwahlrouter konfiguriert. Dieser soll Anrufe der Clients entgegennehmen und die IP-Verbindung zum VPN-Gateway weiterleiten. Im Test wurde dazu unter Linux die ISDN-Einwahl eingerichtet.

Produktkombination	**Ergebnis**
PGP an FreeSWAN	IPSec SA wird wie bei LAN-Verbindung etabliert, Routing ins Zielnetz findet aber nicht statt.
SSH Sentinel an FreeSWAN	Aufgrund manueller Routing-Konfiguration im Test musste der VPN-Client nach Herstellung der Wählverbindung neu gestartet werden, danach IPSec SA etabliert, aber kein Routing ins Zielnetz
SSH Sentinel an Windows 2000	Aufgrund manueller Routing-Konfiguration im Test musste der VPN-Client nach Herstellung der Wählverbindung neu gestartet werden, danach IPSec SA etabliert, aber kein Routing ins Zielnetz

Tabelle 4.5: Testergebnisse bei ISDN-Verbindung

Aus Zeitgründen wurde auf eine detaillierte Fehlersuche beim Routing verzichtet. Da bei allen Tests der Fehler auftrat ist davon auszugehen, dass die Ursache jedoch nicht bei den getesteten Produkte liegt. Es soll an dieser Stelle genügen, dass die IPSec-Verbindung hergestellt wurde.

5 Kosten

Die hier aufgeführten Preise dienen als Orientierung und zur Einschätzung der Einführungskosten einer VPN-Lösung für Unternehmen. Sie geben den aktuellen Stand vom Sommer 2002 wieder. Zusätzlich zu den Hardware- und Lizenzkosten sind ggf. zusätzlich benötigte Administratoren zur Installation und Wartung in Betracht zu ziehen. Ebenso muss das Personal (Administratoren sowie Anwender) in die Technik eingewiesen werden. Für die Administratoren sind je nach Komplexität der Produkte Schulungen über mehrere Tage nötig, wobei der marktübliche Preis für Schulungen bei ca. 1000,- € pro Tag angesiedelt ist. Die Endanwender können dann von den Administratoren firmenintern eingewiesen werden, was etwa einen halben Arbeitstag kosten würde.

Die reinen Anschaffungs- und Lizenzkosten der einzelnen Produkte sind in der nachfolgenden Tabelle 5.1 aufgelistet. Es wurden die vom Hersteller angegebenen Endkundenpreise abgefragt, individuell verhandelbare Preise wurden nicht berücksichtigt.

Produkt	**Preise**
Microsoft Windows 2000 Server	1799,- USD für 25 User 20 User Upgrade 799,- USD
Microsoft Windows 2000 Professional	319,- USD
SuSE Linux Professional	80,- €
iPlanet Netscape CMS (inzwischen von Sun Microsystems als "Sun ONE Certificate Server" erhältlich)	Grundpreis 142,36 €, pro Eintrag + 6,47 €
Sun One Directory Server 5.1 (ehemals Netscape Directory Server)	Grundpreis 260 €, pro Eintrag + 2,59 €
Baltimore UniCert	Core Starter System NT/2000: ca. 71.000,- € 500 User: ca. 11.000,- €
Oracle DB (für Baltimore UniCert erforderlich!)	Lizenz pro CPU: - Standard: 16290 € - Enterprise: 43440 € Lizenz pro Benutzer: - Standard: 326 € - Enterprise : 869 € Support: ca. 22% der Lizenzkosten / Jahr
SSH Sentinel Internet Pilot	Einzellizenz 150,- €; Mengenrabatt gestaffelt bis zu je 50,- € bei 500 Lizenzen
PGP Corporate Desktop	Inzwischen nicht mehr erhältlich, da von Network Associates eingestellt. Teile davon sind in den McAfee E-Business Client übernommen worden.
GemSAFE Workstation 3.0 (Karte, Leser, Treiber)	100,- €
StarcOS Karte + G+D SafeSign	Einzelpreis Karte 56,- €

Tabelle 5.1: Preisübersicht der eingesetzten Produkte (Endkundenpreise)

Folgender fiktiver Fall soll die auftretenden Kosten verdeutlichen. Ein Unternehmen mit vorhandener Internetanbindung und Firewall möchte 100 Mitarbeitern den Zugriff auf das Firmennetz von außen über einen VPN-Tunnel ermöglichen. Die Planungsphase ist in diesem Beispiel mit 20 Arbeitstagen grob geschätzt angegeben. Je nach Benutzerzahl und Firmengröße können sich hier sehr unterschiedliche Werte ergeben. Die angenommene Arbeitszeit bezieht sich auf einen 8-stündigen Arbeitstag und ist in den Geldbeträgen nicht enthalten, da jedes Unternehmen unterschiedliche Stundensätze hat. Die angegebenen Stundenzahlen enthalten alle betroffenen Mitarbeiter, also die Zahl der Arbeitsstunden, die dem Unternehmen durch die Einführung der neuen Infrastruktur "verloren" gehen. Für das VPN-Gateway und die PKI-Systeme werden neue PC-Systeme eingerechnet, während bei den Mitarbeitern ein vorhandener PC mit Windows 2000 angenommen wird.

Nachstehende Tabelle 5.2 zeigt eine Übersicht über die zu erwartenden Kosten.

Posten	**angenommene Anzahl**	**Einzelpreis**	**Gesamtsumme**	**Arbeitszeit [h]**
Planung				160
Schulungstage 2 Administratoren bei den Herstellern	6	1.000,00	6.000,00	48
Installation der PKI-Software durch 1 Administrator				8
Installation VPN-Gateway inkl. Zertifikat				8
Einweisung der Mitarbeiter durch 1 Administrator (3-stündige Einweisung in Gruppen zu 20 MA)				105
Personalisieren der Chipkarten	100			50
Installation der VPN-Software auf den Client PC durch Administrator				100
Lizenzkosten VPN-Gateway (FreeSWAN in SuSE Linux bereits enthalten)	1	-	-	
Lizenzkosten VPN-Clients (SSH Sentinel mit Mengenrabatt)	100	64,00	6.400,00	
Lizenzkosten PKI (iPlanet CMS für 110 Einträge)	1	850,00	850,00	
Kosten Chipkarten inkl. Leser und Treiber	100	100,00	10.000,00	
Anschaffungskosten Betriebssystem für Gateway und PKI (SuSE Linux Professional)	1	80,00	80,00	
Anschaffungskosten PC Systeme für Gateway und PKI	2	1.500,00	3.000,00	
Summen			**26.330,00**	**479**

Tabelle 5.2: Aufstellung zu erwartender Einführungskosten in einem fiktiven Beispiel

Demnach würde die Einführung einer VPN Infrastruktur in diesem Beispiel das Unternehmen rund 27.000,- € zuzüglich ca. 480 Arbeitsstunden kosten. Weiterhin ist im laufenden Betrieb mit Kosten durch Wartungen der Systeme und Erneuerung von Zertifikaten zu rechnen.

6 Fazit

Die Aufgabenstellung konnte gelöst und die Anforderungen aus Kapitel 3.1 erfüllt werden. Durch die Verwendung von PKI und Chipkarten entsteht jedoch ein nicht unerheblicher Aufwand, will man dies komplett selbst verwalten. Dem gegenüber steht ein nicht zu verachtender Gewinn an Sicherheit, da beim Einsatz von Chipkarten sicher gestellt ist, dass die privaten Schlüssel der Anwender nicht ausspioniert werden können. Ebenso erfolgt implizit eine 2-faktor Authentifizierung aus Wissen (Passwort bzw. PIN) und Besitz (Smartcard). Im Gegensatz dazu erfolgt beispielsweise die Speicherung von Pre-Shared Secrets oft im Klartext auf der Festplatte, wo sie leicht ausspioniert werden können.

"Wo Standard drauf steht ist nicht immer Standard drin" - dies ist insbesondere bei der Schnittstelle zur Chipkarte via PKCS#11 festzustellen. Das Beispiel Baltimore UniCert RAO mit der GemSAFE Karte von Gemplus zeigte dies deutlich. In der vorliegenden Version von GemSAFE ist eine im Standard vorgesehene Funktion laut Gemplus nicht enthalten. UniCert wiederum verläßt sich auf den Standard und das Vorhandensein dieser fehlenden Funktion. Daraus folgt der Absturz der Applikation.

Sollte eine eigene Zertifizierungsstelle zuviel Kosten und Aufwand bedeuten, kann sie nötigenfalls an externe Dienstleister ausgelagert werden. Firmen wie z.B. TC Trustcenter oder T-TeleSec bieten virtuelle Trustcenter an, bei denen die Chipkarten gestellt werden. In der Planungsphase ist für eine solche Lösung jedoch zu prüfen, ob die gewählte VPN-Software auch mit den vom Trustcenter gestellten Karten funktioniert. Eine weitere Möglichkeit ist, Smartcards über einen Internetbrowser selbst zu beschreiben, dann genügt die Benutzung einer beliebigen Zertifizierungsstelle, wenn diese via http oder https erreichbar ist. Die Konfiguration der Zugriffsrechte beim VPN-Gateway hängt dabei von der verwendeten CA ab. Wird z.B. eine eigene CA nur für die VPN-Benutzer eingesetzt, so kann das VPN-Gateway einfach sämtliche Zertifikate dieser CA zulassen. Bei Verwendung einer fremden CA muss jedes Zertifikat einzeln als zulässig definiert werden, was je nach Nutzeranzahl recht aufwändig werden kann. In jedem Fall ist eine sorgfältige Planung der Installationen nötig, da eine Vielzahl von Parametern festzulegen ist. Auch sollte die Installation beim Kunden durch Fachpersonal erfolgen, da bereits ein falsch konfigurierter Parameter einen Verbindungsaufbau scheitern lassen kann. Außerdem sollte vor Installation der produktiven Infrastruktur eine Testphase mögliche Probleme aufdecken.

Wenn erst alles installiert und lauffähig ist, so stellt sich eine VPN-Lösung für den Anwender im optimalen Fall nahezu transparent dar. Lediglich die Smartcard muss er in das Lesegerät stecken und die zugehörige PIN eingeben. Der Aspekt der Benutzerfreundlichkeit kann hier also vollkommen als erfüllt angesehen werden, sofern die Installation von einem sachkundigen Administrator vorgenommen wurde.

7 Hilfsmittel

7.1 Quellen

[bug2001] Benutzer "c0redump" der BugTraq Mailing List: UDP DoS attack in Win2k via IKE, http://marc.theaimsgroup.com/?l=bugtraq&m=100774842520403&w=2, 7. Dezember 2001

[Cisco00] Liu, X., Madson, C., McGrew, D., Nourse, A.: Cisco System's Simple Certificate Enrollment Protocol, White Paper, http://www.cisco.com/warp/public/cc/pd/sqsw/tech/scep_wp.htm, Cisco Systems, 3. Juli 2000

[dCERT] T-Systems ISS Computer Emergency Response Team, http://www.dcert.de, Juli 2002

[Fegh98] Feghhi, J., Feghhi, J., Williams, P.: Digital Certificates - Applied Internet Security, Addison-Wesley, September 1998

[FreeSWAN] FreeSWAN Project Homepage, http://www.freeswan.org, April 2002

[Gawor] Gawor, J.: LDAP Browser/Editor, http://www.iit.edu/~gawojar/ldap/, April 2001

[Kömmer99] Kömmerling, O., Kuhn, M. G.: Design Principles for Tamper-Resistant Smartcard Processors, http://www.cl.cam.ac.uk/~mgk25/sc99-tamper.pdf, 1999

[MS249125] Microsoft Corp.: Using Certificates for Windows 2000 and Cisco IOS VPN Interoperation (Q249125), http://support.microsoft.com/support/kb/articles/Q249/1/25.ASP, 31. Juli 2001

[MS252735] Microsoft Corp.: How to Configure IPSec Tunneling in Windows 2000, http://support.microsoft.com/default.aspx?scid=kb;EN-US;q252735, 16. August 2001

[MS318138] Microsoft Corp.: Unchecked Buffer in Remote Access Service Phonebook Could Lead to Code Execution (Q318138), http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-029.asp, Juni 2002

[MSW2KHE] Microsoft Corp.: Windows 2000 High Encryption Pack, http://www.microsoft.com/windows2000/downloads/recommended/encryption/default.asp, 2002

[OSPKI] OpenCA Team: Open Source PKI Book Version 2.4.7, http://ospkibook.sourceforge.net/, 23. Juli 2000

[PKCS1] RSA Laboratories: PKCS #1 v2.0: RSA Cryptography Standard, http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/index.html, 01. Oktober 1998

[PKCS10] RSA Laboratories: PKCS #10 v1.7: Certification Request Syntax Standard, http://www.rsasecurity.com/rsalabs/pkcs/pkcs-10/index.html, 26. Mai 2000

[PKCS11] RSA Laboratories: PKCS #11 v2.1: Cryptographic Token Interface Standard, http://www.rsasecurity.com/rsalabs/pkcs/pkcs-11/index.html, Dezember 1999

[PKCS12] RSA Laboratories: PKCS #12 v1.0: Personal Information Exchange Syntax Standard, http://www.rsasecurity.com/rsalabs/pkcs/pkcs-12/index.html, 24. Juni 1999

[PKCS15] RSA Laboratories: PKCS #15 v1.1: Cryptographic Token Information Format Standard, http://www.rsasecurity.com/rsalabs/pkcs/pkcs-15/index.html, 06. Juni 2000

[RFC2401] Kent, S., Atkinson, R.: Security Architecture for the Internet Protocol, http://www.ietf.org/rfc/rfc2401.txt, November 1998

[RFC2402] Kent, S., Atkinson, R.: IP Authentication Header, http://www.ietf.org/rfc/rfc2402.txt, November 1998

[RFC2406] Kent, S., Atkinson, R.: IP Encapsulating Security Payload (ESP), http://www.ietf.org/rfc/rfc2406.txt, November 1998

[RFC2408] Maughan, D., Schertler, M., Schneider, M., Turner, J.: Internet Security Association and Key Management Protocol (ISAKMP), http://www.ietf.org/rfc/rfc2408.txt, November 1998

[RFC2409] Harkins, D., Carrel, D.: The Internet Key Exchange (IKE), http://www.ietf.org/rfc/rfc2409.txt, November 1998

[RFC2411] Thayer, R., Doraswamy, N., Glenn, R.: IP Security Document Roadmap, http://www.ietf.org/rfc/rfc2411.txt, November 1998

[RFC2510] Adams, C., Farrell, S.: Internet X.509 Public Key Certificate Management Protocols, http://www.ietf.org/rfc/rfc2510.txt, März 1999

[RFC2559] Boeyen, S., Howes, T., Richard, P.: Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2, http://www.ietf.org/rfc/rfc2559.txt, April 1999

[RFC2560] Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, C.: Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP, http://www.ietf.org/rfc/rfc2560.txt, Juni 1999

[RFC2587] Boeyen, S., Howes, T., Richard, P.: Internet X.509 Public Key Infrastructure LDAPv2 Schema, http://www.ietf.org/rfc/rfc2587.txt, Juni 1999

[SecFoc] SecurityFocus.com: Vulnerability Database, http://www.securityfocus.com/corporate/products/vdb, Juli 2002

[SigG] Regierung der Bundesrepublik Deutschland: Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz - SigG), 16. Mai 2001

[sshConf] ssh communications security corp.: SSH Sentinel 1.2 Configuration Examples, April 2002

[sshMan] ssh communications security corp.: SSH Sentinel 1.3 User Manual, 19. April 2002

[X500] ITU-T: Recommendation X.500: Information Technology - Open Systems Interconnection - The Directory: Overview of Concepts, Models and Series, November 1993

[X509] ITU-T: Recommendation X.509: Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, November 1993

[Zimmer99] Zimmer, Tobias: Virtuelle private Netze -- weltweite LANs, http://www.rz.uni-karlsruhe.de/~Tobias.Zimmer/vpn/t15_txt.html, Januar 1999

7.2 Sonstige Hilfsmittel

Laborumgebung:

- 5 PC Systeme
- Betriebssysteme:
  - Microsoft Windows NT 4.0 Workstation
  - Microsoft Windows 2000 Server
  - Microsoft Windows 2000 Professional
  - SuSE Linux Professional 7.3
- 2 AVM Fritz! ISDN Karten (+ ISDN Basisanschluß)
- Chipkartenlesegeräte
  - Towitoko Chipdrive micro
  - Omnikey Cardman 1010
  - Kobil Kaan Standard
- Smartcards mit Verschlüsselungsfunktionen
  - Gemplus GemSAFE 16000 + GemSAFE Libraries 3.0
  - Gemplus GemSAFE 8000
  - Giesecke + Devrient StarcOS v2.3 + SafeSign 1.0.8.4 vom 27. Mai 2002
- Testsoftware
  - SSH Sentinel Internet Pilot 1.3
  - PGP Corporate Desktop 7.1.1
  - Baltimore UniCert 3.5.3 + Oracle Enterprise DB Server 8.1.6i
  - iPlanet Netscape Certificate Management System 4.2
- fun communications Certificate Explorer 1.1

8 Anhang

In der folgenden Tabelle sind die installierten Programme mit zugehörigem Betriebssystem aufgelistet.

Produkt / Komponente	**Betriebsystem**
FreeSWAN 1.91 mit X509 Patch	SuSE Linux 7.3 Professional
Windows 2000 IPSec Gateway	Windows 2000 Server, Service Pack 2, High Encryption Pack
Windows 2000 IPSec Client	Windows 2000 Professional, Service Pack 2, High Encryption Pack
SSH Sentinel Internet Pilot 1.3	Windows 2000 Professional, Service Pack 2
PGP Corporate Desktop 7.1.1 (Teilprogramm PGPvpn)	Windows 2000 Professional, Service Pack 2
Oracle Enterprise DB Server 8.1.6i (für Baltimore UniCert)	Windows 2000 Professional, Service Pack 2
iPlanet Directory Server 4.1 (für Baltimore UniCert; aus dem iPlanet CMS-Paket)	Windows 2000 Professional, Service Pack 2
Baltimore UniCert 3.5.3	Windows NT 4.0 Workstation, Service Pack 6a
iPlanet Certificate Management System 4.2	SuSE Linux 7.3 Professional

Tabelle 8.1: installierte Betriebssysteme

Zur Dokumentation der Versuchsaufbauten sind in den folgenden Abschnitten die Konfigurationen der Systeme dargestellt.

8.1 IP-Adressen

Im Test wurden folgende IP-Adressen verwendet:

- 192.168.5.0/24 ist das unsichere Netz, aus dem der VPN-Client kommt
  - 192.168.5.10 ist das VPN-Gateway zum sicheren Zielnetz
  - 192.168.5.13 ist ein VPN-Client
- 192.168.255.0/24 ist das sichere Zielnetz (in diesem Netz kein VPN-fähiger Rechner)
  - 192.168.255.1 ist das Default-Gateway

8.2 LDAP-Publishing beim iPlanet CMS

Über das Programm "Netscape Console" wird das Konfigurationsfenster für das CMS geöffnet und im Bereich "Certificate Manager / Publishing" werden folgende Parameter eingestellt:

Unter "General:

- "Enable Publishing"
- "Enable Default LDAP Connection"
- "Host Name": 192.168.5.12
- "Port": 389
- "Bind DN": cn=Directory Manager
- "Password": <das zugehörige Passwort>
- "LDAP Version": 3
- "Authentication": Basic Authentication

Unter "Mappers":

- "LdapUserCertMap": cn=$subj.cn, ou=$subj.ou, o=Diploma-Factory, c=de
- "LdapCrlMap": cn=$subj.cn, ou=$subj.ou, o=Diploma-Factory, c=de
  "createCAEntry" = 1
- "LdapCaCertMap": cn=$subj.cn, ou=$subj.ou, o=Diploma-Factory, c=de
  "createCAEntry" = 1

Bevor ein Zertifikat im Verzeichnisdienst veröffentlicht werden kann, muss für den jeweiligen Benutzer bereits ein Verzeichniseintrag existieren, das CMS fügt diesem Eintrag lediglich das Zertifikat hinzu.

8.3 FreeSWAN Konfiguration

Folgende Dateien existieren in der Testkonfiguration:

- `/etc/ipsec.conf` - zentrale Konfigurationsdatei von FreeSWAN
- `/etc/ipsec.secrets` - enthält je nach Konfiguration shared secrets oder private keys
- `/etc/x509cert.der` - enthält das zum privaten Schlüssel gehörende Zertifikat des Gateways
- `/etc/ipsec.d/ca/*` - Zertifikate aller akzeptierten Zertifizierungsstellen im binären Format
- `/etc/ipsec.d/crls/*` - Sperrlisten der Zertifizierungsstellen im binären Format

```
# /etc/ipsec.conf - FreeS/WAN IPsec configuration file

config setup
     interfaces=%defaultroute
     klipsdebug=none
     plutodebug=none
     plutoload=%search
     plutostart=%search
     uniqueids=yes

# defaults for subsequent connection descriptions
conn %default
     keyingtries=1
     keyexchange=ike
     ikelifetime=240m
     keylife=60m
     pfs=no
     compress=no
     authby=rsasig
     type=tunnel
     leftrsasigkey=%cert
     rightrsasigkey=%cert
     left=192.168.5.10
     leftsubnet=192.168.255.0/24

conn srv4
     auto=add
     right=%any
```

Zum automatischen Laden von Sperrlisten aus den Verzeichnisdiensten der Zertifizierungsstellen wurde noch folgendes Shell-Skript entwickelt und im Pfad `/etc/cron.hourly` installiert. Damit werden stündlich die Sperrlisten bezogen und für FreeSWAN aktualisiert.

```
#!/bin/bash

server="192.168.5.12"
caname="CMS-Linux"
basedn="o=Diploma-Factory,c=de"
manager="cn=Directory Manager"
password="********"

# alte ldapsearch-Ergebnisse aus /tmp löschen
rm /tmp/ldapsearch*
# CRL aus LDAP laden und in Datei ablegen (Option -t)
ldapsearch -t -x -b "$basedn" -D "$manager" -h "$server" -w "$password"\
"cn=$caname" "certificaterevocationlist;binary"
# ldapsearch gibt eine oder keine Datei zurück - ist keine vorhanden,
# gibt mv einen Fehler aus
mv /tmp/ldapsearch* /etc/ipsec.d/crls/$caname.crl.bin

server="192.168.5.11"
caname="UniCert"
basedn="o=Diploma-Factory,c=de"
manager="cn=Directory Manager"
password="********"

rm /tmp/ldapsearch*
ldapsearch -t -x -b "$basedn" -D "$manager" -h "$server" -w "$password"\
"cn=$caname" "certificaterevocationlist;binary"
mv /tmp/ldapsearch* /etc/ipsec.d/crls/$caname.crl.bin

ipsec auto --rereadcrls
```

8.4 Konfiguration SSH Sentinel Internet Pilot

Vor der Konfiguration der IPSec-Verbindungen wird die Schnittstelle zur Smartcard eingebunden. Dazu dient das Programm SSH Accession, welches das Schlüsselmanagement übernimmt. Es wird der Pfad zur DLL-Datei der Smartcard Anwendung und ein Bezeichner angegeben. Anschließend wird der neue Eintrag auf "Enabled" eingestellt (Abbildung 8.1). Wird nun eine passende Smartcard in das angeschlossene Lesegerät eingeführt, so stellt Accession die darauf enthaltenen Zertifikate und Schlüssel für den VPN-Client zur Verfügung.

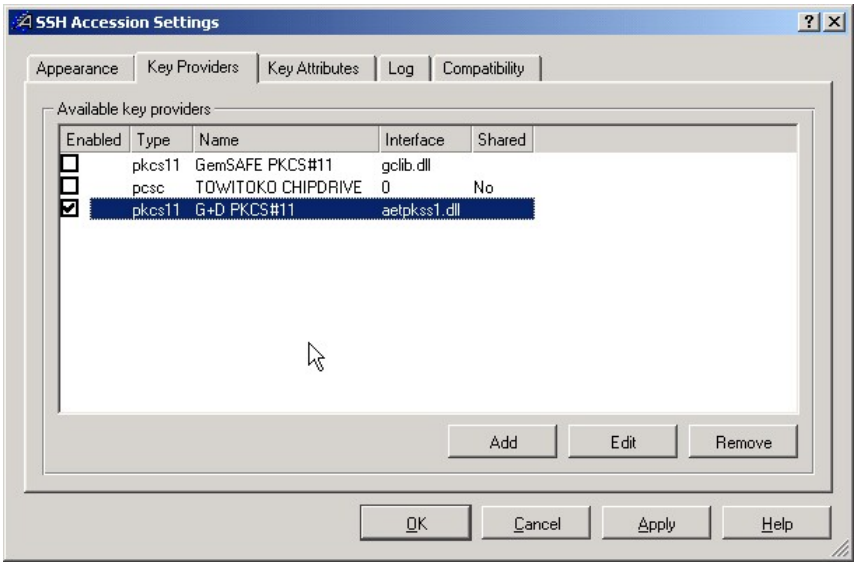

Abbildung 8.1: Einbinden von PKCS#11 Modulen in SSH Sentinel

Anschließend werden die Zertifikate der verwendeten Zertifizierungsstellen im Policy Manager unter "Key Management" / "Trusted Certification Authorities" installiert. Mit einem Klick auch "Übernehmen" werden diese Einstellungen übernommen. Danach kann die erste VPN-Verbindung eingerichtet werden. Dazu werden folgende Parameter eingestellt:

- "Host (IP)": 192.168.5.10
- "Authentication Key": Das Zertifikat der Karte auswählen
- "Proposal type": legacy
  - IKE: 3DES, SHA-1, main mode, group 2
  - IPSec: 3DES, SHA-1, tunnel mode, group 2

8.5 Konfiguration PGP Corporate Desktop

- Globale PGP Optionen / VPN:
  - "Enable VPN Connections"
  - "Setup Keys (IKE)" auf 8 Stunden eingestellt
  - "Primary Keys (IPSec)" auf 1 Stunde eingestellt
- Globale PGP Optionen / VPN Authentication:
  - "Select Certificate" Zertifikat wählen, das zuvor über PGPkeys installiert wurde
- Globale PGP Optionen / VPN Advanced:
  - In den "Proposals" alle Möglichkeiten von "CAST" auf "Triple DES" ändern
- Globale PGP Optionen / Advanced:
  - Bei "Smartcard Support" den Pfad zur DLL-Datei der Smartcard Anwendung eingeben
- PGPnet / neue Verbindung / VPN Gateway
  - IP: 192.168.5.10
  - "Authentication type" = normal
- PGPnet / neue Verbindung / Subnet (Gateway Eintrag markiert)
  - IP: 192.168.255.0, Subnet Mask: 255.255.255.0

8.6 Konfiguration Windows 2000 IP Sicherheitsrichtlinien

Für eine IPSec-Verbindung im Tunnelmodus müssen auf beiden Seiten den Tunnels jeweils zwei Regeln definiert werden. Da diese auf beiden Seiten identisch sind, werden sie hier nur einmal dargestellt. Der einzige Unterschied ist das Computerzertifikat, das für jeden Rechner individuell ausgestellt werden muss. Die Installation eines Computerzertifikats erfolgt über das Management-Console Plugin "Zertifikate (lokaler Computer)" in den Speicher "eigene Zertifikate". Die zugehörigen Wurzelzertifikate werden ebenfalls für das Computerkonto unter "Stammzertifizierungsstellen" installiert.

Der Tunnel wird nun über die "IP-Sicherheitsrichtlinien" konfiguriert. In einer neu anzulegenden Richtlinie werden zwei Regeln definiert:

Regel "gateway zu client":

- IP-Filter (nicht gespiegelt):
  - von 192.168.255.0 / 255.255.255.0 nach 192.168.5.13
  - von 192.168.5.10 nach 192.168.5.13
- Aktion: Sicherheit Erforderlich
- Authentifizierung:
  - Zertifizierungsstelle: CMS-Linux
  - Zertifizierungsstelle: UniCert
- Tunnelendpunkt: 192.168.5.13
- Alle Netzwerkverbindungen

Regel "client zu gateway" (gleiche Einstellungen wie zuvor, mit Ausnahme von):

- IP-Filter (nicht gespiegelt):
  - von 192.168.5.13 nach 192.168.255.0 / 255.255.255.0
  - von 192.168.5.13 nach 192.168.5.10
- Tunnelendpunkt: 192.168.5.10

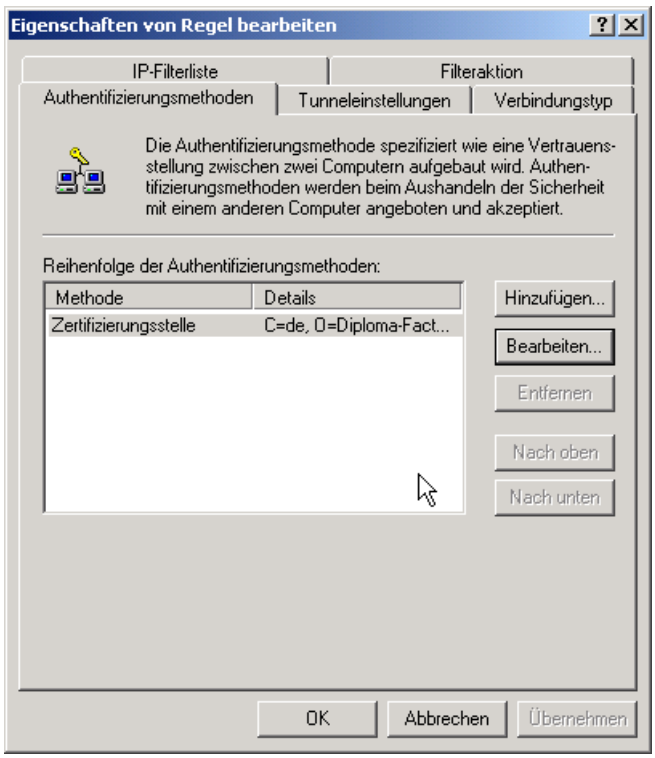

Abbildung 8.2: Konfiguration der Authentifizierung von IPSec in Windows 2000

Damit IP-Pakete vom Client auch ins Zielnetz weitergeleitet werden, muss auf dem Gateway-Rechner noch das Routing aktiviert werden. Beim Windows 2000 Server geschieht dies über das Plugin "Routing und RAS", bei anderen Varianten von Windows kann dies auch durch eine Manipulation der Systemregistrierung erfolgen.

9 Abbildungsverzeichnis

10 Tabellenverzeichnis

11 Stichwortverzeichnis