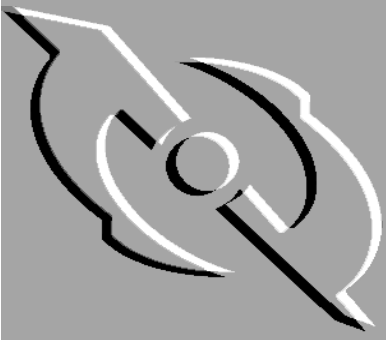


PGP Desktop Security und Personal Privacy

für Windows 95, Windows 98 und Windows NT

Benutzerhandbuch

Version 6.5 Int.

COPYRIGHT

Gedruckt in der EU, PGP, Version 6.5.1 Int, 24-12-99.*

Der Export dieser Software und Dokumentation kann den in bestimmten Abständen durch das Bureau of Export Administration, United States Department of Commerce (Amt für Exportgenehmigungsanträge des Wirtschaftsministeriums der USA) veröffentlichten Vorschriften und Bestimmungen, die die Ausfuhr und die Wiederausfuhr bestimmter Produkte und technischer Daten beschränken, unterliegen.

Network Associates International BV.
Gatwickstraat 25
1043 GL Amsterdam
+31(20)5866100
+31(20)5866101 Fax
http://www.nai.com

info@nai.com

BESCHRÄNKTE GARANTIE

Beschränkte Garantie. Network Associates Inc. garantiert für einen Zeitraum von sechzig (60) Tagen ab Kaufdatum, daß die Software im wesentlichen wie in der schriftlichen Begleitdokumentation beschrieben funktioniert. In dem vom gültigen Recht zugelassenen Maße sind die implizierten Gewährleistungen für die Software, soweit diese existieren, auf die Dauer von sechzig (60) Tagen beschränkt. Einige Rechtsordnungen lassen Beschränkungen der Dauer der gesetzlichen Garantie nicht zu, so daß die obige Beschränkung möglicherweise auf Sie nicht anwendbar ist.

Ansprüche des Kunden. Die gesamte Haftung von Network Associates Inc. sowie von deren Anbietern und Ihr alleiniger Anspruch bestehen nach Wahl von Network Associates Inc. entweder (a) in der Rückerstattung des für die Lizenz bezahlten Preises, falls zutreffend, oder (b) in der Reparatur oder dem Ersatz der Software, die der beschränkten Garantie von Network Associates Inc. nicht genügt und die zusammen mit einer Kopie Ihres Kaufbelegs auf Ihre Kosten an Network Associates Inc. zurückgegeben wird. Diese beschränkte Garantie gilt nicht, wenn der Ausfall der Software auf einen Unfall, auf Mißbrauch oder auf fehlerhafte Anwendung zurückzuführen ist. Für eine Ersatz-Software übernimmt Network Associates nur für den Rest der ursprünglichen Garantiefrist oder für dreißig (30) Tage eine Garantie, wobei der längere Zeitraum maßgebend ist. Außerhalb der USA stehen ohne den Nachweis des Erwerbs von einer autorisierten internationalen Quelle weder diese Ansprüche noch andere Produkt-Support-Dienstleistungen von Network Associates Inc. zur Verfügung und sind unter Umständen nicht von Network Associates Inc. verfügbar, sofern sie den Beschränkungen entsprechend den Exportkontrollgesetzen und -bestimmungen der USA unterliegen.

KEINE WEITERE GEWÄHRLEISTUNG. SOWEIT ES DAS GELTENDE RECHT ZULÄSST, ES SEI DENN, ES IST IN DEN ANGABEN ZUR BESCHRÄNKTEN GARANTIE IN DIESEM DOKUMENT ANDERS VORGESEHEN, WERDEN SOFTWARE UND DOKUMENTATION „OHNE MÄNGELGEWÄHR“ GELIEFERT. NETWORK ASSOCIATES INC. UND DEREN LIEFERANTEN SCHLIESSEN JEDE WEITERE GEWÄHRLEISTUNG UND ALLE ANSPRÜCHE, OB AUSDRÜCKLICH ODER STILLSCHWEIGEND, EINSCHLIESSLICH DER STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN DER HANDELBARKEIT UND DER EIGNUNG FÜR EINEN BESONDEREN ZWECK, DER ÜBEREINSTIMMUNG MIT DER BESCHREIBUNG, DES ANSPRUCHS UND DER NICHT-VERLETZUNG DER RECHTE DRITTER SOWIE DER BEREITSTELLUNG ODER DER NICHT-BEREITSTELLUNG VON SUPPORT-DIENSTLEISTUNGEN, JEDOCH NICHT AUF DIESE BESCHRÄNKT, AUS. DIESE BESCHRÄNKTE GARANTIE GEWÄHRT IHNEN SPEZIFISCHE RECHTE. ES KÖNNEN IHNEN ANDERE ZUSTEHEN, DIE SICH VON RECHTSORDNUNG ZU RECHTSORDNUNG UNTERSCHEIDEN.

BESCHRÄNKTE HAFTUNG. SOWEIT ES DAS GÜLTIGE RECHT ZULÄSST, SIND WEDER NETWORK ASSOCIATES INC. NOCH DIE LIEFERANTEN FÜR IRGENDWELCHE SCHÄDEN, OB INDIREKTE, ZUFÄLLIGE, FOLGESCHÄDEN, KONKRETE ODER EXEMPLARISCHE SCHÄDEN ODER ENTGANGENEN GEWINN (EINGESCHLOSSEN SCHÄDEN AUS ENTGANGENEM GEWINN, BETRIEBSUNTERBRECHUNG, VERLUST VON GESCHÄFTLICHEN INFORMATIONEN ODER DATEN ODER ANDERE FINANZIELLE EINBUSSEN, JEDOCH NICHT AUF DIESE BESCHRÄNKT), DIE AUFGRUND DER BENUTZUNG DIESES SOFTWAREPRODUKTES ODER DER UNMÖGLICHKEIT DER BENUTZUNG ODER DES VERSÄUMNISSES VON SUPPORT-DIENSTLEISTUNGEN ENTSTEHEN, ERSATZPFLICHTIG, SELBST WENN NETWORK ASSOCIATES VON DER MÖGLICHKEIT EINES SOLCHEN SCHADENS UNTERRICHTET WORDEN IST. IN JEDEM FALL IST DIE KUMULIERTE UND GESAMTE HAFTUNG VON NETWORK ASSOCIATES INC. IHNEN ODER JEGLICHEN DRITTEN GEGENÜBER FÜR SÄMTLICHE VERLUSTE ODER SCHÄDEN AUFGRUND VON RECHTSANSPRÜCHEN, FORDERUNGEN ODER HANDLUNGEN, DIE SICH AUS DIESER LIZENZVEREINBARUNG ERGEBEN ODER DAZU IN BEZUG STEHEN, AUF DEN BETRAG BESCHRÄNKT, DEN SIE FÜR DIE LIZENZ BEZAHLT HABEN. DA EINIGE RECHTSORDNUNGEN DEN HAFTUNGSAUSSCHLUSS ODER DIE HAFTUNGSBESCHRÄNKUNG NICHT ZULASSEN, KANN DIE OBIGE BESCHRÄNKUNG FÜR SIE NICHT GELTEN.

Inhalt

Vorwort

Als Bestandteil der Sicherheitswerkzeuge Ihres Unternehmens schützt PGP eines der wichtigsten Güter: *Ihre Daten*. Herkömmlicherweise bewahren viele Unternehmen ihre wichtigen Daten in speziell gesicherten und verschlossenen Räumen auf, zu denen nur Mitarbeiter Zutritt haben, die sich entsprechend ausweisen können. PGP ist ein wertvolles Hilfsmittel, das Sie bei der Gewährleistung der Sicherheit und Integrität der Daten und Nachrichten in Ihrem Unternehmen unterstützt. Die Verletzung der Vertraulichkeit von Informationen hat in den meisten Fällen katastrophale Folgen für die betroffenen Unternehmen.

Zum Thema Netzwerksicherheit und deren Implementierung gibt es eine Vielzahl von Büchern. Im vorliegenden Handbuch wird die Implementierung von PGP als Hilfsmittel zur Sicherung in der gesamten Netzwerkstruktur beschrieben. Obgleich PGP nur einen Teil der Lösung darstellt, ist es für die Sicherheit des gesamten Netzwerksystems von entscheidender Bedeutung. Mit Hilfe von PGP können Sie Ihre Daten verschlüsseln, so daß diese für Unbefugte auch dann vollkommen wertlos sind, wenn sie sich Zugriff auf die verschlüsselten Daten verschaffen. Damit können Sie Ihre Daten wirksam vor den „neugierigen Blicken“ Ihrer eigenen Mitarbeiter und unternehmensfremder Personen schützen.

In diesem Handbuch wird die Verwendung von PGP ® Desktop Security für Windows 95, Windows 98 und Windows NT erläutert. PGP Desktop Security verfügt über viele neue Leistungsmerkmale, die unter „Neue Funktionen in PGP Version 6.5.1“ auf Seite xiv beschrieben werden.

Wenn Sie sich noch nicht näher mit Kryptographie beschäftigt haben und sich einen Überblick über Terminologie und Grundlagen der Anwendung von PGP verschaffen möchten, so finden Sie weitere Informationen im Handbuch *Einführung in die Kryptographie.*

Neue Funktionen in PGP Version 6.5.1

In dieser PGP-Version sind folgende neue Funktionen enthalten:

- **PGPnet** PGPnet ist ein Meilenstein in der Produktgeschichte von PGP. PGPnet sichert sämtliche TCP/IP-Kommunikationsvorgänge zwischen PGPnet selbst und sämtlichen anderen Rechnern ab, auf denen PGPnet ausgeführt wird. Es ist auch voll kompatibel mit der Firewall/dem Gateway von Gauntlet GVPN und liefert durch die Verwendung der IPsec-(Internet Protocol Security) und IKE-(Internet Key Exchange) Protokolle eine vollständige Lösung für Firmenfernzugriffs-VPNs. PGPnet wurde außerdem mit Cisco-Routern (Cisco IOS 12.0(5) oder höher mit IPSec TripleDes Feature Pack), Linux FreeS/WAN 1.0 und vielen anderen erfolgreich getestet. Des weiteren ist PGPnet das erste IPSec-Produkt, das zusätzlich zur Authentisierung mit X.509-Zertifikaten die Verwendung von OpenPGP-Schlüsseln zu Authentisierungszwecken vollständig unterstützt. Weitere Informationen und Anweisungen zur Verwendung von PGPnet finden Sie in Kapitel 8, „PGPnet Virtual Private Networking“.

- **Selbstentschlüsselnde Archive** PGP kann nun Dateien oder Ordner in selbstentschlüsselnde Archive (Self-Decrypting Archives, SDA) verschlüsseln, die sogar an Benutzer gesendet werden können, die nicht mit PGP arbeiten. Die Archive sind vollkommen unabhängig von sämtlichen Anwendungen und werden durch die effiziente Kryptographie von PGP komprimiert und geschützt.

- **X.509-Zertifikat- und CA-Unterstützung.** PGP kann nun mit dem X.509-Zertifikat-Format kooperieren. Dieses Format wird vom Großteil der Web-Browser zur Absicherung der Übertragung von Web-Seiten verwendet. PGP unterstützt die Anforderung von Zertifikaten von Net Tools PKI von Network Associates, OnSite von VeriSign sowie Zertifizierungsinstanzen von Entrust. X.509-Zertifikate sind vergleichbar mit einer PGP-Unterschrift, folglich können Sie X.509-Zertifikate sogar mit Ihrem vorhandenen PGP-Schlüssel anfordern. Wenn Sie mit PGPnet arbeiten, können Sie dank dieser Funktion mit auf X.509 basierenden, vorhandenen VPN-Lösungen kooperieren.

- **Automatisierte Speicherplatz-Löschfunktion.** Über die PGP-Funktion zum Löschen von freiem Speicherplatz können Sie durch den Windows-Taskplaner den freien Speicherplatz auf Ihrem Datenträger regelmäßig auf sichere Weise löschen lassen. Auf diese Weise wird sichergestellt, daß zuvor gelöschte Dateien sicher und zuverlässig gelöscht werden.

- **HotKey**s. Die Funktion „Aktives Fenster verwenden“ wurde durch die Ergänzung durch HotKeys spürbar verbessert. Nun können Sie HotKey-Kombinationen für die Funktionen zum Verschlüsseln / Entschlüsseln / Unterschreiben festlegen.

- **Fingerabdruck-Wortliste.** Bei der Verifizierung von Fingerabdrücken öffentlicher Schlüssel in PGP können Sie den jeweiligen Fingerabdruck nun anstelle von Hexadezimalzeichen als Wortliste anzeigen lassen. Die im Textfeld „Fingerabdruck“ enthaltene Wortliste besteht aus speziellen von PGP verwendeten Worten zur Authentisierung, die sorgfältig ausgewählt wurden und phonetisch eindeutig sowie leicht verständlich sind.

- **HTTP Proxy-Unterstützung.** Falls sich Ihr Computer hinter einer firmenweiten Firewall mit einem HTTP-Proxyserver befindet, können Sie in PGP nun über den Proxy auf HTTP Certificate Server zugreifen.

- **Intelligente Zeilenumbrüche.** Durch die Zeilenumbruchsfunktion in PGP werden Abschnitte und sogar Abschnitte mit Zitaten nun neu umgebrochen, mit dem Ergebnis, daß unterschriebene Nachrichten deutlich übersichtlicher strukturiert sind.

- **PGP-Befehlszeile.** Die PGP-Befehlszeile wurde in Desktop Security integriert. Die Befehlszeilenversion von PGP ermöglicht die Durchführung zweier gängiger Vorgänge, nämlich die sichere Übertragung von Daten zwischen Stapelverarbeitungsservern und die Integration in automatisierte Verfahren.

So erreichen Sie Network Associates

Kundendienst

Wenden Sie sich an den Kundendienst von Network Associates, wenn Sie weitere Produkte bestellen bzw. Produktinformationen anfordern möchten:

Network Associates International BV.
Gatwickstraat 25
1043 GL Amsterdam
Niederlande

Technischer Kundendienst

Network Associates hat es immer als eine der wichtigsten Aufgaben betrachtet, die Kunden voll zufriedenzustellen. Wir setzen diese Tradition fort, indem wir auf unserer Web-Site Antworten auf wichtige Fragen zu technischen Problemen zur Verfügung stellen. Wenn Sie also Antworten auf häufig gestellte Fragen suchen, aktualisierte Software-Versionen von Network Associates-Produkten herunterladen möchten oder die neuesten Nachrichten von Network Associates und Informationen zur Verschlüsselung von Nachrichten erhalten möchten, so schauen Sie zuerst auf unserer Web-Site nach.

World Wide Web	http://www.nai.com

Sie erreichen den technischen Kundendienst für Ihr PGP-Produkt über die folgenden Nummern und Adressen:

Telefon	+31 (20) 586 6100
E-Mail:	tech-support-europe@nai.com

Damit das Network Associates-Kundendienstpersonal Ihre Fragen schnell und effizient beantworten kann, benötigen wir Informationen zu Ihrem Computer und der von Ihnen verwendeten Software. Bitte halten Sie folgende Informationen bei Ihrem Anruf bereit:

Falls Sie durch die automatisierten Dienste keine Antwort auf Ihre Frage erhalten, wenden Sie sich an den Kundendienst von Network Associates, der von Montag bis Freitag zwischen 6.00 Uhr und 18.00 Uhr (USA) unter einer der folgenden Nummern erreichbar ist:.

Telefon	+31 (20) 586 6100

Damit das Network Associates-Kundendienstpersonal Ihre Fragen schnell und effizient beantworten kann, benötigen wir Informationen zu Ihrem Computer und der von Ihnen verwendeten Software. Bitte halten Sie folgende Informationen bei Ihrem Anruf bereit:

- Produktname und Versionsnummer
- Computermarke und -modell
- Weitere an Ihren Computer angeschlossene Hardware oder Peripheriegeräte
- Art des Betriebssystems und Versionsnummern
- Art und Version des Netzwerks (falls vorhanden)
- Inhalt der Status- oder Fehlermeldung, die entweder auf dem Bildschirm oder in der Protokolldatei angezeigt wird (nicht bei allen Produkten werden Protokolldateien erstellt)
- E-Mail-Anwendung und -Version (falls das Problem bei der Anwendung von PGP mit einer E-Mail-Anwendung, beispielsweise dem Eudora-Plug-In, auftritt)
- Zum Reproduzieren des Problems erforderliche Schritte

Jahr 2000-Kompatibilität

Informationen zu Jahr-2000-kompatiblen NAI-Produkten und diesbezüglichen Standards und Testmodellen erhalten Sie auf der NAI-Web-Site unter http://www.nai.com/y2k.

Weitere Informationen sind über E-Mail an die Adresse y2k@nai.com erhältlich.

Network Associates-Schulungen

Informationen zu Schulungen in Ihrem Unternehmen für Network Associates-Produkte erhalten Sie unter der Telefonnummer +31 (20) 586 6100.

Kommentare und Anregungen

Network Associates freut sich über Kommentare und Anregungen, durch die Ihnen selbstverständlich keinerlei Verpflichtungen entstehen. Bitte richten Sie Anmerkungen zur PGP-Produktdokumentation an: Network Associates International BV. Gatwickstraat 25, 1043 GL Amsterdam, Niederlande. Oder schreiben Sie eine E-Mail an tns_documentation@nai.com.

Empfohlene Literatur

Nicht-Technische und technische Einführungsliteratur

- Whitfield Diffie und Susan Eva Landau, „Privacy on the Line“, *MIT Press*; ISBN: 0262041677
  In diesem Buch werden Geschichte und Entwicklung der Kryptographie und Kommunikationssicherheit beschrieben. Dieses Buch eignet sich hervorragend für Einsteiger und Benutzer mit geringem technischem Wissen. Es enthält daneben aber auch Informationen, die selbst vielen Experten unbekannt sein dürften.

- David Kahn, „The Codebreakers“ *Scribner*; ISBN: 0684831309
  In diesem Buch wird die Geschichte der Codierung und der Entschlüsselung von Codes von der Zeit der Ägypter bis zum Ende des II. Weltkrieges beschrieben. Kahn hat das Buch in den sechziger Jahren geschrieben und 1996 eine überarbeitete Ausgabe herausgebracht. Das Buch enthält zwar keine Darstellungen von kryptographischen Verfahrensweisen, diente aber einer neuen Generation von Kryptographen als Anregung.

- Charlie Kaufman, Radia Perlman und Mike Spencer, „Network Security: Private Communication in a Public World“, *Prentice Hall*; ISBN: 0-13-061466-1
  In diesem Buch werden Netzwerk-Sicherheitssysteme und -protokolle, deren Funktionsweise sowie die jeweiligen Vor- und Nachteile beschrieben. Da dieses Buch bereits im Jahre 1995 erschienen ist, ist es nur bedingt auf dem neuesten technischen Stand. Es ist dennoch sehr empfehlenswert. Ferner ist die darin enthaltene Beschreibung der Funktionsweise von DES wohl eine der besten, die jemals in einem Buch veröffentlicht wurde.

Technische Literatur

- Bruce Schneier, „Applied Cryptography: Protocols, Algorithms, and Source Code in C“, *John Wiley & Sons*; ISBN: 0-471-12845-7
  Ein geeignetes Werk für Anfänger über die Funktionsweise der Kryptographie. Wenn Sie ein Experte auf dem Gebiet der Kryptographie werden möchten, empfehlen wir die Lektüre dieses Standardwerks.

- Alfred J. Menezes, Paul C. van Oorschot und Scott Vanstone, „Handbook of Applied Cryptography“, *CRC Press;* ISBN: 0-8493-8523-7
  Dieses Buch sollten Sie im Anschluß an Schneier lesen. Es enthält viele komplizierte mathematische Zusammenhänge, eignet sich aber dennoch für Benutzer, die im Bereich der Mathematik über wenig Fachwissen verfügen.

- Richard E. Smith, „Internet Cryptography“, *Addison-Wesley Pub Co*; ISBN: 020192480
  In diesem Buch wird die Funktionsweise vieler Internet-Sicherheitsprotokolle beschrieben. Es beschreibt in erster Linie Systeme, die hochentwickelt sind, jedoch durch unvorsichtige Verwendung fehlerhaft arbeiten.
  Der Schwerpunkt in diesem Buch liegt nicht auf mathematischen Darstellungen, sondern auf der Vermittlung von praktischem Wissen.

- William R. Cheswick und Steven M. Bellovin, „Firewalls and Internet Security: Repelling the Wily Hacker“ *Addison-Wesley Pub Co*; ISBN: 0201633574
  Die Autoren dieses Buches sind zwei langjährige Forschungsspezialisten von AT&T Bell Labs. Sie berichten über ihre Erfahrungen bei der Wartung und Neugestaltung der Internet-Verbindung von AT&T. Dieses Buch ist äußerst empfehlenswert!

Literatur für Fortgeschrittene

- Neal Koblitz, „A Course in Number Theory and Cryptography“ *Springer-Verlag*; ISBN: 0-387-94293-9
  Ein hervorragendes Mathematikbuch zur Zahlentheorie und Kryptographie, das sich in erster Linie an Hochschulabsolventen richtet.

- Eli Biham und Adi Shamir, „Differential Cryptanalysis of the Data Encryption Standard“, *Springer-Verlag*; ISBN: 0-387-97930-1
  In diesem Buch wird die Differentialkryptoanalyse auf DES angewandt erläutert. Das Buch eignet sich besonders zum Kennenlernen dieses Verfahrens.

PGP installieren 1

In diesem Kapitel wird die Installation und das Ausführen von PGP Desktop Security für Windows beschrieben. Außerdem erhalten Sie einen kurzen Überblick über die bei der Verwendung dieses Produkts auszuführenden Vorgänge.

Bevor Sie mit der Installation von PGP beginnen, gehen Sie noch einmal die unten aufgeführten Systemanforderungen durch.

Systemanforderungen

Für die Installation von PGP auf einem Windows 95-, Windows 98- oder Windows NT-System bestehen folgende Anforderungen:

- Windows 95, Windows 98 oder Windows NT 4.0 (Service Pack 3 oder höher)
- 32 MB RAM
- 16 MB freier Festplattenspeicher

Wenn Sie PGPnet auf diesem System ausführen möchten, bestehen außerdem folgende Anforderungen:

- Microsoft TCP/IP
- Eine kompatible LAN-/WAN-Netzwerkkarte
- Windows 95b (OSR2), wenn Sie die Installation auf einem Windows 95-System durchführen möchten.

Kompatibilität mit anderen Versionen

Seit der Veröffentlichung als Freeware-Produkt 1991 durch Phil Zimmermann hat PGP etliche Änderungen erfahren. Obwohl diese Version von PGP zahlreiche Veränderungen gegenüber der Originalversion umfaßt und eine vollkommen neue Benutzeroberfläche enthält, ist sie mit Vorgängerversionen von PGP kompatibel. Daher können Sie E-Mail-Nachrichten auf sichere Weise mit Personen austauschen, die noch folgende ältere Produktversionen verwenden:

- PGP 2.6 (durch MIT vertrieben)
- PGP for Personal Privacy, Version 5.0 - 5.5

- PGP for Business Security oder PGP for Email and Files Version 5.5
- PGP for Desktop Security oder PGP for Personal Privacy Version 6.0

HINWEIS: Desktop-Produkte von PGP ab Version 5.0 benötigen möglicherweise das RSA-Add-On für Kompatibilität mit älteren Versionen.

Vorgängerversionen aufrüsten

Wenn Sie eine ältere PGP-Version (entweder von PGP, Inc., Network Associates, Inc. oder ViaCrypt) aufrüsten, sollten Sie vor dem Installieren von PGP die alten Programmdateien entfernen, um freien Speicherplatz auf der Festplatte zu schaffen. Löschen Sie jedoch keine privaten und öffentlichen Schlüsselbunddateien, in denen Schlüssel gespeichert sind, die Sie mit Hilfe der Vorgängerversion erstellt oder gesammelt haben. Beim Installieren von PGP haben Sie die Möglichkeit, die vorhandenen privaten und öffentlichen Schlüssel zu behalten, so daß Sie nicht alle alten Schlüssel importieren müssen. Führen Sie zum Aufrüsten einer Vorgängerversion die im folgenden Abschnitt aufgelisteten Schritte aus:

So rüsten Sie von PGP-Version 2.6.2 oder 2.7.1 auf:

1. Beenden Sie alle offenen Programme und Anwendungen.
2. Erstellen Sie auf einem anderen Volume Sicherungskopien Ihrer alten PGP-Schlüsselbunde. Bei den PGP-Versionen 2.6.2 und 2.7.1 für Windows werden Ihre öffentlichen Schlüssel in einer Datei mit dem Namen PUBRING.PGP und Ihre privaten Schlüssel in einer Datei mit dem Namen SECRING.PGP gespeichert. In den Versionen 5.x - 6.5 werden Ihre öffentlichen Schlüssel in einer Datei mit dem Namen PUBRING.PKR und Ihre privaten Schlüssel in einer Datei mit dem Namen SECRING.SKR gespeichert.

   TIP: Sichern Sie Ihre Schlüsselbunde auf zwei verschiedenen Disketten, um ganz sicherzugehen. Achten Sie besonders darauf, Ihren privaten Schlüsselbund nicht zu verlieren. Andernfalls wird es für Sie unmöglich, E-Mail-Nachrichten oder Dateianhänge zu entschlüsseln, die mit den verlorengegangenen Schlüsseln verschlüsselt wurden. Speichern Sie die Schlüsselbunde an einem sicheren Ort, auf den nur Sie Zugriff haben.

3. Wenn Sie eine Sicherungskopie Ihrer alten Schlüsselbunde erstellt haben, entfernen Sie die (alte) PGP-Software von Ihrer Festplatte, oder archivieren Sie sie. Hierfür stehen Ihnen folgende Möglichkeiten zur Verfügung:

   - Löschen Sie manuell den gesamten PGP-Ordner und dessen Inhalt; oder
   - Löschen Sie manuell das alte PGP-Programm, und archivieren Sie die verbleibenden Dateien, insbesondere die Konfigurations- und Schlüsselbunddateien**.**

4. Installieren Sie PGP Version 6.5.1 mit dem dafür vorgesehenen Installationsprogramm.
5. Starten Sie Ihren Computer neu.

So rüsten Sie von PGP Version 5.x auf:

Wenn Sie von PGP Version 4.x oder 5.x aufrüsten möchten, befolgen Sie die Installationsanweisungen im Abschnitt „PGP installieren“.

PGP installieren

Sie können die PGP Desktop Security-Software von einer CD-ROM oder vom Datei-Server Ihrer Firma installieren. Die selbstextrahierende Datei SETUP.EXE wird automatisch extrahiert, und Sie werden schrittweise durch den Installationsvorgang begleitet. Nachdem Sie die Software installiert haben, können Sie Ihr privates und öffentliches Schlüsselpaar erstellen und anfangen, PGP zu verwenden. Anweisungen zum Gebrauch von PGP finden Sie in der im Programm enthaltenen Datei PGPWinUsersGuide.pdf.

Sie installieren PGP Desktop Security für Windows, indem Sie folgende Schritte genau befolgen:

So installieren Sie PGP:

1. Beenden Sie alle laufenden Programme auf Ihrem Computer, und führen Sie einen der folgenden Schritte aus:

   - **Für die Installation von CD-ROM** legen Sie diese in das CD-ROM-Laufwerk ein.

     Das Setup-Programm startet automatisch. Sollte dies nicht geschehen, doppelklicken Sie auf **SETUP.EXE** im Ordner PGP auf der CD-ROM.

- **Für die Installation vom Datei-Server Ihrer Firma** fragen Sie den Sicherheitsbeauftragten Ihrer Firma, von welchem Server Sie PGP herunterladen können. Melden Sie sich bei diesem Server an.

  Doppelklicken Sie auf **SETUP.EXE** im Ordner „PGP“, um das Setup-Programm zu starten.

2. Wenn das Setup-Programm offene Programme findet, werden Sie aufgefordert, diese zu schließen.

   Wenn auf Ihrem Computer PGP Version 4.x - 6.x installiert ist, fordert Sie das PGP-Setup-Programm dazu auf, die alten PGP-Dateien zu deinstallieren. Klicken Sie auf **Ja**, um die alte Version automatisch zu deinstallieren. Ihre Schlüsselbunddateien werden in einer Datei mit dem Namen **Alte Schlüsselbunde** gespeichert.

   Nach dem Deinstallieren der Dateien müssen Sie Ihren Computer neu starten. Nach dem Neustart des Computers fährt das Installationsprogramm fort.

   Der **PGP-Installationsbildschirm** wird angezeigt.

3. Lesen Sie sich die Anweisungen im PGP-Begrüßungsbildschirm durch, und klicken Sie dann auf **Weiter**.

   Die Network Associates-Lizenzvereinbarung wird angezeigt.

4. Lesen Sie sich die Lizenzvereinbarung durch, und klicken Sie auf **Ja**, um die Lizenzbedingungen zu akzeptieren.

   Die Datei WHATSNEW.TXT wird angezeigt, in der neue Funktionen beschrieben werden und weitere wichtige Informationen zu PGP Version 6.5.1 enthalten sind.

5. Lesen Sie die Datei, und klicken Sie dann auf **Weiter**.

6. Registrieren Sie die Software, indem Sie Ihren Namen und den Namen Ihrer Firma im Dialogfeld **Benutzerinformation** eingeben.

7. Klicken Sie auf **Weiter**.

8. Klicken Sie auf **Durchsuchen**, um ein Zielverzeichnis für die PGP-Dateien auszuwählen, oder übernehmen Sie das Standardverzeichnis. Klicken Sie auf **Weiter**, um fortzufahren.

   Das Dialogfeld **Komponenten auswählen** wird angezeigt (siehe Abbildung 1-1).

Abbildung 1-1. PGP-Dialogfeld „Komponenten auswählen“

9. Entfernen Sie die Komponenten, die nicht installiert werden sollen. Standardmäßig sind alle Optionen ausgewählt. Sie haben folgende Installationsoptionen:

   - **PGP-Schlüsselverwaltungsprogramm (erforderlich).** Damit wird das PGP-Programm installiert. Sie müssen die Dienstprogramme zur Schlüsselverwaltung installieren.

   PGPnet Wählen Sie diese Option, um das PGPnet-Programm zu installieren. PGPnet, ein *Virtual Private Network (VPN)*, ist eine benutzerfreundliche Verschlüsselungsanwendung, mit der Sie sicher und kostengünstig mit anderen PGPnet-Benutzern in Ihrem eigenen Firmenintranet sowie weltweit kommunizieren können.

   - **PGP Eudora-Plug-In.** Wählen Sie diese Option, wenn Sie die PGP-Funktionen in Ihre Qualcomm Eudora-E-Mail-Anwendung integrieren möchten. PGP Version 6.5.1 unterstützt Eudora-Versionen ab 3.05.

   - **PGP Microsoft Exchange/Outlook Plug-In.** Wählen Sie diese Option, wenn Sie die PGP-Funktionen in Ihre Microsoft Exchange / Outlook-E-Mail-Anwendung integrieren möchten. PGP Version 6.5.1 unterstützt Outlook 97 und 98.

   - **PGP Microsoft Outlook Express Plug-In.** Wählen Sie diese Option, wenn Sie die PGP-Funktionen in Ihre Microsoft Outlook Express-E-Mail-Anwendung integrieren möchten. PGP Version 6.5.1 unterstützt die Version, die in Internet Explorer Version 4.x enthalten ist.

- **„PGP-Benutzerhandbuch“ (Adobe Acrobat-Format).** Wählen Sie diese Option, um das „PGP-Benutzerhandbuch“ zu installieren.
- **PGP-Befehlszeile.** Wählen Sie diese Option, wenn Sie die Befehlszeilenversion von PGP für Windows NT-Computer installieren möchten. *(nur für Anwendung durch den Kunden gedacht) Für Vorgänge mit Stapelverarbeitungsservern ist eine zusätzliche Lizenz erforderlich.*

10. Klicken Sie auf **Weiter**.

    Ein Dialogfeld wird mit der Meldung angezeigt, daß das Installationsprogramm zum Kopieren von Dateien bereit ist.

11. Überprüfen Sie die Installationseinstellungen, und klicken Sie dann auf **Weiter**.

    Die PGP-Dateien werden auf Ihren Computer kopiert.

12. Wenn sich Schlüsselbunde einer Vorgängerversion auf Ihrem Computer befinden, klicken Sie auf **Ja**, um diese weiter zu verwenden.

    Es wird ein Dialogfeld angezeigt, in dem Sie den Speicherort Ihres öffentlichen (PUBRING.PKR) und Ihres privaten Schlüsselbundes (SECRING.SKR) angeben können.

    Sollten sich keine Schlüsselbunde auf Ihrem Computer befinden, klicken Sie auf **Nein**. Wenn Sie die PGPkeys-Anwendung zum ersten Mal öffnen, werden Sie aufgefordert, ein Schlüsselpaar zu erstellen.

13. Wenn Sie die Anwendung PGPnet installieren, wird die **PGPnet Netzwerkkartenliste** angezeigt, in der die auf Ihrem System vorgefundenen Netzwerkkarten aufgeführt werden (siehe Abbildung 1-2).

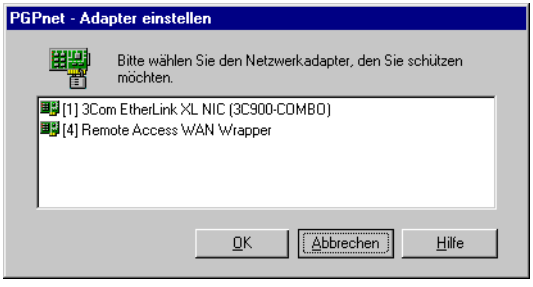


Abbildung 1-2. PGPnet Netzwerkkartenliste.

Wenn Sie über ein Modem sicher kommunizieren möchten, wählen Sie Ihre WAN-Netzwerkkarte aus (z. B. Remote Access WAN Wrapper oder DFÜ-Adapter). Möchten Sie über eine Ethernet-Verbindung sicher kommunizieren, wählen Sie Ihre LAN-Netzwerkkarte aus (z. B. 3COM Megahertz LAN PC-Karte). Wenn Sie die entsprechende Netzwerkkarte gewählt haben, klicken Sie auf **OK**.

HINWEIS: Bei Windows 98-Computern wird WAN statt als „DFÜ-Adapter“ als „Remote WAN Wrapper“ aufgeführt.

Das Installationsprogramm bindet den PGPnet-Treiber an die ausgewählte Netzwerkkarte und konfiguriert Ihren Computer für die Verwendung der PGPnet-Anwendung.

14. Wenn Sie möchten, daß Ihr Computer automatisch neu gestartet wird, klicken Sie auf **Ja, ich möchte meinen Computer jetzt neu starten**.

15. Klicken Sie auf **Fertig stellen**, um die PGP-Installation abzuschließen und Ihren Computer neu zu starten.

HINWEIS: Sie müssen Ihren Computer neu starten, wenn Sie PGPdisk oder PGPnet installieren.

Fertig! PGP ist jetzt auf Ihrem Computer installiert.

PGP verwenden 2

PGP basiert auf einem allgemein anerkannten Verschlüsselungsverfahren, das als *Kryptographie mit öffentlichen Schlüsseln* bekannt ist. Dabei werden zwei zueinander gehörende Schlüssel, d. h. ein *Schlüsselpaar*, zum Schutz von übertragenen Daten verwendet. Einer der Schlüssel ist ein *privater Schlüssel*, auf den nur Sie zugreifen können. Der andere Schlüssel ist ein *öffentlicher Schlüssel*, den Sie offen an andere PGP-Benutzer weitergeben. Sowohl Ihr privater als auch Ihr öffentlicher Schlüssel werden in Schlüsselbunddateien gespeichert, auf die Sie über das PGPkeys-Fenster zugreifen können. In diesem Fenster führen Sie alle Schlüsselverwaltungsfunktionen aus.

In diesem Abschnitt finden Sie eine kurze Darstellung der Vorgänge, die Sie gewöhnlich in PGP durchführen. Ausführliche Informationen zu diesen Vorgängen finden Sie in den entsprechenden Kapiteln dieses Handbuchs. Eine umfassende Übersicht über die PGP-Verschlüsselungsverfahren finden Sie im Handbuch „*Einführung in die Kryptographie*“, das Sie mit diesem Produkt erhalten haben.

Grundlagen für die Verwendung von PGP

1. PGP auf Ihrem Computer installieren. Die vollständigen Installationsanweisungen erhalten Sie unter Kapitel 1, „PGP installieren“.

2. Private und öffentliche Schlüsselpaare erstellen

   Bevor Sie PGP einsetzen können, müssen Sie ein Schlüsselpaar erstellen. Ein PGP-Schlüsselpaar besteht aus einem privaten Schlüssel, auf den nur Sie zugreifen können, und einem öffentlichen Schlüssel, den Sie kopieren und jedem frei zugänglich machen können, mit dem Sie Daten austauschen.

   Sie haben die Möglichkeit, gleich nach der Installation von PGP ein neues Schlüsselpaar zu erstellen. Es ist jedoch auch möglich, Schlüssel zu einem beliebigen anderen Zeitpunkt mit Hilfe der PGPkeys-Anwendung zu erstellen.

   Weitere Informationen zum Erstellen von privaten und öffentlichen Schlüsseln finden Sie im Abschnitt „Schlüsselpaare erstellen“ auf Seite 24.

3. Öffentliche Schlüssel mit anderen Personen austauschen

   Nach der Erstellung eines Schlüsselpaares können Sie Nachrichten mit anderen PGP-Benutzern austauschen. Sie benötigen dazu eine Kopie des öffentlichen Schlüssels der anderen Benutzer, die wiederum eine Kopie Ihres öffentlichen Schlüssels benötigen. Das Austauschen von Schlüsseln ist einfach, da Ihr öffentlicher Schlüssel nur aus Text besteht. Sie können Ihren öffentlichen Schlüssel in eine E-Mail-Nachricht einfügen, in eine Datei kopieren oder an einen öffentlichen oder firmeninternen Schlüssel-Server senden, wo jeder bei Bedarf eine Kopie Ihres Schlüssels erhalten kann.

   Weitere Informationen zum Austauschen von öffentlichen Schlüsseln finden Sie in den Abschnitten „Ihren öffentlichen Schlüssel verteilen“ auf Seite 53 und „Öffentliche Schlüssel von anderen Benutzern erhalten“ auf Seite 58.

4. Echtheit von öffentlichen Schlüsseln überprüfen

   Wenn Sie die Kopie eines öffentlichen Schlüssels von einem anderen Benutzer erhalten haben, können Sie sie Ihrem öffentlichen Schlüsselbund hinzufügen. Vergewissern Sie sich dann, daß der Schlüssel nicht verfälscht wurde und daß er tatsächlich dem angegebenen Eigentümer gehört. Dazu vergleichen Sie den eindeutigen *Fingerabdruck* Ihrer Kopie des öffentlichen Schlüssels des anderen Benutzers mit dem Fingerabdruck des Originalschlüssels dieser Person. Wenn Sie sicher sind, daß Sie über einen echten öffentlichen Schlüssel verfügen, unterschreiben Sie ihn. Dadurch geben Sie an, daß der Schlüssel Ihrer Meinung nach echt ist und verwendet werden kann. Außerdem können Sie dem Schlüsseleigentümer ein bestimmtes Maß an Vertrauen aussprechen. Damit geben Sie an, wieviel Vertrauen Sie dieser Person im Hinblick auf deren Verbürgung für die Echtheit des öffentlichen Schlüssels einer anderen Person entgegenbringen.

   Weitere Informationen zur Überprüfung Ihrer Schlüssel finden Sie im Abschnitt „Die Echtheit eines Schlüssels verifizieren“ auf Seite 63.

5. Ihre E-Mail-Nachrichten und Dateien verschlüsseln und unterschreiben

   Nachdem Sie Ihr Schlüsselpaar erstellt und öffentliche Schlüssel ausgetauscht haben, können Sie mit dem Verschlüsseln und Unterschreiben von E-Mail-Nachrichten und Dateien beginnen.

   PGP arbeitet mit in anderen Anwendungen erstellten Daten. Daher sind die PGP-Funktionen zu den von Ihnen jeweils ausgeführten Vorgängen jederzeit sofort verfügbar. Sie können mehrere Methoden verwenden, um mit PGP zu verschlüsseln und zu unterschreiben:

   - **Über das Systemfeld in der Task-Leiste (PGPtray)** PGPtray enthält Funktionen zum Verschlüsseln von Daten in der Zwischenablage oder im aktuellen Fenster. Siehe „Mit PGPtray“ auf Seite 17.
   - **In unterstützten E-Mail-Anwendungen (E-Mail-Plug-Ins von PGP)** Mit diesen Plug-Ins können Sie Ihre E-Mail in der unterstützten E-Mail-Anwendung schützen. Siehe „PGP innerhalb von unterstützten E-Mail-Anwendungen verwenden“ auf Seite 20.
   - **Über PGPtools.** Mit PGPtools können Sie Verschlüsselungen und andere Sicherheitsvorgänge, wie das Löschen von Dateien von Ihrer Festplatte, in Anwendungen durchführen, die nicht von Plug-Ins unterstützt werden. Siehe „PGPtools verwenden“ auf Seite 19.
   - **Über das Menü „Datei“ des Windows-Explorers** Mit Hilfe des Windows-Explorers können Sie Dateien wie beispielsweise Textverarbeitungsdokumente, Tabellen und Videoclips direkt verschlüsseln und unterschreiben bzw. entschlüsseln und verifizieren. Siehe „PGP über den Windows-Explorer verwenden“ auf Seite 18.

   Weitere Informationen zum Verschlüsseln von E-Mail finden Sie im Abschnitt „E-Mail-Nachrichten verschlüsseln und unterschreiben“ auf Seite 67. Weitere Informationen zum Entschlüsseln von Dateien finden Sie im Abschnitt „Mit PGP Dateien verschlüsseln und entschlüsseln“ auf Seite 81.

6. Eigene E-Mail-Nachrichten und Dateien entschlüsseln und verifizieren

   Wenn Ihnen ein anderer Benutzer verschlüsselte Daten sendet, können Sie den Inhalt entschlüsseln und beigefügte Unterschriften verifizieren, um sicherzustellen, daß die Daten tatsächlich von dem angegebenen Absender stammen und nicht verändert wurden.

   - Wenn Sie eine von den Plug-Ins unterstützte E-Mail-Anwendung verwenden, können Sie Ihre E-Mail-Nachrichten entschlüsseln und verifizieren, indem Sie in der Symbolleiste Ihrer Anwendung die entsprechenden Optionen wählen.
   - Wenn Ihre E-Mail-Anwendung nicht von den Plug-Ins unterstützt wird, können Sie die E-Mail-Nachricht in die Zwischenablage kopieren und die entsprechenden Funktionen von dort aus ausführen. Dateien können Sie mit Hilfe der Zwischenablage, des Windows-Explorers oder mit PGPtools entschlüsseln und verifizieren. Weiterhin können Sie auf Ihrem Computer gespeicherte verschlüsselte Dateien entschlüsseln und unterschriebene Dateien verifizieren, um sicherzustellen, daß sie nicht verfälscht wurden.

   Weitere Informationen zum Schützen von E-Mail finden Sie im Abschnitt „E-Mail-Nachrichten entschlüsseln und verifizieren“ auf Seite 77. Weitere Informationen zum Schützen von Dateien finden Sie im Abschnitt „Mit PGP Dateien verschlüsseln und entschlüsseln“ auf Seite 81.

7. Dateien löschen

   Wenn Sie eine Datei sicher löschen möchten, können Sie mit der Löschfunktion sicherstellen, daß die Datei nicht mehr wiederhergestellt werden kann. Die Datei wird sofort überschrieben, so daß sie nicht mehr mit Software zur Datenrettung wiederhergestellt werden kann.

   Weitere Informationen zum Löschen von Dateien finden Sie im Abschnitt „Dateien mit der PGP-Löschfunktion löschen“ auf Seite 92.

PGPkeys verwenden

Mit der Option **PGPkeys** in PGPtray wird das PGPkeys-Fenster geöffnet (Abbildung 2-1), in dem Ihre privaten und öffentlichen Schlüsselpaare sowie alle öffentlichen Schlüssel anderer Benutzer angezeigt werden, die Sie Ihrem öffentlichen Schlüsselbund hinzugefügt haben.

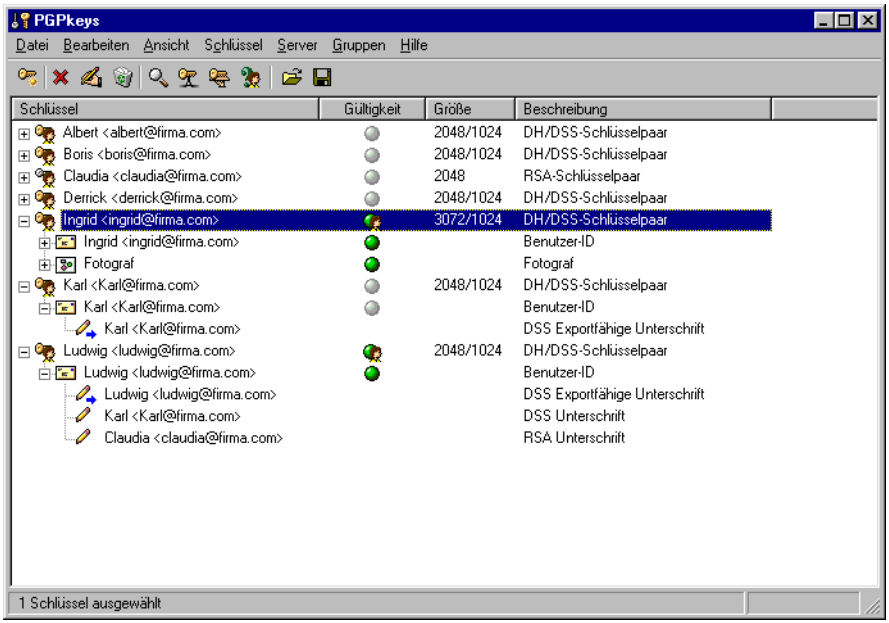


Abbildung 2-1. PGPkeys

(Wenn Sie noch kein neues Schlüsselpaar erstellt haben, können Sie dies mit Hilfe des PGP-Schlüsselerzeugungsassistenten nachholen. Lesen Sie jedoch vor dem Erstellen eines neuen Schlüsselpaares die Informationen zu den verschiedenen Optionen in Kapitel 3, „Schlüssel erstellen und austauschen“ durch.)

Im PGPkeys-Fenster können Sie neue Schlüsselpaare erstellen und Ihre übrigen Schlüssel verwalten. Hier können Sie beispielsweise die mit einem bestimmten Schlüssel verbundenen Attribute überprüfen und angeben, inwieweit Sie darauf vertrauen, daß der Schlüssel tatsächlich dem angegebenen Eigentümer gehört, und ob diese Person zuverlässig genug ist, sich für die Echtheit der Schlüssel anderer Benutzer zu verbürgen. Ausführliche Informationen zu den Schlüsselverwaltungsfunktionen, die Sie im PGPkeys-Fenster ausführen, finden Sie in Kapitel 6.

PGPkeys-Symboldefinitionen

PGPkeys-Symbole in der Menüleiste

In der folgenden Tabelle sind alle in der PGPkeys-Menüleiste verwendeten Symbole sowie Erläuterungen zu deren Funktion aufgelistet.

Tabelle 2-1. PGPkeys-Symbole in der Menüleiste

Symbol	Funktion
	Startet den Schlüsselerzeugungsassistenten. Klicken Sie auf diese Schaltfläche, um ein neues Schlüsselpaar zu erstellen.
	Nimmt den momentan ausgewählten Schlüssel oder die aktuelle Unterschrift zurück. Klicken Sie auf diese Schaltfläche, um einen Schlüssel zu deaktivieren oder eine Unterschrift zurückzunehmen. Wenn Sie einen Schlüssel zurücknehmen, können mit ihm keine Daten mehr verschlüsselt werden.
	Dient zum Unterschreiben des momentan ausgewählten Schlüssels. Dadurch zertifizieren Sie, daß der Schlüssel und die Benutzer-ID zum angegebenen Benutzer gehören.
	Löscht das momentan ausgewählte Element. Klicken Sie auf diese Schaltfläche, um einen Schlüssel, eine Unterschrift oder eine Foto-Benutzer-ID zu entfernen.
	Öffnet das **Schlüsselsuchfenster**, in dem Sie in lokalen Schlüsselbunden und auf entfernten Servern nach Schlüsseln suchen können.
	Sendet den momentan ausgewählten Schlüssel an den Server. Klicken Sie auf diese Schaltfläche, um Ihren Schlüssel auf den Certificate Server oder den Domänen-Server zu laden.
	Aktualisiert den momentan ausgewählten Schlüssel von einem Certificate Server oder Domänen-Server. Klicken Sie auf diese Schaltfläche, um Schlüssel von einem Certificate Server oder Domänen-Server in Ihren Schlüsselbund zu importieren.
	Zeigt das Dialogfeld für die **Schlüsseleigenschaften** des momentan gewählten Schlüssels an. Mit dieser Schaltfläche können Sie für einen Schlüssel **allgemeine** und **Teilschlüsseleigenschaften** anzeigen.
	Ermöglicht das Importieren von Schlüsseln von einer Datei auf Ihren Schlüsselring.
	Ermöglicht das Exportieren des ausgewählten Schlüssels in eine Datei.

Symbole im PGPkeys-Fenster

In der folgenden Tabelle werden alle im PGPkeys-Fenster verwendeten Symbole erklärt.

Tabelle 2-2. Symbole im PGPkeys-Fenster

Symbol	Beschreibung
	Durch einen gelben Schlüssel und einen Benutzer wird Ihr Diffie-Hellman/DSS-Schlüsselpaar dargestellt, das aus Ihrem privaten und Ihrem öffentlichen Schlüssel besteht.
	Durch einen einzelnen gelben Schlüssel wird ein öffentlicher Diffie-Hellman/DSS-Schlüssel dargestellt.
	Durch einen grauen Schlüssel und einen Benutzer wird Ihr RSA-Schlüsselpaar dargestellt, das aus Ihrem privaten und Ihrem öffentlichen Schlüssel besteht.
	Durch einen einzelnen grauen Schlüssel wird ein öffentlicher RSA-Schlüssel dargestellt.
	Wenn ein Schlüssel oder ein Schlüsselpaar grau hinterlegt angezeigt wird, können die Schlüssel vorübergehend nicht zum Verschlüsseln und Unterschreiben verwendet werden. Sie können Schlüssel im PGPkeys-Fenster deaktivieren, um zu verhindern, daß selten verwendete Schlüssel stets im PGP-Dialogfeld zur Schlüsselauswahl angezeigt werden.
	Dieses Symbol zeigt an, daß eine Foto-Benutzer-ID zum öffentlichen Schlüssel gehört.
	Durch einen mit einem roten X gekennzeichneten Schlüssel wird angezeigt, daß der Schlüssel zurückgenommen wurde. Benutzer nehmen Ihre Schlüssel zurück, wenn die Schlüssel nicht mehr echt oder sicher sind.
	Durch einen Schlüssel mit einer Uhr wird angezeigt, daß der Schlüssel abgelaufen ist. Das Gültigkeitsdatum eines Schlüssels wird bei seiner Erstellung festgelegt.
	Durch einen Briefumschlag wird der Schlüsseleigentümer dargestellt. Die Benutzernamen und die mit dem Schlüssel verbundenen E-Mail-Adressen werden ebenfalls angezeigt.
	Ein grauer Kreis bedeutet, daß der Schlüssel ungültig ist.
	Ein grüner Kreis weist auf einen gültigen Schlüssel hin. Ein zusätzlicher roter Kreis in der ADK-Spalte bedeutet, daß der Schlüssel mit einem Zusätzlichen Entschlüsselungsschlüssel (ADK) verknüpft ist; ein weiterer grauer Kreis in der ADK-Spalte weist hingegen darauf hin, daß der Schlüssel mit keinem Zusätzlichen Entschlüsselungsschlüssel (ADK) verknüpft ist.

Tabelle 2-2. Symbole im PGPkeys-Fenster

Symbol	Funktion
	Ein grüner Kreis mit einem Benutzer zeigt an, daß Sie der Eigentümer des Schlüssels sind und dem Schlüssel implizites Vertrauen entgegenbringen.
	Durch ein Stift- oder ein Füllhaltersymbol werden die Unterschriften der PGP-Benutzer gekennzeichnet, die sich für die Echtheit des Schlüssels verbürgen. - Eine mit einem roten X durchgestrichene Unterschrift gibt an, daß die Unterschrift zurückgenommen wurde. - Eine Unterschrift mit einem grau hinterlegten Stiftsymbol ist unecht oder fehlerhaft. - Mit einem blauen Pfeil versehene Unterschriften können exportiert werden.
	Ein Zertifikat stellt ein X.509-Zertifikat dar, d. h. ein anerkanntes elektronisches Dokument zur Prüfung der Identität und der Eigentümer von öffentlichen Schlüsseln in einem Kommunikationsnetzwerk.
	Durch eine Uhr wird angezeigt, daß ein X.509-Zertifikat abgelaufen ist.
	Mit einem roten X wird angezeigt, daß ein X.509-Zertifikat zurückgenommen wurde.
	Durch einen leeren Balken wird ein unechter Schlüssel oder ein nicht vertrauenswürdiger Benutzer dargestellt.
	Durch einen halb gefüllten Balken wird ein zweitrangiger, echter Schlüssel oder gering vertrauenswürdiger Benutzer dargestellt.
	Durch einen gestreiften Balken wird ein gültiger Schlüssel dargestellt, dessen Eigentümer Sie sind und dem Sie unabhängig von den Unterschriften auf dem Schlüssel vertrauen.
	Durch einen vollständig ausgefüllten Balken wird ein echter Schlüssel oder ein vertrauenswürdiger Benutzer dargestellt.

Mit PGPtray

Auf viele der Hauptfunktionen von PGP kann durch Klicken auf das Schloßsymbol () zugegriffen werden, das sich normalerweise im Systemfeld in der Task-Leiste befindet. Hier kann dann der entsprechende Menüeintrag gewählt werden. (Wenn sich dieses Symbol nicht im Systemfeld in der Task-Leiste befindet, starten Sie PGPtray über das Menü **Start**.) Mit dieser Funktion können Sie sofort auf die PGP-Funktionen zugreifen, unabhängig davon, welche Anwendung Sie gerade verwenden. Noch dazu erweist sie sich als besonders hilfreich, wenn Sie eine E-Mail-Anwendung verwenden, die nicht von PGP-Plug-Ins unterstützt wird.

❑ **HINWEIS:** Wenn Sie PGPnet installiert haben, wird dieses Symbol () anstelle des Schloßsymbols in der Taskleiste angezeigt. Je nach Farbe des PGPtray-Symbols können Sie feststellen, ob PGPnet deaktiviert oder nicht installiert (graues Schloß), installiert (in einem Netzwerk gelbes Schloß) oder zwar installiert ist, aber nicht funktioniert (in einem Netzwerk gelbes Schloß mit rotem X).

PGP-Funktionen über die Zwischenablage oder das aktuelle Fenster ausführen

Wenn Sie eine von den PGP-Plug- Ins nicht unterstützte E-Mail-Anwendung verwenden oder mit Text arbeiten, der in einer anderen Anwendung erstellt wurde, können Sie die Funktionen zum Ver- und Entschlüsseln und zum Unterschreiben und Verifizieren mit Hilfe der Windows-Zwischenablage oder innerhalb des aktuellen Anwendungsfensters ausführen.

Mit Hilfe der Windows-Zwischenablage

Wenn Sie beispielsweise Text verschlüsseln oder unterschreiben, kopieren Sie ihn aus Ihrer Anwendung in die Zwischenablage (STRG +C), verschlüsseln oder unterschreiben ihn mittels der entsprechenden PGP-Funktionen und fügen ihn anschließend vor dem Senden an die jeweiligen Empfänger wieder in Ihre Anwendung ein (STRG +V). Wenn Sie eine verschlüsselte oder unterschriebene E-Mail-Nachricht erhalten, führen Sie den Vorgang in umgekehrter Reihenfolge aus. Sie kopieren den verschlüsselten Text, den sogenannten *chiffrierten Text*, aus Ihrer Anwendung in die Zwischenablage, entschlüsseln und verifizieren die Daten und zeigen anschließend den Inhalt an. Nach dem Anzeigen der entschlüsselten Nachricht können Sie entscheiden, ob Sie die entschlüsselten Daten speichern oder in verschlüsselter Form behalten möchten.

Innerhalb des aktuellen Fensters

Mit dem Menüeintrag **Aktuelles Fenster,** mit dem der Text vom aktuellen Fenster in die Zwischenablage kopiert wird und dann die entsprechenden Vorgänge ausgeführt werden, können Sie dieselben Verschlüsselungen durchführen.

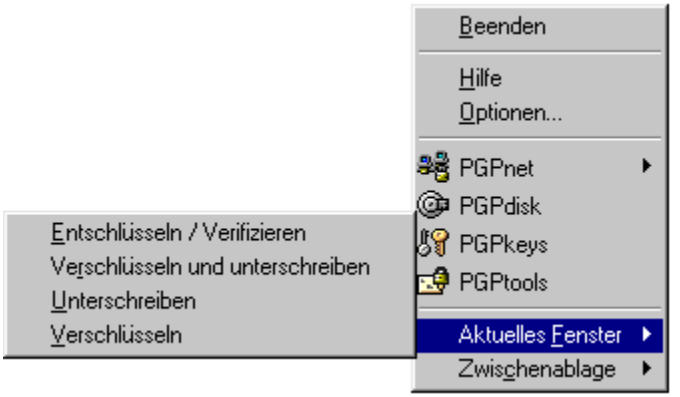


Abbildung 2-2. PGPtray-Funktion „Aktuelles Fenster“

PGP über den Windows-Explorer verwenden

Mit Hilfe des Windows-Explorers können Sie Dateien, wie beispielsweise Textverarbeitungsdokumente, Tabellen und Videoclips, direkt verschlüsseln und unterschreiben bzw. entschlüsseln und verifizieren. Wenn Sie keine E-Mail-Anwendung wie Qualcomm Eudora verwenden, die den PGP / MIME-Standard unterstützt, oder mit einer Anwendung wie Exchange oder Outlook arbeiten, bei der Dateien nicht mit PGP verschlüsselt oder unterschrieben werden müssen, verschlüsseln Sie mit dieser Methode Dateien, die Sie an zu sendende E-Mail-Nachrichten anhängen möchten. Sie können Dateien, die Sie auf Ihrem Computer speichern, auch ver- und entschlüsseln, so daß niemand darauf zugreifen kann.

Wählen Sie im Untermenü **PGP** des Explorer-Menüs **Datei** die entsprechende Option, um mit Hilfe des Windows-Explorers auf die PGP-Funktionen zuzugreifen. Die angezeigten Optionen hängen vom aktuellen Status der ausgewählten Datei ab. Wenn die Datei noch nicht verschlüsselt oder unterschrieben wurde, werden die Optionen zum Verschlüsseln und Unterschreiben im Menü angezeigt. Wenn die Datei hingegen bereits verschlüsselt oder unterschrieben wurde, werden die Optionen zum Entschlüsseln und Verifizieren des Dateiinhalts angezeigt.

PGPtools verwenden

Wenn Sie eine E-Mail-Anwendung verwenden, die nicht von Plug-Ins unterstützt wird, oder wenn Sie PGP-Funktionen über andere Anwendungen ausführen möchten, können Sie Nachrichten und Dateien direkt über PGPtools verschlüsseln und unterschreiben, entschlüsseln und verifizieren, oder unwiederherstellbar löschen. Für das Öffnen von PGPtools gibt es folgende Möglichkeiten:

- Klicken Sie auf **Start-->Programme-->PGP-->PGPtools**

  ODER

- Klicken Sie im Systemfeld in der Task-Leiste auf das PGPtools-Symbol ( ).

Wenn PGPtools (Abbildung 2-3) geöffnet ist, können Sie mit dem Verschlüsseln beginnen.

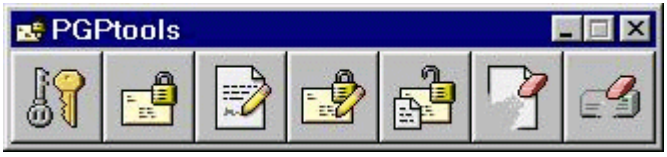


Abbildung 2-3. PGPtools

Sie können Text oder Dateien verschlüsseln, entschlüsseln, unterschreiben und verifizieren, indem Sie sie markieren und auf die entsprechende Schaltfläche in PGPtools verschieben.

Wenn Sie mit Dateien arbeiten, klicken Sie auf die entsprechende Schaltfläche in PGPtools, um eine Datei oder die Zwischenablage auszuwählen.

Wenn Sie eine Datei entschlüsseln, wird das Dialogfeld „Speichern unter“ angezeigt, und PGP erstellt eine neue Klartextdatei mit der Erweiterung .TXT. Die entschlüsselte Datei erhält die Erweiterung .TXT.PGP.

PGP innerhalb von unterstützten E-Mail-Anwendungen verwenden

PGP verwenden Sie am besten mit einer der gängigen E-Mail-Anwendungen, die von den PGP-Plug-Ins unterstützt werden. Wenn Ihre PGP-Version die E-Mail-Plug-Ins von PGP unterstützt, können Sie mit diesen Plug-Ins beim Lesen und Erstellen Ihrer E-Mail-Korrespondenz Nachrichten mit minimalem Arbeitsaufwand sowohl verschlüsseln und unterschreiben als auch entschlüsseln und verifizieren, indem Sie einfach auf die entsprechenden Schaltflächen klicken.

Wenn Sie mit einer E-Mail-Anwendung arbeiten, die nicht durch die PGP-Plug-Ins unterstützt wird, können Sie den Nachrichtentext mit Hilfe von PGPtray dennoch problemlos verschlüsseln. Weiterhin können Sie Dateien direkt aus der Windows-Zwischenablage ver- oder entschlüsseln, indem Sie die entsprechende PGP-Menüoption im Windows-Explorer wählen. Mit PGP können Sie außerdem Dateien auf der Festplatte Ihres Computers zur sicheren Speicherung verschlüsseln und unterschreiben sowie Dateien und nicht mehr benötigte Dateifragmente sicher von der Festplatte löschen, so daß vertrauliche Daten nicht mit einer Software zur Wiederherstellung der Festplatte abgerufen werden können.

Wenn Sie über eine der folgenden von den PGP-Plug- Ins unterstützten E-Mail-Anwendungen verfügen, können Sie auf die jeweiligen PGP-Funktionen zugreifen, indem Sie in der Symbolleiste Ihrer Anwendung auf die entsprechenden Schaltflächen klicken:

- Qualcomm Eudora
- Microsoft Exchange
- Microsoft Outlook
- Microsoft Outlook Express
- Lotus Notes (separat erhältlich)
- Novell Groupwise (separat erhältlich)

Sie klicken beispielsweise auf das Symbol mit dem Briefumschlag und dem Schloß (), um anzugeben, daß Sie Ihre E-Mail-Nachricht verschlüsseln möchten, und auf das Symbol mit dem Stift und dem Blatt Papier (), um anzugeben, daß Sie sie unterschreiben möchten. Einige Anwendungen verfügen auch über ein Symbol mit einem Schloß und einer Feder. Mit dieser Schaltfläche führen Sie beide Funktionen in einem Schritt durch.

Wenn Sie eine E-Mail-Nachricht von einem anderen PGP-Benutzer erhalten, entschlüsseln Sie die Nachricht und verifizieren die digitale Unterschrift dieser Person, indem Sie auf das Symbol mit dem geöffneten Schloß und dem Briefumschlag klicken oder in PGPtools die Option **Entschlüsseln/Verifizieren** wählen ().

In einigen Plug-Ins können Sie das PGPkeys-Fenster auch während des Schreibens oder Abrufens Ihrer Nachrichten durch Klicken auf die **PGPkeys-**Schaltfläche () aufrufen.

PGP/MIME verwenden

Wenn Sie eine E-Mail-Anwendung mit einem Plug-In verwenden, das den PGP / MIME-Standard unterstützt, und Sie mit einem anderen Benutzer kommunizieren, dessen E-Mail-Anwendung diesen Standard auch unterstützt, können beide Benutzer E-Mail-Nachrichten und alle Dateianhänge automatisch beim Senden oder Abrufen der E-Mail-Nachrichten ver- bzw. entschlüsseln. Hierzu müssen Sie nur im Dialogfeld **PGP-Optionen** die Funktionen für die PGP / MIME-Verschlüsselung und -Unterzeichnung aktivieren.

Wenn Sie eine E-Mail-Nachricht von einer Person erhalten, die die PGP / MIME-Funktion verwendet, ist diese E-Mail-Nachricht im Nachrichtenfenster mit einem Symbol versehen, das Ihnen anzeigt, daß sie mit PGP / MIME verschlüsselt wurde.

Doppelklicken Sie zum Entschlüsseln von Text oder Dateianhängen in PGP / MIME-verschlüsselten E-Mail-Nachrichten sowie zum Verifizieren von digitalen Unterschriften einfach auf das Symbol mit dem Schloß und der Feder (). Wenn PGP / MIME nicht verwendet wird, sind Anhänge immer noch verschlüsselt. Der Entschlüsselungsprozeß ist jedoch in der Regel komplizierter für den Empfänger.

Empfänger für verschlüsselte Dateien oder E-Mail auswählen

Wenn Sie E-Mail-Nachrichten an eine Person senden, deren E-Mail-Anwendung von den PGP-Plug-Ins unterstützt wird, entscheidet die E-Mail-Adresse des Empfängers darüber, welche Schlüssel beim Verschlüsseln des Inhalts verwendet werden. Wenn Sie jedoch einen Benutzernamen oder eine E-Mail-Adresse eingeben, die keinem der Schlüssel in Ihrem öffentlichen Schlüsselbund entspricht, oder wenn Sie mit Hilfe von PGPtray bzw. PGPtools verschlüsseln, müssen Sie den öffentlichen Schlüssel des Empfängers manuell im PGP-Dialogfeld zur **Schlüsselauswahl** auswählen.

Ziehen Sie zum Auswählen eines öffentlichen Schlüssels eines Empfängers das Symbol, das den Empfängerschlüssel darstellt, in das **Empfängerlistenfeld**, und klicken Sie anschließend auf **O**K.

Ausführliche Anweisungen zum Verschlüsseln und Unterschreiben sowie zum Entschlüsseln und Verifizieren von E-Mail-Nachrichten finden Sie in Kapitel 4, „E-Mail-Nachrichten sicher senden und empfangen“. Ausführliche Anweisungen zum Verschlüsseln von Dateien, die anschließend auf der Festplatte gespeichert oder als E-Mail-Anhang gesendet werden sollen, finden Sie in Kapitel 5, „PGP zur sicheren Dateispeicherung verwenden“.

Vorgänge vereinfachen

Obwohl PGP sehr benutzerfreundlich ist, können Sie Verschlüsselungen mit Hilfe von Vereinfachungen noch schneller durchführen. Wenn Sie beispielsweise Ihre Schlüssel im PGPkeys-Fenster verwalten, können Sie zum Ausführen aller nötigen PGP-Funktionen anstelle der Menüleiste auch die rechte Maustaste verwenden. Darüber hinaus können Sie eine Datei mit Schlüsseln in das PGPkeys-Fenster ziehen, um die Schlüssel Ihrem Schlüsselbund hinzuzufügen.

Für die meisten Menüoperationen stehen auch Tastenkombinationen zur Verfügung. Diese Tastenkombinationen werden in allen PGP-Menüs angezeigt. Sonstige Tastenkombinationen werden im jeweiligen Kontext in diesem Handbuch beschrieben.

Technische Unterstützung

Wenn Sie die Option **Hilfethemen** in **PGPtray** oder im PGPkeys-**Hilfemenü** wählen, wird das PGP-Hilfesystem geöffnet, in dem Sie einen allgemeinen Überblick und Anweisungen zu allen von Ihnen ausführbaren Vorgängen finden. Viele Dialogfelder verfügen auch über eine kontextsensitive Hilfe, die durch Klicken auf das Fragezeichen in der oberen rechten Fensterecke und anschließendes Zeigen mit dem Cursor auf den betroffenen Bildschirmbereich aufgerufen wird. Daraufhin wird eine kurze Erklärung angezeigt.

Schlüssel erstellen und austauschen 3

In diesem Kapitel wird beschrieben, wie Sie Schlüsselpaare mit öffentlichen und privaten Schlüsseln erstellen, die Sie zur Kommunikation mit anderen PGP-Benutzern benötigen. Es wird auch beschrieben, wie Sie Ihren öffentlichen Schlüssel verteilen und die öffentlichen Schlüssel von anderen erhalten, so daß Sie mit dem Austausch von verschlüsselten und unterschriebenen E-Mail-Nachrichten beginnen können.

Schlüsselkonzepte

PGP basiert auf einem allgemein anerkannten und sehr zuverlässigen *Verschlüsselungssystem mit öffentlichen Schlüsseln* (siehe Abbildung 3-1), mit dem Sie und andere PGP-Benutzer Schlüsselpaare erstellen können, die jeweils aus einem privaten Schlüssel und einem öffentlichen Schlüssel bestehen. Wie der Name schon sagt, haben nur Sie Zugriff auf Ihren privaten Schlüssel.
Zur Kommunikation mit einem anderen PGP-Benutzer benötigt dieser jedoch eine Kopie Ihres öffentlichen Schlüssels, und Sie benötigen eine Kopie seines öffentlichen Schlüssels. Sie benötigen Ihren privaten Schlüssel zum Unterschreiben der E-Mail-Nachrichten und Dateianhänge, die Sie an andere senden, sowie zur Entschlüsselung der von anderen erhaltenen Nachrichten und Dateianhänge. Umgekehrt gilt dasselbe Prinzip: Sie verwenden die öffentlichen Schlüssel anderer Personen, um verschlüsselte E-Mail-Nachrichten an sie zu senden und um ihre digitalen Unterschriften zu verifizieren.

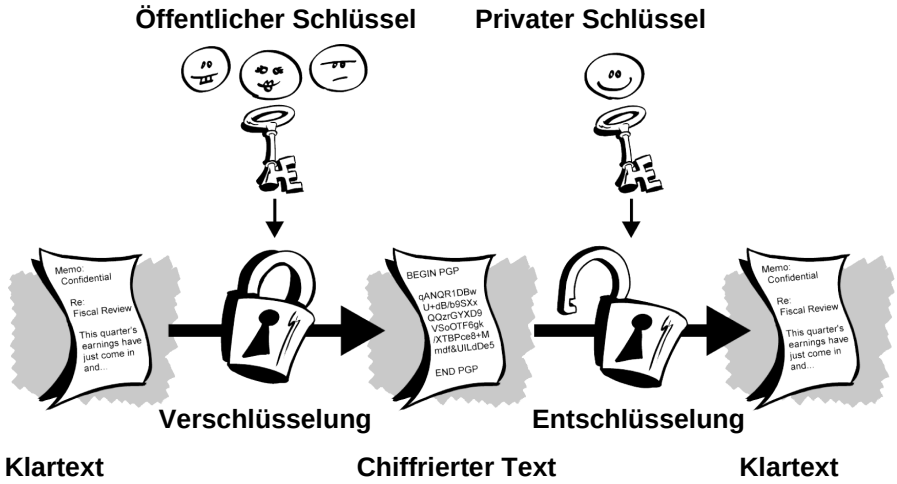


Abbildung 3-1. Kryptographie mit öffentlichen Schlüsseln

Schlüsselpaare erstellen

Wenn Sie diesen Schritt nicht bereits in einer älteren PGP-Version durchgeführt haben, müssen Sie zunächst ein neues Schlüsselpaar erstellen, bevor Sie verschlüsselte und unterschriebene E-Mail-Nachrichten senden oder empfangen. Ein Schlüsselpaar besteht aus zwei Schlüsseln: einem privaten Schlüssel, den nur Sie besitzen, und einem öffentlichen Schlüssel, den Sie frei an alle Personen verteilen, mit denen Sie korrespondieren. In PGPkeys erstellen Sie ein neues Schlüsselpaar mit Hilfe des PGP-Schlüsselerzeugungsassistenten, der Sie in diesem Prozeß begleitet.

❑ **HINWEIS:** Wenn Sie eine ältere PGP-Version aktualisieren, haben Sie wahrscheinlich bereits einen privaten Schlüssel erzeugt und den dazugehörigen öffentlichen Schlüssel an die Personen verteilt, mit denen Sie korrespondieren. In diesem Fall ist die im folgenden Abschnitt beschriebene Erstellung eines neuen Schlüsselpaares nicht erforderlich. Statt dessen legen Sie beim Ausführen der PGPkeys-Anwendung den Pfad für Ihre Schlüssel fest. Im Dialogfeld **Optionen** auf der Registerkarte **Dateien** können Sie jederzeit den Pfad Ihrer Schlüsselbunddateien bestimmen.

So erstellen Sie ein neues Schlüsselpaar

1. Öffnen Sie PGPkeys.

   Für das Öffnen von PGPkeys gibt es folgende Möglichkeiten:

   - Klicken Sie auf **Start–> Programme–> PGP–> PGPkeys**
   - Klicken Sie auf das PGPtray-Symbol ( ) in der Task-Leiste und dann auf „PGPkeys“.

     Oder

   - Klicken Sie auf die Schaltfläche , die sich auf der Symbolleiste Ihrer E-Mail-Anwendung befindet.

   PGPkeys wird geöffnet (siehe Abbildung 3-2).

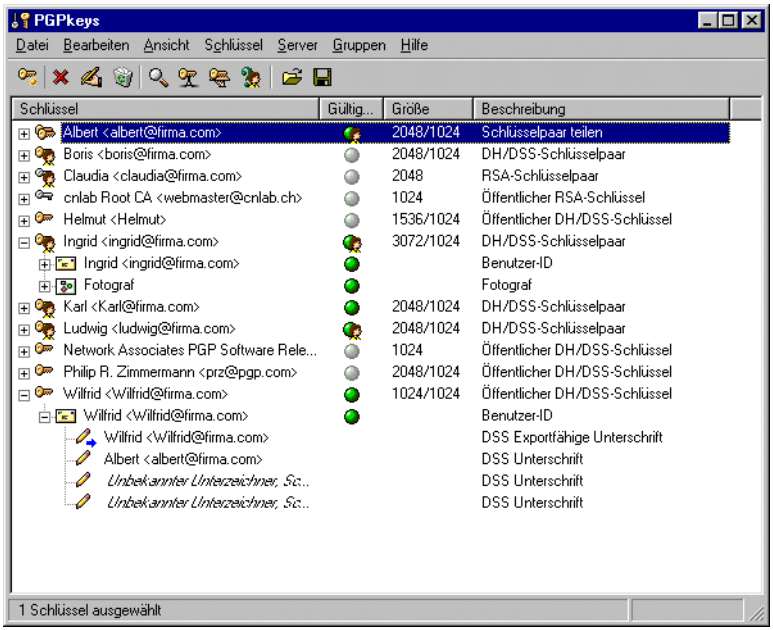
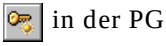


Abbildung 3-2. PGPkeys-Fenster

2. Klicken Sie auf die Schaltfläche  in der PGPkeys-Menüleiste.

   Der PGP-Schlüsselerzeugungsassistent zeigt im ersten Bildschirm einige einführende Informationen an.

3. Wenn Sie mit dem Lesen dieser Informationen fertig sind, klicken Sie auf **Weiter**, um zum nächsten Fenster zu wechseln.

   Sie werden vom PGP-Schlüsselerzeugungsassistenten dazu aufgefordert, Ihren Namen und Ihre E-Mail-Adresse einzugeben.

4. Geben Sie Ihren Namen in der ersten Zeile und Ihre E-Mail-Adresse in der zweiten Zeile ein.

   Die Eingabe Ihres tatsächlichen Namens und Ihrer E-Mail-Adresse ist nicht unbedingt erforderlich. Durch die Verwendung Ihres echten Namens ist es für andere Personen jedoch einfacher, Sie als den Eigentümer Ihres öffentlichen Schlüssels zu identifizieren. Indem Sie Ihre korrekte E-Mail-Adresse verwenden, können Sie und andere außerdem eine Plug-In-Funktion nutzen, die den entsprechenden Schlüssel an Ihrem aktuellen Schlüsselbund automatisch sucht, wenn Sie eine E-Mail-Nachricht an einen bestimmten Empfänger adressieren. Einige firmenweite Unterschriftenschlüssel und zusätzliche Entschlüsselungsschlüssel erfordern nicht die Angabe einer E-Mail-Adresse, da sie keine Einzelpersonen repräsentieren.

5. Klicken Sie auf **Weiter**, um zum nächsten Dialogfeld zu wechseln.

   Sie werden vom Schlüsselerzeugungsassistenten dazu aufgefordert, einen Schlüsseltyp zu wählen.

6. Entscheiden Sie sich für einen Diffie-Hellman / DSS- oder einen RSA-Schlüssel, und klicken Sie dann auf **Weiter**.

   HINWEIS: Wenn Ihre PGP-Version keine RSA-Unterstützung bietet, können Sie diesen Schritt unter Umständen nicht durchführen. Weitere Informationen zur RSA-Unterstützung finden Sie im mitgelieferten Dokument WhatsNew.

   In früheren PGP-Versionen wird zur Schlüsselerzeugung das ältere, als RSA bezeichnete Verfahren verwendet. Ab PGP-Version 5.0 können Sie auch Schlüssel eines neuen Typs erstellen, der auf der verbesserten Elgamal-Variante des Diffie-Hellman-Verfahrens basiert.

   - Wenn Sie mit Personen korrespondieren möchten, die noch mit RSA-Schlüsseln arbeiten, sollten Sie ein RSA-Schlüsselpaar erzeugen. Dieses ist mit älteren PGP-Versionen kompatibel.
   - Wenn Sie mit Personen korrespondieren möchten, die über PGP-Version 5.0 oder höher verfügen, können Sie das neue Verfahren nutzen und ein Diffie-Hellman / DSS-Schlüsselpaar erzeugen.
   - Wenn Sie in der Lage sein möchten, mit allen PGP-Benutzern E-Mail-Nachrichten auszutauschen, sollten Sie ein RSA- und ein Diffie-Hellman / DSS-Schlüsselpaar erstellen und dann abhängig von der PGP-Version des Empfängers das entsprechende Paar verwenden. Sie müssen ein separates Schlüsselpaar für jeden benötigten Schlüsseltyp erstellen.

7. Sie werden vom PGP-Schlüsselerzeugungsassistenten dazu aufgefordert, eine Größe für Ihre neuen Schlüssel festzulegen.

   Wählen Sie eine Schlüsselgröße zwischen 1024 und 3072 Bit, oder geben Sie eine benutzerdefinierte Schlüsselgröße zwischen 1024 und 4096 Bit ein.

   HINWEIS: Die Erzeugung eines benutzerdefinierten Schlüssels nimmt je nach Leistungsfähigkeit Ihres Rechners möglicherweise mehr Zeit in Anspruch.

Die Schlüsselgröße entspricht der Bitanzahl, die zum Erstellen des digitalen Schlüssels benötigt wird. Je größer der Schlüssel ist, desto geringer ist die Gefahr, daß er von jemandem decodiert wird. Allerdings wird mehr Zeit für das Entschlüsseln und Verschlüsseln benötigt. Sie müssen also zwischen einer schnelleren Durchführung der PGP-Funktionen, gewährleistet durch einen kleineren Schlüssel, und einer höheren Sicherheitsebene durch einen größeren Schlüssel wählen. Normalerweise ist ein Schlüssel mit 1024 Bit sicher genug. Ein größerer Schlüssel ist nur dann erforderlich, wenn die auszutauschenden Daten extrem wichtig und vertraulich und für Dritte von so großem Interesse sind, daß sich kosten- und zeitaufwendige kryptographische Anstrengungen zu seiner Decodierung lohnen würden.

HINWEIS: Bei der Erstellung eines Diffie-Hellman / DSS-Schlüsselpaares ist die Größe des DSS-Anteils des Schlüssels geringer oder gleich der Größe des Diffie-Hellman-Anteils des Schlüssels und ist auf eine maximale Größe von 1024 Bit begrenzt.

---

8. Klicken Sie auf **Weiter**, um zum nächsten Fenster zu wechseln.

   Sie werden vom PGP-Schlüsselerzeugungsassistenten dazu aufgefordert, festzulegen, wann die Gültigkeit des Schlüsselpaares ablaufen soll.

9. Geben Sie das Datum an, ab dem Ihre Schlüssel ihre Gültigkeit verlieren sollen. Verwenden Sie die Standardeinstellung **Nie**, wenn sie niemals ungültig werden sollen, oder geben Sie ein bestimmtes Datum ein, nach dem Ihre Schlüssel ihre Gültigkeit verlieren werden.

   Wenn Sie ein Schlüsselpaar erstellen und Ihren öffentlichen Schlüssel an alle Personen verteilt haben, mit denen Sie korrespondieren, verwenden Sie von diesem Zeitpunkt an wahrscheinlich immer dieselben Schlüssel. Unter bestimmten Umständen möchten Sie jedoch möglicherweise ein spezielles Schlüsselpaar nur für einen begrenzten Zeitraum verwenden. In diesem Fall verliert Ihr öffentlicher Schlüssel nach Ablauf der Gültigkeit für andere die Fähigkeit, E-Mail-Nachrichten an Sie zu verschlüsseln, kann aber weiterhin zur Verifizierung Ihrer digitalen Unterschrift verwendet werden. Ebenso kann Ihr privater Schlüssel nach Ablauf der Gültigkeit immer noch zur Entschlüsselung von E-Mail-Nachrichten verwendet werden, die vor dem Ablaufen Ihres öffentlichen Schlüssels an Sie gesendet wurden. Er kann aber nicht mehr zum Unterschreiben von E-Mail-Nachrichten an andere verwendet werden.

10. Klicken Sie auf **Weiter**, um zum nächsten Fenster zu wechseln.

    Sie werden vom Schlüsselerzeugungsassistenten dazu aufgefordert, eine Paßphrase einzugeben.

11. Geben Sie im Dialogfeld zur Eingabe der **Paßphrase** die Folge von Zeichen oder Wörtern ein, die Sie zur Gewährleistung des exklusiven Zugangs zu Ihrem persönlichen Schlüssel verwenden möchten. Drücken Sie zum Bestätigen Ihrer Eingabe die TABULATORTASTE, um zur nächsten Zeile zu gelangen. Wiederholen Sie hier die Eingabe Ihrer Paßphrase.

    Um zusätzliche Sicherheit zu gewährleisten, werden die von Ihnen eingegebenen Zeichen für die Paßphrase normalerweise nicht auf dem Bildschirm angezeigt. Wenn Sie sich jedoch sicher sind, unbeobachtet zu sein, und die Zeichen Ihrer Paßphrase bei der Eingabe sehen möchten, deaktivieren Sie das Kontrollkästchen **Eingabe verbergen**.

    HINWEIS: Ihre Paßphrase sollte aus mehreren Wörtern bestehen und kann Leerzeichen, Ziffern und Interpunktionszeichen enthalten. Denken Sie sich etwas aus, das Sie sich leicht merken können, aber das andere nicht erraten können. Bei der Paßphrase wird die Groß- und Kleinschreibung beachtet, d. h., es wird zwischen großen und kleinen Buchstaben unterschieden. Je länger Ihre Paßphrase und je größer die Verschiedenheit der in ihr enthaltenen Zeichen ist, desto sicherer ist sie. In starken Paßphrasen sind große und kleine Buchstaben, Ziffern, Interpunktionszeichen und Leerzeichen enthalten. Sie werden aber leichter vergessen. Weitere Informationen zur Auswahl einer Paßphrase finden Sie im Abschnitt „Erstellen einer einprägsamen Paßphrase“ auf Seite 30.

    WARNUNG: Keiner, nicht einmal die Mitarbeiter von Network Associates, kann eine vergessene Paßphrase wiederherstellen.

12. Klicken Sie auf **Weiter**, um den Schlüsselerzeugungsprozeß zu starten.

    Der PGP-Schlüsselerzeugungsassistent zeigt an, daß Ihr Schlüssel erzeugt wird.

    Wenn Sie eine unpassende Paßphrase eingegeben haben, wird vor der Erzeugung der Schlüssel eine Warnmeldung angezeigt, und Sie können nun entweder die schlechte Paßphrase akzeptieren oder eine sicherere Paßphrase eingeben, bevor Sie weitermachen. Weitere Informationen zu Paßphrasen finden Sie im Abschnitt „Erstellen einer einprägsamen Paßphrase“ auf Seite 30.

    Wenn nicht genügend Zufallswerte für die Erstellung des Schlüssels zur Verfügung stehen, wird das **PGP-Dialogfeld zur Erzeugung von Zufallswerten** angezeigt. Folgen Sie den Anweisungen im Dialogfeld, bewegen Sie die Maus, und drücken Sie einige beliebige Tasten, bis die

Statusleiste vollständig ausgefüllt ist. Durch die Bewegung der Maus und das Drücken der Tasten werden Zufallswerte erzeugt, die zur Erstellung eines eindeutigen Schlüsselpaares benötigt werden.

HINWEIS: PGPkeys sammelt fortlaufend Zufallswerte aus vielen Quellen im System, einschließlich Mausposition, Zeitabständen und Tastaturanschlägen. Wenn das Dialogfeld zur Erzeugung von Zufallswerten nicht angezeigt wird, bedeutet dies, daß PGP bereits alle benötigten Informationen zur Erzeugung eines Schlüsselpaares gesammelt hat.

Nachdem die Schlüsselerstellung gestartet wurde, kann es einige Zeit dauern, bis der Schlüssel erzeugt sind. Wenn Sie statt der Standardwerte eine andere Schlüsselgröße für einen Diffie-Hellman / DSS-Schlüssel festlegen, wird die Option zur schnelleren Schlüsselerzeugung nicht verwendet, so daß die Erstellung größerer Schlüssel einige Stunden in Anspruch nehmen kann. Wenn die Schlüsselerzeugung abgeschlossen ist, zeigt der PGP-Schlüsselerzeugungsassistent dies an.

13. Klicken Sie auf **Weiter**, um zum nächsten Fenster zu wechseln.

    Der PGP-Schlüsselerzeugungsassistent zeigt die erfolgreiche Erzeugung eines neuen Schlüsselpaares an und fragt, ob Sie Ihren öffentlichen Schlüssel an einen Certificate Server senden möchten.

14. Geben Sie an, ob der neue Schlüssel zum Standard-Server geschickt werden soll, und klicken Sie auf **Weiter** (der Standard-Server kann im Dialogfeld **Server Optionen** festgelegt werden).

    Wenn Sie Ihren öffentlichen Schlüssel an den Certificate Server senden, kann jeder Benutzer mit Zugang zu diesem Certificate Server bei Bedarf eine Kopie von Ihrem Schlüssel erhalten. Genauere Informationen finden Sie im Abschnitt „Ihren öffentlichen Schlüssel verteilen“ auf Seite 53.

    Wenn der Schlüsselerzeugungsprozeß abgeschlossen ist, wird das letzte Fenster angezeigt.

15. Klicken Sie auf **Fertig stellen**.

    Ein Schlüsselpaar, das Ihre neu erstellten Schlüssel darstellt, wird im PGPkeys-Fenster angezeigt. Jetzt können Sie Ihre Schlüssel näher untersuchen, indem Sie die Eigenschaften und Attribute der Schlüssel überprüfen. Sie können nun auch andere E-Mail-Adressen hinzufügen. Nähere Informationen zum Ändern der Informationen Ihres Schlüsselpaares finden Sie im Abschnitt „Neue Benutzernamen und Adressen einem Schlüsselpaar hinzufügen“ auf Seite 36.

Erstellen einer einprägsamen Paßphrase

Wenn Sie einmal eine Datei verschlüsselt haben und dann später feststellen mußten, daß Sie sie nicht wieder entschlüsseln konnten, werden Sie wissen, wie wichtig es ist, eine einprägsame Paßphrase zu wählen. Die meisten Anwendungen verlangen ein Paßwort mit drei bis acht Zeichen. Ein Einwort-Paßwort ist anfällig für einen „Wörterbuchangriff“, welcher darin besteht, einen Computer alle Wörter im Wörterbuch durchprobieren zu lassen, bis Ihr Paßwort gefunden wird. Zum Schutz gegen diese Art des Angriffs werden im allgemeinen Paßwörter aus einer Kombination von Groß- und Kleinbuchstaben, Zahlen, Satz- und Leerzeichen empfohlen. Dadurch kommt ein stärkeres Paßwort zustande, das aber unverständlich und daher leichter zu vergessen ist. Der Gebrauch von Einwort-Paßwörtern wird deshalb nicht empfohlen.

Eine Paßphrase ist weniger anfällig für einen „Wörterbuchangriff“. Dies wird einfach durch die Verwendung von mehreren Wörtern erreicht und nicht durch willkürliches Einfügen einer Menge nicht alphabetischer Zeichen zur Vereitelung eines „Wörterbuchangriffs“, was zu einer leicht zu vergessenden Paßphrase führt. Wenn Sie Ihre Paßphrase vergessen, kann dies wiederum zu einem verhängnisvollen Informationsverlust führen, da Sie in diesem Fall Ihre eigenen Dateien nicht mehr entschlüsseln können. Es ist jedoch unwahrscheinlich, daß Sie sich die Paßphrase wortwörtlich merken können, es sei denn, die von Ihnen gewählte Paßphrase ist sehr einprägsam. Wenn Sie eine Paßphrase einer plötzlichen Eingebung folgend auswählen, ist es eher wahrscheinlich, daß Sie sie vergessen. Wählen Sie statt dessen etwas, was Sie ohnehin schon im Langzeitgedächtnis „gespeichert“ haben. Dabei kann es sich um eine dumme Bemerkung handeln, die Sie vor Jahren einmal gehört haben und an die Sie sich bis heute erinnern. Verwenden Sie jedoch keine Wendung, die Sie in letzter Zeit jemandem gegenüber verwendet haben und auch kein berühmtes Zitat, da Ihre Paßphrase für einen raffinierten Hacker ja schwer zu erraten sein soll. Wenn die gewählte Wendung schon tief in Ihrem Langzeitgedächtnis verwurzelt ist, werden Sie sie wahrscheinlich nicht vergessen.

Wenn Sie leichtsinnig genug sind, Ihre Paßphrase aufzuschreiben und an Ihren Monitor oder in Ihre Schreibtischschublade zu kleben, sind diese Überlegungen ohnehin ohne Bedeutung.

Sicherungskopien für Schlüssel erstellen

Wenn Sie ein Schlüsselpaar erzeugt haben, sollten Sie eine Kopie erstellen und diese an einer sicheren Stelle ablegen, damit sie zur Verfügung steht, falls die Verwendung des Originalpaares einmal nicht möglich sein sollte. Beim Schließen von PGPkeys nach der Erstellung eines neuen Paares werden Sie von PGP aufgefordert, eine Sicherungskopie des Paares zu erstellen.

Ihre privaten und Ihre öffentlichen Schlüssel werden in verschiedenen Schlüsselbunddateien gespeichert. Diese Dateien können Sie problemlos wie andere Dateien auch an einer anderen Stelle auf Ihrer Festplatte oder auf einer Diskette speichern. Standardmäßig werden der private Schlüsselbund (SECRING.SKR) und der öffentliche Schlüsselbund (PUBRING.PKR) zusammen mit den anderen Programmdateien im Unterordner „PGP Keyrings“ Ihres PGP-Ordners gespeichert. Sie können die Sicherungskopien jedoch unter einem anderen Pfad speichern.

Sie werden regelmäßig von PGP zur Sicherung Ihrer Schlüssel aufgefordert. Wenn Sie festlegen, daß eine Sicherungskopie Ihrer Schlüssel erstellt werden soll, wird das Dialogfeld **Speichern unter** angezeigt, in dem Sie einen Zielpfad für die zu erstellenden Sicherungskopien Ihrer privaten und öffentlichen Schlüsselbunddateien angeben können.

Schutz eigener Schlüssel

Neben dem Erstellen von Sicherungskopien für Ihre Schlüssel sollten Sie Ihren privaten Schlüssel an einer besonders sicheren Stelle speichern. Obwohl Ihr privater Schlüssel durch eine Paßphrase geschützt ist, die nur Sie kennen sollten, ist es möglich, daß jemand Ihre Paßphrase entdeckt und dann mit Ihrem privaten Schlüssel Ihre E-Mail-Nachrichten entziffert oder Ihre digitale Unterschrift fälscht. Ihnen könnte beispielsweise jemand über die Schulter schauen und sehen, welche Tasten Sie drücken, oder er könnte die entsprechenden Signale auf dem Netzwerk oder sogar per Funk abfangen.

Um zu verhindern, daß jemand, dem Ihre Paßphrase in die Hände gelangen könnte, Ihren privaten Schlüssel verwendet, sollten Sie diesen nur auf Ihrem eigenen Rechner speichern. Wenn Ihr Rechner an ein Netzwerk angeschlossen ist, sollten Sie auch sicherstellen, daß Ihre Dateien nicht durch einen Sicherungskopiervorgang für das gesamte System automatisch erfaßt werden, wodurch andere Personen Zugang zu Ihrem privaten Schlüssel erhalten könnten. In Anbetracht des leichten Zugriffs auf Computer über Netzwerke sollten Sie Ihren privaten Schlüssel vielleicht auf einer Diskette aufbewahren, wenn Sie mit streng vertraulichen Informationen arbeiten. Wenn Sie dann vertrauliche Informationen lesen und unterschreiben möchten, benutzen Sie die Diskette wie einen herkömmlichen Schlüssel.

Als weitere Sicherheitsmaßnahme können Sie Ihrer privaten Schlüsselbunddatei einen anderen Namen zuweisen und sie an einer anderen Stelle als im Standarddateiverzeichnis von PGP speichern. Dadurch wird das Auffinden dieser Datei erschwert. Namen und Verzeichnisse für Ihre privaten und öffentlichen Schlüsselbunddateien legen Sie im Options-Dialogfeld von **PGPkeys** auf der Registerkarte **Dateien** fest.

Informationen Ihres Schlüsselpaares hinzufügen oder entfernen

Die folgenden Elemente Ihres Schlüsselpaares können jederzeit hinzugefügt, geändert oder entfernt werden:

- Eine Foto-Benutzer-ID
- Zusätzliche Teilschlüssel
- Der Name und die Adresse eines Benutzers
- Zugeordnete Rücknahmeschlüssel
- Ein X.509-Zertifikat
- Eigene Paßphrase

Hinzufügen von Foto-Benutzer-IDs zu Schlüsseln

Sie können eine Foto-Benutzer-ID zu Ihrem Diffie-Hellman-/DSS-Schlüssel hinzufügen.

. **WARNUNG:** Obwohl Sie zum Verifizieren die Foto-Benutzer-ID anzeigen können, die Sie mit einem Schlüssel erhalten, sollten Sie immer sichergehen und die digitalen Fingerabdrücke vergleichen. Weitere Informationen zur Authentisierung finden Sie im Abschnitt „ Öffentliche Schlüssel anderer Benutzer verifizieren“ auf Seite 108.

So fügen Sie Ihr Foto Ihrem öffentlichen Schlüssel hinzu

1. Öffnen Sie PGPkeys.
2. Wählen Sie Ihr Schlüsselpaar aus, und klicken Sie im Menü **Schlüssel** auf **Foto hinzufügen**.

   Das Dialogfeld **Foto hinzufügen** wird geöffnet (siehe Abbildung 3-3).

Abbildung 3-3. Dialogfeld „Foto hinzufügen“

3. Ziehen Sie Ihr Foto auf das Dialogfeld „Foto hinzufügen“, oder fügen Sie es ein. Sie können es auch durch Klicken auf **Datei auswählen** suchen.

   HINWEIS: Das Foto muß eine JPG- oder eine BMP-Datei sein. Zur Erzielung einer optimalen Bildqualität sollten Sie das Bild vor dem Einfügen in das Dialogfeld **Foto hinzufügen** auf 120 x 144 beschneiden. Andernfalls wird das Bild von PGP skaliert.

4. Klicken Sie auf **OK**.

   Das **Dialogfeld zur Eingabe der Paßphrase** wird geöffnet (siehe Abbildung 3-4).

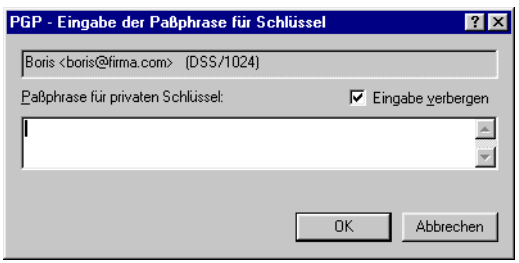


Abbildung 3-4. Dialogfeld „PGP - Eingabe der Paßphrase für Schlüssel“

5. Geben Sie Ihre Paßphrase in dem dafür vorgesehenen Feld ein, und klikken Sie dann auf **OK**.

   Ihre Foto-Benutzer-ID wird Ihrem öffentlichen Schlüssel hinzugefügt und im PGPkeys-Fenster aufgelistet. Nun können Sie Ihren Schlüssel an einen Schlüssel-Server senden. Zusätzliche Anweisungen dazu finden Sie im Abschnitt „So senden Sie Ihren öffentlichen Schlüssel an einen Certificate Server“ auf Seite 54.

So ersetzen Sie Ihre Foto-Benutzer-ID

1. Öffnen Sie PGPkeys.
2. Wählen Sie Ihr Schlüsselpaar aus.
3. Markieren Sie das zu ersetzende Foto.
4. Wählen Sie im Menü **Bearbeiten** die Option **Löschen**.
5. Fügen Sie das neue Foto unter Einhaltung der Anweisungen im Abschnitt „So fügen Sie Ihr Foto Ihrem öffentlichen Schlüssel hinzu“ auf Seite 33 hinzu.

Neue Teilschlüssel erstellen

Jeder Diffie-Hellman-/DSS-Schlüssel besteht aus zwei Schlüsseln: einem DSS-Unterschriftsschlüssel und einem Diffie-Hellman-Verschlüsselungsteilschlüssel. PGP Version 6.5 bietet die Möglichkeit, neue Verschlüsselungsschlüssel zu erstellen und wieder zurückzunehmen, ohne Ihren Haupt-Unterzeichnerschlüssel und die auf ihm gesammelten Unterschriften aufgeben zu müssen. Diese Funktion wird beispielsweise verwendet, um mehrere Teilschlüssel zu erzeugen, die für den abschnittsweisen Einsatz innerhalb der Gültigkeitsdauer des Schlüssels bestimmt sind. Wenn Sie beispielsweise einen Schlüssel erstellen, der in drei Jahren seine Gültigkeit verlieren wird, könnten Sie zusätzlich noch drei Teilschlüssel für jedes Jahr der Gültigkeitsdauer des Schlüssels erzeugen. Dies kann sich als eine nützliche Sicherheitsmaßnahme erweisen und stellt einen automatischen Weg dar, von Zeit zu Zeit auf einen neuen Verschlüsselungsschlüssel zu wechseln, ohne einen neuen öffentlichen Schlüssel erstellen und verteilen zu müssen.

So erstellen Sie neue Teilschlüssel

1. Öffnen Sie PGPkeys.
2. Wählen Sie Ihr Schlüsselpaar aus, und klicken Sie im Menü **Schlüssel** auf **Schlüsseleigenschaften**. Sie können auch auf  klicken.

   Das entsprechende **Eigenschaftsdialogfeld** wird geöffnet.
3. Klicken Sie auf die Registerkarte **Teilschlüssel**.

   Das Dialogfeld zur Eingabe der **Teilschlüssel** wird geöffnet (siehe Abbildung 3-5).

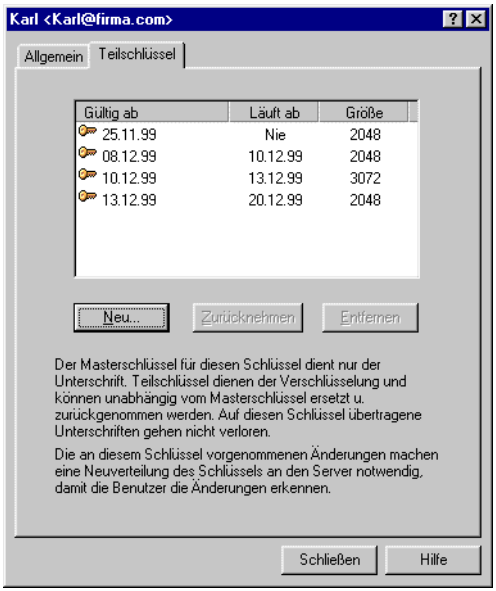


Abbildung 3-5. Registerkarte mit Eigenschaften von PGP-Schlüsseln (Fenster „Teilschlüssel“)

4. Klicken Sie auf **Neu**, um einen neuen Teilschlüssel zu erstellen.

   Das Dialogfeld **Neuer Teilschlüssel** wird geöffnet.
5. Wählen Sie eine Schlüsselgröße von 1024 bis 3072 Bit, oder geben Sie eine benutzerdefinierte Schlüsselgröße von 1024 bis 4096 Bit ein.
6. Geben Sie das Anfangsdatum an, zu dem der Teilschlüssel aktiviert werden soll.

7. Geben Sie dann an, wann Ihr Teilschlüssel ablaufen soll. Verwenden Sie die Standardeinstellung **Nie**, wenn er niemals ungültig werden soll, oder geben Sie ein bestimmtes Datum ein, nach dem der Teilschlüssel seine Gültigkeit verliert.
8. Klicken Sie auf **OK**.

   Das **Dialogfeld zur Eingabe der Paßphrase** wird angezeigt.
9. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **OK**.

   Ihr neuer Teilschlüssel wird im Fenster „Teilschlüssel“ angezeigt.

Neue Benutzernamen und Adressen einem Schlüsselpaar hinzufügen

Möglicherweise möchten Sie das gleiche Schlüsselpaar für mehrere Benutzernamen bzw. E-Mail-Adressen verwenden. Nach dem Erstellen eines neuen Schlüsselpaares können Sie dem Schlüssel weitere Namen und Adressen hinzufügen. Sie können neue Benutzernamen oder E-Mail-Adressen nur dann hinzufügen, wenn Sie sowohl über private als auch öffentliche Schlüssel verfügen.

So fügen Sie Schlüsseln neue Benutzernamen und Adressen hinzu

1. Öffnen Sie PGPkeys.
2. Wählen Sie das Schlüsselpaar aus, dem Sie einen neuen Benutzernamen oder eine neue Adresse hinzufügen möchten.
3. Wählen Sie im Menü **Schlüssel** die Option **Hinzufügen/Name**.

   Das Dialogfeld **PGP - Neuer Benutzername** wird angezeigt (siehe Abbildung 3-6).)

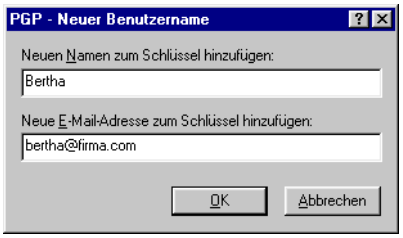


Abbildung 3-6. Dialogfeld „PGP - Neuer Benutzername“

4. Geben Sie den neuen Namen und die neue E-Mail-Adresse in die betreffenden Felder ein, und klicken Sie auf **OK**.

   Das Dialogfeld **PGP-Paßphrase eingeben** wird angezeigt.

5. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **OK**.

   Der neue Name wird am Ende der zu dem Schlüssel gehörenden Benutzernamenliste hinzugefügt. Wenn Sie den neuen Benutzernamen und die neue Benutzeradresse als primäre Kennung für Ihren Schlüssel festlegen möchten, markieren Sie den Namen und die Adresse, und wählen Sie im Menü **Schlüssel** die Option **Als Primärname einstellen** aus.

So legen Sie einen zugeordneten Rücknahmeschlüssel fest

Unter Umständen geht Ihre Paßphrase irgendwann verloren, oder Sie verlieren Ihren privaten Schlüssel. In diesem Fall können Sie Ihren Schlüssel nicht mehr verwenden und Ihren alten Schlüssel auch nicht zurücknehmen, wenn Sie einen neuen erstellen. Um sich gegen diesen Fall abzusichern, können Sie an Ihrem öffentlichen Schlüsselbund für die Zurücknahme Ihres Schlüssels einen Rücknahmeschlüssel bestimmen. Der Halter dieses anderen Schlüssels kann dann so wie Sie selbst zuvor Ihren DH / DSS-Schlüssel zurücknehmen und an den Server senden.

So fügen Sie einen zugeordneten Rücknahmeschlüssel Ihrem öffentlichen Schlüssel hinzu

1. Öffnen Sie PGPkeys.
2. Markieren Sie das Schlüsselpaar, dem Sie einen Rücknahmeschlüssel zuordnen möchten.
3. Wählen Sie im Menü **Schlüssel** die Option **Hinzufügen/Rücknahmeschlüssel**.

   Das angezeigte Dialogfeld enthält eine Liste mit Schlüsseln.

4. Wählen Sie in der Benutzer-ID-Liste die Schlüssel, die zugeordnete Rücknahmeschlüssel sein sollen.
5. Klicken Sie auf **OK**.

   Ein Dialogfeld zur Bestätigung des Vorgangs wird angezeigt.

6. Klicken Sie auf **OK**, um fortzufahren.

   Das Dialogfeld zur Eingabe der **Paßphrase** wird angezeigt.

7. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **OK**.

8. Die gewählten Schlüssel sind jetzt autorisierte Rücknahmeschlüssel. Zur Optimierung der Schlüsselverwaltung sollten Sie eine aktuelle Kopie Ihres Schlüssels an die Eigentümer der Rücknahmeschlüssel verteilen oder den Schlüssel auf den Server laden. Anweisungen dazu finden Sie im Abschnitt „Ihren öffentlichen Schlüssel verteilen“ auf Seite 53.

X.509-Zertifikate PGP-Schlüsseln hinzufügen

HINWEIS: In diesem Abschnitt wird beschrieben, wie Sie bei Net Tools PKI Server Ihrem Schlüsselpaar ein X.509-Zertifikat hinzufügen.

Ein digitales X.509-Zertifikat ist ein anerkanntes elektronisches Dokument zur Prüfung der Identität und der Eigentumsrechte öffentlicher Schlüssel in einem Kommunikationsnetzwerk.

Mit Hilfe der Menüoptionen von PGP und der *Zertifizierungsinstanz* (CA) Ihres Unternehmens, oder auch einer öffentlichen CA (z. B. VeriSign), können Sie ein digitales X.509-Zertifikat anfordern.

Das Hinzufügen eines X.509-Zertifikats zu einem Schlüsselpaar umfaßt vier wichtige Schritte. Zunächst muß das Root-CA-Zertifikat bei der CA angefordert und dem PGP-Schlüsselbund hinzugefügt werden. Nehmen Sie im Feld „CA-Optionen“ von PGPkeys die entsprechenden Einstellungen für die Zertifizierungsinstanz vor. Fordern Sie bei der CA ein Zertifikat an. Ihre Anfrage nach einem X.509-Zertifikat wird von der CA verifiziert und unterschrieben. (Durch die Unterschrift der CA auf dem Zertifikat wird es ermöglicht, an den Identifizierungsinformationen oder dem öffentlichen Schlüssel vorgenommene Manipulationen festzustellen. Außerdem besagt die Unterschrift, daß die CA die im Zertifikat enthaltenen Informationen für gültig befindet.) Fügen Sie abschließend das von der CA ausgegebene Zertifikat Ihrem Schlüsselpaar hinzu.

So fügen Sie Ihrem PGP-Schlüsselpaar ein X.509-Zertifikat hinzu

1. **Fordern Sie das Root-CA-Zertifikat an und fügen Sie es Ihrem PGP-Schlüsselbund hinzu.**

   Führen Sie hierzu die folgenden Schritte durch:

   1. Starten Sie Ihren Webbrowser und stellen Sie eine Verbindung zur CA-Anmeldung her. Falls Ihnen die entsprechende URL nicht bekannt ist, erfragen Sie sie beim zuständigen PGP- bzw. PKI-Administrator.

2. Klicken Sie auf die Verknüpfung zum **Herunterladen des CA-Zertifikats**. Wählen Sie eine Zertifizierungsinstanz und das zugehörige Zertifikat aus der Dropdown-Liste.

3. Klicken Sie auf die Schaltfläche zur Untersuchung des Zertifikats. Kopieren Sie dann den Schlüsselblock für das Root-CA-Zertifikat, und fügen Sie diesen in PGPkeys ein.

   Das Dialogfeld **Schlüssel importieren** wird angezeigt und das Root-CA-Zertifikat in Ihren Schlüsselbund importiert.

4. Unterzeichnen Sie das Root-CA-Zertifikat mit Ihrem Schlüssel, um es gültig zu machen. Öffnen Sie dann das Dialogfeld „Schlüsseleigenschaften“ und stellen Sie den Vertrauensgrad ein. Es muß ein Vertrauensgrad für die Root-CA eingestellt werden.

2. Konfigurieren Sie die Registerkarte für CA-Optionen.

Führen Sie hierzu die folgenden Schritte durch:

1. Wählen Sie im Menü **Bearbeiten** von PGPkeys die Option **Optionen**, und klicken Sie dann auf die Registerkarte **CA**.

   Die Registerkarte **CA** wird angezeigt (siehe Abbildung 3-7).

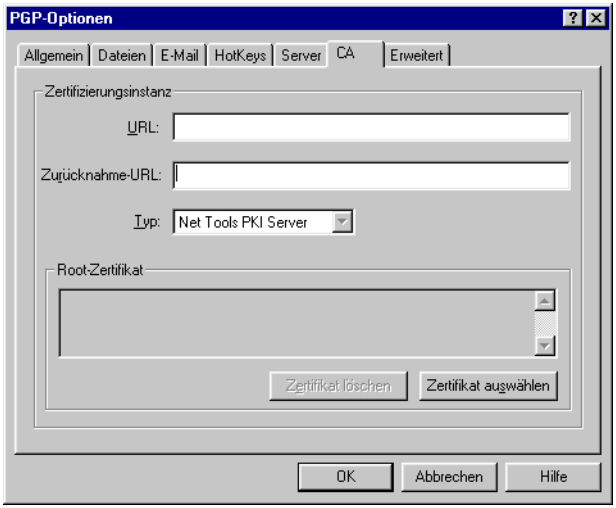


Abbildung 3-7. Dialogfeld „PGP-Optionen“ (Registerkarte „CA“)

2. Geben Sie die URL der CA in das entsprechende Textfeld ein, also beispielsweise https://nnn.nnn.nnn.nnn:nnnnn (die gleiche URL, die Sie für die Anforderung der Root-CA verwendet haben).

3. Falls Sie über eine separate URL zur Anforderung von Listen zurückgenommener Zertifikate (CRL) verfügen, geben Sie diese in das zugehörige Textfeld ein.

   Falls Ihnen die URL zur Zurücknahme nicht bekannt ist, belassen Sie dieses Feld leer oder erfragen Sie sie beim zuständigen PGP- bzw. PKI-Administrator.

4. Geben Sie im Dialogfeld **Typ** den Namen Ihrer Zertifizierungsinstanz ein. Sie haben folgende Optionen:

   - Net Tools PKI Server
   - VeriSign OnSite
   - Entrust

5. Klicken Sie auf die Schaltfläche **Zertifikat auswählen**, und wählen Sie das angeforderte Root-CA-Zertifikat aus.

Im Textfeld **Root-Zertifikat** werden Informationen zum ausgewählten Root-CA-Zertifikat angezeigt. Die Zertifikatsterminologie ist richtlinienabhängig. Normalerweise gilt für X.509-Zertifikate die folgende Terminologie:

BN (Bekannter Name)	Häufig die Beschreibung des Zertifikatstyps (z. B. „Root“).
E-MAIL	Die E-Mail-Adresse des Zertifikatsinhabers.
UA (Unternehmensabteilung)	Die Abteilung, der das Zertifikat zugeordnet ist (z. B. „Buchhaltung“).
U (Unternehmen)	Normalerweise der Name des Unternehmens, dem das Zertifikat zugeordnet ist (z. B. „Sicheres Unternehmen“).
S (Standort)	Der Standort des Zertifikatsinhabers (z. B. „München“).

6. Klicken Sie auf **OK**.

3. Fordern Sie ein Zertifikat an.

Führen Sie hierzu die folgenden Schritte durch:

1. Klicken Sie mit der rechten Maustaste auf Ihr PGP-Schlüsselpaar, und wählen Sie **Schlüssel –> Hinzufügen/Zertifikat** im Kontextmenü.

   Das Dialogfeld **Zertifikatsattribute** wird angezeigt (siehe Abbildung 3-8).

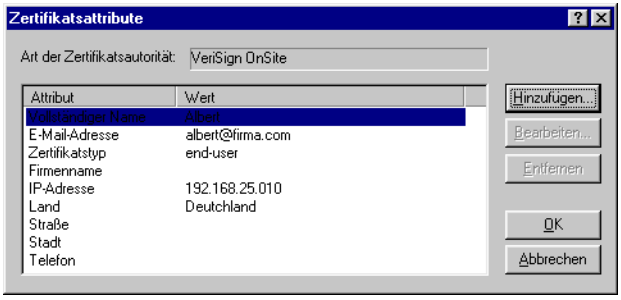


Abbildung 3-8. Dialogfeld „Zertifikatsattribute“

2. Verifizieren Sie die Zertifikatsattribute und verwenden Sie die Schaltflächen **Hinzufügen**, **Bearbeiten** und **Entfernen**, um erforderliche Änderungen vorzunehmen, und klicken Sie danach auf **OK**. Das Dialogfeld **PGP-Paßphrase eingeben** wird angezeigt.

3. Geben Sie die Paßphrase für Ihr Schlüsselpaar ein, und klicken Sie anschließend auf **OK**.

   Die Statusleiste **PGP - Server-Status** wird angezeigt (siehe Abbildung 3-9).

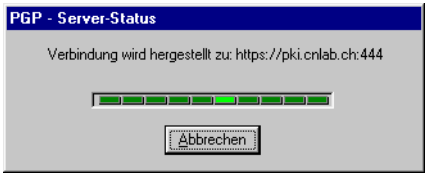


Abbildung 3-9. Statusleiste „PGP - Server-Status“

Die Zertifikatsanfrage wird automatisch an den CA-Server geschickt. Der Server authentisiert sich automatisch bei Ihrem Computer und nimmt Ihre Anfrage entgegen.

Der PGP- bzw. PKI-Administrator Ihres Unternehmens überprüft die Informationen, die Sie in der Anfrage gemacht haben. Die Identifikationsinformationen und der öffentliche Schlüssel werden kombiniert und digital mit der eigenen Unterschrift der CA unterschrieben, um Ihr neues Zertifikat zu erstellen.

Sie erhalten eine E-Mail vom Administrator, die Sie über das abholbereite Zertifikat informiert.

4. Rufen Sie das Zertifikat ab, und fügen Sie es Ihrem PGP-Schlüsselpaar hinzu.

Führen Sie hierzu die folgenden Schritte durch:

1. Wählen Sie in PGPkeys den Schlüssel aus, für den Sie das Zertifikat angefordert haben.
2. Klicken Sie im Menü **Server** auf **Zertifikat abrufen**.

   PGP stellt eine Verbindung mit dem CA-Server her, um Ihr neues X.509-Zertifikat automatisch abzurufen und es Ihrem PGP-Schlüssel hinzuzufügen.
3. Falls Sie PGPnet ausführen, stellen Sie dieses Zertifikat als Ihren X.509-Authentisierungsschlüssel in PGPnet ein **(Ansicht –> Optionen -> Authentisierung**).

Eigene Paßphrase ändern

Es empfiehlt sich, Ihre Paßphrase in regelmäßigen Abständen – etwa alle drei Monate – zu ändern. Noch wichtiger ist jedoch, daß Sie Ihre Paßphrase sofort ändern, wenn Sie das Gefühl haben, daß sie unsicher geworden ist, beispielsweise, wenn sie bei der Eingabe beobachtet wurden.

So ändern Sie Ihre Paßphrase

1. Öffnen Sie PGPkeys.
2. Markieren Sie den Schlüssel, dessen Paßphrase Sie ändern möchten.
3. Wählen Sie im Menü **Schlüssel** die Option **Schlüsseleigenschaften** oder klicken Sie auf  , um das Dialogfeld **Schlüsseleigenschaften** zu öffnen.

Das Dialogfeld **Schlüsseleigenschaften** wird geöffnet (siehe Abbildung 3-10).

Abbildung 3-10. Dialogfeld „Schlüsseleigenschaften“ (Registerkarte „Allgemein“)

4. Klicken Sie auf die Schaltfläche **Paßphrase ändern**.

   Das Dialogfeld zur Eingabe der **Paßphrase** wird angezeigt.

   HINWEIS: Wenn Sie die Paßphrase für einen geteilten Schlüssel ändern möchten, müssen Sie zuerst die Schlüsselteile wieder zusammensetzen. Klicken Sie auf die Schaltfläche zum Zusammensetzen der Schlüsselteile. Informationen zum Zusammenführen von Schlüsselteilen finden Sie im Abschnitt „Dateien mit einem geteilten Schlüssel unterschreiben und entschlüsseln“ auf Seite 88.

   ---

5. Geben Sie Ihre aktuelle Paßphrase in dem dafür vorgesehenen Feld ein, und klicken Sie dann auf **OK**.

   Daraufhin wird das Dialogfeld **Paßphrase ändern** angezeigt.

6. Geben Sie Ihre neue Paßphrase in das erste Textfeld ein. Drücken Sie die TABULATORTASTE, um den Cursor in das nächste Textfeld zu setzen. Bestätigen Sie Ihre Eingabe, indem Sie Ihre neue Paßphrase nochmals eingeben.

7. Klicken Sie auf **OK**.

WARNUNG: Wenn Sie Ihre Paßphrase ändern, weil Sie glauben, daß sie unsicher geworden ist, sollten Sie alle Sicherungskopien Ihrer Schlüsselbunde sowie Ihren freien Speicherplatz löschen.

Schlüssel oder Unterschrift von PGP-Schlüsselbund löschen

Bei Bedarf können Sie Schlüssel oder Unterschriften von Ihrem PGP-Schlüsselbund löschen. Aus einem Schlüssel gelöschte Unterschriften oder Schlüssel werden unwiederherstellbar entfernt. Unterschriften und Benutzer-IDs können erneut zu einem Schlüssel hinzugefügt werden und ein importierter öffentlicher Schlüssel kann wieder zu Ihrem Schlüsselbund hinzugefügt werden. Ein privater Schlüssel jedoch, der nur an diesem Schlüsselbund vorhanden ist, kann nicht neu erstellt werden, und alle Nachrichten, die mit den Kopien des dazugehörigen öffentlichen Schlüssels verschlüsselt wurden, können nicht mehr entschlüsselt werden.

HINWEIS: Falls Sie eine mit Ihrem öffentlichen Schlüssel verbundene Unterschrift oder Benutzer-ID auf einem Certificate Server löschen möchten, finden Sie die erforderlichen Informationen unter „Eigenen Schlüssel auf einem Certificate Server aktualisieren“ auf Seite 55.

So löschen Sie einen Schlüssel oder eine Unterschrift aus Ihrem PGP-Schlüsselbund

1. Öffnen Sie PGPkeys.
2. Wählen Sie den Schlüssel oder die Unterschrift aus, die Sie löschen möchten.
3. Wählen Sie im Menü **Bearbeiten** die Option **Löschen**, oder klicken Sie in der PGPkeys-Symbolleiste auf  .

   Ein Dialogfeld zur Bestätigung des Löschvorgangs wird angezeigt.
4. Klicken Sie auf die Schaltfläche **OK**.

Schlüssel teilen und wieder zusammensetzen

Mit Hilfe eines Verschlüsselungsverfahrens, das als Blakely-Shamir-Splitting bezeichnet wird, kann jeder private Schlüssel in mehrere Teile für verschiedene „Halter“ aufgeteilt werden. Die Verwendung dieses Verfahrens empfiehlt sich für Schlüssel mit sehr hoher Sicherheitsebene. Bei Network Associates wird beispielsweise ein firmenweiter Schlüssel auf mehrere Mitarbeiter aufgeteilt. Wenn mit dem Schlüssel unterzeichnet werden muß, werden die Teile für die Dauer der Unterzeichnung wieder zusammengesetzt.

Geteilten Schlüssel erstellen

Zum Aufteilen eines Schlüssels markieren Sie das gewünschte Schlüsselpaar und wählen im Menü **Schlüssel** die **Schlüsselaufteilung**. Sie werden dann aufgefordert, anzugeben, wie viele Teile für das Zusammensetzen des Schlüssels eingeplant werden sollen. Die Teile werden als Dateien gespeichert, die entweder mit dem öffentlichen Schlüssel eines der Halter oder, wenn der Halter über keinen öffentlichen Schlüssel verfügt, mit einem konventionellen Verschlüsselungsverfahren verschlüsselt werden. Bei Versuchen, mit dem geteilten Schlüssel zu unterschreiben oder zu entschlüsseln, versucht PGP automatisch, den Schlüssel wieder zusammenzusetzen. Informationen zum Zusammensetzen eines aufgeteilten Schlüssels finden Sie im Abschnitt „Dateien mit einem geteilten Schlüssel unterschreiben und entschlüsseln“ auf Seite 88.

So teilen Sie einen Schlüssel in mehrere Teile

1. Öffnen Sie PGPkeys.
2. Erstellen Sie zum Teilen in PGPkeys ein neues Schlüsselpaar, oder wählen Sie ein bereits vorhandenes Schlüsselpaar aus.
3. Klicken Sie im Menü **Schlüssel** auf **Schlüsselaufteilung**.

Das Dialogfeld **Schlüsselaufteilung** wird über dem PGPkeys-Fenster angezeigt (siehe Abbildung 3-11).

Abbildung 3-11. Dialogfeld „Schlüsselaufteilung“

4. Weisen Sie dem Schlüsselpaar Schlüsselhalter zu, indem Sie deren Schlüssel aus dem PGPkeys-Fenster in die Liste **Halter von Schlüsselteilen** des Dialogfelds **Schlüsselaufteilung** ziehen.

   Zum Hinzufügen eines Halters ohne öffentlichen Schlüssel klicken Sie im Dialogfeld **Schlüsselaufteilung** auf **Hinzufügen**, geben den Namen der Person ein und lassen diese dann ihre Paßphrase eingeben.

5. Wenn alle Halter erfaßt sind, können Sie die Anzahl der Schlüsselteile angeben, die für das Entschlüsseln oder Unterschreiben mit diesem Schlüssel notwendig sind.

   Der Schlüssel in Abbildung 3-12 setzt sich beispielsweise aus insgesamt vier Teilen zusammen und die Anzahl der für das Entschlüsseln oder Unterschreiben benötigten Schlüsselteile ist auf drei festgelegt. Damit wird ein Puffer geschaffen für den Fall, daß einer der Halter seinen Schlüsselteil nicht angeben kann oder seine Paßphrase vergessen hat.

Abbildung 3-12. Dialogfeld „Schlüsselaufteilung“ (Beispiel)

Standardmäßig ist jeder Halter für ein Schlüsselteil verantwortlich. Wenn Sie die Anzahl der im Besitz eines Halters befindlichen Teile erhöhen möchten, klicken Sie in der Liste der Halter auf den entsprechenden Namen, um ihn im Textfeld darunter anzuzeigen. Geben Sie die neue Anzahl der Schlüsselteile ein, oder wählen Sie mit Hilfe der Pfeile einen neuen Wert.

6. Klicken Sie auf **Schlüssel teilen**.

   Im angezeigten Dialogfeld werden Sie aufgefordert, ein Verzeichnis anzugeben, in dem die Teile abgelegt werden sollen.

7. Wählen Sie ein Verzeichnis zum Ablegen der Schlüsselteile.

   Das Dialogfeld zur Eingabe der **Paßphrase** wird angezeigt.

8. Geben Sie die Paßphrase für den Schlüssel ein, den Sie teilen möchten, und klicken Sie auf **OK**.

   Ein Dialogfeld zur Bestätigung des Vorgangs wird angezeigt.

9. Klicken Sie auf **Ja**, um den Schlüssel zu teilen.

Der Schlüssel wird geteilt, und die Teile werden in dem von Ihnen angegebenen Verzeichnis gespeichert. Jedes Schlüsselteil wird mit dem Namen des Halters als Dateinamen und der Erweiterung .SHF (siehe Beispiel unten) gespeichert.

10. Verteilen Sie die Schlüsselteile an deren Besitzer, und löschen Sie dann die lokalen Kopien.

    Wenn ein Schlüssel auf mehrere Halter aufgeteilt wurde, versucht PGP bei Versuchen, mit dem geteilten Schlüssel zu unterschreiben oder zu verschlüsseln, automatisch, den Schlüssel wieder zusammenzusetzen. Eine Anleitung zum Zusammensetzen eines geteilten Schlüssels, um damit Dateien zu unterschreiben oder zu entschlüsseln, finden Sie im Abschnitt „Dateien mit einem geteilten Schlüssel unterschreiben und entschlüsseln“ auf Seite 88.

Zusammensetzen geteilter Schlüssel

Wenn ein Schlüssel auf mehrere Halter aufgeteilt wurde, versucht PGP bei Versuchen, mit dem geteilten Schlüssel zu unterschreiben oder zu verschlüsseln, automatisch, den Schlüssel wieder zusammenzusetzen. Der Schlüssel kann lokal oder über das Netzwerk wieder zusammengesetzt werden.

Zum lokalen Zusammensetzen von Schlüsseln müssen die Halter von Schlüsselteilen an dem dafür vorgesehenen Computer anwesend sein. Jeder Halter von Schlüsselteilen muß die Paßphrase für seinen Schlüsselteil eingeben.

Beim Zusammensetzen der Schlüsselteile über das Netz müssen die Halter die Echtheit Ihrer Schlüssel bestätigen und diese entschlüsseln, bevor sie sie über das Netz schicken. Die TLS-Funktion (Transport Layer Security; TLS) von PGP gewährleistet die Sicherheit der Verbindung zur Übertragung der Schlüsselteile. Dadurch können mehrere Benutzer an verschiedenen Standorten mit ihrem Schlüsselteil ohne Risiko unterzeichnen und entschlüsseln.

WICHTIG: Vor Empfang der einzelnen Schlüsselteile über das Netz sollten Sie die Fingerabdrücke der einzelnen Halter überprüfen und deren jeweiligen öffentlichen Schlüssel unterschreiben, damit der Authentisierungsschlüssel legitim ist. Anleitungen zum Verifizieren eines Schlüsselpaares finden Sie im Abschnitt „Mit digitalen Fingerabdrücken verifizieren“ auf Seite 64.

Geteilten Schlüssel zusammensetzen

1. Kontaktieren Sie alle Halter des geteilten Schlüssels. Das lokale Zusammensetzen der Schlüsselteile setzt die Anwesenheit der Halter am entsprechenden Computer voraus.

   Zur Zusammenführung der Schlüsselteile über das Netz müssen alle Halter an den einzelnen Standorten die entsprechenden Vorbereitungen für das Senden Ihres Schlüsselteils getroffen haben. Die Halter von Schlüsselteilen müssen über folgendes verfügen:

   – Einen Schlüsselteil und ein Paßwort

   – Ein Schlüsselpaar (zur Authentisierung für den Computer, auf dem die Schlüsselteile zusammengeführt werden)

   – Eine Netzwerkverbindung

   – Die IP-Adresse oder den Domänennamen des Computers, auf dem die Schlüsselteile zusammengeführt werden.

2. Wählen Sie auf dem für die Zusammenführung verwendeten Computer im Windows-Explorer die Datei(en), die Sie mit dem geteilten Schlüssel unterzeichnen oder entschlüsseln möchten.

3. Klicken Sie mit der rechten Maustaste auf die Dateien, und wählen Sie im PGP-Menü den Befehl **Unterschreiben** oder **Entschlüsseln**.

   Das Dialogfeld **PGP – Eingabe der Paßphrase für ausgewählten Schlüssel** wird angezeigt. Der geteilte Schlüssel ist markiert.

4. Klicken Sie auf **OK**, um den ausgewählten Schlüssel wieder zusammenzusetzen.

   Das Dialogfeld **Sammlung der Schlüsselteile** wird angezeigt (Abbildung 3-13).

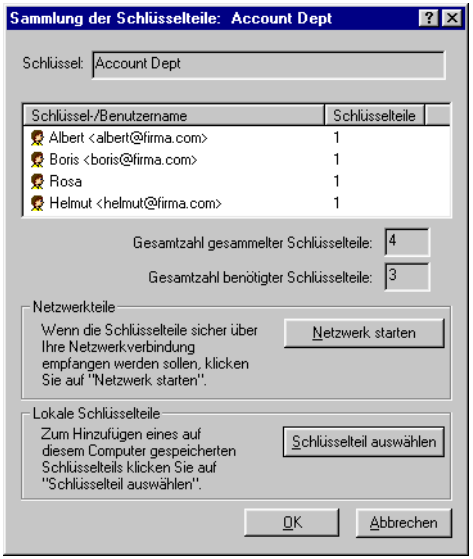


Abbildung 3-13. Dialogfeld „Sammlung der Schlüsselteile“

5. Führen Sie einen der folgenden Schritte aus:

   - **Wenn Sie die Schlüsselteile lokal zusammensetzen**, klicken Sie auf **Schlüsselteil auswählen**, und suchen Sie dann die mit dem geteilten Schlüssel verknüpften Schlüsselteile. Die Schlüsselteile können über die Festplatte, eine Diskette oder ein zugeordnetes Laufwerk zusammengesetzt werden. Fahren Sie mit Schritt 6 fort.

   - **Wenn Sie die Teile über das Netz zusammenführen**, klicken Sie auf **Netzwerk starten**.

     Das Dialogfeld zur Eingabe der **Paßphrase** wird angezeigt. Wählen Sie im Feld **Unterschreiben von Schlüsseln** das Schlüsselpaar für die Authentisierung an das entfernte System, und geben Sie die Paßphrase ein. Klicken Sie auf **OK**. Der Computer wird auf den Empfang der Schlüsselteile vorbereitet.

     Der Status der Übertragung wird im Feld **Netzwerkteile** angezeigt. Wenn der Status „Daten werden gelesen“ angezeigt wird, ist PGP bereit, die Schlüsselteile zu empfangen.

Zu diesem Zeitpunkt müssen die Halter ihre Schlüsselteile abschicken. Anleitungen zum Senden der Schlüsselteile an den für die Zusammenführung verwendeten Computer finden Sie unter „So senden Sie Schlüsselteile über das Netzwerk“ auf Seite 52.

Wenn ein Schlüsselteil empfangen wurde, wird das Dialogfeld **Entfernte Authentisierung** angezeigt (siehe Abbildung 3-14).

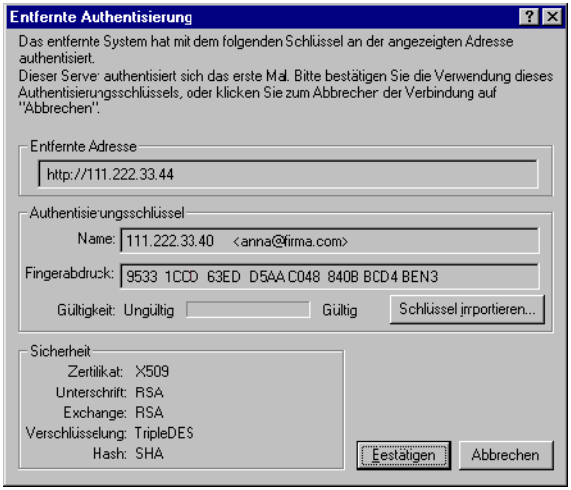


Abbildung 3-14. Dialogfeld „Entfernte Authentisierung“

Wenn Sie den Schlüssel, mit dem die Authentisierung des entfernten Systems durchgeführt wurde, nicht unterschrieben haben, ist der Schlüssel ungültig. Sie können die Schlüsselteile zwar mit einem ungültigen Authentisierungsschlüssel zusammensetzen; dieser Vorgang wird jedoch nicht empfohlen. Sie sollten die Fingerabdrücke der einzelnen Halter überprüfen und deren jeweiligen öffentlichen Schlüssel unterschreiben, um sicherzustellen, daß der Authentisierungsschlüssel legitim ist.

Klicken Sie zur Annahme des Schlüsselteils auf **Bestätigen**.

6. Sammeln Sie die übrigen Teile, bis der Wert für die **Gesamtzahl gesammelter Schlüsselteile** dem Wert für die **Gesamtzahl benötigter Schlüsselteile** entspricht (Dialogfeld **Sammlung der Schlüsselteile**).

7. Klicken Sie auf **OK**.

   Die Datei wird mit dem geteilten Schlüssel unterschrieben oder entschlüsselt.

So senden Sie Schlüsselteile über das Netzwerk

1. Wenn sich die Person, die den geteilten Schlüssel wieder zusammensetzt, an Sie wendet, sollten Sie über folgende Elemente verfügen:
   - Ihr Schlüsselteil und Ihr Paßwort
   - Ihr Schlüsselpaar (zur Authentisierung für den Computer, auf dem die Schlüsselteile zusammengeführt werden)
   - Eine Netzwerkverbindung. Benutzerhandbuch für PGP 6.5
   - Die IP-Adresse oder den Domänennamen des Computers, auf dem die Schlüsselteile zusammengeführt werden.
2. Wählen Sie im Menü **Datei** von PGPkeys die Option **Schlüsselteil senden**.

   Daraufhin wird das Dialogfeld **Schlüsselteil auswählen** angezeigt.
3. Suchen Sie Ihren Schlüsselteil, und klicken Sie dann auf **Öffnen**.

   Das Dialogfeld **PGP-Paßphrase eingeben** wird angezeigt.
4. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **OK**.

   Das Dialogfeld **Schlüsselteil senden** wird angezeigt (Abbildung 3-15).

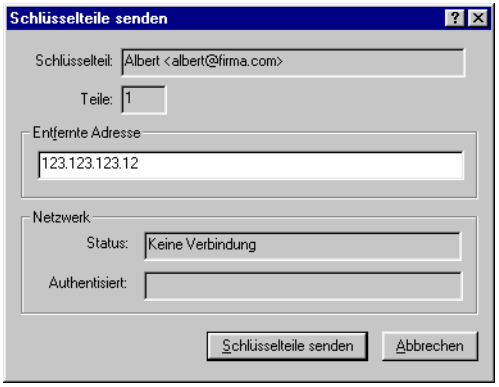


Abbildung 3-15. Dialogfeld „Schlüsselteile senden“

5. Geben Sie im Textfeld **Entfernte Adresse** die IP-Adresse oder den Domänennamen des Computers ein, auf dem die Teile wieder zusammengeführt werden, und klicken Sie dann auf **Schlüsselteile senden**.

   Der Status der Übertragung wird im Feld für den **Netzwerkstatus** angezeigt. Wenn dort „Verbindung hergestellt“ angezeigt wird, werden Sie aufgefordert, sich für den Computer, auf dem die Teile zusammengeführt werden, zu authentisieren.

   Im angezeigten Dialogfeld **Entfernte Authentisierung** müssen Sie bestätigen, daß es sich bei dem entfernten Computer um den handelt, an den Sie Ihren Schlüsselteil senden möchten.

6. Klicken Sie zur Fertigstellung der Transaktion auf **Bestätigen**.

   Wenn der Computer Ihre Schlüsselteile empfangen und deren Empfang bestätigt hat, wird ein Meldungsfeld mit einer Benachrichtigung über die erfolgreiche Übertragung der Teile angezeigt.

7. Klicken Sie auf **OK**.

8. Wenn Sie das Senden Ihres Schlüsselteils abgeschlossen haben, klicken Sie im Fenster für die **Schlüsselteile** auf **Fertig**.

Ihren öffentlichen Schlüssel verteilen

Nach der Erstellung Ihrer Schlüssel müssen Sie sie anderen Personen zugänglich machen, so daß diese verschlüsselte Daten an Sie senden und Ihre digitale Unterschrift verifizieren können. Es gibt drei Möglichkeiten, Ihren öffentlichen Schlüssel zu verteilen:

- Stellen Sie Ihren öffentlichen Schlüssel über einen öffentlichen Certificate Server zur Verfügung,
- Fügen Sie Ihren öffentlichen Schlüssel in eine E-Mail-Nachricht ein,

  – ODER –

- Exportieren oder kopieren Sie Ihren öffentlichen Schlüssel in eine Textdatei.

Ihr öffentlicher Schlüssel besteht im Prinzip aus einem Textblock. Daher ist es ziemlich einfach, ihn auf einem öffentlichen Certificate Server zugänglich zu machen, in eine E-Mail-Nachricht einzufügen oder ihn in eine Datei zu exportieren bzw. zu kopieren. Der Empfänger kann dann auf eine beliebige Art Ihren öffentlichen Schlüssel zu seinem öffentlichen Schlüsselbund hinzufügen.

Öffentliche Schlüssel über einen Certificate Server zur Verfügung stellen

Der beste Weg, Ihren öffentlichen Schlüssel anderen zur Verfügung zu stellen, besteht darin, ihn auf einem öffentlichen Certificate Server abzulegen, wo jeder darauf zugreifen kann. Auf diese Weise können andere Personen E-Mail-Nachrichten an Sie senden, ohne Sie extra um eine Kopie Ihres Schlüssels bitten zu müssen. Es ist dann auch nicht mehr notwendig, daß Sie und andere Benutzer eine Vielzahl öffentlicher Schlüssel verwalten, die Sie nur selten verwenden. Es gibt weltweit eine Anzahl von Schlüssel-Servern, u. a. die von Network Associates, Inc., auf denen Sie Ihren Schlüssel der Allgemeinheit zugänglich machen können. Im Normalfall wird der Sicherheitsbeauftragte Ihrer Firma die Einstellungen für Schlüssel-Server vorkonfigurieren, so daß Sie sich um nichts mehr kümmern müssen.

So senden Sie Ihren öffentlichen Schlüssel an einen Certificate Server

1. Stellen Sie eine Verbindung zum Internet her.
2. Öffnen Sie PGPkeys.
3. Wählen Sie das Symbol des öffentlichen Schlüssels aus, den Sie auf dem Certificate Server ablegen möchten.
4. Öffnen Sie das Menü **Server**, und wählen Sie dann im Untermenü **Senden an** den Certificate Server, auf dem der Schlüssel abgelegt werden soll. Eine Meldung informiert Sie darüber, daß die Schlüssel erfolgreich an den Server übertragen wurden.

Nachdem Sie eine Kopie Ihres öffentlichen Schlüssels an einen Certificate Server gesendet haben, können Sie den Personen, die verschlüsselte Daten an Sie senden möchten oder die Ihre digitale Unterschrift verifizieren möchten, mitteilen, daß eine Kopie Ihres öffentlichen Schlüssels auf dem Server zugänglich ist. Selbst wenn Sie sie nicht ausdrücklich auf Ihren öffentlichen Schlüssel hinweisen, können sie eine Kopie Ihres öffentlichen Schlüssels anfertigen, indem sie den Certificate Server nach Ihrem Namen oder Ihrer E-Mail-Adresse durchsuchen. Viele Personen fügen am Ende ihrer E-Mail-Nachrichten die Web-Adresse für ihren öffentlichen Schlüssel ein. In den meisten Fällen muß der Empfänger nur auf diese Adresse doppelklicken, um Zugang zu einer Kopie Ihres Schlüssels auf dem Server zu erhalten. Es gibt sogar Personen, die ihren PGP-Fingerabdruck zur leichteren Verifizierung in ihre Visitenkarten übernehmen lassen.

Eigenen Schlüssel auf einem Certificate Server aktualisieren

Falls Sie Ihre E-Mail-Adresse ändern müssen oder neue Unterschriften verwenden, müssen Sie zum Ersetzen des alten Schlüssels lediglich eine Kopie des neuen Schlüssels an den Server schicken. Die Server-Informationen werden dann automatisch aktualisiert. Sie sollten jedoch dabei bedenken, daß öffentliche Certificate Server nur in der Lage sind, neue Informationen zu aktualisieren und keine Entfernung von Benutzernamen oder Unterschriften aus Schlüsseln erlauben. Anweisungen zum Entfernen von Unterschriften oder Benutzernamen von einem Schlüssel finden Sie unter „Mit Ihrem Schlüssel verbundene Unterschriften oder Benutzernamen entfernen“. Falls Ihr Schlüssel nicht mehr sicher ist, können Sie ihn zurücknehmen. Dadurch werden andere darüber informiert, daß dieser Schlüsselversion nicht mehr zu trauen ist. Genauere Informationen zum Zurücknehmen von Schlüsseln finden Sie im Abschnitt Kapitel 6, „Schlüssel verwalten und PGP-Optionen festlegen“.

Mit Ihrem Schlüssel verbundene Unterschriften oder Benutzernamen entfernen

Sie können bei Bedarf auch mit einem bestimmten Schlüssel verbundene Schlüssel, Unterschriften oder Benutzer-IDs löschen.

Öffentliche Certificate Server können ausschließlich neue Informationen aktualisieren, erlauben aber keine Entfernung von Benutzernamen oder Unterschriften aus Schlüsseln. Zum Entfernen von Unterschriften oder Benutzernamen, die mit Ihrem öffentlichen Schlüssel verbunden sind, entfernen Sie den Schlüssel zunächst vom Server, nehmen die erforderlichen Änderungen vor und legen den Schlüssel wieder auf dem Server ab.

Falls PGP Server entsprechend konfiguriert wurde, werden Schlüssel beim Hinzufügen von Namen, Fotos oder Rücknahmeschlüsseln automatisch auf dem Server aktualisiert. Falls dies einmal nicht geschehen sollte, befolgen Sie die nachstehenden Anweisungen, um Ihren Schlüssel manuell auf dem Certificate Server zu aktualisieren.

HINWEIS: Aus einem Schlüssel gelöschte Benutzer-IDs, Unterschriften und Schlüssel werden unwiederherstellbar entfernt. Unterschriften und Benutzer-IDs können erneut zu einem Schlüssel hinzugefügt werden und ein importierter öffentlicher Schlüssel kann wieder zu Ihrem Schlüsselbund hinzugefügt werden. Ein privater Schlüssel jedoch, der nur an diesem Schlüsselbund vorhanden ist, kann nicht neu erstellt werden, und alle Nachrichten, die mit den Kopien des dazugehörigen öffentlichen Schlüssels verschlüsselt wurden, können nicht mehr entschlüsselt werden.

So entfernen Sie mit Ihrem Schlüssel verbundene Unterschriften oder Benutzernamen von einem Certificate Server

WICHTIG: Mit dieser Vorgehensweise können ausschließlich mit Ihrem Schlüssel verbundene Unterschriften oder Benutzernamen von LDAP-Certificate Servern entfernt werden. Außerdem muß der Certificate Server für diesen Vorgang entsprechend konfiguriert sein. Falls Sie keine Informationen zum Servertyp oder die Konfigurationseinstellungen verfügen, wenden Sie sich an den Certificate Server-Administrator Ihres Unternehmens, bevor Sie Ihren Schlüssel aktualisieren.

1. Öffnen Sie PGPkeys.
2. Wählen Sie im Menü **Server** die Option **Suchen**, oder klicken Sie im PGPkeys-Menü auf  .

   Daraufhin wird das **PGPkeys-Suchfenster** angezeigt.
3. Wählen Sie im Menü **Suche nach Schlüsseln in** den zu durchsuchenden Server aus.
4. Geben Sie die Suchkriterien für Ihren öffentlichen Schlüssel an:

   Standardmäßig ist **Benutzer-ID** ausgewählt, aber Sie können durch Klikken auf die Pfeile auch **Schlüssel-ID**, **Schlüsselstatus**, **Schlüsseltyp**, **Schlüsselgröße**, **Erstellungsdatum** oder **Gültigkeit** auswählen. Sie können beispielsweise alle Schlüssel mit der Benutzer-ID „Fred“ suchen.
5. Klicken Sie auf **Suchen**, um die Suche zu starten.

   Die Suchergebnisse werden im Fenster angezeigt.
6. Klicken Sie mit der rechten Maustaste auf den Schlüssel, den Sie vom Server entfernen möchten, und wählen Sie **Löschen** im Kontextmenü.

   Das Dialogfeld zur Eingabe der **Paßphrase** wird angezeigt.
7. Geben Sie die Paßphrase für den Schlüssel ein, den Sie vom Server entfernen möchten, und klicken Sie auf **OK**.

   Das Entfernen des Schlüssels wird mit einer entsprechenden Meldung bestätigt.
8. Aktualisieren Sie Ihren Schlüssel (entfernen Sie die unerwünschten Unterschriften oder Benutzernamen).
9. Kopieren Sie den aktualisierten Schlüssel auf den Server (siehe „Öffentliche Schlüssel über einen Certificate Server zur Verfügung stellen“ auf Seite 54.

Falls der Server, auf dem Sie Ihren öffentlichen Schlüssel aktualisieren, für die Synchronisation von Schlüsseln mit anderen Certificate Servern konfiguriert wurde, wird dies automatisch für die anderen Server durchgeführt.

WICHTIG: Falls Sie Ihren Schlüssel von einem Certificate Server löschen, sollten Sie bedenken, daß dieser öffentliche Schlüssel von einer anderen Person wieder auf den Server übertragen werden kann. Überprüfen Sie den Server regelmäßig um sicherzustellen, daß der Schlüssel nicht erneut aufgenommen wurde. Möglicherweise müssen Sie einen Schlüssel also mehr als nur einmal vom Server löschen.

Eigenen öffentlichen Schlüssel in eine E-Mail-Nachricht einfügen

Eine andere praktische Methode zum Verteilen des eigenen öffentlichen Schlüssels besteht darin, ihn in eine E-Mail-Nachricht einzufügen.

So fügen Sie Ihren öffentlichen Schlüssel in eine E-Mail-Nachricht ein

1. Öffnen Sie PGPkeys.
2. Wählen Sie Ihr Schlüsselpaar aus, und wählen Sie im Menü **Bearbeiten** die Option **Kopieren**.
3. Öffnen Sie Ihr E-Mail-Programm, und setzen Sie den Cursor an die gewünschte Stelle. Wählen Sie dann im Menü **Bearbeiten** die Option **Einfügen**. In neueren E-Mail-Anwendungen können Sie den Schlüssel einfach aus PGPkeys in den Textbereich Ihrer E-Mail-Nachricht ziehen.

Wenn Sie jemandem Ihren öffentlichen Schlüssel senden, sollten Sie die E-Mail-Nachricht unterschreiben. Auf diese Weise kann der Empfänger Ihre Unterschrift verifizieren und sicher sein, daß niemand die ursprünglichen Informationen verfälscht hat. Wenn Ihr Schlüssel noch nicht von einem vertrauenswürdigen Schlüsselverwalter unterschrieben worden ist, können die Empfänger Ihrer Unterschrift nur durch die Verifizierung des Fingerabdrucks auf Ihrem Schlüssel sicher sein, daß die Unterschrift wirklich von Ihnen stammt.

Eigenen öffentlichen Schlüssel in eine Datei exportieren

Ein weiterer Weg zum Verteilen Ihres öffentlichen Schlüssels ist, ihn in eine Datei einzufügen und diese Datei dann der Person zur Verfügung zu stellen, mit der Sie kommunizieren möchten.

So exportieren Sie Ihren öffentlichen Schlüssel in eine Datei

Zum Speichern oder Exportieren Ihres öffentlichen Schlüssels in eine Datei haben Sie zwei Möglichkeiten:

- Wählen Sie das Ihr Schlüsselpaar darstellende Symbol in PGPkeys, und klicken Sie dann im Menü **Schlüssel** auf die Option **Exportieren**. Geben Sie anschließend den Namen der Datei ein, in der der Schlüssel gespeichert werden soll.
- Ziehen Sie das Symbol für Ihr Schlüsselpaar aus PGPkeys in den Ordner, in dem der Schlüssel gespeichert werden soll,

  – ODER –

- Markieren Sie das Ihr Schlüsselpaar darstellende Symbol in PGPkeys, und wählen Sie im Menü **Bearbeiten** die Option **Einfügen**, um die Schlüsseldaten in ein Textdokument einzufügen.

> **HINWEIS:** Wenn Sie Ihren Schlüssel an Kollegen schicken, die PCs verwenden, geben Sie den Dateinamen und die Dateierweiterung ein, wobei der Dateiname aus bis zu 8 Zeichen und die Dateierweiterung aus 3 Zeichen besteht (beispielsweise MEINSCHL.TXT).

Öffentliche Schlüssel von anderen Benutzern erhalten

Genauso wie Sie Ihre öffentlichen Schlüssel an die Personen verteilen müssen, die verschlüsselte E-Mail-Nachrichten an Sie senden oder Ihre digitale Unterschrift verifizieren möchten, benötigen Sie die öffentlichen Schlüssel von anderen Personen, damit Sie verschlüsselte E-Mail-Nachrichten an diese senden und ihre digitalen Unterschriften verifizieren können.

So erhalten Sie öffentliche Schlüssel anderer Benutzer

Es gibt drei Möglichkeiten, den Schlüssel eines anderen Benutzers zu erhalten:

- Rufen Sie den Schlüssel über einen öffentlichen Certificate Server ab,
- Nehmen Sie den öffentlichen Schlüssel direkt aus einer E-Mail-Nachricht in Ihren Schlüsselbund auf,

  – ODER –

- Importieren Sie den öffentlichen Schlüssel aus einer exportierten Datei.

Öffentliche Schlüssel sind einfach nur Textblöcke. Daher ist es ziemlich einfach, sie zu Ihrem Schlüsselbund hinzuzufügen, indem Sie sie aus einer Datei importieren oder aus einer E-Mail-Nachricht kopieren und sie anschließend in Ihren öffentlichen Schlüsselbund einfügen.

Öffentliche Schlüssel von einem Certificate Server erhalten

Wenn der Benutzer, dem Sie eine verschlüsselte E-Mail schicken möchten, über ausreichende Kenntnisse bezüglich der Verwendung von PGP verfügt, hat er mit hoher Wahrscheinlichkeit eine Kopie seines öffentlichen Schlüssels auf einem Certificate Server abgelegt. Dadurch haben Sie jederzeit problemlos Zugang zum aktuellsten Schlüssel, wenn Sie ihm eine E-Mail-Nachricht schikken möchten, und Sie müssen nicht eine Vielzahl von Schlüsseln in Ihrem öffentlichen Schlüsselbund speichern.

Unter Umständen werden Sie vom Sicherheitsbeauftragten Ihres Unternehmens angewiesen, einen gemeinsam genutzten Certificate Server zu verwenden, auf dem alle in Ihrem Unternehmen häufig verwendeten Schlüssel gespeichert sind. In diesem Fall ist Ihre PGP-Software wahrscheinlich bereits darauf konfiguriert, auf den richtigen Server zuzugreifen.

Es stehen mehrere öffentliche Certificate Server zur Verfügung (wie beispielsweise der von Network Associates Inc. unterhaltene Server), auf denen Sie die Schlüssel der meisten PGP-Benutzer finden können. Wenn der Empfänger Ihnen nicht die Web-Adresse genannt hat, unter der sein öffentlicher Schlüssel gespeichert ist, können Sie auf einen beliebigen Certificate Server zugreifen und nach dem Namen oder der E-Mail-Adresse des Empfängers suchen, da alle Certificate Server regelmäßig aktualisiert werden, damit die auf den anderen Servern gespeicherten Schlüssel ebenfalls abgerufen werden können.

So rufen Sie den öffentlichen Schlüssel eines Benutzers über einen Certificate Server ab:

1. Öffnen Sie PGPkeys.
2. Wählen Sie im Menü **Server** die Option **Suchen**, oder klicken Sie in PGPkeys auf die Schaltfläche **Suchen** ( ).

   Daraufhin wird das **PGPkeys-Suchfenster** angezeigt (siehe Abbildung 3-16).

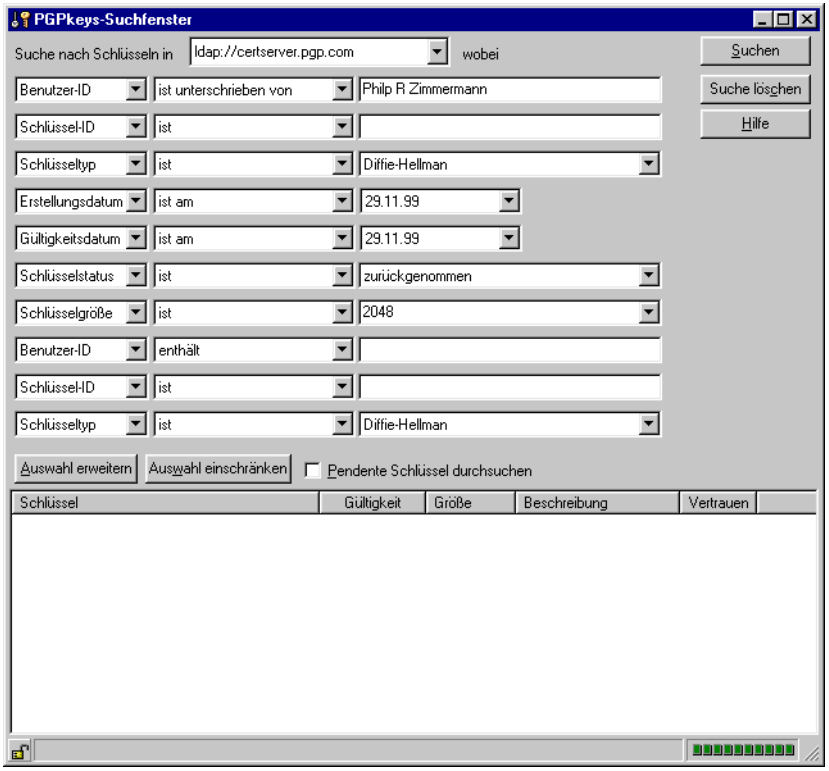


Abbildung 3-16. PGPkeys-Suchfenster (Ansicht „Auswahl erweitern“)

3. Wählen Sie im Menü **Suche nach Schlüsseln in** den zu durchsuchenden Server aus.

4. Geben Sie die Suchkriterien an.

   Sie können nach Schlüsseln auf einem Certificate Server suchen, indem Sie Angaben über die folgenden Schlüsseleigenschaften machen:

   - Benutzer-ID
   - Schlüssel-ID
   - Schlüsselstatus (Zurückgenommen oder Deaktiviert)
   - Schlüsseltyp (Diffie-Hellman oder RSA)
   - Erstellungsdatum
   - Gültigkeit
   - Zurückgenommene Schlüssel
   - Deaktivierte Schlüssel
   - Schlüsselgröße
   - Mit einem bestimmten Schlüssel unterschriebene Schlüssel

   Die Umkehrung der meisten dieser Operationen ist ebenfalls möglich. Ihr Kriterium könnte bei einer Suche beispielsweise auch „Benutzer-ID ist nicht Bob“ lauten.

5. Geben Sie den zu suchenden Wert an.

6. Klicken Sie auf **Auswahl erweitern**, um der Suche zusätzliche Kriterien hinzuzufügen, wie beispielsweise Schlüssel-IDs mit dem Namen „Fred“, die am oder vor dem 6. Oktober 1997 erstellt wurden.

7. Klicken Sie auf **Suchen**, um die Suche zu starten.

   Eine Statusleiste informiert Sie darüber, wie weit die Suche fortgeschritten ist.

   HINWEIS: Um eine Suche abzubrechen, klicken Sie auf **Suche anhalten**.

   Die Suchergebnisse werden im Fenster angezeigt.

8. Um die gefundenen Schlüssel zu importieren, ziehen Sie sie in das Hauptfenster von PGPkeys.

9. Klicken Sie auf **Suche löschen**, um die Suchkriterien zurückzusetzen.

Öffentlichen Schlüssel aus E-Mail-Nachrichten entnehmen

Die bequemste Art, eine Kopie des öffentlichen Schlüssels einer anderen Person zu erhalten, besteht darin, die betreffende Person zu bitten, den Schlüssel an eine E-Mail-Nachricht anzuhängen. Wenn ein öffentlicher Schlüssel per E-Mail gesendet wird, wird er im Nachrichtentextteil als Textblock angezeigt.

So entnehmen Sie einen öffentlichen Schlüssel aus einer E-Mail-Nachricht

Wenn Ihre E-Mail-Anwendung von einem der PGP-Plug-Ins unterstützt wird, klicken Sie auf  in der E-Mail-Anwendung, um den öffentlichen Schlüssel des Absenders aus der E-Mail zu extrahieren und Ihrem öffentlichen Schlüsselbund hinzuzufügen.

Wenn Sie mit einer E-Mail-Anwendung arbeiten, die nicht von den Plug-Ins unterstützt wird, können Sie den öffentlichen Schlüssel Ihrem Schlüsselbund hinzufügen, indem Sie den Textblock, der den öffentlichen Schlüssel darstellt, kopieren und ihn in PGPkeys einfügen.

Schlüssel importieren

Sie können öffentliche Schlüssel und private Schlüssel vom Typ PKCS-12 X.509 in Ihren öffentlichen Schlüsselbund importieren. Kopieren Sie die Schlüssel mit Hilfe Ihres Browsers, und fügen Sie sie in Ihren öffentlichen Schlüsselbund ein.

Eine andere Methode zum Erhalten des öffentlichen Schlüssels einer anderen Person besteht darin, sie zu bitten, ihn in einer Datei zu speichern, aus der Sie ihn importieren oder kopieren und in Ihren öffentlichen Schlüsselbund einfügen können.

So importieren Sie einen öffentlichen Schlüssel aus einer Datei

Es gibt drei Methoden zum Extrahieren des öffentlichen Schlüssels eines anderen Benutzers und zum Einfügen dieses Schlüssel in Ihren öffentlichen Schlüsselbund:

- Klicken Sie im Menü **Schlüssel** auf **Importieren**, und lokalisieren Sie dann die Datei, in der der öffentliche Schlüssel gespeichert ist,
- Ziehen Sie die Datei, die den öffentlichen Schlüssel enthält, auf das PGPkeys-Hauptfenster,

  – ODER –

- Öffnen Sie das Textdokument, in dem der öffentliche Schlüssel gespeichert ist, und markieren Sie den Textblock, der den Schlüssel darstellt. Wählen Sie anschließend im Menü **Bearbeiten** den Befehl **Kopieren**. Wechseln Sie zum PGPkeys-Fenster, und wählen Sie im Menü **Bearbeiten** den Befehl **Einfügen**. Der Schlüssel wird dann als Symbol in PGPkeys angezeigt.

Private Schlüssel vom Typ PKCS-12 X.509 können Sie auch mit Hilfe Ihres Browsers durch Ziehen exportieren und in PGPkeys einfügen, oder Sie wählen **Importieren** im Menü **Schlüssel**.

Die Echtheit eines Schlüssels verifizieren

Wenn Sie mit einer Person Schlüssel austauschen, läßt sich mitunter nur schwer feststellen, ob der Schlüssel wirklich zu dieser Person gehört. Die PGP-Software bietet Ihnen eine Reihe von Sicherungsmechanismen, mit denen Sie die Echtheit eines Schlüssels überprüfen und zertifizieren können, daß er einem bestimmten Eigentümer gehört (d. h., die *Echtheit überprüfen* können). Außerdem warnt Sie das PGP-Programm bei dem Versuch, einen Schlüssel zu verwenden, der nicht echt ist. Standardmäßig werden Sie auch gewarnt, bevor Sie einen zweitrangigen, echten Schlüssel verwenden.

Wozu einen Schlüssel authentisieren?

Einer der Hauptangriffspunkte von Verschlüsselungssystemen mit öffentlichen Schlüsseln ist die Fähigkeit von raffinierten Spionen, einen Abfangangriff („man-in-the-middle attack“) durchzuführen, indem sie den öffentlichen Schlüssel eines Benutzers durch ihren eigenen ersetzen. Auf diese Weise kann jede an diese Person gerichtete verschlüsselte E-Mail-Nachricht abgefangen, mit Hilfe eines eigenen Schlüssels entschlüsselt, anschließend wieder mit dem echten Schlüssel der Person verschlüsselt und an diese weitergeleitet werden, als ob niemals etwas geschehen wäre. Diese Handlungen können sogar mit Hilfe spezieller Programme automatisch vorgenommen werden, die zwischen Ihnen und dem Empfänger Ihrer Nachricht stehen und Ihre gesamte Kommunikation entziffern.

In Anbetracht dieses Risikos müssen Sie und die Personen, mit denen Sie E-Mail-Nachrichten austauschen, einen Weg finden, sicherzugehen, daß Sie wirklich über echte Kopien Ihrer Schlüssel verfügen. Die beste Methode, mit der Sie völlig sicher sein können, daß ein öffentlicher Schlüssel wirklich einer bestimmten Person gehört, besteht darin, den Besitzer darum zu bitten, den Schlüssel auf eine Diskette zu kopieren und Ihnen diese anschließend persönlich auszuhändigen. Sie befinden sich jedoch selten so nahe bei jemandem, daß Sie dieser Person eine Diskette geben können. Normalerweise tauschen Sie öffentliche Schlüssel per E-Mail aus oder erhalten sie über einen öffentlichen Certificate Server.

Mit digitalen Fingerabdrücken verifizieren

Um festzustellen, ob ein Schlüssel tatsächlich einer bestimmten Person gehört, können Sie den digitalen Fingerabdruck – eine eindeutige Reihe von bei der Erstellung des Schlüssels generierten Zahlen oder Worten – überprüfen. Durch einen Vergleich des Originals mit Ihrer Kopie des Fingerabdrucks des öffentlichen Schlüssels einer Person können Sie absolute Gewißheit erlangen, daß es sich tatsächlich um eine gültige Kopie des Schlüssels handelt. Eine Anleitung zum Verifizieren mit einem digitalen Fingerabdruck finden Sie im Abschnitt „Öffentliche Schlüssel anderer Benutzer verifizieren“ auf Seite 108.

Öffentliche Schlüssel überprüfen

Wenn Sie absolut sicher sind, daß Sie über eine gültige Kopie des öffentlichen Schlüssels eines anderen Benutzers verfügen, können Sie den Schlüssel dieser Person unterschreiben. Wenn Sie den öffentlichen Schlüssel einer anderen Person mit Ihrem privaten Schlüssel unterschreiben, zertifizieren Sie, daß Sie sicher sind, daß der Schlüssel tatsächlich dem angegebenen Benutzer gehört. Wenn Sie beispielsweise einen neuen Schlüssel erstellen, wird dieser automatisch mit Ihrer eigenen Unterschrift zertifiziert. Standardmäßig werden Unterschriften, die Sie auf anderen Schlüsseln leisten, nicht exportiert, d. h., sie gelten nur für einen Schlüssel, wenn er sich auf Ihrem Schlüsselbund befindet. Genaue Anweisungen zum Unterschreiben eines Schlüssels finden Sie im Abschnitt „Öffentliche Schlüssel anderer Benutzer unterschreiben“ auf Seite 110.

Mit autorisierten Schlüsselverwaltern arbeiten

Oftmals lassen PGP-Benutzer auch ihre öffentlichen Schlüssel durch andere vertrauenswürdige Benutzer unterzeichnen, um ihre Echtheit zusätzlich attestieren zu lassen. Sie können beispielsweise einem Kollegen Ihres Vertrauens eine Kopie Ihres öffentlichen Schlüssels mit der Bitte schicken, den Schlüssel zu zertifizieren und an Sie zurückzuschicken, damit Sie seine Unterschrift einfügen können, wenn Sie den Schlüssel auf einem öffentlichen Certificate Server ablegen. Mit PGP müssen die Personen, die eine Kopie Ihres öffentlichen Schlüssels erhalten, nicht selbst die Echtheit des Schlüssels überprüfen, sondern können statt dessen dem Urteil derer vertrauen, die Ihren Schlüssel unterzeichnet haben. PGP gibt Ihnen die Möglichkeit, diesen Grad an Echtheit für jeden öffentlichen Schlüssel festzulegen, den Sie zu Ihrem öffentlichen Schlüsselbund hinzufügen. Außerdem wird der Grad an Echtheit und Vertrauen für jeden Schlüssel in PGPkeys angezeigt. Dies bedeutet, daß Sie ziemlich sicher sein können, daß ein Schlüssel vom angegebenen Benutzer stammt, wenn er von einem autorisierten Schlüsselverwalter unterzeichnet wurde. Genauere Informationen zum Unterschreiben von Schlüsseln und zur Authentisierung von Benutzern finden Sie im Abschnitt „Öffentliche Schlüssel anderer Benutzer unterschreiben“ auf Seite 110.

Ihr Sicherheitsbeauftragter kann als vertrauenswürdiger Schlüsselverwalter agieren, und Sie können dann alle durch den firmenweiten Unterzeichnerschlüssel unterzeichneten Schlüssel als gültig betrachten. Wenn Sie für ein großes Unternehmen mit mehreren Niederlassungen arbeiten, haben Sie möglicherweise regionale Schlüsselverwalter, und Ihr Sicherheitsbeauftragter könnte ein höhergestellter Schlüsselverwalter, eine Art autorisierter Schlüsselverwalter der autorisierten Schlüsselverwalter, sein.

Was ist ein autorisierter Schlüsselverwalter?

PGP arbeitet mit sogenannten autorisierten Schlüsselverwaltern, also Personen, deren Schlüssel Sie als vertrauenswürdig ansehen. Dieses Konzept kommt Ihnen vielleicht aus viktorianischen Romanen bekannt vor, in denen man sich gegenseitig schriftliche Empfehlungen zukommen ließ. Wenn also beispielsweise Ihr Onkel jemanden in einer weit entfernten Stadt kannte, mit dem Sie möglichweise Geschäfte tätigen wollten, so schickte er dieser Person ein entsprechendes Schreiben. Bei PGP können Benutzer gegenseitig ihre Schlüssel unterschreiben, um diese zu überprüfen. Wenn Sie einen Schlüssel unterschreiben, bestätigen sie damit dessen Gültigkeit. Sie sind also davon überzeugt, daß der Schlüssel tatsächlich von der entsprechenden Person stammt. Hierzu gibt es mehrere Möglichkeiten. Wenn ein autorisierter Schlüsselverwalter einen fremden Schlüssel unterzeichnet, werden Sie die Gültigkeit dieses Schlüssels nicht mehr in Frage stellen.

Was ist ein höhergestellter Schlüsselverwalter?

PGP unterstützt außerdem sogenannte höhergestellte Schlüsselverwalter – sozusagen eine autorisierte Person für die Vermittlung autorisierter Schlüsselverwalter. Wenn Sie in einem sehr großen Unternehmen arbeiten, wurde möglicherweise ein regionaler Sicherheitsbeauftragter zur Unterzeichnung der Benutzerschlüssel bestimmt. Sie könnten in diesem Fall also auf die Gültigkeit dieser Schlüssel vertrauen, da sie bereits durch den Sicherheitsbeauftragten überprüft wurden. In Ihrem Unternehmen könnte außerdem ein Haupt-Sicherheitsbeauftragter eingesetzt werden, der mit den regionalen Beauftragten zusammenarbeitet. Somit könnte ein Mitarbeiter im südlichen Teil des Landes einem Kollegen aus dem nördlichen Landesteil vertrauen, da ihre Schlüssel von den jeweils zuständigen regionalen Sicherheitsbeauftragten unterzeichnet wurden. Diese wiederum ließen ihre Schlüssel vom Haupt-Sicherheitsbeauftragten unterzeichnen, der in diesem Fall also die Position eines höhergestellten Schlüsselverwalters einnähme. Dies ermöglicht die Einführung einer Vertrauenshierarchie innerhalb des Unternehmens.

E-Mail-Nachrichten sicher senden und empfangen 4

In diesem Kapitel wird beschrieben, wie Sie E-Mail-Nachrichten verschlüsseln und unterschreiben, die Sie an andere Personen senden, und wie Sie E-Mail-Nachrichten entschlüsseln und verifizieren, die andere an Sie senden.

E-Mail-Nachrichten verschlüsseln und unterschreiben

Sie können drei Methoden verwenden, um E-Mail-Nachrichten zu verschlüsseln und zu unterschreiben. E-Mail-Nachrichten können Sie am einfachsten und schnellsten verschlüsseln und unterschreiben, wenn Sie mit einer E-Mail-Anwendung arbeiten, die von den PGP-Plug-Ins unterstützt wird. Obwohl sich die Prozeduren in den verschiedenen E-Mail-Anwendungen etwas voneinander unterscheiden, führen Sie den Vorgang des Verschlüsselns und Unterschreibens aus, indem Sie in der Symbolleiste der jeweiligen Anwendung auf die entsprechenden Schaltflächen klicken.

Wenn Sie mit einer E-Mail-Anwendung arbeiten, die nicht von den PGP-Plug-Ins unterstützt wird, können Sie Ihre E-Mail-Nachrichten mit Hilfe der Windows-Zwischenablage verschlüsseln und unterschreiben, indem Sie im Systemfeld in der Task-Leiste auf das Schloßsymbol klicken und dann die entsprechende Option wählen. Dateianhänge werden vor dem Anhängen mit Hilfe des Windows-Explorers verschlüsselt.

TIP: Wenn Sie vertrauliche E-Mail-Nachrichten senden, sollten Sie in Ihre Betreffzeile nichts eingeben oder einen Betreff eintragen, durch den der Inhalt Ihrer verschlüsselten Nachricht nicht verraten wird.

Wenn Sie keine der E-Mail-Anwendungen verwenden, die von PGP unterstützt werden, finden Sie weitere Informationen zum Verschlüsseln von Dateien in Kapitel 5.

Alternativ zu den Plug-Ins können Sie Ihre E-Mail-Nachrichten und Dateianhänge vor dem Versand mit PGPtools verschlüsseln und unterschreiben. Weitere Informationen finden Sie im Abschnitt „So verschlüsseln und unterzeichnen Sie Text mit PGPtools:“ auf Seite 72.

Mit unterstützten E-Mail-Anwendungen verschlüsseln und unterschreiben

Wenn Sie Dateien mit einer von den PGP-Plug-Ins unterstützten E-Mail-Anwendung verschlüsseln und unterschreiben, stehen Ihnen, abhängig vom Typ der vom Empfänger verwendeten E-Mail-Anwendung, zwei Verfahren zur Auswahl. Wenn Sie mit anderen PGP-Benutzern kommunizieren, die eine E-Mail-Anwendung verwenden, die den PGP / MIME-Standard unterstützt, können Sie mit Hilfe einer PGP / MIME-Funktion E-Mail-Nachrichten und Dateianhänge beim Senden automatisch verschlüsseln und unterschreiben. Wenn Sie mit einer Person kommunizieren, die mit einer PGP / MIME-inkompatiblen E-Mail-Anwendung arbeitet, sollten Sie vor dem Verschlüsseln Ihrer E-Mail-Nachrichten die PGP / MIME-Funktion deaktivieren, um Kompatibilitätsprobleme zu vermeiden. In Tabelle 4-1, „PGP-Plug-In-Funktionen“ finden Sie eine Auflistung der verschiedenen Plug-Ins und deren Funktionen.

Tabelle 4-1. PGP-Plug-In-Funktionen

	Eudora 3.0x	Eudora 4.0x	Exchange/ Outlook	Lotus Notes	Out-look Express
PGP/MIME	Ja	Ja	Nein	Nein	Nein
Automatisch entschlüsseln	Ja	Nein	Ja	Ja	Ja
In HTML verschlüsseln	Nicht zutref-fend	Ja	Konvertiert vor dem Verschlüs-seln in Klartext	Ja	Nein
Entschlüsselte HTML als HTML-Dokumen t anzeigen	Nein	Ja	Nein	Ja	Nein
Anhänge verschlüsseln	Ja	Ja	Ja	Ja	Nein
Standardeinstell ungen für Verschlüsseln/U nterschreiben	Ja	Ja	Ja	Ja	Ja

So verschlüsseln und unterschreiben Sie Nachrichten mit unterstützten E-Mail-Anwendungen:

1. Erstellen Sie die E-Mail-Nachricht wie gewohnt mit Ihrer E-Mail-Anwendung.

2. Wenn Sie die E-Mail-Nachricht erstellt haben, klicken Sie zuerst auf  , um den Text in Ihrer E-Mail-Nachricht zu verschlüsseln, und anschließend auf  , um Ihre Nachricht zu unterschreiben.

   HINWEIS: Wenn Sie PGP / MIME regelmäßig verwenden möchten, aktivieren Sie auf der Registerkarte **E-Mail** im Dialogfeld **Optionen** die entsprechenden Einstellungen.

3. Senden Sie die E-Mail-Nachricht wie gewohnt.

   Wenn Sie für jeden Empfänger eine Kopie der öffentlichen Schlüssel haben, werden die entsprechenden Schlüssel verwendet. Wenn Sie jedoch einen Empfänger angeben, von dem Sie keinen entsprechenden öffentlichen Schlüssel haben oder für den ein oder mehrere Schlüssel nicht über den ausreichenden Echtheitsgrad verfügen, wird das **PGP-Dialogfeld zur Schlüsselauswahl** angezeigt (Abbildung 4-1), so daß Sie den korrekten Schlüssel angeben können.

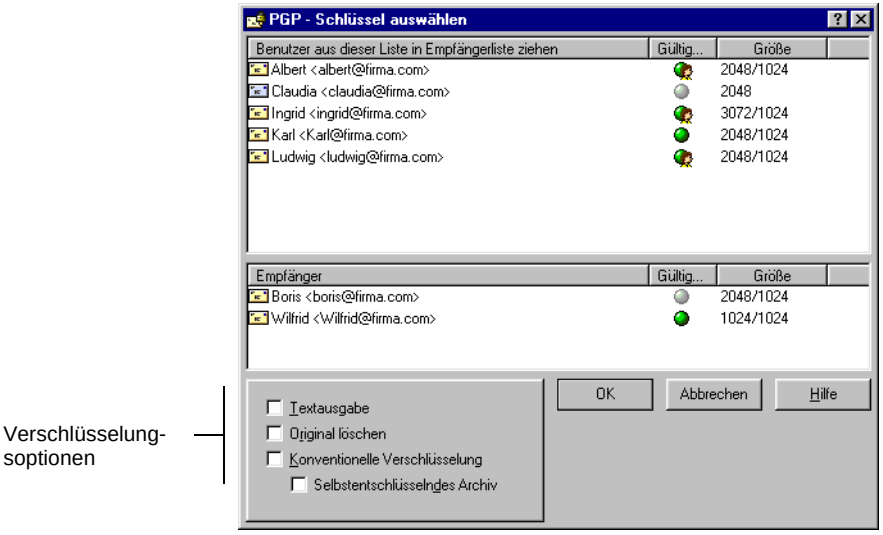


Abbildung 4-1. PGP-Fenster „Empfängerauswahl“

4. Ziehen Sie die öffentlichen Schlüssel der gewünschten Empfänger dieser verschlüsselten E-Mail-Nachricht in das Empfängerlistenfeld. Sie können auch auf jeden beliebigen Schlüssel doppelklicken, um ihn auf dem Bildschirm zu verschieben.

   Durch das **Echtheitssymbol** wird der Grad der Gewißheit angegeben, daß die öffentlichen Schlüssel in der **Empfängerliste** echt sind. Diese Echtheit ergibt sich aus den mit dem Schlüssel verknüpften Unterschriften. Ausführliche Informationen finden Sie in Kapitel 6, „Schlüssel verwalten und PGP-Optionen festlegen“.

5. Sie können abhängig vom Datentyp, den Sie verschlüsseln möchten, eine der folgenden Verschlüsselungsoptionen wählen:

   - **Sichere Darstellung.** Wählen Sie diese Option, um die Daten beim Entschlüsseln vor TEMPEST-Angriffen zu schützen. Wenn Sie diese Option wählen, werden die entschlüsselten Daten in einer speziellen Schriftart zur Verhütung von TEMPEST-Angriffen angezeigt und sind somit unlesbar für Strahlungsauswertegeräte. Weitere Informationen zu TEMPEST-Angriffen finden Sie im Abschnitt „Sicherheitsrisiken“ auf Seite 263.

     ☐ **HINWEIS:** Die Option „Sichere Darstellung“ ist möglicherweise nicht mit früheren PGP-Versionen kompatibel. Mit dieser Option aktivierte verschlüsselte Dateien können mit früheren PGP-Versionen entschlüsselt werden, wobei diese Funktion möglicherweise ignoriert wird.

   - Konventionelle Verschlüsselung. Wählen Sie diese Option, wenn Sie nicht mit öffentlichen Schlüsseln verschlüsseln, sondern eine allgemeine Paßphrase verwenden möchten. Wenn Sie diese Option wählen, wird die Datei mit Hilfe eines Sitzungsschlüssels unter Verwendung einer Paßphrase verschlüsselt (und entschlüsselt). Sie werden aufgefordert, die zu verwendende Paßphrase zu wählen.

   - Selbstentschlüsselndes Archiv. Wählen Sie diese Option, um eine selbstentschlüsselnde, ausführbare Datei zu erstellen. Wenn Sie diese Option wählen, wird die Datei mit Hilfe eines Sitzungsschlüssels unter Verwendung einer Paßphrase verschlüsselt (und entschlüsselt). Sie werden aufgefordert, die zu verwendende Paßphrase zu wählen. Die resultierende ausführbare Datei kann durch Doppelklicken auf die Datei und Eingabe der entsprechen-

den Paßphrase entschlüsselt werden. Diese Option ist besonders für Benutzer geeignet, die verschlüsselte Dateien an andere Personen senden, die die PGP-Software nicht installiert haben. Beachten Sie, daß sich Absender und Empfänger auf derselben Plattform befinden müssen.

6. Klicken Sie auf **OK**, um Ihre E-Mail-Nachricht zu verschlüsseln und zu unterschreiben.

   Wenn Sie die verschlüsselten Daten unterschreiben möchten, werden Sie vor dem Senden der Nachricht im Dialogfeld für die**Paßphrase des Unterschriftenschlüssels** (siehe Abbildung 4-2) dazu aufgefordert, Ihre Paßphrase einzugeben.

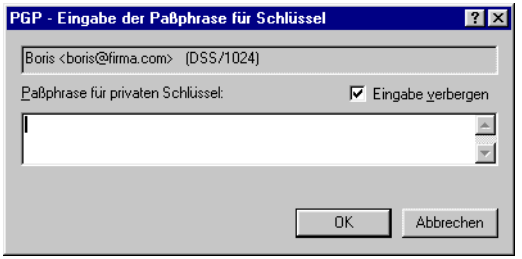


Abbildung 4-2. Dialogfeld für die Paßphrase des Unterschriftenschlüssels

7. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **OK**.

. **WARNUNG:** Wenn Sie Ihre E-Mail-Nachricht nicht sofort senden, sondern in Ihrem E-Mail-Ausgangspostfach speichern, sollten Sie beachten, daß bei einigen E-Mail-Anwendungen die Informationen erst verschlüsselt werden, wenn die E-Mail-Nachricht tatsächlich gesendet wird. Bevor Sie verschlüsselte E-Mail-Nachrichten im E-Mail-Ausgangspostfach speichern, sollten Sie also prüfen, ob Ihre Anwendung die Nachrichten dort auch tatsächlich verschlüsselt. Sollte dies nicht der Fall sein, können Sie Ihre Nachrichten mit der PGPmenu-Option **Jetzt verschlüsseln** verschlüsseln und anschließend im E-Mail-Ausgangspostfach speichern.

So verschlüsseln und unterzeichnen Sie Text mit PGPtools:

1. Kopieren Sie den Text, der verschlüsselt und unterschrieben werden soll, in die Zwischenablage.

2. Klicken Sie in PGPtools auf die Schaltfläche **Verschlüsseln**, **Unterschreiben** oder **Verschlüsseln und Unterschreiben**.

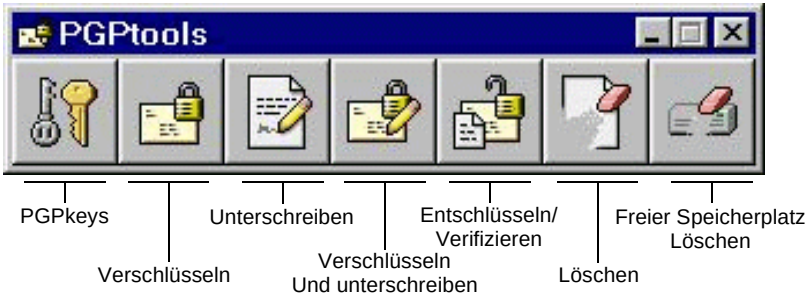


Abbildung 4-3. PGPtools-Fenster

   Das **PGP-Dialogfeld zur Schlüsseldateiauswahl** wird angezeigt.

3. Klicken Sie auf die Schaltfläche **Zwischenablage**.

   Das **PGP-Dialogfeld zur Schlüsselauswahl** wird angezeigt (Abbildung 4-1).

4. Ziehen Sie die öffentlichen Schlüssel der gewünschten Empfänger dieser verschlüsselten E-Mail-Nachricht in das Listenfeld **Empfänger**. Sie können auch auf jeden beliebigen Schlüssel doppelklicken, um ihn auf dem Bildschirm zu verschieben.

   Durch das **Gültigkeitssymbol** wird der Grad der Gewißheit angegeben, daß die öffentlichen Schlüssel in der **Empfängerliste** gültig sind. Diese Echtheit ergibt sich aus den mit dem Schlüssel verknüpften Unterschriften. Ausführliche Informationen finden Sie in Kapitel 6, „Schlüssel verwalten und PGP-Optionen festlegen“.

5. Sie können abhängig von dem Datentyp, den Sie verschlüsseln möchten, eine der folgenden Verschlüsselungsoptionen wählen:

   - **Sichere Darstellung.** Wählen Sie diese Option, um die Daten beim Entschlüsseln vor TEMPEST-Angriffen zu schützen. Wenn Sie diese Option wählen, werden die entschlüsselten Daten in einer speziellen Schriftart zur Verhütung von TEMPEST-Angriffen angezeigt

und sind somit unlesbar für Strahlungsauswertegeräte. Weitere Informationen zu TEMPEST-Angriffen finden Sie im Abschnitt „Sicherheitsrisiken“ auf Seite 263.

HINWEIS: Die Option „Sichere Darstellung“ ist möglicherweise nicht mit früheren PGP-Versionen kompatibel. Mit dieser Option aktivierte verschlüsselte Dateien können mit früheren PGP-Versionen entschlüsselt werden, wobei diese Funktion möglicherweise ignoriert wird.

- **Konventionelle Verschlüsselung.** Wählen Sie diese Option, wenn Sie nicht mit öffentlichen Schlüsseln verschlüsseln sondern eine allgemeine Paßphrase verwenden möchten. Wenn Sie diese Option wählen, wird die Datei mit Hilfe eines Sitzungsschlüssels unter Verwendung einer Paßphrase verschlüsselt (und entschlüsselt). Sie werden aufgefordert, die zu verwendende Paßphrase zu wählen.
- **Selbstentschlüsselndes Archiv.** Wählen Sie diese Option, um eine selbstentschlüsselnde ausführbare Datei zu erstellen. Wenn Sie diese Option wählen, wird die Datei mit Hilfe eines Sitzungsschlüssels unter Verwendung einer Paßphrase verschlüsselt (und entschlüsselt). Sie werden aufgefordert, die zu verwendende Paßphrase zu wählen. Die resultierende ausführbare Datei kann durch Doppelklicken auf die Datei und Eingabe der entsprechenden Paßphrase entschlüsselt werden. Diese Option ist besonders für Benutzer geeignet, die verschlüsselte Dateien an andere Personen senden, die die PGP-Software nicht installiert haben. Beachten Sie, daß sich Absender und Empfänger auf derselben Plattform befinden müssen.

6. Klicken Sie auf **OK**, um Ihre E-Mail-Nachricht zu verschlüsseln und zu unterschreiben.

   Wenn Sie die verschlüsselten Daten unterschreiben möchten, werden Sie vor dem Senden der Nachricht im Dialogfeld für die **Paßphrase des Unterschriftenschlüssels** (siehe Abbildung 4-2) dazu aufgefordert, Ihre Paßphrase einzugeben.

7. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **OK**.

8. Fügen Sie den Text in Ihre E-Mail-Nachricht ein, und senden Sie die Nachricht.

E-Mail-Nachrichten für Empfängergruppen verschlüsseln

Mit PGP können Sie Gruppenverteilungslisten erstellen. Wenn Sie beispielsweise verschlüsselte E-Mail-Nachrichten an zehn Personen mit der E-Mail-Adresse „Verwaltung@xyz.com“ senden möchten, können Sie eine Verteilerliste mit diesem Namen erstellen. Das Menü **Gruppen** in PGPkeys enthält die Option **Gruppen anzeigen**, mit der das Gruppenfenster ein- bzw. ausgeblendet werden kann. Das Fenster **Gruppenliste** wird angezeigt (siehe Abbildung 4-4).

HINWEIS: Wenn Sie bestimmte Nachrichten für alle Mitglieder einer eingerichteten E-Mail-Verteilerliste verschlüsseln möchten, müssen Sie zuerst eine PGP-Gruppe erstellen, die denselben Namen aufweist und dieselben Mitglieder enthält wie die E-Mail-Verteilerliste. Sie haben z. B. in Ihrer E-Mail-Anwendung eine Liste personal@xyz.com eingerichtet. Parallel dazu müssen Sie in PGP eine Gruppe personal@xyz.com anlegen.

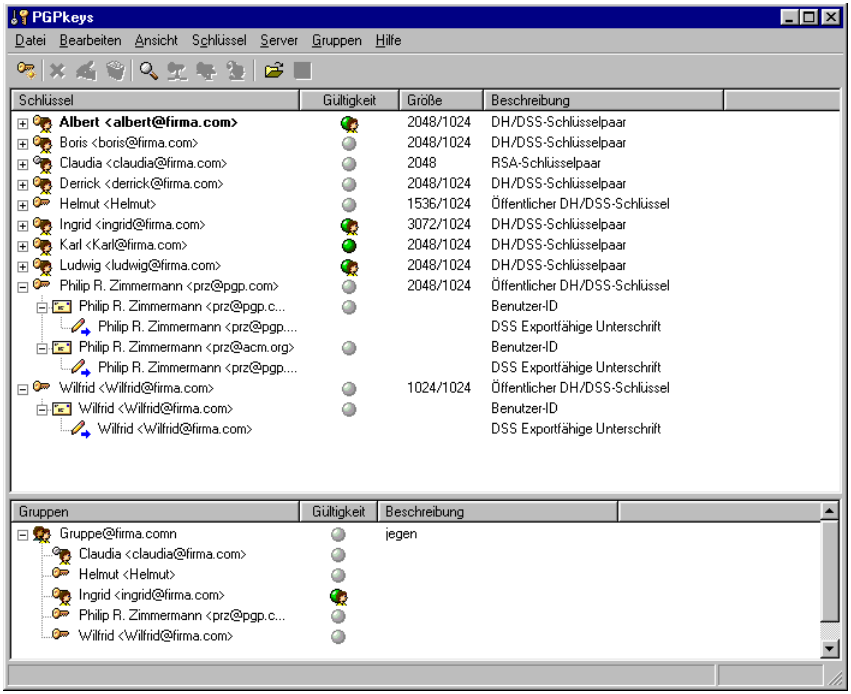


Abbildung 4-4. PGPkeys-Fenster „Gruppen“

Mit Verteilerlisten arbeiten

Mit der Gruppenfunktion können Sie Verteilerlisten erstellen und Listen bearbeiten, an deren Mitglieder Sie verschlüsselte E-Mail-Nachrichten senden möchten.

So erstellen Sie eine Gruppe (Verteilerliste)

1. Wählen Sie im Menü **Gruppen** die Option **Neue Gruppe**.
2. Geben Sie einen Namen für die Gruppenverteilerliste ein. Geben Sie gegebenenfalls eine Gruppenbeschreibung ein. Sie können z. B. die Gruppe „alle@xyz.com“ mit der Beschreibung „Alle Angestellten“ erstellen.
3. Klicken Sie auf **OK**, um die Verteilerliste zu erstellen.

   Die Gruppenverteilerliste wird Ihrem Schlüsselbund hinzugefügt und im Fenster **Gruppen** angezeigt.

So fügen Sie einer Verteilerliste neue Mitglieder hinzu:

1. Markieren Sie im PGPkeys-Fenster die Benutzer oder Listen, die Sie Ihrer Verteilerliste hinzufügen möchten.
2. Ziehen Sie die Benutzer aus dem PGPkeys-Fenster in die gewünschte Verteilerliste im Fenster **Gruppen**.

> **HINWEIS:** Mitglieder einer Verteilerliste können auch anderen Verteilerlisten hinzugefügt werden.

So löschen Sie Mitglieder aus einer Verteilerliste:

1. Markieren Sie in der Verteilerliste das zu löschende Mitglied.
2. Drücken Sie die ENTF-Taste.

   Danach werden Sie von PGP zur Bestätigung Ihrer Auswahl aufgefordert.

So löschen Sie eine Verteilerliste

1. Markieren Sie im Fenster **Gruppen** die zu löschende Verteilerliste.
2. Drücken Sie die ENTF-Taste.

So fügen Sie eine Verteilerliste einer anderen Verteilerliste hinzu:

1. Markieren Sie die hinzuzufügende Verteilerliste.
2. Ziehen Sie die markierte Liste in die Liste, in die sie eingefügt werden soll.

Verschlüsselte und unterschriebene E-Mail-Nachrichten an Verteilerlisten senden

Nachdem Sie Ihre PGP-Verteilerlisten eingerichtet haben, können Sie an diese Empfängergruppen verschlüsselte E-Mail-Nachrichten senden. Weitere Informationen zum Erstellen und Bearbeiten von Verteilerlisten finden Sie im Abschnitt „Mit Verteilerlisten arbeiten“ auf Seite 75.

So senden Sie verschlüsselte und unterschriebene E-Mail-Nachrichten an eine Verteilerliste:

1. Adressieren Sie die E-Mail-Nachricht an die Verteilerliste.

   Der Name der Verteilerliste für die verschlüsselte E-Mail-Nachricht muß mit dem Namen der Verteilerliste für die normale E-Mail-Nachricht übereinstimmen.

2. Erstellen Sie Ihre E-Mail-Nachricht wie gewohnt mit Ihrer E-Mail-Anwendung.
3. Wenn Sie die E-Mail-Nachricht erstellt haben, klicken Sie zuerst auf  , um den Text in Ihrer E-Mail-Nachricht zu verschlüsseln, und anschließend auf  , um Ihre Nachricht zu unterschreiben.

   Das Fenster **PGP – Dialogfeld zur Schlüsselauswahl** wird angezeigt (Abbildung 4-1). Wählen Sie die öffentlichen Schlüssel der Personen aus, die die verschlüsselte oder unterschriebene Datei erhalten sollen. Weitere Informationen zu den verfügbaren Optionen finden Sie im Abschnitt „Mit unterstützten E-Mail-Anwendungen verschlüsseln und unterschreiben“ auf Seite 68.

4. Senden Sie die Nachricht.

E-Mail-Nachrichten entschlüsseln und verifizieren

Ihnen zugesandte E-Mail-Nachrichten können Sie am einfachsten und schnellsten entschlüsseln und verifizieren, wenn Sie mit einer E-Mail-Anwendung arbeiten, die von den PGP-Plug-Ins unterstützt wird. Obwohl bei E-Mail-Anwendungen, die durch Plug-Ins unterstützt werden, die Vorgehensweise je nach E-Mail-Anwendung geringfügig variiert, können Sie E-Mail-Nachrichten entschlüsseln und verifizieren, indem Sie einfach auf die Schaltfläche mit dem Briefumschlag in der E-Mail-Nachricht oder der Symbolleiste Ihrer Anwendung klicken. Gegebenenfalls müssen Sie im Menü Ihrer E-Mail-Anwendung die Option zum **Entschlüsseln/Verifizieren** wählen. Wenn Sie zudem mit einer E-Mail-Anwendung arbeiten, die den PGP / MIME-Standard unterstützt, können Sie sowohl Ihre E-Mail-Nachrichten als auch Dateianhänge entschlüsseln und verifizieren, indem Sie einfach auf ein Symbol klicken, das sich an Ihrer E-Mail-Nachricht befindet.

Wenn Sie mit einer E-Mail-Anwendung arbeiten, die nicht durch die PGP-Plug-Ins unterstützt wird, können Sie Ihre E-Mail-Nachrichten mit PGPtray entschlüsseln und verifizieren. Wenn Ihre E-Mail-Nachricht zusätzlich verschlüsselte Dateianhänge enthält, müssen Sie diese mit PGPtools oder PGPtray separat entschlüsseln.

So entschlüsseln und verifizieren Sie Nachrichten aus unterstützten E-Mail-Anwendungen:

1. Öffnen Sie die E-Mail-Nachricht wie gewohnt.

   Im Textkörper der E-Mail-Nachricht wird ein Block mit unlesbarem, chiffriertem Text angezeigt.

2. Kopieren Sie den chiffrierten Text in die Zwischenablage.

3. Klicken Sie auf das Symbol mit dem Briefumschlag und dem Schloß (), um die Nachricht zu entschlüsseln und zu verifizieren.

   Verwenden Sie PGPtools oder PGPtray, um angehängte Dateien separat zu entschlüsseln und zu verifizieren.

Das Fenster **PGP – Eingabe der Paßphrase für Schlüssel** wird angezeigt. Sie werden aufgefordert, Ihre Paßphrase einzugeben (siehe Abbildung 4-5).

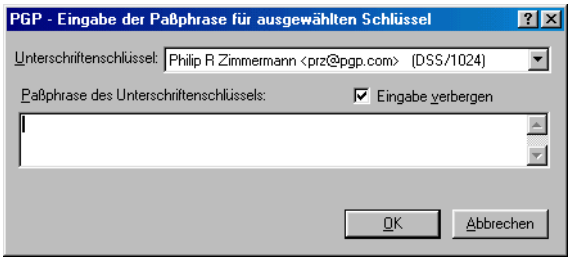


Abbildung 4-5. Dialogfeld für die Paßphrase des Unterschriftenschlüssels

4. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **OK**.

   Die E-Mail-Nachricht wird entschlüsselt. Wenn die Nachricht unterschrieben ist und Sie den öffentlichen Schlüssel des Absenders kennen, wird eine Meldung angezeigt, die die Echtheit der Unterschrift anzeigt.

   Wenn die Nachricht verschlüsselt wird, während die Option **Sichere Darstellung** aktiviert ist, wird eine entsprechende Meldung angezeigt. Klicken Sie auf **OK**, um fortzufahren. Die entschlüsselte Nachricht wird in einem sicheren PGP-Bildschirm in einer speziellen Schriftart zur Verhütung von TEMPEST-Angriffen angezeigt.

5. Sie können die E-Mail-Nachricht im entschlüsselten Zustand speichern, oder Sie können die verschlüsselte Originalversion speichern, so daß sie weiterhin gesichert ist.

HINWEIS: Nachrichten, die verschlüsselt wurden, während die Option **Sichere Darstellung** aktiviert war, können nicht in entschlüsseltem Zustand gespeichert werden.

So entschlüsseln und verifizieren Sie Nachrichten aus nicht-unterstützten E-Mail-Anwendungen:

1. Öffnen Sie die E-Mail-Nachricht wie gewohnt.

   Im Textkörper der E-Mail-Nachricht wird ein Block mit unlesbarem, chiffriertem Text angezeigt.

2. Wählen Sie in PGPtray die Option **Entschlüsseln/Verifizieren**.

   Wenn die E-Mail-Nachricht verschlüsselte Dateianhänge enthält, müssen Sie diese mit PGPtools oder PGPtray separat entschlüsseln.

   Das Fenster **PGP – Eingabe der Paßphrase für Schlüssel** wird angezeigt. Sie werden aufgefordert, Ihre Paßphrase einzugeben (siehe Abbildung 4-5).

3. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **OK**.

   Die E-Mail-Nachricht wird entschlüsselt. Wenn sie unterschrieben wurde, erhalten Sie eine Meldung darüber, ob die Unterschrift echt ist.

   Wenn die Nachricht verschlüsselt wird, während die Option **Sichere Darstellung** aktiviert ist, wird eine entsprechende Meldung angezeigt. Klicken Sie auf **OK**, um fortzufahren. Die entschlüsselte Nachricht wird in einem sicheren PGP-Bildschirm in einer speziellen Schriftart zur Verhütung von TEMPEST-Angriffen angezeigt.

4. Sie können die E-Mail-Nachricht im entschlüsselten Zustand speichern, oder Sie können die verschlüsselte Originalversion speichern, so daß sie weiterhin gesichert ist.

☐ **HINWEIS:** Nachrichten, die verschlüsselt wurden, während die Option **Sichere Darstellung** aktiviert war, können nicht in entschlüsseltem Zustand gespeichert werden.

PGP zur sicheren Dateispeicherung verwenden 5

In diesem Kapitel wird erläutert, wie Sie mit PGP Dateien sicher verwalten können. Es wird beschrieben, wie Sie mit PGP Dateien zum Versenden als E-Mail oder zur sicheren Speicherung auf Ihrem Computer verschlüsseln, entschlüsseln, unterschreiben und verifizieren können. Darüber hinaus werden die PGP-Funktionen zum Löschen und zum Löschen von freiem Speicherplatz beschrieben, mit denen Dateien vollständig von Ihrem Computer gelöscht werden.

Mit PGP Dateien verschlüsseln und entschlüsseln

Mit PGP können Sie Dateien für E-Mail-Anhänge verschlüsseln und unterschreiben. Mit den in diesem Kapitel beschriebenen Verfahren können Sie Dateien auch verschlüsseln und unterschreiben, um sie auf Ihrem Computer sicher zu speichern.

Das PGP-Kontextmenü zum Verschlüsseln und Unterschreiben verwenden

Mit dem PGP-Kontextmenü können Sie verschlüsselte Dateien als Anhang mit Ihrer E-Mail-Nachricht versenden, oder Dateien zum sicheren Speichern auf Ihrem Computer verschlüsseln.

So verschlüsseln und unterschreiben Sie Dateien mit Hilfe des Kontextmenüs

1. Klicken Sie im Windows-Explorer mit der rechten Maustaste auf die zu verschlüsselnden Dateien.
2. Wählen Sie aus dem PGP-Kontextmenü eine der folgenden Optionen:
   - **Verschlüsseln.** Mit dieser Option werden die von Ihnen gewählten Dateien nur verschlüsselt.
   - **Unterschreiben.** Mit dieser Option werden die von Ihnen gewählten Dateien nur unterschrieben.
   - **Verschlüsseln und unterschreiben.** Mit dieser Option werden die von Ihnen gewählten Dateien sowohl verschlüsselt als auch unterschrieben.

Das Dialogfeld **PGP – Dialogfeld zur Schlüsselauswahl** wird angezeigt (siehe Abbildung 5-1).

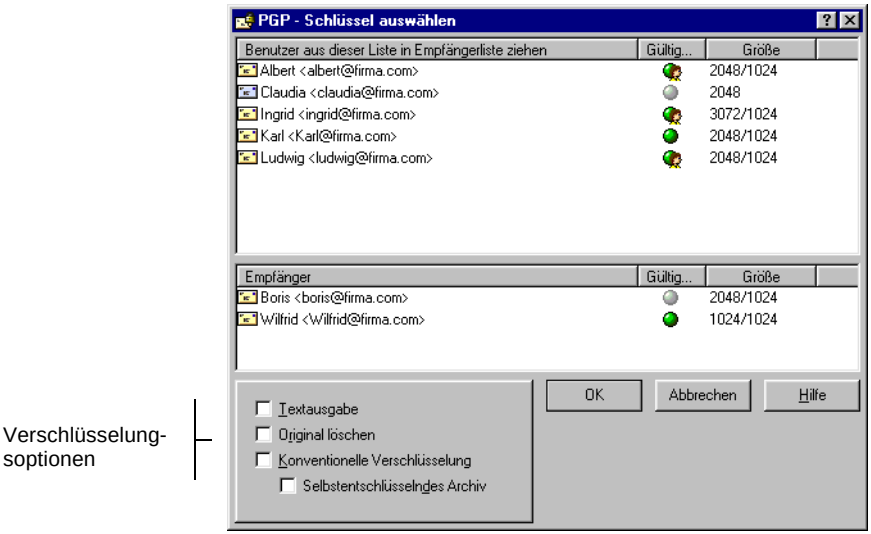


Abbildung 5-1. Fenster „PGP – Dialogfeld zur Schlüsselauswahl“

Wählen Sie die öffentlichen Schlüssel der Person aus, die die verschlüsselte oder unterschriebene Datei erhalten soll.

3. Wählen Sie die öffentlichen Schlüssel aus, indem Sie sie in die **Empfängerliste** ziehen.

   Sie können abhängig von dem Datentyp, den Sie verschlüsseln möchten, eine der folgenden Verschlüsselungsoptionen wählen:

   - **Textausgabe.** Wenn Sie Dateien als Anhänge senden, müssen Sie bei einigen E-Mail-Anwendungen möglicherweise das Kontrollkästchen **Textausgabe** aktivieren, um die Datei als ASCII-Text zu speichern. Dies kann bei älteren E-Mail-Anwendungen notwendig sein, wenn Sie eine Binärdatei senden möchten. Wenn Sie diese Option wählen, wird die verschlüsselte Datei um rund 30 Prozent größer.

   - **Original löschen.** Wenn Sie dieses Kontrollkästchen aktivieren, wird das verschlüsselte Originaldokument überschrieben, so daß auch Personen mit Zugriff auf Ihre Festplatte Ihre vertraulichen Informationen nicht lesen können.

   - **Sichere Darstellung.** Aktivieren Sie dieses Kontrollkästchen, um Text beim Entschlüsseln vor TEMPEST-Angriffen zu schützen. Wenn Sie diese Option wählen, werden die entschlüsselten Daten in

einer speziellen Schriftart zur Verhütung von TEMPEST-Angriffen angezeigt und sind somit unlesbar für Strahlungsauswertegeräte. Weitere Informationen zu TEMPEST-Angriffen finden Sie im Abschnitt „Sicherheitsrisiken“ auf Seite 263.

HINWEIS: Diese Option ist nur verfügbar, wenn Sie Text oder Textdateien verschlüsseln.

- **Konventionelle Verschlüsselung.** Wählen Sie dieses Kontrollkästchen, wenn Sie eine allgemeine Paßphrase statt der Kryptographie mit öffentlichen Schlüsseln verwenden möchten. Die Datei wird mit Hilfe eines Sitzungsschlüssels unter Verwendung einer Paßphrase verschlüsselt (und entschlüsselt). Sie werden aufgefordert, die zu verwendende Paßphrase zu wählen.
- **Selbstentschlüsselndes Archiv.** Wählen Sie dieses Kontrollkästchen, um eine selbstentschlüsselnde ausführbare Datei zu erstellen. Wenn Sie diese Option wählen, wird die Datei mit Hilfe eines Sitzungsschlüssels unter Verwendung einer Paßphrase verschlüsselt (und entschlüsselt). Sie werden aufgefordert, die zu verwendende Paßphrase zu wählen. Die resultierende ausführbare Datei kann durch Doppelklicken auf die Datei und Eingabe der entsprechenden Paßphrase entschlüsselt werden. Diese Option ist besonders für Benutzer geeignet, die verschlüsselte Dateien an andere Personen senden, die die PGP-Software nicht installiert haben. Beachten Sie, daß sich Absender und Empfänger auf derselben Plattform befinden müssen.

Wenn Sie die Dateien unterschreiben, werden Sie zur Eingabe Ihrer Paßphrase aufgefordert.

Nach der Verschlüsselung wird im Ordner, in dem die Originaldatei gespeichert war, diese Datei mit dem angegebenen Namen sowie einem von vier möglichen Symbolen angezeigt:

Verschlüsselt mit Standardausgabe

Verschlüsselt mit Textausgabe

Selbstentschlüsselnde Archivausgabe

Selbstextrahierende Archivausgabe

Wenn Sie einen Ordner verschlüsseln oder unterschreiben, befindet sich die Ausgabe eventuell, abhängig von den gewählten Optionen, in einem neuen Ordner.

Mit Hilfe von PGPtools verschlüsseln und unterschreiben

So verschlüsseln und unterschreiben Sie mit Hilfe von PGPtools

1. Öffnen Sie PGPtools.
2. Wählen Sie im Windows Explorer die zu verschlüsselnden Dateien.

   Sie können mehrere Dateien gleichzeitig auswählen, müssen jedoch jede Datei einzeln verschlüsseln und unterschreiben.
3. Ziehen Sie die Dateien auf die Schaltfläche **Verschlüsseln**, **Unterschreiben** oder **Verschlüsseln** und **Unterschreiben** in PGPtools.

   Das Fenster **PGP – Dialogfeld zur Schlüsselauswahl** wird angezeigt (siehe Abbildung 5-1).
4. Wählen Sie die öffentlichen Schlüssel aus, indem Sie sie in die **Empfängerliste** ziehen.
5. Sie können abhängig von dem Datentyp, den Sie verschlüsseln möchten, eine der folgenden Verschlüsselungsoptionen wählen:

   - **Textausgabe.** Wenn Sie Dateien als Anhänge senden, müssen Sie bei einigen E-Mail-Anwendungen möglicherweise das Kontrollkästchen **Textausgabe** aktivieren, um die Datei als ASCII-Text zu speichern. Dies kann bei älteren E-Mail-Anwendungen notwendig sein, wenn Sie eine Binärdatei senden möchten. Wenn Sie diese Option wählen, wird die verschlüsselte Datei um rund 30 Prozent größer.
   - **Original löschen.** Wenn Sie dieses Kontrollkästchen aktivieren, wird das verschlüsselte Originaldokument überschrieben, so daß auch Personen mit Zugriff auf Ihre Festplatte Ihre vertraulichen Informationen nicht lesen können.
   - **Sichere Darstellung.** Aktivieren Sie dieses Kontrollkästchen, um Text beim Entschlüsseln vor TEMPEST-Angriffen zu schützen. Wenn Sie diese Option wählen, werden die entschlüsselten Daten in einer speziellen Schriftart zur Verhütung von TEMPEST-Angriffen angezeigt und sind somit unlesbar für Strahlungsauswertegeräte. Weitere Informationen zu TEMPEST-Angriffen finden Sie im Abschnitt „Sicherheitsrisiken“ auf Seite 263.

     HINWEIS: Diese Option ist nur verfügbar, wenn Sie Text oder Textdateien verschlüsseln.

- **Konventionelle Verschlüsselung.** Wählen Sie dieses Kontrollkästchen, wenn Sie eine allgemeine Paßphrase statt der Kryptographie mit öffentlichen Schlüsseln verwenden möchten. Die Datei wird mit Hilfe eines Sitzungsschlüssels unter Verwendung einer Paßphrase verschlüsselt (und entschlüsselt). Sie werden aufgefordert, die zu verwendende Paßphrase zu wählen.
- **Selbstentschlüsselndes Archiv.** Wählen Sie dieses Kontrollkästchen, um eine selbstentschlüsselnde ausführbare Datei zu erstellen. Wenn Sie diese Option wählen, wird die Datei mit Hilfe eines Sitzungsschlüssels unter Verwendung einer Paßphrase verschlüsselt (und entschlüsselt). Sie werden aufgefordert, die zu verwendende Paßphrase zu wählen. Die resultierende ausführbare Datei kann durch Doppelklicken auf die Datei und Eingabe der entsprechenden Paßphrase entschlüsselt werden. Diese Option ist besonders für Benutzer geeignet, die verschlüsselte Dateien an andere Personen senden, die die PGP-Software nicht installiert haben. Beachten Sie, daß sich Absender und Empfänger auf derselben Plattform befinden müssen.

6. Klicken Sie auf **OK**.

   Wenn Sie die Dateien unterschreiben, werden Sie zur Eingabe Ihrer Paßphrase aufgefordert.

   Nach der Verschlüsselung wird im Ordner, in dem die Originaldatei gespeichert war, diese Datei mit dem angegebenen Namen sowie einem von vier möglichen Symbolen angezeigt:


Verschlüsselt mit Standardausgabe


Verschlüsselt mit Textausgabe


Selbstentschlüsselnde Archivausgabe


Selbstextrahierende Archivausgabe

   Wenn Sie einen Ordner verschlüsseln oder unterschreiben, befindet sich die Ausgabe eventuell, abhängig von den gewählten Optionen, in einem neuen Ordner.

Mit PGPtray entschlüsseln und verifizieren

Wenn Sie eine E-Mail-Nachricht mit Dateianhängen erhalten und Ihre E-Mail-Anwendung nicht den PGP / MIME-Standard unterstützt, müssen Sie die Nachricht mit Hilfe der Windows-Zwischenablage entschlüsseln.

So entschlüsseln und verifizieren Sie Dateien mit PGPtray

1. Wählen Sie im Windows Explorer die zu entschlüsselnden und zu verifizierenden Dateien.
2. Wählen Sie in PGPtray die Option **Entschlüsseln/Verifizieren**.

   Das Dialogfeld „PGP - Eingabe der Paßphrase für Schlüssel“ wird geöffnet (siehe Abbildung 5-2).

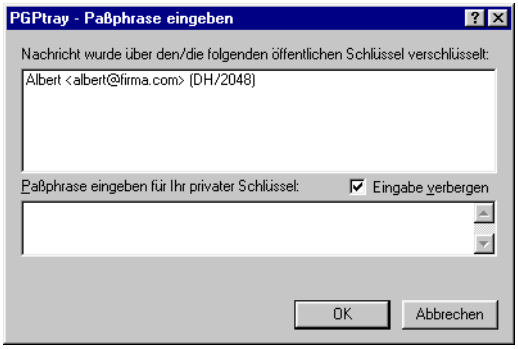


Abbildung 5-2. Dialogfeld „PGP - Eingabe der Paßphrase für Schlüssel“

3. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **O**K.

   Die Datei wird entschlüsselt. Wenn sie unterschrieben wurde, erhalten Sie eine Meldung darüber, ob die Unterschrift echt ist.

   Wenn die Textdatei verschlüsselt wird, während die Option **Sichere Darstellung** aktiviert ist, wird eine entsprechende Meldung angezeigt. Klicken Sie auf **OK**, um fortzufahren. Der entschlüsselte Text wird in einem sicheren PGP-Bildschirm in einer speziellen Schriftart zur Verhütung von TEMPEST-Angriffen angezeigt.

4. Sie können die E-Mail-Nachricht im entschlüsselten Zustand speichern, oder Sie können die verschlüsselte Originalversion speichern, so daß sie weiterhin gesichert ist.

> **HINWEIS:** Nachrichten, die verschlüsselt wurden, während die Option **Sichere Darstellung** aktiviert war können nicht in entschlüsseltem Zustand gespeichert werden. Nach dem Entschlüsseln können Sie nur im sicheren PGP-Bildschirm angezeigt werden.

Mit Hilfe von PGPtools entschlüsseln und verifizieren

So entschlüsseln und verifizieren Sie mit Hilfe von PGPtools:

1. Wählen Sie im Windows-Explorer die zu entschlüsselnden Dateien.
2. Ziehen Sie die Datei auf die Schaltfläche **Entschlüsseln/Verifizieren** in PGPtools.

   Das Fenster **PGP – Eingabe der Paßphrase für Schlüssel** wird angezeigt. Sie werden aufgefordert, Ihre Paßphrase einzugeben (siehe Abbildung 5-2).
3. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **O**K.

   Wenn die Datei unterschrieben wurde, erhalten Sie eine Meldung darüber, ob die Unterschrift echt ist.

   Wenn die Textdatei verschlüsselt wird, während die Option **Sichere Darstellung** aktiviert ist, wird eine entsprechende Meldung angezeigt. Klicken Sie auf **OK**, um fortzufahren. Der entschlüsselte Text wird in einem sicheren PGP-Bildschirm in einer speziellen Schriftart zur Verhütung von TEMPEST-Angriffen angezeigt.
4. Sie können die E-Mail-Nachricht im entschlüsselten Zustand speichern, oder Sie können die verschlüsselte Originalversion speichern, so daß sie weiterhin gesichert ist.

> **HINWEIS:** Nachrichten, die verschlüsselt wurden, während die Option **Sichere Darstellung** aktiviert war können nicht in entschlüsseltem Zustand gespeichert werden. Nach dem Entschlüsseln können Sie nur im sicheren PGP-Bildschirm angezeigt werden.

Dateien mit einem geteilten Schlüssel unterschreiben und entschlüsseln

Wenn ein Schlüssel auf mehrere Halter aufgeteilt wurde, versucht PGP bei Versuchen, mit dem geteilten Schlüssel zu unterschreiben oder zu verschlüsseln, automatisch, den Schlüssel wieder zusammenzusetzen. Der Schlüssel kann lokal oder über das Netzwerk wieder zusammengesetzt werden.

Zum lokalen Zusammensetzen von Schlüsseln müssen die Halter von Schlüsselteilen an dem dafür vorgesehenen Computer anwesend sein. Jeder Halter von Schlüsselteilen muß die Paßphrase für seinen Schlüsselteil eingeben.

Beim Zusammensetzen der Schlüsselteile über das Netz müssen die Halter die Echtheit Ihrer Schlüssel bestätigen und diese entschlüsseln, bevor sie sie über das Netz schicken. Die TLS-Funktion (Transport Layer Security; TLS) von PGP gewährleistet die Sicherheit der Verbindung zur Übertragung der Schlüsselteile. Dadurch können mehrere Benutzer an verschiedenen Standorten mit ihrem Schlüsselteil ohne Risiko unterschreiben und entschlüsseln.

WICHTIG: Vor Empfang der einzelnen Schlüsselteile über das Netz sollten Sie die Fingerabdrücke der einzelnen Halter überprüfen und deren jeweiligen öffentlichen Schlüssel unterschreiben, damit der Authentisierungsschlüssel legitim ist. Anleitungen zum Verifizieren eines Schlüsselpaares finden Sie im Abschnitt „Mit digitalen Fingerabdrücken verifizieren“ auf Seite 64.

So setzten Sie einen geteilten Schlüssel zusammen

1. Kontaktieren Sie alle Halter des geteilten Schlüssels. Das lokale Zusammensetzen der Schlüsselteile setzt die Anwesenheit der Halter am entsprechenden Computer voraus.

   Zur Zusammenführung der Schlüsselteile über das Netz müssen alle Halter an den einzelnen Standorten die entsprechenden Vorbereitungen für das Senden Ihrer Schlüsselteils getroffen haben. Die Halter von Schlüsselteilen müssen über folgendes verfügen:

   - Ein Schlüsselteil und ein Paßwort
   - Einen öffentlichen Schlüssel (zur Authentisierung für den Computer, auf dem die Schlüsselteile zusammengeführt werden)
   - Eine Netzwerkverbindung
   - Die IP-Adresse oder den Domänennamen des Computers, auf dem die Schlüsselteile zusammengeführt werden

2. Wählen Sie auf dem für die Zusammenführung verwendeten Computer im Windows-Explorer die Dateien, die Sie mit dem geteilten Schlüssel unterzeichnen oder entschlüsseln möchten.

3. Klicken Sie mit der rechten Maustaste auf die Dateien, und wählen Sie aus dem PGP-Menü den Befehl **Unterschreiben** oder **Entschlüsseln**.

   Das Dialogfeld **PGP – Eingabe der Paßphrase für ausgewählten Schlüssel** wird angezeigt. Der geteilte Schlüssel ist markiert.

4. Klicken Sie auf **OK**, um den ausgewählten Schlüssel wieder zusammenzusetzen.

   Das Dialogfeld **Sammlung der Schlüsselteile** wird angezeigt (Abbildung 5-3).

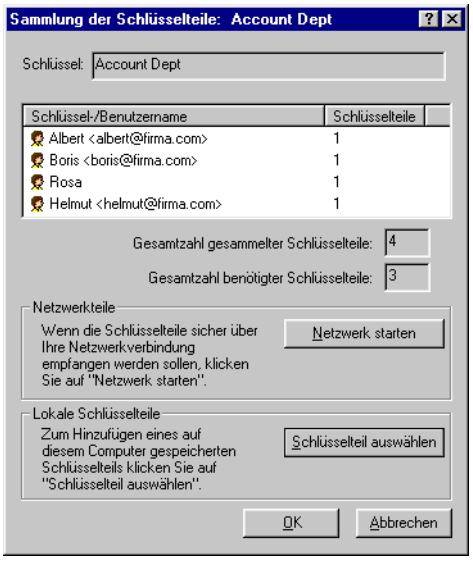


Abbildung 5-3. Dialogfeld „Sammlung der Schlüsselteile“

5. Führen Sie einen der folgenden Schritte aus:

   - **Wenn Sie die Schlüsselteile lokal zusammensetzen**, klicken Sie auf **Schlüsselteil auswählen**, und suchen Sie dann die mit dem geteilten Schlüssel verknüpften Schlüsselteile. Die Schlüsselteile können über die Festplatte, eine Diskette oder ein zugeordnetes Laufwerk zusammengesetzt werden. Fahren Sie mit Schritt 6 fort.

   - **Wenn Sie die Teile über das Netz zusammenführen**, klicken Sie auf **Netzwerk starten**.

Das Dialogfeld zur Eingabe der **Paßphrase** wird angezeigt. Wählen Sie im Feld **Unterschreiben von Schlüsseln** das Schlüsselpaar für die Authentisierung an das entfernte System, und geben Sie die Paßphrase ein. Klicken Sie auf **OK**. Der Computer wird auf den Empfang der Schlüsselteile vorbereitet.

Der Status der Übertragung wird im Feld **Netzwerkteile** angezeigt. Wenn der Status „Daten werden gelesen“ angezeigt wird, ist PGP bereit, die Schlüsselteile zu empfangen.

Zu diesem Zeitpunkt müssen die Halter ihre Schlüsselteile abschicken. Anleitungen zum Senden der Schlüsselteile an den für die Zusammenführung verwendeten Computer finden Sie unter „So senden Sie Schlüsselteile über das Netzwerk“ auf Seite 91.

Wenn ein Schlüssel empfangen wurde, wird das Dialogfeld **Entfernte Authentisierung** angezeigt (siehe Abbildung 5-4).

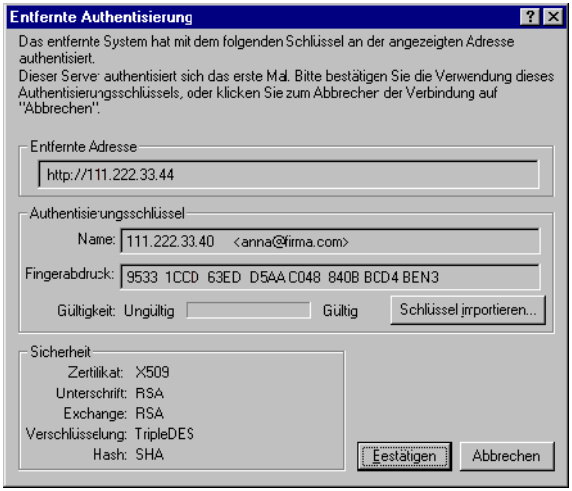


Abbildung 5-4. Dialogfeld „Entfernte Authentisierung“

Wenn Sie den Schlüssel, mit dem die Authentisierung des entfernten Systems durchgeführt wurde, nicht unterschrieben haben, ist der Schlüssel ungültig. Sie können die Schlüsselteile zwar mit einem ungültigen Authentisierungsschlüssel zusammensetzen, dieser Vorgang wird jedoch nicht empfohlen. Sie sollten die Fingerabdrücke der einzelnen Halter überprüfen und deren jeweiligen öffentlichen Schlüssel unterschreiben, um sicherzustellen, daß der Authentisierungsschlüssel legitim ist.

Klicken Sie zur Annahme des Schlüsselteils auf **Bestätigen**.

6. Sammeln Sie die übrigen Teile, bis der Wert für die **Gesamtzahl gesammelter Schlüsselteile** dem Wert für die **Gesamtzahl benötigter Schlüsselteile** entspricht (Dialogfeld **Sammlung der Schlüsselteile**).

7. Klicken Sie auf **OK**.

   Die Datei wird mit dem geteilten Schlüssel unterschrieben oder entschlüsselt.

So senden Sie Schlüsselteile über das Netzwerk

1. Wenn sich die Person, die den geteilten Schlüssel wieder zusammensetzt, an Sie wendet, sollten Sie über folgende Elemente verfügen:

   – Ihr Schlüsselteil und Ihr Paßwort

   – Ihr Schlüsselpaar (zur Authentisierung für den Computer, auf dem die Schlüsselteile zusammengeführt werden)

   – Eine Netzwerkverbindung

   – Die IP-Adresse oder den Domänennamen des Computers, auf dem die Schlüsselteile zusammengeführt werden

2. Wählen Sie im Menü **Datei** von PGPkeys die Option **Schlüsselteil senden**.

   Daraufhin wird das Dialogfeld **Schlüsselteil auswählen** angezeigt.

3. Suchen Sie Ihren Schlüsselteil, und klicken Sie auf **Öffnen**.

   Das Dialogfeld **PGP-Paßphrase eingeben** wird angezeigt.

4. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **O**K.

   Das Dialogfeld **Schlüsselteil senden** wird angezeigt (Abbildung 5-5).

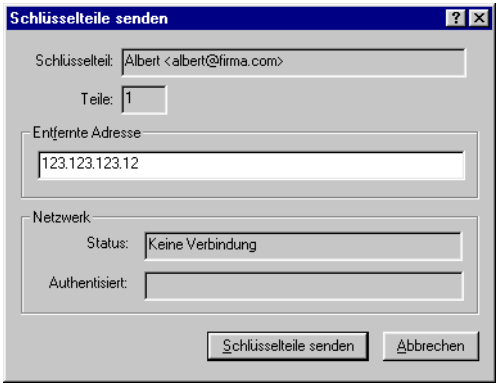


Abbildung 5-5. Dialogfeld „Schlüsselteile senden“

5. Geben Sie im Textfeld **Entfernte Adresse** die IP-Adresse oder den Domänennamen des Computers ein, auf dem die Teile wieder zusammengeführt werden, und klicken Sie dann auf **Schlüsselteile senden**.

   Der Status der Übertragung wird im Feld für den **Netzwerkstatus** angezeigt. Wenn dort „Verbindung hergestellt“ angezeigt wird, werden Sie aufgefordert, sich bei dem Computer, auf dem die Teile zusammengeführt werden, zu authentisieren.

   Im angezeigten Dialogfeld **Entfernte Authentisierung** müssen Sie bestätigen, daß es sich bei dem entfernten Computer um den handelt, an den Sie Ihren Schlüsselteil senden möchten.

6. Klicken Sie zur Fertigstellung der Transaktion auf **Bestätigen**.

   Wenn der Computer Ihre Schlüsselteile empfangen und deren Empfang bestätigt hat, wird ein Meldungsfeld mit einer Benachrichtigung über die erfolgreiche Übertragung der Teile angezeigt.

7. Klicken Sie auf **O**K.

8. Wenn Sie das Senden Ihres Schlüsselteils abgeschlossen haben, klicken Sie im Fenster für die **Schlüsselteile** auf **Fertig**.

Dateien mit der PGP-Löschfunktion löschen

Mit der Option **Löschen** in PGPtools können Sie Dateien und deren Inhalt löschen. Diese Funktion stellt ein sicheres Verfahren zum vollständigen Löschen einer Datei und ihres Inhalts von der Festplatte des Computers dar. Wenn Sie eine Datei wie üblich durch Verschieben in den Papierkorb löschen, wird nur der Name der Datei aus dem Dateiverzeichnis entfernt, der Inhalt der Datei verbleibt jedoch auf der Festplatte. Mit der Funktion zum unwiederherstellbaren **Löschen** werden alle Spuren dieser Datei beseitigt, so daß die Datei mit keinem Software-Tool wiederherstellbar ist.

So löschen Sie eine Datei unwiederherstellbar mit Hilfe des PGP-Kontextmenüs:

1. Wählen Sie im Windows-Explorer die zu löschenden Dateien.

2. Klicken Sie mit der rechten Maustaste auf die Datei, und wählen Sie aus dem Kontextmenü den Befehl **Löschen**.

   Ein Dialogfeld zur Bestätigung des Vorgangs wird angezeigt.

3. Klicken Sie auf **OK**, wenn die Datei unwiederbringlich gelöscht werden soll.

   Wenn der Löschvorgang noch nicht beendet ist und Sie ihn anhalten möchten, klicken Sie auf **Abbrechen**.

   HINWEIS: Durch Klicken auf **Abbrechen** während des Löschvorgangs bleiben eventuell Reste der Datei zurück.

So löschen Sie eine Datei unwiederherstellbar mit Hilfe von PGPtools:

1. Wählen Sie im Windows-Explorer die zu löschenden Dateien.
2. Ziehen Sie die Datei auf die Schaltfläche **Löschen** () in PGPtools.

   Ein Dialogfeld zur Bestätigung des Vorgangs wird angezeigt.

3. Klicken Sie auf **OK**, wenn die Datei unwiederbringlich gelöscht werden soll.

   Wenn der Löschvorgang noch nicht beendet ist und Sie ihn anhalten möchten, klicken Sie auf **Abbrechen**.

   HINWEIS: Durch Klicken auf **Abbrechen** während des Löschvorgangs bleiben eventuell Reste der Datei zurück.

Auch bei Systemen mit virtuellem Speicher wird der gesamte Inhalt der Datei von PGP korrekt überschrieben. Beachten Sie jedoch, daß durch Anwendungen, von denen die Datei vor dem Verschlüsseln gespeichert wurde, möglicherweise Teile der Datei an verschiedenen Stellen auf der Festplatte gespeichert wurden, die nicht mehr als zur Datei gehörig betrachtet werden. Weitere Informationen finden Sie im Abschnitt „Auslagerungsdateien und virtueller Speicher“ auf Seite 267. Um dieses Problem zu lösen, können Sie mit Hilfe des PGP Freespace Wiper alle nicht mehr benötigten Dateifragmente von der Festplatte löschen. Informationen zum PGP Freespace Wiper finden Sie im nächsten Abschnitt. Beachten Sie ebenso, daß viele Programme Dateien während der Bearbeitung automatisch speichern und somit Sicherungskopien der zu löschenden Datei vorhanden sein können.

Mit PGP Free Space Wiper freien Speicherplatz bereinigen

Wenn Sie auf Ihrem Computer Dateien erstellen und löschen, verbleiben die in diesen Dateien enthaltenen Daten auf dem Laufwerk. Mit PGPtools können Sie diese Daten vor dem Löschen der Datei selbst löschen. Damit wird die Möglichkeit der Wiederherstellung dieser Daten ausgeschlossen.

Von vielen Programmen werden bei der Bearbeitung des Inhalts von Dokumenten temporäre Dateien erstellt. Diese Dateien werden beim Schließen der Dokumente gelöscht, aber die eigentlichen Dokumentdaten bleiben über das Laufwerk verstreut. Damit die Chance, daß diese Dokumentdaten später wiederhergestellt werden können, reduziert wird, empfiehlt Ihnen Network Associates, den freien Speicherplatz auf Ihren Laufwerken zu bereinigen und vertrauliche Dokumente zu löschen.

So bereinigen Sie den freien Speicherplatz auf Ihren Laufwerken

WARNUNG: Vor der Ausführung von PGP Free Space Wiper muß die gemeinsame Nutzung von Dateien deaktiviert werden, und alle Anwendungen auf dem zu bereinigenden Volume oder Datenträger müssen geschlossen werden.

1. Öffnen Sie PGPtools.
2. Klicken Sie auf die Schaltfläche **Freien Speicherplatz löschen** () in PGPtools.

   Das Begrüßungsfenster von **PGP Free Space Wiper** wird angezeigt.
3. Lesen Sie die angezeigten Informationen sorgfältig durch, und klicken Sie auf **Weiter**, um zum nächsten Dialogfeld zu wechseln.

   Sie werden aufgefordert, das zu bereinigende Volume und die Anzahl der dazu durchzuführenden Durchläufe anzugeben.
4. Wählen Sie im entsprechenden Feld die Festplatte oder das **Volume**, das von PGP gelöscht werden soll. Wählen Sie anschließend die Anzahl der dazu durchzuführenden Durchläufe. Folgende Werte werden empfohlen:
   - 3 Durchläufe bei privater Nutzung.
   - 10 Durchläufe bei geschäftlicher Nutzung.

- 18 Durchläufe bei militärischer Nutzung.
- 26 Durchläufe für maximale Sicherheit.

HINWEIS: Von professionellen Firmen, die sich mit der Wiederherstellung von Daten befassen, wurden schon Daten wiederhergestellt, die vorher neunmal überschrieben worden waren. PGP arbeitet in den einzelnen Durchläufen mit hochentwickelten Mustern, damit Ihre vertraulichen Daten unter keinen Umständen wiederhergestellt werden können.

5. Klicken Sie auf **Weiter**, um fortzufahren.

   Im angezeigten Dialogfeld **Freien Speicherplatz löschen** (siehe Abbildung 5-6) sind statistische Angaben über das von Ihnen gewählte Laufwerk oder Volume aufgeführt.

Abbildung 5-6. Löschen von freiem Speicherplatz (Dialogfeld „Freien Speicherplatz löschen“)

6. Klicken Sie auf die Schaltfläche **Löschvorgang beginnen**, um das Löschen des Laufwerks oder Volumes zu starten.

   Das Laufwerk oder Volume wird von PGP Free Space Wiper gescannt und anschließend von verbliebenen Fragmenten bereinigt.

7. Nach Abschluß der Bereinigung klicken Sie auf **Vorgang abgeschlossen**.

WARNUNG: Durch Klicken auf **Abbrechen** während des Löschvorgangs bleiben eventuell Reste der Datei auf Ihrer Festplatte zurück.

PGP Free Space Wiper planen

Sie können den Windows-Taskplaner verwenden, um regelmäßiges Löschen von freiem Speicherplatz auf Ihrer Festplatte zu planen.

WICHTIG: Um diese Planungsfunktion zu verwenden, muß der Windows-Taskplaner auf Ihrem Computer installiert sein. Sollte dies nicht der Fall sein, können Sie ihn von der Microsoft-Web-Site (http://www.microsoft.com) herunterladen.

So planen Sie das Löschen von freiem Speicherplatz

1. Befolgen Sie die Schritte 1-5 in „So bereinigen Sie den freien Speicherplatz auf Ihren Laufwerken“ auf Seite 94.

   Im angezeigten Dialogfeld **Freien Speicherplatz löschen** (siehe Abbildung 5-6) sind statistische Angaben über das von Ihnen gewählte Laufwerk oder Volume aufgeführt.

Abbildung 5-7. Free Space Wiper (Dialogfeld „Freien Speicherplatz löschen“)

2. Klicken Sie auf die Schaltfläche **Planen**, um das Löschen des Laufwerks oder Volumes zu starten.

   Das Dialogfeld **PGP Free Space Wipe planen** wird angezeigt.

3. Klicken Sie auf **OK**, um fortzufahren.

   Wenn Sie Windows NT ausführen, wird das Windows NT-Dialogeld zur Bestätigung des Paßworts angezeigt.

   Geben Sie Ihr Paßwort zum Anmelden bei Windows NT in das erste Textfeld ein. Drücken Sie die TABULATORTASTE, um den Cursor in das nächste Textfeld zu setzen. Bestätigen Sie Ihre Eingabe, indem Sie Ihr Paßwort nochmals eingeben. Klicken Sie auf „OK“.

   Das Dialogfeld für den **Windows-Taskplaner** wird angezeigt (siehe Abbildung 5-8).

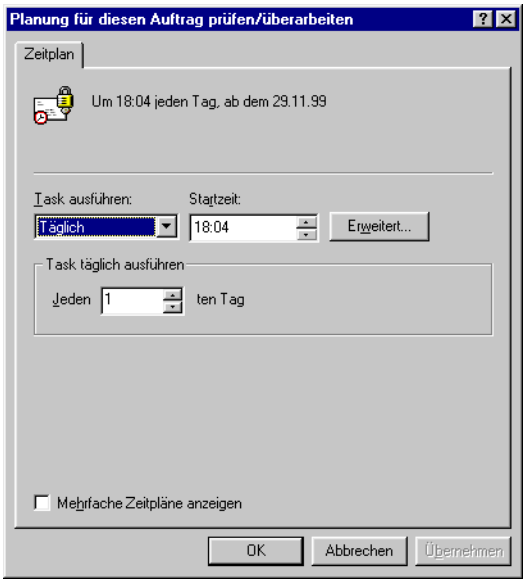


Abbildung 5-8. Dialogfeld für den Windows-Taskplaner

4. Wählen Sie aus, wie oft der entsprechende Task von dem Bereich **Task planen** aus ausgeführt werden soll. Sie haben folgende Möglichkeiten:

   - **Täglich.** Dadurch wird Ihr Task einmal zur angegebenen Zeit am angegebenen Tag ausgeführt. Klicken Sie auf **OK**, um das Dialogfeld zu schließen. Geben Sie dann im Textfeld für die **Anfangszeit** die Uhrzeit ein, zu der der Task täglich ausgeführt werden soll.

   - **Wöchentlich.** Dadurch wird Ihr Task am angegebenen Tag zur angegebenen Zeit wöchentlich ausgeführt. Geben Sie im entsprechenden Textfeld an, wie viele Wochen zwischen dem Bereinigen von Festplatten liegen sollen, und wählen Sie dann einen Tag in der Liste für die **wöchentlichen Taskplanung**.

   - **Monatlich.** Dadurch wird Ihr Task am angegebenen Tag zur angegebenen Zeit einmal im Monat ausgeführt. Geben Sie im entsprechenden Textfeld die Uhrzeit und dann das Datum an, an dem der Task ausgeführt werden soll. Klicken Sie auf **Monate auswählen**, um anzugeben, in welchen Monaten der Task ausgeführt werden soll.

   - **Einmal.** Dadurch wird Ihr Task am angegebenen Tag zur angegebenen Zeit genau einmal ausgeführt. Geben Sie im entsprechenden Textfeld die Uhrzeit an, und wählen Sie dann im Textfeld für die Ausführung einen Monat und ein Datum aus.

   - **Beim Starten des Computers.** Dadurch wird Ihr Task nur beim Starten des Computers ausgeführt.

   - **Beim Anmelden.** Dadurch wird Ihr Task ausgeführt, wenn Sie sich bei Ihrem Computer anmelden.

   - **Im Leerlauf.** Dadurch wird Ihr Task ausgeführt, wenn Ihr Computer sich für den im Textfeld in Minuten angegebenen Zeitraum im Leerlauf befindet.

5. Klicken Sie auf **Erweitert**. Ein Dialogfeld wird geöffnet, in dem Sie zusätzliche Planungsoptionen wie das Anfangs- und das Enddatum sowie die Dauer des Tasks auswählen können.

6. Klicken Sie auf **OK**.

   Ein Dialogfeld zur Bestätigung des Vorgangs wird angezeigt. Ihr Task zum Löschen von freiem Speicherplatz wird nun geplant.

Schlüssel verwalten und PGP-Optionen festlegen 6

In diesem Kapitel werden die Überprüfung und Verwaltung der in Ihren Schlüsselbunden gespeicherten Schlüssel erklärt. Außerdem wird beschrieben, wie Sie die Optionen auf die Anforderungen Ihrer persönlichen Computerumgebung abstimmen.

Schlüssel verwalten

Sowohl die von Ihnen erstellten Schlüssel als auch die Schlüssel, die Sie von anderen erhalten, werden in digitalen Schlüsselbunden gespeichert. Diese Schlüsselbunde sind im wesentlichen Dateien, die auf der Festplatte oder einer Diskette gespeichert werden. Normalerweise werden Ihre privaten Schlüssel in einer Datei mit dem Namen SECRING.SKR und Ihre öffentlichen Schlüssel in einer anderen Datei mit dem Namen PUBRING.PKR gespeichert. Diese Dateien befinden sich für gewöhnlich im Ordner „PGP Keyrings“.

HINWEIS: Da Ihr privater Schlüssel automatisch verschlüsselt wird und Ihre Paßphrase sicher ist, können Ihre Schlüsselbunde gefahrlos auf Ihrem Computer verbleiben. Wenn Sie Ihre Schlüssel jedoch nicht unter dem Standard-Pfad speichern möchten, können Sie einen anderen Dateinamen bzw. ein anderes Verzeichnis wählen. Genauere Informationen finden Sie weiter hinten in diesem Kapitel im Abschnitt „PGP-Optionen festlegen“.

Gelegentlich kann es erforderlich sein, die mit Ihren Schlüsseln verknüpften Attribute zu überprüfen oder zu ändern. Wenn Sie beispielsweise den öffentlichen Schlüssel eines anderen Benutzers erhalten, können Sie den Schlüsseltyp (RSA oder Diffie-Hellman / DSS) identifizieren sowie dessen Fingerabdruck oder seine Gültigkeit anhand der zu dem Schlüssel gehörenden digitalen Unterschriften überprüfen. Darüber hinaus können Sie den öffentlichen Schlüssel eines anderen Benutzers unterschreiben, um die Gültigkeit des Schlüssels zu bestätigen, dem Schlüsseleigentümer ein bestimmtes Maß an Vertrauen aussprechen oder die Paßphrase für Ihren privaten Schlüssel ändern. Vielleicht möchten Sie auch auf einem Schlüssel-Server nach dem Schlüssel eines anderen Benutzers suchen. Diese Schlüsselverwaltungsfunktionen werden über PGPkeys ausgeführt.

Das PGPkeys-Fenster

Zum Öffnen des PGPkeys-Fensters öffnen Sie das Menü **Start**, klicken auf **Programme–>PGP–>PGPkeys**, oder klicken Sie auf das PGPtray-Symbol ( ) in der Taskleiste und dann auf **PGPkeys starten**.

Im **PGPkeys**-Fenster (siehe Abbildung 6-1) werden Ihre selbst erstellten Schlüssel sowie alle öffentlichen Schlüssel angezeigt, die Sie zu Ihrem öffentlichen Schlüsselbund hinzugefügt haben.

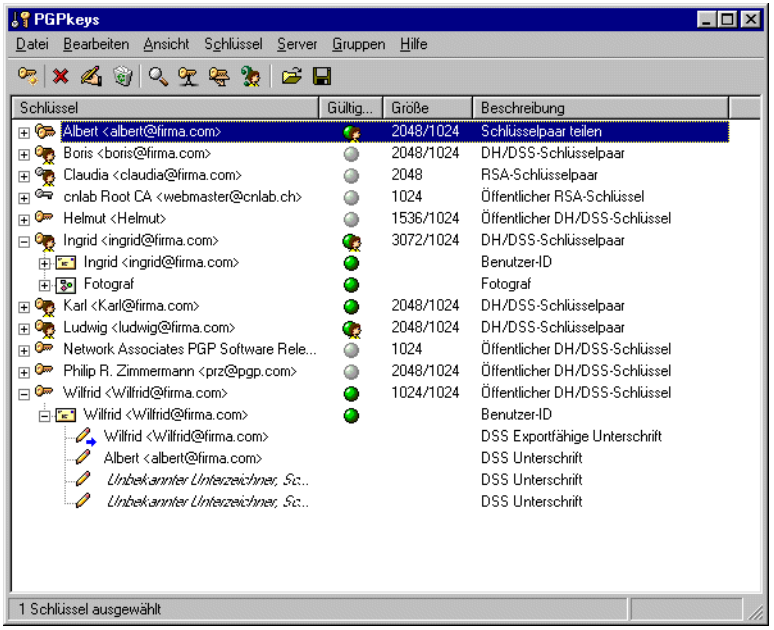


Abbildung 6-1. PGPkeys-Fenster

Symbole mit einem Schlüssel und einem Benutzer ( ) stellen die privaten und öffentlichen Schlüsselpaare dar, die Sie für sich selbst erstellt haben. Symbole mit einem Schlüssel ( ) stellen die öffentlichen Schlüssel dar, die Sie von anderen Benutzern erhalten haben. Wenn Sie mehr als einen Schlüsseltyp besitzen, wird Ihnen auffallen, daß RSA-Schlüssel grau und Diffie-Hellmann / DSS-Schlüssel gelb dargestellt sind.

Durch Klicken auf das Pluszeichen links neben einem Schlüsselsymbol wird die Benutzer-ID und die E-Mail-Adresse des betreffenden Schlüsseleigentümers und links davon ein Umschlagsymbol ( ) angezeigt. Wenn Sie auf das Pluszeichen neben einem Umschlagsymbol klicken, können Sie die Unterschriften der Benutzer sehen, die die entsprechende Benutzer-ID zertifiziert haben. Wenn Sie diese Schritte nicht für jeden Schlüssel einzeln durchführen möchten, wählen Sie die gewünschten Schlüssel und anschließend im Menü **Bearbeiten** den Befehl **Auswahl einblenden**.

Definitionen der PGPkeys-Attribute

Einige der mit Schlüsseln verbundenen Attribute können im PGPkeys-Hauptfenster angezeigt werden. Die anzuzeigenden Attribute können Sie im Menü **Ansicht** auswählen. Für jedes im Menü **Ansicht** ausgewählte Element stellt PGPkeys im Hauptfenster eine Spalte dar. Wenn Sie die Reihenfolge dieser Spalten verändern möchten, klicken Sie auf den Spaltenkopf der zu bewegenden Spalte und ziehen ihn an den gewünschten Platz.

Tabelle 6-1. Überblick über PGPkeys-Attribute

Schlüssel	Zeigt eine symbolische Darstellung des Schlüssels zusammen mit dem Benutzernamen und der E-Mail-Adresse des Eigentümers sowie den Namen der Unterzeichner an.
Gültigkeit	Gibt den Grad der Gewißheit an, mit der der Schlüssel tatsächlich dem angegebenen Eigentümer gehört. Die Gültigkeit richtet sich nach dem Unterzeichner des Schlüssels und dem Grad Ihres Vertrauens in die Unterzeichner, die Echtheit eines Schlüssels bestätigen zu können. Die von Ihnen selbst unterschriebenen öffentlichen Schlüssel verfügen über den höchsten Gültigkeitsgrad. Dabei wird davon ausgegangen, daß Sie einen Schlüssel für eine andere Person nur unterschreiben, wenn Sie von der Gültigkeit des Schlüssels absolut überzeugt sind. Die Gültigkeit aller anderen Schlüssel hängt von dem Maß an Vertrauen ab, das Sie den Benutzern aussprechen, die den Schlüssel unterschrieben haben. Wenn mit dem Schlüssel keine Unterschriften verknüpft sind, wird er als nicht echt angesehen, und bei jeder Verschlüsselung mit dem Schlüssel wird eine entsprechende Meldung angezeigt. Die Gültigkeit wird in Abhängigkeit von den Einstellungen, die von Ihnen in den erweiterten **Optionen** unter „Zweitrangige Gültigkeitsebene anzeigen“ vorgenommen wurden, entweder durch Kreis- oder Balkensymbole angezeigt (siehe „Erweiterte Optionen festlegen“ später in diesem Kapitel). Ist diese Option aktiviert, wird die Gültigkeit von Schlüsseln wie folgt angezeigt:  , Ein unausgefüllter Balken für ungültige Schlüssel  , Ein halb ausgefüllter Balken für zweitrangige gültige Schlüssel  , Ein ausgefüllter Balken für gültige Schlüssel, die Ihnen nicht gehören  , Ein gestreifter Balken für gültige Schlüssel, die Ihnen gehören Ist diese Option deaktiviert, wird die Gültigkeit von Schlüsseln wie folgt angezeigt:  , Eiz grauer Kreis für ungültige und zweitrangige, gültige Schlüssel, wenn unter Erweitert **die Option** „Zweitrangige gültige Schlüssel wie ungültige behandeln“ aktiviert ist  , Ein grüner Kreis für gültige Schlüssel, die Ihnen nicht gehören Es ist möglich, daß Ihr Sicherheitsbeauftragter in Ihrer Firma die Schlüssel der Benutzer mit dem firmenweiten Unterschriftenschlüssel unterzeichnet. So unterschriebene Schlüssel gelten normalerweise als vollständig gültig. Weitere Informationen finden Sie in Kapitel 2, „PGP verwenden“.

Tabelle 6-1. Überblick über PGPkeys-Attribute

Größe	In dieser Spalte wird die Bitanzahl angegeben, die bei der Erzeugung des Schlüssels verwendet wurde. Je größer der Schlüssel ist, desto geringer ist normalerweise die Gefahr, daß er je entschlüsselt wird. Allerdings dauert die Verschlüsselung und Entschlüsselung von Daten bei größeren Schlüsseln etwas länger als bei kleineren Schlüsseln. Wenn Sie einen Diffie-Hellman/DSS-Schlüssel erstellen, steht eine Zahl für den Diffie-Hellman-Anteil und die andere Zahl für den DSS-Anteil. Der DSS-Anteil wird zum Unterschreiben und der Diffie-Hellman-Anteil für die Verschlüsselung verwendet.
Beschreibung	Beschreibt die Art der in der Spalte **Schlüssel** angezeigten Informationen: Schlüsseltyp, Art der ID bzw. Unterschriftstyp.
Zusätzlicher Entschlüsselungsschlüssel	Zeigt an, ob dem Schlüssel ein zusätzlicher Entschlüsselungsschlüssel (Additional Decryption Key, ADK) zugeordnet ist.
Schlüssel-ID	Eine eindeutige Kennung, die mit jedem Schlüssel verknüpft ist. Diese Kennung dient der Unterscheidung zwischen zwei Schlüsseln mit demselben Benutzernamen und derselben E-Mail-Adresse.
Vertrauen	Hier wird das Maß angegeben, in dem Sie dem Schlüsseleigentümer vertrauen, die öffentlichen Schlüssel anderer Personen zu verwalten. Dieses Vertrauen spielt eine Rolle, wenn Sie selbst die Gültigkeit des öffentlichen Schlüssels einer Person nicht verifizieren können und sich daher auf das Urteil anderer Benutzer, die den Schlüssel unterschrieben haben, verlassen müssen. Wenn Sie ein Schlüsselpaar erstellen, wird diesem implizites Vertrauen ausgesprochen. Dies wird durch die gestreiften Vertrauens- oder Gültigkeitsbalken bzw. durch einen grünen Kreis und ein Benutzersymbol angezeigt. Wenn Sie einen öffentlichen Schlüssel erhalten, der mit einem anderen Schlüssel des Benutzers an Ihrem Schlüsselbund unterschrieben wurde, basiert dessen Echtheit auf dem Vertrauen, das Sie dem Unterzeichner dieses Schlüssels ausgesprochen haben. Im Dialogfeld **Schlüsseleigenschaften** können Sie einen Vertrauensgrad festlegen – entweder „Nicht Vertrauenswürdig“, „Eingeschränkt“ oder „Vertrauenswürdig“.
Gültigkeit	Zeigt das Datum an, an dem der Schlüssel abläuft. Die meisten Schlüssel sind so eingestellt, daß sie nie ihre Gültigkeit verlieren. Es gibt jedoch auch Fälle, in denen ein Benutzer will, daß der Schlüssel nur für eine bestimmte Zeitdauer benutzt wird.
Erstellung	Zeigt das Datum der Schlüsselerstellung an. Sie können die Gültigkeit eines Schlüssels zum Teil danach beurteilen, wie lange der Schlüssel schon im Umlauf ist. Wenn ein Schlüssel bereits längere Zeit verwendet wird, ist es unwahrscheinlich, daß jemand versucht, ihn zu ersetzen, da viele Kopien im Umlauf sind. Verlassen Sie sich als Beweis für die Gültigkeit eines Schlüssels jedoch nie allein auf das Erstellungsdatum.

Schlüsseleigenschaften überprüfen

Zusätzlich zu den allgemeinen Attributen, die im **PGPkeys**-Fenster angezeigt werden, können Sie noch weitere Eigenschaften von Schlüsseln und Teilschlüsseln überprüfen und ändern.

Das Fenster **Schlüsseleigenschaften** enthält die Registerkarten **Allgemein**, **Teilschlüssel** und **Rücknahmeschlüssel**, wobei Ihnen jede dieser Registerkarten die nötigen Informationen zum öffentlichen Schlüssel einer Person oder über die Möglichkeit liefert, in Ihrem eigenen öffentlichen Schlüssel Attribute zu erstellen, zu konfigurieren, zu bearbeiten oder zu löschen. Genauere Informationen zu den einzelnen Elementen erhalten Sie in den folgenden Abschnitten.

Um auf die Eigenschaften eines bestimmten Schlüssels zuzugreifen, markieren Sie den gewünschten Schlüssel und wählen anschließend im Menü **Schlüssel** die Option **Schlüsseleigenschaften**. Das Dialogfeld **Schlüsseleigenschaften** wird geöffnet (siehe Abbildung 6-2).

Abbildung 6-2. Dialogfeld „Schlüsseleigenschaften“ (Registerkarte „Allgemein“)

Registerkarte „PGP-Schlüsseleigenschaften - Allgemein“

Um auf die Registerkarte **PGP-Schlüsseleigenschaften** zuzugreifen, markieren Sie den gewünschten Schlüssel und wählen anschließend im Menü „Schlüssel“ die Option **Schlüsseleigenschaften**.

Eine Beschreibung der einzelnen auf der Registerkarte **PGP-Schlüsseleigenschaften - Allgemein** enthaltenen Attribute finden Sie in Tabelle 6-2, „Attribute der Registerkarte „PGP-Schlüsseleigenschaften - Allgemein““ auf Seite 104.

Tabelle 6-2. Attribute der Registerkarte „PGP-Schlüsseleigenschaften - Allgemein“

Schlüssel-ID	Eine eindeutige Kennung, die mit jedem Schlüssel verknüpft ist. Diese Kennung dient der Unterscheidung zwischen zwei Schlüsseln mit demselben Benutzernamen und derselben E-Mail-Adresse.
Typ	Der Schlüsseltyp: RSA oder Diffie-Hellman/DSS.
Schlüsselgröße	Die Größe des Schlüssels.
Erstellt	Das Erstellungsdatum des Schlüssels.
Läuft ab	Das Datum, an dem der Schlüssel seine Gültigkeit verliert Der Eigentümer gibt dieses Datum bei der Erstellung des Schlüssels an. Normalerweise wird dieser Wert auf „Nie“ gesetzt. Wenn der Eigentümer den Schlüssel jedoch nur für einen bestimmten Zeitraum verwenden möchte, gibt er hier die entsprechende Gültigkeit an.
Verschlüsselung	CAST, Triple DES oder IDEA Dies ist der vom Schlüsseleigentümer bevorzugte Verschlüsselungsalgorithmus, mit dem Sie dessen Schlüssel verschlüsseln sollen. Wenn der betreffende Algorithmus in Ihren **erweiterten Optionen** zugelassen ist, wird er immer dann verwendet, wenn mit diesem Schlüssel verschlüsselt wird.
Schlüssel zusammensetzen	Öffnet das Dialogfeld **Sammlung der Schlüsselteile**. Dieses Dialogfeld ist nur bei aufgeteilten Schlüsseln verfügbar. Informationen zum Zusammensetzen von geteilten Schlüsseln finden Sie im Abschnitt „Dateien mit einem geteilten Schlüssel unterschreiben und entschlüsseln“ auf Seite 88.
Aktiviert	Gibt an, ob der Schlüssel zur Zeit aktiviert oder deaktiviert ist. Wenn ein Schlüssel deaktiviert ist, wird er im PGPkeys-Fenster grau hinterlegt angezeigt und kann nur noch zum **Entschlüsseln** und **Verifizieren** verwendet werden. Der Schlüssel verbleibt jedoch in Ihrem Schlüsselbund, und Sie können ihn jederzeit wieder aktivieren. Zur Aktivierung und Deaktivierung eines Schlüssels aktivieren bzw. deaktivieren Sie das Kontrollkästchen **Aktiviert**. (Dieses Kontrollkästchen wird bei Schlüsseln, denen Sie Ihr implizites Vertrauen aussprechen, nicht angezeigt.) Durch diese Funktion wird verhindert, daß beim Senden von verschlüsselten E-Mail-Nachrichten selten verwendete Schlüssel im Dialogfeld zur **Schlüsselauswahl** angezeigt werden.

Tabelle 6-2. Attribute der Registerkarte „PGP-Schlüsseleigenschaften - Allgemein“

Ändern Paßphrase	Ändert die Paßphrase eines privaten Schlüssels. Sobald Sie der Meinung sind, daß Ihre Paßphrase nicht mehr geheim ist, klicken Sie zur Eingabe einer neuen Paßphrase auf diese Schaltfläche. Es empfiehlt sich, die eigene Paßphrase ungefähr alle sechs Monate zu ändern. Anweisungen zum Ändern Ihrer Paßphrase finden Sie weiter hinten in diesem Kapitel im Abschnitt „Ändern Ihrer Paßphrase“.
Fingerabdruck	Eine eindeutige Kennummer, die bei der Schlüsselerstellung erzeugt wird. Dies ist das Hauptkriterium für die Überprüfung der Echtheit eines Schlüssels. Sie überprüfen den Fingerabdruck am besten, indem Sie den Eigentümer bitten, den Fingerabdruck telefonisch durchzugeben. Sie können dann diesen Fingerabdruck mit dem Fingerabdruck Ihrer Kopie des öffentlichen Schlüssels dieser Person vergleichen. Der Fingerabdruck kann auf zwei Weisen angezeigt werden: in einer eindeutigen Wörterliste oder in Hexadezimalform.
Hexadezimal	Zeigt den Fingerabdruck als eindeutige Reihe von Hexadezimalzahlen an. Standardmäßig ist diese Option deaktiviert, und der Fingerabdruck wird als eindeutige Reihe von Wörtern angezeigt.
Vertrauensmodell	Gibt die Echtheit des Schlüssels an. Diese ergibt sich aus der Zertifizierung des Schlüssels und aus dem Maß, in dem Sie dem Schlüsseleigentümer vertrauen, die Echtheit des öffentlichen Schlüssels anderer Personen zu bestätigen. Sie können den Vertrauensgrad einstellen, indem Sie den Schieberegler an die gewünschte Stelle ziehen („Vertrauenswürdig“, „Eingeschränkt“ oder „Nicht Vertrauenswürdig“).Dieser Schieberegler ist bei zurückgenommenen und abgelaufenen Schlüsseln sowie Schlüsseln, denen Ihr implizites Vertrauen gehört, deaktiviert.

Fenster für Teilschlüsseleigenschaften

Um auf die Registerkarte **Teilschlüsseleigenschaften** zuzugreifen, markieren Sie den gewünschten Schlüssel und wählen anschließend im Menü **Schlüssel** die Option **Schlüsseleigenschaften**. Das Dialogfeld **Schlüsseleigenschaften** wird geöffnet (siehe Abbildung 6-2 auf Seite 103). Klicken Sie auf die Registerkarte **Teilschlüssel**. Die Registerkarte **Teilschlüssel** wird angezeigt (siehe Abbildung 6-3).

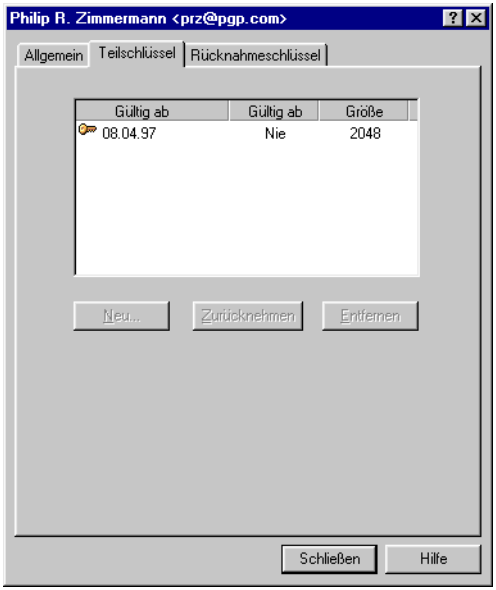


Abbildung 6-3. Dialogfeld „Schlüsseleigenschaften“ (Registerkarte „Teilschlüssel“)

Eine Beschreibung der einzelnen auf der Registerkarte **Teilschlüssel** enthaltenen Attribute und Tasks erhalten Sie in Tabelle 6-2, „ Attribute der Registerkarte „ PGP-Schlüsseleigenschaften - Allgemein““ auf Seite 104.

Tabelle 6-3. Registerkarte „Teilschlüsseleigenschaften“

Gültig ab	Das Datum, ab dem der Teilschlüssel aktiv wird.
Läuft ab	Das Datum, an dem der Teilschlüssel seine Gültigkeit verliert. Eigentümer geben diesen Zeitpunkt bei Erstellung ihrer Teilschlüssel an. Teilschlüssel sind normalerweise nur für einen begrenzten Zeitraum aktiv.
Schlüsselgröße	Die Größe des Teilschlüssels.
Neu	Erstellt einen neuen Teilschlüssel. Informationen zum Erstellen eines neuen Teilschlüssels finden Sie im Abschnitt „Neue Teilschlüssel erstellen“ auf Seite 34.

Tabelle 6-3. Registerkarte „Teilschlüsseleigenschaften“

Zurücknehmen	Nimmt den markierten Verschlüsselungsteilschlüssel zurück. Nachdem Sie den Teilschlüssel zurückgenommen und den Schlüssel neu verteilt haben, werden andere Benutzer nicht mehr in der Lage sein, Daten mit diesem Teilschlüssel zu verschlüsseln.
Entfernen	Entfernt den markierten Verschlüsselungsteilschlüssel endgültig. Diese Prozedur kann nicht rückgängig gemacht werden. Alle Daten, die mit dem entsprechenden Teilschlüssel verschlüsselt wurden, können nicht mehr entschlüsselt werden. **TIP:** Verwenden Sie die Option „Zurücknehmen“, wenn Sie einen Teilschlüssel deaktivieren und den Eintrag auf dem Schlüssel-Server aktualisieren möchten. Ein einmal auf dem Server abgelegter Teilschlüssel kann nicht wieder entfernt werden.

Fenster für zugeordneten Rücknahmeschlüssel

Um auf die Registerkarte **Rücknahmeschlüssel** zuzugreifen, markieren Sie den gewünschten Schlüssel und wählen anschließend im Menü **Schlüssel** die Option **Schlüsseleigenschaften**. Das Dialogfeld **Schlüsseleigenschaften** wird geöffnet (siehe Abbildung 6-2 auf Seite 103). Klicken Sie auf die Registerkarte **Rücknahmeschlüssel**. Die Registerkarte **Rücknahmeschlüssel** wird angezeigt (siehe Abbildung 6-4).

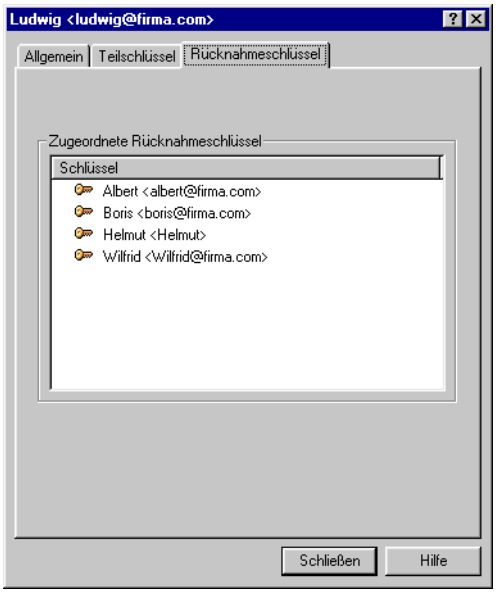


Abbildung 6-4. Dialogfeld „Schlüsseleigenschaften“ (Registerkarte „Rücknahmeschlüssel“)

Auf der Registerkarte „Rücknahmeschlüssel“ werden alle Schlüssel aufgeführt, mit denen Sie Ihren PGP-Schlüssel zurücknehmen können. Weitere Anweisungen zum Hinzufügen eines Rücknahmeschlüssels zu Ihrem Schlüssel finden Sie im Abschnitt „So legen Sie einen zugeordneten Rücknahmeschlüssel fest“ auf Seite 37.

Ein Standardschlüsselpaar festlegen

Beim Verschlüsseln von Nachrichten oder Dateien gibt Ihnen PGP die Option, zusätzlich mit einem von Ihnen als Standard definierten Schlüsselpaar zu verschlüsseln. Dieses Standardschlüsselpaar wird dann standardmäßig von PGP verwendet, wenn Sie eine Nachricht oder den öffentlichen Schlüssel eines anderen Benutzers unterschreiben. Ihr Standardschlüsselpaar wird zur Unterscheidung von anderen Schlüsseln in Fettdruck angezeigt. Wenn sich nur ein Schlüsselpaar auf Ihrem Schlüsselring befindet, wird dieses automatisch zum Standardschlüsselpaar. Wenn Sie über mehrere Schlüsselpaare verfügen, sollten Sie selbst ein Standardschlüsselpaar festlegen.

So legen Sie ein Standardschlüsselpaar fest

1. Öffnen Sie PGPkeys.
2. Markieren Sie das Schlüsselpaar, das als Standardschlüssel festgelegt werden soll.
3. Wählen Sie im Menü **Schlüssel** die Option **Als Standard festlegen**.

   Das ausgewählte Schlüsselpaar wird daraufhin in Fettdruck angezeigt. Dadurch wird angegeben, daß diese Schlüssel als Standardschlüssel festgelegt wurden.

Öffentliche Schlüssel anderer Benutzer verifizieren

In der Vergangenheit war es schwierig, mit Sicherheit festzustellen, ob ein Schlüssel einer bestimmten Person gehörte, wenn diese Person Ihnen ihren Schlüssel nicht persönlich auf einer Diskette übergab. Diese Art des Austausches von Schlüsseln ist in der Regel etwas unpraktisch, insbesondere für Benutzer, deren Wohn- bzw. Arbeitsorte weit auseinanderliegen.

Es gibt verschiedene Möglichkeiten zur Überprüfung des Fingerabdrucks eines Schlüssels. Die sicherste Art ist ein direkter Anruf bei der entsprechenden Person, damit der Fingerabdruck telefonisch durchgegeben werden kann. Sofern diese Person nicht das Ziel eines Angriffs ist, ist es sehr unwahrscheinlich, daß jemand diesen zufälligen Anruf abfangen und sich für die Person

ausgeben könnte, die Sie anrufen möchten. Sie können außerdem den Fingerabdruck Ihrer Kopie des öffentlichen Schlüssels einer Person mit dem Fingerabdruck des Originalschlüssels dieser Person, der sich auf einem öffentlichen Schlüssel-Server befindet, vergleichen.

Der Fingerabdruck kann auf zwei Weisen angezeigt werden: in einer eindeutigen Wörterliste oder in Hexadezimalform.

So überprüfen Sie einen öffentlichen Schlüssel mit seinem digitalen Fingerabdruck

1. Öffnen Sie PGPkeys.
2. Markieren Sie den öffentlichen Schlüssel, den Sie überprüfen möchten.
3. Wählen Sie im Menü **Schlüssel** die Option **Schlüsseleigenschaften**, oder klicken Sie auf  , um das Dialogfeld **Schlüsseleigenschaften** zu öffnen.

   Das Dialogfeld **Schlüsseleigenschaften** wird geöffnet (siehe Abbildung 6-5).

Abbildung 6-5. Dialogfeld für Schlüsseleigenschaften

4. Vergleichen Sie die im Textfeld **Fingerabdruck** angezeigte Folge von Wörtern oder Zeichen mit denen des Originalabdrucks.

Standardmäßig wird im Textfeld **Fingerabdruck** eine Wörterliste angezeigt (siehe Abbildung 6-6). Sie können jedoch das Kontrollkästchen **Hexadezimal** aktivieren, um den Fingerabdruck in Form von 20 Hexadezimalzeichen anzuzeigen (siehe Abbildung 6-6).

Wörterlistenansicht Hexadezimalansicht

Abbildung 6-6. Textfeld „Fingerabdruck“

Die im Textfeld „Fingerabdruck“ enthaltene Wörterliste besteht aus speziellen von PGP verwendeten Wörtern zur Authentisierung, die sorgfältig ausgewählt wurden und phonetisch eindeutig und leicht verständlich sind.

Die Wörterliste hat denselben Zweck wie das Militäralphabet, mit dem Piloten Informationen deutlich über einen rauschenden Funksprechkanal übertragen können. Weitere Informationen zum Wort-Hash-Verfahren und die Wörterliste erhalten Sie unter Anhang D, „Liste biometrischer Worte“.

Öffentliche Schlüssel anderer Benutzer unterschreiben

Wenn Sie einen Schlüsselsatz erstellen, werden die Schlüssel automatisch mit Ihrem öffentlichen Schlüssel unterschrieben. Auf ähnliche Weise können Sie, wenn Sie sicher sind, daß ein Schlüssel zu einer bestimmten Person gehört, den öffentlichen Schlüssel dieser Person unterschreiben. Damit geben Sie an, daß Sie sicher sind, daß es sich um einen gültigen Schlüssel handelt. Wenn Sie den öffentlichen Schlüssel eines anderen Benutzers unterschreiben, wird zu diesem Schlüssel ein Symbol mit Ihrem Benutzernamen angezeigt.

So unterschreiben Sie öffentliche Schlüssel anderer Benutzer

1. Öffnen Sie das PGPkeys-Fenster.
2. Markieren Sie den öffentlichen Schlüssel, den Sie unterschreiben möchten.
3. Wählen Sie im Menü **Schlüssel** die Option **Unterschreiben**, oder klicken Sie auf  , um das Dialogfeld **Schlüssel unterschreiben** zu öffnen.

   Das Dialogfeld **PGP-Schlüssel unterschreiben** wird angezeigt (Abbildung 6-7), in dessen Textfeld der öffentliche Schlüssel und der Fingerabdruck angezeigt werden.

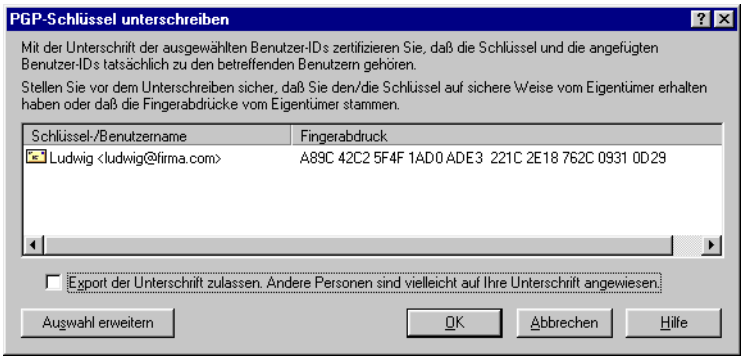


Abbildung 6-7. Dialogfeld „PGP-Schlüssel unterschreiben“ („Auswahl einschränken“)

4. Aktivieren Sie das Kontrollkästchen **Export der Unterschrift zulassen**, damit Ihre Unterschrift zusammen mit diesem Schlüssel exportiert werden kann.

   Eine exportierbare Unterschrift kann an Server gesendet werden und wird stets mit dem Schlüssel weitergegeben, wenn dieser exportiert wird, beispielsweise durch Ziehen in eine E-Mail-Nachricht. Mit diesem Kontrollkästchen können Sie auf einfache Art angeben, daß Ihre Unterschrift exportiert werden soll.

   – ODER –

Wenn Sie weitere Optionen, wie den Unterschriftstyp und die Gültigkeitsdauer der Unterschrift, konfigurieren möchten, klicken Sie auf die Schaltfläche **Auswahl erweitern** (Abbildung 6-8).

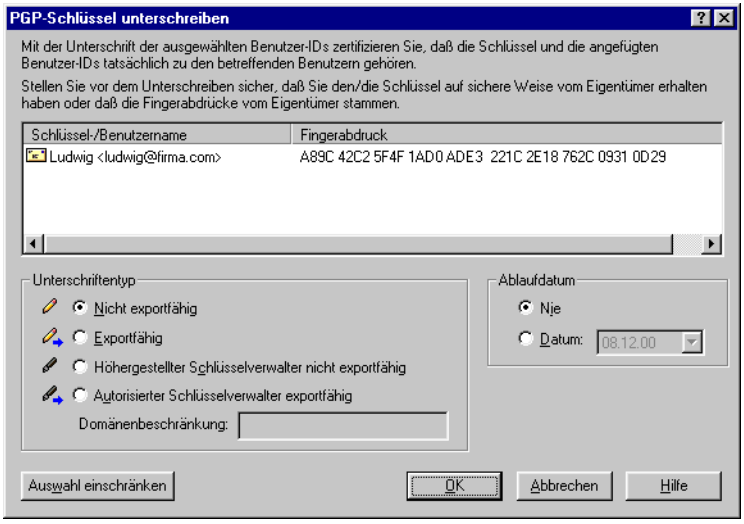


Abbildung 6-8. Dialogfeld „PGP-Schlüssel unterschreiben“ („Auswahl erweitern“)

Wählen Sie den Unterschriftstyp, mit dem öffentliche Schlüssel unterzeichnet werden sollen: Sie haben folgende Optionen:

- **Nicht exportfähig.** Verwenden Sie diese Unterschrift, wenn Sie überzeugt sind, daß der Schlüssel echt ist, aber nicht möchten, daß sich andere auf Ihre Einschätzung verlassen. Dieser Unterschriftstyp kann nicht mit dem dazugehörigen Schlüssel an einen Schlüssel-Server gesendet oder auf andere Art exportiert werden.
- **Exportfähig.** Verwenden Sie exportfähige Unterschriften dann, wenn Ihre Unterschrift mit dem Schlüssel an den Schlüssel-Server gesendet werden soll und sich andere Benutzer auf Ihre Unterschrift verlassen und infolgedessen den von Ihnen unterschriebenen Schlüsseln vertrauen sollen. Dieses Vorgehen entspricht dem Aktivieren des Kontrollkästchens **Export der Unterschrift zulassen** im Menü **PGP-Schlüssel unterschreiben**.

- **Höhergestellter Schlüsselverwalter nicht exportfähig.** Bestätigt, daß dieser Schlüssel sowie alle mit diesem Schlüssel mit einer Bestätigung als autorisierter Schlüsselverwalter unterschriebenen Schlüssel von Ihnen als vollständig autorisierter Schlüsselverwalter akzeptiert wurden. Dieser Unterschriftstyp ist nicht exportfähig.
- **Autorisierter Schlüsselverwalter exportfähig.** Verwenden Sie diese Unterschrift, um die Gültigkeit eines Schlüssels zu zertifizieren und anzugeben, daß dem Schlüsseleigentümer vollständiges Vertrauen entgegengebracht werden sollte, wenn er sich für andere Schlüssel verbürgt. Dieser Unterschriftstyp kann exportiert werden. Die Befugnisse zur Schlüsselüberprüfung eines autorisierten Schlüsselverwalters können auf eine bestimmte E-Mail-Domäne beschränkt werden.

5. Wenn Sie die Befugnisse eines autorisierten Schlüsselverwalters zur Überprüfung von Zertifikaten auf eine Einzeldomäne beschränken möchten, geben Sie den Domänennamen in das Textfeld „Domäne“ ein.
6. Wenn Sie dieser Unterschrift ein Gültigkeitsdatum zuordnen möchten, geben Sie das Datum, an dem diese Unterschrift ablaufen soll, in das Textfeld „Datum“ ein. Andernfalls läuft die Unterschrift nie ab.
7. Klicken Sie auf **OK**.

   Das Dialogfeld zur Eingabe der **Paßphrase** wird angezeigt.
8. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **OK**.

   Dem gerade von Ihnen unterschriebenen Schlüssel wird ein mit Ihrem Benutzernamen verknüpftes Symbol hinzugefügt.

Vertrauen für Schlüsselüberprüfungen aussprechen

Neben der Zertifizierung, daß ein Schlüssel zu einer bestimmten Person gehört, können Sie den Schlüsseleigentümern auch ein bestimmtes Maß an Vertrauen aussprechen. Sie drücken damit aus, in welchem Maße Sie diesen Personen vertrauen, die Gültigkeit von Schlüsseln anderer Personen als Schlüsselverwalter zu gewährleisten. Wenn Sie also einen Schlüssel erhalten, der von einer Person unterschrieben wurde, der Sie Vertrauen ausgesprochen haben, wird dieser Schlüssel als echt betrachtet werden, obwohl Sie den Schlüssel nicht selbst überprüft haben.

So sprechen Sie Ihr Vertrauen für einen Schlüssel aus

1. Öffnen Sie PGPkeys.
2. Markieren Sie den Schlüssel, dessen Vertrauensebene Sie ändern möchten.

   HINWEIS: Bevor Sie die Vertrauensebene für einen Schlüssel ändern können, müssen Sie ihn zuerst unterschreiben. Wenn Sie den Schlüssel noch nicht unterschrieben haben, finden Sie Anweisungen dazu im Abschnitt „Öffentliche Schlüssel überprüfen“ auf Seite 64.

3. Wählen Sie im Menü **Schlüssel** die Option **Schlüsseleigenschaften**, oder klicken Sie auf  , um das Dialogfeld **Schlüsseleigenschaften** zu öffnen (siehe Abbildung 6-5).
4. Stellen Sie den gewünschten Vertrauensgrad für das Schlüsselpaar mit dem Schieberegler ein.

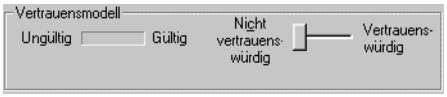


Abbildung 6-9. Dialogfeld „Vertrauensmodell“

5. Schließen Sie das Dialogfeld, damit die neue Einstellung übernommen wird.

Wenn Sie einem Schlüssel mit Foto eine hohe Vertrauensstufe zuordnen, entfernt PGP das rote Fragezeichen von der Fotografie.

Schlüssel aktivieren und deaktivieren

Gelegentlich müssen Schlüssel zeitweilig deaktiviert werden. Diese Funktion ist nützlich, wenn Sie einen öffentlichen Schlüssel zum späteren Gebrauch behalten möchten, der Eigentümer jedoch nicht bei jedem Senden einer E-Mail-Nachricht in der Empfängerliste aufgeführt werden soll.

So deaktivieren Sie einen Schlüssel

1. Öffnen Sie PGPkeys.
2. Wählen Sie den Schlüssel, den Sie deaktivieren möchten.

3. Wählen Sie im Menü **Schlüssel** die Option **Deaktivieren**.

   Der Schlüssel wird grau unterlegt angezeigt und ist vorübergehend nicht verfügbar.

So aktivieren Sie einen Schlüssel

1. Öffnen Sie PGPkeys.
2. Wählen Sie den Schlüssel, den Sie aktivieren möchten.
3. Wählen Sie im Menü **Schlüssel** die Option **Aktivieren**.

   Der Schlüssel wird nicht mehr grau unterlegt angezeigt und kann wieder verwendet werden.

Schlüssel importieren und exportieren

Die öffentlichen Schlüssel können in der Regel gesendet und empfangen werden, indem der zugrundeliegende Text von einem öffentlichen oder unternehmenseigenen Schlüssel-Server kopiert wird. Schlüssel können aber auch ausgetauscht werden, indem sie als separate Textdateien im- und exportiert werden. So kann ein anderer Benutzer Ihnen eine Diskette mit seinem öffentlichen Schlüssel aushändigen, oder Sie können Ihren öffentlichen Schlüssel über einen FTP-Server zur Verfügung stellen.

So importieren Sie Schlüssel aus Dateien

1. Öffnen Sie PGPkeys.
2. Wählen Sie im Menü **Schlüssel**die Option **Importieren**.

   Das Dialogfeld **Importieren** wird angezeigt.
3. Wählen Sie die Datei aus, die den zu importierenden Schlüssel enthält, und klicken Sie auf **Öffnen**.

   Das Dialogfeld zur **Auswahl des zu importierenden Schlüssels** wird angezeigt.
4. Markieren Sie die in Ihren Schlüsselbund zu importierenden Schlüssel, und klicken Sie auf die Schaltfläche **Importieren**.
5. Importierte Schlüssel werden in PGPkeys angezeigt, wo sie zum Verschlüsseln von Daten und zum Verifizieren von digitalen Unterschriften verwendet werden können.

So entnehmen Sie einen öffentlichen Schlüssel aus einer E-Mail-Nachricht

Wenn Ihnen jemand eine E-Mail-Nachricht mit seinem Schlüssel als Textblock sendet, können Sie diesen Schlüssel Ihrem Schlüsselbund hinzufügen.

1. Öffnen Sie PGPkeys, während das Fenster der betreffenden E-Mail-Nachricht geöffnet ist.
2. Ordnen Sie die beiden Fenster so an, daß Sie PGPkeys hinter dem Fenster mit der E-Mail-Nachricht sehen können.
3. Markieren Sie den Schlüsseltext, einschließlich des Textes `BEGIN PGP PUBLIC KEY BLOCK` und `END PGP PUBLIC KEY BLOCK`, und ziehen Sie den Text auf das PGPkeys-Fenster.

   Das Dialogfeld zur **Auswahl des zu importierenden Schlüssels** wird angezeigt.
4. Markieren Sie die in Ihren Schlüsselbund zu importierenden Schlüssel, und klicken Sie auf die Schaltfläche **Importieren**.
5. Importierte Schlüssel werden in PGPkeys angezeigt, wo sie zum Verschlüsseln von Daten und zum Verifizieren von digitalen Unterschriften verwendet werden können.

So exportieren Sie Schlüssel in Dateien

1. Öffnen Sie das PGPkeys-Fenster.
2. Wählen Sie den Schlüssel aus, den Sie in eine Datei exportieren möchten.
3. Wählen Sie im Menü **Schlüssel**die Option **Exportieren**.

   Das **Export**-Dialogfeld wird angezeigt.
4. Geben Sie den Namen der Datei an bzw. suchen Sie die Datei, in die der Schlüssel exportiert werden soll, und klicken Sie auf **Speichern**.

   Der exportierte Schlüssel wird in der Datei in dem angegebenen Ordner gespeichert.

Ihre privaten Schlüssel vom Typ PKCS-12 X.509 können Sie auch mit Hilfe Ihres Browsers durch Ziehen exportieren und in PGPkeys einfügen, oder Sie wählen **Importieren** im Menü **Schlüssel**.

Schlüssel zurücknehmen

Sollte der Fall eintreten, daß Ihr persönliches Schlüsselpaar nicht mehr sicher ist, können Sie mit Hilfe einer Zurücknahme veranlassen, daß Ihr öffentlicher Schlüssel nicht mehr benutzt wird. Ein zurückgenommener Schlüssel läßt sich am besten in Umlauf bringen, indem er auf einem öffentlichen Schlüssel-Server abgelegt wird.

So nehmen Sie einen Schlüssel zurück

1. Öffnen Sie PGPkeys.
2. Markieren Sie das zurückzunehmende Schlüsselpaar.
3. Wählen Sie im Menü **Schlüssel**die Option **Zurücknehmen**.

   Ein Dialogfeld zur **Bestätigung der Zurücknahme** wird angezeigt.
4. Klicken Sie auf **OK**, um die Zurücknahme des ausgewählten Schlüssels zu bestätigen.

   Das Dialogfeld **PGP-Paßphrase eingeben** wird angezeigt.
5. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **O**K.

   Ein zurückgenommener Schlüssel wird mit einer roten Linie durchgestrichen angezeigt, wodurch die Ungültigkeit des Schlüssels gekennzeichnet wird.
6. Senden Sie den zurückgenommenen Schlüssel an den Server, so daß alle anderen PGP-Benutzer wissen, daß Sie Ihren alten Schlüssel nicht mehr verwenden sollen.

Zugeordneten Rücknahmeschlüssel festlegen

Unter Umständen geht Ihre Paßphrase irgendwann verloren, oder Sie verlieren Ihren privaten Schlüssel. In diesem Fall können Sie Ihren Schlüssel nicht mehr verwenden und Ihren alten Schlüssel auch nicht zurücknehmen, wenn Sie einen neuen erstellen. Um sich gegen diesen Fall abzusichern, können Sie an Ihrem öffentlichen Schlüsselbund für die Zurücknahme Ihres Schlüssels einen Rücknahmeschlüssel bestimmen. Der Halter dieses anderen Schlüssels kann dann so wie Sie selbst zuvor Ihren DH / DSS-Schlüssel zurücknehmen und an den Server senden.

So legen Sie einen zugeordneten Rücknahmeschlüssel fest

1. Öffnen Sie PGPkeys.
2. Markieren Sie das Schlüsselpaar, dem Sie einen Rücknahmeschlüssel zuordnen möchten.
3. Wählen Sie im Menü **Schlüssel** die Option **Hinzufügen/Rücknahmeschlüssel**.

   Das angezeigte Dialogfeld enthält eine Liste mit Schlüsseln.
4. Wählen Sie in der Benutzer-ID-Liste die Schlüssel, die zugeordnete Rücknahmeschlüssel sein sollen.
5. Klicken Sie auf **OK**.

   Ein Dialogfeld zur Bestätigung des Vorgangs wird angezeigt.
6. Klicken Sie auf **OK**, um fortzufahren.

   Das Dialogfeld zur Eingabe der **Paßphrase** wird angezeigt.
7. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **O**K.
8. Die gewählten Schlüssel sind jetzt autorisierte Rücknahmeschlüssel. Zur Optimierung der Schlüsselverwaltung sollten Sie eine aktuelle Kopie Ihres Schlüssels an die Eigentümer der Rücknahmeschlüssel verteilen oder den Schlüssel auf den Server laden. Anweisungen dazu finden Sie im Abschnitt „Ihren öffentlichen Schlüssel verteilen“ auf Seite 53.

PGP-Optionen festlegen

Obwohl PGP bereits auf die Bedürfnisse der meisten Benutzer ausgelegt ist, haben Sie die Möglichkeit, einige Einstellungen auf die Anforderungen Ihrer persönlichen Computerumgebung abzustimmen. Sie können diese Einstellungen im Dialogfeld **Optionen** vornehmen, das Sie über den Befehl **Optionen** im Menü **Bearbeiten** von PGPkeys aufrufen können.

Allgemeine Optionen festlegen

Verwenden Sie die Registerkarte „Allgemein“, um Ihre Voreinstellung für das Verschlüsseln, Unterschreiben und Löschen von Dateien festzulegen.

So legen Sie allgemeine PGP-Optionen fest

1. Öffnen Sie PGPkeys.
2. Wählen Sie im Menü **Bearbeiten** von PGPkeys den Befehl **Optionen**.

   Die Registerkarte **Allgemein** des Dialogfelds **Optionen** wird angezeigt (Abbildung 6-10).

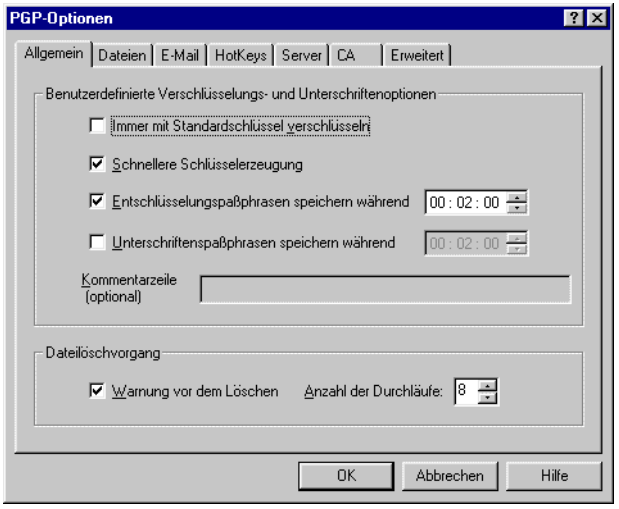


Abbildung 6-10. Dialogfeld „PGP-Optionen“ (Registerkarte „Allgemein“)

3. Legen Sie auf dieser Registerkarte die allgemeinen Verschlüsselungseinstellungen fest. Sie haben folgende Optionen:

   - **Immer mit Standardschlüssel verschlüsseln.** Wenn dieses Kontrollkästchen aktiviert ist, werden alle E-Mail-Nachrichten und Dateien, die Sie mit einem öffentlichen Empfängerschlüssel verschlüsseln, auch für Sie mit Ihrem öffentlichen Standardschlüssel verschlüsselt. Sie sollten diese Einstellung aktiviert lassen, damit Sie den Inhalt jeder E-Mail-Nachricht oder Datei, die Sie zuvor verschlüsselt haben, entschlüsseln können.

   - **Schnellere Schlüsselerzeugung.** Wenn dieses Kontrollkästchen aktiviert ist, wird weniger Zeit zum Erzeugen eines neuen Diffie-Hellman / DSS-Schlüsselpaares benötigt. Dieser Prozeß wird beschleunigt, indem die Schlüssel mit Hilfe eines zuvor berechneten Primzahlsatzes erstellt werden und die zeitaufwendige Primzahlberechnung bei der Schlüsselerstellung somit übersprungen wird. Schnellere Schlüsselerzeugung ist jedoch nur bei der Schlüsselerzeugung mit festen Schlüsselgrößen zwischen 1024 und 4096 Bit möglich und nicht bei benutzerdefinierten Schlüsselgrößen. Obwohl es für andere Personen nahezu unmöglich ist, Ihren Schlüssel mit Hilfe des zuvor berechneten Primzahlsatzes zu decodieren, sollten Sie zusätzlich ein Schlüsselpaar mit maximalen Sicherheitsvorkehrungen erstellen.

     In der Verschlüsselungstechnik wird im allgemeinen davon ausgegangen, daß die Verwendung solcher vorgefertigter Primzahlsätze für Diffie-Hellman / DSS-Algorithmen keinen Verlust an Sicherheit mit sich bringt. Wenn Sie mit dieser Funktion nicht arbeiten möchten, deaktivieren Sie sie.

   - **Entschlüsselungspaßphrasen speichern um [ ].** Wenn dieses Kontrollkästchen aktiviert ist, wird Ihre Entschlüsselungspaßphrase automatisch vom Computer gespeichert. Legen Sie die Häufigkeit fest (im Format Stunden : Minuten : Sekunden), mit der Ihre Paßphrase gespeichert werden soll. Der Standardwert beträgt 2 Minuten.

- **Unterzeichnerpaßphrasen speichern um [ ].** Wenn dieses Kontrollkästchen aktiviert ist, wird Ihre Unterzeichnerpaßphrase automatisch vom Computer gespeichert. Legen Sie die Häufigkeit fest (im Format Stunden : Minuten : Sekunden), mit der Ihre Unterzeichnerpaßphrase gespeichert werden soll. Der Standardwert beträgt 2 Minuten.

- **Kommentarzeile.** In diesem Bereich können Sie Kommentare schreiben. Der hier eingegebene Text wird dann immer in Nachrichten und Dateien eingefügt, die Sie verschlüsseln oder unterschreiben. Der Text wird unter dem Kopf BEGIN PGP MESSAGE BLOCK und der PGP-Versionsnummer jeder Nachricht angezeigt.

- **Warnung vor dem Löschen.** Wenn diese Einstellung aktiviert ist, wird vor dem unwiederherstellbaren Löschen einer Datei ein Dialogfeld angezeigt, um Ihnen noch eine letzte Möglichkeit zu geben, den Vorgang abzubrechen, bevor PGP den Inhalt der Datei überschreibt und sie von Ihrer Festplatte löscht.

- **Anzahl der Durchläufe.** Mit dieser Einstellung wird gesteuert, wie oft die Programme zum Löschen auf der Festplatte angewandt werden.

4. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zum PGPkeys-Menü zurückzukehren, oder wählen Sie eine andere Registerkarte zur Konfiguration weiterer PGP-Voreinstellungen.

Dateioptionen festlegen

Verwenden Sie die Registerkarte **Dateien**, um den Pfad der Schlüsselbunddateien anzugeben, in denen Ihre privaten und öffentlichen Schlüssel gespeichert sind.

So legen Sie die PGP-Dateioptionen fest

1. Öffnen Sie PGPkeys.
2. Wählen Sie im Menü **Bearbeiten** von PGPkeys den Befehl **Optionen**, und klicken Sie dann auf die Registerkarte **Dateien**.

   Die Registerkarte **Dateien** des Dialogfelds **Optionen** wird angezeigt (Abbildung 6-11).

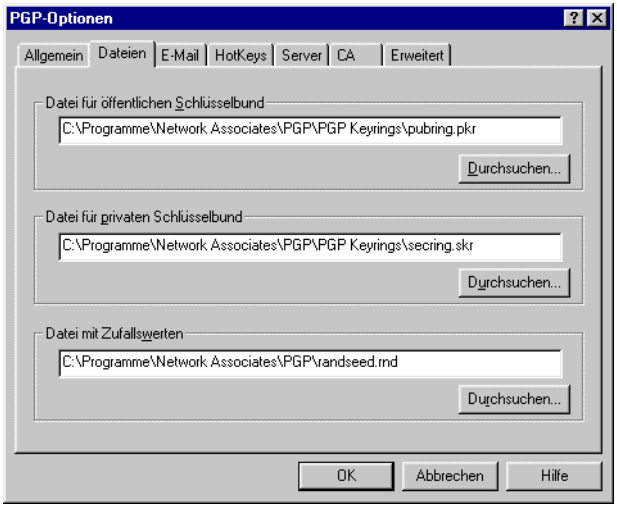


Abbildung 6-11. Dialogfeld „PGP-Optionen“ (Registerkarte „Dateien“)

3. Mit den auf der Registerkarte **Dateien** befindlichen Schaltflächen können Sie das Verzeichnis für Ihre öffentlichen und privaten Schlüsselbunde sowie für die Datei mit Zufallswerten angeben:

   - **Datei mit öffentlichem Schlüsselbund.** In diesem Feld werden der Name der Datei und der Speicherort angezeigt, an dem PGP Ihre öffentliche Schlüsselbunddatei vermutet. Wenn Sie Ihre öffentlichen Schlüssel in einer Datei mit einem anderen Namen oder an einem anderen Ort speichern möchten, geben Sie diese Informationen hier an. In dem von Ihnen angegebenen Verzeichnis werden auch alle automatisch erstellten Sicherheitskopien des öffentlichen Schlüsselbundes gespeichert.

   - **Datei mit privatem Schlüsselbund.** In diesem Feld werden der Name der Datei und der Speicherort angezeigt, an dem PGP Ihre private Schlüsselbunddatei vermutet. Wenn Sie Ihre privaten Schlüssel in einer Datei mit einem anderen Namen oder an einem anderen Ort speichern möchten, geben Sie diese Informationen hier an. Einige Benutzer bewahren Ihren privaten Schlüsselbund auf einer Diskette auf, die sie wie einen Schlüssel einlegen, wenn sie eine E-Mail-Nachricht unterzeichnen oder entschlüsseln müssen. In dem von Ihnen angegebenen Verzeichnis werden auch alle automatisch erstellten Sicherheitskopien des öffentlichen Schlüsselbundes gespeichert.

   - **Speicherort mit Zufallswerten festlegen.** Gibt den Speicherort der Datei mit Zufallswerten an. Aus Sicherheitsgründen speichern einige Benutzer ihre Datei mit Zufallswerten in einem sicheren Pfad. Da ein unbefugter Zugriff auf diese Datei sehr schwierig ist und PGP dagegen schon Vorkehrungen getroffen hat, hat das Verschieben der Datei aus dem Standardverzeichnis nur begrenzten Wert.

4. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zum PGPkeys-Menü zurückzukehren, oder wählen Sie eine andere Registerkarte zur Konfiguration weiterer PGP-Voreinstellungen.

E-Mail-Optionen festlegen

Auf der Registerkarte **E-Mail** können Sie die Optionen festlegen, mit denen die Art der Implementierung der PGP-Funktionen für Ihre spezielle E-Mail-Anwendung bestimmt wird. Unter Umständen lassen sich nicht alle der hier vorgenommenen Einstellungen in Ihrer E-Mail-Anwendung umsetzen.

So legen Sie E-Mail-Optionen fest

1. Öffnen Sie PGPkeys.
2. Wählen Sie im Menü **Bearbeiten** von PGPkeys den Befehl **Optionen**, und klicken Sie dann auf die Registerkarte **E-Mail**.

   Die Registerkarte **E-Mail** des Dialogfelds **Optionen** wird angezeigt (Abbildung 6-12).

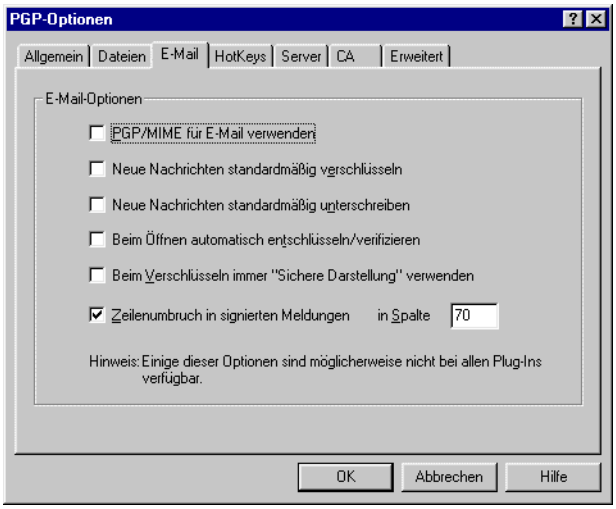


Abbildung 6-12. Dialogfeld „PGP-Optionen“ (Registerkarte „E-Mail“)

3. Stellen Sie auf dieser Registerkarte die Optionen für die **E-Mail**-Verschlüsselung ein. Sie haben folgende Optionen:

   - **PGP/MIME für E-Mail verwenden.** Wenn Sie Eudora verwenden und diese Einstellung aktivieren, werden alle E-Mail-Nachrichten und Dateianhänge automatisch für den gewünschten Empfänger verschlüsselt. Diese Einstellung wirkt sich nicht auf andere Verschlüsselungen aus, die Sie über die Zwischenablage oder mit dem Windows-Explorer durchführen. Sie sollte nicht verwendet wer-

den, wenn Sie E-Mails an Empfänger senden möchten, deren E-Mail-Anwendungen den PGP/MIME-Standard nicht unterstützen. In Eudora werden Dateianhänge unabhängig von dieser Einstellung stets verschlüsselt. Wenn der Empfänger jedoch nicht über PGP/MIME verfügt, muß die Entschlüsselung manuell erfolgen.

- **Neue Nachrichten standardmäßig verschlüsseln.** Wenn Sie diese Einstellung aktivieren, werden alle E-Mail-Nachrichten und Dateianhänge automatisch verschlüsselt. Von einigen E-Mail-Anwendungen wird diese Funktion nicht unterstützt.

- **Neue Nachrichten standardmäßig unterschreiben.** Wenn Sie diese Einstellung aktivieren, werden alle E-Mail-Nachrichten und Dateianhänge automatisch unterschrieben. Von einigen E-Mail-Anwendungen wird diese Funktion nicht unterstützt. Diese Einstellung hat keine Auswirkung auf andere Unterschriften, die Sie mit Hilfe der Zwischenablage oder des Windows-Explorers hinzufügen.

- **Beim Öffnen automatisch entschlüsseln/verifizieren.** Wenn Sie diese Einstellung aktivieren, werden alle verschlüsselten und/oder unterschriebenen E-Mail-Nachrichten und Dateianhänge automatisch entschlüsselt und verifiziert. Von einigen E-Mail-Anwendungen wird diese Funktion nicht unterstützt.

- **Beim Verschlüsseln immer „Sichere Darstellung“ verwenden.** Wenn Sie diese Einstellung aktivieren, werden all Ihre entschlüsselten E-Mail-Nachrichten im Fenster „Sichere Darstellung“ in einer speziellen Schriftart zur Verhütung von TEMPEST-Angriffen angezeigt. Weitere Informationen zu TEMPEST-Angriffen finden Sie im Abschnitt „Sicherheitsrisiken“ auf Seite 263.

- **Zeilenumbruch in signierten Meldungen in Spalte [ ].** Mit dieser Einstellung wird die Spaltennummer festgelegt, an der der Text in der digitalen Unterschrift durch eine Absatzmarke umgebrochen wird. Diese Funktion ist erforderlich, da Zeilenumbrüche nicht bei allen Anwendungen auf die gleiche Weise vorgenommen werden, wodurch die Zeilen in Ihren digital unterschriebenen Nachrichten eventuell so umgebrochen werden, daß sie schwer lesbar sind. Bei der Standardeinstellung von 70 wird dieses Problem bei den meisten Anwendungen vermieden.

. **WARNUNG:** Wenn Sie die Zeilenumbruch-Einstellung in PGP ändern, müssen Sie einen Wert wählen, der unter dem in Ihrer E-Mail-Anwendung eingestellten Wert liegt. Wenn der Wert gleich oder größer dem Wert Ihrer E-Mail-Anwendung ist, werden möglicherweise Zeilenumbrüche eingefügt, die Ihre PGP-Unterschrift ungültig machen.

---

4. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zum PGPkeys-Menü zurückzukehren, oder wählen Sie eine andere Registerkarte zur Konfiguration weiterer PGP-Voreinstellungen.

HotKey-Einstellungen festlegen

Verwenden Sie die Registerkarte **HotKeys,** um Tastenkombinationen für PGP-Funktionen festzulegen.

So legen Sie HotKey-Einstellungen fest

1. Öffnen Sie PGPkeys.
2. Wählen Sie im Menü **Bearbeiten** von PGPkeys den Befehl **Optionen**, und klicken Sie dann auf die Registerkarte **HotKeys**.

   Die Registerkarte **HotKeys** des Dialogfelds **Optionen** wird angezeigt (Abbildung 6-13).

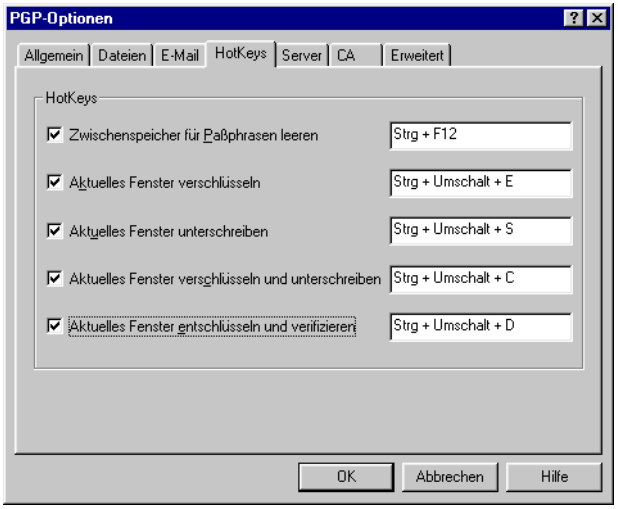


Abbildung 6-13. Dialogfeld „PGP-Optionen“ (Registerkarte „HotKeys“)

3. Wählen Sie die HotKey-Optionen, die Sie von der Registerkarte **HotKey** aus verwenden möchten. Sie haben folgende Optionen:

   - **Zwischenspeicher für Paßphrasen leeren.** Wählen Sie diese Option, um einen HotKey zu erstellen, mit dem Sie den Cache-Speicher, der Ihre PGP-Entschlüsselungspaßphrase enthält, durch Betätigung einer oder mehrerer Tasten löschen können. Der Standard-HotKey für diese Funktion lautet STRG+F12.

   - **Aktuelles Fenster verschlüsseln.** Wählen Sie diese Option, um einen HotKey zu erstellen, mit dem Sie alle im aktuellen Fenster enthaltenen Daten durch Betätigung einer oder mehrerer Tasten verschlüsseln können. Die Standard-Tastenkombination für diese Funktion lautet STRG+UMSCHALT+E.

   - **Aktuelles Fenster unterschreiben.** Wählen Sie diese Option, um einen HotKey zu erstellen, mit dem Sie alle im aktuellen Fenster enthaltenen Daten durch Betätigung einer oder mehrerer Tasten unterschreiben können. Der Standard-HotKey für diese Funktion lautet STRG+UMSCHALT+S.

   - **Aktuelles Fenster verschlüsseln und unterschreiben.** Wählen Sie diese Option, um einen HotKey zu erstellen, mit dem Sie die im aktuellen Fenster enthaltenen Daten durch Betätigung einer oder mehrerer Tasten verschlüsseln und unterschreiben können. Der Standard-HotKey für diese Funktion lautet STRG+UMSCHALT+C.

   - **Aktuelles Fenster entschlüsseln und verifizieren** Wählen Sie diese Option, um einen HotKey zu erstellen, mit dem Sie die im aktuellen Fenster enthaltenen geschützten Daten durch Betätigung einer oder mehrerer Tasten entschlüsseln und verifizieren können. Die Standard-Tastenkombination für diese Funktion lautet STRG+UMSCHALT+D.

4. Klicken Sie auf **OK** oder wählen Sie eine Registerkarte mit anderen **Optionen**, um mit dem Konfigurieren von PGP fortzufahren.

Server-Optionen festlegen

Auf der Registerkarte **Server** können Sie Einstellungen für die öffentlichen Schlüssel-Server festlegen, die Sie zum Senden und Abrufen öffentlicher Schlüssel und zum automatischen Synchronisieren von Schlüsseln verwenden.

So legen Sie Schlüssel-Server-Optionen fest

1. Öffnen Sie PGPkeys.
2. Wählen Sie im Menü **Bearbeiten** von PGPkeys den Befehl **Optionen**, und klicken Sie dann auf die Registerkarte **Server**.
3. Die Registerkarte **Server** des Dialogfelds **Optionen** wird angezeigt (Abbildung 6-14).

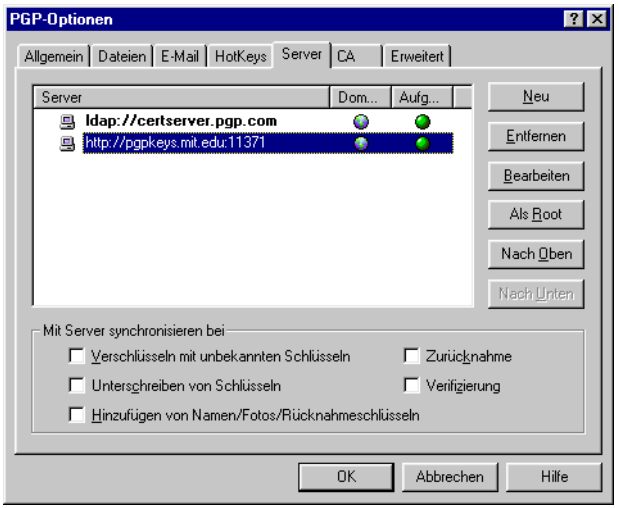


Abbildung 6-14. Dialogfeld „PGP-Optionen“ (Registerkarte „Server“)

In der Spalte **Domäne** werden die Internet-Domänen (z. B. „firma.com“) der verfügbaren Schlüssel-Server aufgelistet. PGP versucht beim Senden von Schlüsseln an einen Server, die Domäne des betreffenden Schlüssels in der Liste und dadurch den richtigen Server-Eintrag zu finden.
Wird die Domäne nicht gefunden, wird der Server für den ersten globalen Domänen-Server verwendet, der für alle Schlüssel zuständig ist.
Wenn diese erste Suche keinen Erfolg zeigt, kann auf weiteren globalen Domänen-Servern in der Liste gesucht werden.

4. Zum Einstellen der Server-Optionen verwenden Sie die folgenden Schaltflächen:

   - **Neu.** Fügt einen neuen Server zu Ihrer Liste hinzu.
   - **Entfernen.** Entfernt den gegenwärtig gewählten Server aus der Liste.
   - **Bearbeiten.** Ermöglicht das Bearbeiten der Server-Informationen für den ausgewählten Server.
   - **Als Root.** Kennzeichnet den Root-Server, der für bestimmte firmeninterne Operationen (z. B. Aktualisieren und Senden von Gruppenlisten, Aktualisieren von Schlüsselverwaltern etc.) benötigt wird. In einer Firmenumgebung ist diese Option bereits von Ihrem Sicherheitsbeauftragten konfiguriert worden.
   - **Nach Oben**und **Nach Unten.** Verwenden Sie diese Schaltflächen, um die Server nach Belieben anzuordnen.

5. Im Feld **Mit Server synchronisieren bei** wählen Sie die bei der Synchronisierung Ihres privaten Schlüsselbundes mit dem Schlüssel-Server zu verwendenden Optionen. Sie haben folgende Optionen:

   - **Mit unbekannten Schlüsseln verschlüsseln.** Wenn Sie diese Option wählen, sucht PGP automatisch auf dem Server nach unbekannten Empfängern, um Benutzer zu finden, die sich nicht an Ihrem Schlüsselbund befinden, wenn eine E-Mail-Nachricht verschlüsselt wird.
   - **Unterzeichnerschlüssel.** Wenn Sie diese Option wählen, werden Schlüssel, denen Sie Ihre Unterschrift hinzufügen, zuerst vom Server aktualisiert. Nach Beendigung der Aktualisierung werden die von Ihnen vorgenommenen Änderungen an den Server gesendet.
   - **Hinzufügen von Namen/Fotos/Rücknahmeschlüsseln.** Wenn Sie diese Option wählen, werden Schlüssel, denen Sie Namen, Fotos oder Rücknahmeschlüssel hinzugefügt haben, zuerst vom Server aktualisiert. Nach Beendigung der Aktualisierung werden die von Ihnen vorgenommenen Änderungen an den Server gesendet. Durch die vorherige Aktualisierung wird sichergestellt, daß der Schlüssel seit der letzten Aktualisierung nicht zurückgenommen wurde.
   - **Zurücknahme.** Wenn Sie diese Option wählen, werden zurückgenommene Schlüssel zuerst vom Server aktualisiert. Nach Beendigung der Aktualisierung werden die von Ihnen vorgenommenen Änderungen an den Server gesendet.

- **Verifizierung.** Wenn Sie diese Option wählen, sucht und importiert PGP automatisch vom Schlüssel-Server, wenn eine unterschriebene E-Mail-Nachricht oder -Datei verifiziert wird, für die Sie nicht den öffentlichen Schlüssel des Absenders besitzen.

6. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und zum PGPkeys-Menü zurückzukehren, oder wählen Sie eine andere Registerkarte zur Konfiguration weiterer PGP-Voreinstellungen.

So fügen Sie der Server-Liste einen Schlüsselserver hinzu

1. Öffnen Sie **PGP-Optionen**, und klicken Sie auf die Registerkarte **Server**.
2. Klicken Sie auf die Schaltfläche **Neu**.

   Das Dialogfeld **Neuen Server hinzufügen** wird geöffnet (siehe Abbildung 6-15).

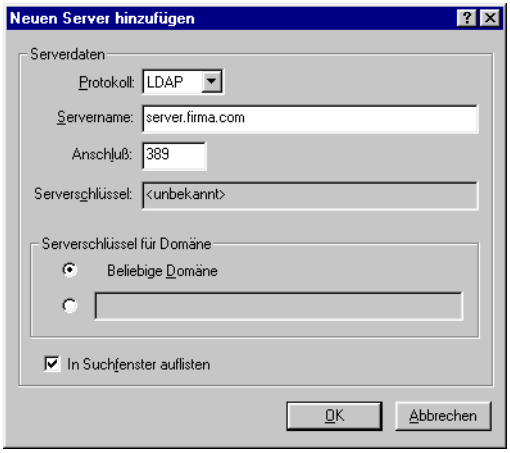


Abbildung 6-15. Dialogfeld „Neuen Server hinzufügen“

3. Wählen Sie im Feld **Protokoll** das Protokoll, mit dem Sie auf den Server zugreifen möchten. Sie haben folgende Möglichkeiten: **LDAP**, **LDAPS** und **HTTP**.
4. Geben Sie im Feld **Servername** den Domänennamen oder die IP-Adresse des Servers an. Beispielsweise server.firma.com oder 123.445.67.
5. Geben Sie im Feld **Anschluß** die Anschlußnummer des Servers an. 11371 wird beispielsweise für ältere HTTP-Certificate Server verwendet, während 389 häufig für LDAP-Certificate Server verwendet wird.

6. Das Feld **Serverschlüssel** ist für LDAPS-Server bestimmt. Der Serverschlüssel wird vom Server zur Authentisierung der Verbindung verwendet. (Schlüsselinformationen werden so lange nicht angezeigt, bis Sie eine Verbindung mit dem Server hergestellt haben.)

7. Wählen Sie die Option **Beliebige Domäne**, so daß PGP Schlüssel von jeder beliebigen Domäne an diesen Schlüsselserver senden kann. Diese Option ist standardmäßig aktiviert.

   Wenn Sie möchten, daß PGP nur von einer bestimmten Domäne aus Schlüssel an diesen Server sendet, wählen Sie die Option unter **Beliebige Domäne**. Geben Sie dann den Firmennamen ein. Wenn Sie beispielsweise die Domäne „firma.com“ festlegen, werden nur die Schlüssel, deren E-Mail-Adresse mit „firma.com“ endet, an diesen Server gesendet.

8. Wählen Sie das Kontrollkästchen **In Suchfenster auflisten**, wenn Sie diesen Schlüsselserver im **PGPkeys-Suchfenster** auflisten möchten.

CA-Optionen festlegen

Verwenden Sie die Registerkarte **CA,** um Ihr X.509-Zertifikat Ihrem PGP-Schlüssel hinzuzufügen. Sie müssen jedoch zuerst das Root-CA-Zertifikat von dem Certificate Server Ihres Unternehmens erhalten haben, bevor Sie Ihr X.509-Zertifikat hinzufügen können. Weitere Informationen zum Erhalten des Root-CA-Zertifikats des Servers erhalten Sie unter „Fordern Sie das Root-CA-Zertifikat an und fügen Sie es Ihrem PGP-Schlüsselbund hinzu.“ auf Seite 38. Weitere Anweisungen zum Festlegen von CA-Optionen und zum Hinzufügen Ihres X.509-Zertifikats zu Ihrem Schlüssel erhalten Sie unter „X.509-Zertifikate PGP-Schlüsseln hinzufügen“ auf Seite 38.

Erweiterte Optionen festlegen

Mit der Registerkarte **Erweitert** können Sie Verschlüsselungsalgorithmen und Vertrauensoptionen für Schlüssel auswählen.

PGP bietet Ihnen die Möglichkeit, Verschlüsselungsalgorithmen für Schlüssel zu wählen bzw. zu ändern. Sie können einen der folgenden Verschlüsselungsalgorithmen für Ihre PGP-Schlüssel auswählen: CAST (Standard), IDEA oder Triple-DES. Wenn Sie IDEA oder Triple-DES verwenden möchten, müssen Sie diese Auswahl vor dem Erstellen der Schlüssel treffen. CAST ist ein neuer Algorithmus, der das Vertrauen von PGP und anderen Kryptographieexperten genießt. Triple-DES ist ein Algorithmus der US-Regierung, der sich über die Jahre bewährt hat. IDEA ist der Algorithmus, der für alle durch PGP generierten RSA-Schlüssel erzeugt wird. Weitere Informationen zu diesen Algorithmen finden Sie im Abschnitt „Die symmetrischen Algorithmen von PGP“ auf Seite 243.

Durch die Auswahl **Bevorzugter Algorithmus** wird folgendes beeinflußt:

- Bei der konventionellen Verschlüsselung wird der bevorzugte Verschlüsselungsalgorithmus verwendet.
- Beim Erstellen eines Schlüssels wird der bevorzugte Verschlüsselungsalgorithmus als Teil des Schlüssels aufgezeichnet, so daß andere Benutzer diesen Algorithmus verwenden, wenn sie für Sie Daten verschlüsseln.

Durch die Auswahl **Zulässige Algorithmen** wird folgendes beeinflußt:

- Beim Erstellen eines Schlüssels werden die zulässigen Verschlüsselungsalgorithmen als Teil des Schlüssels aufgezeichnet, so daß andere Benutzer einen dieser Algorithmen verwenden, wenn ihnen der bevorzugte Verschlüsselungsalgorithmus nicht erhältlich ist.

HINWEIS: Die Verschlüsselung mit einem öffentlichen Schlüssel schlägt fehl, wenn die Person, welche die Nachricht verschlüsselt, weder über den bevorzugten noch über einen der zulässigen Verschlüsselungsalgorithmen verfügt.

WARNUNG: Verwenden Sie die Kontrollkästchen für CAST, IDEA und Triple-DES nur dann, wenn Sie erfahren haben, daß ein bestimmter Algorithmus nicht mehr sicher ist. Wenn Sie beispielsweise bemerken, daß Triple-DES von Unbefugten entschlüsselt wurde, können Sie dieses Kontrollkästchen deaktivieren. Alle neu erzeugten Schlüssel werden dann mit einem Datensatz versehen, der besagt, daß Triple-DES beim Verschlüsseln für Sie nicht verwendet werden sollte.

PGP gibt Ihnen die Option, die Anzeige des Vertrauens in Schlüssel zu aktivieren bzw. zu ändern. Außerdem können Sie einstellen, ob Sie vor dem Verschlüsseln einer Nachricht mit einem öffentlichen Schlüssel, zu dem es einen zusätzlichen Entschlüsselungsschlüssel gibt, gewarnt werden oder nicht. Wählen Sie im Bereich „Vertrauensmodell“ eine der folgenden Optionen:

- **Zweitrangige Gültigkeitsebene anzeigen.** Aktivieren Sie dieses Kontrollkästchen, wenn die Schlüssel zweitrangiger Gültigkeitsebene selbst oder die Aktivierung bzw. Deaktivierung der Gültigkeit angezeigt werden sollen. Die zweitrangige Gültigkeitsebene wird durch Balkensymbole mit verschiedenen Musterungen angezeigt. Die Aktivierung / Deaktivierung der Gültigkeit wird mit Kreissymbolen dargestellt – grün für „Gültig“, grau für „Ungültig“ (Gültigkeit des Schlüssels wurde nicht bestätigt; er wurde weder von einem autorisierten Schlüsselverwalter noch von Ihnen selbst unterzeichnet).

- **Zweitrangige, echte Schlüssel wie unechte behandeln.** Wenn Sie dieses Kontrollkästchen aktivieren, werden alle zweitrangigen, echten Schlüssel wie unechte behandelt. Bei Auswahl dieser Option wird immer, wenn Sie mit zweitrangigen echten Schlüsseln verschlüsseln, das Dialogfeld **PGP-Schlüsselauswahl** angezeigt.

- **Warnmeldung beim Verschlüsseln mit einem ADK.** Über dieses Kontrollkästchen können Sie festlegen, ob beim Verschlüsseln mit einem Schlüssel, mit dem ein ADK verknüpft ist, eine Warnung ausgegeben werden soll.

- **Exportformat.**

  – **Kompatibel:** Exportiert Schlüssel in einem Format, das mit früheren PGP-Versionen kompatibel ist.

  – **Fertig stellen:** Exportiert das neue Schlüsselformat, das Foto-Benutzer-IDs und X.509-Zertifikate enthält.

PGPdisk 7

In diesem Kapitel werden das Modul PGPdisk und seine Funktionen beschrieben sowie Hinweise zur Benutzung von PGPdisk gegeben.

Was ist PGPdisk?

PGPdisk ist eine benutzerfreundliche Verschlüsselungsanwendung, die es Ihnen ermöglicht, einen Bereich auf Ihrer Festplatte für die Speicherung Ihrer vertraulichen Daten zu reservieren. Dieser Bereich wird zum Erstellen einer Datei verwendet, die als PGPdisk-*Volume* bezeichnet wird.

Obwohl es sich nur um eine Datei handelt, funktioniert ein PGPdisk-Volume in etwa wie eine Festplatte, da es Speicherplatz für Ihre Dateien und Anwendungen zur Verfügung stellt. Sie können es sich ungefähr wie eine Diskette oder eine externe Festplatte vorstellen. Wenn Sie die im Volume gespeicherten Anwendungen und Dateien verwenden möchten, müssen Sie das Volume *verbinden*, d. h. für Sie zugänglich machen.

Danach können Sie mit einem PGPdisk-Volume wie mit einem normalen Datenträger arbeiten. Sie können auf dem Volume Anwendungen installieren oder Ihre Dateien in das Volume verschieben oder dort speichern. Wenn das Volume *getrennt* wird, kann es nur noch von Benutzern aufgerufen werden, die Ihre geheime *Paßphrase* kennen. Dabei handelt es sich um ein längeres Paßwort. Auch ein verbundenes Volume ist geschützt; sofern keine Datei oder Anwendung geöffnet ist, wird es in verschlüsselter Form gespeichert. Sollte Ihr Computer abstürzen während ein Volume verbunden ist, bleibt der Inhalt des Volumes verschlüsselt.

❑ **HINWEIS:** Bei PGP-Produkten wird empfohlen, zum Schutz von vertraulichen Daten einen ganzen Satz oder eine lange Zeichenfolge zu verwenden. Derartige Paßphrasen sind in der Regel sicherer als herkömmlich aus sechs bis zehn Zeichen bestehende Paßwörter.

PGPdisk-Funktionen

Das PGPdisk-Programm verfügt über folgende Funktionen bzw. ermöglicht Ihnen folgendes:

- Erstellen von geschützten Volumes mit verschlüsselten Daten, die wie alle anderen Volumes funktionieren, mit deren Verwendung zum Speichern von Dateien Sie bereits vertraut sind.
- Schnelle und sichere Verschlüsselung Ihrer Daten mit minimalem Einfluß auf die Zeit, die zum Aufrufen Ihrer Programme und Dateien benötigt wird.
- Das Programm verwendet den zuverlässigen, für militärische Zwecke geeigneten Verschlüsselungsalgorithmus CAST, der dafür bekannt ist, daß unberechtigte Zugriffe verhindert werden.
- Speichern des Inhalts aller geschützten Volumes in einer verschlüsselten Datei, von der problemlos Sicherheitskopien erstellt werden können und die mit Kollegen ausgetauscht werden kann.

Sinn und Zweck von PGPdisk

Der Zugriff auf Dateien wird bei anderen Produkten durch Zugriffsattribute und einfache Paßwörter geregelt. Damit sind Ihre vertraulichen Daten allerdings nicht uneingeschränkt geschützt. Erst durch Verschlüsseln Ihrer Daten können Sie sicher sein, daß der Inhalt Ihrer Dateien selbst durch die modernste Technik nicht entschlüsselt werden kann.

In der folgenden Liste finden Sie einige Gründe für die Verwendung von PGPdisk zum Sichern Ihrer Dateien:

- Zum Schutz von vertraulichen finanziellen, medizinischen und persönlichen Daten, auf die andere keinen Zugriff haben sollen. Dies ist besonders in der heutigen Internetumgebung wichtig, in der Informationen auf Ihrem PC für die ganze Welt zugänglich sind, wenn Sie im Internet surfen.
- Zum Einrichten von persönlichen Arbeitsbereichen auf einem gemeinsam genutzten Rechner, auf dem jedem Benutzer ein exklusiver Zugriff auf seine Programme und Dateien garantiert wird. Jeder Benutzer kann seine eigenen Volumes verbinden, während er mit dem Rechner arbeitet. Nach dem Trennen kann er dann sicher sein, daß niemand unbefugt auf seine Dateien zugreifen kann.
- Zum Erstellen von Volumes mit Daten, die nur festgelegten Mitgliedern einer bestimmten Arbeitsgruppe zugänglich sind. Ein Volume kann verbunden werden, wenn Mitglieder des Teams an einem bestimmten Projekt arbeiten möchten. Nach der Arbeit kann es wieder getrennt und im verschlüsselten Format gespeichert werden.

- Zum Schutz vor unberechtigtem Zugriff auf die auf einem Notebook-Computer gespeicherten Informationen. Wenn Sie Ihr Notebook verlieren (oder es gestohlen wird), sind Ihre gesamten persönlichen Daten (einschließlich Zugriff auf Online-Dienste und zugehörige Paßwörter, Daten über Geschäftspartner und Bekannte, finanzielle Daten usw.) im allgemeinen gegenüber kriminellem Mißbrauch ungeschützt, wodurch Ihnen Verluste entstehen können, die die Kosten des Notebooks weit übersteigen.
- Zum Sichern des Inhalts von externen Medien, wie beispielsweise von Disketten und Magnetbändern. Die Möglichkeit des Verschlüsselns von externen Medien bietet einen zusätzlichen Schutz beim Speichern und Austauschen von vertraulichen Informationen.

Das PGPdisk-Programm starten

So starten Sie PGPdisk

Wählen Sie die Optionsfolge **Start–>Programme–>PGP–>PGPdisk**. Hiermit wird die PGPdisk-Symbolleiste geöffnet (siehe Abbildung 7-1.).

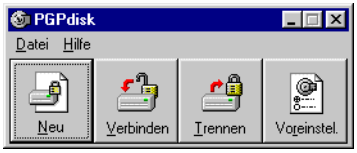


Abbildung 7-1. PGPdisk-Symbolleiste

Über die PGPdisk-Symbolleiste können Sie Volumes problemlos erstellen und verbinden. In der folgenden Liste werden die einzelnen Schaltflächen kurz beschrieben:

Neu	Ruft den PGPdisk-Assistenten auf, der Ihnen beim Erstellen eines neuen PGPdisk-Volumes behilflich ist.
Verbinden	Verbindet das angegebene PGPdisk-Volume, wenn die Paßphrase korrekt eingegeben wurde.
Trennen	Trennt das angegebene PGPdisk-Volume.
Voreinstellungen	Gibt an, wie Sie Ihre Volumes trennen möchten.

Mit PGPdisk-Volumes arbeiten

In diesem Abschnitt wird erläutert, wie Sie PGPdisk-Volumes erstellen, verbinden oder trennen, und wie Einstellungen festgelegt werden, mit denen der Inhalt eines Volumes geschützt ist, wenn es unter bestimmten Umständen getrennt wird.

HINWEIS: Die meisten PGPdisk-Vorgänge können ausgeführt werden, indem Sie mit der rechten Maustaste auf das Symbol für die PGPdisk-Volume-Datei klicken.

Ein neues PGPdisk-Volume erstellen

So erstellen Sie ein neues PGPdisk-Volume

1. Starten Sie PGPdisk. Daraufhin wird die PGPdisk-Symbolleiste angezeigt.
2. Klicken Sie auf **Neu**. Auf dem Bildschirm wird der PGPdisk-Assistent angezeigt. Lesen Sie die einführenden Informationen.
3. Klicken Sie auf **Weiter**.
4. Geben Sie Namen und Pfad des neuen Volumes an.
5. Klicken Sie auf die Schaltfläche **Speichern**.
6. Geben Sie den Speicherplatz ein, den Sie für das neue Volume reservieren möchten (Feld für PGPdisk-Größe). Verwenden Sie ganze Zahlen ohne Dezimalstellen. Um die im Feld angezeigte Zahl zu erhöhen oder zu verringern, können Sie die Pfeiltasten verwenden.

   Die Menge des freien Speicherplatzes für das ausgewählte Laufwerk wird über dem Feld „Größe“ angezeigt.
7. Klicken Sie auf die entsprechende runde Optionsschaltfläche, um als Einheit Kilobyte, Megabyte oder Gigabyte festzulegen.

   Je nach Umfang des verfügbaren Speicherplatzes können Sie Volumes beliebiger Größe zwischen 100 Kilobyte und 2 Gigabyte erstellen.
8. Wählen Sie den Laufwerksbuchstaben für die Verbindung dieses PGPdisk-Volumes (Feld für den PGPdisk-Laufwerksbuchstaben). Mit Hilfe der Pfeiltaste können Sie einen anderen Laufwerksbuchstaben anzeigen und auswählen.
9. Klicken Sie auf **Weiter**.

10. Geben Sie die Folge von Zeichen oder Wörtern ein, die für den Zugriff auf das neue Volume als Paßphrase dienen werden (auch Master-Paßphrase genannt). Drücken Sie die TABULATORTASTE, um Ihre Eingabe zu bestätigen und zum nächsten Textfeld zu gelangen. Wiederholen Sie hier die Eingabe Ihrer Paßphrase. Die Paßphrase muß aus mindestens acht Zeichen bestehen.

    Um zusätzliche Sicherheit zu gewährleisten, werden die Zeichen, die Sie für die Paßphrase eingeben, normalerweise nicht auf dem Bildschirm angezeigt. Wenn Sie jedoch sicher sind, daß Ihnen niemand zuschaut (direkt oder über das Netzwerk), und Sie die Zeichen Ihrer Paßphrase während der Eingabe sehen möchten, deaktivieren Sie das Kontrollkästchen **Eingabe verbergen**.

    HINWEIS: Ihre Sicherheit hängt wesentlich von Ihrer Paßphrase ab. Sie sollten mehrere Wörter, Leerzeichen, Ziffern und andere druckbare Zeichen enthalten. Bei Eingabe der Paßphrase muß die Groß- und Kleinschreibung beachtet werden. Die Paßphrase muß mindestens acht Zeichen enthalten. Wählen Sie etwas, das Ihnen sehr vertraut ist und das Sie bereits in Ihrem Langzeitgedächtnis gespeichert haben. Wenn Sie eine Paßphrase einer plötzlichen Eingebung folgend auswählen, ist es eher wahrscheinlich, daß Sie sie vergessen. Es ist sehr wichtig, daß Sie *Ihre Paßphrase nicht vergessen, andernfalls gehen Ihre Daten verloren!* Weitere Informationen finden Sie im Abschnitt „Paßphrasenqualität“ auf Seite 153.

    ---

11. Klicken Sie auf **Weiter**.

12. Bewegen Sie die Maus im Fenster des PGPdisk-Assistenten in beliebiger Richtung, und / oder betätigen Sie einige Tasten, bis die im Dialogfeld angezeigte Statusleiste vollständig ausgefüllt ist.

    Die Mausbewegungen sowie die eingegebenen Zeichen werden zum Erstellen von Zufallsinformationen verwendet, mit denen das PGPdisk-Programm Daten verschlüsselt.

13. Klicken Sie auf **Weiter**. In der Statusleiste wird angezeigt, wieviel des PGPdisk-Volumes bereits initialisiert wurde.

14. Klicken Sie auf **Weiter**, um PGPdisk zu verbinden.

15. Klicken Sie auf **Fertig stellen**. Auf dem Bildschirm wird das Formatierungsfenster angezeigt.

16. Geben Sie eine Bezeichnung für das neue Volume ein (damit wird das Volume im Windows-Explorer gekennzeichnet).

17. Klicken Sie auf **Start**. Daraufhin wird ein Warnhinweis angezeigt.

18. Klicken Sie auf **OK**. (Im neuen Volume sind keine Daten vorhanden.) Sie erhalten bei Abschluß der Formatierung eine Systemmeldung.

19. Klicken Sie im Formatierungsfenster auf **Schließen**.

    Das PGPdisk-Volume wird in einem der Explorer-Fenster angezeigt.

    Durch ein Symbol für ein verbundenes Volume in PGPdisk wird das Volume im angegebenen Pfad angezeigt.

    Ein verschlüsseltes Volume in PGPdisk wird für Ihr sicheres Volume im angegebenen Pfad wie folgt durch ein Symbol gekennzeichnet:

Verbundenes PGPdisk-Volume

Verschlüsseltes PGPdisk-Volume

20. Doppelklicken Sie auf das Symbol, um das Volume zu öffnen.

Paßphrasen ändern

Sie können die Master-Paßphrase oder eine alternative Paßphrase für ein PGPdisk-Volume ändern.

So ändern Sie Ihre Paßphrase

1. Stellen Sie sicher, daß das PGPdisk-Volume nicht verbunden ist. Sie können keine Paßphrasen ändern, wenn das PGPdisk-Volume verbunden ist.

2. Wählen Sie im Menü **Datei**die Option **Paßphrase ändern**.

   Das Dialogfeld **Öffnen** wird angezeigt.

3. Suchen Sie die betreffende Datei auf dem Datenträger.

4. Das Dialogfeld **Paßphrase** wird geöffnet (siehe Abbildung 7-2).

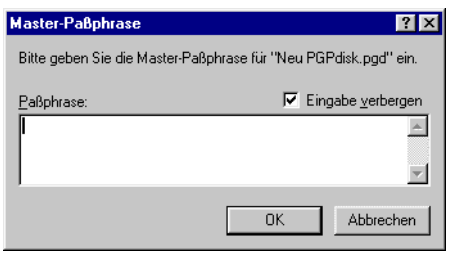


Abbildung 7-2. Dialogfeld „Paßphrase ändern“

5. Geben Sie Ihre Paßphrase ein, und klicken Sie auf **OK**.

   Das Fenster **Neue Paßphrase** wird angezeigt (siehe Abbildung 7-3).

Abbildung 7-3. Dialogfeld „Neue Paßphrase“

6. Geben Sie die Folge von Zeichen oder Wörtern ein, die für den Zugriff auf das neue Volume als Paßphrase dienen wird (auch Master-Paßphrase genannt). Drücken Sie die TABULATORTASTE, um Ihre Eingabe zu bestätigen und zum nächsten Textfeld zu gelangen. Wiederholen Sie hier die Eingabe Ihrer Paßphrase. Die Paßphrase muß aus mindestens acht Zeichen bestehen.

7. Klicken Sie auf **OK**.

   Das Dialogfeld **Neue Paßphrase** wird geschlossen.

Alternative Paßphrasen hinzufügen

Wenn Sie die Master-Paßphrase eingegeben haben (die zum Erstellen des Datenträgers verwendet wurde), können Sie bis zu sieben alternative Paßphrasen hinzufügen, die zum Verbinden des Volumes verwendet werden können. Dies ist dann sinnvoll, wenn Sie regelmäßig dieselbe Master-Paßphrase verwenden und das Volume auch anderen Personen zur Verfügung stellen möchten, die eigene eindeutige Paßphrasen verwenden. Alternative Paßphrasen können nur von einer Person hinzugefügt werden, der die Master-Paßphrase bekannt ist.

Alle Benutzer, die eine Paßphrase kennen, können diese auch ändern. Auf den Inhalt des Volumes können Sie unabhängig davon jedoch immer zugreifen. Sie können dem Volume auch den Status „Schreibgeschützt“ zuweisen, wodurch Personen die Dateien zwar lesen, jedoch nicht ändern können.

So fügen Sie alternative Paßphrasen hinzu

1. Stellen Sie sicher, daß das PGPdisk-Volume momentan nicht verbunden ist. Sie können keine Paßphrasen hinzufügen oder ändern, solange das PGPdisk-Volume verbunden ist.
2. Wählen Sie im Menü **Datei**die Option **Paßphrase hinzufügen**.

   Daraufhin wird das Dialogfeld **Paßphrase** angezeigt, in dem Sie zur Eingabe der Master-Paßphrase aufgefordert werden. Wenn auf Ihrem Rechner mehrere PGPdisk-Volumes vorhanden sind, müssen Sie ein Volume auswählen.
3. Geben Sie die Master-Paßphrase ein, und klicken Sie auf **OK**.

   Das Dialogfeld **Neue Paßphrase** wird geöffnet (siehe Abbildung 7-4).

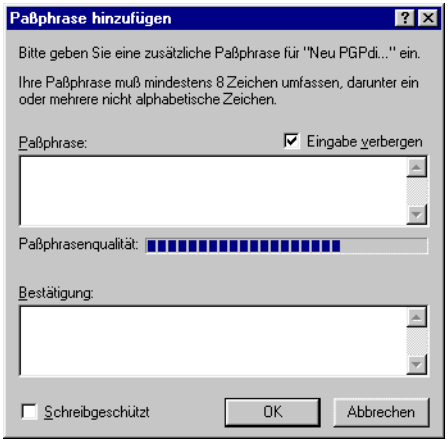


Abbildung 7-4. Dialogfeld „Neue Paßphrase“

4. Geben Sie eine alternative Paßphrase für das genannte Volume ein, und drücken Sie dann die TABULATORTASTE. Geben Sie die Paßphrase erneut ein, um sie zu bestätigen.

   Dabei können Sie das Kontrollkästchen **Schreibgeschützte Paßphrase** aktivieren, um anzugeben, ob der gesamte Inhalt des Volumes als „schreibgeschützt“ gelten soll.
5. Klicken Sie auf **OK**.

Nach dem Erstellen einer alternativen Paßphrase können Sie (oder eine andere Person, der die Paßphrase bekannt ist) diese Paßphrase wieder entfernen. Wählen Sie dazu im Menü **Datei** die Option **Paßphrase entfernen**. Master-Paßphrasen können nicht entfernt werden. Weitere Informationen finden Sie im Abschnitt „Paßphrasen entfernen“.

Paßphrasen entfernen

Der Vorgang zum Entfernen einer Paßphrase ist dem zum Hinzufügen oder Ändern einer Paßphrase ähnlich. Eine Master-Paßphrase kann nicht entfernt werden.

So entfernen Sie eine Paßphrase

1. Stellen Sie sicher, daß das PGPdisk-Volume nicht verbunden ist. Sie können keine Paßphrasen entfernen, wenn das PGPdisk-Volume verbunden ist.
2. Wählen Sie im Menü **Datei** die Option **Paßphrase entfernen**.

   In einem Dialogfeld werden Sie aufgefordert, die zu entfernende Paßphrase einzugeben.
3. Geben Sie die Paßphrase ein, und klicken Sie auf **OK**.

Alle alternativen Paßphrasen entfernen

Sie können alle alternativen Paßphrasen gleichzeitig entfernen. Dies ist vor allem dann zweckmäßig, wenn auch andere Benutzer mit alternativen Paßphrasen Zugriff auf das PGPdisk-Volume haben, und Sie Ihnen den Zugriff verweigern möchten.

So entfernen Sie alle alternativen Paßphrasen

1. Stellen Sie sicher, daß das PGPdisk-Volume nicht verbunden ist. Sie können keine Paßphrasen entfernen, wenn das PGPdisk-Volume verbunden ist.
2. Halten Sie die UMSCHALTTASTE gedrückt, und wählen Sie im Menü **Datei** die Option **Alternative Paßphrasen entfernen**.

   Ein Dialogfeld wird angezeigt, in dem Sie bestätigen müssen, daß Sie alle alternativen Paßphrasen entfernen möchten.
3. Klicken Sie auf **Ja**.

   Über ein Dialogfeld werden Sie informiert, daß alle alternativen Paßphrasen erfolgreich entfernt wurden.

Öffentliche Schlüssel hinzufügen/entfernen

Sie können öffentliche Schlüssel einer PGPdisk-Datei hinzufügen und aus dieser entfernen. Mit dieser Funktion können Sie und andere, denen die Paßphrasen für diese Schlüssel bekannt sind, das Volume mit Hilfe der Schlüssel verbinden.

So fügen Sie einen öffentlichen Schlüssel Ihrem PGPdisk-Volume hinzu

1. Stellen Sie sicher, daß das PGPdisk-Volume nicht verbunden ist. Sie können keine öffentlichen Schlüssel hinzufügen, solange das PGPdisk-Volume verbunden ist.
2. Wählen Sie im Menü **Datei** die Option **Öffentliche Schlüssel hinzufügen/entfernen**.
3. Wählen Sie aus der Symbolleiste **PGPdisk wählen** die Option „PGPdisk“ aus.

   Sie werden zur Eingabe der Master-Paßphrase aufgefordert.

   Das Fenster **Empfängerauswahl** wird angezeigt.
4. Ziehen Sie den oder die Schlüssel vom oberen Bereich des Fensters in den unteren Bereich.
5. Klicken Sie auf **OK**.

So entfernen Sie einen öffentlichen Schlüssel aus Ihrem PGPdisk-Volume

1. Stellen Sie sicher, daß das PGPdisk-Volume nicht verbunden ist. Sie können keine öffentlichen Schlüssel entfernen, wenn das PGPdisk-Volume verbunden ist.
2. Wählen Sie im Menü **Datei** die Option **Öffentliche Schlüssel hinzufügen/entfernen**.
3. Wählen Sie aus der Symbolleiste **PGPdisk wählen** die Option „PGPdisk“ aus.

   Sie werden zur Eingabe der Master-Paßphrase aufgefordert.

   Das Fenster **PGP – Schlüssel auswählen** wird angezeigt (siehe Abbildung 7-5).

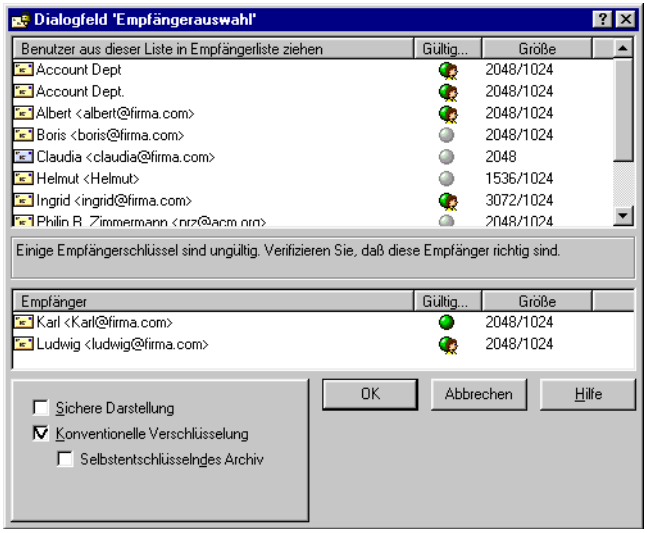


Abbildung 7-5. Dialogfeld „PGP – Schlüssel auswählen“

4. Ziehen Sie den oder die Schlüssel vom unteren Bereich des Fensters in den oberen Bereich.

5. Klicken Sie auf **OK**.

Ein PGPdisk-Volume verbinden

Beim Erstellen eines neuen Volumes wird dieses durch das PGPdisk-Programm automatisch verbunden, so daß Sie es sofort zum Speichern Ihrer Dateien verwenden können. Wenn Sie den Inhalt des Volumes speichern möchten, müssen Sie das Volume trennen (weitere Informationen finden Sie unter „Ein PGPdisk-Volume trennen“ auf Seite 147). Nachdem ein Volume getrennt wurde, ist der Inhalt des Volumes in einer verschlüsselten Datei gespeichert und erst wieder zugänglich, wenn das Volume wieder verbunden wird.

Zum Verbinden eines Volumes gibt es mehrere Möglichkeiten:

- Doppelklicken Sie auf das Symbol für das Volume.
- Ziehen Sie das Symbol des Volumes auf das PGPdisk-Symbol im Ordner für PGP 6.5.
- Ziehen Sie das Symbol des Volumes auf die Schaltfläche **Verbinden** der PGPdisk-Symbolleiste.
- Klicken Sie mit der rechten Maustaste auf das Symbol für das betreffende Volume. Wählen Sie **PGPdisk–>PGPdisk verbinden**.
- Verwenden Sie in der PGPdisk-Symbolleiste die Schaltfläche **Verbinden**.

So verbinden Sie ein Volume mit der Schaltfläche „Verbinden“

1. Starten Sie PGPdisk.

   Daraufhin wird die **PGPdisk-Symbolleiste** angezeigt.

2. Klicken Sie auf **Verbinden**, oder wählen Sie im Menü **Datei** die Option **PGPdisk verbinden**.

   Daraufhin wird das Dialogfeld **PGPdisk verbinden** angezeigt.

3. Wählen Sie das verschlüsselte Volume aus, das Sie verbinden möchten, und klicken Sie dann auf **Öffnen**.
   Sie werden aufgefordert, die Paßphrase für das gewählte Volume einzugeben.

4. Geben Sie die Paßphrase ein, und klicken Sie auf **OK**. Wenn Sie die Dateien im Volume nicht bearbeiten möchten, klicken Sie auf das Kontrollkästchen **Schreibgeschützt**. Wenn Sie die Paßphrase korrekt eingegeben haben, wird das Volume verbunden, und Sie können auf die Daten in der verschlüsselten Datei zugreifen. Das Volume wird in der Ordnerstruktur des Windows Explorers angezeigt.

   Andererseits können Sie ein Volume auch verbinden, ohne das Programm PGPdisk auszuführen. Sie können stattdessen einfach über den Finder auf den Namen der verschlüsselten Datei (oder das entsprechende Symbol) doppelklicken oder die Datei auf das Programmsymbol von PGPdisk ziehen.

Ein verbundenes PGPdisk-Volume verwenden

Sie können Dateien und Ordner auf einem PGPdisk-Volume wie auf jedem anderen Volume erstellen, kopieren, verschieben und löschen. Analog kann jeder andere Benutzer, der (entweder auf demselben Rechner oder evtl. über das Netzwerk) über Zugriff auf das Volume verfügt, ebenfalls auf die im Volume gespeicherten Daten zugreifen. Erst wenn Sie das Volume trennen, kann auf die Daten in der dem Volume zugeordneten verschlüsselten Datei nicht mehr zugegriffen werden.

WARNUNG: Obwohl die verschlüsselten, den einzelnen Volumes zugeordneten Dateien vor mißbräuchlichem Zugriff geschützt sind, können sie gelöscht werden. Wenn eine unbefugte Person auf Ihre Daten zugreifen kann, ist es möglich, daß sie die verschlüsselte Datei löscht, die die Grundlage für das Volume bildet. Es wird daher empfohlen, eine Sicherungskopie der verschlüsselten Datei zu erstellen.

Ein PGPdisk-Volume trennen

Wenn Sie auf ein bestimmtes Volume nicht mehr zugreifen und dessen Inhalt sperren möchten, müssen Sie das Volume trennen. Ein Volume mit geöffneten Dateien kann nicht getrennt werden.

So trennen Sie ein PGPdisk-Volume

1. Schließen Sie alle Dateien im PGPdisk-Volume, das Sie trennen möchten.
2. Wählen Sie im Menü **Datei** die Option **PGPdisk trennen**.

   Außerdem stehen Ihnen zum Trennen eines PGPdisk-Volumes folgende Methoden zur Verfügung:

   - Klicken Sie in der PGPdisk-Symbolleiste auf die Schaltfläche **Trennen**,
   - Klicken Sie mit der rechten Maustaste auf den Laufwerksbuchstaben im Windows Explorer,

     UND

   - Klicken Sie mit der rechten Maustaste auf die betreffende Volume-Datei.

Wenn ein Volume getrennt ist, wird sein Inhalt in der verschlüsselten, dem Volume zugeordneten Datei gesperrt. Der Inhalt des Volumes wird in der verschlüsselten Datei gespeichert, und ist erst wieder zugänglich, wenn das Volume verbunden wird. Es ist u. U. hilfreich, PGPdisk-Volumes als Fenster anzuzeigen, in dem die Daten in der verschlüsselten Datei angezeigt werden können. Der Inhalt einer PGPdisk-Datei ist erst verfügbar, wenn ein Benutzer eine gültige Paßphrase kennt und die Datei als Volume verbindet.

Voreinstellungen festlegen

Mit der Schaltfläche **Voreinstellungen** in der PGPdisk-Symbolleiste können Sie festlegen, mit welcher Methode Sie Ihre Volumes erstellen und trennen möchten.

So legen Sie die Voreinstellungen fest

1. Klicken Sie in der PGPdisk-Symbolleiste auf **Voreinstellungen**, oder wählen Sie im Menü **Datei** die Option **Voreinstellungen**.

   Das Dialogfeld **Voreinstellungen** wird angezeigt.

2. Wählen Sie die gewünschten Optionen, indem Sie auf die entsprechenden Registerkarten und Kontrollkästchen klicken.

   Registerkarte „Automatisch trennen“

   - **Nach [15] Minuten ohne Aktivität automatisch trennen.** Ist diese Option aktiviert, trennt PGPdisk automatisch alle verbundenen PGPdisk-Volumes, wenn Ihr Computer so viele Minuten inaktiv ist, wie im Feld angezeigt wird. Sie können einen Wert zwischen 1 und 999 Minuten einstellen.

     HINWEIS: PGPdisk kann ein PGPdisk-Volume nicht automatisch trennen, wenn Dateien in diesem Volume geöffnet sind.

   - **Automatisch trennen im Standby-Modus des Computers.** Ist diese Option aktiviert, trennt PGPdisk automatisch alle verbundenen PGPdisk-Volumes, wenn Ihr Computer in den Standby-Modus geschaltet wird. (Nicht alle Computer-Modelle verfügen über einen Standby-Modus.)

     Mit der Option **Standby verhindern, wenn PGP-Volumes nicht getrennt werden konnten** wird gewährleistet, daß Ihr Computer nicht in den Standby-Modus schaltet, wenn ein PGP-Datenträger nicht getrennt werden kann.

     HINWEIS: Diese beiden Optionen **(Automatisch trennen im Standby-Modus des Computers** und **Standby verhindern, wenn PGP-Volumes nicht getrennt werden konnten**) sind bei NT-Systemen deaktiviert.

   Registerkarte „HotKey zum Trennen“

   - **Registerkarte „Hotkey zum Trennen aktivieren“.** Wenn Sie in das Textfeld eine Tastenkombination eingeben und dieses Kontrollkästchen aktivieren, erstellen und aktivieren Sie damit eine Tastenkombination, mit der Sie alle PGP-Datenträger im System mit einem einzigen Tastendruck trennen können.

3. Klicken Sie auf **OK**, wenn Sie alle Einstellungen festgelegt haben.

   Die Einstellungen zum automatischen Trennen sind hilfreich, wenn Sie Ihren Computer für eine bestimmte Zeit unbeaufsichtigt lassen müssen. Sie müssen die Zeitangaben für diese Einstellungen in Abhängigkeit davon einrichten, wie sicher Ihr System vor unbefugtem Zugriff ist. Sie können beide Voreinstellungen gleichzeitig festlegen.

PGPdisk-Volumes verwalten

In diesem Abschnitt wird beschrieben, wie PGPdisk-Volumes beim Systemstart automatisch verbunden werden, und wie Sicherungskopien von Daten erstellt und mit anderen ausgetauscht werden können.

PGPdisk-Dateien mit einem entfernten Server verbinden

Sie können PGPdisk-Volumes auf allen Arten von Servern (Windows NT, 95, 98 oder UNIX) ablegen. Diese Volumes können dann von allen Benutzern verbunden werden, die über einen Computer mit Windows 95 verfügen.

☐ **HINWEIS:** Der erste Benutzer, der das Volume lokal verbindet, verfügt über Lese- und Schreibzugriff auf das Volume. Danach kann kein anderer auf das Volume zugreifen. Wenn Sie möchten, daß auch andere Benutzer auf die Dateien des Volumes zugreifen können, müssen Sie das Volume im Modus „Schreibgeschützt“ verbinden. *Alle* Benutzer des Volumes verfügen dann über schreibgeschützten Zugriff.

Wenn das Volume auf einem Server mit Windows 95 gespeichert ist, können Sie es auch mit dem entfernten Server verbinden und damit die gemeinsame Nutzung des verbundenen Volumes zulassen. Bei diesem Vorgang ist allerdings keine Sicherheit für die Dateien im Volume gewährleistet.

PGPdisk-Volumes automatisch verbinden

Auf Wunsch können Sie PGPdisk-Volumes beim Systemstart automatisch verbinden.

So werden PGPdisk-Volumes automatisch verbunden

1. Erstellen Sie eine Tastenkombination für alle PGPdisk-Dateien, die beim Starten Ihres Computers verbunden werden sollen.
2. Legen Sie die Verknüpfungen im Ordner **Winnt–>Profiles–>{Name des aktuellen Benutzers}–> Startmenü–> Programme** ab.

   Wenn sich die Shortcuts in diesem Ordner befinden, werden die PGPdisk-Volumes bei jedem Starten Ihres Computers verbunden. Sie werden beim Verbinden aufgefordert, die Paßphrase für jedes PGPdisk-Volume einzugeben.

Sicherungskopien für PGPdisk-Volumes erstellen

Es wird empfohlen, Sicherungskopien des Inhalts Ihrer PGPdisk-Volumes zu erstellen, um Ihre Daten bei Systemausfällen und Festplattenfehlern zu schützen. Obwohl es möglich ist, eine Sicherungskopie des Inhalts eines verbundenen PGPdisk-Volumes wie bei jedem anderen Volume zu erstellen, wird dies nicht empfohlen, da der Inhalt nicht verschlüsselt wird und somit jedem zugänglich ist, der die Sicherungskopie wiederherstellen kann. Statt den Inhalt eines verbundenen PGPdisk-Volumes zu sichern, sollten Sie eine Sicherungskopie des verschlüsselten PGPdisk-Volumes erstellen.

So erstellen Sie Sicherungskopien von PGPdisk-Volumes

1. Klicken Sie auf das Symbol für das PGPdisk-Volume. Wählen Sie die Option **PGPdisk trennen**.
2. Kopieren Sie die getrennte, verschlüsselte Datei auf eine Diskette, ein Band oder einen Wechseldatenträger analog zur Vorgehensweise bei einer normalen Datei. Selbst wenn eine unbefugte Person Zugriff auf die Sicherungskopie hat, kann sie deren Inhalt nicht entschlüsseln.

Beim Erstellen von Sicherungskopien der verschlüsselten Dateien müssen Sie an folgendes denken:

- PGPdisk ist ein Produkt für sicherheitsbewußte Menschen und Unternehmen. Das Erstellen einer Sicherungskopie auf einem Netzwerklaufwerk räumt Dritten genügend Möglichkeiten ein, eine einfache Paßphrase zu erraten. Wir empfehlen Ihnen, Sicherungskopien nur auf Geräten zu erstellen, auf die Sie physischen Zugang haben. Eine lange, komplizierte Paßphrase hilft darüber hinaus in dieser Situation, das Risiko zu verringern. Siehe „Paßphrasenqualität“ auf Seite 153.
- Vergewissern Sie sich, wenn Sie mit einem Netzwerk verbunden sind, daß nicht jedes Netzwerksicherungssystem eine Sicherungskopie Ihrer verbundenen Volumes erstellt. Sie müssen sich darüber möglicherweise mit Ihrem Systemadministrator unterhalten. Unter gewissen Umständen haben Sie vielleicht nichts dagegen, wenn von Ihren verschlüsselten Dateien Sicherungskopien erstellt werden, da die Informationen dann sicher sind. Es ist unter keinen Umständen ratsam, den Inhalt Ihrer verbundenen Volumes sichern zu lassen, da dies den Zweck der Informationsverschlüsselung zunichte macht.

PGPdisk-Volumes austauschen

Sie können PGPdisk-Volumes mit Kollegen austauschen, die über ein eigenes PGPdisk-Programm verfügen, indem Sie ihnen eine Kopie der verschlüsselten Datei mit den dem Volume zugeordneten Daten senden. Zum Austauschen von PGPdisk-Volumes gibt es folgende Möglichkeiten:

- Als E-Mail-Anhänge
- Auf Disketten oder Magnetbändern.
- Über ein Netzwerk

TIP: Überlegen Sie sich genau, wie Sie jemandem die Paßphrase für den Zugriff auf ein PGPdisk-Volume zukommen lassen. Wenn Sie nicht gerade PGP verwenden, wird das Austauschen von Paßphrasen über E-Mail nicht empfohlen. Auch Telefonleitungen können überwacht und abgehört werden. Je mehr Sicherheitsvorkehrungen Sie treffen, desto sicherer können Sie sein, daß Ihre vertraulichen Informationen auch geheim bleiben. Wenn Sie nicht über ein sicheres E-Mail-System verfügen, wird empfohlen, der anderen Person die Paßphrase in einem persönlichen Gespräch oder über die reguläre Post mitzuteilen.

Wenn die Zielperson eine Kopie der verschlüsselten Datei erhalten hat, muß das Volume nur noch mit der entsprechenden Paßphrase bzw. mit dem privaten Schlüssel (wenn die Verschlüsselung des Volumes auf dem öffentlichen Schlüssel der Zielperson basiert) verbunden werden. Außerdem wird eine Kopie des PGPdisk-Programms benötigt. Weitere Informationen zum Verbinden eines PGPdisk-Volumes finden Sie im Abschnitt „Ein PGPdisk-Volume verbinden“ auf Seite 145.

Größe eines PGPdisk-Volumes ändern

Die Größe eines bereits erstellten PGPdisk-Volumes kann zwar nicht geändert werden, dafür können Sie aber ein größeres oder kleineres Volume erstellen und dann den Inhalt des alten Volumes in das neue Volume kopieren.

So ändern Sie die Größe eines PGPdisk-Volumes

1. Erstellen Sie ein neues PGPdisk-Volume, und geben Sie die gewünschte Größe an.
2. Kopieren Sie den Inhalt des vorhandenen verbundenen PGPdisk-Volumes in das neu erstellte Volume.
3. Trennen Sie das alte PGPdisk-Volume, und löschen Sie dann die dem Volume zugeordnete verschlüsselte Datei, um den Speicherplatz wieder freizugeben.

Technische Daten und Sicherheitsvorkehrungen

In diesem Abschnitt werden Aspekte zur Verschlüsselung und zu Sicherheitsvorkehrungen besprochen sowie Hinweise für Benutzer und technische Informationen zu PGPdisk gegeben.

Überblick über PGPdisk-Volumes

PGPdisk-Volumes dienen zum Strukturieren Ihrer Arbeit, zum Auseinanderhalten von Dateien mit ähnlichen Namen und zum Getrennthalten von verschiedenen Versionen eines Dokuments oder Programms.

Obwohl die von Ihnen mit der PGPdisk-Funktion erstellten Volumes wie normale, Ihnen bereits bekannte Volumes funktionieren, werden die Daten in einer großen verschlüsselten Datei gespeichert. Nur beim Verbinden der Datei wird der Inhalt in Form eines Volumes dargestellt. Ihre gesamten Daten bleiben in der verschlüsselten Datei gesichert und werden nur entschlüsselt, wenn Sie auf eine der Dateien zugreifen. Wenn die Daten für ein Volume auf diese Weise gespeichert werden, können PGPdisk-Volumes problemlos mit anderen ausgetauscht oder bearbeitet werden. Allerdings können Daten auch leichter verlorengehen, wenn die Datei versehentlich gelöscht wird. Es empfiehlt sich, eine Sicherungskopie dieser verschlüsselten Dateien zu erstellen, damit die Daten wiederhergestellt werden können, falls die Originaldatei beschädigt wird. Sie können die verschlüsselten Dateien selbst zwar nicht

komprimieren, um deren Größe zu verringern, es ist jedoch möglich, die einzelnen Dateien im verbundenen Volume zu komprimieren und dadurch mehr verschlüsselte Daten im Volume zu speichern. Außerdem können Sie ein geschütztes PGPdisk-Volume in einem anderen speichern und so verschiedene Volumes ineinander einbetten, um den Grad der Sicherheit zu erhöhen.

PGPdisk-Verschlüsselungsalgorithmus

Bei der Verschlüsselung wird eine mathematische Formel verwendet, mit der Ihre Daten so kodiert werden, daß sie nur von Ihnen verwendet werden können. Bei Verwendung des richtigen mathematischen Schlüssels können Sie Ihre Daten decodieren. Mit der PGPdisk-Verschlüsselungsformel wird ein Teil des Verschlüsselungsprozesses auf Grundlage von Zufallsdaten ausgeführt. Die Zufallsdaten resultieren zum Teil aus den Mausbewegungen während der Verschlüsselung und ergeben sich teilweise auch direkt aus der Paßphrase.

Beim PGPdisk-Programm wird ein komplizierter Verschlüsselungsalgorithmus verwendet, der unter der Bezeichnung CAST bekannt ist. Er gilt gegenwärtig als ideale Blockchiffre, da er schnell arbeitet und äußerst schwer zu entschlüsseln ist. Der Name dieses Algorithmus wurde aus den Anfangsbuchstaben seiner Entwickler abgeleitet, Carlisle Adams und Stafford Tavares von Northern Telecom (Nortel). Nortel hat zwar ein Patent für CAST angemeldet, die Firma hat jedoch zugesichert, CAST jedermann ohne Lizenzgebühren zur Verfügung zu stellen. CAST scheint ausgesprochen gut entwickelt zu sein, und zwar von Personen mit einem guten Namen in diesem Bereich. Die Entwicklung basiert auf einem sehr formalen Ansatz, mit einigen formal nachweisbaren Hypothesen. Daraus ergeben sich gute Gründe für die Annahme, daß der 128-Bit-Schlüssel dieses Algorithmus mit den gegenwärtig bekannten Verfahren nicht entschlüsselt werden kann. CAST hat keine ineffizienten Schlüssel. Es sprechen viele Argumente dafür, daß CAST immun gegen lineare und differentiale Kryptoanalyse ist. Diese Methoden werden in der Fachliteratur allgemein als die leistungsfähigsten Kryptoanalyseformen dargestellt und waren gleich leistungsstark im Decodieren von DES (Data Encryption Standard).

Paßphrasenqualität

Ihre Sicherheit hängt wesentlich von Ihrer Paßphrase ab. Wenn Sie jedoch einmal eine Datei verschlüsselt haben und dann feststellen mußten, daß Sie sie nicht wieder entschlüsseln konnten, werden Sie wissen, wie wichtig es ist, eine unvergeßliche Paßphrase zu wählen.

Die meisten Anwendungen verlangen ein Paßwort mit drei bis acht Zeichen. Ein Einwort-Paßwort ist anfällig für einen „Wörterbuchangriff“, welcher darin besteht, einen Computer alle Wörter im Wörterbuch durchprobieren zu lassen, bis er Ihr Paßwort gefunden hat. Zum Schutz gegen diese Art des Angriffs werden im allgemeinen Paßwörter aus einer Kombination von Groß- und Kleinbuchstaben, Zahlen, Satz- und Leerzeichen empfohlen. Dadurch kommt ein stärkeres Paßwort zustande, das aber unverständlich und daher leichter zu vergessen ist. Der Gebrauch von Einwort-Paßwörtern wird deshalb nicht empfohlen.

Eine Paßphrase ist weniger anfällig für einen „Wörterbuchangriff“. Dies wird einfach durch die Verwendung von mehreren Wörtern erreicht und nicht durch willkürliches Einfügen einer Menge nicht alphabetischer Zeichen zur Vereitelung eines „Wörterbuchangriffs“, was zu einer leicht zu vergessenden Paßphrase führt. Wenn Sie Ihre Paßphrase vergessen, kann daraus wiederum ein verhängnisvoller Informationsverlust resultieren, da Sie in diesem Fall Ihre eigenen Dateien nicht mehr entschlüsseln können. Es ist jedoch unwahrscheinlich, daß Sie sich die Paßphrase wortwörtlich merken können, es sei denn, die von Ihnen gewählte Paßphrase ist sehr einprägsam. Wenn Sie eine Paßphrase einer plötzlichen Eingebung folgend auswählen, ist es eher wahrscheinlich, daß Sie sie vergessen. Wählen Sie stattdessen etwas, was Sie ohnehin schon im Langzeitgedächtnis „gespeichert“ haben. Verwenden Sie jedoch keine Wendung, die Sie in letzter Zeit jemandem gegenüber verwendet haben und auch kein berühmtes Zitat, da Ihre Paßphrase für einen raffinierten Hacker ja schwer zu erraten sein soll. Wenn die gewählte Wendung schon tief in Ihrem Langzeitgedächtnis verwurzelt ist, werden Sie sie wahrscheinlich nicht vergessen. *Schreiben Sie sie auf keinen Fall auf!*

Ihre Paßphrase ist Teil der Zufallsdaten, die zum Verschlüsseln Ihrer PGPdisk-Dateien verwendet werden. Die Paßphrasenqualitätsanzeige sollte mindestens halb ausgefüllt sein, wenn Sie Ihre Paßphrase eingeben. Nur wenn die ganze Leiste ausgefüllt ist, wird ein maximaler Schutz gewährleistet.

Sie können eine separate oder alternative Paßphrase für jedes von Ihnen erstellte PGPdisk-Volume erstellen. Dadurch können Sie einigen Benutzern Zugriff auf ausgewählte PGPdisk-Dateien auf einer Volume-für-Volume-Basis gewähren. Sie können eine Paßphrase für PGPdisk-Dateien verwenden, die Sie einem Kollegen senden, und trotzdem verhindern, daß dieser Kollege auf andere Ihrer PGPdisk-Dateien zugreifen kann.

Besondere Sicherheitsvorkehrungen von PGPdisk

PGPdisk trifft spezielle Vorkehrungen, um Sicherheitsprobleme zu vermeiden, was bei anderen Programmen unter Umständen nicht der Fall ist. Dazu gehören folgende Funktionen:

Paßphrase löschen

Wenn Sie eine Paßphrase eingeben, wird sie von PGPdisk nur für kurze Zeit verwendet und dann aus dem Speicher gelöscht. PGPdisk vermeidet darüber hinaus, daß Kopien von der Paßphrase gemacht werden. Folglich verbleibt Ihre Paßphrase in der Regel nur einen Bruchteil einer Sekunde im Speicher. Diese Funktion ist von besonderer Bedeutung, denn bliebe die Paßphrase im Speicher, könnte jemand dort nach ihr suchen, wenn Ihr Computer unbeaufsichtigt ist. Sie würden davon nichts merken, doch diejenige Person hätte dann vollen Zugriff auf alle PGPdisk-Volumes, die von dieser Paßphrase geschützt werden.

Schutz des virtuellen Speichers

Ihre Paßphrase oder andere Schlüssel könnten auf Festplatte geschrieben werden, wenn das virtuelle Speichersystem Speicherdaten auf die Festplatte auslagert. PGPdisk sorgt dafür, daß Paßphrasen und Schlüssel nie auf Festplatte geschrieben werden. Diese Funktion ist besonders wichtig, da jemand die virtuelle Speicherdatei nach Paßphrasen durchsuchen könnte.

Schutz vor statischer Ionenmigration im Speicher

Beim Verbinden von PGPdisk wird Ihre Paßphrase in einen Schlüssel umgewandelt. Mit diesem Schlüssel werden die Daten auf Ihrem PGPdisk-Volume ver- und entschlüsselt. Während die Paßphrase sofort aus dem Speicher gelöscht wird, verbleibt der Schlüssel (aus dem Ihre Paßphrase nicht wieder abgeleitet werden kann) beim Verbinden im Speicher. Der Schlüssel ist im virtuellen Speicher zwar geschützt, wenn jedoch in einem bestimmten Speicherbereich dieselben Daten über einen extrem langen Zeitraum gespeichert sind, ohne daß der Computer ausgeschaltet oder neu gestartet wird, bleibt im Speicher möglicherweise eine statische Ladung zurück, die von Hackern gelesen werden kann. Wenn ein PGPdisk über einen langen Zeitraum verbunden bleibt, können erkennbare Spuren Ihres Schlüssels im Speicher zurückbleiben. Derartige Geräte finden sich natürlich nicht bei Ihrem Computerhändler um die Ecke, wohl aber auf Regierungsebene.

Dagegen werden in PGPdisk Vorkehrungen getroffen, indem zwei Kopien des Schlüssels im RAM gespeichert werden: eine normale Kopie und eine bitinvertierte Kopie, die beide in einem Sekundenrhythmus invertiert werden.

Zusätzliche Sicherheitsvorkehrungen

In der Regel hängt der Schutz Ihrer Daten von den getroffenen Vorkehrungen ab, denn kein Verschlüsselungsprogramm kann Ihre Daten schützen, wenn unzureichende Vorsichtsmaßnahmen getroffen werden. Wenn beispielsweise Ihr Computer eingeschaltet ist und Sie vertrauliche Dateien geöffnet haben und Ihren Arbeitsplatz verlassen, kann jeder auf diese Informationen zugreifen und sogar den Schlüssel für den Zugriff auf die Daten erhalten. Beachten Sie daher zum optimalen Schutz folgende Tips:

- Trennen Sie PGPdisk-Volumes stets, wenn Sie Ihren Computer verlassen. Auf diese Weise wird der Inhalt sicher in der verschlüsselten, zum Volume gehörigen Datei gespeichert, bis Sie erneut darauf zugreifen.
- Verwenden Sie einen Bildschirmschoner mit einer Paßwort-Option, damit es für andere schwieriger ist, sich Zugang zu Ihrem Rechner zu verschaffen oder Einsicht auf Ihren Bildschirm zu nehmen, wenn Sie nicht an Ihrem Arbeitsplatz sind.
- Stellen Sie sicher, daß Ihre PGPdisk-Volumes nicht von anderen Computern im Netzwerk gesehen werden können. Eventuell müssen Sie dies mit den Mitarbeitern der Netzwerkverwaltung abklären. Auf die Dateien in einem verbundenen PGPdisk-Volume kann jeder zugreifen, der sie im Netzwerk sieht.
- Notieren Sie sich nie Ihre Paßphrasen. Wählen Sie etwas, an das Sie sich erinnern können. Wenn Sie Schwierigkeiten haben, sich an Ihre Paßphrase zu erinnern, helfen Sie Ihrem Gedächtnis mit einem Poster, einem Lied, einem Gedicht oder einem Witz auf die Sprünge. *Notieren Sie jedoch nie Ihre Paßphrasen*.
- Wenn Sie PGPdisk zu Hause verwenden und auch andere Personen auf Ihren Computer Zugriff haben, können diese wahrscheinlich Ihre PGPdisk-Dateien anzeigen. Solange Sie die PGPdisk-Volumes trennen, wenn Sie sie nicht mehr verwenden, kann kein anderer deren Inhalt lesen.
- Wenn ein anderer Benutzer über physischen Zugriff auf Ihren Rechner verfügt, kann er sowohl Ihre PGPdisk-Dateien als auch alle anderen Dateien und Volumes löschen. In diesem Fall sollten Sie entweder Sicherheitskopien von Ihren PGPdisk-Dateien erstellen oder sie auf externen Medien speichern, zu denen sich kein anderer physischen Zugang verschaffen kann.
- Denken Sie daran, daß Kopien Ihres PGPdisk-Volumes denselben geheimen Schlüssel wie das Original verwenden. Wenn Sie eine Kopie Ihres Volumes mit einem anderen Benutzer austauschen und Sie beide Ihre Master-Paßwörter ändern, verwenden Sie und die andere Person immer noch denselben Schlüssel für die Verschlüsselung der Daten. Obwohl es nicht einfach ist, den Schlüssel wiederherzustellen, ist dies nicht unmöglich.

PGPnet Virtual Private Networking

8

In diesem Kapitel werden das Modul PGPnet und seine Funkionen beschrieben sowie Hinweise zur Benutzung von PGPdisk gegeben. In diesem Kapitel wird ebenfalls der Begriff Virtual Private Networks (virtuelle private Netzwerke) erläutert.

Durch moderne Technologien wurde der Arbeitsplatz als solcher revolutioniert. Die zahlreichen innerbetrieblichen Memos und Berichte, die bisher auf dem Postweg versandt wurden und meist erst nach einigen Tagen beim Empfänger ankamen, werden heutzutage elektronisch verschickt und gehen innerhalb von Sekunden an ihrem Bestimmungsort ein. Angestellte, die von zu Hause aus arbeiten oder beruflich viel unterwegs sind, können nun per Telefon Daten an ihre jeweilige Arbeitsstelle übertragen und von dort abfragen.

Zwei „Nebenerscheinungen“ dieser Fortschritte sind zu einem eine größere Gefährdung der Daten bei der Übertragung über Telefonleitungen und zum anderen ein erhöhter Kostenaufwand für Telefondienstleistungen. Durch die Nutzung des Internets konnten viele Unternehmen ihre Kosten senken, mit dem Sicherheitsaspekt gab es jedoch weiterhin Schwierigkeiten.

Diese Probleme können jedoch glücklicherweise durch allerneueste Technologien behoben werden. Durch *Virtual Private Networks (VPNs)* können Unternehmen Daten auf sichere Weise über das Internet übertragen. Hierdurch wird die Gefährdung der Daten bei der Übertragung vermindert, und bei Telefondienstleistungen können drastische Einsparungen erzielt werden.

Was ist ein VPN?

Über ein VPN können Unternehmen ihre Anwendungen und Daten sämtlichen firmenweiten Benutzern und Zweigstellen auf sichere Weise zur Verfügung stellen. Dabei spielt es keinerlei Rolle, wo auf der Welt sich diese befinden, solange sie über einen Internetzugang verfügen. VPNs ermöglichen sichere Verbindungen zwischen zwei Rechnern, zwischen einem Rechner und einem Teilnetz oder zwischen zwei Teilnetzen.

Hier ein Beispiel zur Veranschaulichung: Unternehmen A, dessen Firmensitz in Boston ist, hat Zweigstellen in Kalifornien, Texas und Florida. Jede dieser Zweigstellen schickt einmal pro Woche Verkaufsberichte an die Hauptverwaltung. Bevor bei Unternehmen A ein VPN eingerichtet wurde, wurden die Verkaufsberichte von den einzelnen Zweigstellen per Telefon an die Hauptverwaltung übertragen. Nach der Einrichtung des VPNs konnten die Zweigstellen über ihren lokalen *Internetdienstanbieter (Internet Service Provider, ISP)* auf das Internet zugreifen, über das Internet auf das Intranet der Hauptverwaltung zugreifen und Daten über das VPN übertragen. Wo zuvor ein teures Ferngespräch notwendig war, ist nun ein Ortsgespräch ausreichend. Es gibt noch einen weiteren großen Pluspunkt – einen erhöhten Grad an Sicherheit und Privatsphäre. Die Daten sind während der Übertragung vom Absender an den Empfänger – über den ISP, das Internet bis zu möglichen Routern und Gateways – stets geschützt. Ein VPN bietet Benutzern Privatsphäre, Integrität und Ursprungsauthentisierung ihrer Daten.

Unternehmen, die VPNs einrichten, stellen auf diese Weise vertrauenswürdigen Firmen und Personen (z. B. Lieferanten und Beratern) ihre internen Daten zur Verfügung. Durch diese Vorgehensweise sparen sämtliche Beteiligte Zeit, Geld und andere Ressourcen. Ein VPN, das in Verbindung mit einer Firewall verwendet wird, ermöglicht es nicht nur berechtigten Benutzern, Daten zu versenden und zu empfangen, sondern verwehrt Unbefugten auch den Zugang zu Ihrem Intranet. (Eine *Firewall* steuert, welche Rechner für einen externen Host im Intranet des Unternehmens angezeigt werden. Außerdem wird hierdurch festgelegt, auf welche Dienste der Host zugreifen kann. Über eine Firwall wird außerdem gesteuert, welche Rechner für einen Host im Intranet des Unternehmens über das Internet angezeigt werden, und auf welche Dienste der Host Zugriff hat.)

Zusätzlich zu den Vorteilen erhöhter Sicherheit und reduzierter Kosten wird durch VPNs ebenfalls verhindert, daß Internetdienstanbieter (ISPs) Klartextnachrichten (d. h. unverschlüsselte Nachrichten) lesen. Außerdem werden Sie verstärkt vor internen Angriffen geschützt.

Funktionsweise von VPNs

Durch ein VPN wird das *Intranet* (also das interne Netzwerk) eines Unternehmens internetweit erweitert (durch die Erstellung eines sicheren privaten *Tunnels*). Funktionsweise: Ein VPN setzt ein Tunneling-Protokoll (z. B. Internet Protocol Security (IPsec)) sowie Verschlüsselungsverfahren ein, um Daten von dem Zeitpunkt, zu dem sie vom Absender verschickt werden, bis zu dem Zeitpunkt, zu dem sie beim vorgesehenen Empfänger eingehen, zu schützen.

Was muß geschützt werden?

Es ist von größter Wichtigkeit, daß Sie möglichst viele verschiedene Informationen schützen, die auf Ihrem Computer gespeichert sind oder an Dritte übertragen werden (z. B. Banken, Clients, Geschäftspartener, sowie Finanzbehörden). Beispiele hierfür sind:

- Angestelltenunterlagen
- Unterlagen der Lohnbuchhaltung
- Benutzerpaßwörter und -konten
- Verkaufsunterlagen
- Produktforschungs- und Produktentwicklungsdateien
- Quellcodedateien

Weitere Sicherheitsaspekte beziehen sich unter anderem auf Hacker, die Zugriff auf Ihr Intranet haben und eine Vielzahl verschiedener Angriffe durchführen. Beispiele hierfür sind:

- Löschen oder Herunterladen wichtiger Dateien
- Lesen von E-Mails
- Computer zum Abstürzen bringen
- Autorisierte Benutzer vom Zugriff auf Computer abhalten (Sevicever-weigerung)
- Pakete von der Festplatte kopieren, um an Informationen wie Benutzerkennwörter zu gelangen.

Die Sicherheit Ihrer Daten, Geräte und Netzwerke ist sehr wichtig. Mit PGPnet wird eine Vielzahl von Bedrohungen, denen Netzwerke fortwährend ausgesetzt sind, ausgeschaltet.

Funktionen von PGPnet

Die Anwendung PGPnet enthält folgende Funktionen:

- Konfigurationsassistent, mit dem Sie die Hosts, Gateways und Teilnetze konfigurieren können, mit denen Sie auf sichere Weise kommunizieren können.
- Sichere Peer-To-Peer-Kommunikation – es ist kein Zwischen-Gateway erforderlich.
- Leicht verständliche Benutzeroberfläche.
- Liste aller aktiven PGPnet Sicherheitsverknüpfungen auf einen Blick. (Eine *Sicherheitsverknüpfung (Security Association, SA)* enthält Informationen, die beschreiben, auf welche Weise zwei Rechner miteinander kommunizieren.)
- Automatische Neuverschlüsselung (d. h. Initialisierung und Abstimmung) auslaufender Sicherheitsverknüpfungen.
- Einen Profi-Modus, mit dem Benutzer, die über ausreichende Kenntnisse bezüglich der Verwendung von PGPnet verfügen, den Konfigurationsassistenten umgehen können.
- Für Diagnosezwecke bestimmte Protokollinformationen werden in einem gut lesbaren Format angezeigt – das Durchsuchen von Protokolldateien erübrigt sich.

Was ist PGPnet?

PGPnet, ein *Virtual Private Network (VPN)*, ist eine einfach zu verwendende Verschlüsselungsanwendung, mit der Sie sicher und kostengünstig mit anderen PGPnet Benutzern kommunizieren können. Es baut auf Standards auf, basiert auf den Protokollen IETF IPsec und IETF IKE (Internet Key Exchange) und erweitert das IKE-Protokoll so, daß die Authentisierung von Schlüsseln in PGP unterstützt wird.

PGPnet gewährleistet die Geheimhaltung, Integrität und Echtheit von Informationen, die von einem PGPnet-Host an einen sicheren Host, ein Gateway oder Teilnetz gesendet werden.

- Ein *sicherer Host* ist ein Rechner, auf dem PGPnet oder eine andere IPsec-kompatible, Peer-To-Peer-fähige Client-Software (d. h. Software, die es Hosts ermöglicht, direkt miteinander zu kommunizieren) ausgeführt wird.
- Ein *sicheres Gateway* ist ein Firewall- oder anderer Gateway-Rechner, durch den Pakete für autorisierte Benutzer geleitet werden. „Autorisiert“ bedeutet in diesem Fall, daß das Zertifikat oder die gemeinsame Paßphrase der Client-Software so konfiguriert ist, daß Sie am Gateway angenommen wird. (Wenn Sie PGPnet verwenden, können Sie mit einem Host wahlweise über Ihren PGP-Schlüssel, ein X.509-Zertifikat oder eine gemeinsame Paßphrase kommunizieren).
- Ein *sicheres Teilnetz* besteht aus maximal 254 vernetzten Computern, auf denen in der Regel PGPnet oder eine kompatible Client-Software ausgeführt wird. In einem sicheren Teilnetz können Sie oder Ihr Administrator eine Anzahl von Computern im selben IP-Adreßbereich angeben, von denen Sie wissen, daß sie IPsec-kompatibel sind. Beachten Sie, daß sich sichere Teilnetze nicht hinter Gateways befinden müssen.

TIP: Wenn ein Teilnetz viele sichere Hosts und wenige unsichere Hosts aufweist, sollten Sie das Teilnetz als sicheres Teilnetz einrichten und anschließend für jede Ausnahme unsichere Hosts hinzufügen.

Sie können mit PGPnet-Benutzern in Ihrem persönlichen bzw. im firmeneigenen Intranet sowie mit anderen PGPnet-Benutzern weltweit kommunizieren. Gateways, Teilnetze und Hosts, die von Ihnen (bzw. gegebenenfalls dem PGPnet-Administrator) als sicher gekennzeichnet wurden, stehen Ihnen für die Kommunikation zur Verfügung. Mit PGPnet können Sie Daten auf sichere Weise über das Internet oder andere nicht vertrauenswürdige Netzwerke versenden.

Was ist eine Sicherheitsverknüpfung?

Bei der erstmaligen Kommunikation zwischen einem lokalen und einem entfernten Rechner führt PGPnet eine Internet Key Exchange (IKE)-Abstimmung durch und erstellt eine Sicherheitsverknüpfung.

- Bei der *IKE-Abstimmung* vereinbaren die beiden Rechner, wie sie miteinander kommunizieren. Hierbei werden beispielsweise Verschlüsselungstyp, Dauer der Sicherheitsverknüpfung und Authentisierungsmethode festgelegt.
- Die resultierende *Sicherheitsverknüpfung (SA)* enthält Informationen, aus denen hervorgeht, wie die beiden Rechner miteinander kommunizieren.

PGPnet protokolliert und überwacht sämtliche SAs, die Ihr Rechner initialisiert und die von anderen Rechnern mit Ihrem Rechner initialisiert werden. Wenn eine von Ihrem Rechner initialisierte SA in naher Zukunft ungültig wird, initialisiert PGPnet eine weitere SA mit dem entfernten Host. Sie können sämtliche aktiven SAs auf der Registerkarte **Status** von PGP anzeigen lassen. Weitere Informationen zur Registerkarte **Status** finden Sie unter „Registerkarte „Status“ anzeigen“ auf Seite 171.

Die beiden Modi von PGPnet: Tunnel-Modus und Transport-Modus

PGPnet verwendet den Tunnel-Modus zur Kommunikation mit Hosts und Teilnetzen hinter einem sicheren Gateway und den Transport-Modus für die Peer-To-Peer-Kommunikation zwischen zwei sicheren Hosts, zwischen denen sich kein Gateway befindet.

Was ist der Tunnel-Modus?

Wenn der Rechner, auf dem PGPnet ausgeführt wird, Pakete über ein sicheres Gateway an einen Host oder ein Teilnetz hinter einem Gateway sendet, spricht man von Tunneling. (Im Fenster „Hosts“ von PGPnet ist der Ziel-Host bzw. das Ziel-Teilnetz unterhalb des Gateways eingerückt dargestellt.) Bei Paketen, die an Hosts dieses Typs gesendet werden, wird *Tunneling* durchgeführt. Mit anderen Worten wird das gesamte an das Ziel gesendete Paket physisch in ein anderes Paket plaziert, verschlüsselt und an das Gateway gesendet.

Was ist der Transport-Modus?

PGP ist vollständig fähig, Peer-To-Peer-Kommunikationen durchzuführen. Zwei Rechner, auf denen PGP ausgeführt wird, können ungeachtet ihres jeweiligen Standorts im Internet auf sichere Weise miteinander kommunizieren. Ein sicheres Gateway ist nicht erforderlich. Diese Art der Kommunikation wird als *Transport-Modus* bezeichnet. Es gibt kein sicheres Gateway und keine Firewall. Pakete werden auf sichere Weise vom Quellrechner auf den Zielrechner übertragen. In diesem Modus werden Pakete verschlüsselt und authentisiert.

Wie kommuniziert PGPnet mit sicheren und unsicheren Hosts?

In den folgenden Abschnitten wird beschrieben, wie PGPnet mit Hosts kommuniziert:

Sichere Hosts ohne sicheres Gateway zwischen den Hosts – PGPnet-Pakete werden für ihr Ziel verschlüsselt und authentisiert (Transport-Modus).

Sicherer Host hinter sicherem Gateway – PGPnet verschlüsselt jedes Paket für dessen endgültiges Ziel und führt anschließend das Tunneling der einzelnen Pakete an das Gateway durch. Durch diese Funktion wird sichergestellt, daß das Gateway nicht von unbefugten Dritten zu Abhörzwecken genutzt wird (Tunnel-Modus).

Unsicherer Host hinter sicherem Gateway – PGPnet führt das Tunneling von Paketen an das Gateway durch, und das Gateway leitet die Pakete an das endgültige Ziel weiter (Tunnel-Modus).

Verwendung von PGPnet?

Wenn es bei Ihnen einen PGPnet-Administrator gibt, ist PGPnet bei der Installation möglicherweise bereits konfiguriert.

Falls es bei Ihnen keinen PGPnet-Administrator gibt bzw. falls PGPnet nicht vorkonfiguriert war, installieren Sie PGPnet, wählen Ihren Authentisierungsschlüssel bzw. Ihr Authentisierungszertifikat (oder beides) aus und konfigurieren im Feld des Assistenten zum Hinzufügen von Hosts die erforderlichen Hosts, Gateways und Teilnetze für PGP.

Wenn PGPnet konfiguriert wurde, wird die Software im Hintergrund ausgeführt. Jedesmal, wenn Sie mit einem anderen Rechner kommunizieren möchten (z. B. über E-Mail oder Webbrowser), prüft PGPnet, ob eine aktive SA für den Rechner vorhanden ist.

- Wenn dies der Fall ist, erfolgt die Kommunikation in PGPnet gemäß der Bedingungen der vorhandenen SA.
- Falls keine SA für den Zielrechner vorhanden ist und der Rechner als sicher gilt, initialisiert PGPnet eine IKE-Abstimmung, bei der eine SA erstellt wird, und führt Ihre Kommunikationsvorgänge durch.
- Falls keine SA für den Zielrechner vorhanden ist und der Rechner nicht als sicher gilt, werden die Kommunikationsvorgänge gemäß der auf der Registerkarte „Allgemein“ vorgenommenen Sicherheitseinstellungen durchgeführt (**Ansicht–>Optionen–>Allgemein**). Mit anderen Worten: Falls sowohl die Option **Sichere Kommunikation mit allen Hosts fordern** als auch **Kommunikation mit unkonfigurierten Hosts zulassen** aktiviert ist, ist lediglich die sichere Kommunikation zulässig.

HINWEIS: Dies birgt ein potentielles Sicherheitsrisiko in sich, da hierbei die Kommunikation mit DNS-, DHCP- bzw. WINS-Servern nur möglich ist, wenn PGPnet auf ihnen ausgeführt wird oder sie ausdrücklich als unsichere Hosts definiert wurden.

Bitte beachten Sie folgendes:

- Wenn Sie Ihren Rechner neu starten oder ihn in den Standby-Modus versetzen, werden sämtliche SAs beendet. Folglich ist für sämtliche Rechner, mit denen Sie seit dem letzten Neustart nicht kommuniziert haben, eine neue IKE-Abstimmung erforderlich.
- Wenn Sie sich bei PGPnet abmelden, werden unter Umständen SAs ungültig, und es können möglicherweise keine neuen erstellt werden, bis Sie sich wieder bei PGPnet anmelden.
- PGPnet prüft stets, ob SA-Anforderungen von anderen Rechnern vorliegen.

Netzwerkeinstellungen in der Systemsteuerung ändern

PGPnet ist an eine spezielle Netzwerkkarte gebunden und sichert diese ab. Wenn Sie die Netzwerkeinstellungen in der Systemsteuerung ändern, überprüft PGPnet automatisch die Bindungen, und Sie werden aufgefordert, das System neu zu starten. Der Neustart ist erforderlich, um die vorschriftsmäßige Funktionsweise von PGPnet sicherzustellen.

PGPnet-Anwendung starten

So starten Sie PGPnet

1. Wählen Sie die Optionsfolge **Start–>Programme–>PGP–>PGPnet**.

   Oder

   Starten Sie die Anwendung über das PGPtray-Symbol in der Task-Leiste von Windows (**PGPtray–> PGPnet–>Status, Protokoll** oder **Hosts**.

   Durch jeden dieser Schritte wird das PGPnet-Fenster geöffnet (siehe Abbildung 8-1).

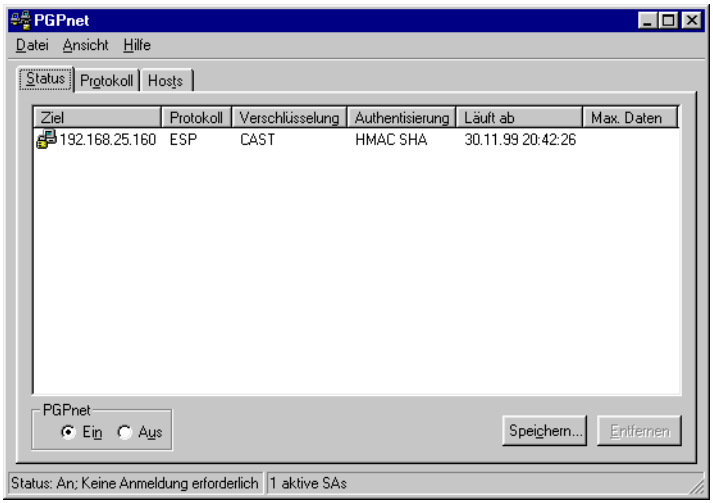


Abbildung 8-1. Das PGPnet-Fenster

Standardmäßig ist PGPnet aktiviert. Mit den Optionsfeldern links unten im Fenster können Sie PGPnet aktivieren bzw. deaktivieren. Wenn PGPnet jedoch deaktiviert ist und der Rechner neu gestartet wird, ist PGPnet nach dem Neustart deaktiviert. Weitere Informationen finden Sie unter „PGPnet deaktivieren“ auf Seite 170 und unter „PGPnet aktivieren“ auf Seite 170.

Authentisierungsschlüssel bzw. -zertifikat auswählen

Bevor Sie mit PGPnet arbeiten können, müssen Sie den Schlüssel und / oder das X.509-Zertifikat auswählen, der bzw. das für Authentisierungszwecke verwendet wird. Falls kein Schlüssel oder X.509-Zertifikat vorhanden ist, lesen Sie unter „Schlüssel erstellen und austauschen“ auf Seite 23 nach.

So wählen Sie Ihren Authentisierungsschlüssel und/oder Ihr -zertifikat aus

1. Wählen Sie im PGPnet-Fenster das Menü **Ansicht,** und klicken Sie auf **Optionen** (Sie können auch **PGPnet** in **PGPtray** auswählen und auf **Optionen** klicken).
2. Klicken Sie auf die Registerkarte **Authentisierung** (siehe Abbildung 8-2 auf Seite 167).
3. Wählen Sie den Schlüssel und / oder das Zertifikat aus, der bzw. das zur Authentisierung verwendet wird (klicken Sie auf **Schlüssel auswählen** oder auf **Zertifikat auswählen**). Beachten Sie, daß der Schlüssel bzw. das Zertifikat Bestandteil eines Schlüsselpaares sein muß. Sie müssen über den privaten Schlüssel verfügen. Der ausgewählte Schlüssel bzw. das ausgewählte Zertifikat wird im Feld **PGP-Authentisierung** oder **X.509-Authentisierung** angezeigt.
4. Klicken Sie auf **OK**. In einem Dialogfeld werden Sie zur Eingabe der Paßphrase für den ausgewählten Schlüssel aufgefordert.
5. Geben Sie sie ein, und klicken Sie anschließend auf **OK**.

WICHTIG: Wenn Sie derzeit eine VPN-Verbindung mit einem anderen PGPnet-Host aufbauen und PGPkeys zu Authentisierungszwecken verwenden, müssen beide Seiten denselben Typ von PGP-Schlüsseln verwenden. Wenn eine Seite der Verbindung einen RSA-Schlüssel und die andere einen Diffie-Hellman-Schlüssel verwendet, kann keine SA abgestimmt werden.

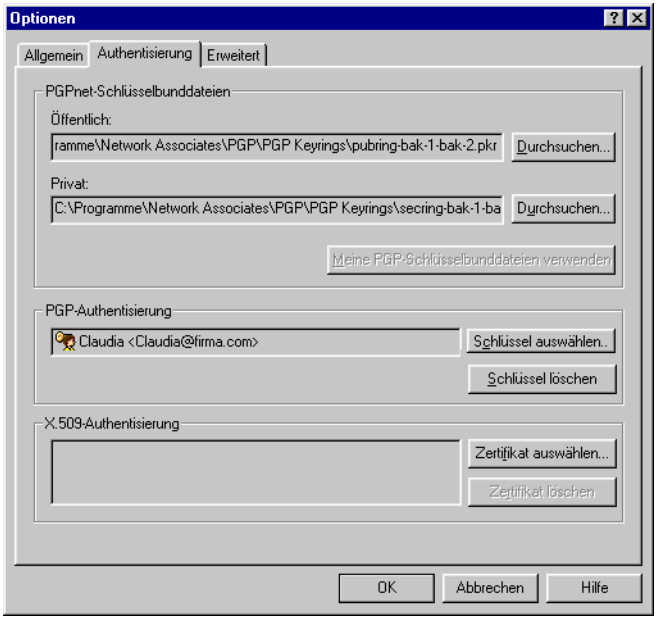


Abbildung 8-2. Die Registerkarte „Authentisierung“

Das PGPnet-Fenster auf einen Blick

Das PGPnet-Fenster enthält drei Menüs:

- **Datei** (**Beenden**)
- **Ansicht** (**Status**, **Protokoll**, **Hosts** und **Optionen**)
- **Hilfe** (**Inhalt** und **Info**)

Das PGPnet-Fenster enthält drei Registerkarten:

- Registerkarte **Status** – Hier können Sie den Status vorhandener SAs überprüfen (siehe „Registerkarte „Status“ anzeigen“ auf Seite 171).
- Registerkarte **Protokoll** – Hier können Sie Protokolleinträge zu Diagnosezwecken überprüfen (siehe „Registerkarte „Protokoll“ anzeigen“ auf Seite 173).
- Registerkarte **Hosts** – Hier können Sie der Host-Liste in PGPnet Einträge hinzufügen, Einträge bearbeiten oder entfernen sowie SAs erstellen und beenden (siehe „Registerkarte „Hosts“ verwenden“ auf Seite 174).

Standardmäßig ist PGPnet aktiviert. Mit den Optionsfeldern links unten im Fenster können Sie PGPnet aktivieren bzw. deaktivieren.

Am unteren Rand des PGPnet-Fensters, in der Statusleiste, werden Meldungen angezeigt, die sich auf den Status von PGPnet links und auf die Anzahl der aktiven SAs rechts beziehen. Folgende Meldungen können in der Statusleiste angezeigt werden:

Tabelle 8-1. Statusmeldungen

Meldung	Beschreibung
Status: Ein; Benutzer angemeldet	PGPnet ist aktiviert, Benutzer ist angemeldet
Status: Ein; Benutzer abgemeldet	PGPnet ist aktiviert, Benutzer ist abgemeldet
Status: Keine Anmeldung erforderlich	Trifft zu, wenn kein Authentisierungsschlüssel eingestellt wurde
Status: Aus	PGPnet wurde vom Benutzer deaktiviert
Treiber nicht installiert	Der PGPnet-Treiber reagiert nicht auf den Service. Starten Sie Ihr System neu. Falls der Treiber daraufhin noch immer nicht reagiert, installieren Sie PGPnet erneut. Falls diese Meldung von PGPnet weiterhin angezeigt wird, wenden Sie sich an den technischen Kundendienst von NAI.
Service wird nicht ausgeführt	Der PGPnet-Service wird nicht ausgeführt. Starten Sie Ihr System neu. Falls diese Meldung von PGPnet weiterhin angezeigt wird, installieren Sie PGPnet erneut. Wenn sich das Problem hierdurch nicht beheben läßt, wenden Sie sich an den technischen Kundendienst von NAI.
Service antwortet nicht	Der PGPnet-Service wird zwar ausgeführt, antwortet jedoch nicht auf Meldungen der Anwendung. Starten Sie Ihr System neu. Falls diese Meldung von PGPnet weiterhin angezeigt wird, installieren Sie PGPnet erneut. Wenn sich das Problem hierdurch nicht beheben läßt, wenden Sie sich an den technischen Kundendienst von NAI.

PGPnet von PGPtray aus verwenden

Mit dem PGPnet-Untermenü in PGPtray in der Task-Leiste von Windows können Sie folgende Tasks durchführen:

Wenn Sie folgenden Task durchführen möchten, ...	Gehen Sie wie folgt vor...
Die Registerkarte „Protokoll“ anzeigen	Klicken Sie auf das PGPtray-Symbol, wählen Sie „PGPnet“, und klicken Sie auf **Protokoll**.
Die Registerkarte „Status“ anzeigen	Klicken Sie auf das PGPtray-Symbol, wählen Sie „PGPnet“, und klicken Sie auf **Status**.
Die Registerkarte „Hosts“ anzeigen	Klicken Sie auf das PGPtray-Symbol, wählen Sie „PGPnet“, und klicken Sie auf **Hosts**.
Das Fenster „Optionen“ anzeigen	Klicken Sie auf das PGPtray-Symbol, wählen Sie „PGPnet“, und klicken Sie auf **Hosts**.
Bei PGPnet anmelden	Klicken Sie auf das PGPtray-Symbol, wählen Sie „PGPnet“, und klicken Sie auf **Anmelden**. Diese Option ist grau hinterlegt, wenn kein Authentisierungsschlüssel ausgewählt wurde.
.Bei PGPnet abmelden	Klicken Sie auf das PGPtray-Symbol, wählen Sie „PGPnet“, und klicken Sie auf **Abmelden**. Diese Option ist grau hinterlegt, wenn kein Authentisierungsschlüssel ausgewählt wurde.
Beenden	Klicken Sie auf das PGPtray-Symbol, und wählen Sie **Beenden**.

PGPtray-Symbol

Je nach Farbe des PGPtray-Symbols können Sie feststellen, ob PGPnet deaktiviert oder nicht installiert (graues Schloß), installiert und aktiviert (gelbes Schloß in einem Netzwerk) oder zwar installiert ist, aber nicht funktioniert (gelbes Schloß in einem Netzwerk mit rotem Ausrufezeichen in gelbem Kreis). Wenn Sie den Mauszeiger über das **PGPtray**-Symbol bewegen, wird hierdurch eine QuickInfo angezeigt, aus der der Status von PGPnet hervorgeht. Hier werden auch Fehlermeldungen erläutert, beispielsweise die Meldung „Service nicht installiert“

PGPnet deaktivieren

In einigen Situation ist es empfehlenswert, PGPnet zu deaktivieren, beispielsweise zu Diagnosezwecken. Wenn PGPnet deaktiviert wird, erfolgen sämtliche Kommunikationsvorgänge mit sämtlichen Rechnern auf unveränderte und unsichere Weise.

Wenn Sie PGPnet deaktivieren möchten, klicken Sie im PGPnet-Fenster auf **Aus** (siehe Abbildung 8-3 auf Seite 170).

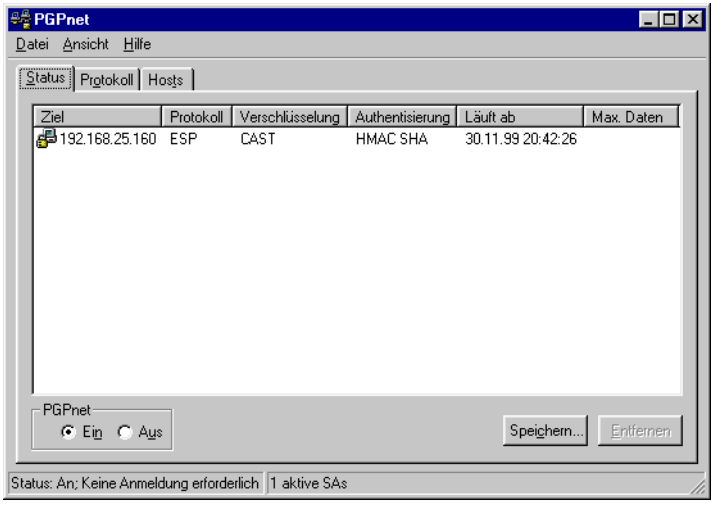


Abbildung 8-3. PGPnet-Fenster

PGPnet aktivieren

Wenn Sie PGPnet aktivieren möchten, klicken Sie im PGPnet-Fenster auf **Ein** (siehe Abbildung 8-3 auf Seite 170).

PGPnet beenden

Wählen Sie im PGPnet-Fenster im Menü „Datei“ den Befehl **Beenden.**
Sie können auch in der rechten oberen Ecke des PGPnet-Fensters auf das **X** klicken oder auf das PGPtray-Symbol und anschließend auf **Beenden**.

Beachten Sie folgendes: Durch das Beenden von PGPnet wird weder der PGPnet-Service deaktiviert noch werden SAs beendet.

PGPnet verwenden

Wenn PGPnet aktiviert ist, wird die Anwendung im Hintergrund ausgeführt. Wenn Sie mit einem Rechner kommunizieren möchten, verwenden Sie hierzu wie gewohnt Ihre jeweilige Software (z. B. E-Mail oder Webbrowser). PGPnet bewertet jeden Kommunikationsvorgang und nimmt Verschlüsselung und Tunneling wie erforderlich vor.

Registerkarte „Status“ anzeigen

Auf der Registerkarte **Status** im PGPnet-Fenster werden aktive PGPnet-SAs aufgeführt und gegebenenfalls der Ablauf deren Gültigkeit (siehe Abbildung 8-4 auf Seite 172). Eine SA wird unter Umständen beendet, wenn ihr Umfang einen bestimmten Wert in Byte erreicht (es werden z. B. 4 MB Daten über die SA übertragen) bzw. wenn ein bestimmter Zeitraum verstrichen ist. Die Dauer einer SA wird bei deren Initialisierung abgestimmt. Bei der Abstimmung der SA wird ein Ablaufwert für die Gültigkeit festgelegt. Wenn die SA diesen Ablaufwert erreicht und ungültig wird, wird automatisch eine neue SA erstellt. (Der Ablaufwert der Gültigkeit für die SA kann vom Benutzer konfiguriert werden; weitere Informationen finden Sie unter „Schlüsselgültigkeitswerte festlegen“ auf Seite 197.)

- Falls von Ihrem Rechner eine SA initialisiert wurde, die demnächst abläuft, initialisiert PGPnet automatisch die Abstimmung einer neuen SA als Ersatz für die ablaufende SA. Folglich kann es vorkommen, daß auf der Registerkarte **Status** zeitweise zwei SAs für denselben Rechner angezeigt werden.
- Wenn Sie eine SA mit einem anderen Host einrichten, verwendet PGPnet den strikteren der beiden Ablaufwerte. Folglich läuft eine SA möglicherweise ab, bevor der von Ihnen festgelegte Ablaufhöchstwert erreicht wurde.

In der folgenden Tabelle werden die Informationen erläutert, die auf der Registerkarte **Status** in PGPnet für die einzelnen SAs angezeigt werden:

Spalte	Beschreibung
Ziel	IP-Adresse von Ziel-Host oder -Gateway.
Protokoll	Typ des abgestimmten Protokolls, beispielsweise AH, ESP oder IPCOMP.
Verschlüsselung	Typ des abgestimmten Verschlüsselungsalgorithmus. Falls es sich um eine reine Authentisierungs-SA handelt, ist diese Spalte möglicherweise leer. Zu den Verschlüsselungstypen zählen TripleDES bzw. CAST.

Spalte	Beschreibung
Authentisierung	Typ des abgestimmten Authentisierungssalgorithmus. Diese Spalte ist möglicherweise leer oder enthält eine der folgenden Typenbezeichnungen: HMAC MD5 oder HMAC SHA. Falls sowohl ESP- als auch AH-Protokolle verwendet werden, weist diese Spalte eventuell zwei Einträge auf.
Läuft ab	Datum und Uhrzeit für die Gültigkeit der SA (MM/TT/JJ hh:mm:ss). Falls der Ablaufzeitpunkt der SA auf MB und nicht auf einem Zeitwert basiert, wird hier „Nie“ angezeigt.
Max. Daten	Maximale Anzahl an MB, die von der SA vor deren Ablauf übertragen werden.

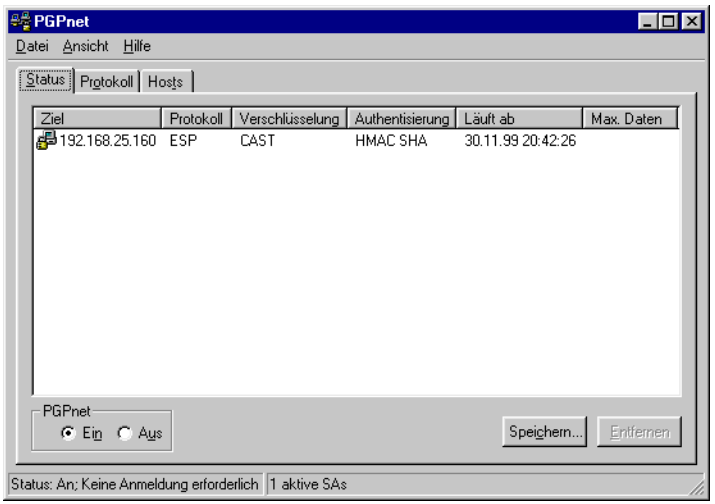


Abbildung 8-4. Die Registerkarte „Status“

Mit der Funktion **Speichern** können Sie eine Liste aktiver SAs zu Diagnosezwecken speichern. Wenn Sie die Liste der SAs in einer Datei im Textformat (durch Tabs getrennt) speichern möchten, klicken Sie auf **Speichern**.

Mit der Funktion **Entfernen** können Sie eine SA entfernen. Das Entfernen einer SA empfiehlt sich, wenn Sie sie nicht mehr für sicher halten, wenn Sie wissen, daß der Ziel-Host ausgefallen ist, oder wenn Sie aus einem anderen Grund der Ansicht sind, daß die Verbindung nicht mehr aufrechterhalten werden sollte.

Mit **Ein** und **Aus** können Sie PGPnet aktivieren bzw. deaktivieren.

Sie können auch auf die Registerkarte **Protokoll** klicken, um zuletzt gespeicherte Protokolleinträge einzusehen.

Registerkarte „Protokoll“ anzeigen

Auf der Registerkarte **Protokoll** werden System- und Servicefehler angezeigt, einschließlich des Zeitpunkts, zu dem sie aufgetreten sind (Datum und Uhrzeit); außerdem wird eine Beschreibung des jeweiligen Fehlers angezeigt. Diese Informationen unterstützen Sie bei der Behebung auftretender Probleme (siehe Abbildung 8-5 auf Seite 173).

Mit den Kontrollkästchen neben **Ereignisse anzeigen** können Sie die anzuzeigenden Ereignistypen auswählen: Service, IKE, IPsec, PGP und / oder System. Um PGPnet anzuweisen, eine bestimmte Art von Ereignis anzuzeigen, aktivieren Sie das Kontrollkästchen neben dem jeweiligen Ereignistyp.

Mit **Speichern** können Sie aktuelle Protokollinformationen in einer Textdatei speichern.

Mit **Löschen** können Sie aktuelle Protokollinformationen aus der Protokolldatei und vom Bildschirm löschen.

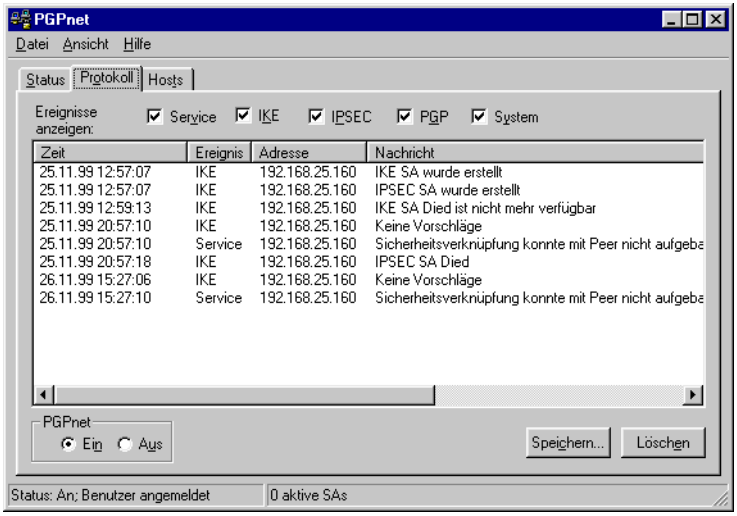


Abbildung 8-5. Die Registerkarte „Protokoll“

In der folgenden Tabelle werden die Informationen erläutert, die PGPnet zu den einzelnen Protokolleinträgen anzeigt:

Spalte	Beschreibung
Zeit	Datum und Uhrzeit, zu der der Fehler auftrat (Anzeige im Format MM/TT/JJ hh:mm:ss)
Ereignis	Typ des Ereignis-, Service-, IKE-, IPsec-, PGP- bzw. Systemfehlers
Adresse	IP-Adresse des entfernten Hosts.
Nachricht	Text, mit dem der Fehlertyp beschrieben wird (z. B. Sicherheitsverknüpfung konnte mit Peer nicht aufgebaut werden).

Registerkarte „Hosts“ verwenden

Auf der Registerkarte **Hosts** werden sichere Gateways, Teilnetze und Hosts angezeigt. Wenn links neben einem Element ein Pluszeichen (+) angezeigt wird, klicken Sie darauf, um die Anzeige zu erweitern und weitere mit dem Element verbundene Einträge einzusehen (siehe Abbildung 8-7 auf Seite 180).

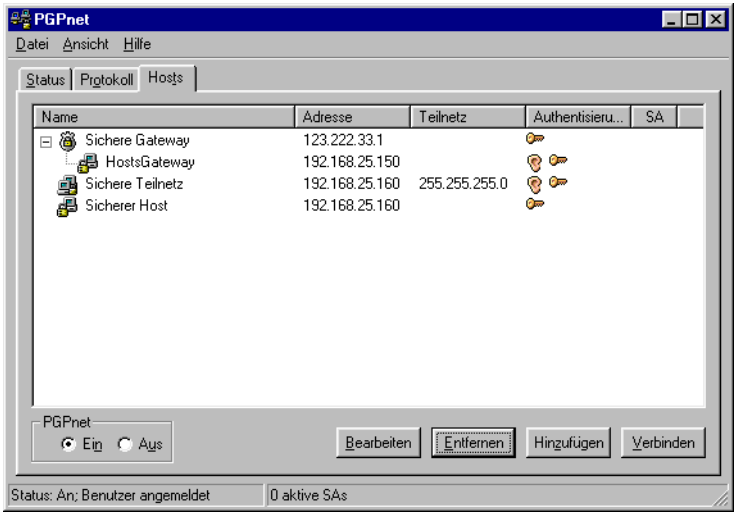


Abbildung 8-6. Die Registerkarte „Hosts“

In der folgenden Tabelle werden die Informationen erläutert, die zu den einzelnen Elementen angezeigt werden.

Spalte	Beschreibung
Name	Bezeichnender Name des Host-, Teilnetz- oder Gateway-Eintrags.
Adresse	IP-Adresse von Host, Teilnetz oder Gateway.
Teilnetz	Falls es sich bei dem Host-Eintrag um ein Teilnetz handelt, wird in diesem Feld die Teilnetz-Maske angezeigt. Andernfalls ist dieses Feld leer.
Authentisierung	Es wird ein Symbol angezeigt, aus dem der für den Host-Eintrag verwendete Authentisierungstyp hervorgeht. • Ein Schlüsselsymbol weist auf Authentisierung durch Verschlüsselungssysteme mit öffentlichen Schlüsseln hin. • Ein Zertifikatssymbol weist auf Authentisierung mit X.509-Zertifikaten hin. • Ein Ohrsymbol weist auf eine gemeinsame geheime Authentisierung hin. • Wenn keinerlei Symbol angezeigt wird, bedeutet dies, daß der Eintrag des konfigurierten Hosts unsicher ist.
SA	In dieser Spalte wird ein grüner Kreis angezeigt, wenn eine SA mit dem Host vorhanden ist. Wenn dies nicht der Fall ist, ist diese Spalte leer.

In der folgenden Tabelle werden die Schaltflächen auf der Registerkarte **Hosts** beschrieben.

Schaltfläche	Beschreibung
Bearbeiten	Zeigt die Werte für das ausgewählte Element im Dialogfeld zur Bearbeitung eines Hosts/Gateways an.
Entfernen	Entfernt den ausgewählten Host-Eintrag.
Hinzufügen	Ruft den Assistenten zum Hinzufügen eines Hosts/Gateways auf (wenn Sie sich derzeit im Profi-Modus befinden, wird hierdurch das Dialogfeld zur Bearbeitung von Hosts/Gateways aufgerufen).
Verbinden/ Trennen	Mit „Verbinden“ wird eine SA erstellt, mit „Trennen“ wird eine SA beendet.

Die Schaltflächen „Verbinden“ und „Trennen“

Richten Sie über die Schaltfläche **Verbinden** eine SA mit einem konfigurierten Host ein. Wählen Sie den Host aus, und klicken Sie anschließend auf **Verbinden**. Die Schaltfläche **Verbinden** steht nicht zur Verfügung, wenn ein unzulässiger Host-Eintrag ausgewählt wurde (z. B. wenn Sie ein sicheres Teilnetz oder einen unsicheren Host wählen, der sich nicht hinter einem Gateway befindet).

Beenden Sie über die Schaltfläche **Trennen** eine SA mit einem konfigurierten Host. Wählen Sie den Host aus, und klicken Sie anschließend auf **Trennen**.

Weitere Informationen zum Einrichten von SAs finden Sie unter „SAs einrichten“ auf Seite 176.

SAs einrichten

SAs mit PGP-Schlüsseln zur Authentisierung einrichten

Befolgen Sie die unten aufgeführten Schritte, um unter Verwendung von PGP-Schlüsseln zur Authentisierung eine SA mit einem anderen Host einzurichten.

So richten Sie eine SA unter Verwendung von PGP-Schlüsseln zur Authentisierung mit einem anderen Host ein

1. Vergewissern Sie sich, daß jedes System über eine Netzwerkverbindung verfügt.
2. Installieren Sie PGPnet auf beiden Systemen.

   Bei der Installation müssen Sie die jeweilige Netzwerkkarte für PGPnet auswählen. Falls es sich bei der Netzwerkverbindung beispielsweise um eine Ethernet-Verbindung handelt, muß PGPnet an den Ethernet-Adapter gebunden sein. Falls die Netzwerkverbindung über ein Modem hergestellt wird, muß PGPnet an die Modemkarte gebunden sein (diese wird auch als Remote Access WAN Wrapper oder DFÜ-Adapter bezeichnet).
3. Starten Sie nach der Installation von PGPnet beide Systeme neu.
4. Vergewissern Sie sich auf der Registerkarte **Authentisierung** (**Ansicht–>Optionen–>Authentisierung**) im Abschnitt **PGP-Authentisierung**, daß für jedes System ein Authentisierungsschlüssel eingestellt wurde.

5. Unterschreiben, überprüfen und tauschen Sie die öffentlichen Schlüssel aus, die von den einzelnen System zur Authentisierung verwendet werden. Weitere Informationen finden Sie im Abschnitt Kapitel 2, „PGP verwenden“.

   TIP: Aus Gründen der Skalierbarkeit sollten Sie dies mit Hilfe eines autorisierten Dritten oder einer CA durchführen.

6. Mindestens ein Benutzer muß in der Host-Liste von PGPnet einen Eintrag für das andere System erstellen. Hierzu muß Ihnen der Host-Name oder die IP-Adresse des anderen Systems bekannt sein. Vergewissern Sie sich, daß der Host im Eintrag als sicherer Host angegeben wird (wenn der Host sicher ist, zeigt das Symbol neben dem Host-Eintrag auf der Registerkarte **Hosts** einen Computer mit einem Schloß an.)

7. Wählen Sie den Host-Eintrag auf der Registerkarte **Hosts** aus, und klikken Sie anschließend auf **Verbinden**. Falls der Verbindungsaufbau erfolgreich war, wird in der SA-Spalte ein grüner Kreis angezeigt.

SAs mit X.509-Schlüsseln zur Authentisierung einrichten

Befolgen Sie die unten aufgeführten Schritte, um unter Verwendung von X.509-Schlüsseln zur Authentisierung eine SA mit einem anderen Host einzurichten.

So richten Sie eine SA unter Verwendung von X.509-Zertifikaten zur Authentisierung mit einem anderen Host ein

1. Vergewissern Sie sich, daß jedes System über eine Netzwerkverbindung verfügt.

2. Installieren Sie PGPnet auf beiden Systemen.

   Bei der Installation müssen Sie die jeweilige Netzwerkkarte für PGPnet auswählen. Falls es sich bei der Netzwerkverbindung beispielsweise um eine Ethernet-Verbindung handelt, muß PGPnet an den Ethernet-Adapter gebunden sein. Falls die Netzwerkverbindung über ein Modem hergestellt wird, muß PGPnet an die Modemkarte gebunden sein (diese wird auch als Remote Access WAN Wrapper oder DFÜ-Adapter bezeichnet).

3. Starten Sie nach der Installation von PGPnet beide Systeme neu.

4. Vergewissern Sie sich auf der Registerkarte **X.509-Authentisierung** (**Ansicht–>Optionen–>Authentisierung**) im Abschnitt **PGP-Authentisierung**, daß für jedes System ein Authentisierungszertifikat eingestellt wurde.

5. Stellen Sie sicher, daß die Root-CA für das X.509-Zertifikat vorhanden, unterschrieben und auf beiden Systemen vollständig autorisiert ist. Beide Systeme müssen dieselbe Root-CA aufweisen.

6. Mindestens ein Benutzer muß in der Host-Liste von PGPnet einen Eintrag für das andere System erstellen. Hierzu muß Ihnen der Host-Name oder die IP-Adresse des anderen Systems bekannt sein. Vergewissern Sie sich, daß der Host im Eintrag als sicherer Host angegeben wird (wenn der Host sicher ist, zeigt das Symbol neben dem Host-Eintrag auf der Registerkarte **Hosts** einen Computer mit einem Schloß).

7. Wählen Sie den Host-Eintrag auf der Registerkarte **Hosts** aus, und klikken Sie anschließend auf **Verbinden**. Falls der Verbindungsaufbau erfolgreich war, wird in der SA-Spalte ein grüner Kreis angezeigt.

SAs mit gemeinsamer geheimer Paßphrase zur Authentisierung einrichten

Befolgen Sie die unten aufgeführten Schritte, um unter Verwendung von gemeinsamen geheimen Paßphrasen zur Authentisierung eine SA mit einem anderen Host einzurichten.

So richten Sie eine SA unter Verwendung von gemeinsamen Geheimnissen zur Authentisierung mit einem anderen Host ein

> **WARNUNG:** Im Gegensatz zu den traditionellen PGP-Paßphrasen werden gemeinsame geheime Paßphrasen unverschlüsselt auf Ihrem Computer gespeichert. Dies stellt ein mögliches Sicherheitsrisiko dar. Verwenden Sie Schlüssel oder Zertifikate, um diesem Risiko vorzubeugen.

1. Vergewissern Sie sich, daß jedes System über eine Netzwerkverbindung verfügt.

2. Installieren Sie PGPnet auf beiden Systemen.

   Bei der Installation müssen Sie die jeweilige Netzwerkkarte für PGPnet auswählen. Falls es sich bei der Netzwerkverbindung beispielsweise um eine Ethernet-Verbindung handelt, muß PGPnet an den Ethernet-Adapter gebunden sein. Falls die Netzwerkverbindung über ein Modem hergestellt wird, muß PGPnet an die Modemkarte gebunden sein (diese wird auch als Remote Access WAN Wrapper oder DFÜ-Adapter bezeichnet).

3. Starten Sie nach der Installation von PGPnet beide Systeme neu.

4. Beide Benutzer müssen in der Host-Liste von PGPnet einen Eintrag für das jeweils andere System erstellen. Hierzu muß Ihnen der Host-Name oder die IP-Adresse des anderen Systems bekannt sein, und es muß eine gemeinsame geheime Paßphrase verwendet werden.

   Weitere Informationen zur Konfiguration sicherer Hosts finden Sie unter „Hosts, Teilnetze oder Gateways hinzufügen“ auf Seite 179.

5. Wählen Sie den Host-Eintrag auf der Registerkarte **Hosts** aus, und klikken Sie anschließend auf **Verbinden**. Falls der Verbindungsaufbau erfolgreich war, wird in der SA-Spalte ein grüner Kreis angezeigt.

Hosts, Teilnetze oder Gateways hinzufügen

❑ **HINWEIS:** Falls Sie zu den erfahrenen Benutzern zählen, ziehen Sie bitte „Profi-Modus: Umgehen des Assistenten, um Hosts, Gateways und Teilnetze hinzuzufügen“ auf Seite 191 zu Rate.

Bei einer Umgebung, für deren Betreuung ein PGPnet-Administrator eingesetzt wird, wurden viele der Hosts, Teilnetze und Gateways möglicherweise bereits vorkonfiguriert. Für alle vorkonfigurierten Hosts, Teilnetze und Gateways gibt es einen Eintrag in der Host-Liste von PGPnet. Mit dem Assistenten zum **Hinzufügen von Hosts** oder dem Dialogfeld **Host/Gateway** von PGPnet können Sie der Host-Liste zusätzliche Einträge hinzufügen.

Wenn Sie über keinen PGPnet-Administrator verfügen, oder bei der Installierung von PGPnet keine Hosts, Teilnetze oder Gateways konfiguriert sind, wird der Assistent zum **Hinzufügen von Hosts** automatisch beim ersten Start von PGPnet gestartet. Mit dem Assistenten können Sie die notwendigen Hosts, Teilnetze und Gateways hinzufügen.

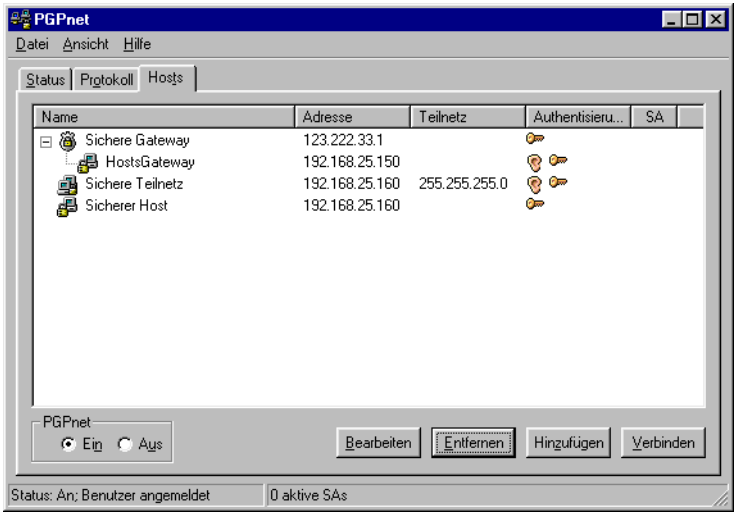


Abbildung 8-7. Die Registerkarte „Hosts“

Was Sie wissen sollten

Die folgenden Abschnitte enthalten Informationen, die Sie einem Host, einem Teilnetz oder einem Gateway hinzufügen müssen.

Tabelle 8-1. Was Sie beim Hinzufügen von Hosts, Gateways und Teilnetzen wissen müssen

Wenn Sie folgenden Task durchführen möchten:	Fertigkeiten und Kenntnisse:
Hinzufügen eines sicheren Hosts	Host-Name oder IP-Adresse
Hinzufügen eines Teilnetzes	IP-Adresse und Teilnetz-Maske
Hinzufügen eines Gateways	Host-Name oder IP-Adresse
Hinzufügen eines Hosts hinter einem konfigurierten Gateway	Host-Name oder IP-Adresse
Hinzufügen eines Teilnetzes hinter einem konfigurierten Gateway	IP-Adresse und Teilnetz-Maske

Tabelle 8-2. Wo werden Hosts, Teilnetze und Gateways hinzugefügt

Wenn Sie folgenden Task durchführen möchten:	Siehe Seite...
Hinzufügen eines Hosts	Seite 181
Hinzufügen eines Teilnetzes	Seite 183
Hinzufügen eines Gateways	Seite 184
Hinzufügen eines Hosts hinter einem konfigurierten Gateway	Seite 186
Hinzufügen eines Teilnetzes hinter einem konfigurierten Gateway	Seite 187

Hinzufügen eines Hosts

HINWEIS: Weitere Informationen zum Hinzufügen eines Hosts, der hinter einem bereits vorhandenen konfigurierten Gateway liegt, finden Sie unter „Host hinter einem konfigurierten Gateway einfügen“ auf Seite 186.

Mit dem Assistenten zum **Hinzufügen von Hosts** von PGPnet können Sie der Host-Liste einen Host-Eintrag hinzufügen.

1. Klicken Sie im Hauptfenster von PGPnet auf die Registerkarte **Hosts**.
2. Klicken Sie auf **Hinzufügen** (oder Alt+A). Der Assistent zum **Hinzufügen von Hosts** wird angezeigt. Lesen Sie den Inhalt des ersten Bildschirms, und klicken Sie auf **Weiter**.
3. Im Assistenten müssen Sie angeben, ob Sie einen Host, ein Teilnetz oder ein Gateway hinzufügen möchten. Klicken Sie auf **Host** und anschließend auf **Weiter**.
4. Wählen Sie, ob Sie die sichere Kommunikation erzwingen oder die unsichere Kommunikation zulassen möchten. Klicken Sie in das Optionsfeld neben der getroffenen Auswahl und anschließend auf **Weiter**.
5. Geben Sie für den Computer, mit dem Sie eine sichere Kommunikation führen möchten, einen bezeichnenden Namen ein. Klicken Sie auf **Weiter**.
6. Geben Sie entweder den Host-Namen oder die IP-Adresse für den Host ein. Klicken Sie auf **Weiter**. Der Assistent sucht nach Ihrem Eintrag. Falls der Assistent Ihren Eintrag nicht finden kann, klicken Sie auf **Zurück**, um zum vorigen Bildschirm zurückzukehren, und geben Sie erneut den Namen oder die IP-Adresse ein.

Die folgenden Schritte treffen zu, wenn Sie sich dazu entschließen, eine sichere Kommunikation zu erzwingen.

7. Wählen Sie die gewünschte Kommunikationsmethode für die Kommunikation mit diesem Rechner aus: Verschlüsselungsschutz mit öffentlichen Schlüsseln oder gemeinsame geheime (auf Paßphrasen basierende) Sicherheit. Klicken Sie auf **Weiter**. Geben Sie die Paßphrase ein, wenn Sie sich für die gemeinsame geheime Sicherheit entschließen. Beachten Sie, daß beide Hosts dieselbe gemeinsame geheime Paßphrase konfigurieren müssen. Klicken Sie auf **Weiter**.

   WARNUNG: Im Gegensatz zu den traditionellen PGP-Paßphrasen werden gemeinsame geheime Paßphrasen unverschlüsselt auf Ihrem Computer gespeichert. Dies stellt ein mögliches Sicherheitsrisiko dar.

   Wenn Sie keinen Authentisierungsschlüssel oder kein -zertifikat gewählt haben, werden Sie vom Assistenten aufgefordert, jetzt eine Auswahl zu treffen.

   - Wenn Sie sich für die gemeinsame geheime Sicherheit entschließen, gehen Sie über zu Schritt 8.
   - Wenn Sie sich für den Verschlüsselungsschutz mit öffentlichen Schlüsseln entschließen, gehen Sie über zu Schritt 9.

8. Wählen Sie aus, wie Sie sich beim entfernten Computer identifizieren möchten (trifft nur auf die gemeinsame geheime Authentisierung zu): IP-Adresse, Hostname, Benutzer-Domänenname oder Eindeutiger Name.

   IP-Adresse – Durch die IP-Adresse des Computers [nnn.nnn.nnn.nnn]

   Hostname – durch den Host-Namen dieses Computers [computername.netzwerkname]

   Benutzer-Domänenname – durch den von Ihnen angegebenen Benutzer- und Host-Namen [benutzername@computername.netzwerkname]

   Eindeutiger Name – durch eine von Ihnen festgelegte Textfolge, wie beispielsweise „CN=“Bob Jones“,_C=US,_O=“Acme,_Inc.““

   Klicken Sie auf **Weiter**. Geben Sie den Namen in „Benutzer-Domänenname“ oder „Eindeutiger Name“ ein. Klicken Sie auf **Weiter**.

9. Der Assistent fügt Ihrer Host-Liste den Eintrag hinzu. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

Teilnetz hinzufügen

HINWEIS: Weitere Informationen zum Hinzufügen eines Teilnetzes, das hinter einem bereits vorhandenen konfigurierten Gateway liegt, finden Sie unter „Teilnetz hinter einem konfigurierten Gateway hinzufügen“ auf Seite 187.

Mit dem Assistenten zum **Hinzufügen von Hosts** von PGPnet können Sie der Host-Liste Teilnetz-Einträge hinzufügen.

1. Klicken Sie im Hauptfenster von PGPnet auf die Registerkarte **Hosts**.
2. Klicken Sie auf **Hinzufügen** (oder Alt+A). Der Assistent zum **Hinzufügen von Hosts** wird angezeigt. Lesen Sie den Inhalt des ersten Bildschirms, und klicken Sie auf **Weiter**.
3. Im Assistenten müssen Sie angeben, ob Sie einen Host, ein Teilnetz oder ein Gateway hinzufügen möchten. Klicken Sie auf **Teilnetz** und anschließend auf **Weiter**.
4. Wählen Sie, ob Sie die sichere Kommunikation erzwingen oder die unsichere Kommunikation zulassen möchten. Klicken Sie in das Optionsfeld neben der getroffenen Auswahl und anschließend auf **Weiter**.
5. Geben Sie für das Teilnetz, mit dem Sie eine sichere Kommunikation führen möchten, einen bezeichnenden Namen ein. Klicken Sie auf **Weiter**.
6. Geben Sie die IP-Adresse und die Teilnetz-Maske für das Teilnetz ein. Klicken Sie auf **Weiter**.

   HINWEIS: Wenn Sie ein Teilnetz mit gemeinsamen geheimen Paßphrasen konfigurieren, müssen alle Rechner dieses Teilnetzes mit derselben gemeinsamen geheimen Paßphrase konfiguriert werden.

Die folgenden Schritte treffen zu, wenn Sie sich dazu entschließen, eine sichere Kommunikation zu erzwingen.

7. Wählen Sie die gewünschte Kommunikationsmethode für die Kommunikation mit diesem Teilnetz aus: Verschlüsselungsschutz mit öffentlichen Schlüsseln oder gemeinsame geheime (auf Paßphrasen basierende) Sicherheit. Klicken Sie auf **Weiter**. Geben Sie die Paßphrase ein, wenn Sie sich für die gemeinsame geheime Sicherheit entschließen. Wenn Sie das gemeinsame Geheimnis auswählen, muß jeder Rechner dieses Teilnetzes mit derselben gemeinsamen geheimen Paßphrase konfiguriert werden. Klicken Sie auf **Weiter**.

WARNUNG: Im Gegensatz zu den traditionellen PGP-Paßphrasen werden gemeinsame geheime Paßphrasen unverschlüsselt auf Ihrem Computer gespeichert. Dies stellt ein mögliches Sicherheitsrisiko dar.

8. Wählen Sie aus, wie Sie sich beim entfernten Computer identifizieren möchten (trifft nur auf die gemeinsame geheime Authentisierung zu): IP-Adresse, Hostname, Benutzer-Domänenname oder Eindeutiger Name.

   IP-Adresse – durch die IP-Adresse des Computers [nnn.nnn.nnn.nnn]

   Hostname – durch den Host-Namen dieses Computers [computername.netzwerkname]

   Benutzer-Domänenname – durch den von Ihnen angegebenen Benutzer- und Host-Namen [benutzername@computername.netzwerkname]

   Eindeutiger Name – durch eine von Ihnen festgelegte Textfolge, wie beispielsweise „CN=“Bob Jones“,_C=US,_O=“Acme,_Inc.““

   Klicken Sie auf **Weiter**. Geben Sie den Namen in „Benutzer-Domänenname“ oder „Eindeutiger Name“ ein. Klicken Sie auf **Weiter**.

9. Der Assistent fügt Ihrer Host-Liste den Eintrag hinzu. Klicken Sie auf **Fertig stellen**.

Gateway hinzufügen

Mit dem Assistenten zum **Hinzufügen von Hosts** von PGPnet können Sie der Host-Liste einen sicheren Gateway-Eintrag hinzufügen.

1. Klicken Sie im Hauptfenster von PGPnet auf die Registerkarte **Hosts**.
2. Klicken Sie auf **Hinzufügen** (oder Alt+A). Der Assistent zum **Hinzufügen von Hosts** wird angezeigt. Lesen Sie den Inhalt des ersten Bildschirms, und klicken Sie auf **Weiter**.
3. Im Assistenten müssen Sie angeben, ob Sie einen Host, ein Teilnetz oder ein Gateway hinzufügen möchten. Klicken Sie in das Optionsfeld neben **Gateway** und anschließend auf **Weiter**.
4. Geben Sie für das Gateway, mit dem Sie eine sichere Kommunikation führen möchten, einen bezeichnenden Namen ein. Klicken Sie auf **Weiter**.

5. Geben Sie entweder den Host-Namen oder die IP-Adresse für den Host ein. Klicken Sie auf **Weiter**. Der Assistent sucht nach Ihrem Eintrag. Falls der Assistent Ihren Eintrag nicht finden kann, klicken Sie auf **Zurück**, um zum vorigen Bildschirm zurückzukehren, und geben Sie erneut den Namen und die IP-Adresse ein. Klicken Sie nach Eingabe der entsprechenden IP-Adresse auf **Weiter.**

6. Wählen Sie die gewünschte Kommunikationsmethode für die Kommunikation mit diesem Rechner aus: Verschlüsselungsschutz mit öffentlichen Schlüsseln oder gemeinsame geheime (auf Paßphrasen basierende) Sicherheit. Klicken Sie auf **Weiter**. Geben Sie die Paßphrase ein, wenn Sie sich für die gemeinsame geheime Sicherheit entschließen. Klicken Sie auf **Weiter**.

   WARNUNG: Im Gegensatz zu den traditionellen PGP-Paßphrasen werden gemeinsame geheime Paßphrasen unverschlüsselt auf Ihrem Computer gespeichert. Dies stellt ein mögliches Sicherheitsrisiko dar.

   - Wenn Sie sich für die gemeinsame geheime Sicherheit entschließen, gehen Sie über zu Schritt 7.
   - Wenn Sie sich für den Verschlüsselungsschutz mit öffentlichen Schlüsseln entschließen, gehen Sie über zu Schritt 8.

7. Wählen Sie aus, wie Sie sich beim entfernten Computer identifizieren möchten (trifft nur auf die gemeinsame geheime Authentisierung zu): IP-Adresse, Hostname, Benutzer-Domänenname oder Eindeutiger Name.

   IP-Adresse – durch die IP-Adresse des Computers [nnn.nnn.nnn.nnn]

   Hostname – durch den Host-Namen dieses Computers [computername.netzwerkname]

   Benutzer-Domänenname – durch den von Ihnen angegebenen Benutzer- und Host-Namen [benutzername@computername.netzwerkname]

   Eindeutiger Name – durch eine von Ihnen festgelegte Textfolge, wie beispielsweise „CN=“Bob Jones“,_C=US,_O=“Acme,_Inc.““

   Klicken Sie auf **Weiter**. Geben Sie den Namen in „Benutzer-Domänenname“ oder „Eindeutiger Name“ ein. Klicken Sie auf **Weiter**.

8. Der Assistent fügt Ihrer Host-Liste den Eintrag für das sichere Gateway hinzu.

   Zu diesem Zeitpunkt können Sie wählen, ob Sie einen neuen Host oder ein dem Gateway zugeordnetes Teilnetz erstellen möchten. Klicken Sie gegebenenfalls in das Optionsfeld neben **Ja**. Wenn Sie keinen neuen Host oder kein neues Teilnetz erstellen möchten, klicken Sie in das Optionsfeld neben **Nein**. Klicken Sie auf **Weiter**.

   – Zum Erstellen eines neuen Hosts fahren Sie fort mit Schritt 2 auf Seite 181.

   – Zum Erstellen eines neuen Teilnetzes fahren Sie fort mit Schritt 2 auf Seite 183.

   – Wenn Sie zu diesem Zeitpunkt weder einen neuen Host noch ein neues Teilnetz erstellen möchten, klicken Sie auf **Fertig stellen**.

Host hinter einem konfigurierten Gateway einfügen

Mit dem Assistenten zum **Hinzufügen von Hosts** von PGPnet können Sie der Host-Liste einen sicheren Host hinter einem konfigurierten Gateway hinzufügen.

1. Klicken Sie im Hauptfenster von PGPnet auf die Registerkarte **Hosts**.

2. Wählen Sie das konfigurierte Gateway aus und klicken Sie auf **Hinzufügen**. Der Assistent zum **Hinzufügen von Hosts** wird angezeigt. Lesen Sie den Inhalt des ersten Bildschirms, und klicken Sie auf **Weiter**.

3. Der Assistent fordert den Benutzer auf einzugeben, ob ein neuer Host-Eintrag für einen durch dieses Gateway zugänglichen Computer oder für ein entsprechendes Teilnetz erstellt werden soll. Zur Erstellung wählen Sie **Ja** und klicken anschließend auf **Weiter**.

4. Sie werden aufgefordert, die Art der Kommunikation auszuwählen, die Sie konfigurieren möchten. Wählen Sie **Host,** und klicken Sie anschließend auf **Weiter**. Zum Hinzufügen eines sicheren Hosts fahren Sie fort mit „Hinzufügen eines Hosts“ auf Seite 181. Zum Hinzufügen eines unsicheren Hosts fahren Sie mit Schritt 5 fort.

5. Sie müssen angeben, ob Sie einen sicheren oder einen unsicheren Host hinzufügen möchten. Wählen Sie **Unsichere Kommunikation zulassen,** und klicken Sie auf **Weiter**.

6. Geben Sie für den Computer, mit dem Sie kommunizieren möchten, einen bezeichnenden Namen ein. Klicken Sie auf **Weiter**.

7. Geben Sie entweder den Hostnamen oder die IP-Adresse für den Host ein. Klicken Sie auf **Weiter**. Der Assistent sucht nach Ihrem Eintrag. Falls der Assistent Ihren Eintrag nicht finden kann, klicken Sie auf **Zurück**, um zum vorigen Bildschirm zurückzukehren, und geben Sie erneut den Namen oder die IP-Adresse ein.

8. Der Assistent fügt Ihrer Host-Liste den Eintrag hinzu. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

Teilnetz hinter einem konfigurierten Gateway hinzufügen

HINWEIS: Weitere Informationen zum Hinzufügen eines Teilnetzes, das nicht hinter einem bereits vorhandenen konfigurierten Gateway liegt, finden Sie unter „Teilnetz hinzufügen“ auf Seite 183.

Mit dem Assistenten zum **Hinzufügen von Hosts** von PGPnet können Sie der Host-Liste ein Teilnetz hinter einem konfigurierten Gateway hinzufügen.

1. Klicken Sie im Hauptfenster von PGPnet auf die Registerkarte **Hosts**.

2. Wählen Sie das konfigurierte Gateway aus und klicken Sie auf **Hinzufügen**. Der Assistent zum **Hinzufügen von Hosts** wird angezeigt. Lesen Sie den Inhalt des ersten Bildschirms, und klicken Sie auf **Weiter**.

3. Der Assistent fordert den Benutzer auf einzugeben, ob ein neuer Host-Eintrag für einen durch dieses Gateway zugänglichen Computer oder für ein entsprechendes Teilnetz erstellt werden soll. Zur Erstellung wählen Sie **Ja** und klicken anschließend auf **Weiter**.

4. Sie werden aufgefordert, die Art der Kommunikation auszuwählen, die Sie konfigurieren möchten. Wählen Sie **Teilnetz** und klicken Sie anschließend auf **Weiter**. Zum Hinzufügen eines sicheren Teilnetzes fahren Sie fort mit „Teilnetz hinzufügen“ auf Seite 183**.** Zum Hinzufügen eines unsicheren Teilnetzes fahren Sie fort mit Schritt 5.

5. Sie müssen angeben, ob Sie ein sicheres oder ein unsicheres Teilnetz hinzufügen möchten. Wählen Sie **Unsichere Kommunikation zulassen** und klicken Sie auf **Weiter**.

6. Geben Sie für das Teilnetz, mit dem Sie eine sichere Kommunikation führen möchten, einen bezeichnenden Namen ein. Klicken Sie auf **Weiter**.

7. Geben Sie die IP-Adresse und die Teilnetz-Maske für das Teilnetz ein, mit dem Sie kommunizieren möchten. Klicken Sie auf **Weiter**.

8. Der Assistent fügt Ihrer Host-Liste den Eintrag für das Teilnetz hinzu. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.

Host-, Teilnetz- oder Gateway-Eintrag ändern

Gelegentlich müssen Sie möglicherweise die Konfiguration eines Hosts, Teilnetzes oder eines Gateways ändern. Dies ist beispielsweise der Fall, wenn eine IP-Adresse, Teilnetz-Maske oder ein Hostnamen geändert wurde. So ändern Sie eine Konfiguration

1. Klicken Sie auf die Registerkarte **Hosts**.
2. Wählen Sie den Host, das Teilnetz oder das Gateway aus, das Sie ändern möchten.
3. Klicken Sie auf **Bearbeiten**.

   Verknüpfung: Statt einen Host auszuwählen und auf **Bearbeiten** zu klikken, können Sie auch auf den Host in der Host-Liste doppelklicken.
4. Nehmen Sie die erforderlichen Eingaben zum Bearbeiten vor.
5. Klicken Sie auf **OK**.

Die PGPnet-Datenbank wird sofort aktualisiert. Die PGPnet-Datenbank wird jedoch erst aktualisiert, wenn die ordnungsgemäße Funktionsweise des PGPnet-Services oder des -Treibers gewährleistet ist. Möglicherweise muß der Computer neu gestartet werden.

Host-, Teilnetz- oder Gateway-Eintrag entfernen

Möglicherweise möchten Sie gelegentlich einen konfigurierten Host, ein Teilnetz oder ein Gateway entfernen. Beispielsweise, wenn Sie der Meinung sind, daß alle Elemente nicht mehr sicher sind. So entfernen Sie einen Host, ein Teilnetz oder ein Gateway

1. Klicken Sie auf die Registerkarte **Hosts**.
2. Wählen Sie den Host, das Teilnetz oder das Gateway aus, das Sie entfernen möchten.
3. Klicken Sie auf **Entfernen**.

Host muß einen bestimmten Schlüssel oder ein bestimmtes Zertifikat angeben

Sie möchten möglicherweise, daß ein Host einen bestimmten Schlüssel oder ein ein bestimmtes Zertifikat angibt, wenn der Host eine SA zu erstellen versucht. Wenn der Host nicht den entsprechenden Schlüssel oder das entsprechende Zertifikat angibt, wird die Kommunikation mit dem Host vom System verweigert.

So legen Sie fest, daß ein Host einen bestimmten Schlüssel oder ein bestimmtes Zertifikat angeben muß

1. Falls nicht bereits vorhanden, fügen Sie PGPnet einen Host, ein Teilnetz oder ein Gateway hinzu, (Anweisungen dazu finden Sie im Abschnitt „Hosts, Teilnetze oder Gateways hinzufügen“ auf Seite 179). PGPnet fügt der Host-Liste auf der Registerkarte **Hosts** einen Eintrag hinzu.

2. Wählen Sie den Eintrag auf der Registerkarte **Hosts** aus, und klicken Sie anschließend auf **Bearbeiten**. PGPnet zeigt das Dialogfeld **Host/Gateway** an. Der Abschnitt **Entfernte Authentisierung** wird unten im Dialogfeld angezeigt.

3. Sie können festlegen, daß der Host, das Teilnetz oder das Gateway für die eigene Authentisierung einen bestimmten PGP-Schlüssel oder ein X.509-Zertifikat erfordern.

   - Klicken Sie in das Optionsfeld neben **PGP-Schlüssel**, um einen bestimmten PGP-Schlüssel anzufordern. PGPnet zeigt das Dialogfeld „Schlüssel auswählen“ an. Klicken Sie auf den entsprechenden Schlüssel, und klicken Sie anschließend auf **OK**. PGPnet zeigt den Schlüssel im Feld **Entfernte Authentisierung** an. Klicken Sie auf **OK**, um das Dialogfeld „Host/Gateway“ zu schließen.

   - Klicken Sie in das Optionsfeld neben „X.509-Zertifikat“, um ein bestimmtes X.509-Zertifikat anzufordern. PGPnet zeigt das Dialogfeld **X.509-Zertifikat auswählen** an. Klicken Sie auf das entsprechende Zertifikat, und klicken Sie anschließend auf **OK**. PGPnet zeigt das Zertifikat im Feld **Entfernte Authentisierung** an. Klicken Sie auf **OK**, um das Dialogfeld „Host/Gateway“ zu schließen.

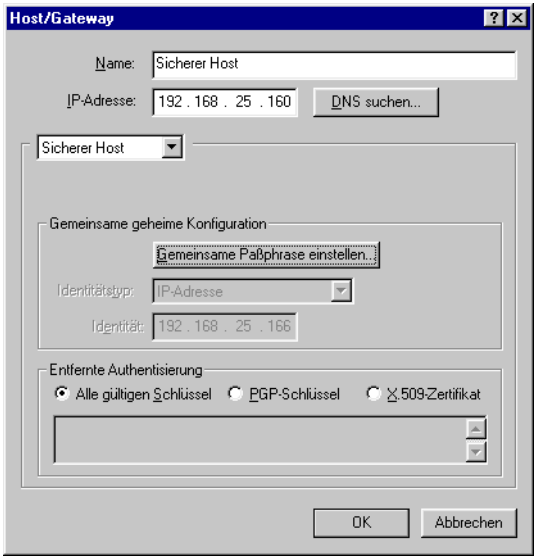


Abbildung 8-8. Dialogfeld „Host/Gateway“

Registerkarte „Allgemein“ anzeigen

Wählen Sie im PGPnet-Fenster im Menü „Ansicht“ den Befehl „Optionen“ aus, um die Registerkarte **Allgemein** anzuzeigen.

Führen Sie die folgenden Aufgaben auf der Registerkarte **Allgemein** aus:

- Aktivieren und Deaktivieren des Profi-Modus
- Überprüfen der Sicherheitsstufe der Kommunikation mit Hosts
- Überprüfen der Paßphrasen-Zwischenspeicherung zwischen Anmeldevorgängen
- Fordern gültiger Authentisierungsschlüssel von allen Hosts
- Festlegen gültiger Werte für Setup-Schlüssel (IKE) und Primärschlüssel (IPsec) zur Erstellung von Sicherheitsverknüpfungen mit anderen konfigurierten Hosts.

Profi-Modus: Umgehen des Assistenten, um Hosts, Gateways und Teilnetze hinzuzufügen

Wenn Sie im Umgang mit PGPnet geübter sind, können Sie zum schnellen Hinzufügen und Bearbeiten von Hosts, Gateways und Teilnetzen den **Profi-Modus** (**Ansicht–>Optionen–>Allgemein**) verwenden. Im Gegensatz zum Assistenten, der Sie schrittweise durch den Vorgang für das Hinzufügen von Einträgen führt, wird im **Profi-Modus** ein Formular angezeigt, in dem Sie einen neuen Eintrag vornehmen können.

HINWEIS: Bei der Verwendung des Profi-Modus müssen Sie darauf achten, einen Authentisierungsschlüssel oder ein -zertifikat auszuwählen (**Ansicht–>Optionen–>Authentisierung**).

So aktivieren und verwenden Sie den Profi-Modus

1. Wählen Sie im Menü **Ansicht** den Befehl **Optionen**, um die Registerkarte **Allgemein** anzuzeigen.
2. Klicken Sie auf **Profi-Modus** (ein Häkchen wird angezeigt).
3. Klicken Sie auf **OK**.
4. Klicken Sie auf die Registerkarte **Hosts**. Klicken Sie auf **Hinzufügen**, um das Dialogfeld **Host/Gateway** zu schließen.

DNS-Suche IP-Adresse eines Hosts finden

Der Profi-Modus von PGPnet schließt eine DNS-Suchfunktion ein. Verwenden Sie diese Funktion, um die IP-Adresse eines Hosts zu finden.

Führen Sie die folgenden Schritte aus, um die DNS-Suchfunktion zu verwenden

1. Klicken Sie auf **DNS-Suche**. PGPnet zeigt das Dialogfeld „DNS-Suche“ an.
2. Geben Sie den Host-Namen des Systems in das Feld **Zu suchender Hostname** ein, und klicken Sie anschließend auf **Suchen**. PGPnet sucht die IP-Adresse für den eingegebenen Host-Namen.
   - Wenn PGPnet die IP-Adresse findet, wird diese angezeigt. Klicken Sie auf **Verwenden,** um die IP-Adresse im Formular zum Bearbeiten von Hosts / Gateways zu verwenden.
   - Wird keine IP-Adresse für den Host gefunden, blendet PGPnet die folgenden Vorgehensweisen ein.

. **TIP:** Sie können den Host-Namen des Systems in das Namensfeld im Dialogfeld „Host/Gateway“ eingeben und anschließend auf **DNS-Suche** klicken. Das Fenster „Suchen“ wird angezeigt. Klicken Sie auf **Suchen**, um die IP-Adresse für den eingegebenen Host-Namen zu suchen.

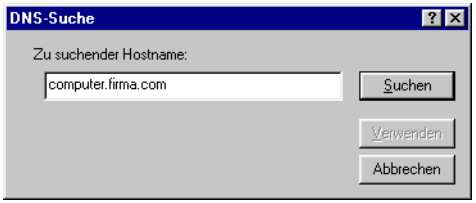


Abbildung 8-9. Dialogfeld „DNS-Suche“

Entfernte Authentisierung

Mit den Steuerungen im Abschnitt **Entfernte Authentisierung** im Dialogfeld **Host/Gateway** können Sie den entfernten Host auffordern, jedesmal einen bestimmten PGP-Schlüssel oder ein bestimmtes X.509-Zertifikat anzugeben, wenn er den Aufbau einer SA mit Ihrem Host versucht. Wenn der Host versucht, eine Verbindung herzustellen, und nicht den entsprechenden Schlüssel oder das entsprechende Zertifikat angibt, wird auf Ihrem Rechner die Verbindung verweigert. Die Standardeinstellung ist **Alle gültigen Schlüssel**.

WICHTIG: Wenn Sie für einen sicheren Teilnetzeintrag einen bestimmten PGP-Schlüssel oder ein X.509-Zertifikat auswählen, müssen alle Benutzer innerhalb dieses Teilnetzes denselben Schlüssel verwenden, um sich selbst zu authentisieren.

So kennzeichnen Sie einen bestimmten PGP-Schlüssel, den der entfernte Host für die Authentisierung vorweisen muß

1. Klicken Sie auf **PGP-Schlüssel**.
2. Wählen Sie einen Schlüssel aus dem Popup-Dialogfeld aus, und klicken Sie anschließend auf **OK**. Der Schlüssel wird im Abschnitt **Entfernte Authentisierung** im Dialogfeld **Host/Gateway** angezeigt.
3. Klicken Sie auf **OK**.

So kennzeichnen Sie ein bestimmtes X.509-Zertifikat, das der entfernte Host für die Authentisierung vorweisen muß

1. Klicken Sie auf „X.509-Zertifikat“.
2. Wählen Sie ein Zertifikat aus dem Popup-Dialogfeld aus, und klicken Sie anschließend auf **OK**. Der Schlüssel wird im Abschnitt **Entfernte Authentisierung** im Dialogfeld **Host/Gateway** angezeigt.
3. Klicken Sie auf **OK**.

Profi-Modus deaktivieren

So deaktivieren Sie den Profi-Modus

1. Wählen Sie im Menü **Ansicht** den Befehl **Optionen**, um die Registerkarte **Allgemein** anzuzeigen.
2. Klicken Sie auf **Profi-Modus** (kein Häkchen wird angezeigt).
3. Klicken Sie auf **OK**.

Sicherheitsstufe der Kommunikation mit Hosts überprüfen

Die sichere Kommunikation mit anderen Hosts ist einer der Hauptgründe für die Verwendung von PGPnet. Die Sicherheitsfunktionen von PGPnet (Verschlüsselung, Authentisierung und Tunneling) ermöglichen die sichere Datenübertragung über das Internet oder über andere öffentliche oder private Netzwerke. Ihre Daten werden bei der Übertragung über das Netzwerk und über Rechner, die nicht vom Unternehmen gesteuert werden, geschützt. Jeder Versuch von Hackern zum Abfangen, Entschlüsseln oder Ändern von Daten wird außer Kraft gesetzt. Ihre Daten erreichen unbeschädigt den entgültigen Bestimmungsort.

PGPnet enthält die Funktion zur Kommunikation mit unkonfigurierten Hosts (d. h. Hosts, die nicht der Host-Liste von PGPnet hinzugefügt wurden) und die Funktion zur sicheren Kommunikation mit allen Hosts.

Kommunikation mit unkonfigurierten Hosts zulassen und sichere Kommunikation mit allen Hosts fordern

Mit diesen beiden Einstellungen können Sie steuern, mit wem Sie kommunizieren, und Sie können die Anzahl der Systeme minimieren, die Sie der Host-Liste hinzufügen müssen.

Wenn die meisten Systeme, mit denen Sie kommunizieren PGPnet nicht ausführen, fügen Sie mit dem Assistenten der Host-Liste die wenigen sicheren Hosts hinzu, und aktivieren Sie die Einstellung **Kommunikation mit unkonfigurierten Hosts zulassen**. Dies ermöglicht sowohl die Kommunikation mit den von Ihnen in der Host-Liste gekennzeichneten sicheren Hosts als auch mit allen anderen Hosts.

Wenn die meisten Systeme, mit denen Sie kommunizieren, PGPnet nicht ausführen, fügen Sie mit dem Assistenten der Host-Liste die wenigen unsicheren Hosts als unsichere Hosts hinzu, und aktivieren Sie die Einstellung **Sichere Kommunikation mit allen Hosts fordern**. Dies ermöglicht die Kommunikation mit den von Ihnen in der Host-Liste gekennzeichneten unsicheren Hosts und mit allen anderen IPsec-kompatiblen Hosts.

Kommunikation mit unkonfigurierten Hosts zulassen

Mit dieser Funktion (**Ansicht–>Optionen–>Allgemein**), können Sie Daten, die nicht vertraulich sind, an nicht in PGPnet konfigurierte Hosts senden oder von diesen empfangen. Sie möchten diese Funktion möglicherweise für die Suche im Web verwenden. Diese Einstellung ist standardmäßig aktiviert.

- Aktivieren Sie dieses Kontrollkästchen, um die Kommunikation mit unkonfigurierten Hosts zuzulassen.S
- Deaktivieren Sie dieses Kontrollkästchen, um die Kommunikation mit unkonfigurierten Hosts nicht zuzulassen.

Sichere Kommunikation mit allen Hosts fordern

Mit dieser Funktion (**Ansicht–>Optionen–>Allgemein**) fordern Sie sichere Kommunikation mit allen Hosts. Wenn beispielsweise alle Systeme Ihres Unternehmens mit PGPnet konfiguriert sind, können Sie mit dieser Funktion die Notwendigkeit zur Kennzeichnung aller Hosts ausschalten.

Wenn dieses Kontrollkästchen aktiviert ist, stimmt PGPnet eine SA mit jedem Zielrechner ab, bevor die Kommunikation zugelassen wird. Die Standardeinstellung ist deaktiviert.

- Um PGPnet zur sicheren Kommunikation mit allen Hosts aufzufordern, aktivieren Sie dieses Kontrollkästchen.
- Um unsichere Kommunikation mit allen Hosts zuzulassen, aktivieren Sie dieses Kontrollkästchen.

HINWEIS: Wenn diese Funktion aktiviert ist, können zwei Rechner, die als unsicherer Host konfiguriert wurden, immer noch miteinander kommunizieren.

WARNUNG: Diese Sicherheitsfunktion wurde für Umgebungen entwickelt, in denen alle Rechner mit PGPnet konfiguriert sind. Ist diese Funktion aktiviert, wird die Kommunikation mit allen Rechnern, die nicht mit PGPnet konfiguriert sind, gesperrt. Folglich ist es möglich, daß Sie manches aus Ihrem Netzwerkverkehr verlieren, wenn Sie sich nicht in einer konfigurierten PGPnet-Umgebung befinden und Sie diese Funktion aktivieren.

Gültige Authentisierungsschlüssel anfordern

Mit dieser Funktion (**Ansicht–>Optionen–>Allgemein**) können Sie steuern, ob PGPnet verifiziert, daß die von entfernten Hosts vorgelegten Schlüssel auf dem lokalen Schlüsselbund gültig sind.

- Um zu fordern, daß PGPnet die Gültigkeit der von entfernten Hosts vorgelegten Schlüssel auf dem lokalen Schlüsselbund verifiziert, aktivieren Sie diese Funktion. Verwenden Sie diese Einstellung, wenn Sie nur mit Hosts kommunizieren, die gültige Schlüssel und Zertifikate aus Ihrem Schlüsselbund verwenden.
- Ist diese Einstellung deaktiviert, wird PGPnet angewiesen, alle Schlüssel unabhängig von der Gültigkeit zu akzeptieren. Verwenden Sie diese Einstellung, wenn Sie PGPnet auf Servern ausführen (z. B. Mail- oder Web-Server), die mit jedem Client-Host verbunden werden können. Der Server verwendet den entsprechenden Schlüssel für die eigene Authentisierung bei einem Client-Host, der Server jedoch akzeptiert jeden vom Client-Host vorgeschlagenen Schlüssel. (In diesem Fall ist die Einstellung für den Server deaktiviert und für den Client-Host aktiviert.) Der Client-Host muß zur Ausführung dieses Szenarios über den vertrauten Authentisierungsschlüssel des Servers verfügen.

WICHTIG: Wenn dieses Kontrollkästchen deaktiviert ist, wird die Einstellung **Alle gültigen Schlüssel** im Abschnitt **Authentisierung** im Dialogfeld **Host/Gateway** überschrieben. Wenn dieser Fall eintritt, akzeptiert der Server alle Schlüssel und nicht nur die gültigen Schlüssel. Sie können jedoch immer noch das Dialogfeld **Host/Gateway** verwenden, um einen bestimmten Schlüssel oder ein Zertifikat für jeden Host anzufordern. Weitere Informationen finden Sie unter „Host muß einen bestimmten Schlüssel oder ein bestimmtes Zertifikat angeben“ auf Seite 189.

❑ **HINWEIS:** Alle Schlüsselauthentisierungen werden auf der Registerkarte **Protokoll** angezeigt, und jeder Eintrag zeigt die Schlüssel-ID an.

❑ **HINWEIS:** Wenn dieses Kontrollkästchen aktiviert ist und ein PGP-Schlüssel als Methode für die **Entfernte Authentisierung** ausgewählt wurde (Dialogfeld **Host/Gateway**), treffen beide Anforderungen zu (der Rechner muß den richtigen Schlüssel aufweisen, und der Schlüssel muß gültig sein).

Paßphrasen zwischen Anmeldevorgängen zwischenspeichern

Mit dieser Funktion (**Ansicht–>Optionen–>Allgemein**) fordern Sie PGPnet zur Zwischenspeicherung von Paßphrasen zwischen Anmeldevorgängen auf.

- Wenn diese Funktion aktiviert ist, bewahrt PGPnet die von Ihnen eingegebenen Paßphrasen. Bei der Ab- und erneuten Anmeldung bei Windows müssen Sie die Paßphrase nicht erneut eingeben.
- Ist diese Funktion deaktiviert, werden Paßphrasen bei der Abmeldung bei Windows nicht gespeichert. Wenn Sie sich erneut anmelden, müssen Sie die Paßphrase erneut eingeben.

❑ **HINWEIS:** Dies trifft nur auf die An- und Abmeldung bei Windows zu. Ist diese Funktion aktiviert, und Sie melden sich bei Windows ab und als anderer Benutzer wieder an, müssen Sie die Paßphrase nicht erneut eingeben. Dies trifft nicht auf die An- und Abmeldung bei PGPnet zu.

Beachten Sie, daß die Verwendung eines Schlüssels ohne Paßphrase die Zwischenspeicherung der Paßphrase unnötig macht. Sie können unter Umständen einen Schlüssel ohne Paßphrase verwenden, wenn es sich bei Ihrem Rechner um einen automatisierten Rechner, beispielsweise einen Server handelt.

- Wenn Sie möchten, daß PGPnet Paßphrasen zwischen Anmeldevorgängen zwischenspeichert, aktivieren Sie dieses Kontrollkästchen.
- Andernfalls deaktivieren Sie das Kontrollkästchen.

Schlüsselgültigkeitswerte festlegen

Sie können die Gültigkeitswerte für Setup-Schlüssel (IKE) und Primärschlüssel (IPsec) festlegen. Diese Schlüssel werden für die Erstellung der Sicherheitsverknüpfungen herangezogen. Werte können durch zeitliche Werte (**Dauer**) oder Datengröße (**MB**) erstellt werden.

Dauer wird auf die folgende Art und Weise dargestellt:

2t, 08h, 04m (Schlüssel läuft in 2 Tagen, 8 Stunden und 4 Minuten ab)

MB wird auf die folgende Art und Weise dargestellt:

99 (Schlüssel läuft nach einer Datenübertragung von 99 MB ab)

Wenn Sie eine SA mit einem anderen Host einrichten, verwendet PGPnet den strikteren der beiden Ablaufwerte. Folglich läuft eine SA möglicherweise ab, bevor der von Ihnen festgelegte Ablaufhöchstwert erreicht wurde.

WARNUNG: Das Herabsetzen des Standardwertes für MB hat möglicherweise eine mehrfache erneute Eingabe bei der Übertragung von großen Dateien zur Folge, die darüber hinaus eine Störung der normalen Netzwerkfunktionen verursachen können.

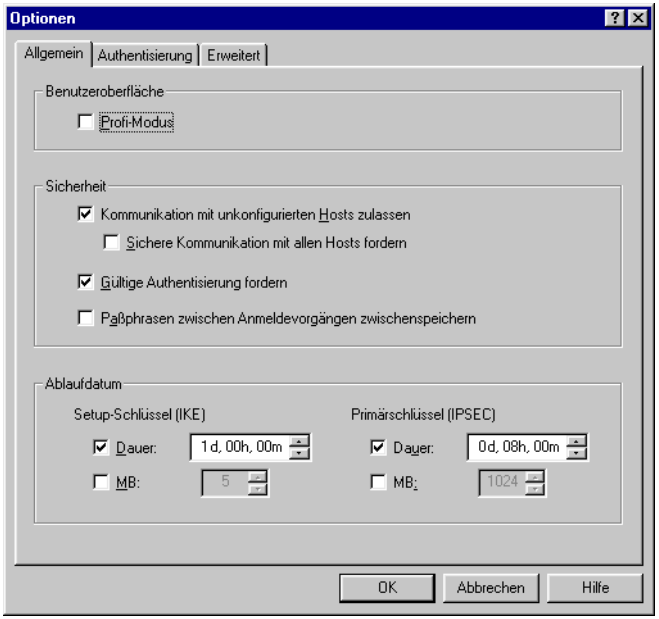


Abbildung 8-10. Die Registerkarte „Allgemein“

So legen Sie Gültigkeitswerte für Setup-Schlüssel (IKE) fest

1. Zeigen Sie die Registerkarte **Allgemein** (**Ansicht–>Optionen**) an. Die Informationen zur **Gültigkeit** werden im unteren Abschnitt im Dialogfeld **Allgemein** angezeigt.
2. Um die Dauer für einen Setup-Schlüssel festzulegen, klicken Sie in das Feld neben **Dauer**. Mit den Auf- und Abwärtspfeilen neben dem Feld „Dauer“ können Sie die entsprechende zeitliche Begrenzung festlegen oder einen numerischen Wert in jedes Feld eingeben: t, h, m.
3. Um einen Datenwert in **MB** für Setup-Schlüssel festzulegen, klicken Sie auf **MB**. Mit den Auf- und Abwärtspfeilen können Sie die entsprechende MB-Begrenzung festlegen oder einen numerischen Wert eingeben.
4. Klicken Sie auf **OK**.

So legen Sie Gültigkeitswerte für Primärschlüssel (IPsec) fest

1. Zeigen Sie die Registerkarte **Allgemein** (**Ansicht–>Optionen**) an. Die Informationen zur **Gültigkeit** werden im unteren Abschnitt im Dialogfeld **Allgemein** angezeigt.
2. Um die Dauer für einen Primärschlüssel festzulegen, klicken Sie in das Feld neben **Dauer**. Mit den Auf- und Abwärtspfeilen neben dem Feld **Dauer** können Sie die entsprechende zeitliche Begrenzung festlegen oder einen numerischen Wert in jedes Feld eingeben: t, h, m.
3. Um einen Datenwert in **MB** für Primärschlüssel festzulegen, klicken Sie auf das Feld neben **MB**. Mit den Auf- und Abwärtspfeilen können Sie die entsprechende MB-Begrenzung festlegen oder einen numerischen Wert eingeben.
4. Klicken Sie auf **OK**.

Verbindung authentisieren

Mit den Steuerungen auf der Registerkarte **Authentisierung** können Sie die folgenden Aufgaben ausführen:

- Auswählen von öffentlichen und privaten PGPnet-Schlüsselbunddateien als aktive Authentisierungs-Schlüsselbunde (**PGPnet-Schlüsselbunddateien**). Mit dieser Funktion können Sie unabhängige PGPnet-Schlüsselbunddateien festlegen.

  Die Felder **Öffentlich** und **Privat** zeigen ursprünglich den öffentlichen Schlüsselbund der Person an, die PGPnet installiert hat (für gewöhnlich der Administrator). Zur Auswahl von verschiedenen Schlüsselbunddateien klicken Sie auf **Durchsuchen**.

  Wenn Ihnen keine PGPnet-Schlüsselbunddateien vorliegen, klicken Sie auf **Meine PGP-Schlüsselbunddateien verwenden**, damit PGPnet Ihre PGP-Schlüsselbunddateien verwendet. Wenn Sie auf diese Schaltfläche klicken, PGPnet die PGP-Schlüsselbunddateien des Benutzers verwendet, der zuletzt im System angemeldet war. Wenn Sie auf die Schaltfläche **Meine PGP-Schlüsselbunddateien verwenden** klicken, werden die öffentlichen und die privaten PGP-Schlüsselbunddateien auf Ihren PGP-Schlüsselbund zurückgesetzt.

- Wählen Sie einen PGP-Schlüssel aus, um Ihren lokalen Rechner zu authentisieren (**PGP-Authentisierung**).

- Wählen Sie ein X.509-Zertifikat aus, um Ihren lokalen Rechner zu authentisieren (**X.509-Authentisierung**).

- Wenn Sie auf **OK** klicken, werden Sie zur Eingabe der Paßphrase für den ausgewählten Authentisierungsschlüssel oder das -zertifikat aufgefordert. Geben Sie die Paßphrase ein, und klicken Sie auf **OK**. Sie werden bei jeder Anmeldung bei PGPnet zur Eingabe dieser Paßphrase aufgefordert. Dies ist nicht der Fall, wenn auf der Registerkarte **Allgemein** die Option **Paßphrasen zwischen Anmeldevorgängen zwischenspeichern** aktiviert ist.

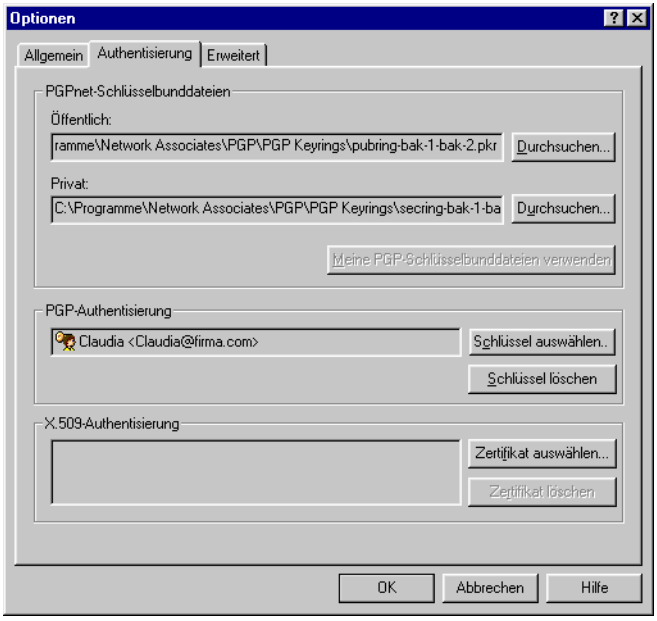


Abbildung 8-11. Die Registerkarte „Authentisierung“

In der folgenden Tabelle werden die Schaltflächen auf der Registerkarte **Authentisierung** beschrieben.

Schaltfläche	Beschreibung
Durchsuchen Schaltflächen	Zeigt die Dialogfelder "Öffentliche Schlüsselbunddateien auswählen" und "Private Schlüsselbunddateien auswählen" an. In diesen Dialogfeldern wählen Sie Ihre öffentlichen und privaten PGPnet-Schlüsselbunddateien als aktive Authentisierungs-Schlüsselbunde aus.
Mein PGP verwenden Schlüsselbunddateien	PGPnet verwendet Ihre PGPnet-Schlüsselbunddateien als Ihren aktiven Authentisierungsschlüsselbund.
Schlüssel auswählen	Zeigt das PGP-Dialogfeld "Schlüssel auswählen" an. Verwenden Sie dieses Dialogfeld zur Auswahl eines Schlüsselpaares für die Authentisierung Ihres Rechners. Sie werden aufgefordert, die Paßphrase für den ausgewählten Schlüssel einzugeben.
Schlüssel löschen	Löscht den ausgewählten PGP-Schlüssel.

Schaltfläche	Beschreibung
Zertifikat	Zeigt das Dialogfeld für die Auswahl des Zertifikats an. Verwenden Sie dieses Dialogfeld zur Auswahl eines X.509-Zertifikats für die Authentisierung Ihres Rechners. Sie werden aufgefordert, die Paßphrase für den dem Zertifikat zugeordneten Schlüssel einzugeben.
Löschen Zertifikat	Löscht das ausgewählte X.509-Zertifikat.

Registerkarte „Erweitert“

WARNUNG: Die Standardeinstellungen auf dieser Registerkarte ermöglichen die Kommunikation mit PGPnet oder Benutzern der starken Verschlüsselung GVPN. Ändern Sie die Einstellungen nur, wenn Sie ein erfahrener Benutzer von IPsec sind.

Die Registerkarte **Erweitert** (**Ansicht–>Optionen**) zeigt die Optionen **Zulässige externe Vorschläge** und IKE und IPsec-**Vorschläge** an.

- Mit dem Abschnitt **Zulässige externe Vorschläge** wird PGPnet angewiesen, alle Vorschläge von anderen Benutzern zu akzeptieren, die ein in diesem Feld aktiviertes Element enthalten. In den Optionen „Keine“ für Chiffriercode und Hashes sind die Ausnahmen hierzu aufgeführt. Die Option „Keine“ sollte mit größter Vorsicht bzw. überhaupt nicht verwendet werden. Falls Sie für den Chiffriercode (Verschlüsselung) das Merkmal „Keine“ wählen, akzeptiert PGPnet Vorschläge, die keine Verschlüsselung aufweisen. Falls Sie für die Authentisierung (Hashes) die Option „Keine“ wählen, akzeptiert PGPnet Vorschläge, die keine Authentisierung aufweisen.
- In den Abschnitten IKE- und IPsec-**Vorschläge** werden die Vorschläge erläutert, die Sie anderen unterbreiten. Andere Benutzer müssen mindestens einen der Vorschläge für IKE und IPsec genau wie angegeben akzeptieren.

Zulässige externe Vorschläge

Im Teil **Zulässige externe Vorschläge** dieser Registerkarte werden die in PGPnet zulässigen Typen von Chiffriercodes, Hashes, Komprimierung und Diffie-Hellman-Schlüsseln gekennzeichnet. Einstellungsänderungen auf dieser Registerkarte sollten nur von erfahrenen IPsec-Benutzern vorgenommen werden.

Ein *Chiffriercode* ist ein zur Ver- und Entschlüsselungen verwendeter Algorithmus. Um eine bestimmte Art von Chiffriercode (CAST oder TripleDES) verwenden zu können, müssen Sie das Kontrollkästchen links neben dem jeweiligen Chiffriercode aktivieren. Die Option „Keine“ sollte mit größter Vorsicht bzw. überhaupt nicht verwendet werden, da PGPnet angewiesen wird, Vorschläge von anderen Benutzern zu akzeptieren, die keine Verschlüsselung aufweisen.

Eine *Hash-Funktion* verwendet eine Eingabezeichenkette beliebiger Länge und konvertiert diese in eine Ausgabezeichenkette mit fester Länge. Um eine bestimmte Art von Hash (SHA-1 oder MD5) verwenden zu können, müssen Sie das Kontrollkästchen links neben der Hash-Funktion aktivieren.
Die Option „Keine“ sollte mit größter Vorsicht bzw. überhaupt nicht verwendet werden, da PGPnet angewiesen wird, Vorschläge von anderen Benutzern zu akzeptieren, die keine Verschlüsselung aufweisen.

Eine *Komprimierungsfunktion* verwendet eine Eingabe fester Länge und gibt eine kürzere Ausgabe mit fester Länge aus. Es gibt zwei Arten von Komprimierung. LZS und Deflate. Um eine bestimmte Komprimierungsart verwenden zu können, müssen Sie das Kontrollkästchen links neben der jeweiligen Komprimierungsart aktivieren.

❑ **HINWEIS:** LZS und Deflate erhöhen die Leistung der langsamen Kommunikation, wie beispielsweise mit Modem und ISDN. LZS und Deflate verringern die Leistung der schnellen Kommunikation (z. B. mit Kabelmodem, DSL, T-1 und T-3). Das liegt an den allgemeinen Komprimierungsroutinen.

Diffie-Hellman ist ein Schlüsselabkommenprotokoll. Um eine bestimmte Art von Schlüsselgröße (1024 oder 1536) verwenden zu können, müssen Sie das Kontrollkästchen links neben der Schlüsselgröße aktivieren.

Begriff	Beschreibung
Chiffriercodes	Ein zur Ver- und Entschlüsselungen verwendeter Algorithmus. Typen: CAST TripleDES Wenn die Option „Keine“ aktiviert ist, akzeptiert PGPnet Vorschläge von anderen Benutzern, die keine Authentisierung aufweisen.
Hashes	Eine Hash-Funktion verwendet eine Eingabezeichenkette beliebiger Länge und konvertiert diese in eine Ausgabezeichenkette mit fester Länge. Typen: SHA-1 (Secure Hash Algorithm) MD5 (Message Digest Algorithm). Wenn die Option „Keine“ aktiviert ist, akzeptiert PGPnet Vorschläge von anderen Benutzern, die keine Authentisierung aufweisen.
Diffie-Hellman	Schlüsselabkommenprotokoll. Größe: 1024 Bit 1536 Bit
Komprimierung	Verwendet eine Eingabe fester Länge und erstellt eine kürzere Ausgabe mit fester Länge. Typen: LZS Deflate HINWEIS: LZS und Deflate erhöhen die Leistung der langsamen Kommunikation, wie beispielsweise mit Modem und ISDN. LZS und Deflate verringern die Leistung der schnellen Kommunikation (z. B. mit Kabelmodem, DSL, T-1 und T-3). Das liegt an den allgemeinen Komprimierungsroutinen.

So fügen Sie ein Element zu „Zulässige externe Vorschläge“ hinzu

1. Zeigen Sie das Fenster **Optionen** (**Ansicht–>Optionen**) an.
2. Klicken Sie auf die Registerkarte **Erweitert**.
3. Aktivieren Sie das Kontrollkästchen links neben dem Element.
4. Klicken Sie auf **OK**.

So entfernen Sie ein Element aus „Zulässige externe Vorschläge“

1. Zeigen Sie das Fenster **Optionen** (**Ansicht–>Optionen**) an.
2. Klicken Sie auf die Registerkarte **Erweitert**.
3. Deaktivieren Sie das Kontrollkästchen links neben dem Element.
4. Klicken Sie auf **OK**.

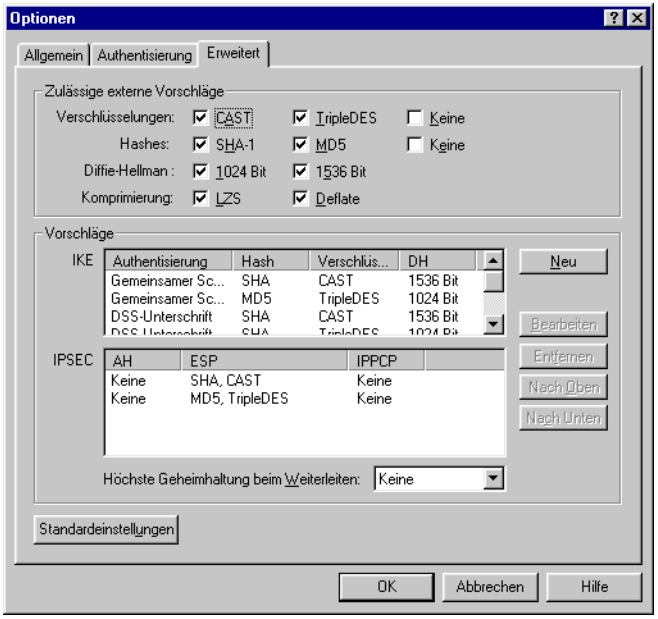


Abbildung 8-12. Die Registerkarte „Erweitert“

Vorschläge

Mit dem Teil **Vorschläge** auf der Registerkarte **Erweitert** können Sie Vorschläge hinzufügen, bearbeiten oder die Reihenfogle Ihrer vorhandenen Vorschläge neu ordnen. Auch diese Registerkarte sollte nur von erfahrenen IPsec-Benutzern bearbeitet werden. Die IKE- und IPsec-Vorschläge kennzeichnen die Vorschläge, die Sie anderen Benutzern unterbreiten sollen. Vorschläge müssen genau wie angegeben akzeptiert werden. Beachten Sie, daß in PGPnet mindestens ein und maximal 16 Vorschläge für IKE und IPsec-Vorschläge zulässig sind.

❑ **HINWEIS:** LZS und Deflate erhöhen die Leistung der langsamen Kommunikation, wie beispielsweise mit Modem und ISDN. LZS und Deflate verringern die Leistung der schnellen Kommunikation (z. B. mit Kabelmodem, DSL, T-1 und T-3). Das liegt an den allgemeinen Komprimierungsroutinen.

In der folgenden Tabelle werden die Arten der Authentisierung, Hashes, Chiffriercodes und Diffie-Hellmans erläutert, die in IKE-Vorschlägen verwendet werden.

Begriff	Beschreibung
Authentisierung	Bedeutung bestätigender Informationen, beispielsweise der Identität. Typen: Gemeinsamer Schlüssel (ein geheimer Schlüssel wird von zwei oder mehreren Benutzern gemeinsam verwendet) DSS (ein digitaler Standard für Unterschriften (Digital Signature Standard)) RSA-Unterschrift
Hash	Eine Hash-Funktion verwendet eine Eingabezeichenkette beliebiger Länge und konvertiert diese in eine Ausgabezeichenkette mit fester Länge. Typen: SHA-1 (Secure Hash Algorithm) MD5 (Message Digest Algorithm).

Begriff	Beschreibung
Verschlüsselung	Ein zur Ver- und Entschlüsselungen verwendeter Algorithmus. Typen: CAST TripleDES
DH (Diffie-Hellman)	Schlüsselabkommenprotokoll. Größe: 1024 Bit 1536 Bit.

In der folgenden Tabelle werden die Arten von AH, ESP und IPPCP erläutert, die in IPsec-Vorschlägen verwendet werden.

Begriff	Beschreibung
AH	Beim Authentisierungskopf handelt es sich um ein Unterprotokoll von IPsec, das nur die Authentisierung bearbeitet. Darüber hinaus werden damit verschiedene Teile des IP-Kopfes authentisiert. Besonders hilfreich, wenn eine Verschlüsselung nicht nötig ist, beispielsweise wenn eine ESP-Kommunikation durch ein Gateway mit AH getunnelt ist. Typen: SHA und MD5.
ESP	Encapsulating Security Payload ist ein Unterprotokoll von IPsec zur Bearbeitung der Verschlüsselung und der Authentisierung. Hash-Typen: Keine, SHA und MD5. Typen von Chiffriercodes: Keine, CAST und TripleDES.
IPPCP	IP-Payload Compression Protocol. Typen: Deflate und LZS. HINWEIS: LZS und Deflate erhöhen die Leistung der langsamen Kommunikation, wie beispielsweise mit Modem und ISDN. LZS und Deflate verringern die Leistung der schnellen Kommunikation (z. B. mit Kabelmodem, DSL, T-1 und T-3). Das liegt an den allgemeinen Komprimierungsroutinen.

Höchste Geheimhaltung beim Weiterleiten

Alle IPsec-Vorschläge verwenden dieselbe Diffie-Hellman-Einstellung: Keine, 1024 oder 1536.

IKE- oder IPsec-Vorschlag hinzufügen

So fügen Sie einen IKE- oder IPsec-Vorschlag hinzu

1. Zeigen Sie das Fenster **Optionen** (**Ansicht–>Optionen**) an.
2. Klicken Sie auf die Registerkarte **Erweitert**.
3. Klicken Sie auf **Neu**, und wählen Sie IKE oder IPsec.
4. Treffen Sie die entsprechende Auswahl im Popup-Fenster „IKE- oder IPsec-Vorschlag“.
5. Klicken Sie auf **OK**.
6. Wenn Sie einen IPsec-Vorschlag hinzufügen, wählen Sie die entsprechende Diffie-Hellman-Einstellung (Keine, 1024 und 1536) für die Option **Höchste Geheimhaltung beim Weiterleiten** aus. Alle IPsec-Vorschläge verwenden dieselbe Diffie-Hellman-Einstellung.
7. Klicken Sie auf **OK**.

IKE- oder IPsec-Vorschlag bearbeiten

So bearbeiten Sie einen IKE- oder IPsec-Vorschlag

1. Zeigen Sie das Fenster „Optionen“ (**Ansicht–>Optionen**) an.
2. Klicken Sie auf die Registerkarte **Erweitert**.
3. Wählen Sie den Vorschlag aus.
4. Klicken Sie auf **Bearbeiten**.
5. Nehmen Sie die entsprechende Änderung im Popup-Fenster „IKE- oder IPsec-Vorschlag“ vor.
6. Klicken Sie im Popup-Fenster auf **OK**.
7. Überprüfen Sie die Einstellung im angezeigten Feld **Höchste Geheimhaltung beim Weiterleiten**. Beachten Sie, daß alle IPsec-Vorschläge dieselbe Diffie-Hellman-Einstellung verwenden. Ändern Sie gegebenenfalls die Einstellung.

8. Klicken Sie in der Registerkarte**Erweitert** auf **OK**.

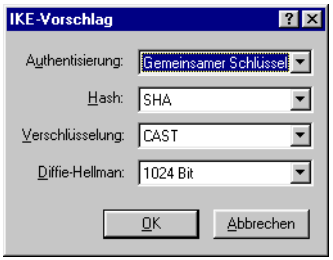


Abbildung 8-13. Dialogfeld „IKE-Vorschlag“

Abbildung 8-14. Dialogfeld „IPsec“

IKE- oder IPsec-Vorschlag entfernen

So entfernen Sie einen IKE- oder IPsec-Vorschlag

1. Zeigen Sie das Fenster **Optionen** (**Ansicht–>Optionen**) an.
2. Klicken Sie auf die Registerkarte **Erweitert**.
3. Klicken Sie auf den Vorschlag.
4. Klicken Sie auf **Entfernen**.
5. Klicken Sie auf **OK**.

IKE- oder IPsec-Vorschläge neu anordnen

So ordnen Sie IKE- oder IPsec-Vorschläge neu an

1. Zeigen Sie das Fenster **Optionen** (**Ansicht–>Optionen**) an.
2. Klicken Sie auf die Registerkarte **Erweitert**.
3. Wählen Sie den Vorschlag aus.
4. Klicken Sie auf **Nach Oben**, um die Vorschläge nach oben zu verschieben. Klicken Sie auf **Nach Unten**, um die Vorschläge nach unten zu verschieben.
5. Klicken Sie auf **OK**.

Schaltfläche „Standardeinstellungen“

Mit dieser Schaltfläche stellen Sie die Standardeinstellungen für alle Felder in diesem Bildschirm wieder her. In den meisten Fällen reichen die Standardeinstellungen zur Erstellung von SAs und zur Verwendung von PGPnet aus.

Adapter einstellen: Ändern Ihrer sicheren Netzwerkschnittstelle

Beim Installieren von PGPnet wählen Sie die zu sichernde Netzwerkschnittstelle auf Ihrem Computer aus. Bei Ihrer Netzwerkschnittstelle handelt es sich normalerweise um eine Ethernet-, eine DFÜ- oder eine Remote Access WAN-Karte (Ihr Modem).

Verwenden Sie die Funktion „Adapter einstellen“ von PGPnet (**Start–>Programme–>PGP–>Adapter einstellen**) in den folgenden Fällen:

- Wenn Sie eine andere Netzwerkschnittstelle sichern möchten.
- Wenn Ihr Rechner Ihre Netzwerkprotokolle und die Adapterbindungen überprüft. Tritt dieser Fall ein, werden Sie von PGPnet dazu aufgefordert, Ihr System neu zu starten und die Funktion „Adapter einstellen“ von PGPnet auszuführen, um eine Netzwerkschnittstelle erneut zu sichern.

So sichern Sie eine andere Netzwerkschnittstelle (Windows 95/98)

1. Wählen Sie im Menü **Start** (**Start–>Programme–>PGP–>Adapter einstellen**) die Funktion „Adapter einstellen“ aus. Das Dialogfeld „Adapter einstellen“ von PGPnet wird an Ihrem Bildschirm mit einer Auflistung aller anderen Adapter angezeigt.

2. Wählen Sie die entsprechende Netzwerkschnittstelle, und klicken Sie anschließend auf **OK**. Sie werden von PGP zum Neustart Ihres Rechners aufgefordert.

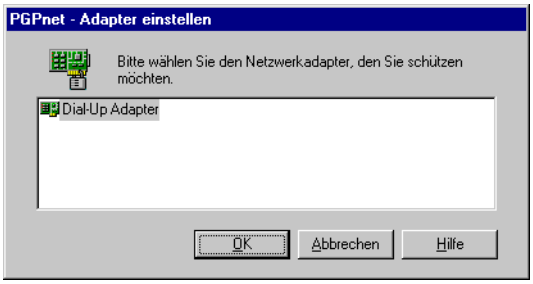


Abbildung 8-15. Auswahldialogfeld „Adapter einstellen“

3. Starten Sie Ihren Rechner neu (zwingend für die gesamte Netzwerkfunktionalität).

So sichern Sie eine andere Netzwerkschnittstelle (Windows NT)

1. Wählen Sie im Menü „Start“ (**Start–>Programme–>PGP–>Adapter einstellen**) die Funktion „Adapter einstellen“ aus. Das Dialogfeld „Adapter einstellen“ von PGPnet wird an Ihrem Bildschirm angezeigt. Lesen Sie den Text im Dialogfeld.

2. Klicken Sie auf **OK**, um eine andere Netzwerkschnittstelle zu sichern. PGP überprüft die Bindungen Ihres Rechners und löst selbst die Bindung zum aktuellen Adapter.

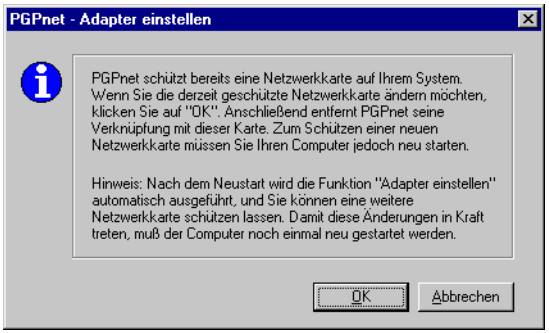


Abbildung 8-16. Dialogfeld „Adapter einstellen“

3. Starten Sie Ihren Rechner neu, wenn Sie dazu aufgefordert werden.
4. Beim Neustart wird die Funktion „Adapter einstellen“ automatisch erneut gestartet, und Sie werden aufgefordert, einen Adapter für die Bindung mit PGPnet auszuwählen.
5. Wählen Sie die entsprechende Netzwerkschnittstelle aus. PGP überprüft die Bindungen Ihres Rechners und fordert Sie auf, den Rechner neu zu starten.

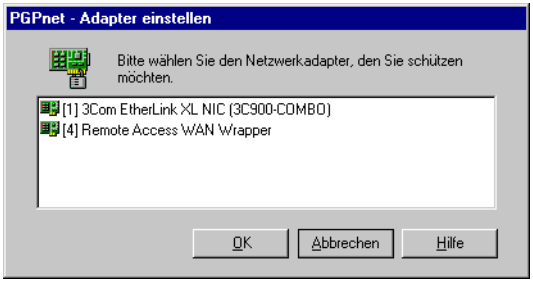


Abbildung 8-17. Auswahldialogfeld „Adapter einstellen“

6. Starten Sie Ihren Rechner neu (zwingend für die gesamte Netzwerkfunktionalität).

So sichern Sie eine Netzwerkschnittstelle nach der Bindungsüberprüfung erneut (Windows NT)

1. Starten Sie Ihren Rechner neu, wenn Sie dazu aufgefordert werden.
2. Beim Neustart wird die Funktion „Adapter einstellen“ automatisch gestartet, und Sie werden aufgefordert, einen Adapter für die Bindung mit PGPnet auszuwählen.
3. Wählen Sie die entsprechende Netzwerkschnittstelle aus. PGP überprüft die Bindungen Ihres Rechners und fordert Sie auf, Ihren Rechner neu zu starten.

Starten Sie Ihren Rechner neu (zwingend für die gesamte Netzwerkfunktionalität).

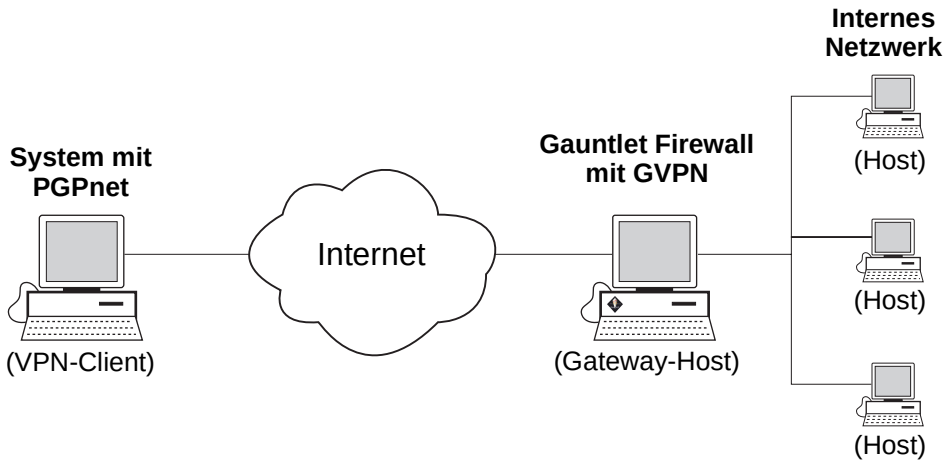
VPN mit PGPnet erstellen 9

In diesem Kapitel wird eine der Verwendungsarten von PGPnet beschrieben, nämlich die Festlegung eines VPN mit einer Gauntlet Firewall mit Hilfe der Funktion GVPN.

In diesem Abschnitt werden wir beispielsweise mit dem IKE-Client-Modus und der auf Zertifikaten basierenden Authentisierung eine vertrauenswürdige Verknüpfung zwischen den beiden Geräten erstellen. Dieser Typ der VPN-Konfiguration ist für Situationen geeignet, in denen ein Firmenmitarbeiter mit einem Internetdienstanbieter (Internet Service Provider) durch eine Firewall über das Internet auf das Unternehmensnetzwerk zugreift, oder Mitarbeiter die IP-7Adresse dynamisch, beispielsweise über DHCP, beziehen.

Topologie

Die Topologie eines solchen VPN sieht folgendermaßen aus:



Firewall-Begriffe

Es ist unerläßlich, die folgenden Firewall-Begriffe zu kennen, wenn Sie ein VPN mit einer Gauntlet Firewall erstellen.

- **Zuvor vereinbartes gemeinsames Geheimnis und auf Zertifikaten basierende Authentisierung** – Gauntlet Firewalls unterstützen zwei Authentisierungsmethoden. Zuvor vereinbartes gemeinsames Geheimnis: Bei dieser Methode konfigurieren eine oder mehrere Personen eine Verknüpfung mit einer zuvor vereinbarten Paßphrase für die Authentisierung. Bei der auf Zertifikaten basierenden Authentisierung tauschen die beiden Geräte der Verknüpfung die Zertifikate für die Authentisierung untereinander aus.

- **Vertrauenswürdige und private Verknüpfungen** – In einer vertrauenswürdigen Verknüpfung umgehen Daten, die von einem VPN-Client gesendet werden, die Proxies der Firewall und werden direkt an das vorgesehene Ziel weitergeleitet. Hiermit umgehen Sie die Sicherheitsfunktionen der Firewall. Wählen Sie diese Vorgehensweise also nur, wenn Sie dem VPN-Client vollkommen vertrauen, wenn es sich beispielsweise um einen Mitarbeiter Ihres Unternehmens handelt. Eine private Verknüpfung umgeht die Proxies nicht. Das bedeutet, daß der VPN-Client sich bei der Firewall authentisieren muß, um Zugriff auf das vorgesehene Ziel zu erhalten.

- **Interne und externe Schnittstellen** – Firewalls haben zwei physische Schnittstellen: Eine für das Internet (der Außenwelt) und eine für das interne Netzwerk. Jede hat eine eigene IP-Adresse. Die Schnittstelle, die mit dem Internet verknüpft ist, wird äußere oder externe Schnittstelle genannt. Die Schnittstelle für die Verknüpfung mit dem internen Netzwerk wird innere oder interne Schnittstelle genannt. In den meisten Fällen schützt die Firewall das interne Netzwerk vor dem, was über die externe Schnittstelle eingeht.

- **IKE-Client und IPsec mit IKE-Modi** – Gauntlet Firewall unterstützt zwei Verknüpfungsmodi: Der IKE-Client arbeitet nur mit der auf Zertifikaten basierenden Authentisierung, unterstützt jedoch VPN-Clients, die Ihre IP-Adresse über DHCP beziehen (d. h., sie verfügen nicht über eine feste IP-Adresse, sondern ihnen wird bei jeder Anmeldung eine andere IP-Adresse zugeordnet). IPsec mit IKE unterstützt die auf Zertifikaten basierende Authentisierung oder die Authentisierung mit gemeinsamen Geheimnissen, erfordert jedoch, daß alle Hosts oder Teilnetze über feste IP-Adressen verfügen (d. h. DHCP wird unterstützt).

Der Modus IKE-Client ist normalerweise besser für Konfigurationen von VPN-Client an VPN-Gateway geeignet (z. B. PGPnet an Firewall), während der Modus IPsec mit IKE besser für Konfigurationen von VPN-Gateway an VPN-Gateway (Firewall an Firewall) dient.

VPN festlegen

Um zwischen dem System ein VPN mit dem IKE-Client-Modus und der auf Zertifikaten basierenden Authentisierung mit PGPnet und der Gauntlet Firewall festzulegen, müssen Sie folgende Schritte ausführen:

- Einrichten von auf Zertifikaten basierender Authentisierung
- Konfigurieren der Gauntlet Firewall
- Konfigurieren von PGPnet.
- Festlegen der VPN mit PGPnet

Alle diese Elemente werden im folgenden Abschnitt beschrieben.

Auf Zertifikaten basierende Authentisierung einrichten

Bei der Einrichtung des VPN müssen die beiden Geräte zuerst für die Verwendung der auf Zertifikaten basierenden Authentisierung konfiguriert werden. Es werden gültige Zertifikate für die Vertrauensfestlegung zwischen den beiden Geräten im VPN benötigt.

Weitere Anweisungen zum Erhalt von gültigen X.509-Zertifikaten für eine Gauntlet Firewall finden Sie im Benutzerhandbuch „Gauntlet Firewall Global Virtual Private Network“ für Windows NT oder UNIX (abhängig von der verwendeten Version der Gauntlet Firewall). Die Unterlagen wurden als Kopie mit der Firewall geliefert und sind darüber hinaus auch auf der Installations-CD und als PDF-Datei erhältlich.

Um ein gültiges X.509-Zertifikat für PGPnet (VPN-Client) zu erhalten, müssen Sie das Root-CA-Zertifikat bei der Zertifizierungsinstanz (CA), der das Vertrauen beider Geräte im VPN zugeordnet wurde, (in diesem Fall Ihre Unternehmens-CA) abrufen, und Ihrem Schlüsselbund hinzufügen. Fordern Sie anschließend von der CA ein Zertifikat für PGPnet und rufen Sie dieses nach dessen Ausstellung ab. Diese Funktionen werden alle mit PGPkeys ausgeführt.

Gültiges X.509-Zertifikat für PGPnet (VPN-Client) erhalten:

1. Starten Sie Ihren Webbrowser und stellen Sie eine Verbindung zur CA-Anmeldung her.

   Wenn Ihr Unternehmen beispielsweise den Net Tools PKI Server als Zertifizierungsinstanz verwendet, hat die URL in etwa dieses Format: **https://10.0.1.54**

   Falls Ihnen die URL für diese Site nicht bekannt ist, erfragen Sie sie beim zuständigen PGP- bzw. PKI-Administrator.

2. Suchen und Prüfen des Root-CA-Zertifikats.

   Wenn in Ihrem Unternehmen beispielsweise der Net Tools PKI Server verwendet wird, können Sie auf die Verknüpfung zum Herunterladen des CA-Zertifikats klicken und anschließend das Root-CA-Zertifikat prüfen.

3. Kopieren Sie den Schlüsselblock (einschließlich der Erweiterungen „– Zugeordnetes Zertifikat –“ und der Zertifikatserweiterungen) für das Root-CA-Zertifikat, und fügen Sie ihn in das PGPkeys-Fenster ein.

   Das Dialogfeld zum Importieren von Schlüsseln wird angezeigt, und das Root-CA-Zertifikat wird in Ihren Schlüsselbund importiert.

4. Unterschreiben Sie das Root-CA-Zertifikat mit Ihrem Schlüssel, um diesem Gültigkeit zu verleihen.

   Sie möchten möglicherweise das Root-CA-Zertifikat zu einem höhergestellten Schlüsselverwalter machen, so daß Sie Zertifikaten, die damit unterschrieben wurden, automatisch vertrauen können.

5. Zeigen Sie die Eigenschaften an und legen Sie als Vertrauen **Vertrauenswürdig** fest.

6. Wählen Sie im Menü „Bearbeiten“ von PGPkeys den Befehl **Optionen**, und klicken Sie anschließend auf die Registerkarte **CA**.

   Die Registerkarte „CA“ wird angezeigt.

7. Geben Sie die URL für die Root-CA in das Textfeld für die **Certificate Authority URL** ein.

   Hierbei handelt es sich um dieselbe URL, die Sie in Schritt 1 verwendet haben.

   Falls Sie über eine separate URL zur Anforderung der zurückgenommenen CA verfügen, geben Sie diese in das zugehörige Textfeld ein. Falls Ihnen die URL der zurückgenommenen CA nicht bekannt ist, belassen Sie dieses Feld leer oder erfragen Sie sie beim zuständigen PGP- bzw. PKI-Administrator.

8. Wählen Sie im Feld **Typ** den vom Unternehmen verwendeten PKI-Server. Net Tools PKI Server, VeriSign OnSite oder Entrust.

9. Klicken Sie auf die Schaltfläche „Zertifikat auswählen“, und wählen Sie anschließend das Root-CA-Zertifikat aus.

10. Klicken Sie auf **OK**.

11. Wählen Sie im Bildschirm „PGPkeys“ Ihr Schlüsselpaar aus (oder den privaten Schlüssel), öffnen Sie das Menü „Schlüssel“, wählen Sie **Hinzufügen** und anschließend **Zertifikat** aus.

    Daraufhin wird das Dialogfeld „Zertifikatsattribute“ angezeigt.

12. Verifizieren Sie die Zertifikatsattribute und verwenden Sie die Schaltflächen „Hinzufügen“, „Bearbeiten“ und „Entfernen“, um erforderliche Änderungen vorzunehmen.

13. Klicken Sie auf **OK**.

    Das Dialogfeld zur Eingabe der PGP-Paßphrase wird angezeigt.

14. Geben Sie die Paßphrase für Ihr Schlüsselpaar ein, und klicken Sie anschließend auf **OK**.

    Die Zertifikatsanfrage wird automatisch an den CA-Server geschickt. Der Server authentisiert sich automatisch bei Ihrem Computer und nimmt anschließend Ihre Anfrage entgegen.

    Zu diesem Zeitpunkt überprüft der PGP- bzw. PKI-Administrator Ihres Unternehmens die Informationen, die Sie in der Anfrage eingetragen haben. Die Identifikationsinformationen und der öffentliche Schlüssel werden kombiniert und digital mit der eigenen Unterschrift der CA unterschrieben. Das ist das gesamte, unterschriebene Paket für die Erstellung Ihres neuen Zertifikats.

    Sie erhalten eine E-Mail vom Administrator (unter der mit dem Schlüsselpaar angegebenen E-Mail-Adresse), die Sie über das abholbereite Zertifikat informiert.

15. Um Ihr Zertifikat abzurufen und es Ihrem PGP-Schlüsselpaar hinzuzufügen, öffnen Sie PGPkeys (falls notwendig) und wählen den PGP-Schlüssel, für den Sie das Zertifikat angefordert haben.

16. Öffnen Sie das Menü „Server“, und wählen Sie **Zertifikat abrufen**.

    PGP stellt eine Verbindung mit dem CA-Server her, um Ihr neues X.509-Zertifikat automatisch abzurufen und Ihrem PGP-Schlüssel hinzuzufügen.

Gauntlet Firewall konfigurieren

Der nächste Schritt zur Festlegung eines VPN zwischen einem System mit PGPnet und einer Gauntlet Firewall ist die entsprechende Konfiguration der Firewall.

HINWEIS: Dieses Verfahren setzt eine funktionstüchtige Gauntlet Firewall voraus. Weitere Informationen finden Sie in der im Lieferumfang der Firewall enthaltenen Dokumentation.

WICHTIG: Damit ein VPN zwischen einem System mit PGPnet und einer Gauntlet Firewall Version 5.0 ordnungsgemäß arbeitet, muß die Firewall das standardmäßige Gateway für die Hosts im sicheren Teilnetz sein. Wenn das standardmäßige Gateway und das sichere Gateway verschieden sind (das standardmäßige Gateway ist z. B. ein Router), können Probleme beim Weiterleiten der Rückantworten in einem lokalen Ethernet-LAN auftreten.

Diese Verfahrensweise betrifft die Gauntlet Firewall für Windows NT und die Gauntlet Firewall für UNIX. Bedeutende Unterschiede zwischen den beiden werden im Text beschrieben.

So konfigurieren Sie eine Gauntlet Firewall für ein VPN:

1. Im Gauntlet Firewall Manager klicken Sie auf die Registerkarte VPN.

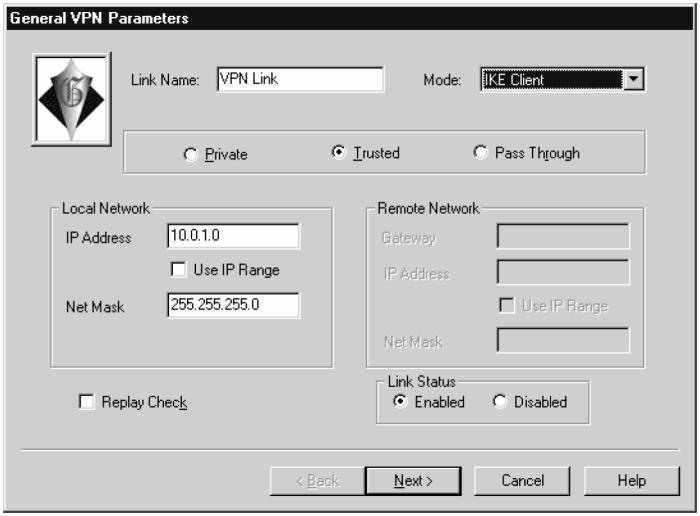
   Der Bildschirm VPN wird angezeigt.

   (In Gauntlet Firewall für UNIX wählen Sie den Ordner **VPNs** und klikken anschließend auf **Links**.)

2. Klicken Sie auf die Schaltfläche **Add**.

   Der Bildschirm mit den allgemeinen VPN-Parametern wird angezeigt.

   (In Gauntlet Firewall für UNIX heißt dieser Bildschirm „Add GVPN Link Configuration“.)



3. Fügen Sie eine VPN-Verknüpfung mit den folgenden Einstellungen hinzu:

   Link Name: Geben Sie einen bezeichnenden Namen ein

   Mode: IKE-Client

   Link Type: Vertrauenswürdig (Trusted)

   IP Address: Geben Sie nach der Firewall die IP-Adresse des Hosts oder des Teilnetzes aus dem VPN ein (normalerweise konfigurieren Sie ein Teilnetz hier, so daß Sie nicht nur auf einen Computer Zugriff haben).

   Use IP Range: Deaktiviert

   Net Mask: Geben Sie die Teilnetz-Maske des im Feld „IP-Adresse“ eingegebenen Teilnetzes oder 255.255.255.255 ein, wenn es sich bei der im Feld „IP-Adresse“ angegebenen um eine Host- und nicht um eine Teilnetz-IP-Adresse handelt.

HINWEIS: Die hier für den von Ihnen konfigurierten Host oder das Teilnetz eingegebenen IP-Adress- und Netz-Maskeninformationen müssen auch in PGPnet eingegeben werden.

   Replay Check: Deaktiviert

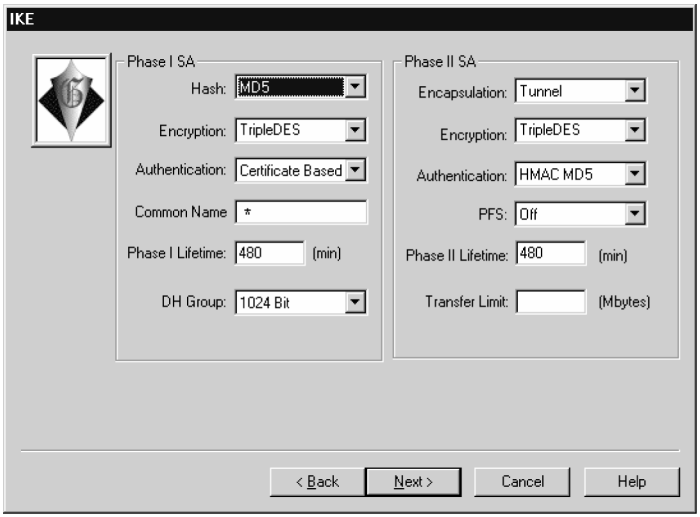
   Link Status: Aktiviert

4. Klicken Sie auf **Next**, um zum nächsten Bildschirm zu wechseln.

   (In Gauntlet Firewall für UNIX klicken Sie auf **Link Details**.)

   Der Bildschirm „IKE“ wird angezeigt.

   (Dies ist der Bildschirm „Edit IKE Configuration“ in Gauntlet Firewall für UNIX.)



   Verwenden Sie die folgenden Einstellungen:

   Phase I SA

   Hash: MD5

   Encryption: TripleDES

   Authentication: Certificate Based (Auf Zertifikaten basierend)

   Common Name: * (In Gauntlet Firewall für UNIX leer lassen.)

   Phase I Lifetime: 480

   DH Group: 1024 Bit

   Phase II SA

   Encapsulation: Tunnel

   Encryption: TripleDES

   Authentication: HMAC MD5

   PFS: Aus

Phase II Lifetime: 480

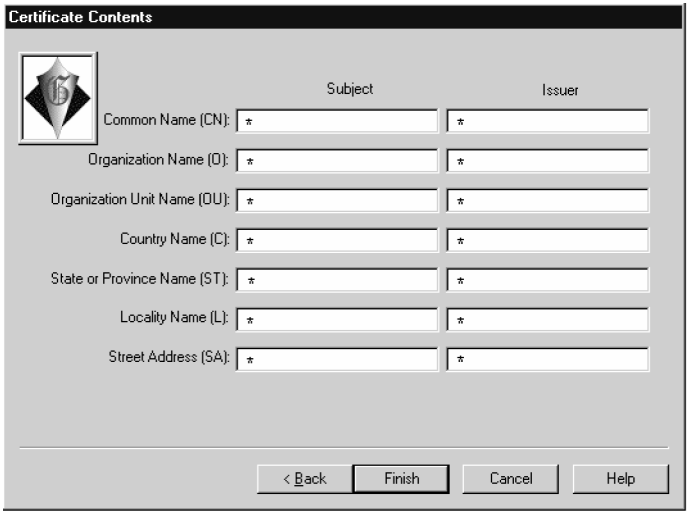
Transfer Limit: Leer lassen

5. Klicken Sie auf **Next**, um zum nächsten Bildschirm zu wechseln.

   (In Gauntlet Firewall für UNIX klicken Sie auf die Schaltfläche **Certificate Contents**.)

   Der Bildschirm „Certificate Contents“ wird angezeigt. Jedes Feld sollte ein Sternchen (*) enthalten.

   (Dies ist der Bildschirm „Client Certificate Configuration“ in Gauntlet Firewall für UNIX.) Alle Felder sollten leer sein. Geben Sie keine Sternchen ein.



6. Klicken Sie auf **Finish**, und übernehmen Sie die Änderungen für die Firewall.

   (Klicken Sie in Gauntlet Firewall für UNIX auf **OK**, und übernehmen Sie anschließend die Änderungen in die Firewall.)

PGPnet konfigurieren

Der nächste Schritt zur Festlegung eines VPN zwischen einem System mit PGPnet und einer Gauntlet Firewall ist die entsprechende Konfiguration von PGPnet.

HINWEIS: Dieses Verfahren setzt eine ordnungsgemäß funktionierende Installation von PGP 6.5 oder höher mit der installierten PGPnet-Komponente voraus.

In diesem Beispiel werden Kommunikationen mit einem unsicheren Host oder Teilnetz hinter einem sicheren Gateway konfiguriert.

HINWEIS: Die Kommunikation mit einem sicheren Host hinter einem sicheren Gateway erfordert die Version 5.0 oder höher der Gauntlet Firewall für UNIX oder die Version 5.5 oder höher der Gauntlet Firewall für Windows NT.

So konfigurieren Sie PGPnet mit dem Assistenten zum Hinzufügen von Hosts für das VPN:

1. Öffnen Sie PGPnet, und wählen Sie die Registerkarte **Hosts**.
2. Klicken Sie auf der Registerkarte „Hosts“ auf die Schaltfläche **Hinzufügen**.

   Der „Assistent zum Hinzufügen“ von Hosts wird angezeigt.
3. Lesen Sie den Inhalt des Bildschirms, und klicken Sie anschließend auf **Weiter**.
4. Wählen Sie **Gateway** für den Host-Typ aus, und klicken Sie anschließend auf **Weiter**.

   Da Sie mit einem Host hinter einer Firewall kommunizieren möchten, müssen Sie zuerst den Gateway-Host (die Firewall) und anschließend den Host hinter der Firewall konfigurieren.
5. Geben Sie einen beschreibenden Namen für den Gateway-Host ein, und klicken Sie anschließend auf **Weiter**.
6. Geben Sie die IP-Adresse des Gateway-Hosts ein (d. h., die IP-Adresse der externen Schnittstelle der Firewall), und klicken Sie anschließend auf **Weiter**.

7. Aktivieren Sie **Verwenden Sie ausschließlich Verschlüsselungschutz mit öffentlichen Schlüsseln**, und klicken Sie anschließend auf **Weiter**.

   Sie werden aufgefordert, jetzt einen Host- oder Teilnetz-Eintrag hinzuzufügen.

8. Aktivieren Sie **Ja**, und klicken Sie auf **Weiter**.

9. Treffen Sie die entsprechende Auswahl (Host oder Teilnetz), und klicken Sie anschließend auf **Weiter**.

   Das ist der Host oder das Teilnetz hinter der Firewall, mit dem Sie kommunizieren möchten.

WICHTIG: Sie müssen in PGPnet dieselben Konfigurationsvorgänge für einen Host oder ein Teilnetz durchführen wie bei der Konfiguration der Gauntlet Firewall. Wenn Sie beispielsweise beim Konfigurieren der Gauntlet Firewall in Schritt 3 die IP-Adresse und die Teilnetz-Maske eines Teilnetzes eingegeben haben, müssen Sie hier in PGPnet die IP-Adresse und Teilnetz-Maske desselben Teilnetzes eingeben.

---

10. Aktivieren Sie **Unsichere Kommunikation zulassen**, und klicken Sie auf **Weiter**.

11. Geben Sie dem Host oder dem Teilnetz, das Sie hinzufügen, einen beschreibenden Namen, und klicken Sie anschließend auf **Weiter**.

12. Geben Sie die IP-Adresse des Hosts oder des Teilnetzes ein (und gegebenenfalls die Teilnetz-Maske), und klicken Sie auf **Weiter**.

    Diese Informationen zur IP-Adresse ***müssen*** mit den in Schritt 3 zur Konfiguration der Gauntlet Firewall eingegebenen Informationen übereinstimmen.

13. Fügen Sie Ihrer Konfiguration so viele Hosts und / oder Teilnetze hinzu, wie nötig. Wenn Sie die gewünschten Hosts und Teilnetze alle hinzugefügt haben, wählen Sie „Nein“ und klicken auf **Weiter**.

14. Wenn für die Authentisierung kein Schlüssel eingerichtet wurde, wird ein Bildschirm angezeigt, auf dem Sie aufgefordert werden, einen Authentisierungsschlüssel auszuwählen. Klicken Sie auf **Zertifikat auswählen**, wählen Sie das hinzugefügte X.509-Zertifikat aus, und klicken Sie anschließend auf **Weiter**.

15. Klicken Sie auf **Fertig stellen**.

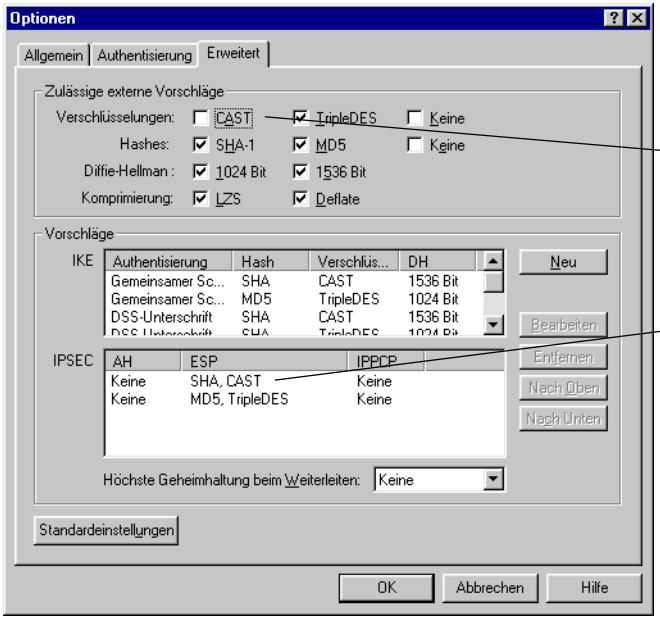
16. Wenn Sie einen Authentisierungsschlüssel angegebenen haben werden Sie aufgefordert, Ihre Paßphrase einzugeben. Geben Sie die Paßphrase ein, und klicken Sie auf **OK**.

    Die Registerkarte „Hosts“ wird angezeigt.

17. Verwenden Sie die standardmäßigen PGPnet-Einstellungen, außer Sie möchten den Ablaufwert der Gültigkeit einer SA festlegen (auf der Registerkarte „Allgemein“ im Fenster „Optionen“).

WICHTIG: Wenn Sie ein VPN mit einem Host oder einem Teilnetz hinter einer Gauntlet Firewall für Windows NT Version 5.0 festlegen, müssen Sie CAST auf der Liste der zulässigen externen Vorschläge deaktivieren. Öffnen Sie hierfür in der Menüleiste für PGPnet das Menü „Ansicht“, und wählen Sie die Option „Optionen“ aus. Klicken Sie auf die Registerkarte „Erweitert“, und aktivieren Sie anschließend die Option CAST.

Wenn Sie ein VPN mit einem Host oder einem Teilnetz hinter einer Gauntlet Firewall für UNIX Version 5.0 festlegen, müssen Sie den IPsec-Vorschlag (in diesem Beispiel MD5, TripleDES) auf der Liste der IPsec-Vorschläge an die oberste Stelle verschieben. Gehen Sie hierzu wie folgt vor: Öffnen Sie in PGPnet das Menü „Ansicht“, und wählen Sie den Befehl „Optionen“ aus. Klicken Sie auf die Registerkarte „Erweitert“, und suchen Sie die IPsec-Vorschläge. Klicken Sie in der Spalte „ESP“ auf die Einträge MD5 und Triple-DES. Anschließend klicken Sie auf die Schaltfläche „Nach Oben“, bis MD5 und Triple-DES oben auf der Liste stehen, und klicken dann auf OK.



Für ein VPN mit einer Gauntlet Firewall für Windows NT 5.0 muß CAST deaktiviert sein.

Für ein VPN mit einer Gauntlet Firewall für UNIX 5.0 muß der verwendete IPsec-Vorschlag (in diesem Beispiel MD5, TripleDES) ganz oben auf der Liste der IPsec-Vorschläge stehen.

VPN mit PGPnet festlegen

Der letzte Schritt zur Festlegung eines VPN zwischen einem System mit PGPnet und einer Gauntlet Firewall ist die eigentliche Festlegung des VPN mit PGPnet (in der PGPnet-Terminologie Sicherheitsverknüpfung genannt).

So legen Sie das VPN mit PGPnet fest:

1. Öffnen Sie PGPnet und klicken Sie auf die Registerkarte **Hosts**.
2. Klicken Sie auf den Namen Ihres konfigurierten Gateway-Hosts (die Firewall).
3. Wenn Ihr X.509-Zertifikat bereits als Authentisierungsschlüssel bestimmt wurde, können Sie zu Schritt 10 übergehen. Ist dies nicht der Fall, oder Sie sind sich nicht sicher, fahren Sie mit Schritt 4 fort.
4. Öffnen Sie das Menü „Ansicht“, und wählen Sie **Optionen**.

   Der Bildschirm „Optionen“ wird angezeigt.
5. Klicken Sie auf die Registerkarte **Authentisierung**.

6. Klicken Sie auf der Registerkarte „Authentisierung“ auf die Option **Zertifikat auswählen**.

   Eine Liste mit X.509-Zertifikaten in Ihrem Schlüsselbund wird angezeigt.

7. Klicken Sie auf den Namen des Zertifikats, das Sie für Ihre eigene Authentisierung verwenden möchten, und klicken Sie auf **OK**.

8. Klicken Sie erneut auf **OK**, um den Bildschirm „Optionen“ zu schließen.

   In einem Dialogfeld werden Sie zur Eingabe der Paßphrase für den ausgewählten Schlüssel aufgefordert.

9. Geben Sie sie ein, und klicken Sie anschließend auf **OK**.

   Der Bildschirm „Hosts“ wird angezeigt.

10. Klicken Sie auf das Pluszeichen neben dem von Ihnen konfigurierten Gateway-Host (Firewall).

    Eine Liste mit Host-Einträgen (Hosts oder Teilnetze hinter dem Gateway) wird angezeigt.

11. Um die Kommunikation mit einem unsicheren Host oder Teilnetz zu starten, müssen Sie auf den Host-Eintrag klicken, mit dem Sie eine Verbindung herstellen möchten und anschließend auf **Verbinden** klicken.

    Wurde die Konfiguration ordnungsgemäß ausgeführt, wird mit den IPsec-Protokollen eine Sicherheitsverknüpfung zwischen dem VPN-Client (PGPnet) und der Gauntlet Firewall hergestellt.

    Bei der Erstellung der Sicherheitsverknüpfung wird ein grüner Punkt rechts neben dem Gateway-Host in der Spalte SA angezeigt.

12. Klicken Sie auf die Registerkarte **Status**.

    Die Sicherheitsverknüpfung wird aufgeführt.

13. Wenn die Sicherheitsverknüpfung nicht aufgeführt wird, klicken Sie auf die Registerkarte **Protokoll** um nachzuprüfen, wo das Problem liegt.

❑ **HINWEIS:** Weitere Informationen über das Festlegen von Sicherheitsverknüpfungen, über Protokolleinträge zu Fehlerbeschreibungen und detaillierte PGPnet-Konfigurationsinformationen erhalten Sie im Kapitel „PGPnet“.

Problembehebung in PGP A

In diesem Abschnitt finden Sie Informationen zu Problemen, die bei der Arbeit mit PGP möglicherweise auftreten, außerdem erhalten Sie Lösungsvorschläge.

Fehler	Ursache	Lösung
Authentisierung durch entfernte SKEP-Verbindung abgewiesen	Der Benutzer an der entfernten Seite der Schlüsselteil-Netzwerkverbindung hat den Schlüssel abgewiesen, den Sie zu Authentisierungszwecken vorgelegt haben.	Verwenden Sie einen anderen Schlüssel zur Authentisierung der Schlüsselteil-Netzwerkverbindung bzw. versichern Sie dem entfernten Benutzer, daß der von Ihnen verwendete Schlüssel gültig ist.
Beim Erstellen eines Schlüsselbundes oder der exportierten Datei ist ein Fehler aufgetreten.	Das Schreiben von Daten in eine bestimmte Datei war nicht möglich.	Möglicherweise ist Ihre Festplatte voll. Eventuell befindet sich die Datei auch auf einer Diskette, die nicht in das Diskettenlaufwerk eingelegt wurde.
Beim Öffnen oder Erstellen des Schlüsselbundes oder der Ausgabedatei ist ein Fehler aufgetreten.	Eine erforderliche Datei konnte nicht geöffnet werden.	Vergewissern Sie sich, daß die Einstellung in den PGP-Voreinstellungen richtig ist. Falls Sie in letzter Zeit Dateien in dem Verzeichnis gelöscht haben, in dem PGP installiert wurde, müssen Sie möglicherweise das Produkt erneut installieren.
Der angegebene Schlüssel kann nur für Unterschriften verwendet werden. Die Verschlüsselung war daher nicht möglich.	Der ausgewählte Schlüssel darf nur für Unterschriften verwendet werden.	Wählen Sie einen anderen Schlüssel aus, oder erzeugen Sie einen neuen, mit dem Daten verschlüsselt werden können.
Der angegebene Schlüssel kann nur zur Verschlüsselung verwendet werden. Die Unterschrift war daher nicht möglich.	Der ausgewählte Schlüssel darf nur zur Verschlüsselung verwendet werden.	Wählen Sie einen anderen Schlüssel aus, oder erzeugen Sie einen neuen, mit dem Daten unterschrieben werden können.
Der angegebene Schlüssel konnte in Ihrem Schlüsselbund nicht gefunden werden.	Der zur Entschlüsselung der aktuellen Nachricht benötigte Schlüssel befindet sich nicht in Ihrem Schlüsselbund.	Bitten Sie den Absender der Nachricht, diese erneut zu senden, und vergewissern Sie sich, daß die Nachricht mit Ihrem öffentlichen Schlüssel verschlüsselt wird.

Fehler	Ursache	Lösung
Der gewünschte Vorgang kann nicht ausgeführt werden, da der Ausgabepuffer zu klein ist.	Die Ausgabe ist für die Bearbeitung im internen Puffer zu umfangreich.	Beim Verschlüsseln oder Unterschreiben müssen Sie die Nachricht möglicherweise unterteilen und jeweils kleinere Teile verschlüsseln/unterschreiben. Beim Entschlüsseln oder Verifizieren bitten Sie den Absender, jeweils kleinere Teile zu verschlüsseln/zu unterschreiben und diese erneut zu senden.
Der Schlüsselbund enthält ein fehlerhaftes PGP-Paket.	Die PGP-Nachricht, mit der Sie derzeit arbeiten, wurde beschädigt. Möglicherweise wurde auch Ihr Schlüsselbund beschädigt.	Falls die Nachricht beschädigt ist, bitten Sie den Absender, sie erneut zu senden. Falls Ihr Schlüsselbund beschädigt ist, versuchen Sie ihn mit Hilfe der Sicherungskopie des Schlüsselbundes wiederherzustellen.
Die Aktion konnte aufgrund eines ungültigen Dateivorgangs nicht ausgeführt werden.	Daten in einer bestimmten Datei konnten entweder nicht gelesen oder nicht geschrieben werden.	Die Datei ist wahrscheinlich beschädigt. Versuchen Sie gegebenenfalls, die PGP-Voreinstellungen dahingehend zu ändern, daß eine andere Datei verwendet wird.
Die angegebene Benutzer-ID ist in dem ausgewählten Schlüssel bereits vorhanden. Sie wurde daher nicht hinzugefügt.	Ein Schlüssel kann nicht um eine Benutzer-ID ergänzt werden, wenn bereits eine identische im jeweiligen Schlüssel vorhanden ist.	Versuchen Sie, eine andere Benutzer-ID hinzuzufügen, oder löschen Sie zuerst die identische Benutzer-ID.
Die Bewertungszeit zur PGP-Verschlüsselung und Unterschrift ist abgelaufen. Der Vorgang wurde abgebrochen.	Der Testzeitraum für das Produkt ist abgelaufen.	Laden Sie die Freeware-Version herunter, oder kaufen Sie die im Handel erhältliche Version des Produkts.
Die Datei mit den Verwaltungseinstellungen konnte nicht gefunden werden	Die Datei mit den Einstellungen, die die vom PGP-Administrator (hierbei handelt es sich üblicherweise um einen Mitarbeiter der IS/IT-Abteilung) eingerichtete Konfiguration enthält, ist nicht vorhanden.	Installieren Sie PGP erneut auf Ihrem Rechner. Falls die Meldung daraufhin noch immer angezeigt wird, wenden Sie sich an den PGP-Administrator und informieren ihn bezüglich dieser Meldung. Es muß ein neues PGP-Installationsprogramm für Sie erzeugt werden.
Die eingegebene Paßphrase stimmt nicht mit der Paßphrase des Schlüssels überein.	Sie haben eine falsche Paßphrase eingegeben.	Möglicherweise ist die Feststelltaste aktiviert, oder Ihnen ist bei der Eingabe ein Fehler unterlaufen. Versuchen Sie es erneut.

Fehler	Ursache	Lösung
Die gekennzeichnete Eingabedatei ist nicht vorhanden.	Der eingegebene Dateiname ist nicht vorhanden.	Verwenden Sie die Durchsuchen-Funktion, um den genauen Namen und Pfad der gewünschten Datei zu ermitteln.
Die Nachricht/Daten enthält/enthalten eine separate Unterschrift.	Die Unterschrift für die Nachricht/Datei befindet sich in einer separaten Datei.	Doppelklicken Sie zuerst auf die Datei mit der separaten Unterschrift.
Die Schlüsselbunddatei ist fehlerhaft.	Daten in einer bestimmten Datei konnten entweder nicht gelesen oder nicht geschrieben werden.	Eine bestimmte Datei ist höchstwahrscheinlich beschädigt oder nicht vorhanden. Dabei muß es sich nicht zwangsweise um die Schlüsselbunddatei handeln. Versuchen Sie gegebenenfalls, einen anderen Dateinamen oder Pfad zu verwenden.
Diese Datei ist schreibgeschützt oder in anderer Weise geschützt. Der Vorgang konnte daher nicht ausgeführt werden. Falls Sie Ihre Schlüsselbunddateien auf einem Wechseldatenträger speichern, ist möglicherweise das Volume nicht vorhanden.	Eine erforderliche Datei ist schreibgeschützt oder wird derzeit von einem anderen Programm verwendet.	Schließen Sie die anderen Anwendungen, die unter Umständen auf dieselben Dateien zugreifen wie die derzeit ausgeführte Anwendung. Falls Sie Ihre Schlüsselbunddateien auf Diskette gespeichert haben, vergewissern Sie sich, daß diese in das Diskettenlaufwerk eingelegt wurde.
Dieser Schlüssel wurde bereits mit dem angegebenen Unterschriftenschlüssel unterschrieben.	Ein bereits unterschriebener Schlüssel kann nicht erneut unterschrieben werden.	Möglicherweise haben Sie versehentlich den falschen Schlüssel ausgewählt. Wenn dies der Fall ist, wählen Sie einen anderen Schlüssel.
Es sind zur Zeit nicht genügend Zufallsdaten verfügbar.	Zur Erzeugung gültiger Zufallswerte benötigt der Zufallswertegenerator weitere Eingaben.	Wenn Sie dazu aufgefordert werden, bewegen Sie die Maus oder betätigen beliebige Tasten, um Eingaben zu erzeugen.
Fehler in Domänennamenssystem	Die von Ihnen angegebene Zieladresse ist falsch, oder die Netzwerkverbindung wurde falsch konfiguriert.	Vergewissern Sie sich, daß Sie die richtige Zieladresse angegeben haben. Wenn Sie sich diesbezüglich sicher sind, überprüfen Sie die Verbindung mit dem Netzwerk.

Fehler	Ursache	Lösung
Identische Schlüsselteile können nicht kombiniert werden	Sie haben versucht, dasselbe Schlüsselteil zweimal zu kombinieren.	Falls diese aus einem Schlüsselteil stammen, ist die Auswahl eines anderen Schlüsselteils empfehlenswert. Falls die Schlüsselteile aus einem Netzwerk stammen, müssen Sie den Benutzer am entfernten Ort bitten, einen anderen Satz von Schlüsselteilen zu senden.
In der PGP-Bibliothek ist nicht genügend Speicherplatz.	Das Betriebssystem verfügt nicht über ausreichend Speicherplatz.	Schließen Sie andere derzeit ausgeführte Programme. Läßt sich das Problem hierdurch nicht beheben, benötigt Ihr Rechner möglicherweise zusätzlichen Speicher.
In Ihrem Schlüsselbund konnten keine geheimen Schlüssel gefunden werden.	In Ihrem Schlüsselbund sind keine privaten Schlüssel vorhanden.	Erzeugen Sie in PGPkeys Ihr persönliches Schlüsselpaar.
Socket nicht verbunden	Die Netzwerkverbindung mit dem Certificate Server von PGP bzw. mit der Schlüsselteil-Netzwerkverbindung wurde unterbrochen.	Versuchen Sie, die Verbindung wieder herzustellen. Wiederholen Sie hierzu den Vorgang, mit dem Sie die Verbindung anfangs aufgebaut haben. Falls dies fehlschlägt, überprüfen Sie die Verbindung zum Netzwerk.

Übertragen von Dateien zwischen den Betriebssystemen Mac OS und Windows

B

Das Übertragen von Dateien nach und aus Mac OS stellt ein häufiges Problem bei der Verwendung fast aller Datenübertragungsprogramme dar. Dazu gehören E-Mail-Anwendungen, FTP, Komprimierungsdienstprogramme und PGP. In diesem Anhang wird gezeigt, wie dieses Problem in Version 5.5.x von PGP gelöst wurde. Außerdem wird erläutert, wie die Kommunikation mit älteren Versionen von PGP erfolgt.

In Mac OS werden Dateien nicht wie in anderen Betriebssystemen gespeichert. Sogar das Textdateiformat von Mac OS ist anders. Mac OS-Dateien bestehen aus zwei Dateihälften: einem Datensegment und einem Ressourcensegment. Wenn Sie eine Datei von Mac OS nach Windows ohne Datenverlust senden möchten, müssen die beiden Segmente vereinigt werden. Diese Vereinigung für die Übertragung auf einen anderen Mac OS oder PC ohne Verlust einer Dateihälfte erfolgt mit dem Standardverfahren „MacBinary“.

Ohne spezielle Software können Windows und andere Betriebssysteme allerdings das MacBinary-Format nicht lesen. Kann die Ziel-Software die Datei im MacBinary-Format nicht in eine Windows-Datei umwandeln, ist die resultierende Datei nicht verwendbar. Unter Windows gibt es zwar Dienstprogramme von Drittanbietern zum Umwandeln der Datei in eine brauchbare Datei, jedoch kann dies ziemlich umständlich sein.

Ältere PGP-Versionen sowie die meisten momentan auf dem Markt verfügbaren Dienstprogramme versuchen in der Regel, dieses Problem weitgehend zu ignorieren: Der Benutzer allein muß entscheiden, ob er eine Datei beim Senden aus Mac OS mit MacBinary verschlüsseln möchte oder nicht. Die Qual der Wahl wird in diesem Fall dem Benutzer überlassen, der meist nicht weiß, ob er mit MacBinary senden soll, um keine Daten zu verlieren, oder in der Hoffnung, daß keine wichtigen Daten verlorengehen, auf MacBinary verzichtet. Die Entscheidung richtet sich in der Regel danach, ob die Datei nach Windows oder Mac OS gesendet wird. Doch wie sollen Sie sich entscheiden, wenn Sie an beide Betriebssysteme gleichzeitig senden möchten? In älteren PGP-Versionen und vielen anderen Dienstprogrammen gibt es dafür keine befriedigende Lösung. Dies führte oft zu Verwirrungen und Unannehmlichkeiten bei den Benutzern.

Auch der umgekehrte Fall, das Senden von Windows-Dateien in die Mac OS-Umgebung, stellte bislang ein großes Problem dar. Unter Windows werden zum Identifizieren der Dateitypen Dateierweiterungen (z. B. .doc) verwendet. Unter Mac OS haben diese Erweiterungen keinerlei Bedeutung. Das heißt, die Dateien werden ohne Informationen zum Dateityp oder den Ersteller an einen Macintosh-Computer gesendet. Wenn diese Informationen nach der Übertragung lesbar sein sollen, müssen verschiedene komplizierte Schritte im Dialogfeld „Öffnen“ der Erstelleranwendung vorgenommen werden. In vielen Fällen muß der Benutzer sich mit den Ersteller- und Typencodes von Mac OS auskennen, um diese in einer Drittanbieter-Anwendung manuell einstellen zu können.

Zum Glück gibt es in den neuesten Versionen von PGP (5.5 bis 6.5) eine Lösung für diese Probleme. Wenn alle PGP-Benutzer eine dieser beiden Versionen verwenden würden, müßte sich keiner mehr den Kopf darüber zerbrechen, wie Dateien von Mac OS nach Windows und umgekehrt gesendet werden.

Übertragen von Dateien aus Mac OS nach Windows

Unter Mac OS gibt es für das Verschlüsseln bzw. Unterschreiben von Dateien drei Optionen:

- **MacBinary: Yes.** Dies ist die empfohlene Option für alle Verschlüsselungen beim Senden an einen Benutzer, der unter einem beliebigen Betriebssystem ebenfalls mit PGP-Version 5.5 oder höher arbeitet. Dies bedeutet, daß Mac OS-Benutzer genau die Ursprungsdatei empfangen und unter Windows automatisch der MacBinary-Code decodiert und sogar die entsprechende Dateierweiterung (z. B. .doc für Microsoft Word- oder .ppt für Microsoft PowerPoint-Dateien) angehängt wird. PGP enthält Informationen zur Dateierweiterungen der gängigsten Anwendungen sowie Erstellercodes von Macintosh. Sollte der Dateityp unbekannt sein oder es sich um ein Dateiformat handeln, das es nur in Mac OS gibt, wie beispielsweise bei einer Mac OS-Anwendung, bleibt die Datei im MacBinary-Format und kann später völlig intakt an einen Macintosh gesendet werden.

- **MacBinary: No.** Wenn Sie mit Benutzern kommunizieren, die mit einer älteren Version von PGP arbeiten, muß der Absender entscheiden, ob mit MacBinary gesendet werden soll, was auch für die meisten anderen Programme und ältere Versionen von PGP für Mac OS gilt. Wählen Sie diese Option, wenn Sie an einen PC mit einer älteren Version senden und wissen, daß die Datei ohne Verwendung von MacBinary von Windows-Anwendungen gelesen werden kann. Dies trifft für die meisten Dateien zu, die in der Regel plattformübergreifend sind, wie beispielsweise die von Microsoft Office-Programmen erstellten Dateien, Grafikdateien, komprimierte Dateien und viele andere. Der Absender oder der Empfänger muß die Datei manuell umbenennen, damit unter Windows die korrekte Dateierweiterung angezeigt wird. Dies ist erforderlich, da der Windows-Empfänger nicht über die Erstellerinformationen verfügt, die normalerweise mit MacBinary verschlüsselt sind.

- **MacBinary: Smart.** Diese Option erweist sich in ganz seltenen Fällen als sinnvoll, wenn mit Benutzern kommuniziert wird, die über keine neueren Versionen von PGP verfügen. Bei dieser Option wird anhand einer Daten-Analyse der Datei entschieden, ob mit MacBinary codiert wird. Folgende Dateitypen werden nicht mit MacBinary codiert und sind daher auf einem PC mit einer beliebigen PGP-Version lesbar:

  – Mit PKzip komprimierte Dateien

  – Mit Lempel-Ziv komprimierte Dateien

  – Musikdateien im MIDI-Format

  – Mit PackIt komprimierte Dateien unter Windows

  – GIF-Grafikdateien

  – Mit StuffIt komprimierte Dateien

  – Mit Compactor komprimierte Dateien

  – Mit Arc komprimierte Dateien

  – JPEG-Grafikdateien

Wie gezeigt wurde, ist es nur bei einer begrenzten Auswahl von Dateien möglich, diese mit älteren Versionen von PGP auf anderen Plattformen zu lesen, wenn die Option „Smart“ verwendet wird. Alle anderen auf PCs mit einer älteren PGP-Version empfangenen Dateien sind erst lesbar, wenn die MacBinary-Codierung mit einem Drittanbieter-Dienstprogramm entfernt wird. Außerdem verfügt die Datei auf dem PC nur über die korrekte Dateierweiterung, wenn diese vom Benutzer vor dem Senden manuell hinzugefügt wurde. Bei Verwendung des „Smart“-Modus weicht die resultierende Datei u. U.

vom Original ab, wenn sie an einen Macintosh gesendet wird, da die Ersteller- und Typencodes verlorengehen können. Dieser Modus wird größtenteils nur deshalb beibehalten, da es ihn in PGP-Version 5.0 gab und einige Benutzer eventuell nur die obengenannten Dateitypen senden möchten. Für die meisten Fälle wird diese Option nicht empfohlen.

Zusammenfassend ist festzuhalten, daß Sie immer „MacBinary: Yes“ (den Standardwert) wählen sollten, wenn Sie nur an Version 6.x oder höher senden. Wenn in Ihrer Umgebung ausschließlich PGP-Version 6.x verwendet wird, müssen Sie sich also keine Gedanken über den zu wählenden Modus machen. Wenn Sie an Benutzer mit älteren Versionen senden, wählen Sie bei plattformübergreifenden Dateitypen „MacBinary: No“ und bei Dateien, die für PC-Benutzer sowieso nicht lesbar wären (wie z. B. eine Mac OS-Anwendung), den Modus „MacBinary: Yes“.

HINWEIS: In PGP Version 5.0 gab es die Option „MacBinary: No“ nicht. Um an einen PC mit Version 5.0 Dateitypen, die nicht in der „MacBinary: Smart“-Liste aufgeführt sind, ohne MacBinary zu senden, muß die Datei vor dem Senden manuell auf einen der Ersteller- und Typencodes in der „Smart“-Liste gesetzt werden.

Windows-Dateien unter Mac OS empfangen

Beim Decodieren wird in PGP Version 5.5 und höher automatisch versucht, Dateierweiterungen von Dateien, die keine MacBinary-Dateien sind, in Ersteller- und Typeninformationen von Mac OS umzuwandeln. Wenn Sie beispielsweise eine Datei aus Windows mit der Erweiterung DOC empfangen, wird die Datei als ein Microsoft Word-Dokument gespeichert. Zum Rückumwandeln von Dateierweiterungen in die Mac OS-Entsprechung bei Empfang auf einem Macintosh-Computer wird dieselbe Anwendungsliste wie beim Hinzufügen von Dateierweiterungen bei Empfang von MacBinary-Dateien in Windows verwendet. In fast allen Fällen erhalten Sie Dateien, die in Mac OS sofort lesbar sind und die Sie durch Doppelklick anzeigen können.

Ältere Versionen von PGP für Mac OS verfügen nicht über diese Funktion. Der Benutzer muß dort manuell festlegen, daß eine Datei mit dem Namen report.doc eine Microsoft Word-Datei ist. Nach dem Bestimmen der Erstelleranwendung (Microsoft Word) können Sie einfach im Pulldown-Menü des Dialogfelds „Öffnen“ die Option „Alle Dateien“ wählen und die Datei öffnen. Diese Funktion gibt es auch noch in vielen anderen Anwendungen, jedoch nicht in allen. Wenn das Dokument nicht in der Anwendung geöffnet werden

kann, muß der Benutzer herausfinden, wie die entsprechenden Macintosh-Ersteller- und Typencodes für die Datei lauten und diese manuell mit einem Drittanbieter-Dienstprogramm einstellen. Dafür werden viele kostenlose Dienstprogramme angeboten. Um dieses Problem zu umgehen, ist es jedoch am einfachsten, Ihr Programm auf Version 6.x zu aktualisieren.

Unterstützte Anwendungen

In der folgenden Liste sind gängige Anwendungen genannt, in denen Dokumente erstellt werden, die beim Senden von Windows nach Mac OS und umgekehrt automatisch durch PGP umgewandelt werden. Sie können dieser Liste Einträge hinzufügen, indem Sie die Datei PGPMacBinaryMappings.txt bearbeiten. Entfernen Sie bei einem Mac-Computer die Dateinamenerweiterung .TXT vom Dateinamen (die Datei PGPMacBinaryMappings finden Sie im Verzeichnis System Folder / Preferences / Pretty Good Preferences).

- PhotoShop (GIF, Photoshop-Dokumente, TGA, JPEG)
- PageMaker (Versionen 3.X, 4.X, 5.X, 6.X)
- Microsoft Project (Projekt- und Vorlagendateien)
- FileMaker Pro
- Adobe Acrobat
- Lotus 123
- Microsoft Word (Text-, RTF- und Vorlagendateien)
- PGP
- Microsoft PowerPoint
- StuffIt
- QuickTime
- Corel WordPerfect
- Microsoft Excel (viele verschiedene Dateitypen)
- Quark XPress

Ebenso werden die folgenden Dateierweiterungen umgewandelt:

CVS	ARJ	IMA	EPS	MAC	CGM
DL	FLI	ICO	IFF	IMG	LBM
MSP	PAC	PBM	PCS	PCX	PGM
PLT	PM	PPM	RIF	RLE	SHP
SPC	SR	SUN	SUP	WMF	FLC
GZ	VGA	HAL	LZH	Z	EXE
MPG	DVI	TEX	AIF	ZIP	AU
MOD	SVX	WAV	TAR	PCT	PIC
PIT	TXT	MDI	PAK	TIF	EPS

Phil Zimmermann über PGP C

Dieses Kapitel enthält eine Einführung und Hintergrundinformationen zur Kryptographie und zu PGP, verfaßt von Phil Zimmermann.

Weshalb ich PGP entwickelt habe

Was auch immer du tust, ist nicht von Bedeutung. Aber es ist sehr wichtig, daß du es tust.“
– Mahatma Gandhi.

Es ist persönlich. Es ist vertraulich. Und außer Sie geht es niemanden etwas an. Unter Umständen bereiten Sie derzeit eine politische Kampagne vor, sprechen über Ihre Steuerangelegenheiten oder haben eine geheime Liebesaffäre. Oder aber Sie stehen mit einem politischen Dissidenten in einem autoritären Staat in Kontakt. Worum es sich auch handeln mag, Sie möchten sicherlich nicht, daß eine dritte Person Ihre elektronische Post (E-Mail) oder Ihre vertraulichen Dokumente liest. Es ist völlig normal, daß Sie Ihre Privatsphäre bewahren möchten. Die Wahrung der Privatsphäre ist genauso selbstverständlich wie die amerikanische Verfassung.

Das Recht auf Privatsphäre ist implizit durchgehend in den verfassungsmäßig garantierten Grundrechten der Vereinigten Staaten, der Bill of Rights, enthalten. Aber als die amerikanische Verfassung aufgesetzt wurde, sahen die Gründerväter keine Notwendigkeit, das Recht auf private Kommunikation ausdrücklich festzuschreiben. Dafür gab es ja damals auch noch keinen Grund. Schließlich waren vor zweihundert Jahren alle Unterhaltungen privat. Wenn sich eine andere Person näherte, ist man eben einfach hinter die nächste Scheune gegangen und hat das Gespräch dort fortgesetzt. Es war unmöglich, fremde Gespräche heimlich zu belauschen. Das Recht auf private Unterhaltung war ein natürliches Recht, und zwar nicht nur im philosophischen Sinne, sondern sozusagen als physikalisches Gesetz aufgrund des damaligen Standes der Technik.

Dies jedoch sollte sich mit dem Beginn des Informationszeitalters, das durch die Erfindung des Telefons eingeläutet wurde, schlagartig ändern. Heutzutage werden die meisten Unterhaltungen unter Nutzung elektronischer Medien geführt. Damit sind all unsere Unterhaltungen, auch die noch so privaten, fremden Personen ohne unser Wissen zugänglich. Mobiltelefone können von jedermann mit einem Funkgerät abgehört werden. Viel sicherer als über Mobiltelefone geführte Gespräche sind auch die via Internet übermittelten E-Mail-Nachrichten nicht. E-Mail-Nachrichten laufen den herkömmlichen, per Post versandten Briefen zunehmend den Rang ab. Sie werden immer selbstverständlicher und sind längst nicht mehr so außergewöhnlich wie noch vor wenigen Jahren. E-Mail-Nachrichten können jedoch von interessierten Dritten regelmäßig und auf automatische Weise nach beliebigen Schlüsselwörtern durchsucht werden – auf breit angelegter Basis und ohne Nachweismöglichkeit. Dies ist vergleichbar mit dem Treibnetzfischen.

Möglicherweise sind Sie der Meinung, daß der Inhalt Ihrer E-Mail-Nachricht legitim genug ist und eine Verschlüsselung ungerechtfertigt wäre. Doch wenn Sie wirklich ein gesetzestreuer Bürger sind, der nichts zu verbergen hat – warum verschicken Sie Ihre herkömmliche Post dann nicht immer in Form von Postkarten? Warum fänden Sie es nicht in Ordnung, wenn sich jedermann auf Verlangen einem Drogentest unterziehen müßte? Warum würden Sie bei einer Hausdurchsuchung durch die Polizei einen Durchsuchungsbefehl verlangen? Haben Sie vielleicht etwas zu verbergen? Ist die Tatsache, daß Sie Ihre Post in Briefumschlägen verbergen, ein Zeichen dafür, daß Sie subversive Absichten haben, ein Drogenhändler sind oder unter Verfolgungswahn leiden? Haben Bürger, die die Gesetze befolgen, irgendeinen Grund, ihre E-Mail-Nachrichten zu verschlüsseln?

Was wäre, wenn die allgemeine Ansicht bestünde, daß gesetzestreue Bürger ausschließlich Postkarten für ihre Post verwenden müßten? Wenn ein Mensch, der diese allgemeine Ansicht nicht teilt, zum Schutz seiner Privatsphäre einen Umschlag für seine Post verwenden würde, würde er Verdacht auf sich ziehen. Die Behörden würden möglicherweise die Post öffnen, um herauszufinden, was diese Person verbirgt. Glücklicherweise ist dies nicht die Realität, da die meisten Briefe durch Briefumschläge geschützt werden. Und niemand, der Briefumschläge zum Schutz seiner Privatsphäre verwendet, macht sich dadurch verdächtig. Mit dem, was alle machen, liegt man am sichersten. Im gleichen Maße wäre es gut, wenn jeder seine E-Mails verschlüsseln würde, unabhängig davon, ob schuldig oder unschuldig, so daß keiner sich durch Verschlüsselung von E-Mails zum Schutze seiner Privatsphäre verdächtig machen würde. Betrachten Sie es einfach als eine Form von Solidarität.

Bis jetzt mußte die Regierung, wenn sie in die Privatsphäre eines normalen Bürgers eindringen wollte, eine bestimmte Menge an Geld und Arbeit investieren, um Briefpost abzufangen, den Umschlag mit Wasserdampf zu öffnen und den Brief zu lesen. Bei telefonischer Kommunikation mußten Telefongespräche abgehört und möglicherweise transkribiert werden, zumindest bevor automatische Spracherkennung verfügbar wurde. Solche arbeitsaufwendigen Überwachungsmaßnahmen waren in einem großen Maßstab nicht zweckmäßig. Sie wurden lediglich in wichtigen Fällen durchgeführt, für die sich der Aufwand zu lohnen schien.

Die „Senate Bill 266“, eine 1991 eingebrachte, allgemeine Gesetzesvorlage zur Verbrechensbekämpfung, sah einen beunruhigenden Handlungsspielraum vor. Wenn dieser nicht bindende Beschluß zum Gesetz geworden wäre, wären Hersteller von sicheren Kommunikationsanlagen gezwungen worden, spezielle „Zugangstüren“ in ihre Produkte einzubauen. Auf diese Weise hätte die Regierung verschlüsselte Nachrichten von beliebigen Personen lesen können. Die Gesetzesvorlage drückt die Auffassung des Kongresses aus, daß Firmen, die elektronische Kommunikationsdienste anbieten, und Firmen, die Anlagen für elektronische Kommunikationsdienste herstellen, sicherstellen sollen, daß die Kommunikationssysteme der Regierung die Möglichkeit eröffnen, auf die Klartextinhalte von Sprach- und anderen Daten sowie auf sonstige übertragene Informationen zuzugreifen, wenn die entsprechende gesetzliche Grundlage dafür besteht. Dieser Beschluß gab den Ausschlag für mich, PGP im selben Jahr auf elektronischem Wege kostenfrei zugänglich zu machen, kurz bevor die Maßnahme nach heftigem Protest durch Bürgerrechtsvereinigungen und Vertreter der Industrie abgewendet wurde.

Die Gesetzesvorlage bezüglich digitaler Telefone von 1994 (Digital Telephony Bill) sah vor, daß Telefongesellschaften in die digitalen Schalter ihrer Zentrale fernbedienbare Abhöranschlüsse einbauen sollten, um so eine neue technische Infrastruktur zum Abhören per Mausklick zu schaffen. Dadurch müssen die zuständigen Staatsbediensteten nicht einmal mehr ihr Büro verlassen und vor Ort Krokodilklemmen an Telefonleitungen installieren. Statt dessen können sie nun in ihrem Hauptsitz in Washington bleiben und nach Belieben Ihren Telefongesprächen zuhören. Selbstverständlich ist nach diesem Gesetz immer noch eine gerichtliche Verfügung zur Abhörung eines Gesprächs erforderlich. Doch während eine technische Infrastruktur mehrere Generationen lang bestehen kann, können Gesetze und Richtlinien sich über Nacht ändern. Wenn sich eine Kommunikationsinfrastruktur, die für Überwachungszwecke optimiert wurde, etabliert, kann ein Wechsel der politischen Gegebenheiten zu einem Mißbrauch dieses neu geschaffenen Machtmittels führen. Politische Verhältnisse können sich durch die Wahl einer neuen Regierung ändern, aber unter Umständen auch ganz plötzlich, beispielsweise durch die Bombardierung eines Bundesgebäudes.

Ein Jahr, nachdem die Digital Telephony Bill von 1994 verabschiedet wurde, enthüllte das FBI Pläne, nach denen die Telefongesellschaften verpflichtet werden sollten, in ihrer Infrastruktur die Möglichkeit zu schaffen, 1 Prozent aller Telefongespräche in den größten amerikanischen Städten zur gleichen Zeit abzuhören. Dies würde im Vergleich zur vorherigen Situation die Anzahl der abhörbaren Telefone vertausendfachen. Vor 1994 wurden lediglich ungefähr tausend gerichtliche Abhörverfügungen pro Jahr in den USA ausgestellt, alle Verfügungen auf Bundes-, Staats- und lokaler Ebene zusammengenommen. Es ist schwer vorstellbar, wie die Regierung auch nur genug Richter einstellen könnte, um genügend gerichtliche Abhörverfügungen für 1 Prozent sämtlicher in den USA geführten Telefongespräche unterzeichnen zu können, und es ist noch weniger vorstellbar, wie genügend Bundesbeamte eingestellt werden könnten, um alle Gespräche in Echtzeit abzuhören. Die einzig plausible Erklärung zur Verarbeitung dieser Gesprächsmengen wäre die Verwendung einer automatisierten Spracherkennungstechnologie in Orwellschen Dimensionen, um alle Gespräche zu „durchsieben“ und nach interessanten Schlüsselwörtern oder nach der Stimme eines bestimmten Sprechers zu suchen. Falls die Regierung im ersten 1-Prozent-Anteil der Telefongespräche nicht findet, was sie sucht, können die Abhörmaßnahmen auf einen anderen 1-Prozent-Anteil gerichtet werden, bis das Gesuchte gefunden wird – oder bis die Telefonleitungen aller Personen auf subversive Gespräche hin überprüft worden sind. Laut FBI wird diese Kapazität benötigt, damit sich auf künftige Gegebenheiten eingestellt werden könne. Dieses Vorhaben führte zu einer solchen Entrüstung, daß es im Kongreß nicht angenommen wurde – zumindest in diesem Fall, im Jahre 1995. Doch die bloße Tatsache, daß das FBI um die Einräumung dieser enormen Machtmittel gebeten hat, sagt einiges über seine Absichten aus. Die Ablehnung des Plans stimmt auch nicht ausschließlich positiv, wenn Sie daran denken, daß die Digital Telephony Bill von 1994 auch beim ersten Antrag im Jahre 1993 abgelehnt wurde.

Der technische Fortschritt erschwert die Aufrechterhaltung des privaten Status Quo. Dieser Zustand ist alles andere als stabil. Wenn wir nichts unternehmen, werden der Regierung durch neue Technologien neue Möglichkeiten der automatisierten Überwachung eröffnet, von denen Stalin nur träumen konnte. Der einzige Weg, die Privatsphäre auch im Informationszeitalter zu schützen, ist die Verwendung einer effizienten Kryptographie.

Sie müssen nicht unbedingt der Regierung mißtrauen, um Kryptographie verwenden zu möchten. Ihr Unternehmen kann von Konkurrenzfirmen, dem organisierten Verbrechen oder ausländischen Regierungen abgehört werden. Mehrere ausländische Regierungen sind beispielsweise dafür bekannt, daß sie das Signalerkennungssystem ihres Nachrichtendienstes gegen Unternehmen aus anderen Ländern einsetzt, um ihren eigenen Firmen einen Wettbewerbsvorteil zu verschaffen. Ironischerweise haben die Beschränkungen der US-Regierung im Hinblick auf die Kryptographie die Schutzmöglichkeiten amerikanischer Firmen gegenüber ausländischen Geheimdiensten und dem organisierten Verbrechen untergraben.

Die Regierung ist sich der zentralen Rolle bewußt, die die Kryptographie im Machtverhältnis gegenüber der Bevölkerung spielen wird. Im April 1993 gab die Clinton-Regierung eine neue politische Initiative zum Thema Verschlüsselung bekannt, die der Nationale Sicherheitsdienst (NSA) seit Beginn der Amtszeit von Präsident Bush entwickelt hatte. Das Kernstück dieser Initiative besteht aus einem von der Regierung hergestellten Verschlüsselungsgerät, dem „Clipper-Chip", der einen neu klassifizierten NSA-Verschlüsselungsalgorithmus enthält. Die Regierung versuchte, die Privatindustrie zu ermutigen, diesen Clip in all ihre Geräte zur abhörgeschützten Kommunikation zu integrieren, wie beispielsweise abhörgeschützte Telefone, abhörgeschützte Faxgeräte usw. AT&T integrierte den Clipper-Chip in seine abhörgeschützten Sprachprodukte. Der Haken an der Sache: Bei der Herstellung wird jeder Clipper-Chip mit einem eigenen, eindeutigen Schlüssel geladen, und die Regierung erhält eine Kopie dieses Schlüssels, die hinterlegt wird. Es besteht jedoch kein Grund zur Beunruhigung: Die Regierung verspricht, diese Schlüssel nur zum Abhören zu verwenden, wenn sie dazu „durch ein Gesetz ordnungsgemäß ermächtigt" ist. Der nächste logische Schritt zur vollständig effektiven Verwendung des Clipper-Chips bestünde dann natürlich im Verbot anderer Formen von Kryptographie.

Die Regierung wies anfangs darauf hin, daß der Gebrauch des Clipper-Chips nicht vorgeschrieben sei, und daß niemand gezwungen würde, diese Technologie anstelle anderer Formen von Kryptographie zu verwenden. Aber die öffentliche Reaktion auf den Clipper-Chip war stark, stärker, als von der Regierung erwartet. Die Computer-Industrie sprach sich einheitlich gegen die Verwendung des Clipper-Chip aus. FBI-Direktor Louis Freeh antwortete 1994 auf eine Frage in einer Pressekonferenz, daß im Falle einer Nichtakzeptanz des Clipper-Chip durch die Öffentlichkeit und dem Umgehen von FBI-Abhöreinrichtungen durch nicht von der Regierung kontrollierte Kryptographie seiner Behörde nur der Ausweg einer Rechtsklage bliebe. Später, nach der Tragödie von Oklahoma City, sagte Louis Freeh vor dem Rechtskommittee des Senats aus, daß der Zugang der Öffentlichkeit zu einer effizienten Kryptographie durch die Regierung eingeschränkt werden müsse (obwohl niemand die Vermutung ausgesprochen hatte, daß die Bombenleger Kryptographie verwendet hätten).

Das Informationszentrum zum Schutz der Privatsphäre in elektronischen Medien (EPIC) gelangte in den Besitz einiger aufschlußreicher Dokumente, die unter das Gesetz zur Wahrung des Rechts auf Auskunft (Freedom of Information Act) fallen. In einem Informationsdokument über die Bedrohung, Anwendungen und mögliche Lösungen des Phänomens Verschlüsselung (Originaltitel: „Encryption: The Threat, Applications and Potential Solutions"), das im Februar 1993 an den Nationalen Sicherheitsrat geschickt worden war, kamen das FBI, der NSA und das Justizministerium zu dem Schluß, daß „bestehende technische Lösungen nur funktionieren werden, wenn sie in alle Verschlüsselungsprodukte integriert werden". Um dies sicherzustellen, müsse durch die Gesetzgebung die Verwendung von staatlich genehmigten Verschlüsselungsprodukten oder die Befolgung von staatlich vorgegebenen Verschlüsselungskriterien vorgeschrieben werden.

Die politische Vergangenheit stärkt nicht gerade das Vertrauen der Bevölkerung darauf, daß ein Mißbrauch von Bürgerrechten seitens der Regierung absolut ausgeschlossen ist. Das COINTELPRO-Programm des FBI war gegen Gruppen gerichtet, die die Regierungspolitik ablehnten.
Die Anti-Kriegs-Bewegung und die Bürgerrechtsbewegung wurden bespitzelt. Das Telefon von Martin Luther King Jr. wurde abgehört. Nixon hatte eine „Feindliste". Nicht zu vergessen die Watergate-Affäre. Der Kongreß ist nun offenbar bestrebt, Gesetze zu verabschieden, die die Bürgerrechte im Medium Internet einschränken. Zu keiner Zeit im vergangenen Jahrhundert war ein Mißtrauen gegenüber der Öffentlichkeit von seiten der Regierung so weit über das gesamte politische Spektrum verteilt wie heutzutage.

Wenn wir uns dem beunruhigenden Trend der Regierung widersetzen möchten, Kryptographie gesetzlich zu verbieten, besteht eine Möglichkeit des Widerstands darin, Kryptographie so intensiv wie möglich zu verwenden, solange es noch legal ist. Je stärker sich die Verwendung von effizienter Kryptographie verbreitet, desto schwieriger wird es für die Regierung, die Verwendung unter Strafe zu stellen. Aus diesem Grunde trägt die Verwendung von PGP zum Erhalt der Demokratie bei.

Wenn Privatsphäre nicht mehr legal ist, ist die Privatsphäre den Gesetzesbrechern vorbehalten. Geheimdienste haben Zugang zu guten Verschlüsselungstechniken. Dies trifft ebenfalls auf große Waffen- und Drogenhändler zu. Aber die allgemeine Bevölkerung und politische Basisorganisationen hatten normalerweise keinen Zugang zu Kryptographietechniken mit öffentlichen Schlüsseln, die erschwinglich und zugleich so sicher wie die für militärische Zwecke verwendeten Verschlüsselungsmethoden waren. Bis jetzt.

PGP ist ein Instrument, mit dem Menschen den Schutz ihrer Privatsphäre in die eigene Hand nehmen können. In unserer Gesellschaft besteht dafür ein wachsendes Bedürfnis. Deshalb habe ich PGP entwickelt.

Die symmetrischen Algorithmen von PGP

PGP verfügt über verschiedene Geheimschlüsselalgorithmen zur Verschlüsselung der eigentlichen Nachricht. Als Geheimschlüsselalgorithmus bezeichnet man eine konventionelle oder symmetrische Blockchiffre, die denselben Schlüssel zum Ver- und zum Entschlüsseln verwendet. Bei den drei symmetrischen, von PGP angebotenen Blockchiffren handelt es sich um CAST, Triple-DES und IDEA. Diese Algorithmen entsprechen den höchsten professionellen Anforderungen und wurden von renommierten Kryptographen-Teams entwickelt.

Für diejenigen, die sich näher für Kryptographie interessieren, sei angemerkt, daß alle drei Chiffriercodes auf der Basis von 64-Bit-Blöcken von Klar- und chiffriertem Text funktionieren. CAST und IDEA verfügen über Schlüsselgrößen von 128 Bit, während Triple-DES einen 168-Bit-Schlüssel verwendet. Wie der Data Encryption Standard (DES), können alle drei Verschlüsselungsarten in den Modi Cipher Feedback (CFB) oder Cipher Block Chaining (CBC) verwendet werden. Sie werden von PGP im 64-Bit-CFB-Modus verwendet.

Der CAST-Verschlüsselungsalgorithmus wurde in PGP aufgenommen, da es sich dabei um einen vielversprechenden, sehr schnellen und kostenfreien 128-Bit-Blockchiffrierer handelt. Der Name dieses Algorithmus wurde aus den Anfangsbuchstaben seiner Entwickler abgeleitet, Carlisle Adams und Stafford Tavares von Northern Telecom (Nortel). Nortel hat zwar ein Patent für CAST angemeldet, die Firma hat jedoch schriftlich zugesichert, CAST jedem ohne Lizenzgebühren zur Verfügung zu stellen. CAST ist ein hervorragend entwickelter Algorithmus, der von Personen mit einem guten Namen in diesem Bereich entwickelt wurde. Die Entwicklung basiert auf einem sehr formalen Ansatz, mit einigen formal nachweisbaren Hypothesen. Daraus ergeben sich gute Gründe für die Annahme, daß der 128-Bit-Schlüssel dieses Algorithmus mit den gegenwärtig bekannten Verfahren nicht entschlüsselt werden kann. CAST hat keine ineffizienten oder halb-effizienten Schlüssel. Es sprechen viele Argumente dafür, daß CAST immun gegen lineare und differentiale Kryptoanalyse ist. Diese Methoden werden in der Fachliteratur allgemein als die leistungsfähigsten Kryptoanalyseformen dargestellt, und waren gleich leistungsstark im Dekodieren von DES (Data Encryption Standard). CAST ist noch zu neu, um anhand konkreter Ergebnisse beurteilt werden zu können, aber seine formale Gestaltung und der gute Ruf seiner Entwickler werden sicherlich die Aufmerksamkeit sowie kryptoanalytische Angriffe des Restes der akademischen kryptographischen Gemeinschaft auf sich ziehen. Ich habe fast das gleiche gute Gefühl und Vertrauen in CAST, wie ich es vor Jahren für IDEA hatte, den Chiffriercode, den ich für frühere PGP-Versionen ausgewählt hatte. Zu dieser Zeit war IDEA auch noch nicht längerfristig erprobt, aber es hat die Erwartungen nicht enttäuscht.

Die Blockchiffre IDEA (International Data Encryption Algorithm; internationaler Datenverschlüsselungsalgorithmus) basiert auf dem Entwicklungskonzept, Vorgänge von verschiedenen algebraischen Gruppen zu mischen. Der Algorithmus wurde von James L. Massey und Xuejia Lai an der ETH in Zürich entwickelt und 1990 veröffentlicht. In früheren Veröffentlichungen über den Algorithmus wurde er als IPES (Improved Proposed Encryption Standard; verbesserter, vorgeschlagener Verschlüsselungsstandard) bezeichnet, der Name wurde später jedoch in IDEA geändert. Bis heute hat IDEA Angriffen wesentlich besser widerstanden als andere Chiffriercodes (beispielsweise FEAL, REDOC-II, LOKI, Snefru und Khafre). Darüber hinaus widersteht IDEA den höchst erfolgreichen differential-kryptoanalytischen Angriffen von Biham und Shamir sowie Attacken durch lineare Kryptoanalyse besser als DES. Da weiterhin viele Kryptoanalyse-Spezialisten vergeblich versuchen, IDEA zu dekodieren, wächst das Vertrauen in IDEA mit der Zeit immer mehr. Leider war das größte Hindernis für die Akzeptanz von IDEA als Standard die Tatsache, daß Ascom Systec ein Patent auf seine Entwicklung hat und IDEA im Gegensatz zu DES und CAST nicht allgemein kostenfrei zur Verfügung gestellt wurde.

Als Schutz enthält PGP im Repertoire seiner Blockchiffren Drei-Schlüssel-Triple-DES. DES wurde von IBM Mitte der 70er Jahre entwickelt. Obwohl er gut entwickelt ist, ist die Schlüsselgröße von 56 Bit für heutige Standards zu gering. Triple-DES ist sehr effizient und wurde mehrere Jahre lang ausführlich untersucht. Er könnte also ein sichererer Chiffriercode sein als die neueren Chiffriercodes CAST und IDEA. Triple-DES bedeutet, daß DES dreimal auf den gleichen Datenblock angewandt wird. Dabei werden drei verschiedene Schlüssel verwendet; der zweite DES-Vorgang wird rückwärts, im Entschlüsselungsmodus, durchgeführt. Triple-DES ist zwar deutlich langsamer als CAST oder IDEA, jedoch ist die Geschwindigkeit für E-Mail-Anwendungen normalerweise nicht von großer Bedeutung. Obwohl Triple-DES eine Schlüsselgröße von 168 Bit verwendet, scheint es über eine effektive Schlüsselstärke von mindestens 112 Bit bei Angriffen mit einer äußerst großen Datenspeicherungskapazität zu verfügen. Gemäß einer Veröffentlichung von Michael Weiner auf der Crypto96 würde eine auch nur annähernd ausreichende Datenspeicherungsmöglichkeit dem Hacker einen Angriff ermöglichen, der genausoviel Aufwand wie das Aufbrechen eines 129-Bit-Schlüssels erfordern würde. Die Verwendung von Triple-DES wird durch keinerlei Patente beschränkt.

Die öffentlichen Schlüssel, die mit PGP Version 5.0 oder höher erzeugt werden, enthalten eingebettete Daten, die dem Absender mitteilen, welche Blockchiffren von der Empfängersoftware verstanden werden, so daß die Software des Absenders „weiß“, welche Chiffriercodes zum Verschlüsseln verwendet werden können. Die öffentlichen Diffie-Hellman / DSS-Schlüssel akzeptieren CAST, IDEA oder Triple-DES als Blockchiffre, mit CAST als Standardeinstellung. Zur Zeit bieten RSA-Schlüssel aus Kompatibilitätsgründen diese Funktion nicht an. Zum Senden von Nachrichten an RSA-Schlüssel wird von PGP nur die IDEA-Verschlüsselung verwendet, da ältere PGP-Versionen nur RSA und IDEA unterstützen.

PGP-Datenkomprimierungsroutinen

PGP komprimiert normalerweise den Klartext vor der Verschlüsselung, da der Klartext nach der Verschlüsselung nicht mehr komprimiert werden kann; verschlüsselte Daten können nicht komprimiert werden. Durch Datenkomprimierung wird die Übertragungszeit bei Modemübertragungen verringert sowie Platz auf der Festplatte gespart und, was wichtiger ist, die kryptographische Sicherheit gesteigert. Die meisten kryptoanalytischen Verfahren nutzen im Klartext gefundene Wiederholungen zum Decodieren der Chiffriercodes. Durch Datenkomprimierung wird diese Redundanz im Klartext reduziert, wodurch der Schutz vor kryptoanalytischen Angriffen deutlich vergrößert wird. Die Komprimierung des Klartextes bedeutet einen zusätzlichen Zeitaufwand, doch vom Sicherheitsstandpunkt aus gesehen lohnt sich der Aufwand.

Dateien, die zum Komprimieren zu kurz sind oder die nicht gut komprimiert werden können, werden von PGP nicht komprimiert. Außerdem erkennt das Programm Dateien, die mit den meisten bekannten Komprimierungsprogrammen erstellt wurden, wie beispielsweise PKZIP, und versucht nicht, Dateien zu komprimieren, die bereits komprimiert worden sind.

Zur Information für die technisch Interessierten sei angemerkt, daß das Programm die Freeware-ZIP-Komprimierungsroutinen verwendet, die von Jean-Loup Gailly, Mark Adler und Richard B. Wales geschrieben wurden. Diese ZIP-Software verwendet Komprimierungsalgorithmen, die in ihrer Funktionsweise den von PKZIP 2.x von PKWare verwendeten Algorithmen entsprechen. Diese ZIP-Komprimierungssoftware wurde für PGP hauptsächlich aufgrund des guten Komprimierungsverhältnisses und aufgrund ihrer Schnelligkeit ausgewählt.

Als Sitzungsschlüssel verwendete Zufallszahlen

PGP verwendet zur Erstellung von temporären Sitzungsschlüsseln einen kryptographisch leistungsfähigen Generator für Pseudo-Zufallswerte. Wenn diese Datei mit Zufallswerten nicht existiert, wird sie automatisch erstellt und mit echten Zufallswerten aufgefüllt. Diese Zufallswerte werden durch das PGP-Programm aus Zufallsereignissen auf der Grundlage der zeitlichen Koordination von Tastaturbetätigungen und Mausbewegungen abgeleitet.

Dieser Generator füllt die Zufallswertedatei bei jeder Verwendung mit neuen Zufallswerten auf. Dabei wird neues Datenmaterial, das teilweise von der Tageszeit oder anderen echten Zufallsquellen abgeleitet wurde, hinzugefügt und mit den alten Daten vermischt. Der konventionelle Verschlüsselungsalgorithmus wird dabei als Motor für den Zufallswertegenerator verwendet. Die Datei mit den Zufallswerten enthält sowohl Zufallsdatenmaterial als auch Zufallsverschlüsselungsmaterial, das zur Verschlüsselung des konventionellen Verschlüsselungsmotors für den Zufallsgenerator verwendet wird.

Diese Zufallswertedatei sollte besonders geschützt werden, um das Risiko zu verringern, daß ein Hacker Ihre nächsten oder zuvor verwendeten Sitzungsschlüssel aus ihr ableiten kann. Der Hacker hätte zwar sehr viel Mühe, nützliche Informationen aus dieser Datei mit Zufallswerten zu ziehen, da die Datei vor und nach jeder Verwendung kryptographisch „gereinigt“ wird. Dennoch ist es sinnvoll, sie vor unbefugtem Zugriff zu schützen. Stellen Sie nach Möglichkeit sicher, daß nur Sie diese Datei lesen können. Falls dies nicht möglich ist, lassen Sie andere Personen nicht beliebig Dateien von Ihrem Computer kopieren.

Nachrichtenkern

Der Nachrichtenkern ist die kompakte „Essenz“ von 160 oder 128 Bit Größe Ihrer Nachricht oder eine Dateiprüfsumme. Sie können ihn sich als „Fingerabdruck“ der Nachricht oder der Datei vorstellen. Der Nachrichtenkern „repräsentiert“ Ihre E-Mail-Nachricht. Wenn die Nachricht in irgendeiner Form verändert wird, ändert sich auch der aus ihr berechnete Nachrichtenkern. Dadurch können alle von einem Fälscher an der Nachricht vorgenommenen Änderungen aufgedeckt werden. Der Nachrichtenkern wird mit Hilfe einer kryptographisch leistungsfähigen, einseitigen Hash-Funktion der Nachricht berechnet. Für einen Hacker sollte es rechnerisch unmöglich sein, eine Ersatznachricht zu erstellen, die einen identischen Nachrichtenkern erzeugen würde. In dieser Hinsicht ist ein Nachrichtenkern sehr viel besser als eine Prüfsumme, da es leicht ist, eine Nachricht mit anderem Inhalt zu erstellen, die dieselbe Prüfsumme erzeugt. Wie bei einer Prüfsumme können Sie die Originalnachricht jedoch nicht von ihrem Nachrichtenkern herleiten.

Der derzeit in PGP (Version 5.0 oder höher) verwendete Nachrichtenkernalgorithmus wird SHA (Secure Hash Algorithmus; Sicherer Hash-Algorithmus) genannt. Er wurde vom NSA für das nationale Institut für Standards und Technologie (National Institute of Standards and Technology, NIST) entwikkelt. SHA ist ein 160-Bit-Hash-Algorithmus. Es mag Personen geben, die dem nationalen Sicherheitsdienst NSA skeptisch gegenüberstehen, da der NSA auf das Abhören von Gesprächen und Entschlüsseln von Codes spezialisiert ist. Bedenken Sie jedoch, daß der NSA kein Interesse am Fälschen von Unterschriften hat, und daß die Regierung von einem nicht zu fälschenden Unterschriftsstandard profitieren würde, der verhindert, daß jemand seine Unterschrift zurückweist. Dies hat verschiedene Vorteile für die Strafverfolgung und das Sammeln von Beweisen. Der Algorithmus wurde außerdem in der gängigen Literatur veröffentlicht und von vielen der weltweit besten Kryptologen, die sich auf Hash-Funktionen spezialisiert haben, genauestens überprüft. Es besteht die allgemeine Meinung, daß SHA ausgesprochen gut entwickelt ist. Der Algorithmus verfügt über einige Verbesserungen in der Entwicklung, mit denen alle in Nachrichtenkernalgorithmen beobachteten Schwächen, die von Kryptologen bislang entdeckt wurden, behoben werden. Alle neuen PGP-Versionen verwenden SHA als Nachrichtenkernalgorithmus, um Unterschriften mit den neuen DSS-Schlüsseln zu erstellen, die dem digitalen Standard für Unterschriften NIST entsprechen. Aus Kompatibilitätsgründen wird in neuen PGP-Versionen immer noch MD5 für RSA-Unterschriften verwendet, da MD5 bereits in älteren PGP-Versionen für RSA-Unterschriften verwendet wurde.

Der von älteren PGP-Versionen verwendete Nachrichtenkernalgorithmus ist der MD5-Nachrichtenkernalgorithmus, der durch RSA Data Security frei zugänglich gemacht wurde. MD5 ist ein 128-Bit-Hash-Algorithmus. 1996 wäre es dem deutschen Kryptologen Hans Dobbertin fast gelungen, MD5 zu entschlüsseln. Obwohl MD5 zu diesem Zeitpunkt noch nicht vollständig entschlüsselt wurde, wurden doch so ernsthafte Schwächen festgestellt, daß es nicht mehr zur Erzeugung von Unterschriften verwendet werden sollte. Weitere Anstrengungen auf diesem Gebiet könnten dazu führen, daß der Algorithmus vollständig entschlüsselt wird und Unterschriften somit gefälscht werden könnten. Wenn Sie nicht eines Tages Ihre digitale PGP-Unterschrift auf einem gefälschten Geständnis finden möchten, sind Sie am besten beraten, wenn Sie die neuen PGP-DSS-Schlüssel in Zukunft bevorzugt zum Erstellen von digitalen Unterschriften verwenden, da DSS SHA als sicheren Hash-Algorithmus verwendet.

So schützen Sie öffentliche Schlüssel vor Manipulation

In einem Verschlüsselungssystem mit öffentlichen Schlüsseln brauchen Sie öffentliche Schlüssel nicht nach außen zu schützen. Es ist sogar besser, sie so weit wie möglich zu verbreiten. Es ist jedoch wichtig, öffentliche Schlüssel vor Manipulation zu schützen. Nur so können Sie sicherstellen, daß ein öffentlicher Schlüssel tatsächlich der Person gehört, zu der er zu gehören scheint. Dies ist wahrscheinlich die größte potentielle Schwachstelle in einem Kryptosystem mit öffentlichen Schlüsseln. Im folgenden wird zuerst eine Situation beschrieben, die im schlimmsten Fall eintreten könnte, und dann wird erläutert, wie Sie solch eine Katastrophe mit PGP sicher verhindern können.

Angenommen, Sie möchten an eine Person namens Susanne eine private Nachricht senden. Sie laden das öffentliche Schlüsselzertifikat von Susanne von einem elektronischen BBS (Bulletin Board System), d. h. einer Mailbox, herunter. Sie verschlüsseln Ihre Nachricht an Susanne mit diesem öffentlichen Schlüssel und senden ihn über die E-Mail-Funktion der Mailbox an sie.

Unglücklicherweise ist ohne Ihr oder Susannes Wissen ein anderer Benutzer in die Mailbox eingedrungen, den wir Rainer nennen. Rainer hat einen eigenen öffentlichen Schlüssel erzeugt und die Benutzer-ID von Susanne mit diesem öffentlichen Schlüssel verknüpft. Er hat heimlich den echten öffentlichen Schlüssel von Susanne durch seinen unechten Schlüssel ersetzt. Sie benutzen nun unwissentlich diesen unechten Schlüssel von Rainer anstatt Susannes öffentlichen Schlüssel. Diese Situation bleibt unbemerkt, da der unechte Schlüssel die Benutzer-ID von Susanne hat. Rainer kann nun die für Susanne bestimmte Nachricht dechiffrieren, da er über den passenden privaten Schlüssel verfügt. Er könnte sogar die dechiffrierte Nachricht mit dem echten öffentlichen Schlüssel von Susanne wieder verschlüsseln und sie an Susanne schicken, so daß kein Verdacht entsteht. Zudem kann er mit diesem privaten Schlüssel scheinbar gültige Unterschriften von Susanne erzeugen, da alle den unechten Schlüssel zur Überprüfung von Susannes Unterschrift verwenden.

Sie können dies nur verhindern, indem Sie öffentliche Schlüssel vor jeglicher Manipulation schützen. Wenn Sie den öffentlichen Schlüssel von Susanne direkt von Susanne erhalten, besteht keinerlei Problem. Dies könnte jedoch mit Schwierigkeiten verbunden sein, wenn Susanne tausende von Kilometern entfernt wohnt oder zur Zeit nicht erreichbar ist.

Möglicherweise können Sie den öffentlichen Schlüssel von Susanne über einen gemeinsamen Freund, Claus, erhalten, der weiß, daß er über eine echte Kopie von Susannes öffentlichem Schlüssel verfügt. Claus könnte Susannes öffentlichen Schlüssel unterschreiben und sich somit für die Echtheit von Susannes Schlüssel verbürgen. Claus würde diese Unterschrift mit seinem eigenen privaten Schlüssel erstellen.

Dadurch würde ein Unterschriftszertifikat für den öffentlichen Schlüssel erstellt, das beweist, daß Susannes Schlüssel nicht manipuliert wurde. Voraussetzung hierfür ist, daß Sie über eine anerkannt echte Kopie von Claus' öffentlichem Schlüssel zum Überprüfen seiner Unterschrift verfügen. Möglicherweise könnte Claus Susanne auch eine unterschriebene Kopie Ihres öffentlichen Schlüssels zur Verfügung stellen. Claus würde dann als „Schlüsselverwalter" für Sie und Susanne fungieren.

Dieses unterschriebene Zertifikat für den öffentlichen Schlüssel von Susanne könnte von Claus oder Susanne in die Mailbox geladen werden. Sie haben die Möglichkeit, es später wieder herunterzuladen. Sie könnten dann die Unterschrift mit Hilfe von Claus' öffentlichem Schlüssel überprüfen und folglich sicher sein, daß es sich tatsächlich um Susannes öffentlichen Schlüssel handelt. Ein Betrüger könnte Sie nicht täuschen und dazu verleiten, seinen falschen Schlüssel als Susannes Schlüssel zu akzeptieren, da keine andere Person von Claus erzeugte Unterschriften fälschen kann.

Eine allgemein als vertrauenswürdig erachtete Person könnte sich sogar darauf spezialisieren, als Schlüsselverwalter für Benutzer zu fungieren, indem sie Unterschriftszertifikate für öffentliche Schlüssel dieser Benutzer liefert. Diese vertrauenswürdige Person könnte als „Zertifizierungsinstanz" betrachtet werden. Bei allen Zertifikaten für öffentliche Schlüssel, die über die Unterschrift der Zertifizierungsinstanz verfügen, könnte vollständig darauf vertraut werden, daß der öffentliche Schlüssel tatsächlich und nicht nur dem Anschein nach der entsprechenden Person gehört. Alle Benutzer, die teilnehmen möchten, benötigen lediglich eine bekanntermaßen gute Kopie des öffentlichen Schlüssels der Instanz, um die Unterschriften der Zertifizierungsinstanz verifizieren zu können. In manchen Fällen kann die Zertifizierungsinstanz auch als Schlüssel-Server fungieren. Benutzer, die an ein Netzwerk angeschlossen sind, könnten dann über den Schlüssel-Server öffentliche Schlüssel in Erfahrung bringen. Es besteht jedoch kein Grund für eine Zertifizierung der Schlüssel durch den Schlüssel-Server.

Eine vertrauenswürdige Zertifizierungsinstanz bietet sich besonders für große, anonyme und zentral geleitete Firmen oder Regierungsinstitutionen an. In einigen institutionellen Arbeitsumgebungen existieren Hierarchien von Zertifizierungsinstanzen.

Bei dezentralisierteren Umgebungen ist es wahrscheinlich effektiver, es allen Benutzern zu ermöglichen, als vertrauenswürdige Schlüsselverwalter für ihre Freunde zu fungieren, anstatt auf eine zentralisierte Schlüsselzertifizierungsinstanz zurückzugreifen.

Eine der herausragenden Funktionen von PGP ist, daß das Programm sowohl in einer zentralisierten Umgebung mit einer Zertifizierungsinstanz als auch in einer weiter dezentralisierten Umgebung, in der einzelne Personen ihre privaten Schlüssel miteinander austauschen, verwendet werden kann.

Der Schutz öffentlicher Schlüssel vor möglicher Verfälschung ist das schwierigste Problem in der praktischen Anwendung der Kryptographie mit öffentlichen Schlüsseln. Dieses Problem ist die „Achillessehne“ der Kryptographie mit öffentlichen Schlüsseln, und große Teile der Software sind ausschließlich dazu da, dieses Problem zu lösen.

Sie sollten einen öffentlichen Schlüssel nur verwenden, wenn Sie sicher sind, daß es sich um einen echten öffentlichen Schlüssel handelt, der nicht verfälscht wurde, und daß er tatsächlich der Person gehört, zu der er angeblich gehört. Sie können sicher sein, daß dies der Fall ist, wenn Sie das Zertifikat für den öffentlichen Schlüssel direkt von seinem Eigentümer erhalten haben, oder wenn es über die Unterschrift einer dritten Person verfügt, der Sie vertrauen und von der Sie bereits einen echten öffentlichen Schlüssel erhalten haben. Darüber hinaus sollte die Benutzer-ID den vollständigen Namen des Schlüssel-Eigentümers enthalten, nicht nur den Vornamen.

Sie sollten *in keinem Fall*, so einfach es auch erscheinen mag, einem öffentlichen Schlüssel vertrauen, den Sie von einer Mailbox heruntergeladen haben, wenn dieser nicht von einer Person unterschrieben wurde, der Sie vertrauen. Dieser nicht zertifizierte öffentliche Schlüssel kann durch eine beliebige Person verfälscht worden sein, möglicherweise sogar durch den Systemadministrator der Mailbox.

Wenn Sie gebeten werden, das Zertifikat des öffentlichen Schlüssels einer anderen Person zu unterschreiben, sollten Sie sicherstellen, daß es tatsächlich von der Person stammt, die in der Benutzer-ID dieses Zertifikats genannt wird. Denn mit Ihrer Unterschrift auf dem Zertifikat des öffentlichen Schlüssels dieser Person verbürgen Sie sich dafür, daß dieser öffentliche Schlüssel tatsächlich ihr gehört. Andere Personen, die Ihnen vertrauen, akzeptieren den öffentlichen Schlüssel dieser Person, weil er mit Ihrer Unterschrift versehen ist. Sie sollten nicht auf Informationen aus zweiter Hand vertrauen. Unterschreiben Sie den öffentlichen Schlüssel der anderen Person erst, wenn Sie über unabhängige Informationen aus erster Hand verfügen, daß der Schlüssel tatsächlich zu dieser Person gehört. Sie sollten ihn nur dann unterschreiben, wenn Sie ihn direkt von der betreffenden Person selbst erhalten haben.

Um einen öffentlichen Schlüssel zu unterschreiben, müssen Sie nicht nur sicherstellen, daß der Schlüssel tatsächlich zum angegebenen Eigentümer gehört, da Sie den Schlüssel nicht nur zum Verschlüsseln einer Nachricht verwenden möchten. Zertifizierende Unterschriften von autorisierten Schlüsselverwaltern sollten ausreichend sein, um Sie davon zu überzeugen, daß ein Schlüssel wirklich echt ist und Sie ihn verwenden können. Wenn Sie jedoch selbst einen Schlüssel unterschreiben möchten, sollten Sie über unabhängige Informationen aus erster Hand zu dem Eigentümer dieses Schlüssels verfügen. Sie könnten beispielsweise den Eigentümer des Schlüssels anrufen und ihm den Fingerabdruck des Schlüssels nennen, um zu bestätigen, daß der Schlüssel, den Sie haben, tatsächlich der Schlüssel dieser Person ist. Stellen Sie sicher, daß Sie mit der richtigen Person sprechen.

Denken Sie daran, daß Sie sich mit Ihrer Unterschrift für das Zertifikat des öffentlichen Schlüssels nicht für die Integrität dieser Person verbürgen, sondern lediglich für die Integrität dieses öffentlichen Schlüssels, d. h. für die Tatsache, daß der Schlüssel zu dieser Person gehört. Sie riskieren also Ihre Glaubwürdigkeit nicht, wenn Sie den öffentlichen Schlüssel eines Kriminellen unterschreiben, wenn Sie absolut sicher sind, daß dieser Schlüssel tatsächlich zu ihm gehört. Andere Personen werden dann den Schlüssel als seinen Schlüssel akzeptieren, da er von Ihnen unterschrieben wurde (vorausgesetzt, diese Personen vertrauen Ihnen), doch sie würden deshalb nicht dem Eigentümer des Schlüssels vertrauen. Vertrauen in einen Schlüssel ist nicht identisch mit dem Vertrauen in den Eigentümer eines Schlüssels.

Es ist empfehlenswert, Ihren eigenen öffentlichen Schlüssel zusammen mit einer Sammlung zertifizierender Unterschriften von verschiedenen Schlüsselverwaltern aufzubewahren. So besteht die Chance, daß die meisten Personen zumindest einem der Schlüsselverwalter vertrauen, die sich für die Gültigkeit Ihres öffentlichen Schlüssels verbürgen. Sie könnten Ihren Schlüssel mit der angehängten Sammlung zertifizierender Unterschriften in verschiedenen Mailboxen ablegen. Wenn Sie den öffentlichen Schlüssel einer anderen Person unterschreiben, senden Sie ihn mit Ihrer Unterschrift an diese Person zurück, so daß diese Person Ihre Unterschrift in ihre Sammlung an Authentisierungen für ihren eigenen öffentlichen Schlüssel aufnehmen kann.

Stellen Sie sicher, daß keine andere Person die Möglichkeit hat, Ihren eigenen öffentlichen Schlüsselbund zu verfälschen. Die Überprüfung eines neu unterzeichneten Zertifikats für einen öffentlichen Schlüssel hängt letztlich von der Integrität der vertrauenswürdigen öffentlichen Schlüssel ab, die sich bereits in Ihrem Schlüsselbund befinden. Stellen Sie sicher, daß Sie die physische Kontrolle über Ihren öffentlichen Schlüsselbund haben. Er sollte sich, wie Ihr privater Schlüssel, vorzugsweise auf Ihrem eigenen PC befinden und nicht auf einem entfernten Mehrbenutzersystem. Dadurch schützen Sie den öffentlichen Schlüsselbund vor Verfälschungen, nicht vor Zugriff. Bewahren Sie eine Sicherungskopie Ihres öffentlichen Schlüsselbundes und Ihres privaten Schlüssels auf einem schreibgeschützten Medium auf.

Da Ihr eigener vertrauenswürdiger öffentlicher Schlüssel die letztgültige Autorität zum direkten oder indirekten Zertifizieren aller anderen Schlüssel in Ihrem Schlüsselbund ist, ist er der wichtigste Schlüssel, der vor Fälschungsversuchen geschützt werden muß. Bewahren Sie eine Sicherungskopie auf einer schreibgeschützten Diskette auf.

PGP arbeitet allgemein unter der Voraussetzung, daß Sie die physische Sicherheit Ihres Systems und Ihrer Schlüsselbunde und auch Ihrer PGP-Version selbst sicherstellen. Wenn ein Eindringling die Möglichkeit hat, Ihre Festplatte zu manipulieren, kann er theoretisch auch Änderungen am Programm vornehmen und Sicherheitsfunktionen des Programms ausschalten, mit denen das Verfälschen von Schlüsseln verhindert wird.

Eine etwas komplizierte Art, Ihren gesamten öffentlichen Schlüsselbund vor Verfälschung zu schützen, besteht darin, den gesamten Schlüsselbund mit Ihrem eigenen privaten Schlüssel zu unterschreiben. Dies ist beispielsweise möglich durch das Erstellen eines separaten Unterschriftszertifikats von Ihrem öffentlichen Schlüsselbund.

Wie verfolgt PGP, welche Schlüssel gültig sind?

Lesen Sie zuerst den vorangegangenen Abschnitt („So schützen Sie öffentliche Schlüssel vor Manipulation“), bevor Sie mit diesem Abschnitt beginnen.

PGP zeichnet auf, welche Schlüssel Ihres öffentlichen Schlüsselbundes ordnungsgemäß mit Unterschriften von vertrauenswürdigen Schlüsselverwaltern zertifiziert wurden. Sie müssen PGP lediglich mitteilen, welchen Personen Sie als Schlüsselverwalter vertrauen, und deren Schlüssel mit Ihrem eigenen, unbedingt vertrauenswürdigen Schlüssel selbst unterschreiben. PGP kann dann das „Steuer übernehmen“ und automatisch andere Schlüssel überprüfen, die die von Ihnen bestimmten Schlüsselverwalter unterschrieben haben. Und Sie können selbstverständlich auch selbst weitere Schlüssel direkt unterschreiben.

PGP verwendet zur Beurteilung des Wertes eines öffentlichen Schlüssels zwei voneinander völlig unabhängige Kriterien, die Sie nicht miteinander verwechseln sollten:

1. Gehört der Schlüssel tatsächlich zu der Person, zu der er zu gehören scheint? Anders ausgedrückt: Wurde der Schlüssel durch eine vertrauenswürdige Unterschrift zertifiziert?

2. Gehört der Schlüssel zu einer Person, der Sie bezüglich der Zertifizierung anderer Schlüssel vertrauen können?

PGP kann die Antwort auf die erste Frage errechnen. Die Antwort auf die zweite Frage müssen Sie PGP genau mitteilen. Wenn Sie Frage 2 beantwortet haben, kann PGP die Antwort zu Frage 1 für andere Schlüssel berechnen, die von dem Schlüsselverwalter unterschrieben wurden, dem Sie Ihr Vertrauen ausgesprochen haben.

Schlüssel, die von einem autorisierten Schlüsselverwalter zertifiziert worden sind, werden von PGP für echt gehalten. Die zu autorisierten Schlüsselverwaltern gehörenden Schlüssel wiederum müssen entweder von Ihnen oder von anderen vertrauenswürdigen Schlüsselverwaltern zertifiziert werden.

Darüber hinaus können Sie mit PGP die Eignung von bestimmten Personen als Schlüsselverwalter durch Zuweisung eines bestimmten Vertrauensgrads präzisieren. Das Vertrauen, das Sie einem Schlüsseleigentümer bezüglich seiner Eignung als Schlüsselverwalter aussprechen, spiegelt nicht nur Ihre Einschätzung der persönlichen Integrität dieser Personen wider. Es sollte auch ausdrücken, in welchem Maße Sie dieser Person Kompetenz bei der Schlüsselverwaltung und gutes Urteilsvermögen beim Unterschreiben von Schlüsseln zutrauen. Sie können einer Person kein, geringes oder volles Vertrauen zum Zertifizieren von anderen öffentlichen Schlüsseln aussprechen. Der angegebene Vertrauensgrad wird in Ihrem Schlüsselbund zusammen mit dem Schlüssel dieser Personen gespeichert. Wenn Sie PGP jedoch zum Kopieren eines Schlüssels von Ihrem Schlüsselbund auffordern, werden diese Vertrauensinformationen nicht mitkopiert, da Ihre private Meinung bezüglich des Vertrauens vertraulich behandelt wird.

Wenn PGP die Echtheit eines öffentlichen Schlüssels berechnet, überprüft es den Vertrauensgrad aller angehängten zertifizierenden Unterschriften. Es berechnet einen abgewogenen Echtheitswert. Zwei Unterschriften mit einem geringen Vertrauen werden beispielsweise als genauso vertrauenswürdig betrachtet wie eine Unterschrift mit vollem Vertrauen. Die Skepsis des Programms kann eingestellt werden. Sie können beispielsweise PGP so einstellen, daß zwei Unterschriften mit vollem Vertrauen oder drei Unterschriften mit geringem Vertrauen notwendig sind, damit ein Schlüssel als echt beurteilt wird.

Ihr eigener Schlüssel wird „axiomatisch“ von PGP als echt anerkannt und benötigt keine Unterschrift eines Schlüsselverwalters als Gültigkeitsbeweis. PGP weiß, welche öffentlichen Schlüssel zu Ihnen gehören, indem es im privaten Schlüsselbund nach den entsprechenden privaten Schlüsseln sucht. PGP geht auch davon aus, daß Sie sich selbst zum Zertifizieren anderer Schlüssel volles Vertrauen aussprechen.

Im Laufe der Zeit werden Sie über immer mehr Schlüssel von anderen Personen verfügen, die Sie möglicherweise als autorisierte Schlüsselverwalter bestimmen möchten. Alle anderen Personen werden ihre eigenen autorisierten Schlüsselverwalter wählen. So bauen alle nach und nach eine Sammlung von zertifizierenden Unterschriften anderer Personen auf und verteilen sie mit ihrem Schlüssel in der Hoffnung, daß die Empfänger zumindest einer oder zwei der Unterschriften vertrauen. Dadurch entsteht ein dezentrales, fehlertolerantes Vertrauensnetz für alle öffentlichen Schlüssel.

Dieser einzigartige basisorientierte Ansatz unterscheidet sich erheblich von den üblichen Verwaltungssystemen für öffentliche Schlüssel, die von der Regierung und anderen Institutionen entwickelt wurden, wie beispielsweise Internet Privacy Enhanced Mail (PEM), die auf einer zentralisierten Kontrolle und vorgeschriebenem zentralisiertem Vertrauen basieren. Diese Standardsysteme beruhen auf einer Hierarchie an Zertifizierungsinstanzen, die vorschreiben, wem Sie vertrauen müssen. Die dezentralisierte, probabilistische Methode des Programms zur Bestimmung der Legitimität öffentlicher Schlüssel stellt das Herzstück seiner Schlüsselverwaltungsarchitektur dar. In PGP bestimmen Sie allein, wem Sie vertrauen, so daß Sie an der Spitze Ihrer privaten Zertifizierungspyramide stehen. PGP ist für Personen bestimmt, die Verantwortung lieber selbst wahrnehmen.

Die Betonung dieses dezentralisierten, basisorientierten Ansatzes bedeutet jedoch nicht, daß PGP in stärker hierarchisch ausgeprägten, zentralisierten Verwaltungssystemen für öffentliche Schlüssel nicht ebenso leistungsfähig ist. Beispielsweise ziehen es große Unternehmen möglicherweise vor, das Unterschreiben aller Mitarbeiterschlüssel von einer zentralen Stelle oder Person vornehmen zu lassen. PGP ermöglicht dieses zentralisierte Szenario als speziellen Ausnahmefall im Rahmen des allgemeineren Vertrauensmodells von PGP.

So schützen Sie private Schlüssel vor unbefugtem Zugriff

Schützen Sie Ihren privaten Schlüssel und Ihre Paßphrase sorgfältig. Falls Ihr privater Schlüssel nicht mehr sicher sein sollte, informieren Sie so schnell wie möglich alle betroffenen Personen darüber, bevor eine dritte Person diesen Schlüssel verwendet, um in Ihrem Namen zu unterschreiben. Ein Dritter könnte beispielsweise den privaten Schlüssel zum Unterschreiben von gefälschten Zertifikaten für öffentliche Schlüssel verwenden. Dies könnte für viele Personen problematisch werden, insbesondere dann, wenn ein großer Personenkreis Ihrer Unterschrift vertraut. Eine Gefährdung Ihres eigenen privaten Schlüssels könnte selbstverständlich auch zur Offenlegung aller an Sie gesendeten Nachrichten führen.

Um Ihren privaten Schlüssel zu schützen, sollten Sie ihn zuallererst stets sicher aufbewahren. Sie können ihn auf Ihrem PC zu Hause oder auf Ihrem Notebook-Computer speichern, den Sie mit sich führen. Wenn Sie einen Computer im Büro verwenden müssen, zu dem nicht nur Sie allein physischen Zugang haben, sollten Sie Ihren öffentlichen und privaten Schlüsselbund auf einer schreibgeschützten Diskette aufbewahren und diese nicht unbeaufsichtigt lassen. Es ist nicht ratsam, den privaten Schlüssel auf einem entfernten Host, wie beispielsweise einem UNIX-System zur Ferneinwahl aufzubewahren. Jemand könnte heimlich Ihre Modem-Leitung abhören, Ihre Paßphrase abfangen und dann Ihren privaten Schlüssel von dem entfernten System abrufen. Sie sollten einen privaten Schlüssel nur auf einem Computer verwenden, auf den Sie ständig zugreifen.

Speichern Sie Ihre Paßphrase nicht auf dem Computer, auf dem sich Ihre private Schlüsseldatei befindet. Das Speichern Ihres privaten Schlüssels und der Paßphrase auf dem gleichen Computer ist genauso gefährlich wie das Aufbewahren der Karte für den Geldautomaten zusammen mit der Geheimnummer in einem Portemonnaie. Die Paßphrase darf sich also nicht auf demselben Datenträger befinden wie die private Schlüsseldatei. Am sichersten ist es, wenn Sie Ihre Paßphrase auswendig lernen und sie ausschließlich in Ihrem Kopf speichern. Wenn Sie Ihre Paßphrase aufschreiben müssen, sollten Sie eine sichere Stelle wählen, möglicherweise sogar sicherer als die Stelle, an der Sie Ihre private Schlüsseldatei aufbewahren.

Fertigen Sie außerdem Sicherungskopien von Ihrem privaten Schlüssel an. Denken Sie daran, daß Sie über die einzige Kopie Ihres privaten Schlüssels verfügen. Wenn Sie diese Kopie verlieren, sind alle Kopien Ihres öffentlichen Schlüssels, die Sie über die ganze Welt hinweg verteilt haben, nicht mehr zu verwenden.

Der dezentralisierte, nicht institutionelle Ansatz, den PGP zur Verwaltung von öffentlichen Schlüsseln unterstützt, hat seine Vorteile. Sein Nachteil ist, daß es keine einzige zentralisierte Liste von Schlüsseln gibt, die nicht mehr sicher sind. Dadurch wird es etwas schwieriger, den durch unsicher gewordene Schlüssel verursachten Schaden einzugrenzen. Sie können nur die Information verbreiten und darauf hoffen, daß sie bei allen betroffenen Personen ankommt.

Im schlimmsten Fall, d. h., wenn sowohl Ihr privater Schlüssel als auch die Paßphrase nicht mehr sicher sind (und Sie dies hoffentlich auch entdecken), müssen Sie ein „Schlüsselrücknahmezertifikat“ ausstellen. Mit diesem Zertifikat warnen Sie andere Personen davor, Ihren öffentlichen Schlüssel weiterhin zu verwenden. Sie können ein solches Zertifikat mit PGP erstellen, indem Sie im PGPkeys-Menü den Befehl „Zurücknehmen“ wählen. Alternativ kann der zugeordnete Schlüssel zur Zurücknahme diese Aufgabe für Sie übernehmen. Sie müssen das Zertifikat anschließend an den Certificate Server senden, so daß andere Benutzer auf das Zertifikat zugreifen können. Die PGP-Software der Empfänger wiederum installiert das Zurücknahmezertifikat für den Schlüssel in deren öffentlichen Schlüsselbunden und verhindert automatisch, daß Ihr öffentlicher Schlüssel versehentlich wieder verwendet wird. Sie können dann ein neues Schlüsselpaar (d. h. einen neuen privaten und einen zugehörigen öffentlichen Schlüssel) erstellen und den neuen öffentlichen Schlüssel veröffentlichen. Sie können auch Ihren neuen öffentlichen Schlüssel und das Zurücknahmezertifikat für den Schlüssel für Ihren alten Schlüssel zusammen verschicken.

Was passiert, wenn Sie Ihren privaten Schlüssel verlieren?

Sie können Ihren eigenen privaten Schlüssel zurücknehmen, indem Sie im PGPkeys-Menü den Befehl „Zurücknehmen“ wählen und ein Zurücknahmezertifikat ausstellen, das mit Ihrem eigenen privaten Schlüssel unterschrieben wird.

Aber was können Sie tun, wenn Sie Ihren privaten Schlüssel verlieren, oder wenn Ihr privater Schlüssel zerstört wurde? Sie können den öffentlichen Schlüssel nicht selbst zurücknehmen, da Sie Ihren eigenen privaten Schlüssel zum Zurücknehmen benötigen, diesen aber nicht mehr besitzen. Wenn Sie Ihrem Schlüssel keinen Rücknahmeschlüssel zugeordnet haben (d. h., einen PGP-Benutzer, der den Schlüssel in Ihrem Namen zurücknehmen kann), so müssen Sie jeden Benutzer, der Ihren Schlüssel unterzeichnet hat, darum bitten, seine Zertifizierung zurückzunehmen. Dadurch erfahren alle Personen, die Ihren Schlüssel aufgrund des ausgesprochenen Vertrauens einer Ihrer Schlüsselverwalter verwenden möchten, daß Sie Ihrem öffentlichen Schlüssel nicht vertrauen können.

Weitere Informationen zu zugeordneten Rücknahmeschlüsseln finden Sie im Abschnitt „So legen Sie einen zugeordneten Rücknahmeschlüssel fest“ in Kapitel 6.

Lassen Sie sich nicht täuschen

Wenn Sie ein kryptographisches Software-Paket überprüfen, stellt sich am Ende immer die Frage, warum Sie diesem Produkt trauen sollten. Selbst wenn Sie den Quellcode selbst überprüfen, haben Sie vielleicht nicht genügend Erfahrung in der Kryptographie, um die Sicherheit wirklich beurteilen zu können. Und selbst wenn Sie viel Erfahrung in der Kryptographie besitzen, können Sie kleine Schwächen in den Algorithmen möglicherweise übersehen.

Als Student erfand ich in den frühen siebziger Jahren ein meiner Meinung nach brillantes Verschlüsselungssystem. Um chiffrierten Text zu erzeugen, fügte ich zum Klartextdatenstrom einen einfachen Datenstrom aus Pseudozufallswerten hinzu. Ich war der Ansicht, daß dadurch jedwede Häufigkeitsanalyse an dem chiffrierten Text vereitelt würde und selbst die raffiniertesten Geheimdienste der Regierung den Text nicht decodieren könnten. Ich war mehr als stolz auf meine Idee.

Jahre später entdeckte ich genau dieses System in mehreren einleitenden Texten und Lernmaterialien zur Kryptographie. Großartig. Andere Kryptologen hatten dieselbe Idee gehabt. Leider wurde das System als einfache Übung zu dem Thema verwendet, wie ein Verschlüsselungssystem mit einfachen kryptographischen Techniken aufgebrochen werden kann. So viel zu meiner genialen Idee.

Aus dieser demütigenden Erfahrung lernte ich, wie schnell man beim Entwikkeln eines Verschlüsselungsalgorithmus ein falsches Sicherheitsgefühl entwickeln kann. Die wenigsten Menschen sind sich bewußt, wie extrem schwierig es ist, einen Verschlüsselungsalgorithmus zu entwickeln, der andauernden und hartnäckigen Angriffen eines raffinierten Gegners widerstehen kann. Viele allgemein ausgebildete Software-Ingenieure haben in bester Absicht ebenso einfach zu decodierende Verschlüsselungssysteme (oftmals sogar dasselbe Verschlüsselungssystem) entwickelt, und manche dieser Systeme wurden in kommerzielle Verschlüsselungssoftwarepakete eingebunden und für sehr viel Geld an Tausende arglose Benutzer verkauft.

Dies ist vergleichbar mit dem Verkauf eines Sicherheitsgurtes, dessen Design vom äußeren Eindruck her überzeugend ist, der jedoch bei der geringsten Geschwindigkeit im Aufpralltest aufspringt. Sich auf diese Sicherheitsgurte zu verlassen, kann schlimmere Folgen haben, als gar keinen Sicherheitsgurt zu verwenden. Denn niemand vermutet, daß Gurte untauglich sind – bis es wirklich zum Unfall kommt. Wenn Sie sich auf eine schwache kryptographische Software verlassen, setzen Sie unter Umständen wichtige und vertrauliche Daten unbewußt einem Risiko aus, was Sie ohne die kryptographische Software vielleicht nicht getan hätten. Möglicherweise fällt Ihnen noch nicht einmal auf, daß eine unbefugte Person auf Ihre Daten zugegriffen hat.

In manchen kommerziellen Software-Paketen wird der DES-Standard (Federal Data Encryption Standard) verwendet, ein recht guter, konventioneller Algorithmus, der von der Regierung für den professionellen Gebrauch (seltsamerweise jedoch nicht für unter Geheimschutz gestellte Informationen – hmmm..) empfohlen wird. DES kann in verschiedenen „Betriebsmodi“ verwendet werden, wobei einige qualitativ besser sind als andere. Die Regierung empfiehlt ausdrücklich, für Nachrichten nicht den einfachsten und unsichersten Modus, den ECB-Modus (Electronic Codebook), zu verwenden. Sie empfiehlt jedoch die leistungsstärkeren und komplexeren Modi CFB (Cipher Feedback) und CBC (Cipher Block Chaining).

Leider wird in den meisten mir bekannten kommerziellen Verschlüsselungsprogrammpaketen der ECB-Modus verwendet. Als ich mit einigen der Entwickler dieser Programme sprach, sagten sie mir, daß sie noch nie vom CBC- oder CFB-Modus gehört hätten und daß ihnen nichts über die Schwächen des ECB-Modus bekannt sei. Schon allein die Tatsache, daß die Entwickler dieser Programme über so wenig kryptographische Kenntnisse verfügen, daß ihnen diese elementaren Konzepte nicht bekannt sind, ist nicht gerade beruhigend. Außerdem werden die DES-Schlüssel in diesen Programmen zum Teil auf ungeeignete und unsichere Weise verwaltet. Diese Software-Pakete enthalten oft auch einen zweiten, schnelleren Verschlüsselungsalgorithmus, der anstelle des langsameren DES verwendet werden kann. Die Entwickler dieser Programmpakete waren oft der Meinung, daß der eigene schnelle Algorithmus genauso sicher wie DES sei, doch nach einigen Nachfragen stellte ich immer wieder fest, daß es sich lediglich um eine Variante des „genialen Systems“ aus meiner Studentenzeit handelte. Teilweise wollten die Entwickler die Funktionsweise ihrer eigenen Verschlüsselungssysteme überhaupt nicht preisgeben, versicherten mir jedoch, es handle sich um ein geniales System, und ich solle ihnen ruhig vertrauen. Ich bin sicher, daß die Entwickler ihren Algorithmus für genial halten, aber wie kann ich sicher sein, wenn ich ihn mir nicht ansehen kann?

Fairerweise muß ich an dieser Stelle anmerken, daß diese extrem leistungsschwachen Produkte in den meisten Fällen nicht von Firmen stammen, die sich auf kryptographische Technologie spezialisiert haben.

Selbst die wirklich guten Software-Pakete, die DES in den korrekten Betriebsmodi verwenden, weisen noch Probleme auf. Der Standard-DES-Modus verwendet einen 56-Bit-Schlüssel, der nach heutigen Standards zu klein ist und auf dem gegenwärtigen Stand der Technik durch umfangreiche Schlüssel-Suchfunktionen auf speziellen, extrem leistungsfähigen Rechnern leicht aufgebrochen werden kann. Der DES-Algorithmus hat seinen Zweck erfüllt und sollte nun in Rente gehen, ebenso wie die Software-Pakete, die auf diesem Algorithmus aufbauen.

Der Hersteller AccessData (http://www.accessdata.com) bietet ein kostengünstiges Software-Paket an, durch das die in WordPerfect, Lotus 1-2-3, MS Excel, Symphony, Quattro Pro, Paradox, MS Word und PKZIP verwendeten integrierten Verschlüsselungssysteme aufgebrochen werden. Es errät nicht nur einfach Paßwörter – es bedient sich richtiger Kryptoanalyse. Manche Personen kaufen es, weil sie das Paßwort für ihre eigenen Dateien vergessen haben. Strafrechtliche Behörden nutzen diese Programme ebenfalls, um die von ihnen beschlagnahmten Dateien lesen zu können. Der Entwickler des Programms, Eric Thompson, erzählte mir, daß sein Programm zum Entschlüsseln lediglich den Bruchteil einer Sekunde benötigt, doch daß er einige Verzögerungsschleifen eingebaut habe, um den Decodierungsprozeß zu verlangsamen, so daß dieser für den Kunden nicht zu einfach erscheint.

Im Bereich abhörsicherer Telefonanlagen sind Ihre Auswahlmöglichkeiten beschränkt. Das meistverkaufte System ist die STU-III (Secure Telephone Unit), hergestellt von Motorola und AT&T für einen Preis zwischen 2.000 und 3.000 US-Dollar und von der Regierung für Geheimhaltungszwecke verwendet. Es verwendet leistungsfähige Kryptographie. Zum Kauf dieser leistungsfähigen Version benötigt man jedoch eine spezielle Lizenz von der Regierung. Auf dem Markt ist eine Version von STU-III erhältlich, die entsprechend den Wünschen des NSA abgeschwächt wurde. Darüber hinaus gibt es eine Exportversion, die noch wesentlich stärker abgeschwächt wurde. Außerdem gibt es das System Surity 3600 von AT&T für 1.200 US-Dollar, das den berühmten Clipper-Chip der Regierung zur Verschlüsselung verwendet, mit bei der Regierung hinterlegten Schlüsseln, um Abhöraktionen zu erleichtern. Darüber hinaus gibt es natürlich noch die analogen (nicht digitalen) Sprachverwürfler, die Sie über Kataloge für Möchtegernspione bestellen können und die im Sinne der Kryptographie absolut nutzlos sind. Sie werden jedoch als „sichere“ Kommunikationsprodukte an Kunden verkauft, die sich in der Materie nicht auskennen.

Auf eine gewisse Art ist Kryptographie mit Medikamenten zu vergleichen. Die richtige Qualität und Zusammensetzung kann von größter Bedeutung sein. Penicillin schlechter Qualität sieht genauso aus wie Penicillin guter Qualität. Sie können feststellen, ob Ihr Tabellenkalkulationsprogramm funktioniert, aber wie stellen Sie fest, ob das Kryptographieprogramm leistungsschwach ist? Von einem schwachen Verschlüsselungsalgorithmus erzeugter chiffrierter Text sieht genauso überzeugend aus wie von einem effizienten Verschlüsselungsalgorithmus erzeugter chiffrierter Text. Es gibt viel unwirksame Medizin auf dem Markt. Und es gibt viele Kurpfuscher. Doch im Gegensatz zu den Wunderdoktoren von früher wissen die Software-Entwickler von heute oft noch nicht einmal, daß ihr Produkt wirkungslos ist.
Sie mögen gute Software-Ingenieure sein, doch sie haben im Regelfall nicht eine einzige wissenschaftliche Veröffentlichung über Kryptographie gelesen. Sie sind jedoch der Meinung, daß sie ein gutes kryptographisches Programm schreiben können. Und warum auch nicht? Schließlich scheint es vom Gefühl her so einfach zu sein. Und ihre Programme scheinen gut zu funktionieren.

Jeder, der der Meinung ist, ein nicht zu entschlüsselndes Verschlüsselungssystem entwickelt zu haben, ist entweder ein unglaublich begnadetes Genie oder naiv und unerfahren. Unglücklicherweise habe ich es manchmal mit Möchtegernkryptologen zu tun, die „Verbesserungen“ an PGP durch Hinzufügen von selbstentwickelten Verschlüsselungsalgorithmen durchführen möchten.

Ich erinnere mich an ein Gespräch mit Brian Snow, einem angesehenen NSA-Kryptologen. Er sagte mir, er würde keinem Verschlüsselungsalgorithmus vertrauen, dessen Entwickler sein Metier nicht „von der Pike auf“ durch intensive Beschäftigung mit dem Entschlüsseln von Codes erlernt hätte.
Das hörte sich sehr vernünftig an. Ich stellte fest, daß so gut wie kein beruflicher Kryptograph dieses Kriterium erfüllte. „Stimmt,“ sagte er mit einem selbstbewußten Lächeln, „und das macht die Arbeit für den NSA um einiges einfacher.“ Ein beängstigender Gedanke. Auch ich erfüllte dieses Kriterium nicht.

Und auch die Regierung hat unwirksame Medizin verbreitet. Nach dem Zweiten Weltkrieg verkauften die USA deutsche Enigma-Chiffriergeräte an Regierungen der Dritten Welt. Sie sagten ihnen jedoch nicht, daß die Alliierten den Enigma-Code schon während des Krieges entschlüsselt hatten. Diese Tatsache wurde jahrelang geheimgehalten. Selbst heute wird weltweit in vielen UNIX-Systemen noch die Enigma-Chiffriercodes zur Verschlüsselung von Dateien verwendet, was teilweise darin begründet ist, daß die Regierung der Verwendung von besseren Algorithmen durch Gesetze Steine in den Weg gelegt hat. Sie versuchte sogar, die erstmalige Veröffentlichung des RSA-Algorithmus im Jahre 1977 zu verhindern. Außerdem bekämpft die Regierung seit Jahren rigoros alle Anstrengungen von seiten der Wirtschaft, sichere Telefone für die breite Öffentlichkeit zu entwickeln.

Die wichtigste Aufgabe des Nationalen Sicherheitsdienstes der amerikanischen Regierung besteht im Sammeln von Informationen, in erster Linie durch verdecktes Abhören von Privatgesprächen (Buchtip: *The Puzzle Palace* von James Bamford). Der NSA hat erhebliche Fähigkeiten und Ressourcen zum Entschlüsseln von Codes aufgebaut. Wenn die Bevölkerung keine Möglichkeit hat, ihre Privatsphäre durch Anwendung effektiver kryptographischer Methoden zu schützen, wird dem NSA die Arbeit um einiges leichter gemacht. Der NSA hat auch das Recht, Verschlüsselungsalgorithmen zu bewilligen und zu empfehlen. Manche Kritiker führen an, daß hier ein Interessenkonflikt vorliegt, so als würde man „den Bock zum Gärtner machen“. In den 80er Jahren unterstützte der NSA intensiv einen konventionellen Verschlüsselungsalgorithmus, der von ihm selbst entwickelt wurde (das COMSEC-Programm) – über die Funktionsweise konnte jedoch keine Auskunft gegeben werden, da diese der Geheimhaltung unterlag. Der NSA wollte erreichen, daß andere dem Algorithmus vertrauen und ihn verwenden. Aber jeder Kryptologe kann Ihnen sagen, daß ein gut entwickelter Verschlüsselungsalgorithmus nicht geheimgehalten werden muß, um sicher zu bleiben. Es müssen lediglich die Schlüssel geschützt werden. Wie kann irgend jemand wirklich wissen, ob der von der NSA geheimgehaltene Algorithmus sicher ist? Es ist nicht schwer für den NSA, einen Verschlüsselungsalgorithmus zu entwickeln, der nur von ihm entschlüsselt werden kann, wenn niemand sonst den Algorithmus überprüfen kann.

Es gibt drei Hauptfaktoren, die die Qualität von kommerziellen kryptographischen Programmen in den USA unterminiert haben:

- Der erste Faktor ist das praktisch allgegenwärtige Kompetenzdefizit bei Programmierern kommerzieller Verschlüsselungsprogramme (obwohl sich dies seit der Veröffentlichung von PGP allmählich ändert). Jeder Software-Ingenieur hält sich für einen Kryptologen, was zu einer enormen Verbreitung von äußerst schlechter Verschlüsselungssoftware geführt hat.
- Der zweite Faktor ist, daß der NSA absichtlich und systematisch alle guten kommerziellen Verschlüsselungstechnologien durch Einschüchterungsmaßnahmen und wirtschaftlichen Druck unterdrückt. Eine Methode sind u. a. strikte Exportkontrollen für Verschlüsselungsprogramme, was aufgrund der wirtschaftlichen Gesetzmäßigkeiten im Software-Marketing dazu führt, daß amerikanische Verschlüsselungsprogramme im internationalen Wettbewerb direkt benachteiligt werden.
- Die dritte der drei wichtigsten Unterdrückungsmethoden besteht darin, daß alle Softwarepatente für alle auf öffentlichen Schlüsseln basierenden Verschlüsselungsalgorithmen an eine einzige Firma vergeben wurden, wodurch ein Hindernis geschaffen wurde, durch das die Verbreitung dieser Technologie weiter unterdrückt wurde (obwohl dieses Kartell für kryptographische Patente im Herbst 1995 zusammenbrach).

Die eindeutige Konsequenz all dieser Faktoren war, daß vor der Veröffentlichung von PGP in den USA kaum ein Verschlüsselungsprogramm erhältlich war, das höchsten Sicherheitsanforderungen entsprach und vielseitig einsetzbar war.

Ich bin nicht so überzeugt von der Sicherheit von PGP, wie ich als Student von der Genialität meines Verschlüsselungsprogramms überzeugt war. Wenn ich so sicher wäre, wäre das ein schlechtes Zeichen. Aber ich glaube nicht, daß PGP eklatante Schwächen aufweist (obwohl ich ziemlich sicher bin, daß es Fehler enthält). Ich habe die besten Algorithmen aus der kryptographischen Standardliteratur ausgewählt. Die meisten dieser Algorithmen wurden von Experten genauestens überprüft. Ich kenne viele der weltweit führenden Kryptologen und habe mit einigen von ihnen eine Vielzahl der in PGP verwendeten kryptographischen Algorithmen und Protokolle besprochen. Das Programm ist ausgiebig erforscht und geprüft worden und wurde nach jahrelanger Arbeit fertiggestellt. Und ich arbeite nicht für den NSA. Aber Sie müssen sich bezüglich der kryptographischen Verläßlichkeit von PGP nicht bloß auf mein Wort verlassen, da der Quellcode zum Überprüfen meiner Aussage zur Verfügung steht.

Noch eine letzte Aussage zu meiner Bemühung um kryptographische Qualität in PGP: Seit der Entwicklung und Freigabe der ersten PGP-Version im Jahr 1991 wurde drei Jahre lang vom amerikanischen Zoll wegen der Verbreitung von PGP außerhalb der USA strafrechtlich gegen mich ermittelt. Es bestand die Gefahr einer strafrechtlichen Verfolgung und jahrelanger Gefängnisstrafe. Die Regierung zeigte übrigens bei keinem anderen kryptographischen Programm irgendwelche Zeichen von Aufregung. Erst PGP löste Alarm aus. Was sagt Ihnen dies bezüglich der Qualität von PGP? Mein Ruf beruht auf der kryptographischen Qualität meiner Produkte. Ich werde meinen Einsatz für unser Recht auf Privatsphäre, für das ich meine Freiheit aufs Spiel gesetzt habe, nicht verraten. Ich werde kein Produkt zulassen, das meinen Namen trägt und über geheime Hintertüren verfügt.

Sicherheitsrisiken

„Wenn alle PCs weltweit – d. h. 260 Millionen Computer – an einer einzigen von PGP verschlüsselten Nachricht arbeiten würden, würde es im Schnitt immer noch ungefähr 12 Millionen mal das Alter des Universums dauern, bis eine einzige Nachricht decodiert werden könnte.“

– William Crowell, Stellvertretender Direktor des Nationalen Sicherheitsdienstes der USA (NSA), 20. März 1997.

Es gibt kein Datensicherheitssystem, das absolut sicher ist. PGP kann auf verschiedene Weise umgangen werden. In allen Datensicherheitssystemen müssen Sie sich selbst die Frage stellen, ob der Wert der Daten, die Sie zu schützen versuchen, für den Hacker höher einzustufen ist als die Kosten für den Angriff. Sie sollten sich also vor Angriffen schützen, die geringen Aufwand erfordern, und sich keine Sorgen über aufwendige Angriffe machen. Einige der im folgenden beschriebenen Szenarios erscheinen vielleicht übermäßig paranoid, doch ein solcher Ansatz ist geeignet, um eine vernünftige Diskussion über Sicherheitsrisiken zu führen.

Kompromittierte Paßphrasen oder private Schlüssel

Der wahrscheinlich einfachste Angriff ist möglich, wenn Sie die Paßphrase für Ihren privaten Schlüssel aufschreiben. Wenn jemand die Paßphrase herausfindet und zudem Zugriff auf Ihre private Schlüsseldatei erhält, kann er Ihre Nachrichten lesen und Nachrichten und Dateien in Ihrem Namen unterschreiben.

Im folgenden finden Sie einige Empfehlungen zum Schutz Ihrer Paßphrase:

1. Verwenden Sie keine Paßphrasen, die leicht erraten werden können, wie beispielsweise den Namen Ihrer Kinder oder Ihres Partners.

2. Verwenden Sie Leerzeichen und eine Kombination aus Zahlen und Buchstaben in Ihrer Paßphrase. Wenn Sie ein einziges Wort für Ihre Paßphrase verwenden, kann es von einem Computer leicht durch Ausprobieren aller Wörter im Wörterbuch gefunden werden. Deshalb ist eine Paßphrase wesentlich besser als ein Paßwort. Ein raffinierterer Hacker könnte allerdings auch ein Buch mit berühmten Zitaten in seinen Computer einscannen, um Ihre Paßphrase zu finden.

3. Seien Sie kreativ. Verwenden Sie eine leicht zu merkende, aber schwer zu erratende Paßphrase. Sie können schnell selbst eine Paßphrase erfinden, indem Sie kreativ unsinnige Redewendungen oder unbekannte oder leicht veränderte literarische Zitate verwenden.

Verfälschter öffentlicher Schlüssel

Eines der größten Sicherheitsrisiken besteht, wenn öffentliche Schlüssel verfälscht werden. Dies ist möglicherweise das größte Sicherheitsrisiko in einem Kryptosystem mit öffentlichen Schlüsseln, zum Teil deshalb, weil die meisten Neueinsteiger es nicht direkt erkennen.

Noch einmal zusammengefaßt: Vergewissern Sie sich, wenn Sie den öffentlichen Schlüssel von einer anderen Person verwenden, daß dieser Schlüssel nicht verfälscht wurde. Sie sollten einem neuen öffentlichen Schlüssel einer anderen Person nur trauen, wenn Sie ihn direkt von seinem Eigentümer erhalten haben oder wenn er von jemandem unterschrieben wurde, dem Sie vertrauen. Stellen Sie sicher, daß keine andere Person die Möglichkeit hat, Ihren eigenen öffentlichen Schlüsselbund zu verfälschen.
Stellen Sie sicher, daß Sie die physische Kontrolle über Ihren öffentlichen Schlüsselbund und Ihren privaten Schlüssel haben. Ihr Schlüsselpaar sollte sich vorzugsweise auf Ihrem eigenen PC und nicht auf einem entfernten Mehrbenutzersystem befinden. Behalten Sie eine Sicherungskopie von beiden Schlüsselbunden.

Nicht vollständig gelöschte Dateien

Ein weiteres potentielles Sicherheitsproblem wird durch die Art und Weise verursacht, mit der in den meisten Betriebssystemen das Löschen von Dateien gehandhabt wird. Wenn Sie eine Datei verschlüsseln und dann die ursprüngliche Klartextdatei löschen, werden die Daten durch das Betriebssystem nicht wirklich physisch gelöscht. Es markiert die Datenblöcke auf der Festplatte lediglich als gelöscht, um so zu kennzeichnen, daß der Speicherplatz später wieder verwendet werden kann. Das ist so, als ob man vertrauliche Papierdokumente ins Altpapier und nicht in den Papier-Shredder geben würde. Die Datenblöcke auf der Festplatte enthalten immer noch die ursprünglichen, vertraulichen Daten, die Sie löschen wollten, und werden wahrscheinlich später einmal durch neue Daten überschrieben. Wenn ein Hacker diese gelöschten Datenblöcke von Ihrer Festplatte kurz nach der Zuordnungsaufhebung einliest, könnte er Ihren Klartext wiederherstellen.

Dies könnte sogar versehentlich geschehen, falls ein Problem mit der Festplatte besteht und Dateien unabsichtlich gelöscht oder beschädigt wurden. Ein Wiederherstellungsprogramm für die Festplatte kann zur Wiederherstellung der beschädigten Dateien verwendet werden. Das hat jedoch oft zur Folge, daß vorher gelöschte Dateien zusammen mit allen anderen Daten wiederhergestellt werden. Ihre vertraulichen Dateien, die Sie nie mehr wiederzusehen glaubten, könnten dann wieder auftauchen und von der Person, die versucht, Ihre beschädigte Festplatte wiederherzustellen, eingesehen werden. Auch während Sie die ursprüngliche Nachricht mit einem Textverarbeitungsprogramm oder einem Texteditor erstellen, können, bedingt durch die interne Arbeitsweise dieser Programme, möglicherweise mehrere temporäre Kopien Ihres Textes auf der Festplatte erstellt werden. Diese temporären Kopien Ihres Textes werden vom Textverarbeitungsprogramm nach der Fertigstellung gelöscht, doch die heiklen Daten befinden sich als Fragmente immer noch irgendwo auf Ihrer Festplatte.

Die einzige Möglichkeit, die Wiederherstellung des Klartextes unmöglich zu machen, besteht darin, die gelöschten Klartextdateien auf irgendeine Art zu überschreiben. Wenn Sie nicht sicher sind, ob die gelöschten Datenblöcke auf der Festplatte bald überschrieben werden, müssen Sie absolut sicherstellen, daß die Klartextdatei sowie alle Dateifragmente, die möglicherweise vom Textverarbeitungsprogramm auf der Festplatte zurückgelassen wurden, überschrieben werden. Sie können alle auf der Festplatte verbliebenen Klartextfragmente überschreiben. Verwenden Sie dazu PGP Secure Wipe oder PGP Freespace Wipe.

Viren und Trojanische Pferde

Ein Angriff könnte auch durch einen speziell entwickelten, feindlichen Computer-Virus oder „-Wurm“ erfolgen, der PGP oder Ihr Betriebssystem infizieren könnte. Dieser hypothetische Virus könnte so programmiert sein, daß er Ihre Paßphrase, Ihren privaten Schlüssel oder dechiffrierte Nachrichten erfaßt und die erfaßten Daten in eine Datei schreibt oder über ein Netzwerk an den Eigentümer des Virus schickt. Der Virus könnte möglicherweise auch die Funktionsweise von PGP verändern, so daß Unterschriften nicht mehr richtig überprüft werden. Dieser Angriff ist kostengünstiger als ein kryptoanalytischer Angriff.

Der Schutz vor dieser Art von Angriffen fällt in den Bereich des allgemeinen Schutzes vor Virusinfektionen. Es werden einige relativ brauchbare Antivirenprodukte auf dem Markt angeboten, und es gibt einige „Hygienemaßnahmen“, mit denen die Gefahr einer Virusinfektion in hohem Maße verringert werden kann. Eine vollständige Darstellung möglicher Maßnahmen gegen Viren und Würmer geht über den Rahmen dieses Dokuments hinaus.
PGP verfügt über keine Verteidigungsmechanismen gegen Viren und geht davon aus, daß Ihr PC eine sichere Umgebung für die Ausführung des Programms darstellt. Falls tatsächlich ein Virus oder Wurm der oben beschriebenen Art auftreten sollte, würde sich das hoffentlich bald herumsprechen, so daß alle betroffenen Personen gewarnt würden.

Ein ähnlicher Angriff könnte durch eine geschickt gestaltete Imitation von PGP erfolgen, die sich zwar weitgehend wie PGP verhält, jedoch nicht in der vorgesehenen Art funktioniert. Das Programm könnte beispielsweise absichtlich deformiert worden sein, so daß Unterschriften nicht mehr korrekt überprüft werden, wodurch gefälschte Schlüsselzertifikate akzeptiert würden. Diese PGP-Version, deren Wirkungsweise mit einem *Trojanischen Pferd* vergleichbar ist, kann leicht erstellt werden, da der PGP-Quellcode überall verfügbar ist, so daß jeder den Quellcode verändern und somit ein PGP-Imitat erstellen kann, das zwar echt aussieht, in Wahrheit aber eine Fälschung ist. Diese „Trojanische“ PGP-Version könnte dann in Umlauf gebracht werden, da an der Echtheit keine Zweifel bestehen. Wie heimtückisch.

Sie sollten sich daher bemühen, Ihre PGP-Kopie direkt von Network Associates, Inc., zu erwerben.

Sie können auch mit Hilfe von digitalen Unterschriften überprüfen, ob PGP verfälscht worden ist. Sie könnten beispielsweise eine andere PGP-Version, der Sie vertrauen, zum Überprüfen der Unterschrift einer verdächtigen PGP-Version verwenden. Allerdings ist dies nicht von Nutzen, wenn Ihr Betriebssystem infiziert ist, und es kann dadurch auch nicht festgestellt werden, ob die ursprüngliche Kopie der Datei PGP.EXE absichtlich so verändert wurde, daß die Funktion des Programms zur Überprüfung von Unterschriften beschädigt wurde. Dieser Test geht außerdem von der Voraussetzung aus, daß Sie über eine gute, vertrauenswürdige Kopie des öffentlichen Schlüssels verfügen, mit dem die Unterschrift der verdächtigen ausführbaren PGP-Datei überprüft wird.

Auslagerungsdateien und virtueller Speicher

PGP wurde ursprünglich für MS-DOS entwickelt, ein nach heutigen Standards einfaches Betriebssystem. Als es auf andere, komplexere Betriebssysteme, wie Microsoft Windows oder Macintosh OS portiert wurde, brachte dies ein neues Sicherheitsrisiko mit sich. Dieses Risiko liegt in der Tatsache begründet, daß diese neuen, aufwendigeren Betriebssysteme über einen sogenannten *virtuellen Speicher* verfügen.

Aufgrund des virtuellen Speichers können auf dem Computer riesige Programme ausgeführt werden, deren Größe den Speicherplatz überschreiten, der auf den Halbleiterspeicherchips des Computers zur Verfügung steht. Dies ist sehr nützlich, da Software mehr und mehr „aufgeblasen“ wurde, seit grafische Benutzeroberflächen zur Norm wurden und Benutzer anfingen, mehrere große Anwendungen zur gleichen Zeit auszuführen. Das Betriebssystem verwendet die Festplatte zur Zwischenspeicherung von Softwareteilen, die zur Zeit nicht benötigt werden. Dies hat zur Folge, daß das Betriebssystem möglicherweise ohne Ihr Wissen Daten auf die Festplatte schreibt, die sich Ihrer Meinung nach nur im Hauptspeicher befinden, wie beispielsweise Schlüssel, Paßphrasen oder dechiffrierten Klartext. PGP bewahrt wichtige und vertrauliche Daten dieser Art nicht länger als nötig im Speicher auf, möglicherweise schreibt das Betriebssystem die Daten aber trotzdem auf die Festplatte.

Die Daten werden in einen Notizblockbereich auf der Festplatte geschrieben, der auch als *Auslagerungsdatei* bekannt ist. Wieder benötigte Daten werden wieder aus der Auslagerungsdatei eingelesen, so daß sich jeweils nur ein Teil des Programms oder der Daten im physischen Speicher befindet. All diese Vorgänge sind für den Benutzer nicht sichtbar, er registriert lediglich, daß die Festplatte arbeitet. Microsoft Windows lagert Teile des Speichers, sogenannte *Seiten*, mit Hilfe eines LRU-Seitenersetzungsalgorithmus (LRU = Least Recently Used) ein und aus. Dies bedeutet, daß die Seiten, die den längsten Zeitraum über nicht mehr verwendet wurden, zuerst auf die Festplatte ausgelagert werden. Dieser Ansatz läßt vermuten, daß in den meisten Fällen das Risiko einer Auslagerung vertraulicher Daten auf Festplatte relativ gering ist, da PGP diese Daten nur für kurze Zeit im Speicher aufbewahrt. Eine Garantie wird von uns allerdings nicht gegeben.

Jede Person, die physischen Zugriff auf Ihren Computer hat, kann auf die Auslagerungsdatei zugreifen. Wenn Sie gegen dieses Problem etwas unternehmen möchten, können Sie beispielsweise spezielle Software zum Überschreiben der Auslagerungsdatei erwerben. Eine andere Möglichkeit besteht in der Deaktivierung der Funktion des virtuellen Speichers in Ihrem Betriebssystem. Unter Microsoft Windows ist dies ebenso möglich wie unter Mac OS.
Die Deaktivierung des virtuellen Speichers kann zur Folge haben, daß Sie mehr physische RAM-Chips installieren müssen, um alle Daten im RAM speichern zu können.

Physischer Eingriff in die Privatsphäre

Durch einen physischen Eingriff in Ihre Privatsphäre kann eine Person in den physischen Besitz Ihrer Klartextdateien oder ausgedruckter Nachrichten kommen. Ein entschlossener Gegner kann dies beispielsweise durch Einbruch, Durchsuchen des Abfalls, widerrechtliche Durchsuchung oder Beschlagnahme, Bestechung, Erpressung oder Einschleusen eines Mitarbeiters in Ihre Organisation erreichen. Manche dieser Angriffe können insbesondere bei politischen Basisorganisationen leicht durchzuführen sein, die mit einer Vielzahl freiwilliger Mitarbeiter arbeiten.

Verlieren Sie nicht durch ein falsches Sicherheitsgefühl Ihre Wachsamkeit, weil Sie über ein kryptograpisches Werkzeug verfügen. Kryptographische Techniken schützen Daten nur, während sie verschlüsselt sind. Direkte physische Sicherheitsverletzungen können weiterhin Klartextdaten oder schriftliche oder mündliche Informationen gefährden.

Diese Angriffe sind unaufwendiger als kryptoanalytische Angriffe auf PGP.

Tempest-Angriffe

Eine andere Angriffsform, die von Gegnern mit einer sehr guten Ausrüstung verwendet werden kann, besteht im Aufzeichnen der durch Ihren Computer ausgegebenen elektromagnetischen Signale von einer entfernten Stelle aus. Dieser kosten- und relativ arbeitsintensive Angriff ist wahrscheinlich immer noch weniger aufwendig als ein direkter kryptoanalytischer Angriff. Ein für diesen Zweck ausgestattetes Fahrzeug, z. B. ein Lieferwagen, kann in der Nähe Ihres Büros geparkt werden und von dort aus all Ihre Tastenbetätigungen verfolgen und die auf Ihrem Computerbildschirm angezeigten Nachrichten aufzeichnen. Dadurch würden Ihre Paßwörter, Nachrichten usw. gefährdet. Diese Art von Angriff kann abgewehrt werden, indem Sie Ihre Computer-Ausrüstung und Ihre Netzwerkverkabelung mit einem Schutz versehen, so daß keine elektromagnetischen Signale mehr nach außen dringen können. Diese Schutztechnologie ist als „Tempest“ bekannt und wird von Regierungsdiensten und im Bereich der Verteidigung tätigen Unternehmen verwendet. Es gibt Hardware-Vertreiber, die den Tempest-Schutz auch kommerziell anbieten.

Manche neuere Versionen von PGP (Version 6.0 oder höher) können entschlüsselten Klartext mit Hilfe einer speziell für diesen Zweck entwickelten Schriftart anzeigen, die eine geringere Strahlung des Bildschirms verursachen sollen. Hierdurch könnte es schwieriger werden, die verbleibende Strahlung aufzufangen und Inhalte abzulesen. Diese spezielle Schriftart ist in manchen PGP-Versionen verfügbar, die die Funktion „Sichere Darstellung“ unterstützen.

Schutz vor gefälschten Zeitmarkierungen

Ein unwahrscheinlicheres Sicherheitsrisiko von PGP ist die Möglichkeit, daß unehrliche Benutzer die Zertifikate für ihre eigenen öffentlichen Schlüssel und Unterschriften mit falschen Zeitmarkierungen versehen. Sie können diesen Abschnitt überspringen, wenn Sie PGP nur gelegentlich verwenden und sich nicht ausführlich mit den weniger wichtigen Aspekten des Umgangs mit öffentlichen Schlüssel-Protokollen befassen möchten.

Ein unehrlicher Benutzer kann ohne Probleme die Datums- und Zeiteinstellung seines eigenen Systems ändern und so eigene Zertifikate für öffentliche Schlüssel sowie Unterschriften erzeugen, die den Anschein erwecken, sie seien zu einem anderen Zeitpunkt erstellt worden. Er kann es so aussehen lassen, daß er etwas früher oder später unterschrieben hat, als es in Wirklichkeit der Fall war, oder daß sein Schlüsselpaar aus öffentlichem und privatem Schlüssel zu einem früheren oder späteren Zeitpunkt erstellt wurde.
Dies kann für ihn mit einem rechtlichen oder finanziellen Vorteil verbunden sein, wenn er sich dadurch beispielsweise eine Möglichkeit schafft, seine eigene Unterschrift abzustreiten.

Meiner Meinung nach ist dieses Problem der gefälschten Zeitmarkierungen bei digitalen Unterschriften nicht gravierender, als es auch bei handschriftlichen Unterschriften ist. Jeder kann ein beliebiges Datum neben seine handschriftliche Unterschrift auf einen Vertrag schreiben, doch niemand zeigt sich aufgrund dieses Zustandes alarmiert. In manchen Fällen hat ein „inkorrektes" Datum im Zusammenhang mit einer handschriftlichen Unterschrift vielleicht gar nichts mit einem tatsächlichen Betrug zu tun. Die Zeitangabe kann der Zeitpunkt sein, an dem der Unterschreibende bestätigt, daß er ein Dokument unterschrieben hat, oder vielleicht der Zeitpunkt, zu dem die Unterschrift wirksam werden soll.

In Situationen, in denen das richtige Datum einer Unterschrift von größter Wichtigkeit ist, kann einfach ein Notar herangezogen werden, um die handschriftliche Unterschrift zu bezeugen und zu datieren. Genauso kann bei digitalen Unterschriften ein vertrauenswürdiger Dritter herangezogen werden, wenn ein Unterschriftszertifikat in Verbindung mit einer zuverlässigen Zeitmarkierung unterschrieben werden soll. Dazu sind keine exotischen oder übermäßig formalen Protokolle notwendig. Unter Zeugen ausgeführte Unterschriften sind schon lange als eine rechtmäßige Form anerkannt, um den Zeitpunkt zu bestimmen, an dem ein Dokument unterschrieben wurde.

Eine vertrauenswürdige Zertifizierungsinstanz oder ein Notar könnte notariell beglaubigte Unterschriften mit einer zuverlässigen Zeitmarkierung versehen. Dazu wäre nicht notwendigerweise eine zentralisierte Autorität erforderlich. Gegebenenfalls könnten beliebige vertrauenswürdige Verwalter oder nicht betroffene Parteien diese Funktion übernehmen, in der gleichen Form, wie dies auch bei zur Beglaubigung von Dokumenten berechtigten öffentlichen Stellen der Fall ist. Wenn ein Notar Unterschriften anderer Personen unterschreibt, wird ein Unterschriftszertifikat von einem Unterschriftszertifikat erstellt. Dies würde die Unterschrift auf die gleiche Weise bezeugen, wie es bei der Bezeugung einer handschriftlichen Unterschrift durch einen vereidigten Notar der Fall ist. Der Notar könnte das Unterschriftszertifikat separat (ohne das eigentliche Dokument, das unterschrieben wurde) in eine spezielle, vom Notar kontrollierte Protokolldatei einfügen. Diese Protokolldatei könnte von jedermann eingesehen werden. Die Unterschrift des Notars würde über eine zuverlässige Zeitmarkierung verfügen, die möglicherweise eine größere Glaubwürdigkeit oder eine größere rechtliche Bedeutung hat als die Zeitmarkierung in der ursprünglichen Unterschrift.

Eine gute Abhandlung zu diesem Thema finden Sie in einem Artikel von Denning, der 1983 in „IEEE Computer" veröffentlicht wurde. Zukünftige Erweiterungen von PGP werden möglicherweise über Funktionen verfügen, mit denen notariell beglaubigte Unterschriften für andere Unterschriften in Verbindung mit zuverlässigen Zeitmarkierungen auf einfache Weise verwaltet werden können.

Datengefährdung in Mehrbenutzersystemen

PGP wurde ursprünglich für Einzelbenutzer-PCs entwickelt, auf die der Eigentümer direkt zugreifen kann. Wenn Sie PGP zu Hause auf Ihrem eigenen PC ausführen, sind Ihre verschlüsselten Dateien relativ sicher, es sei denn, jemand bricht in Ihr Haus ein, stiehlt Ihren PC und bringt Sie dazu, Ihre Paßphrase preiszugeben (falls Ihre Paßphrase nicht sehr leicht erraten werden kann).

PGP ist nicht darauf ausgerichtet, Daten zu schützen, die sich in Klartextform auf einem nicht abgesicherten System befinden. PGP kann auch nicht verhindern, daß ein Eindringling ausgeklügelte Methoden verwendet, um Ihren privaten Schlüssel zu lesen, während er verwendet wird. Sie müssen diese Risiken auf einem Mehrbenutzersystem berücksichtigen und Ihre Erwartungen und Ihr Verhalten dementsprechend anpassen. Möglicherweise empfiehlt es sich in Ihrer Situation, PGP nur auf einem isolierten Einzelbenutzersystem zu verwenden, auf das Sie direkt zugreifen können.

Datenverkehrsanalyse

Selbst wenn der Hacker den Inhalt Ihrer verschlüsselten Nachrichten nicht entziffern kann, kann er möglicherweise zumindest einige nützliche Informationen aus Beobachtungen bezüglich der Herkunft und des Ziels der Nachrichten, ihrer Größe sowie der Tageszeit ziehen, zu der sie versendet wurden. Dies ist vergleichbar mit Informationen, die ein Hacker durch Untersuchung Ihrer detaillierten Telefonrechnung erhalten würde, um zu erfahren, mit wem Sie zu welchem Zeitpunkt wie lange telefoniert haben. Diese Informationen sind dem Hacker zugänglich, obwohl er den tatsächlichen Inhalt der Gespräche nicht kennt. Dies wird Datenverkehrsanalyse genannt. PGP allein schützt nicht gegen Datenverkehrsanalyse. Die Lösung dieses Problems würde spezielle Kommunikationsprotokolle erforderlich machen, die speziell darauf ausgerichtet sind, das Ableiten von Informationen aus Ihrem Kommunikationssystem durch Datenverkehrsanalysen zu verringern, möglicherweise mit Hilfe von Kryptographie.

Kryptoanalyse

Ein aufwendiger und gefährlicher kryptoanalytischer Angriff könnte von einer Person oder Institution durchgeführt werden, der überdurchschnittliche Computer-Ressourcen zur Verfügung stehen, wie beispielsweise dem Geheimdienst einer Regierung. Dadurch könnte Ihr öffentlicher Schlüssel unter Verwendung einer neuen mathematischen Geheimmethode entschlüsselt werden. Die nichtmilitärische akademische Welt hat jedoch die Kryptographie mit öffentlichen Schlüsseln seit 1978 erfolglos attackiert.

Möglicherweise verfügt die Regierung über bestimmte Methoden zur Entschlüsselung der in PGP verwendeten konventionellen Verschlüsselungsalgorithmen. Dies ist der Alptraum eines jeden Kryptologen. In praktischen kryptographischen Anwendungen kann es keine absoluten Sicherheitsgarantien geben.

Ein gewisser Grad an Optimismus ist dennoch gerechtfertigt. Die in PGP verwendeten Algorithmen für öffentliche Schlüssel, Nachrichtenkernalgorithmen und Blockchiffrierer wurden von weltweit führenden Kryptographen entwickelt. Sie wurden von den besten Kryptoanalytikern umfangreichen Sicherheitsanalysen und Überprüfungen unterzogen.

Auch wenn die in PGP verwendeten Blockchiffrierer über leichte, nicht bekannte Schwächen verfügen sollten, werden diese Schwächen in hohem Maße dadurch reduziert, daß PGP den Klartext vor der Verschlüsselung komprimiert. Die rechnerische Arbeitsleistung, die zum Aufbrechen erforderlich wäre, wäre wahrscheinlich um ein Vielfaches umfangreicher, als es der Wert der Nachricht rechtfertigen würde.

Falls Sie Grund zu der Annahme haben, daß ernstzunehmende Angriffe dieser Größenordnung auf Ihre Daten vorgenommen werden könnten, sollten Sie möglicherweise einen Datensicherheitsberater zu Rate ziehen, der Ihnen an bestimmte Gegebenheiten angepaßte Sicherheitskonzepte vorstellen kann, die auf Ihre individuellen Bedürfnisse zugeschnitten sind.

Zusammenfassend ist festzuhalten, daß ohne effektiven kryptographischen Schutz ein Gegner keinerlei Mühe aufwenden muß, um Ihre Nachrichten abzuhören, und dies vielleicht sogar gewohnheitsmäßig tut, insbesondere, wenn diese Daten über eine Modemverbindung oder über ein E-Mail-System gesendet werden. Wenn Sie jedoch PGP verwenden und entsprechende Vorsichtsmaßnahmen befolgen, muß der Hacker weit mehr Mühe und Kosten aufwenden, um in Ihre Privatsphäre einzudringen.

Wenn Sie sich gegen sämtliche Angriffe auf Ihre Privatsphäre schützen möchten und sicherstellen möchten, daß keine über überdurchschnittliche Ressourcen verfügenden Personen in Ihre Privatsphäre eindringen können, sind Sie mit PGP hervorragend beraten. PGP schützt Ihre Privatsphäre ausgesprochen gut, daher auch der Name „Pretty Good Privacy“.

Liste biometrischer Worte

Von Philip Zimmermann und Patrick Juola

Die authentisierte Übertragung binärer Informationen erfolgt in PGP anhand einer speziellen Wortliste über einen Sprechkanal, beispielsweise ein Telefon, und zwar unter Verwendung biometrischer Unterschriften. Vorausgesetzt, der jeweilige Zuhörer versteht sie, dienen die durch die menschliche Stimme gesprochenen Worte der biometrischen Authentisierung der Daten, die in gesprochener Form übermittelt werden. Die Wortliste hat denselben Zweck wie das Militäralphabet, das zur Übertragung von Buchstaben über einen verrauschten Funksprechkanal verwendet wird. Das Militäralphabet umfaßt jedoch 26 Worte, wobei jedes Wort für einen Buchstaben steht. Für unsere Zwecke enthält unsere Liste 256 sorgfältig ausgewählte, phonetisch eindeutige Worte, die für die 256 möglichen Byte-Werte von 0 bis 255 stehen.

Wir haben eine Wortliste ausgearbeitet, anhand derer binäre Informationen per Telefon übermittelt werden können; jedes Wort steht hierbei für einen anderen Byte-Wert. Dabei waren wir bemüht, die Liste so zu gestalten, daß sie mit einer Vielzahl von Anwendungen einsetzbar ist. Die erste dieser Anwendungen sollte die Fingerabdrücke des öffentlichen Schlüssels aus PGP über das Telefon lesen, um den öffentlichen Schlüssel so zu authentisieren.
In diesem Fall ist der Fingerabdruck 20 Byte lang – es müssen also 20 Worte laut vorgelesen werden. Aus Erfahrung wissen wir, daß das Lesen so vieler Byte in Hexadezimalform relativ aufwendig und fehleranfällig ist. Die Verwendung einer Wortliste, in der jedes Byte durch ein Wort dargestellt wird, scheint sich in diesem Fall also anzubieten.

Bei einigen Anwendungen ist es möglicherweise sogar erforderlich, noch deutlich längere Byte-Folgen per Telefon zu übertragen; dies trifft beispielsweise auf vollständige Schlüssel oder Unterschriften zu. Hierbei müssen unter Umständen über 100 Byte gelesen werden. In diesem Fall scheint es oft sinnvoller zu sein, Worte anstelle von Hexadezimalbyte zu verwenden.

Beim lauten Vorlesen langer Byte-Folgen schleichen sich leicht Fehler ein. Die Art Fehler, die bei der Sprachübertragung von Daten auftreten, unterscheiden sich von den Fehlern, die bei der Datenübertragung per Modem vorkommen. Bei Modems werden Bit normalerweise durch Leitungsgeräusche gestört. Zur Fehlererkennung werden bei Modems meist CRCs hinzugefügt, die optimiert wurden, um Signalbündel von Leitungsgeräuschen zu erkennen. Bei willkürlichen Folgen gesprochener Worte kommt es üblicherweise zu einem der folgenden drei Fehler: 1) Vertauschung zweier aufeinanderfolgender Worte, 2) doppelte Worte oder 3) ausgelassene Worte. Bei der Entwicklung einer Fehlererkennungsmethode für diese Art von Datenübertragungskanal sollte besonderes Augenmerk auf der Abstimmung auf diese drei Fehlerarten liegen. 1991 unterhielt ich mich mit Zhahai Stewart, der eine gute Methode zur Fehlererkennung bezüglich dieser Fehler vorzuschlagen hatte.

Stewarts Ansatz zur Fehlererkennung beim lauten Vorlesen langer Byte-Folgen unter Verwendung einer Wortliste sieht vor, nicht nur eine, sondern zwei solcher Listen zu verwenden. Jede Liste enthält 256 phonetisch eindeutige Worte; jedes Wort steht für einen anderen Byte-Wert zwischen 0 und 255.

Das erste Byte (Versatz 0 in der Folge) wird zur Auswahl eines Wortes in der Liste mit den geraden Einträgen verwendet. Das Byte bei Versatz 1 wird zur Auswahl eines Wortes in der Liste mit den ungeraden Einträgen verwendet. Das Byte bei Versatz 2 wählt wieder ein Wort in der Liste der geraden Einträge, und das Byte bei Versatz 3 trifft wieder eine Auswahl in der Liste der ungeraden Einträge. Tatsächlich wird jeder Byte-Wert durch zwei unterschiedliche Worte dargestellt, abhängig davon, ob das jeweilige Byte vom Beginn der Byte-Folge gesehen bei einem geraden oder ungeraden Versatz angezeigt wird. Nehmen wir beispielsweise an, daß sowohl das Wort „adult“ als auch das Wort „amulet“ in den beiden Wortlisten jeweils an derselben Position aufgeführt wird, nämlich an Position 5. Das bedeutet, daß die wiederholende 3-Byte-Folge 05 05 05 für die 3-Wort-Folge „adult, amulet, adult“ steht.

Bei dieser Vorgehensweise lassen sich alle drei gängigen Fehlerarten in Sprachdatenströmen problemlos erkennen: Vertauschung, Duplikation und Auslassung. Bei einer Vertauschung werden zwei aufeinanderfolgenden Worten aus der Liste mit geraden Einträgen zwei aufeinanderfolgende Worte aus der Liste mit ungeraden Einträgen nachgestellt (oder andersherum). Eine Duplikation fällt durch zwei aufeinanderfolgende doppelte Worte auf, etwas, was in einer normalen Folge nicht vorkommt. Bei einer Auslassung werden zwei aufeinanderfolgende Worte aus derselben Liste verwendet.

Um die sofortige und zweifelsfreie Entdeckung der oben erläuterten drei Fehlerarten ohne Computerunterstützung zu ermöglichen, haben wir zwei Listen erarbeitet, die sich in einem Punkt deutlich unterscheiden: In der Liste mit den geraden Einträgen sind ausschließlich zweisilbige Worte, in der Liste mit den ungeraden Einträgen sind hingegen ausschließlich dreisilbige Worte enthalten. Dieser Vorschlag wurde von Computerlinguist Patrick Juola unterbreitet.

Die tatsächliche Ausarbeitung der Wortliste durch Patrick Juola und Phil Zimmermann wurde durch die Anwendung PGPfone beschleunigt. PGPfone ist eine Anwendung, durch die Ihr Computer zu einem sicheren Telefon wird. Wir haben diese Anwendung zur Authentisierung des erstmaligen Diffie-Hellman-Schlüsselaustauschs verwendet; digitale Unterschriften und Infrastrukturen öffentlicher Schlüssel kamen hierbei nicht zum Einsatz. Wir wußten, daß wir sie bei der Anwendung auf PGP zu einem späteren Zeitpunkt zur Authentisierung von Fingerabdrücken von PGP-Schlüsseln erneut verwenden würden.

Durch die Ausarbeitung der Wortlisten wollten wir eine Einheit zum Messen des phonetischen Abstands zwischen zwei Worten entwickeln, die dann als Anhaltspunkt zur Ausarbeitung einer vollständigen Liste dienen sollte. Grady Ward stellte uns eine umfangreiche Zusammenstellung von Worten und deren Aussprache zur Verfügung, und Patrick Juola erstellte mit genetischen Algorithmen die am besten geeignete Teilmenge aus Grady Wards Liste. Hier eine kurze Zusammenfassung von Juolas Arbeit: Er stellte eine große Anzahl von Annahmen auf, die er sich „vermehren“ ließ (durch den Ersatz von Annahmen durch andere Worte). Wie in der Entwicklungsgeschichte bildeten die besser geeigneten Annahmen die nächste Generation. Nach etwa 200 Generationen war die Liste ihrer Idealform schon sehr nahegekommen: Der phonetische Abstand zwischen den Worten war deutlich größer als bei der ursprünglichen Liste.

Die erste große Hürde war die Entwicklung der Metrik. Linguisten befassen sich seit Jahrzehnten mit der Erzeugung und Wahrnehmung von Tönen, und es gibt eine Reihe von Standardausdrücken, mit denen die Töne in der jeweiligen Sprache beschrieben werden. Wenn Sie zum Beispiel die englischen Worte „pun“, „fun“, „dun“ und „gun sagen (versuchen Sie es ruhig einmal), fällt auf, daß sich die Zunge bei jedem dieser Worte nach hinten bewegt. Linguisten bezeichnen dies als „Artikulationspunkt“. Geräusche, die sich diesbezüglich deutlich unterscheiden, hören sich für englische Muttersprachler unterschiedlich an. Wenn die Merkmale aller Töne in einem Wort kombiniert werden, erhalten wir die Tondarstellung des gesamten Wortes – und wir können den phonetischen Abstand zwischen einem Wortpaar errechnen.

Ganz so einfach war es dann doch nicht. Wir wußten nicht, welche Bedeutung den einzelnen Merkmalen zukommt, wortebenenbezogene Merkmale wie Akzente ließen sich nur schwer darstellen, und für bestimmte Töne war die merkmalsbasierte Analyse schlichtweg nicht durchführbar. Außerdem gab es noch einige weitere Feinheiten: Wir suchten nach Worten, die gängig genug waren, um allgemein bekannt zu sein – sie sollten jedoch wiederum nicht langweilig sein. Verwirrende Worte wie „Wiederholen", „Anfangen" oder „Fehler" sollten vermieden werden. Personen, deren Muttersprache nicht Englisch ist, nehmen bestimmte Tonmerkmale weniger ausgeprägt war. Ein Beispiel: Für Personen mit japanischer Muttersprache hören sich „r" und „l" möglicherweise gleich an und werden folglich auch gleich ausgesprochen. Wenn die Worte so kurz wären, daß eine ausreichende Anzahl davon auf einem kleinen LCD-Display Platz findet, wäre dies ebenfalls von Vorteil. Große Konsonantenblöcke („corkscrew" enthält fünf betonte Konsonanten hintereinander) sind in einigen Fällen schwer auszusprechen, besonders für Personen, deren Muttersprache nicht Englisch ist. Wie dem auch sei, wir waren bemüht, anhand all dieser Kriterien einen Filter für die ursprüngliche Wörterbuchliste bzw. für die Abstandsmetrik selbst zu erstellen.

Nachdem der Computer die am besten geeignete Liste „ausgespuckt" hatte, sahen wir sie uns noch einmal genau an. Ja, die Worte waren phonetisch eindeutig. Viele sahen jedoch so aus, als wären sie von einem Computer, nicht von einem menschlichen Wesen, ausgewählt worden. Eine Menge der Worte waren schlichtweg schrecklich und dumm. Einige waren abstoßend, andere waren nichtssagend und fad. Also haben wir die Liste ein bißchen „aufgefrischt". Einige Worte wurden gelöscht und durch solche ersetzt, die ein menschliches Wesen ausgesucht hätte. Wir ließen den Computer die neuen Worte mit der Liste vergleichen, um deren phonetische Eindeutigkeit im Vergleich zur restlichen Liste sicherzustellen. Außerdem versuchten wir, die Worte so zu gestalten, daß es nicht zu phonetischen Konflikten mit den anderen Worten im größeren Wörterbuch kommen konnte. Hierzu mußten wir darauf achten, daß die ausgewählten Worte nicht versehentlich für andere gehalten wurden, die sich nicht auf der Liste befanden.

In seinen Algorithmen verwendete Patrick Juola eine Reihe von Auswahlkriterien. Zu diesem Thema veröffentlichte er ein Dokument, in dem die Vorgänge detaillierter beschrieben werden. Das vorliegende Dokument bietet lediglich einen kurzen Abriß unserer Vorgehensweise bei der Ausarbeitung der Liste.

Ich bin mit der Wortliste nicht hunderprozentig zufrieden. Wenn es nach mir ginge, sollten mehr eingängige und weniger nichtssagende Worte enthalten sein. Mir persönlich gefallen Worte wie „Aztec“ und „Capricorn“ und die Worte im standardmäßigen Militäralphabet. Obwohl wir uns das Recht vorbehalten möchten, die Liste zu einem späteren Zeitpunkt zu überarbeiten, ist dies aufgrund der Probleme, die durch diese erste Version entstehen werden, eher unwahrscheinlich. Die vorliegende Version der Liste wurde zuletzt im September 1998 geändert.

Falls Sie bestimmte Worte in die Liste aufnehmen bzw. vorgeschlagene Worte daraus löschen lassen möchten, senden Sie diese an pgpfone-bugs@mit.edu. Wenn Sie möchten, können Sie auch gleich eine Kopie an Patrick Juola unter juola@mathcs.duq.edu senden. Unten werden die vollständigen Wortlisten aufgeführt (sowohl die Version mit den ungeraden als auch die mit den geraden Einträgen).

Wortliste mit zweisilbigen Einträgen

aardvark	absurd	accrue	acme	adrift
adult	afflict	ahead	aimless	Algol
allow	alone	ammo	ancient	apple
artist	assume	Athens	atlas	Aztec
baboon	backfield	backward	banjo	beaming
bedlamp	beehive	beeswax	befriend	Belfast
berserk	billiard	bison	blackjack	blockade
blowtorch	bluebird	bombast	bookshelf	brackish
breadline	breakup	brickyard	briefcase	Burbank
button	buzzard	cement	chairlift	chatter
checkup	chisel	choking	chopper	Christmas
clamshell	classic	classroom	cleanup	clockwork
cobra	commence	concert	cowbell	crackdown
cranky	crowfoot	crucial	crumpled	crusade
cubic	dashboard	deadbolt	deckhand	dogsled
dragnet	drainage	dreadful	drifter	dropper
drumbeat	drunken	Dupont	dwelling	eating
edict	egghead	eightball	endorse	endow
enlist	erase	escape	exceed	eyeglass
eyetooth	facial	fallout	flagpole	flatfoot
flytrap	fracture	framework	freedom	frighten
gazelle	Geiger	glitter	glucose	goggles
goldfish	gremlin	guidance	hamlet	highchair
hockey	indoors	indulge	inverse	involve
island	jawbone	keyboard	kickoff	kiwi
klaxon	locale	lockup	merit	minnow
miser	Mohawk	mural	music	necklace
Neptune	newborn	nightbird	Oakland	obtuse
offload	optic	orca	payday	peachy
pheasant	physique	playhouse	Pluto	preclude
prefer	preshrunk	printer	prowler	pupil
puppy	python	quadrant	quiver	quota
ragtime	ratchet	rebirth	reform	regain
reindeer	rematch	repay	retouch	revenge
reward	rhythm	ribcage	ringbolt	robust
rocker	ruffled	sailboat	sawdust	scallion
scenic	scorecard	Scotland	seabird	select
sentence	shadow	shamrock	showgirl	skullcap
skydive	slingshot	slowdown	snapline	snapshot
snowcap	snowslide	solo	southward	soybean
spaniel	spearhead	spellbind	spheroid	spigot
spindle	spyglass	stagehand	stagnate	stairway
standard	stapler	steamship	sterling	stockman
stopwatch	stormy	sugar	surmount	suspense
sweatband	swelter	tactics	talon	tapeworm
Tempest	tiger	tissue	tonic	topmost
tracker	transit	trauma	treadmill	Trojan
trouble	tumor	tunnel	tycoon	uncut
unearth	unwind	uproot	upset	upshot
vapor	village	Virus	Vulcan	waffle
wallet	watchword	wayside	willow	woodlark
Zulu				

Wortliste mit dreisilbigen Einträgen

adroitness	adviser	aftermath	aggregate	alkali
almighty	amulet	amusement	antenna	applicant
Apollo	armistice	article	asteroid	Atlantic
atmosphere	autopsy	Babylon	backwater	barbecue
belowground	bifocals	bodyguard	bookseller	borderline
bottomless	Bradbury	bravado	Brazilian	breakaway
Burlington	businessman	butterfat	Camelot	candidate
cannonball	Capricorn	caravan	caretaker	celebrate
cellulose	certify	chambermaid	Cherokee	Chicago
clergyman	coherence	combustion	commando	company
component	concurrent	confidence	conformist	congregate
consensus	consulting	corporate	corrosion	councilman
crossover	crucifix	cumbersome	customer	Dakota
decadence	December	decimal	designing	detector
detergent	determine	dictator	dinosaur	direction
disable	disbelief	disruptive	distortion	document
embezzle	enchanting	enrollment	enterprise	equation
equipment	escapade	Eskimo	everyday	examine
existence	exodus	fascinate	filament	finicky
forever	fortitude	frequency	gadgetry	Galveston
getaway	glossary	gossamer	graduate	gravity
guitarist	hamburger	Hamilton	handiwork	hazardous
headwaters	hemisphere	hesitate	hideaway	holiness
hurricane	hydraulic	impartial	impetus	inception
indigo	inertia	infancy	inferno	informant
insincere	insurgent	integrate	intention	inventive
Istanbul	Jamaica	Jupiter	leprosy	letterhead
liberty	maritime	matchmaker	maverick	Medusa
megaton	microscope	microwave	midsummer	millionaire
miracle	misnomer	molasses	molecule	Montana
monument	mosquito	narrative	nebula	newsletter
Norwegian	October	Ohio	onlooker	opulent
Orlando	outfielder	Pacific	pandemic	Pandora
paperweight	paragon	paragraph	paramount	passenger
pedigree	Pegasus	penetrate	perceptive	performance
pharmacy	phonetic	photograph	pioneer	pocketful
politeness	positive	potato	processor	provincial
proximate	puberty	publisher	pyramid	quantity
racketeer	rebellion	recipe	recover	repellent
replica	reproduce	resistor	responsive	retraction
retrieval	retrospect	revenue	revival	revolver
sandalwood	sardonic	Saturday	savagery	scavenger
sensation	sociable	souvenir	specialist	speculate
stethoscope	stupendous	supportive	surrender	suspicious
sympathy	tambourine	telephone	therapist	tobacco
tolerance	tomorrow	torpedo	tradition	travesty
trombonist	truncated	typewriter	ultimate	undaunted
underfoot	unicorn	unify	universe	unravel
upcoming	vacancy	vagabond	vertigo	Virginia
visitor	vocalist	voyager	warranty	Waterloo
whimsical	Wichita	Wilmington	Wyoming	yesteryear
Yucatan				

Glossar

AES (Advanced Encryption Standard)	Vom National Institute of Standards and Technology (NIST) genehmigte Standards. In der Regel werden diese in den nächsten 20 bis 30 Jahren verwendet.
Algorithmus (Hash)	Eine Reihe von mathematischen (logischen) Regeln, die für die Erstellung von Nachrichtenkernen und die Erzeugung von Schlüsseln / Unterschriften verwendet werden.
Algorithmus (Verschlüsselung)	Eine Reihe von mathematischen (logischen) Regeln, die für die Verschlüsselung und Entschlüsselung verwendet werden.
Anonymität	Der Ursprung oder Autor der Informationen ist unbekannt oder nicht angegeben, so daß die Identität des Erstellers / Absenders nicht herausgefunden werden kann.
ANSI (American National Standards Institute)	Entwickelt Standards über verschiedene akkreditierte Normen-Gremien (Accredited Standards Committee; ASC). Das X9-Komitee beschäftigt sich vorwiegend mit Sicherheitsstandards für Finanzdienstleistungen.
ASCII-geschützter Text	Binäre Informationen, die in druckbarem ASCII-Standardzeichensatz mit 7 Bit verschlüsselt wurden. Dsies dient der einfacheren Übertragung über Kommunikationssysteme. Bei PGP wird ASCII-geschützten Textdateien die normale Dateinamenerweiterung zugewiesen. Die Dateien werden im ASCII-Format Radix-64 ver- und auch entschlüsselt.
Asymmetrische Schlüssel	Ein zwar separates, jedoch integriertes Benutzerschlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel. Es handelt sich dabei um Einwegschlüssel, d. h. ein Schlüssel, der zur Verschlüsselung bestimmter Daten verwendet wurde, kann nicht zur Entschlüsselung derselben Daten benutzt werden.
Authentisierung	Die Bestimmung des Ursprungs verschlüsselter Informationen durch die Überprüfung der digitalen Unterschrift oder des öffentlichen Schlüssels einer Person, indem der eindeutige Fingerabdruck überprüft wird.
Autorisierter Schlüsselverwalter	Eine Person, der Sie dahingehend vertrauen, daß sie Ihnen echte Schlüssel anbietet. Wenn ein autorisierter Schlüsselverwalter einen fremden Schlüssel unterzeichnet, müssen Sie die Gültigkeit dieses Schlüssels nicht mehr in Frage stellen.

Benutzer-ID
Eine Textphrase, mit der ein Schlüsselpaar identifiziert wird. Ein übliches Format für eine Benutzer-ID ist beispielsweise der Name und die E-Mail-Adresse des Eigentümers. Mit der Benutzer-ID können Benutzer (d. h. sowohl der Eigentümer selbst als auch dessen Kollegen) den Eigentümer des Schlüsselpaares erkennen.

Bevollmächtigung
Übertragen von offiziellen Genehmigungen, Zugriffsrechten oder juristischen Vollmachten an einen Benutzer.

Blankounterschrift
Möglichkeit zum Unterschreiben von Dokumenten ohne Kenntnis des Inhalts, ähnlich wie bei zur Beglaubigung von Dokumenten berechtigten öffentlichen Stellen.

Blockchiffrierer
Ein symmetrischer Chiffriercode, der auf der Basis von Blökken (in der Regel 64-Bit-Blöcke) von Klartext und verschlüsseltem Text funktioniert.

CA (Certificate Authority)
Ein vertrauenswürdiger Dritter (Trust Third- Party; TTP), der Zertifikate mit Beurteilungen über verschiedene Attribute erstellt und diese einem Benutzer und / oder dem zugehörigen öffentlichen Schlüssel zuordnet.

CAPI (Crypto API)
Die kryptographische API von Microsoft für Windows-basierte Betriebssysteme und Anwendungen.

CAST
Ein 64-Bit-Blockchiffrierer, der 64-Bit-Schlüssel, sechs S-Boxen mit 8-Bit-Eingabe und 32-Bit-Ausgabe verwendet. Er wurde in Kanada von Carlisle Adams und Stafford Tavares entwickelt.

Chiffrierter Text
Klartext, der mit einem Verschlüsselungsalgorithmus in ein nicht lesbares Format verarbeitet wurde. Mit einem Entschlüsselungsschlüssel kann dieser Vorgang rückgängig gemacht und der Originaltext wieder hergestellt werden.

CRYPTOKI
Entspricht PKCS #11.

Datenintegrität
Ein Verfahren zum Prüfen, ob Informationen noch im Ursprungszustand vorliegen und nicht durch Unbefugte oder auf unbekannte Weise verändert wurden.

DES (Data Encryption Standard; Datenverschlüsselungsstandard)
Ein 64-Bit-Blockchiffrierer oder symmetrischer Algorithmus, der auch als Data Encryption Algorithm (DEA) (vom ANSI) bzw. DEA-1 (von der ISO) bezeichnet wird. Seit über 20 Jahren weit verbreitet, 1976 übernommen als „FIPS 46“.

Diffie-Hellman
Der erste Verschlüsselungsalgorithmus für öffentliche Schlüssel, der diskrete Logarithmen in einem endlichen Feld verwendete. Er wurde 1976 erfunden.

Digitale Unterschrift	Siehe Unterschrift
Direktes Vertrauen	Schaffung von Vertrauen auf gegenseitiger Basis.
DSA (Digital Signature Algorithm)	Ein vom NIST entworfener digitaler Unterschriftenalgorithmus für öffentliche Schlüssel zur Verwendung in DSS.
DSS (Digital Signature Standard)	Ein vom NIST vorgeschlagener Standard (FIPS) für digitale Unterschriften unter Verwendung des DSA.
ECC (Elliptic Curve Cryptosystem)	Ein eindeutiges Verfahren zur Erstellung von Verschlüsselungsalgorithmen für öffentliche Schlüssel auf der Grundlage von mathematischen Kurven in endlichen Feldern oder mit großen Primzahlen.
Echtheit	Gibt den Grad der Gewißheit an, mit der der Schlüssel tatsächlich dem angegebenen Eigentümer gehört.
EES (Escrowed Encryption Standard)	Eine von der Regierung der USA vorgeschlagene Norm zur Hinterlegung privater Schlüssel.
Einweg-Hash	Eine Funktion einer variablen Zeichenfolge zum Erstellen eines Wertes mit fester Länge, der das ursprüngliche Abbild darstellt. Wird auch Nachrichtenkern, Fingerabdruck und Message Integrity Check (MIC) genannt.
Elektronisches Geld	Geld in elektronischer Form, das über eine Vielzahl von komplexen Protokollen gespeichert und übertragen wird.
Elgamal-Schema	Wird für digitale Unterschriften und zur Verschlüsselung auf der Basis von diskreten Logarithmen in einem endlichen Feld verwendet. Kann mit der DAS-Funktion kombiniert werden.
Entschlüsselung	Eine Methode, mit der die Verschlüsselung von Informationen rückgängig gemacht werden kann, so daß diese wieder lesbar werden. Die Entschlüsselung wird mit dem privaten Schlüssel des Empfängers durchgeführt.
Fingerabdruck	Eine eindeutig identifizierende Zahlen- und Zeichenfolge zur Authentisierung öffentlicher Schlüssel. Dies ist das Hauptkriterium, mit dem die Echtheit eines Schlüssels überprüft werden kann. Siehe *Fingerabdruck eines Schlüssels*.

Fingerabdruck eines Schlüssels

Eine eindeutig identifizierende Zahlen- und Zeichenfolge zur Authentisierung öffentlicher Schlüssel. Sie können beispielsweise den Eigentümer eines öffentlichen Schlüssels anrufen und sich nach dem Fingerabdruck seines Schlüssels erkundigen, um diesen mit Ihrem Fingerabdruck des öffentlichen Schlüssels zu vergleichen und zu sehen, ob beide Schlüssel miteinander übereinstimmen. Falls die Fingerabdrücke nicht übereinstimmen, ist einer der Schlüssel falsch.

FIPS (Federal Information Processing Standard)

Eine vom NIST veröffentlichte Norm der Regierung der USA.

Firewall

Eine Kombination aus Hardware und Software zum Schutz des öffentlichen / privaten Netzwerks gegen bestimmte Angriffe von außen zur Gewährleistung eines bestimmten Maßes an Sicherheit.

Firmenweiter Unterschriftenschlüssel

Ein öffentlicher Schlüssel, der vom Sicherheitsbeauftragten eines Unternehmens als Schlüssel für das ganze System festgelegt wird und den alle Benutzer dieses Unternehmens bei der Unterzeichnung anderer Schlüssel als zuverlässig betrachten können.

Geheimnisverteilung

siehe „Teilen von Schlüsseln“.

Hash-Funktion

Eine Einweg-Hash-Funktion ist eine Funktion, die einen Nachrichtenkern erzeugt, der zur Erzeugung des Originals nicht umgekehrt werden kann.

Hexadezimal

Das Hexadezimalsystem ist ein Zahlensystem, das auf der Zahl 16 basiert. Bei diesem System werden 16 aufeinanderfolgende Nummern für jede Stelle einer Zahl verwendet (einschließlich Null), bevor eine weitere Stelle hinzugefügt wird. (Bitte beachten Sie, daß in dieser Erklärung die dezimale Zahl „16“ verwendet wird, um die hexadezimale Zahl „10“ zu beschreiben.) Hexadezimale Zahlen bestehen aus den Ziffern 0-9 und danach aus A-F.

Höhergestellter Schlüsselverwalter

Ein höhergestellter Schlüsselverwalter für autorisierte Schlüsselverwalter.

HTTP (HyperText Transfer Protocol)

Ein Protokoll zum Übertragen von Dokumenten zwischen Servern oder von einem Server zu einem Client.

IDEA (International Data Encryption Standard)

Ein symmetrischer 64-Bit-Blockchiffrierer unter Verwendung von 128-Bit-Schlüsseln. Er basiert auf dem Konzept, Vorgänge aus verschiedenen algebraischen Gruppen zu mischen. Wird als einer der wirksamsten Algorithmen angesehen.

IKE (Internet Key Exchange)
Dient der sicheren Übertragung von Schlüsseln über das Internet. IKE kann auch für Sicherheitsarchitekturen mit IPsec eingesetzt werden.

Implizites Vertrauen
Implizites Vertrauen ist für Schlüssel*paare* an Ihrem lokalen Schlüsselbund vorgesehen. Falls der private Anteil eines Schlüsselpaares an Ihrem Schlüsselbund gefunden wird, geht PGP davon aus, daß Sie der Eigentümer dieses Schlüsselpaares sind und sich selbst implizit vertrauen.

Integrität
Ein Beleg dafür, daß Daten bei der Speicherung oder Übertragung (durch unbefugte Personen) nicht verändert werden.

IPsec
Ein von der IETF in Erwägung gezogenes Verschlüsselungssystem auf TCP / IP-Ebene.

ISO (International Organization for Standardization)
Diese Organisation ist für eine Vielzahl von Normen verantwortlich, wie das OSI-Modell sowie internationale Beziehungen mit dem ANSI bezüglich X. 509.

Klartext
Daten oder Nachrichten in einer für den Menschen lesbaren Form vor dem Verschlüsseln (auch unverschlüsselter Text genannt).

Klartext
Normaler, lesbarer, unverschlüsselter und nicht unterschriebener Text.

Konventionelle Verschlüsselung
Eine Verschlüsselungsmethode, die statt eines öffentlichen Schlüssels eine allgemein bekannte Paßphrase verwendet. Hierbei wird die Datei mit einem Sitzungsschlüssel verschlüsselt, der die Verschlüsselung mit einer angegebenen Paßphrase durchführt.

Kryptoanalyse
Die Kunst oder Wissenschaft des Konvertierens von chiffriertem Text in Klartext ohne anfängliche Kenntnis des für die Verschlüsselung des Textes verwendeten Schlüssels.

Kryptographie
Die Kunst und Wissenschaft des Erstellens von Nachrichten, die eine beliebige Kombination der Attribute „vertraulich“, „unterschrieben“, „unverändert“ mit Urheberschaftsnachweis aufweisen.

Kryptographie mit öffentlichen Schlüsseln
Kryptographie, bei der Schlüsselpaare mit jeweils einem öffentlichen und einem privaten Schlüssel verwendet werden. Bei dieser Technik sind keine Sicherheitsvorkehrungen für den Datenübertragungsweg selbst erforderlich.

LDAP (Lightweight Directory Access Protocol)
Ein einfaches Protokoll zur Unterstützung von Zugriff und Suchvorgängen in Verzeichnissen mit Informationen, wie beispielsweise Namen, Telefonnummern und Adressen in sonst inkompatiblen Systemen über das Internet.

MIC (Message Integrity Check)
Wurde anfangs in PEM zur Authentisierung mittels MD2 oder MD5 definiert. Micalg (Message Integrity Calculation) wird in sicheren MIME-Anwendungen eingesetzt.

MIME (Multipurpose Internet Mail Extensions)
Eine frei verfügbare Menge von Spezifikationen, mit denen Text in Sprachen mit verschiedenen Zeichensätzen sowie Multimedia-E-Mails zwischen vielen verschiedenen Computer-Systemen mit Internet-E-Mail-Standards ausgetauscht werden können.

Nachrichtenkern
Ein kompaktes „Destillat“ Ihrer E-Mail-Nachricht bzw. Datei-Prüfsumme. Der Nachrichtenkern „repräsentiert“ Ihre E-Mail-Nachricht. Wenn die Nachricht in irgendeiner Form verändert wird, ändert sich auch der aus ihr berechnete Nachrichtenkern.

Öffentlicher Schlüssel
Einer der beiden Schlüssel eines Schlüsselpaares. Mit dem öffentlichen Schlüssel werden Informationen verschlüsselt und Unterschriften verifiziert. Der öffentliche Schlüssel eines Benutzers kann an viele bekannte oder unbekannte Personen innerhalb und außerhalb eines Unternehmens weitergegeben werden. Mit Hilfe des öffentlichen Schlüssels einer Person kann niemand an den entsprechenden privaten Schlüssel gelangen.

Öffentlicher Schlüsselbund
Eine Reihe von öffentlichen Schlüsseln. Ihr öffentlicher Schlüsselbund enthält Ihre eigenen öffentlichen Schlüssel.

Paßphrase
Eine einprägsame Wortgruppe, die eine höhere Sicherheit als ein einzelnes Paßwort gewährleistet. Durch „Verwürfeln“ von Schlüsseln wird sie in einen Zufallsschlüssel umgewandelt.

Paßwort
Eine Zeichenfolge oder ein Wort, die oder das eine Person zur Authentisierung, Überprüfung oder Verifizierung in ein System eingibt.

PGP/MIME
Eine IETF-Norm (RFC 2015) zur Geheimhaltung und Authentisierung unter Verwendung der in RFC1847 erläuterten MIME-Sicherheitsinhaltstypen (Multipurpose Internet Mail Extensions; MIME). PGP / MIME wird momentan in PGP 5.0 und späteren Versionen verwendet.

PKCS (Public Key Crypto Standards)

Eine Reihe von *De-facto*-Normen zur Verschlüsselung mit öffentlichen Schlüsseln, die in Zusammenarbeit mit einem informellen Konsortium (Apple, DEC, Lotus, Microsoft, MIT, RSA und Sun) entwickelt wurden. Dazu gehören algorithmus-spezifische und von Algorithmen unabhängige Implementierungsnormen. Spezifikationen zur Definition von Nachrichtensyntax und anderen Protokollen, die von RSA Data Security, Inc., gesteuert werden.

PKI (Public Key Infrastructure)

Ein weitverbreitetes und zugängliches Zertifikatssystem zum Erhalt von öffentlichen Schlüsseln eines Benutzers, bei dem Sie bis zu einem gewissen Grad sicher sein können, daß Sie den „richtigen“ Schlüssel erhalten haben und daß dieser nicht zurückgenommen wurde.

Privater Schlüssel

Der geheime Teil eines Schlüsselpaares, mit dem Informationen unterschrieben und entschlüsselt werden. Der private Schlüssel eines Benutzers sollte geheim gehalten werden und nur diesem bekannt sein.

Privater Schlüsselbund

Ein Satz aus einem oder mehreren privaten Schlüsseln, die alle dem Eigentümer des privaten Schlüsselbundes gehören.

RFC (Request for Comment)

Ein IETF-Dokument, aus der Untergruppe FYI RFC (geben Überblicke und Einführungen) oder aus der Untergruppe STD RFC (geben Internet-Normen an). Die Abkürzung FYI steht für „For Your Information“ (Zu Ihrer Information). Jede RFC hat zur Indizierung eine RFC-Nummer, anhand deren er abgerufen werden kann (www. ietf. org).

RSA

Abkürzung von RSA Data Security, Inc. Steht auch für die Firmenchefs Ron Rivest, Adi Shamir und Len Adleman oder bezieht sich auf den von ihnen erfundenen Algorithmus. Der RSA-Algorithmus wird in der Kryptographie mit öffentlichen Schlüsseln verwendet. Seine Funktionsweise beruht auf der Tatsache, daß zwei große Primzahlen zwar leicht miteinander zu multiplizieren sind, aber das Produkt nur schwer wieder in sie zu zerlegen ist.

S/MIME (Secure Multipurpose Mail Extension)

Ein von Deming Software und RSA Data Security entwickelter Normvorschlag zum Verschlüsseln und/oder zur Authentisierung von MIME-Daten. S/MIME definiert ein Format für die MIME-Daten, für die zur Abstimmung der Kommunikationssysteme erforderlichen Algorithmen (RSA, RC2, SHA-1) und für die weiteren Betriebsfragen, wie beispielsweise ANSI X. 509-Zertifikate sowie die Übertragung über das Internet.

Schlüssel Ein digitaler Code zur Verschlüsselung und Unterzeichnung sowie zur Entschlüsselung und Verifizierung von E-Mail-Nachrichten und Dateien. Schlüssel werden paarweise erstellt und in Schlüsselbunden gespeichert.

Schlüsselaustausch Ein Schema mit zwei oder mehreren Knoten zum Übertragen eines geheimen Sitzungsschlüssels über einen nicht gesicherten Kanal.

Schlüsselbund Eine Reihe von Schlüsseln. Jeder Benutzer verfügt über zwei Arten von Schlüsselbunden: einen privaten und einen öffentlichen Schlüsselbund.

Schlüsselhinterlegung/ -wiederherstellung Ein Verfahren, bei dem der Benutzer eines Verschlüsselungssystems mit öffentlichen Schlüsseln seinen privaten Schlüssel an einen Dritten übergibt, so daß dieser den Austausch von verschlüsselten E-Mail-Nachrichten überwachen kann.

Schlüssel-ID Ein lesbarer Code, mit dem ein Schlüsselpaar eindeutig identifiziert wird. Zwei Schlüsselpaare können dieselbe Benutzer-ID haben, die Schlüssel-IDs sind jedoch stets verschieden.

Schlüssellänge Die Anzahl der Bits zur Darstellung der Schlüsselgröße. Je länger der Schlüssel, desto stärker ist er.

Schlüsselpaar Ein öffentlicher und der zugehörige private Schlüssel. In Kryptographiesystemen mit öffentlichen Schlüsseln (wie PGP) verfügt jeder Benutzer über mindestens ein Schlüsselpaar.

Schlüsselverwalter Eine Person oder ein Unternehmen mit der Erlaubnis, sich für die Echtheit der öffentlichen Schlüssel anderer Benutzer zu verbürgen. Sie können einen Schlüsselverwalter festlegen, indem Sie seinen öffentlichen Schlüssel unterschreiben.

Schlüsselverwaltung Das Verfahren zum sicheren Speichern und Verteilen akkurater kryptographischer Schlüssel. Der Gesamtprozeß des sicheren Erstellens und Verteilens von kryptographischen Schlüsseln an befugte Empfänger.

Selbstunterschriebener Schlüssel Ein öffentlicher Schlüssel, der zum Eigentumsnachweis mit dem entsprechenden privaten Schlüssel unterschrieben wurde.

Sicherer Kanal Ein Mittel zur Übertragung von Informationen zwischen Terminals, bei der kein Gegner diese Informationen umstellen, löschen, lesen oder andere Informationen einfügen kann (SSL, IPsec, „Ins-Ohr-Flüstern“).

Sitzungsschlüssel	Der geheime (symmetrische) Schlüssel zum Verschlüsseln aller Datensätze auf Transaktionsbasis. Für jede Kommunikationssitzung wird ein anderer Sitzungsschlüssel verwendet.
SSL (Secure Socket Layer)	Wurde von Netscape zur Gewährleistung von Sicherheit und zur Geheimhaltung im Internet entwickelt. SSL unterstützt die Server- und Client-Authentisierung und gewährleistet die Sicherheit und Integrität des Übertragungskanals. Wirkt auf der Übertragungsebene und dient als „Socket-Bibliothek“, wodurch eine anwendungsunabhängige Wirkungsweise ermöglicht wird. Verschlüsselt den gesamten Kommunikationskanal und unterstützt keine digitalen Unterschriften auf Nachrichtenebene.
Symmetrischer Algorithmus	Wird auch als konventioneller, geheimer Schlüssel- oder Einzelschlüsselalgorithmus bezeichnet. Der Verschlüsselungsschlüssel ist entweder mit dem Entschlüsselungsschlüssel identisch, oder ein Schlüssel kann aus dem anderen abgeleitet werden. Es gibt zwei Unterkategorien – Block und Strom.
Teilen von Schlüsseln oder „Geheimnisverteilung“	Ein Vorgang, bei dem ein privater Schlüssel in viele Teile zerlegt und an mehrere Personen verteilt wird. Zur Verwendung des Schlüssels muß eine festgelegte Anzahl Personen ihre Schlüsselteile zusammensetzen.
Teilschlüssel	Unter einem Teilschlüssel versteht man einen Diffie-Hellman-Verschlüsselungsschlüssel, der dem Masterschlüssel als Teilmenge hinzugefügt wird. Nach der Erstellung eines Teilschlüssels können Sie diesen ungültig werden lassen oder zurücknehmen, ohne daß der Masterschlüssel oder die darauf gesammelten Unterschriften hierdurch beeinflußt werden.
Text	Druckbarer ASCII-Standardzeichensatz mit 7-Bit.
TLS (Transport Layer Security)	Ein IETF-Entwurf. Version 1 basiert auf Version 3.0 des SSL-Protokolls (Secure Sockets Layer; SSL) und dient zur Wahrung der Privatsphäre bei der Kommunikation über das Internet.
TLSP (Transport Layer Security Protocol)	ISO 10736, Entwurf des internationalen Standards.
Triple-DES	Eine Verschlüsselungskonfiguration, in der der DES-Algorithmus dreimal mit drei unterschiedlichen Schlüsseln verwendet wird.
Unterschreiben	Eine Unterschrift leisten.

Unterschrift

Ein digitaler, mit einem privaten Schlüssel erstellter Code. Unterschriften ermöglichen im Prozeß der Unterschriftsverifizierung die Authentisierung von Informationen. Wenn Sie eine E-Mail-Nachricht oder eine Datei unterschreiben, erstellt PGP mit Ihrem privaten Schlüssel einen digitalen Code, der sowohl für den Inhalt der Nachricht als auch für Ihren privaten Schlüssel eindeutig ist. Jeder kann mit Ihrem öffentlichen Schlüssel Ihre Unterschrift verifizieren.

Urheberschaftsnachweis

Verhindert die Verweigerung von früheren Verpflichtungen oder Leugnung von Handlungen.

Verifizierung

Das Vergleichen einer mit Hilfe eines privaten Schlüssels erstellten Unterschrift mit dem entsprechenden öffentlichen Schlüssel. Die Verifizierung beweist, daß die Informationen tatsächlich vom Unterzeichner gesendet wurden und daß die E-Mail-Nachricht nicht nachträglich von einer dritten Person verändert wurde.

Verschlüsselung

Eine Methode zum Chiffrieren von Informationen, um sie für jeden außer für den gewünschten Empfänger unlesbar zu machen.

Verschlüsselungssystem

Ein System, das aus kryptographischen Algorithmen, beliebigem Klartext, chiffriertem Text und Schlüsseln besteht.

Vertrauenshierarchie

Benutzer auf verschiedenen Ebenen, die Vertrauen auf organisierte Weise verteilen. Häufig in ANSI X. 509 zum Verteilen von Zertifizierungsinstanzen verwendet.

Vertrauenswürdig

Ein öffentlicher Schlüssel kann von Ihnen als vertrauenswürdig betrachtet werden, wenn er von Ihnen oder einer anderen Person, die Sie als Schlüsselverwalter festgelegt haben, zertifiziert wurde.

Vollmachtszertifikat

Ein elektronisches Dokument, das als Bestätigung des Vorhandenseins von Zugriffsrechten sowie der angegebenen Identität von Benutzern dient.

VPN (Virtual Private Network)

Ermöglicht die Ausdehnung von privaten Netzwerken vom Endbenutzer über ein öffentliches Netzwerk (Internet) direkt bis zum Home-Gateway Ihrer Wahl, wie beispielsweise zum Intranet Ihrer Firma.

Web of Trust

Ein Modell des verteilten Vertrauens, mit dem PGP den Eigentümer eines öffentlichen Schlüssels bestimmt. Der Grad des Vertrauens ist kumulativ und basiert auf der Kenntnis einer Person über die Schlüsselverwalter.

Wörterbuchangriff	Berechneter schwerer Angriff zum Entschlüsseln eines Paßworts durch Durchprobieren von offensichtlichen und logischen Wortkombinationen.
X.509	Ein digitales ITU-T-Zertifikat, bei dem es sich um ein international anerkanntes elektronisches Dokument zur Prüfung der Identität und der Eigentümer von öffentlichen Schlüsseln in einem Kommunikationsnetzwerk handelt. Es enthält den Namen des Absenders, Informationen zur Identifizierung des Benutzers und die digitale Unterschrift des Absenders sowie andere mögliche Erweiterungen.
Zeitangaben	Aufzeichnen der Erstellungszeit oder der Zeit des Vorhandenseins von Informationen.
Zertifikat (digitales Zertifikat)	Ein von einem vertrauenswürdigen Dritten mit einem öffentlichen Schlüssel verbundenes elektronisches Dokument, das beweist, daß der öffentliche Schlüssel einem rechtmäßigen Eigentümer gehört und nicht verfälscht wurde.
Zertifizieren	Den öffentlichen Schlüssel einer anderen Person unterschreiben.
Zertifizierung	Bestätigung von Informationen durch einen vertrauenswürdigen Benutzer.
Zertifizierungsinstanz	Eine oder mehrere vertrauenswürdige Personen, denen die Verantwortung zugewiesen wird, den Ursprung von Schlüsseln zu zertifizieren und diese einer allgemein zugänglichen Datenbank hinzuzufügen.
Zufallszahl	Ein wichtiger Aspekt für viele Verschlüsselungssysteme sowie ein notwendiges Element beim Erzeugen von eindeutigen Schlüsseln, die für Gegner nicht berechenbar sind. Echte Zufallszahlen werden normalerweise aus analogen Quellen abgeleitet und erfordern in der Regel den Einsatz von besonderer Hardware.
Zurücknahme	Widerrufen von Zertifizierungen oder Bevollmächtigungen.

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

Z