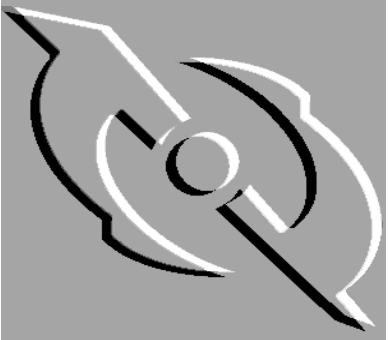

PGP Command Line

Befehlszeilenhandbuch

Version 6.5 Int.

BESCHRÄNKTE GARANTIE

Beschränkte Garantie. Network Associates garantiert für einen Zeitraum von sechzig (60) Tagen ab Kaufdatum, daß das Medium, auf dem die Software gespeichert ist (z. B. Disketten), frei von Mängeln in bezug auf Material und Verarbeitung ist.

Ansprüche des Kunden. Die gesamte Haftung von Network Associates sowie von deren Anbietern und Ihr alleiniger Anspruch bestehen nach Wahl von Network Associates entweder (i) in der Rückerstattung des für die Lizenz bezahlten Preises, falls zutreffend, oder (ii) im Ersatz des fehlerhaften Mediums, auf dem die Software gespeichert ist, durch eine Kopie der Software auf einem fehlerfreien Medium. Das fehlerhafte Medium ist gemeinsam mit einer Kopie des Kaufbelegs an Network Associates zurückzugeben. Die Kosten dafür sind vom Kunden zu tragen. Diese beschränkte Garantie gilt nicht, wenn der Fehler auf einen Unfall, auf Mißbrauch oder auf fehlerhafte Anwendung zurückzuführen ist. Für Ersatzmedien wird nur für den Rest der ursprünglichen Garantiefrist eine Garantie übernommen. Außerhalb der Vereinigten Staaten von Amerika steht dieser Anspruch nicht zur Verfügung, sofern Network Associates den Beschränkungen entsprechend den Exportkontrollgesetzen und -bestimmungen der USA unterliegt.

Garantieausschluß. Soweit es das geltende Recht zuläßt, es sei denn, es ist in den Angaben zur beschränkten Garantie in diesem Dokument anders vorgesehen, WIRD DIE SOFTWARE „OHNE MÄNGELGEWÄHR“ GELIEFERT. OHNE EINSCHRÄNKUNG DER VORGENANNTEN BESTIMMUNGEN ÜBERNEHMEN SIE DIE VOLLE VERANTWORTUNG FÜR DIE AUSWAHL DER SOFTWARE, MIT DER SIE DIE GEWÜNSCHTEN ERGEBNISSE ERZIELEN MÖCHTEN, SOWIE FÜR DIE INSTALLATION UND VERWENDUNG DER SOFTWARE UND DIE DURCH DEN EINSATZ DER SOFTWARE ERZIELTEN ERGEBNISSE: OHNE EINSCHRÄNKUNG DER VORGENANNTEN BESTIMMUNGEN ÜBERNIMMT NETWORK ASSOCIATES KEINERLEI GARANTIE DAFÜR, DASS DIE SOFTWARE FREI VON FEHLERN UND UNTERBRECHUNGEN ODER ANDEREN AUSFÄLLEN IST UND DASS SIE IHREN ANFORDERUNGEN ENTSPRICHT. SOWEIT ES DAS GÜLTIGE RECHT ZULÄSST, SCHLIESST NETWORK ASSOCIATES JEGLICHE GARANTIEANSPRÜCHE, OB AUSDRÜCKLICH ODER STILLSCHWEIGEND, EINSCHLIESSLICH DER STILLSCHWEIGENDEN GEWÄHRLEISTUNG DER HANDELBARKEIT UND DER EIGNUNG FÜR EINEN BESONDEREN ZWECK, DES NICHTVERSTOSSES IN BEZUG AUF DIE SOFTWARE UND DIE DAZUGEHÖRIGE DOKUMENTATION, JEDOCH NICHT AUF DIESE BESCHRÄNKT, AUS. DA HAFTUNGSBESCHRÄNKUNGEN BEZÜGLICH STILLSCHWEIGENDER GEWÄHRLEISTUNGEN IN EINIGEN STAATEN UND RECHTSORDNUNGEN NICHT ZULÄSSIG SIND, TRIFFT DIE OBIGE BESCHRÄNKUNG AUF SIE MÖGLICHERWEISE NICHT ZU. Die vorgenannten Bestimmungen sind in dem im Rahmen des geltenden Rechts zulässigen Umfang einklagbar.

LIZENZVEREINBARUNG

HINWEIS FÜR ALLE BENUTZER: DIE GENAUEN BEDINGUNGEN, DENEN DIE VERWENDUNG DER IN DIESER DOKUMENTATION BESCHRIEBENEN SOFTWARE UNTERLIEGT, FINDEN SIE IN DER DATEI README.1ST, LICENSE.TXT BZW. IN DEM JEWEILIGEN LIZENZDOKUMENT, DAS DER SOFTWARE ENTWEDER ALS TEXTDATEI BEILIEGT ODER BESTANDTEIL DER VERPACKUNG DER SOFTWARE IST. FALLS SIE NICHT SÄMTLICHEN DARIN DARGELEGTEN BEDINGUNGEN ZUSTIMMEN, INSTALLIEREN SIE DIE SOFTWARE NICHT. IN DIESEM FALL KÖNNEN SIE DAS PRODUKT AM ERWERBSORT ZURÜCKGEBEN, UND IHNEN WIRD DER VOLLE KAUFPREIS ERSTATTET.

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. +31(20)5866100
Gatwickstraat 25
1043 GL Amsterdam
http://www.nai.com

info@nai.com

* wird gelegentlich anstelle von ® für die Kennzeichnung von eingetragenen Warenzeichen verwendet, um Warenzeichen, die nicht in den USA eingetragen sind, zu schützen.

Inhalt

Vorwort

Aufbau dieses Handbuchs

Das Handbuch ist in folgende Kapitel unterteilt:

- Kapitel 1, „Einführung in PGP“ Dieses Kapitel enthält eine Einführung zur Verwendung der PGP-Befehlszeilensoftware.
- Kapitel 2, „Erste Schritte“ In diesem Kapitel wird beschrieben, wie PGP gestartet und beendet wird, wie Schlüssel erstellt und ausgetauscht werden und wie häufige PGP-Funktionen über die Befehlszeile ausgeführt werden.
- Kapitel 3, „Weiterführende Themen“ In diesem Kapitel wird beschrieben, wie PGP nicht interaktiv von UNIX-Shell-Skripten oder MSDOS-Stapelverarbeitungsdateien und wie PGP als UNIX-Filter verwendet wird. Außerdem wird die Verschlüsselung und Übertragung binärer Daten behandelt.
- Kapitel 4, „PGP-Konfigurationsdatei“ Dieses Kapitel enthält eine Einführung zur Konfigurationsdatei von PGP und den zugehörigen Parametern.

Konventionen in diesem Handbuch

Nachfolgend werden die in diesem Handbuch verwendeten Konventionen beschrieben:

Fettdruck	Menüs, Felder, Optionen und Schaltflächen werden fett formatiert. Beispiel: Wählen Sie im Menü **Bearbeiten** die Option **Löschen**.
`Schriftart „Sans Serif“`	Pfadangaben, Dateinamen, Symbolunterschriften, Bildschirmtext und bestimmte Tasten auf der Tastatur werden in der Schriftart „Sans Serif“ dargestellt.
`Tastenanschläge`	Ihre Tastenanschläge werden in der Schriftart „Sans Serif“ fett formatiert dargestellt.
`Variablen`	Befehlszeilentext, für den ein Wert eingegeben werden muß, wird in der Schriftart „Sans Serif“ kursiv formatiert dargestellt.

So erreichen Sie Network Associates

Kundendienst

Wenden Sie sich an den Kundendienst von Network Associates, wenn Sie weitere Produkte bestellen oder Produktinformationen erhalten möchten, oder schreiben Sie an folgende Adresse:

Network Associates International BV.
Gatwickstraat 25
NL-1043 GL Amsterdam

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 oder die neuesten Nachrichten von Network Associates sowie zur Verschlüsselung von Nachrichten erhalten möchten, so sehen 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 über Ihren Computer und die von Ihnen verwendete 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 über Ihren Computer und die von Ihnen verwendete 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, z. B. 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-Website unter http://www.nai.com/y2k. Weitere Informationen sind über E-Mail an die Adresse y2k@nai.com erhältlich.

Network Associates-Schulungen

Informationen über 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 geringes 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.

Einführung in PGP 1

Willkommen bei PGP. Mit PGP können Sie Ihre Daten einfach und sicher durch Verschlüsselung schützen, so daß sie nur von den gewünschten Empfängern gelesen werden können. Sie können Informationen auch digital unterschreiben, wodurch ihre Echtheit garantiert wird.

PGP verwenden

Diese Befehlszeilenversion von PGP wurde für zwei weitläufige Anwendungstypen entwickelt: Sichere Übertragung von Informationen zwischen Stapelverarbeitungsservern und Integration in automatisierte Vorgänge.

- Kreditinstitute können PGP zur sicheren Übertragung von Dateien von einer Geschäftsstelle zu einer anderen verwenden. Die Dateien werden mit dem Schlüssel des Empfängerservers und dem FTP in einem Verzeichnis auf einem entfernten Server verschlüsselt. Der entfernte Server überprüft regelmäßig sein Empfangsverzeichnis. Sobald der entfernte Server neu übertragene Dateien identifiziert hat, entschlüsselt er diese und sendet sie an ihr Zielverzeichnis.
- UNIX- und Windows-Entwickler können dieses Produkt verwenden, um Finanzgeschäfte, die Benutzer im Internet tätigen, zu sichern. Wenn Sie beispielsweise Produkte auf Ihrer Web-Site zum Kauf anbieten, können Sie PGP in Ihre Skripten einfügen, so daß Bestellungen von Kunden und Kreditkarteninformationen zum Speichern und zur Übertragung an einen sicheren Computer automatisch verschlüsselt werden. Der Begriff *MSDOS-Stapelverarbeitungsdateien* bezieht sich auf eine Windows NT-Eingabeaufforderung.

Der Begriff *MSDOS* bezieht sich auf das Fenster mit der Eingabeaufforderung in Windows NT.

Kurzer Überblick

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. Ihre privaten und Ihre öffentlichen Schlüssel werden in Schlüsselbunddateien gespeichert.

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

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.

1. PGP auf Ihrem Computer installieren. Die vollständigen Installationsanweisungen finden Sie in der Dokumentation, die Sie mit PGP erhalten haben.

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.

   Nach der Installation von PGP können Sie jederzeit ein neues Schlüsselpaar erstellen.

   Weitere Informationen über das Erstellen von privaten und öffentlichen Schlüsselpaaren finden Sie im Abschnitt „Schlüsselpaare erstellen“ auf Seite 8.

3. Öffentliche Schlüssel mit anderen Personen austauschen

   Nach der Erstellung eines Schlüsselpaars 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 erhalten Sie unter „Schlüssel erstellen und austauschen“ auf Seite 7 und unter „Ihren öffentlichen Schlüssel verteilen“ auf Seite 12.

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 eines anderen Benutzers mit dem Fingerabdruck des Originalschlüssels dieser Person.

   Sie können einen Schlüssel auch als gültig akzeptieren, wenn sich auf diesem die Unterschrift eines autorisierten Schlüsselverwalters befindet. 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 zurückzuschikken, damit Sie seine Unterschrift einfügen können, wenn Sie den Schlüssel auf einem Server für öffentliche Schlüssel 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 Ihrem öffentlichen Schlüsselbund hinzufügen. Dies bedeutet, daß Sie ziemlich sicher sein können, daß ein Schlüssel vom angegebenen Benutzer stammt, wenn er von einem autorisierten Schlüsselverwalter unterzeichnet wurde.

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.

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.

5. Eigene 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.

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.

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.

Erste Schritte 2

In diesem Kapitel werden folgende Themen behandelt:

- Starten und Beenden von PGP
- Erstellen und Austauschen von Schlüsselpaaren
- Ausführung gängiger PGP-Funktionen von der Befehlszeile aus
- Anzeigen des Online-Benutzerhandbuchs von PGP

PGP starten

Zum Starten von PGP geben Sie folgendes in der Befehlszeile ein:

pgp

Sämtliche PGP-Funktionen können von der Befehlszeile aus ausgeführt werden.

Speicherort von PGP-Dateien

Unter UNIX:

Wenn Sie PGP erstmals starten, prüft die Software, ob die Umgebungsvariable PGPPATH definiert wurde oder nicht. Falls PGPPATH definiert wurde, werden die Datei mit den PGP-Voreinstellungen, Schlüsselbunddateien, PGP.CFG sowie die Zufallswert-Datei im Verzeichnis %PGPPATH% gespeichert.

Falls PGPPATH nicht definiert wurde, prüft die Software, ob die Umgebungsvariable USERPROFILE definiert wurde oder nicht. Wenn dies der Fall ist, werden die Dateien im Verzeichnis %USERPROFILE%\Application Data\pgp gespeichert.

Falls USERPROFILE nicht definiert wurde, werden die Dateien im Verzeichnis %SYSTEMROOT%\pgp gespeichert.

Unter Windows NT:

Wenn Sie PGP erstmals starten, prüft die Software, ob die Umgebungsvariable PGPPATH definiert wurde oder nicht. Falls PGPPATH definiert wurde, wird die Datei PGP.CFG im Verzeichnis %PGPPATH% gespeichert.

Falls PGPPATH nicht definiert wurde, prüft die Software, ob die Umgebungsvariable USERPROFILE definiert wurde. Wenn dies der Fall ist, wird die Datei PGP.CFG im Verzeichnis %USERPROFILE%\Application Data\pgp gespeichert.

Falls USERPROFILE nicht definiert wurde, wird die Datei PGP.CFG im Verzeichnis %SYSTEMROOT%\pgp gespeichert.

Die Datei mit den Voreinstellungen wird im Verzeichnis %USERPROFILE%\Application Data\pgp gespeichert. Über diese Datei wird definiert, wo die Standardschlüsselbunde gespeichert werden (normalerweise im selben Verzeichnis, also %USERPROFILE%\Application Data\pgp).

Die Zufallswert-Datei wird stets im Verzeichnis %SYSTEMROOT% gespeichert.

PGPPATH: Pfadname für PGP festlegen

Dieser Parameter gibt den Speicherort bestimmter PGP-Dateien an:

SET PGPPATH=<PGPpathname>

Beispiel:

SET PGPPATH=C:\PGP

PGP muß wissen, wo sich folgende Dateien befinden:

- Ihre Schlüsselbunddateien PUBRING.PKR und SECRING.SKR
- Die Datei mit Zufallswerten RANDSEED.RND
- Die PGP-Konfigurationsdatei PGP.CFG (bzw. .PGPRC)

Diese Dateien können sich in einem beliebigen Verzeichnis befinden. Mit dem Parameter PGPPATH können Sie ihren Speicherort ermitteln.

Kompatibilität von PGP mit PGP 2.6.2 sicherstellen

Diese Version von PGP enthält eine Kompatibilitätsoption, die die Kompatibilität der Benutzeroberfläche mit PGP 2.6.2 ermöglicht. Diese Funktion benötigen Sie unter Umständen für die Interaktion mit Skripten, die das Parsing der Ausgabe durchführen bzw. auf andere Weise mit PGP-Dialogfeldern interagieren.

Zur Aktivierung dieser Funktion ergänzen Sie die Konfigurationsdatei, PGP.CFG, um folgende Zeile:

```
COMPATIBLE=ON
```

Sie können in der Befehlszeile auch +COMPATIBLE eingeben.

Schlüssel erstellen und austauschen

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 2-1), 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 Personen 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.

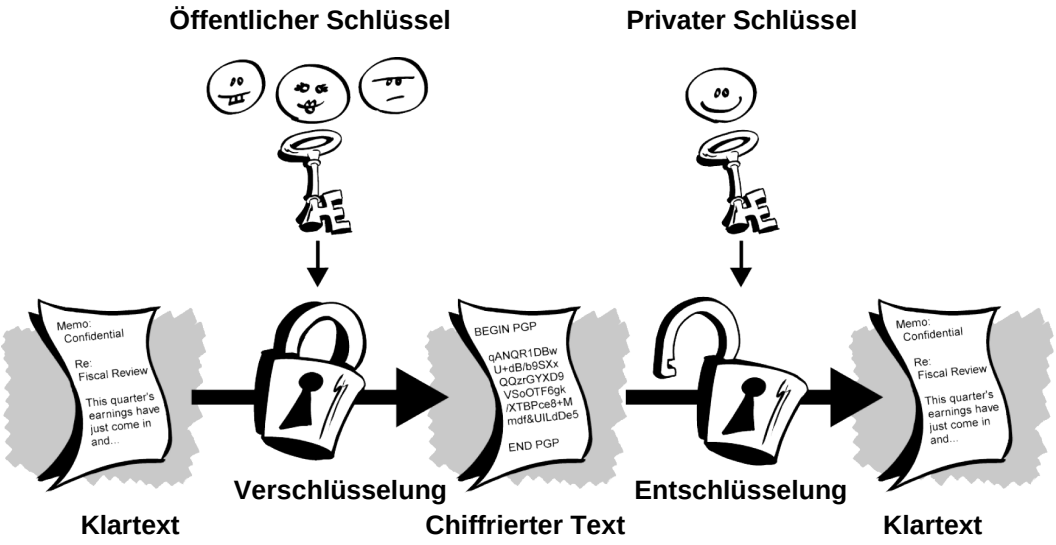

Abbildung 2-1. Kryptographie mit öffentlichen Schlüsseln

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. Ein neues Schlüsselpaar können Sie von der PGP-Befehlszeile aus erzeugen.

❑ **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. Stattdessen können Sie mit der PGPPATH-Umgebungsvariable ermitteln, wo Ihre vorhandenen Schlüsselbunde gespeichert wurden. Weitere Informationen finden Sie im Abschnitt „PGPPATH: Pfadname für PGP festlegen“ auf Seite 6.

So erstellen Sie ein neues Schlüsselpaar

1. Geben Sie folgendes in der Befehlszeile ein:

   pgp -kg

2. Anweisungen zur DSS / DH-fähigen Version finden Sie unter Schritt 4.

   Bei RSA-fähigen Versionen wählen Sie den Schlüsseltyp aus:

   a. DSS / DH

   b. RSA

   Fahren Sie mit Schritt 4 fort.

3. Bei DSS / DH-fähigen Versionen wählen Sie entweder einen neuen Unterschriftenschlüssel aus oder ergänzen einen vorhandenen DSS-Schlüssel um einen neuen Verschlüsselungsteilschlüssel.

4. Markieren Sie die zu erzeugende Schlüsselgröße. Die Erzeugung eines größeren 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. Ein größerer Schlüssel ist zuverlässiger. Der Nachteil hierbei liegt jedoch im vermehrten Zeitaufwand für Ver- und Entschlüsselung. 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.

5. Geben Sie Ihre Benutzer-ID 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. Beispiel:

   Robert M. Smith <rms@xyzcorp.com>

   Falls Sie keine E-Mail-Adresse haben, können Sie beispielsweise Ihre Telefonnummer oder andere aussagekräftige Daten verwenden, anhand derer sichergestellt werden kann, daß Ihre Benutzer-ID eindeutig ist.

6. Anweisungen zu RSA-fähigen Versionen finden Sie unter Schritt 7.

   Falls Sie sich für die Erstellung eines neuen Unterschriftenschlüssels entschieden haben, geben Sie **y** ein, um einen Verschlüsselungsschlüssel zu erstellen, und wählen anschließend die Größe aus.

   Falls Sie keinen Verschlüsselungsschlüssel erstellen möchten, geben Sie **n** ein, um lediglich einen neuen Unterschriftenschlüssel zu erstellen.

7. Geben Sie eine Paßphrase ein, eine Folge von Zeichen oder Wörtern, die Sie zur Gewährleistung des exklusiven Zugriffs auf Ihren persönlichen Schlüssel verwenden möchten. Weitere Informationen finden Sie im Abschnitt „Erstellen einer einprägsamen Paßphrase“ auf Seite 13.

   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.

8. Sie werden aufgefordert, beliebigen Text einzugeben, damit einige zufällige Bit mit Zufallswerten gesammelt werden können, die für die Erstellung der Schlüssel benötigt werden. Die Eingabe sollte nicht zu schnell und über einen gewissen Zeitraum hinweg erfolgen.

9. Das erzeugte Schlüsselpaar wird auf Ihren öffentlichen und geheimen Schlüsselbunden plaziert.

   Mit der -kx-Befehlsoption können Sie Ihren neuen öffentlichen Schlüssel aus Ihrem öffentlichen Schlüsselbund kopieren und in eine öffentliche Schlüsseldatei plazieren, die sich für die Verteilung an Ihre Freunde eignet. Diese öffentliche Schlüsseldatei können Ihre Freunde in deren öffentliche Schlüsselbunde aufnehmen. Weitere Informationen finden Sie im Abschnitt „Ihren öffentlichen Schlüssel verteilen“ auf Seite 12.

Eigene Schlüssel schützen

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.

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 die privaten und öffentlichen Schlüsselbunde (PUBRING.PKR und SECRING.SKR) gemeinsam mit den anderen Programmdateien in dem Verzeichnis gespeichert, das durch die PGPPATH-Umgebungsvariable definiert wurde. Sicherungskopien können jedoch an jedem beliebigen Speicherort gespeichert werden. Weitere Informationen finden Sie im Abschnitt „PGPPATH: Pfadname für PGP festlegen“ auf Seite 6.

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.

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.

Sie können Ihren öffentlichen Schlüssel auf drei verschiedene Arten verteilen:

- Stellen Sie Ihren öffentlichen Schlüssel über einen Server für öffentliche Schlüssel zur Verfügung.
- Fügen Sie Ihren öffentlichen Schlüssel in eine E-Mail-Nachricht ein.
- 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 Schlüssel-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.

Zusammenfassung von Schlüssel-Server-Befehlen

So extrahieren Sie einen Schlüssel aus Ihrem Schlüsselbund und senden ihn an den Schlüssel-Server

```
pgp -kx <userid> <keyfile> <URL>
```

So fragen Sie einen Schlüssel vom Schlüssel-Server ab und fügen ihn Ihrem Schlüsselbund hinzu (zwei Befehle erforderlich)

```
pgp -kx <userid> <keyfile> <URL>

pgp -ka <keyfile>
```

So entfernen Sie einen Schlüssel aus Ihrem Schlüsselbund bzw. von Ihrem Schlüssel-Server

```
pgp -kr <userid> <URL>
```

So zeigen Sie Schlüssel an, die mit einer bestimmten Benutzer-ID auf dem Schlüssel-Server übereinstimmen

```
pgp -kv <userid> <URL>
```

Beachten Sie, daß die Umgebungsvariable KEYSERVER_URL die URL des standardmäßigen Schlüssel-Servers kennzeichnet, beispielsweise ldap://certserver.pgp.com.

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 stattdessen 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.

Befehlszeilenoptionen in PGP

In der folgenden Tabelle werden die Befehlszeilenoptionen in PGP aufgeführt und beschrieben, die zur Verschlüsselung, Entschlüsselung und Verwaltung von Dateien und Schlüsseln verwendet werden. Im nachfolgenden Abschnitt, „Gängige PGP-Funktionen“ auf Seite 16, erhalten Sie Anweisungen zur Verwendung dieser Optionen von der Befehlszeile aus.

Option	Beschreibung
-a	Konvertiert bei Verwendung mit anderen Optionen (z. B. zum Verschlüsseln oder Unterschreiben) eine Datei in ein ASCII-geschütztes Format (erstellt eine .ASC-Datei).
-c	Verschlüsselt konventionell.
-e	Verschlüsselt mit öffentlichen Schlüsseln.
-f	Verwendet den UNIX-Filtermodus zum Lesen in der Standardeingabe und zum Schreiben in die Standardausgabe.
-g	Zeigt Hilfe zu Gruppenoptionen an. Die Kombinationsmöglichkeiten entnehmen Sie der untenstehenden Tabelle.
-h	Zeigt eine Zusammenfassung der Befehle an.
-k	Zeigt Hilfe zu Schlüsseloptionen an. Die Kombinationsmöglichkeiten für -k entnehmen Sie der untenstehenden Tabelle.
-m	Zeigt Klartextausgabe am Bildschirm an.
-o	Gibt bei Verwendung mit anderen Optionen (z. B. zum Verschlüsseln, Entschlüsseln und Überprüfen von Unterschriften sowie im Filtermodus) den Ausgabedateinamen an.
-p	Stellt den ursprünglichen Klartextdateinamen wieder her.
-s	Unterschreiben
-t	Kennzeichnet die Eingabedatei als Textdatei.
-u	Gibt den Schlüssel an, der zum Unterschreiben verwendet werden soll.
-w	Weist PGP an, die Datei zu löschen.
-z	Identifiziert die Paßphrase in der Befehlzeile.

Die -k-Option zeigt Hilfe zu Schlüsseloptionen an. Sie wird auch in Kombination mit anderen Optionen verwendet. In der folgenden Tabelle werden diese Kombinationsmöglichkeiten aufgeführt und beschrieben.

Option	Beschreibung
-k	Zeigt Hilfe zu Schlüsseloptionen an.
-kg	Erzeugt einen Schlüssel.
-ka	Fügt dem jeweiligen Schlüsselbund Schlüssel hinzu.
-kc	Prüft Unterschriften.
-ke	Bearbeitet Benutzer-ID oder Paßphrase für Ihren geheimen Schlüssel bzw. macht einen vorhandenen Schlüssel zu Ihrem standardmäßigen Unterschriftenschlüssel.
-kr	Entfernt Schlüssel aus dem Schlüsselbund bzw. vom Schlüssel-Server.
-krs	Entfernt Unterschriften, die mit Schlüsseln im Schlüsselbund verknüpft sind.
-ks	Unterschreibt Schlüssel im Schlüsselbund.
-kd	Nimmt Schlüssel im Schlüsselbund zurück oder deaktiviert sie.
-kds	Nimmt Unterschriften zurück, die mit Schlüsseln im Schlüsselbund verknüpft sind.
-kx	Extrahiert Schlüssel aus dem Schlüsselbund und sendet Sie an den Schlüssel-Server.
-kv	Zeigt Schlüssel im Schlüsselbund an.
-kvc	Zeigt die Fingerabdrücke eines Schlüsselsatzes an.
-kw	Zeigt Schlüssel und Unterschriften im Schlüsselbund an.

Die -g-Option wird stets in Kombination mit einer anderen Option verwendet. In der nachfolgenden Tabelle werden diese Kombinationsmöglichkeiten aufgeführt und ihre Verwendungsweise wird erklärt.

Option	Beschreibung
-g	Zeigt Hilfe zu Gruppenoptionen an.
-ga	Fügt Gruppen Elemente hinzu.
-gr	Entfernt Elemente aus Gruppen.
-gv	Zeigt Gruppen an.
-gvv	Zeigt Gruppen und die darin enthaltenen Schlüssel an. Standardmäßig werden sämtliche Gruppen und die Schlüssel angezeigt, aus denen sie bestehen.

PGP-Konfigurationsparameter in der Befehls zeile eingeben

Beachten Sie, daß sämtliche in Kapitel 4, „PGP-Konfigurationsdatei“ beschriebenen Konfigurationsparameter von PGP in der Befehlszeile als lange Optionen eingegeben werden können (z. B. +fastkeygen oder +passthrough).

Gängige PGP-Funktionen

In diesem Abschnitt werden gängige PGP-Funktionen in folgenden Kategorien beschrieben:

- Erstellen, Deaktivieren, erneutes Aktivieren und Zurücknehmen von Schlüsseln
- Verschlüsseln und Entschlüsseln von Nachrichten
- Löschen von Text
- Unterschreiben von Nachrichten
- Angeben von Dateitypen
- Befehle zur Schlüsselwartung

Beachten Sie, daß [Klammern] ein optionales Feld bezeichnen; die Klammern müssen nicht eingegeben werden.

Schlüssel erstellen, deaktivieren, erneut aktivieren und zurücknehmen

Schlüsselpaare erstellen

Wenn Sie Ihr persönliches Paar aus öffentlichen und geheimen Schlüsseln erstellen möchten, geben Sie folgendes in der Befehlszeile ein:

```
pgp -kg
```

Schlüssel zurücknehmen

Wenn Sie Ihren persönlichen Schlüssel dauerhaft zurücknehmen möchten, stellen Sie ein Schlüsselrücknahmezertifikat aus:

```
pgp -kd <your_userid>
```

Schlüssel deaktivieren oder erneut aktivieren

So deaktivieren bzw. aktivieren Sie einen öffentlichen Schlüssel in Ihrem persönlichen öffentlichen Schlüsselbund erneut:

```
pgp -kd <userid>
```

Nachrichten ver- und entschlüsseln

Nachrichten entschlüsseln bzw. Unterschriftenintegrität unterschriebener Dateien prüfen

pgp <ciphertext_filename> [-o plaintext_filename]

Nachrichten entschlüsseln und ursprüngliche Klartext-Dateinamen wiederherstellen

pgp -p <ciphertext_filename>

Weitere Informationen finden Sie im Abschnitt „Nachrichten entschlüsseln und ursprüngliche Klartext-Dateinamen wiederherstellen“ auf Seite 29.

Nachrichten entschlüsseln und Klartextausgabe am Bildschirm anzeigen

pgp -m <ciphertext_filename>

Die Ausgabe ist vergleichbar mit dem „More“-Befehl unter UNIX. Sie wird nicht in eine Datei geschrieben. Weitere Informationen finden Sie im Abschnitt „Nachrichten entschlüsseln und Klartextausgabe am Bildschirm anzeigen“ auf Seite 29.

ASCII-geschützte Nachrichten entschlüsseln

pgp <ASCII-armored_message>

Dieser Befehl entschlüsselt ASCII-geschützte Nachrichten. PGP konvertiert die jeweilige Nachricht in ein binäres Format. Anschließend wird zuerst eine Datei mit chiffriertem Text mit der Endung .PGP im Binärformat erstellt und dann die Ausgabedatei in Klartext. Weitere Informationen finden Sie im Abschnitt „ASCII-geschützte Nachrichten entschlüsseln“ auf Seite 26.

Nachrichten entschlüsseln, aus Standardeingabe lesen und in Standardausgabe schreiben

pgp -feast <recipients_userid> <<input_filename> ><output_filename>

Weitere Informationen finden Sie im Abschnitt „PGP als UNIX-Filter verwenden“ auf Seite 24.

Klartextdateien ausschließlich mit konventioneller Verschlüsselung verschlüsseln

pgp -c <plaintext_filename>

Klartextdateien mit dem öffentlichen Schlüssel des Empfängers verschlüsseln

pgp -e <plaintext_filename> <recipients_userid>

Nachrichten für beliebige Anzahl von Empfängern verschlüsseln

pgp -e <textfile-filename> <userid1> <userid2> <userid3>

Nachrichten zur ausschließlichen Anzeige durch den Empfänger verschlüsseln

Mit diesem Befehl können Sie festlegen, daß der vom Empfänger entschlüsselte Klartext lediglich am Bildschirm des Empfängers angezeigt und nicht auf Festplatte gespeichert werden kann.

pgp -sem <message.txt> <recipients_userid>

Weitere Informationen finden Sie unter „Zur ausschließlichen Anzeige durch den Empfänger verschlüsseln“ auf Seite 30.

Festplatte bereinigen

Ursprüngliche Klartextdateien löschen

pgp -ew <message.txt> <recipients_userid>

PGP löscht die Klartextdatei, nachdem die Datei mit dem chiffrierten Text erstellt wurde.

- Hinzufügen der -w (Löschen)-Option bei der Verschlüsselung.
- Hinzufügen der -m (More)-Option bei der Entschlüsselung.

Weitere Informationen finden Sie im Abschnitt „Festplatte bereinigen“ auf Seite 30.

Nachrichten unterschreiben

Klartextdateien mit geheimem Schlüssel unterschreiben und mit öffentlichem Schlüssel des Empfängers verschlüsseln

pgp -es <plaintext filename> <recipients_userid> [-u your_userid]

Klartextdateien mit Ihrem geheimen Schlüssel unterschreiben

pgp -s <plaintext_filename> [-u your_userid]

Klartext-Textdateien im ASCII-Format unterschreiben

pgp -sta <plaintext_filename> [-u your_userid]

PGP unterschreibt die jeweilige Klartext-Textdatei im ASCII-Format mit Ihrem geheimen Schlüssel und erstellt eine unterschriebene Klartextnachricht, die für den E-Mail-Einsatz geeignet ist.

Dateitypen angeben

Dateien mit chiffriertem Text im ASCII-geschützten-64-Format erstellen

pgp -sea <plaintext_filename> <recipients_userid>

oder

pgp -kxa <userid> <keyfile> [keyring]

Sie können die generierte Datei über 7-Bit-Kanäle in ein Textverarbeitungsprogramm laden, um sie als normale E-Mail senden zu können.

Fügt die -a-Option hinzu, wenn Sie eine Nachricht verschlüsseln oder unterschreiben bzw. einen Schlüssel extrahieren. Weitere Informationen finden Sie unter „Binäre Daten verschlüsseln und übertragen“ auf Seite 25.

Klartext-Dateien im ASCII-Format erstellen

pgp -seat <message.txt> <recipients_userid>

Die Datei wird gemäß der lokalen Textzeilenkonventionen des jeweiligen Empfängers konvertiert.

Fügt die -t (Text)-Option anderen Optionen hinzu.

Befehle zur Schlüsselwartung

Inhalt von öffentlichen bzw. geheimen Schlüsseldateien Ihrem öffentlichen bzw. geheimen Schlüsselbund hinzufügen

pgp -ka <keyfile> [keyring]

Schlüssel aus Ihrem öffentlichen oder geheimen Schlüsselbund kopieren

pgp -kx <userid> <keyfile> [keyring]

oder:

pgp -kxa <userid> <keyfile> [keyring]

Schlüssel vom Schlüssel-Server abfragen und Ihrem Schlüsselbund hinzufügen (zwei Befehle erforderlich)

pgp -kx <userid> <keyfile> <URL>

pgp -ka <keyfile>

Ein Beispiel für eine URL: ldap://certserver.pgp.com

Inhalt Ihres öffentlichen Schlüsselbunds anzeigen

pgp -kv[v] [userid] [keyring]

Alle an einzelne Schlüssel angehängte zertifizierende Unterschriften anzeigen

pgp -kvv [userid] [keyring]

Fingerabdrücke öffentlicher Schlüssel anzeigen

pgp -kvc [userid] [keyring]

PGP zeigt den „Fingerabdruck“ eines öffentlichen Schlüssels an. Dadurch wird dessen telefonische Überprüfung mit dem Eigentümer des Schlüssels erleichtert. Weitere Informationen zu Fingerabdrücken finden Sie unter „Die Echtheit eines öffentlichen Schlüssels über das Telefon verifizieren“ auf Seite 33.

Inhalt Ihres öffentlichen Schlüsselbunds anzeigen und zertifizierende Unterschriften prüfen

pgp -kc [your_userid] [keyring]

Weitere Informationen hierzu finden Sie unter „Inhalt Ihres öffentlichen Schlüsselbunds verifizieren“ auf Seite 32.

Sämtliche Schlüssel in einem bestimmten Schlüsselbunddateinamen anzeigen

pgp <keyring_filename>

PGP zeigt sämtliche Schlüssel in einem bestimmten Schlüsselbunddateinamen an. Wenn Sie diesen Befehl verwenden, listet PGP sämtliche Schlüssel in der Datei KEYFILE.PGP auf und versucht außerdem, sie Ihrem Schlüsselbund hinzuzufügen, falls dies noch nicht geschehen ist.

Benutzer-IDs oder Paßphrasen für Ihren geheimen Schlüssel bearbeiten bzw. vorhandene Schlüssel als Ihre standardmäßigen Unterschriftenschlüssel definieren

pgp -ke <userid> [keyring]

Vertrauensparameter für öffentliche Schlüssel bearbeiten

pgp -ke <userid> [keyring]

Weitere Informationen hierzu finden Sie unter „Vertrauensparameter für öffentliche Schlüssel bearbeiten“ auf Seite 32.

Schlüssel oder Benutzer-IDs aus Ihrem öffentlichen Schlüsselbund entfernen

pgp -kr <userid> [keyring]

Wenn Sie eine Schlüsselbunddatei angeben, versucht PGP, diese Datei sowie die entsprechende öffentliche bzw. private Schlüsselbunddatei zu öffnen. Falls die zu löschende Benutzer-ID zu einem Schlüssel gehört, der sowohl einen öffentlichen als auch einen privaten Schlüssel aufweist, werden Sie gefragt, ob der private Schlüssel ebenfalls gelöscht werden soll. Wenn Sie die Option „Nein“ wählen, wird kein Löschvorgang durchgeführt.

Ausgewählte Unterschriften aus Benutzer-ID in Schlüsselbund entfernen

pgp -krs <userid> [keyring]

Öffentliche Schlüssel anderer Benutzer in Ihrem öffentlichen Schlüsselbund unterschreiben und zertifizieren

pgp -ks <recipients_userid> [-u your_userid] [keyring]

Unterschriftenzertifikate erstellen

Separate Unterschriftenzertifikate erstellen

pgp -sb <plaintext_filename> [-u your_userid]

Weitere Informationen finden Sie im Abschnitt „Getrenntes Unterschriften-zertifikat und Textdateien erstellen“ auf Seite 28.

Zusammenfassung von Befehlen

Wenn Sie eine kurze Zusammenfassung der Befehlsverwendung in PGP anzeigen lassen möchten, geben Sie folgendes in der Befehlszeile ein:

pgp -h

Vorgänge abbrechen

Wenn Sie den aktuellen Vorgang abbrechen möchten, betätigen Sie in einer beliebigen Eingabeaufforderung die Tastenkombination Strg-C.

Wenn Sie einen Vorgang abbrechen möchten, dessen Durchführung mehr Zeit in Anspruch nimmt, können Sie zu jedem beliebigen Zeitpunkt die Tasten-kombination Strg-C betätigen.

Weiterführende Themen 3

In diesem Kapitel werden weiterführende PGP-Themen und -Befehle beschrieben:

- Stammverzeichnis kennzeichnen.
- PGP nicht interaktiv von UNIX-Shell-Skripten oder MSDOS-Stapelverarbeitungsdateien aus verwenden.
- PGP als UNIX-Filter verwenden.
- Binäre Daten verschlüsseln und übertragen.
- ASCII-Dateien an andere Rechnerumgebungen senden.

Stammverzeichnis kennzeichnen: HOME

Nur UNIX. Diese Umgebungsvariable kennzeichnet das Stammverzeichnis des Benutzers.

PGP nicht interaktiv von UNIX-Shell-Skripten oder MSDOS-Stapelverarbeitungsdateien aus verwenden

MSDOS bezieht sich auf die Windows NT-Eingabeaufforderung.

Unwichtige Fragen unterdrücken: BATCHMODE

Wenn das Kennzeichen BATCHMODE in der Befehlszeile aktiviert ist, werden von PGP keine unwichtigen Fragen gestellt, und Sie werden nicht zur Eingabe von alternativen Dateinamen aufgefordert:

```
pgp +batchmode <ciphertext_filename>
```

Diese Variable ist sehr hilfreich, wenn PGP von Shell-Skripten oder Stapelverarbeitungsdateien aus ausgeführt wird. Wenn BATCHMODE aktiviert ist (ON), wird für manche Schlüsselverwaltungsbefehle noch immer die Interaktion mit dem Benutzer benötigt, so daß bei der Verwendung von Shell-Skripten diese Befehle besser vermieden werden sollten.

Sie können BATCHMODE auch aktivieren, um die Gültigkeit einer Unterschrift in einer Datei zu überprüfen:

- Enthält die Dateien keine Unterschrift, beträgt der Beendigungscode 1.
- Enthält die Datei eine gültige Unterschrift, beträgt der Beendigungscode 0.

Bestätigungsfragen vermeiden: FORCE

Wenn Sie PGP anweisen, eine vorhandene Datei zu überschreiben oder einen Schlüssel aus einem Schlüsselbund zu entfernen (mit dem -kr-Befehl), müssen Sie den jeweiligen Vorgang bestätigen.

Zur nicht interaktiven Ausführung von PGP von einem UNIX-Shell-Skript oder einer MSDOS-Stapelverarbeitungsdatei aus können Sie PGP mit der FORCE-Option anweisen, immer anzunehmen, die Antwort auf eine Frage sei „Ja“, wenn PGP eine Bestätigung benötigt.

pgp +force <ciphertext_filename>

oder:

pgp -kr +force <your_userid>

PGP-Beendigungsstatuscodes

Wenn PGP im Stapelverarbeitungsmodus ausgeführt wird (z. B. von einer MSDOS-Datei [.bat] oder von einem UNIX-Shell-Skript aus), gibt PGP einen fehlerhaften Beendigungsstatus an die Shell zurück.

- Ein Beendigungsstatuscode von Null bedeutet eine normale Ausgabe.
- Beträgt der Beendigungsstatuscode nicht Null, ist ein Fehler aufgetreten. Unterschiedliche Fehlerbedingungen für die Beendigung geben verschiedene Beendigungsstatuscodes an die Shell zurück.

PGP als UNIX-Filter verwenden

UNIX verwendet Pipes, damit zwei Anwendungen zusammenarbeiten können. Die Ausgabe einer Anwendung kann direkt durch eine Pipe übertragen werden, um als Eingabe von einer anderen Anwendung gelesen zu werden. Damit dieser Vorgang funktioniert, müssen die Anwendungen die Fähigkeit haben, das Originalmaterial aus „Standardeingabe“ zu lesen und anschließend die fertigen Ausgabedaten in „Standardausgabe“ zu schreiben.

Um den UNIX-Filtermodus von PGP zum Lesen aus der Standardeingabe und zum Schreiben in die Standardausgabe zu verwenden, müssen Sie die -f-Option hinzufügen:

pgp -feast <recipients_userid> <<input_filename> ><output_filename>

Mit dieser Funktion wird die Verwendung von PGP mit E-Mail-Anwendungen vereinfacht.

Wenn Sie den Filtermodus von PGP verwenden, um eine Datei mit chiffriertem Text zu entschlüsseln, ist die Umgebungsvariable PGPPASS unter Umständen hilfreich. Diese Variable enthält die Paßphrase, so daß Sie von PGP nicht zur Eingabe dieser Information aufgefordert werden. Weitere Informationen finden Sie im Abschnitt „PGPPASS: Eigene Paßphrase speichern“ auf Seite 34.

Binäre Daten verschlüsseln und übertragen

Bei vielen E-Mail-Systemen sind nur Nachrichten mit Text im ASCII-Format zulässig. Aus diesem Grund unterstützt PGP ein ASCII-geschütztes Format für Nachrichten mit chiffriertem Text (ähnlich wie MIME).

Mit diesem Format, in dem binäre Daten ausschließlich durch druckbare ASCII-Zeichen dargestellt werden, können Sie binäre, verschlüsselte Daten über 7-Bit-Kanäle übertragen oder sie als normalen E-Mail-Text versenden. Das ASCII-geschützte Format von PGP hat die Funktion eines „Transportschutzes“, der die Nachricht bei der Übertragung durch die Gateways zwischen den Systemen im Internet vor Beschädigungen schützt. PGP hängt ebenfalls eine CRC an, um Übertragungsfehler zu erkennen.

Das ASCII-geschützte Format konvertiert den Klartext, indem Gruppen von 3 Binärbyte mit 8 Bit auf vier druckbare ASCII-Zeichen erweitert werden. Die Datei wird um etwa 33% vergrößert. Diese Erweiterung wird jedoch durch die Komprimierung ausgeglichen, die vor der Verschlüsselung vorgenommen wird.

Um eine Datei im ASCII-geschützten Format zu erstellen, geben Sie den folgenden Befehl ein:

pgp -ea <plaintext_filename> <recipients_userid>

Mit diesem Befehl wird PGP angewiesen, eine Datei mit chiffriertem Text im ASCII-geschützten Format mit dem Namen MESSAGE.ASC zu erstellen. Diese Datei enthält Daten im ASCII-geschützten Format, das MIME ähnelt. Sie können die Datei über 7-Bit-Kanäle in ein Textverarbeitungsprogramm laden oder sie als normale E-Mail senden.

Die meisten E-Mail-Funktionen lassen Nachrichten mit mehr als 50.000 oder 65.000 Byte nicht zu. Längere Nachrichten werden in kleinere Dateien unterteilt. Wenn Sie für eine größere Datei das ASCII-geschützte Format anfordern, wird die Datei von PGP in kleinere Dateien mit den Dateinamenerweiterungen .AS1, .AS2, .AS3 usw. unterteilt.

Dateien mit binären Daten im ASCII-geschützten Format ohne Verschlüsselung oder Unterschrift senden

Mit der -a-Option von PGP können Sie Dateien in das ASCII-geschützte Format konvertieren. Es ist keine Verschlüsselung bzw. kein Unterschreiben nötig, so daß weder der Absender noch der Empfänger einen Schlüssel benötigt. Bei Verwendung der -a-Option unterteilt PGP große Dateien in kleinere Dateien, die über E-Mail gesendet werden können, versucht die Daten vor der Konvertierung in das ASCII-geschützte Format zu komprimieren und hängt jeder kleineren Datei einen CRC-Fehlererkennungscode an. Verwenden Sie den Befehl folgendermaßen:

pgp -a <binary_filename>

Dieser Befehl gibt PGP die Anweisung, eine ASCII-geschützte Datei mit dem Namen FILENAME.ASC zu erstellen. Der Empfänger verwendet die -p-Option, um die Nachricht zu öffnen und den ursprünglichen Dateinamen des Senders wiederherzustellen.

ASCII-geschützte Nachrichten entschlüsseln

Um eine Nachricht im ASCII-geschützten Format zu entschlüsseln, geben Sie den folgenden Befehl ein:

pgp <ASCII-armored_filename>

PGP erkennt, daß die Datei im ASCII-geschützten Format vorliegt, konvertiert die Datei zurück in das binäre Format (durch Erstellung einer Binärdatei mit chiffriertem Text mit der Erweiterung .PGP) und erstellt eine Ausgabedatei in der normalen Klartextform.

Wenn die ursprüngliche Nachricht ausführlich war und in verschiedenen kleineren Dateien abgeschickt wurde, müssen Sie die Dateien in der richtigen Reihenfolge zu einer Datei verknüpfen, bevor Sie die Nachricht entschlüsseln. Wenn mit PGP Nachrichten entschlüsselt werden, wird unwesentlicher Text im Kopf der Mail ignoriert, wenn dieser nicht in den ASCII-geschützten Nachrichtenblöcken enthalten ist.

Öffentlichen Schlüssel im ASCII-geschützten Format senden

Um einen öffentlichen Schlüssel an einen anderen Benutzer im ASCII-geschützten Format zu senden, fügen Sie die -a-Option hinzu, während Sie den Schlüssel von Ihrem Schlüsselbund extrahieren.

Wenn Sie nicht daran gedacht haben, die -a-Option zur Erstellung einer Datei mit chiffriertem Text oder zum Extrahieren eines Schlüssels zu verwenden, können Sie die Binärdatei mit der -a-Option in das ASCII-geschützte Format konvertieren (keine Verschlüsselung angeben). PGP konvertiert die Datei in eine .ASC-Datei.

ASCII-Textdateien an andere Umgebungen für Rechner senden

Mit PGP können Sie alle Klartextdateien, Binärdaten mit 8 Bit oder alle ASCII-Texte verschlüsseln. Am häufigsten wird PGP für E-Mail verwendet. Hierbei handelt es sich um ASCII-Text.

ASCII-Text wird auf verschiedenen Rechnern unterschiedlich angezeigt. Auf einem MSDOS-System beispielsweise werden alle Zeilen, die ASCII-Text enthalten, mit Zeilenumbruch und anschließendem Zeilenvorschub beendet. Auf einem UNIX-System enden alle Zeilen nur mit einem Zeilenvorschub. Auf einem Macintosh enden alle Zeilen nur mit einem Zeilenumbruch.

Normale unverschlüsselte ASCII-Textnachrichten werden zur Übertragung von einem Rechner auf einen anderen häufig automatisch in eine gängige „kanonische“ Form übersetzt. Kanonischer Text endet an jeder Textzeile mit einem Zeilenumbruch und einem Zeilenvorschub.

Verschlüsselter Text kann nicht automatisch mit einem Kommunikationsprotokoll konvertiert werden, da der Klartext durch Verschlüsselung unkenntlich ist. Zur Behebung dieses Problems haben Sie mit der t-Option die Möglichkeit festzulegen, daß Klartext als ASCII-Text angesehen und kanonischer Text vor der Verschlüsselung konvertiert wird. Beim Empfang der Nachricht wird der entschlüsselte Klartext automatisch in die geeignete Textform für die lokale Umgebung konvertiert.

Geben Sie für die Verwendung dieser Funktion bei der Verschlüsselung oder beim Unterschreiben einer Nachricht die t-Option ein.

pgp -et <plaintext_filename> <recipients_userid>

Wenn PGP in der Klartextdatei auf binäre Daten stößt, die nicht im Textformat vorliegen, wird die t-Option ignoriert.

PGP enthält eine Umgebungsvariable, die der t-Option TEXTMODE entspricht. Wenn Sie fortwährend Klartextdateien anstelle von binären Daten empfangen, dann nehmen Sie die Einstellung TEXTMODE=ON vor.

Unterschriftenzertifikat verwalten

Getrenntes Unterschriftenzertifikat und Textdateien erstellen

In den meisten Fällen sind die Unterschriftenzertifikate physischer Anhang des zu unterschreibenden Textes. Dadurch ist die Unterschriftenverifizierung sehr unkompliziert. Sie können jedoch eine separate Unterschriftenzertifikatsdatei erstellen und anschließend beide Dateien (die Textdatei und die Unterschriftenzertifikatsdatei) an den Empfänger senden. Diese Funktion ist nützlich, wenn mehrere Parteien ein Dokument ohne Unterschrifteneinbettung, wie beispielsweise einen Vertrag, unterschreiben müssen. Die Unterschriften aller Personen sind voneinander unabhängig.

Kombinieren Sie die b- (unterteilen) mit der s (unterschreiben)-Option, um eine separate Unterschriftenzertifikatsdatei zu erstellen. Geben Sie den folgenden Befehl ein:

pgp -sb <plaintext_filename> [-u <your_userid>]

Mit diesem Befehl weisen Sie PGP an, ein separates Unterschriftenzertifikat in einer Datei mit dem Namen LETTER.SIG zu erstellen. Der Inhalt der Datei LETTER.SIG wird nicht als Anhang von <LETTER.TXT> behandelt.

Separate Unterschriftenzertifikate und Textdateien empfangen

Wenn Sie versuchen, eine Unterschriftenzertifikatsdatei zu verarbeiten, werden Sie von PGP aufgefordert, die entsprechende Textdatei anzugeben. PGP überprüft die Unterschriftenintegrität der angegebenen Textdatei.

Wenn Ihnen bekannt ist, daß eine separate Unterschriften- und eine Textdatei vorhanden sind, können Sie beide Dateinamen in der Befehlszeile eingeben.

pgp <letter.sig> <letter.txt>

oder

pgp <letter> <letter.txt>

Dateiverwaltungsbefehle

Nachrichten entschlüsseln und Klartextausgabe am Bildschirm anzeigen

Zur Anzeige entschlüsselter Klartextausgabe am Bildschirm (vergleichbar mit dem More-Befehl unter UNIX), ohne das Schreiben der Ausgabe in eine Datei, verwenden Sie für die Entschlüsselung die -m (More)-Option.

pgp -m <ciphertext_filename>

Dieser Befehl weist PGP an, den entschlüsselten Klartext nacheinander am Bildschirm anzuzeigen.

Nachrichten entschlüsseln und die Ausgabe der Klartextdatei umbenennen

Wird mit PGP eine Klartextdatei verschlüsselt, wird der ursprüngliche Dateiname gespeichert und dem Klartext angehängt, bevor dieser komprimiert und verschlüsselt wird. Wird eine Datei mit chiffriertem Text von PGP entschlüsselt, wird die Klartextausgabedatei mit einem ähnlichen Namen versehen (jedoch ohne Dateinamenerweiterung).

Mit der -o-Option in der Befehlszeile können Sie einen aussagekräftigeren Klartext-Dateinamen für die Ausgabe angeben:

pgp -o <ciphertext_filename> <new_plaintext_filename>

Nachrichten entschlüsseln und ursprüngliche Klartext-Dateinamen wiederherstellen

Wie im obigen Abschnitt erläutert, wird bei der Verschlüsselung einer Klartextdatei der ursprüngliche Dateiname gespeichert und dem Klartext angehängt, bevor dieser komprimiert und verschlüsselt wird. Mit der -p-Option können Sie PGP anweisen, den ursprünglichen Klartext-Dateinamen beizubehalten und diesen als Namen der entschlüsselten Klartextausgabedatei zu verwenden.

pgp -p <ciphertext_filename>

Schlüssel vom Schlüssel-Server löschen

pgp -kr <userid> <URL>

Beispiel für eine URL: ldap:/ /certserver.pgp.com.

Zur ausschließlichen Anzeige durch den Empfänger verschlüsseln

Sie können durch Hinzufügen der -m-Option festlegen, daß der vom Empfänger entschlüsselte Klartext lediglich am Bildschirm des Empfängers angezeigt und nicht auf Festplatte gespeichert werden kann.

pgp -sem <message.txt> <recipients_userid>

Wenn der Empfänger den chiffrierten Text mit dem entsprechenden geheimen Schlüssel und der Paßphrase entschlüsselt, wird der Klartext am Bildschirm des Empfängers angezeigt, jedoch nicht auf Festplatte gespeichert. Der Text wird Bildschirm nach Bildschirm angezeigt, als würde der Empfänger den More-Befehl unter UNIX verwenden. Wenn der Empfänger die Nachricht noch einmal durchlesen möchte, muß der chiffrierte Text ein zweites Mal entschlüsselt werden.

Diese Funktion ist optimal um sicherzustellen, daß vertrauliche Nachrichten nicht versehentlich auf der Festplatte des Empfängers vergessen werden.

Beachten Sie, daß mit dieser Funktion nicht verhindert werden kann, daß eine schlaue, hartnäckige Person einen Weg findet, den entschlüsselten Klartext auf Festplatte zu speichern. Diese Funktion wurde entwickelt, um den gelegentlichen Benutzer von einem versehentlichen Speichern abzuhalten.

Unterschriebene Dateien speichern: Unterschreiben einer Datei ohne Verschlüsselung

Wenn Sie eine Klartextdatei speichern, ohne eine Verschlüsselung anzugeben, wird die Datei von PGP komprimiert, nachdem Sie sie unterschrieben haben. Dadurch ist die Datei für den gelegentlichen Benutzer nicht lesbar. Das ist eine geeignete Art und Weise, unterschriebene Dateien in Archivanwendungen zu speichern.

Festplatte bereinigen

Nachdem von PGP eine Datei mit chiffriertem Text erstellt wurde, können Sie PGP so einstellen, daß die Klartextdatei automatisch überschrieben und gelöscht und somit jede Spur des Klartextes auf der Festplatte beseitigt wird. Verwenden Sie die w-Option, wenn die Klartextdatei vertrauliche Informationen enthält. Hiermit wird verhindert, daß die Datei mit einem Dienstprogramm zum Scannen von Festplattenblöcken wiederhergestellt werden kann.

Verwenden Sie die w-Option, wenn Sie eine Nachricht verschlüsseln und unterschreiben:

pgp -ew <message.txt> <recipients_userid>

Mit diesem Befehl wird PGP angewiesen, die Datei MESSAGE.PGP mit chiffriertem Text zu erstellen, und die Klartextdatei MESSAGE.TXT zu löschen.

Beachten Sie, daß mit dieser Option keine Klartextfragmente gelöscht werden, die möglicherweise vom Textverarbeitungsprogramm auf der Festplatte erstellt wurden, während Sie die Nachricht vor Ausführung von PGP bearbeitet haben. Die meisten Textverarbeitungsprogramme erstellen Sicherungsdateien, Arbeitsdateien oder beides.

PGP überschreibt die Datei 26 Mal.

Schlüsselverwaltungsbefehle

Eigene Benutzer-ID oder Paßphrase bearbeiten bzw. einen vorhandenen Schlüssel als Ihren standardmäßigen Unterschriftenschlüssel definieren

Sie müssen möglicherweise Ihre Paßphrase ändern, da Ihnen vielleicht jemand bei der Eingabe über die Schulter gesehen hat. Möglicherweise müssen Sie Ihre Benutzer-ID ändern, da Sie Ihren Namen oder Ihre E-Mail-Adresse geändert haben. Vielleicht müssen Sie eine zweite oder dritte Benutzer-ID hinzufügen, da Sie unter mehreren Namen, E-Mail-Adressen oder Berufsbezeichnungen geführt werden. In PGP können Sie Ihrem Schlüssel mehrere Benutzer-IDs anhängen, von denen alle zur Suche nach Ihrem Schlüssel im Schlüsselbund verwendet werden können. Sie müssen möglicherweise auch einen der vorhandenen Schlüssel zu Ihrem standardmäßigen Unterschriftenschlüssel bestimmen.

Zum Bearbeiten Ihrer Benutzer-ID oder Paßphrase für Ihren geheimen Schlüssel bzw. zur Definition eines vorhandenen Schlüssels als Ihren standardmäßigen Unterschriftenschlüssel verwenden Sie den folgenden Befehl:

pgp -ke <your_userid> [keyring]

Sie werden von PGP zur Eingabe einer neuen Benutzer-ID oder einer neuen Paßphrase aufgefordert.

Bei der Bearbeitung Ihrer Benutzer-ID fügt PGP eine neue Benutzer-ID hinzu, ohne die alte zu löschen. Das Löschen einer alten Benutzer-ID muß separat erfolgen.

Wenn Sie sich dazu entschließen, den Schlüssel als vollständig autorisierter Schlüsselverwalter zu verwenden, können Sie den Schlüssel als Ihren standardmäßigen Unterschriftenschlüssel definieren.

Falls ein optionaler Parameter [Schlüsselbund] vorhanden ist, muß es sich dabei um einen öffentlichen und nicht um einen geheimen Schlüsselbund handeln. Das Feld „Benutzer-ID“ muß die Benutzer-ID enthalten, die PGP als Ihre eigene bekannt ist, da diese sowohl in Ihrem öffentlichen als auch in Ihrem geheimen Schlüsselbund vorkommt. Beide Schlüsselbunde werden aktualisiert, auch wenn Sie nur den öffentlichen Schlüsselbund angegeben haben.

Sie können ebenfalls den -ke-Befehl verwenden, um die Vertrauensparameter für einen öffentlichen Schlüssel zu bearbeiten. Informationen finden Sie im Abschnitt „Vertrauensparameter für öffentliche Schlüssel bearbeiten“ auf Seite 32.

Vertrauensparameter für öffentliche Schlüssel bearbeiten

Zum Bearbeiten der Vertrauensparameter eines öffentlichen Schlüssels in Ihrem Schlüsselbund geben Sie den folgenden Befehl ein:

pgp -ke <userid> [keyring]

Falls ein optionaler Parameter [Schlüsselbund] vorhanden ist, muß es sich dabei um einen öffentlichen und nicht um einen geheimen Schlüsselbund handeln.

Inhalt Ihres öffentlichen Schlüsselbunds verifizieren

Alle neuen Schlüssel oder Unterschriften in Ihrem öffentlichen Schlüsselbund werden von PGP automatisch überprüft, und alle Vertrauensparameter und Gültigkeitsauswertungen werden aktualisiert. Theoretisch werden alle Statusinformationen zur Schlüsselgültigkeit auf dem neuesten Stand gehalten, wenn Ihrem öffentlichen Schlüsselbund Material hinzugefügt oder daraus gelöscht wird.

An einem gewissen Punkt möchten Sie PGP jedoch möglicherweise dazu auffordern, eine umfassende Analyse Ihres öffentlichen Schlüsselbundes durchzuführen, alle zertifizierenden Unterschriften zu überprüfen, die Vertrauensparameter zu überprüfen, alle Gültigkeitsauswertungen zu aktualisieren und Ihren eigenen vollständig autorisierten Schlüssel mit einer Sicherungskopie auf einer schreibgeschützten Diskette zu vergleichen. Es ist ratsam, diese bereinigenden Wartungsmaßnahmen in regelmäßigen Abständen durchzuführen, um sicherzustellen, daß mit Ihrem öffentlichen Schlüsselbund alles in Ordnung ist.

Um von PGP eine vollständige Analyse der öffentlichen Schlüsselbunde durchführen zu lassen, verwenden Sie den -kc-Befehl (Schlüsselbundüberprüfung):

pgp -kc

Sie können ebenfalls den folgenden Befehl verwenden, damit PGP die Überprüfung aller Unterschriften für einen ausgewählten öffentlichen Schlüssel durchführt:

pgp -kc <your_userid> [keyring]

Weitere Informationen zur Überprüfung der Sicherungskopie Ihres eigenen Schlüssels finden Sie in „CERT_DEPTH: Tiefe der einzubettenden Schlüsselverwalter“ auf Seite 39.

Die Echtheit eines öffentlichen Schlüssels über das Telefon verifizieren

Wenn Sie einen öffentlichen Schlüssel von einer Person erhalten, die nicht von einer Person Ihres Vertrauens zertifiziert wurde, wie können Sie dann sichergehen, daß der Schlüssel wirklich der Person gehört? Wenn Ihnen der Eigentümer des Schlüssel bekannt ist und Sie dessen Stimme am Telefon erkennen würden, rufen Sie die entsprechende Person an, und verifizieren Sie den Fingerabdruck des Schlüssels über Telefon. Hierfür müssen Sie und auch der Eigentümer des Schlüssels den -kvd-Befehl verwenden, um den Fingerabdruck des Schlüssels anzuzeigen:

pgp -kvc <userid> [keyring]

Durch diesen Befehl wird PGP angewiesen, den Schlüssel mit dem Nachrichtenkern von 32 Zeichen der öffentlichen Schlüsselkomponenten anzuzeigen (Diffie-Hellman-Schlüssel haben Fingerabdrücke mit 40 Zeichen). Lesen Sie den Fingerabdruck des Schlüsseleigentümers, um zu überprüfen, ob die Fingerabdrücke übereinstimmen.

Mit diesem Verfahren können Sie unbesorgt gegenseitig Schlüssel verifizieren und unterschreiben. So können Sie auf sichere und bequeme Art und Weise ein Netzwerk mit vertrauenswürdigen Schlüsseln für Ihren Freundeskreis aufbauen.

Denken Sie daran, daß das Senden eines Schlüsselfingerabdrucks über E-Mail nicht der beste Weg ist, einen Schlüssel zu verifizieren, da eine E-Mail abgefangen und geändert werden kann. Am besten verwendet man für das Senden des Fingerabdrucks einen anderen Kanal als für das Senden des Schlüssels selbst. Eine sichere Kombination ist gewährleistet, wenn Sie den Schlüssel in einer E-Mail senden und den Schlüsselfingerabdruck in einem Telefongespräch weitergeben. Manche Personen verteilen ihre Schlüsselfingerabdrücke auf ihren Visitenkarten.

Schlüssel mit der Schlüssel-ID auswählen

In den meisten Fällen geben Sie eine Benutzer-ID oder ein Bruchstück einer Benutzer-ID ein, um einen Schlüssel auszuwählen. Sie können zur Auswahl eines Schlüssels jedoch auch die hexadezimale Schlüssel-ID eingeben. Geben Sie anstelle der Benutzer-ID eine Schlüssel-ID mit dem Präfix „0x“ ein:

pgp -kv 0x67F796C2

Mit diesem Befehl weisen Sie PGP an, alle Schlüssel anzuzeigen, deren Schlüssel-IDs 67F796C2 beinhalten.

Diese Funktion ist besonders hilfreich, wenn Sie von einer Person zwei verschiedene Schlüssel mit derselben Benutzer-ID vorliegen haben. Sie können den richtigen Schlüssel durch Angabe der bestimmten Schlüssel-ID herausfinden.

PGPPASS: Eigene Paßphrase speichern

Wenn PGP eine Paßphrase benötigt, um einen geheimen Schlüssel zu entsperren, werden Sie zur Eingabe Ihrer Paßphrase aufgefordert. Verwenden Sie die in der Befehlszeile eingegebene Umgebungsvariable PGPPASS zum Speichern Ihrer Paßphrase. Wenn von PGP eine Paßphrase benötigt wird, wird die Verwendung der gespeicherten Paßphrase versucht. Handelt es sich bei der gespeicherten Paßphrase um eine falsche Paßphrase, werden Sie zur Eingabe Ihrer richtigen Paßphrase aufgefordert.

SET PGPPASS=zaphod beeblebrox for president

Das oben aufgeführte Beispiel würde die Eingabeaufforderung für die Paßphrase ausschalten, wenn die Paßphrase „zaphod beeblebrox for president“ heißt.

Diese Funktion ist praktisch, wenn regelmäßig viele an Ihren geheimen Schlüssel adressierte Nachrichten eingehen. Die wiederholte Eingabe Ihrer Paßphrase wird somit hinfällig.

Die sicherste Verwendung dieser Funktion ist gewährleistet, wenn Sie den Befehl bei jedem Systemneustart eingeben und ihn löschen oder den Rechner herunterfahren, wenn Sie fertig sind. Verwenden Sie diese Funktion nicht in einer Umgebung, in der eine andere Person Zugriff auf Ihren Rechner hat.

Paßphrase aus einer anderen Anwendung übertragen

PGP enthält die Befehlszeilenoption „-z“, mit der Sie Ihre Paßphrase aus einer anderen Anwendung in PGP übertragen können. Diese Option wird hauptsächlich zum Starten von PGP aus einem E-Mail-Paket heraus verwendet.

Die Paßphrase wird der -z-Option in der Befehlszeile nachgestellt. Bei der Verwendung dieser Funktion sollten Sie mit Bedacht vorgehen.

PGPPASSFD

Die Beschreibung der Paßphrasendatei. Falls diese Umgebungsvariable auf Null (0) gesetzt wurde, verwendet PGP die erste Textzeile aus stdin als Paßwort.

PGP-Konfigurationsdatei 4

Informationen zur PGP-Konfigurationsdatei pgp.cfg

PGP speichert eine gewisse Anzahl an benutzerdefinierten Parametern in der Konfigurationstextdatei PGP.CFG. Mit einer Konfigurationsdatei können Sie Kennzeichen und Parameter (auch Umgebungsvariable genannt) für PGP definieren. Dazu müssen Sie diese Parameter nicht mehr in der PGP-Befehlszeile definieren.

Verwenden Sie diese Konfigurationsparameter, um unter anderem folgende Aufgaben auszuführen:

- Steuerung der Speicherung von temporären Arbeitsdateien in PGP.
- Grad der Skepsis in PGP anpassen, wenn die Gültigkeit eines Schlüssels aufgrund der Anzahl an zertifizierenden Unterschriften auf diesem Schlüssel bewertet wird.

Konfigurationsparameter können zugeordnete Ganzzahl-, Zeichenketten- oder Ein- / Aus-Werte (ON / OFF) sein, wobei der Typ des Wertes vom Typ des Parameters abhängt. PGP enthält zum Überprüfen eine entsprechende Konfigurationsdatei.

Für die Konfigurationsdatei gelten folgende Regeln:

- Leerzeilen werden ignoriert.
- Zeichen, die nach dem Kommentarzeichen „#“ stehen, werden ignoriert.
- Bei Eingabe von Schlüsselwörtern muß die Groß- und Kleinschreibung nicht beachtet werden.

Ein Beispiel für eine typische Konfigurationsdatei:

```
#TMP ist das Verzeichnis für PGP-Arbeitsdateien, wie
beispielsweise RAM-Datenträger.
TMP = "e:\" # kann von der Umgebungsvariable TMP überschrieben
werden.
ARMOR=ON # Verwenden Sie das Kennzeichen "-a" für den
ASCII-Schutz (falls vorhanden).
# CERT_DEPTH gibt an, wie genau Schlüsselverwalter andere
Schlüsselverwalter angeben können.
cert_depth = 3
```

Unter folgenden Bedingungen verwendet PGP Standardwerte für die Konfigurationsparameter:

- Konfigurationsparameter sind nicht definiert.
- Konfigurationsdatei existiert nicht.
- PGP kann die Konfigurationsdatei nicht finden.

Beachten Sie, daß Sie diese Konfigurationsparameter durch Voranstellen eines Plus-Zeichens auch direkt von der PGP-Befehlszeile aus festlegen können. Die folgenden beiden PGP-Befehle führen beispielsweise zum selben Ziel:

pgp -e +armor=on message.txt smith

pgp -ea message.txt smith

Den Speicherort der Datei PGP.CFG können Sie unter „Speicherort von PGP-Dateien“ auf Seite 5 nachlesen.

Im letzten Teil dieses Kapitels werden die PGP-Konfigurationsparameter zusammengefaßt. Die Parameter werden in alphabetischer Reihenfolge aufgeführt.

ARMOR: ASCII-geschützte Ausgabe

Standardeinstellung: ARMOR=OFF

Der Konfigurationsparameter ARMOR entspricht der Befehlszeilenoption „-a“. Wenn dieser Parameter aktiviert ist, werden chiffrierter Text oder Schlüssel von PGP in ASCII-geschütztem Format abgegeben, so daß sie sicher durch E-Mail-Kanäle transportiert werden können. Ausgabedateien sind mit der Erweiterung .ASC versehen.

Wenn Sie PGP in erster Linie zu E-Mail-Zwecken nutzen möchten, sollten Sie diesen Parameter aktivieren (ARMOR=ON).

ARMORLINES: Größe der ASCII-geschützten mehrteiligen Dateien

Standardeinstellung: ARMORLINES=0

Die meisten E-Mail-Funktionen lassen Nachrichten mit mehr als 50.000 oder 65.000 Byte nicht zu. Daher beschränkt PGP die Zeilenanzahl einer Datei auf 720. Wenn PGP eine große ASCII-geschützte Datei mit der Erweiterung .ASC erstellt, wird die Datei in kleinere mehrteilige Dateien aufgeteilt und kann somit per E-Mail gesendet werden. Die kleineren Dateien werden dann mit Erweiterungen wie .AS1, .AS2, .AS3 usw. versehen.

Der Konfigurationsparameter ARMORLINES legt die maximale Zeilenanzahl jeder kleineren Datei in einer Folge von mehrteiligen Dateien mit der Erweiterung .ASC fest. Wenn Sie die ARMORLINES-Einstellung auf Null setzen, teilt PGP die große Datei nicht in kleinere Dateien auf.

CERT_DEPTH: Tiefe der einzubettenden Schlüsselverwalter

Standardeinstellung: CERT_DEPTH=4

Der Konfigurationsparameter CERT_DEPTH gibt die maximale Anzahl der Ebenen an, in denen Schlüsselverwalter eingebettet werden können, um andere Schlüsselverwalter dahingehend zu zertifizieren, daß sie öffentliche Schlüssel auf Ihrem öffentlichen Schlüsselbund zertifizieren.

Wenn die Einstellung dieses Konfigurationsparameters beispielsweise 1 lautet, kann es nur eine Schlüsselverwalterebene unter Ihrem vollständig autorisierten Schlüssel geben. Sollte das der Fall sein, müssen Sie die öffentlichen Schlüssel aller autorisierten Schlüsselverwalter auf Ihrem Schlüsselbund direkt zertifizieren. Wenn Sie die CERT_DEPTH-Einstellung auf 0 setzen, steht Ihnen möglicherweise kein Schlüsselverwalter zur Verfügung, und Sie müssen jeden einzelnen Schlüssel auf Ihrem öffentlichen Schlüsselbund direkt zertifizieren, um ihn verwenden zu können. Die minimale CERT_DEPTH lautet 0, die maximale 8.

CLEARSIG: Unterschriebene Nachricht, die mit dem menschlichen Auge gelesen werden kann

Standardeinstellung: CLEARSIG=ON

Verwenden Sie den Parameter CLEARSIG, um eine unterschriebene Nachricht zu erstellen, die mit dem menschlichen Auge ohne Hilfe von PGP gelesen werden kann. Der Empfänger muß PGP jedoch verwenden, um die Unterschrift zu verifizieren.

Unverschlüsselten mit PGP unterschriebenen Nachrichten wird ein Unterschriftenzertifikat in Binärform vorangestellt. Die unterschriebene Nachricht wird komprimiert, wodurch sie, auch wenn sie unverschlüsselt ist, für das menschliche Auge unlesbar wird.

Um diese binären Daten durch einen 7-Bit E-Mail-Kanal zu senden, verwendet PGP den ASCII-Schutz (siehe ARMOR-Parameter). Selbst wenn PGP die Nachricht nicht komprimiert hat, wird die Nachricht durch den ASCII-Schutz für das menschliche Auge unlesbar. Der Empfänger muß zunächst PGP verwenden, um den Schutz von der Nachricht zu entfernen, und diese dann zum Lesen dekomprimieren.

Sollte die ursprüngliche Klartextnachricht im Text- und nicht im Binärformat vorliegen, können Sie den CLEARSIG-Parameter verwenden, um eine unterschriebene Nachricht durch einen E-Mail-Kanal zu senden. Die unterschriebene Nachricht wird hierbei nicht komprimiert, und der ASCII-Schutz wird auf das binäre Unterschriftenzertifikat, nicht aber auf die Klartextnachricht, angewandt. Mit dem Parameter CLEARSIG können Sie eine unterschriebene Nachricht erstellen, die mit dem menschlichen Auge ohne Hilfe von PGP gelesen werden kann (auch hier benötigt der Empfänger jedoch PGP, um die Unterschrift zu verifizieren).

Das CLEARSIG-Kennzeichen ist standardmäßig aktiviert (ON). Um die Funktionsweise von CLEARSIG voll zu aktivieren, müssen die ARMOR- und TEXTMODE-Kennzeichen ebenfalls aktiviert sein. Stellen Sie ARMOR=ON ein (oder verwenden Sie die -a-Option), und stellen Sie TEXTMODE=ON ein (oder verwenden Sie die -t-Option). Wenn der Parameter CLEARSIG in Ihrer Konfigurationsdatei deaktiviert ist (OFF), können Sie ihn direkt in der Befehlszeile wieder aktivieren (ON).

pgp -sta +clearsig=on message.txt.

Da bei dieser Methode nur das binäre Unterschriftenzertifikat und nicht der Nachrichtentext an sich ASCII-geschützt wird, besteht eine potentielle Gefahr, daß die ungeschützte Nachricht während des Transports beschädigt wird. Dies kann geschehen, wenn die Nachricht ein E-Mail-Gateway durchläuft, das Zeichensatzkonvertierungen vornimmt. In einigen Fällen können aber auch zusätzliche Leerschritte dem Zeilenende hinzugefügt oder Leerschritte vom Zeilenende entfernt werden. In diesem Fall kann die Unterschrift nicht verifiziert werden, was fälschlicherweise auf eine vorsätzliche Manipulation schließen lassen kann.

Wenn PGP die Textunterschrift im CLEARSIG-Modus berechnet, werden nachstehende Leerzeichen in jeder Zeile ignoriert.

COMMENT: ASCII-geschützter Kommentar

Der ASCII-geschützte Kommentar wird in jeder geschützten Ausgabe als Kommentarkopf gleich unter dem Versionskopf angezeigt.

COMPATIBLE: Benutzeroberflächenkompatibilität mit PGP 2.6.2 aktivieren

Standardeinstellung: COMPATIBLE=OFF

Mit dem Konfigurationsparameter COMPATIBLE wird die Benutzeroberflächenkompatibilität mit PGP 2.6.2 aktiviert. Diese Funktion benötigen Sie unter Umständen für die Interaktion mit Skripten, die das Parsing der Ausgabe durchführen bzw. auf andere Weise mit PGP-Dialogfeldern interagieren.

Zur Aktivierung dieser Funktion ergänzen Sie die Konfigurationsdatei (PGP.CFG) um folgende Zeile:

```
COMPATIBLE=OFF
```

COMPLETES_NEEDED: Anzahl der erforderlichen, vollständig autorisierten Schlüsselverwalter

Standardeinstellung: COMPLETES_NEEDED=1

Der Konfigurationsparameter COMPLETES_NEEDED gibt die Mindestzahl der vollständig autorisierten Schlüsselverwalter an, die zur vollständigen Zertifizierung eines öffentlichen Schlüssels in Ihrem öffentlichen Schlüsselbund erforderlich sind.

COMPRESS: Komprimierung vor Verschlüsselung

Standardeinstellung: COMPRESS=ON

Der Konfigurationsparameter COMPRESS aktiviert / deaktiviert die Datenkomprimierung vor der Verschlüsselung. Er wird hauptsächlich zum Debuggen von PGP verwendet. Normalerweise versucht PGP, den Klartext vor seiner Verschlüsselung zu komprimieren. Ändern Sie diese Einstellung nicht.

CIPHERNUM

Verwenden Sie diesen Parameter, um den symmetrischen Chiffriercode festzulegen. Die Werte lauten wie folgt:

kPGPCipherAlgorithm_IDEA = 1

kPGPCipherAlgorithm_3DES = 2

kPGPCipherAlgorithm_CAST5 = 3

Dies wird festgelegt, damit der Anwendung die im SDK kodierten Werte nicht bekannt sein müssen. In zukünftigen Versionen werden möglicherweise noch mehr Algorithmen vorhanden sein.

ENCRYPTTOSELF: Verschlüsselung mit eigenem Namen

Standardeinstellung: ENCRYPTTOSELF=PFF

Mit dieser Variablen fügt PGP Nachrichten dem Empfänger MYNAME hinzu.

FASTKEYGEN: Schnellere Schlüsselerzeugung

Standardeinstellung: FASTKEYGEN=ON

Verwenden Sie diese Variable, um eine schnellere Schlüsselerzeugung festzulegen.

HASHNUM

Eine Zahl, die den verwendeten Hash-Algorithmus beschreibt. Die Werte des Typs PGPHashAlgorithm lauten:

kPGPHashAlgorithm_MD5 = 1

kPGPHashAlgorithm_SHA = 2

kPGPHashAlgorithm_RIPEMD160 = 3

Dies wird festgelegt, damit der Anwendung die im SDK kodierten Werte nicht bekannt sein müssen. In zukünftigen Versionen werden möglicherweise noch mehr Algorithmen vorhanden sein.

INTERACTIVE: Schlüsselergänzungen bestätigen

Standardeinstellung: INTERACTIVE=OFF

Mit dieser Variablen weisen Sie PGP an, eine Bestätigung anzufordern, wenn Sie Ihrem Schlüsselbund eine Schlüsseldatei mit mehreren Schlüsseln hinzufügen. Wenn diese Variable auf „Ein“ gesetzt wurde (ON), fordert PGP für jeden einzelnen Schlüssel in der Schlüsseldatei eine Bestätigung an, bevor der jeweilige Schlüssel dem Schlüsselbund hinzugefügt wird.

KEYSERVER_URL

Standardeinstellung: KEYSERVER_URL=““

Gibt die URL des standardmäßigen Schlüssel-Servers an, beispielsweise ldap://certserver.pgp.com.

MARGINALS_NEEDED: Anzahl der erforderlichen, eingeschränkt autorisierten Schlüsselverwalter

Standardeinstellung: MARGINALS_NEEDED=2

Der Konfigurationsparameter MARGINALS_NEEDED gibt die Mindestzahl der eingeschränkt autorisierten Schlüsselverwalter an, die zur vollständigen Zertifizierung eines öffentlichen Schlüssels in Ihrem öffentlichen Schlüsselbund erforderlich sind.

MYNAME: Standardmäßige Benutzer-ID für Unterschriften

Standardeinstellung: MYNAME= ““

Der Konfigurationsparameter MYNAME gibt die standardmäßige Benutzer-ID an, die für die Auswahl des geheimen Schlüssels, mit dem Unterschriften erstellt werden, verwendet werden soll. Falls MYNAME nicht definiert wurde, wird der geheime Schlüssel verwendet, der zuletzt auf Ihrem geheimen Schlüsselbund installiert wurde. Mit der -u-Option können Sie diese Einstellung außer Kraft setzen und in der Befehlszeile von PGP eine Benutzer-ID festlegen.

PAGER: Shell-Befehl zur Anzeige der Klartextausgabe

Standardeinstellung: PAGER= ““

Mit der -m-Option von PGP können Sie entschlüsselte Klartextausgaben nacheinander am Bildschirm anzeigen, ohne daß die jeweilige Ausgabe in eine Datei geschrieben wird.

PGP weist ein integriertes Dienstprogramm zur Seitenanzeige auf. Falls Sie ein anderes Dienstprogramm verwenden möchten, können Sie dies mit dem PAGER-Parameter angeben. Dieser Parameter gibt den Shell-Befehl an, den PGP zur Anzeige von Dateien verwendet.

Beachten Sie folgendes: Wenn ein Absender festgelegt hat, daß eine bestimmte Datei nur für Ihre Augen bestimmt ist, verwendet PGP stets die in die Anwendung integrierte Anzeigefunktion.

Weitere Informationen hierzu finden Sie unter „Nachrichten entschlüsseln und Klartextausgabe am Bildschirm anzeigen“ auf Seite 29.

PGP_MIME

Standardeinstellung: PGP_MIME=OFF

Verwenden Sie diese Einstellung zur Festlegung der Kompatibilität mit PGP-MIME.

PGP_MIMEPARSE

Standardeinstellung: PGP_MIMEPARSE=OFF

Mit dieser Einstellung können Sie PGP anweisen, das Parsing der Nachrichtentextteile von MIME durchzuführen.

PUBRING: Dateiname für Ihren öffentlichen Schlüsselbund

Standardeinstellung: PUBRING = „%PGPPATH%/pubring.pkr“ on UNIX

%USERPROFILE%\Application Data\pgp\pubring.pkr on NT

Unter Umständen ist es empfehlenswert, Ihren öffentlichen Schlüsselbund in einem anderen Verzeichnis als Ihre PGP-Konfigurationsdatei zu speichern (d. h. in dem Verzeichnis, das durch die Umgebungsvariable PGPPATH definiert wurde). Mit dem Parameter PUBRING können Sie den vollständigen Pfad und Dateinamen für Ihren öffentlichen Schlüsselbund ermitteln.

In der Befehlszeile können Sie mit dieser Funktion auch einen alternativen Schlüsselbund angeben.

RANDOMDEVICE

Standardeinstellung: RANDOMDEVICE = /dev/random on UNIX

Nur UNIX. Kennzeichnet den Entropiepool des Systems, /dev/random. PGP versucht, dieses Gerät zur Entropieabfrage zu öffnen. Falls dieser Vorgang fehlschlägt, wird versucht, die Entropie anhand von Benutzertastenanschlägen zu ermitteln. Dies trifft nicht auf Windows NT zu.

RANDSEED: Dateiname für Datei mit Zufallswerten

Standardeinstellung: RANDSEED = „%PGPPATH%/randseed.rnd“ unter UNIX

„%SYSTEMROOT% /randseed.rnd“ unter Windows NT

Die Datei mit Zufallswerten, RANDSEED.RND, wird zur Generierung von Sitzungsschlüsseln verwendet. Unter Umständen ist es empfehlenswert, die Datei mit den Zufallswerten in einem Verzeichnis bzw. auf einem Gerät mit höherem Sicherheitsgrad zu speichern (normalerweise befindet sich diese Datei in dem Verzeichnis, das durch die Umgebungsvariable PGPPATH definiert wurde). Mit dem Parameter RANDSEED können Sie den vollständigen Pfad und Dateinamen für die Datei mit Zufallswerten ermitteln.

SECRING: Dateiname für Ihren geheimen Schlüsselbund

Standardeinstellung: SECRING = „%PGPPATH%/secring.pgp“

Unter Umständen ist es empfehlenswert, Ihren geheimen Schlüsselbund in einem anderen Verzeichnis als Ihre PGP-Konfigurationsdatei zu speichern (d. h. in dem Verzeichnis, das durch die Umgebungsvariable PGPPATH definiert wurde). Mit dem Parameter PUBRING können Sie den vollständigen Pfad und Dateinamen für Ihren geheimen Schlüsselbund ermitteln.

SHOWPASS: Paßphrasen-Echo an Benutzer

Standardeinstellung: SHOWPASS=OFF

Ihre Paßphrase wird bei der Eingabe in PGP nicht angezeigt. Hierdurch verringert sich das Risiko, daß Sie bei der Eingabe von einer anderen Person beobachtet werden, die auf diese Weise Ihre Paßphrase herausfinden kann. Unter Umständen haben Sie jedoch Schwierigkeiten bei der Paßphraseneingabe, wenn Sie nicht sehen können, was Sie tippen. Außerdem kann es sein, daß Sie zuhause arbeiten, wo das oben erläuterte Sicherheitsrisiko nicht besteht.

Mit dem Konfigurationsparameter SHOWPASS zeigt PGP während der Paßphraseneingabe an, was Sie gerade tippen (d. h. Sie erhalten ein Echo der jeweiligen Eingabe).

TMP: Verzeichnispfadname für temporäre Dateien

Standardeinstellung: TMP = ““

Über den Konfigurationsparameter TMP wird festgelegt, welches Verzeichnis von PGP für temporäre Arbeitsdateien verwendet wird. Falls TMP nicht definiert wurde, werden die temporären Dateien im aktuellen Verzeichnis gespeichert. Wenn die Shell-Umgebungsvariable TMP definiert wurde, werden die temporären Dateien im angegebenen Verzeichnis gespeichert.

TEXTMODE: Klartext als Textdatei behandeln

Standardeinstellung: TEXTMODE=OFF

Der Konfigurationsparameter TEXTMODE entspricht der Befehlszeilenoption „-t“. Wenn dieser Parameter aktiviert wurde, geht PGP davon aus, daß es sich bei dem jeweiligen Klartext um eine Textdatei und nicht um eine Binärdatei handelt, und konvertiert ihn vor der Verschlüsselung in „kanonischen Text“. Kanonischer Text endet an jeder Textzeile mit einem Wagenrücklauf und einem Zeilenvorschub.

Dieser Parameter wird automatisch deaktiviert, wenn PGP erkennt, daß die Klartextdatei Binärdaten enthält, die nicht im Textformat vorliegen. Wenn Sie PGP in erster Linie zu E-Mail-Zwecken nutzen möchten, ist folgende Einstellung empfehlenswert: TEXTMODE=ON.

Weitere Informationen hierzu finden Sie unter „ASCII-Textdateien an andere Umgebungen für Rechner senden“ auf Seite 27.

TZFIX: Zeitzonenanpassung

Standardeinstellung: TZFIX=0

Nur UNIX. PGP enthält für Schlüssel und Unterschriftenzertifikate Zeitmarkierungen gemäß Greenwich Mean Time (GMT). Wenn PGP die Uhrzeit vom System abfragt, sollte diese gemäß GMT zurückgegeben werden. Auf einigen nicht ordnungsgemäß konfigurierten Systemen wird die Systemzeit jedoch als Pazifik Normalzeit (USA) plus acht Stunden zurückgegeben.

Aus dem Konfigurationsparameter TZFIX geht die Anzahl der Stunden hervor, die der Systemzeitfunktion hinzugefügt werden müssen, damit die Anzeige gemäß GMT erfolgt. Falls die Zeit vom Betriebssystem nicht gemäß GMT angegeben wird, können Sie dies mit TZFIX beheben.

Für Los Angeles:	SET TZ=PST8PDT
Für Denver:	SET TZ=MST7MDT
Für Arizona:	SET TZ=MST7

(In Arizona wird die Umstellung auf Sommerzeit nicht vorgenommen)

Für Chicago:	SET TZ=CST6CDT
Für New York:	SET TZ=EST5EDT
Für London:	SET TZ=GMT0BST
Für Amsterdam:	SET TZ=MET-1DST
Für Moskau:	SET TZ=MSK-3MSD
Für Auckland:	SET TZ=NZT-13

VERBOSE: Nachrichten ohne Status, normale Nachrichten bzw. Nachrichten mit ausführlicher Anzeige

Standardeinstellung: VERBOSE = 1

Die VERBOSE-Variable steuert, wie ausführlich die Diagnosenachrichten von PGP ausfallen. Die Einstellungen lauten wie folgt:

0 - Zeigt nur Anfragen und Fehler an (d. h. es werden Benutzereingaben angefordert, und Fehler werden bei Ihrem Auftreten gemeldet).

1 - Normal-Standardeinstellung. Der Detailgrad von Diagnosemeldungen und Tips bewegt sich in einem angemessenen Rahmen.

2 - Zeigt sämtliche Informationen an. Dies ist hilfreich, wenn Sie Probleme in PGP diagnostizieren möchten. Diese Einstellung ist für den normalen Gebrauch nicht empfehlenswert.

Fehler- und Abbruchcodes A

Die in diesem Anhang aufgeführten Tabellen enthalten die Fehler- und Abbruchcodes von PGP.

Allgemeine Fehler

Fehler	Erklärung
0	Beenden OK, kein Fehler
1	Ungültige Datei
2	Datei nicht gefunden
3	Unbekannte Datei
4	Batchmode-Fehler
5	Ungültiges Argument
6	Prozeß unterbrochen
7	Fehler: Nicht genügend Arbeitsspeicher

Schlüsselbundfehler

Fehler	Code
10	Fehler bei Schlüsselerzeugung
11	Fehler: Schlüssel nicht vorhanden
12	Fehler beim Hinzufügen zu Schlüsselbund
13	Fehler beim Extrahieren des Schlüsselbunds
14	Fehler beim Bearbeiten des Schlüsselbunds
15	Fehler beim Anzeigen des Schlüsselbunds
16	Fehler beim Löschen des Schlüsselbunds
17	Fehler bei der Schlüsselbundüberprüfung
18	Schlüsselunterschriftenfehler
19	Fehler beim Löschen von Schlüsselunterschriften

Schlüsselbundfehler

Fehler	Code
KEY_SIGNATURE_ERROR	Schlüsselunterschriftenfehler

Verschlüsselungsfehler

Fehler	Code
20	Unterschriftenfehler
21	Fehler beim Verschlüsseln mit öffentlichen Schlüsseln
22	Verschlüsselungsfehler
23	Komprimierungsfehler

Decodierungsfehler

Fehler	Beschreibung
30	Fehler bei der Unterschriftenprüfung
31	Fehler beim Entschlüsseln mit öffentlichen Schlüsseln
32	Entschlüsselungsfehler
33	Dekomprimierungsfehler

Index

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

Z