



# PGP® Universal Produktfamilie

Vollautomatischer Schutz von Daten durch Verschlüsselung von E-Mails, Festplatten, Dateien und Instant Messaging

## Integrierte Verschlüsselungslösung mit automatisierter Schlüsselverwaltung

Die PGP Universal Produktfamilie schützt vertrauliche Daten, egal wie und wo ein Unternehmen diese nutzt. PGP Universal schützt Betriebsgeheimnisse und ermöglicht Unternehmen das Erfüllen von Sicherheitsvorgaben der Kunden und Geschäftspartner. Mit dem Einsatz von PGP Universal nutzen Unternehmen eine Infrastruktur, die sie später mit der gleichen Infrastruktur um weitere Verschlüsselungsfunktionen erweitern können. PGP Universal basiert auf ausgereifter Kryptographie-Technologie, die sich dem Anwender als eine sichere, einfach bedienbare und einsetzbare Familie von Verschlüsselungsprodukten darstellt.

### Integrierte Anwendungen, eine Lösung

PGP Universal bietet mehrere Verschlüsselungslösungen, die über eine zentrale Konsole verwaltet werden. Die Lösung umfasst die Verschlüsselung von E-Mails samt Anhängen, Dateien und Festplatten, außerdem digitale Signaturen und Signaturprüfung und den Schutz von Instant Messaging. Dazu bietet PGP Universal als Alternativen gatewaybasierte und durchgehende Sicherheit sowie alle Werkzeuge zum Schutz vertraulicher Daten bei der Übertragung oder auf der lokalen Festplatte.

### Bewährter Einsatz, weltweite Erfahrung

PGP-Produkte kommen bei mehreren zehntausend Unternehmen in über 90 Ländern zum Schutz von E-Mails und Daten zum Einsatz. Der Einsatz von PGP Universal hat sich in großen Unternehmen mit verschiedensten E-Mail-, Netzwerk- und Sicherheitsumgebungen über viele Industriezweige hinweg weltweit bewährt.

### Automatische Regelerfüllung ohne Lücken

PGP Universal setzt auf der Netzwerkebene auf und arbeitet selbstverwaltend. Die Software erstellt selbständig Schlüssel für neue Mitarbeiter und widerruft diese automatisch, wenn ein Mitarbeiter das Unternehmen wieder verlässt. PGP Universal synchronisiert Daten mit existierenden LDAP-Verzeichnisdiensten.

## Drei Einsatzmöglichkeiten

PGP Universal bietet drei Einsatzmöglichkeiten:

- Gateway-Sicherheit – Keine Client-Software
  - Keine Benutzerdialoge, umfassende Sicherheit – automatisierter Client
  - Wahlweise manuell oder automatisch, umfassende Sicherheit – Client für Anwender mit höheren Ansprüchen
- Alle PGP-Anwender werden zentral verwaltet und sind an die zentralen Sicherheitsrichtlinien gebunden, können aber einzelne E-Mails explizit verschlüsseln.

### Externe Partner mit und ohne Schlüssel schützen

PGP Universal arbeitet mit bestehenden Installationen auf Basis von OpenPGP, PGP Desktop und PGP Universal ebenso zusammen wie mit Anwendern von S/MIME, X.509 oder bereits installierten, kompatiblen PKIs. PGP Universal wird schnell von Partnern akzeptiert, da es Schlüssel für Empfänger erstellen und Nachrichten direkt per E-Mail oder über einen Webzugang ausliefern kann.

### Automatischer Betrieb, geringe Betriebskosten

Die Kombination von netzwerk- und clientbasierter Verschlüsselung durch PGP Universal minimiert Verwaltungsaufgaben und reduziert Kosten. Automatische Anmeldung, kein Schulungsbedarf, wenige Support-Anfragen, geringe Belastung der Infrastruktur und einfache Integration in bestehende E-Mail-, Netzwerk- oder PKI-Umgebungen bedeuten geringe und planbare Kosten.

### Innovative Technologie, bewährte Qualitätssicherheit

Wonach suchen Unternehmen bei einem Partner im Bereich Sicherheit? PGP Universal nutzt eine einzigartige Proxy-Architektur, die auf der ausgereiften, seit langem bewährten PGP-Technologie basiert. Die von PGP patentierte Technologie des Additional Decryption Keys (ADK) garantiert den Zugriff auf verschlüsselte Unternehmensdaten sofern dies durch die Sicherheitsrichtlinien erwünscht ist. Der Quellcode der Kryptographie-Bibliothek wurde offen gelegt und in den letzten zehn Jahren von den besten Kryptographie-Experten der Welt untersucht und als sicher erachtet.

## Überblick – PGP Universal Produktfamilie

Die PGP Universal Produktfamilie bietet drei Optionen zum Schutz von E-Mails und Festplatten. Alle Produkte sind modular aufgebaut. Bestehende Systeme können daher problemlos auf eine höhere Version mit mehr Funktionalität aufgerüstet werden.

### PGP Universal Series 100

PGP Universal Series 100 verschlüsselt und signiert E-Mails auf dem Gateway und schützt die Daten von Ihrem Netzwerk bis zu Ihrem Geschäftspartner, selbst wenn dieser keine Schlüssel besitzt.

- Automatische Verschlüsselung, Entschlüsselung, digitale Signatur und Signaturprüfung basierend auf zentralen Richtlinien am Gateway
- Integration mit Content-Filtern, um die Informationen nach Versender, Empfänger, Inhalt, Schlüsselwörtern oder Format zu schützen
- Automatische Anmeldung neuer Benutzer durch Integration mit LDAP-Verzeichnisdiensten
- Automatisches Schlüsselmanagement und Suche nach Empfängerschlüsseln
- Externe Empfänger müssen nicht zwingend über einen Schlüssel verfügen
- Benötigt keine Client-Software für interne Nutzer
- E-Mails können manuell explizit verschlüsselt werden

### PGP Universal Series 200

PGP Universal Series 200 schützt besonders gefährdete Mitarbeiter über zentral verwaltete Sicherheit für E-Mail, Instant Messaging, Dateien und Festplatten.

- Sicherheit für E-Mails und gespeicherte Daten auf dem lokalen Rechner, dem E-Mail-Server, Gateway bis hin zum Empfänger
- Automatische Verschlüsselung, Entschlüsselung, digitale Signatur und Signaturprüfung am Desktop-PC nach zentralen Richtlinien
- Automatische Verschlüsselung am Client
- Automatisches Schlüssel-Management
- E-Mails können explizit manuell verschlüsselt werden
- Die optionale Komponente PGP Whole Disk lässt sich mittels eines Passworts oder einer Zwei-Faktoren-Authentifizierung über einen auf einem Aladdin eToken gespeicherten Schlüssel schützen

### PGP Universal Series 500

PGP Universal Series 500 bietet umfassenden Schutz und deckt Kommunikation mit internen und externen Benutzern sowie auf Festplatten gespeicherte Informationen ab.

- Kombiniert alle Funktionen von PGP Universal Series 100 und 200
- Automatische Sicherheit für gespeicherte Daten und E-Mails, wahlweise ab dem Gateway oder Ende-zu-Ende

## PGP Universal – Komponenten

### PGP Universal Server – Gateway und Keyserver

Der PGP Universal Server wird zwischen dem E-Mail-Server im Unternehmen und dem Internet installiert und schützt automatisch den ein- und ausgehenden E-Mail-Verkehr über zentrale Sicherheitsrichtlinien. Der PGP Universal Server fungiert dabei als Proxy für den E-Mail-Verkehr zwischen dem Gateway und dem Internet. Er regelt bei Bedarf Verschlüsselung und Entschlüsselung, digitale Signaturen und Signaturprüfung der Nachrichten. Die integrierte Keyserver-Funktionalität erlaubt es, die Schlüssel interner Benutzer auf den Keyserver zu laden, um sie dort automatisch oder vom Administrator verifizieren zu lassen. PGP Universal Server kann zudem außerhalb des Mailverkehrs genutzt werden, um Anwender mit PGP Desktop und die zentralen Sicherheitsrichtlinien zu verwalten.

### PGP Universal Management-Konsole

Die PGP Universal Management-Konsole bietet rollenbasiertes Management von PGP Desktop und PGP Universal Server. Mit Hilfe von LDAP-Attributen kann der Administrator die Konsole einsetzen, um PGP Desktop Konfigurationen dynamisch zuzuweisen, einzusetzen und zu aktualisieren sowie zentral definierte Verschlüsselungsrichtlinien an Desktop-Benutzer zu übertragen. Die vereinheitlichte Management-Konsole gibt Administratoren Zugriff auf alle Tools, die benötigt werden, um auf die Funktionen des PGP Additional Decryption Keys (ADK) und PGP Whole Disk Wiederherstellungs-Tokens zuzugreifen.

### PGP Universal Satellite

PGP Universal Satellite ermöglicht die Durchsetzung von bilateralen Richtlinien bei internen Benutzern, die nicht die volle Funktionalität von PGP Desktop benötigen. Die Software beinhaltet nur wenige Benutzerdialoge und übernimmt automatisch die zentral definierten Richtlinien. PGP Universal Satellite ver- und entschlüsselt E-Mails vollkommen transparent für den Anwender und garantiert die Einhaltung der Sicherheitsrichtlinien für alle E-Mail-Nachrichten, die zum PGP Universal Server gesendet werden.

### PGP Desktop

Die mehrfach ausgezeichnete PGP Desktop Software bietet eine komplette, clientbasierte Lösung zum Schutz von E-Mails, Festplatten und Instant Messaging. PGP Desktop ermöglicht den Einsatz und das Durchsetzen von zentral festgelegten Sicherheitsrichtlinien. PGP Desktop erlaubt es Benutzern, zusätzliche Sicherheitsrichtlinien zu definieren und zu nutzen. Diese zusätzlichen Richtlinien können sich auf Merkmale einer Nachricht beziehen, wie den Empfänger einer E-Mail, den Betreff, den Header, die Nachricht selbst, die Priorität oder den Vermerk „Vertraulich“. PGP Desktop bietet zudem Verschlüsselung für virtuelle Laufwerke und Instant Messaging.

### PGP Whole Disk

PGP Whole Disk ist ein Produkt zur Verschlüsselung der gesamten Festplatte. Dabei werden ständig alle Daten auf der Festplatte inklusive der temporären Dateien und Auslagerungsdateien verschlüsselt. PGP Whole Disk schützt den kompletten Inhalt eines Laptops, Desktop-PCs, einer Festplatte oder eines USB-Speicher-Sticks. PGP Whole Disk lässt sich auch in Kombination mit PGP Virtual Disk einsetzen, wenn Dateien und Verzeichnisse auch geschützt werden sollen, nachdem die Festplatte entschlüsselt wurde.

### Verschlüsselung von virtuellen Laufwerken

PGP Virtual Disk erzeugt transparent virtuelle Laufwerke, deren Inhalt zum Schutz vor unerlaubtem Zugriff verschlüsselt ist, solange kein autorisierter Benutzer darauf zugreift.

- Unterstützt automatisches Trennen von verschlüsselten virtuellen Laufwerken nach einer gewissen Zeitspanne
- Kann in Kombination mit PGP Whole Disk genutzt werden, wenn nach dem Entschlüsseln der ganzen Festplatte einzelne Dateien weiterhin geschützt bleiben sollen

### PGP Universal Web Messenger

Um sicheren E-Mail-Verkehr auch dann zu gewährleisten, wenn der Nutzer nicht über einen E-Mail-Client verfügt, bietet PGP Universal die Möglichkeit, vertrauliche Nachrichten per Internet-Browser zu senden und zu empfangen. PGP Universal Web Messenger ermöglicht Nutzern den Zugang zu gesicherten E-Mails über ein per SSL gesichertes, web-basiertes E-Mail-Postfach auf dem PGP Universal Server.

### PGP Verified Directory

PGP Verified Directory setzt auf die grundlegende Keyserver-Funktionalität des PGP Universal Servers auf, um eine einfache, intuitive Schnittstelle für die Verwaltung der Schlüssel zu ermöglichen. PGP Verified Directory ermöglicht die Übertragung von Schlüsseln interner Benutzer auf den Schlüsselsever, um sie dort automatisch oder vom Administrator prüfen zu lassen.

### Symantec AntiVirus™ Scanner

PGP Corporation hat den Virens scanner Symantec AntiVirus in die PGP Universal Produktlinie integriert. Die Antivirus-Technologie bietet schnellen, skalierbaren und verlässlichen Schutz für alle E-Mails und Dokumente, die den PGP Universal Server durchlaufen.

### Komponenten der PGP Universal Produktfamilie

	Series 100	Series 200	Series 500
PGP Universal Server & Keyserver	●	●	●
PGP Universal Management Console	●	●	●
PGP Desktop		●	●
PGP Universal Satellite	●	●	●
PGP Universal Web Messenger	●		●
PGP Verified Directory	●	●	●
PGP Whole Disk		●	●
Symantec AntiVirus Scan Engine (optional)	●		●

### PGP Universal – Einsatzoptionen

**PGP Universal Series 100**  
Sensible Daten schützen – Sichern Sie an zentraler Stelle vertrauliche E-Mails zu externen Partnern, Zulieferern und Kunden

**PGP Universal Series 200**  
Schützen Sie gefährdete Anwender – Zentraler Schutz von E-Mails, Instant Messaging und gespeicherten Daten für interne und externe Benutzer

**PGP Universal Series 500**  
Schützen Sie Ihr komplettes Unternehmen – Zentraler Schutz von E-Mails, Instant Messaging, gespeicherte Daten bei Mitarbeitern und externen Partnern

## Technische Spezifikationen

### Unterstützte Verschlüsselungsstandards

- PGP/MIME RFC 3156
- OpenPGP RFC 2440
- S/MIME v3
- X.509 v3

### Unterstützte Kommunikationsprotokolle

- POP
- POPS
- IMAP
- IMAPS
- SMTP
- SMTPS
- STARTTLS für POP/IMAP/SMTP
- Microsoft Exchange MAPI
- IBM Lotus Notes
- AOL OSCAR (AIM)

### Unterstützte E-Mail-Server

- Microsoft Exchange Server 2003 SP1 oder 2000 SP3
- Lotus Domino Server 6.5 oder 5.0.11
- Stalker CommuniGate 4.2

### Unterstützte E-Mail-Clients

- Microsoft Outlook 2003 SP1, XP SP3 oder 2000 SP3, Microsoft Outlook Express 6, Microsoft Entourage 2004
- Lotus Notes 6.x oder 5.0.11 für Windows
- Mozilla Thunderbird 1.0
- Qualcomm Eudora 6.2
- Apple Mail 1.3.9

### Unterstützte Instant Messaging Clients

- AOL Instant Messenger 5.5-5.9.x für Windows
- AOL Instant Messenger 4.7 für Mac OS X
- Trillian 2.2-3.0 für Windows
- Apple iChat 2.1 für Mac OS X

## Systemanforderungen

### PGP Universal Server

- Wird als reine Softwarelösung ausgeliefert
- Bitte informieren Sie sich auf der PGP-Website ([www.pgp.de](http://www.pgp.de)) über die aktuellen Systemanforderungen

### PGP Desktop für Windows

- Microsoft Windows 2000 SP3, XP SP1 oder SP2
- PGP Whole Disk benötigt Windows XP SP1 oder SP2
- 128 MB Hauptspeicher
- 64 MB freier Festplattenspeicher

### PGP Desktop für Mac OS X

- Mac OS X 10.3
- 128 MB Hauptspeicher
- 64 MB freier Festplattenspeicher

### PGP Universal Satellite für Windows

- Microsoft Windows 2000 SP3, Microsoft Windows Server 2003 oder Microsoft Windows XP SP1 oder SP2
- 64 MB Hauptspeicher
- 20 MB freier Festplattenspeicher

### PGP Universal Satellite für Mac OS X

- Mac OS X 10.2.8 oder Mac OS X 10.3
- 128 MB Hauptspeicher
- 20 MB freier Festplattenspeicher

PGP ist ein eingetragenes Warenzeichen und das PGP Logo ist ein Warenzeichen der PGP Corporation. Produkte und Markennamen, die in diesem Dokument verwendet werden, sind unter Umständen Warenzeichen oder eingetragene Warenzeichen ihrer jeweiligen Besitzer. Alle diese Warenzeichen oder eingetragenen Warenzeichen sind alleiniges Eigentum ihrer jeweiligen Besitzer.

