

PGP BUSINESS SECURITY SUITE 1.0

Comprehensive, Integrated Security from the Desktop to the Internet

PGP® Business Security Suite supports the critical corporate task of protecting digital property, both locally and across intranets, extranets, and the public Internet. This comprehensive, scalable security solution gives you all of the advantages that organizations have come to expect – superior cryptographic solutions, flexible security management tools, and sound security policy administration – from the most trusted name in security: PGP.

PGP for Business Security: Industrial-strength cryptography

PGP for Business Security makes it easy for users to safeguard digital communications and data by encrypting them so that only the intended recipients can decipher the contents. PGP uses only the strongest commercially available encryption to ensure secure communications. PGP also incorporates powerful digital signature capabilities that verify authorship as well as the integrity of a document. A full suite of management tools gives security administrators flexible control over corporate security policies.

PGP Certificate Server: Centralized storage and management

PGP Certificate Server lets organizations from small companies to multi-national corporations quickly create and manage a scalable public-key infrastructure. It takes advantage of a Lightweight Directory Access Protocol (LDAP) directory to receive and process incoming PGP certificates, index the attributes for easy search and retrieval, and automatically update certificates when changes are made. PGP Certificate Server simplifies certificate management by including configuration and policy templates that can be easily tailored to an organization's specific requirements.

PGP Policy Management Agent for SMTP: Automatic policy enforcement

PGP Policy Management Agent for SMTP enforces corporate security policies for email communications, ensuring that incoming and outgoing email adheres to policies established for a given site. This important component of the PGP Business Security Suite transparently operates with any version of PGP client software and works with standard SMTP mail servers.

Easy to install, use, and administer

PGP Business Security Suite is designed to be quickly deployed across an organization. It works seamlessly with popular productivity tools, email applications, and operating systems; relies on Administrative tools for easy configuration; and is so easy to operate that users can learn to encrypt, decrypt, digitally sign, and verify documents in a matter of minutes.

General Features

- Worldwide de facto standard for email and file security
- Scalable cross-platform architecture
- Intuitive user interface
- Configurable security policies, easy installation and administration

PGP for Business Security

- Only strong (128-bit minimum) encryption of email and files
- Unforgeable digital signatures
- Control over client configuration, including corporate message recovery

PGP Certificate Server

- Scalable centralized storage and management of digital certificates
- Fast certificate retrieval with multiple-attribute searches
- Customizable values for configuration and policy management

PGP Policy Management Agent for SMTP

- Policy enforcement for email within intranets and over the Internet
- Automatic enforcement of encryption and corporate message recovery policy
- Support for standard SMTP servers



PRETTY GOOD
PRIVACY

PGP BUSINESS SECURITY SUITE 1.0



PRETTY GOOD
PRIVACY™

PGP FOR BUSINESS SECURITY

- User-specified or automatic encryption and digital signing of email and attachments
- Folder encryption to safeguard local files
- Wipe to securely remove original files
- Group recipient list for encrypting email to multiple recipients
- Plug-ins for popular email programs and desktop toolbar for easy, convenient access to cryptographic functions
- Support for centralized hierarchical and/or Web-of-Trust security models
- Support for Diffie-Hellman/DSS and RSA public key algorithms; MD5, RIPEMD-160, and SHA-1 hash functions; and CAST, International Data Encryption Algorithm (IDEA), and Triple-DES symmetric algorithms
- Applications and documents supported:

Seamless integration with email applications, including Claris Mailer for Macintosh; Microsoft Exchange for Windows 95 and Windows NT 4.0; Microsoft Outlook for Windows 95 and Windows NT 4.0; Netscape Communicator 4.0 for Windows, Macintosh, and UNIX; and QUALCOMM Eudora for Windows 95, Windows NT 4.0, and Macintosh

Any file, including text, spreadsheet, audio, or video

Clipboard contents (Macintosh and PC)

Administrative capabilities

Administrator's Wizard for custom configuration of PGP before it is installed on each user's personal computer:

Corporate message recovery configurable for inbound and outbound messages

Disable use of conventional (symmetric key) encryption

Disable key generation

Password strength control (minimum length and quality)

PGP Certificate Server support:

Synchronization of local keyrings and Certificate Servers

Advanced search and retrieval of public keys on local keyring or Certificate Servers

Key Server Preferences dialog to specify searchable and default Certificate Servers

PGP CERTIFICATE SERVER

- Policy configuration options, including policy requirements for certificate storage, advanced filtering for removal of extraneous data, authenticated requests for Add, Delete, and Disable, and remote administration, monitoring, and configuration
- Administrative controls, including access control by IP address or host name for specific functions
- Access logging, error logging, reporting, and audit trails
- Compatibility and integration:
 - Support for LDAP and HTTP protocols*
 - Seamless integration with PGP 5.0 and later*
 - Support for client synchronization update requests*
 - Import/export of standard PGP keyring and ASCII armored files*

POLICY MANAGEMENT FOR SMTP

- Corporate message recovery: Rejects all encrypted messages that have not also been encrypted to one or more corporate message recovery keys
- Digital signatures: Allows, disallows, or requires the use of digital signatures on messages
- Encryption: Determines whether all email and attachments must be encrypted before passing policy requirements
- Conventional encryption: Rejects all messages using conventional (symmetric) encryption
- Forbidden keys: Disallows the use of encryption to specific keys
- Specified address: Limits the checking of policies to be enforced for a specified IP address or domain

© 1997 Pretty Good Privacy, Inc. All rights reserved. PGP and Pretty Good Privacy are registered trademarks of Pretty Good Privacy, Inc. This software uses public key algorithms described in U.S. patent numbers 4,200,770, 4,218,582, 4,405,829, and 4,424,414, licensed exclusively by Public Key Partners; the IDEA cryptographic cipher described in U.S. patent number 5,214,703, licensed from Ascom Tech AG; and the Northern Telecom Ltd. CAST Encryption Algorithm, licensed from Northern Telecom, Ltd. IDEA is a trademark of Ascom Tech AG. Other product names are trademarks of their respective owners.

301-600-000004

SYSTEM REQUIREMENTS

PGP FOR BUSINESS SECURITY

Microsoft Windows 95 or Windows NT 4.0 with 8 MB of RAM and 15 MB of free disk space

Macintosh system 7.5.3 or later with 68030 processor or later, 8 MB of RAM, and 10 MB of free disk space

UNIX systems running Sun Solaris 2.5.1 or later, HP-UX 9.0 or later, IBM AIX 3.2.5 or later, SGI IRIX 5.2 or later, or Linux 1.2.13 or later; plus 8 MB RAM and 8 MB of free disk space

PGP CERTIFICATE SERVER

Sun Solaris (SPARC) 2.5.1 or later, Windows NT Server (Intel) Version 4.0; 64 MB of RAM; 15 MB disk space for software; 10-500 MB disk space for database

Network interface

CD-ROM drive

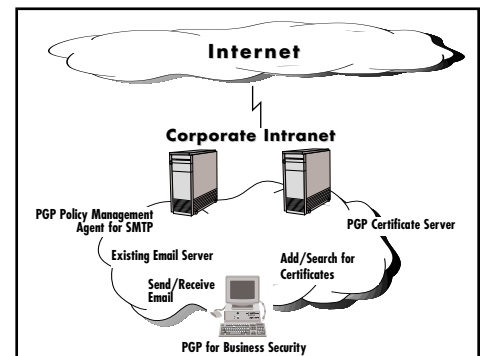
POLICY MANAGEMENT FOR SMTP

SMTP server can be run in either of two configurations:

SMTP server that can listen on a port other than 25 (the standard SMTP port) and will only allow connections from its own machine

SMTP server configured to allow connections only from the server running the Policy Management Agent for SMTP

Sun Solaris (SPARC) 2.5.1 or later, or Windows NT (Intel) 4.0



PGP Business Security Suite provides the most comprehensive set of products to safeguard your organization's digital assets.

FOR MORE INFORMATION

address: Pretty Good Privacy
2121 S. El Camino Real
San Mateo, CA, 94403

telephone: 602.944.0773

toll free: 888.747.3011

internet: www.pgp.com