P G P
CORPORATION

PGP Enterprise for Windows 8.0

Overview:

PGP Enterprise is a fully scalable encryption security solution for enterprises. PGP Enterprise provides everything you need to implement secure messaging and data storage at all levels of the enterprise. Customers can use PGP technology on the desktop, for security management, and as a PKI, or interoperate with existing PKI investments.

PGP Enterprise combines PGP Mail (encryption, digital signatures, and key management to secure your electronic mail, attachments, and instant messages), PGP Disk (create encrypted disks, whose entire contents are encrypted at all times. PGP Mail combines encryption, digital signatures, and key management to secure your electronic mail, attachments, and instant messages) and PGP Admin tools (setup and enforce policies across your organization including doing large implementations from a centralized location).

PGP products keep your confidential information secure. Whether it's in transit over a network or stored on desktops, laptops, or mobile devices, PGP prevents unauthorized access to your data. PGP products have developed a reputation for excellence based on high technical standards and long-term proven encryption solutions.

New in PGP 8.0:
- Windows XP and XP Office support
- Directory integration with Microsoft Active Directory, iPlanet Directory Server, Novell NDS, OpenLDAP Keyserver, Novell GroupWise 5.5 and 6.0 messaging client
- Enhanced Smart Card support for Aladdin eTokens
- Expanded Unicode support for multiple language and country support in keys and data
- Use one PGP key to encrypt/decrypt files across Windows, Macintosh and Palm OS
- Additional Decryption Key (ADK) management for safe enterprise data encryption
- Automatic key setup/generation, certificate request, approval, retrieval, smart card integration
- Silent pre-configured installs for easy mass deployment
- Automatic LDAP policy and keyring synchronization
- Extensive policy integration between PGP Keyserver and PGP Desktop

PGP Enterprise Solutions

PGP Enterprise includes everything required for successful implementation at each layer:

Desktop Solutions – PGP Enterprise provides secure messaging (PGP Mail) and data storage (PGP Disk) solutions on the desktop to simply and easily secure data both in transit and at rest. PGP solutions work with existing investments, such as X.509-based PKIs.

Enterprise Tools – PGP Enterprise provides a comprehensive solution for security and network administrators (PGP Admin, available during 2003) to allow them to set and enforce policy for encrypted messaging & storage solutions, and to allow them to pre-configure desktop software to conform to policy requirements prior to deployment. Once configured, the process of deploying these configurations to users, and managing their ongoing use and compliance with security policy, is drastically simplified. PGP solutions work with existing investments, such as X.509-based PKIs.

Key Infrastructure (PKI) – PGP Enterprise provides solutions (PGP Keyserver) that allow IT security to create, manage, authenticate, and revoke key, using either the PGP Keyserver or one of many LDAP-based directory services. However PGP solutions also work with existing investments, such as X.509-based PKIs, without modification to either the PKI or PGP products.

Components:

PGP Disk allows you to create disks whose contents are encrypted at all times. PGP Disk is particularly critical on laptops, which are increasingly vulnerable to being lost or stolen. By storing data with PGP Disk, users are assured that no unauthorized individual has access to it. PGP Disk can be configured to automatically un-mount after specified periods of inactivity, optionally regardless of open files for additional guaranteed security. PGP disks can also automatically be un-mounted if a computer goes into sleep mode.

PGP Mail combines encryption and digital signatures to secure your e-mail, attachments, and instant messages. While encryption ensures that a message can't be read by anyone other than its intended recipient. PGP Mail also gives you the flexibility and power to use digital signatures that guarantee the message creator's identity as well as that the message wasn't tampered with, defeating anyone attempting to alter critical communication. Use the various PGP Mail options to automatically encrypt outbound e-mails when the send button is selected.

PGP Admin allows the configuration of PGP Mail and PGP Disk before installation on individual users' machines. PGP Admin can pre-install corporate PGP keys into users' keyrings as well as require the use of additional decryption keys (ADKs) to guarantee authorized access to confidential corporate data. PGP Admin also defines the servers from which client installations automatically retrieve up to date policy settings and keyrings. Settings pre-configured by PGP Admin are cryptographically locked down: individual users cannot override them, which guarantees consistency and adherence to policies throughout an organization.

PGP Keyserver is an LDAP server with integrated support for PGP keys. When used in combination with the Keyserver Replication Engine, the PGP Keyserver can distribute and synchronize PGP keys across multiple servers. PGP Keyserver simplifies PGP key management in an enterprise by providing a web-based administration console for administrators to control both policies for keys as well as the policies of the PGP desktop clients in the enterprise. PGP Keyserver runs on Windows NT 4 SP6a, Windows 2000 SP3, and Solaris 2.8.

Key Benefits:

Strongest & Trusted Encryption
The core of all security solutions is the quality and integrity of the underlying encryption. PGP supports a variety of encryption algorithms, but only those with a 128-bit or greater symmetrical crypto key length. PGP products do not interoperate with products using low-security and easily compromised encryption systems. To ensure the integrity of its products, PGP publishes source code for peer review.

Time & Customer Tested
The true test of product quality is how it performs in real customer environments over a long period of time. PGP holds nine patents with more pending, its underlying technology has been in use for over a decade, and the current product line has evolved over the last six years. PGP products have proven themselves to be reliable and scalable during their time in use by thousands of enterprise and government organizations, and millions of individual users, including the experts in the cryptographic field.

Enterprise Manageability
Implementing effective security solutions requires the ability for security managers to set and enforce policy for encrypted messaging & data storage. PGP enterprise tools permit the pre-configuration of desktop software to conform to policy requirements, simplify its deployment, management, and ongoing use, and guarantees compliance with security policy. PGP provides a full solution from desktop, to policy and deployment, to key management and PKI.

Interoperable and Standards Based
Open standards are required for secure messaging and data security to be interoperable and therefore widely adopted; PGP is committed to non-proprietary, open standards including OpenPGP, also known as RFC 2440, and X.509. Though PGP has a full-function Keyserver product, it is PKI agnostic, supporting certificates and PKIs from all standards-conforming vendors. PGP supports LDAP-based directories inluding, iPlanet, Microsoft Active Directory, Novell NDS as well as wide range of SmartCards and other PKCS#11 tokens. PGP is has been certified as FIPS 140-1 compliant, a standard used by the U.S. and Canadian governments.

Multiple Platforms & Mail Systems
Security issues have proliferated with the growth of portable, and personal electronic devices. For security to be effective, users of all platforms and mail systems must be able to work together using the same products and keys. On Windows, PGP supports versions from Windows 95 to Windows XP. On Macintosh, PGP has products for both Mac OS 9 and Mac OS X. For mobile users, PGP currently offers Palm OS and Windows CE solutions. Via

its SDK, PGP supports a variety of Unix systems. PGP products work in environments with Microsoft Outlook and Exchange, Lotus Notes, Novell GroupWise, and Eudora solutions.

End-to-End Security
A complete security solution requires messages and data to be protected in transit, at rest, and at every point in between. PGP solutions protect user data while stored on the sender's desktop, when it's within an outbound encrypted email message, while in transit within the perimeter of firewall-protected company network, across all its stops across the Internet, within the receiver's company network, to the receiver's desktop email folder, and in storage on the receiver's desktop. PGP solutions protect information end-to-end.

Advanced Key Features
The reconstruction, and recovery of keys is part of the practical reality of managing corporate security. A balance must be struck between keeping information secure and the need for a company to recover proprietary information held by its employees. PGP offers a variety of options including key reconstruction, integration of additional corporate decryption keys (ADK), and split keys that require multiple individuals to cooperate to recreate a key, such as an ADK.

Technical Specifications

Public Key Formats	*Symmetric Key Algorithms*	*Hashes*
OpenPGP RFC 2440	AES with up to 256-bit keys	SHA-1
X.509	CAST	MD5
	TripleDES	RIPEMD-160
	IDEA	
	Twofish	

Public Key Formats	*Network Protocols*
Diffie-Hellman	TLS/SSLv3 with OpenPGP Extensions
DSS	
RSA v4 up to 4096-bit	

Desktop Systems Supported	*PGP Admin Supports:*
Windows XP SP1	PGP Keyserver
Windows 2000 SP2 and SP3	Lotus Notes 4.5, 4.6, R5.x
Windows NT SP6a	Windows XP SP1
Windows ME	Windows 2000 SP2 and SP3
Windows 98SE	Windows NT SP6a
Windows 98	Windows ME
	Windows 98SE
	Windows 98

PGP Mail Supports:
Microsoft Outlook 97, 98, 2000, and Outlook XP
Microsoft Outlook Express 4.x and 5.x
Lotus Notes 4.5.x, 4.6.x, and R5.x
Server-side support for the Lotus Notes plug-ins
Novell GroupWise 5.5 and 6.0 messaging client
ICQ 99b-2001b Instant Messenger

Note: Users of Windows 95 must use PGP 7.0.4 for Windows.
    To purchase, users order a PGP 8.0 license plus an Install Kit for PGP 7.0.4