P G P
CORPORATION

PGP Personal for Windows 8.0

Overview:

Corporations aren't the only ones who need to keep their confidential information secure, whether it's in transit over a network or stored on desktop or laptop computers. PGP Corporation recognizes the need of small businesses and individuals to conduct their business without worrying about communications being intercepted, or the data on personal computers being accessed by others.

PGP Personal is a single-user product that includes the same core PGP Mail and PGP Disk capabilities as our corporate Desktop product. PGP Mail encrypts electronic mail, files, and Instant Messages, and also provides the ability to create and manage PGP keys; PGP Disk transparently encrypts disks. Together, these two provide ironclad security for your confidential information.

PGP Personal cannot be pre-configured using PGP Admin and thus does not support the creation of keys with Additional Decryption Keys, nor does it automatically integrate into an enterprise's public key hierarchy. PGP Personal is for individuals that do not require enterprise features such as integration with Exchange, Notes, or GroupWise servers.

New in PGP 8.0:
- Windows XP and XP Office support
- 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

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.

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.

Key Benefits (continued)

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 options including key reconstruction, integration of additional corporate decryption keys (ADK), and split keys that require multiple individuals to cooperate to recreate a key.

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 Mail Supports*:
Windows XP SP1	Microsoft Outlook 97, 98, 2000, and Outlook XP
Windows 2000 SP2 and SP3	Microsoft Outlook Express 4.x and 5.x
Windows NT SP6a	Lotus Notes 4.5.x, 4.6.x, and R5.x
Windows ME	Server-side support for the Lotus Notes plug-ins
Windows 98SE	Novell GroupWise 5.5 and 6.0 messaging client
Windows 98	ICQ 99b-2001b Instant Messenger

Note: Users of Windows 95 must use PGP 7.0.4 for Windows.