# PGP® Command Line for IBM® iSeries™

Proven encryption for data storage, transfer, and backup

Part of the PGP® Encryption Platform

## Secure files for network transfer, online storage, or backup

PGP Command Line enables IBM iSeries administrators to automate the encrypted transfer and backup of large volumes of business data to help ensure compliance with corporate mandates and information security regulations.

### PGP Command Line secures data:

- Moving to and from remote corporate offices, partner, or customer sites over internal networks or the public Internet
- Residing on servers accessible by local system administrators or exposed to other unauthorized personnel by gaps in the local security infrastructure
- Transferred for offsite storage and in danger of being lost, misplaced, or stolen

### Automating Business Information Security

Using PGP Command Line, an organization can:

- Easily integrate information security into existing automation scripts and backup systems
- Ensure confidential information is protected by strong encryption no matter where it resides
- Leverage existing infrastructure and work with business partners with support for OpenPGP keys, X.509 certificates, PGP Universal™ Server, and PGP keyservers
- Retain corporate recovery and access to encrypted data when necessary using patent PGP Additional Decryption Key (ADK) technology

### Interoperable Solutions

PGP Command Line for iSeries is fully interoperable with PGP Command Line for UNIX and Windows systems and other PGP® Encryption Platform–enabled applications, including PGP® Desktop, PGP® Whole Disk Encryption, and PGP Universal Server as well as the PGP® Global Directory service. Based on OpenPGP, an open standard encrypted message format, PGP Command Line interoperates across applications and platforms.

## Enterprise Benefits

### Protect Data Instead of Writing Code

- Encryption can be quickly added to new or existing processes instead of spending time writing new programming code.
- Systems administrators can use existing scripting skills to quickly add encryption.

### Corporate Data Access & Retention

PGP Command Line allows the use of an ADK to ensure confidential information is available when needed—a policy requirement in many organizations—in the event of key loss or as required by regulatory mandates.

## Business Partner Benefits

### Protect Partner & Supply Chain Networks

- Broad platform support across Windows and UNIX operating systems in addition to IBM iSeries and IBM® zSeries®
- Easy scripting integration so partners can quickly add encryption without burdensome coding, eliminating the need to learn new programming tools

### Support for Small Business Partners

For ad-hoc transfers and sending data to partners without existing encryption software, PGP Command Line supports:

- Creation of PGP® Self-Decrypting Archives (SDAs), com-pressed and encrypted archives packaged as an executable

## Features

### Scripting & Application Integration

Encryption, digital signatures, and secure file deletion with PGP Command Line easily integrate into existing scripts. PGP Command Line can be called from:

- Popular scripting languages, including PERL, Shell Scripts, and Windows batch files
- Applications and other programming languages

### Comprehensive Enterprise Platform Support

In addition to IBM iSeries and IBM zSeries mainframe and midrange systems, PGP Command Line is available on five UNIX-based operating systems and Microsoft Windows.

### PGP Zip

- PGP Zip archives are compatible across supported operating systems.
- PGP Zip archives are also compatible with PGP Desktop, PGP Whole Disk Encryption, and PGP NetShare clients.

### PGP Self-Decrypting Archives

Encrypted files and directories can be packaged into a single PGP Self-Decrypting Archive (SDA). SDAs can be created and executed on any of the UNIX and Windows operating systems supported by PGP Command Line.

### Secure File Deletion

PGP Command Line includes integrated secure file wiping that permanently removes deleted files by overwriting data.

### Directory Integration

PGP Command Line can search and retrieve OpenPGP keys from PGP Universal Server, the PGP Global Directory, and PGP keyservers. X.509 certificates can be retrieved from PGP Universal Server and LDAP v3 directories.

### Support for Long-Term Data Access & Retention

With patented PGP Additional Decryption Key (ADK) technology, PGP Command Line provides organizations the option of retaining data access in the event the original decryption key(s) are no longer available or when required by security policy or regulatory mandate.

### Advanced Key Management – Key Splitting

To protect against misuse by one or more unauthorized administrators, PGP Command Line allows organization to split a PGP key into multiple shares. A minimum number of authorized share holders are required to authorize key use.

## Technical specifications

### Supported Operating Systems

- IBM i5/OS™ V5R3*
- IBM OS/400® V5R1*
- SUSE® Linux Enterprise Server 9.0
- Red Hat Enterprise Linux 4

### Scripting & Batch Interfaces

- i5/OS and OS/400: CL & other batch control interfaces
- Linux: Shell Scripts, PERL, & other scripting languages

### Public Key Formats

- OpenPGP RFC 2440
- X.509 v3

### Directory Servers

- LDAP
- PGP Universal Server
- PGP Global Directory
- PGP keyservers

### Symmetric Key Algorithms

- AES (up to 256-bit keys)
- CAST5
- TripleDES
- IDEA
- Twofish
- Blowfish[1]

### Public Key Algorithms

- Diffie-Hellman (up to 4096-bit keys)
- DSA (1024-bit keys, verification up to 3072 bits)
- RSA (up to 4096-bit keys)

### Hashes

- SHA-1, SHA-256,
- SHA-384, SHA-512
- MD5
- RIPEMD-160

### Compression Algorithms

- Zip
- BZip2
- ZLib

(For current product specifications, see www.pgp.com/products/pgp_commandline/mainframes/techspecs.html)

* Coming soon

[1] Support for Blowfish is limited to decrypting existing messages encrypted with Blowfish or encrypting to existing keys that specify Blowfish as the preferred cipher.

PGP Corporation
www.pgp.com

PGP Corporate Headquarters
Tel: +1 650 319 9000

PGP (GB) Ltd.
Tel: +44 (0) 208 622 3039

PGP Deutschland AG
Tel: +49 69 838310 0

PGP Japan K.K.
Tel: +81 03 4360 8308