

PGP COMMAND LINE 9 FOR IBM SYSTEM Z

FREQUENTLY ASKED QUESTIONS

HOW IS PGP COMMAND LINE 9 DIFFERENT ON THE IBM Z PLATFORM?

PGP Command Line 9 on the IBM System z platform is a full port of the product and works the same way as it does on Windows, Linux and UNIX platforms. You have all of the normal PGP encryption, decryption, file signing, and key management functions that you would have on any platform. For example, PGP on the System z platform can use keys on a public PGP key server and keys stored on a PGP Universal server. You can create self-decrypting archives for all of the normal supported platforms including Windows and Linux. There are some minor limitations for the IBM System z platform that are documented in the PGP z/OS User Guide.

IS PGP COMMAND LINE 9 ON THE IBM SYSTEM Z COMPATIBLE WITH PGP ON OTHER PLATFORMS?

Yes, you can encrypt on the IBM System z and decrypt on Windows, Linux, UNIX, IBM System z, IBM System i, Apple OSX, and other platforms. Files encrypted on those platforms can be decrypted on the IBM System z. PGP Command Line 9 is also compatible with the Open PGP standard and can work with GNU Privacy Guard (GPG) and other encryption products based on the open standard (see RFC 2440 for the Open PGP standard).

DOES PGP COMMAND LINE 9 RUN IN Z/OS BATCH?

Yes, PGP Command Line 9 runs in normal z/OS Batch environments. When you purchase a license to PGP Command Line 9 on System z you have the choice of running the z/OS Batch version, or the USS version. Most System z customers prefer to use the z/OS Batch version as it provides a familiar JCL implementation and integrates with their systems management, and security strategy better than USS/OMVS applications. However, you can install and use the USS version if you wish. The USS version runs from OMVS and can be scripted like any OMVS application.

HOW IS PGP INSTALLED ON THE IBM SYSTEM Z?

PGP Command Line 9 for the IBM z platform is delivered in a compressed zip file that you uncompress on your PC. A pass phrase is required to uncompress the file. Instructions are provided in the Readme file and in the PGP z/OS documentation on how to install the PGP software.

WHAT DOCUMENTATION IS PROVIDED FOR THE IBM SYSTEM Z?

The documentation set includes an Introduction to PGP, a PGP User's Guide that applies to all PGP platforms, and a PGP z/OS User Guide that provides information specifically for the IBM System z platform.

WHAT VERSIONS OF Z/OS ARE SUPPORTED?

PGP Command Line 9 for IBM z can run on any version of z/OS from 1.7 and later.

IS PGP FIPS-140-2 CERTIFIED?

Yes, the PGP Command Line 9 cryptographic functions have been certified and re-certified to the FIPS-140-2 standard many times over the years. PGP meets the recommendations of many compliance regulations for the use of industry-approved methods, independent review, and NIST certification.

HOW IS PGP LICENSED?

You have many licensing options for PGP Command Line 9 including a system-wide machine license, a logical partition license, and a subscription license. You will need to provide system information to your account manager in order to create the license. Evaluation licenses can be provided that expire on a certain date. During the evaluation period the PGP application is fully functional.

DOES PGP USE ICSF ENCRYPTION HARDWARE ON Z/OS?

PGP Command Line 9 is currently being enhanced to work with the ICSF cryptographic facility and hardware accelerators. This enhancement will be provided at no charge to current customers. The enhancement is expected in early 2011.

HOW MUCH DISK SPACE IS REQUIRED FOR PGP COMMAND LINE 9?

The application and related configuration files require approximately 25 megabytes of disk storage. Any files you encrypt or decrypt on the IBM System z will require additional storage.

HOW MUCH MEMORY IS REQUIRED FOR PGP COMMAND LINE 9?

We recommend a minimum of 1 Gigabyte of main storage for use of the program. The application does not have special memory requirements and will function like any other application on your IBM System z platform.

HOW DOES PGP HANDLE EBCDIC FILES?

PGP can encrypt both EBCDIC files as well as ASCII files. The internal header information of a PGP files is in the ASCII character set, but the payload that is encrypted can be either EBCDIC or ASCII. If the recipient uses as ASCII system such as Windows, Linux, or UNIX, you will want to convert the EBCDIC file to the ASCII character set before encrypting the file. You can do this with standard IBM commands, or with utilities provided with PGP Command Line 9.

CAN PGP BE USED IN MY BATCH PROGRAMS?

Yes, PGP can be called from JCL to manage keys, encrypt or decrypt a file, and so forth. The program is called in the normal way and passes parameters for the input and output file names, key name, and so forth. The PGP Command Line 9 z/OS User Guide provides over 20 examples of how to call PGP in a z/OS batch application.

ARE VSAM FILES SUPPORTED?

Yes, you can encrypt and decrypt VSAM files. Both fixed length records and variable length records are supported. See the PGP Command Line 9 z/OS User Guide for examples of VSAM file encryption and decryption.

WHERE DOES PGP STORE ENCRYPTION KEYS?

PGP can use keys stored on a public PGP key server, on a PGP Universal key server, and on your local system. When storing keys on your local system, PGP stores the keys in a PDS data set. You can easily place the keys under RACF, ACF2, or Top Secret access control. If you are using the USS version of PGP, keys are stored in user directories in the USS file system.

CAN PGP WORK WITH A KEY STORE?

Yes, PGP Command Line 9 can access keys on a PGP key server on the local network or the Internet, and can access keys stored in a PGP Universal key server.