



## OpenPGP Encryption Option

"PGP has been sufficiently influential that its algorithms and data formats have been standardised [as] an Internet standards-track specification known as OpenPGP."

—Wikipedia PGP Pretty Good Privacy Article

The MOVEit Central client software from Ipswitch is a powerful managed file transfer (MFT) solution that enterprise IT staff use to automatically "pull, process and push" files between a wide variety of internal and external systems, including Ipswitch MOVEit DMZ secure MFT servers. MOVEit Central does this using easy-to-create tasks (*no scripting or programming needed*). It can easily manage multiple tasks simultaneously, with each running on its own scheduled, event-driven or ad hoc basis. Tasks can also process files using built-in functions as well as with sample and custom VBS scripts.

The following built-in PGP encryption/decryption and key management functions are provided by the MOVEit Central OpenPGP option, which uses commercially licensed software from Veridis.

- **Encrypt, Encrypt-and-Sign, and Decrypt Files** as part of a new or existing task.
- **Create Public/Private Key Pairs** and password protect each private key.
- **Import Public/Private Key Pairs** from OpenPGP key generating applications, and password protect each imported private key.
- **Import ASCII-Armored and Binary Public Keys** including multiple keys as a single file if (like GnuPG/GPG) the application exporting them can create such a file.
- **Export ASCII-Armored Public Keys** as a text file, with the option to send the key to a specified address as an email file attachment.
- **Backup Keyring Contents** in the vendor neutral ASCII-armored format.
- **View and Delete Keys** on the MOVEit Central keyring.

In addition to the above, the OpenPGP option offers the ability to specify SHA1, SHA256 or SHA512 signing hash algorithms, and to force the use of older version 3 signatures (as per RFC 1991).

All of these MOVEit Central capabilities are fully compatible with all other OpenPGP software products (including, but not limited to, GNU Privacy Guard (GnuPG/GPG), McAfee eBusiness Server, Veridis FileCrypt, and PGP Command-Line by PGP Corporation).

Commercial use of the OpenPGP option requires payment of a one-time license fee and an annual maintenance fee. The option permits unlimited use of the OpenPGP capabilities with a commercially licensed MOVEit Central (v.5.2 recommended). Maintenance provides unlimited access to MOVEit support staff between 8:00 AM and 6:00 PM Central US time (0800—1800 GMT-6) Monday through Friday, 24/7 access to the MOVEit support site, and upgrades to new versions at no additional cost.

### Public Key Formats

- OpenPGP (RFC 2440, 1991)

### Compression Algorithm

- ZIP

### Symmetric Key Algorithms

- AES-128, AES-192, AES-256
- IDEA, 3DES ("Triple DES"),
- CAST5 (RFC 2144), Twofish

### Public Key Algorithms

- DSA up to 1024 bits
- RSA "legacy" up to 4096 bits
- RSA up to 4096 bits