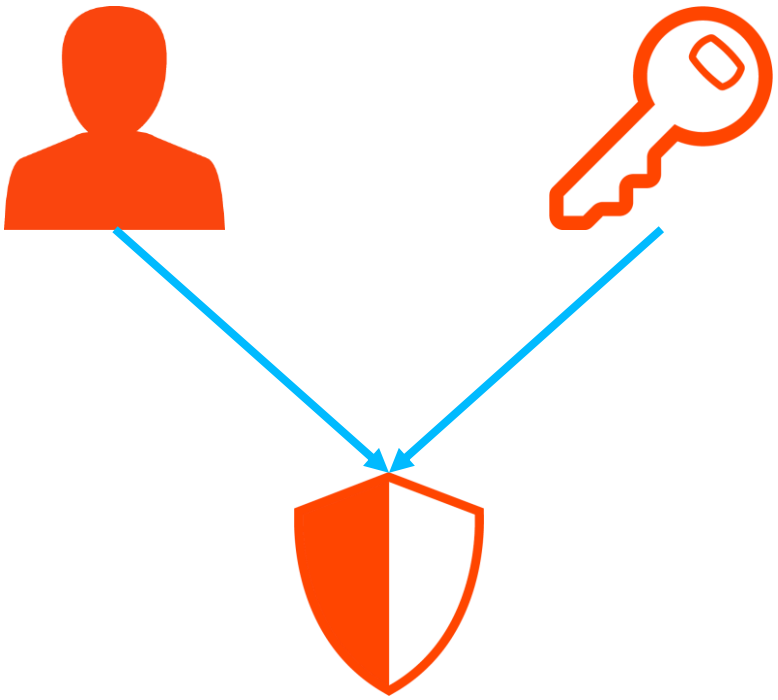
PGP Encryption

Overview

These days, everyone and everything is interconnected on the web, so security breaches easily become widespread. Transferring files between devices multiplies the risk of data being exposed to unauthorized entities. So files must be encrypted from source to target- oftentimes between different platforms, environments and devices- with the highest level of efficiency and accountability.

The world has chosen PGP to be the standard for file encryption; indeed file encryption is a basic requirement for industry regulations such as PCI-DSS, HIPAA, SOX, FDA and others.



The iSecurity PGP Solution

Raz-Lee's PGP for File Encryption solution allows users to encrypt IBM i files using a public encryption key. The product supports multiple encryption algorithms, including AES and TDES. Only users possessing the correct private key can decrypt and open the protected files. The product also provides key management capabilities, enabling users to create, import, and export the keys needed to encrypt and decrypt files.

Raz-Lee's PGP implementation provides a wide set of CL commands which cover virtually all aspects of PGP, including encryption, decryption, signing, identifying fingerprints, creating key pairs, import, export, keeping key stores and more.

PGP for File Encryption supports unlimited sets of definition parameters to preserve different settings that may be required for different uses. A simple CL program can then be created and made part of the regular process. This eliminates manual processes and ensures that the entire transmission is encrypted end to end.

Files can be automatically encrypted and transmitted to recipients. Received files can be automatically decrypted and processed by user applications.

PGP encryption uses a combination of encryption methodologies such as hashing, data compression, symmetric-key cryptography and public key cryptography to keep data secure.

This process can be used to encrypt any type of Native or IFS file or directory.

Product Features

- Helps protect sensitive IBM i data
- Helps secure e-mail communications with automatic, policy-based message encryption.
- Supports regulatory compliance requirements
- Prevents the need for manual processes to first transfer files to a PC and then encrypt them
- Ensures real end-to-end encrypted transmissions