PGP Encryption

DATASHEET (iSecurity Suite Encryption)

World Standard for File Encryption

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 requirement for industry regulations such as PCIDSS, HIPAA, SOX, FDA and others.

iSecurity PGP Encryption At a Glance

iSecurity PGP for File Encryption solution allows users to encrypt IBM i files using a public encryption key.

Advantages:

- Supports multiple encryption algorithms, including AES and TDES
- Only users possessing the correct private key can decrypt and open the protected files.
- Built to support also multi-site, multi-LPAR organizations
- Key management capabilities, enabling users to create, import, and export the keys needed to encrypt and decrypt files

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

Key Features

- Helps protect sensitive IBM i data.
- Secures 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.

Installation Requirements

- Operating system 7.1 or higher
- 300 MB of disk space for initial installation

Compliance and Encryption

Files can be automatically encrypted and transmitted to recipients. Received files can be automatically decrypted and processed by user applications. This process can be used with any type of Native or IFS file or directory.

Raz-Lee's PGP implementation provides a wide set of CL commands which cover virtually all aspects of PGP, including:

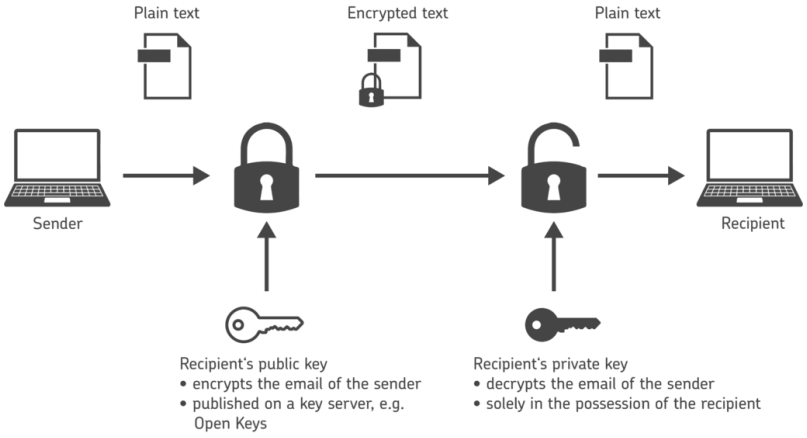
encryption, decryption, signing, identify fingerprints, creating key pairs, import, export, keeping key stores and more.

iSecurity PGP Encryption Benefits

iSecurity PGP Encryption allows you to encrypt files that are transferred to the cloud or to encrypt files on the cloud that are to be transferred to on-premises.

CLOUD Advantages:

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



Let's Get Started

Schedule your Demo and start protecting your data transmission and expediting compliance with iSecurity PGP Encryption

RAZ-LEE iSecurity