IBM i Encryption Suite
- Field (Column) Encryption
- PGP for File Encryption

iSecurity

Field (Column) Encryption

Data encryption is an increasingly essential element of effective computer security systems.

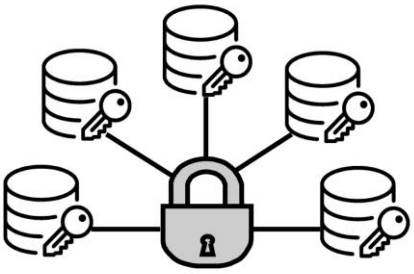
Encryption is the final layer of protection for your business-critical data from those who managed to pass through your other protection techniques. So, even if the data is accessed, it is entirely meaningless.

Encryption is also the way to ensure that those who are entitled to access your data will see the data in clear text, masked, scrambled, or not see it at all, as appropriate.

PCI-DSS, HIPAA, and other regulatory bodies require encrypting sensitive parts of the data.

Raz-Lee Security's iSecurity Encryption solution, part of the iSecurity suite, allows you to fully protect all sensitive data and will give you full ROI within a very short period of time.

IBM i 7.1 introduced the database exit program FIELDPROC. Using this feature for encryption makes it part of the database capabilities and eliminates use of additional files.



Multiple IBM i LPARs using single IBM i Key Manager

Designed after the FIELDPROC announcement, the product does not need to have backward capability with outdated technology – providing efficiency and simplicity.

Finding Sensitive Data Fields

A fully comprehensive system is provided to help you discover ALL your sensitive fields. All database fields are considered and the product offers selection aids based on field size, name, text, and column headings. This prevents a situation where sensitive data is kept in the clear in a forgotten, copied version of a file.

Product Features

Unique design provides a more efficient product, which ensures that making your data safer does not require you to invest in additional resources.

With iSecurity Encryption:

- Your files are never locked. They are available for application use even when encryption keys are refreshed.
- Master Keys as well as Data Keys can be automatically changed, unattended.
- In a multi-site environment, a single key manager can be set to support all sites, centralizing all keys-related activity.
- Keys are hexadecimal based rather than character based. This provides much stronger encryption for the same usage of computer resources. For example, in AES 256, hex based keys are 10^{18} stronger.
- The product is optimized towards displaying the standard masked data. Choosing this option greatly reduces performance impact.
- Key Manager, Data Manager, and Token Manager can optionally be installed on different IBM i LPARs.
- Supports both Encryption and Tokenization.
- Policy driven security and limitation of capabilities ensures Separation of Duties
- Comprehensive logs for tracing of activities
- Full journaling system guarantees that any change in parameters is logged
- Uses NIST encryption standards
- Adheres to both PCI and COBIT standards
- 128-bit, 192-bit, and 256-bit AES encryption supported
- Based on IBM Native APIs

PGP 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; 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 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.

The product 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.

Raz-Lee's PGP for File Encryption solution allows users to encrypt IBM i files using a public encryption key. The software 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.

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

Together, iSecurity PGP encryption & iSecurity Field Encryption, make your IBM i a safer place to store and use data!