Field Encryption

DATASHEET (iSecurity Suite Encryption)

First Way to Secure Your Data

Encryption is the process of encoding information. Encryption is vital for protecting confidential information and expediting compliance with PCI-DSS, GDPR, HIPAA, SOX, other government regulations and state privacy laws.

Restricting access is sometimes sufficient, but encryption is stronger

What's Field Encryption used for?

Information that usually needs to be encrypted:

- Credit Card Numbers
- Personal Information, Medical information
- Account numbers, ID numbers
- Passwords

Segregate the way data is displayed:

- Clear text 5201 1234 5554 0830
- Masked **** **** **** 0830
- No data ----------

iSecurity Field Encryption At a Glance

iSecurity Field Encryption solution, part of the iSecurity suite, allows you to fully protect all sensitive data without modifying your software. A change that is done externally without changing the Level-Check of your file (i.e. Files remain intact), but is reflected in:

- Your programs, regardless of whether they use SQL or Native IO
- Any system utility including FTP, Query, DFU
- DB-Journal

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. iSecurity Encryption was designed after the FIELDPROC announcement and does not need to have backward capability with outdated technology – providing efficiency and simplicity.

Key Features

- Files are never locked; they are available for application use even when encryption keys are refreshed.
- Supports all types of data: Character, Zoned Decimal, Packed Decimal, Clob and Blob. Supports null-capable data as well as non-null-capable data.
- Comprehensive Find Sensitive Fields system provides superior quality in finding based on iterations over partial estimation of size, type, name, text, etc.
- Works on a wrapper program thus does not require the program source.
- Optimized for data masking and consumes no CPU for decryption in such cases.
- KEK (Key encrypting 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.
- Key Manager, Data Manager, and Token Manager can optionally be installed on different IBM i LPARs.
- Supports both Encryption and Tokenization.
- Uses NIST encryption standards.
- Adheres to both GDPR, PCI and COBIT standards.
- 128-bit, 192-bit, and 256-bit AES encryption supported.
- Based on IBM Native APIs.

Installation Requirements

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

Compliance and Encryption

Encryption is also the way to ensure that sensitive data is presented in the way that suits the user, and the circumstances.

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, GDPR and other regulatory bodies require encrypting sensitive parts of the data.

iSecurity Field Encryption Keys

Supports a single Key Manager / single Token Manager for multiple Data Managers

Built to support also multi-site, multi-LPAR organizations

- Local Master Key (a feature of OS400) protects an Organization Key.
- Organization Key protects the Key Encrypting Keys (KEK)
- KEK is used to protect the Data Key
- Data Keys encrypt data
- Organization Key is entered once on each LPAR (including HA).
- Master, KEK and Data Keys can & should be periodically modified.
- There is no way to see or access any actual Key Value

Let's Get Started

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

RAZ-LEE iSecurity