Encryption

Field Level Encryption on the IBM i

SEA™ | SOFTWARE
ENGINEERING
OF AMERICA

Software Engineering of America
info@seasoft.com www.seasoft.com 516.328.7000

What is iSecurity Encryption?

Field (Column) Encryption

Data encryption is an increasingly essential element of effective IBM i security. It is the final layer of protection for all of your business-critical data, making your data entirely meaningless to those who manage to pass through your other protection layers.

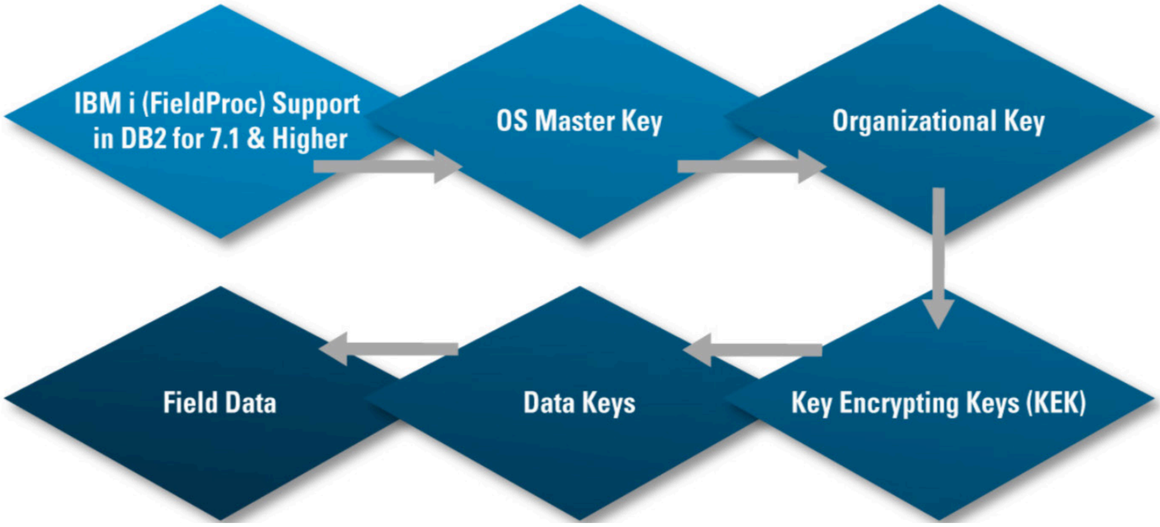
Using an encryption solution ensures that your data is viewed in clear text, masked, scrambled, or not seen at all by those who are not entitled to access your files.

To stay in compliance with PCI-DSS, HIPAA, and other regulatory bodies, sensitive parts of your data are required to be encrypted, ensuring the safety of your company and customer's critical information.

The iSecurity Encryption solution, part of the iSecurity suite, allows you to fully protect all sensitive data and meet your compliance and regulatory requirements.

IBM i 7.1 introduced exit program FIELDPROC, now added to the encryption database capabilities, reducing the use of additional files. Designed after the FIELDPROC announcement, iSecurity Encryption is compatible with the most updated versions of the IBM i, eliminating the need for backwards capabilities that come with outdated technology. The unique design provides a more efficient solution, reducing the need to invest in additional resources, to make your data safer.

Encryption Layered Architecture

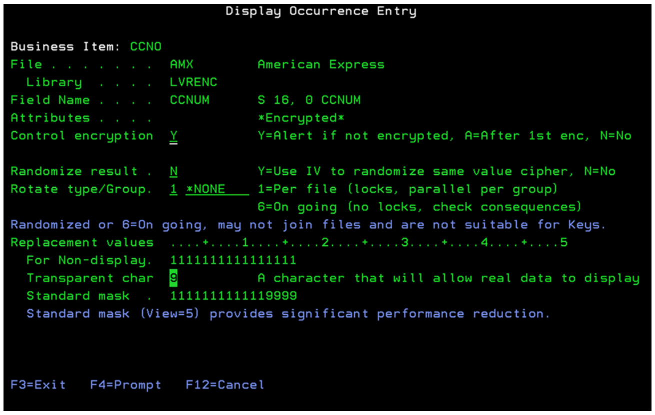

IBM i (FieldProc) Support in DB2 for 7.1 & Higher
OS Master Key
Organizational Key
Key Encrypting Keys (KEK)
Data Keys
Field Data

Layered field encryption on user authorization:

The built-in layers of Encryption segregate keys into hierarchical systems, designed to secure your keys from hackers. Even if hackers gain access to just one layer, they are still unable to break through encryption or key retrieval Using the appropriate Authorization Groups, you may enable additional security, which allows users to view the appropriate sensitive information based on specific levels of authority given.

All non-authorized users will have no access to view the data, while pre-authorized users view encrypted data as hidden, masked, or shown in clear text.

- Policy driven security and limitation of capabilities ensures Separation of Duties



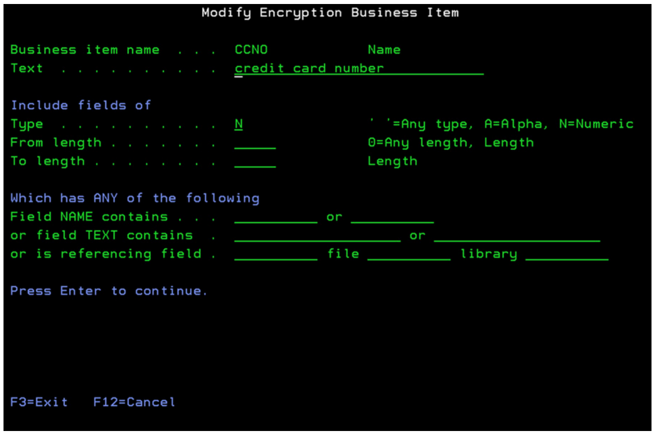
```
                        Display Occurrence Entry

Business Item: CCNO
File . . . . . . . .  AMX          American Express
  Library  . . . . .  LVRENC
Field Name . . . . .  CCNUM        S 16, 0 CCNUM
Attributes . . . . .               *Encrypted*
Control encryption    Y            Y=Alert if not encrypted, A=After 1st enc, N=No

Randomize result .    N            Y=Use IV to randomize same value cipher, N=No
Rotate type/Group.    1 *NONE      1=Per file (locks, parallel per group)
                                   6=On going (no locks, check consequences)
Randomized or 6=On going, may not join files and are not suitable for Keys.
Replacement values    ....+....1....+....2....+....3....+....4....+....5
  For Non-display.    1111111111111111
  Transparent char    9            A character that will allow real data to display
  Standard mask  .    1111111111119999
  Standard mask (View=5) provides significant performance reduction.



F3=Exit   F4=Prompt   F12=Cancel
```

Keys are kept for several generations:

Automated renewal or refreshed key operations will have no impact on accessing encrypted data that was previously encrypted by a discontinued key.

Since inactive key information is retained in the original system where the initial encryption took place, transition from old key to new key is automatic, therefore restoring and accessing older encrypted data has become less challenging.

- 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.



```
                     Modify Encryption Business Item

Business item name  . . .  CCNO             Name
Text  . . . . . . . . . .  credit card number______________

Include fields of
Type  . . . . . . . . . .  N                ' '=Any type, A=Alpha, N=Numeric
From length . . . . . . .  _____            0=Any length, Length
To length . . . . . . . .  _____            Length

Which has ANY of the following
Field NAME contains . . .  __________ or __________
or field TEXT contains  .  ____________________ or ____________________
or is referencing field .  __________ file __________ library __________

Press Enter to continue.





F3=Exit   F12=Cancel
```

Sensitive data fields, or reference fields needing encryption can be easily identified:

Interrogate files using search utility to locate and select the appropriate fields slated for encryption.

- A fully comprehensive system is provided to help you discover all of 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 clear in a forgotten and copied version of a file.

Multi LPARs managed with a single key:

You can select a controlling system to manage all keys from a central repository. Additionally, you could restrict configuration access on that system so that unauthorized changes are not allowed.

- In a multi-site environment, a single key manager can be set to support all sites, centralizing all key-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 1018 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.

Full log trail for encryption definition changes:

You can select a controlling system to manage all keys from a central repository. Additionally, you could restrict configuration access on that system so that unauthorized changes are not allowed.

With our fundamental logs and reports, you can fulfill your Audit and Compliance requirements.

- Full journaling system guarantees that any change in parameters is logged
- Uses NIST encryption standards
- Adheres to both PCI and COBIT standards
- Supports 128-bit, 192-bit, and 256-bit AES encryption
- Based on IBM Native APIs

Software Engineering
Raz-Lee
Security
Partner
of America

Key Features

- Based on IBM Native APIs
- Works transparently with all kinds of applications
- Supports DDS and SQL defined files
- Supports Traditional I/O as well as SQL access
- Supports AES 256, 192, 128 bit encryption
- Adheres to NIST (National Institute of Standards and Technology)
- 3 Key Levels: Super Key, Master Key, Data Key
- Master Keys and Data Keys are segmented, requiring several people to define a single key
- Supports all types of data: Character, Zoned Decimal, Packed Decimal, Clob and Blob
- Full journaling system guarantees that any changes in parameters are logged

For a Free Trial Contact SEA Today

Call: 516.328.7000 or Visit: www.SeaSoft.com