RAZ-LEE

iSecurity

Field Encryption

iSecurity
Field Encryption

First Way to Secure Your Data

iSecurity Field Encryption is based on IBM Native APIs and supports both Encryption and Tokenization.

RAZ-LEE

What's Encryption used for?

Encryption is the process of encoding information. Restricting access is sometimes sufficient, but encryption is stronger.

Information that usually needs to be encrypted:

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

Data Segregation

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, NIS2, DORA** and other regulatory bodies require encrypting sensitive parts of the data.

Segregate the way data is displayed:

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

iSecurity Field Encryption Insights

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

Our Solution:

✓ Based on IBM Native APIs.

✓ Supports both Encryption and Tokenization.

✓ Files are Never Locked.

RAZ-LEE
iSecurity

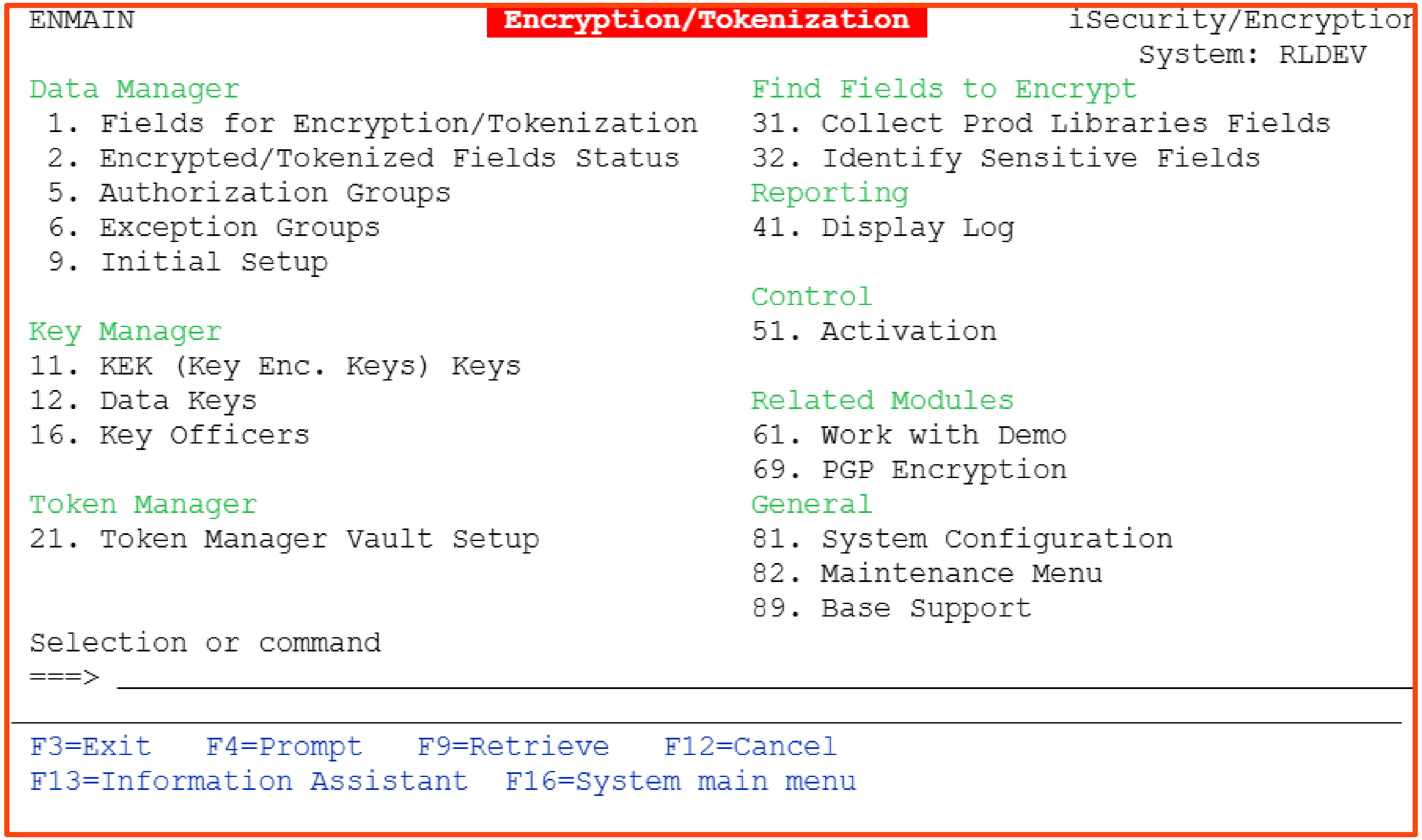
iSecurity
Field Encryption

Let’s see our Product in Action!

The best way to see how it works is a demo with **iSecurity Field Encryption** running on a real environment.

RAZ-LEE

Field Encryption Start Screen



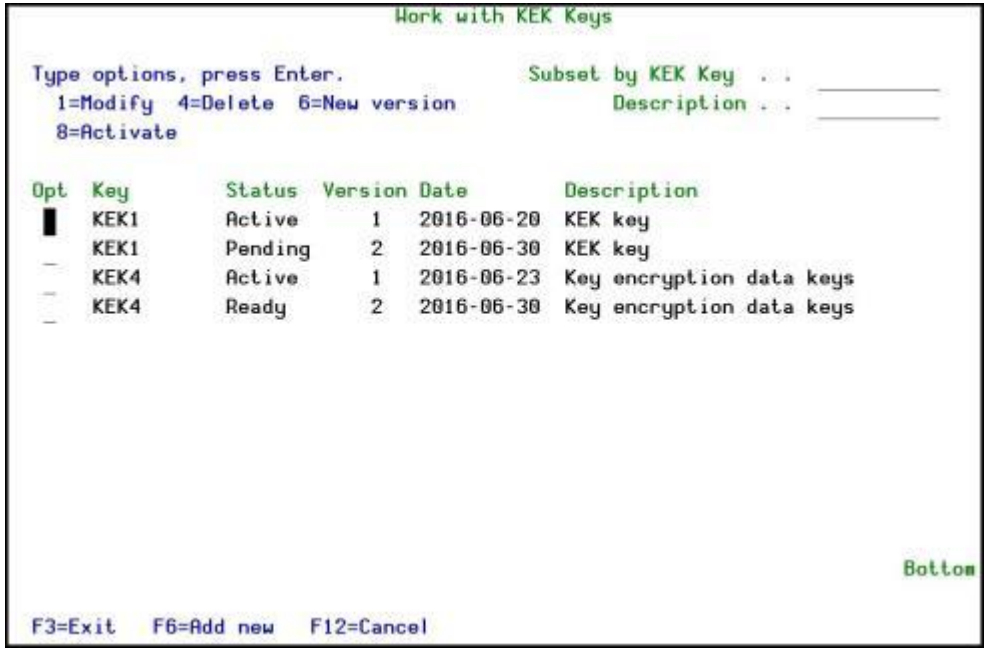
```
ENMAIN                     Encryption/Tokenization          iSecurity/Encryptio
                                                                System: RLDEV
Data Manager                             Find Fields to Encrypt
 1. Fields for Encryption/Tokenization   31. Collect Prod Libraries Fields
 2. Encrypted/Tokenized Fields Status    32. Identify Sensitive Fields
 5. Authorization Groups                 Reporting
 6. Exception Groups                     41. Display Log
 9. Initial Setup
                                         Control
Key Manager                              51. Activation
11. KEK (Key Enc. Keys) Keys
12. Data Keys                            Related Modules
16. Key Officers                         61. Work with Demo
                                         69. PGP Encryption
Token Manager                            General
21. Token Manager Vault Setup            81. System Configuration
                                         82. Maintenance Menu
                                         89. Base Support
Selection or command
===> ___________________________________________________________________________

F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel
F13=Information Assistant  F16=System main menu
```

Encryption Keys

Only Key Officers can administrate KEK Keys, and Data Keys. Define which users can perform these tasks. You can define that users who maintain KEK Keys cannot maintain Data Keys and visa versa.

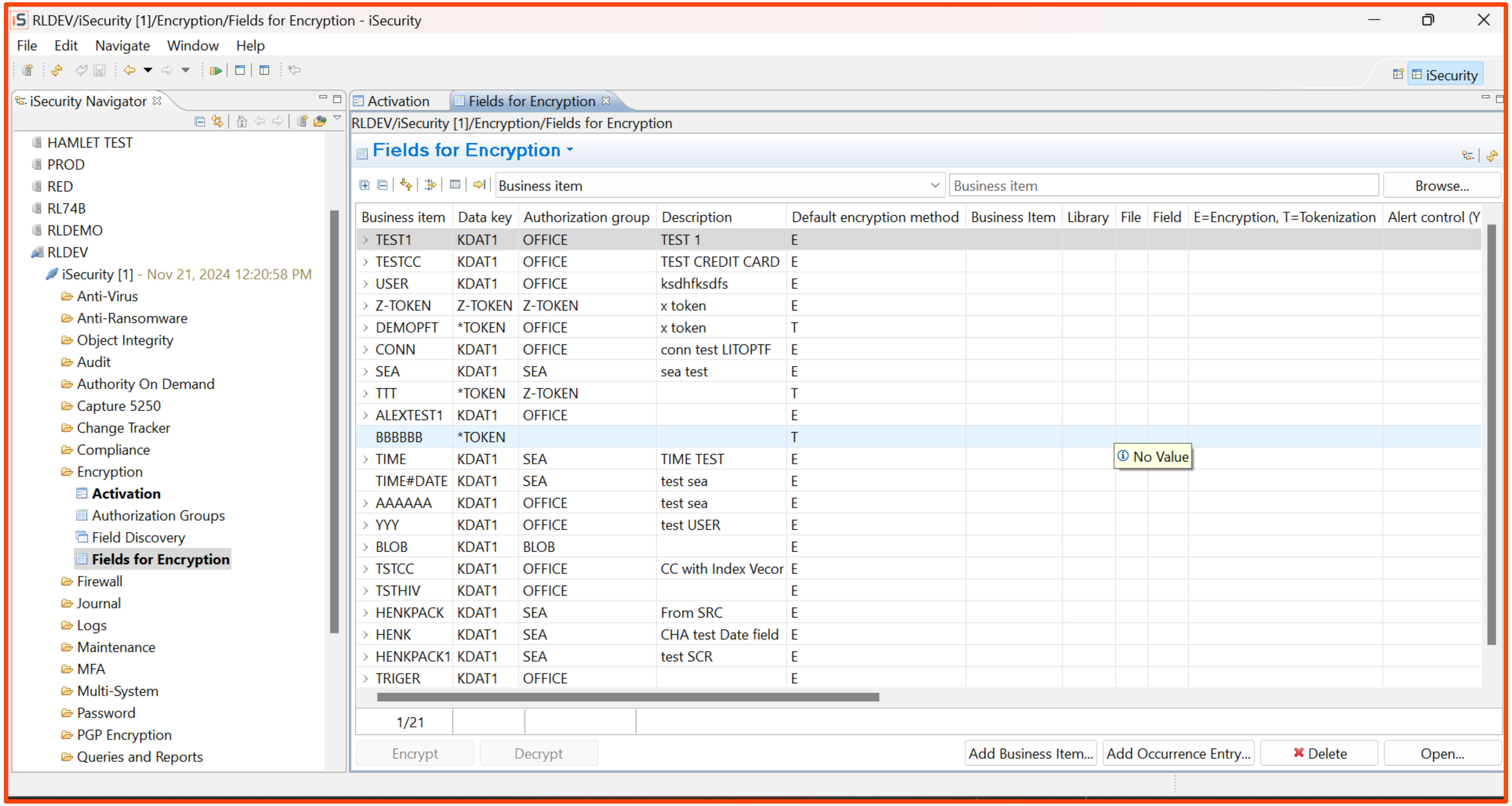
You can also limit users to be able to maintain only part of a key, so that for a new key, more than one user needs authentication.

- Supports a single Key Manager / Single Token Manager for multiple Data Managers.
- Built to support also multi-site, multi-LPAR organizations.



```
                          Work with KEK Keys

 Type options, press Enter.                 Subset by KEK Key  . .  __________
   1=Modify   4=Delete   6=New version            Description . .   __________
   8=Activate

 Opt  Key        Status   Version Date        Description
 █    KEK1       Active         1  2016-06-20  KEK key
 _    KEK1       Pending        2  2016-06-30  KEK key
 _    KEK4       Active         1  2016-06-23  Key encryption data keys
 _    KEK4       Ready          2  2016-06-30  Key encryption data keys





                                                                       Bottom
 F3=Exit   F6=Add new   F12=Cancel
```

Fields for Encryption (GUI)



iSecurity Navigator

- HAMLET TEST
- PROD
- RED
- RL74B
- RLDEMO
- RLDEV
  - iSecurity [1] - Nov 21, 2024 12:20:58 PM
    - Anti-Virus
    - Anti-Ransomware
    - Object Integrity
    - Audit
    - Authority On Demand
    - Capture 5250
    - Change Tracker
    - Compliance
    - Encryption
      - **Activation**
      - Authorization Groups
      - Field Discovery
      - **Fields for Encryption**
    - Firewall
    - Journal
    - Logs
    - Maintenance
    - MFA
    - Multi-System
    - Password
    - PGP Encryption
    - Queries and Reports

RLDEV/iSecurity [1]/Encryption/Fields for Encryption

Fields for Encryption

Business item	Data key	Authorization group	Description	Default encryption method	Business Item	Library	File	Field	E=Encryption, T=Tokenization	Alert control (Y
TEST1	KDAT1	OFFICE	TEST 1	E						
TESTCC	KDAT1	OFFICE	TEST CREDIT CARD	E						
USER	KDAT1	OFFICE	ksdhfksdfs	E						
Z-TOKEN	Z-TOKEN	Z-TOKEN	x token	E						
DEMOPFT	*TOKEN	OFFICE	x token	T						
CONN	KDAT1	OFFICE	conn test LITOPTF	E						
SEA	KDAT1	SEA	sea test	E						
TTT	*TOKEN	Z-TOKEN		T						
ALEXTEST1	KDAT1	OFFICE		E						
BBBBBB	*TOKEN			T						
TIME	KDAT1	SEA	TIME TEST	E						
TIME#DATE	KDAT1	SEA	test sea	E						
AAAAAA	KDAT1	OFFICE	test sea	E						
YYY	KDAT1	OFFICE	test USER	E						
BLOB	KDAT1	BLOB		E						
TSTCC	KDAT1	OFFICE	CC with Index Vecor	E						
TSTHIV	KDAT1	OFFICE		E						
HENKPACK	KDAT1	SEA	From SRC	E						
HENK	KDAT1	SEA	CHA test Date field	E						
HENKPACK1	KDAT1	SEA	test SCR	E						
TRIGER	KDAT1	OFFICE		E						

ⓘ No Value

1/21

RAZ-LEE iSecurity

iSecurity
Field Encryption

Advantages on our Solution

iSecurity Field Encryption allows you to fully protect all sensitive data without modifying your software.

RAZ-LEE

Disk Space Consideration

AES requires encryption in “blocks” so the disk usage space is increased. As even AES 128 is considered by NAS suitable to encrypt “top secret” documents, and as such encryption is faster, we recommend using AES 128 especially for fields shorter then 16.

Example:

For a file with a record length of 200 bytes of which 2 fields of 10 bytes should be encrypted, the record length will be:

- Original: 200
- AES 128: 232
- AES 192: 248
- AES 256: 264

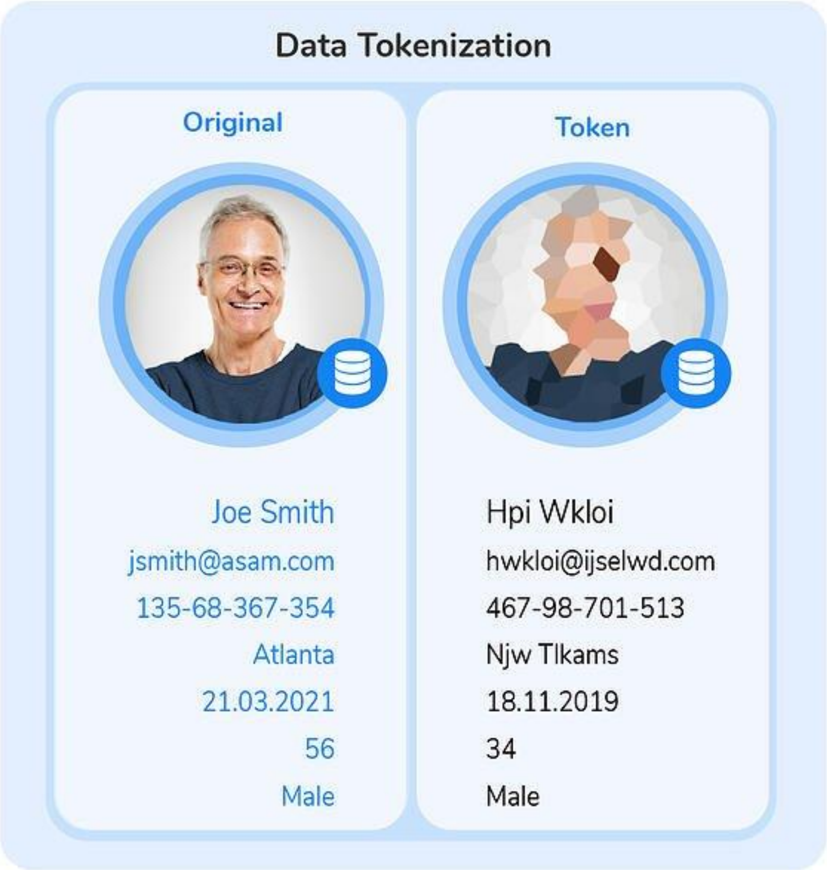
Original Length	In AES 128	In AES 192	In AES 256
1-16	16	24	32
17-24	32	24	32
25-32	32	48	32
33	48	48	64

*If the field is a Key, the length is further increased

Tokenization

Tokenization is a non-mathematical approach that replaces sensitive data with non-sensitive substitutes without altering the type or length of data.

✓ This is an important distinction from encryption because changes in data length and type can render information unreadable in intermediate systems such as databases.



Data Tokenization

Original	Token
Joe Smith	Hpi Wkloi
jsmith@asam.com	hwkloi@ijselwd.com
135-68-367-354	467-98-701-513
Atlanta	Njw Tlkams
21.03.2021	18.11.2019
56	34
Male	Male

iSecurity Field Encryption Advantages

iSecurity Field Encryption Solution is based on IBM Native APIs and supports both Encryption and Tokenization.

- ✓ 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.

RAZ-LEE

Contact us About our Products

Sales Representatives

sales@razlee.com

Visit Our Website

www.razlee.com

iSecurity

Field Encryption