RAZ-LEE

FIELD ENCRYPTION

First Way to Secure Your Data

About Raz-Lee Security

Founded in 1983, Raz-Lee Security is one of the world’s leading independent owned cybersecurity and compliance solution providers for IBM i servers (AS/400).

Raz-Lee’s flagship iSecurity suite guards organizations against insider threats and unauthorized external access to business-critical information hosted on their IBM i. We have developed cutting-edge solutions that have revolutionized analysis and fortification of IBM i servers.

We build solutions that work with other companies’ technologies allowing organizations to monitor IBM i activity via SIEM or DAM dashboards.

Technology Business Partners

imperva

IBM

McAfee™

Akamai

RSA®

SEA™ SOFTWARE ENGINEERING OF AMERICA

About iSecurity Suite

Advanced Threat Protection

- **Anti-Ransomware**
- **Antivirus** / Malware protection
  - **ICAP** Optional Client/Server for Antivirus

Authentication & Authorization

- **MFA** Multi Factor Authentication
- Self **Password Reset**
- **Authority On Demand**

Protection

- **Firewall** FTP, ODBC…access
- Monitor CL **Commands**
- **Safe-Update** to protect production files

Evaluation, Reporting & Alerts

SIEM & DAM Support

Syslog, SNMP, CEF, LEEF

Visualizer

Business Intelligence for Security

Score Cards

for GDPR, SOX, PCI, HIPAA…

Security Investigator

Data Discovery, Authority Inspector, Assessment

Encryption

- DB2 **Field Encryption** (FIELDPROC)
- **PGP File Encryption**

Data Base Solutions

- **AP-Journal** DB Audit, Filter, Alerts, SIEM
- **DB-Gate** Native SQL to Oracle, MSSQL…
- **FileScope** Secured file editor

Auditing & Response

- **Audit** Journal, System Values, Status…
- Proactive re-**Action** in real time
- **Capture** screen activity
- **Compliance** of Users, Objects, IFS
- **Change Tracker** watch Production Libraries

RAZ-LEE iSecurity

Field Encryption

First Way to Secure Your Data

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

Segregate the way data is displayed:

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

iSecurity Field 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.

Our Solution:

- Based on IBM Native APIs
- Supports both Encryption and Tokenization
- Files are Never Locked

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

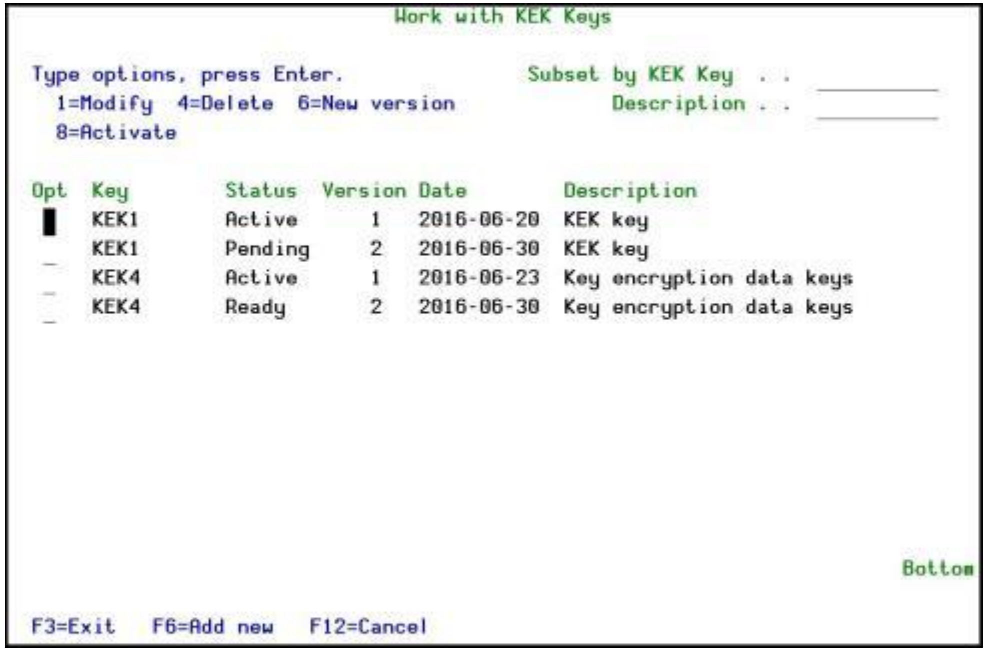
*If the field is a Key, the length is further increased

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

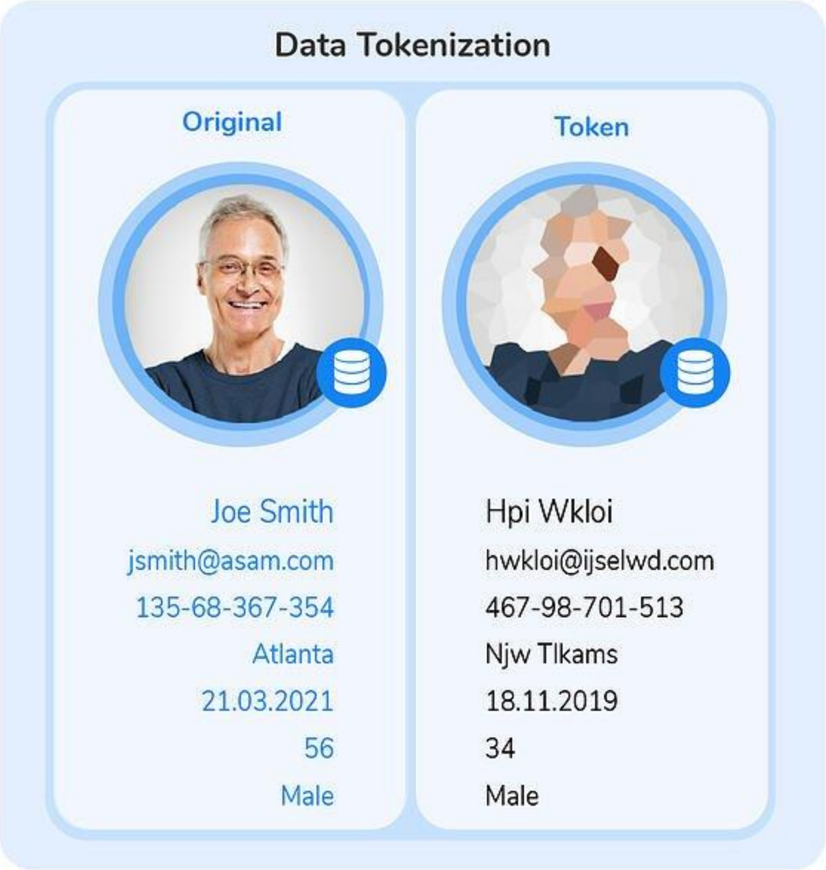


```
                         Work with KEK Keys

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
```

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

- 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

Thank You

For more information about our company and products please visit

www.razlee.com