CASE STUDY

IBM i Data Encryption & Secure File Protection

Latin American Banking Institution *Anonymized | Confidential*

Client Profile

Industry	Latin American Banking Institution
Region	Latin America
Environment	IBM i — 3 LPARs supporting core banking, customer account management, payment processing, loan administration, and regulatory reporting
Security Scope	Data Encryption, Sensitive Information Protection, Secure File Transfer, and Regulatory Compliance
Assessment Type	Data Protection & Regulatory Compliance Initiative

The Challenge

The bank processed and stored large volumes of sensitive customer and financial information within its IBM i environment. Increasing cybersecurity threats, data privacy regulations, and banking compliance requirements created a need for stronger controls protecting data both at rest and in transit.

Protection of Sensitive Financial Data

Critical banking applications contained confidential information including customer records, account details, transaction data, and personally identifiable information (PII). Key concerns included:

- Exposure of sensitive customer information to unauthorized access
- Protection of financial and personal data stored in IBM i databases
- Compliance with banking regulations and data privacy requirements
- Risk associated with insider threats and excessive user privileges
- Increasing auditor focus on encryption controls

The institution required a robust encryption strategy that could be implemented without disrupting existing banking applications.

Securing File Transfers and External Communications

The organization regularly exchanged files containing sensitive financial information with:

- Regulatory authorities
- Payment processors
- Business partners
- Clearing and settlement providers
- Internal regional offices

Existing file transfer processes lacked consistent encryption controls, creating concerns regarding data confidentiality and regulatory compliance. The bank required a secure method for encrypting and exchanging files while maintaining operational efficiency.

Solution Deployed

Raz-Lee deployed the following iSecurity modules across the IBM i environment:

iSecurity Encryption Field

Implemented field-level encryption to protect sensitive information stored within IBM i. Including:

- Encryption of sensitive customer and financial data
- Protection of personally identifiable information (PII)
- Granular control over encrypted database fields
- Secure key management capabilities
- Transparent integration with business applications
- Reduced exposure of confidential information

The solution allowed the organization to secure critical data without requiring extensive application modifications.

iSecurity Encryption Open PGP

Implemented Open PGP encryption for secure file protection and external data exchanges. Including:

- Automated encryption and decryption of files
- Protection of sensitive information during transmission
- Support for secure file exchanges with external partners
- Compliance with data protection and banking requirements

The implementation ensured that sensitive files remained protected throughout the transfer process.

Results

- Reduced Strengthened protection of sensitive customer and financial information
- Reduced risk of unauthorized access to confidential data
- Improved compliance with banking regulations and data privacy requirements
- Secured file transfers with regulators, partners, and third-party providers
- Enhanced protection of personally identifiable information (PII)
- Simplified management of encryption processes across the IBM i environment
- Increased auditor confidence in data protection controls
- Deployment completed without disruption to banking operations or customer services

The organization significantly improved its ability to protect sensitive information while meeting regulatory and compliance requirements across its IBM i infrastructure.

Key QSA Feedback

> *“Data protection is a critical requirement in the banking sector. Encryption Field allowed us to secure sensitive customer and financial information directly within our IBM i databases, while Open PGP ensured that files exchanged with external organizations remained protected at all times. Together, these solutions significantly strengthened our overall data security strategy.”*

— Chief Information Security Officer (paraphrased)