FIELDPROC Encryption for IBM i
## Encryption without Application Changes

Townsend SECURITY®

Alliance AES/400 Software Enables Automatic Data Encryption for IBM i

Alliance AES/400 performs automatic field and column level encryption using the IBM FIELDPROC exit point, available in IBM i V7R1-V7R3. Administrators can easily implement database encryption on the IBM i platform without making source code changes or altering applications [See illustration below].

In release V7R1 of the IBM i operating system IBM released column-level API called FIELDPROC or "Field Procedure". This feature of DB2/400 provides for an exit point at the column level enabling IBM i users to integrate Townsend Security's AES/400 encryption software to apply instant field and column level encryption routines without impacting applications.

Application → INSERT → FIELDPROC → ENCRYPTED → Database

Alliance AES Encryption ← Alliance Key Manager
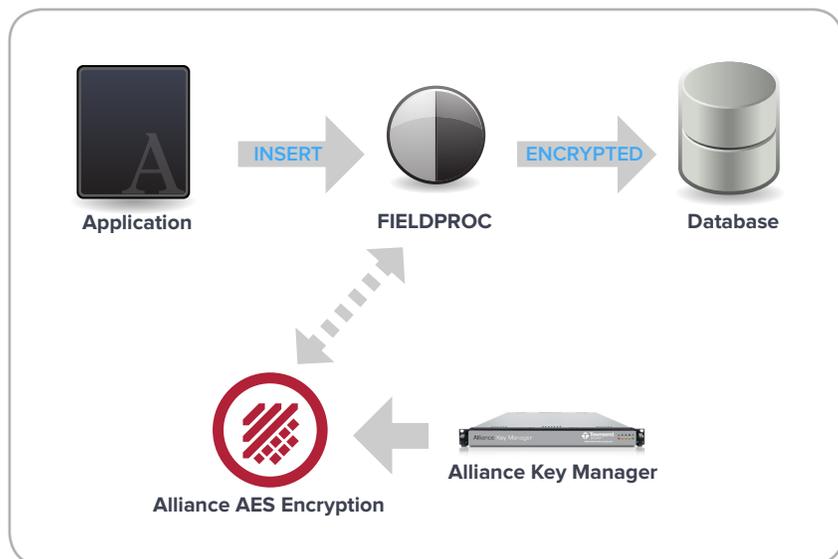
"Push Button" Automatic Encryption
Encrypt fields such as credit card numbers, SSN, birth dates, address, account numbers and other PII instantly without impacting applications.

NIST Validated AES Encryption
The only NIST validated encryption product on the market for the IBM i. Alliance AES/400 is guaranteed to always meet or exceed encryption standards held under PCI, HIPAA/HITECH, State Privacy and other regulations.

Optimized for Performance
Encrypt a large database in seconds. Alliance AES/400 APIs perform 100X faster than the competition.

Meet Compliance Requirements
An intuitive and familiar IBM i interface makes it easy to configure and manage encrypted files. Security Administrators can reduce security exposures by implementing controls about who can view decrypted data.

Key Management - Secure Your Data
Built to integrate with Townsend Security's FIPS 140-2 compliant Alliance Key Manager - Available as an HSM, Cloud HSM, VMWare, or in the Cloud (AWS or Microsoft Azure).

www.townsendsecurity.com

724 Columbia Street NW, Suite 400, Olympia, WA 98501 | 800 357 1019 +1 360 359 4400 Fax 360 357 9047

Encrypt Sensitive Information without Changing Your Database

IBM i database applications use a variety of fields to store sensitive information. Encrypt fields that store data such as credit card numbers, SSN, birth dates, address, account numbers and other PII instantly without impacting applications. Alliance AES/400 FIELDPROC support will protect access to the data without changing your database or your applications. With Alliance AES/400 there is no need to reformat your database, or expand field sizes.

Database	Field Types:	Alliance AES/400	Encrypted Data:
	Character		Social Security Number
	Zoned		Credit Card Number
	Binary		Birthdates
	Packed		Address
	Numeric		Account Numbers
	DBCS		Other PII

In addition to working with legacy RPG and COBOL applications, Alliance AES/400 FIELDPROC support also works with SQL applications. The application source code is not needed to implement Alliance AES/400 encryption.

Meet Compliance Requirements with Validated Encryption

Alliance AES/400 is the only NIST-validated AES encryption solution for IBM i V7R1-V7R3 (and all supported IBM i releases). AES/400 uses validated 256-bit AES encryption for FIELDPROC data protection.   Our customers can be certain that their solutions provably meet the high standards required by compliance regulations.

Strong Encryption

Alliance AES/400 uses National Institute of Standards and Technology (NIST) validated 256-bit AES encryption for FIELDPROC data protection. The encryption software has been independently tested by a NIST accredited Cryptographic and Security Testing (CST) laboratory certified by the National Voluntary Laboratory Accreditation Program (NVLAP), and certified as compliant by NIST. Alliance AES/400 customers can be certain that their solutions provably meet the high standards required by compliance regulations.

Optimized for Performance

The Alliance AES/400 encryption APIs are capable of encrypting 1 million credit card numbers in less than one CPU second. They are highly optimized for performance, and perform up to 100X faster than equivalent IBM APIs on the IBM i platform. These same Alliance AES APIs are used for FIELDPROC encryption.

Easily Enforce User Access Control with Data Masking

Automatic encryption and decryption works for all users and applications. Administrators cannot rely on native IBM i object or user authorities to control access to protected data, additional controls and policies must be put in place.

 Alliance AES/400 allows administrators to define which users should have access to data and exclude those who should not with data masking. Security administrators can define users who should have access to the data, and define a default policy that masks the data for others.

FIELDPROC Encryption with Legacy RPG Applications

With Alliance AES/400, IBM i customers with legacy RPG applications can deploy automatic DB2 encryption over sensitive data which are indexes. Townsend Security has leveraged OAR capabilities to replace the legacy RPG file I/O with modern SQL operations. Alliance AES/400 maps legacy RPG file operations like CHAIN, SETLL and other operations to native SQL statements, while preserving the functional integrity of the original RPG business logic.

Townsend Security

Townsend Security provides data encryption & tokenization, key management, secure communications, and compliance logging solutions to Enterprise customers on a variety of server platforms including IBM i, IBM z, Windows, and Linux. The company can be reached on the web at www.townsendsecurity.com, or (800) 357-1019.