syncsort

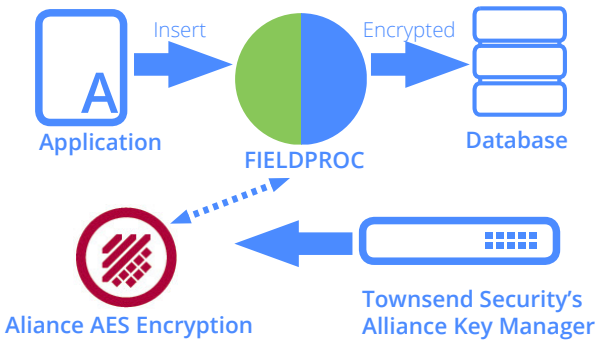
PRODUCT SHEET

Alliance AES/400

FIELDPROC Encryption for IBM i without Application Changes

In release V7R1 of the IBM i operating system IBM released a new column-level API called FIELDPROC. IBM also referred to this as "Transparent Encryption." This new feature of Db2/400 provides for an exit point at the column level and many IBM i users will be able to implement encryption and decryption without making any changes to their application source code. IBM does not provide any exit point software, they only provide the ability to register a user exit point for the column. While IBM initially called this "Transparent Encryption," the FIELDPROC exit point can be used for many purposes other than encryption. For example, an application can tokenize data, monitor column level usage, mask data, and so forth. Encryption is probably the most common use of the API.

IBM does not provide actual exit point software. That is the responsibility of software vendors and end customers. Syncsort provides software to perform automatic encryption and security of Db2/400 columns using the IBM FIELDPROC exit point in the Alliance AES/400 product. AES/400 integrates user access controls, context sensitive application access controls, audit and system logging, and many other features needed to make the FIELDPROC implementation secure for IBM i users.



Benefits

"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, GDPR, 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).

Alliance AES/400 Support for FIELDPROC

IBM FIELDPROC encryption is implemented in version 5.30 or greater of the Alliance AES/400 solution for IBM i. The FIELDPROC support leverages the NIST-validated AES encryption libraries on V7R1/V7R2 and integrates with Townsend Security's Alliance Key Manager, a FIPS 140-2 compliant key management solution. IBM i customers can deploy this solution to protect credit card Primary Account Numbers (PAN), social security numbers, and all other Personally Identifiable Information (PII).

A security administrator can manage multiple file protections using a simple, native IBM i interface. The interface allows for easy definition of the FIELDPROC control, and there is no need for SQL programming or technical skills. The status of all protected files is easy to view on the configuration panel, and the security administrator can control the file protection from one place.

The Alliance AES/400 FIELDPROC implementation also supports user and application controls. This is a crucial security component of any transparent database encryption facility. These controls are not based on native object authority which can be easily circumvented. The user and application control facility is described in more detail below.

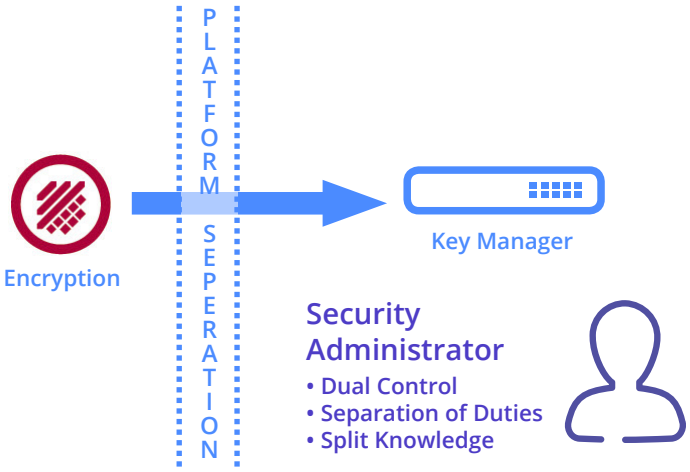
Decryption data masking also allows the security administrator the ability to specify which users are allowed to view the encrypted data, and which users can only view masked values. This provides an easy way to implement controls on who can view fully decrypted values.

Strong Encryption

Alliance AES/400 uses National Institute of Standards and Technology (NIST) validated 256-bit AES encryption for FIELDPROC data protection. The encryption softwarehas been independently tested by a NIST accreditedCryptographic 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.

Key Management

Proper encryption key management is a critical part of companies' data protection strategy. Encryption keys are the most valuable asset that must be protected from loss, and compliance regulations such as PCI DSS recommend key management solutions that have been through NIST validations. Encryption keys stored locally on the IBM i platform cannot meet compliance requirements for Dual Control and Separation of Duties. Alliance Key Manager from Townsend Security is a FIPS 140-2 compliant key management solution and meets the PCI DSS requirements for Dual Control and Separation of Duties. Syncsort's Alliance AES/400 FIELDPROC support integrates seamlessly with Townsend's Key Manager to provide the highest standard of protection.



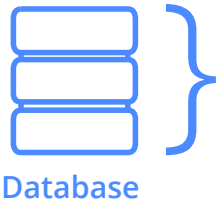
In addition to supporting IBM i data protection, Townsend's Alliance Key Manager works with Windows, Linux, Unix, and IBM System z Mainframes to provide easy to deploy and cost effective key management.

Key Rotation

To assist IBM i customers with key rotation, Alliance AES/400 provides for an optimized batch process that decrypts the file with the old encryption key, and reencrypts the file with a new encryption key. This process is designed to minimize the amount of time required to roll the encryption key for a field. Key rotation can be performed interactively, or submitted to batch for background processing. Multiple key rotation jobs can be active at the same time.

Supported Field Types and Applications

IBM i database applications use a variety of data types to store sensitive information. Some customers store credit card numbers in character fields, others in zoned or packed numeric fields. Customers using Double Byte Character Sets (DBCS) may use these field types for sensitive data. Alliance AES/400 FIELDPROC support will protect any of these field types without changing your database or your business applications. There is no need to reformat your database, or expand field sizes.



Field Types:
Character
Zoned
Packed
Binary
Hex
DBCS

While most IBM i customers will use FIELDPROC encryption with legacy RPG and COBOL applications, FIELDPROC support also works with SQL applications, and Alliance AES/400 supports both program models concurrently. Your ILE and OPM applications will work well with FIELDPROC data protection. You do not have to have the source code for your application to implement Alliance AES/400.

User Access Control and Data Masking

Automatic encryption and decryption works for all users and applications. This represents a security exposure if you do not deploy additional controls on who can access and view protected data. Alliance AES/400 implements data masking by policy. Your security administrator can define which users can view unencrypted data, which users can only view masked data (first 6, last 4, etc.), and which users are not allowed to view the information.

User controls work on the basis of a user profile or a group profile. For each definition you can specify which level of data masking you want to deploy. Data masking works on both character and numeric data, and you can specify the character you want to use for masking (Asterisk, etc.).

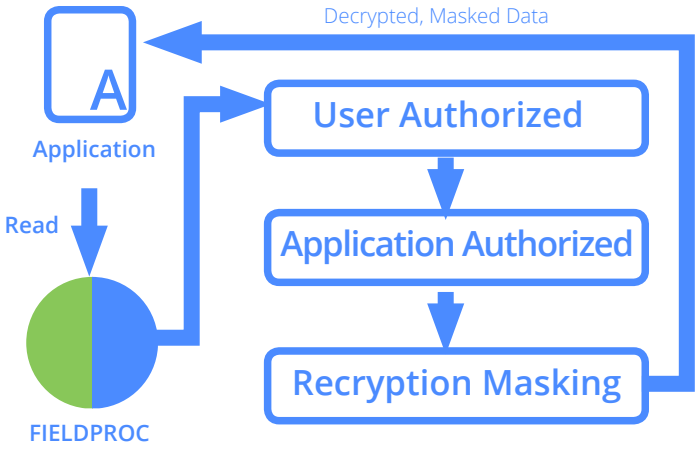
To make administration of user controls easier, you can define a DEFAULT user. Any user not specifically included in the access control and masking definition will be controlled by the default user. This means that you can easily define the users who should have access to the data, and define a default policy that masks the data for everyone else.

Alliance AES/400 does not rely on native IBM i object or user authorities. Controls based on native authority can be easily circumvented by any security administrator or user with All Object (*ALLOBJ) authority. Instead, Alliance AES/400 uses white lists of users and applications to control access.

Context Sensitive Application Controls and Masking

Context sensitive access controls lets the security administrator define which applications have access to protected data. For example, you may want Bill in Human Resources to use the JD Edwards application to view social security numbers, but you wouldn't want Bill using FTP to transfer the HR file to his PC.

Alliance AES/400 lets you define application white lists for data access, and gives you the ability to prevent other applications from decrypting the data. Because Alliance application controls do not use native IBM i object authority, you can easily protect data from automatic decryption by FIELDPROC with unauthorized applications like FTP, DFU, and DBU.



Context sensitive application controls also let you define a DEFAULT policy to apply to any undefined applications. This means you can enforce data masking on any undefined application without generated application level errors and program abends.

Performance

The IBM FIELDPROC exit point works by calling the exit program for each database insert, read, or update. The exit point program is also called on certain query and file positioning operations. This is a dynamic application call in the database space and bears the overhead of a dynamic call. Alliance AES/400 FIELDPROC support has been optimized for performance, but can never achieve the performance of the original service program APIs. While the performance is not as fast as service program APIs, it will be very good for most IBM i application requirements.

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 100 times faster than equivalent IBM APIs on the IBM i platform. These same Alliance AES APIs are used for FIELDPROC encryption. On an entry level model 515 system with one CPU processor, the Alliance AES/400 FIELDPROC procedure is able to encrypt a database of 1 million records in 80 seconds.

The IBM FIELDPROC approach will not be appropriate for all customers. If you have very large files that are processed in total by many applications, the architectural overhead of FIELDPROC may mitigate against its use. Also, if you have many fields in a file or table that must be protected, IBM FIELDPROC will make an encryption or decryption call for each field. This can also mitigate against using the FIELDPROC approach to encryption.

Command Interfaces

In addition to the standard IBM i interactive configuration interfaces, Alliance AES/400 supports a command level interface for starting and stopping FIELDPROC control, and for performing FIELDPROC key change operations. This means that your security administrator can submit long running applications to batch. This is especially helpful when key rotation is required on large files. These jobs can be submitted to batch for off-hours and low priority processing.

Encrypting Fields in Database Files

Securing sensitive data in database files is an imperative for large enterprises. Alliance AES Encryption for IBM i provides a complete set of APIs to let you easily secure data in individual fields in your database, or you can use SQL views and triggers for encryption tasks. Alliance AES APIs integrate with IBM i OPM and ILE applications built with RPG, Cobol, and other languages. There is no need to change the database field definitions or expand a field size, and 256-bit AES in CTR counter mode is used for maximum security. The only applications impacted are those that need to use the sensitive data. Encrypting at the field level also gives you the best security for backup tapes, etc.

syncsort