

# Alliance AES Encryption for IBM i

## Solution Brief



## A Complete AES Encryption Solution

Alliance AES Encryption for IBM i provides AES encryption for sensitive data everywhere it resides on your IBM i platform: Database files, tape, IFS files, Save Files, reports, and messages. With integrated key management you can secure data on your IBM i, Windows, Linux, and UNIX applications using a common, cross-platform strategy. You can encrypt with confidence using the only NIST certified solution for the IBM i.

## Avoiding the Pitfalls of a Partial Solution

A large US-based theme park and entertainment company had to encrypt data on multiple Point-of-Sale, IBM i, and Windows servers to meet PCI compliance. Vendors had used a variety of approaches to AES encryption. Only one IBM i encryption vendor supported all of the needed encryption modes – Townsend Security.



### High Performance

Reduce hardware and software costs and improve application run times with high performance encryption

### Meets Compliance Regulations

Meet PCI, HIPAA, and Privacy Notification requirements for strong encryption

### NIST Certified

Build customer confidence with NIST certified solutions

### Cross-Platform Compatibility

Reduce complexity with a cross-platform solution

### Strong Solution

Avoid field expansion and poorly performing shadow files

### Built for IBM i

Runs on any version of the OS/400 and i5/OS operating systems from V5R2 forward

### Cost-Effective

Reduce costs with an affordable solution

[www.townsendsecurity.com](http://www.townsendsecurity.com)

---

## Introduction

---

Alliance AES Encryption for the IBM i platform is a data security product that protects sensitive information in database fields, on backup tapes, in Save Files, in IFS files, in reports, and everywhere your data resides on the IBM i platform. Alliance AES can help you meet the data security requirements of PCI, HIPAA, Sarbanes-Oxley, and state Privacy Notification laws.

---

## Strong Encryption

---

The Alliance AES solution implements the strong encryption standard defined by the [National Institute of Standards and Technology \(NIST\)](#) defined as Advanced Encryption Standard (AES). The Alliance AES implementation includes support for all NIST recommended modes of encryption including:

- Electronic Code Book (ECB)
- Cipher Block Chaining (CBC)
- Counter (CTR)
- Output Feed Back (OFB)
- Cipher Feed Back (CFB)

All of the NIST key sizes are supported including 128-bit, 192-bit, and 256-bit keys. The Alliance AES solution gives you the depth and breadth of encryption support that you will need to insure the strongest data security.

---

## NIST Certified

---

NIST established a testing and certification process and licensed independent laboratories to conduct the testing. The testing involves hundreds of tests to ascertain the security, reliability, and completeness of an encryption solution using all of the key sizes. The entire Alliance suite of solutions for the IBM i, Microsoft Windows, Linux (SUSE, Red Hat, on Intel and POWER), UNIX (IBM AIX and Sun Solaris), and IBM z (mainframe) passed all of the [NIST AES Validation](#) tests.

As of September 2008 only three other data security vendors have been certified using all key sizes and all NIST approved modes of encryption. No other IBM i vendor has passed this level of certification.

---

## Cross-Platform Integration

---

A data security strategy must embrace a wide variety of computing platforms. Data may be encrypted in Oracle on UNIX, then be transferred to an IBM I, then to a Windows platform with SQL Server. Your data security application must provide the ability to encrypt on one platform and decrypt on a different platform. Incompatible encryption APIs on each platform results in exposing data to loss as they decrypt, transfer, and then re-encrypt. Many large data losses have occurred when data was moved in the clear between systems. Alliance AES solves the problem by providing compatible encryption support for Windows, Linux, UNIX, IBM i and z platforms.

---

## High Performance is Crucial

---

By its nature encryption is a CPU-intensive process. This means that implementing encryption can increase work loads, increase job run times, and lead to expensive processor and server upgrades. Alliance AES Encryption is optimized for performance. Here is a typical profile of an Alliance AES encryption performance run:

System Model: 515 Express  
Feature: 6011  
Processors: 1  
CPW Rating: 3800  
Field Size: 16 bytes emulating a credit card number  
Encryption Method: AES with CBC mode  
Repetitions: 80,000,000  
CPU Seconds Used: 66  
Encryption Per CPU Second: 1,212,121  
CPU Seconds Per Encryption: .000000825  
Megabytes per CPU Second: 18.49

Based on initial performance analysis Alliance AES encryption is:

*1,100 times faster than server-based encryption  
93 times faster than native IBM encryption in V5R4 i5/OS*

While any encryption will increase application work loads, high performing Alliance AES encryption APIs minimize the impact of encryption and reduce server upgrade costs.

---

## Integrated Key Management

---

Key management is as important as encryption services for data security. When encryption and decryption are

performed on a single system with a symmetric encryption algorithm like AES, the key store must be encrypted and secured from unwanted access. Alliance AES implements a secure encrypted key store with alias naming so that you do not need to expose keys and other sensitive cryptographic information in your application programs. You can easily exchange keys between systems, and the Alliance key store can be automatically mirrored to a backup or off-site disaster recovery system.

---

## Key Server for IBM i

---

For IBM i customers who want to isolate the key management and key store facilities from their business applications, Alliance AES provides a key management server that provides both key retrieval and encryption functions. By deploying the Alliance key management server in another i5/OS logical partition, or on a separate IBM i Server, IBM i customers can achieve physical separation of encrypted data and encryption keys.

The Alliance IBM i key server provides key retrieval for all of your business applications on Windows, Linux, UNIX (AIX, Solaris), and IBM System z using a variety of programming languages such as C, C++, RPG, Java, Cobol, .NET, VBNET, and others.

---

## PCI Compliance

---

Data encryption is a crucial part of Payment Card Industry (PCI) compliance (see Section 3 of the PCI Data Security Standard). Alliance AES Encryption customers have achieved full PCI compliance with no compensating controls, using Alliance AES encryption for the IBM i. We are committed to helping our customers meet any PCI audit requirements. As of September 2008, no Alliance AES customer has reported an audit failure using Alliance AES encryption solutions.

---

## Privacy Notification

---

Many states have passed privacy notification laws that require businesses to publicly notify customers and employees if sensitive data is lost. In all cases the notification requirement is waived if the data is secured using strong encryption. Alliance AES encryption uses the federal standard for encryption – Advanced Encryption Standard. The Alliance AES solutions have passed the rigorous testing standards of the National Institute of

Standards and Technology. The Alliance AES solutions will help reduce your exposure to notification requirements.

---

## Encrypting Fields in Database Files

---

Securing sensitive data in database files is an imperative for Enterprise customers. 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.

---

## Securing Backup Tapes

---

Alliance AES encrypted archival tape support provides the best security for your tapes, even when those tapes are archived with a secure service. The loss of a tape in transit to or from the service is a risk that must be managed. With Alliance AES tape encryption you have a software-only solution that works well with your High Availability strategy and provides the highest level of data security. The Alliance AES tape encryption solution is designed for maximum speed in software-based save and restore operations.

---

## Encrypting IFS, Windows Networking, and NFS Files

---

You may have very sensitive information stored in IFS files and Windows networking files. For example, many retailers transfer point-of-sale transaction log files to an IFS directory on the IBM i. Alliance AES can encrypt these files for secure on-line storage. The IFS files that are encrypted can be in normal IFS files or in Windows Network or UNIX NFS shared directories. These files can be encrypted or decrypted on demand or automatically by Alliance AES automation procedures. IFS files encrypted by Alliance AES can be decrypted on Windows, UNIX, Linux and mainframe platforms.

---

## Encrypting Save Files

---

Save files are special types of files that contain on-line save images of your libraries and data. Alliance AES can encrypt these files for secure on-line storage, transfer to remote systems, or transfer to tape. Save files can be easily decrypted back to their original save file format on the IBM i platform. Encrypted save file archives can also be mirrored to a remote system using a high availability product such as MIMIX, Vision or iTera.

---

## Encrypting and Retrieving Printed Reports

---

Printed reports that contain sensitive information such as social security numbers, credit card numbers, or other sensitive information must be protected from loss just like sensitive data on tapes or in files. Alliance AES provides a spooled file report encryption solution that automatically saves and encrypts to an on-line archive. Reports can be accessed for viewing and re-printing by authorized users that you define. Encrypted reports are automatically purged based on rules you define.

---

## Self-Decrypting Archives

---

IBM I customers want to distribute data to their business partners without requiring the purchase of expensive software solutions. With Alliance AES Encryption you can create self-decrypting archives. Self-decrypting archives are Windows .EXE programs that contain an encrypted file. When run on the recipient's Windows PC the program validates the user pass phrase, and decrypts the file to the PC hard drive. With Alliance AES you can create and automatically distribute these self-decrypting archives to your smaller business partners. No external PC or server is required to create self-decrypting archives.

---

## User Access Control and Authentication

---

Federal standards and data security initiatives like PCI and HIPAA require that encryption and key management functions be restricted based on user roles. Certain activities like key management should be restricted to the

security administrator. Alliance AES implements a user authentication system that restricts all application access by user and function.

---

## Developer Support

---

Alliance AES Encryption for IBM i provides a number of resources to developers to make it easier to deploy data security solutions. On the IBM i platform the developer will find sample code for both OPM and ILE applications including RPG, Cobol and CL. Extensive documentation of the encryption APIs and developer guidelines will help speed your project. These facilities shorten the development and deployment time for a project.

For developers on Windows, Linux, AIX, Solaris, and System z platforms, Alliance AES provides example source code to implement key retrieval from the Alliance Key Server. Developers can access encryption keys from .NET, VBNET, C, C++, Java, C# and other languages.

---

## Compliance Logging

---

Alliance AES Encryption implements compliance logging at multiple levels. You can log all user access to Alliance key management and configuration functions to the IBM security audit journal QAUDJRN. You can also enable object level auditing of the Alliance AES application or to any user files. At the encryption and decryption level, Alliance AES supports optional compliance logging for encryption and decryption operations, and these can be enabled by policy. For customers who need log collection and compliance support, the separately licensed Alliance LogAgent application provides full support for PCI, HIPAA, SOX, and other system logging regulations.

---

## Securing Data as it Moves Across the Network

---

In addition to helping you secure your sensitive data on the IBM i platform, Alliance solutions can help you move data securely across servers in your company, and over

the Internet to customers and vendors. Alliance products support Web services and XML, FTP file transfer, Secure Shell sFTP, the Internet AS1/AS2/AS3 formats for EDI, SharePoint WebDAV, and a variety of other secure transport mechanisms. These facilities integrate with Alliance AES encryption solutions to secure your data in transit.

---

### **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, Linux, and UNIX. The company can be reached on the web at [www.townsendsecurity.com](http://www.townsendsecurity.com), or (800) 357-1019.