

Alliance AES Encryption Solution Brief



A Complete Solution for Cross-Platform Compatibility

Alliance AES Encryption for the Windows, Linux, and UNIX platforms protects sensitive information in your database tables and in unstructured files. Alliance AES Encryption can help you meet the data security requirements of PCI, HIPAA, Sarbanes-Oxley, and state Privacy Notification laws.

Improving Encryption Performance

On an entry level Intel server, Alliance AES encrypted 1 million credit card numbers in under 1 second! High speed encryption saves CPU resources, reduces job run times, and reduces upgrade costs.



High Performance

Protects your server resources and reduces job run times

Cross-Platform Compatibility

Reduce developer training and implementation time and cost

Meets Compliance Regulations

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

NIST Certification

Build customer confidence with NIST certified solutions and may reduce legal liability

Supports Many Languages

Such as Java, C/C++, .NET, VBNET, C#, RPG, Cobol, etc

Affordable Solution

Helps protect your investment in your server hardware and software solutions

www.townsendsecurity.com

Introduction

Alliance AES Encryption for Windows, Linux, and UNIX is a library of encryption functions that implement the Advanced Encryption Standard (AES) to protect sensitive data. Alliance AES Encryption implements the three main key sizes and five main encryption modes of AES and follows the National Institute of Standards and Technologies' recommendations for AES. This library is compatible with the Alliance AES Encryption on IBM System i (AS/400, iSeries) and IBM System z (mainframe, OS/390, z/OS) platforms. All Alliance AES encryption solutions are NIST certified to ensure the quality and accuracy of the implementation and to help you meet compliance regulations.

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

CPU: Single Processor running Windows
Credit Cards Encrypted: 1 million
Timing: Under 7 seconds

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

Alliance Key Manager

Windows, UNIX, Linux customers can deploy Alliance Key Manager, and can achieve physical separation of encrypted data and encryption keys. Alliance Key Manager is an Enterprise symmetric key management appliance that creates, manages, and distributes symmetric encryption keys for any application or database running on any Enterprise operating system. With Alliance Key Manager you can deploy a scalable, resilient, and high performance key management solution to meet compliance regulations and ensure data security.

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.

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.

Hardware/Software Requirements

Alliance AES encryption is available for Windows XP/2000/2003/2008, Red Hat and SUSE Linux, IBM AIX, Sun Solaris, IBM i, and IBM z z/OS. No additional third-party software or hardware is required.

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, or (800) 357-1019.