Alliance AES Encryption for IBM i

Why NIST Certification is Important to Your Company

THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) defines the standard for strong encryption, and provides a rigorous testing process for software vendors. This paper discusses why this is important to your Enterprise security. This document is designed to introduce the Advanced Encryption Standard (AES) and how it is used to secure sensitive data. This is intended as an introduction to AES and is not an exhaustive history or explanation about cryptography. You will find links later in this document to help you explore the subject in more detail.
What is the NIST?
The National Institute of Standards and Technology (NIST) is a US government agency that is a part of the Department of Commerce. The NIST sets non-military government standards for a wide variety of technologies including data encryption. Because the NIST uses an open and professional process to establish standards, the private sector usually adopts NIST standards for commercial use. The NIST is one of the most trusted sources for technology standards.

What is AES?
The Advanced Encryption Standard (AES) is the standard for data encryption adopted by the NIST in 2001. This encryption standard replaced the earlier Data Encryption Standard (DES). The DES encryption standard became weaker due to the advancing power of computer systems. The NIST began a process in the late 1990’s to find a replacement for DES. After a lengthy examination of several alternatives, the AES standard for encryption was adopted and codified as FIPS-197. AES encryption is now the de-facto standard for strong data encryption.

What is AES Validation Testing?
The NIST sets the standard for AES encryption testing, and charters independent labs to administer and oversee the testing process. Through the National Voluntary Laboratory Accreditation Program (NVLAP) the NIST certifies independent testing labs for the Cryptographic Module Validation Program (CMVP). Data security software vendors administer the tests, validate the results, and submit the results to the NIST for acceptance. Software vendors work with an independent certification laboratory and not with the NIST directly.

The NIST established five methods, or modes, of encryption that can be used with AES. These are Electronic Code Book (ECB), Cipher Block Chaining (CBC), Counter (CTR), Output Feed Back (OFB), and Cipher Feed Back (CFB) modes. There are separate tests for each mode. A software vendor can choose to validate on only one mode, a subset of the five modes, or all modes of encryption. In addition, the NIST defines three key sizes for encryption: 128-bit, 192-bit, and 256-bit keys. A software vendor can choose from one to three key sizes to certify. Most software vendors choose to certify just one or two modes of encryption, and on one key size. The Alliance AES Encryption products are certified on ALL five modes of encryption, and all three key sizes.

How Does the AES Validation Test Work?
A data security software vendor contracts with an independent CMVP test laboratory to certify their AES encryption products. The test lab provides a wide range of tests the vendor must execute on each computing platform to be certified. The tests are designed to certify that the encryption software performs correctly under a variety of conditions. These include proper implementation of different key sizes, proper handling of small and large blocks of data, proper handling of large numbers of encryptions, and other encryption reliability tests. The tests are designed to insure that the software vendor cannot fudge the results, and the testing lab validates all results submitted by the software vendor.

Each mode of encryption and key size tested involves hundreds of tests and millions of encryptions. Every single test must be passed to achieve certified status.

The Alliance AES encryption solutions passed every certification test for every mode of encryption and every key size, on all nine Enterprise server platforms. The certification involves thousands of tests and hundreds of millions of encryptions. As of March, 2010, only three other data security vendors had certified all modes of encryption. Only one vendor had certified on all nine Enterprise server platforms – Townsend Security.

Certification Means Strong Encryption
NIST certification is your assurance that a vendor’s AES encryption solution implements data encryption the right way. There are many ways to use encryption and a wide variety of modes of encryption. Improperly implemented solutions may work for one type of task, but fail under different application requirements. All software vendors claim they implement strong encryption. Can they prove it? Ask them for their NIST certification.
**Certification Means Compatibility**

One of the biggest challenges facing Enterprise customers is encrypting and decrypting data on a variety of platforms. Data may be encrypted in an Oracle database, then transferred to Microsoft SQL Server, then to an IBM i (AS/400) platform. Computer vendors use different methods of encryption, and different modes of encryption. How can you be sure that your encryption solution will be able to handle all of your requirements?

The NIST certification provides the assurance you need that your software is up to the task. Certified software must work the same way for all of the NIST defined encryption tasks.

The Alliance AES solutions provide even more assurance of compatibility – Alliance AES solutions are certified on all key sizes and all modes of encryption. No other data security vendor provides this level of certified support.

**Certification Means Reliability**

The NIST testing process is designed to exercise a vendor’s encryption solution under stress conditions. Large numbers of repeated encryptions are performed with the output of one encryption used as input for the next encryption. Failures in memory management or reliability will be exposed in the testing process. Encryption software may work without errors for 100 or 1,000 encryptions, but will it work on 1 million encryptions? How about 100 million encryptions?

No one wants the unpleasant experience of a system failure due to unreliable software. NIST certification helps provide some assurance of a reliable implementation.

**Alliance AES Encryption on Every Enterprise Platform**

The modern Enterprise uses a wide variety of server platforms from a number of different vendors. In addition, data is exchanged with customers, vendors, and service providers outside the organization. To meet these challenges the Alliance AES Encryption products are certified and available on all Enterprise platforms including:

- Linux (SUSE and Red Hat, on Intel and POWER)
- UNIX (AIX, Solaris)
- IBM i (AS/400, iSeries)
- IBM z [mainframe]

All of the certified Alliance AES encryption solutions work the same way on every platform.

**Townsend Security**

We know that data gets out, and that it can and routinely does fall into the wrong hands. When this happens, our solutions for encryption, key management, and system logging ensure that your Enterprise is compliant with regulations and that your sensitive data is protected.

Our data security solutions work on a variety of server platforms including IBM i, IBM z, Windows, Linux, and UNIX. Many of these solutions are currently used by leaders in retail, health care, banking, and government.

You can contact Townsend Security for an initial consultation at the following locations:

- **Web:** [www.townsendsecurity.com](http://www.townsendsecurity.com)
- **Phone:** (800) 357-1019 or (360) 359-4400
- **International:** +1 360 359 4400
- **Email:** Info@townsendsecurity.com

A fully functional free trial is available for all Alliance products. You can evaluate Alliance capabilities on your own server systems.