NIST Validation for AES Encryption
Solution Brief

All Encryption is Not Created Equal

The National Institute of Standards and Technology (NIST) defines the standard for AES encryption, and provides a rigorous testing process for software vendors. The validation process is carried out by independent testing labs who report the results to NIST for validation. The AES validation process tests every aspect of encryption and involves millions of encryption and decryption operations. Only the most dedicated security vendors are able to pass the tests and achieve NIST validation. Townsend Security has achieved AES validation for all key sizes and modes of operation, on every major Enterprise platform.

Need Encryption Done Right? Insist on NIST.

In a study of the validation program, NIST found nearly 50 percent of software vendors had errors in their encryption solutions. It isn't easy to get encryption right. A certificate of validation from NIST is your assurance that AES encryption does what it is supposed to do. Every time.

Townsend® SECURITY

How Important is NIST Validation?

"Staples wouldn't even consider a vendor solution that didn't have NIST validation. The fact that Townsend Security has NIST validated solutions on the major Enterprise server platform was a big plus."

- Steve Tenore
  Staples Senior System i Consultant

www.townsendsecurity.com

What is AES Validation Testing?

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) 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 NIST for acceptance. Software vendors always work with an independent validation laboratory and not with 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 validate.

Most software vendors choose to validate just one or two modes of encryption, and on one key size. The Alliance AES Encryption products are validated on ALL five modes of encryption, and all three key sizes.

How Does the AES Validation Testing Work?

A data security software vendor contracts with an independent CMVP test laboratory to validated their AES encryption products. The test lab provides a wide range of tests the vendor must execute on each computing platform to be validated. The tests are designed to validate that the encryption software performs correctly under a variety of conditions.

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

The Alliance AES encryption solutions passed every validation test for every mode of encryption and every key size, on all nine Enterprise server platforms.

Validation Means Better Encryption

NIST validation 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 validation.

Validation 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 validation 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 provides outside the organization. To meet these challenges the Alliance AES Encryption products are validated and available on all Enterprise platforms including:

IBM System i (AS/400, iSeries) all supported releases
IBM System z (z/OS, mainframe)
Microsoft Windows (2000/XP/2003/2008) and SharePoint

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

Definitions

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.

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.

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.