Assurance in Implementation Correctness of Cryptographic Algorithms Gained Through the NIST Cryptographic Algorithm Validation Program

Fiona Pattinson

atsec information security corporation
9130 Jollyville Road, Austin, Texas 78759 USA
fiona@atsec.com

Abstract. The CAVP scheme provides validation testing for FIPS-approved and NIST-recommended cryptographic algorithms. CAVP certification is of interest to vendors in the finance and commerce sectors because the program provides impartial assurance to potential customers that cryptographic algorithms are implemented correctly.

Keywords: CAVP, cryptographic algorithm testing, implementation testing

The Computer Security Division at the U.S. National Institute of Standards and Technology (NIST) maintains a number of cryptographic standards, and coordinates algorithm validation test suites for many of those standards. The Cryptographic Algorithm Validation Program (CAVP) encompasses validation testing for FIPS-approved and NIST-recommended cryptographic algorithms. This list includes many popular algorithms, such as the symmetric key algorithms; Advanced Encryption Standard (AES), Triple DES (TDES), and Skipjack; asymmetric key encryption algorithms including the Signature Standard (DSS) (DSA, RSA, and ECDSA) algorithms; secure hash functions; SHA-1, SHA-224, SHA-256, SHA-384, SHA-512; random number generators (RNG) such as those designed to meet FIPS 186-2 Appendix 3.1 and 3.2 , ANSI X9.31 Appendix A.2.4 , and ANSI X9.62, Appendix A.4; and message authentication algorithms including CCM, HMAC-SHA1, -SHA256, -SHA384, -and SHA512 - RC4.

The CAVP certifies that these algorithms are implemented correctly through formal testing supervised by accredited testing laboratories using test vectors that can informally verify the correctness of the algorithm implementation using the associated validation system document.
The certification program was instigated to provide assurance that cryptographic algorithms are implemented correctly in cryptographic modules. CAVP certification is mandatory for all modules being certified as conformant with the FIPS 140-2 standard. NIST statistics indicate that close to 25% of algorithms tested showed errors in implementation that were corrected as a result of the testing process.
In addition to satisfying NIST requirements, the assurance given by CAVP certification can be used by other programs and industries, for example, in financial applications and in the Payment Card Industry (PCI). Forward-looking vendors are turning to the CAVP certification scheme to provide assurance to an audience demanding assurance that software algorithm implementations have been instantiated correctly. Costs for CAVP certification are relatively small compared to certifications such as Common Criteria and FIPS 140-2.
It should be pointed out that CAVP certification does not by itself provide any assurance that the algorithm itself is sound. It does, however, provide assurance that the algorithm was implemented correctly.

More information about the CAVP scheme, including the official validation lists, can be found at: http://csrc.nist.gov/groups/STM/cavp/index.html

A list of laboratories providing the testing service is found at:
http://csrc.nist.gov/groups/STM/testing_labs/index.html

NOTE: Some assurance to developers and the users of algorithms can be also be gained by having third party analysis of the implementation correctness of algorithms outside of the NIST CAVP performed. Some laboratories will also offer an independent review of implementations of other algorithms such as RC4, CRCs, single DES, MAC, Blowfish and others.