ITL’s Cryptographic Algorithm Validation Program (CAVP)

The CAVP is a collaborative program based on a partnership between NIST’s Computer Security Division (CSD) and the Communication Security Establishment Canada (CSEC). The program provides federal agencies—in the United States and Canada—confidence that a validated cryptographic algorithm has been implemented correctly. The CAVP validates cryptographic algorithms that may be integrated in one or more cryptographic modules. The validation of cryptographic algorithms is a prerequisite to the validation of cryptographic modules by the Cryptographic Module Validation Program (CMVP). Federal agencies are required to use validated cryptographic algorithms for the protection of sensitive non-classified information.

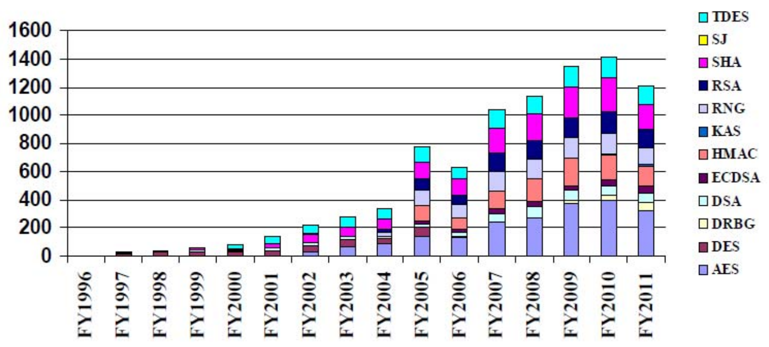
The CAVP designs and develops validation test suites for all FIPS-recommended and NIST-approved cryptographic algorithms recognized by the Federal Government. The validation tests provide a uniform, documented method of assuring that the cryptographic algorithm implementation adheres to the detailed specifications in the Federal Information Processing Standards (FIPS) and NIST Special Publications (SP). These validation tests exercise the mathematical formulas detailed in the algorithm to assure the detailed specifications are implemented correctly and completely. If the implementer deviates from these instructions or excludes any part of the instructions, the validation test will fail, indicating that the algorithm implementation does not function properly or is incomplete.

The testing of cryptographic algorithm implementations is performed by third-party laboratories that are accredited as Cryptographic and Security Testing (CST) laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP).

The CAVP has stimulated improved quality and security assurance of cryptographic algorithms. The latest set of statistics which are collected quarterly from each of the testing laboratories show that 8 percent of the cryptographic algorithms brought in for voluntary testing had security flaws that were corrected during testing. Without this program, the federal government would not know if they were buying correctly implemented cryptography. To date, over 8,700 cryptographic algorithm validations have been issued.

The CAVP issued 1,475 algorithm validations in FY2010. To this date in FY2011, the CAVP has issued 1211 algorithm validations. The number of algorithms submitted for validation continues to grow, representing significant growth in the number of validated products expected to be available in the future.

CAVP Validation Status By FYs



Website: http://csrc.nist.gov/groups/STM CAVP Contact: Ms. Sharon Keller sharon.keller@nist.gov

NIST National Institute of Standards and Technology / U.S. Department of Commerce