Advanced Encryption Standard Algorithm Validation List

Last Update: 10/16/2008

The page provides technical information about implementations that have been validated as conforming to the **Advanced Encryption Standard (AES) Algorithm,** as specified in Federal Information Processing Standard Publication 197, *Advanced Encryption Standard.*

The list below describes implementations which have been validated as correctly implementing the AES algorithm, using the tests found in The Advanced Encryption Standard Algorithm Validation Suite (AESAVS). This testing is performed by NVLAP accredited Cryptographic Module Testing (CMT) laboratories.

The implementations below consist of software, firmware, hardware, and any combination thereof. The National Institute of Standards and Technology (NIST) has made every attempt to provide complete and accurate information about the implementations described in this document. However, due to the possibility of changes made within individual companies, NIST cannot guarantee that this document reflects the current status of each product. It is the responsibility of the vendor to notify NIST of any necessary changes to its entry in the following list. A validation certificate issued to each vendor also indicates 1) the CMT laboratory that tested the implementation, and 2) the operating environment used to test the implementation (if software or firmware).

This list is ordered in reverse numerical order, by certificate number. Thus, the more recent validations are located closer to the top of the list. The column after the Validation Date column contains information indicating what modes and features for these modes has been successfully tested.

For the original modes of operation (ECB, CBC, CFB, OFB), this information consists of the **modes of operation** tested (e.g., ECB, CBC, CFB, OFB), **states** (encryption(e) and/or decryption(d)), and **key sizes** (128-bit, 192-bit, and/or 256-bit) for which the implementation was validated. For Counter (CTR) mode, the counter source (internal(int) and/or external(ext)) is also indicated.

For the authenticate encryption mode of operation CCM, this information consists of the following:

Legend for Description Field

Key Sizes Tested	128, 192, 256
Associated Data Length Range Tested	Minimum - Maximum, 2^16 The values listed indicate the formatting of the Associated Data cases that were tested (Refer to Appendix A.2.2 of SP800-38C): * If Minimum = 0, the formatting case where Associated Data Length (Alen) = 0 is tested. * If values ranging from 1 to 32 are listed, the formatting case where 0 < Alen < 2^16 - 2^8 is tested. * If 2^16 is listed, the formatting case where 2^8 < Alen < 2^32 is tested.
Payload Length Range Tested	Minimum - Maximum
Nonce Length(s) tested	7, 8, 9, 10, 11, 12, 13

4, 6, 8, 10, 12, 14, 1

For the CMAC authentication mode of operation, this information consists of the **key sizes** (128-bit, 192-bit, and/or 256-bit) **(KS 128,192,256)** for which the implementation was validated.

Advanced Encryption Standard (AES) Algorithm Validated Implementations

878	Digital Security Controls, a Division of Tyco Safety Products Canada Ltd. 3301 Langstaff Road Concord, Ontario L4K 4L2	**SG-SYSTEM I** Version 1.00 (Firmware)	Freescale MPC885VR133	9/29/2008	**ECB(e/d; 128** "The SG-SYS encrypted line required per U

	Canada -Dan Nita TEL: (905) 760-3000 x2706 FAX: (905) 760-3020				

Need Assistance?

Computer Security Division
National Institute of Standards and Technology