TecSec® FIPS 140-2 Testing Certificates - Algorithms

Listed on web site http://csrc.nist.gov/cryptvall

Certificate No.	Description (URL)	Platform/OS Tested	Date
131	RSA Validation Certificate (http://csrc.nist.gov/cryptval/dss/rsaval.html)	Pentium III 933 MHz processor w/ Windows 2000	April 2006
163	Digital Signature Algorithm (DSA) Validation Certificate (http://csrc.nist.gov/cryptval/dss/dsaval.htm)	Pentium III 933 MHz processor w/ Windows 2000	April 2006
165	Digital Signature Algorithm (DSA) Validation Certificate (http://csrc.nist.gov/cryptval/dss/dsaval.htm)	Pentium III 933 MHz processor w/ Windows XP Pentium III 933 MHz processor w/ Windows 2000	April 2006
167	Keyed-Hash Message Authentication Code (HMAC) Validation Certificate (http://csrc.nist.gov/cryptval/mac/hmacval.html)	Pentium III 933 MHz processor w/ Windows 2000	April 2006
181	Random Number Generator (RNG) Validation Certificate (http://csrc.nist.gov/cryptval/rng/rngval.html)	Pentium III 933 MHz processor w/ Windows 2000	April 2006
379	Advanced Encryption Standard Algorithm Validation Certificate (http://csrc.nist.gov/cryptval/aes/aesval.html)	Pentium III 933 MHz processor w/ Windows 2000	April 2006
422	Triple DES Modes of Operation Validation Certificate (http://csrc.nist.gov/cryptval/des/tripledesval.html)	Pentium III 933 MHz processor w/ Windows 2000	April 2006
450	Secure Hash Standard (SHS) Validation Certificate (http://csrc.nist.gov/cryptval/shs/shaval.htm)	Pentium III 933 MHz processor w/ Windows 2000	April 2006
116	RSA Validation Certificate (http://csrc.nist.gov/cryptval/dss/rsaval.html)	Pentium III 933 MHz w/ Windows XP	January 2006
149	Keyed-Hash Message Authentication Code (HMAC) Validation Certificate (http://csrc.nist.gov/cryptval/mac/hmacval.html)	Pentium III 933 MHz w/ Windows XP	January 2006
155	Digital Signature Algorithm (DSA) Validation Certificate (http://csrc.nist.gov/cryptval/dss/dsaval.htm)	Pentium III 933 MHz w/ Windows XP	January 2006

CERTIFICATE NO.	DESCRIPTION (URL)	PLATFORM/OS TESTED	DATE
165	Random Number Generator (RNG) Validation Certificate (http://csrc.nist.gov/cryptval/rng/rngval.html)	Pentium III 933 MHz w/ Windows XP	January 2006
345	Advanced Encryption Standard Algorithm Validation Certificate (http://csrc.nist.gov/cryptval/aes/aesval.html)	Pentium III 933 MHz w/ Windows XP	January 2006
407	Triple DES Modes of Operation Validation Certificate (http://csrc.nist.gov/cryptval/des/tripledesval.html)	Pentium III 933 MHz w/ Windows XP	January 2006
420	Secure Hash Standard (SHS) Validation Certificate (http://csrc.nist.gov/cryptval/shs/shaval.htm)	Pentium III 933 MHz w/ Windows XP	January 2006

TecSec® FIPS 140-2 Testing Certificates – Cryptographic Module

CERTIFICATE NO.	DESCRIPTION (URL)	PLATFORM/OS TESTED	DATE
687 FIPS 140-2	CKM Cryptographic Module by TecSec Incorporated (When operated in FIPS Mode) (http://csrc.nist.gov/cryptval/140-1/1401vend.htm)	Windows 2000 and Windows XP (in single user mode)	July 2006

TecSec® FIPS 140-2 Testing Certificates - Hardware

Certificate No.	Description (URL)	Date
1118	TecSec PIV Eagle Card- Contactless (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm)	April 2009
1120	TecSec PIV Eagle Card -Contact by TecSec, Atmel, CPI Card Group and Athena Smartcard (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm)	April 2009

Revision History

Date	Version/Revision No.	Revision/Change Description
8/1/2006		Original Issue
8/25/2010	1	Updated with latest certificates