



SecureParser® Certifications

The SecureParser cryptographic module has been evaluated by the National Institute of Standards and Technology (NIST) against the cryptographic module standard, FIPS 140-2, and been assigned certificate number 920 validating the security claims made in the submitted security policy. The certification is valid on four different operating environments (X86-compatible w/ Windows 2003 Server; X86-compatible w/ Windows XP X86-compatible w/ Red Hat Enterprise Linux 4; X86-compatible w/ SUSE Enterprise Linux 10; X86-compatible w/ Windows XP). Each system was validated for user mode, Multi-threading capability, and (for the WindowsXP and Server 2003 environments) Kernel mode.

Additionally, the following encryption algorithms were certified to be appropriately utilized as validated by the Cryptographic Algorithm Validation Program (CAVP):

- AES Modes: (ECB(e/d; 128,192,256); CBC(e/d; 128,192,256); CTR(int/ext; 128,192,256),
- DSA: SIG(gen) MOD(1024); SIG(ver) MOD(1024);
- RSA: ALG[RSASSA-PSS]; SIG(gen); SIG(ver); 1024 , 2048 , 4096 , SHS:
- ECDSA: SIG(gen): CURVES(P-521) and SIG(ver): CURVES(P-521)
- SHA: SHA 1and SHA 256
- RNG: ANSI X9.31, [AES-128Key]
- HMAC: HMAC-SHA1 and HMAC SHA 256

Assigned an overall level 1 rating, it is important to note that a level 3 rating was assigned to the following areas of the module:

- Cryptographic Module Specification
- Cryptographic Key Management
- Design Assurance
- EMI/EMC

The SecureParser cryptographic module makes use of the following algorithms and employs those algorithms in the secure manner outlined by NIST. The certificate number assigned by NIST validating the secure implementation of those algorithms is provided below:

Algorithm	Certificate Numbers
AES	594, 697
RNG	330, 401
RSA	262, 331
DSA	229, 260
SHS	631, 716
HMAC	302, 366
ECDSA	63, 77

For more information contact us at info@securityfirstcorp.com