Pre-Compiled OpenSSL FIPS Modules

TELEGRID

TELEGRID provides pre-compiled distributions of the OpenSSL FIPS Object Module v2.0 (FIPS Module) for multiple operating systems and platforms. FIPS Modules are available for both Linux and Windows on embedded and enterprise systems. The FIPS Modules helps engineers design secure compliant systems quickly.

OpenSSL™ Cryptography and SSL/TLS Toolkit

The FIPS Module provides an API for invocation of FIPS approved cryptographic functions from external applications and operates in conjunction with standard OpenSSL 1.0.1 distributions. The FIPS Module meets FIPS 140-2, Level 1 requirements and there are no additional tasks to ensure compliance other than building and initializing the FIPS approved and HMACSHA-1 digest verified source code. The FIPS Module provides confidentiality, integrity signing, and verification services.

FIPS 140-2 Compliant Cryptographic Algorithms

These standard OpenSSL 1.0.1 source distributions supports FIPS Mode in which the FIPS approved algorithms are implemented by the FIPS Module and non-FIPS approved algorithms are disabled by default. The FIPS Module supports the following algorithms: Triple DES, AES, CMAC, CCM, RSA (for digital signatures), DH, DSA/DSA2, ECDSA/ECDSA2, SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, and HMAC-SHA-1, HMAC-SHA-224, HMAC-SHA-256, HMAC-SHA-384, HMACSHA-512. Non-validated algorithms include Blowfish, CAST, IDEA, RC-family, and non-SHA message digest and other algorithms among others.

Supported Algorithms	
• Triple DES	• SHA-224
• AES	• SHA-256
• CMAC	• SHA-384
• CCM	• SHA-512
• RSA	• HMAC-SHA-1
• DH	• HMAC-SHA-224
• DSA/DSA2	• HMAC-SHA-256
• ECDSA/ECDSA2	• HMAC-SHA-384
• SHA-1	• HMACSHA-512

FIPS 140-2 Compliant Random Number Generator

The FIPS Module supports SP 800-90 and ANSI X9.31 compliant pseudorandom number generators. It also supports the Suite B cryptographic algorithms and can be used with Suite B cryptography exclusively. Suite B requires 128-bit security levels and forbids use of TLS lesser than 1.2 (TLS 1.0 and 1.1 use MD5 as a PRF during key agreement).

Custom Applications

Custom integration into external proprietary as well as open source applications is available. TELEGRID's application modules include a wide array of Open Source applications built from source with the integrated FIPS Module including:

- Apache HTTP Server
- Subversion
- OpenSSH
- OpenVPN
- PostgreSQL
- MySQL
- Python Compiler

TELEGRID Technologies, Inc.
23 Vreeland Road
Florham Park, NJ 07932
(973) 994-4440
sales@telegrid.com