OpenSSL FIPS
Object Module
Version 1.2.2
By the
Open Source Software Institute
http://www.oss-institute.org/

OpenSSL FIPS 140-2 Security Policy
Version 1.2.2
November 5, 2010
Copyright Notice


This document may be freely reproduced in whole or part without permission and without restriction.

Sponsored by:

[Symantec Logo]

[OpenGear Secure Server Management Logo]
OpenSSL FIPS 140-2 Security Policy

Acknowledgments

The Open Source Software Institute (OSSI) serves as the "vendor" for this validation. Project management coordination for this effort was provided by:

Steve Marquess
President
The OpenSSL Software Foundation
1829 Mount Ephraim Road
Adamstown, MD 21710
USA

John Weathersby
Executive Director
Open Source Software Institute
Administrative Office
P.O. Box 547
Oxford, MS 38655
USA

with technical work by:

Stephen Henson
4 Monaco Place,
Westlands, Newcastle-under-Lyme
Staffordshire. ST5 2QT.
England, United Kingdom

Andy Polyakov
Chalmers University of Technology
SE-412 96 Gothenburg
Sweden

Tim Hudson
P.O. Box 6389
Fairfield Gardens 4103
Australia

in coordination with the OpenSSL Team at www.openssl.org.

Initial validation testing was performed by The DOMUS IT Security Laboratory. For information on validation or revalidations of software contact:

Eric Stevens
Laboratory Director
DOMUS IT Security Laboratory
400 March Road, Suite 190
Kanata, Ontario
K2K 3H4
Canada

Additional validation testing was performed by Infogard Laboratories. For information on validation or revalidations of software contact:

Mark Minnoch
FIPS Program Manager, CISSP
InfoGard Laboratories
709 Fiero Lane, Suite 25
San Luis Obispo, CA 93401
## Modification History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010-11-04</td>
<td>Addition of the Motorola Droid II platform</td>
</tr>
<tr>
<td></td>
<td>Retesting for Windows 64bit portability bugfix, Appendix A: incorporate earlier</td>
</tr>
<tr>
<td></td>
<td>uCLinux patch in new source distribution</td>
</tr>
<tr>
<td>2009-11-03</td>
<td>Section 2, Appendix A: Addition of a new platform.</td>
</tr>
<tr>
<td>2008-08-08</td>
<td>Original validation.</td>
</tr>
</tbody>
</table>
## Table of Contents

1. Introduction..........................................................................................................................6

2. Module Specification.............................................................................................................6
   2.1 Roles and Services.............................................................................................................7
   2.2 Ports and Interfaces...........................................................................................................8
   2.3 Self Tests............................................................................................................................9
   2.4 Mitigation of Other Attacks............................................................................................11
   2.5 Physical Security.............................................................................................................11

3. Secure Operation..................................................................................................................12

4. Cryptographic Key Management..........................................................................................13
   4.1 Key Generation..................................................................................................................13
   4.2 Key Storage........................................................................................................................13
   4.3 Key Access........................................................................................................................13
   4.4 Key Protection and Zeroization.......................................................................................13
   4.5 Cryptographic Algorithms...............................................................................................13

Appendix A Installation Instructions.........................................................................................15
Appendix B Controlled Distribution File Fingerprint...............................................................17
1. Introduction

This document is the non-proprietary security policy for the OpenSSL FIPS Object Module. This document was prepared as part of the Federal Information Processing Standard (FIPS) 140-2 Level 1 validation process.

FIPS 140-2, Security Requirements for Cryptographic Modules, describes the requirements for cryptographic modules. For more information about the FIPS 140-2 standard and the cryptographic module validation process see http://csrc.nist.gov/cryptval/.

2. Module Specification

The OpenSSL FIPS Object Module (hereafter referred to as the Module) is a software library supporting FIPS-approved cryptographic algorithms. For the purposes of the FIPS 140-2 level 1 validation, the OpenSSL FIPS Object Module v1.2.2 is a single object module file named fipscanister.o (Linux®/Unix®) or fipscanister.lib (Microsoft Windows®). This module provides a C-language application program interface (API) for use by other processes that require cryptographic functionality.

Note that the OpenSSL FIPS Object Module v1.2.2 completely replaces the earlier OpenSSL FIPS Object Module v1.2. The v1.2.2 Module incorporates support for the cross-compiled UCLinux platform and a bugfix that prevented correct operation on certain Microsoft Windows 64bit environments. The v1.2.2 Module can be used in any environment supported by the earlier v1.2 Module.

For FIPS 140-2 purposes the Module is classified as a multi-chip standalone module. The logical cryptographic boundary of the Module is the fipscanister object module. The physical cryptographic boundary of the Module is the enclosure of the computer system on which it is executing. The Module performs no communications other than with the process that calls it. It makes no network or interprocess connections and creates no files.

The Module was tested on the following platforms:

1. Linux x86 no-asm Linux.2.6.18_i686_gcc-4.1.2 (OpenSuSE 10.2) no-asm
2. Linux x86-64 no-asm Linux.2.6.20_x86-64_gcc-4.1.2 (OpenSuSE 10.2)
3. Linux x86 asm Linux.2.6.18_i686_gcc-4.1.2 (OpenSuSE 10.2)
4. Linux x86-64 asm Linux.2.6.20_x86-64_gcc-4.1.2 (OpenSuSE 10.2)
5. Windows x86 no-asm WinXP.SP2_i386_MSVC.8.0 no-asm
6. Windows x64 no-asm WinXP.SP2_x86-64_MSVC.8.0 no-asm
7. Windows x86 asm WinXP.SP2_i386_MSVC.8.0 NASM, SSE2
8. Windows x64 asm WinXP.SP2_x86-64_MSVC.8.0
9. Linux ARM no-asm Linux.2.4.32-uc0_armv4l gcc-3.4.4 (uCLinux)
10. Linux ARM no-asm Linux.2.6.32.9-g59f039501_armv7l gcc-4.4.0 (Android 2.2)

---

1 Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.
2 UNIX is a registered trademark of The Open Group
3 Windows is a registered trademark of Microsoft Corporation in the United States and other countries.
The “asm” designation means that assembler language optimizations were enabled when the binary code was built, “no-asm” means that only C language code was compiled.

2.1 Roles and Services

The Module meets all FIPS 140-2 level 1 requirements for Roles and Services, implementing both Crypto-User and Crypto-Officer roles. As allowed by FIPS 140-2, the Module does not support user authentication for those roles. Only one role may be active at a time and the Module does not allow concurrent operators.

The User and Crypto Officer roles are implicitly assumed by the entity accessing services implemented by the Module. The Crypto Officer can install and initialize the Module. The Crypto Officer role is implicitly entered when installing the Module or performing system administration functions on the host operating system.

- **User Role:** Loading the Module and calling any of the API functions. This role has access to all of the services provided by the Module.
- **Crypto-Officer Role:** Installation of the Module on the host computer system. This role is assumed implicitly when the system administrator installs the Module library file.
## Table 2.1

<table>
<thead>
<tr>
<th>Service</th>
<th>Role</th>
<th>CSP</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symmetric encryption/decryption</td>
<td>User, Crypto Officer</td>
<td>symmetric key AES, TDES</td>
<td>read/write/execute</td>
</tr>
<tr>
<td>Key transport</td>
<td>User, Crypto Officer</td>
<td>asymmetric private key RSA</td>
<td>read/write/execute</td>
</tr>
<tr>
<td>Digital signature</td>
<td>User, Crypto Officer</td>
<td>asymmetric private key RSA, DSA</td>
<td>read/write/execute</td>
</tr>
<tr>
<td>Symmetric key generation</td>
<td>User, Crypto Officer</td>
<td>symmetric key AES, TDES</td>
<td>read/write/execute</td>
</tr>
<tr>
<td>Asymmetric key generation</td>
<td>User, Crypto Officer</td>
<td>asymmetric private key RSA, DSA</td>
<td>read/write/execute</td>
</tr>
<tr>
<td>Keyed Hash (HMAC)</td>
<td>User, Crypto Officer</td>
<td>HMAC SHA-1 key HMAC-SHA-1</td>
<td>read/write/execute</td>
</tr>
<tr>
<td>Message digest (SHS)</td>
<td>User, Crypto Officer</td>
<td>none SHA-1, SHA-2</td>
<td>read/write/execute</td>
</tr>
<tr>
<td>Random number generation</td>
<td>User, Crypto Officer</td>
<td>seed key seed AES</td>
<td>read/write/execute</td>
</tr>
<tr>
<td>Show status</td>
<td>User, Crypto Officer</td>
<td>none</td>
<td>execute</td>
</tr>
<tr>
<td>Module initialization(^1)</td>
<td>User, Crypto Officer</td>
<td>none</td>
<td>execute</td>
</tr>
<tr>
<td>Self test</td>
<td>User, Crypto Officer</td>
<td>none</td>
<td>execute</td>
</tr>
<tr>
<td>Zeroize</td>
<td>User, Crypto Officer</td>
<td>symmetric key, asymmetric key, HMAC-SHA-1 key, seed key AES</td>
<td>execute</td>
</tr>
</tbody>
</table>

\(^1\) The FIPS mode initialization is performed when the application invokes the `FIPS_mode_set()` call which returns a “1” for success and “0” for failure; see section 2.3.

## 2.2 Ports and Interfaces

The physical ports of the Module are the same as the computer system on which it is executing. The logical interface is a C-language application program interface (API).

The Data Input interface consists of the input parameters of the API functions. The Data Output interface consists of the output parameters of the API functions. The Control Input interface consists of the actual API functions. The Status Output interface includes the return values of the API functions.
2.3 **Self Tests**

The Module performs both power-up self tests at module initialization\(^2\) and continuous condition tests during operation. Input, output, and cryptographic functions cannot be performed while the Module is in a self-test or error state as the module is single threaded and will not return to the calling application until the power-up self tests are complete. If the power-up self tests fail subsequent calls to the module will fail and thus no further cryptographic operations are possible.

**Power-Up Self Tests**

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>KAT</td>
</tr>
<tr>
<td>Triple-DES</td>
<td>KAT</td>
</tr>
<tr>
<td>DSA</td>
<td>pairwise consistency test, sign/verify</td>
</tr>
<tr>
<td>RSA</td>
<td>KAT</td>
</tr>
<tr>
<td>PRNG</td>
<td>KAT</td>
</tr>
<tr>
<td>HMAC-SHA-1</td>
<td>KAT</td>
</tr>
<tr>
<td>HMAC-SHA-224</td>
<td>KAT</td>
</tr>
<tr>
<td>HMAC-SHA-256</td>
<td>KAT</td>
</tr>
<tr>
<td>HMAC-SHA-384</td>
<td>KAT</td>
</tr>
<tr>
<td>HMAC-SHA-512</td>
<td>KAT</td>
</tr>
<tr>
<td>SHA-1</td>
<td>KAT(^3)</td>
</tr>
<tr>
<td>SHA-224</td>
<td>KAT(^1)</td>
</tr>
</tbody>
</table>

\(^2\) The FIPS mode initialization is performed when the application invokes the `FIPS_mode_set()` call which returns a “1” for success and “0” for failure; see section 2.3.

\(^3\) Tested as part of the HMAC known answer tests.
OpenSSL FIPS 140-2 Security Policy

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA-256</td>
<td>KAT₁</td>
</tr>
<tr>
<td>SHA-384</td>
<td>KAT₁</td>
</tr>
<tr>
<td>SHA-512</td>
<td>KAT₁</td>
</tr>
<tr>
<td>module integrity</td>
<td>HMAC-SHA-1</td>
</tr>
</tbody>
</table>

Table 2.3a

Conditional Self Tests

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSA</td>
<td>pairwise consistency</td>
</tr>
<tr>
<td>RSA</td>
<td>pairwise consistency</td>
</tr>
<tr>
<td>PRNG</td>
<td>continuous test</td>
</tr>
</tbody>
</table>

Table 2.3b

A single initialization call, FIPS_mode_set(), is required to initialize the Module for operation in the FIPS 140-2 Approved mode. When the Module is in FIPS mode all security functions and cryptographic algorithms are performed in Approved mode.

The FIPS mode initialization is performed when the application invokes the FIPS_mode_set() call which returns a “1” for success and “0” for failure. Interpretation of this return code is the responsibility of the host application. Prior to this invocation the Module is uninitialized in the non-FIPS mode by default.

The FIPS_mode_set() function verifies the integrity of the runtime executable using a HMAC-SHA-1 digest computed at build time. If this computed HMAC-SHA-1 digest matches the stored known digest then the power-up self-test, consisting of the algorithm specific Pairwise Consistency and Known Answer tests, is performed. If any component of the power-up self-test fails an internal global error flag is set to prevent subsequent invocation of any cryptographic function calls. Any such power-up self test failure is a hard error that can only be recovered by reinstalling the Module. If all components of the power-up self-test are successful then the Module is in FIPS mode. The power-up self-tests may be performed at any time with a separate function call, FIPS_selftest(). This function call also returns a “1” for success and “0” for failure, and interpretation of this return code is the responsibility of the host application.

A power-up self-test failure can only be cleared by a successful FIPS_mode_set() invocation. No operator intervention is required during the running of the self-tests.

---

4 The FIPS_mode_set() function could be re-invoked but such re-invocation does not provide a means from recovering from an integrity test or known answer test failure.
2.4 Mitigation of Other Attacks

The Module does not contain additional security mechanisms beyond the requirements for FIPS 140-2 level 1 cryptographic modules.

2.5 Physical Security

The Module is comprised of software only and thus does not claim any physical security.
3. Secure Operation

The tested operating systems segregate user processes into separate process spaces. Each process space is an independent virtual memory area that is logically separated from all other processes by the operating system software and hardware. The Module functions entirely within the process space of the process that invokes it, and thus satisfies the FIPS 140-2 requirement for a single user mode of operation.

The Module is installed using one of the set of instructions in Appendix A appropriate to the target system. A complete revision history of the source code from which the Module was generated is maintained in a version control database\(^5\). The HMAC-SHA-1 of the Module distribution file as tested by the CMT Laboratory and listed in Appendix A is verified during installation of the Module file as described in Appendix A.

Upon initialization\(^6\) of the Module, the module will run its power-up self tests. Successful completion of the power-up self tests\(^7\) ensures that the module is operating in the FIPS mode of operation.

As the Module has no way of managing keys, any keys that are input or output from applications utilizing the module must be input or output in encrypted form using FIPS approved algorithms.

The self-tests can be called on demand by reinitializing the module using the `FIPS_mode_set()` function call, or alternatively using the `FIPS_selftest()` function call.

---


\(^6\) The FIPS mode initialization is performed when the application invokes the `FIPS_mode_set()` call which returns a “1” for success and “0” for failure; see section 2.3.

\(^7\) The power-up self tests are performed as part of the FIPS mode initialization process; see section 2.3.
4. Cryptographic Key Management

4.1 Key Generation

The Module supports generation of DH, DSA, and RSA public-private key pairs. The Module employs an ANSI X9.31 compliant random number generator for creation of asymmetric and symmetric keys. The developer shall use entropy sources that contain at least 128 bits of entropy to seed the RNG as the module is not capable of detecting randomness or quality of the seeding material provided.

4.2 Key Storage

Public and private keys are provided to the Module by the calling process, and are destroyed when released by the appropriate API function calls. The Module does not perform persistent storage of keys.

4.3 Key Access

An authorized application as user (the Crypto-User) has access to all key data generated during the operation of the Module.

4.4 Key Protection and Zeroization

Keys residing in internally allocated data structures can only be accessed using the Module defined API. The operating system protects memory and process space from unauthorized access. Zeroization of sensitive data is performed automatically by API function calls for intermediate data items, and on demand by the calling process using Module provided API function calls provided for that purpose.

Only the process that creates or imports keys can use or export them. No persistent storage of key data is performed by the Module. All API functions are executed by the invoking process in a non-overlapping sequence such that no two API functions will execute concurrently.

The calling process can perform key zeroization of keys by calling an API function.

4.5 Cryptographic Algorithms

The Module supports the following FIPS approved or allowed algorithms:

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Validation Certificate</th>
<th>Usage</th>
<th>Keys/CSPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>#695</td>
<td>encrypt/decrypt</td>
<td>AES keys 128, 192, 256 bits</td>
</tr>
<tr>
<td>TDES</td>
<td>#627</td>
<td>encrypt/decrypt</td>
<td>Triple-DES keys 168 bits</td>
</tr>
<tr>
<td>DSA</td>
<td>#264</td>
<td>sign and verify</td>
<td>DSA keys 1024 bits</td>
</tr>
<tr>
<td>PRNG (ANSI X9.31 Appendix)</td>
<td>#407</td>
<td>random number generation</td>
<td>PRNG seed value is 128 bits; seed key values are 128 bits</td>
</tr>
</tbody>
</table>
Table 4.5a

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Validation Certificate</th>
<th>Usage</th>
<th>Keys/CSPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.2.4 using AES)</td>
<td></td>
<td></td>
<td>192 bits, and 256 bits</td>
</tr>
<tr>
<td>RSA (X9.31, PKCS #1.5, PSS)</td>
<td>#323</td>
<td>sign and verify</td>
<td>RSA keys 1024 to 16384 bits</td>
</tr>
<tr>
<td>RSA encrypt/decrypt (allowed in FIPS mode, see caveat below)</td>
<td>key wrapping</td>
<td></td>
<td>RSA (key wrapping; key establishment methodology provides 80 to 256 bits of encryption strength)</td>
</tr>
<tr>
<td>SHA-1</td>
<td>#723</td>
<td>hashing</td>
<td>N/A</td>
</tr>
<tr>
<td>SHA-224</td>
<td>#723</td>
<td>hashing</td>
<td>N/A</td>
</tr>
<tr>
<td>SHA-256</td>
<td>#723</td>
<td>hashing</td>
<td>N/A</td>
</tr>
<tr>
<td>SHA-384</td>
<td>#723</td>
<td>hashing</td>
<td>N/A</td>
</tr>
<tr>
<td>SHA-512</td>
<td>#723</td>
<td>hashing</td>
<td>N/A</td>
</tr>
<tr>
<td>HMAC-SHA-1</td>
<td>#373</td>
<td>message integrity</td>
<td>HMAC key</td>
</tr>
<tr>
<td>HMAC-SHA224</td>
<td>#373</td>
<td>message integrity</td>
<td>HMAC key</td>
</tr>
<tr>
<td>HMAC-SHA256</td>
<td>#373</td>
<td>message integrity</td>
<td>HMAC key</td>
</tr>
<tr>
<td>HMAC-SHA384</td>
<td>#373</td>
<td>message integrity</td>
<td>HMAC key</td>
</tr>
<tr>
<td>HMAC-SHA512</td>
<td>#373</td>
<td>message integrity</td>
<td>HMAC key</td>
</tr>
</tbody>
</table>

Table 4.5b

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Usage</th>
<th>Keys/CSPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Diffie-Hellman</td>
<td>key establishment</td>
<td>Diffie-Hellman keys</td>
</tr>
</tbody>
</table>

DSA supports a key size of less than 1024 bits except when not in FIPS mode.

RSA (key wrapping; key establishment methodology provides between 80 and 256 bits of encryption strength).

The Module supports the following non-FIPS approved algorithms:

The Module only provides functions that implement Diffie-Hellman primitives. The shared secret provides between 80 and 219 bits of encryption strength.
Appendix A  Installation Instructions

The test platforms represent different combinations of installation instructions and “code paths” -- the distinct set of object code generated depending on the host hardware and operating system platform. For each of these code paths there is a build system, the host providing the build environment in which the installation instructions are executed, and a target system on which the generated object code is executed. The build and target systems may be the same type of system or even the same device, or may be different systems.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Code Path</th>
<th>Installation Instruction Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>pure C 32 bit</td>
<td>U1</td>
</tr>
<tr>
<td>2</td>
<td>pure C 32 bit</td>
<td>W1</td>
</tr>
<tr>
<td>3</td>
<td>pure C 64 bit</td>
<td>U1</td>
</tr>
<tr>
<td>4</td>
<td>pure C 64 bit</td>
<td>W1</td>
</tr>
<tr>
<td>5</td>
<td>x86 asm</td>
<td>U2</td>
</tr>
<tr>
<td>6</td>
<td>x86 asm</td>
<td>W2</td>
</tr>
<tr>
<td>7</td>
<td>x86-64 asm</td>
<td>U2</td>
</tr>
<tr>
<td>8</td>
<td>x84-64 asm</td>
<td>W2</td>
</tr>
<tr>
<td>9</td>
<td>pure C 32 bit</td>
<td>U2</td>
</tr>
<tr>
<td>10</td>
<td>pure C 32 bit</td>
<td>U2</td>
</tr>
</tbody>
</table>

Each of these command sets are relative to the top of the directory containing the uncompressed and expanded contents of the distribution file openssl-fips-1.2.2.tar.gz. The command sets are:

**U1:**

```
./config fipscanisterbuild no-asm
make
make install
```

**U2:**

```
./config fipscanisterbuild
make
make install
```

**W1:**

```
ms\do_fips no-asm
```

**W2:**

```
ms\do_fips
```

Installation instructions
OpenSSL FIPS 140-2 Security Policy

1. Download and copy the distribution file openss-fips-1.2.2.tar.gz to the target system. These files can be downloaded from http://www.openssl.org/source.

2. Verify the SHA-1 HMAC digest of the distribution file; see Appendix B. Note that if a suitable utility to generate SHA1 HMAC digests is not available, this check will need to be deferred until the openssl command is generated in the following step.

3. Unpack the distribution

   gunzip -c openssl-fips-1.2.2.tar.gz | tar xf -
   cd openssl-fips-1.2.2

4. Execute one of the installation command sets U1, W1, U2, W2 as shown above. No other command sets shall be used.

5. The resulting fipscanister.o or fipscanister.lib file is now available for use.

6. The calling application enables FIPS mode by calling the FIPS_mode_set() function.

Note that failure to use one of the specified commands sets exactly as shown will result in a module that cannot be considered compliant with FIPS 140-2.

Linking the Runtime Executable Application

Note that applications interfacing with the FIPS Object Module are outside of the cryptographic boundary. When linking the application with the FIPS Object Module two steps are necessary:

1. The HMAC-SHA-1 digest of the FIPS Object Module file must be calculated and verified against the installed digest to ensure the integrity of the FIPS object module.

2. A HMAC-SHA1 digest of the FIPS Object Module must be generated and embedded in the FIPS Object Module for use by the FIPS_mode_set() function at runtime initialization.

The OpenSSL distribution contains a reference utility which can be used to perform the verification of the FIPS Object Module and to generate the new HMAC-SHA-1 digest for the runtime executable application. Failure to embed the digest in the executable object will prevent initialization of FIPS mode.

At runtime the FIPS_mode_set() function compares the embedded HMAC-SHA-1 digest with a digest generated from the FIPS Object Module object code. This digest is the final link in the chain of validation from the original source to the runtime executable application file.

---

8 This utility is the “openssl sha” command with the -hmac option switch. It is included in the FIPS Object Module distribution and also in all recent OpenSSL distributions. The version of this utility generated from the FIPS Object Module distribution can be used to check the validity of the distribution tarball digest after the fact. Note that in principle a software distribution could be corrupted in such a way as to incorrectly return the expected digest. This risk is present for all validated products, of course, and would be even harder to detect without visible source code.
Appendix B  Controlled Distribution File Fingerprint

The OpenSSL FIPS Object Module v1.2.2 consists of the FIPS Object Module (the fipscanister.o or fipscanister.lib contiguous unit of binary object code) generated from the specific source files found in the specific special OpenSSL distribution openssl-fips-1.2.2.tar.gz with HMAC-SHA-1 digest of

4a8e3144895dfe1950f19b7445e8d55f5b09c8d8

located at http://www.openssl.org/source/openssl-fips-1.2.2.tar.gz.

This digests can be calculated and displayed with the commands

openssl sha1 -hmac etaonrishdlcupfm openssl-fips-1.2.2.tar.gz

The set of files specified in this tar file (or these files as modified by the aforementioned patch only) constitutes the complete set of source files of this module. There shall be no additions, deletions, or alterations of this set as used during module build. The OpenSSL distribution tar file (and patch file if used) shall be verified using the above HMAC-SHA-1 digest(s).

The arbitrary 16 byte key of:

65 74 61 6f 6e 72 69 73 68 64 6c 63 75 70 66 6d

(equivalent to the ASCII string "etaonrishdlcupfm") is used to generate the HMAC-SHA-1 value for the FIPS Object Module integrity check.