

# OpenSSL<sup>TM</sup>

Cryptography and SSL/TLS Toolkit

**OpenSSL FIPS  
Object Module**  
Version 2.0.10  
By the  
OpenSSL Software Foundation

**OpenSSL FIPS 140-2 Security Policy**  
Version 2.0.10

**August 14, 2015**

## Copyright Notice

Copyright © 2003-2015 the OpenSSL Software Foundation, Inc.

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

### Sponsored by:

[Intersoft International, Inc.](#)



## Acknowledgments

The OpenSSL Software Foundation (OSF) serves as the "vendor" for this validation. Project management coordination for this effort was provided by:

Steve Marquess	+1 877-673-6775
The OpenSSL Software Foundation	marquess@openssl.com
1829 Mount Ephraim Road	
Adamstown, MD 21710	
USA	

with technical work by:

Stephen Henson	shenson@openssl.com
4 Monaco Place,	shenson@drh-consultancy.co.uk
Westlands, Newcastle-under-Lyme	
Staffordshire. ST5 2QT.	
England, United Kingdom	<a href="http://www.drh-consultancy.co.uk/">http://www.drh-consultancy.co.uk/</a>

Andy Polyakov	appro@openssl.org
Chalmers University of Technology	appro@fy.chalmers.se
SE-412 96 Gothenburg	
Sweden	

Tim Hudson	tjh@openssl.com
P.O. Box 6389	tjh@cryptsoft.com
Fairfield Gardens 4103	
Australia	<a href="http://www.cryptsoft.com/">http://www.cryptsoft.com/</a>
ACN 074 537 821	

in coordination with the OpenSSL Team at [www.openssl.org](http://www.openssl.org).

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

Marc Ireland	805-783-0810 tel
FIPS Program Manager, CISSP	805-783-0889 fax
InfoGard Laboratories	mireland@infogard.com
709 Fiero Lane, Suite 25	<a href="http://www.infogard.com/">http://www.infogard.com/</a>
San Luis Obispo, CA 93401	

## Modification History

- 2015-06-29 Revised description for platforms 71, 72, 73, 74, 75, 76, 79, 80
- 2015-06-20 Revised description for platforms 66, 67
- 2015-06-16 Removed entries for platforms 47, 48, 49, 50, 59, 66, 67, 71, 72, 73, 74, 75, 76, 79, 80 to reflect prior CMVP action
- 2015-05-08 (2.0.10) Addition of nine platforms:
  - #103/104 iOS 8.1 64-bit on Apple A7 (ARMv8) (without/with optimizations)
  - #105 VxWorks 6.0 on Freescale P2020 (PPC)
  - #106/107 iOS 8.1 32-bit on Apple A7 (ARMv8) (without/with optimizations)
  - #108/109 Android 5.0 on Qualcomm APQ8084 (ARMv7) (without/with optimizations)
  - #110/111 Android 5.0 64-bit on SAMSUNG Exynos7420 (ARMv8) (without/with optimizations)
- 2015-02-02 (2.0.9) Addition of new platform #102, TS-Linux 2.4 on ARMv4
- 2014-11-25 (2.0.9) Addition of new platforms #97, #98, VMware Horizon Workspace 2.1 x86 under vSphere
  - Addition of new platform #99, QNX on ARMv4
  - Addition of new platforms #100, #101, Apple iOS 7.1 64-bit on ARMv8
- 2014-01-04 Addition of new platform #96, FreeBSD 8.4 on x86 without AES-NI
- 2014-07-30 Addition of two platforms #94, #95, FreeBSD 10.0 on x86, and re-removal of Dual EC DRBG
- 2014-07-28 Changed processor names for platforms #90, #91
- 2014-07-11 Added new platforms #88, #89, ArbOS 5.3 on x86 and #92, #93 FreeBSD 9.2 on x86
- 2014-06-12 Temporarily remove misplaced platform, move Dual EC DRBG to the Non-Approved Table 4c
- 2014-05-29 Added platforms #86, #87 FreeBSD 9.1 on x86, #90 Linux ORACLESP 2.6 on ASPEED AST-Series (ARMv5) , #91 ORACLESP 2.6 on Emulex PILOT 3 (ARMv5)
- 2014-05-12 Added platforms #81 Linux 2.6 on PPC, #82, #83 AcanOS 1.0 on x86, #84 AcanOS 1.0 on ARMv5, #85 FreeBSD 8.4 on x86
  - Multiple changes to separate the Approved services from those that are non-Approved per the SP 800-131A transition
- 2013-11-08 Added two platforms #79, #80 PexOS 1.0 under vSphere with/without AES-NI
- 2013-11-01 Added two platforms #77, #78 iOS 6.0 with/without NEON
- 2013-10-02 Added six platforms (Linux 3.4 x86 virtualized under XenSource/VMware/Hyper-V, with/without AES-NI)
  - Updated URL in Appendix A footnote

OpenSSL FIPS 140-2 Security Policy

2013-08-29 Added new sponsor acknowledgment  
2013-08-14 Added two Ubuntu 13.04 on ARMv7 (Beaglebone Black) and one Linux 3.8 on ARMv5TEJ platforms  
2013-07-24 Added two VMware Horizon Workspace platforms  
Fixed typo in Table 4.1a, Hash DRBGs 888 bits not 880  
2013-06-09 Added QNX, iOS 6.1, eCos for revision 2.0.5  
2013-05-01 Added OpenWRT 2.6 for revision 2.0.4  
2013-03-01 Added VMware Horizon Mobile 1.3, Apple OS X 10.7 , Apple iOS 5.0  
2013-02-23 Added WinEC7 and Android 4.0 for revision 2.0.3  
2013-02-14 Table 5: Removed references to non-existent Table 9  
Table 4a: added certs  
Table 4.1a: Added AES GCM  
2013-01-28 Added four platforms: Android 4.1 and Android 4.2 with and without NEON  
2013-01-08 Reworded section 8  
2013-01-03 Added Win2008, RHEL 32/64 bit under vSphere and Win7 with AES-NI.  
2012-12-08 Note EC DH Key Agreement and RSA Key Wrapping strength.  
2012-10-10 Added NetBSD 5.1 on PowerPC-e500, NetBSD 5.1 on Intel Xeon 5500 (x86-64) for revision 2.0.2  
2011-07-02 Added DSP Media Framework, Linux 2.6/Freescale PowerPC-e500, Android 4.0  
2011-06-15 Added iOS, WinCE 5, WinCE 6 OEs

OpenSSL FIPS 140-2 Security Policy

References

<i>Reference</i>	<i>Full Specification Name</i>
[ANS X9.31]	<i>Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)</i>
[FIPS 140-2]	<i><a href="#">Security Requirements for Cryptographic modules, May 25, 2001</a></i>
[FIPS 180-3]	<i><a href="#">Secure Hash Standard</a></i>
[FIPS 186-4]	<i><a href="#">Digital Signature Standard</a></i>
[FIPS 197]	<i><a href="#">Advanced Encryption Standard</a></i>
[FIPS 198-1]	<i><a href="#">The Keyed-Hash Message Authentication Code (HMAC)</a></i>
[SP 800-38B]	<i><a href="#">Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication</a></i>
[SP 800-38C]	<i><a href="#">Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality</a></i>
[SP 800-38D]	<i><a href="#">Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC</a></i>
[SP 800-56A]	<i><a href="#">Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography</a></i>
[SP 800-67R1]	<i><a href="#">Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher</a></i>
[SP 800-89]	<i><a href="#">Recommendation for Obtaining Assurances for Digital Signature Applications</a></i>
[SP 800-90]	<i><a href="#">Recommendation for Random Number Generation Using Deterministic Random Bit Generators</a></i>
[SP 800-131A]	<i><a href="#">Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths</a></i>

## Table of Contents

1 Introduction.....	8
2 Tested Configurations.....	10
3 Ports and Interfaces.....	15
4 Modes of Operation and Cryptographic Functionality.....	16
4.1 Critical Security Parameters and Public Keys.....	21
5 Roles, Authentication and Services.....	24
6 Self-test.....	26
7 Operational Environment.....	28
8 Mitigation of other Attacks.....	29
Appendix A Installation and Usage Guidance.....	30
Appendix B Controlled Distribution File Fingerprint.....	33
Appendix C Compilers.....	36

# 1 Introduction

This document is the non-proprietary security policy for the OpenSSL FIPS Object Module, hereafter referred to as the Module.

The Module is a software library providing a C-language application program interface (API) for use by other processes that require cryptographic functionality. The Module is classified by FIPS 140-2 as a software module, multi-chip standalone module embodiment. The physical cryptographic boundary is the general purpose computer on which the module is installed. The logical cryptographic boundary of the Module is the `fipscanister` object module, a single object module file named `fipscanister.o` (Linux<sup>®1</sup>/Unix<sup>®2</sup> and Vxworks<sup>®3</sup>) or `fipscanister.lib` (Microsoft Windows<sup>®4</sup>). The Module performs no communications other than with the calling application (the process that invokes the Module services).

Note that the OpenSSL FIPS Object Module v2.0.10 is fully backwards compatible with all earlier revisions of the OpenSSL FIPS Object Module v2.0. The v2.0.10 Module incorporates support for new platforms without disturbing functionality for any previously tested platforms. The v2.0.10 Module can be used in any environment supported by the earlier revisions of the Module, and those earlier revisions remain valid.

The FIPS 140-2 security levels for the Module are as follows:

Security Requirement	Security Level
Cryptographic Module Specification	1
Cryptographic Module Ports and Interfaces	1
Roles, Services, and Authentication	2
Finite State Model	1
Physical Security	NA
Operational Environment	1
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	NA

*Table 1 – Security Level of Security Requirements*

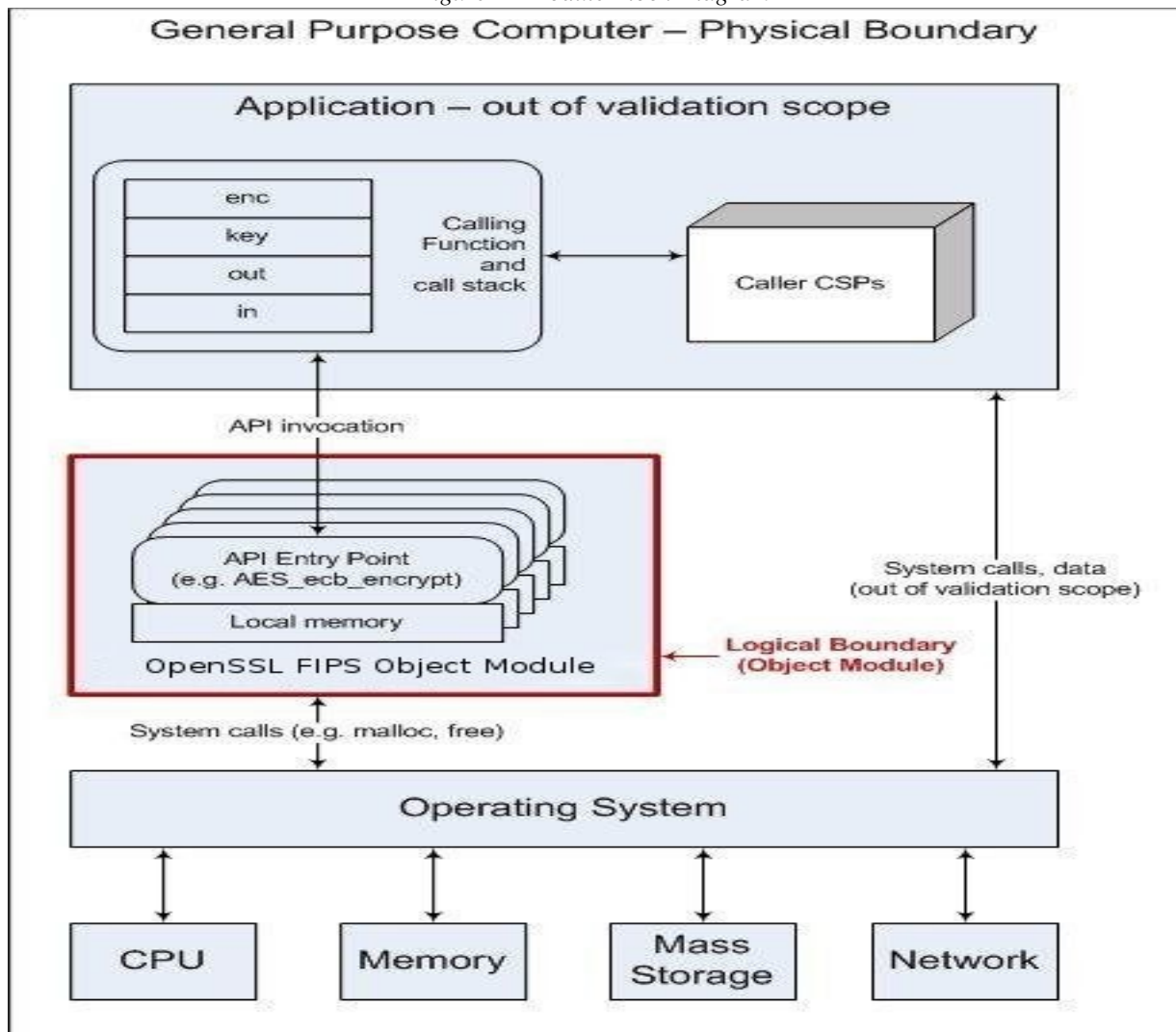
- 
- 1 Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.
  - 2 UNIX is a registered trademark of The Open Group
  - 3 Vxworks is a registered trademark owned by Wind River Systems, Inc
  - 4 Windows is a registered trademark of Microsoft Corporation in the United States and other countries.



The Module’s software version for this validation is 2.0.10. The v2.0.10 Module incorporates changes from the v2.0 module to support additional platforms. The v2.0.10 Module can be used in all the environments supported by the earlier v2.0, v2.0.1, v2.0.2, v2.0.3, v2.0.4, v2.0.5, v2.0.6, v2.0.7, v2.0.8 and v2.0.9 revisions of the Module.

Note, the v2.0.6 Module revision only incorporates changes from the v2.0 module to completely remove the Dual EC DRBG algorithm. All revisions prior to v2.0.8 that are not v2.0.6, in particular v2.0.7, still contain the Dual EC DRBG algorithm. The v2.0.8 revision again removes Dual EC DRBG that was restored in 2.0.7, and it will remain absent from all future revisions. The Dual EC DRBG algorithm shall not be used in the FIPS Approved mode of operation

Figure 1 - Module Block Diagram



## 2 Tested Configurations

#	Operational Environment	Processor	Optimizations (Target)	EC	B
1	Android 2.2 (HTC Desire)	Qualcomm QSD 8250 (ARMv7)	NEON	P	U2
2	Android 2.2 (Dell Streak)	Qualcomm QSD 8250 (ARMv7)	None	P	U2
3	Microsoft Windows 7 32 bit	Intel Celeron (x86)	None	BKP	W2
4	uClinux 0.9.29	ARM 922T (ARMv4)	None	BKP	U2
5	Fedora 14	Intel Core i5 (x86)	AES-NI	BKP	U2
6	HP-UX 11i ( hpux-ia64-cc, 32 bit mode)	Intel Itanium 2 (IA64)	None	BKP	U1
7	HP-UX 11i ( hpux64-ia64-cc, 64 bit mode)	Intel Itanium 2 (IA64)	None	BKP	U1
8	Ubuntu 10.04	Intel Pentium T4200 (x86)	None	BKP	U2
9	Android 3.0	NVIDIA Tegra 250 T20 (ARMv7)	None	P	U2
10	Linux 2.6.27	PowerPC e300c3 (PPC)	None	BKP	U2
11	Microsoft Windows 7 64 bit	Intel Pentium 4 (x86)	None	BKP	W2
12	Ubuntu 10.04 32 bit	Intel Core i5 (x86)	AES-NI	BKP	U2
13	Linux 2.6.33	PowerPC32 e300 (PPC)	None	BKP	U2
16	Android 2.2	OMAP 3530 (ARMv7)	NEON	BKP	U2
17	DSP Media Framework 1.4	TI C64x+	None	BKP	U2
19	VxWorks 6.8	TI TNETV1050 (MIPS)	None	BKP	U2
20	Linux 2.6	Broadcom BCM11107 (ARMv6)	None	BKP	U2
21	Linux 2.6	TI TMS320DM6446 (ARMv4)	None	BKP	U2
22	Linux 2.6.32	TI AM3703CBP (ARMv7)	None	BKP	U2
23	Solaris 10 32bit	SPARC-T3 (SPARCv9)	None	BKP	U2
24	Solaris 10 64bit	SPARC-T3 (SPARCv9)	None	BKP	U2
25	Solaris 11 32bit	Intel Xeon 5675 (x86)	None	BKP	U2
26	Solaris 11 64bit	Intel Xeon 5675 (x86)	None	BKP	U2
27	Solaris 11 32bit	Intel Xeon 5675 (x86)	AES-NI	BKP	U2
28	Solaris 11 64bit	Intel Xeon 5675 (x86)	AES-NI	BKP	U2

OpenSSL FIPS 140-2 Security Policy

29	Oracle Linux 5 64bit	Intel Xeon 5675 (x86)	None	BKP	U2
30	CascadeOS 6.1 32bit	Intel Pentium T4200 (x86)	None	BKP	U2
31	CascadeOS 6.1 64bit	Intel Pentium T4200 (x86)	None	BKP	U2
32	Ubuntu 10.04 32bit	Intel Pentium T4200 (x86)	None	BKP	U1
33	Ubuntu 10.04 64bit	Intel Pentium T4200 (x86)	None	BKP	U1
34	Oracle Linux 5	Intel Xeon 5675 (x86)	AES-NI	BKP	U2
35	Oracle Linux 6	Intel Xeon 5675 (x86)	None	BKP	U2
36	Oracle Linux 6	Intel Xeon 5675 (x86)	AES-NI	BKP	U2
37	Solaris 11 32bit	SPARC-T3 (SPARCv9)	None	BKP	U2
38	Solaris 11 64bit	SPARC-T3 (SPARCv9)	None	BKP	U2
39	Android 4.0	NVIDIA Tegra 250 T20 (ARMv7)	None	P	U2
40	Linux 2.6	Freescale PowerPC-e500	None	BKP	U2
41	Apple iOS 5.1	ARMv7	None	BKP	U2
42	WinCE 6.0	ARMv5TEJ	None	BKP	W2
43	WinCE 5.0	ARMv7	None	BKP	W2
44	Android 4.0	OMAP 3	NEON	P	U2
45	NetBSD 5.1	PowerPC-e500	None	BKP	U2
46	NetBSD 5.1	Intel Xeon 5500 (x86)	None	BKP	U2
47					
48					
49					
50					
51	Windows 7 64-bit	Intel Core i5-2430M (x86)	AES-NI	BKP	W2
52	Android 4.1	TI DM3730 (ARMv7)	None	P	U2
53	Android 4.1	TI DM3730 (ARMv7)	NEON	P	U2
54	Android 4.2	Nvidia Tegra 3 (ARMv7)	None	P	U2
55	Android 4.2	Nvidia Tegra 3 (ARMv7)	NEON	P	U2
56	Windows Embedded Compact 7	Freescale i.MX53xA (ARMv7)	NEON	BKP	W2
57	Windows Embedded Compact 7	Freescale i.MX53xD (ARMv7)	NEON	BKP	W2

OpenSSL FIPS 140-2 Security Policy

58	Android 4.0	Qualcomm Snapdragon APQ8060 (ARMv7)	NEON	BKP	U2
59					
60	Apple OS X 10.7	Intel Core i7-3615QM	None	BKP	U2
61	Apple iOS 5.0	ARM Cortex A8 (ARMv7)	NEON	BKP	U2
62	OpenWRT 2.6	MIPS 24Kc	None	BKP	U2
63	QNX 6.4	Freescale i.MX25 (ARMv4)	None	BKP	U2
64	Apple iOS 6.1	Apple A6X SoC (ARMv7s)	None	BKP	U2
65	eCos 3	Freescale i.MX27 926ejs (ARMv5TEJ)	None	BKP	U2
66	VMware Horizon Workspace 1.5 under VMware ESXi 5.0	Intel Xeon E3-1220 (x86)	None	BKP	U2
67	VMware Horizon Workspace 1.5 under VMware ESXi 5.0	Intel Xeon E3-1220 (x86)	AES-NI	BKP	U2
68	Ubuntu 13.04	AM335x Cortex-A8 (ARMv7)	None	BKP	U2
69	Ubuntu 13.04	AM335x Cortex-A8 (ARMv7)	NEON	BKP	U2
70	Linux 3.8	ARM926 (ARMv5TEJ)	None	BKP	U2
71	Linux 3.4 under Citrix XenServer 6.2	Intel Xeon E5-2430L (x86)	None	BKP	U2
72	Linux 3.4 under Citrix XenServer 6.2	Intel Xeon E5-2430L (x86)	AES-NI	BKP	U2
73	Linux 3.4 under VMware ESXi 5.1	Intel Xeon E5-2430L (x86)	None	BKP	U2
74	Linux 3.4 under VMware ESXi 5.1	Intel Xeon E5-2430L (x86)	AES-NI	BKP	U2
75	Linux 3.4 under Microsoft Windows 2012 Hyper-V	Intel Xeon E5-2430L (x86)	None	BKP	U2
76	Linux 3.4 under Microsoft Windows 2012 Hyper-V	Intel Xeon E5-2430L (x86)	AES-NI	BKP	U2
77	Apple iOS 6.0	Apple A5 / ARM Cortex-A9 (ARMv7)	None	BKP	U2
78	Apple iOS 6.0	Apple A5 / ARM Cortex-A9 (ARMv7)	NEON	BKP	U2
79	PexOS 1.0 under vSphere ESXi 5.1	Intel Xeon E5-2430L (x86)	None	BKP	U2
80	PexOS 1.0 under vSphere ESXi 5.1	Intel Xeon E5-2430L (x86)	AES-NI	BKP	U2
81	Linux 2.6	Freescale e500v2 (PPC)	None	BKP	U2

OpenSSL FIPS 140-2 Security Policy

82	AcanOS 1.0	Intel Core i7-3612QE (x86)	None	BKP	U2
83	AcanOS 1.0	Intel Core i7-3612QE (x86)	AES-NI	BKP	U2
84	AcanOS 1.0	Feroceon 88FR131 (ARMv5)	None	BKP	U2
85	FreeBSD 8.4	Intel Xeon E5440 (x86)	None	BKP	U2
86	FreeBSD 9.1	Xeon E5-2430L (x86)	None	BKP	U2
87	FreeBSD 9.1	Xeon E5-2430L (x86)	AES-NI	BKP	U2
88	ArbOS 5.3	Xeon E5645 (x86)	None	BKP	U2
89	ArbOS 5.3	Xeon E5645 (x86)	AES-NI	BKP	U2
90	Linux ORACLESP 2.6	ASPEED AST-Series (ARMv5)	None	BKP	U2
91	Linux ORACLESP 2.6	Emulex PILOT 3 (ARMv5)	None	BKP	U2
92	FreeBSD 9.2	Xeon E5-2430L (x86)	None	BKP	U2
93	FreeBSD 9.2	Xeon E5-2430L (x86)	AES-NI	BKP	U2
94	FreeBSD 10.0	Xeon E5-2430L (x86)	None	BKP	U2
95	FreeBSD 10.0	Xeon E5-2430L (x86)	AES-NI	BKP	U2
96	FreeBSD 8.4 32-bit	Xeon E5440 (x86)	None	BKP	U2
97	VMware Horizon Workspace 2.1 x86 under vSphere ESXi 5.5	Intel Xeon E3-1220	None	BKP	U2
98	VMware Horizon Workspace 2.1 x86 under vSphere ESXi 5.5	Intel Xeon E3-1220	AES-NI	BKP	U2
99	QNX 6.5 on ARMv4	Freescale i.MX25 (ARMv4)	None	BKP	U2
100	Apple iOS 7.1 64-bit on ARMv8	Apple A7 (ARMv8)	None	BKP	U2
101	Apple iOS 7.1 64-bit on ARMv8	Apple A7 (ARMv8)	NEON	BKP	U2
102	TS-Linux 2.4	Arm920Tid (ARMv4)	None	BKP	U2
103	iOS 8.1 64-bit	Apple A7 (ARMv8)	None	BKP	U2
104	iOS 8.1 64-bit	Apple A7 (ARMv8)	NEON and Crypto Extensions	BKP	U2
105	VxWorks 6.9	Freescale P2020 (PPC)	None	BKP	U2
106	iOS 8.1 32-bit	Apple A7 (ARMv8)	None	BKP	U2

OpenSSL FIPS 140-2 Security Policy

107	iOS 8.1 32-bit	Apple A7 (ARMv8)	NEON	BKP	U2
108	Android 5.0 32-bit	Qualcomm APQ8084 (ARMv7)	None	BKP	U2
109	Android 5.0 32-bit	Qualcomm APQ8084 (ARMv7)	NEON	BKP	U2
110	Android 5.0 64-bit	SAMSUNG Exynos7420 (ARMv8)	None	BKP	U2
111	Android 5.0 64-bit	SAMSUNG Exynos7420 (ARMv8)	NEON and Crypto Extensions	BKP	U2

*Table 2 - Tested Configurations (B = Build Method; EC = Elliptic Curve Support). The EC column indicates support for prime curve only (P), or all NIST defined B, K, and P curves (BKP).*

See Appendix A for additional information on build method and optimizations. See Appendix C for a list of the specific compilers used to generate the Module for the respective operational environments.

### 3 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).

<b>Logical interface type</b>	<b>Description</b>
<i>Control input</i>	<i>API entry point and corresponding stack parameters</i>
<i>Data input</i>	<i>API entry point data input stack parameters</i>
<i>Status output</i>	<i>API entry point return values and status stack parameters</i>
<i>Data output</i>	<i>API entry point data output stack parameters</i>

*Table 3 - Logical interfaces*

As a software module, control of the physical ports is outside module scope. However, when the module is performing self-tests, or is in an error state, all output on the logical data output interface is inhibited. The module is single-threaded and in error scenarios returns only an error value (no data output is returned).

## 4 Modes of Operation and Cryptographic Functionality

The Module supports only a FIPS 140-2 Approved mode. Tables 4a and 4b list the Approved and Non-approved but Allowed algorithms, respectively.

Function	Algorithm	Options	Cert #
Random Number Generation; Symmetric key generation	[ANS X9.31] RNG	AES 128/192/256	985, 1087, 1119, 1166, 1186, 1202, 1278 1292, 1314, 1349
	[SP 800-90] DRBG <sup>5</sup> Prediction resistance supported for all variations	Hash DRBG HMAC DRBG, no reseed CTR DRBG (AES), no derivation function	157, 229, 264, 292, 316, 342, 485, 540, 607, 723
Encryption, Decryption and CMAC	[SP 800-67]	3-Key TDES ECB, TCBC, TCFB, TOFB; CMAC generate and verify	1223, 1346, 1398, 1465, 1492, 1522, 1695, 1742, 1780, 1853
	[FIPS 197] AES	128/ 192/256 ECB, CBC, OFB, CFB 1, CFB 8,	1884,

---

5 For all DRBGs the "supported security strengths" is just the highest supported security strength per [SP800-90] and [SP800-57].



OpenSSL FIPS 140-2 Security Policy

	[SP 800-38B] CMAC [SP 800-38C] CCM [SP 800-38D] GCM [SP 800-38E] XTS	CFB 128, CTR, XTS; CCM; GCM; CMAC generate and verify	2116, 2234, 2342, 2394, 2484, 2824, 2929, 3090, 3264
Message Digests	[FIPS 180-3]	SHA-1, SHA-2 (224, 256, 384, 512)	1655, 1840, 1923, 2019, 2056, 2102, 2368, 2465, 2553, 2702
Keyed Hash	[FIPS 198] HMAC	SHA-1, SHA-2 (224, 256, 384, 512)	1126, 1288, 1363, 1451, 1485, 1526, 1768, 1856, 1937, 2063
Digital Signature and Asymmetric Key Generation	[FIPS 186-2] RSA	GenKey9.31, SigGen9.31, SigGenPKCS1.5, SigGenPSS, SigVer9.31, SigVerPKCS1.5, SigVerPSS (2048/3072/4096 with all SHA-2 sizes)	960, 1086, 1145, 1205, 1273, 1477, 1535, 1581, 1664
	[FIPS 186-4] DSA	PQG Gen, PQG Ver, Key Pair Gen, Sig Gen, Sig Ver (1024/2048/3072 with all SHA-2 sizes)	589, 661, 693, 734, 748, 764, 853, 870, 896, 933

OpenSSL FIPS 140-2 Security Policy

	[FIPS 186-2] ECDSA	PKG: CURVES( P-224 P-384 P-521 K-233 K-283 K-409 K-571 B-233 B-283 B-409 B-571 ) PKV: CURVES( P-192 P-224 P-256 P-384 P-521 K-163 K-233 K-283 K-409 K-571 B-163 B-233 B-283 B-409 B-571 )	270, 315, 347, 383, 394, 413, 496, 528, 558, 620
		PKG: CURVES( P-224 P-384 P-521 ) PKV: CURVES( P-192 P-224 P-256 P-384 P-521 )	264, 378
	[FIPS 186-4] ECDSA	PKG: CURVES( P-224 P-256 P-384 P-521 K-224 K-256 K-384 K-521 B-224 B-256 B-384 B-521 ExtraRandomBits TestingCandidates ) PKV: CURVES( ALL-P ALL-K ALL-B ) SigGen: CURVES( P-224: (SHA-224, 256, 384, 512) P-256: (SHA-224, 256, 384, 512) P-384: (SHA-224, 256, 384, 512) P-521: (SHA-224, 256, 384, 512) K-233: (SHA-224, 256, 384, 512) K-283: (SHA-224, 256, 384, 512) K-409: (SHA-224, 256, 384, 512) K-571: (SHA-224, 256, 384, 512) B-233: (SHA-224, 256, 384, 512) B-283: (SHA-224, 256, 384, 512) B-409: (SHA-224, 256, 384, 512) B-571: (SHA-224, 256, 384, 512) ) SigVer: CURVES( P-192: (SHA-1, 224, 256, 384, 512) P-224: (SHA-1, 224, 256, 384, 512) P-256: (SHA-1, 224, 256, 384, 512) P-384: (SHA-1, 224, 256, 384, 512) P-521: (SHA-1, 224, 256, 384, 512) K-163: (SHA-1, 224, 256, 384, 512) K-233: (SHA-1, 224, 256, 384, 512) K-283: (SHA-1, 224, 256, 384, 512) K-409: (SHA-1, 224, 256, 384, 512) K-571: (SHA-1, 224, 256, 384, 512) B-163: (SHA-1, 224, 256, 384, 512) B-233: (SHA-1, 224, 256, 384, 512) B-283: (SHA-1, 224, 256, 384, 512) B-409: (SHA-1, 224, 256, 384, 512) B-571: (SHA-1, 224, 256, 384, 512) )	270, 315, 347, 383, 394, 413, 496, 528, 558, 620, 663

OpenSSL FIPS 140-2 Security Policy

		PKG: CURVES( P-224 P-256 P-384 P-521 ) PKV: CURVES( ALL-P ) SigGen: CURVES( P-224: (SHA-224, 256, 384, 512) P-256: (SHA-224, 256, 384, 512) P-384: (SHA-224, 256, 384, 512) P-521: (SHA-224, 256, 384, 512) ) SigVer: CURVES( P-192: (SHA-1, 224, 256, 384, 512) P-224: (SHA-1, 224, 256, 384, 512) P-256: (SHA-1, 224, 256, 384, 512) P-384: (SHA-1, 224, 256, 384, 512) P-521: (SHA-1, 224, 256, 384, 512) )	264, 378
ECC CDH (KAS)	[SP 800-56A] (§5.7.1.2)	All NIST defined B, K and P curves except sizes 163 and 192	12, 24, 36, 53, 71, 85, 260, 331, 372, 472
		All NIST defined P curves	10, 49

Table 4a – FIPS Approved Cryptographic Functions

The Module supports only NIST defined curves for use with ECDSA and ECC CDH. The Module supports two operational environment configurations for elliptic curve; NIST prime curve only (listed in Table 2 with the EC column marked "P") and all NIST defined curves (listed in Table 2 with the EC column marked "BKP").

Category	Algorithm	Description
Key Agreement	EC DH	Non-compliant (untested) DH scheme using elliptic curve, supporting all NIST defined B, K and P curves. Key agreement is a service provided for calling process use, but is not used to establish keys into the Module.
Key Encryption, Decryption	RSA	The RSA algorithm may be used by the calling application for encryption or decryption of keys. No claim is made for SP 800-56B compliance, and no CSPs are established into or exported out of the module using these services.

Table 4b – Non-FIPS Approved But Allowed Cryptographic Functions

The Module implements the following services which are Non-Approved per the SP 800-131A transition:

Function	Algorithm	Options	Cert #

OpenSSL FIPS 140-2 Security Policy

Random Number Generation; Symmetric key generation	[SP 800-90] DRBG	Dual EC DRBG	157, 229, 264, 292, 316, 342, 485
Digital Signature and Asymmetric Key Generation	[FIPS 186-2] RSA	GenKey9.31, SigGen9.31, SigGenPKCS1.5, SigGenPSS (1024/1536 with all SHA sizes, 2048/3072/4096 with SHA-1)	589, 661, 693, 734, 748, 764
	[FIPS 186-2] DSA	PQG Gen, Key Pair Gen, Sig Gen (1024 with all SHA sizes, 2048/3072 with SHA-1)	589, 661, 693, 734, 748, 764
	[FIPS 186-4] DSA	PQG Gen, Key Pair Gen, Sig Gen (1024 with all SHA sizes, 2048/3072 with SHA-1)	589, 661, 693, 734, 748, 764
	[FIPS 186-2] ECDSA	PKG: CURVES( P-192 K-163 B-163 ) SIG(gen): CURVES( P-192 P-224 P-256 P-384 P-521 K-163 K-233 K-283 K-409 K-571 B-163 B-233 B-283 B-409 B-571 )	270, 315, 347, 383, 394, 413
	[FIPS 186-4] ECDSA	PKG: CURVES( P-192 K-163 B-163 ) SigGen: CURVES( P-192: (SHA-1, 224, 256, 384, 512) P-224:(SHA-1) P-256:(SHA-1) P-384: (SHA-1) P-521:(SHA-1) K-163: (SHA-1, 224, 256, 384, 512) K-233:(SHA-1) K-283:(SHA-1) K-409:(SHA-1) K-571:(SHA-1) B-163: (SHA-1, 224, 256, 384, 512) B-233:(SHA-1) B-283: (SHA-1) B-409:(SHA-1) B-571:(SHA-1) )	270, 315, 347, 383, 394, 413
ECC CDH (CVL)	[SP 800-56A] (§5.7.1.2)	All NIST Recommended B, K and P curves sizes 163 and 192	264, 378
			12, 24, 36, 53, 71, 85
			10, 49

Table 4c – FIPS Non-Approved Cryptographic Functions

These algorithms shall not be used when operating in the FIPS Approved mode of operation. EC DH Key Agreement provides a maximum of 256 bits of security strength. RSA Key Wrapping provides a maximum of 256 bits of security strength.

The Module requires an initialization sequence (see IG 9.5): the calling application invokes `FIPS_mode_set()`<sup>6</sup>, which returns a “1” for success and “0” for failure. If `FIPS_mode_set()` fails then all cryptographic services fail from then on. The application can test to see if FIPS mode has been successfully performed.

The Module is a cryptographic engine library, which can be used only in conjunction with additional software. Aside from the use of the NIST defined elliptic curves as trusted third party domain parameters, all other FIPS 186-3 assurances are outside the scope of the Module, and are the responsibility of the calling process.

#### 4.1 Critical Security Parameters and Public Keys

All CSPs used by the Module are described in this section. All access to these CSPs by Module services are described in Section 4. The CSP names are generic, corresponding to API parameter data structures.

CSP Name	Description
RSA SGK	RSA (1024 to 16384 bits) signature generation key
RSA KDK	RSA (1024 to 16384 bits) key decryption (private key transport) key
DSA SGK	[FIPS 186-4] DSA (1024/2048/3072) signature generation key or [FIPS 186-2] DSA (1024) signature generation key
ECDSA SGK	ECDSA (All NIST defined B, K, and P curves) signature generation key
EC DH Private	EC DH (All NIST defined B, K, and P curves) private key agreement key.
AES EDK	AES (128/192/256) encrypt / decrypt key
AES CMAC	AES (128/192/256) CMAC generate / verify key
AES GCM	AES (128/192/256) encrypt / decrypt / generate / verify key
AES XTS	AES (256/512) XTS encrypt / decrypt key
TDES EDK	TDES (3-Key) encrypt / decrypt key
TDES CMAC	TDES (3-Key) CMAC generate / verify key
HMAC Key	Keyed hash key (160/224/256/384/512)
RNG CSPs	Seed (128 bit), AES 128/192/256 seed key and associated state variables for ANS X9.31 AES based RNG <sup>7</sup>
Hash_DRBG CSPs	V (440/888 bits) and C (440/888 bits), entropy input (length dependent on security strength)

6 The function call in the Module is `FIPS_module_mode_set()` which is typically used by an application via the `FIPS_mode_set()` wrapper function.

7 There is an explicit test for equality of the seed and seed key inputs

OpenSSL FIPS 140-2 Security Policy

HMAC_DRBG CSPs	V (160/224/256/384/512 bits) and Key (160/224/256/384/512 bits), entropy input (length dependent on security strength)
CTR_DRBG CSPs	V (128 bits) and Key (AES 128/192/256), entropy input (length dependent on security strength)
Dual_EC_DRBG CSPs	S (P-256, P-384, P-521), entropy input (length dependent on security strength)
CO-AD-Digest	Pre-calculated HMAC-SHA-1 digest used for Crypto Officer role authentication
User-AD-Digest	Pre-calculated HMAC-SHA-1 digest used for User role authentication

Table 4.1a – Critical Security Parameters

Authentication data is loaded into the module during the module build process, performed by an authorized operator (Crypto Officer), and otherwise cannot be accessed.

The module does not output intermediate key generation values.

CSP Name	Description
RSA SVK	RSA (1024 to 16384 bits) signature verification public key
RSA KEK	RSA (1024 to 16384 bits) key encryption (public key transport) key
DSA SVK	[FIPS 186-4] DSA (1024/2048/3072) signature verification key or [FIPS 186-2] DSA (1024) signature verification key
ECDSA SVK	ECDSA (All NIST defined B, K and P curves) signature verification key
EC DH Public	EC DH (All NIST defined B, K and P curves) public key agreement key.

Table 4.1b – Public Keys

**For all CSPs and Public Keys:**

**Storage:** RAM, associated to entities by memory location. The Module stores RNG and DRBG state values for the lifetime of the RNG or DRBG instance. The module uses CSPs passed in by the calling application on the stack. The Module does not store any CSP persistently (beyond the lifetime of an API call), with the exception of RNG and DRBG state values used for the Modules' default key generation service.

**Generation:** The Module implements ANSI X9.31 compliant RNG and SP 800-90 compliant DRBG services for creation of symmetric keys, and for generation of DSA, elliptic curve, and RSA keys as shown in Table 4a. The calling application is responsible for storage of generated keys returned by the module.

**Entry:** All CSPs enter the Module's logical boundary in plaintext as API parameters, associated by memory location. However, none cross the physical boundary.

**Output:** The Module does not output CSPs, other than as explicit results of key generation services. However, none cross the physical boundary.

**Destruction:** Zeroization of sensitive data is performed automatically by API function calls for temporarily stored CSPs. In addition, the module provides functions to explicitly destroy CSPs related to random number generation services. The calling application is responsible for parameters passed in and out of the module.

Private and secret keys as well as seeds and entropy input are provided to the Module by the calling application, and are destroyed when released by the appropriate API function calls. Keys residing in internally allocated data structures (during the lifetime of an API call) can only be accessed using the Module defined API. The operating system protects memory and process space from unauthorized access. Only the calling application that creates or imports keys can use or export such keys. All API functions are executed by the invoking calling application in a non-overlapping sequence such that no two API functions will execute concurrently. An authorized application as user (Crypto-Officer and User) has access to all key data generated during the operation of the Module.

In the event Module power is lost and restored the calling application must ensure that any AES-GCM keys used for encryption or decryption are re-distributed.

Module users (the calling applications) shall use entropy sources that meet the security strength required for the random number generation mechanism: 128 bits for the [ANS X9.31] RNG mechanism, and as shown in [SP 800-90] Table 2 (Hash\_DRBG, HMAC\_DRBG), Table 3 (CTR\_DRBG) and Table 4 (Dual\_EC\_DRBG). This entropy is supplied by means of callback functions. Those functions must return an error if the minimum entropy strength cannot be met.

## 5 Roles, Authentication and Services

The Module implements the required User and Crypto Officer roles and requires authentication for those roles. Only one role may be active at a time and the Module does not allow concurrent operators. The User or Crypto Officer role is assumed by passing the appropriate password to the `FIPS_module_mode_set()` function. The password values may be specified at build time and must have a minimum length of 16 characters. Any attempt to authenticate with an invalid password will result in an immediate and permanent failure condition rendering the Module unable to enter the FIPS mode of operation, even with subsequent use of a correct password.

Authentication data is loaded into the Module during the Module build process, performed by the Crypto Officer, and otherwise cannot be accessed.

Since minimum password length is 16 characters, the probability of a random successful authentication attempt in one try is a maximum of  $1/256^{16}$ , or less than  $1/10^{38}$ . The Module permanently disables further authentication attempts after a single failure, so this probability is independent of time.

Both roles have access to all of the services provided by the Module.

- User Role (User): Loading the Module and calling any of the API functions.
- Crypto Officer Role (CO): Installation of the Module on the host computer system and calling of any API functions.

All services implemented by the Module are listed below, along with a description of service CSP access.

Service	Role	Description
Initialize	User, CO	Module initialization. Does not access CSPs.
Self-test	User, CO	Perform self tests ( <code>FIPS_selftest</code> ). Does not access CSPs.
Show status	User, CO	Functions that provide module status information: <ul style="list-style-type: none"> <li>• Version (as unsigned long or const char *)</li> <li>• FIPS Mode (Boolean)</li> </ul> Does not access CSPs.
Zeroize	User, CO	Functions that destroy CSPs: <ul style="list-style-type: none"> <li>• <code>fips_rand_prng_reset</code>: destroys RNG CSPs.</li> <li>• <code>fips_drbg_uninstantiate</code>: for a given DRBG context, overwrites DRBG CSPs (Hash_DRBG CSPs, HMAC_DRBG CSPs, CTR_DRBG CSPs, Dual_EC_DRBG CSPs.)</li> </ul> All other services automatically overwrite CSPs stored in allocated memory. Stack cleanup is the responsibility of the calling application.



OpenSSL FIPS 140-2 Security Policy

Service	Role	Description
Random number generation	User, CO	Used for random number and symmetric key generation. <ul style="list-style-type: none"> <li>Seed or reseed an RNG or DRBG instance</li> <li>Determine security strength of an RNG or DRBG instance</li> <li>Obtain random data</li> </ul> Uses and updates RNG CSPs, Hash_DRBG CSPs, HMAC_DRBG CSPs, CTR_DRBG CSPs, Dual_EC_DRBG CSPs.
Asymmetric key generation	User, CO	Used to generate DSA, ECDSA and RSA keys: RSA SGK, RSA SVK; DSA SGK, DSA SVK; ECDSA SGK, ECDSA SVK There is one supported entropy strength for each mechanism and algorithm type, the maximum specified in SP800-90
Symmetric encrypt/decrypt	User, CO	Used to encrypt or decrypt data. Executes using AES EDK, TDES EDK (passed in by the calling process).
Symmetric digest	User, CO	Used to generate or verify data integrity with CMAC. Executes using AES CMAC, TDES, CMAC (passed in by the calling process).
Message digest	User, CO	Used to generate a SHA-1 or SHA-2 message digest. Does not access CSPs.
Keyed Hash	User, CO	Used to generate or verify data integrity with HMAC. Executes using HMAC Key (passed in by the calling process).
Key transport <sup>8</sup>	User, CO	Used to encrypt or decrypt a key value on behalf of the calling process (does not establish keys into the module). Executes using RSA KDK, RSA KEK (passed in by the calling process).
Key agreement	User, CO	Used to perform key agreement primitives on behalf of the calling process (does not establish keys into the module). Executes using EC DH Private, EC DH Public (passed in by the calling process).
Digital signature	User, CO	Used to generate or verify RSA, DSA or ECDSA digital signatures. Executes using RSA SGK, RSA SVK; DSA SGK, DSA SVK; ECDSA SGK, ECDSA SVK (passed in by the calling process).
Utility	User, CO	Miscellaneous helper functions. Does not access CSPs.

Table 5 - Services and CSP Access

---

<sup>8</sup> "Key transport" can refer to a) moving keys in and out of the module or b) the use of keys by an external application. The latter definition is the one that applies to the OpenSSL FIPS Object Module.

## 6 Self-test

The Module performs the self-tests listed below on invocation of Initialize or Self-test.

Algorithm	Type	Test Attributes
Software integrity	KAT	HMAC-SHA1
HMAC	KAT	One KAT per SHA1, SHA224, SHA256, SHA384 and SHA512 Per IG 9.3, this testing covers SHA POST requirements.
AES	KAT	Separate encrypt and decrypt, ECB mode, 128 bit key length
AES CCM	KAT	Separate encrypt and decrypt, 192 key length
AES GCM	KAT	Separate encrypt and decrypt, 256 key length
XTS-AES	KAT	128, 256 bit key sizes to support either the 256-bit key size (for XTS-AES-128) or the 512-bit key size (for XTS-AES-256)
AES CMAC	KAT	Sign and verify CBC mode, 128, 192, 256 key lengths
TDES	KAT	Separate encrypt and decrypt, ECB mode, 3-Key
TDES CMAC	KAT	CMAC generate and verify, CBC mode, 3-Key
RSA	KAT	Sign and verify using 2048 bit key, SHA-256, PKCS#1
DSA	PCT	Sign and verify using 2048 bit key, SHA-384
DRBG	KAT	CTR_DRBG: AES, 256 bit with and without derivation function HASH_DRBG: SHA256 HMAC_DRBG: SHA256 Dual_EC_DRBG: P-256 and SHA256
ECDSA	PCT	Keygen, sign, verify using P-224, K-233 and SHA512. The K-233 self-test is not performed for operational environments that support prime curve only (see Table 2).
ECC CDH	KAT	Shared secret calculation per SP 800-56A §5.7.1.2, IG 9.6
X9.31 RNG	KAT	128, 192, 256 bit AES keys

Table 6a - Power On Self Tests (KAT = Known answer test; PCT = Pairwise consistency test)

The Module is installed using one of the set of instructions in Appendix A, as appropriate for the target system. 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.

The `FIPS_mode_set()`<sup>9</sup> function performs all power-up self-tests listed above with no operator intervention required, returning a “1” if all power-up self-tests succeed, and a “0” otherwise. If any component of the power-up self-test fails an internal flag is set to prevent subsequent invocation of any cryptographic function calls. The module will only enter the FIPS Approved mode if the module is reloaded and the call to `FIPS_mode_set()`<sup>9</sup> succeeds.

<sup>9</sup> `FIPS_mode_set()` calls Module function `FIPS_module_mode_set()`

The power-up self-tests may also be performed on-demand by calling `FIPS_selftest()`, which returns a “1” for success and “0” for failure. Interpretation of this return code is the responsibility of the calling application.

The Module also implements the following conditional tests:

<b>Algorithm</b>	<b>Test</b>
DRBG	Tested as required by [SP800-90] Section 11
DRBG	FIPS 140-2 continuous test for stuck fault
DSA	Pairwise consistency test on each generation of a key pair
ECDSA	Pairwise consistency test on each generation of a key pair
RSA	Pairwise consistency test on each generation of a key pair
ANSI X9.31 RNG	Continuous test for stuck fault

*Table 6b - Conditional Tests*

In the event of a DRBG self-test failure the calling application must uninstantiate and re-instantiate the DRBG per the requirements of [SP 800-90]; this is not something the Module can do itself.

Pairwise consistency tests are performed for both possible modes of use, e.g. Sign/Verify and Encrypt/Decrypt.

The Module supports two operational environment configurations for elliptic curve: NIST prime curves only (listed in Table 2 with the EC column marked "P") and all NIST defined curves (listed in Table 2 with the EC column marked "BKP").

## **7 Operational Environment**

The tested operating systems segregate user processes into separate process spaces. Each process space is logically separated from all other processes by the operating system software and hardware. The Module functions entirely within the process space of the calling application, and implicitly satisfies the FIPS 140-2 requirement for a single user mode of operation.

## **8 Mitigation of other Attacks**

The module is not designed to mitigate against attacks which are outside of the scope of FIPS 140-2.

## Appendix A Installation and Usage Guidance

The test platforms represent different combinations of installation instructions. For each platform 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 – the Module supports cross-compilation environments.

Each of these command sets are relative to the top of the directory containing the uncompressed and expanded contents of the distribution files *openssl-fips-2.0.10.tar.gz* (all NIST defined curves as listed in Table 2 with the EC column marked "BKP") or *openssl-fips-ecp-2.0.10.tar.gz* (NIST prime curves only as listed in Table 2 with the EC column marked "P"). The command sets are:

```
U1:
    ./config no-asm
    make
    make install
```

```
U2:
    ./config
    make
    make install
```

```
W1:
    ms\do_fips no-asm
```

```
W2:
    ms\do_fips
```

### Installation instructions

1. Download and copy the distribution file to the build system.  
These files can be downloaded from <http://www.openssl.org/source/>.
2. Verify the HMAC-SHA-1 digest of the distribution file; see Appendix B. An independently acquired FIPS 140-2 validated implementation of SHA-1 HMAC must be used for this digest verification. Note that this verification can be performed on any convenient system and not necessarily on the specific build or target system. Alternatively, a copy of the distribution on physical media can be obtained from OSF<sup>10</sup>.

---

<sup>10</sup> For some prospective users the acquisition, installation, and configuration of a suitable FIPS 140-2 validated product may not be convenient. OSF will on request mail a CD containing the source code distribution, via USPS or international post. A distribution file received by that means need not be verified by a FIPS 140-2 validated implementation of HMAC-SHA-1. For instructions on requesting this CD see <http://openssl.com/fips/verify.html>.

3. Unpack the distribution

```
gunzip -c openssl-fips-2.0.10.tar.gz | tar xf -  
cd openssl-fips-2.0.10
```

or

```
gunzip -c openssl-fips-ecp-2.0.10.tar.gz | tar xf -  
cd openssl-fips-ecp-2.0.10
```

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 *fipsanister.o* or *fipsanister.lib* file is now available for use.
6. The calling application enables FIPS mode by calling the `FIPS_mode_set()`<sup>11</sup> 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()`<sup>11</sup> function at runtime initialization.

The `fips_standalone_sha1` command 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()`<sup>11</sup> 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.

#### **Optimization**

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.

For OpenSSL with x86 there are three possible optimization levels:

---

<sup>11</sup> `FIPS_mode_set()` calls the Module function `FIPS_module_mode_set()`

1. No optimization (plain C)
2. SSE2 optimization
3. AES-NI+PCLMULQDQ+SSSE3 optimization

Other theoretically possible combinations (e.g. AES-NI only, or SSE3 only) are not addressed individually, so that a processor which does not support all three of AES-NI, PCLMULQDQ, and SSSE3 will fall back to SSE2 optimization.

For more information, see:

- <http://www.intel.com/support/processors/sb/CS-030123.htm?wapkw=sse2>
- <http://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni/?wapkw=aes-ni>

For OpenSSL with ARM there are two possible optimization levels:

1. Without NEON
2. With NEON (ARM7 only)

For more information, see <http://www.arm.com/products/processors/technologies/neon.php>



## Appendix B Controlled Distribution File Fingerprint

The *OpenSSL FIPS Object Module v2.0.10* consists of the FIPS Object Module (the *fipscanister.o* or *fipscanister.lib* contiguous unit of binary object code) generated from the specific source files.

For all NIST defined curves (listed in Table 2 with the EC column marked "BKP") the source files are in the specific special OpenSSL distribution *openssl-fips-2.0.10.tar.gz* with HMAC-SHA-1 digest of

af8bda4bb9739e35b4ef00a9bc40d21a6a97a780

located at <http://www.openssl.org/source/openssl-fips-2.0.10.tar.gz>.

The `openssl` command from a version of OpenSSL that incorporates a previously validated version of the module may be used:

```
openssl sha1 -hmac etaonrishdlcupfm openssl-fips-2.0.10.tar.gz
```

For NIST prime curves only (listed in Table 2 with the EC column marked "P") the source files are in the specific special OpenSSL distribution *openssl-fips-ecp-2.0.10.tar.gz* with HMAC-SHA-1 digest of

02cc9ddffffb2e917d1cdc9ebc97a9731c40f6394

located at <http://www.openssl.org/source/openssl-fips-ecp-2.0.10.tar.gz>. Note this is from the previous revision of the FIPS Object Module as no modifications relevant to NIST prime curves only were introduced in revision 2.0.10.

The set of files specified in this tar file 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.

The functionality of all earlier revisions of the FIPS Object Module are subsumed by this latest revision, so there is no reason to use older revisions for any new deployments. However, older revisions remain valid. The source distribution files and corresponding HMAC-SHA-1 digests are listed below:

`openssl-fips-2.0.9.tar.gz`

OpenSSL FIPS 140-2 Security Policy

URL: <http://www.openssl.org/source/openssl-fips-2.0.9.tar.gz>

Digest: 54552e9a3ed8d1561341e8945fcdec55af961322

openssl-fips-ecp-2.0.9.tar.gz

URL: <http://www.openssl.org/source/openssl-fips-ecp-2.0.9.tar.gz>

Digest: 91d267688713c920f85bc5e69c8b5d34e1112672

openssl-fips-2.0.8.tar.gz

URL: <http://www.openssl.org/source/old/fips/openssl-fips-2.0.8.tar.gz>

Digest: 7f486fbb598f3247ab9db10c1308f1c19f384671

openssl-fips-ecp-2.0.8.tar.gz

URL: <http://www.openssl.org/source/old/fips/openssl-fips-ecp-2.0.8.tar.gz>

Digest: 7a5f40ef8cebe959372d16e26391fcf23689209b

openssl-fips-2.0.7.tar.gz

URL: <http://www.openssl.org/source/old/fips/openssl-fips-2.0.7.tar.gz>

Digest: 295064925a6d95271e2fa2920181ec060f95c7ab

openssl-fips-ecp-2.0.7.tar.gz

URL: <http://www.openssl.org/source/old/fips/openssl-fips-ecp-2.0.7.tar.gz>

Digest: dddfdc78c7e827c61fe92bd4817a7f2c3e67153

openssl-fips-2.0.6.tar.gz

URL: <http://www.openssl.org/source/old/fips/openssl-fips-2.0.6.tar.gz>

Digest: 2b8d831df22d4dfe6169aa2a8e74c35484c26c21

openssl-fips-ecp-2.0.6.tar.gz

URL: <http://www.openssl.org/source/old/fips/openssl-fips-ecp-2.0.6.tar.gz>

Digest: 852f43cd9ae1bd2eba60e4f9f1f266d3c16c0319

openssl-fips-2.0.5.tar.gz

URL: <http://www.openssl.org/source/old/fips/openssl-fips-2.0.5.tar.gz>

Digest: 8b44f2a43d098f6858eb1ebe77b73f8f027a9c29

openssl-fips-ecp-2.0.5.tar.gz

URL: <http://www.openssl.org/source/old/fips/openssl-fips-ecp-2.0.5.tar.gz>

Digest: 148e4e127ffef1df80c0ed61bae35b07ec7b7b36

openssl-fips-2.0.4.tar.gz

URL: <http://www.openssl.org/source/old/fips/openssl-fips-2.0.4.tar.gz>

OpenSSL FIPS 140-2 Security Policy

Digest: eaa5f86dab2c5da7086aec4786bce27d3b3c1b8a  
openssl-fips-ecp-2.0.4.tar.gz  
URL: <http://www.openssl.org/source/old/fips/openssl-fips-ecp-2.0.4.tar.gz>  
Digest: 13302f75c82c8b482c9ac96828984a270a45c284

openssl-fips-2.0.3.tar.gz  
URL: <http://www.openssl.org/source/old/fips/openssl-fips-2.0.3.tar.gz>  
Digest: 5dfe03bc3f57c2862ea97823ea3111d7faf711b2

openssl-fips-ecp-2.0.3.tar.gz  
URL: <http://www.openssl.org/source/old/fips/openssl-fips-ecp-2.0.3.tar.gz>  
Digest: 9d6b21218d7d5480aa0add68e682d321e3ffbf7a7

openssl-fips-2.0.2.tar.gz  
URL: <http://www.openssl.org/source/old/fips/openssl-fips-2.0.2.tar.gz>  
Digest: e099d5096eb69c2dd8591379f38b985801188663

openssl-fips-ecp-2.0.2.tar.gz  
URL: <http://www.openssl.org/source/old/fips/openssl-fips-ecp-2.0.2.tar.gz>  
Digest: 887fa6802c253c32e6c4c83b7a091118fa8c6217

openssl-fips-2.0.1.tar.gz  
URL: <http://www.openssl.org/source/old/fips/openssl-fips-2.0.1.tar.gz>  
Digest: 1e05b021fdcd6e77c6155512bbce2d0cbc725aec

openssl-fips-ecp-2.0.1.tar.gz  
URL: <http://www.openssl.org/source/old/fips/openssl-fips-ecp-2.0.1.tar.gz>  
Digest: af82c8ebb9d3276be11feffd35e6b55bd0d1839f

openssl-fips-2.0.tar.gz  
URL: <http://www.openssl.org/source/old/fips/openssl-fips-2.0.tar.gz>  
Digest: 2cdd29913c6523df8ad38da11c342b80ed3f1dae

openssl-fips-ecp-2.0.tar.gz  
URL: <http://www.openssl.org/source/openssl-fips-ecp-2.0.tar.gz>  
Digest: e8d5ee306425b278bf6c8b077dae8e4a542e8215

## Appendix C Compilers

This appendix lists the specific compilers used to generate the Module for the respective Operational Environments. Note this list does not imply that use of the Module is restricted to only the listed compiler versions, only that the use of other versions has not been confirmed to produce a correct result.

#	Operational Environment	Compiler
1	Android 2.2 (HTC Desire)	gcc 4.4.0
2	Android 2.2 (Dell Streak)	gcc 4.4.0
3	Microsoft Windows 7 32 bit	Microsoft 32-bit C/C++ Optimizing Compiler Version 16.00
4	uClinux 0.9.29	gcc 4.2.1
5	Fedora 14	gcc 4.5.1
6	HP-UX 11i ( hpux-ia64-cc, 32 bit mode)	HP C/aC++ B3910B
7	HP-UX 11i ( hpux64-ia64-cc, 64 bit mode)	HP C/aC++ B3910B
8	Ubuntu 10.04	gcc 4.1.3
9	Android 3.0	gcc 4.4.0
10	Linux 2.6.27	gcc 4.2.4
11	Microsoft Windows 7 64 bit	Microsoft C/C++ Optimizing Compiler Version 16.00 for x64
12	Ubuntu 10.04 32 bit	gcc 4.1.3
13	Linux 2.6.33	gcc 4.1.0
16	Android 2.2	gcc 4.1.0
17	DSP Media Framework 1.4	TMS320C6x C/C++ Compiler v6.0.13
19	VxWorks 6.8	gcc 4.1.2
20	Linux 2.6	gcc 4.3.2
21	Linux 2.6	gcc 4.3.2
22	Linux 2.6.32	gcc 4.3.2
23	Solaris 10 32bit	gcc 3.4.3
24	Solaris 10 64bit	gcc 3.4.3
25	Solaris 11 32bit	gcc 4.5.2

OpenSSL FIPS 140-2 Security Policy

#	Operational Environment	Compiler
26	Solaris 11 64bit	gcc 4.5.2
27	Solaris 11 32bit	gcc 4.5.2
28	Solaris 11 64bit	gcc 4.5.2
29	Oracle Linux 5 64bit	gcc 4.1.2
30	CascadeOS 6.1 32bit	gcc 4.4.5
31	CascadeOS 6.1 64bit	gcc 4.4.5
32	Ubuntu 10.04 32bit	gcc 4.1.3
33	Ubuntu 10.04 64bit	gcc 4.1.3
34	Oracle Linux 5	gcc 4.1.2
35	Oracle Linux 6	gcc 4.4.6
36	Oracle Linux 6	gcc 4.4.6
37	Solaris 11 32bit	Sun C 5.12
38	Solaris 11 64bit	Sun C 5.12
39	Android 4.0	gcc 4.4.3
40	Linux 2.6	gcc 4.1.0
41	Apple iOS 5.1	gcc 4.2.1
42	WinCE 6.0	Microsoft C/C++ Optimizing Compiler Version 15.00 for ARM
43	WinCE 5.0	Microsoft C/C++ Optimizing Compiler Version 13.10 for ARM
44	Android 4.0	gcc 4.4.3
45	NetBSD 5.1	gcc 4.1.3
46	NetBSD 5.1	gcc 4.1.3
47		
48		
49		
50		
51	Windows 7	Microsoft (R) C/C++ Optimizing Compiler Version 16.00 for x64

OpenSSL FIPS 140-2 Security Policy

#	Operational Environment	Compiler
52	Android 4.1	gcc 4.6
53	Android 4.1	gcc 4.6
54	Android 4.2	gcc 4.6
55	Android 4.2	gcc 4.6
56	Windows Embedded Compact 7	Microsoft C/C++ Optimizing Compiler Version 15.00.20720 for ARM
57	Windows Embedded Compact 7	Microsoft C/C++ Optimizing Compiler Version 15.00.20720 for ARM
58	Android 4.0	gcc 4.4.3
59		
60	Apple OS X 10.7	Apple LLVM version 4.2
61	Apple iOS 5.0	gcc 4.2.1
62	OpenWRT 2.6	gcc 4.6.3
63	QNX 6.4	gcc 4.3.3
64	Apple iOS 6.1	gcc 4.2.1
65	eCos 3	gcc 4.3.2
66	VMware Horizon Workspace 1.5 under vSphere	gcc 4.5.1
67	VMware Horizon Workspace 1.5 under vSphere	gcc 4.5.1
68	Ubuntu 13.04	gcc 4.7.3
69	Ubuntu 13.04	gcc 4.7.3
70	Linux 3.8	gcc 4.7.3
71	Linux 3.4 under Citrix XenServer 6.2	gcc 4.8.0
72	Linux 3.4 under Citrix XenServer 6.2	gcc 4.8.0
73	Linux 3.4 under VMware ESXi 5.1	gcc 4.8.0
74	Linux 3.4 under VMware ESXi 5.1	gcc 4.8.0
75	Linux 3.4 under Microsoft Windows 2012 Hyper-V	gcc 4.8.0
76	Linux 3.4 under Microsoft Windows 2012 Hyper-V	gcc 4.8.0
77	Apple iOS 6.0	gcc 4.2.1

OpenSSL FIPS 140-2 Security Policy

#	Operational Environment	Compiler
78	Apple iOS 6.0	gcc 4.2.1
79	PexOS 1.0 under vSphere	gcc 4.6.3
80	PexOS 1.0 under vSphere	gcc 4.6.3
81	Linux 2.6	gcc 4.4.1
82	AcanOS 1.0	gcc 4.6.2
83	AcanOS 1.0	gcc 4.6.2
84	AcanOS 1.0	gcc 4.5.3
85	FreeBSD 8.4	gcc 4.2.1
86	FreeBSD 9.1	gcc 4.2.1
87	FreeBSD 9.1	gcc 4.2.1
88	ArbOS 5.3	gcc 4.1.2
89	ArbOS 5.3	gcc 4.1.2
90	Linux ORACLESP 2.6	gcc 4.4.5
91	Linux ORACLESP 2.6	gcc 4.4.5
92	FreeBSD 9.2	gcc 4.2.1
93	FreeBSD 9.2	gcc 4.2.1
94	FreeBSD 10.0	clang 3.3
95	FreeBSD 10.0	clang 3.3
96	FreeBSD 8.4	gcc 4.2.1
97	VMware Horizon Workspace 2.1 x86 under vSphere	gcc 4.5.1
98	VMware Horizon Workspace 2.1 x86 under vSphere	gcc 4.5.1
99	QNX on ARMv4	gcc 4.3.3
100	Apple iOS 7.1 64-bit on ARMv8	clang 5.1
101	Apple iOS 7.1 64-bit on ARMv8	clang 5.1
102	TS-Linux 2.4	gcc 4.3.2

OpenSSL FIPS 140-2 Security Policy

#	Operational Environment	Compiler
103	iOS 8.1 64-bit	clang-600.0.56
104	iOS 8.1 64-bit	clang-600.0.56
105	VxWorks 6.9	gcc 4.3.3
106	iOS 8.1 32-bit	clang-600.0.56
107	iOS 8.1 32-bit	clang-600.0.56
108	Android 5.0	gcc 4.9
109	Android 5.0	gcc 4.9
110	Android 5.0 64-bit	gcc 4.9
111	Android 5.0 64-bit	gcc 4.9

*Table C - Compilers*