OpenSSL-3.0.13 on vxWorks6.9.4.1

Acceptance Test Plan and Report

Prepared For Customer Review

CONFIDENTIAL

DOCUMENT NO. **JPN-MIT315868_ATP**
VERSION DATE **DECEMBER 18 2024**

Acceptance Test Plan and Report
Document No. JPN-MIT315868_ATP
Version 2.2
December 18 2024
Prepared For Mitsubishi Electric Corporation
Project Number JPN-MIT315868
Project Name OpenSSL-3.0.13 on vxWorks6.9.4.1

Wind River Systems, Inc.
500 Wind River Way
San Diego, CA 94501
510-749-2288 phone
510-749-2006 fax
www.windriver.com

Copyright

Unless otherwise agreed in writing, all copyright and intellectual property rights embodied in this document are and shall remain the property of Wind River Systems, Inc. This document is provided solely for the purposes of evaluating the work proposed and no other rights whatsoever to use the information herein are granted. The contents of this document may not be disclosed to any third party without the prior written consent of Wind River Systems, Inc.

Trademarks

Wind River, the Wind River logo, Tornado, and VxWorks are registered trademarks of Wind River Systems, Inc. Any third party trademarks referenced are the property of their respective owners. For further information regarding Wind River trademarks, please see http://www.windriver.com/corporate/html/trademark.html.

REVISION HISTORY			
Date	**Version**	**By**	**Description of Change**
2024-07-31	0.01	Liang, Shan	Initial Version
2024-08-01	1.00	Liang, Shan	Alpha Release
2024-08-30	2.00	Liang, Shan	Formal Release
2024-10-18	2.10	Liang, Shan	Updated release to fix test cases of 8.1.26, 8.1.27, 8.1.28, 8.1.29
2024-12-16	2.20	Liang, Shan	Updated section 8.2.1, Updated section 9 to reflect the latest test result.

Table of Contents

1 Applicable Documents

The following documents are referenced within:

No.	Document	Version	Notes
1.	OpenSSL page	N/A	https://openssl-library.org/

2 Glossary of Terms

For this document, the following terms and abbreviations apply:

Term	Definition
AES	Advanced Encryption Standard
ASN	Abstract Syntax Notation
ATP	Acceptance Test Procedure
CAST	Carlisle Adams and Stafford Tavares
CBC	Cipher Block Chain
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DUT	Device Under Test
EVP	ENveloPe
HMAC	keyed-Hash Message Authentication Code
IDEA	International Data Encryption Algorithm
IKE	Internet Key Exchange
MD	Message Digest
RAND	Random
RC	Ron's Code or Rivest Cipher
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SOW	Statement of Work
SSH	Secure SHell
SSL	Secure Sockets Layer

3 Introduction

3.1 Purpose and Scope

The purpose of this document is to define the acceptance test plan and procedures for the porting of OpenSSL3.0.13 to VxWorks 6.9.4.1(PNE). The purpose of acceptance testing is to demonstrate that the delivery meets the requirements specified in the SOW.

3.2 Overview

Acceptance testing includes three phases:

1. Developing an acceptance test plan (this document)
2. Executing the acceptance test plan
3. Achieving acceptance based on the test results

Section 4 provides the overview of acceptance test plan.

Section 5 of this document identifies test resources, test environment, and any required test software.

Section 6 of this document identifies test configurations and installation procedures.

Section 7 of this document identifies build instructions.

Section 8 of this document specifies the tests that will be performed. Each test will identify which requirements are being tested, specify any preconditions, and expected results.

3.3 Testing Criteria Definition

3.3.1 Entrance Criteria

The following entrance criteria must be completed prior to starting acceptance testing:

- All software development must be complete.
- All software must be under configuration control.
- All resources (human, hardware, or software) must be assigned and in place.

3.3.2 Exit Criteria

The following exit criteria must be accomplished to complete acceptance testing:

- All acceptance tests have been conducted with a pass rate of 100%. (A lower pass rate may be acceptable by mutual agreement.)
- The test report has been written, reviewed, and accepted.

4 Test Plan

Updating the OpenSSL3.0.13 in VxWorks6.9.4.1(PNE) involves changes to two components – ipcrypto and ipssl2.

4.1 Test Plan

The ipcrypto component contains all the cryptography related code. All the available test cases of openssl3.0.13 are ported to vxWorks6.9.4.1(PNE).

A series of applicable test cases will be verified on target. The following OpenSSL tests (testname) are inclusive:

1. Stack Tests (test_stack)
2. Obj Provider Tests (test_upcalls)
3. PKEY method Tests (test_pkey_meth)
4. Internal Tests (test_internal_ctype)
5. Internal Tests (test_internal_asn1_dsa)
6. Internal Tests (test_internal_exts)
7. Internal Tests (test_internal_chacha)
8. Internal Tests (test_internal_sm3)
9. Internal Tests (test_internal_sm4)
10. Internal Tests (test_internal_ssl_cert_table)
11. HASH Tests (test_lhash)
12. Sparse Array Tests (test_sparse_array)
13. Big Number Tests (test_test)
14. Asn Tests (test_asn1_string_table)
15. Asn Tests (test_cmp_asn)
16. Asn Tests (test_asn1_time)
17. Err String Tests (test_errstr)
18. PKISI Tests (test_cmp_status)
19. Memleak Tests (test_bio_memleak)
20. Constant Time Tests (test_constant_time)
21. Pbelu Tests (test_pbelu)
22. AES Tests (test_ige)
23. x509 Tests (test_v3name)
24. Blowfish Tests (test_bf)
25. CAST Tests (test_cast)
26. EVP Tests (test_evp)
27. HMAC Tests (test_hmac)
28. RAND Tests (test_rand)
29. Whirlpool Hashing Tests (test_wpacket)
30. SSL Test (test_ssl_new)

5 Test Resources

This ATP will be executed at Wind River facilities.

5.1 Wind River Acceptance Phase

5.1.1 Test Resources

One Wind River engineer shall be sufficient to perform the test.

5.1.2 Test Environment

VxWorks6.9.4.1(PNE) will be installed on a Windows XP host. Figure 1 provides the expected Wind River test environment.

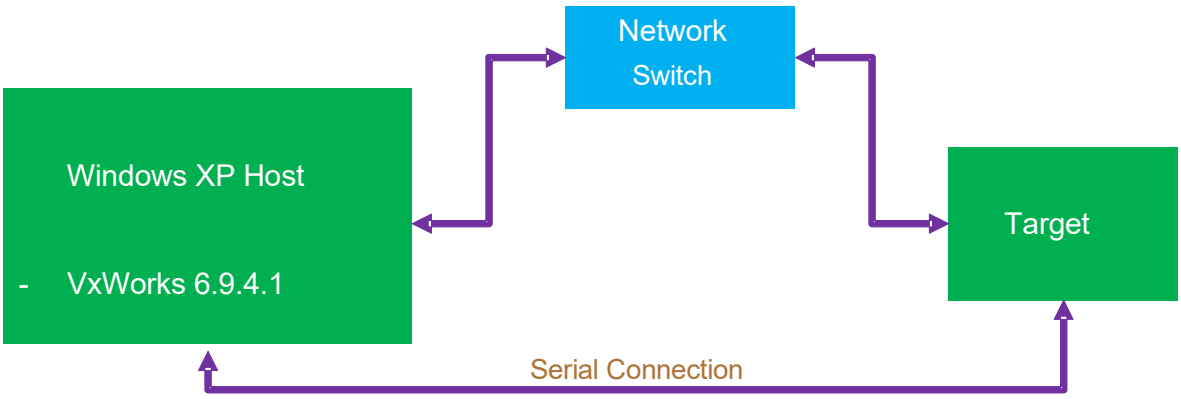

Figure 1. Wind River Test Environment

5.2 Acceptance Phase

5.2.1 Test Resources

One Wind River engineer shall be sufficient to perform the testing.

5.2.2 Test Environment

The appropriate target system will be used to verify the OpenSSL3.0.13 port for the specific version of VxWorks6.9.4.1(PNE).

6 Configuration and Installation

6.1 Installation Procedure

This section will contain the steps necessary to take a VxWorks 6.9.4.1(PNE) tree and install OpenSSL.

Install the following VxWorks DVD on a Windows XP host:

- DVD-R147826.1-1-01: VxWorks 6.9 and VxWorks Edition 6.9 Platforms(media)
- DVD-R158451.1-1-19: Wind River Workbench 3.3.4(media)
- DVD-R158451.1-1-24: Wind River Workbench 3.3.5(media)
- DVD-R158451.1-1-25: Wind River Workbench 3.3.5.1(media)
- DVD-R147826.1-19-00: VxWorks 6.9.4 and VxWorks Edition 6.9.4 Platforms(media)
- DVD-R147826.1-20-00: VxWorks 6.9.4.1 and VxWorks Edition 6.9.4.1 Platforms(media)
- DVD-R158451.1-1-28: Wind River Workbench 3.3.5.2(media)

6.2 Build Configuration Set-up

6.2.1 Enable components for test

1. Create a VSB project in Workbench based on CPU type or board support package.
2. Enable components “COMPONENT_IPSSL” and “COMPONENT_IPCRYPTO” in the “Source Build Configuration” view.

6.2.2 Install the openssl3.0.13 Package

1. Backup the $(WIND_HOME)/ components\ip_net2-6.9\ipcrypto and $(WIND_HOME)/ components\ip_net2-6.9\ipssl2 directory in your system.
2. Backup the ssl and security related initialization and function call in your application.
3. Replace the related files with files from the openssl3.0.13 package.

4. Copy the new source code and makefile files to local host from the openssl3.0.13 package.

6.2.3 Build openssl library

1. Build the VSB project in workbench to generate openssl3.0.13 library.
2. Check that the corresponding library files are updated and ready for VIP build.

7 Build VxWorks

After Openssl library built, you can create VIP project in workbench and build the VxWorks image.

8 Test Procedures

The following table summarizes the categories of tests to be performed,

Test	Description
Cryptography tests	Tests of openssl3.0.13 crypto algorithms
SSL Tests	Test SSL

8.1 Cryptography Tests

These tests are run from the VxWorks command shell.

8.1.1 Stack Tests (test_stack)

Test Case Name	Expected Test Result	Expected Output
test_int_stack	PASS	-> test_stack PASS test_int_stack. PASS test_uchar_stack. PASS test_SS_stack. PASS test_SU_stack. value = 1 = 0x1 ->
test_uchar_stack	PASS	
test_SS_stack	PASS	
test_SU_stack	PASS	

8.1.2 Obj Provider Tests (test_upcalls)

Test Case Name	Expected Test Result	Expected Output
obj_create_test	PASS	-> test_upcalls PASS obj_create_test value = 1 = 0x1

		->

8.1.3 PKEY method Tests (test_pkey_meth)

Test Case Name	Expected Test Result	Expected Output
test_asn1_meths	PASS	-> test_pkey_meth PASS test_asn1_meths PASS test_pkey_meths value = 1 = 0x1 ->
test_pkey_meths	PASS	

8.1.4 Internal Tests(test_internal_ctype)

Test Case Name	Expected Test Result	Expected Output
test_ctype_chars	PASS	-> test_internal_ctype PASS test_ctype_chars PASS test_ctype_toupper PASS test_ctype_tolower PASS test_ctype_eof value = 1 = 0x1 ->
test_ctype_toupper	PASS	
test_ctype_tolower	PASS	
test_ctype_eof	PASS	

8.1.5 Internal Tests(test_internal_asn1_dsa)

Test Case Name	Expected Test Result	Expected Output
test_decode	PASS	-> test_internal_asn1_dsa PASS test_decode value = 1 = 0x1

		->

8.1.6 Internal Tests(test_internal_exts)

Test Case Name	Expected Test Result	Expected Output
test_extension_list	PASS	-> test_internal_exts PASS test_extension_list value = 1 = 0x1 ->

8.1.7 Internal Tests(test_internal_chacha)

Test Case Name	Expected Test Result	Expected Output
test_cha_cha_internal	PASS	-> test_internal_chacha PASS test_cha_cha_internal value = 1 = 0x1 ->

8.1.8 test_internal_sm3

Test Case Name	Expected Test Result	Expected Output
test_sm3	PASS	-> test_internal_sm3 PASS test_sm3 value = 1 = 0x1 ->

8.1.9 test_internal_sm4

Test Case Name	Expected Test Result	Expected Output
test_sm4_ecb	PASS	-> test_internal_sm4

		PASS test_sm4_ecb value = 1 = 0x1 ->

8.1.10 test_internal_ssl_cert_table

Test Case Name	Expected Test Result	Expected Output
test_ssl_cert_table	PASS	-> test_internal_ssl_cert_table PASS test_ssl_cert_table value = 1 = 0x1 ->

8.1.11 HASH Tests (test_lhash)

Test Case Name	Expected Test Result	Expected Output
test_int_lhash	PASS	-> test_lhash PASS test_int_lhash. .....test_info: file=-6.9/ipcrypto/src/lhash_test.c, line=216. .....TEST_note: hash full node usage:. .....test_info: file=-6.9/ipcrypto/src/lhash_test.c, line=236. .....TEST_note: hash empty node usage:. PASS test_stress. value = 1 = 0x1
test_stress	PASS	

8.1.12 Sparse Array Tests (test_sparse_array)

Test Case Name	Expected Test Result	Expected Output
test_sparse_array_def	PASS	-> test_sparse_array PASS test_sparse_array_def PASS test_sparse_array_num PASS test_sparse_array_doall value = 1 = 0x1 ->
test_sparse_array_num	PASS	
test_sparse_array_doall	PASS	

8.1.13 Big Number Tests (test_test)

Test Case Name	Expected Test Result	Expected Output
test_int	PASS	-> test_test .....test_fail_message: file=2-6.9/ipcrypto/src/test_test.c, line=37. .....test_fail_message: file=2-6.9/ipcrypto/src/test_test.c, line=39. .....test_fail_message: file=2-6.9/ipcrypto/src/test_test.c, line=41. .....test_fail_message: file=2-6.9/ipcrypto/src/test_test.c, line=44. .....test_fail_message: file=2-6.9/ipcrypto/src/test_test.c, line=46. .....test_fail_message: file=2-6.9/ipcrypto/src/test_test.c,
test_uint	PASS	
test_char	PASS	
test_uchar	PASS	
test_long	PASS	
test_ulong	PASS	
test_size_t	PASS	
test_time_t	PASS	
test_pointer	PASS	
test_bool	PASS	
test_string	PASS	
test_memory	PASS	

test_memory_overflow	PASS	line=49. PASS test_int. .....test_fail_message: file=2-6.9/ipcrypto/src/test_test.c, line=60. .....test_fail_message: file=2-6.9/ipcrypto/src/test_test.c, line=62. < Omit other output> PASS test_uint < Omit other output> PASS test_char < Omit other output> PASS test_uchar < Omit other output> PASS test_long < Omit other output> PASS test_ulong < Omit other output> PASS test_size_t < Omit other output> PASS test_time_t < Omit other output> PASS test_pointer
test_bignum	PASS	
test_long_bignum	PASS	
test_long_output	PASS	
test_messages	PASS	
test_single_eval	PASS	
test_output	PASS	
test_bn_output	PASS	
test_skip_one	PASS	
test_skip_null	PASS	
test_skip_many	PASS	

		< Omit other output> PASS test_bool < Omit other output> PASS test_string < Omit other output> PASS test_memory < Omit other output> PASS test_memory_overflow < Omit other output> PASS test_bignum < Omit other output> PASS test_long_bignum < Omit other output> PASS test_long_output < Omit other output> PASS test_messages. PASS test_single_eval. PASS test_output. PASS test_bn_output. .....test_skip: file=2-6.9/ipcrypto/src/test_test.c, line=543.

		PASS test_skip_one. .....test_skip: file=2-6.9/ipcrypto/src/test_test.c, line=557. PASS test_skip_null. .....test_skip: file=2-6.9/ipcrypto/src/test_test.c, line=548. PASS test_skip_many. value = 1 = 0x1

8.1.14 Asn Tests (test_asn1_string_table)

Test Case Name	Expected Test Result	Expected Output
test_string_tbl	PASS	-> test_asn1_string_table PASS test_string_tbl value = 1 = 0x1 ->

8.1.15 Asn Tests (test_cmp_asn)

Test Case Name	Expected Test Result	Expected Output
test_cmp_asn1_get_int	PASS	-> test_cmp_asn
test_ASN1_OCTET_STRING_set	PASS	PASS test_cmp_asn1_get_int
test_ASN1_OCTET_STRING_set_tgt_is_src	PASS	PASS test_ASN1_OCTET_STRING_set PASS

		test_ASN1_OCTET_STRING_set_tgt_is_src value = 1 = 0x1 ->

8.1.16 Asn Tests (test_asn1_time)

Test Case Name	Expected Test Result	Expected Output
test_table_pos	PASS	-> test_asn1_time PASS test_table_pos. .....test_info: file=/ipcrypto/src/asn1_time_test.c, line=406. PASS test_table_neg. PASS test_table_compare. PASS test_time_dup. value = 1 = 0x1
test_table_neg	PASS	
test_table_compare	PASS	
test_time_dup	PASS	

8.1.17 Err String Tests (test_errstr)

Test Case Name	Expected Test Result	Expected Output
preserves_system_error	PASS	-> test_errstr PASS preserves_system_error value = 1 = 0x1 ->

8.1.18 PKISI Tests (test_cmp_status)

Test Case Name	Expected Test Result	Expected Output
test_PKISI	PASS	-> test_cmp_status

		PASS test_PKISI value = 1 = 0x1 ->

8.1.19 Memleak Tests (test_bio_memleak)

Test Case Name	Expected Test Result	Expected Output
test_bio_memleak_def	PASS	-> test_bio_memleak PASS test_bio_memleak_def PASS test_bio_get_mem PASS test_bio_new_mem_buf PASS test_bio_rdonly_mem_buf PASS test_bio_rdwr_rdonly PASS test_bio_nonclear_rst PASS test_bio_i2d_ASN1_mime PASS value = 1 = 0x1 ->
test_bio_get_mem	PASS	
test_bio_new_mem_buf	PASS	
test_bio_rdonly_mem_buf	PASS	
test_bio_rdwr_rdonly	PASS	
test_bio_nonclear_rst	PASS	
test_bio_i2d_ASN1_mime	PASS	

8.1.20 Constant Time Tests (test_constant_time)

Test Case Name	Expected Test Result	Expected Output
test_sizeofs	PASS	-> test_constant_time PASS test_sizeofs PASS test_is_zero PASS test_is_zero_8 PASS test_is_zero_32
test_is_zero	PASS	
test_is_zero_8	PASS	
test_is_zero_32	PASS	

test_is_zero_s	PASS	PASS test_is_zero_32 PASS test_is_zero_s PASS test_binops PASS test_binops_8 PASS test_binops_s PASS test_signed PASS test_8values PASS test_32values PASS test_64values value = 1 = 0x1 ->
test_binops	PASS	
test_binops_8	PASS	
test_binops_s	PASS	
test_signed	PASS	
test_8values	PASS	
test_32values	PASS	
test_64values	PASS	

8.1.21 Pbelu Tests (test_pbelu)

Test Case Name	Expected Test Result	Expected Output
test_pbelu_def	PASS	->test_pbelu PASS test_pbelu_def value = 1 = 0x1 ->

8.1.22 AES Tests (test_ige)

Test Case Name	Expected Test Result	Expected Output
test_ige_enc_dec	PASS	-> test_ige PASS test_ige_enc_dec
test_ige_enc_chaining	PASS	

test_ige_dec_chaining	PASS	PASS test_ige_enc_chaining PASS test_ige_dec_chaining PASS test_ige_garble_forwards PASS test_bi_ige_enc_dec PASS test_bi_ige_garble1 PASS test_bi_ige_garble2 PASS test_bi_ige_garble3 PASS test_ige_vectors PASS test_bi_ige_vectors value = 1 = 0x1 ->
test_ige_garble_forwards	PASS	
test_bi_ige_enc_dec	PASS	
test_bi_ige_garble1	PASS	
test_bi_ige_garble2	PASS	
test_bi_ige_garble3	PASS	
test_ige_vectors	PASS	
test_bi_ige_vectors	PASS	

8.1.23 x509 Tests (test_v3name)

Test Case Name	Expected Test Result	Expected Output
call_run_cert	PASS	-> test_v3name .....test_info: file=-6.9/ipcrypto/src/v3nametest.c, line=370. PASS call_run_cert. PASS test_GENERAL_NAME_cmp. value = 1 = 0x1
test_GENERAL_NAME_cmp	PASS	

8.1.24 Blowfish Tests (test_bf)

Test Case Name	Expected Test Result	Expected Output

test_bf_ecb_raw	PASS	-> test_bf PASS test_bf_ecb_raw PASS test_bf_ecb PASS test_bf_set_key PASS test_bf_cbc PASS test_bf_cfb64 PASS test_bf_ofb64 value = 1 = 0x1 ->
test_bf_ecb	PASS	
test_bf_set_key	PASS	
test_bf_cbc	PASS	
test_bf_cfb64	PASS	
test_bf_ofb64	PASS	

8.1.25 CAST Tests (test_cast)

Test Case Name	Expected Test Result	Expected Output
cast_test_vector	PASS	-> test_cast PASS cast_test_vector PASS cast_test_iterations value = 1 = 0x1 ->
cast_test_iterations	PASS	

8.1.26 EVP Tests (test_evp)

Test Case Name	Expected Test Result	Expected Output
run_file_tests	PASS	-> test_evp PASS run_file_tests value = 1 = 0x1

		->

8.1.27 HMAC Tests (test_hmac)

Test Case Name	Expected Test Result	Expected Output
test_hmac_md5	PASS	-> test_hmac PASS test_hmac_md5 PASS test_hmac_single_shot PASS test_hmac_bad PASS test_hmac_run PASS test_hmac_copy PASS test_hmac_copy_uninited value = 1 = 0x1 ->
test_hmac_single_shot	PASS	
test_hmac_bad	PASS	
test_hmac_run	PASS	
test_hmac_copy	PASS	
test_hmac_copy_uninited	PASS	

8.1.28 RAND Tests (test_rand)

Test Case Name	Expected Test Result	Expected Output
test_rand_def	PASS	-> test_rand PASS test_rand_def value = 1 = 0x1 ->

8.1.29 Whirlpool Hashing Tests (test_wpacket)

Test Case Name	Expected Test Result	Expected Output
test_WPACKET_init	PASS	-> test_wpacket

test_WPACKET_set_max_size	PASS	PASS test_WPACKET_init PASS test_WPACKET_set_max_size PASS test_WPACKET_start_sub_packet PASS test_WPACKET_set_flags PASS test_WPACKET_allocate_bytes PASS test_WPACKET_memcpy PASS test_WPACKET_init_der value = 1 = 0x1 ->
test_WPACKET_start_sub_packet	PASS	
test_WPACKET_set_flags	PASS	
test_WPACKET_allocate_bytes	PASS	
test_WPACKET_memcpy	PASS	
test_WPACKET_init_der	PASS	

8.2 SSL Test

These tests are run from the VxWorks command shell.

8.2.1 SSL Tests (test_ssl_new)

Test Case Name	Expected Test Result	Expected Output
test_handshake	PASS	-> a = calloc(4,2) New symbol "a" added to kernel symbol table. a = 0xbf23d0: value = 12590488 = 0xc01d98 -> a[0] = 0x56D29D75 0xc01d98: value = 1456643445 = 0x56d29d75 = 'u'

		-> clock_settime 0,a value = 0 = 0x0 -> test_ssl_new PASS test_handshake. value = 1 = 0x1 ->

9 Test Results

Table Results

TEST	RESULTS	COMMENTS / EVIDENCE
8.1.1 Stack Tests (test_stack)	PASS	
8.1.2 Obj Provider Tests (test_upcalls)	PASS	
8.1.3 PKEY method Tests (test_pkey_meth)	PASS	
8.1.4 Internal Tests(test_internal_ctype)	PASS	
8.1.5 Internal Tests(test_internal_asn1_dsa)	PASS	
8.1.6 Internal Tests(test_internal_exts)	PASS	
8.1.7 Internal Tests(test_internal_chacha)	PASS	
8.1.8 test_internal_sm3	PASS	
8.1.9 test_internal_sm4	PASS	
8.1.10 test_internal_ssl_cert_table	PASS	
8.1.11 HASH Tests (test_lhash)	PASS	Note that in this test, test info and note messages are correct test information.
8.1.12 Sparse Array Tests (test_sparse_array)	PASS	
8.1.13 Big Number Tests (test_test)	PASS	Note that in this test, error info messages are functional acceptable. The reason is that the error info message will show when some unexpected cases are tested. The error info message does not indicate the test case fail.

TEST	RESULTS	COMMENTS / EVIDENCE
8.1.14 Asn Tests (test_asn1_string_table)	PASS	
8.1.15 Asn Tests (test_cmp_asn)	PASS	
8.1.16 Asn Tests (test_asn1_time)	PASS	Note that in this test, test info messages are correct test information.
8.1.17 Err String Tests (test_errstr)	PASS	
8.1.18 PKISI Tests (test_cmp_status)	PASS	
8.1.19 Memleak Tests (test_bio_memleak)	PASS	
8.1.20 Constant Time Tests (test_constant_time)	PASS	
8.1.21 Pbelu Tests (test_pbelu)	PASS	
8.1.22 AES Tests (test_ige)	PASS	
8.1.23 x509 Tests (test_v3name)	PASS	Note that in this test, test info messages are correct test information.
8.1.24 Blowfish Tests (test_bf)	PASS	
8.1.25 CAST Tests (test_cast)	PASS	
8.1.26 EVP Tests (test_evp)	PASS	
8.1.27 HMAC Tests (test_hmac)	PASS	
8.1.28 RAND Tests (test_rand)	PASS	
8.1.29 Whirlpool Hashing Tests (test_wpacket)	PASS	
8.2.1 SSL Tests (test_ssl_new)	PASS	