

7.3.8 WINNF.FT.C.HBT.10

#	Test Execution Steps	Results	
1	Ensure the following conditions are met for test entry: - UUT has registered successfully with SAS Test Harness - UUT has a valid single grant as follows: - valid cbsdId = C - valid grantId = G - grant is for frequency range F, power P - grantExpireTime = UTC time greater than duration of the test - UUT is in AUTHORIZED state and is transmitting within the grant bandwidth F on RF interface	--	—
2	UUT sends a Heartbeat Request message. Verify Heartbeat Request message is sent within latest specified heartbeatInterval, and is formatted correctly, including: - cbsdId = C - grantId = G - operationState = "AUTHORIZED"	■ Pass	□ Fail
3	SAS Test Harness sends a Heartbeat Response message, including the following parameters: - cbsdId = C - grantId = G - transmitExpireTime = T = current UTC time + 200 seconds - responseCode = 0	--	—
4	After completion of step 3, SAS Test Harness shall not allow any further grants to the UUT.	--	—
5	Monitor the RF output of the UUT. Verify: UUT shall stop all transmission on RF interface within (transmitExpireTime + 60 seconds), using the transmitExpireTime sent in Step 3.	■ Pass	□ Fail

7.3.9 WINNF.FT.C.HBT.11

#	Test Execution Steps	Results	
1	Ensure the following conditions are met for test entry: - UUT has registered successfully with SAS Test Harness - UUT has a valid single grant as follows: - valid cbsdId = C - valid grantId = G - grant is for frequency range F, power P - UUT is in AUTHORIZED state and is transmitting within the grant bandwidth F on RF interface. - Grant has the following parameters at the start of the test: - grantExpireTime = UTC time equal to time at start of test + 300 seconds = Tgrant_expire - transmitExpireTime = UTC time equal to time at start of test + 200 seconds - heartbeatInterval = 60 seconds	--	--
2	UUT sends a Heartbeat Request message. If Heartbeat Request message contains grantRenew = TRUE, go to Step 6, else go to Step 3.	--	--
3	Verify Heartbeat Request message is sent within the latest specified heartbeatInterval, and is formatted correctly, including: - cbsdId = C - grantId = G - operationState = "AUTHORIZED"	☒ Pass	☐ Fail
4	SAS Test Harness sends a Heartbeat Response message, with the following parameters: - cbsdId = C - grantId = G - transmitExpireTime = current UTC + 200 seconds - grantExpireTime = same as Step 1 - responseCode = 0	--	--
5	Go to Step 2	--	--
6	Verify Heartbeat Request message is sent within the latest specified heartbeatInterval, and is formatted correctly, including: - cbsdId = C - grantId = G - operationState = "AUTHORIZED" - grantRenew = TRUE	☒ Pass	☐ Fail
7	SAS Test Harness sends a Heartbeat Response message, with the following parameters: - cbsdId = C - grantId = G - grantExpireTime = UTC time set far in the future - transmitExpireTime = current UTC time + 200 seconds - responseCode = 0	--	--
8	Continue to respond to any subsequent Heartbeat Request from CBSD with Heartbeat Response with the following parameters: - cbsdId = C - grantId = G - transmitExpireTime = same as Step 7 - responseCode = 0	--	--
9	Monitor RF transmission of UUT from start of test until Tgrant_expire + 60 seconds and ensure UUT continues to transmit throughout the time period.	☒ Pass	☐ Fail



7.4 CBSD Measurement Report

7.4.1 WINNF.FT.C.MES.1

#	Test Execution Steps	Results	
1	Ensure the following conditions are met for test entry: UUT has successfully completed SAS Discovery and Authentication with SAS Test Harness	—	--
2	UUT sends a Registration Request message. - userId is present and correct - fcid is present and correct - cbsdSerialNumber is present and correct - measCapability = "RECEIVED_POWER_WITHOUT_GRANT"	■ Pass	□ Fail
3	SAS Test Harness sends a Grant Response message, with the following parameters: - cbsdId = C = valid cbsdId for this UUT - measReportConfig= "RECEIVED_POWER_WITHOUT_GRANT" - responseCode = 0	—	--
4	UUT sends a message. - If message is type Spectrum Inquiry Request, go to step 5, or - If message is type Grant Request, go to step 7	—	--
5	UUT sends message type Spectrum Inquiry Request. - cbsdId = C - measReport is present, and is a properly formatted rcvdPowerMeasReport.	■ Pass	□ Fail
6	SAS Test Harness sends a Heartbeat Response message, containing all required parameters properly formatted, and specifically: - cbsdId = C - availableChannel is an array of availableChannel /objects - responseCode = 0	—	--
7	UUT sends message type Grant Request message. Verify message contains all required parameters properly formatted, and specifically: - cbsdId = C - measReport is present, and is a properly formatted rcvdPowerMeasReport.	■ Pass	□ Fail

7.4.2 WINNF.FT.C.MES.3

#	Test Execution Steps	Results	
1	Ensure the following conditions are met for test entry: - UUT has successfully completed SAS Discovery and Authentication with SAS Test Harness - UUT has successfully registered with SAS Test Harness, with cbsdId=C and measCapability = "RECEIVED_POWER_WITH_GRANT"	—	--

2	UUT sends a Grant Request message. Verify Grant Request message contains all required parameters properly formatted, and specifically: ● cbsdId = C ● operationParam is present and format is valid	■ Pass	□ Fail
3	SAS Test Harness sends a Grant Response message, with the following parameters: ● cbsdId = C ● grantId = G = valid grant ID ● grantExpireTime = UTC time in the future ● heartbeatInterval = 60 seconds ● measReportConfig= "RECEIVED_POWER_WITH_GRANT" ● operationParam is set to valid operating parameters ● channelType = "GAA" ● responseCode = 0	—	--
4	UUT sends a Heartbeat Request message. Verify message contains all required parameters properly formatted, and specifically: ● cbsdId = C ● grantId = G ● operationState = "GRANTED"	■ Pass	□ Fail
5	If Heartbeat Request message (step 4) contains measReport object, then: ● verify measReport is properly formatted as object rcvdPowerMeasReport ● end test, with PASS result else, if Heartbeat Request message (step 4) does not contain measReport object, then: ● If number of Heartbeat Requests sent by UUT after Step 3 is =5, then stop test with result of FAIL	■ Pass	□ Fail
6	SAS Test Harness sends a Heartbeat Response message, containing all required parameters properly formatted, and specifically: ● cbsdId = C ● grantId = G ● transmitExpireTime = current UTC time + 200 seconds ● responseCode = 0 Go to Step 4, above	—	--

7.4.3 WINNF.FT.C.MES.4

#	Test Execution Steps	Results	
1	Ensure the following conditions are met for test entry: - UUT has successfully completed SAS Discovery and Authentication with SAS Test Harness - UUT has successfully registered with SAS Test Harness, with cbsdId=C and measCapability = "RECEIVED_POWER_WITH_GRANT" - UUT has received a valid grant with grantId = G - UUT is in Grant State AUTHORIZED and is actively transmitting within the bounds of its grant. - Grant has heartbeatInterval = 60 seconds	—	--
2	UUT sends a Heartbeat Request message. Verify Heartbeat Request message contains all required parameters properly formatted, and specifically: - cbsdId = C - grantId = G - operationState = "AUTHORIZED"	☒ Pass	☐ Fail
3	SAS Test Harness sends a Heartbeat Response message, containing all required parameters properly formatted, and specifically: - cbsdId = C - grantId = G - measReportConfig= "RECEIVED_POWER_WITH_GRANT" - responseCode = 0	—	--
4	UUT sends a Heartbeat Request message. Verify message contains all required parameters properly formatted, and specifically: - cbsdId = C - grantId = G - operationState = "AUTHORIZED"	☒ Pass	☐ Fail
5	If Heartbeat Request message (step 4) contains measReport object, then: - verify measReport is properly formatted as object - rcvdPowerMeasReport - end test, with PASS result else, if Heartbeat Request message (step 4) does not contain measReport object, then: - If number of Heartbeat Requests sent by UUT after Step 3 is = 5, then stop test with result of FAIL	☒ Pass	☐ Fail
6	SAS Test Harness sends a Heartbeat Response message, containing all required parameters properly formatted, and specifically: - cbsdId = C - grantId = G - responseCode = 0 Go to Step 4, above	—	--

7.5 CBSD Relinquishment Process

7.5.1 WINNF.FT.C.RLQ.1

#	Test Execution Steps	Results	
1	Ensure the following conditions are met for test entry: UUT has successfully completed SAS Discovery and Authentication with SAS	—	--

	Test Harness - UUT has successfully registered with SAS Test Harness, with cbsdId=C - UUT has received a valid grant with grantId = G - UUT is in Grant State AUTHORIZED and is actively transmitting within the bounds of its grant. Invoke trigger to relinquish UUT Grant from the SAS Test Harness		
2	UUT sends a Relinquishment Request message. Verify message contains all required parameters properly formatted, and specifically: - cbsdId = C - grantId = G	☒ Pass	☐ Fail
3	SAS Test Harness shall approve the request with a Relinquishment Response message with parameters: - cbsdId = C - grantId = G - responseCode = 0	—	--
4	After completion of step 3, SAS Test Harness will not provide any additional positive response (responseCode=0) to further request messages from the UUT	—	--
5	Monitor the RF output of the UUT from start of test until 60 seconds after Step 3 is complete. This is the end of the test. Verify: UUT shall stop RF transmission at any time between triggering the relinquishment and UUT sending the relinquishment request	☒ Pass	☐ Fail

7.5.2 WINNF.FT.C.RLQ.3

#	Test Execution Steps	Results	
1	Ensure the following conditions are met for test entry: ● UUT has successfully completed SAS Discovery and Authentication with SAS Test Harness ● UUT has successfully registered with SAS Test Harness, with cbsdId=C ● UUT has received a valid grant with grantId = G ● UUT is in Grant State AUTHORIZED and is actively transmitting within the bounds of its grant. Invoke trigger to relinquish UUT Grant from the SAS Test Harness	—	--
2	UUT sends a Relinquishment Request message. Verify message contains all required parameters properly formatted, and specifically: ● cbsdId = C ● grantId = G	—	--
3	SAS Test Harness shall approve the request with a Relinquishment Response message with parameters: - cbsdId = C - grantId = G ● responseCode = R	—	--
4	After completion of step 3, SAS Test Harness will not provide any additional positive response (responseCode=0) to further request messages from the UUT	—	--
5	Monitor the RF output of the UUT from start of test until 60 seconds after Step 3 is complete. This is the end of the test. Verify: ● UUT shall stop RF transmission at any time between triggering the relinquishment and UUT sending the relinquishment request	☒ Pass	☐ Fail

7.5.3 WINNF.FT.C.RLQ.5

#	Test Execution Steps	Results	
1	Ensure the following conditions are met for test entry: ● UUT has successfully completed SAS Discovery and Authentication with SAS Test Harness ● UUT has successfully registered with SAS Test Harness, with cbsdId=C ● UUT has received a valid grant with grantId = G ● UUT is in Grant State AUTHORIZED and is actively transmitting within the bounds of its grant. Invoke trigger to relinquish UUT Grant from the SAS Test Harness	—	--
2	UUT sends a Relinquishment Request message. Verify message contains all required parameters properly formatted, and specifically: ● cbsdId = C ● grantId = G	—	--
3	SAS Test Harness shall approve the request with a Relinquishment Response message with parameters: - cbsdId = C - grantId = G ● responseCode = 103	—	--
4	After completion of step 3, SAS Test Harness will not provide any additional positive response (responseCode=0) to further request messages from the UUT	—	--
5	Monitor the RF output of the UUT from start of test until 60 seconds after Step 3 is complete. This is the end of the test. Verify: ● UUT shall stop RF transmission at any time between triggering the relinquishment and UUT sending the relinquishment request	☒ Pass	☐ Fail

7.6 CBSD Deregistration Process

7.6.1 WINNF.FT.C.DRG.1

#	Test Execution Steps	Results	
1	Ensure the following conditions are met for test entry: - UUT has successfully completed SAS Discovery and Authentication with SAS Test Harness - UUT has successfully registered with SAS Test Harness, with cbsdId=C - UUT has received a valid grant with grantId = G - UUT is in Grant State AUTHORIZED and is actively transmitting within the bounds of its grant. Invoke trigger to deregister UUT from the SAS Test Harness	--	--
2	UUT sends a Relinquishment request and receives Relinquishment response with responseCode=0	--	--
3	UUT sends Deregistration Request to SAS Test Harness with cbsdId = C.	☒ Pass	☐ Fail
4	SAS Test Harness shall approve the request with a Deregistration Response message with parameters: - cbsdId = C - responseCode = 0	--	--
5	After completion of step 3, SAS Test Harness will not provide any additional positive response (responseCode=0) to further request messages from the UUT.	--	--
6	Monitor the RF output of the UUT from start of test until 60 seconds after Step 4 is complete. This is the end of the test. Verify: - UUT stopped RF transmission at any time between triggering the deregistration and either A OR B occurs: A. UUT sending a Registration Request message, as this is not mandatory B. UUT sending a Deregistration Request message	☒ Pass	☐ Fail

7.6.2 WINNF.FT.C.DRG.3

#	Test Execution Steps	Results	
1	Ensure the following conditions are met for test entry: - UUT has successfully completed SAS Discovery and Authentication with SAS Test Harness - UUT has successfully registered with SAS Test Harness, with cbsdId=C - UUT has received a valid grant with grantId = G - UUT is in Grant State AUTHORIZED and is actively transmitting within the bounds of its grant. Invoke trigger to deregister UUT from the SAS Test Harness	–	--
2	UUT sends a Relinquishment request and receives Relinquishment response with responseCode=0	–	--
3	UUT sends Deregistration Request to SAS Test Harness with cbsdId = C.	–	--
4	The SAS Test Harness sends the Deregistration Response Message to UUT with: - No cbsdId - responseCode = 103	–	--
5	After completion of step 3, SAS Test Harness will not provide any additional positive response (responseCode=0) to further request messages from the UUT.	–	--
6	Monitor the RF output of the UUT from start of test until 60 seconds after Step 4 is complete. This is the end of the test. Verify: - UUT stopped RF transmission at any time between triggering the deregistration and either A OR B occurs: A. UUT sending a Registration Request message, as this is not mandatory B. UUT sending a Deregistration Request message	☒ Pass	☐ Fail

7.6.3 WINNF.FT.C.DRG.5

#	Test Execution Steps	Results	
1	Ensure the following conditions are met for test entry: - UUT has successfully completed SAS Discovery and Authentication with SAS Test Harness - UUT has successfully registered with SAS Test Harness, with cbsdId=C - UUT has received a valid grant with grantId = G - UUT is in Grant State AUTHORIZED and is actively transmitting within the bounds of its grant. Invoke trigger to deregister UUT from the SAS Test Harness	–	–
2	UUT sends a Relinquishment request and receives Relinquishment response with responseCode=0	–	–
3	UUT sends Deregistration Request to SAS Test Harness with cbsdId = C.	–	–
4	The SAS Test Harness sends the Deregistration Response Message to UUT with: - cbsdId=C - responseCode = 103	–	–
5	After completion of step 3, SAS Test Harness will not provide any additional positive response (responseCode=0) to further request messages from the UUT.	–	–
6	Monitor the RF output of the UUT from start of test until 60 seconds after Step 4 is complete. This is the end of the test. Verify: - UUT stopped RF transmission at any time between triggering the deregistration and either A OR B occurs: C. UUT sending a Registration Request message, as this is not mandatory D. UUT sending a Deregistration Request message	■ Pass	□ Fail

7.7 CBSD Security Validation

7.7.1 WINNF.FT.C.SCS.1

#	Test Execution Steps	Results	
1	- UUT shall start CBSD-SAS communication with the security procedure - The UUT shall establish a TLS handshake with the SAS Test Harness using configured certificate. - Configure the SAS Test Harness to accept the security procedure and establish the connection	☒ Pass	☐ Fail
2	- Make sure that Mutual authentication happens between UUT and the SAS Test Harness. - Make sure that UUT uses TLS v1.2 - Make sure that cipher suites from one of the following is selected, - TLS_RSA_WITH_AES_128_GCM_SHA256 - TLS_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	☒ Pass	☐ Fail
3	A successful registration is accomplished using one of the test cases described in section 6.1.4.1, depending on CBSD capability. E. UUT sends a registration request to the SAS Test Harness and the SAS Test Harness sends a Registration Response with responseCode = 0 and cbsdId.	☒ Pass	☐ Fail
4	Monitor the RF output of the UUT from start of test until 60 seconds after Step 3 is complete. This is the end of the test. Verify: UUT shall not transmit RF	☒ Pass	☐ Fail

7.7.2 WINNF.FT.C.SCS.2

#	Test Execution Steps	Results	
1	UUT shall start CBSD-SAS communication with the security procedures	☒ Pass	☐ Fail
2	- Make sure that UUT uses TLS v1.2 for security establishment. - Make sure UUT selects the correct cipher suite. - UUT shall use CRL or OCSP to verify the validity of the server certificate. - Make sure that Mutual authentication does not happen between UUT and the SAS Test Harness.	☒ Pass	☐ Fail
3	F. UUT may retry for the security procedure which shall fail.	☒ Pass	☐ Fail
4	SAS Test-Harness shall not receive any Registration request or any application data.	☐ --	☐ --
5	Monitor the RF output of the UUT from start of test until 60 seconds after Step 3 is complete. This is the end of the test. Verify: UUT shall not transmit RF	☒ Pass	☐ Fail

7.7.3 WINNF.FT.C.SCS.3

#	Test Execution Steps	Results	
1	UUT shall start CBSD-SAS communication with the security procedures	☒ Pass	☐ Fail

2	- Make sure that UUT uses TLS v1.2 for security establishment. - Make sure UUT selects the correct cipher suite. - UUT shall use CRL or OCSP to verify the validity of the server certificate. - Make sure that Mutual authentication does not happen between UUT and the SAS Test Harness.	☒ Pass	☐ Fail
3	G. UUT may retry for the security procedure which shall fail.	☒ Pass	☐ Fail
4	SAS Test-Harness shall not receive any Registration request or any application data.	—	--
5	Monitor the RF output of the UUT from start of test until 60 seconds after Step 3 is complete. This is the end of the test. Verify: UUT shall not transmit RF	☒ Pass	☐ Fail

7.7.4 WINNF.FT.C.SCS.4

#	Test Execution Steps	Results	
1	UUT shall start CBSD-SAS communication with the security procedures	☒ Pass	☐ Fail
2	- Make sure that UUT uses TLS v1.2 for security establishment. - Make sure UUT selects the correct cipher suite. - UUT shall use CRL or OCSP to verify the validity of the server certificate - Make sure that Mutual authentication does not happen between UUT and the SAS Test Harness.	☒ Pass	☐ Fail
3	H. UUT may retry for the security procedure which shall fail.	☒ Pass	☐ Fail
4	SAS Test-Harness shall not receive any Registration request or any application data.	—	--
5	Monitor the RF output of the UUT from start of test until 60 seconds after Step 3 is complete. This is the end of the test. Verify: UUT shall not transmit RF	☒ Pass	☐ Fail

**7.7.5 WINNF.FT.C.SCS.5**

#	Test Execution Steps	Results	
1	● UUT shall start CBSD-SAS communication with the security procedures	☒ Pass	☐ Fail
2	● Make sure that UUT uses TLS v1.2 for security establishment. ● Make sure UUT selects the correct cipher suite. ● UUT shall use CRL or OCSP to verify the validity of the server certificate ● Make sure that Mutual authentication does not happen between UUT and the SAS Test Harness.	☒ Pass	☐ Fail
3	I. UUT may retry for the security procedure which shall fail.	☒ Pass	☐ Fail
4	● SAS Test-Harness shall not receive any Registration request or any application data.	—	--
5	Monitor the RF output of the UUT from start of test until 60 seconds after Step 3 is complete. This is the end of the test. Verify: ● UUT shall not transmit RF	☒ Pass	☐ Fail

7.8 CBSD RF Power Measurement

7.8.1 WINNF.PT.C.HBT.1

#	Test Execution Steps	Results	
1	Ensure the following conditions are met for test entry: - UUT has successfully completed SAS Discovery and Authentication with the SAS Test Harness - UUT has registered with the SAS, with CBSD ID = C - UUT has a single valid grant G with parameters {lowFrequency = FL, highFrequency = FH, maxEirp = Pi}, with grant in AUTHORIZED state, and grantExpireTime set to a value far past the duration of this test case Note: in order for the UUT to request a grant with the parameters {lowFrequency, highFrequency, maxEirp}, the SAS Test Harness may need to provide appropriate guidance in the availableChannel object of the spectrumInquiry response message, and the operationParam object of the grant response message. Alternately, the UUT vendor may provide the ability to set those parameters on the UUT so that the UUT will request a grant with those parameters	–	--
2	UUT and SAS Test Harness perform a series of Heartbeat Request/Response cycles, which continues until the other test steps are complete. Messaging for each cycle is as follows: - UUT sends Heartbeat Request, including: - cbsdId = C - grantId = G - SAS Test Harness responds with Heartbeat Response, including: - cbsdId = C - grantId = G - transmitExpireTime = current UTC time + 200 seconds - responseCode = 0	–	--
3	Tester performs power measurement on RF interface(s) of UUT, and verifies it complies with the maxEirp setting, Pi. The RF measurement method is out of scope of this document, but may include additional configuration of the UUT, as required, to fulfill the requirements of the power measurement method. J. Note: it may be required for the vendor to provide a method or configuration to bring the UUT to a mode which is required by the measurement methodology. Any such mode is vendor-specific and depends upon UUT behavior and the measurement methodology.	☒ Pass	☐ Fail

RF measurement plot for Test Case:

- Tester performs power measurement on RF interface(s) of UUT, and verifies it complies with the maxEirp setting, Pi. The RF measurement method is out of scope of this document, but may include additional configuration of the UUT, as required, to fulfill the requirements of the power measurement method.

Frequency (MHz)	Channel Bandwidth (MHz)	Granted maxEIRP (dBm/MHz)	Conducted PSD (dBm/MHz)	MIMO Factor (dB)	Antenna Gain (dBi)	Cable Loss (dB)	maxEIRP (dBm/MHz)
3555	10	18	-18.322	6.02	7	22.8	17.498
3555	10	15	-21.947	6.02	7	22.8	13.873
3555	10	10	-27.028	6.02	7	22.8	8.792

Note:

MaxEIRP= Conducted PSD+ Antenna Gain+ Cable loss+MIMO Factor

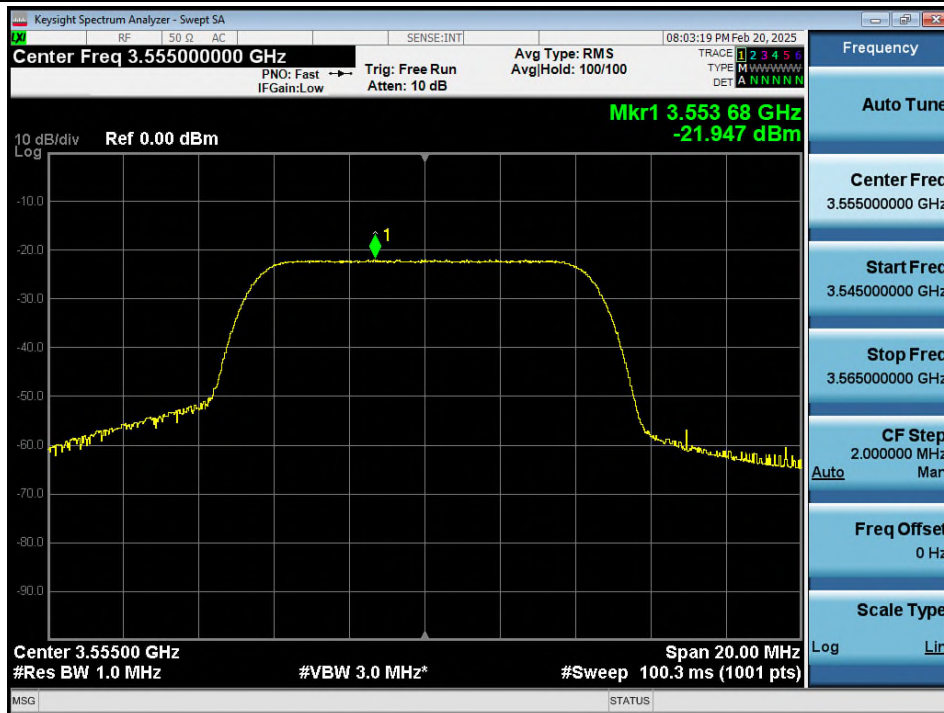




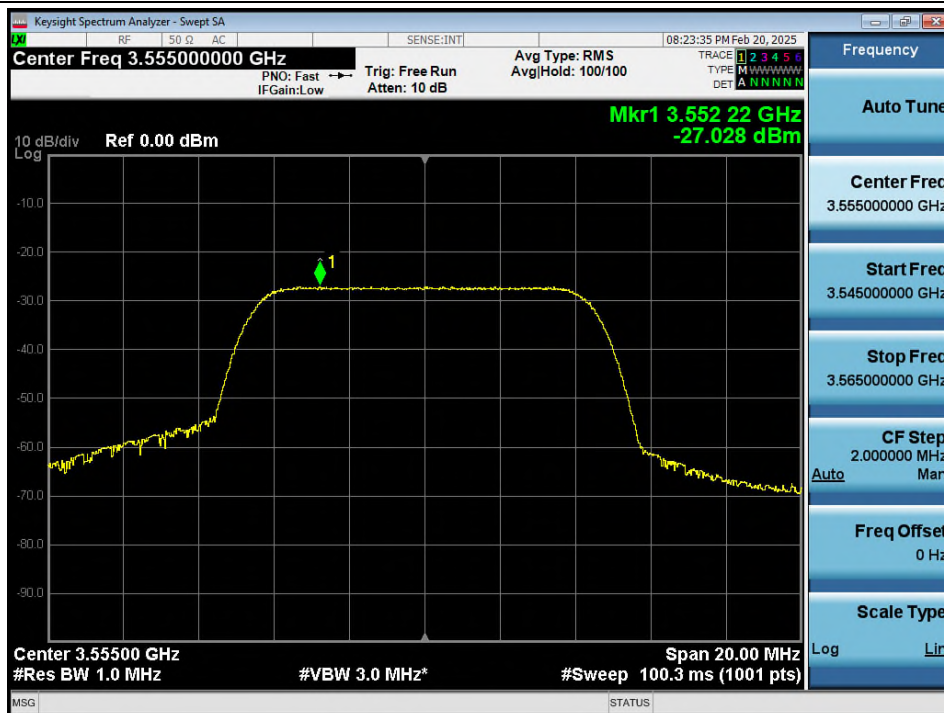
Report No.: KSCR240700144906

Page: 48 of 54

Target Power: 15 dBm/MHz



Target Power: 10 dBm/MHz



8 Test Data Log

Test data log refer to log files (Log files appendix) except for security test cases which shows below.

8.1 WINNF.FT.C.SCS.1

WINNF.CT.CCS.1.pcap

No.	Time	Source	Destination	Protocol	Length	Info
12	0.005335	10.120.8.10	10.120.8.205	TLSv1.2		589 Client Hello
14	0.005361	10.120.8.10	172.19.0.2	TLSv1.2		589 Client Hello
19	0.005568	172.19.0.2	10.120.8.10	TLSv1.2		3379 Server Hello, Certificate, Certificate Request, Server Hello
21	0.005602	10.120.8.205	10.120.8.10	TLSv1.2		3379 Server Hello, Certificate, Certificate Request, Server Hello
26	0.022170	10.120.8.10	10.120.8.205	TLSv1.2		3860 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
28	0.022222	10.120.8.10	172.19.0.2	TLSv1.2		3860 Certificate, Client Key Exchange, Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
33	0.024808	172.19.0.2	10.120.8.10	TLSv1.2		123 Change Cipher Spec, Encrypted Handshake Message
35	0.024829	10.120.8.205	10.120.8.10	TLSv1.2		123 Change Cipher Spec, Encrypted Handshake Message
40	0.025571	10.120.8.10	10.120.8.205	TLSv1.2		611 Application Data
42	0.025589	10.120.8.10	172.19.0.2	TLSv1.2		611 Application Data
44	0.066184	172.19.0.2	10.120.8.10	TLSv1.2		118 Application Data
46	0.066232	10.120.8.205	10.120.8.10	TLSv1.2		118 Application Data
51	0.066604	172.19.0.2	10.120.8.10	TLSv1.2		551 Application Data, Application Data, Application Data, Application Data
53	0.066622	10.120.8.205	10.120.8.10	TLSv1.2		551 Application Data, Application Data, Application Data, Application Data
58	0.068059	10.120.8.10	10.120.8.205	TLSv1.2		103 Encrypted Alert
60	0.068075	10.120.8.10	172.19.0.2	TLSv1.2		103 Encrypted Alert
87	0.997328	10.120.8.10	10.120.8.205	TLSv1.2		589 Client Hello

Frame 19: 3379 bytes on wire (27032 bits), 3379 bytes captured (27032 bits) on interface eth0

Ethernet II, Src: Intel E81C8:8A3E:0000, Dst: Intel E81C8:8A3E:0000

Internet Protocol Version 4, Src: 172.19.0.2, Dst: 10.120.8.10

Transmission Control Protocol, Src Port: 9990, Dst Port: 47004, Seq: 1, Ack: 518, Len: 3387

Transport Layer Security

- TLSv1.2 Record Layer: Handshake Protocol: Server Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 81
 - Handshake Protocol: Server Hello (2)
 - Handshake Type: Server Hello (2)
 - Length: 77
 - Version: TLS 1.2 (0x0303)
 - Random: 6e727c7dd2804ffac602bde193df02809c699cfa787fcea5c53657e8bd002c6
 - Session ID Length: 32
 - Session ID: e72fabce2fc7e8dc5077c9643514924a621edc01657219b5f4ac86e8ea59a6ea

0000 00 00 00 00 00 00 00 00 01 03 06 02 42 ac 13 14
 0010 00 02 00 00 45 00 0d 1f 59 f7 40 00 40 06 1e 4b
 0020 ac 13 00 02 0a 78 00 0a 27 06 b7 9c b2 88 f9 39
 0030 d0 3f 2b 08 00 18 01 fa cb a8 00 00 01 01 08 0a
 0040 e7 bc ab 33 30 32 01 c2 16 03 03 00 51 02 00 00
 0050 4d 03 03 0e 72 7c d2 d2 80 4f fa c6 02 bd e1 93
 0060 df 82 80 9c 69 9c fa 78 7f ce 1a 5c 53 65 7a 0b
 0070 d0 02 c6 20 e7 2f ab ce 2f c7 e8 dc 50 77 c9 64
 0080 35 14 92 4a 62 1e dc 01 65 72 19 b5 f4 ac 86 e8
 0090 ea 59 a6 ea 00 9d 00 00 05 ff 01 00 01 00 16 03
 00a0 03 0c 5d 00 00 8c 59 00 0c 56 00 05 a7 30 82 05
 00b0 a5 30 82 03 0b a0 03 02 01 02 02 14 5d 1b 61 2c
 00c0 62 bc 03 c6 5f 9e ce 8e f7 8d 6d c6 ff 28 d1 8c
 00d0 30 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00 30
 00e0 75 31 0b 30 09 06 03 55 04 06 13 02 43 41 31 17
 00f0 30 15 06 03 55 04 0a 0c 0e 42 4c 69 4e 51 20 4e
 0100 65 74 77 6f 72 6b 73 31 20 30 1e 06 03 55 04 0b

8.2 WINNF.FT.C.SCS.2

WINNF.CFT.CS.2.pcap

文件(F) 编辑(E) 视图(V) 捕获(C) 分析(A) 统计(S) 电话(T) 无线(W) 工具(I) 帮助(H)

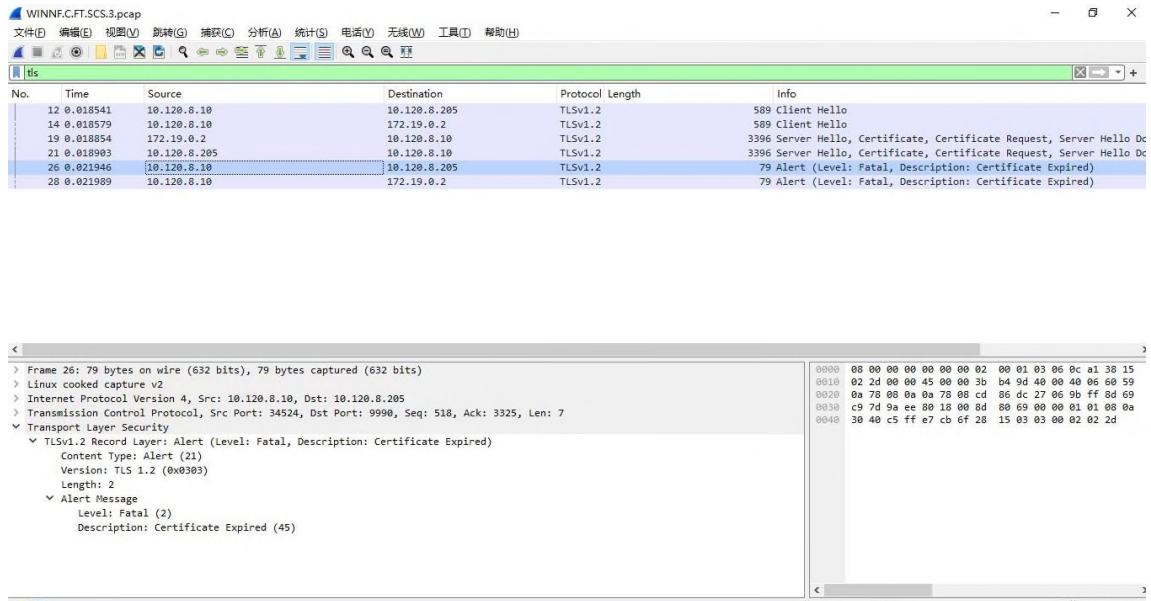
tlc

No.	Time	Source	Destination	Protocol	Length	Info
12	0.012111	10.120.8.10	10.120.8.205	TLSv1.2	589	Client Hello
14	0.012151	10.120.8.10	172.19.0.2	TLSv1.2	589	Client Hello
19	0.012427	172.19.0.2	10.120.8.10	TLSv1.2	3396	Server Hello, Certificate, Certificate Request, Server Hello Do
21	0.012453	10.120.8.205	10.120.8.10	TLSv1.2	3396	Server Hello, Certificate, Certificate Request, Server Hello Do
26	0.016405	10.120.8.10	10.120.8.205	TLSv1.2	79	Alert (Level: Fatal, Description: Certificate Revoked)
28	0.016438	10.120.8.10	172.19.0.2	TLSv1.2	79	Alert (Level: Fatal, Description: Certificate Revoked)

< Frame 26: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
 > Linux cooked capture v2
 > Internet Protocol Version 4, Src: 10.120.8.10, Dst: 10.120.8.205
 > Transmission Control Protocol, Src Port: 53652, Dst Port: 9990, Seq: 518, Ack: 3325, Len: 7
 > Transport Layer Security
 > TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Certificate Revoked)
 > Content Type: Alert (21)
 > Version: TLS 1.2 (0x0303)
 > Length: 2
 > Alert Message
 > Level: Fatal (2)
 > Description: Certificate Revoked (44)

0000 08 00 00 00 00 00 02 00 01 03 06 0c a1 38 15
 0010 02 2d 00 00 45 00 00 3b 97 2a 40 00 40 06 7d cc
 0020 0a 78 08 0a 0a 78 08 cd d1 94 27 06 cc 9f 0e 90
 0030 fd 65 e0 ba 00 18 00 6d 4f b8 00 00 01 01 00 0a
 0040 30 38 23 b3 e7 c2 03 15 03 03 00 02 02 2c

8.3 WINNF.FT.C.SCS.3



Wireshark packet capture analysis of WINNF.FT.C.SCS.3.pcap. The top pane shows a list of packets, with packet 26 selected. The bottom pane shows the details of packet 26, which is a TLSv1.2 Alert (Level: Fatal, Description: Certificate Expired). The packet bytes pane shows the raw data of the alert message.

No.	Time	Source	Destination	Protocol	Length	Info
12	0.018541	10.120.8.10	10.120.8.205	TLSv1.2	589	Client Hello
14	0.018579	10.120.8.10	172.19.0.2	TLSv1.2	589	Client Hello
19	0.018854	172.19.0.2	10.120.8.10	TLSv1.2	3396	Server Hello, Certificate, Certificate Request, Server Hello Dc
21	0.018983	10.120.8.205	10.120.8.10	TLSv1.2	3396	Server Hello, Certificate, Certificate Request, Server Hello Dc
26	0.021946	10.120.8.10	10.120.8.205	TLSv1.2	79	Alert (Level: Fatal, Description: Certificate Expired)
28	0.021989	10.120.8.10	172.19.0.2	TLSv1.2	79	Alert (Level: Fatal, Description: Certificate Expired)

Frame 26: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)

Linux cooked capture v2

Internet Protocol Version 4, Src: 10.120.8.10, Dst: 10.120.8.205

Transmission Control Protocol, Src Port: 34524, Dst Port: 9990, Seq: 518, Ack: 3325, Len: 7

Transport Layer Security

TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Certificate Expired)

Content Type: Alert (21)

Version: TLS 1.2 (0x0303)

Length: 2

Alert Message

Level: Fatal (2)

Description: Certificate Expired (45)

0000 08 00 00 00 00 00 02 00 01 03 06 0c a1 38 15

0010 02 2d 00 00 45 00 00 3b b4 9d 40 00 40 00 59

0020 0a 78 00 0a 0a 78 00 cd 06 dc 27 06 0b ff 0d 69

0030 c9 7d 9a ee 80 18 00 8d 80 69 00 00 01 01 08 0a

0040 30 40 c5 ff e7 cb 6f 28 15 03 03 00 02 02 2d

8.4 WINNF.FT.C.SCS.4

WINNF.C.FT.C.SCS.4.pcap

文件(F) 编辑(E) 视图(V) 跟踪(T) 捕获(C) 分析(A) 统计(S) 电话(W) 无线(W) 工具(I) 帮助(H)

tls

No.	Time	Source	Destination	Protocol	Length	Info
12	0.019146	10.120.8.10	10.120.8.205	TLSv1.2		589 Client Hello
14	0.019178	10.120.8.10	172.19.0.2	TLSv1.2		589 Client Hello
19	0.019456	172.19.0.2	10.120.8.10	TLSv1.2		3368 Server Hello, Certificate, Certificate Request, Server Hello Do
21	0.019510	10.120.8.205	10.120.8.10	TLSv1.2		3368 Server Hello, Certificate, Certificate Request, Server Hello Do
26	0.022912	10.120.8.10	10.120.8.205	TLSv1.2		79 Alert (Level: Fatal, Description: Unknown CA)
30	0.022941	10.120.8.10	172.19.0.2	TLSv1.2		79 Alert (Level: Fatal, Description: Unknown CA)

< >

> Frame 26: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
 > Linux cooked capture v2
 > Internet Protocol Version 4, Src: 10.120.8.10, Dst: 10.120.8.205
 > Transmission Control Protocol, Src Port: 41686, Dst Port: 9990, Seq: 518, Ack: 3297, Len: 7
 > Transport Layer Security
 > TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Unknown CA)
 Content Type: Alert (21)
 Version: TLS 1.2 (0x0303)
 Length: 2
 > Alert Message
 Level: Fatal (2)
 Description: Unknown CA (48)

0000 08 00 00 00 00 00 02 00 01 03 06 0c a1 30 15
 0010 02 2d 00 00 45 00 00 3b c3 13 40 00 40 06 51 e3
 0020 0a 70 00 0a 0a 70 00 cd a2 d6 27 00 0a 3f 40 63
 0030 cb 9e db 2f 80 18 00 8d e3 c6 00 00 01 01 08 0a
 0040 30 47 93 0e e7 d2 3c 18 15 03 03 00 02 02 30

< >



Page: 53 of 54

8.5 WINNF.FT.C.SCS.5

The figure displays a Wireshark network traffic capture. The top pane shows a list of packets, with packet 23 selected. The middle pane shows the packet details for the selected packet, and the bottom pane shows the raw packet data in hexadecimal and ASCII.

Packets List:

No.	Time	Source	Destination	Protocol	Length	Info
12	0.129179	10.120.8.10	10.120.8.205	TLSv1.2	589	Client Hello
14	0.129249	10.120.8.10	172.19.0.2	TLSv1.2	589	Client Hello
19	0.129648	172.19.0.2	10.120.8.10	TLSv1.2	1671	Server Hello, Certificate, Certificate Request, Server Hello Done
21	0.129675	10.120.8.205	10.120.8.10	TLSv1.2	1671	Server Hello, Certificate, Certificate Request, Server Hello Done
23	0.133638	10.120.8.10	10.120.8.205	TLSv1.2	79	Alert (Level: Fatal, Description: Decrypt Error)
30	0.133701	10.120.8.10	172.19.0.2	TLSv1.2	79	Alert (Level: Fatal, Description: Decrypt Error)

Packet Details (Packet 23):

- Frame 23: 79 bytes on wire (632 bits), 79 bytes captured (632 bits)
- Linux cooked capture v2
- Internet Protocol Version 4, Src: 10.120.8.10, Dst: 10.120.8.205
- Transmission Control Protocol, Src Port: 45806, Dst Port: 9990, Seq: 518, Ack: 1600, Len: 7
- Transport Layer Security
 - TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Decrypt Error)
 - Content Type: Alert (21)
 - Version: TLS 1.2 (0x0303)
 - Length: 2
 - Alert Message
 - Level: Fatal (2)
 - Description: Decrypt Error (51)

Raw Data (Hex):

```

0000  08 00 00 00 00 00 02 00 01 03 06 0c a1 38 15
0010  02 2d 00 00 45 00 00 3b 10 e5 48 00 48 06 04 11
0020  0a 78 08 0a 0a 78 08 cd b2 ee 27 06 04 d2 f7 2d
0030  ec 4c bc a4 88 18 00 87 4c d7 00 00 01 01 08 0a
0040  30 4b 7b 41 e7 d6 24 3a 15 03 03 00 02 02 33
  
```



Report No.: KSCR240700144906

Page: 54 of 54

9 Test Setup Photo

Refer to Appendix - Test Setup Photo for KSCR2403000374AT

10 EUT Constructional Details (EUT Photos)

Refer to Appendix - Photographs of EUT Constructional Details for KSCR2403000374AT