

Test Report

As per

FCC Part 96 SAS requirements (CBRS Test Plan)

on the

LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz)
Base Station

Issued by:
TÜV SÜD Canada

Inc.
2972 Joseph-A-
Bombardier
Laval, QC, H7P 6E3
Canada
Ph: (450) 687-4976

Scott Drysdale.
Test Personnel



Abderrahmane Ferhat
Report Reviewer



Canada

**Choose certainty.
Add value.**

Testing produced for

Ericcson Canada

See Appendix A for
full client & EUT
details.



Testing Laboratory
Certificate #2955.02

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



Table of Contents

Table of Contents	2
Report Scope	3
Summary	4
Test Results Summary	5
Notes, Justifications, or Deviations	14
Applicable Standards, Specifications and Methods	15
Document Revision Status	16
Definitions and Acronyms	17
Testing Facility	18
Calibrations and Accreditations	18
Testing Environmental Conditions and Dates	19
Detailed Test Results Section	20
Authorization transmit after it receives authorization from a SAS	21
Check the device registration and authorization with the SAS	30
Confirm that the device changes its operating power and/or channel in response to a command from the SAS and Confirm that the device correctly configures based on the different license classes.	30
Confirm that the device transmits at a power level less than or equal to the maximum power level approved by the SAS	47
WINNF Security Test Case Analysis	55
WINNF.FT.C.SCS.1	55
WINNF.FT.C.SCS.2	60
WINNF.FT.C.SCS.3	67
WINNF.FT.C.SCS.4	72
WINNF.FT.C.SCS.5	76
Appendix A – EUT & Client Provided Details	82
Technical Description	84
Appendix B – EUT, Peripherals, and Test Setup Photos	85

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



Report Scope

This report addresses the EMC verification testing and test results of the **LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station** herein referred to as EUT (Equipment Under Test). The EUT was tested for compliance against the following standards:

FCC Part 96 SAS requirements (CBRS Test Plan)

. Test procedures, results, justifications, and engineering considerations, if any, follow later in this report.

For a more detailed list of the standards and the revision used, see the "Applicable Standards, Specifications and Methods" section of this report.

This report does not imply product endorsement by any government, accreditation agency, or TÜV SÜD Canada Inc.

Opinions or interpretations expressed in this report, if any, are outside the scope of TÜV SÜD Canada Inc accreditations. Any opinions expressed do not necessarily reflect the opinions of TÜV SÜD Canada Inc, unless otherwise stated.

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Summary

The results contained in this report relate only to the item(s) tested.

Equipment Under Test (EUT)	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
EUT passed all tests performed	Yes
Tests conducted by	Scott Drysdale

For testing dates, see 'Testing Environmental Conditions and Dates'.

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Test Results Summary

Section as per Working Document WINNF-TS-0122

Section	CBS D	D P	Test Case ID	Test Case Title	RF Measurement Requirement	Pass / Fail
6.1.4.1. 1	X	--	WINNF.FT.C.R EG.1	Multi-Step registration	Monitor for 60 seconds after REG message sent. No transmission during test.	N/A
6.1.4.1. 2	--	X	WINNF.FT.D.R EG.2	Domain Proxy Multi-Step registration	Monitor for 60 seconds after REG message sent. No transmission during test.	P
6.1.4.1. 3	X	--	WINNF.FT.C.R EG.3	Single-Step registration for Category A CBSD	Monitor for 60 seconds after REG message sent. No transmission during test.	N/A
6.1.4.1. 4	--	X	WINNF.FT.D.R EG.4	Domain Proxy Single-Step registration for Cat A CBSD (Note: Mandatory for without CPI, if EUT will always have signed CPI – asked for email waiver)	Monitor for 60 seconds after REG message sent. No transmission during test.	N/A
6.1.4.1. 5	X	--	WINNF.FT.C.R EG.5	Single-Step registration for CBSD with CPI signed data	Monitor for 60 seconds after REG message sent. No transmission during test.	N/A
6.1.4.1. 6	--	X	WINNF.FT.D.R EG.6	Domain Proxy Single-Step registration for CBSD with CPI signed data	Monitor for 60 seconds after REG message sent. No transmission during test.	P
6.1.4.1. 7	X	X	WINNF.FT.C.R EG.7	Registration due to change of an installation parameter	Test waits until transmission starts, then trigger an	P

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

					installationParam change. <ul style="list-style-type: none">Record time at which transmission stops. Time must be within 60 seconds of the installationParam change taking effect.	
6.1.4.2. 1	X	--	WINNF.FT.C.R EG.8	Missing Required parameters (responseCode 102)	Monitor for 60 seconds after REG message sent. No transmission during test.	N/A
6.1.4.2. 2	--	X	WINNF.FT.D.R EG.9	Domain Proxy Missing Required parameters (responseCode 102)	Monitor for 60 seconds after REG message sent. No transmission during test.	P
6.1.4.2. 3	X	--	WINNF.FT.C.R EG.10	Pending registration (responseCode 200)	Monitor for 60 seconds after REG message sent. No transmission during test.	N/A
6.1.4.2. 4	--	X	WINNF.FT.D.R EG.11	Domain Proxy Pending registration (responseCode 200)	Monitor for 60 seconds after REG message sent. No transmission during test.	P
6.1.4.2. 5	X	--	WINNF.FT.C.R EG.12	Invalid parameter (responseCode 103)	Monitor for 60 seconds after REG message sent. No transmission during test.	N/A
6.1.4.2. 6	--	X	WINNF.FT.D.R EG.13	Domain Proxy Invalid parameters (responseCode 103)	Monitor for 60 seconds after REG message sent. No transmission during test.	P
6.1.4.2. 7	X	--	WINNF.FT.C.R EG.14	Blacklisted CBSD (responseCode 101)	Monitor for 60 seconds after REG message sent. No	N/A

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

					transmission during test.	
6.1.4.2. 8	--	X	WINNF.FT.D.R EG.15	Domain Proxy Blacklisted CBSD (responseCode 101)	Monitor for 60 seconds after REG message sent. No transmission during test.	P
6.1.4.2. 9	X	--	WINNF.FT.C.R EG.16	Unsupported SAS protocol version (responseCode 100)	Monitor for 60 seconds after REG message sent. No transmission during test.	N/A
6.1.4.2. 10	--	X	WINNF.FT.D.R EG.17	Domain Proxy Unsupported SAS protocol version responseCode 100)	Monitor for 60 seconds after REG message sent. No transmission during test.	P
6.1.4.2. 11	X	--	WINNF.FT.C.R EG.18	Group Error (responseCode 201)	Monitor for 60 seconds after REG message sent. No transmission during test.	N/A
6.1.4.2. 12	--	X	WINNF.FT.D.R EG.19	Domain Proxy Group Error (responseCode 201)	Monitor for 60 seconds after REG message sent. No transmission during test.	P
6.1.4.3. 1	X	X	WINNF.FT.C.R EG.20	Category A CBSD location update		N/A
6.3.4.2. 1	X	X	WINNF.FT.C.G RA.1 (TYPO FIXED D TO C)	Unsuccessful Grant responseCode=400 (INTERFERENCE)	Monitor for 60 seconds after REG message sent. No transmission during test.	P
6.3.4.2. 2	X	X	WINNF.FT.C.G RA.2	Unsuccessful Grant responseCode=401 (GRANT_CONFLICT)	Monitor for 60 seconds after REG message sent. No transmission during test.	P
6.4.4.1. 1	X	--	WINNF.FT.C.H BT.1	Heartbeat Success Case (first Heartbeat Response)	Monitor RF from start of test. Ensure that: <ul style="list-style-type: none">• Transmission does not start until time of first	N/A

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

					<p>heartbeat response or after.</p> <ul style="list-style-type: none"> After transmission starts, measure that transmission is within the granted channel (frequencyLow, frequencyHigh) 	
6.4.4.1.2	--	X	WINNF.FT.D.H BT.2	Domain Proxy Heartbeat Success Case (first Heartbeat Response)	<p>Monitor RF from start of test. Ensure that:</p> <ul style="list-style-type: none"> Transmission does not start until time of first heartbeat response or after. After transmission starts, measure that transmission is within the granted channel (frequencyLow, frequencyHigh) 	P
6.4.4.2.1	X	X	WINNF.FT.C.H BT.3	Heartbeat responseCode=105 (DREGISTER)	<p>Monitor RF transmission. Ensure that:</p> <ul style="list-style-type: none"> CBSD stops transmission within 60 seconds of the heartbeatResponse which contains 	P

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

					responseCode = 105	
6.4.4.2.2	X	--	WINNF.FT.C.H BT.4	Heartbeat responseCode=500 (TERMINATED_GRANT)		N/A
6.4.4.2.3	X	X	WINNF.FT.C.H BT.5	Heartbeat responseCode=501 (SUSPENDED_GRANT) in First Heartbeat Response	Monitor RF transmission from start of test. Ensure there is no transmission during the test	p
6.4.4.2.4	X	X	WINNF.FT.C.H BT.6	Heartbeat responseCode=501 (SUSPENDED_GRANT) in Subsequent Heartbeat Response	Monitor RF transmission. Ensure: <ul style="list-style-type: none">CBSD stops transmission within 60 seconds of heartbeatResponse which contains responseCode=501	p
6.4.4.2.5	X	X	WINNF.FT.C.H BT.7	Heartbeat responseCode=502 (UNSYNC_OP_PARAM)	Monitor RF transmission. Ensure: <ul style="list-style-type: none">CBSD stops transmission within 60 seconds of heartbeatResponse which contains responseCode=502	p
6.4.4.2.6	--	X	WINNF.FT.D.H BT.8	Domain Proxy Heartbeat responseCode=500 (TERMINATED_GRANT)	Monitor RF transmission. CBSDs will have different behavior: <ul style="list-style-type: none">CBSD1: will continue to transmit to end of test	P

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

					(this is not a pass/fail criteria, but check) <ul style="list-style-type: none"> • CBSD2: must stop transmission within 60 seconds of being sent heartbeatResponse with responseCode = 500 	
6.4.4.3.1	X	X	WINNF.FT.C.H BT.9	Heartbeat Response Absent (First Heartbeat)	Monitor RF from start of test to 60 seconds after last heartbeatResponse message was sent. CBSD should not transmit at any time during test	P
6.4.4.3.2	X	X	WINNF.FT.C.H BT.10	Heartbeat Response Absent (Subsequent Heartbeat)	Monitor RF transmission. Verify: <ul style="list-style-type: none"> • CBSD must stop transmission within transmitExpiresTime+60 seconds, where transmitExpiresTime is from last successful heartbeatResponse message 	P
6.5.4.2.1	X	--	WINNF.FT.C.M ES.1	Registration Response contains measReportConfig	No RF monitoring	N/A
6.5.4.2.2	--	X	WINNF.FT.D.M ES.2	Domain Proxy Registration Response contains measReportConfig	No RF monitoring	P

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

6.5.4.2.3	X	X	WINNF.FT.C.M ES.3	Grant Response contains measReportConfig	No RF monitoring	P
6.5.4.2.4	X	--	WINNF.FT.C.M ES.4	Heartbeat Response contains measReportConfig	No RF monitoring	N/A
6.5.4.2.5	--	X	WINNF.FT.D.M ES.5	Domain Proxy Heartbeat Response contains measReportConfig	No RF monitoring	P
6.6.4.1.1	X	--	WINNF.FT.C.R LQ.1	Successful Relinquishment	Monitor RF transmission. Ensure: <ul style="list-style-type: none">CBSD stops transmission at any time prior to sending the relinquishmentRequest message.	N/A
6.6.4.1.2	--	X	WINNF.FT.D.R LQ.2	Domain Proxy Successful Relinquishment	Monitor RF transmission. Ensure: <ul style="list-style-type: none">CBSD stops transmission at any time prior to sending the relinquishmentRequest message.	P
6.7.4.1.1	X	--	WINNF.FT.C.D RG.1	Successful Deregistration	Monitor RF transmission. Ensure: <ul style="list-style-type: none">CBSD stops transmission at any time prior to sending the relinquishmentRequest message or deregistrationRequest message (whichever is sent first)	N/A

Client	Ericsson			 Canada	
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station				
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)				

6.7.4.1.2	--	X	WINNF.FT.D.DRG.2	Domain Proxy Successful Deregistration	Monitor RF transmission. Ensure : • CBSD stops transmission at any time prior to sending the relinquishmentRequest message or deregistrationRequest message (whichever is sent first)	P
6.8.4.1.1	X	X	WINNF.FT.C.SCS.1	Successful TLS connection between UUT and SAS Test Harness	No RF transmission during test Check the tcpdump for the TLS information	P
6.8.4.2.1	X	X	WINNF.FT.C.SCS.2	TLS failure due to revoked certificate	No RF transmission during test Check the tcpdump for the TLS information	P
6.8.4.2.2	X	X	WINNF.FT.C.SCS.3	TLS failure due to expired server certificate	No RF transmission during test Check the tcpdump for the TLS information	P
6.8.4.2.3	X	X	WINNF.FT.C.SCS.4	TLS failure when SAS Test Harness certificate is issued by unknown CA	No RF transmission during test Check the tcpdump for the TLS information	P
6.8.4.2.4	X	X	WINNF.FT.C.SCS.5	TLS failure when certificate at the SAS Test Harness is corrupted	No RF transmission during test Check the tcpdump for the TLS information	P
7.1.4.1.1	X	X	WINNF.PT.C.HBT	UUT RF Transmit Power Measurement	Power Spectral Density test case. Assume we use 1 carrier bandwidth	P

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

					(say, 5 or 10 MHz), one frequency (say middle channel in band) for test. Measure at max transmit power, and reduce in steps of 3 dB to minimum declared transmit power.	
--	--	--	--	--	--	--

If the product as tested complies with the specification, the EUT is deemed to comply with the standard and is deemed a 'PASS' or 'P' grade. If not 'FAIL' grade is issued. Where 'N/A' is stated this means the test case is not applicable, and see Notes, Justifications or Deviations Section for details.

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



Notes, Justifications, or Deviations

The following notes, justifications for tests not performed or deviations from the above listed specifications apply:

A later revision of the standard may have been substituted in place of the previous dated referenced revision. The year of the specification used is listed under applicable standards. Using the later revision accomplishes the goal of ensuring compliance to the intent of the previous specification, while allowing the laboratory to incorporate the extensions and clarifications made available by a later revision.

For the N/A test cases, the following justifications apply:

- a. EUT is a CBSD with Domain Proxy
- b. EUT supports the following Conditional functionality from WINNF-TS-0122-V1.0.0, Table 6-2:
 - i. C1 – Multi-step registration (WINNF.FT.D.REG.2)
 - ii. C3 – Single step registration containing CPI-signed data in the registration message (WINNF.FT.D.REG.6)
 - iii. C4 – RECEIVED_POWER_WITHOUT_GRANT measurement report (WINNF.FT.D.MES.2)
 - iv. C5 – RECEIVED_POWER_WITH_GRANT measurement report (WINNF.FT.D.MES.3, WINNF.FT.D.MES.5)
 - v. C6 – UUT supports installation parameter change (WINNF.FT.C.REG.7)
- c. Optional test cases were not performed

Note, where graph sweeps are incomplete, this was used to set the time stamp of when the events occurred. This can be accomplished by determining the time at which the graph was captured and subtracting the remaining time. For example if there was a 30 second sweep, and 9 out of 10 is complete, that means the end occurred at the 27 second mark. If the time on the graph was 12:03:35, this means the graph started at 12:03:08. This allows us to co-ordinate graph with UTC in the logs.

Logs are kept on file.

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



Applicable Standards, Specifications and Methods

ANSI C63.4:2014 Methods of Measurement of Radio-Noise Emissions from Low-Voltage Electrical and Electronic Equipment in the Range of 9 kHz to 40 GHz

CFR47 FCC Part 96 Code of Federal Regulations – Citizens Broadband Radio Service

WINNF-TS-0122 Conformance and Performance Test Technical Specification;
Version V1.0.0 CBSD/DP as Unit Under Test (UUT)
19 December 2017 Working Document

ISO/IEC 17025:2005 General requirements for the competence of testing and calibration laboratories

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



Document Revision Status

Revision 000:	July 26, 2018	Initial (Draft) Release
Revision 001:	August 9, 2018	Revisions as per customer request – kept on file
Revision 002:	August 10, 2018	Revisions as per customer request – kept on file
Revision 003:	August 12, 2018	Revisions as per customer request – kept on file

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Definitions and Acronyms

The following definitions and acronyms are applicable in this report.
See also ANSI C63.14.

AE – Auxiliary Equipment. A digital accessory that feeds data into or receives data from another device (host) that in turn, controls its operation.

AM – Amplitude Modulation

Class A device – A device that is marketed for use in a commercial, industrial or business environment. A 'Class A' device should not be marketed for use by the general public and the instructions for use accompanying the product shall contain the following text:

Caution: This equipment is not intended for use in residential environments and may not provide adequate protection to radio reception in such environments.

Class B device – A device that is marketed for use in a residential environment and may also be used in a commercial, business or industrial environments.

EMC – Electro-Magnetic Compatibility. The ability of an equipment or system to function satisfactorily in its electromagnetic environment without introducing intolerable electromagnetic disturbances to anything in that environment.

EMI – Electro-Magnetic Immunity. The ability to maintain a specified performance when the equipment is subjected to disturbance (unwanted) signals of specified levels.

Enclosure Port – Physical boundary of equipment through which electromagnetic fields may radiate or impinge.

EUT – Equipment Under Test. A device or system being evaluated for compliance that is representative of a product to be marketed.

LISN – Line Impedance Stabilization Network

NCR – No Calibration Required

NSA – Normalized Site Attenuation

RF – Radio Frequency

EMC Test Plan – An EMC test plan established prior to testing. See 'Appendix A – EUT & Client Provided Details'.

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



Testing Facility

Testing for EMC on the EUT was carried out at customer location as described in Appendix A.

Calibrations and Accreditations

TÜV SÜD Canada Inc is accredited to ISO/IEC 17025 by A2LA with Testing Certificate #2955.02. The laboratory's current scope of accreditation listing can be found as listed on the A2LA website. All measuring equipment is calibrated on an annual or bi-annual basis as listed for each respective test.

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Testing Environmental Conditions and Dates

Following environmental conditions were recorded in the facility during time of testing

Date	Test	Initials	Temperature (°C)	Humidity (%)	Pressure (kPa)
June 11, 2018	All	SD	20-23	40-55	96.106

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



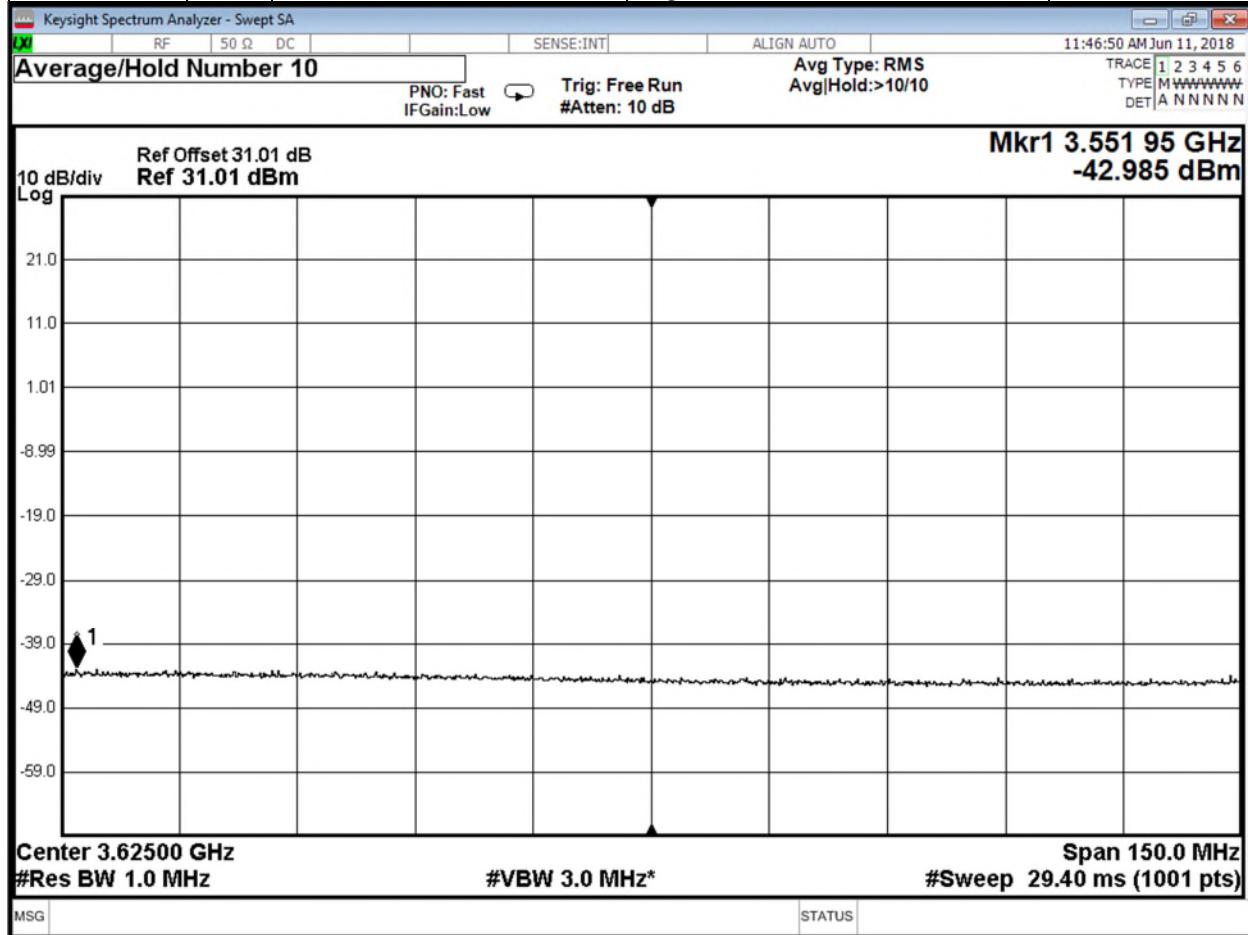
Detailed Test Results Section

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)

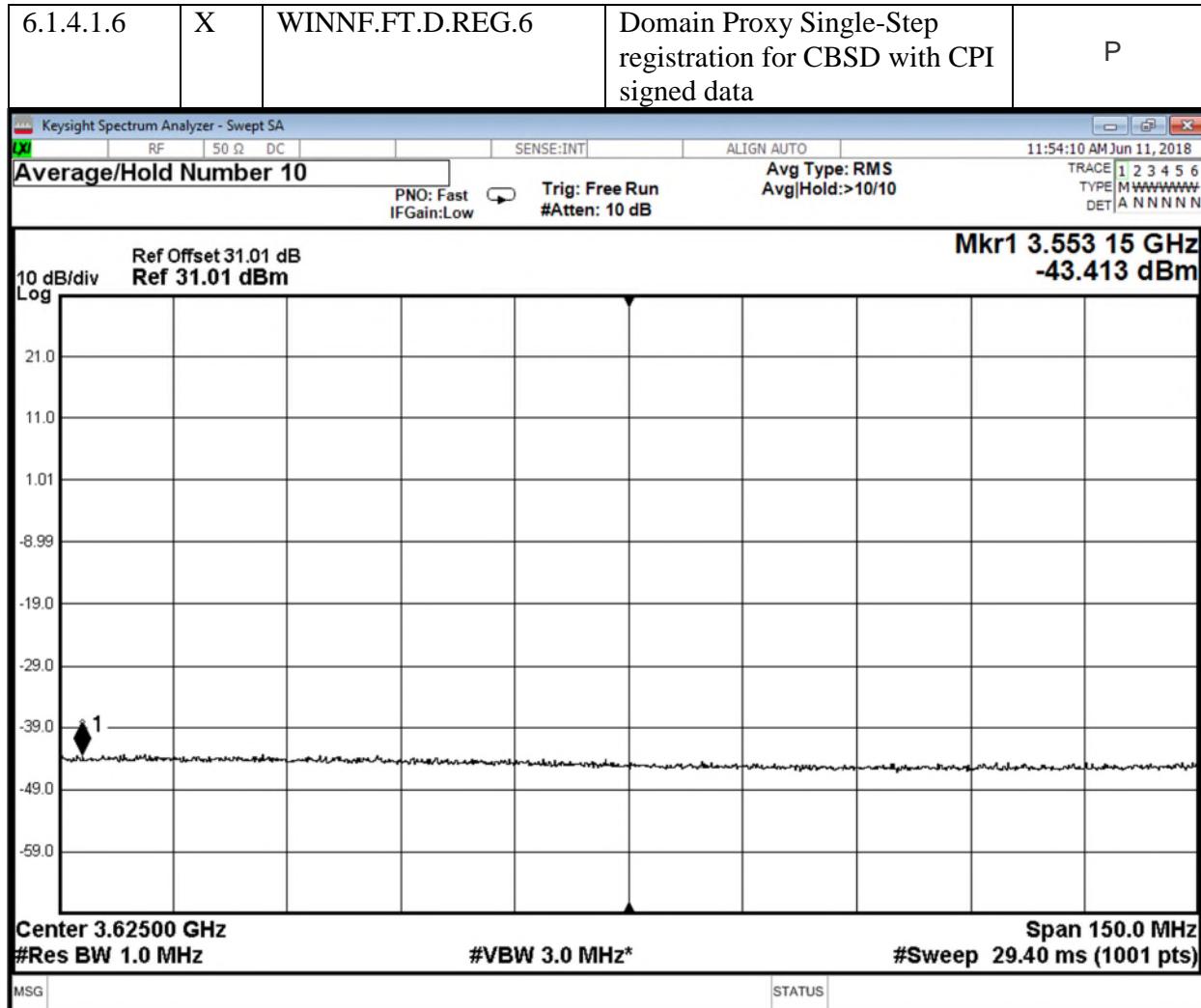


Authorization transmit after it receives authorization from a SAS.

Section	DP	Test Case ID	Test Case Title	Pass / Fail
6.1.4.1.2	X	WINNF.FT.D.REG.2	Domain Proxy Multi-Step registration	P



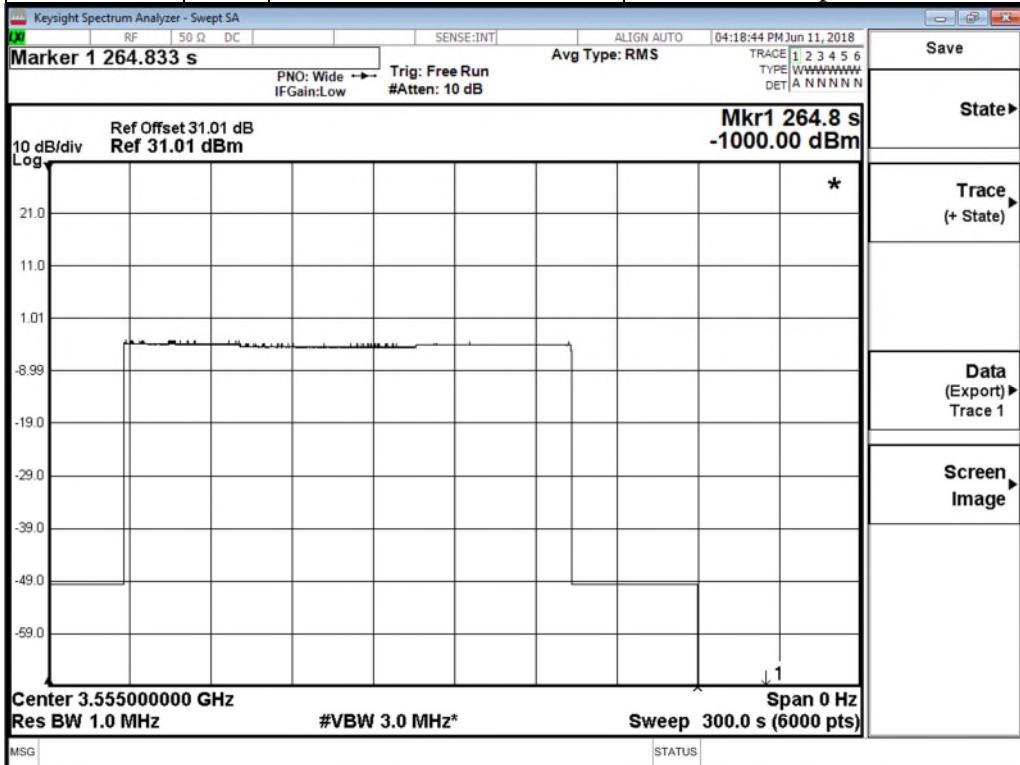
Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	



Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



6.1.4.1.7	X	WINNF.FT.C.REG.7	Registration due to change of an installation parameter	P
-----------	---	------------------	---	---



From Test Harness Logs:

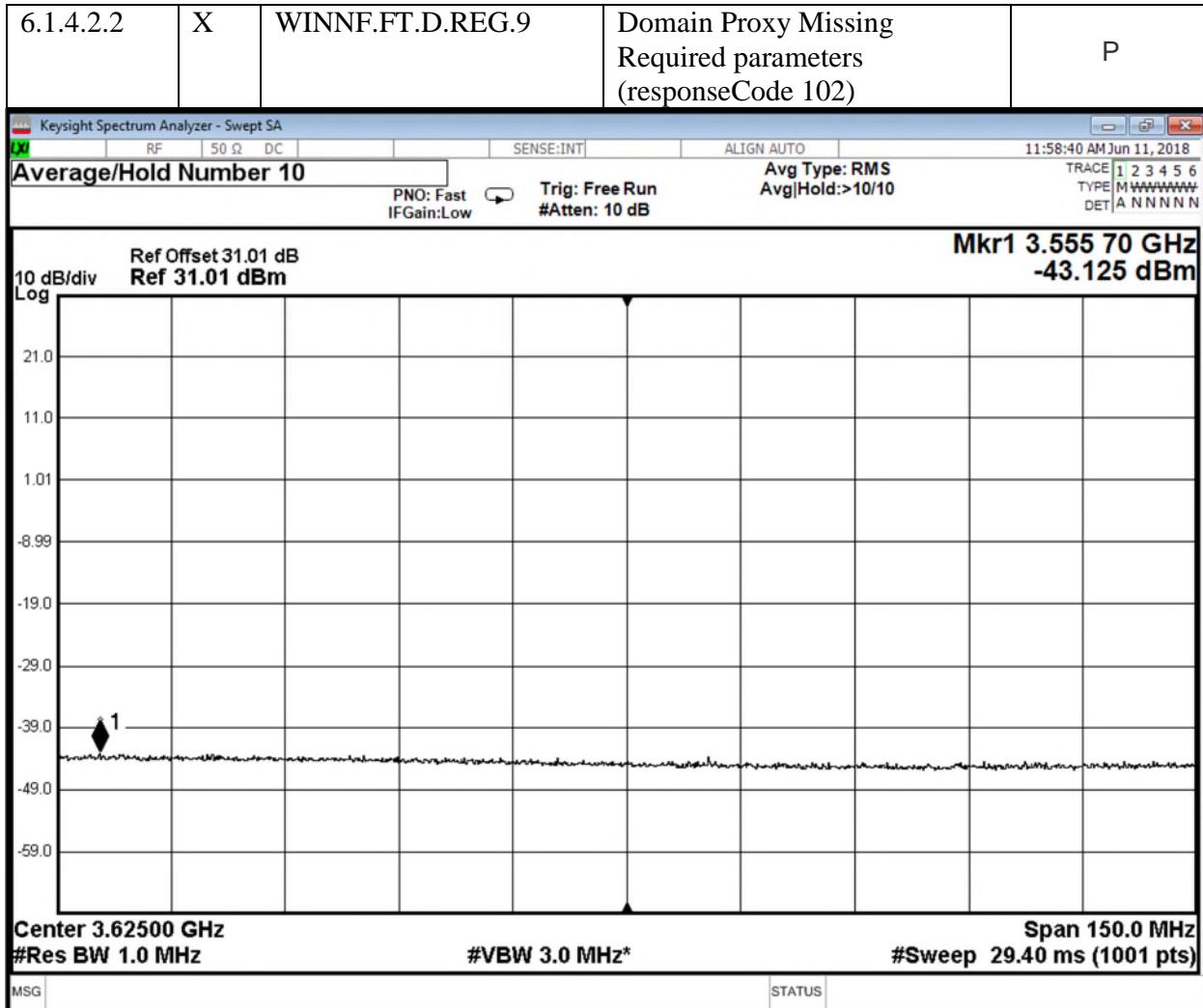
eventTime (from logs)	Comment
20:18:04	RLQ.request sent at 2018-06-11T20:18:04.503Z, first HBT.response sent at 2018-06-11T20:15:08.432Z

From Spectrum Analyzer Capture:

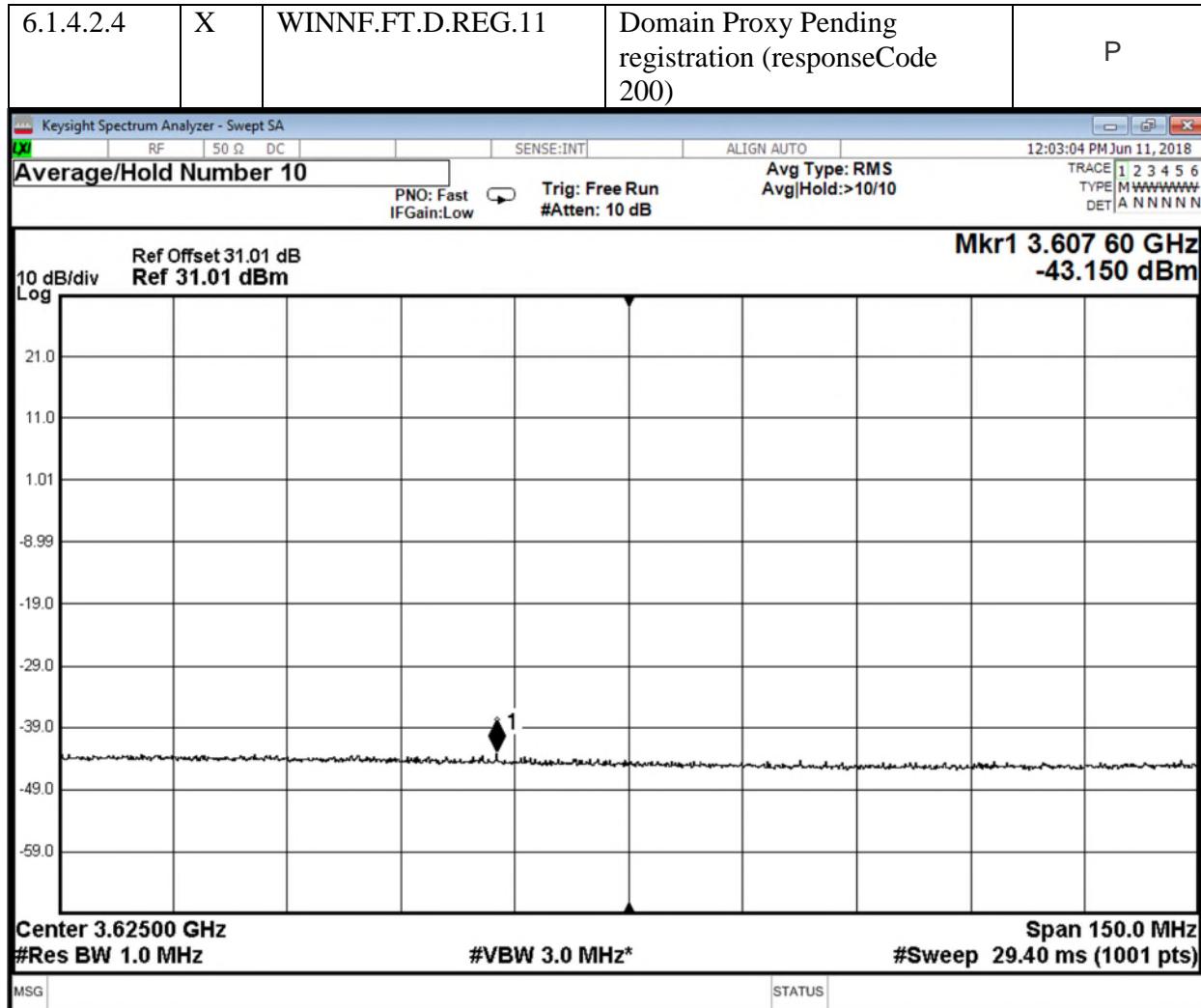
Test	plot time [h:m:s]	sweep [s]	plot start time [h:m:s]	mrk [s]	event time [h:m:s]	eventTime UTC	
REG.7	16:18:44	240	16:14:44 DP logs (on file)	192	16:17:56	20:17:56 20:17:59	ok ok

Note: DP log time result was taken from Domain Proxy internal logs, to verify shutdown time .

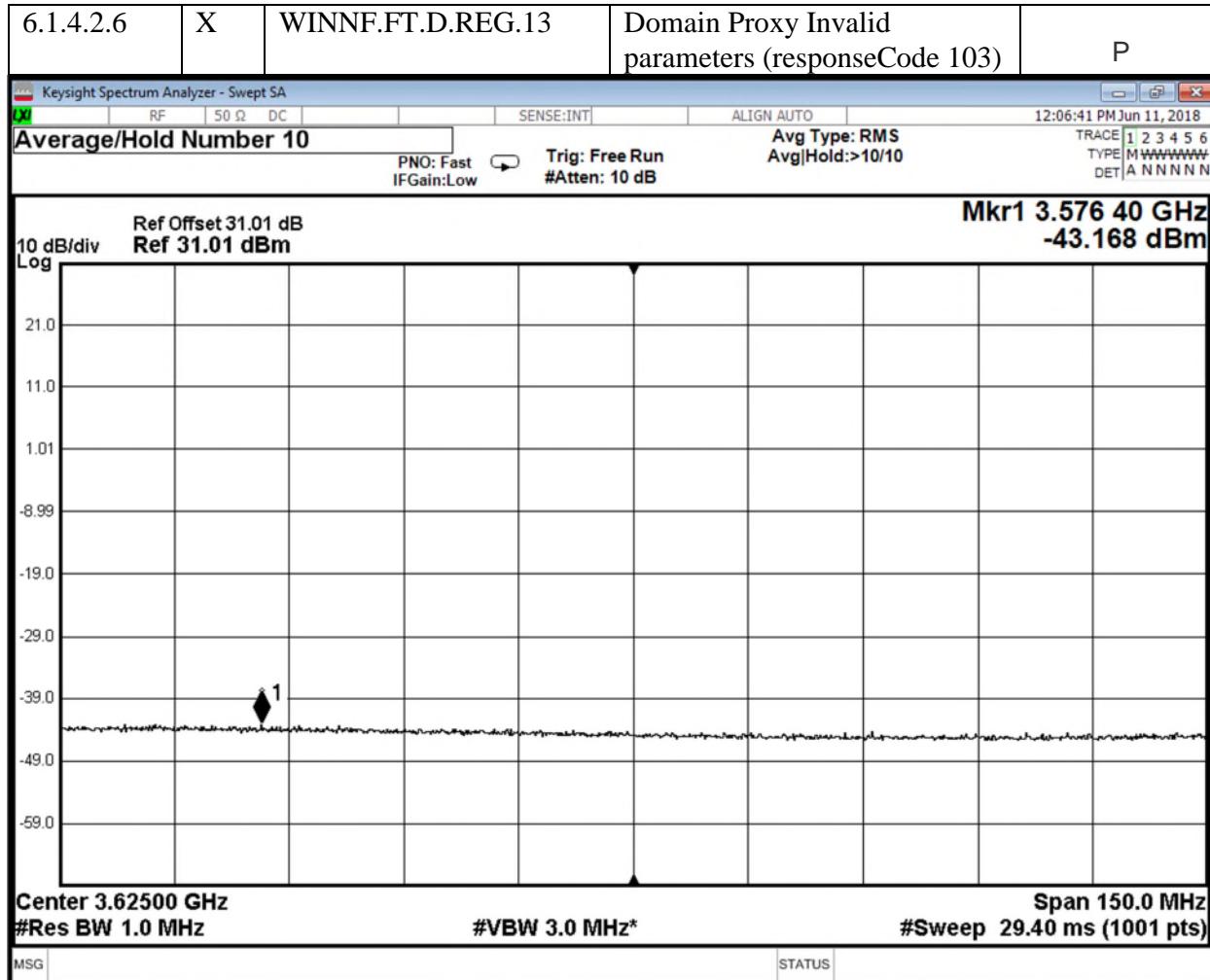
Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	



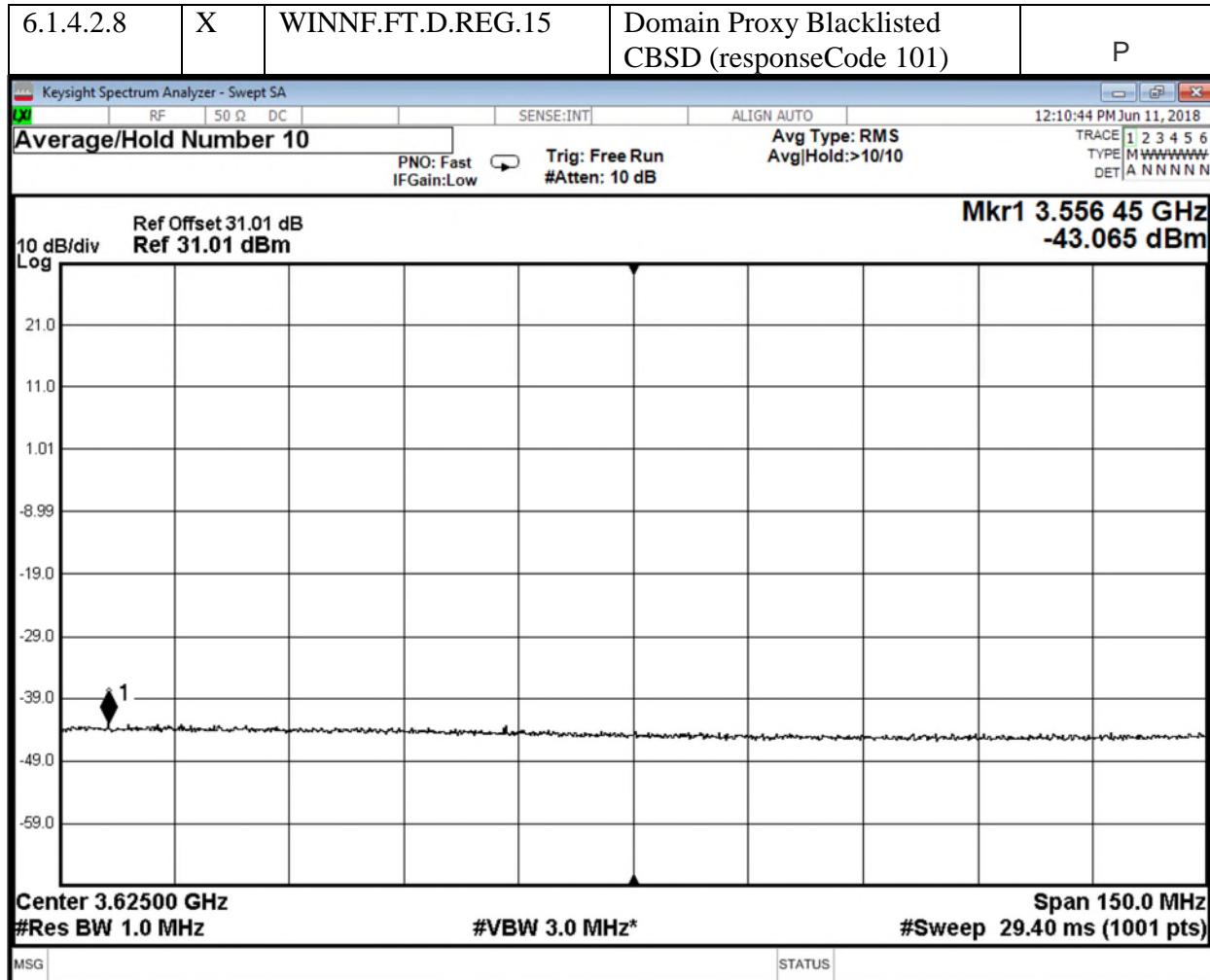
Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



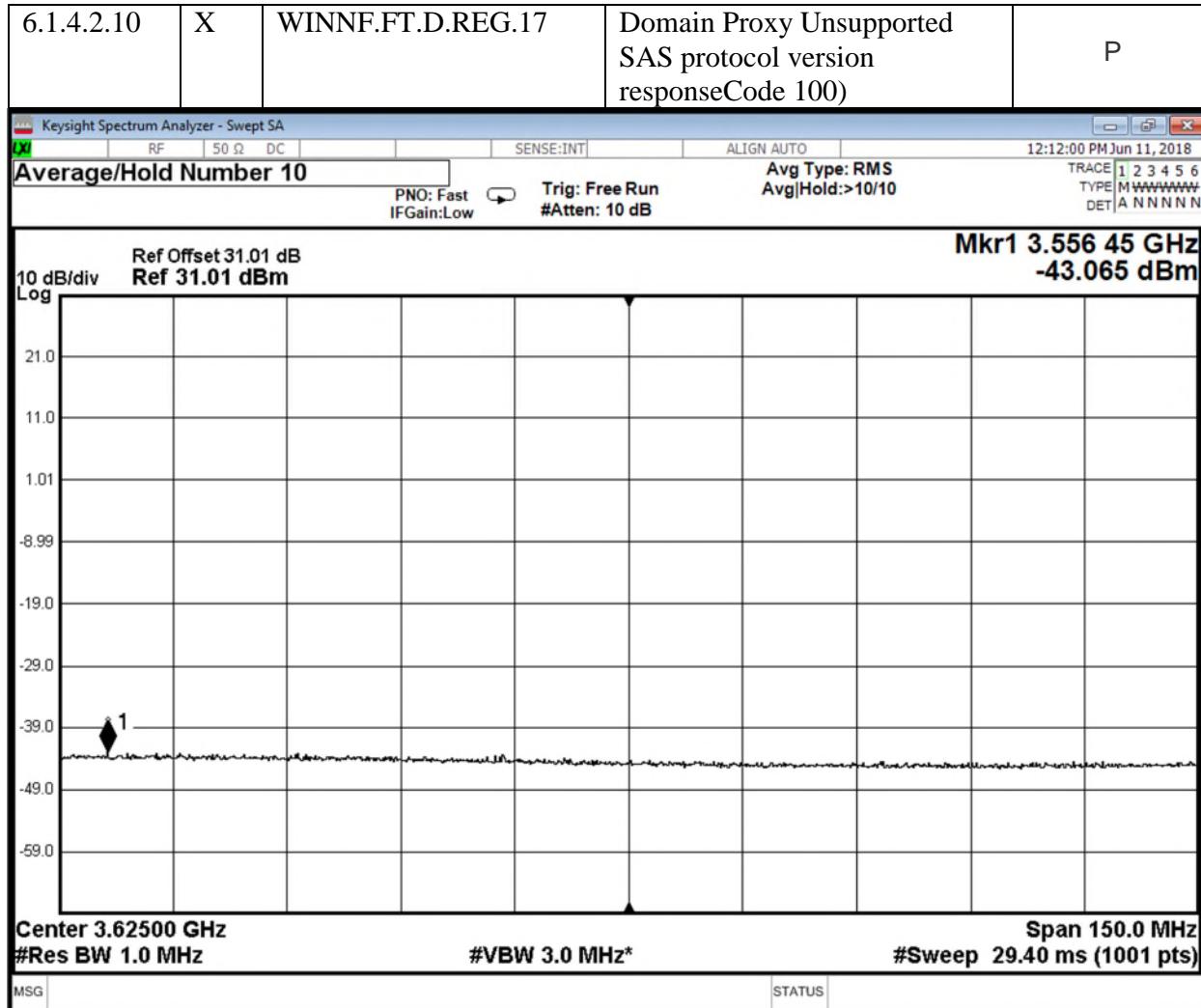
Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	



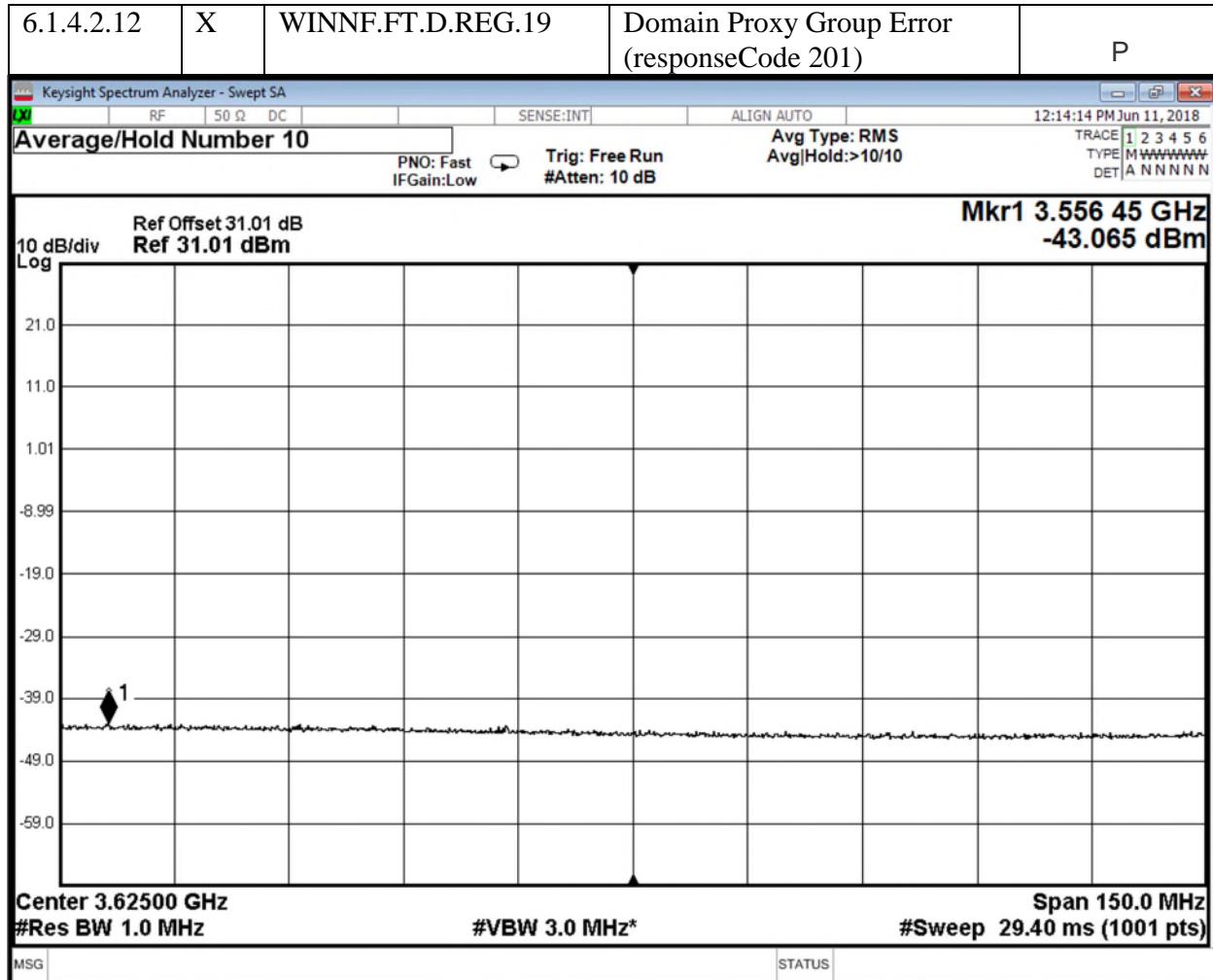
Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	



Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	



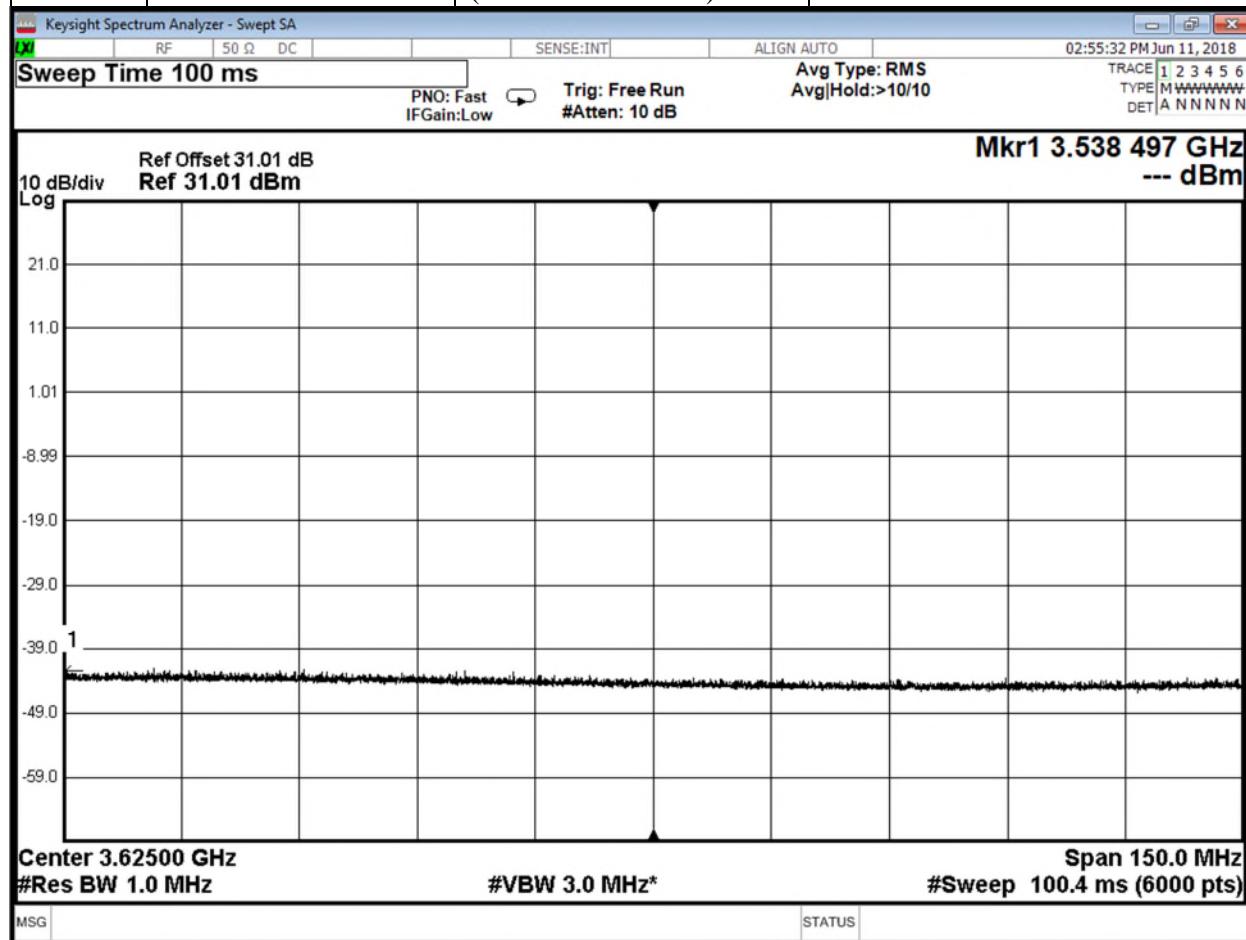
Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	



Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

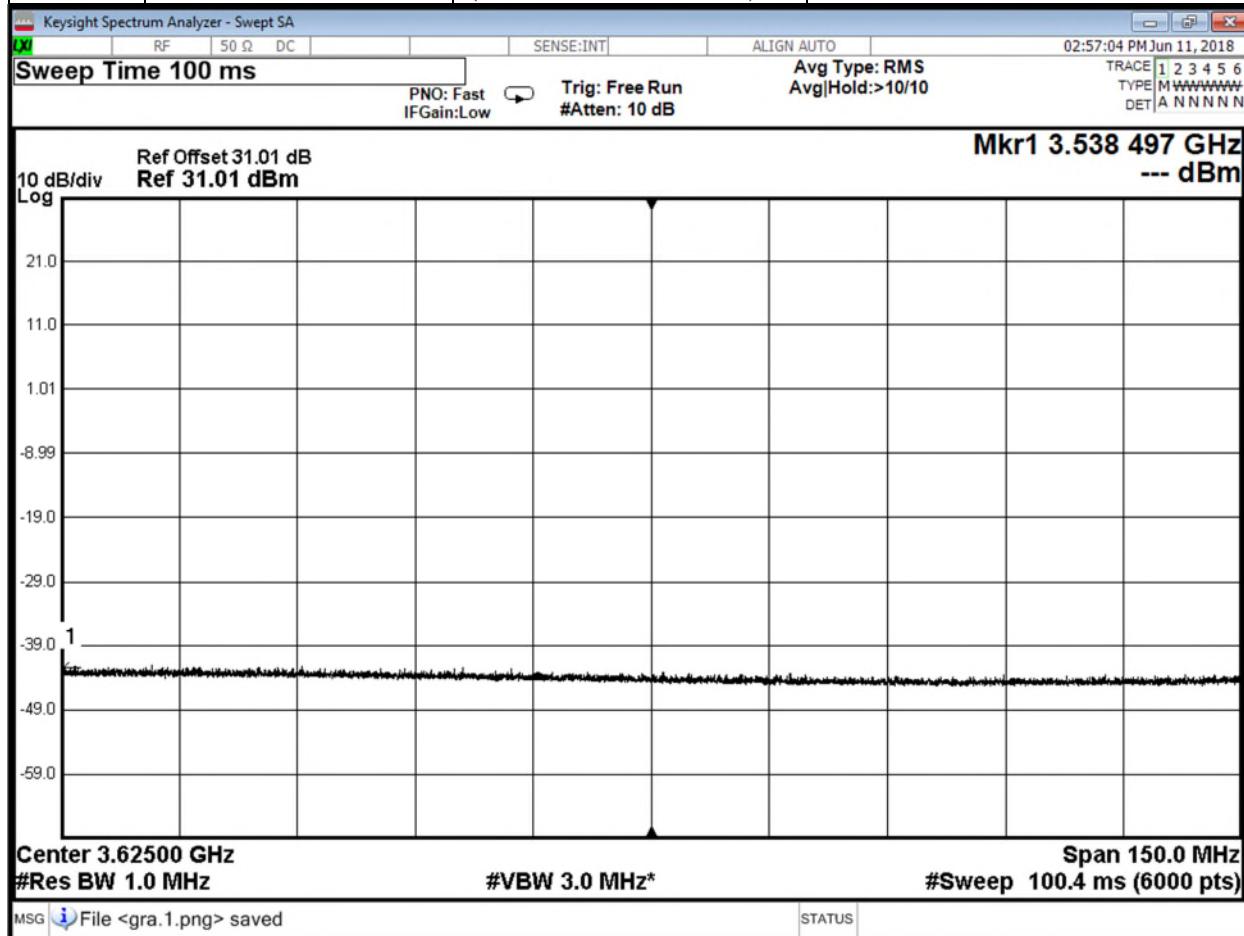
Check the device registration and authorization with the SAS, Confirm that the device changes its operating power and/or channel in response to a command from the SAS and Confirm that the device correctly configures based on the different license classes.

6.3.4.2.1	WINNF.FT.C.GRA.1	Unsuccessful Grant responseCode=400 (INTERFERENCE)	Monitor for 60 seconds after REG message sent. No transmission during test.	P
-----------	------------------	--	---	---



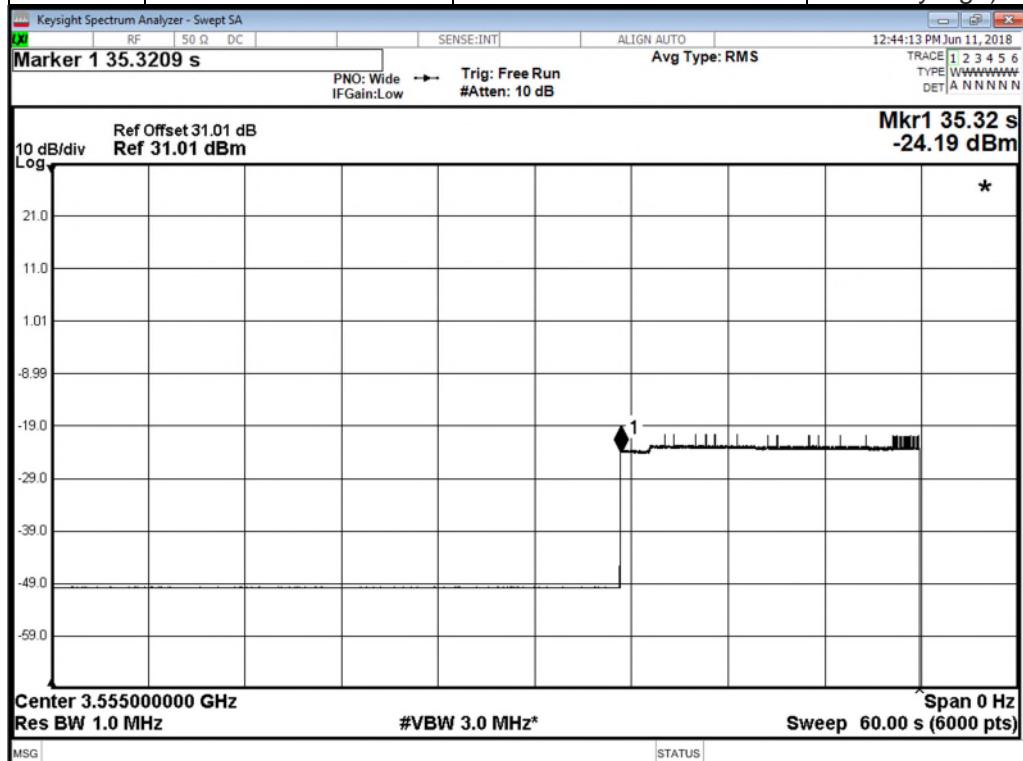
Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

6.3.4.2.2	WINNF.FT.C.GRA.2	Unsuccessful Grant responseCode=401 (GRANT_CONFLICT)	Monitor for 60 seconds after REG message sent. No transmission during test.	P
-----------	------------------	--	---	---



Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

6.4.4.1.2	WINNF.FT.D.HBT.2	Domain Proxy Heartbeat Success Case (first Heartbeat Response)	Monitor RF from start of test. Ensure that: <ul style="list-style-type: none"> Transmission does not start until time of first heartbeat response or after. After transmission starts, measure that transmission is within the granted channel (frequencyLow, frequencyHigh) 	P
-----------	------------------	--	--	---



From Test Harness Logs:	
eventTime (from logs)	Comment
16:43:52	first HBT.response sent at 2018-06-11T16:43:52.052Z

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

From Spectrum Analyzer Capture:						
Test	plot time [h:m:s]	sweep [s]	plot start time [h:m:s]	mrk [s]	event time [h:m:s]	eventTime UTC
HBT.2	12:44:13	54	12:43:19	35.35	12:43:54	16:43:54 ok

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

6.4.4.2.1	WINNF.FT.C.HBT.3	Heartbeat responseCode=105 (DREGISTER)	Monitor RF transmission. Ensure that: <ul style="list-style-type: none"> CBSD stops transmission within 60 seconds of the heartbeatResponse which contains responseCode = 105 	P
-----------	------------------	--	---	---

From Test Harness Logs:	
eventTime (from logs)	Comment
19:04:18	HBT.response with respCode=105 sent at: 2018-06-11T19:04:18.367Z

From Domain Proxy Logs:						
Test	plot time [h:m:s]	sweep [s]	plot start time [h:m:s]	mrk [s]	event time [h:m:s]	eventTime UTC
HBT.3			from DP logs (below)			19:04:23 ok -from DP

HBT.3

19:04:22,607 INFO [com.ericsson.oss.sas.handler.network.cm.CMHandler] (EJB timerService - 1) Set the CbrsTxExpireTime on the cell:

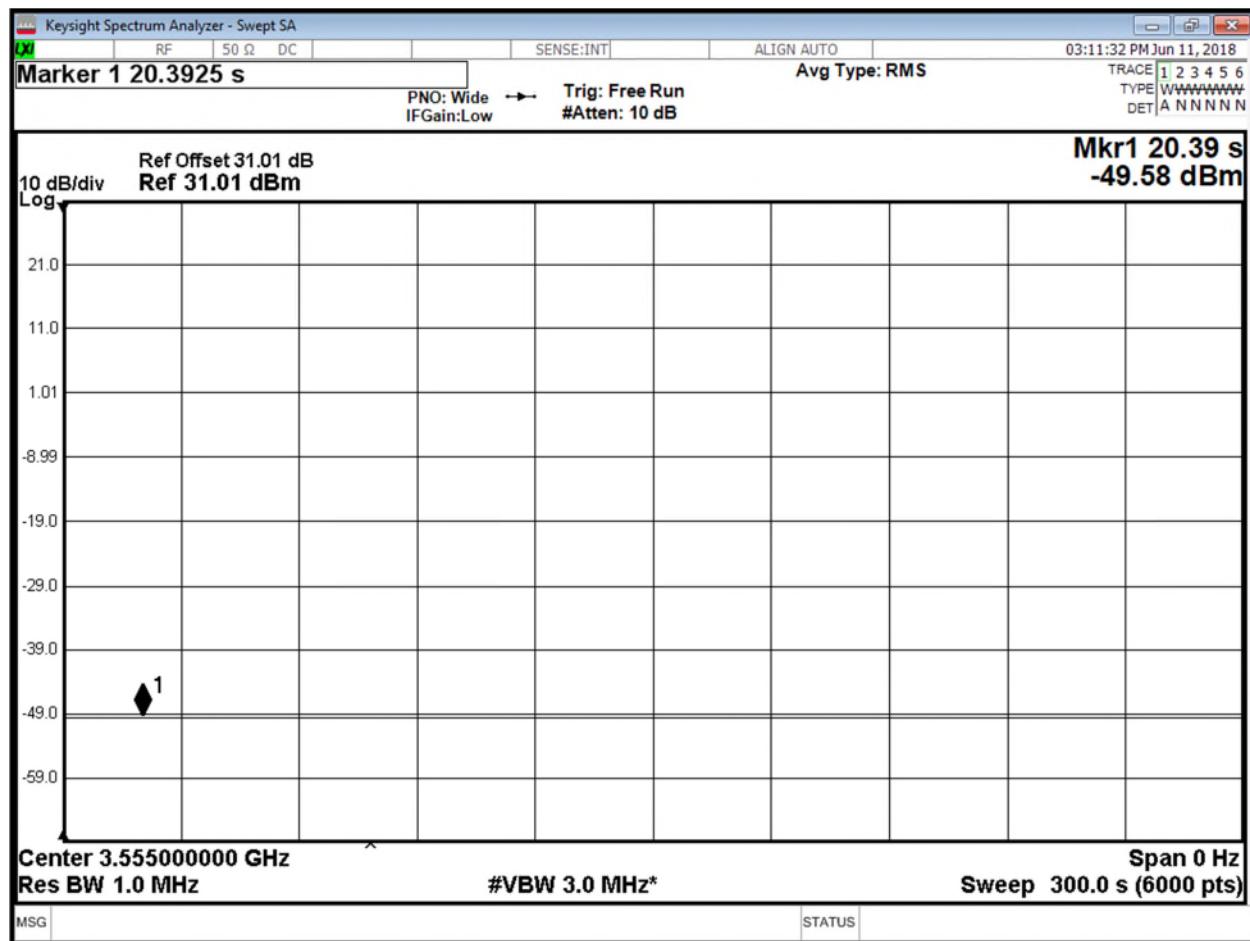
SubNetwork=G2RBS,ManagedElement=OTENB5311,ENodeBFunction=1,EUtranCellTDD=12 to: -1 in DPS. Time taken: 1749

19:04:24,627 INFO [com.ericsson.oss.sas.handler.network.cm.CMHandler] (EJB timerService - 7) Set the CbrsTxExpireTime on the cell:

SubNetwork=G2RBS,ManagedElement=OTENB5311,ENodeBFunction=1,EUtranCellTDD=12 to: -1 in DPS. Time taken: 1772

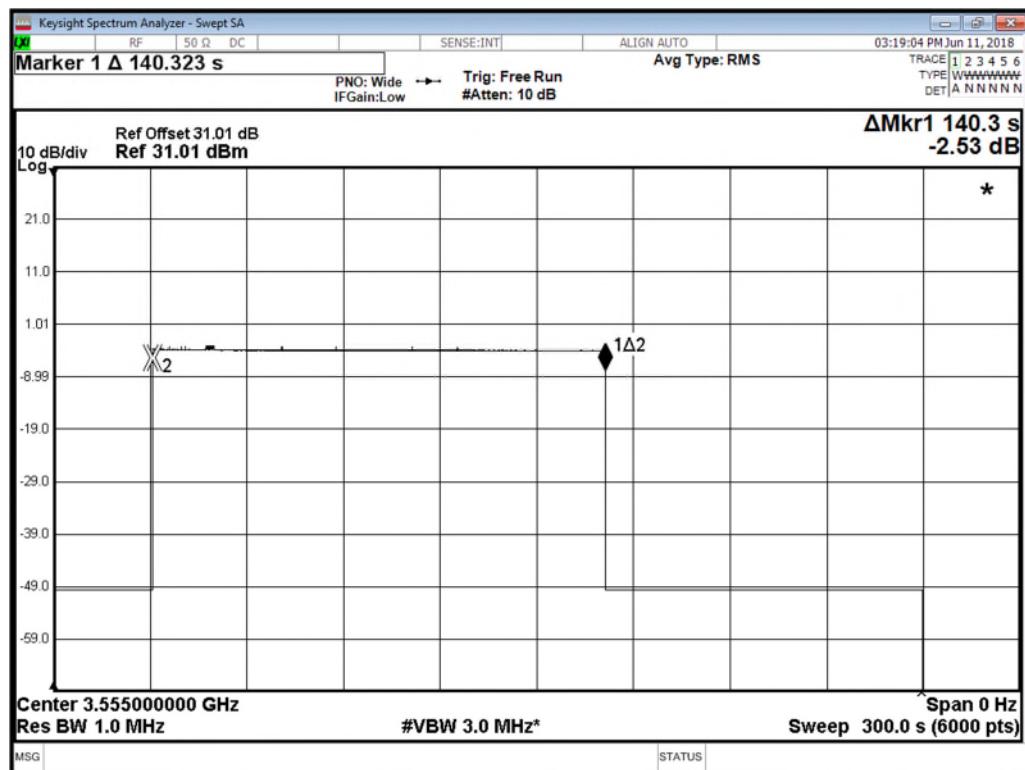
Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

6.4.4.2.3	WINNF.FT.C.HBT.5	Heartbeat responseCode=501 (SUSPENDED_GRANT) in First Heartbeat Response	Monitor RF transmission from start of test. Ensure there is no transmission during the test	p
-----------	------------------	--	---	---



Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

6.4.4.2.4	WINNF.FT.C.HBT.6	Heartbeat responseCode=501 (SUSPENDED_GRANT) in Subsequent Heartbeat Response	Monitor RF transmission. Ensure: <ul style="list-style-type: none"> CBSD stops transmission within 60 seconds of heartbeatResponse which contains responseCode=501 	p
-----------	------------------	---	--	---

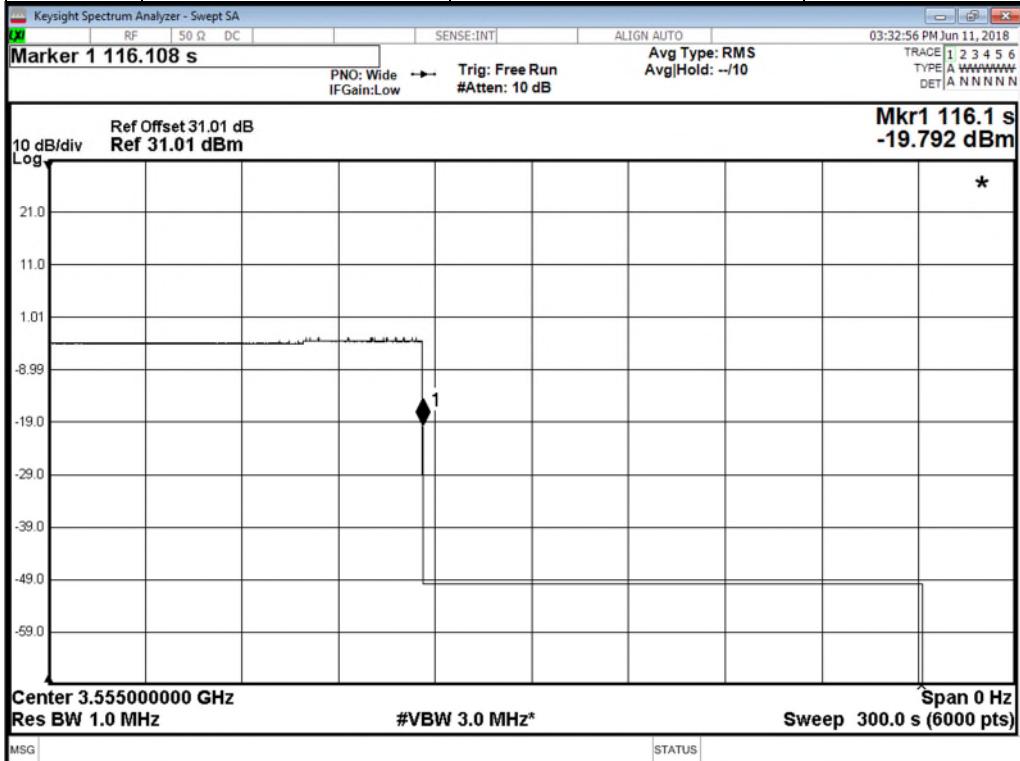


From Test Harness Logs:	
eventTime (from logs)	Comment
19:17:26	HBT.response with respCode=501 sent at: 2018-06-11T19:17:26.918Z

From Spectrum Analyzer Capture:						
Test	plot time [h:m:s]	sweep [s]	plot start time [h:m:s]	mrk [s]	event time [h:m:s]	eventTime UTC
HBT.6	15:19:04	270	15:14:34	174	15:17:28	19:17:28 ok

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

6.4.4.2.5	WINNF.FT.C.HBT.7	Heartbeat responseCode=502 (UNSYNC_OP_PARAM)	Monitor RF transmission. Ensure: <ul style="list-style-type: none">CBSD stops transmission within 60 seconds of heartbeatResponse which contains responseCode=502	p
-----------	------------------	---	--	---



From Test Harness Logs:

eventTime (from logs)	Comment
19:30:18	HBT.response with respCode=502 send at: 2018-06-11T19:30:17.235Z, RLQ.request sent at: 2018-06-11T19:30:18.609Z

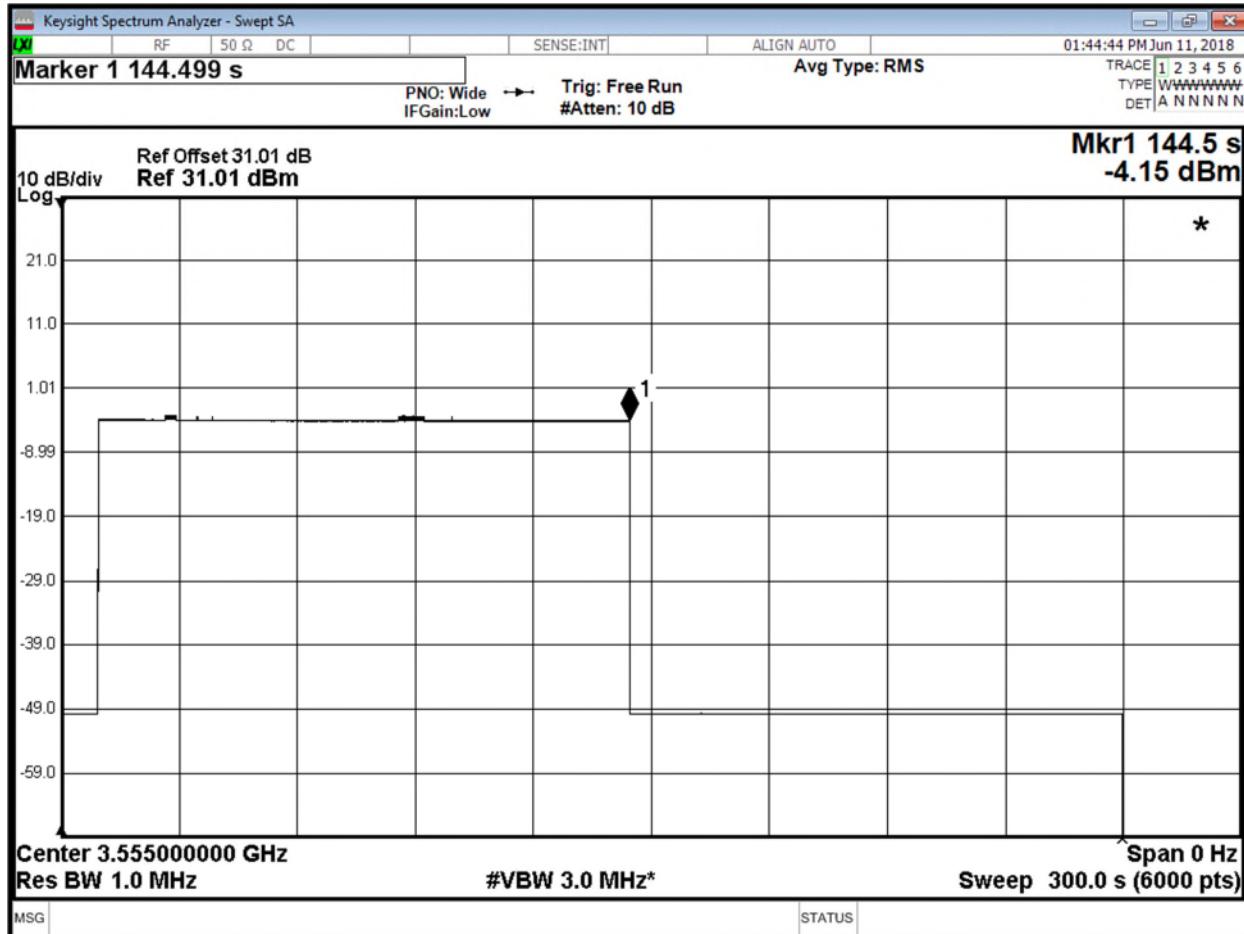
From Spectrum Analyzer Capture:

Test	plot time [h:m:s]	sweep [s]	plot start time [h:m:s]	mrk [s]	event time [h:m:s]	eventTime UTC
HBT.7	15:32:56	274.5	15:28:22	116.1	15:30:18	19:30:18 ok

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

6.4.4.2.6	--	X	WINNF.FT.D.H BT.8	Domain Proxy Heartbeat responseCode=500 (TERMINATED_GR ANT)	<p>Monitor RF transmission. CBSDs will have different behavior:</p> <ul style="list-style-type: none"> • CBSD1: will continue to transmit to end of test (this is not a pass/fail criteria, but check) • CBSD2: must stop transmission within 60 seconds of being sent heartbeatResponse with responseCode = 500 	P
-----------	----	---	----------------------	---	--	---

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

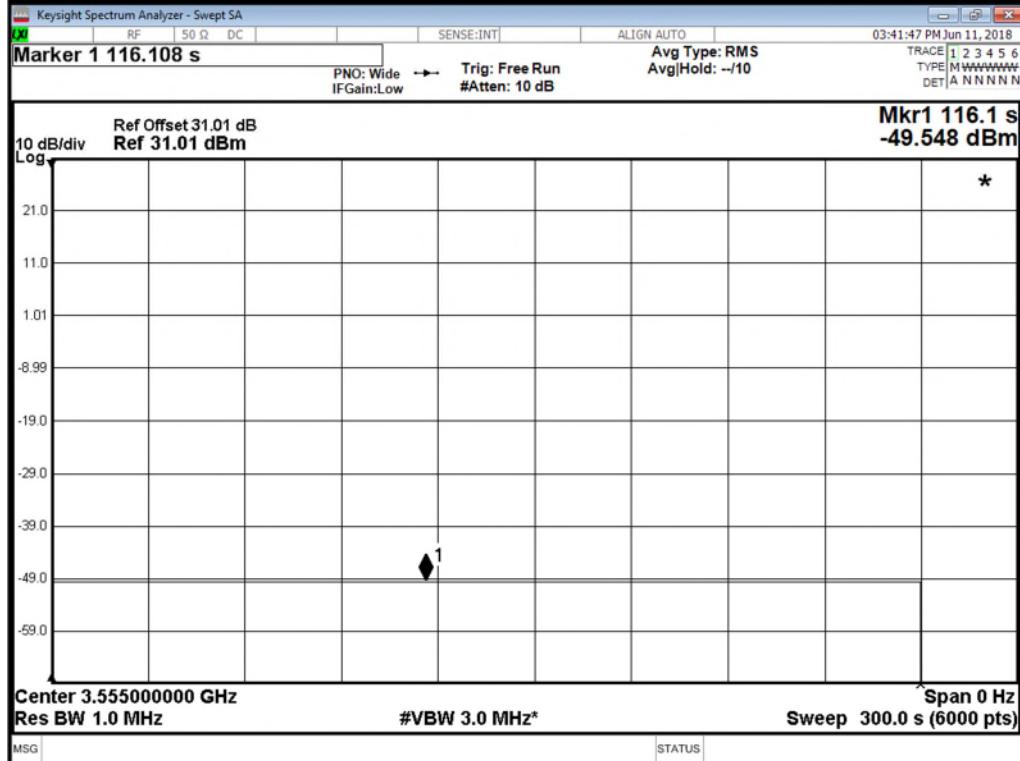


From Test Harness Logs:	
eventTime (from logs)	Comment
17:42:37	HBT.response with respCode= 500 sent at: 2018-06-11T17:42:37.559Z

From Spectrum Analyzer Capture:						
Test	plot time [h:m:s]	sweep [s]	plot start time [h:m:s]	mrk [s]	event time [h:m:s]	eventTime UTC
HBT.8	13:44:44	270	13:40:14	144.5	13:42:38	17:42:38 ok

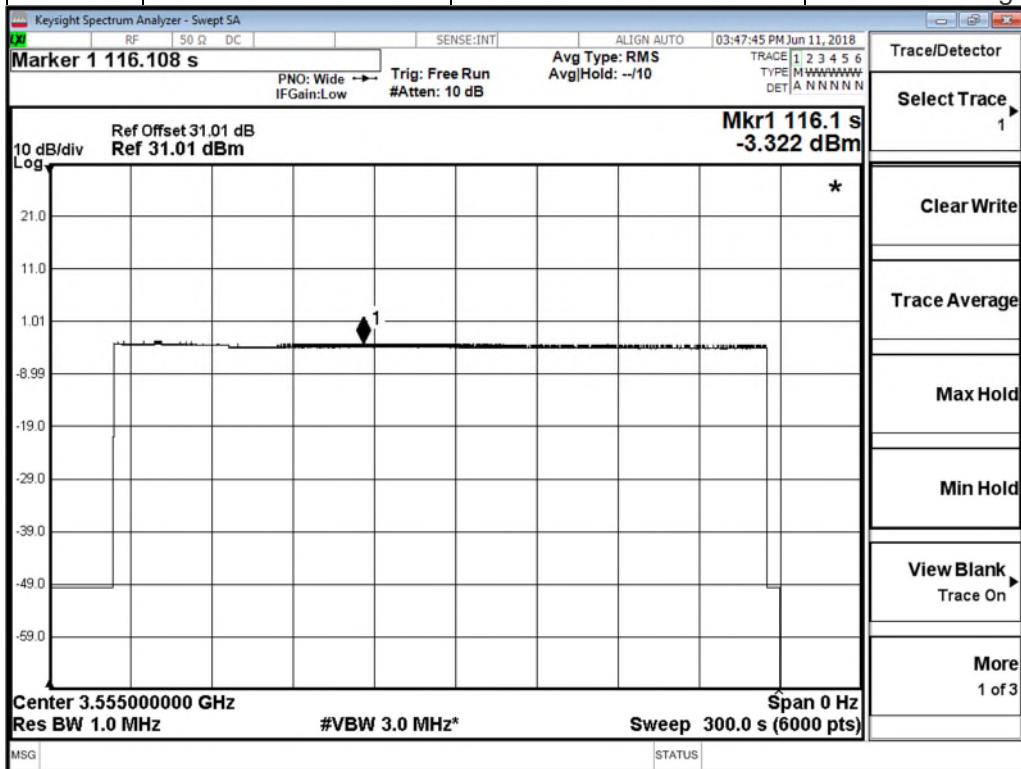
Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

6.4.4.3.1	WINNF.FT.C.HBT.9	Heartbeat Response Absent (First Heartbeat)	Monitor RF from start of test to 60 seconds after last heartbeatResponse message was sent. CBSD should not transmit at any time during test	P
-----------	------------------	--	---	---



Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

6.4.4.3.2	WINNF.FT.C.HBT.10	Heartbeat Response Absent (Subsequent Heartbeat)	Monitor RF transmission. Verify: • CBSD must stop transmission within transmitExpireTime+60 seconds, where transmitExpireTime is from last successful heartbeatResponse message	P
-----------	-------------------	--	---	---



From Test Harness Logs:

eventTime (from logs)	Comment
19:47:41	Last HBT.response that set TxExpire time @ 2018-06-11T19:44:21.647Z, transmitExpireTime = 2018-06-11T19:47:41Z

From Spectrum Analyzer Capture:

Test	plot time [h:m:s]	sweep [s]	plot start time [h:m:s]	mrk [s]	event time [h:m:s]	eventTime UTC
HBT.10	15:47:45	270	15:43:15	240	15:47:15	19:47:15 ok

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

6.5.4.2.2	WINNF.FT.D.MES.2	Domain Proxy Registration Response contains measReportConfig	No RF monitoring	P
-----------	------------------	---	------------------	---

Pass saw "measreportconfig" in logs

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

6.5.4.2.3	WINNF.FT.C.MES.3	Grant Response contains measReportConfig	No RF monitoring	P
-----------	------------------	---	------------------	---

Pass saw “measreportconfig” in logs

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

6.5.4.2.5	WINNF.FT.D.MES.5	Domain Proxy Heartbeat Response contains measReportConfig	No RF monitoring	P
-----------	------------------	---	------------------	---

Pass saw "measreportconfig" in logs

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

6.6.4.1. 2	WINNF.FT.D.RLQ.2	Domain Proxy Successful Relinquishment	Monitor RF transmission. Ensure: • CBSD stops transmission at any time prior to sending the relinquishmentRequest message.	P
---------------	------------------	---	---	---

From Test Harness Logs:

eventTime (from logs)	Comment
17:57:46	RLQ.request sent at: 2018-06-11T17:57:46.023Z

From Spectrum Analyzer Capture:

Test	plot time [h:m:s]	sweep [s]	plot start time [h:m:s]	mrk [s]	event time [h:m:s]	eventTime UTC	
RLQ.2			from DP logs (below)			17:57:44	ok from DP log

RLQ.2:

17:57:42,792 INFO [com.ericsson.oss.sas.handler.network.cm.CMHandler] (EJB timerService - 5) Set the CbrsTxExpireTime on the cell:

SubNetwork=G2RBS,ManagedElement=OTENB5311,ENodeBFunction=1,EUtranCellTDD=12 to: -1 in DPS. Time taken: 1765

17:57:44,607 INFO [com.ericsson.oss.sas.handler.network.cm.CMHandler] (EJB timerService - 5) Set the CbrsTxExpireTime on the cell:

SubNetwork=G2RBS,ManagedElement=OTENB5311,ENodeBFunction=1,EUtranCellTDD=14 to: -1 in DPS. Time taken: 1796

Note: shutdown time taken from Domain Proxy logs, and shutdown confirmed by RF monitoring.

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

6.7.4.1.2	WINNF.FT.D.DRG.2	Domain Proxy Successful Deregistration	Monitor RF transmission. Ensure: • CBSD stops transmission at any time prior to sending the relinquishmentRequest message or deregistrationRequest message (whichever is sent first)	P
-----------	------------------	--	---	---

From Test Harness Logs:	
eventTime (from logs)	Comment
18:13:38	RLQ.request sent at: 2018-06-11T18:13:38.532Z, DRG.request sent at: 2018-06-11T18:13:40.598Z

From Spectrum Analyzer Capture:						
Test	plot time [h:m:s]	sweep [s]	plot start time [h:m:s]	mrk [s]	event time [h:m:s]	eventTime UTC
DRG.2			from DP logs (below)			18:13:37 ok from DP

DRG.2

18:13:34,794 INFO [com.ericsson.oss.sas.handler.network.cm.CMHandler] (EJB timerService - 6) Set the CbrsTxExpireTime on the cell:

SubNetwork=G2RBS,ManagedElement=OTENB5311,ENodeBFunction=1,EUtranCellTDD=12 to: -1 in DPS. Time taken: 1768

18:13:36,565 INFO [com.ericsson.oss.sas.handler.network.cm.CMHandler] (EJB timerService - 6) Set the CbrsTxExpireTime on the cell:

SubNetwork=G2RBS,ManagedElement=OTENB5311,ENodeBFunction=1,EUtranCellTDD=14 to: -1 in DPS. Time taken: 1753

Note: shutdown time taken from Domain Proxy logs, and shutdown confirmed by RF monitoring.

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Confirm that the device transmits at a power level less than or equal to the maximum power level approved by the SAS.

7.1.4.1.1	X	X	WINNF.PT.C.H BT	UUT RF Transmit Power Measurement	Power Spectral Density test case. Assume we use 1 carrier bandwidth (say, 5 or 10 MHz), one frequency (say middle channel in band) for test. Measure at max transmit power, and reduce in steps of 3 dB to minimum declared transmit power.	P
-----------	---	---	-----------------	-----------------------------------	--	---

Information from grantRequest				
	lowFrequency	highFrequency	maxEirp	Grant Center Freq
Log file name	[MHz]	[MHz]	[dBm/MHz]	[MHz]
PowerMeasTest_2018-06-11T14.15.51Z	3625	3635	13.7	3630
PowerMeasTest_2018-06-11T14.43.18Z	3625	3635	7.679400087	3630
PowerMeasTest_2018-06-11T15.03.45Z	3550	3560	13.7	3555
PowerMeasTest_2018-06-11T14.54.15Z	3550	3560	7.679400087	3555
PowerMeasTest_2018-06-11T15.14.15Z	3690	3700	13.7	3695
PowerMeasTest_2018-06-11T15.20.57Z	3690	3700	7.679400087	3695

Information from Measurement plots

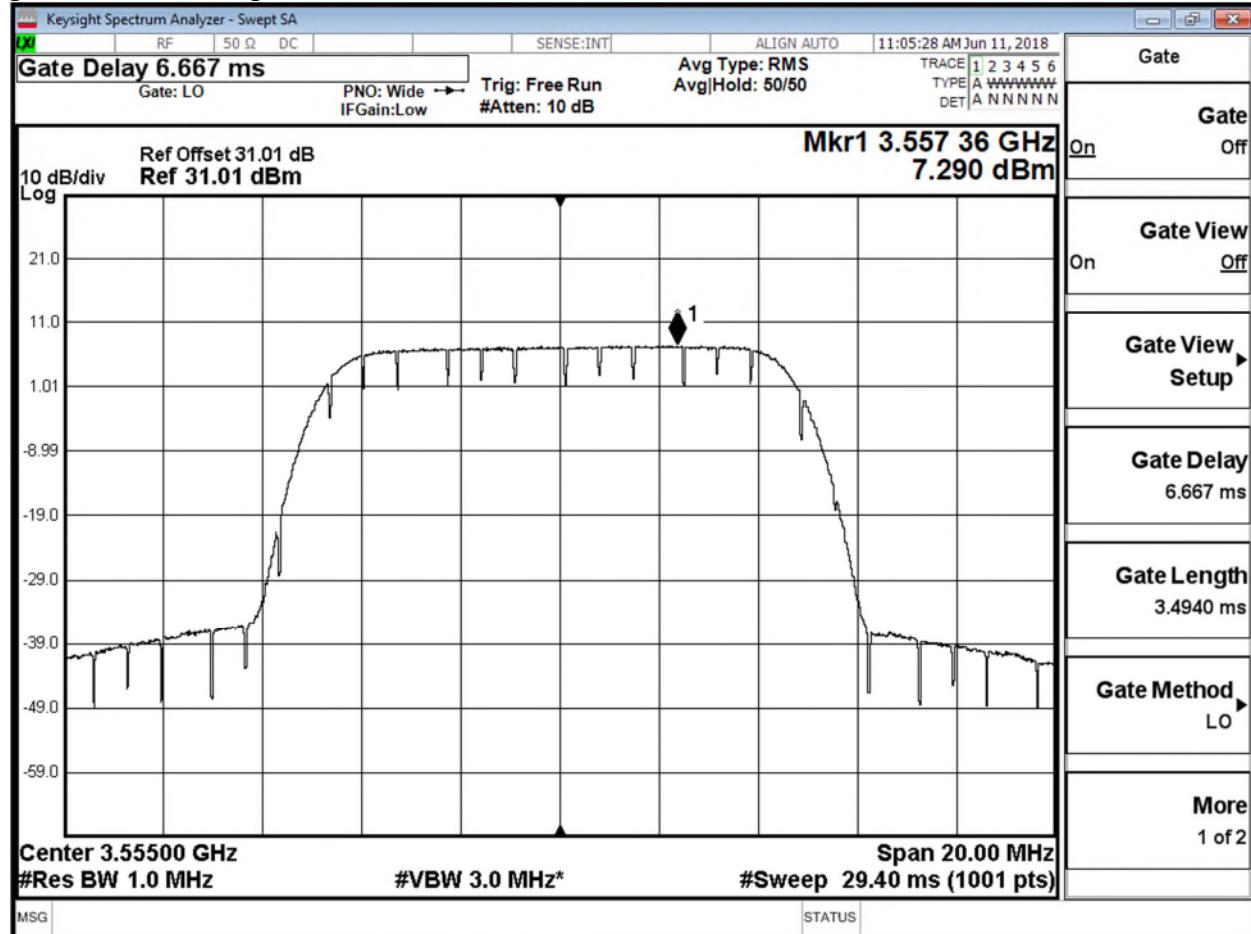
Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

plot name	Plot time		Center Freq [MHz]	single port, conducted PSD [dBm/MHz]	total PSD EIRP, measured [dBm/MHz]	Margin [dB]
	local	UTC				
psd low chan_low power 13.7	11:05:28	15:05:28	3555	7.29	13.39	0.3
psd low chan_low power 7.7						
dBm_10MHz.png	10:58:45	14:58:45	3555	0.756	6.856	0.8
psd mid chan high power 13.7	10:24:43	14:24:43	3630	6.418	12.518	1.2
psd mid chan low power 7.7	10:48:08	14:48:08	3630	0.184	6.284	1.4
psd high chan_high_power 13.7_10MHz.png	11:17:06	15:17:06	3695	5.403	11.503	2.2
psd high chan_high_power 7.7_10MHz	11:26:26	15:26:26	3695	-0.698	5.402	2.3

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



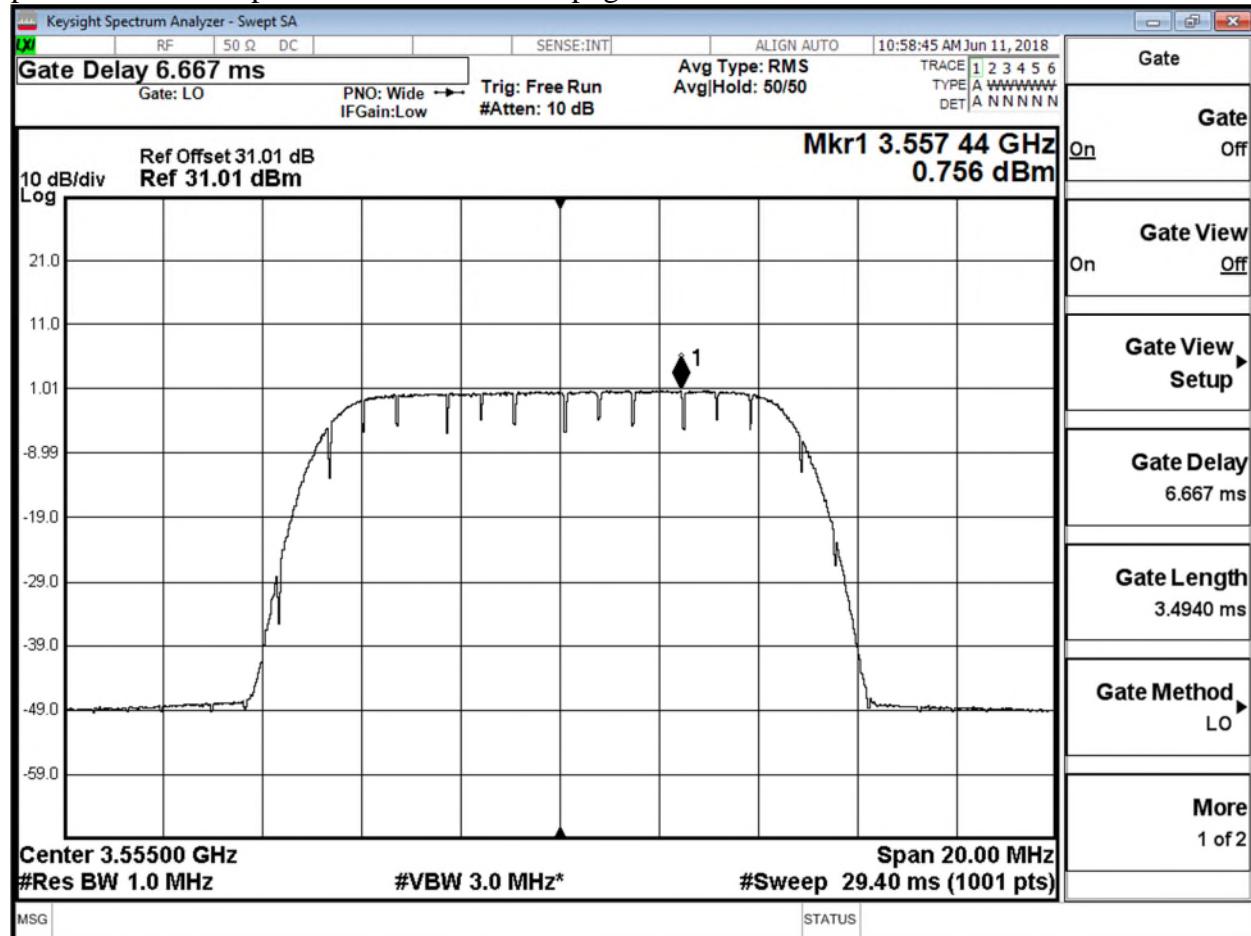
psd low chan_low power 13.7



Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



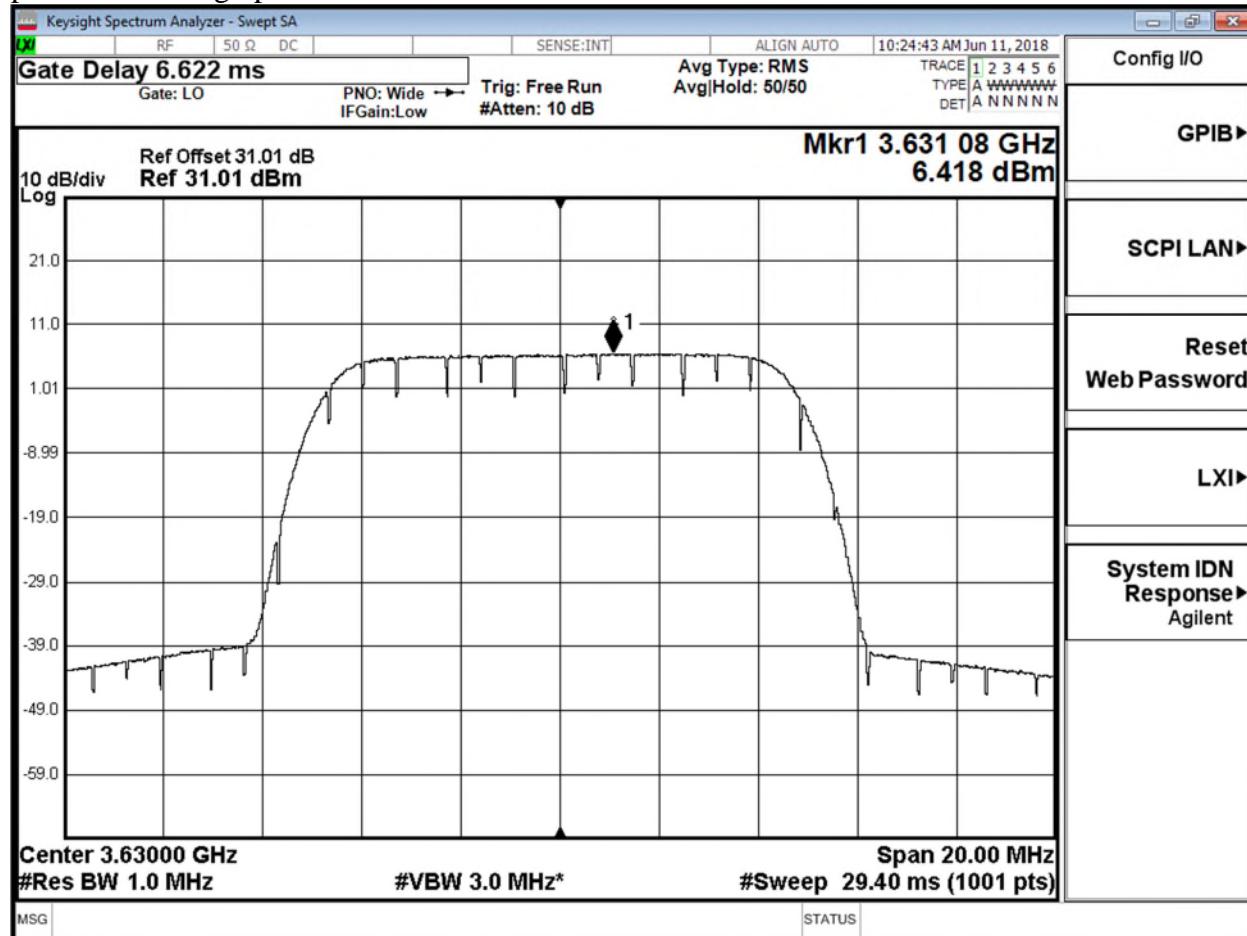
psd low chan_low power 7.7 dBm_10MHz.png



Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



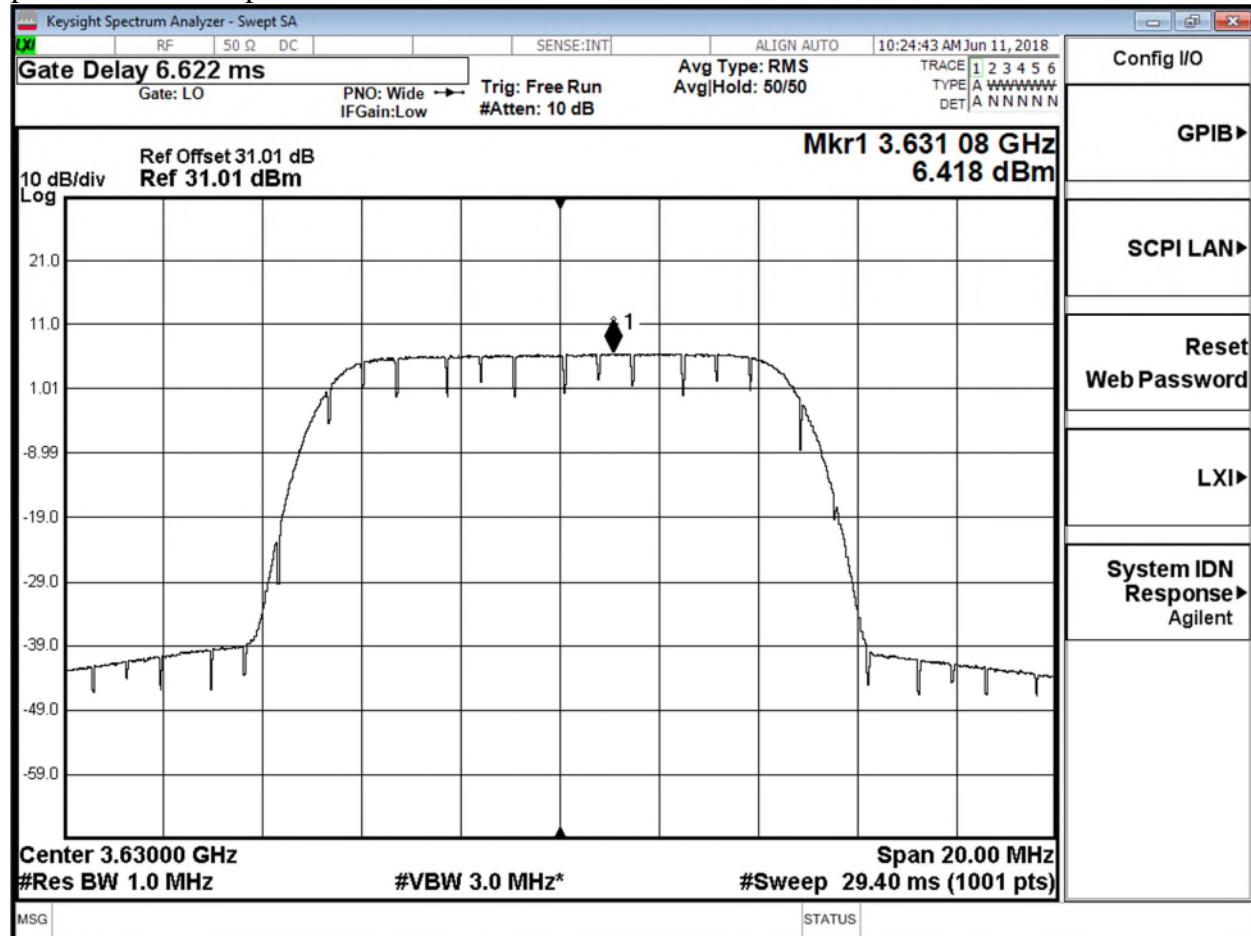
psd mid chan high power 13.7



Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)

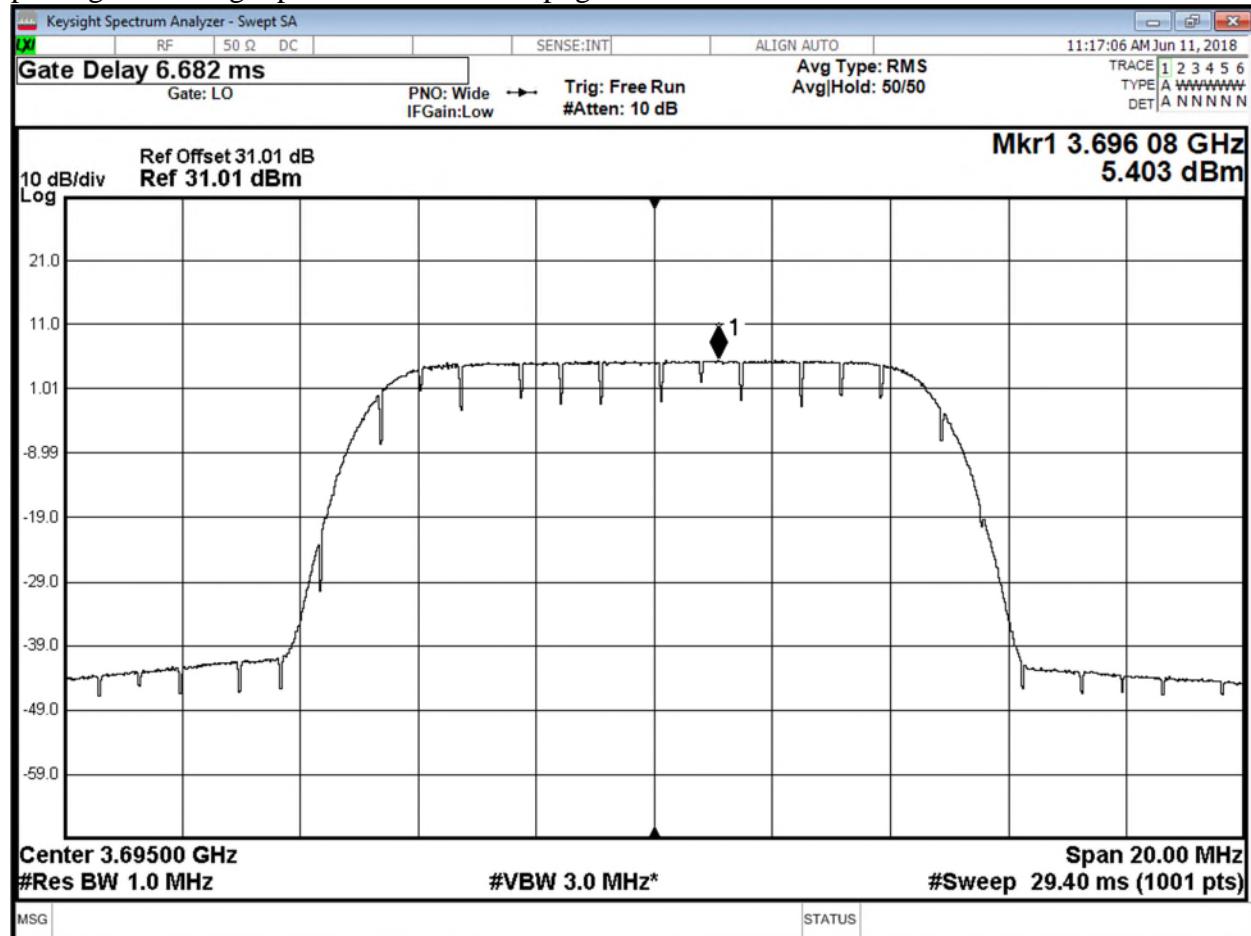


psd mid chan low power 7.7



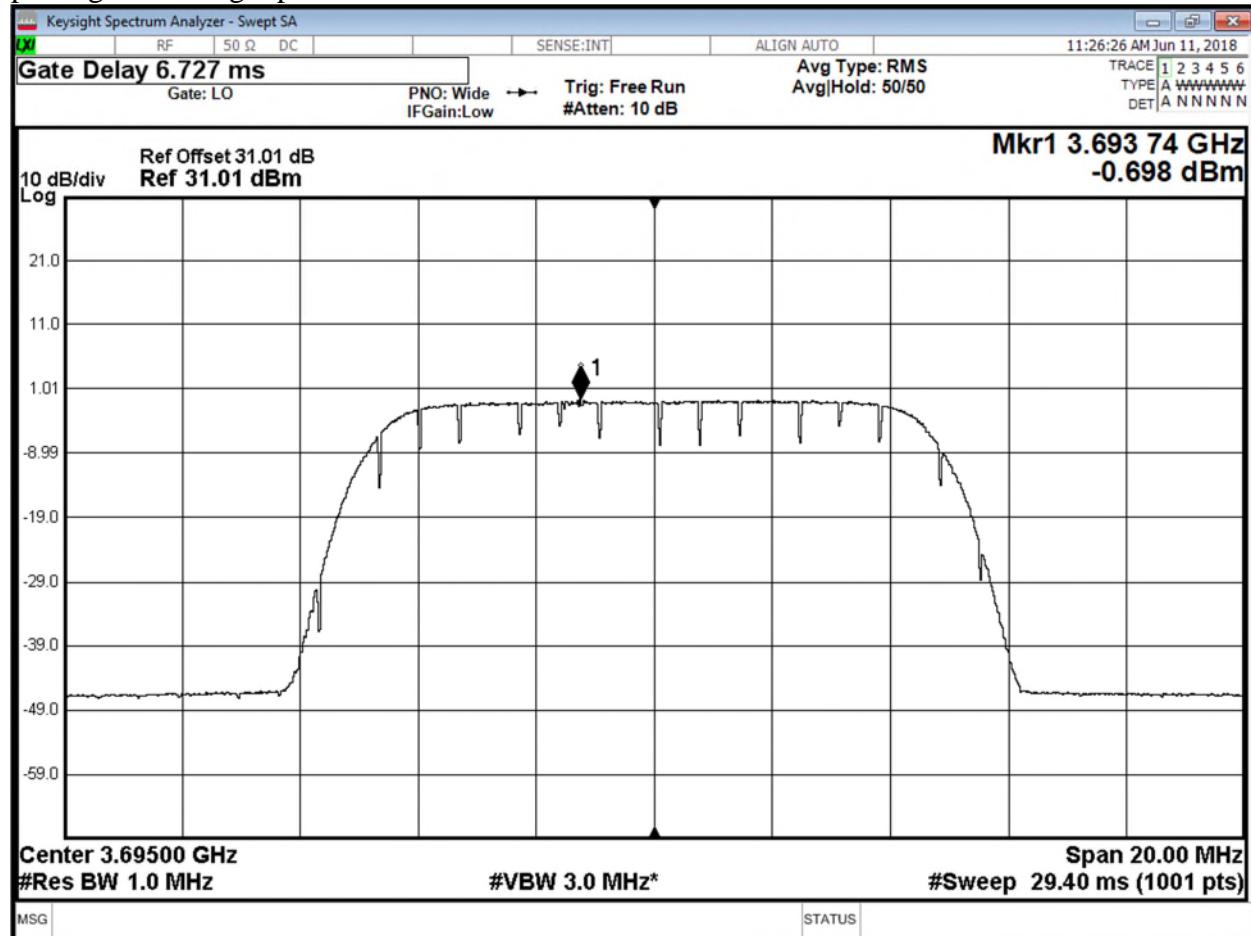
Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

psd high chan_high_power 13.7_10MHz.png



Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

psd high chan_high_power 7.7_10MHz



Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)

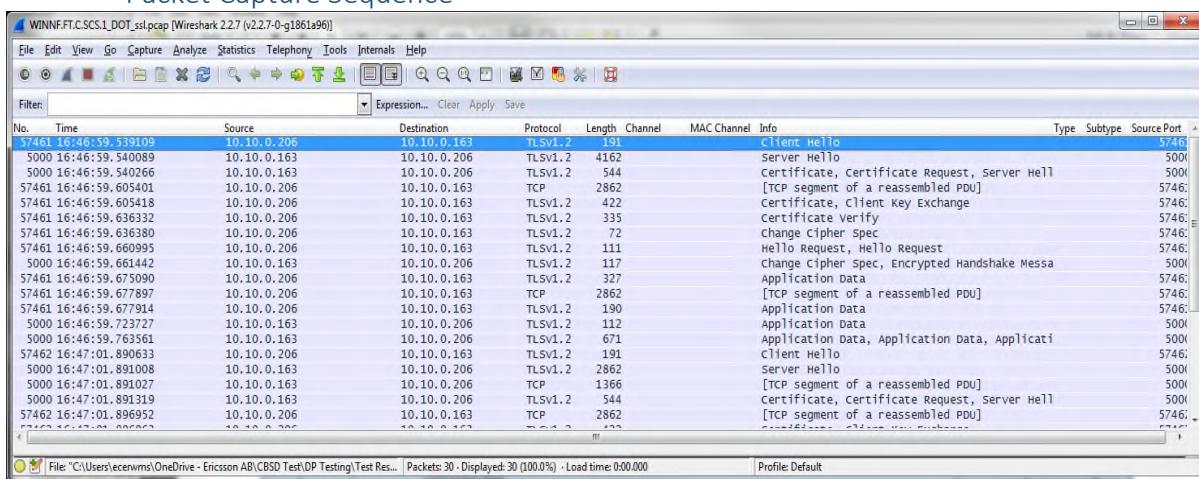


DOT CBRS Radio: WINNF / Security Test Case Analysis

WINNF Security Test Case Analysis

WINNF.FT.C.SCS.1

Packet Capture Sequence



WINNF test requirements:

WINNF test requirements from WINNF-TS-0122-V1.0.0 CBRS CBSD Test Specification:

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

2	<ul style="list-style-type: none"> • 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, <ul style="list-style-type: none"> • <u>TLS_RSA_WITH_AES_128_GCM_SHA256</u> • <u>TLS_RSA_WITH_AES_256_GCM_SHA384</u> • <u>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</u> • <u>TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384</u> • <u>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</u> 	PASS	FAIL

Analysis of WINNF Test Requirements

1. From Client Hello: TLS version = TLS 1.2

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



57461 16:46:59.539109 10.10.0.206 10.10.0.163 TLSv1.2 191 Client Hello 57461

Frame 1: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits)
 Ethernet II, src: fa:16:3e:56:06:a3 (fa:16:3e:56:06:a3), Dst: fa:16:3e:b1:8d:79 (fa:16:3e:b1:8d:79)
 Internet Protocol Version 4, Src: 10.10.0.206, Dst: 10.10.0.163
 Transmission Control Protocol, Src Port: 57461, Dst Port: 5000, Seq: 1, Ack: 1, Len: 125
 Secure Sockets Layer
 TLSv1.2 Record Layer: Handshake Protocol: client Hello
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 120
 Handshake Protocol: client Hello
 Handshake Type: Client Hello (1)
 Length: 116
 Version: TLS 1.2 (0x0303)
 Random
 Session ID Length: 0
 Cipher Suites Length: 6
 Cipher Suites (3 suites)
 Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
 Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
 Compression Methods Length: 1
 Compression Methods (1 method)
 Extensions Length: 69
 Extension: elliptic_curves
 Extension: ec_point_formats
 Extension: signature_algorithms
 Extension: renegotiation_info

```

0040  ac 00 16 03 03 00 78 01 00 00 74 03 03 5b 1e df  ...x. .t..[. .
0050  c3 b2 0c 4e 57 29 19 11 7e f8 21 6f 3f 97 ae 81  ...NW).. ~.!?...
0060  01 db 73 1e 88 1f 19 ef 7d d5 83 25 b7 00 00 06  ...s.... ].%. ...
0070  00 9c c0 2b c0 2f 01 00 00 45 00 0a 00 16 00 14  ...+./... .E.....
0080  00 17 00 18 00 19 00 09 00 0a 00 0b 00 0c 00 0d  .....
0090  00 00 00 16 00 00 00 01 00 00 0d 00 15 00 17

```

2. Cipher suite list from Client Hello is from WINNF approved list:

TLS_RSA_WITH_AES_128_GCM_SHA25
 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



```

57461 16:46:59.539109 10.10.0.206 10.10.0.163 TLSv1.2 191 Client Hello 57461
Frame 1: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits)
Ethernet II, Src: fa:16:3e:56:06:a3 (fa:16:3e:56:06:a3), Dst: fa:16:3e:b1:8d:79 (fa:16:3e:b1:8d:79)
Internet Protocol Version 4, Src: 10.10.0.206, Dst: 10.10.0.163
Transmission Control Protocol, Src Port: 57461, Dst Port: 5000, Seq: 1, Ack: 1, Len: 125
Secure Sockets Layer
  TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 120
    Handshake Protocol: client Hello
      Handshake Type: Client Hello (1)
      Length: 116
      Version: TLS 1.2 (0x0303)
      Random
        Session ID Length: 0
        Cipher Suites Length: 6
      Cipher Suites (3 suites)
        Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
        Compression Methods Length: 1
        Compression Methods (1 method)
        Extensions Length: 69
        Extension: elliptic_curves
        Extension: ec_point_formats
        Extension: signature_algorithms
        Extension: renegotiation_info

0070 00 9c c0 2b c0 2f 01 00 00 45 00 0a 00 16 00 14  ....+./... .E.....
0080 00 17 00 18 00 19 00 09 00 0a 00 0b 00 0c 00 0d  .....
0090 00 0e 00 16 00 0b 00 02 01 00 00 0d 00 1c 00 1a  .....
00a0 06 03 06 01 05 03 05 01 04 03 04 01 04 02 03 03  .....
00b0 03 01 03 02 02 03 02 01 02 02 ff 01 00 01 00  .....


```

3. Cipher suite chosen (from Server Hello):
TLS_RSA_WITH_AES_128_GCM_SHA256

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



5000 16:46:59.540089 10.10.0.163 10.10.0.206 TLSv1.2 4162 Server Hello 5000

Frame 2: 4162 bytes on wire (33296 bits), 4162 bytes captured (33296 bits)

Ethernet II, Src: fa:16:3e:b1:8d:79 (fa:16:3e:b1:8d:79), Dst: fa:16:3e:56:06:a3 (fa:16:3e:56:06:a3)

Internet Protocol Version 4, Src: 10.10.0.163, Dst: 10.10.0.206

Transmission Control Protocol, Src Port: 5000, Dst Port: 57461, Seq: 1, Ack: 126, Len: 4096

Secure Sockets Layer

- TLsv1.2 Record Layer: Handshake Protocol: Server Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 81
- Handshake Protocol: Server Hello
 - Handshake Type: Server Hello (2)
 - Length: 77
 - Version: TLS 1.2 (0x0303)
- Random
 - Session ID Length: 32
 - Session ID: eaebce6fc96739bb35f7769118a4c71f98f00b97a9001c06...
- Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- Compression Method: null (0)
- Extensions Length: 5
- Extension: renegotiation_info

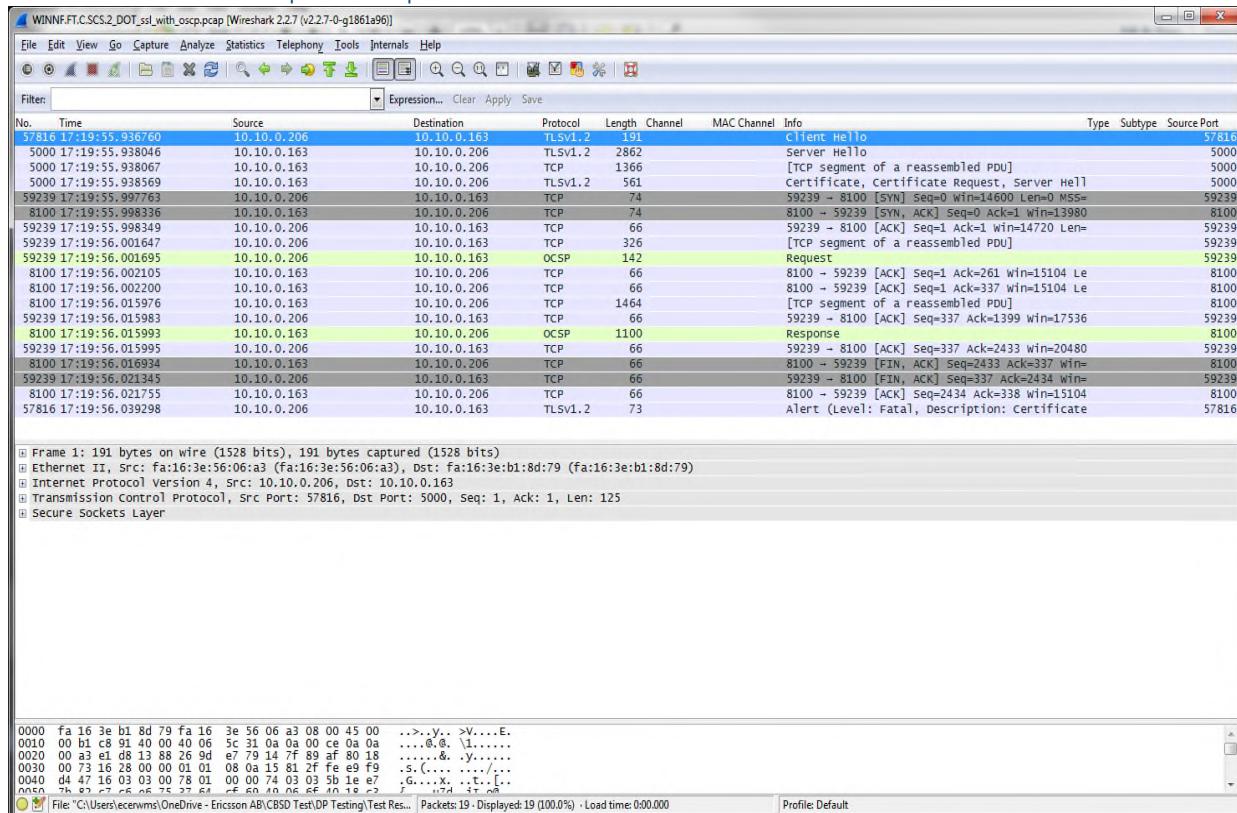
0080 0b 97 a9 00 1c 06 8c 07 0c 28 eb 28 e8 eb 00 9c(.(...
0090 00 00 05 ff 01 00 01 00 16 03 03 11 4e 0b 00 11N...
00a0 4a 00 11 47 00 05 81 30 82 05 7d 30 82 03 65 a0 J..G...0 ..}0..e.
00b0 03 02 01 02 02 09 00 be 97 89 d1 60 22 5b da 30".[.0
00c0 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00 30 72 ...*.H..Or
00d0 31 0b 30 00 05 03 ee 04 06 13 02 ee e3 31 10 20 1 0 .. 0001 0

4. The Registration request message arrived at the Test Harness, so authentication was completed.

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

WINNF.FT.C.SCS.2

Packet Capture Sequence



WINNF Test Requirements:

WINNF test requirements from WINNF-TS-0122-V1.0.0 CBRS CBSD Test Specification:

2	<ul style="list-style-type: none"> 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
---	--	------	------

Analysis of WINNF Test Requirements

- From Client Hello can read: TLS version = TLS 1.2

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



```

57816 17:19:55.936760 10.10.0.206 10.10.0.163 TLSv1.2 191 Client Hello 57816
Frame 6607: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits)
Ethernet II, src: fa:16:3e:56:06:a3 (fa:16:3e:56:06:a3), Dst: fa:16:3e:b1:8d:79 (fa:16:3e:b1:8d:79)
Internet Protocol Version 4, Src: 10.10.0.206, Dst: 10.10.0.163
Transmission Control Protocol, Src Port: 57816, Dst Port: 5000, Seq: 1, Ack: 1, Len: 125
Secure Sockets Layer
  TLSv1.2 Record Layer: Handshake Protocol: client Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 120
    Handshake Protocol: Client Hello
      Handshake Type: client Hello (1)
      Length: 116
      Version: TLS 1.2 (0x0303)
      Random
        Session ID Length: 0
        Cipher Suites Length: 6
      Cipher Suites (3 suites)
        Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
      Compression Methods Length: 1
      Compression Methods (1 method)
      Extensions Length: 69
      Extension: elliptic_curves
0040 d4 47 16 03 03 00 78 01 00 00 74 03 03 5b 1e e7 .G. ....x. ....t..[..
0050 7b 82 c7 c6 e6 75 37 64 cf 69 49 06 6f 40 18 c3 {....u7d. ....i1.o8.
0060 6e fe 03 b0 44 6c be fe 0f 03 d1 47 d1 00 00 06 n....D]. ....G....
0070 00 9c c0 2b c0 2f 00 00 00 45 00 0a 00 16 00 14 ....+./....E.....
0080 00 17 00 18 00 19 00 09 00 0a 00 0b 00 0c 00 0d .....
0090 00 00 16 00 0b 00 07 01 00 00 0d 00 1c 00 13 .....

```

2. From Client Hello, cipher suite list is from WINNF approved list:

TLS_RSA_WITH_AES_128_GCM_SHA25
 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



```

57816 17:19:55.936760 10.10.0.206 10.10.0.163 TLSv1.2 191 Client Hello 57816
Frame 6607: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits)
Ethernet II, src: fa:16:3e:56:06:a3 (fa:16:3e:56:06:a3), Dst: fa:16:3e:b1:8d:79 (fa:16:3e:b1:8d:79)
Internet Protocol Version 4, Src: 10.10.0.206, Dst: 10.10.0.163
Transmission Control Protocol, Src Port: 57816, Dst Port: 5000, Seq: 1, Ack: 1, Len: 125
Secure Sockets Layer
  TLSv1.2 Record Layer: Handshake Protocol: client Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 120
    Handshake Protocol: Client Hello
      Handshake Type: client Hello (1)
      Length: 116
      Version: TLS 1.2 (0x0303)
      Random
        Session ID Length: 0
        Cipher Suites Length: 6
      Cipher Suites (3 suites)
        Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
      Compression Methods Length: 1
      Compression Methods (1 method)
      Extensions Length: 69
      Extension: elliptic_curves
      Extension: ec_point_formats
      Extension: signature_algorithms
      Extension: renegotiation_info
0070 00 9c c0 2b c0 2f 01 00 00 45 00 0a 00 16 00 14  ...+.4... .E.....
0080 00 17 00 18 00 19 00 09 00 0a 00 0b 00 0c 00 0d  .....
0090 00 0e 00 16 00 0b 00 02 01 00 00 0d 00 1c 00 1a  .....
00a0 06 03 06 01 05 03 05 01 04 03 04 01 04 02 03 03  .....
00b0 03 01 03 02 02 03 02 01 02 02 ff 01 00 01 00  .....

```

3. From Server Hello, cipher suite chosen:

TLS_RSA_WITH_AES_128_GCM_SHA256

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



5000 17:19:55.938046 10.10.0.163 10.10.0.206 TLSv1.2 2862 Server Hello 5000

Frame 6610: 2862 bytes on wire (22896 bits), 2862 bytes captured (22896 bits)

Ethernet II, src: fa:16:3e:b1:8d:79 (fa:16:3e:b1:8d:79), Dst: fa:16:3e:56:06:a3 (fa:16:3e:56:06:a3)

Internet Protocol Version 4, Src: 10.10.0.163, Dst: 10.10.0.206

Transmission Control Protocol, Src Port: 5000, Dst Port: 57816, Seq: 1, Ack: 126, Len: 2796

Secure Sockets Layer

- TLsv1.2 Record Layer: Handshake Protocol: Server Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 81
- Handshake Protocol: Server Hello
 - Handshake Type: Server Hello (2)
 - Length: 77
 - Version: TLS 1.2 (0x0303)
- Random
 - Session ID Length: 32
 - Session ID: eb02152a420a218bab406966ad7871e3c7ab1fd27fe730c0...
- Cipher Suite: **TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)**
 - Compression Method: null (0)
 - Extensions Length: 5
- Extension: renegotiation_info

0080 1f d2 7f e7 30 c0 50 9e 02 d8 74 93 dc 19 **00 9c**0.P.t.....
 0090 00 00 05 ff 01 00 01 00 16 03 03 11 5f 0b 00 11
 00a0 5b 00 11 58 00 05 92 30 82 05 8e 30 82 03 76 a0
 00b0 03 02 01 02 02 09 00 be 97 89 d1 60 22 5b dc 30
 00c0 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00 30 72
 00d0 31 0b 20 00 06 02 55 04 06 12 02 55 53 21 10 20
0.H.Or
 1 0 11 11 11 11 11 11 11 11 11 11 11 11 11 11

4. Read OSCP Request/Response to/from server:

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



```

59239 17:19:56.001695 10.10.0.206 10.10.0.163 OCSP 142 Request 59239
Frame 6631: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits)
Ethernet II, Src: fa:16:3e:56:06:a3 (fa:16:3e:56:06:a3), Dst: fa:16:3e:b1:8d:79 (fa:16:3e:b1:8d:79)
Internet Protocol Version 4, Src: 10.10.0.206, Dst: 10.10.0.163
Transmission Control Protocol, Src Port: 59239, Dst Port: 8100, Seq: 261, Ack: 1, Len: 76
[2 Reassembled TCP Segments (336 bytes): #6630(260), #6631(76)]
Hypertext Transfer Protocol
Online Certificate Status Protocol
  tbsRequest
    requestList: 1 item
      Request
        reqcert
          hashAlgorithm (SHA-1)
            Algorithm Id: 1.3.14.3.2.26 (SHA-1)
            issuerNameHash: 5368d21d2529427538588c5ccba4c4e6f3b96641
            issuerKeyHash: 28dfa5dc7e01810db98617066e4d66400f514713
            serialNumber: 13733597121043651548

0100 0d 0a 0d 0a 30 4a 30 48 30 46 30 44 30 42 30 09  ....0J0H 0F0D0B0.
0110 06 05 2b 0e 03 02 1a 05 00 04 14 53 68 d2 1d 25  .+.... .sh..%
0120 29 42 75 38 58 8c 5c cb a4 c4 e6 f3 b9 66 41 04  )Bu8X.\. ....fa.

Frame (142 bytes) Reassembled TCP (336 bytes)

```

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



8100 17:19:56.015993 10.10.0.163 10.10.0.206 OCSP 1100 Response 8100

```

Frame 6636: 1100 bytes on wire (8800 bits), 1100 bytes captured (8800 bits)
Ethernet II, Src: fa:16:3e:b1:8d:79 (fa:16:3e:b1:8d:79), Dst: fa:16:3e:56:06:a3 (fa:16:3e:56:06:a3)
Internet Protocol Version 4, Src: 10.10.0.163, Dst: 10.10.0.206
Transmission Control Protocol, Src Port: 8100, Dst Port: 59239, Seq: 1399, Ack: 337, Len: 1034
[2 Reassembled TCP Segments (2432 bytes): #6634(1398), #6636(1034)]
Hypertext Transfer Protocol
  Online Certificate Status Protocol
    responseStatus: successful (0)
    responseBytes
      responseType Id: 1.3.6.1.5.5.7.48.1.1 (id-pkix-ocsp-basic)
      BasicOCSPResponse
        tbsResponseData
          responderID: byName (1)
            producedAt: 2018-06-11 21:19:56 (UTC)
          responses: 1 item
            SingleResponse
              certID
                hashAlgorithm (SHA-1)
                  Algorithm Id: 1.3.14.3.2.26 (SHA-1)
                  issuerNameHash: 5368d21d2529427538588c5ccba4c4e6f3b96641
                  issuerKeyHash: 28dfa5dc7e01810db98617066e4d66400f514713
                  serialNumber: 13733597121043651548
                certStatus: revoked (1)
                  revoked
                    revocationTime: 2018-05-24 13:46:38 (UTC)
                    thisUpdate: 2018-06-11 21:19:56 (UTC)
                  signatureAlgorithm (sha1withRSAEncryption)
                    Padding: 0
                    signature: 5f09dfac4aea6a5a68aaa9521bf62720dd5078b0a24a4e72...
                certs: 1 item
                  Certificate (id-at-commonName=SAS.OCSP.EXAMPLE, id-at-organizationalUnitName=WinnForum SAS OCSP Responder CE)
                    signedCertificate
                    algorithmIdentifier (sha256withRSAEncryption)
                    Padding: 0
                    encrypted: 36db8b95399edae9857a41c7aec684ecfb3b7e2a5a539d25...
  
```

Frame (1100 bytes) Reassembled TCP (2432 bytes)

0150	60	22	5b	dc	a1	11	18	0f	32	30	31	38	30	35	32	34	20180524	
0160	31	33	34	36	33	38	5a	18	0f	32	30	31	38	30	36	31	134638z	.2018061
0170	31	32	31	31	39	35	36	5a	30	0d	06	09	2a	86	48	86	1211956z	0...*H.

5. Authentication exchange ends with TLS Alert message (i.e. authentication fails):

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



57816 17:19:56.039298 10.10.0.206 10.10.0.163 TLSv1.2 73 Alert (Level: Fatal, Description: Certificate Unknown) 57816

Frame 6645: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)

Ethernet II, Src: Fa:16:3e:56:06:a3 (fa:16:3e:56:06:a3), Dst: fa:16:3e:b1:8d:79 (fa:16:3e:b1:8d:79)

Internet Protocol Version 4, Src: 10.10.0.206, Dst: 10.10.0.163

Transmission Control Protocol, Src Port: 57816, Dst Port: 5000, Seq: 126, Ack: 4592, Len: 7

Secure Sockets Layer

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

 Content Type: Alert (21)

 Version: TLS 1.2 (0x0303)

 Length: 2

 Alert Message

 Level: Fatal (2)

 Description: Certificate unknown (46)

0000 fa 16 3e b1 8d 79 fa 16 3e 56 06 a3 08 00 45 00 ..>..y.. >V....E.

0010 00 3b c8 95 40 00 40 06 5c a3 0a 0a 00 ce 0a 0a .;..@.g. \.....

0020 00 a3 e1 d8 13 88 26 9d e7 f6 14 7f 9b 9e 80 18&.....

0030 00 b6 15 b2 00 00 01 01 08 0a 15 81 30 65 e9 f90e..

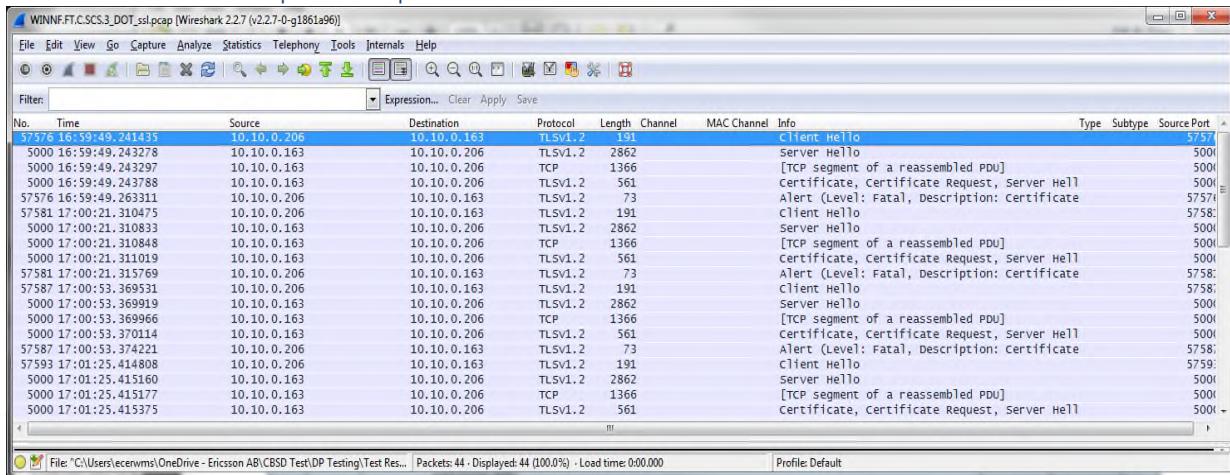
0040 d4 4e 15 03 03 00 02 02 2e .N.....

6. Registration request message is not received at Test Harness (authentication fails)

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

WINNF.FT.C.SCS.3

Packet Capture Sequence



WINNF Test Requirements:

WINNF test requirements from WINNF-TS-0122-V1.0.0 CBRS CBSD Test Specification:

2	<ul style="list-style-type: none"> 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
---	--	------	------

Analysis of WINNF Test Requirements

- From Client Hello can read: TLS version = TLS 1.2

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



```

57576 16:59:49.241435 10.10.0.206 10.10.0.163 TLSv1.2 191 Client Hello 57576
Frame 1: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits)
Ethernet II, Src: fa:16:3e:56:06:a3 (fa:16:3e:56:06:a3), Dst: fa:16:3e:b1:8d:79 (fa:16:3e:b1:8d:79)
Internet Protocol Version 4, Src: 10.10.0.206, Dst: 10.10.0.163
Transmission Control Protocol, Src Port: 57576, Dst Port: 5000, Seq: 1, Ack: 1, Len: 125
Secure Sockets Layer
  TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 120
    Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 116
      Version: TLS 1.2 (0x0303)
      Random
        Session ID Length: 0
        Cipher Suites Length: 6
      Cipher Suites (3 suites)
        Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
      Compression Methods Length: 1
      Compression Methods (1 method)
        Extensions Length: 69
      Extension: elliptic_curves
      Extension: ec_point_formats
      Extension: signature_algorithms
      Extension: renegotiation_info

0040 6a a3 16 03 03 00 78 01 00 00 74 03 03 5b 1e e2 j...x..t..[..
0050 c5 b9 25 83 93 9d 8c d7 62 70 d5 2e 98 5d 83 35 ..%.... bp...].5
0060 a0 ac 8e 86 12 a7 d7 e7 a4 03 d6 8b 61 00 00 06 .....
0070 00 9c c0 2b c0 2f 01 00 00 45 00 0a 00 16 00 14 ...+/. .E.....
0080 00 17 00 18 00 19 00 09 00 0a 00 0b 00 0c 00 0d .....
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```

- From Client Hello, cipher suite list is from WINNF approved list:

TLS_RSA_WITH_AES_128_GCM_SHA25
 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



57576 16:59:49.241435 10.10.0.206 10.10.0.163 TLSv1.2 191 Client Hello 57576

Frame 1: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits)

Ethernet II, Src: fa:16:3e:56:06:a3 (fa:16:3e:56:06:a3), Dst: fa:16:3e:b1:8d:79 (fa:16:3e:b1:8d:79)

Internet Protocol Version 4, Src: 10.10.0.206, Dst: 10.10.0.163

Transmission Control Protocol, Src Port: 57576, Dst Port: 5000, Seq: 1, Ack: 1, Len: 125

Secure Sockets Layer

- TLSv1.2 Record Layer: Handshake Protocol: client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 120
 - Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 116
 - Version: TLS 1.2 (0x0303)
 - Random
 - Session ID Length: 0
 - Cipher Suites Length: 6
 - Cipher Suites (3 suites)
 - Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
 - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
 - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
 - Compression Methods Length: 1
 - Compression Methods (1 method)
 - Extensions Length: 69
 - Extension: elliptic_curves
 - Extension: ec_point_formats
 - Extension: signature_algorithms
 - Extension: renegotiation_info

0070 00 9c c0 2b c0 2f 01 00 00 45 00 0a 00 16 00 14 .+. / . E.....
 0080 00 17 00 18 00 19 00 09 00 0a 00 0b 00 0c 00 0d
 0090 00 0e 00 16 00 0b 00 02 01 00 00 0d 00 1c 00 1a
 00a0 06 03 06 01 05 03 05 01 04 03 04 01 04 02 03 03
 00b0 03 01 03 02 02 03 02 01 02 02 ff 01 00 01 00

3. From Server Hello, cipher suite chosen:
TLS_RSA_WITH_AES_128_GCM_SHA256

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



5000 16:59:49.243278 10.10.0.163 10.10.0.206 TLSv1.2 2862 Server Hello 5000

Frame 2: 2862 bytes on wire (22896 bits), 2862 bytes captured (22896 bits)

Ethernet II, src: fa:16:3e:b1:8d:79 (fa:16:3e:b1:8d:79), Dst: fa:16:3e:56:06:a3 (fa:16:3e:56:06:a3)

Internet Protocol Version 4, Src: 10.10.0.163, Dst: 10.10.0.206

Transmission Control Protocol, Src Port: 5000, Dst Port: 57576, Seq: 1, Ack: 126, Len: 2796

Secure Sockets Layer

- TLSv1.2 Record Layer: Handshake Protocol: Server Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 81
- Handshake Protocol: Server Hello
 - Handshake Type: Server Hello (2)
 - Length: 77
 - Version: TLS 1.2 (0x0303)
- Random
 - Session ID Length: 32
 - Session ID: 7acaf29e8d6f98b94c22e6431d4f614c7bbe00faf0a784bc...
- Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- Compression Method: null (0)
- Extensions Length: 5
- Extension: renegotiation_info

0080	00	fa	f0	a7	84	bc	79	d8	76	76	65	da	52	83	00	9cy,	vve.R.	..		
0090	00	00	05	ff	01	00	01	00	16	03	03	11	5f	0b	00	11	
00a0	5b	00	11	58	00	05	92	30	82	05	8e	30	82	03	76	a0	[..X...	0	..0..v.	.	
00b0	03	02	01	02	02	09	00	be	97	89	d1	60	22	5b	db	30	"[..0	
00c0	0d	06	09	2a	86	48	86	f7	0d	01	01	0b	05	00	30	72	...".H..	0r	.	
00d0	31	0h	20	00	06	02	55	04	0f	12	07	55	53	21	10	20	1	0	..	00c1	0

4. Authentication exchange ends with TLS Alert message (i.e. authentication fails):

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



57576 16:59:49.263311 10.10.0.206 10.10.0.163 TLSv1.2 73 Alert (Level: Fatal, Description: Certificate Unknown) 57576

Frame 5: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
 Ethernet II, Src: fa:16:3e:56:06:a3 (fa:16:3e:56:06:a3), Dst: fa:16:3e:b1:8d:79 (fa:16:3e:b1:8d:79)
 Internet Protocol Version 4, Src: 10.10.0.206, Dst: 10.10.0.163
 Transmission Control Protocol, Src Port: 57576, Dst Port: 5000, Seq: 126, Ack: 4592, Len: 7
 Secure Sockets Layer
 TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Certificate Unknown)
 Content Type: Alert (21)
 Version: TLS 1.2 (0x0303)
 Length: 2
 Alert Message
 Level: Fatal (2)
 Description: Certificate unknown (46)

```

0000  fa 16 3e b1 8d 79 fa 16 3e 56 06 a3 08 00 45 00  ..>..y.. >V.....E.
0010  00 3b 14 da 40 00 40 06 10 5f 0a 0a 00 ce 0a 0a  ;..@. @. ._. .....
0020  00 a3 e0 e8 13 88 72 47 d3 18 7f c6 0e 70 80 18  .....rg .....p..
0030  00 b6 15 b2 00 00 01 01 08 0a 15 6e c6 6d e9 e7  ..... .n.m..
0040  6a ab 15 03 03 00 02 02 2e  j..... .

```

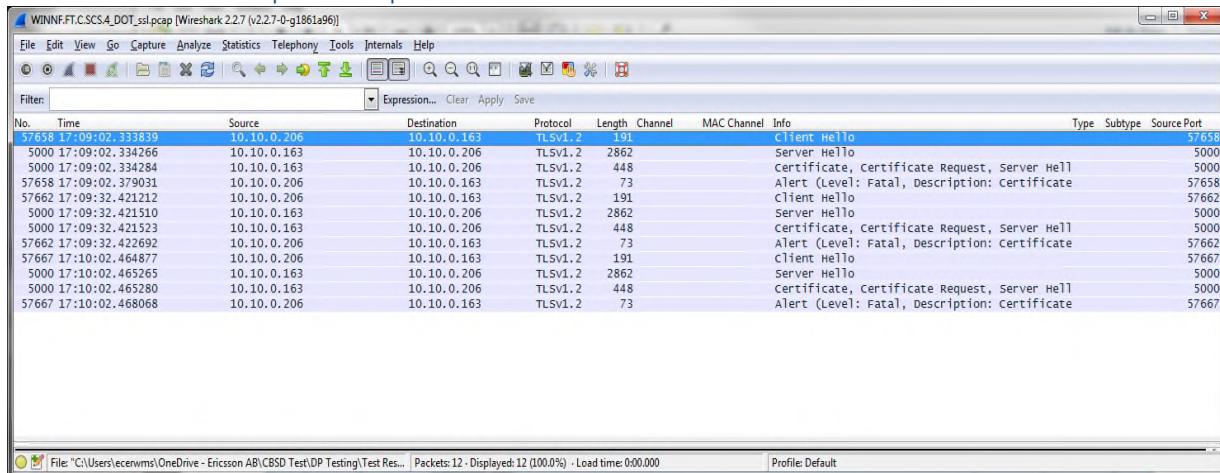
5. Registration request message is not received at Test Harness
 (authentication fails)

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



WINNF.FT.C.SCS.4

Packet Capture Sequence



WINNF Test Requirements:

WINNF test requirements from WINNF-TS-0122-V1.0.0 CBRS CBSD Test Specification:

2	<ul style="list-style-type: none"> 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
---	---	------	------

Analysis of WINNF Test Requirements

- From Client Hello can read: TLS version = TLS 1.2

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



57658 17:09:02.333839 10.10.0.206 10.10.0.163 TLSv1.2 191 Client Hello 57658

Frame 7126: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits)

Ethernet II, Src: fa:16:3e:56:06:a3 (fa:16:3e:56:06:a3), Dst: fa:16:3e:b1:8d:79 (fa:16:3e:b1:8d:79)

Internet Protocol Version 4, Src: 10.10.0.206, Dst: 10.10.0.163

Transmission Control Protocol, Src Port: 57658, Dst Port: 5000, Seq: 1, Ack: 1, Len: 125

Secure Sockets Layer

 TLSv1.2 Record Layer: Handshake Protocol: client Hello

 Content Type: Handshake (22)

 Version: TLS 1.2 (0x0303)

 Length: 120

 Handshake Protocol: client Hello

 Handshake Type: Client Hello (1)

 Length: 116

 Version: TLS 1.2 (0x0303)

 Random

 Session ID Length: 0

 Cipher Suites Length: 6

 Cipher Suites (3 suites)

 Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)

 Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)

 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

 Compression Methods Length: 1

 Compression Methods (1 method)

 Extensions Length: 69

 Extension: elliptic_curves

 Extension: ec_point_formats

 Extension: signature_algorithms

 Extension: renegotiation_info

0040 db 26 16 03 03 00 78 01 00 00 74 03 03 5b 1e e4 .& ..x. ...[..

0050 ee 6e db 81 cb 96 0c 9d e9 da 26 7d db da dc b8 ..n..... ..&}{..

0060 af 98 0d 09 fc 4b d8 0d 59 21 3c 2f 64 00 00 06K.. Y!</d...

0070 00 9c c0 2b c0 2f 01 00 00 45 00 0a 00 16 00 14 ...+./.. .E.....

0080 00 17 00 18 00 19 00 09 00 0a 00 0b 00 0c 00 0d

0090 00 00 00 16 00 0b 00 07 01 00 00 0d 00 1c 00 17

2. From Client Hello, cipher suite list is from WINNF approved list:

TLS_RSA_WITH_AES_128_GCM_SHA25
 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



57658 17:09:02.333839 10.10.0.206 10.10.0.163 TLSv1.2 191 Client Hello 57658

Frame 7126: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits)

Ethernet II, Src: fa:16:3e:56:06:a3 (fa:16:3e:56:06:a3), Dst: fa:16:3e:b1:8d:79 (fa:16:3e:b1:8d:79)

Internet Protocol Version 4, Src: 10.10.0.206, Dst: 10.10.0.163

Transmission Control Protocol, Src Port: 57658, Dst Port: 5000, Seq: 1, Ack: 1, Len: 125

Secure Sockets Layer

- TLSv1.2 Record Layer: Handshake Protocol: client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 120
- Handshake Protocol: client Hello
 - Handshake Type: Client Hello (1)
 - Length: 116
 - Version: TLS 1.2 (0x0303)
- Random
 - Session ID Length: 0
 - Cipher Suites Length: 6
- Cipher suites (3 suites)
 - Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
 - Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
 - Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
- Compression Methods Length: 1
- Compression Methods (1 method)
 - Extensions Length: 69
- Extension: elliptic_curves
- Extension: ec_point_formats
- Extension: signature_algorithms
- Extension: renegotiation_info

0070 00 9c c0 2b c0 2f 01 00 00 45 00 0a 00 16 00 14+...E.....
 0080 00 17 00 18 00 19 00 09 00 0a 00 0b 00 0c 00 0d
 0090 00 0e 00 16 00 0b 00 02 01 00 00 0d 00 1c 00 1a
 00a0 06 03 06 01 05 03 05 01 04 03 04 01 04 02 03 03
 00b0 03 01 03 02 02 03 02 01 02 02 ff 01 00 01 00

3. From Server Hello, cipher suite chosen:
TLS_RSA_WITH_AES_128_GCM_SHA256

Client	Ericsson	
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	Canada

```
5000 17:09:02.334266 10.10.0.163 10.10.0.206 TLSv1.2 2862 Server Hello 5000
Frame 7129: 2862 bytes on wire (22896 bits), 2862 bytes captured (22896 bits)
Ethernet II, Src: fa:16:3e:b1:8d:79 (fa:16:3e:b1:8d:79), Dst: fa:16:3e:56:06:a3 (fa:16:3e:56:06:a3)
Internet Protocol Version 4, Src: 10.10.0.163, Dst: 10.10.0.206
Transmission Control Protocol, Src Port: 5000, Dst Port: 57658, Seq: 1, Ack: 126, Len: 2796
Secure Sockets Layer
  TLSV1.2 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 81
  Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 77
    Version: TLS 1.2 (0x0303)
  Random
    Session ID Length: 32
    Session ID: 50ddb23b112926f850acd19623e2c30578a887e3da71c845...
    Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
    Compression Method: null (0)
    Extensions Length: 5
  Extension: renegotiation_info

0080  87 e3 da 71 c8 45 47 51  17 22 3c c6 e9 ff 00 9c  ...q.EGQ . "<... .
0090  00 00 05 ff 01 00 01 00  16 03 03 0b da 0b 00 0b  .....
00a0  d6 00 0b d3 00 05 a0 30  82 05 9c 30 82 03 84 a0  ....0 ...0.....
00b0  03 02 01 02 02 09 00 e5  f5 79 29 eb 1a cd b6 30  ....y....0
00c0  0d 06 09 2a 86 48 86 f7  0d 01 01 0b 05 00 30 7a  ...*.H... 0z
00d0  21 0b 30 00 06 02 55 04  06 12 07 55 52 30 10 20  1 0 11 001 0
```

4. Authentication exchange ends with TLS Alert message (i.e. authentication fails):

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



57658 17:09:02.379031 10.10.0.206 10.10.0.163 TLSv1.2 73 Alert (Level: Fatal, Description: Certificate Unknown) 57658

Frame 7134: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
 Ethernet II, Src: fa:16:3e:56:06:a3 (fa:16:3e:56:06:a3), Dst: fa:16:3e:b1:8d:79 (fa:16:3e:b1:8d:79)
 Internet Protocol Version 4, Src: 10.10.0.206, Dst: 10.10.0.163
 Transmission Control Protocol, Src Port: 57658, Dst Port: 5000, seq: 126, Ack: 3179, Len: 7
 Secure Sockets Layer
 TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Certificate Unknown)
 Content Type: Alert (21)
 Version: TLS 1.2 (0x0303)
 Length: 2
 Alert Message
 Level: Fatal (2)
 Description: Certificate unknown (46)

0000 fa 16 3e b1 8d 79 fa 16 3e 56 06 a3 08 00 45 00 ..>..y.. >v....E.
 0010 00 3b 0f 07 40 00 40 06 16 32 0a 0a 00 ce 0a 0a .;..@. 2.....
 0020 00 a3 e1 3a 13 88 e8 cb 3a 55 e9 d6 13 3b 80 18:U.....
 0030 00 9f 15 b2 00 00 01 01 08 0a 15 77 37 08 e9 efw7...
 0040 db 2c 15 03 03 00 02 02 2e

5. Registration request message is not received at Test Harness (authentication fails)

WINNF.FT.C.SCS.5

Packet Capture Sequence

WINNF.FT.C.SCS.5_DOT_ssl.pcap [Wireshark 2.2.7 (v2.2.7-0-g1861a96)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Channel	MAC Channel	Info	Type	Subtype	Source Port
57690	17:13:07.020079	10.10.0.206	10.10.0.163	TLSv1.2	191			client Hello			57690
5000	17:13:07.021420	10.10.0.163	10.10.0.206	TLSv1.2	2862			Server Hello			5000
5000	17:13:07.021437	10.10.0.163	10.10.0.206	TCP	1366			[TCP segment of a reassembled PDU]			5000
5000	17:13:07.021690	10.10.0.163	10.10.0.206	TLSv1.2	544			Certificate, Certificate Request, Server Hell			5000
57690	17:13:07.064639	10.10.0.206	10.10.0.163	TLSv1.2	73			Alert (Level: Fatal, Description: Certificate			57690
57694	17:13:39.098920	10.10.0.206	10.10.0.163	TLSv1.2	191			client Hello			57694
5000	17:13:39.099656	10.10.0.163	10.10.0.206	TLSv1.2	2862			Server Hello			5000
5000	17:13:39.099672	10.10.0.163	10.10.0.206	TCP	1366			[TCP segment of a reassembled PDU]			5000
5000	17:13:39.099852	10.10.0.163	10.10.0.206	TLSv1.2	544			Certificate, Certificate Request, Server Hell			5000
57694	17:13:39.101773	10.10.0.206	10.10.0.163	TLSv1.2	73			Alert (Level: Fatal, Description: certificate			57694

File: "C:\Users\ecenewms\OneDrive - Ericsson AB\CBSD Test\DP Testing\Test Res... | Packets: 10 - Displayed: 10 (100.0%) - Load time: 0:00:015 | Profile: Default

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

WINNF Test Requirements:

WINNF test requirements from WINNF-TS-0122-V1.0.0 CBRS CBSD Test Specification:

2	<ul style="list-style-type: none"> • 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
---	--	------	------

Analysis of WINNF Test Requirements

1. From Client Hello can read: TLS version = TLS 1.2

57690 17:07:02.0079 10.10.0.206 10.10.0.163 TLSv1.2 191 Client Hello 57690

Frame 1: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits)

Ethernet II, Src: fa:16:3e:56:06:a3 (fa:16:3e:56:06:a3), Dst: fa:16:3e:b1:8d:79 (fa:16:3e:b1:8d:79)

Internet Protocol Version 4, Src: 10.10.0.206, Dst: 10.10.0.163

Transmission Control Protocol, Src Port: 57690, Dst Port: 5000, Seq: 1, Ack: 1, Len: 125

Secure Sockets Layer

 TLSv1.2 Record Layer: Handshake Protocol: Client Hello

 Content Type: Handshake (22)

 Version: TLS 1.2 (0x0303)

 Length: 120

 Handshake Protocol: Client Hello

 Handshake Type: Client Hello (1)

 Length: 116

 Version: TLS 1.2 (0x0303)

 Random

 Session ID Length: 0

 Cipher Suites Length: 6

 Cipher Suites (3 suites)

 Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)

 Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)

 Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

 Compression Methods Length: 1

 Compression Methods (1 method)

 Extensions Length: 69

 Extension: elliptic_curves

 Extension: ec_point_formats

 Extension: signature_algorithms

 Extension: renegotiation_info

0040 96 f3 16 03 03 00 78 01 00 00 74 03 03 5b 1e e5 . . . x . . t . . [. .

0050 e3 c0 47 54 c9 fc 6f 5a 3c 07 7b 06 c8 d0 5e 96 . . G T . . O Z < . { . . ^ .

0060 87 26 67 c0 53 da 22 f5 91 18 d4 3b 77 00 00 06 & g . S ; W . . .

0070 00 9c c0 2b c0 2f 01 00 00 45 00 0a 00 16 00 14 . . + . / . . . E

0080 00 17 00 18 00 19 00 09 00 0a 00 0b 00 0c 00 0d

0090 00 00 00 16 00 0b 00 07 01 00 00 0d 00 1c 00 17

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



2. From Client Hello, cipher suite list is from WINNF approved list:

TLS_RSA_WITH_AES_128_GCM_SHA25
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

57690 17:13:07.020079 10.10.0.206 10.10.0.163 TLSv1.2 191 Client Hello 57690

```

⊕ Frame 1: 191 bytes on wire (1528 bits), 191 bytes captured (1528 bits)
⊕ Ethernet II, Src: fa:16:3e:56:06:a3 (fa:16:3e:56:06:a3), Dst: fa:16:3e:b1:8d:79 (fa:16:3e:b1:8d:79)
⊕ Internet Protocol Version 4, Src: 10.10.0.206, Dst: 10.10.0.163
⊕ Transmission Control Protocol, Src Port: 57690, Dst Port: 5000, Seq: 1, Ack: 1, Len: 125
⊕ Secure Sockets Layer
  ⊕ TLSv1.2 Record Layer: Handshake Protocol: client Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 120
    ⊕ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 116
      Version: TLS 1.2 (0x0303)
      ⊕ Random
        Session ID Length: 0
        Cipher Suites Length: 6
      ⊕ Cipher Suites (3 suites)
        Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
        Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
        Compression Methods Length: 1
      ⊕ Compression Methods (1 method)
        Extensions Length: 69
      ⊕ Extension: elliptic_curves
      ⊕ Extension: ec_point_formats
      ⊕ Extension: signature_algorithms
      ⊕ Extension: renegotiation_info
  0070 00 9c c0 2b c0 2f 01 00 00 45 00 0a 00 16 00 14  ....../... .E.....
  0080 00 17 00 18 00 19 00 09 00 0a 00 0b 00 0c 00 0d  .....
  0090 00 0e 00 16 00 0b 00 02 01 00 00 0d 00 1c 00 1a  .....
  00a0 06 03 06 01 05 03 05 01 04 03 04 01 04 02 03 03  .....
  00b0 03 01 03 02 02 03 02 01 02 02 ff 01 00 01 00  .....

```

3. From Server Hello, cipher suite chosen:
TLS_RSA_WITH_AES_128_GCM_SHA256

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



5000 17:13:07.021420 10.10.0.163 10.10.0.206 TLSv1.2 2862 Server Hello 5000

Frame 2: 2862 bytes on wire (22896 bits), 2862 bytes captured (22896 bits)

Ethernet II, Src: fa:16:3e:b1:8d:79 (fa:16:3e:b1:8d:79), Dst: fa:16:3e:56:06:a3 (fa:16:3e:56:06:a3)

Internet Protocol Version 4, Src: 10.10.0.163, Dst: 10.10.0.206

Transmission Control Protocol, Src Port: 5000, Dst Port: 57690, Seq: 1, Ack: 126, Len: 2796

Secure Sockets Layer

- TLSv1.2 Record Layer: Handshake Protocol: Server Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 81
- Handshake Protocol: Server Hello
 - Handshake Type: Server Hello (2)
 - Length: 77
 - Version: TLS 1.2 (0x0303)
- Random
 - Session ID Length: 32
 - Session ID: ad18dd2a99b4d550099735fb8f06edffef9e8cd2a2e9a54c...
 - Cipher Suite: **TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)**
 - Compression Method: null (0)
 - Extensions Length: 5
- Extension: renegotiation_info

0080 8c d2 a2 e9 a5 4c 3b 0d 55 e9 21 98 0f 68 00 9cL;.. u.!.h..
 0090 00 00 05 ff 01 00 01 00 16 03 03 11 4e 0b 00 11N...
 00a0 4a 00 11 47 00 05 81 30 82 05 7d 30 82 03 65 a0 J..G...0 ..j0..e.
 00b0 03 02 01 02 02 09 04 be 97 89 d1 60 22 5b da 30"[.0
 00c0 0d 06 09 2a 86 48 86 f7 0d 01 01 0b 05 00 30 72 ...*.H..Or
 00d0 21 0b 20 00 06 02 55 04 06 12 02 55 52 21 10 20 10 .. u... u51 0

4. Authentication exchange ends with TLS Alert message (i.e. authentication fails):

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



```

57690 17:13:07.064639 10.10.0.206 10.10.0.163 TLSv1.2 73 Alert (Level: Fatal, Description: Certificate Unknown) 57690
⊕ Frame 5: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
⊕ Ethernet II, Src: fa:16:3e:56:06:a3 (fa:16:3e:56:06:a3), Dst: fa:16:3e:b1:8d:79 (fa:16:3e:b1:8d:79)
⊕ Internet Protocol Version 4, Src: 10.10.0.206, Dst: 10.10.0.163
⊕ Transmission Control Protocol, Src Port: 57690, Dst Port: 5000, Seq: 126, Ack: 4575, Len: 7
⊖ Secure Sockets Layer
  ⊖ TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Certificate Unknown)
    Content Type: Alert (21)
    Version: TLS 1.2 (0x0303)
    Length: 2
  ⊖ Alert Message
    Level: Fatal (2)
    Description: Certificate Unknown (46)

0000  fa 16 3e b1 8d 79 fa 16 3e 56 06 a3 08 00 45 00  ..>..y.. >V....E.
0010  00 3b 64 36 40 00 40 06 c1 02 0a 0a 00 ce 0a 0a  .;d6@.@. .....
0020  00 a3 e1 5a 13 88 f8 3f 97 10 7f d7 a0 07 80 18  ....Z...? .....
0030  00 b6 15 b2 00 00 01 01 08 0a 15 7a f2 d6 e9 f3  .....z.....
0040  96 fb 15 03 03 00 02 02 2e  .....z.....

```

5. Registration request message is not received at Test Harness (authentication fails)

Client	Ericsson	 Canada
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Test Equipment

Instrument	Manufacturer	Type No.	Serial No	Calibration Period (months)	Calibration Due
THG	Fluke	77 IV	34770264	12	18-Apr-2019
DVM	VWR	61161-378	170120564	24	17-Feb-2019
Power Supply	Xantrex	XKW 60-50	E00109863	O/P Mon	-
Spectrum Analyser	Keysight	N9030A	MY55410202	12	26-Sep-2019
Attenuator	Pasternack	PE7004-10	N/S	O/P Mon	-
Switching Control Unit	Hewlett Packard	11713A	3748A060876	O/P Mon	-
RF Switch Unit	Burnsco	RARFSW 4x1	001	O/P Mon	-
Power Supply	Leader	730-3D	9801135	O/P Mon	-
Receiver	Rohde & Schwarz	ESU40	1001162	24	20-Apr-2019

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



Appendix A – EUT & Client Provided Details

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



General EUT Description

Manufacturer	Ericsson
Address	349 Terry Fox Drive Ottawa Ontario K2K 2V6 Canada
Product Name	RD 4442 B48
Product Number	KRY 901 385/1
Serial Number(s)	TD3T428815 TD3T428820
Software Version	CXP 901 3268/14: R70AK
Hardware Version	R1C
Test Specification/Issue/Date	FCC CFR 47 Part 2: 2017 FCC CFR 47 Part 96: 2017 (Winnforum test suite)
Product Name	RD 4442 B48

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



Technical Description

The Equipment Under Test (EUT) RD 4442 B48 KRY 901 385/1 is an Ericsson AB Radio Unit working in the public mobile service (3550-3700 MHz) band which provides communication connections to (Band) network. The RD 4442 B48 KRY 901 385/1 operates from a -48V DC supply.

The Equipment Under Test (EUT) is shown in the photograph below. A full technical description can be found in the Manufacturer's documentation.



Equipment Under Test

EUT Configuration

Please see Appendix B for close up pictures of the unit as configured during testing

- Cables and earthing when applicable were connected as per manufacturer's specification.

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)

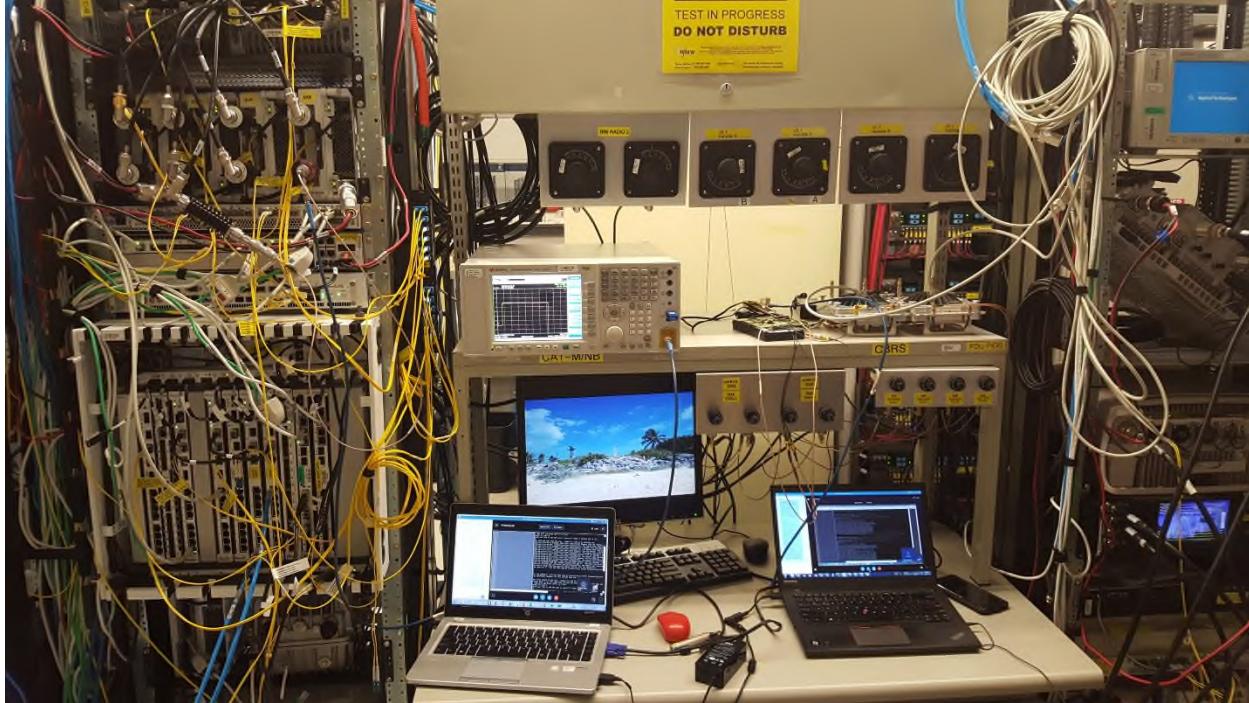


Appendix B – EUT, Peripherals, and Test Setup Photos

Client	Ericsson
Product	LTE KRY 901 385/1 RD 4442 B48 (3550-3700 MHz) Base Station
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)



Canada



Test setup