

# Test Report

As per

## FCC Part 96 SAS requirements (CBRS Test Plan)

on the

**Ericsson Remote Radio Unit LTE KRC 161 746/1  
Radio 4408 B48 (3550-3700MHz)**

Issued by:  
**TÜV SÜD Canada  
Inc.**  
1280 Teron Rd,  
Ottawa, ON K2K  
2C1  
Canada

Scott Drysdale.  
Test Personnel



Sivaratnam,  
Kasinathan  
Technical Reviewer



Canada

**Choose certainty.  
Add value.**


Testing produced  
for

Ericsson Canada

See Appendix A for  
full client & EUT  
details.




Testing Laboratory  
Certificate #2955.19

Client	<b>Ericsson</b>	
Product	<b>LTE KRC 161 711/7461 Radio 4408 B48</b>	
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.....	46
WINNF Security Test Case Analysis .....	57
WINNF.FT.C.SCS.1 .....	57
WINNF.FT.C.SCS.2 .....	60
WINNF.FT.C.SCS.3 .....	64
WINNF.FT.C.SCS.4 .....	67
WINNF.FT.C.SCS.5 .....	70
Appendix A – EUT & Client Provided Details .....	74
Technical Description .....	76
Appendix B – EUT, Peripherals, and Test Setup Photos.....	77

Client	<b>Ericsson</b>	
Product	<b>LTE KRC 161 711/7461 Radio 4408 B48</b>	
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 KRC 161 746/1 Radio 4408 B48(3550-3700 MHz)** 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	<b>Ericsson</b>	
Product	<b>LTE KRC 161 711/7461 Radio 4408 B48</b>	
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)	<b>LTE KRC 161 746/1 Radio 4408 B48(3550-3700 MHz)</b>
EUT passed all tests performed	Yes
Tests conducted by	Scott Drysdale


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

Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
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	<b>Ericsson</b>	
Product	<b>LTE KRC 161 711/7461 Radio 4408 B48</b>	
Standard(s)	<b>FCC Part 96 SAS requirements (CBRS Test Plan)</b>	

					installationParam change. <ul style="list-style-type: none"> <li>Record time at which transmission stops. Time must be within 60 seconds of the installationParam change taking effect.</li> </ul>	
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	<b>Ericsson</b>	
Product	<b>LTE KRC 161 711/7461 Radio 4408 B48</b>	
Standard(s)	<b>FCC Part 96 SAS requirements (CBRS Test Plan)</b>	

					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"> <li>Transmission does not start until time of first</li> </ul>	N/A


Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

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




Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
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"> <li>CBSD stops transmission within 60 seconds of heartbeatResponse which contains responseCode=501</li> </ul>	p
6.4.4.2.5	X	X	WINNF.FT.C.H BT.7	Heartbeat responseCode=502 (UNSYNC_OP_PARAMETER)	Monitor RF transmission. Ensure: <ul style="list-style-type: none"> <li>CBSD stops transmission within 60 seconds of heartbeatResponse which contains responseCode=502</li> </ul>	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"> <li>CBSD1: will continue to transmit to end of test</li> </ul>	P

Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
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"> <li>• CBSD2: must stop transmission within 60 seconds of being sent heartbeatResponse with responseCode = 500</li> </ul>	
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"> <li>• CBSD must stop transmission within transmitExpirationTime+60 seconds, where transmitExpirationTime is from last successful heartbeatResponse message</li> </ul>	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	<b>Ericsson</b>	
Product	<b>LTE KRC 161 711/7461 Radio 4408 B48</b>	
Standard(s)	<b>FCC Part 96 SAS requirements (CBRS Test Plan)</b>	

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"> <li>• CBSD stops transmission at any time prior to sending the relinquishmentRequest message.</li> </ul>	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"> <li>• CBSD stops transmission at any time prior to sending the relinquishmentRequest message.</li> </ul>	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"> <li>• CBSD stops transmission at any time prior to sending the relinquishmentRequest message or deregistrationRequest message (whichever is sent first)</li> </ul>	N/A


Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

6.7.4.1.2	--	X	WINNF.FT.D.D RG.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.SC S.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.SC S.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.SC S.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.SC S.4	TLS failure when SAS Test Harness certificate is issue 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.SC S.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.H BT	UUT RF Transmit Power Measurement	Power Spectral Density test case.  Assume we use 1 carrier bandwidth	P

Client	<b>Ericsson</b>	
Product	<b>LTE KRC 161 711/7461 Radio 4408 B48</b>	
Standard(s)	<b>FCC Part 96 SAS requirements (CBRS Test Plan)</b>	

					(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 KRC 161 711/7461 Radio 4408 B48	
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

The device does not use single-step registration (as defined in condition C2 in WINNF-TS-0122-V1.0.0, Table 6-2), therefore test cases 6.1.4.1.4, and 6.1.4.3.1 are not applicable as per WINNF-TS-0122-V1.0.0, Table 6-3 and therefore not required or 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 timing provided in the logs.

Logs are kept on file.

Client	<b>Ericsson</b>	
Product	<b>LTE KRC 161 711/7461 Radio 4408 B48</b>	
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	<b>Ericsson</b>	
Product	<b>LTE KRC 161 711/7461 Radio 4408 B48</b>	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

## Document Revision Status

Revision 000:    September 11, 2019    First release



Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
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 KRC 161 711/7461 Radio 4408 B48	
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 #2955.19. 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	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
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)
Sept 3 – 5, 2019	All	SD	20-23	40-55	96.106

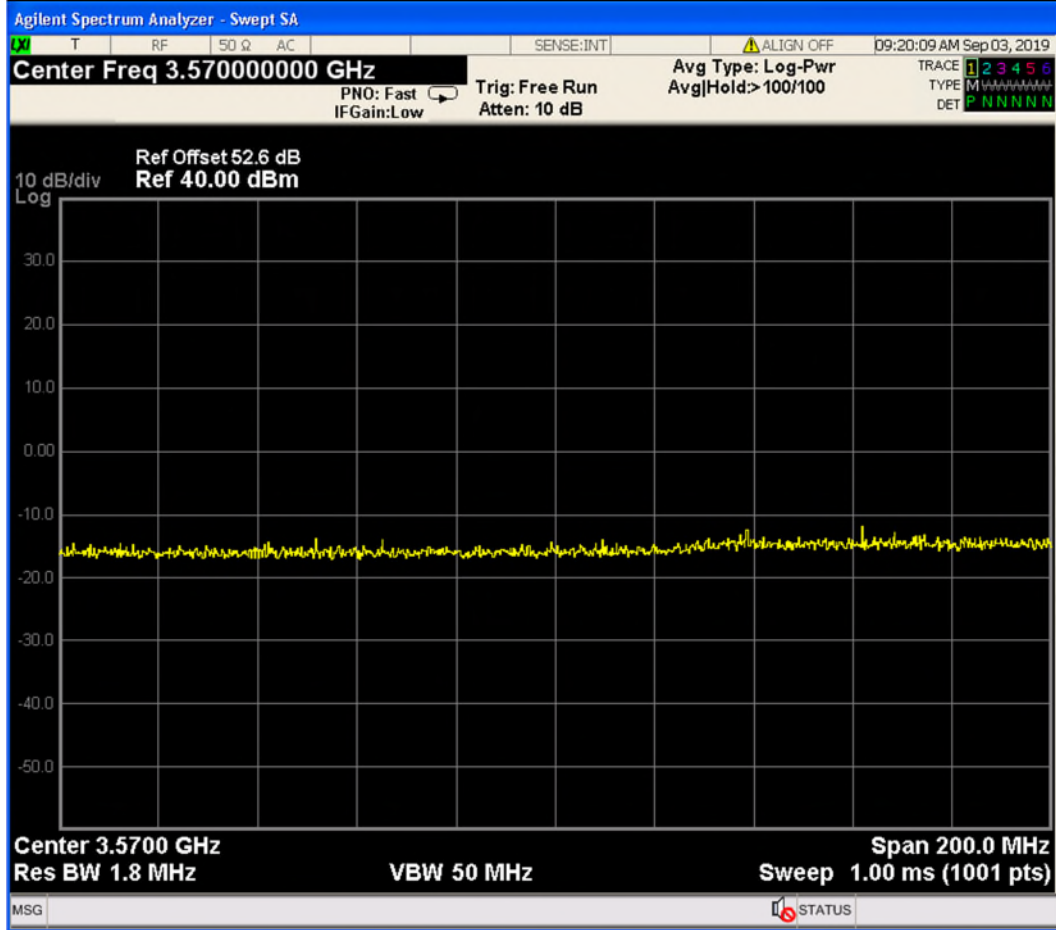
Client	<b>Ericsson</b>	
Product	<b>LTE KRC 161 711/7461 Radio 4408 B48</b>	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	


## Detailed Test Results Section

Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

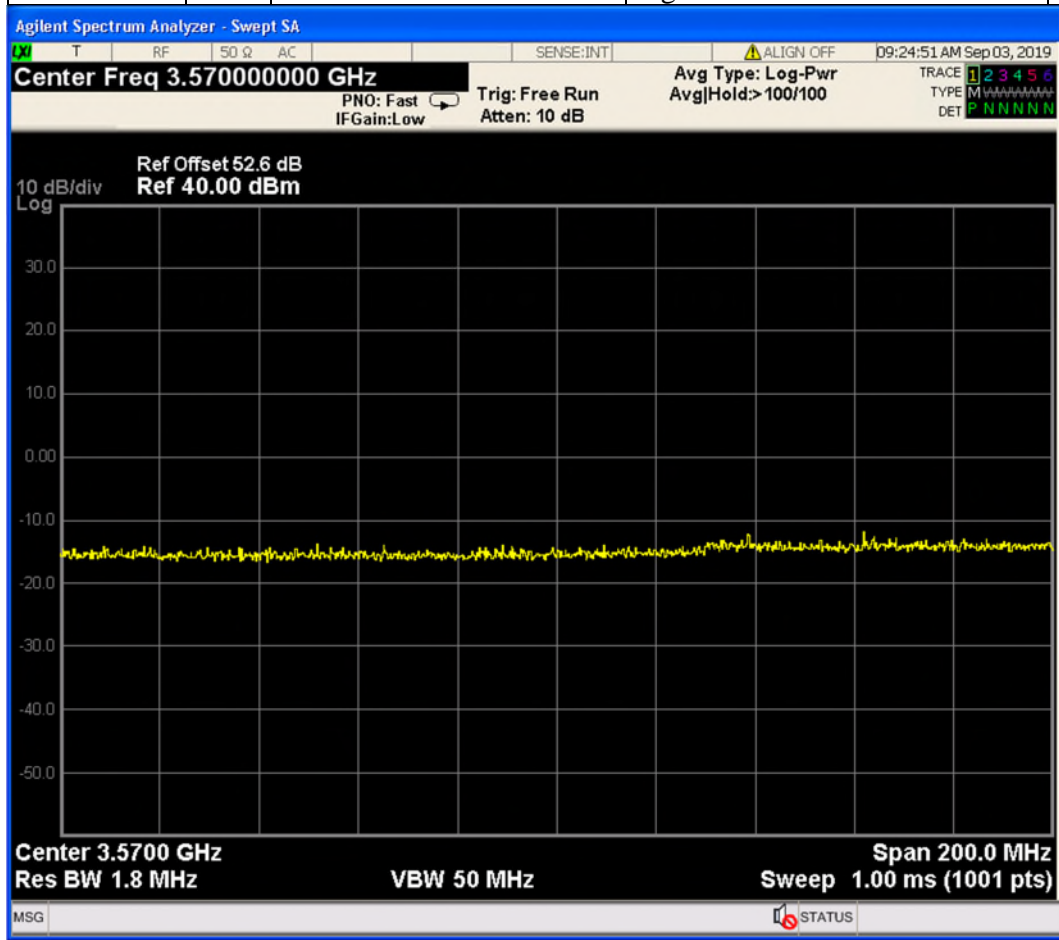
**Authorization transmit after it receives authorization from a SAS.**


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



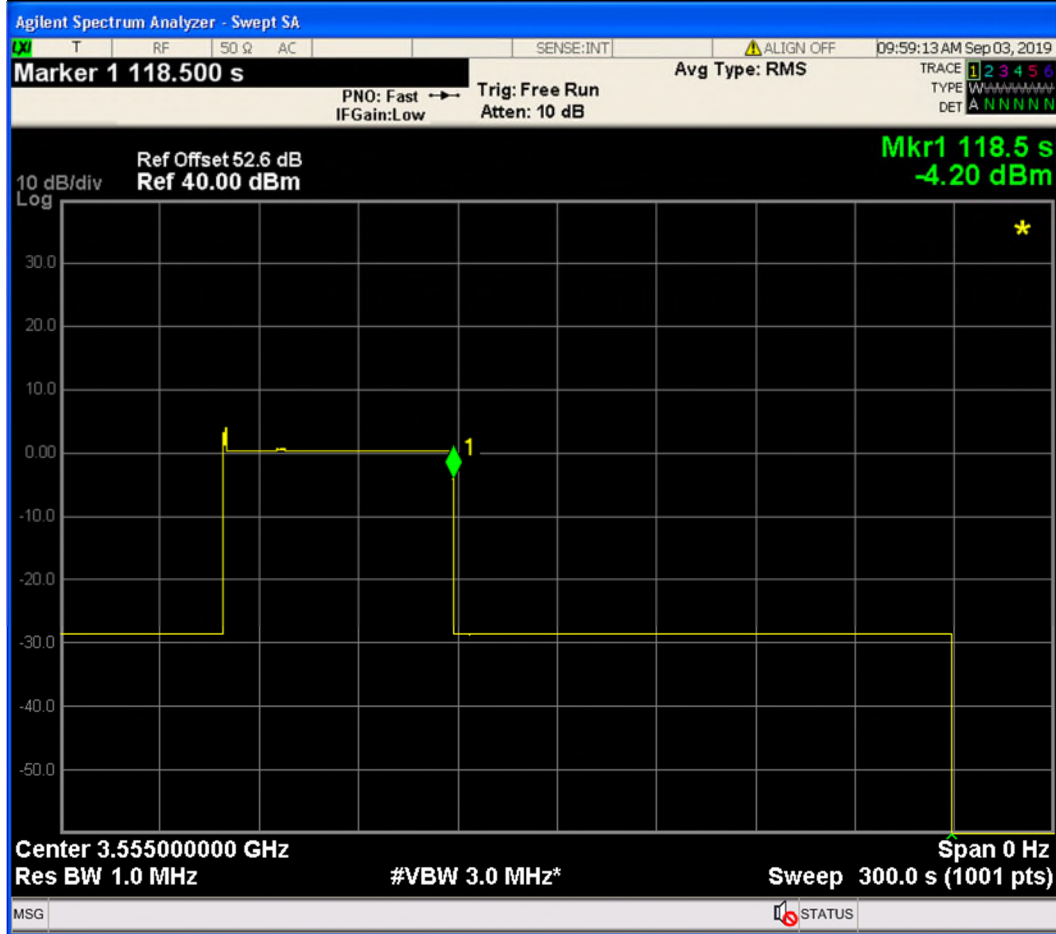
Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

6.1.4.1.6	X	WINNF.TT.D.REG.6	Domain Proxy Single-Step registration for CBSD with CPI signed data	P
-----------	---	------------------	---	---




Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

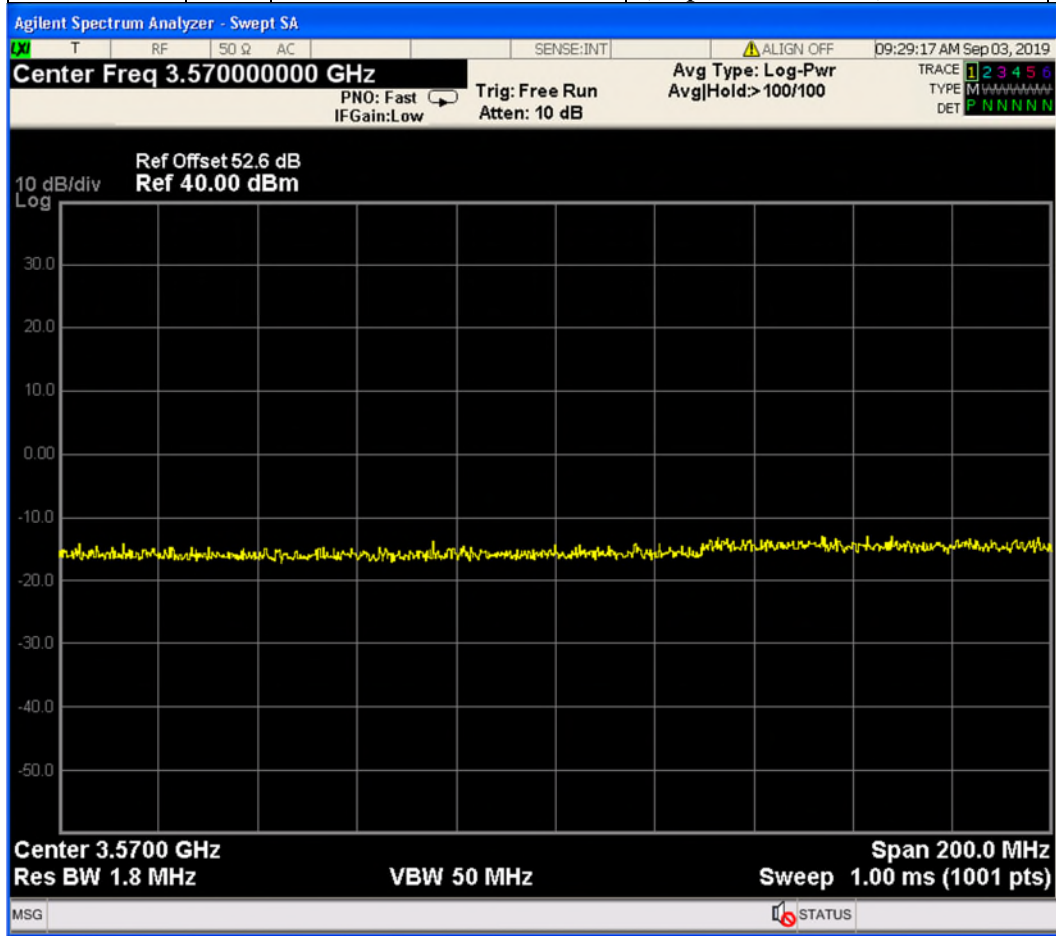
6.1.4.1.7	X	WINNF.FT.C.REG.7	Registration due to change of an installation parameter	P
-----------	---	------------------	---	---




Test Harness logs and timing on graph was verified, the EUT passed the requirement.

Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

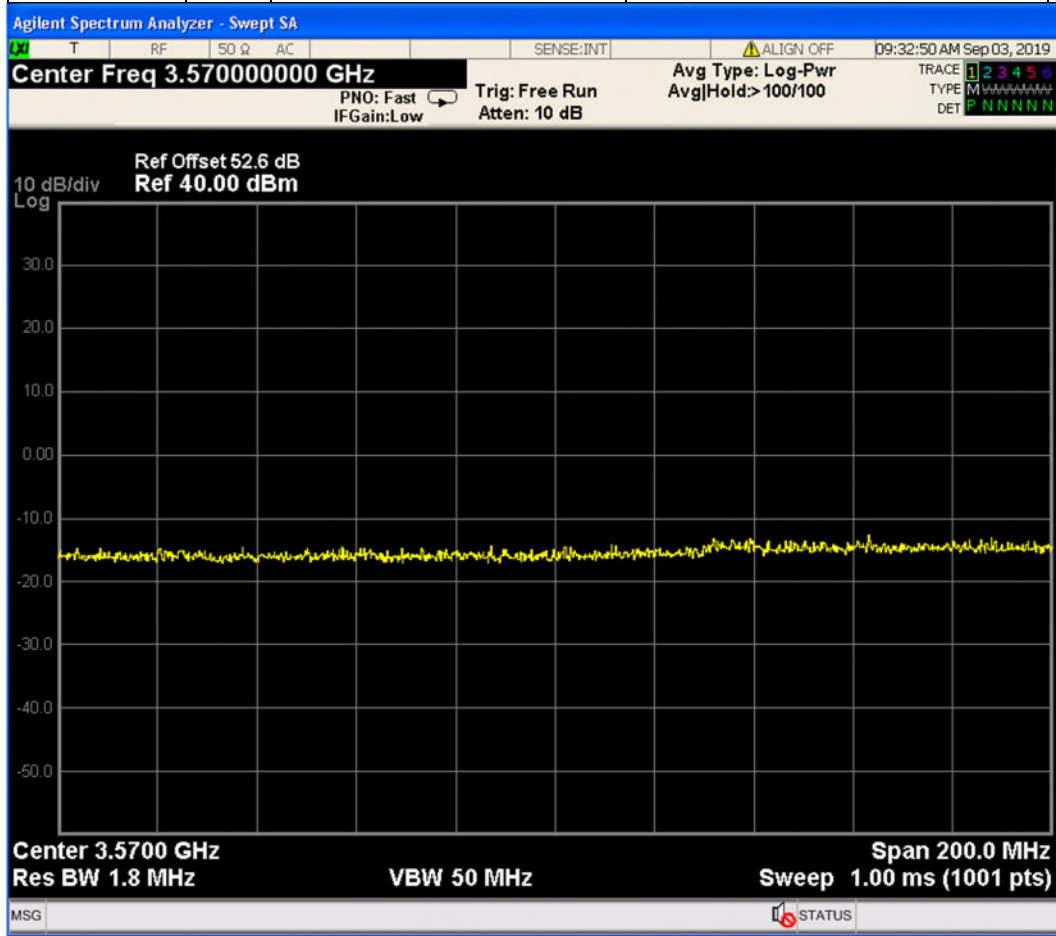
6.1.4.2.2	X	WINNF.FT.D.REG.9	Domain Proxy Missing Required parameters (responseCode 102)	P
-----------	---	------------------	---	---






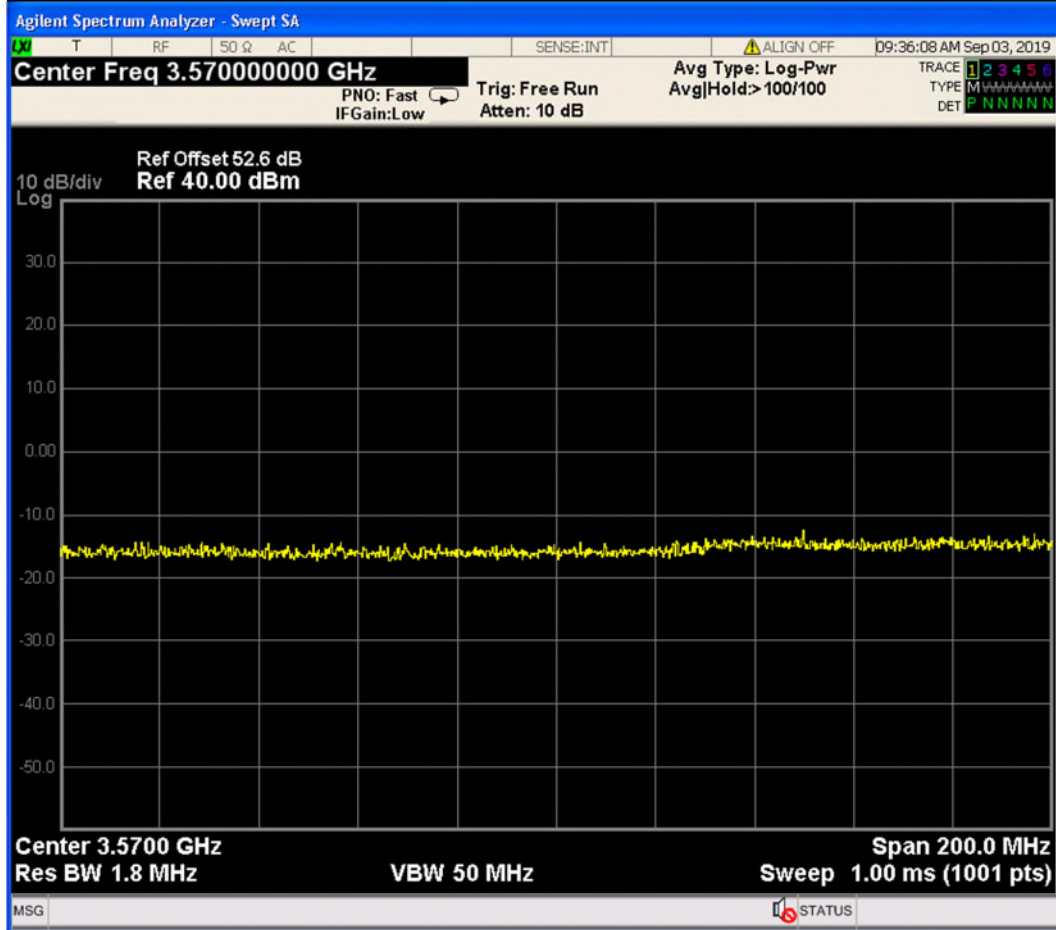
Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	


6.1.4.2.4	X	WINNF.TT.D.REG.11	Domain Proxy Pending registration (responseCode 200)	P
-----------	---	-------------------	--	---



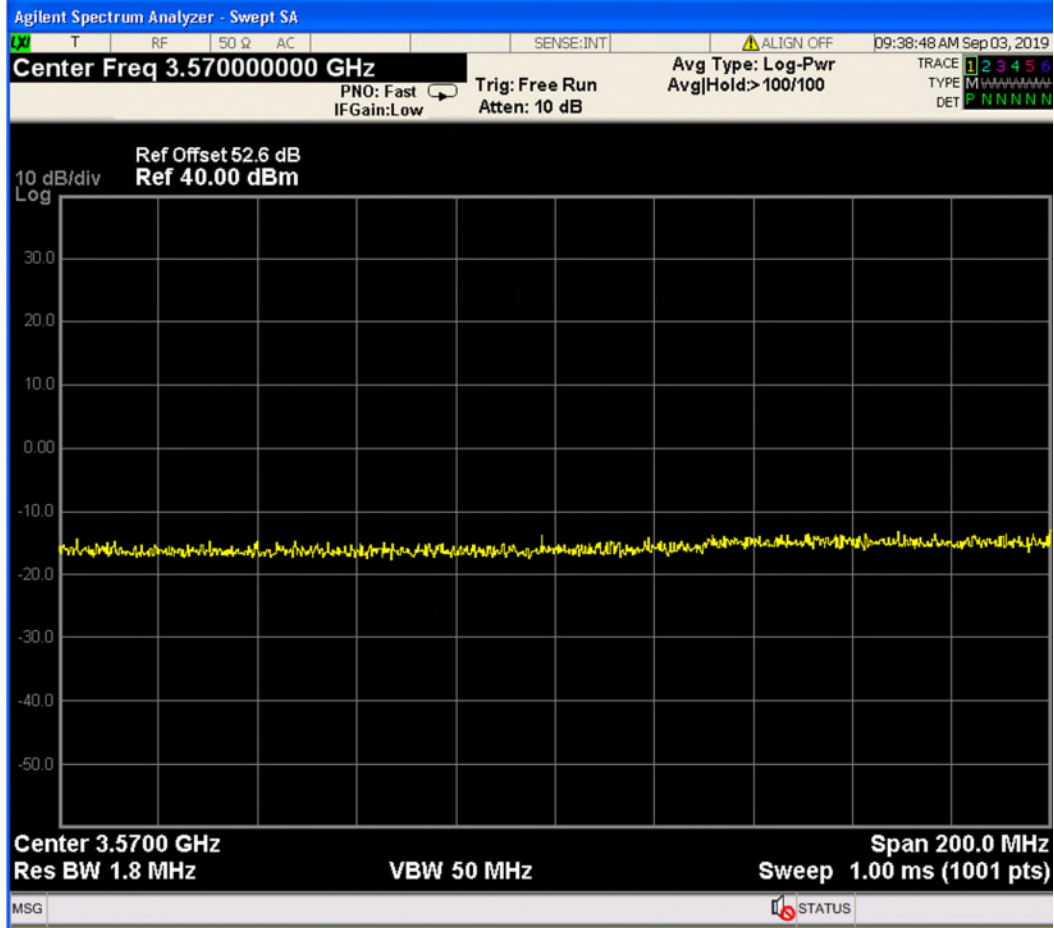
Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	


6.1.4.2.6	X	WINNF.FT.D.REG.13	Domain Proxy Invalid parameters (responseCode 103)	P
-----------	---	-------------------	--	---



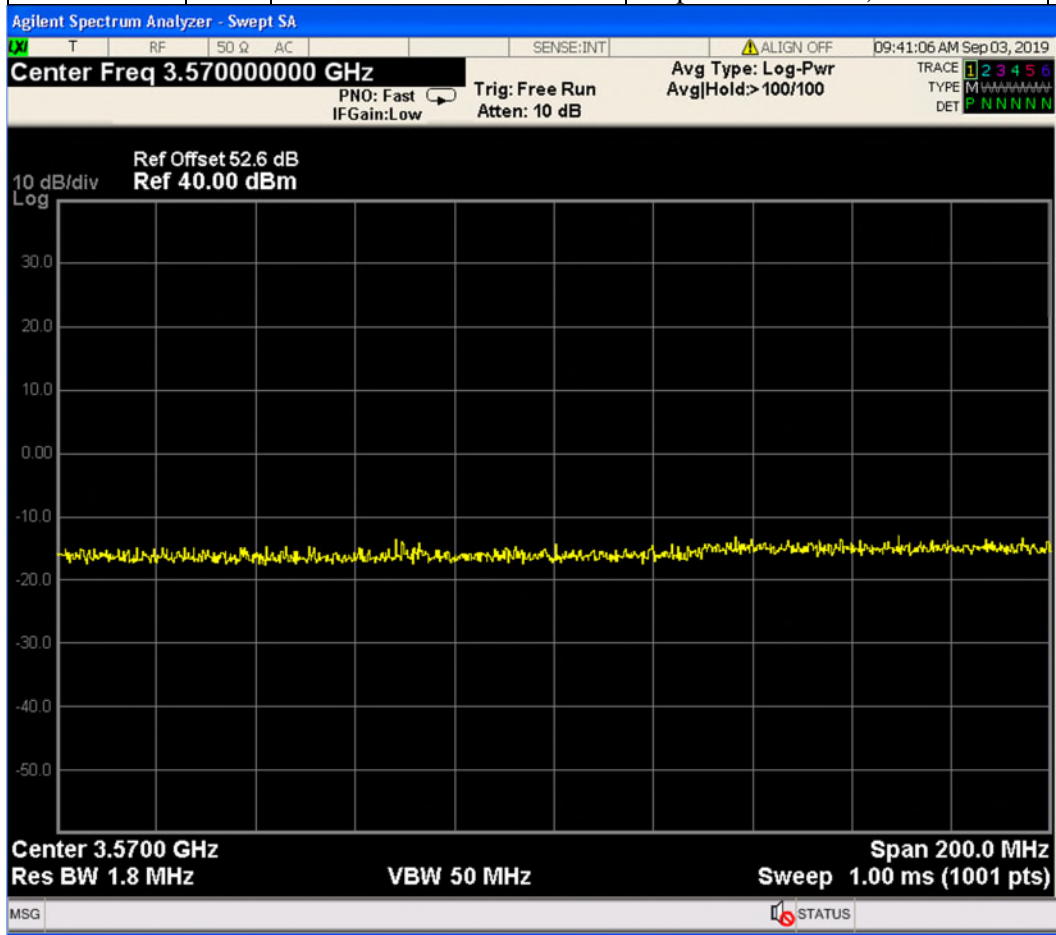
Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	


6.1.4.2.8	X	WINNF.FT.D.REG.15	Domain Proxy Blacklisted CBSD (responseCode 101)	P
-----------	---	-------------------	---	---



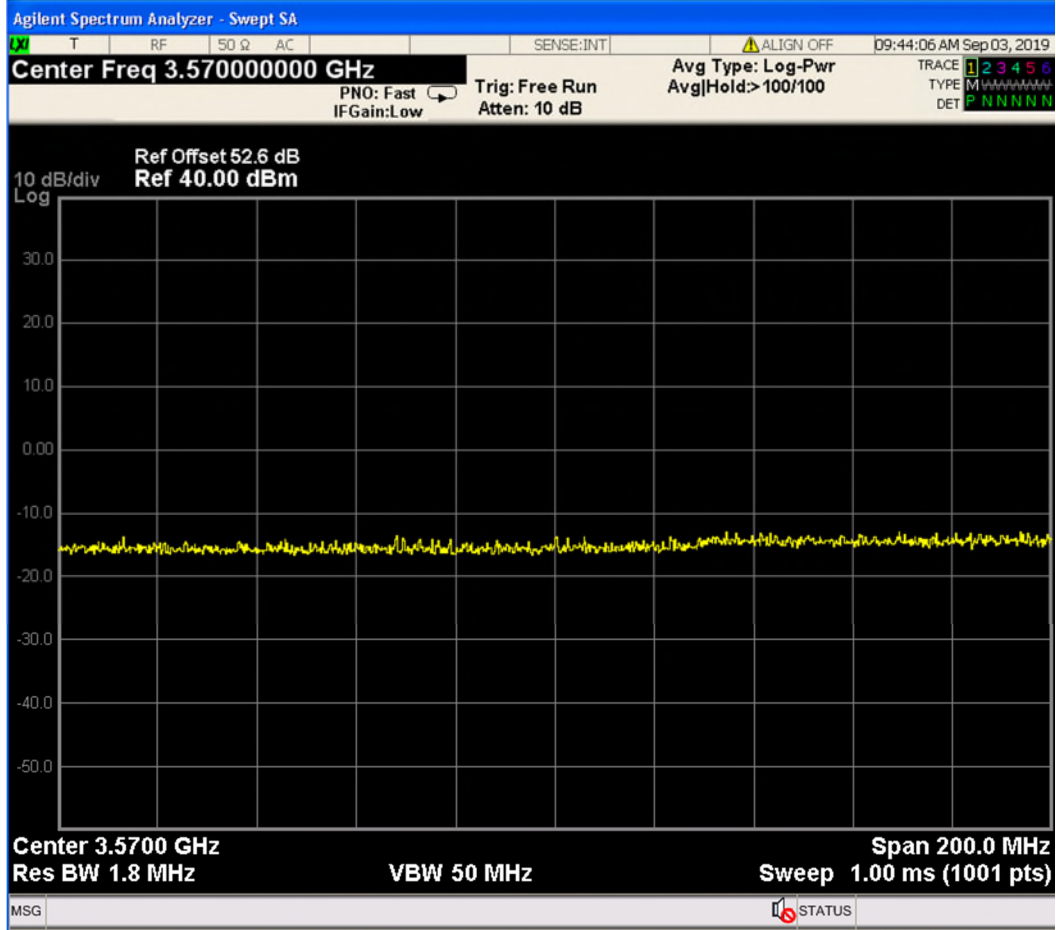
Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	


6.1.4.2.10	X	WINNF.FT.D.REG.17	Domain Proxy Unsupported SAS protocol version responseCode 100)	P
------------	---	-------------------	---	---



Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

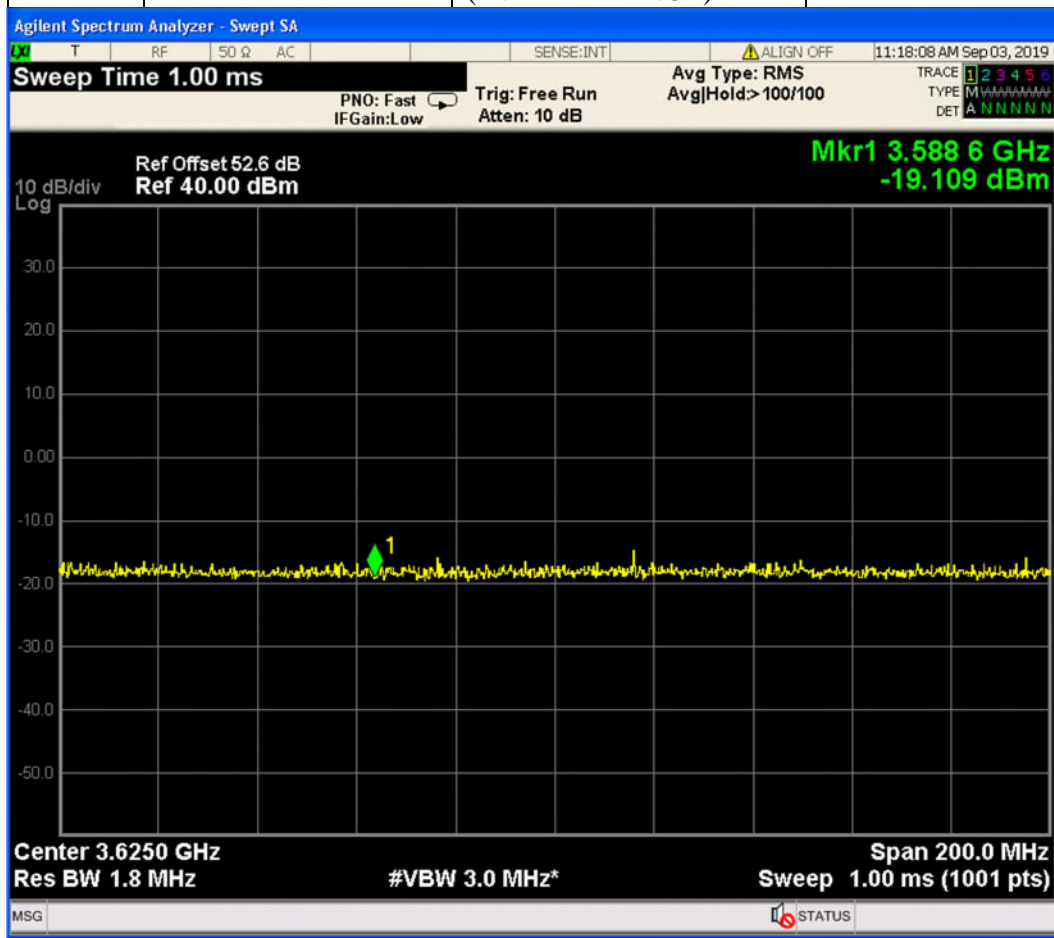
6.1.4.2.12	X	WINNF.FT.D.REG.19	Domain Proxy Group Error (responseCode 201)	P
------------	---	-------------------	--	---



Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
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
-----------	------------------	--	---	---

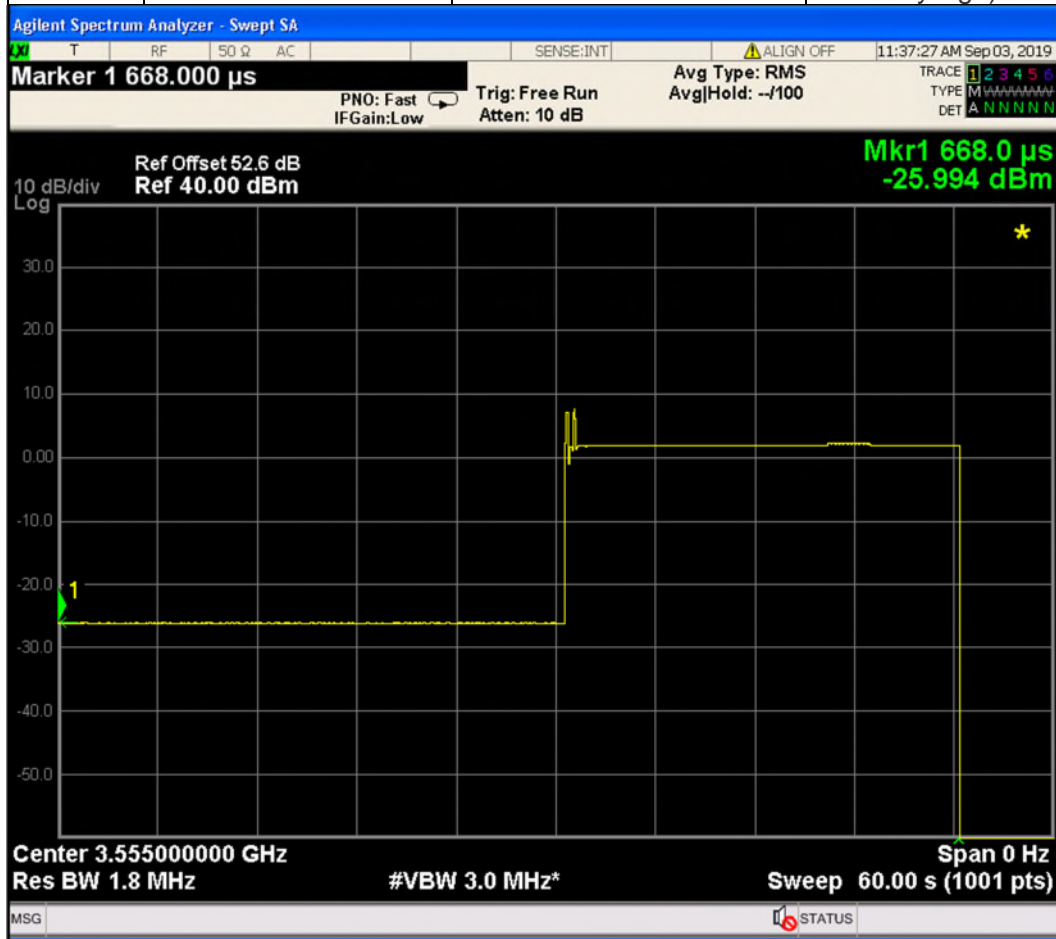







Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

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

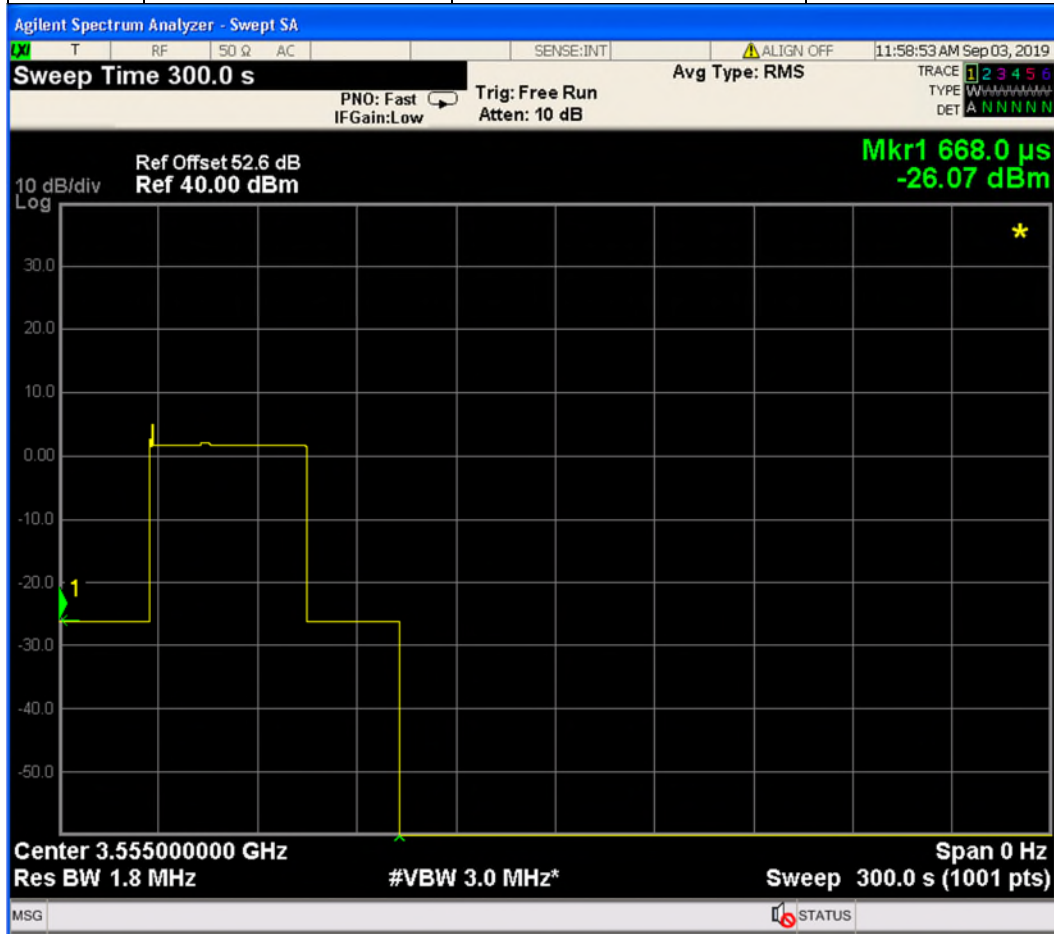


Test Harness logs and timing on graph was verified, the EUT passed the requirement.




Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

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




Test Harness logs and timing on graph was verified, the EUT passed the requirement.

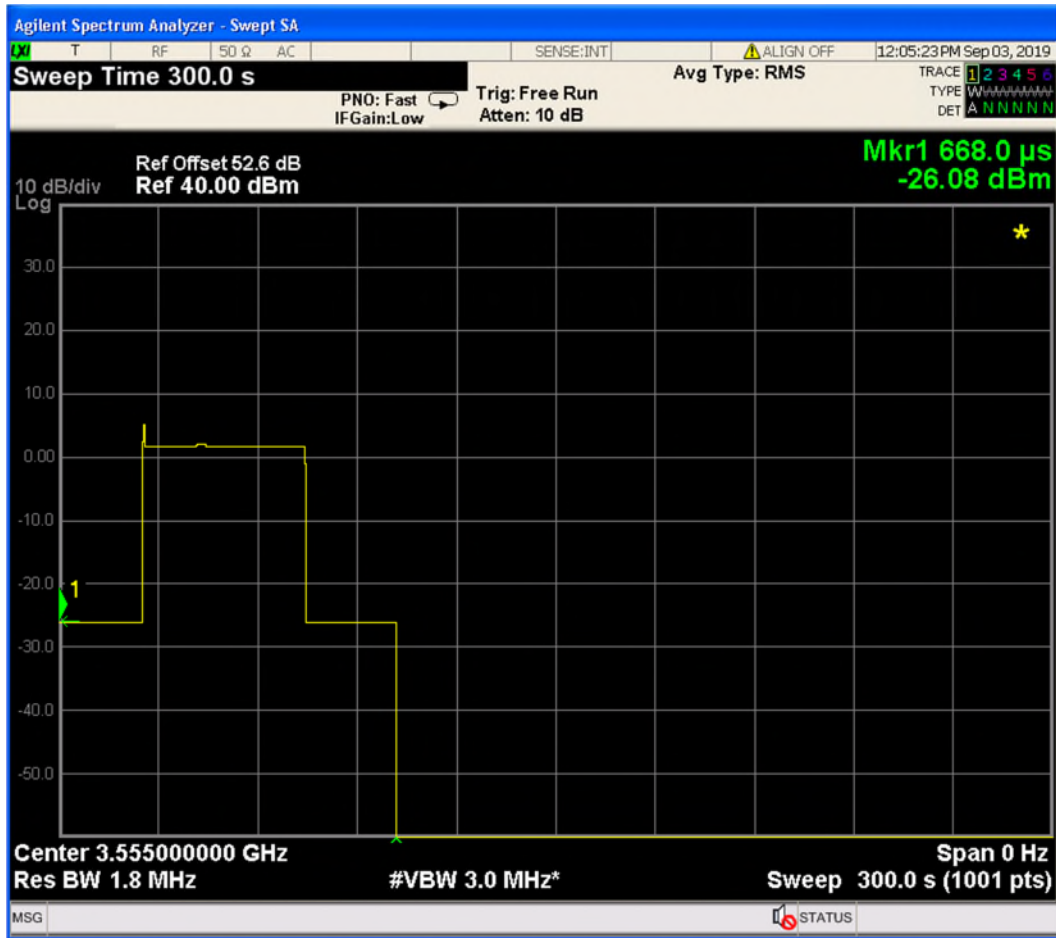
Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

6.4.4.2.3	WINNF.TC.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	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

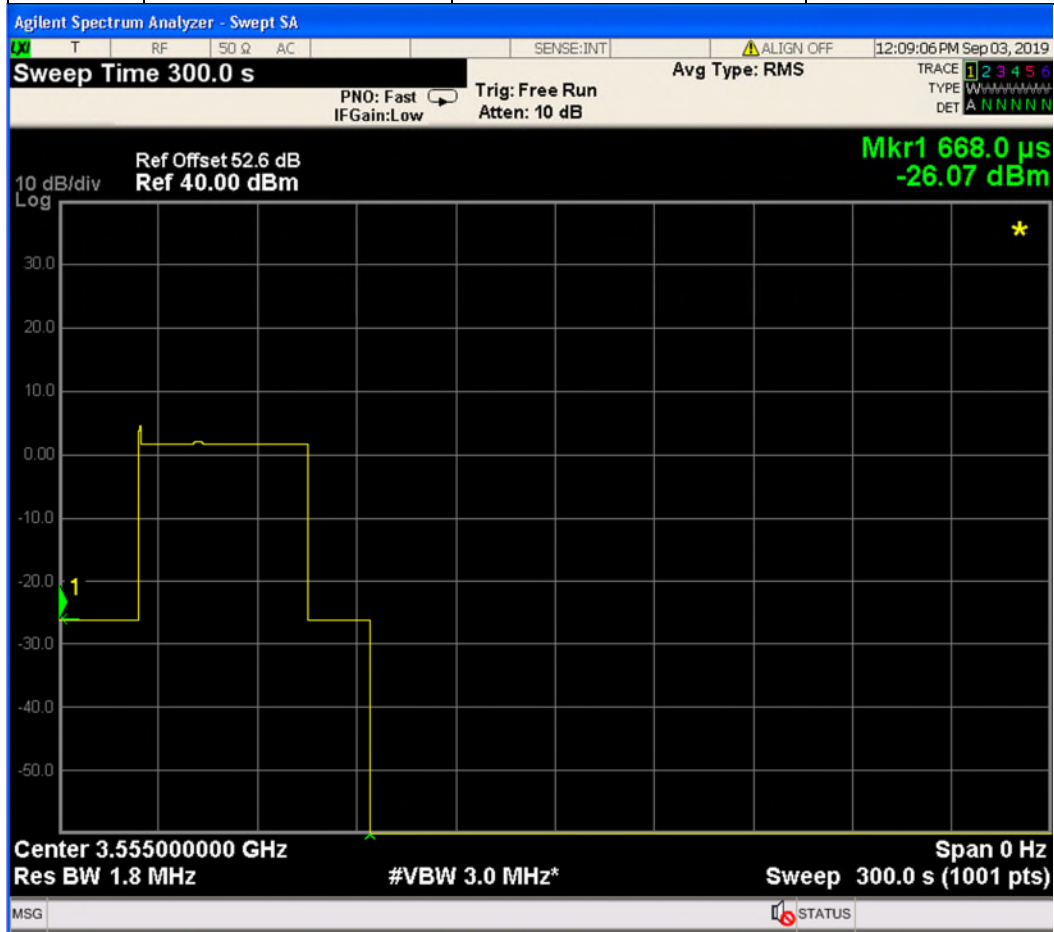
6.4.4.2.4	WINNF.FT.C.HBT.6	Heartbeat responseCode=501 (SUSPENDED_GRANT) in Subsequent Heartbeat Response	Monitor RF transmission. Ensure: <ul style="list-style-type: none"> <li>CBSD stops transmission within 60 seconds of heartbeatResponse which contains responseCode=501</li> </ul>	p
-----------	------------------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




Test Harness logs and timing on graph was verified, the EUT passed the requirement.


Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
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"> <li>CBSD stops transmission within 60 seconds of heartbeatResponse which contains responseCode=502</li> </ul>	p
-----------	------------------	--	---	---

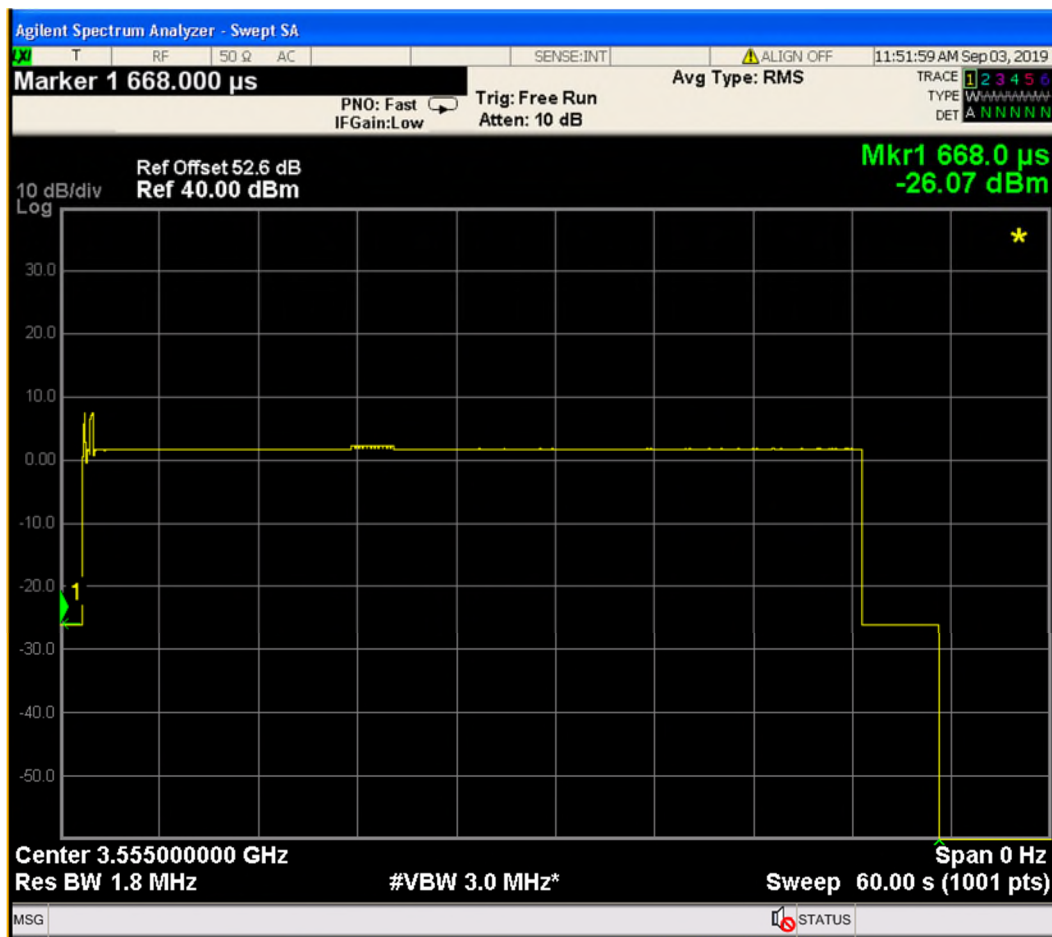


Client	<b>Ericsson</b>	
Product	<b>LTE KRC 161 711/7461 Radio 4408 B48</b>	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	


Test Harness logs and timing on graph was verified, the EUT passed the requirement.

Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

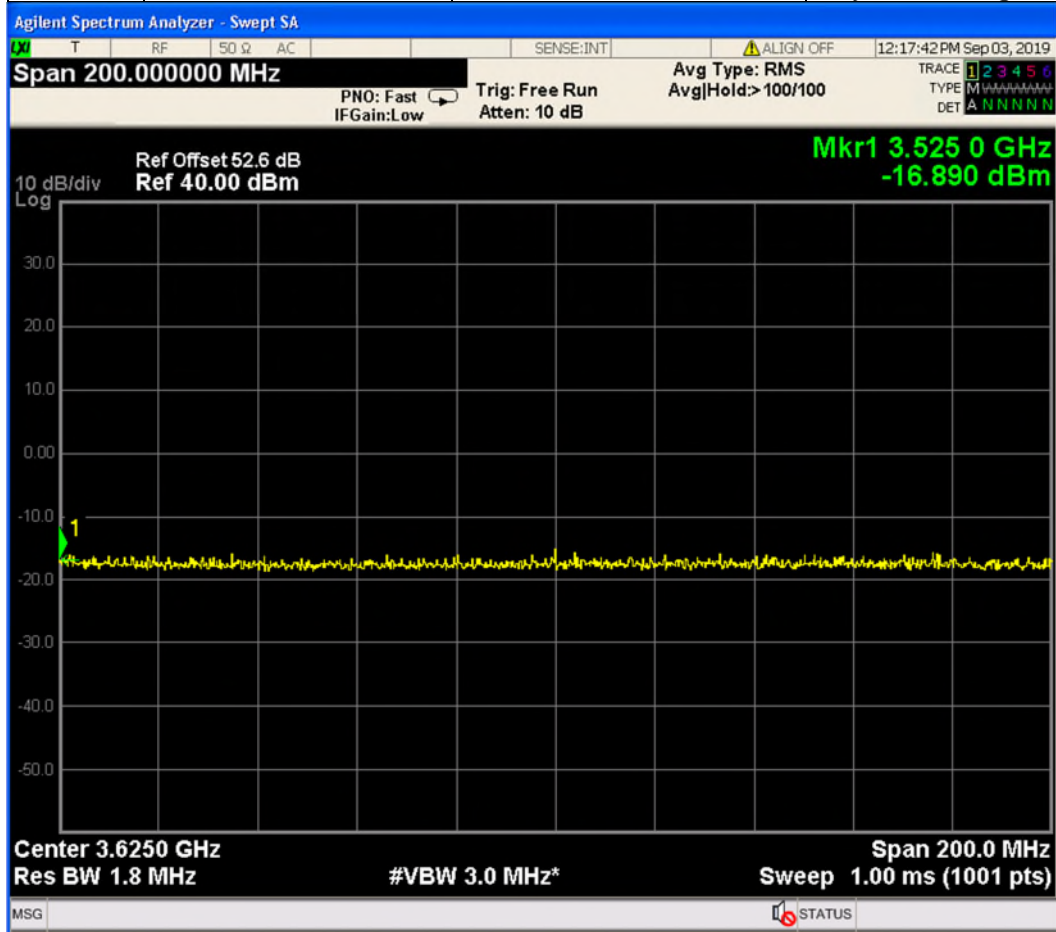
6.4.4.2.6	--	X	WINNF.FT.D.H BT.8	Domain Proxy Heartbeat responseCode=500 (TEMINATED_GR ANT)	Monitor RF transmission. CBSDs will have different behavior: <ul style="list-style-type: none"> <li>• CBSD1: will continue to transmit to end of test (this is not a pass/fail criteria, but check)</li> <li>• CBSD2: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




Test Harness logs and timing on graph was verified, the EUT passed the requirement.

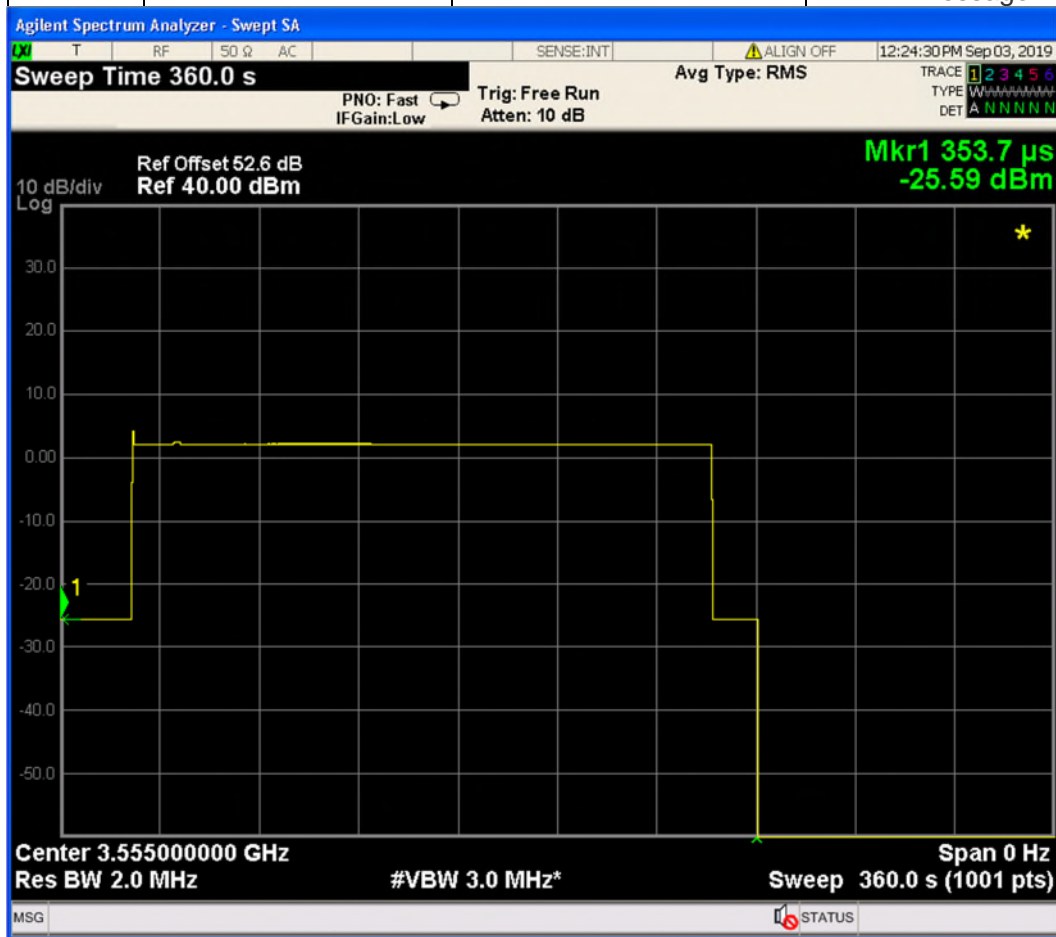
Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

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	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
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: <ul style="list-style-type: none"> <li>CBSD must stop transmission within transmitExpireTime+60 seconds, where transmitExpireTime is from last successful heartbeatResponse message</li> </ul>	P
-----------	-------------------	--	---	---




Test Harness logs and timing on graph was verified, the EUT passed the requirement.



Client	<b>Ericsson</b>	
Product	<b>LTE KRC 161 711/7461 Radio 4408 B48</b>	
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. "measreportconfig" in logs. All other requirements verified.

Client	<b>Ericsson</b>	
Product	<b>LTE KRC 161 711/7461 Radio 4408 B48</b>	
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. “measreportconfig” in logs. All other requirements verified.

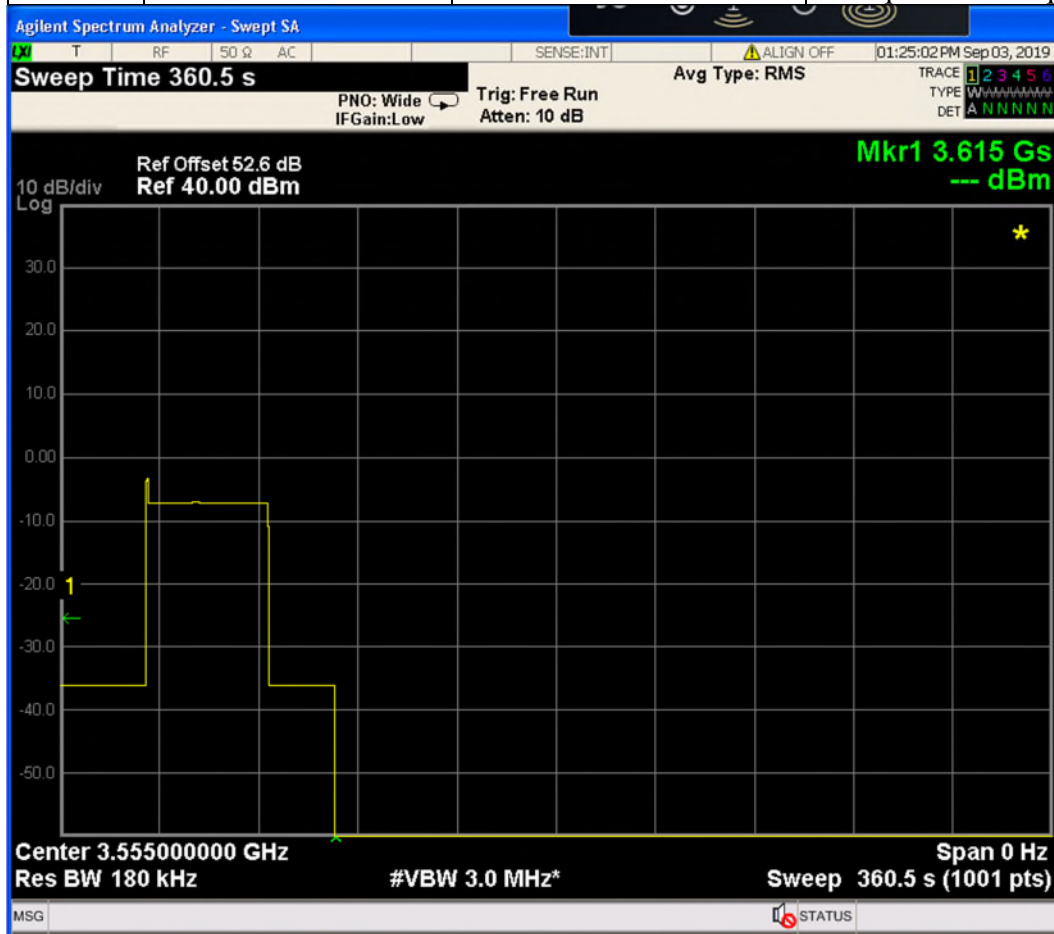
Client	<b>Ericsson</b>	
Product	<b>LTE KRC 161 711/7461 Radio 4408 B48</b>	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

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

Pass. “measreportconfig” in logs. All other requirements verified.


Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
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: <ul style="list-style-type: none"> <li>• CBSD stops transmission at any time prior to sending the relinquishmentRequest message.</li> </ul>	P
-----------	------------------	--	--	---

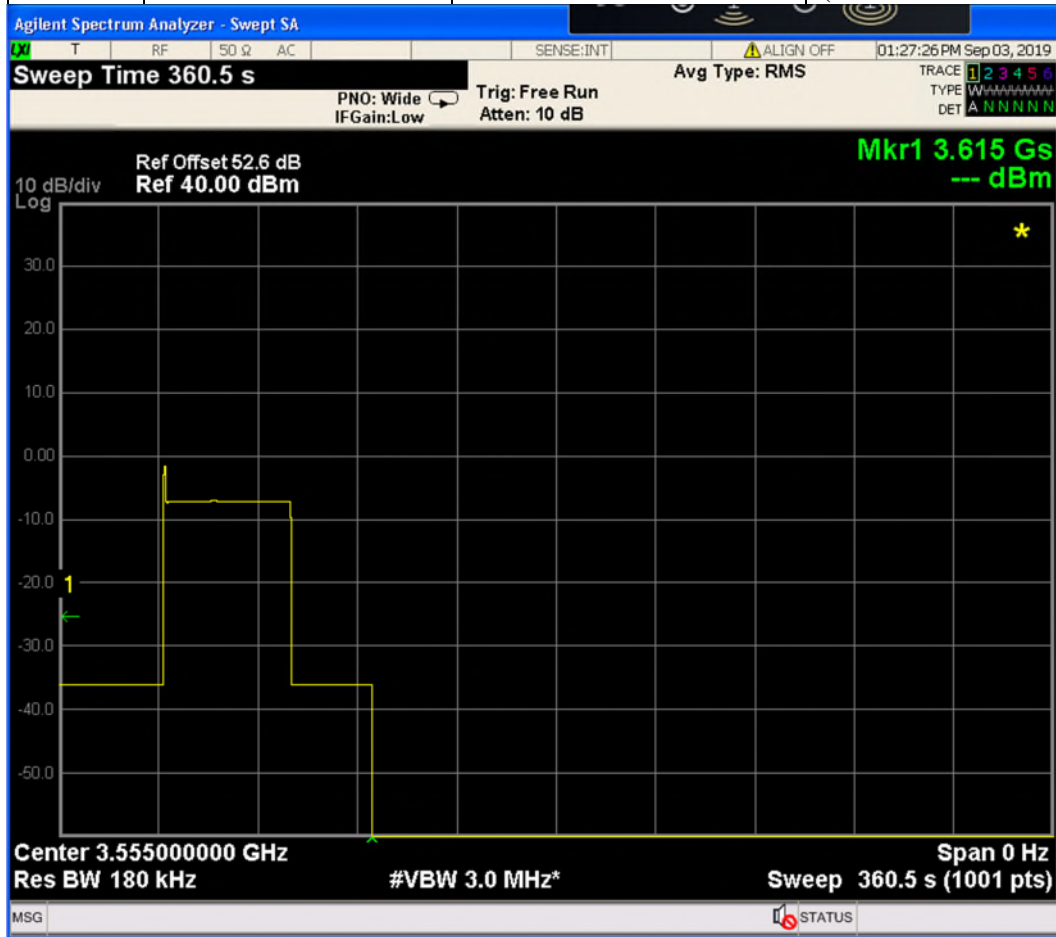


Test Harness logs and timing on graph was verified, the EUT passed the requirement.

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


Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

6.7.4.1.2	WINNF.TT.D.DRG.2	Domain Proxy Successful Deregistration	Monitor RF transmission. Ensure: <ul style="list-style-type: none"> <li>• CBSD stops transmission at any time prior to sending the relinquishmentRequest message or deregistrationRequest message (whichever is sent first)</li> </ul>	P
-----------	------------------	--	--	---




Test Harness logs and timing on graph was verified, the EUT passed the requirement.

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


Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
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.***

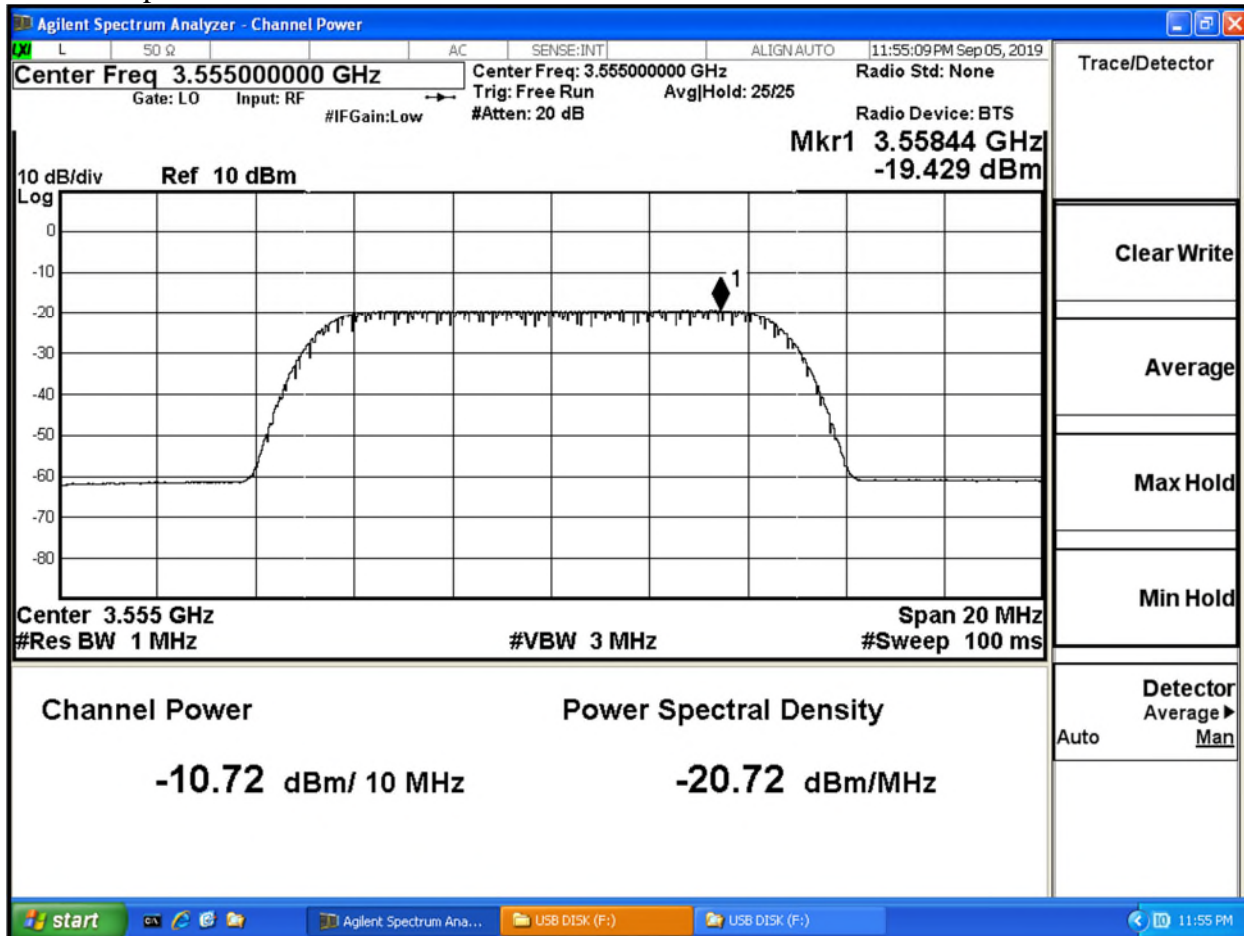
7.1.4.1.1	X	X	WINNF.PT.C.H BT	UUT RF Transmit Power Measurement	<p>Power Spectral Density test case.</p> <p>Assume we use 1 carrier bandwidth (say, 5 or 10 MHz), one frequency (say middle channel in band) for test. Measure at max transmit power, and reduce in steps of 3 dB to minimum declared transmit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

Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	


Freq	1MHz EIRP limit (target) dBm	Raw 10 MHz	Raw 1MHz	External Losses (dB)	Raw dBm/MHz	antenna gain dBi	port s	port gain (dB)	EIRP 1MHz dBm/MHz	EIRP 10 MHz dBm	margi n dB
3555 low	20	-10.7	-19.4	19.93	0.53	12	4	6.02	18.55	27.25	1.45
3555-mid	32	1.3	-7.4	19.93	12.53	12	4	6.02	30.55	39.25	1.45
3555-High	37	-23	-32.8	50.53	17.73	12	4	6.02	35.75	45.55	1.25
3630 low	20	-9.36	18.14	19.93	1.79	12	4	6.02	19.81	28.59	0.19
3630-mid	32	1.74	-6.3	19.93	13.63	12	4	6.02	31.65	39.69	0.35
3630-high	37	-22.79	-31.8	50.53	18.73	12	4	6.02	36.75	45.76	0.25
3695 low	20	-9.53	-18.3	19.93	1.63	12	4	6.02	19.65	28.42	0.35
3695-mid	32		-6.4	19.93	13.53	12	4	6.02	31.55	37.95	0.45
3695-high	37	-22.7	-31.6	50.53	18.93	12	4	6.02	36.95	45.85	0.05

Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

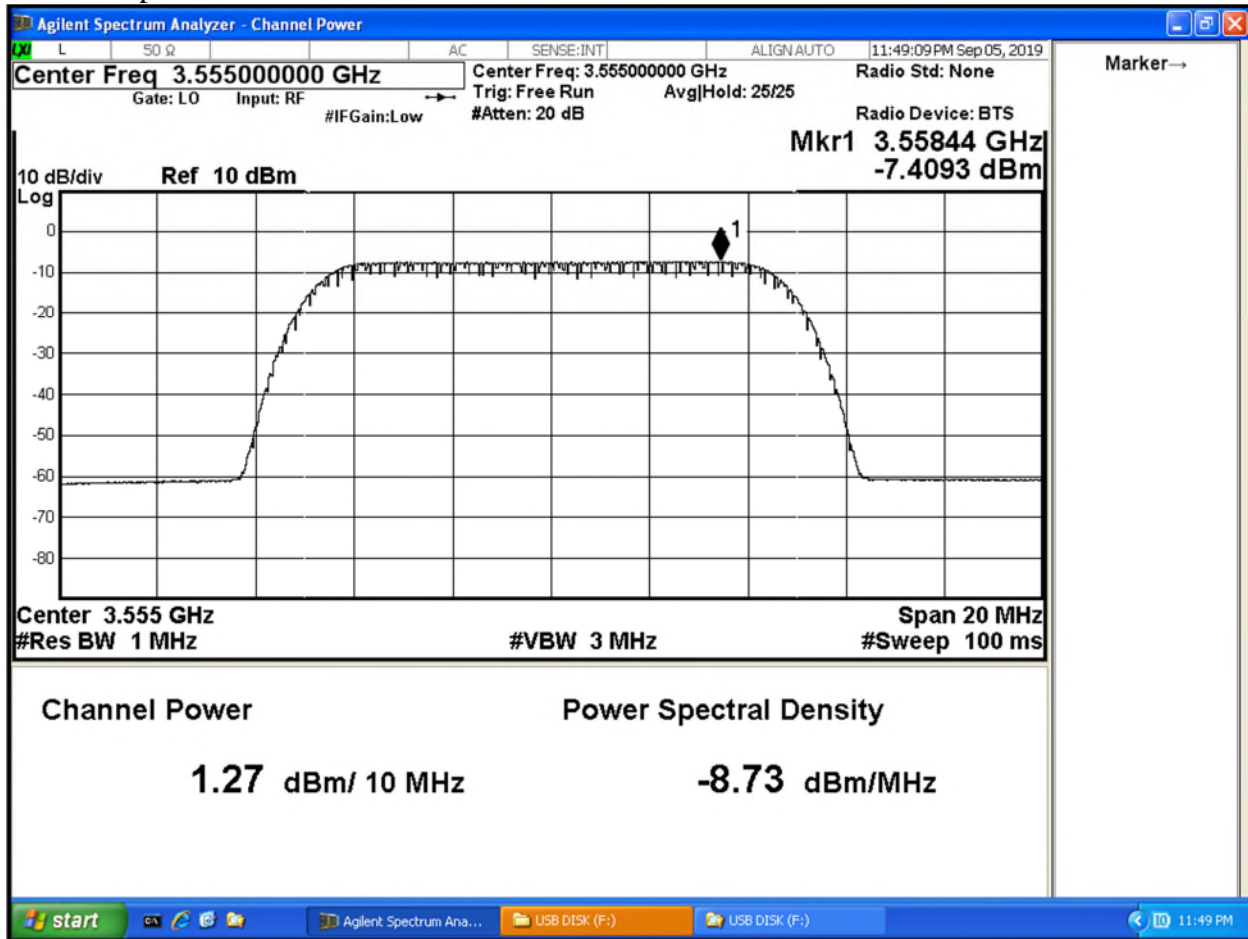
3555 low power






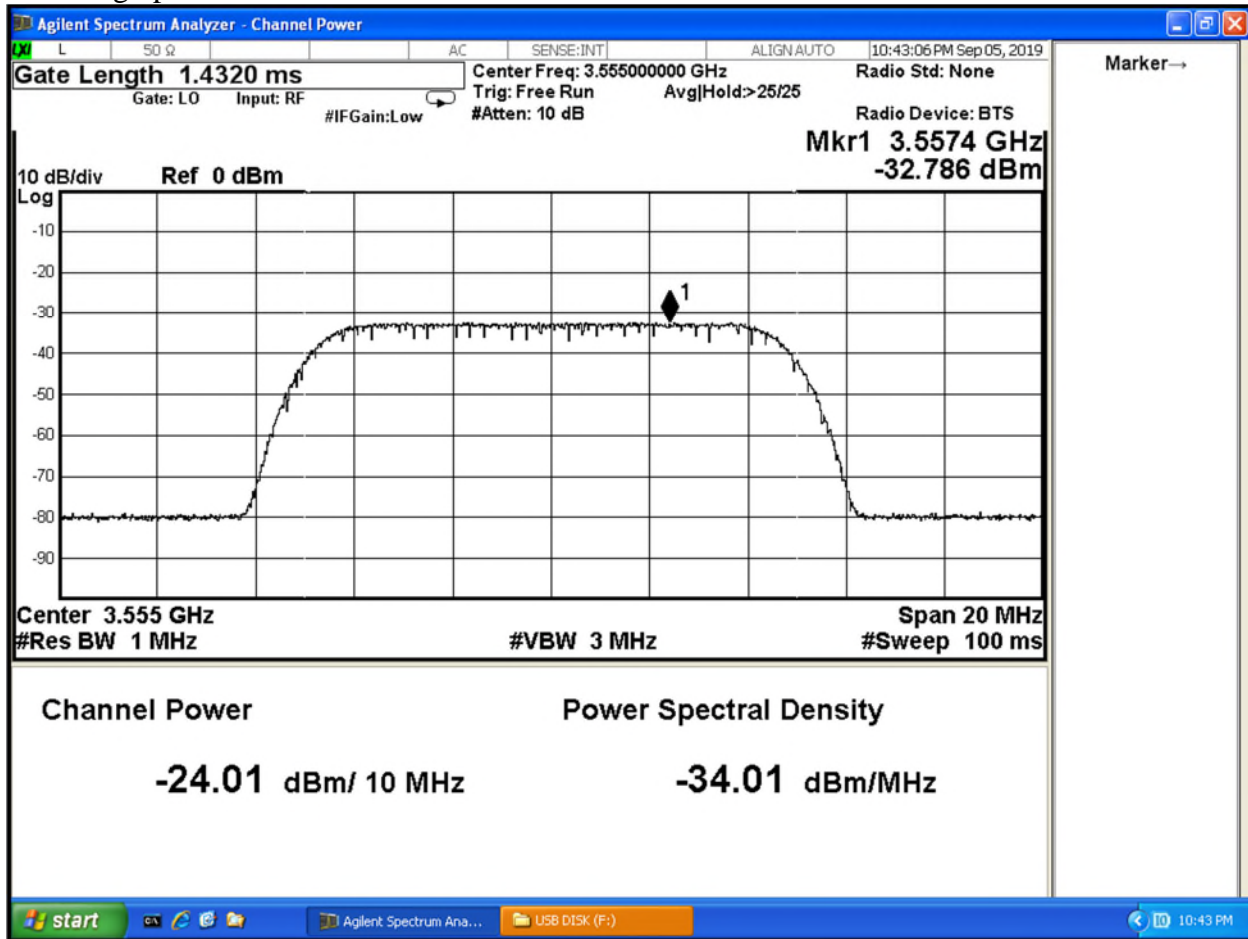
Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	


3555-mid power



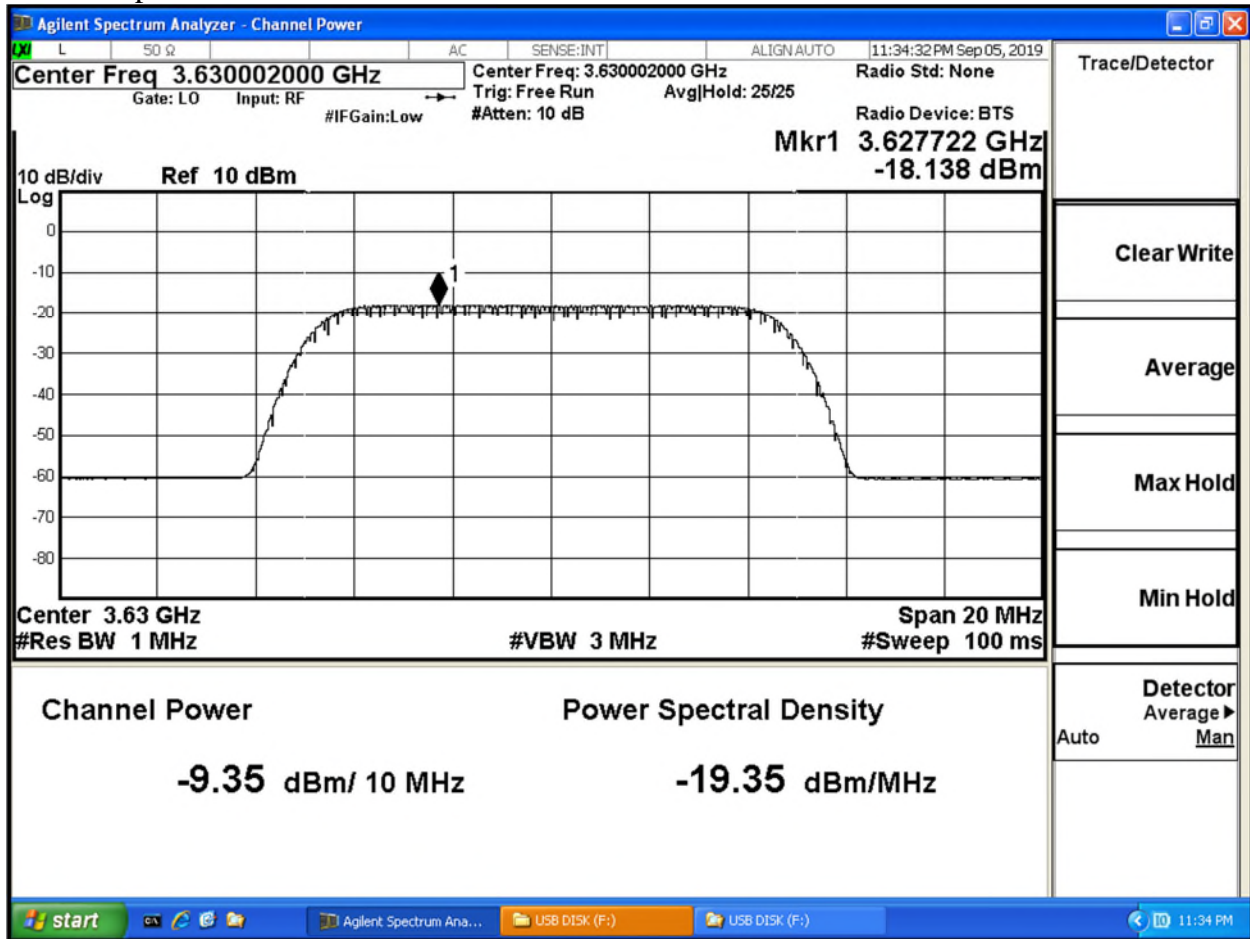
Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	


### 3555-High power



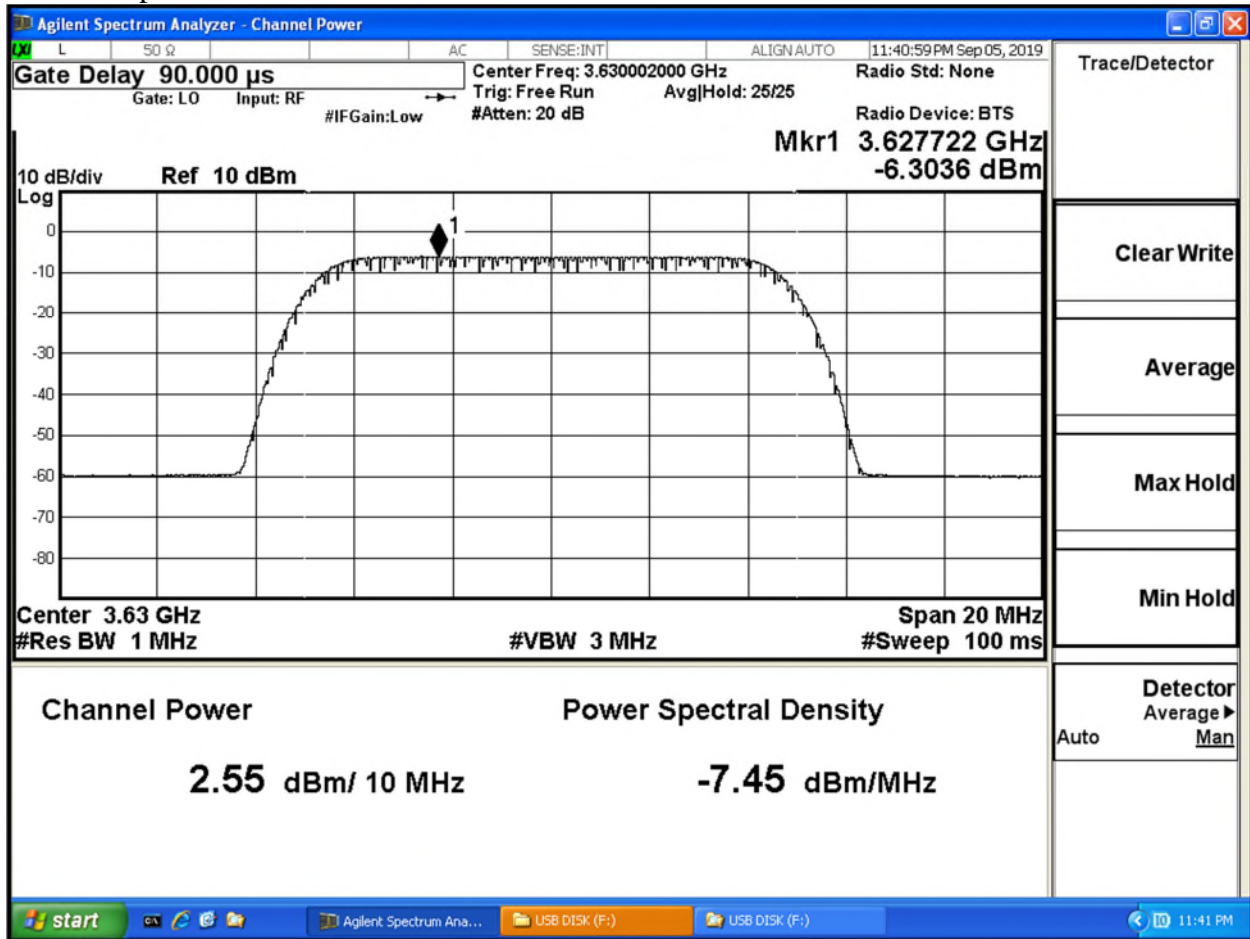
Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	


3630 low power



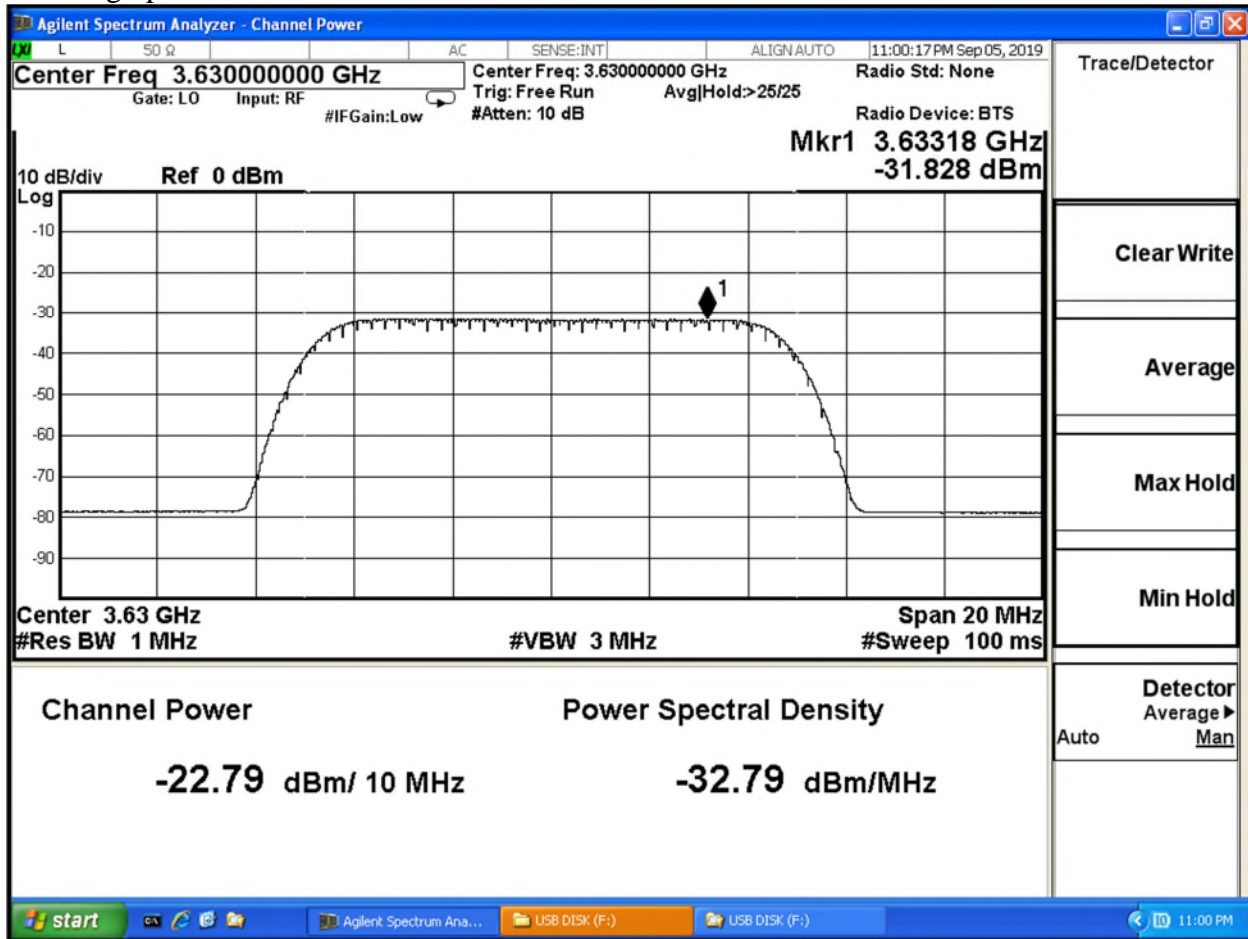
Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	


3630-mid power



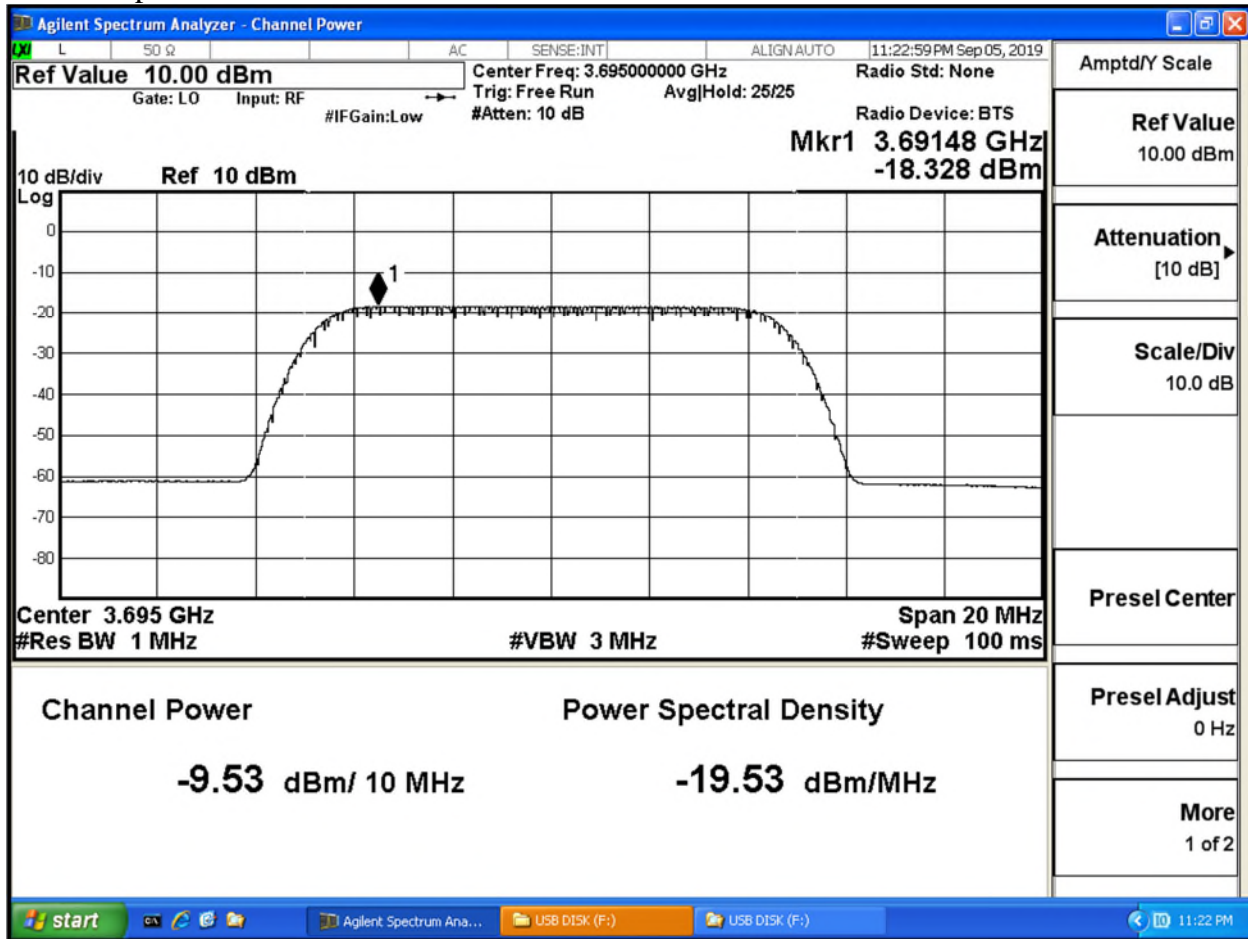
Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

3630-high power




Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

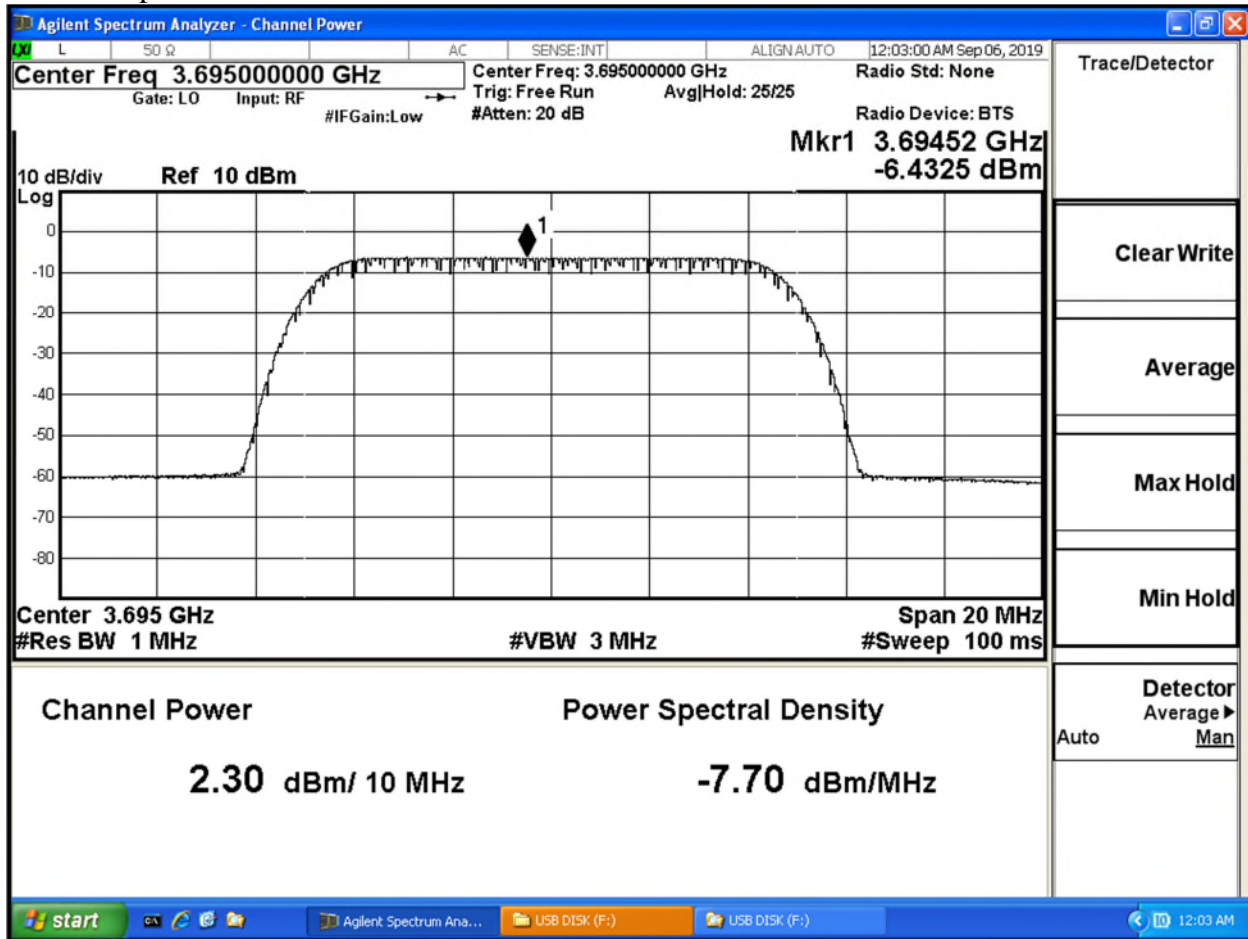
3695 low power






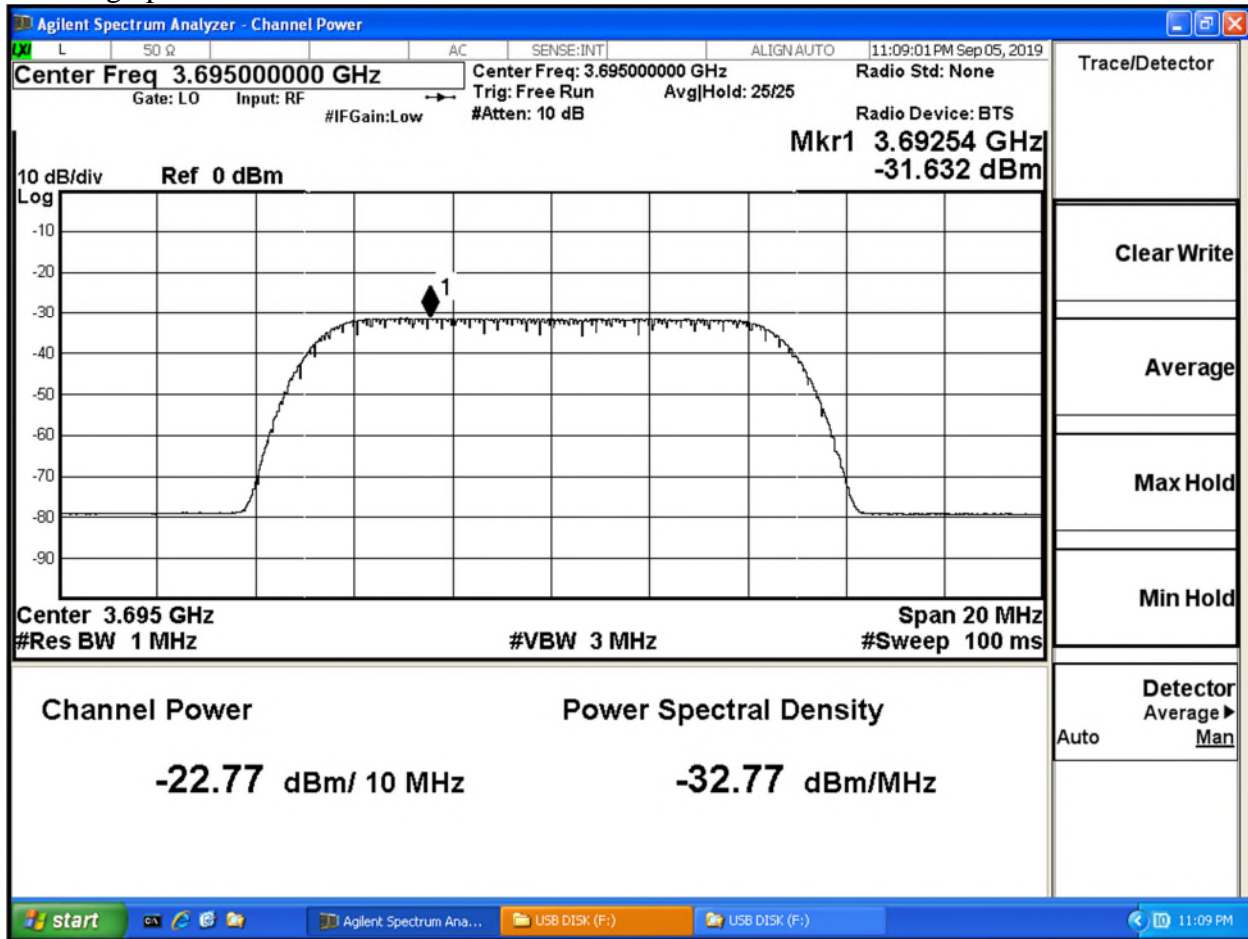
Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

3695-mid power




Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

3695-high power





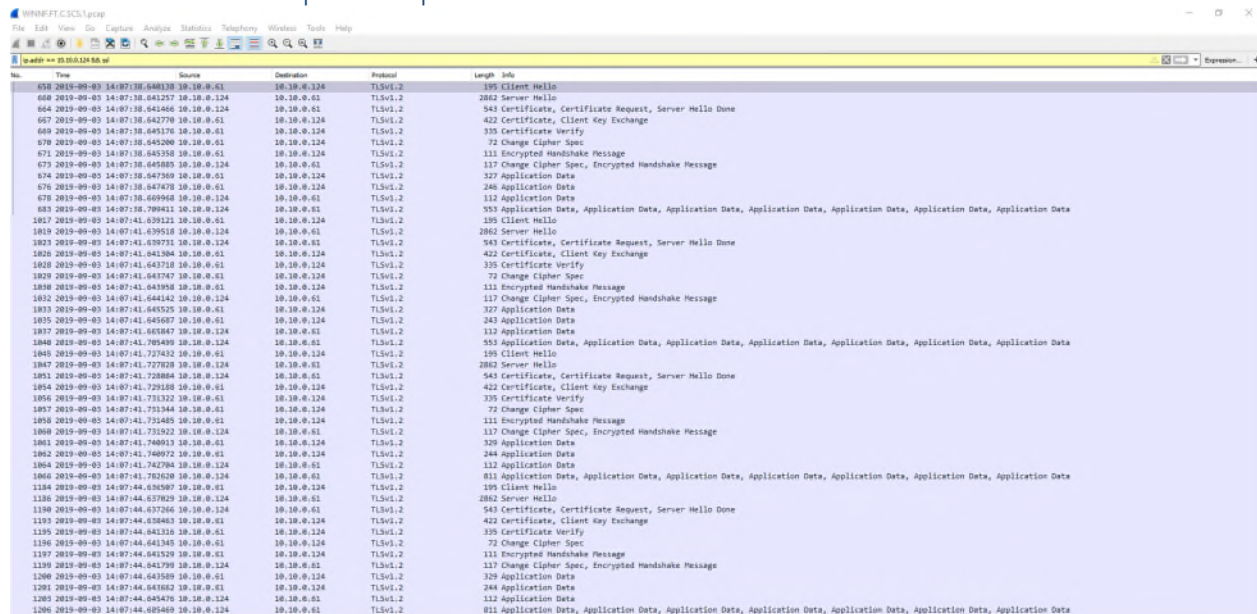
Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

## DOT CBRS Radio: WINNF / Security Test Case Analysis

### WINNF Security Test Case Analysis

#### WINNF.FT.C.SCS.1


#### Packet Capture Sequence



No.	Time	Source	Destination	Protocol	Length	Info
608	2019-09-03 14:07:18.648136	10.10.0.124	10.10.0.61	TLSv1.2	195	Client Hello
609	2019-09-03 14:07:18.648257	10.10.0.124	10.10.0.61	TLSv1.2	2862	Server Hello
610	2019-09-03 14:07:18.648466	10.10.0.124	10.10.0.61	TLSv1.2	543	Certificate, Certificate Request, Server Hello Done
611	2019-09-03 14:07:18.648770	10.10.0.124	10.10.0.61	TLSv1.2	422	Certificate, Client Key Exchange
612	2019-09-03 14:07:18.649176	10.10.0.61	10.10.0.124	TLSv1.2	335	Certificate Verify
613	2019-09-03 14:07:18.649200	10.10.0.61	10.10.0.124	TLSv1.2	72	Change Cipher Spec
614	2019-09-03 14:07:18.649350	10.10.0.61	10.10.0.124	TLSv1.2	111	Encrypted Handshake Message
615	2019-09-03 14:07:18.649580	10.10.0.124	10.10.0.61	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
616	2019-09-03 14:07:18.649769	10.10.0.61	10.10.0.124	TLSv1.2	327	Application Data
617	2019-09-03 14:07:18.649960	10.10.0.124	10.10.0.61	TLSv1.2	246	Application Data
618	2019-09-03 14:07:18.650141	10.10.0.124	10.10.0.61	TLSv1.2	112	Application Data
619	2019-09-03 14:07:18.650321	10.10.0.124	10.10.0.61	TLSv1.2	553	Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data
620	2019-09-03 14:07:18.650502	10.10.0.124	10.10.0.61	TLSv1.2	195	Client Hello
621	2019-09-03 14:07:18.650683	10.10.0.124	10.10.0.61	TLSv1.2	2862	Server Hello
622	2019-09-03 14:07:18.650864	10.10.0.124	10.10.0.61	TLSv1.2	543	Certificate, Certificate Request, Server Hello Done
623	2019-09-03 14:07:18.651045	10.10.0.124	10.10.0.61	TLSv1.2	422	Certificate, Client Key Exchange
624	2019-09-03 14:07:18.651226	10.10.0.61	10.10.0.124	TLSv1.2	335	Certificate Verify
625	2019-09-03 14:07:18.651407	10.10.0.61	10.10.0.124	TLSv1.2	72	Change Cipher Spec
626	2019-09-03 14:07:18.651588	10.10.0.61	10.10.0.124	TLSv1.2	111	Encrypted Handshake Message
627	2019-09-03 14:07:18.651769	10.10.0.124	10.10.0.61	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
628	2019-09-03 14:07:18.651950	10.10.0.61	10.10.0.124	TLSv1.2	327	Application Data
629	2019-09-03 14:07:18.652131	10.10.0.124	10.10.0.61	TLSv1.2	243	Application Data
630	2019-09-03 14:07:18.652312	10.10.0.124	10.10.0.61	TLSv1.2	112	Application Data
631	2019-09-03 14:07:18.652493	10.10.0.124	10.10.0.61	TLSv1.2	553	Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data
632	2019-09-03 14:07:18.652674	10.10.0.124	10.10.0.61	TLSv1.2	195	Client Hello
633	2019-09-03 14:07:18.652855	10.10.0.124	10.10.0.61	TLSv1.2	2862	Server Hello
634	2019-09-03 14:07:18.653036	10.10.0.124	10.10.0.61	TLSv1.2	543	Certificate, Certificate Request, Server Hello Done
635	2019-09-03 14:07:18.653217	10.10.0.124	10.10.0.61	TLSv1.2	422	Certificate, Client Key Exchange
636	2019-09-03 14:07:18.653398	10.10.0.61	10.10.0.124	TLSv1.2	335	Certificate Verify
637	2019-09-03 14:07:18.653579	10.10.0.61	10.10.0.124	TLSv1.2	72	Change Cipher Spec
638	2019-09-03 14:07:18.653760	10.10.0.61	10.10.0.124	TLSv1.2	111	Encrypted Handshake Message
639	2019-09-03 14:07:18.653941	10.10.0.124	10.10.0.61	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
640	2019-09-03 14:07:18.654122	10.10.0.61	10.10.0.124	TLSv1.2	327	Application Data
641	2019-09-03 14:07:18.654303	10.10.0.124	10.10.0.61	TLSv1.2	243	Application Data
642	2019-09-03 14:07:18.654484	10.10.0.124	10.10.0.61	TLSv1.2	112	Application Data
643	2019-09-03 14:07:18.654665	10.10.0.124	10.10.0.61	TLSv1.2	553	Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data
644	2019-09-03 14:07:18.654846	10.10.0.124	10.10.0.61	TLSv1.2	195	Client Hello
645	2019-09-03 14:07:18.655027	10.10.0.124	10.10.0.61	TLSv1.2	2862	Server Hello
646	2019-09-03 14:07:18.655208	10.10.0.124	10.10.0.61	TLSv1.2	543	Certificate, Certificate Request, Server Hello Done
647	2019-09-03 14:07:18.655389	10.10.0.124	10.10.0.61	TLSv1.2	422	Certificate, Client Key Exchange
648	2019-09-03 14:07:18.655570	10.10.0.61	10.10.0.124	TLSv1.2	335	Certificate Verify
649	2019-09-03 14:07:18.655751	10.10.0.61	10.10.0.124	TLSv1.2	72	Change Cipher Spec
650	2019-09-03 14:07:18.655932	10.10.0.61	10.10.0.124	TLSv1.2	111	Encrypted Handshake Message
651	2019-09-03 14:07:18.656113	10.10.0.124	10.10.0.61	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
652	2019-09-03 14:07:18.656294	10.10.0.61	10.10.0.124	TLSv1.2	329	Application Data
653	2019-09-03 14:07:18.656475	10.10.0.124	10.10.0.61	TLSv1.2	244	Application Data
654	2019-09-03 14:07:18.656656	10.10.0.124	10.10.0.61	TLSv1.2	112	Application Data
655	2019-09-03 14:07:18.656837	10.10.0.124	10.10.0.61	TLSv1.2	811	Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data
656	2019-09-03 14:07:18.657018	10.10.0.124	10.10.0.61	TLSv1.2	195	Client Hello
657	2019-09-03 14:07:18.657199	10.10.0.124	10.10.0.61	TLSv1.2	2862	Server Hello
658	2019-09-03 14:07:18.657380	10.10.0.124	10.10.0.61	TLSv1.2	543	Certificate, Certificate Request, Server Hello Done
659	2019-09-03 14:07:18.657561	10.10.0.124	10.10.0.61	TLSv1.2	422	Certificate, Client Key Exchange
660	2019-09-03 14:07:18.657742	10.10.0.61	10.10.0.124	TLSv1.2	335	Certificate Verify
661	2019-09-03 14:07:18.657923	10.10.0.61	10.10.0.124	TLSv1.2	72	Change Cipher Spec
662	2019-09-03 14:07:18.658104	10.10.0.61	10.10.0.124	TLSv1.2	111	Encrypted Handshake Message
663	2019-09-03 14:07:18.658285	10.10.0.124	10.10.0.61	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
664	2019-09-03 14:07:18.658466	10.10.0.61	10.10.0.124	TLSv1.2	329	Application Data
665	2019-09-03 14:07:18.658647	10.10.0.124	10.10.0.61	TLSv1.2	244	Application Data
666	2019-09-03 14:07:18.658828	10.10.0.124	10.10.0.61	TLSv1.2	112	Application Data
667	2019-09-03 14:07:18.659009	10.10.0.124	10.10.0.61	TLSv1.2	811	Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data
668	2019-09-03 14:07:18.659190	10.10.0.124	10.10.0.61	TLSv1.2	195	Client Hello
669	2019-09-03 14:07:18.659371	10.10.0.124	10.10.0.61	TLSv1.2	2862	Server Hello
670	2019-09-03 14:07:18.659552	10.10.0.124	10.10.0.61	TLSv1.2	543	Certificate, Certificate Request, Server Hello Done
671	2019-09-03 14:07:18.659733	10.10.0.124	10.10.0.61	TLSv1.2	422	Certificate, Client Key Exchange
672	2019-09-03 14:07:18.659914	10.10.0.61	10.10.0.124	TLSv1.2	335	Certificate Verify
673	2019-09-03 14:07:18.660095	10.10.0.61	10.10.0.124	TLSv1.2	72	Change Cipher Spec
674	2019-09-03 14:07:18.660276	10.10.0.61	10.10.0.124	TLSv1.2	111	Encrypted Handshake Message
675	2019-09-03 14:07:18.660457	10.10.0.124	10.10.0.61	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
676	2019-09-03 14:07:18.660638	10.10.0.61	10.10.0.124	TLSv1.2	329	Application Data
677	2019-09-03 14:07:18.660819	10.10.0.124	10.10.0.61	TLSv1.2	244	Application Data
678	2019-09-03 14:07:18.661000	10.10.0.124	10.10.0.61	TLSv1.2	112	Application Data
679	2019-09-03 14:07:18.661181	10.10.0.124	10.10.0.61	TLSv1.2	811	Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data
680	2019-09-03 14:07:18.661362	10.10.0.124	10.10.0.61	TLSv1.2	195	Client Hello
681	2019-09-03 14:07:18.661543	10.10.0.124	10.10.0.61	TLSv1.2	2862	Server Hello
682	2019-09-03 14:07:18.661724	10.10.0.124	10.10.0.61	TLSv1.2	543	Certificate, Certificate Request, Server Hello Done
683	2019-09-03 14:07:18.661905	10.10.0.124	10.10.0.61	TLSv1.2	422	Certificate, Client Key Exchange
684	2019-09-03 14:07:18.662086	10.10.0.61	10.10.0.124	TLSv1.2	335	Certificate Verify
685	2019-09-03 14:07:18.662267	10.10.0.61	10.10.0.124	TLSv1.2	72	Change Cipher Spec
686	2019-09-03 14:07:18.662448	10.10.0.61	10.10.0.124	TLSv1.2	111	Encrypted Handshake Message
687	2019-09-03 14:07:18.662629	10.10.0.124	10.10.0.61	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
688	2019-09-03 14:07:18.662810	10.10.0.61	10.10.0.124	TLSv1.2	329	Application Data
689	2019-09-03 14:07:18.662991	10.10.0.124	10.10.0.61	TLSv1.2	244	Application Data
690	2019-09-03 14:07:18.663172	10.10.0.124	10.10.0.61	TLSv1.2	112	Application Data
691	2019-09-03 14:07:18.663353	10.10.0.124	10.10.0.61	TLSv1.2	811	Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data
692	2019-09-03 14:07:18.663534	10.10.0.124	10.10.0.61	TLSv1.2	195	Client Hello
693	2019-09-03 14:07:18.663715	10.10.0.124	10.10.0.61	TLSv1.2	2862	Server Hello
694	2019-09-03 14:07:18.663896	10.10.0.124	10.10.0.61	TLSv1.2	543	Certificate, Certificate Request, Server Hello Done
695	2019-09-03 14:07:18.664077	10.10.0.124	10.10.0.61	TLSv1.2	422	Certificate, Client Key Exchange
696	2019-09-03 14:07:18.664258	10.10.0.61	10.10.0.124	TLSv1.2	335	Certificate Verify
697	2019-09-03 14:07:18.664439	10.10.0.61	10.10.0.124	TLSv1.2	72	Change Cipher Spec
698	2019-09-03 14:07:18.664620	10.10.0.61	10.10.0.124	TLSv1.2	111	Encrypted Handshake Message
699	2019-09-03 14:07:18.664801	10.10.0.124	10.10.0.61	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
700	2019-09-03 14:07:18.664982	10.10.0.61	10.10.0.124	TLSv1.2	329	Application Data
701	2019-09-03 14:07:18.665163	10.10.0.124	10.10.0.61	TLSv1.2	244	Application Data
702	2019-09-03 14:07:18.665344	10.10.0.124	10.10.0.61	TLSv1.2	112	Application Data
703	2019-09-03 14:07:18.665525	10.10.0.124	10.10.0.61	TLSv1.2	811	Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data

#### WINNF test requirements:

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

Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

2	<ul style="list-style-type: none"> <li>• Make sure that Mutual authentication happens between UUT and the SAS Test Harness.</li> <li>• Make sure that UUT uses TLS v1.2</li> <li>• Make sure that cipher suites from one of the following is selected, <ul style="list-style-type: none"> <li>• TLS_RSA_WITH_AES_128_GCM_SHA256</li> <li>• TLS_RSA_WITH_AES_256_GCM_SHA384</li> <li>• TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256</li> <li>• TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384</li> <li>• TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</li> </ul> </li> </ul>	PASS
---	--	------


## Analysis of WINNF Test Requirements

### 1. From Client Hello: TLS version = TLS 1.2

```

> Frame 658: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits)
> Ethernet II, Src: fa:16:3e:17:b4:ec (fa:16:3e:17:b4:ec), Dst: fa:16:3e:41:fa:8b (fa:16:3e:41:fa:8b)
> Internet Protocol Version 4, Src: 10.10.0.61, Dst: 10.10.0.124
> Transmission Control Protocol, Src Port: 55482, Dst Port: 5000, Seq: 1, Ack: 1, Len: 129
✓ Transport Layer Security
  ✓ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 124
  ✓ Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 120
    Version: TLS 1.2 (0x0303)
    > Random: 5d6e73aaa319bed5672f75f9f4ac9b12db5d59130b44f1cc...
    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: 73
    > Extension: supported_groups (len=22)
    > Extension: ec_point_formats (len=2)
    > Extension: signature_algorithms (len=28)
    > Extension: extended_master_secret (len=0)
    > Extension: renegotiation_info (len=1)

```

Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

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

TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
 TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256  
 TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

3. Cipher suite chosen (from Server Hello):

TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256


```

> Frame 660: 2862 bytes on wire (22896 bits), 2862 bytes captured (22896 bits)
> Ethernet II, Src: fa:16:3e:41:fa:8b (fa:16:3e:41:fa:8b), Dst: fa:16:3e:17:b4:ec (fa:16:3e:17:b4:ec)
> Internet Protocol Version 4, Src: 10.10.0.124, Dst: 10.10.0.61
> Transmission Control Protocol, Src Port: 5000, Dst Port: 55482, Seq: 1, Ack: 130, Len: 2796
✓ 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
    Handshake Type: Server Hello (2)
    Length: 77
    Version: TLS 1.2 (0x0303)
  > Random: 5d6e73b5267853f94c269c3818f0a575ac5d562d15e544eb...
    Session ID Length: 32
    Session ID: 22698059d7a584ee0cd7b1905af413c1fa4241c12a49862c...
    Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
    Compression Method: null (0)
    Extensions Length: 5
  > Extension: renegotiation_info (len=1)

```

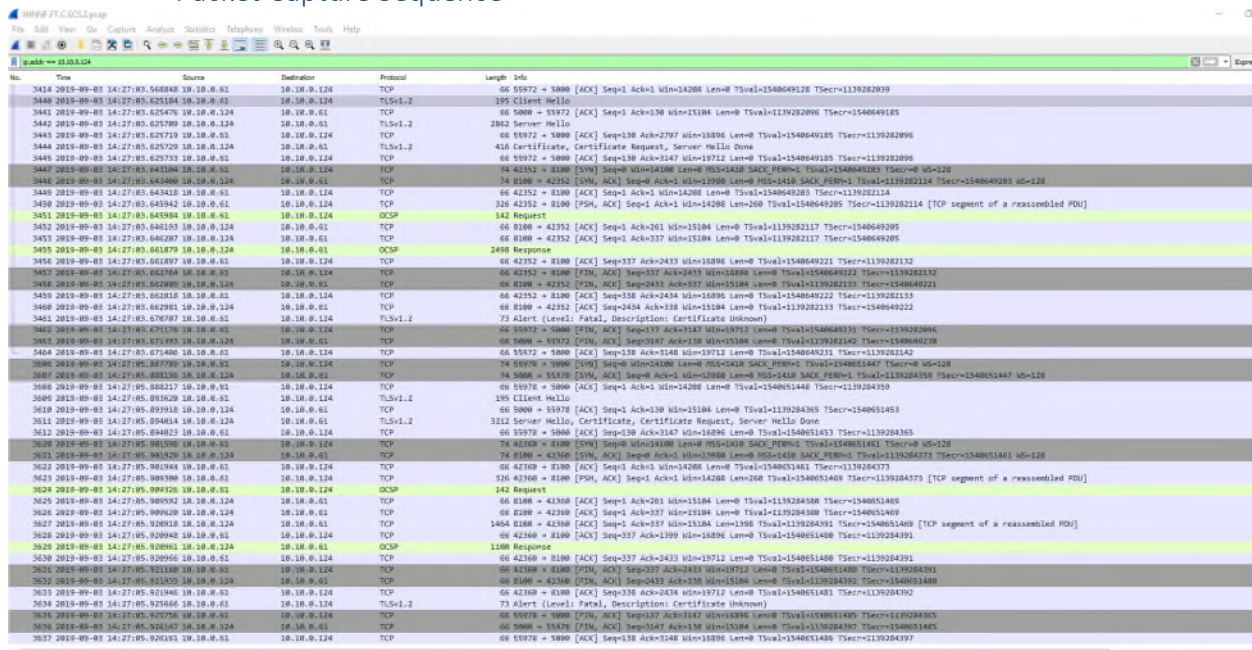
4. The Registration request message arrived at the Test Harness, so authentication was completed.



Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

## WINNF.FT.C.SCS.2

### Packet Capture Sequence



The screenshot displays a Wireshark packet capture sequence. The interface shows a list of packets with columns for No., Time, Source, Destination, Protocol, and Length. The packets are numbered from 3414 to 3537. The protocols include TCP, TLSv1.2, and OSCP. The source and destination IP addresses are 10.10.0.1 and 10.10.0.124. The packets show a sequence of network interactions, including client hello, server hello, certificate exchange, and OSCP requests and responses.


### WINNF Test Requirements:

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

2	<ul style="list-style-type: none"> <li>Make sure that UUT uses TLS v1.2 for security establishment.</li> <li>Make sure UUT selects the correct cipher suite.</li> <li>UUT shall use CRL or OSCP to verify the validity of the server certificate.</li> <li>Make sure that Mutual authentication does not happen between UUT and the SAS Test Harness.</li> </ul>	PASS
---	--	------

### Analysis of WINNF Test Requirements

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

Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

```


> Frame 3440: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits)
> Ethernet II, Src: fa:16:3e:17:b4:ec (fa:16:3e:17:b4:ec), Dst: fa:16:3e:41:fa:8b (fa:16:3e:41:fa:8b)
> Internet Protocol Version 4, Src: 10.10.0.61, Dst: 10.10.0.124
> Transmission Control Protocol, Src Port: 55972, Dst Port: 5000, Seq: 1, Ack: 1, Len: 129
✓ Transport Layer Security
  ✓ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 124
    ✓ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 120
      Version: TLS 1.2 (0x0303)
      > Random: 5d6e7837c5e3315b08e80a896946254509886b3c5b562820...
      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: 73
      > Extension: supported_groups (len=22)
      > Extension: ec_point_formats (len=2)
      > Extension: signature_algorithms (len=28)
      > Extension: extended_master_secret (len=0)
      > Extension: renegotiation_info (len=1)

```

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

TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
 TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256  
 TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

3. From Server Hello, cipher suite chosen:  
 TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256

Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

```

> Frame 3442: 2862 bytes on wire (22896 bits), 2862 bytes captured (22896 bits)
> Ethernet II, Src: fa:16:3e:41:fa:8b (fa:16:3e:41:fa:8b), Dst: fa:16:3e:17:b4:ec (fa:16:3e:17:b4:ec)
> Internet Protocol Version 4, Src: 10.10.0.124, Dst: 10.10.0.61
> Transmission Control Protocol, Src Port: 5000, Dst Port: 55972, Seq: 1, Ack: 130, Len: 2796
✓ 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
      Handshake Type: Server Hello (2)
      Length: 77
      Version: TLS 1.2 (0x0303)
      > Random: 5d6e7842d84d8cbfc7078fe9e913fcf7eb0fe3354f54f192...
      Session ID Length: 32
      Session ID: e50dd1e43d8d5028f12ae61800ad52ffd4fe63dce8630ea5...
      Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
      Compression Method: null (0)
      Extensions Length: 5
      > Extension: renegotiation_info (len=1)

```


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

```

> Frame 3451: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits)
> Ethernet II, Src: fa:16:3e:17:b4:ec (fa:16:3e:17:b4:ec), Dst: fa:16:3e:41:fa:8b (fa:16:3e:41:fa:8b)
> Internet Protocol Version 4, Src: 10.10.0.61, Dst: 10.10.0.124
> Transmission Control Protocol, Src Port: 42352, Dst Port: 8100, Seq: 261, Ack: 1, Len: 76
> [2 Reassembled TCP Segments (336 bytes): #3450(260), #3451(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: 5b63d7bb6e95ca42c49450451b47e5cd6ee1fdb4
            serialNumber: 18248749012425898463

```



Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

```

> Frame 3455: 2498 bytes on wire (19984 bits), 2498 bytes captured (19984 bits)
> Ethernet II, Src: fa:16:3e:41:fa:8b (fa:16:3e:41:fa:8b), Dst: fa:16:3e:17:b4:ec (fa:16:3e:17:b4:ec)
> Internet Protocol Version 4, Src: 10.10.0.124, Dst: 10.10.0.61
> Transmission Control Protocol, Src Port: 8100, Dst Port: 42352, Seq: 1, Ack: 337, Len: 2432
> Hypertext Transfer Protocol
> Online Certificate Status Protocol
  responseStatus: successful (0)
  responseBytes
    responseType: Id: 1.3.6.1.5.5.7.40.1.1 (id-pkix-ocsp-basic)
    basicOCSPResponse
      tbsResponseData
        responderID: byName (1)
        producedAt: 2019-09-03 14:27:14 (UTC)
        responses: 1 item
          singleResponse
            certID
              hashAlgorithm (SHA-1)
                algorithmId: 1.3.14.3.2.26 (SHA-1)
                issuerNameHash: 5368d21d2529427538588c5ccba4c4e6f3b96641
                issuerKeyHash: 5b63d7bb6e95ca42c49450451b47e5cd6eefdb4
                serialNumber: 18240749012425898463
              certStatus: revoked (1)
                revoked
                  revocationTime: 2019-09-02 13:59:41 (UTC)
                  thisUpdate: 2019-09-03 14:27:14 (UTC)
            signatureAlgorithm (sha1WithRSAEncryption)
              algorithmId: 1.2.840.113549.1.1.5 (sha1WithRSAEncryption)
              padding: 0
              signature: 906f60430a1260eb9d7e21c1f2049042f94c7f6ee489ad67...
          certs: 1 item
            certificate (id-at-commonName=SAS.OCSP.EXAMPLE,id-at-organizationalUnitName=WiInnForum SAS OCSP Responder Certi,id-at-organizationName=Test Lab for FCC PART 96,id-at-countryName=US)
              signedCertificate
                algorithmIdentifier (sha256WithRSAEncryption)
                  padding: 0
                  encrypted: 88a547c487789b3ad084c353a8cc7d0ff2c507626c62494b...

```

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

```


> Frame 3461: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
> Ethernet II, Src: fa:16:3e:17:b4:ec (fa:16:3e:17:b4:ec), Dst: fa:16:3e:41:fa:8b (fa:16:3e:41:fa:8b)
> Internet Protocol Version 4, Src: 10.10.0.61, Dst: 10.10.0.124
> Transmission Control Protocol, Src Port: 55972, Dst Port: 5000, Seq: 130, Ack: 3147, Len: 7
> Transport Layer Security
  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)

```

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





Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

```


> Frame 893: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits)
> Ethernet II, Src: fa:16:3e:17:b4:ec (fa:16:3e:17:b4:ec), Dst: fa:16:3e:41:fa:8b (fa:16:3e:41:fa:8b)
> Internet Protocol Version 4, Src: 10.10.0.61, Dst: 10.10.0.124
> Transmission Control Protocol, Src Port: 55560, Dst Port: 5000, Seq: 1, Ack: 1, Len: 129
▼ Transport Layer Security
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 124
    ▼ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 120
      Version: TLS 1.2 (0x0303)
      > Random: 5d6e74c8e3b9907c8bf1d8d3b2e41de44ff3d4d88a2df236...
      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: 73
      > Extension: supported_groups (len=22)
      > Extension: ec_point_formats (len=2)
      > Extension: signature_algorithms (len=28)
      > Extension: extended_master_secret (len=0)
      > Extension: renegotiation_info (len=1)

```

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

TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
 TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256  
 TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

3. From Server Hello, cipher suite chosen:  
 TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256

Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

```

> Frame 895: 3213 bytes on wire (25704 bits), 3213 bytes captured (25704 bits)
> Ethernet II, Src: fa:16:3e:41:fa:8b (fa:16:3e:41:fa:8b), Dst: fa:16:3e:17:b4:ec (fa:16:3e:17:b4:ec)
> Internet Protocol Version 4, Src: 10.10.0.124, Dst: 10.10.0.61
> Transmission Control Protocol, Src Port: 5000, Dst Port: 55560, Seq: 1, Ack: 130, Len: 3147
✓ 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
      Handshake Type: Server Hello (2)
      Length: 77
      Version: TLS 1.2 (0x0303)
      > Random: 5d6e74d363b38c017e0456ec16e593567a70151d81f72696...
      Session ID Length: 32
      Session ID: 9736c983db797e9cedf3a8d3ff5cde8d50f9f0d983a75c99...
      Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
      Compression Method: null (0)
      Extensions Length: 5
      > Extension: renegotiation_info (len=1)
    > TLSv1.2 Record Layer: Handshake Protocol: Certificate
    > TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages

```

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


```

> Frame 897: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
> Ethernet II, Src: fa:16:3e:17:b4:ec (fa:16:3e:17:b4:ec), Dst: fa:16:3e:41:fa:8b (fa:16:3e:41:fa:8b)
> Internet Protocol Version 4, Src: 10.10.0.61, Dst: 10.10.0.124
> Transmission Control Protocol, Src Port: 55560, Dst Port: 5000, Seq: 130, Ack: 3148, Len: 7
✓ Transport Layer Security
  ✓ 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)

```

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



Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

```

> Frame 636: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits)
> Ethernet II, Src: fa:16:3e:17:b4:ec (fa:16:3e:17:b4:ec), Dst: fa:16:3e:41:fa:8b (fa:16:3e:41:fa:8b)
> Internet Protocol Version 4, Src: 10.10.0.61, Dst: 10.10.0.124
> Transmission Control Protocol, Src Port: 55648, Dst Port: 5000, Seq: 1, Ack: 1, Len: 129
✓ Transport Layer Security
  ✓ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 124
    ✓ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 120
      Version: TLS 1.2 (0x0303)
      > Random: 5d6e75b8e4794caba494c3d4e26398551122b1995d332a19...
      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: 73
      > Extension: supported_groups (len=22)
      > Extension: ec_point_formats (len=2)
      > Extension: signature_algorithms (len=28)
      > Extension: extended_master_secret (len=0)
      > Extension: renegotiation_info (len=1)


```

- 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

- From Server Hello, cipher suite chosen:  
 TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256



Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

```

> Frame 638: 3243 bytes on wire (25944 bits), 3243 bytes captured (25944 bits)
> Ethernet II, Src: fa:16:3e:41:fa:8b (fa:16:3e:41:fa:8b), Dst: fa:16:3e:17:b4:ec (fa:16:3e:17:b4:ec)
> Internet Protocol Version 4, Src: 10.10.0.124, Dst: 10.10.0.61
> Transmission Control Protocol, Src Port: 5000, Dst Port: 55648, Seq: 1, Ack: 130, Len: 3177
✓ 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
    Handshake Type: Server Hello (2)
    Length: 77
    Version: TLS 1.2 (0x0303)
    > Random: 5d6e75c348790b56a8a2b2e56c0448af8a18c8b5f0ca8790...
    Session ID Length: 32
    Session ID: 51f334de8b50d6a093491444515eaa5feb9995af54e66e30...
    Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
    Compression Method: null (0)
    Extensions Length: 5
    > Extension: renegotiation_info (len=1)
  > TLSv1.2 Record Layer: Handshake Protocol: Certificate
  > TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages

```


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

```

> Frame 640: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
> Ethernet II, Src: fa:16:3e:17:b4:ec (fa:16:3e:17:b4:ec), Dst: fa:16:3e:41:fa:8b (fa:16:3e:41:fa:8b)
> Internet Protocol Version 4, Src: 10.10.0.61, Dst: 10.10.0.124
> Transmission Control Protocol, Src Port: 55648, Dst Port: 5000, Seq: 130, Ack: 3178, Len: 7
✓ Transport Layer Security
  ✓ 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)

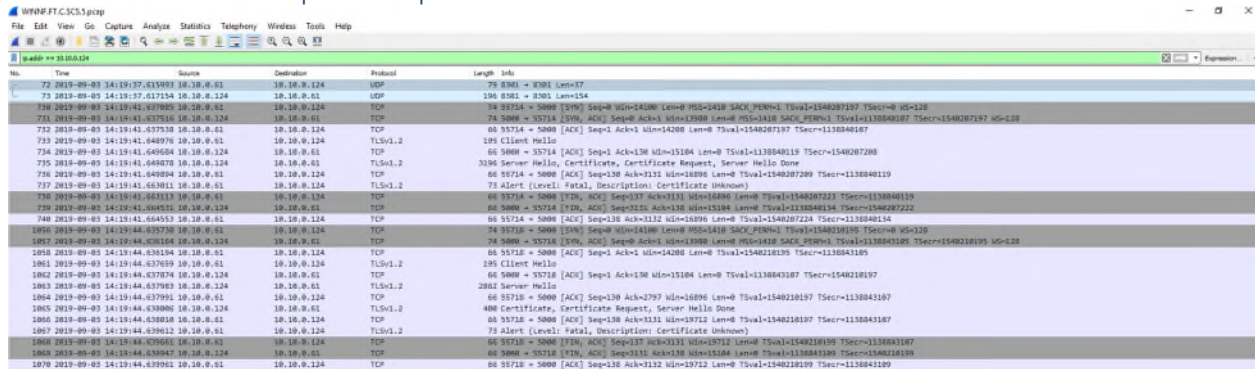
```

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

Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

## WINNF.FT.C.SCS.5

### Packet Capture Sequence



No.	Time	Source	Destination	Protocol	Length	Info
72	2019-09-03 14:19:37.615993	10.10.9.124	10.10.9.124	UDP	78	8301 → 8301 [Len=57]
73	2019-09-03 14:19:37.617154	10.10.9.124	10.10.9.124	UDP	190	8301 → 8301 [Len=154]
719	2019-09-03 14:19:40.637965	10.10.9.124	10.10.9.124	TCP	74	83716 → 5000 [SYN] Seq=0 Win=14180 Len=0 MSS=1418 SACK_PERM=1 TSval=1540207197 TSecr=0 WS=128
721	2019-09-03 14:19:41.637510	10.10.9.124	10.10.9.124	TCP	74	5000 → 83716 [SYN, ACK] Seq=0 Ack=1 Win=0 MSS=1418 SACK_PERM=1 TSval=1138840187 TSecr=1540207197 WS=128
732	2019-09-03 14:19:41.637510	10.10.9.124	10.10.9.124	TCP	60	83716 → 5000 [ACK] Seq=1 Ack=136 Win=0 TSval=1540207197 TSecr=1138840187
733	2019-09-03 14:19:41.640970	10.10.9.124	10.10.9.124	TLSv1.2	295	Client Hello
734	2019-09-03 14:19:41.640970	10.10.9.124	10.10.9.124	TCP	60	5000 → 83716 [ACK] Seq=1 Ack=136 Win=0 TSval=1138840119 TSecr=1540207208
735	2019-09-03 14:19:41.640970	10.10.9.124	10.10.9.124	TLSv1.2	3394	Server Hello, Certificate, Certificate Request, Server Hello Done
736	2019-09-03 14:19:41.640970	10.10.9.124	10.10.9.124	TCP	60	83716 → 5000 [ACK] Seq=130 Ack=131 Win=16896 Len=0 TSval=1540207209 TSecr=1138840119
737	2019-09-03 14:19:41.643011	10.10.9.124	10.10.9.124	TLSv1.2	73	Alert (Level: Fatal, Description: Certificate unknown)
738	2019-09-03 14:19:41.643113	10.10.9.124	10.10.9.124	TCP	60	83716 → 5000 [FIN, ACK] Seq=137 Ack=131 Win=16896 Len=0 TSval=1540207213 TSecr=1138840119
739	2019-09-03 14:19:41.643113	10.10.9.124	10.10.9.124	TCP	60	5000 → 83716 [FIN, ACK] Seq=138 Ack=136 Win=0 Len=0 TSval=1138840134 TSecr=1540207222
740	2019-09-03 14:19:41.644553	10.10.9.124	10.10.9.124	TCP	60	83716 → 5000 [ACK] Seq=138 Ack=132 Win=16896 Len=0 TSval=1540207219 TSecr=1138840119
1896	2019-09-03 14:19:44.637510	10.10.9.124	10.10.9.124	TCP	74	83716 → 5000 [SYN] Seq=0 Win=14180 Len=0 MSS=1418 SACK_PERM=1 TSval=1540210195 TSecr=0 WS=128
1897	2019-09-03 14:19:44.638164	10.10.9.124	10.10.9.124	TCP	74	5000 → 83716 [SYN, ACK] Seq=0 Ack=1 Win=0 MSS=1418 SACK_PERM=1 TSval=1138841195 TSecr=1540210195 WS=128
1898	2019-09-03 14:19:44.638164	10.10.9.124	10.10.9.124	TCP	60	83716 → 5000 [ACK] Seq=1 Ack=136 Win=0 TSval=1540210195 TSecr=1138841195
1899	2019-09-03 14:19:44.637619	10.10.9.124	10.10.9.124	TLSv1.2	295	Client Hello
1900	2019-09-03 14:19:44.637619	10.10.9.124	10.10.9.124	TCP	60	5000 → 83716 [ACK] Seq=1 Ack=136 Win=0 TSval=1138841187 TSecr=1540210197
1901	2019-09-03 14:19:44.637619	10.10.9.124	10.10.9.124	TCP	2862	Server Hello
1902	2019-09-03 14:19:44.637619	10.10.9.124	10.10.9.124	TCP	60	83716 → 5000 [ACK] Seq=130 Ack=1797 Win=16896 Len=0 TSval=1540210197 TSecr=1138841187
1903	2019-09-03 14:19:44.638006	10.10.9.124	10.10.9.124	TLSv1.2	408	Certificate, Certificate Request, Server Hello Done
1904	2019-09-03 14:19:44.638006	10.10.9.124	10.10.9.124	TCP	60	83716 → 5000 [ACK] Seq=130 Ack=1511 Win=13712 Len=0 TSval=1540210197 TSecr=1138841187
1905	2019-09-03 14:19:44.638006	10.10.9.124	10.10.9.124	TCP	73	Alert (Level: Fatal, Description: Certificate unknown)
1906	2019-09-03 14:19:44.638006	10.10.9.124	10.10.9.124	TCP	60	83716 → 5000 [FIN, ACK] Seq=137 Ack=131 Win=13712 Len=0 TSval=1540210199 TSecr=1138841187
1907	2019-09-03 14:19:44.638006	10.10.9.124	10.10.9.124	TCP	60	5000 → 83716 [FIN, ACK] Seq=138 Ack=136 Win=16896 Len=0 TSval=1138841189 TSecr=1540210199
1978	2019-09-03 14:19:44.637965	10.10.9.124	10.10.9.124	TCP	60	83716 → 5000 [ACK] Seq=138 Ack=132 Win=16896 Len=0 TSval=1540210199 TSecr=1138841189


### WINNF Test Requirements:

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

2	<ul style="list-style-type: none"> <li>Make sure that UUT uses TLS v1.2 for security establishment.</li> <li>Make sure UUT selects the correct cipher suite.</li> <li>UUT shall use CRL or OCSP to verify the validity of the server certificate.</li> <li>Make sure that Mutual authentication does not happen between UUT and the SAS Test Harness.</li> </ul>	PASS
---	--	------

### Analysis of WINNF Test Requirements

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

Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

```


> Frame 733: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits)
> Ethernet II, Src: fa:16:3e:17:b4:ec (fa:16:3e:17:b4:ec), Dst: fa:16:3e:41:fa:8b (fa:16:3e:41:fa:8b)
> Internet Protocol Version 4, Src: 10.10.0.61, Dst: 10.10.0.124
> Transmission Control Protocol, Src Port: 55714, Dst Port: 5000, Seq: 1, Ack: 1, Len: 129
✓ Transport Layer Security
  ✓ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 124
    ✓ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 120
      Version: TLS 1.2 (0x0303)
      > Random: 5d6e767d62c21254967019646a3fc8da4d00c8eca5e78cc9...
      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: 73
      > Extension: supported_groups (len=22)
      > Extension: ec_point_formats (len=2)
      > Extension: signature_algorithms (len=28)
      > Extension: extended_master_secret (len=0)
      > Extension: renegotiation_info (len=1)

```

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

TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256  
 TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256  
 TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256

3. From Server Hello, cipher suite chosen:  
 TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256

Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

```

> Frame 735: 3196 bytes on wire (25568 bits), 3196 bytes captured (25568 bits)
> Ethernet II, Src: fa:16:3e:41:fa:8b (fa:16:3e:41:fa:8b), Dst: fa:16:3e:17:b4:ec (fa:16:3e:17:b4:ec)
> Internet Protocol Version 4, Src: 10.10.0.124, Dst: 10.10.0.61
> Transmission Control Protocol, Src Port: 5000, Dst Port: 55714, Seq: 1, Ack: 130, Len: 3130
▼ 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
      Handshake Type: Server Hello (2)
      Length: 77
      Version: TLS 1.2 (0x0303)
      > Random: 5d6e768814d017b54b1c55f0176bf996f1b41c32231ba2fd...
      Session ID Length: 32
      Session ID: fb8025d3eec7ffc9f97f61f574942c6276f822812fac30f4...
      Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
      Compression Method: null (0)
      Extensions Length: 5
      > Extension: renegotiation_info (len=1)
    > TLSv1.2 Record Layer: Handshake Protocol: Certificate
    > TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages

```

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


```

> Frame 737: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
> Ethernet II, Src: fa:16:3e:17:b4:ec (fa:16:3e:17:b4:ec), Dst: fa:16:3e:41:fa:8b (fa:16:3e:41:fa:8b)
> Internet Protocol Version 4, Src: 10.10.0.61, Dst: 10.10.0.124
> Transmission Control Protocol, Src Port: 55714, Dst Port: 5000, Seq: 130, Ack: 3131, Len: 7
▼ Transport Layer Security
  ▼ 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)

```


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




Client	<b>Ericsson</b>	
Product	<b>LTE KRC 161 711/7461 Radio 4408 B48</b>	
Standard(s)	<b>FCC Part 96 SAS requirements (CBRS Test Plan)</b>	

## Test Equipment

Instrument	Manufacturer	Type No.	Serial No	Calibration Period (months)	Calibration Due
Power Supply	Xantrex	XKW 60-50	E00109863	O/P Mon	-
Signal Analyzer	Agilent	MXA	SSG013930	12 months	2020-01-15
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	-


Client	<b>Ericsson</b>	
Product	<b>LTE KRC 161 711/7461 Radio 4408 B48</b>	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

## Appendix A – EUT & Client Provided Details

Client	<b>Ericsson</b>	
Product	<b>LTE KRC 161 711/7461 Radio 4408 B48</b>	
Standard(s)	<b>FCC Part 96 SAS requirements (CBRS Test Plan)</b>	

#### General EUT Description

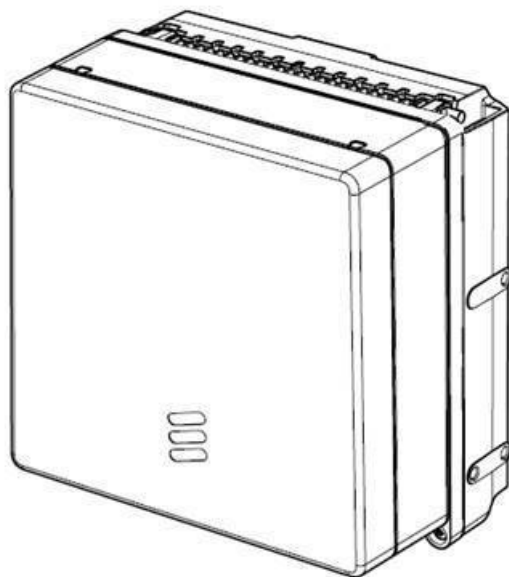
Manufacturer	Ericsson
Address	Torshamnsgatan 23 Kista SE-16480 Stockholm Sweden
Product Name	Radio 4408 B48
Product Number	KRC 161 746/1
Serial Number(s)	D829203626
Software Version	CXP 901 3268/15_R79GC
Hardware Version	R1B
Test Specification/Issue/Date	FCC CFR 47 Part 96: 2018

Client	<b>Ericsson</b>	
Product	<b>LTE KRC 161 711/7461 Radio 4408 B48</b>	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

### Technical Description

The Equipment Under Test (EUT) Radio 4408 B48 KRC 161 746/1 is an Ericsson AB Radio Unit working in the public mobile service (3550-3700 MHz) band which provides communication connections to 3550-3700 MHz network. The Radio 4408 B48 KRC 161 746/1 operates from a -48V DC or a 120V AC power supply.

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




### 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.

Domain Proxy Software Version: = 1.36.1 (ENM version ENM 19.14)

Client	<b>Ericsson</b>	
Product	<b>LTE KRC 161 711/7461 Radio 4408 B48</b>	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

## Appendix B – EUT, Peripherals, and Test Setup Photos

Client	Ericsson	
Product	LTE KRC 161 711/7461 Radio 4408 B48	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

## Test setup

