

Test Report

As per

FCC Part 96 SAS requirements (CBRS Test Plan)

on the

KRD 901 254 Air 3268 B48 (3550-3700MHz)

FCC ID(s): TA8AKRD901254



**Add value.
Inspire trust.**

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

Testing produced
for

Ericsson Canada

See Appendix A for
full client & EUT
details.

Steve McFarlane.
Test Personnel

Handwritten signature of Steve McFarlane in black ink, positioned above a horizontal line.

Scott Drysdale
Report Reviewer

Handwritten signature of Scott Drysdale in black ink, positioned above a horizontal line.



Testing Laboratory
Certificate #2955.19

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
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
Check the device registration and authorization with the SAS.....	29
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.	29
Appendix A – EUT & Client Provided Details	67
Technical Description	69
Appendix B – EUT, Peripherals, and Test Setup Photos.....	70

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Report Scope

This report addresses the EMC verification testing and test results of the **Ericsson Remote Radio Air 3268 B48 KRD 901 254 (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	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
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)	Ericsson Remote Radio Air 3268 B48 KRD 901 254 (3550-3700MHz)
EUT passed all tests performed	Yes
Tests conducted by	Steve McFarlane / Scott Drysdale


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

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
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	N/A

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
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	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
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	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
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 (DEREGISTER)	<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	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
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_PARAMETER)	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	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	


					<p>(this is not a pass/fail criteria, but check)</p> <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 transmitExpirationTime+60 seconds, where transmitExpirationTime 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	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

6.5.4.2.3	X	X	WINNF.FT.C.MES.3	Grant Response contains measReportConfig	No RF monitoring	P
6.5.4.2.4	X	--	WINNF.FT.C.MES.4	Heartbeat Response contains measReportConfig	No RF monitoring	N/A
6.5.4.2.5	--	X	WINNF.FT.D.MES.5	Domain Proxy Heartbeat Response contains measReportConfig	No RF monitoring	P
6.6.4.1.1	X	--	WINNF.FT.C.RLQ.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.RLQ.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.DRG.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	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
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 relinquishmentReque st message or deregistrationReques t 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	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
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	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
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.

Test results were obtained using the KRD 901 254/31 model, the client attests the test results are representative or worst case of all models as listed in appendix A

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)
- 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.

Additional testing for power spectral density (PSD) requirements were evaluated as the original EUT firmware was changed to allow for higher conducted power with different antenna gains. All other parameters were deemed to not be affected as there was no other changes.

Logs are kept on file.

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
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 V1.0.2 CBSD/DP as Unit Under Test (UUT)
 25 November 2020 Working Document

ISO/IEC 17025:2017 General requirements for the competence of testing and calibration laboratories

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Document Revision Status


TR-7169012035-000: Nov 19, 2022. First Draft, unsigned. Subject to review

TR-7169012035-001: Nov 21, 2022. Minor revisions as per customer request. Reviewed and signed.

TR-7169012035-002: Nov 22, 2022. Minor typographical errors corrected as per customer request. Reviewed and signed.

TR-7169012035-003: Nov 24, 2022. Corrected Domain proxy software version on page 68.

TR-7169012035-004: Nov 24, 2022. Removed Appendix C as per client request.

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
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	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
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	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
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)
Nov 16-17, 2022	All	SD	20-23	40-55	96.106

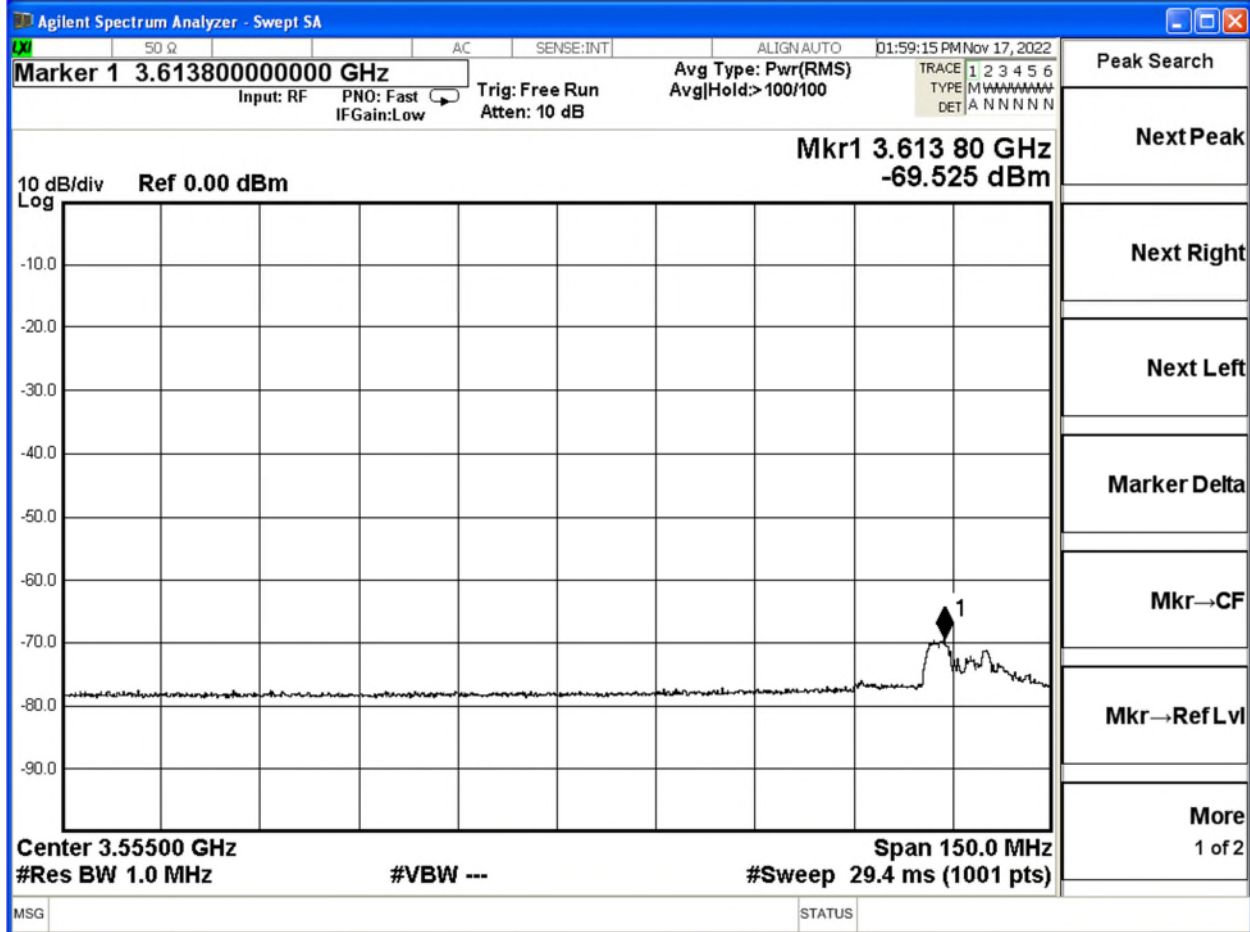
Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	


Detailed Test Results Section

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

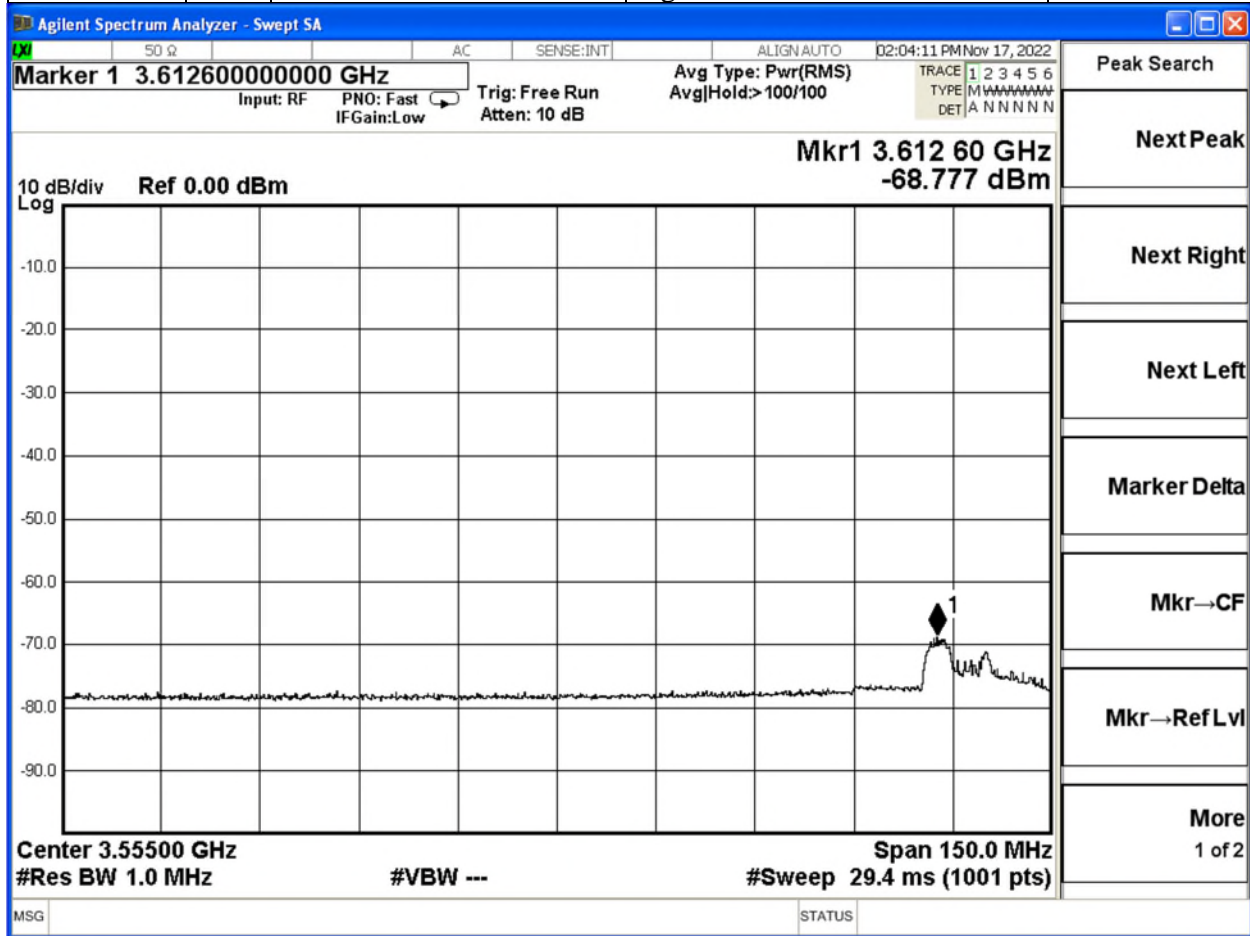
Authorization transmit after it receives authorization from a SAS.


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



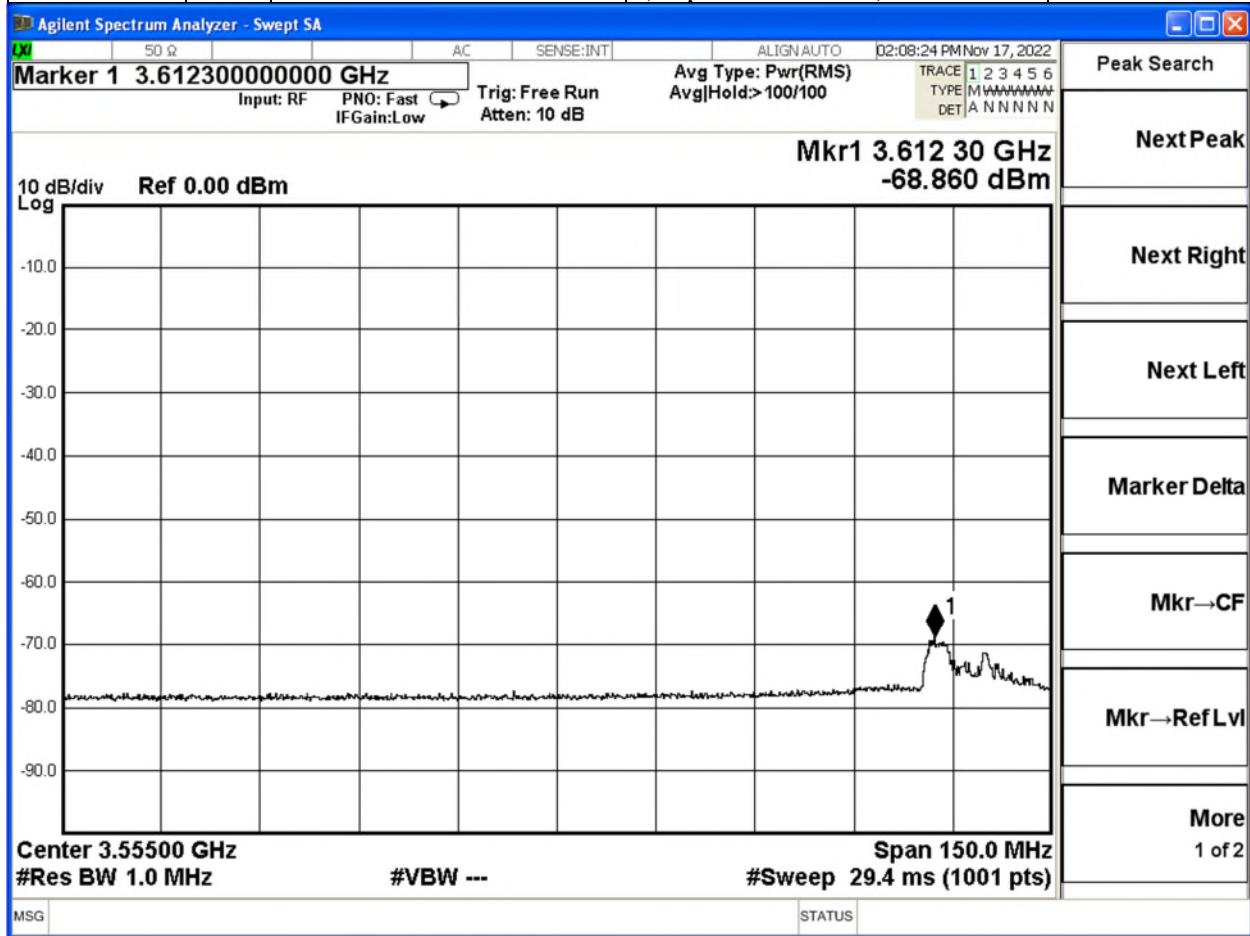
Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	


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



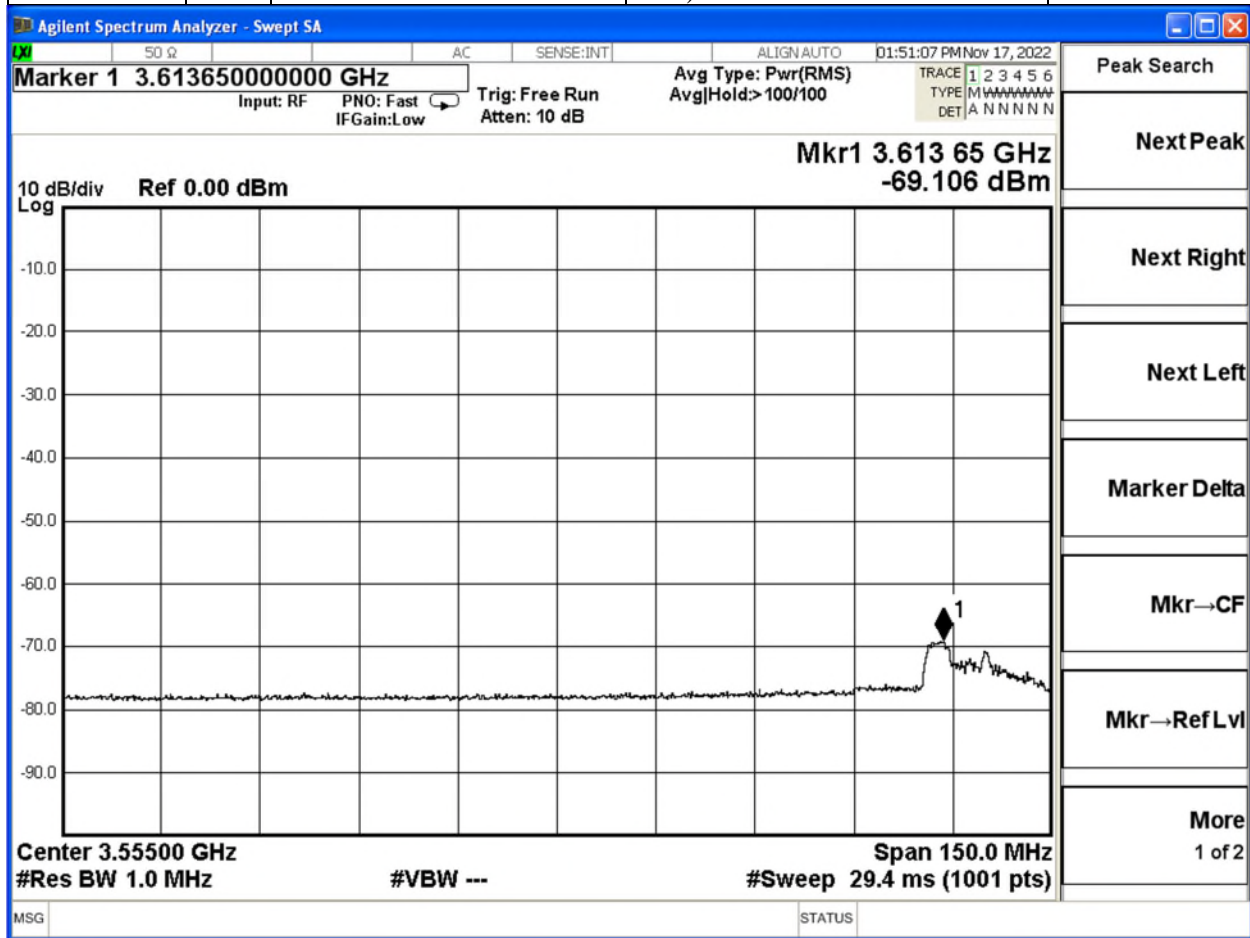
Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

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



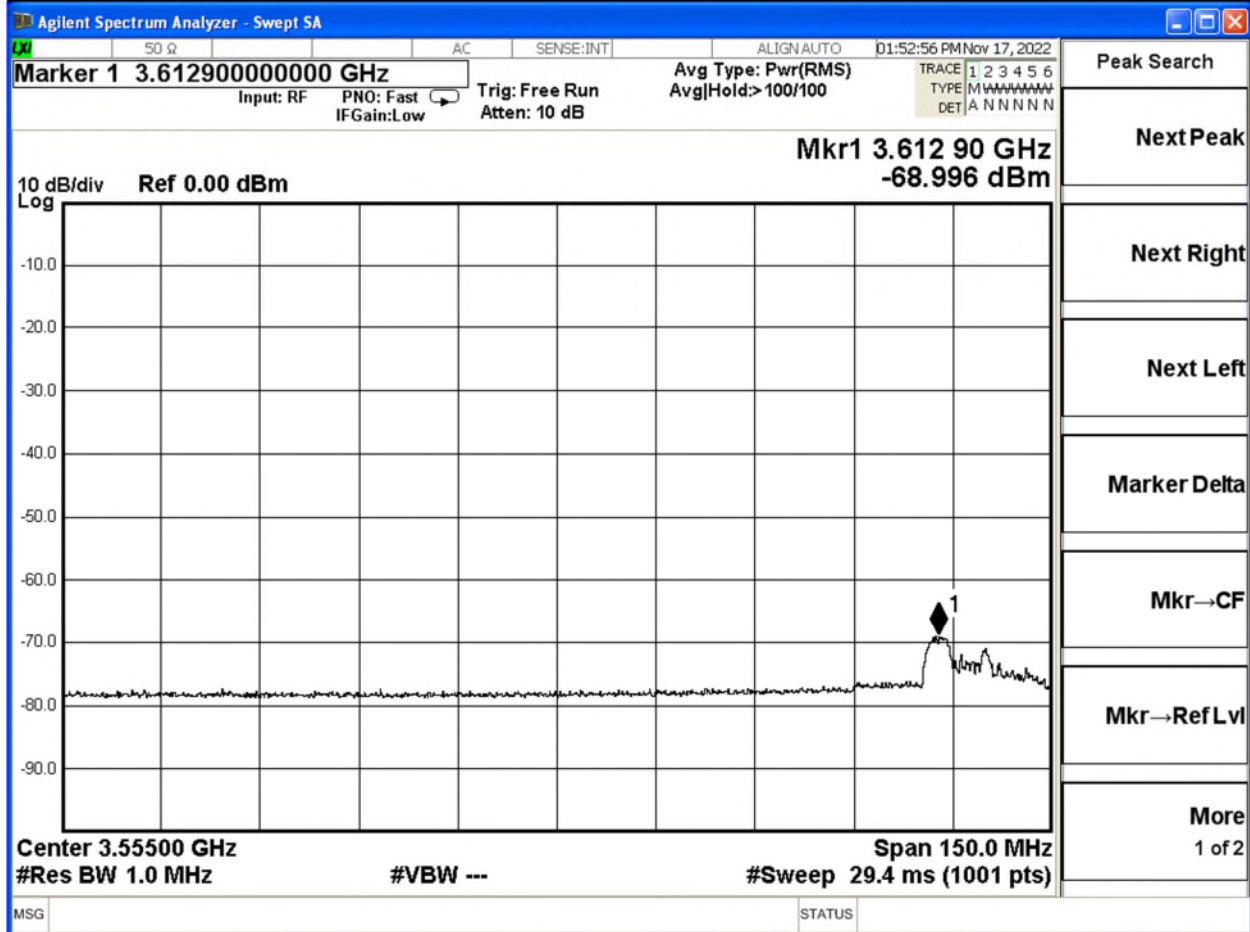
Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

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



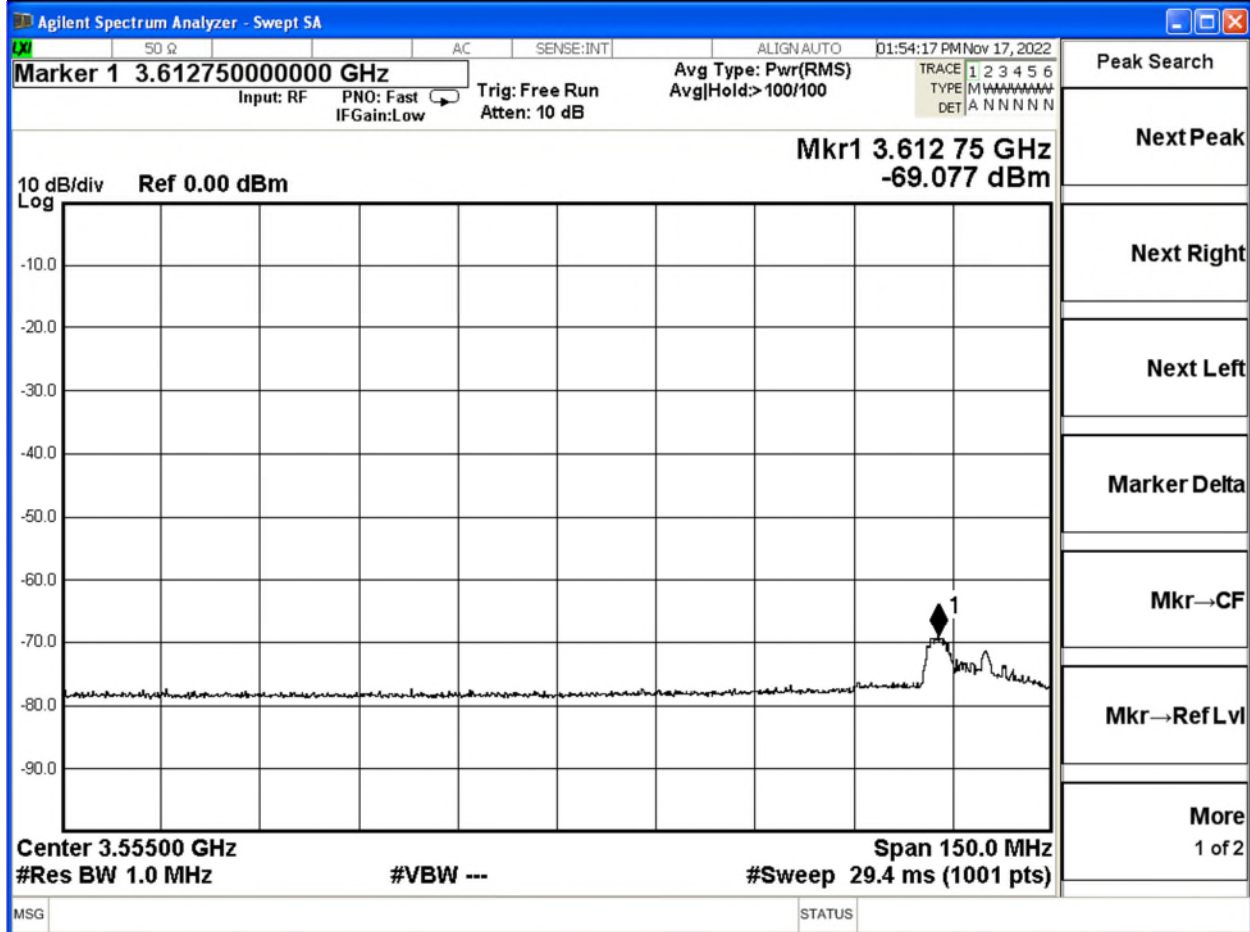
Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

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



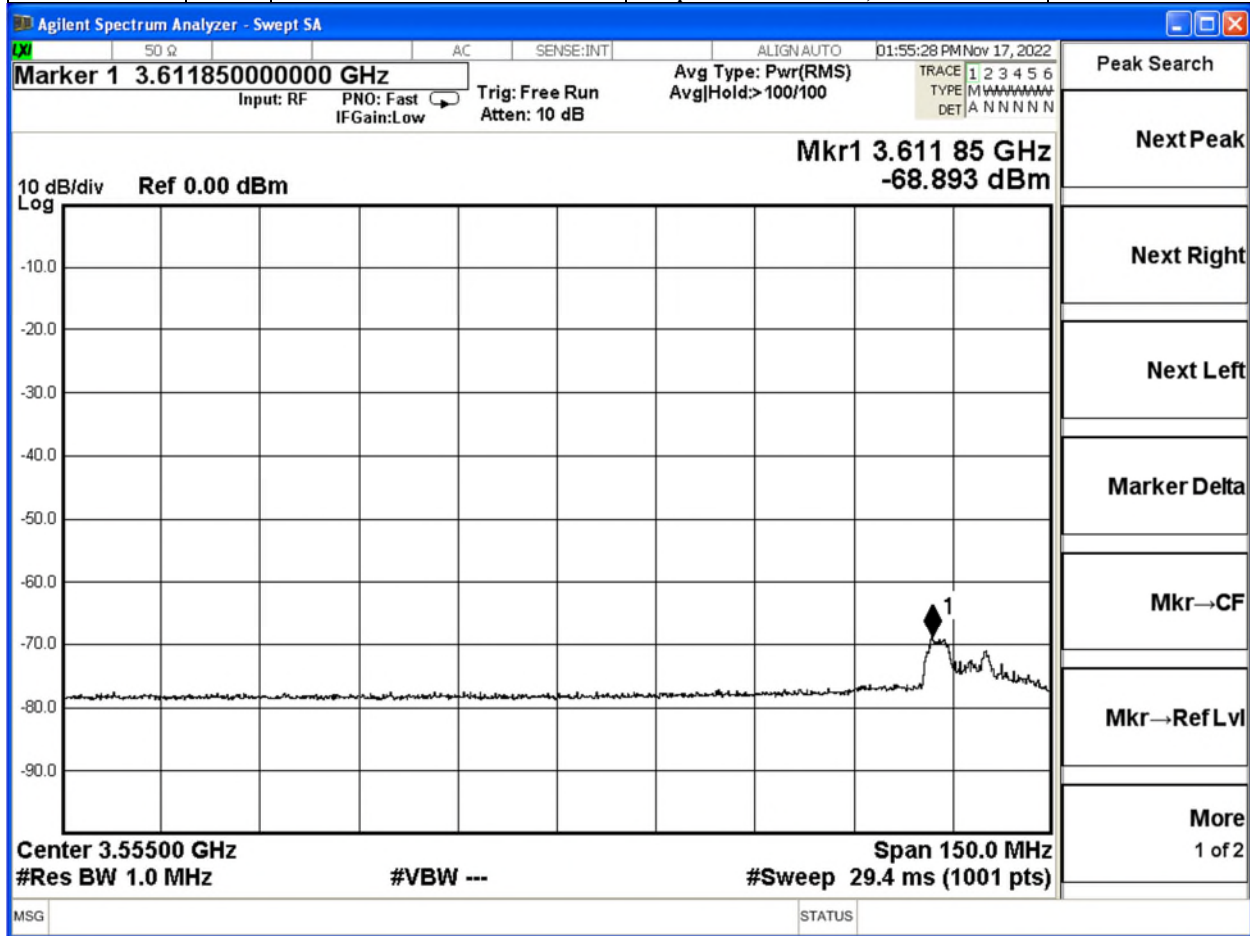
Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	


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



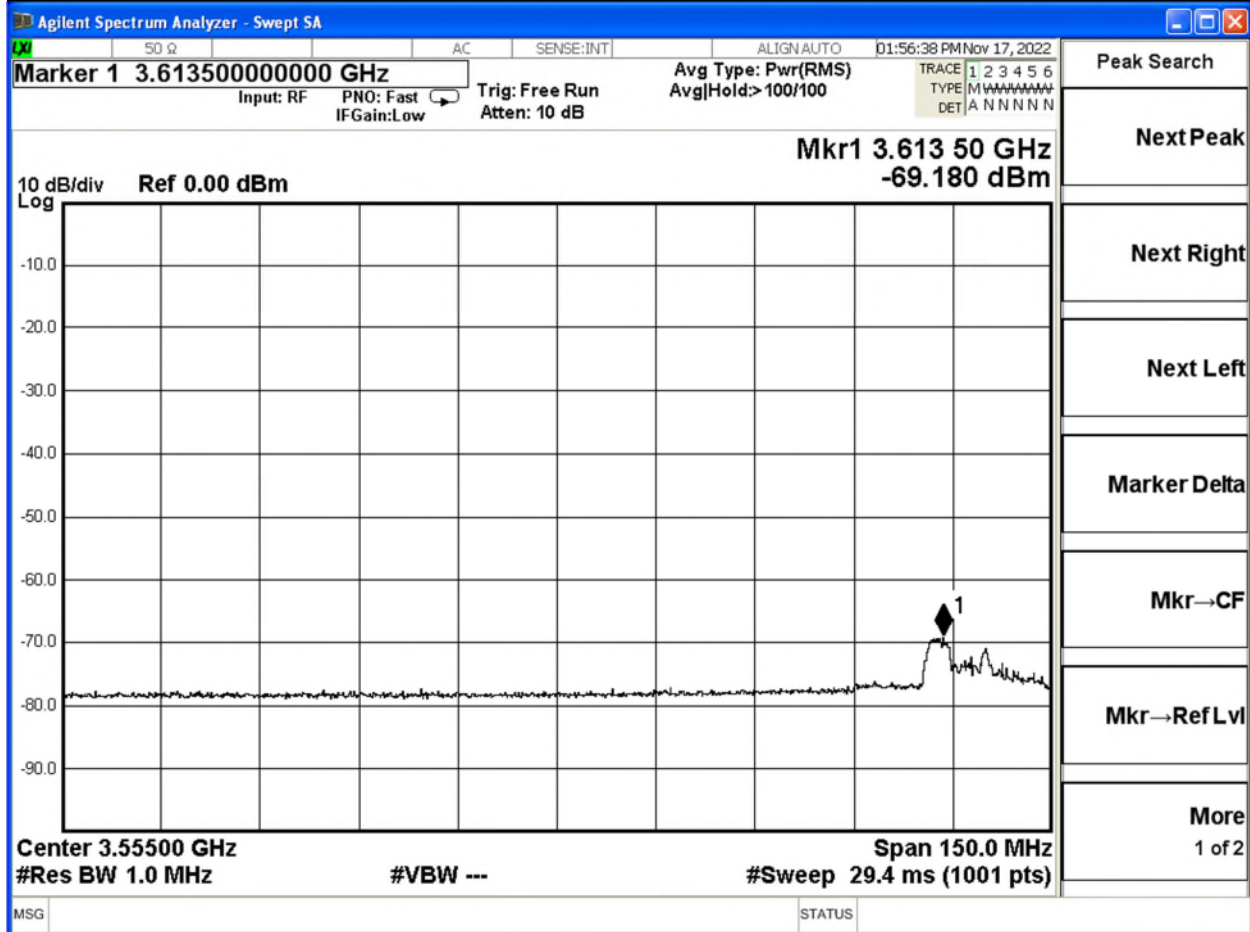
Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	


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



Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

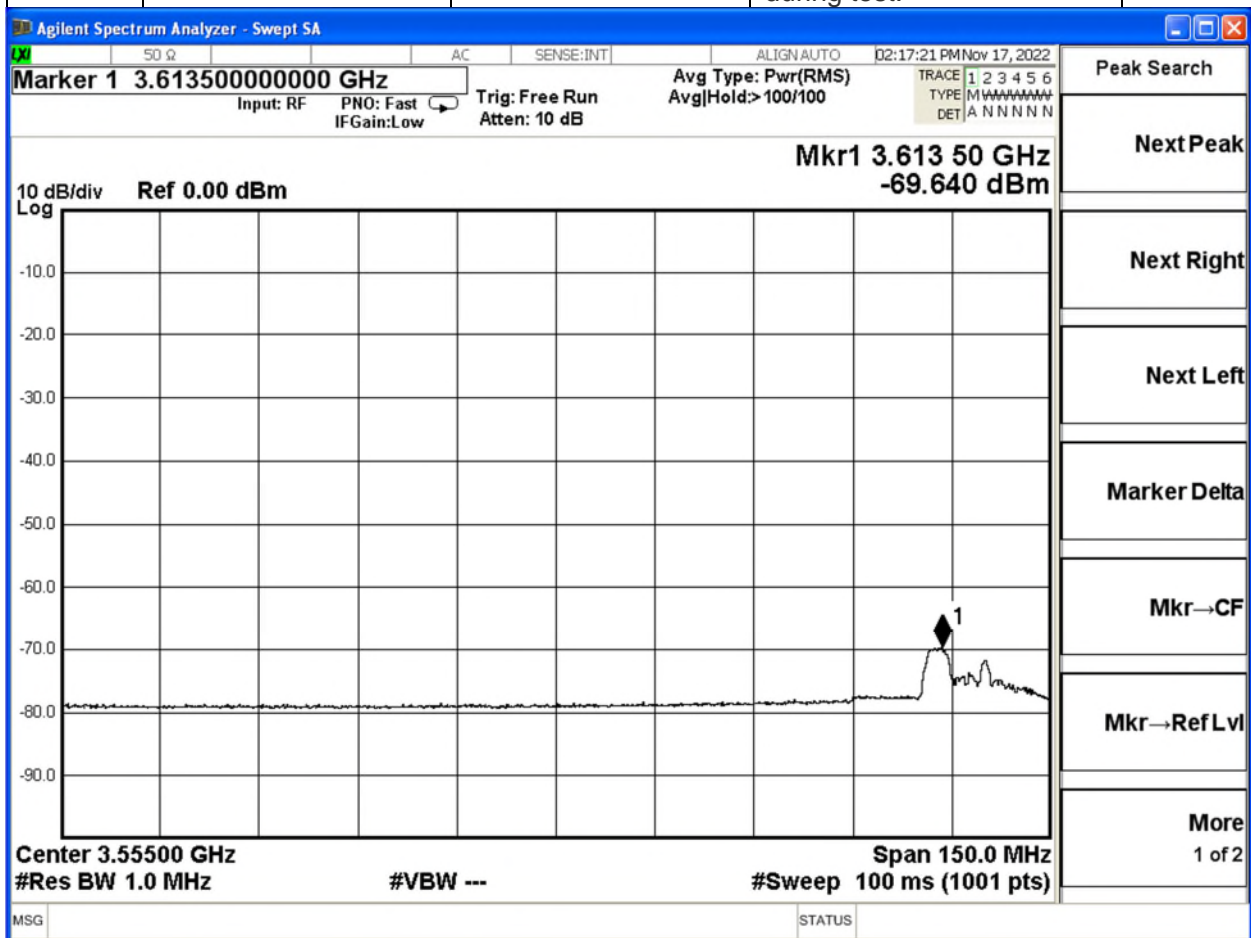
6.1.4.2.12	X	WINNF.FT.D.REG.19	Domain Proxy Group Error (responseCode 201)	P
------------	---	-------------------	---	---




Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

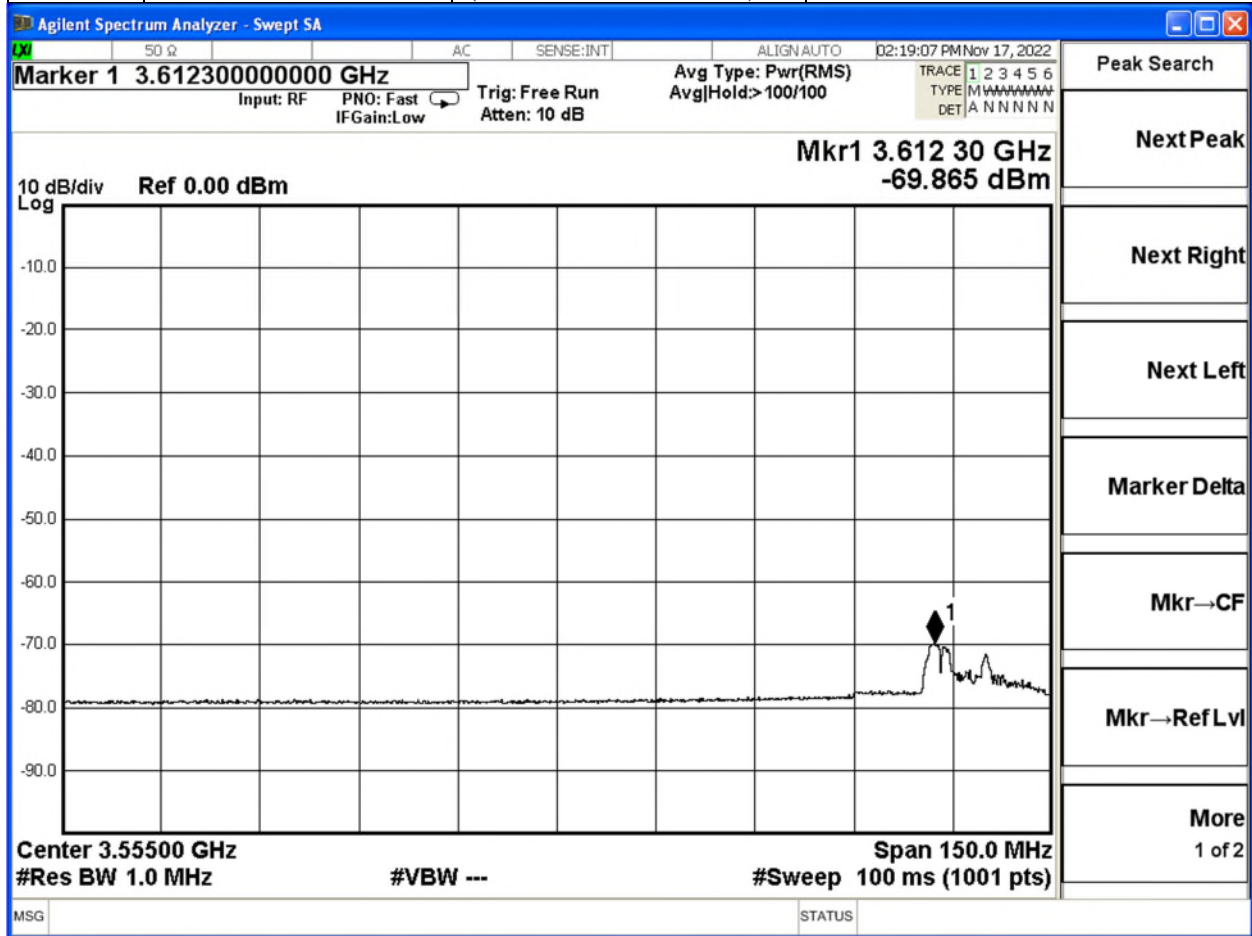
Check the device registration and authorization with the SAS, Confirm that the device changes its operating power and/or channel in response to a command from the SAS and Confirm that the device correctly configures based on the different license classes.

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
-----------	------------------	--	---	---



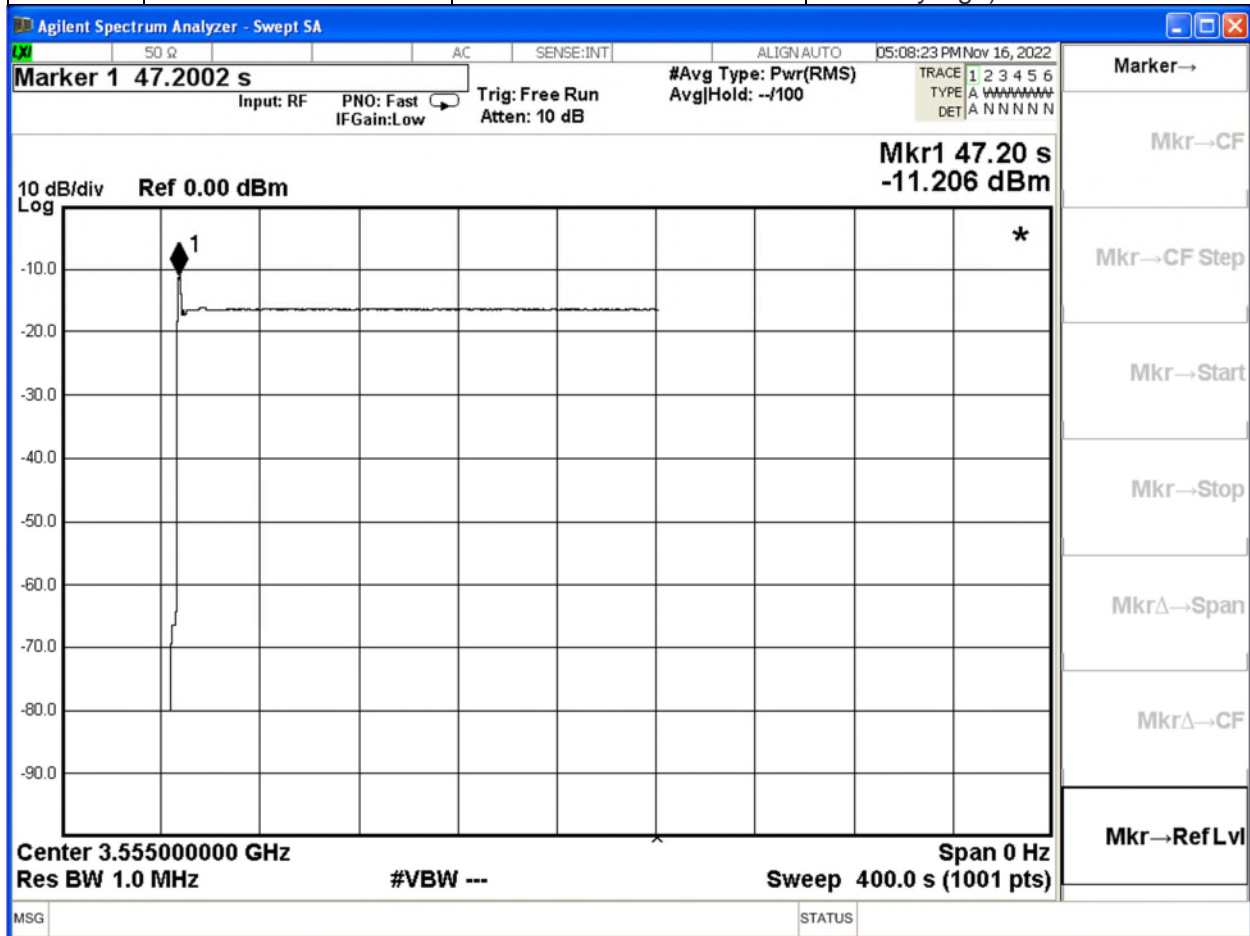
Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

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	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

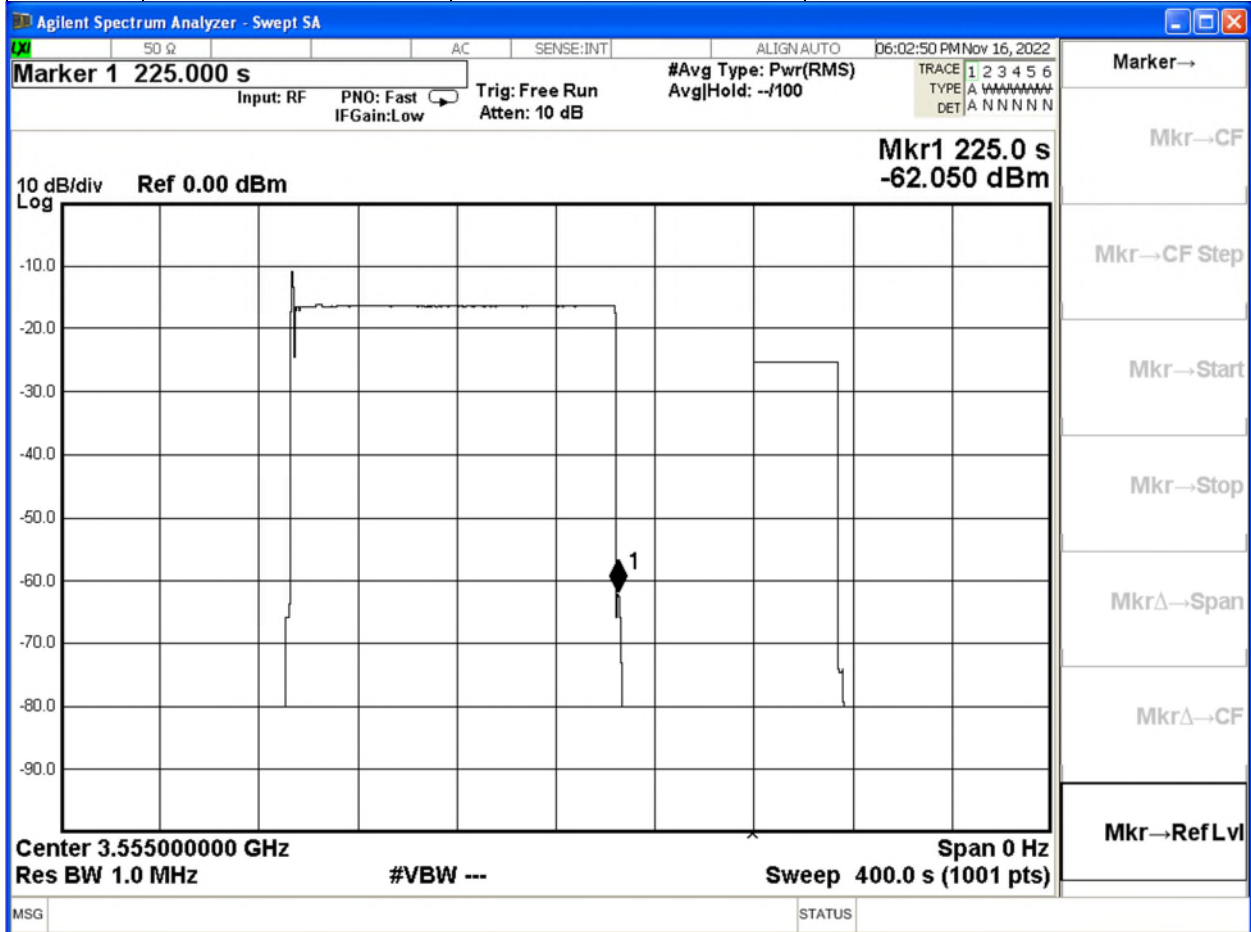
6.4.4.1.2	WINNF.FT.D.HBT.2	Domain Proxy Heartbeat Success Case (first Heartbeat Response)	Monitor RF from start of test. Ensure that: <ul style="list-style-type: none"> • Transmission does not start until time of first heartbeat response or after. • After transmission starts, measure that transmission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



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

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

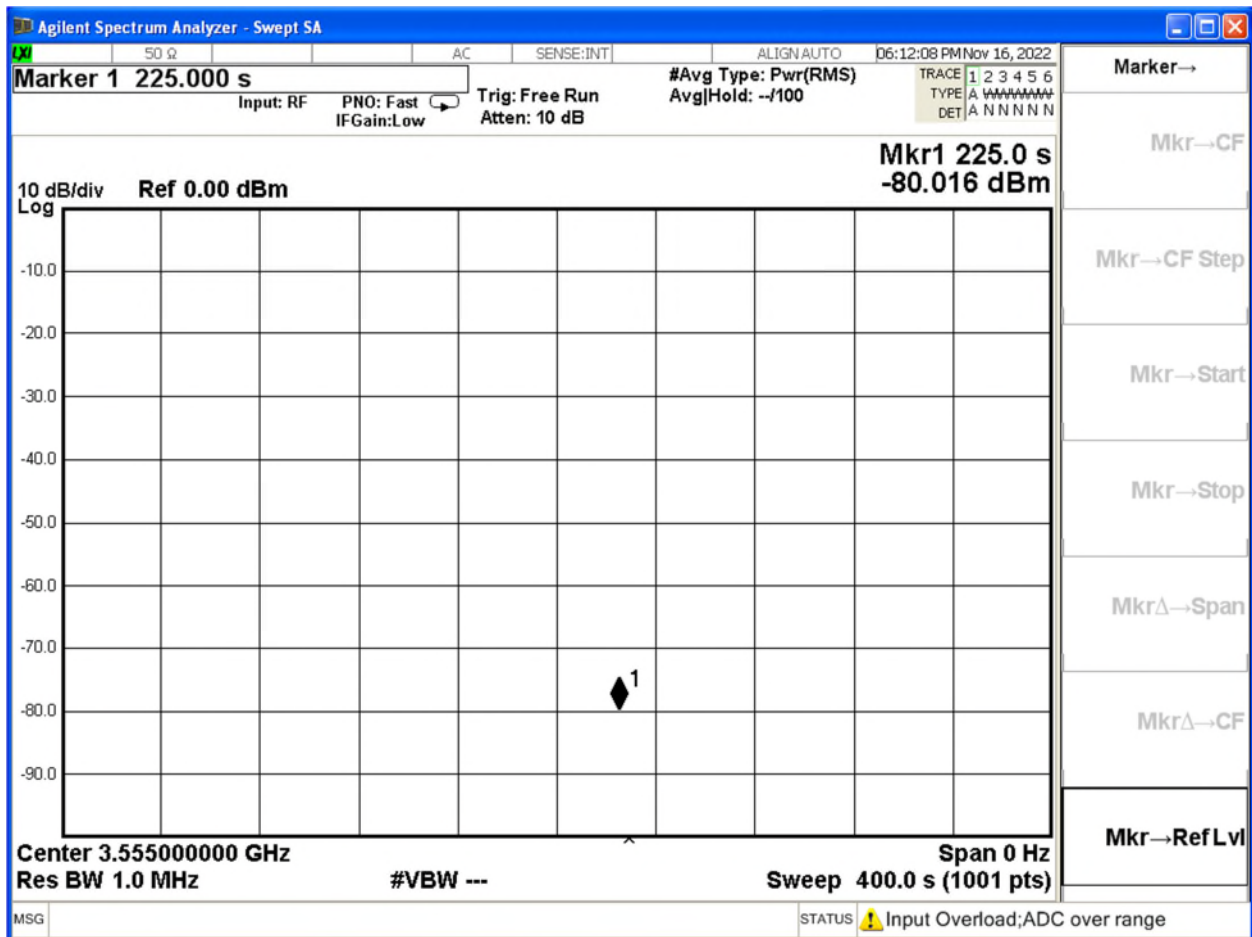
6.4.4.2.1	WINNF.FT.C.HBT.3	Heartbeat responseCode=105 (DEREGISTER)	Monitor RF transmission. Ensure that: <ul style="list-style-type: none"> • CBSD stops transmission within 60 seconds of the heartbeatResponse which contains responseCode = 105 	P
-----------	------------------	---	--	---



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

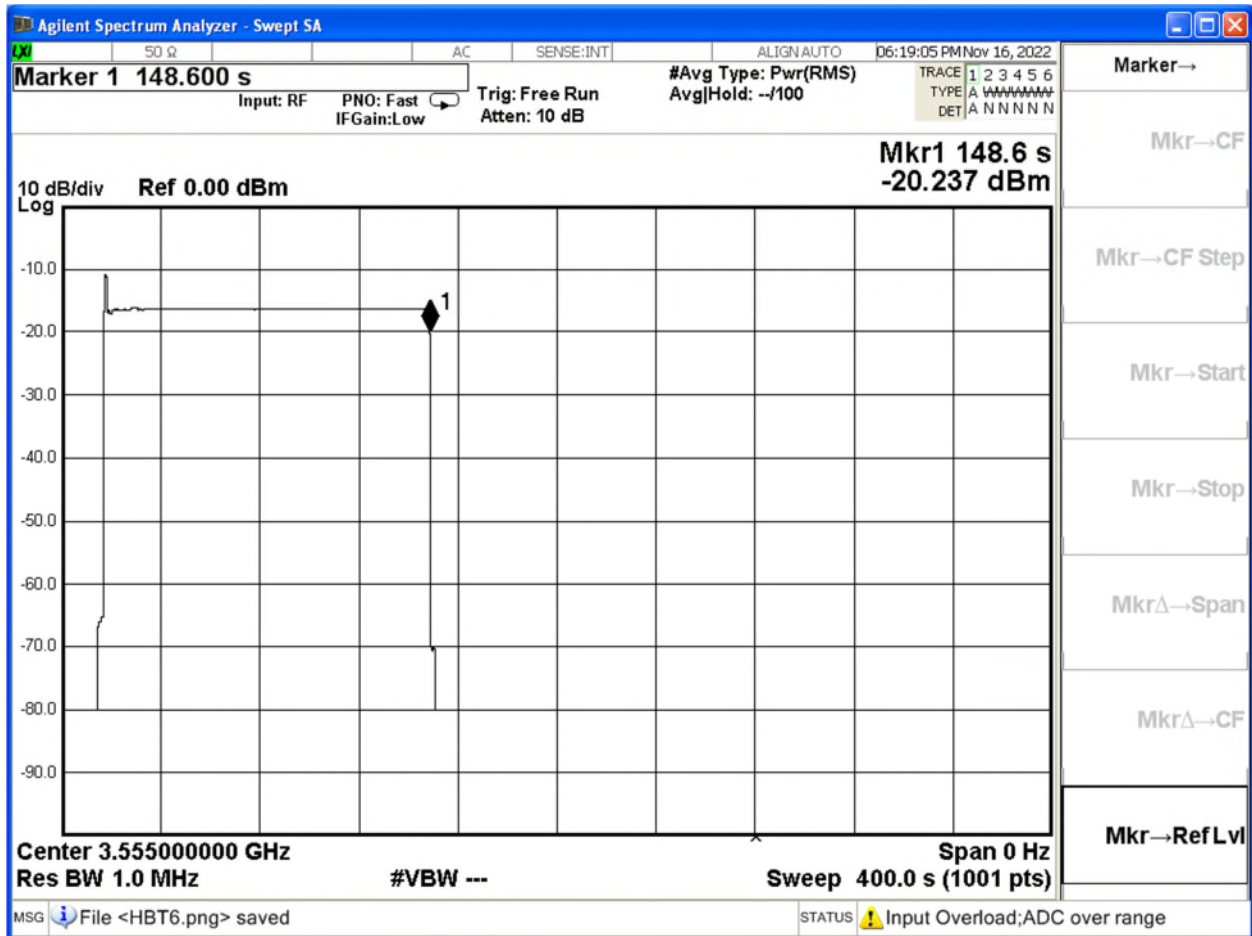
Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

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	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

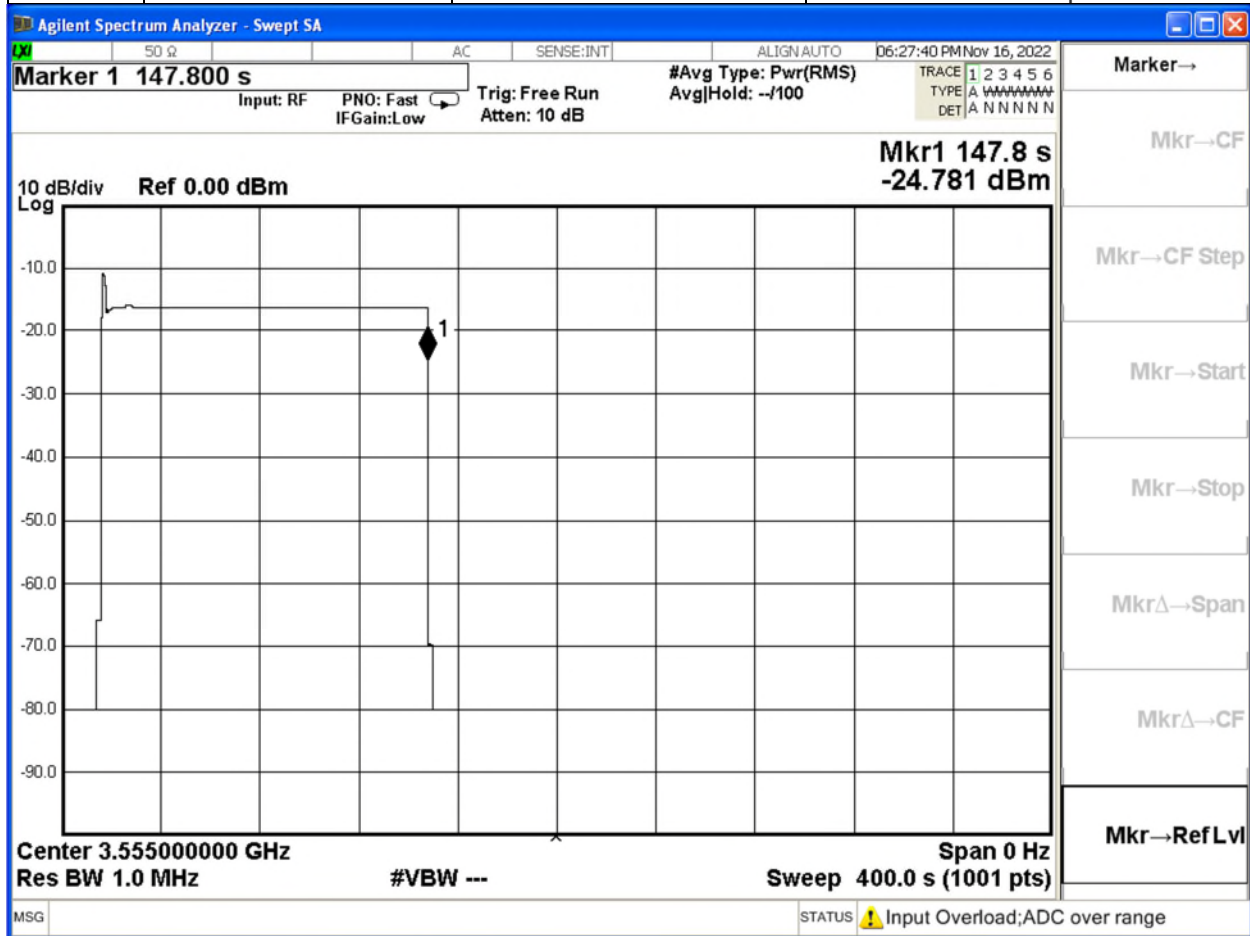
6.4.4.2.4	WINNF.FT.C.HBT.6	Heartbeat responseCode=501 (SUSPENDED_GRANT) in Subsequent Heartbeat Response	Monitor RF transmission. Ensure: <ul style="list-style-type: none"> CBSD stops transmission within 60 seconds of heartbeatResponse which contains responseCode=501 	p
-----------	------------------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




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

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

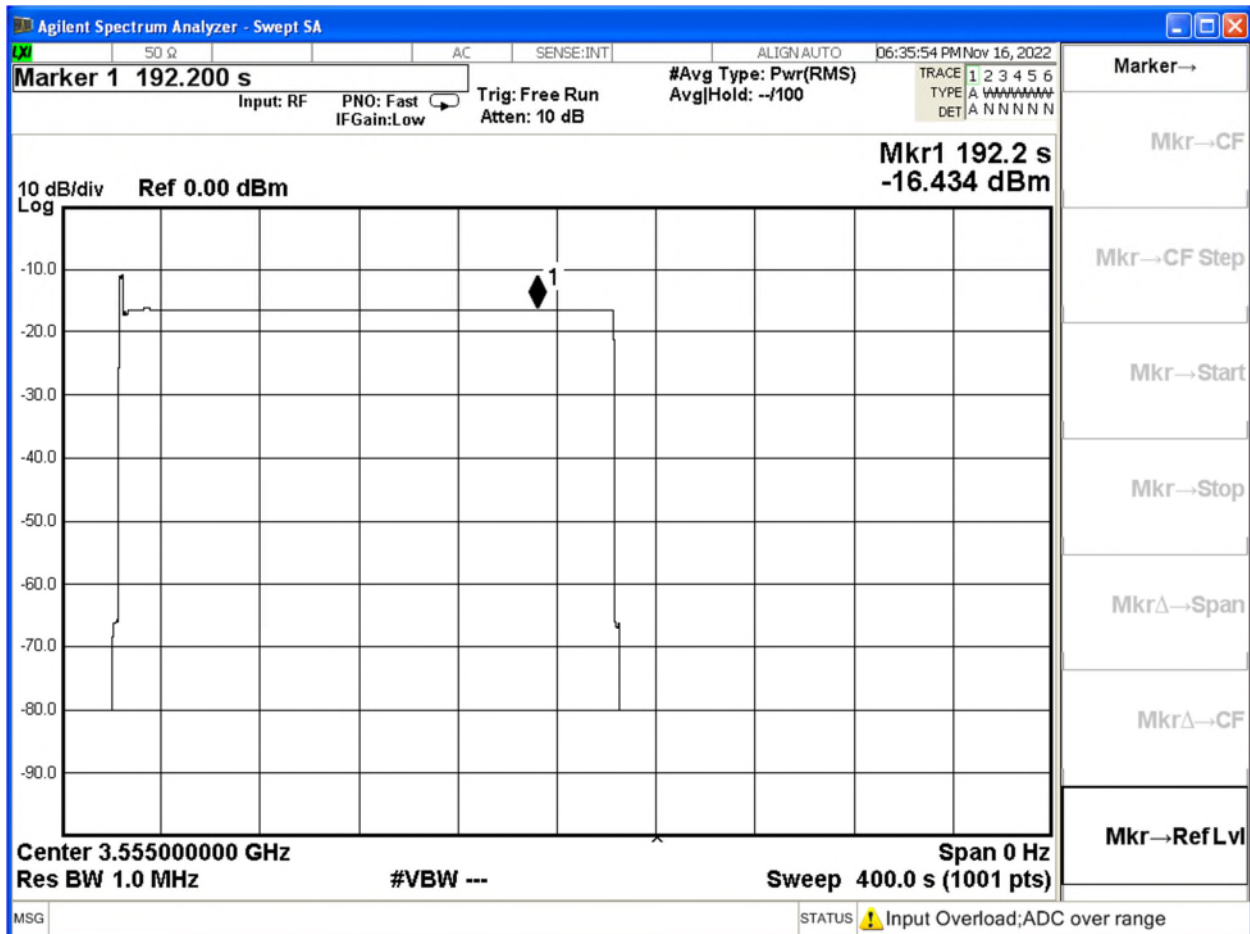
6.4.4.2.5	WINNF.FT.C.HBT.7	Heartbeat responseCode=502 (UNSYNC_OP_PARAM)	Monitor RF transmission. Ensure: <ul style="list-style-type: none"> • CBSD stops transmission within 60 seconds of heartbeatResponse which contains responseCode=502 	p
-----------	------------------	--	---	---




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

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

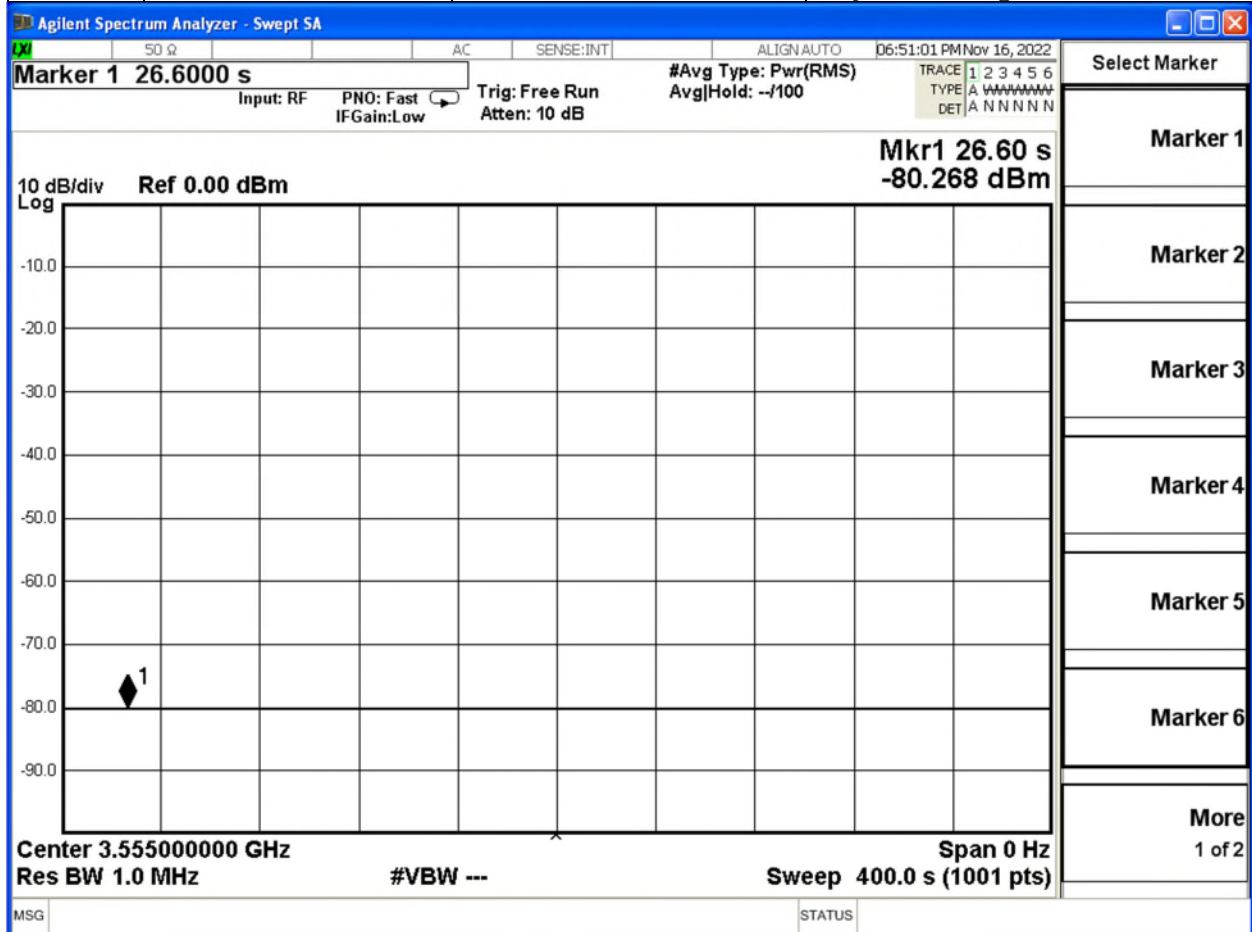
6.4.4.2.6	--	X	WINNF.FT.D.H BT.8	Domain Proxy Heartbeat responseCode=500 (TEMINATED_GRANT)	Monitor RF transmission. CBSDs will have different behavior: <ul style="list-style-type: none"> • CBSD1: will continue to transmit to end of test (this is not a pass/fail criteria, but check) • CBSD2: must stop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




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

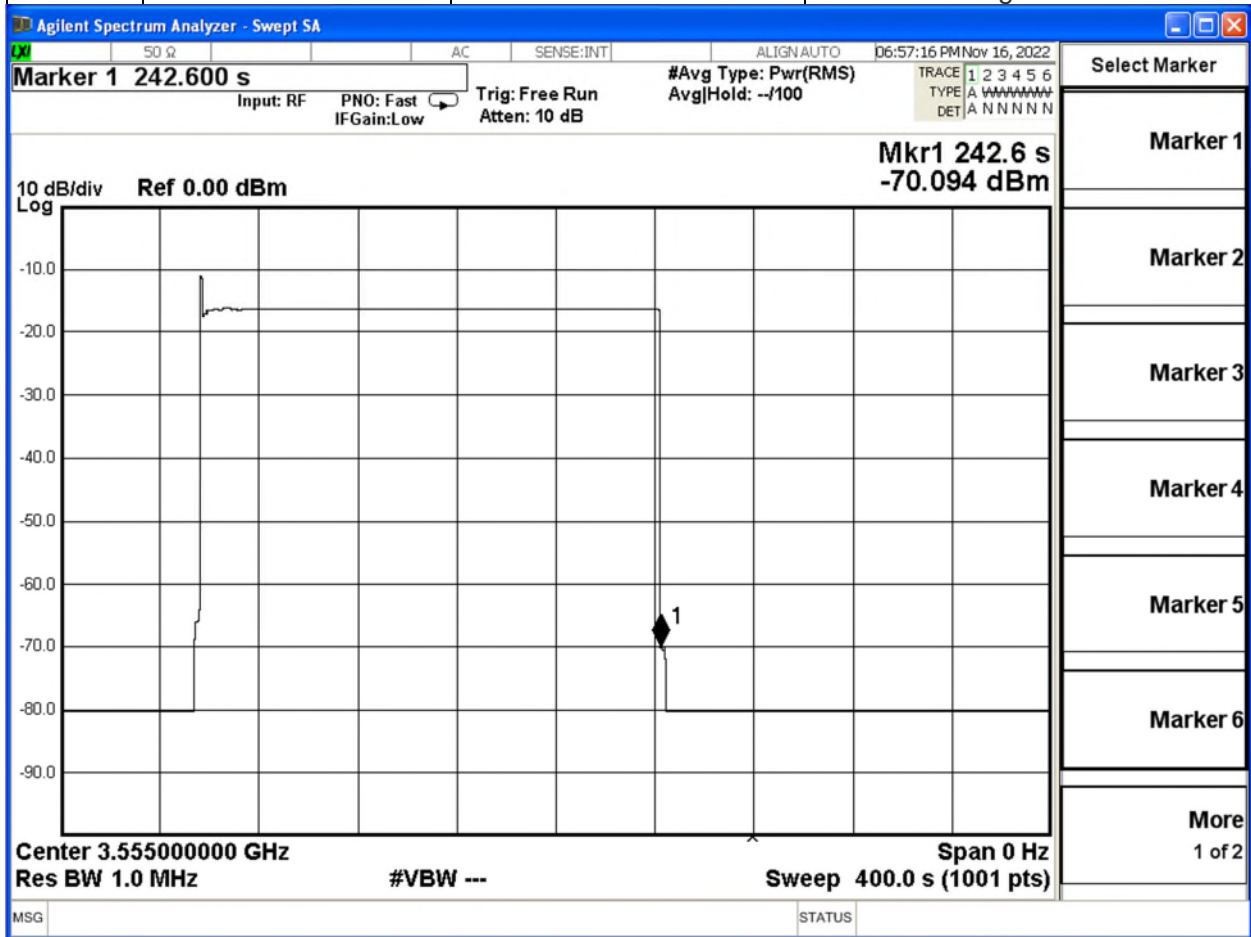
Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

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	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
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"> • CBSD must stop transmission within transmitExpireTime+60 seconds, where transmitExpireTime is from last successful heartbeatResponse message 	P
-----------	-------------------	--	---	---




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

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
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	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
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.

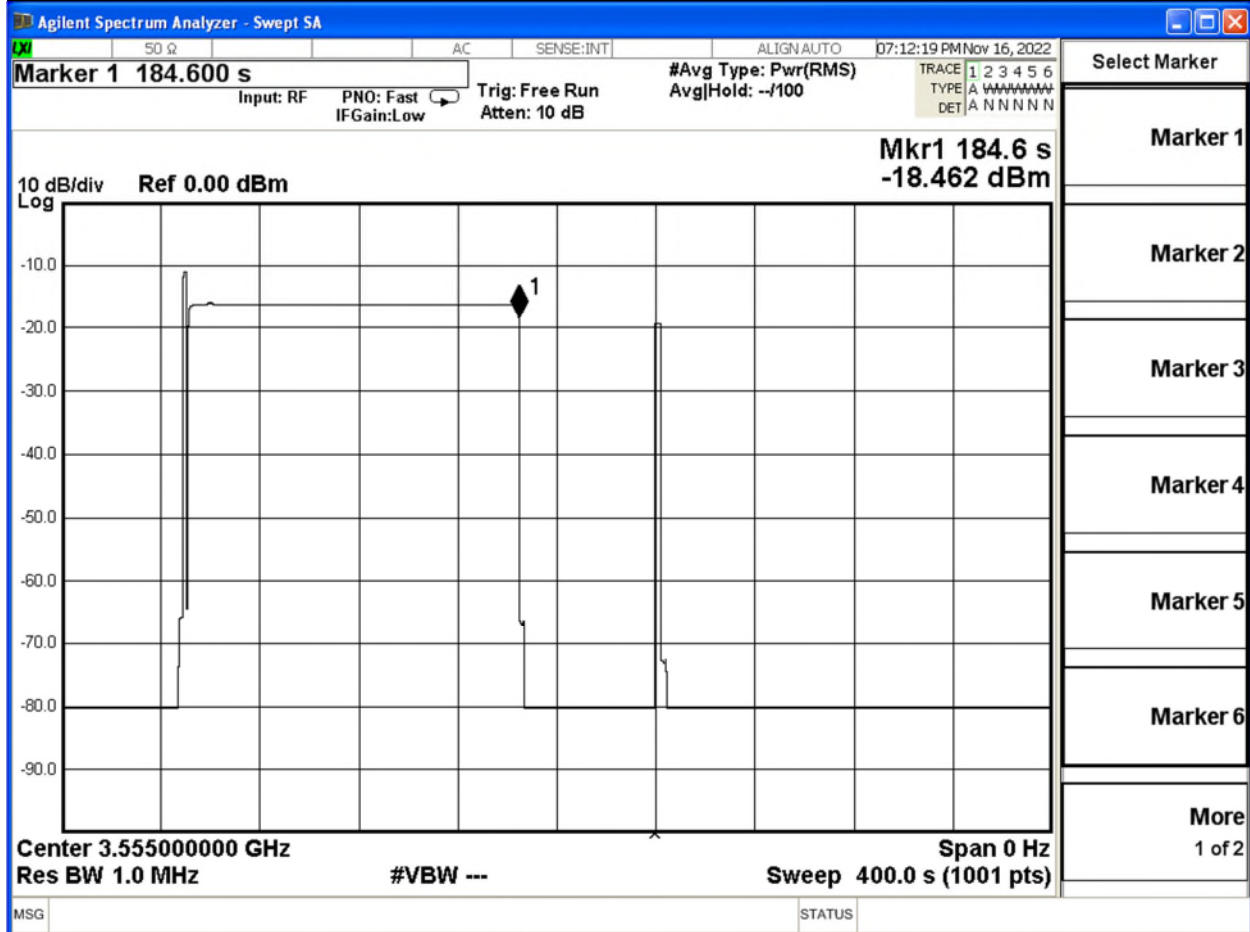
Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

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	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
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"> • CBSD stops transmission at any time prior to sending the relinquishmentRequest message. 	P
-----------	------------------	--	--	---

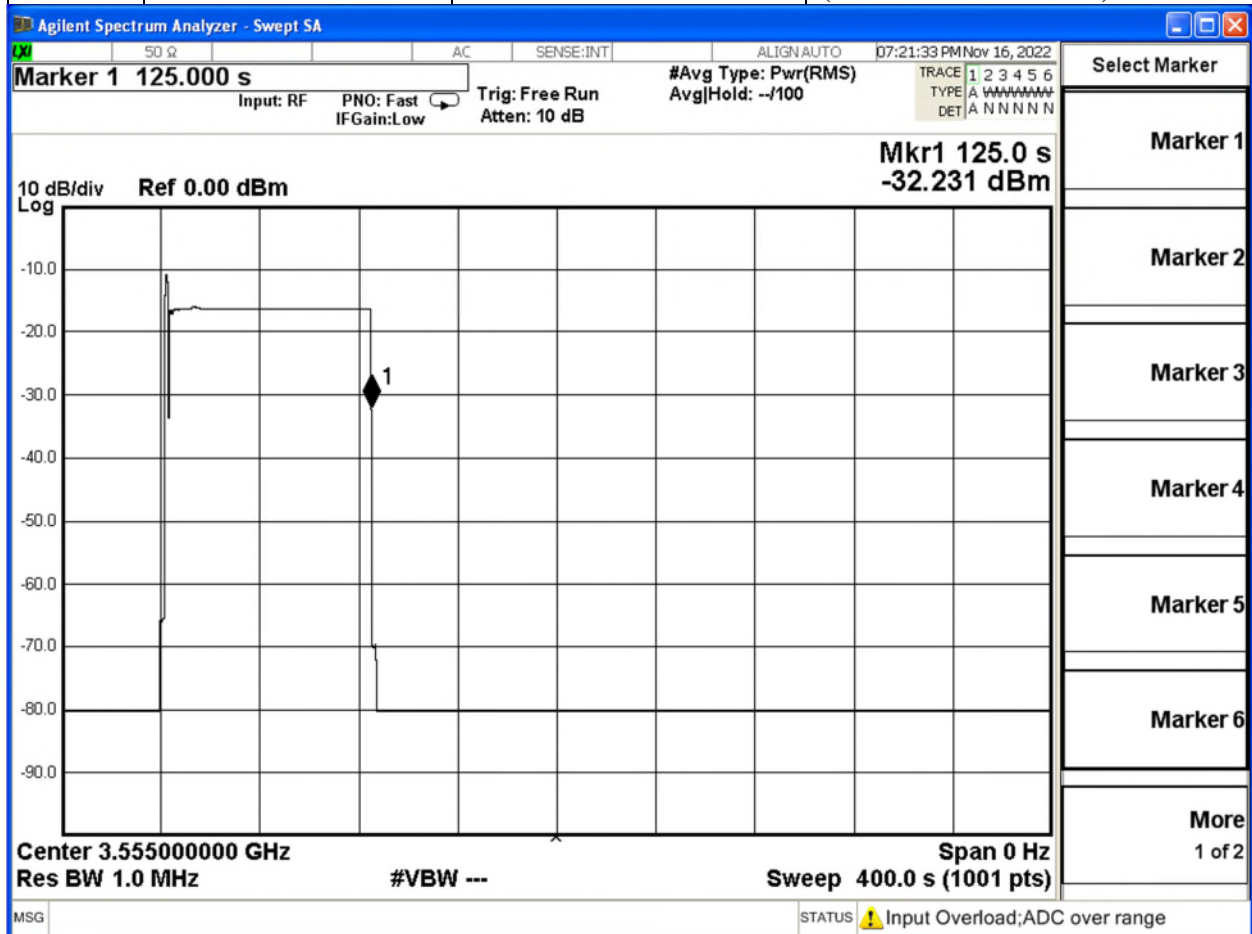


Test Harness logs and timing on graph was verified, the EUT passed the requirement.

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


Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
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: <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) 	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	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
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.

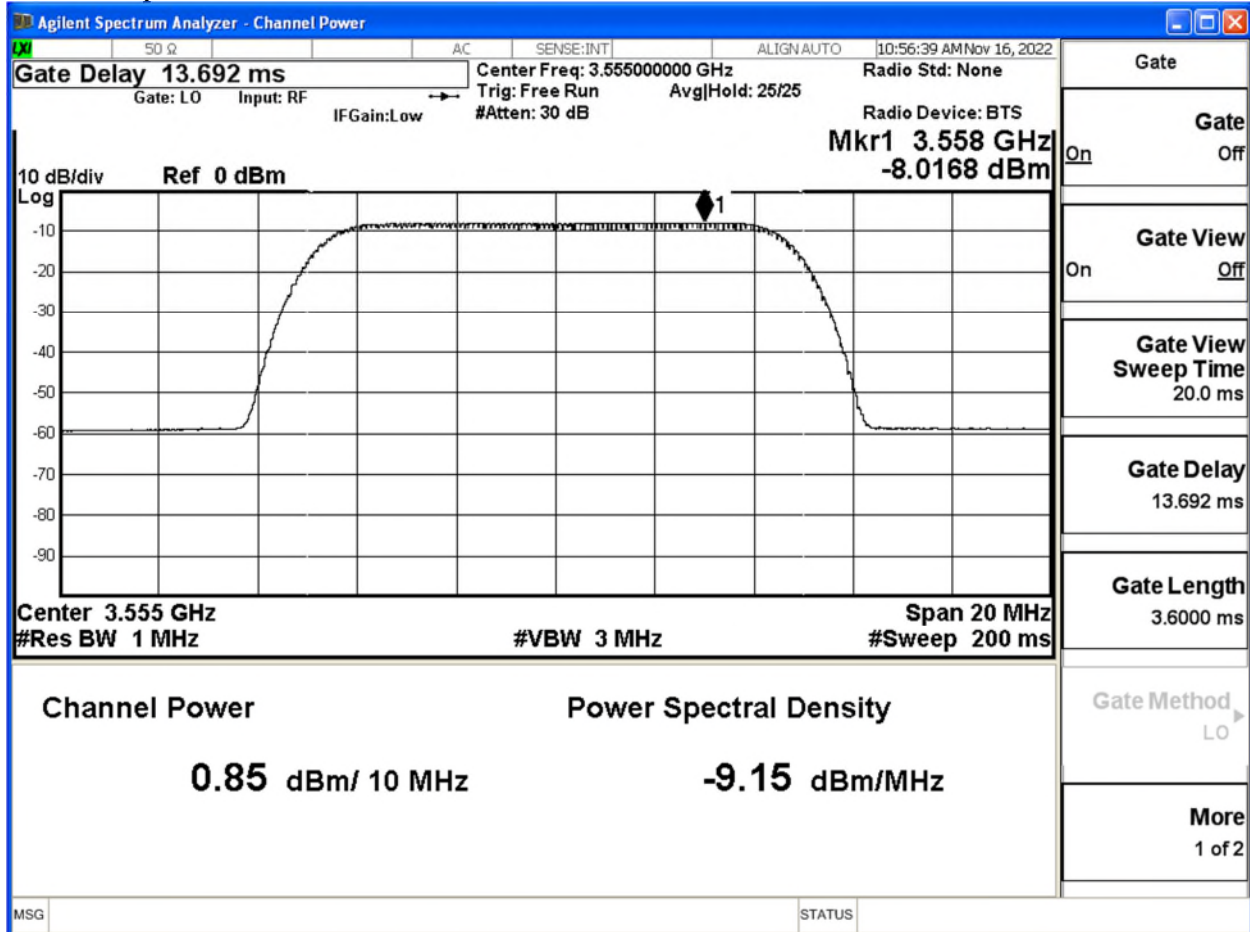
7.1.4.1.1	X	X	WINNF.PT.C.H BT	UUT RF Transmit Power Measurement	Power Spectral Density test case. Assume we use 1 carrier bandwidth (say, 5 or 10 MHz), one frequency (say middle channel in band) for test. Measure at max transmit power, and reduce in steps of 3 dB to minimum declared transmit power.	P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


Test Table

		Raw	Raw	External	Conducted				EIRP 1 MHz	EIRP 10 MHz	Margin
Freq	1MHz EIRP limit (target) dBm	10 MHz		Losses (dB)	dBm/MHz	Antenna gain dBi	Ports	Port gain (dB)	dBm/MHz	dBm	dB
3555-Low	34	0.85	-8.01	14.39	6.38	11	32	15.05	32.43	41.29	1.57
3555-High	37	3.77	-5.08	14.39	9.31	11	32	15.05	35.36	44.21	1.64
3630-low	34	0.62	-8.22	14.44	6.22	11	32	15.05	32.27	41.11	1.73
3630-high	37	3.62	-5.56	14.44	8.88	11	32	15.05	34.93	44.93	2.07
3695-low	34	0.84	-7.94	14.53	6.59	11	32	15.05	32.64	41.42	1.36
3695-high	37	3.73	-5.06	14.53	9.47	11	32	15.05	35.52	44.31	1.48

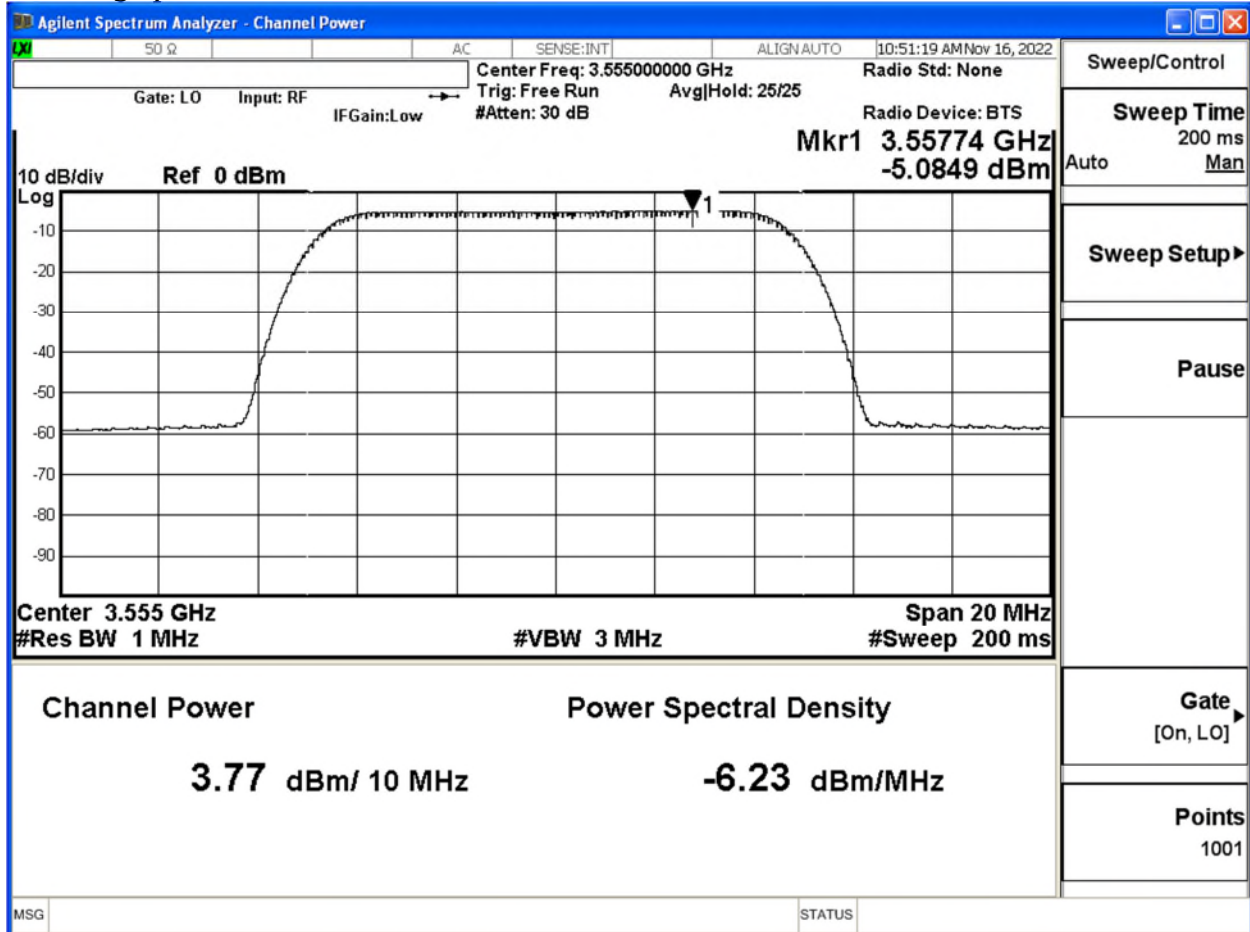
Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	


3555 low power



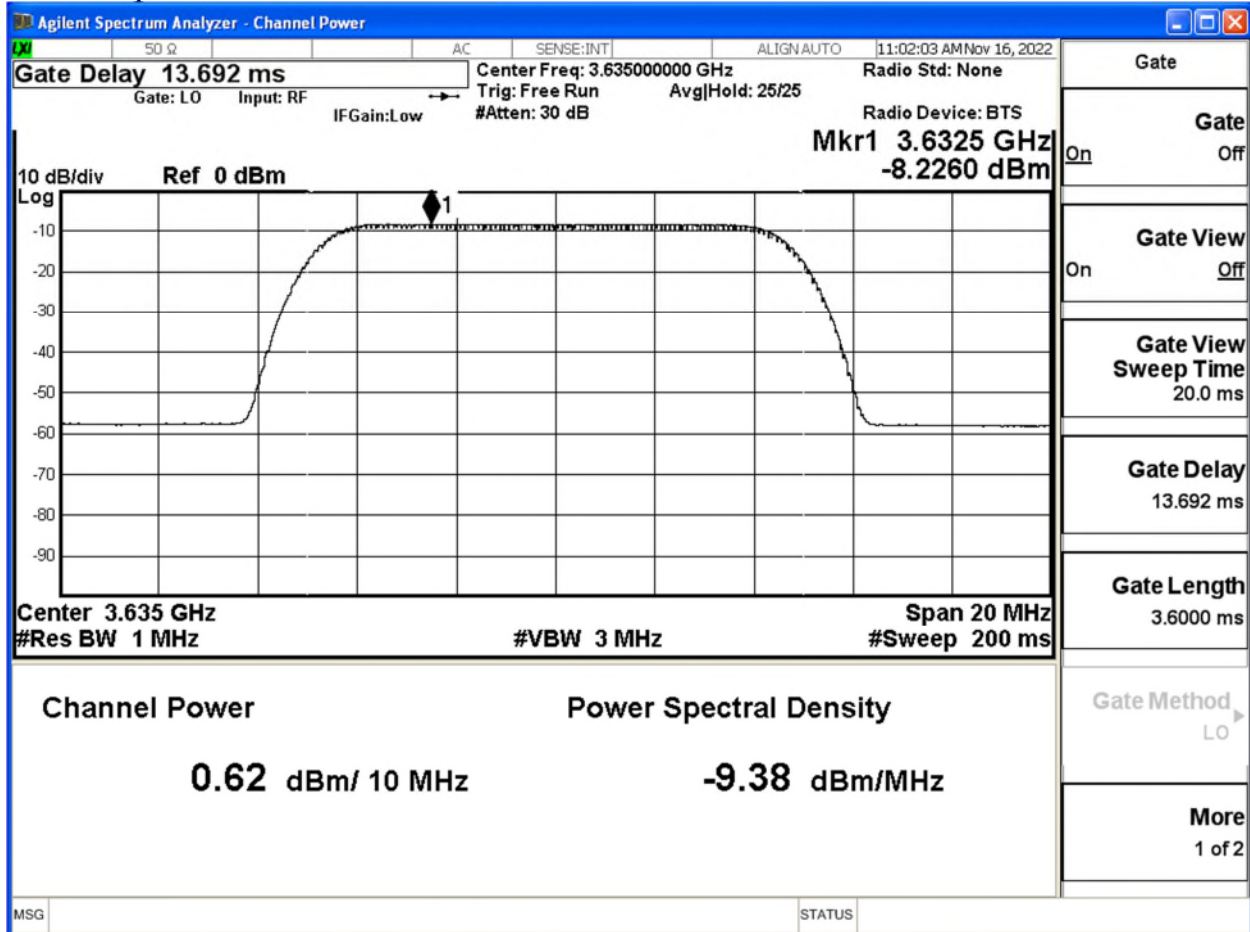
Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	


3555-High power



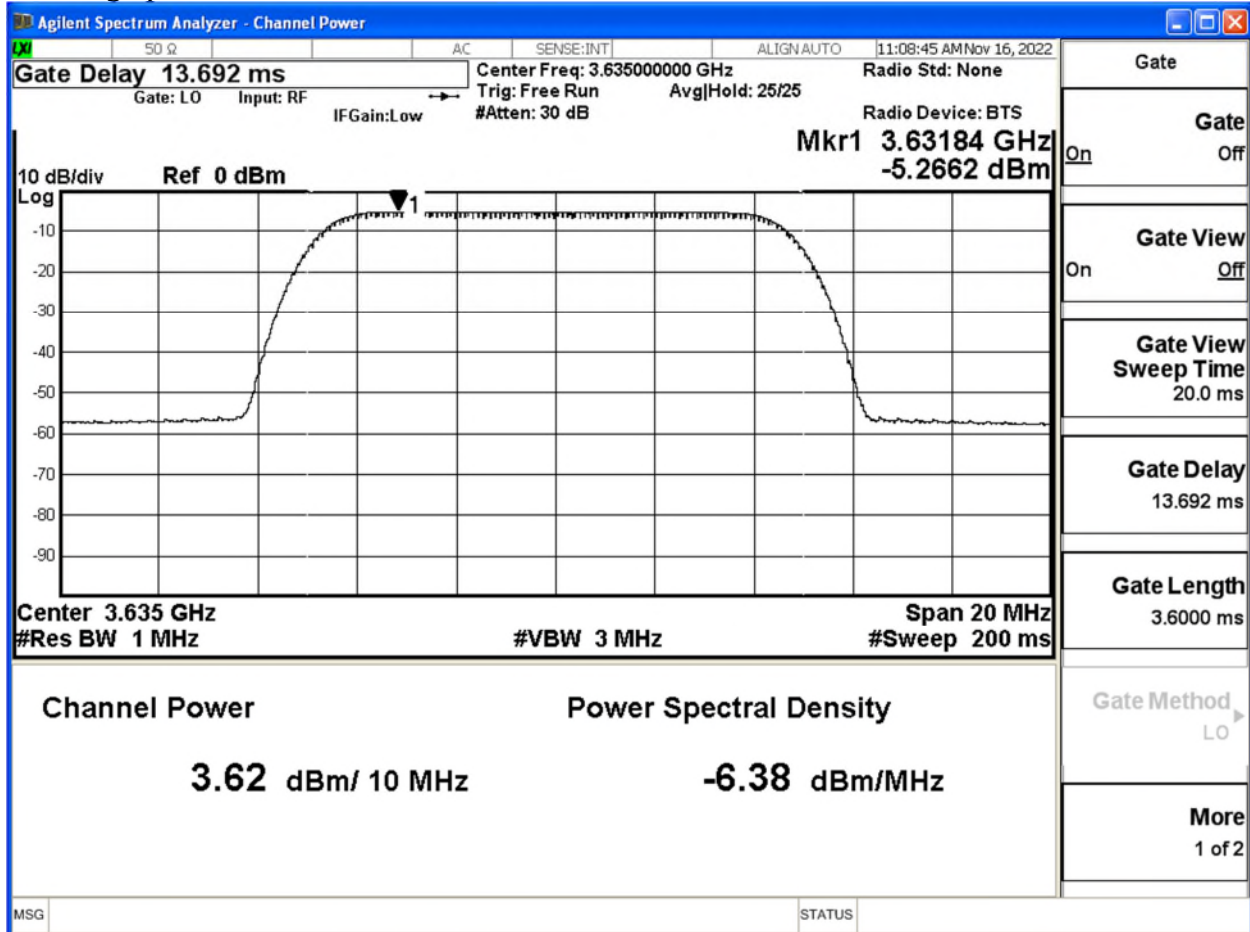
Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	


3630 low power



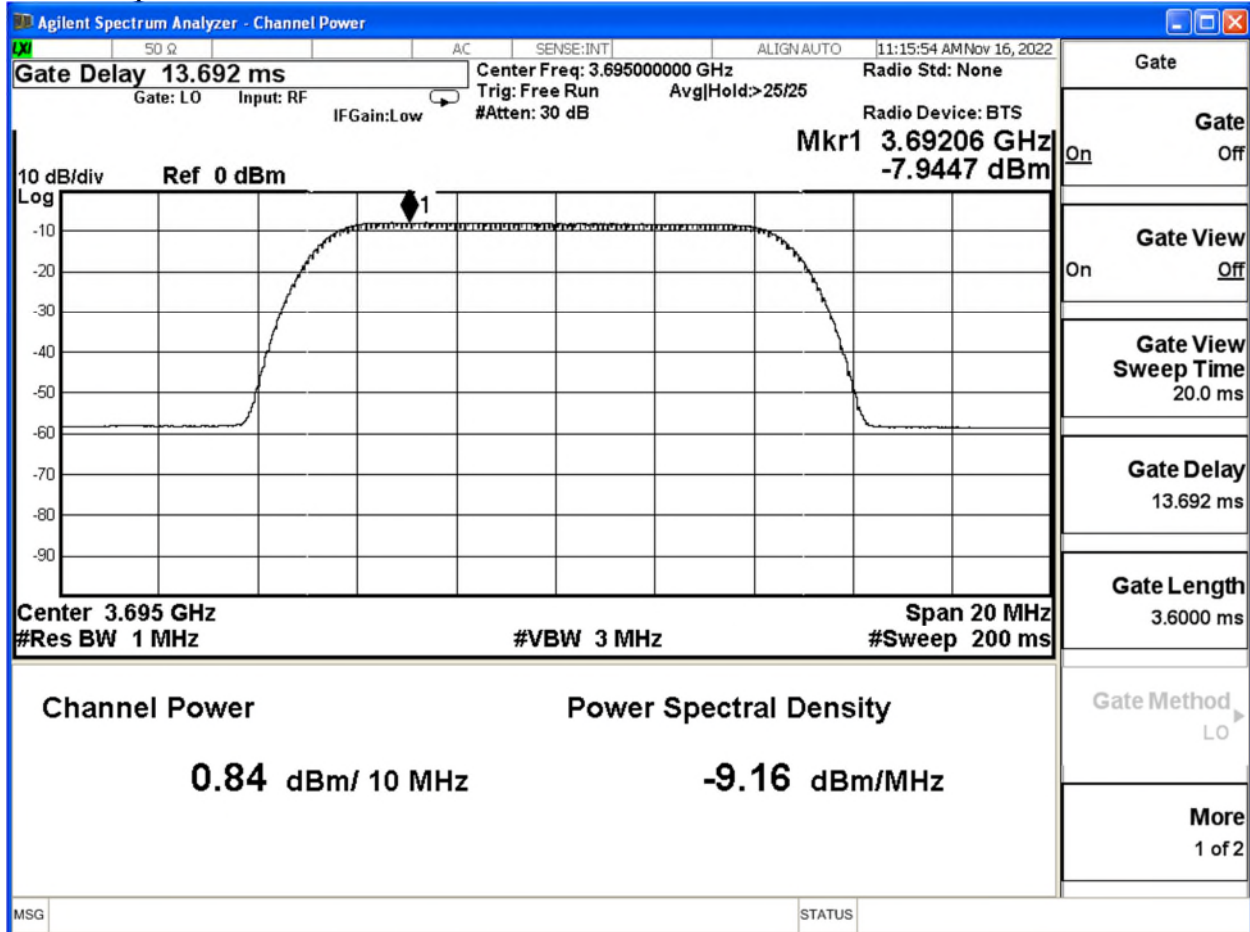
Client	Ericsson	 Canada
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	


3630-high power



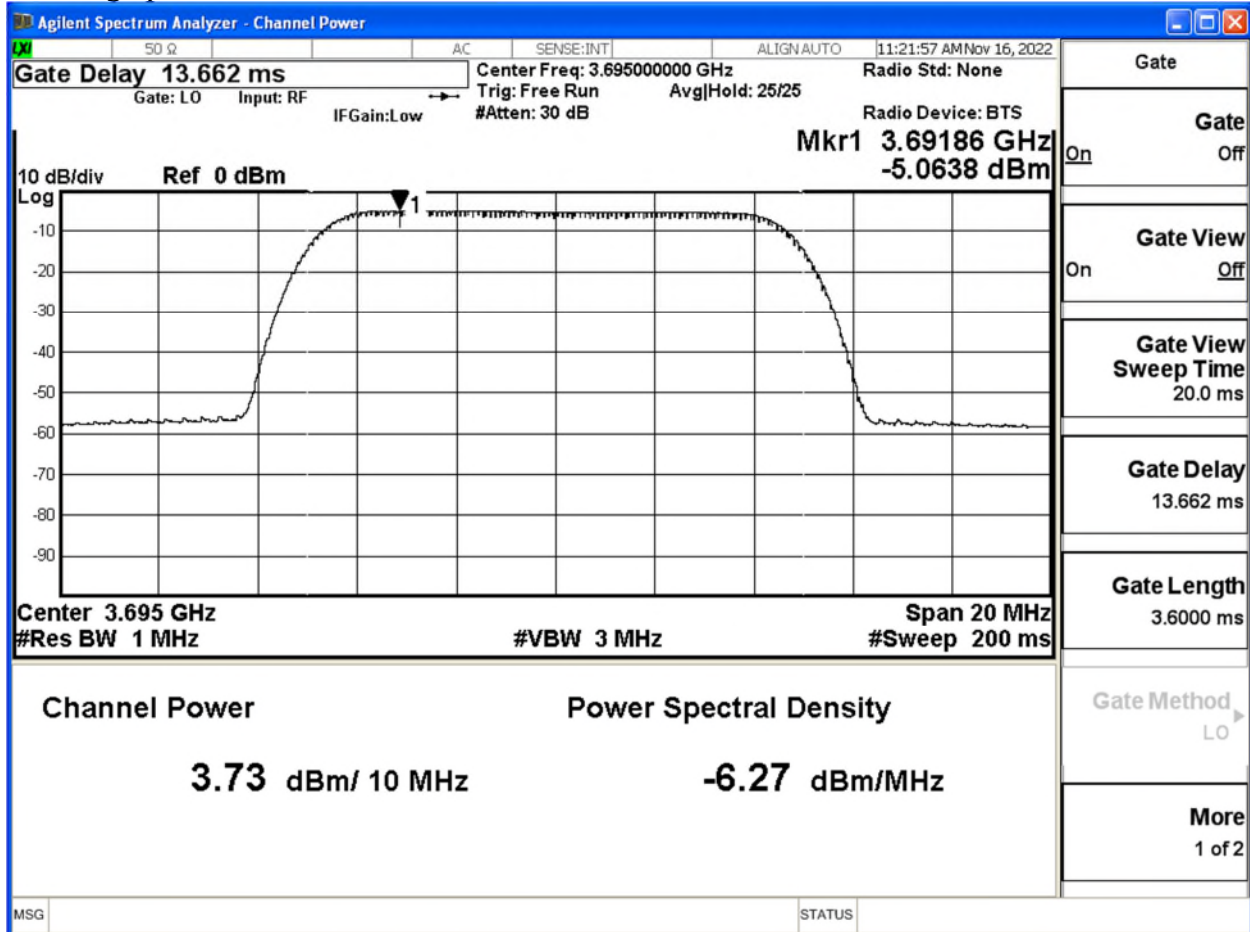
Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

3695 low power



Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

3695-high power

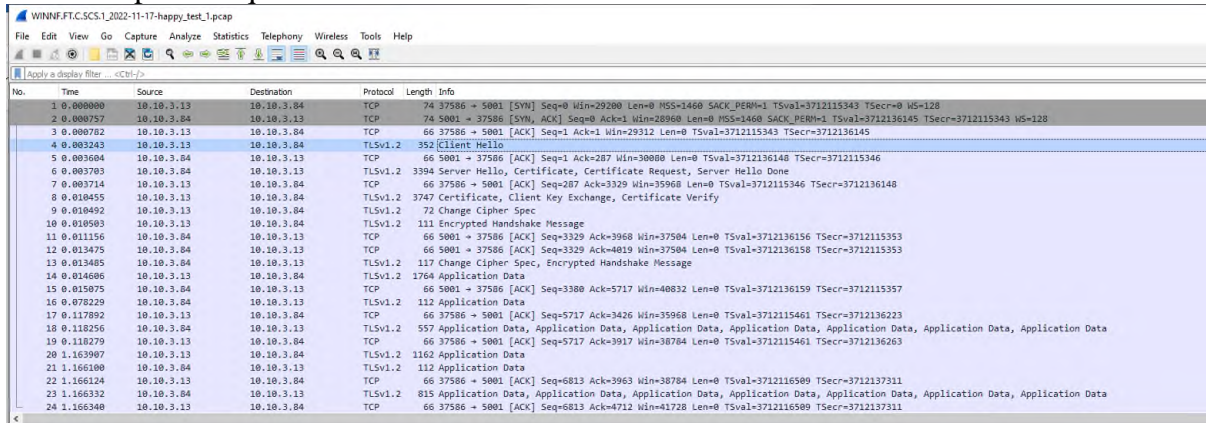


Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

DOT CBRS Radio: WINNF / Security Test Case Analysis

1. WINNF.FT.C.SCS.1

Packet Capture Sequence



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.3.13	10.10.3.04	TCP	74	37586 → 5001 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3712115343 TSecr=0 WS=128
2	0.000757	10.10.3.04	10.10.3.13	TCP	74	5001 → 37586 [SYN, ACK] Seq=0 Ack=1 Win=20800 Len=0 MSS=1460 SACK_PERM=1 TSval=3712136145 TSecr=3712115343 WS=128
3	0.000762	10.10.3.13	10.10.3.04	TCP	66	37586 → 5001 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3712115343 TSecr=3712136145
4	0.003243	10.10.3.13	10.10.3.04	TLSv1.2	352	Client Hello
5	0.003604	10.10.3.04	10.10.3.13	TCP	66	5001 → 37586 [ACK] Seq=1 Ack=287 Win=30000 Len=0 TSval=3712136148 TSecr=3712115346
6	0.003703	10.10.3.04	10.10.3.13	TLSv1.2	3394	Server Hello, Certificate, Certificate Request, Server Hello Done
7	0.003714	10.10.3.13	10.10.3.04	TCP	66	37586 → 5001 [ACK] Seq=287 Ack=3329 Win=35960 Len=0 TSval=3712115346 TSecr=3712136148
8	0.010455	10.10.3.13	10.10.3.04	TLSv1.2	3747	Certificate, Client Key Exchange, Certificate Verify
9	0.010492	10.10.3.13	10.10.3.04	TLSv1.2	72	Change Cipher Spec
10	0.010503	10.10.3.13	10.10.3.04	TLSv1.2	111	Encrypted Handshake Message
11	0.011156	10.10.3.04	10.10.3.13	TCP	66	5001 → 37586 [ACK] Seq=3329 Ack=3960 Win=37504 Len=0 TSval=3712136156 TSecr=3712115353
12	0.013475	10.10.3.04	10.10.3.13	TCP	66	5001 → 37586 [ACK] Seq=3329 Ack=4019 Win=37504 Len=0 TSval=3712136158 TSecr=3712115353
13	0.013485	10.10.3.04	10.10.3.13	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
14	0.014086	10.10.3.13	10.10.3.04	TLSv1.2	1764	Application Data
15	0.015075	10.10.3.04	10.10.3.13	TCP	66	5001 → 37586 [ACK] Seq=3380 Ack=5717 Win=40832 Len=0 TSval=3712136159 TSecr=3712115357
16	0.078229	10.10.3.04	10.10.3.13	TLSv1.2	112	Application Data
17	0.117892	10.10.3.13	10.10.3.04	TCP	66	37586 → 5001 [ACK] Seq=5717 Ack=3426 Win=35960 Len=0 TSval=3712115461 TSecr=3712136223
18	0.118256	10.10.3.04	10.10.3.13	TLSv1.2	557	Application Data, Application Data, Application Data, Application Data, Application Data
19	0.118279	10.10.3.13	10.10.3.04	TCP	66	37586 → 5001 [ACK] Seq=5717 Ack=3917 Win=30784 Len=0 TSval=3712115461 TSecr=3712136263
20	1.163907	10.10.3.13	10.10.3.04	TLSv1.2	1162	Application Data
21	1.166100	10.10.3.13	10.10.3.04	TLSv1.2	112	Application Data
22	1.166124	10.10.3.13	10.10.3.04	TCP	66	37586 → 5001 [ACK] Seq=6813 Ack=3963 Win=30784 Len=0 TSval=3712116509 TSecr=3712137311
23	1.166332	10.10.3.04	10.10.3.13	TLSv1.2	815	Application Data, Application Data, Application Data, Application Data, Application Data, Application Data, Application Data
24	1.166340	10.10.3.13	10.10.3.04	TCP	66	37586 → 5001 [ACK] Seq=6813 Ack=4712 Win=41728 Len=0 TSval=3712116509 TSecr=3712137311


WINNF test requirements:

WINNF test requirements from WINNF-TS-0122-V1.0.2 CBRS CBSD Test Specification:

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"> TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 	PASS
---	--	------

Analysis of WINNF Test Requirements

1. From Client Hello: TLS version = TLS 1.2

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

```

> Frame 4: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits)
> Ethernet II, Src: fa:16:3e:f6:32:cb (fa:16:3e:f6:32:cb), Dst: fa:16:3e:b0:f3:e6 (fa:16:3e:b0:f3:e6)
> Internet Protocol Version 4, Src: 10.10.3.13, Dst: 10.10.3.84
> Transmission Control Protocol, Src Port: 37586, Dst Port: 5001, Seq: 1, Ack: 1, Len: 286
▼ Transport Layer Security
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 281
    ▼ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 277
      Version: TLS 1.2 (0x0303)
      ▼ Random: 555e75a845ef20741d1c2502edded93ffcc6c68d5b81fcd646640089ce175e73
        GMT Unix Time: May 21, 2015 20:17:44.000000000 Eastern Daylight Time
        Random Bytes: 45ef20741d1c2502edded93ffcc6c68d5b81fcd646640089ce175e73
        Session ID Length: 0
        Cipher Suites Length: 86

```

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

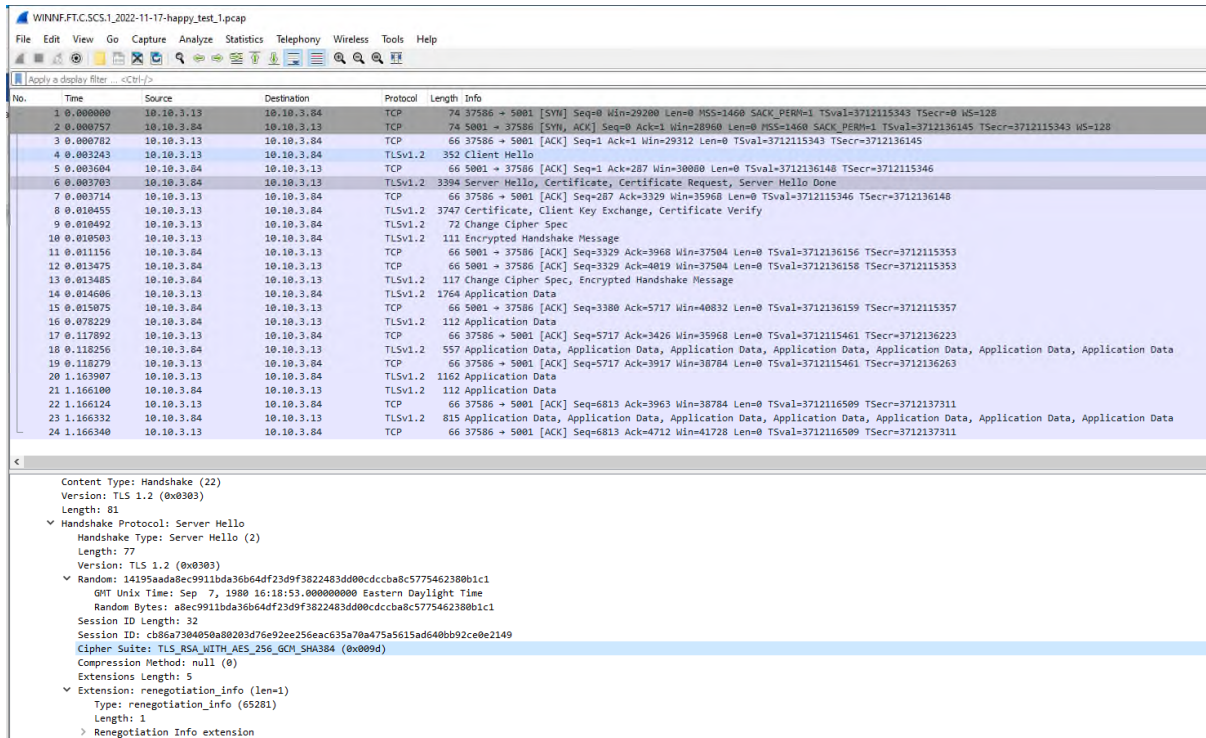
Cipher Suites (43 suites)

- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
- Cipher Suite: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
- Cipher Suite: TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (0x00a3)
- Cipher Suite: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
- Cipher Suite: TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (0x00a2)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
- Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)
- Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (0x006a)
- Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
- Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (0x0040)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02e)
- Cipher Suite: TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 (0xc032)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)
- Cipher Suite: TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 (0xc031)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)
- Cipher Suite: TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 (0xc02a)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 (0xc025)
- Cipher Suite: TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 (0xc029)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
- Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

- Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
- Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
- Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
- Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
- Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc005)
- Cipher Suite: TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc00f)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc004)
- Cipher Suite: TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc00e)
- Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
- Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

3. Cipher suite chosen (from Server Hello):
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)




The screenshot shows a Wireshark capture of a TLS handshake. The selected packet is a Server Hello message (packet 6) with details expanded to show the chosen cipher suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d). The details pane shows the following information:

- 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: 14195aada8ec9911bda36b64df23d9f3822483dd00cddc8bc5775462380b1c1
- GMT Unix Time: Sep 7, 1980 16:18:53.000000000 Eastern Daylight Time
- Random Bytes: a8ec9911bda36b64df23d9f3822483dd00cddc8bc5775462380b1c1
- Session ID Length: 32
- Session ID: cb86a7304056b00203d76e92ee256eac635a70a475a5615ad640bb920e2c419
- Cipher Suites: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- Compression Method: null (0)
- Extensions Length: 5
- Extension: renegotiation_info (len=1)
- Type: renegotiation_info (65281)
- Length: 1
- Renegotiation Info extension

4. The Registration request message arrived at the Test Harness,

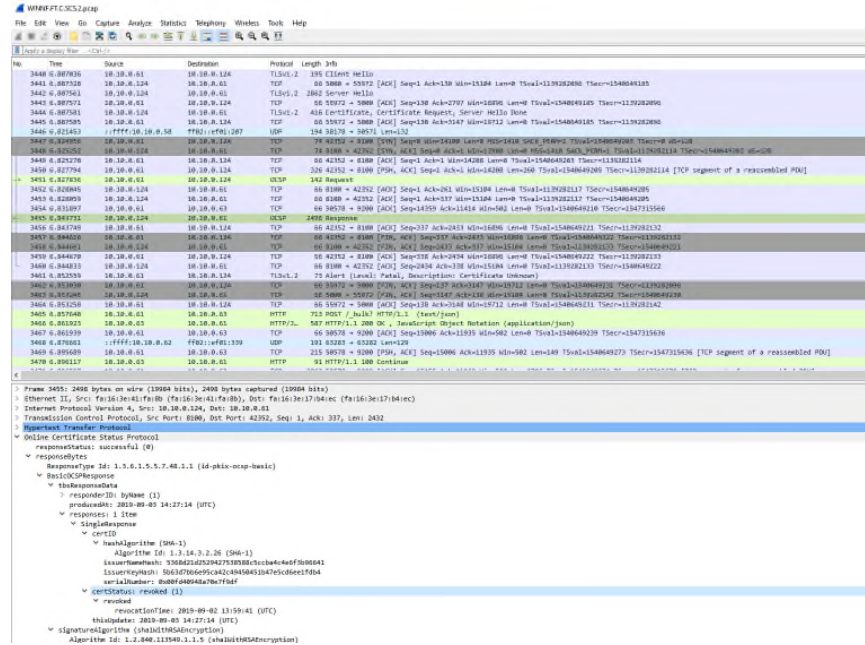
Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

so authentication was completed.

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

2. WINNF.FT.C.SCS.2

Packet Capture Sequence



The screenshot shows a packet capture sequence for a TLS handshake. The 'Details' pane is expanded to show the 'Online Certificate Status Protocol' section, which includes 'responseBytes' and 'CertificateStatus'. The 'CertificateStatus' section shows 'revocationInfo' and 'signatureAlgorithm'.

WINNF Test


Requirements:

WINNF test requirements from WINNF-TS-0122-V1.0.2 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

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
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: 5d6e7842d84d8cbfc7078fe9e913fcf7eb0fe3354f54f192c27204d2031e9aae
      Session ID Length: 32
      Session ID: e50dd1e43d8d5028f12ae61800ad52ffd4fe63dce8630ea523a1fd33b4cc72a4
      Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
      Compression Method: null (0)
      Extensions Length: 5
      > 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

```

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

```

> 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: 1.3.6.1.5.5.7.48.1.1 (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)
                Algorithm Id: 1.3.14.3.2.26 (SHA-1)
                issuerNameHash: 5368d21d2529427538588c5ccb4c46f3b96641
                issuerKeyHash: 5b63d7bb6e95ca42c49450451b47e5cd6ee1fdb4
                serialNumber: 0x00f040948a70e7f9df
              certStatus: revoked (1)
                revoked
                  revocationTime: 2019-09-02 13:59:41 (UTC)
                  thisUpdate: 2019-09-03 14:27:14 (UTC)
            ▼ signatureAlgorithm (sha1withRSAEncryption)
              Algorithm Id: 1.2.840.113549.1.1.5 (sha1withRSAEncryption)
              Padding: 0
              signature: 906f60430a1260eb9d7e21c1f2049842f94c7f6ee489ad67ebb9148a771cfe3e7ec59a0..
          certs: 1 item
            ▼ Certificate (id-at-commonName=SAS.OSCP.EXAMPLE,id-at-organizationalUnitName=UInnform SAS OSCP Responder Certi,id-at-organizationName=Test Lab for FCC PART 96,id-at-countryName=US)
              signatureAlgorithm (sha256withRSAEncryption)
                Algorithm Identifier (sha256withRSAEncryption)
                  Algorithm Id: 1.2.840.113549.1.1.11 (sha256withRSAEncryption)
                  Padding: 0
                  encrypted: 88a547c487789b3ad084c353a8cc700ff2c507626c62494bc12b172f6282a46f870bae87..

```

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

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

```

> 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)

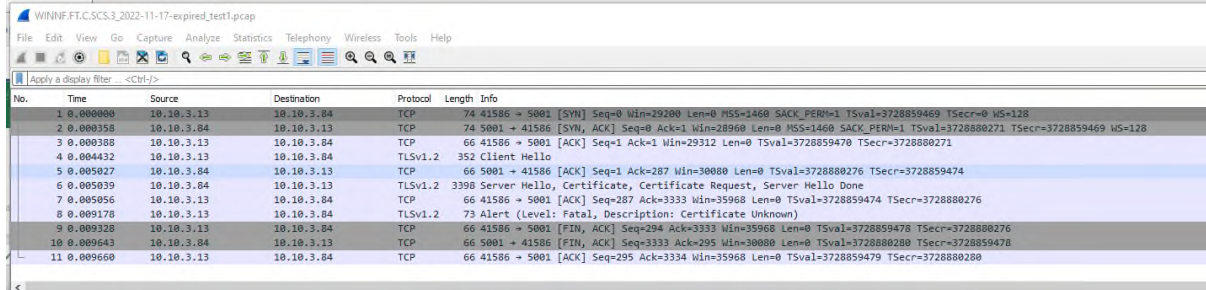
```

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

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

3. WINNF.FT.C.SCS.3

Packet Capture Sequence



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.3.13	10.10.3.84	TCP	74	41586 → 5001 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3728859469 TSecr=0 WS=128
2	0.000358	10.10.3.84	10.10.3.13	TCP	74	5001 → 41586 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=3728880271 TSecr=3728859469 WS=128
3	0.000388	10.10.3.13	10.10.3.84	TCP	66	41586 → 5001 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3728859470 TSecr=3728880271
4	0.004432	10.10.3.13	10.10.3.84	TLSv1.2	352	Client Hello
5	0.005027	10.10.3.84	10.10.3.13	TCP	66	5001 → 41586 [ACK] Seq=1 Ack=287 Win=30080 Len=0 TSval=3728880276 TSecr=3728859474
6	0.005039	10.10.3.84	10.10.3.13	TLSv1.2	3398	Server Hello, Certificate, Certificate Request, Server Hello Done
7	0.005056	10.10.3.13	10.10.3.84	TCP	66	41586 → 5001 [ACK] Seq=287 Ack=3333 Win=35968 Len=0 TSval=3728880276 TSecr=3728880276
8	0.009178	10.10.3.13	10.10.3.84	TLSv1.2	73	Alert (Level: Fatal, Description: Certificate Unknown)
9	0.009328	10.10.3.13	10.10.3.84	TCP	66	41586 → 5001 [FIN, ACK] Seq=294 Ack=3333 Win=35968 Len=0 TSval=3728859478 TSecr=3728880276
10	0.009643	10.10.3.84	10.10.3.13	TCP	66	5001 → 41586 [FIN, ACK] Seq=3333 Ack=295 Win=30080 Len=0 TSval=3728880280 TSecr=3728859478
11	0.009660	10.10.3.13	10.10.3.84	TCP	66	41586 → 5001 [ACK] Seq=295 Ack=3334 Win=35968 Len=0 TSval=3728859479 TSecr=3728880280

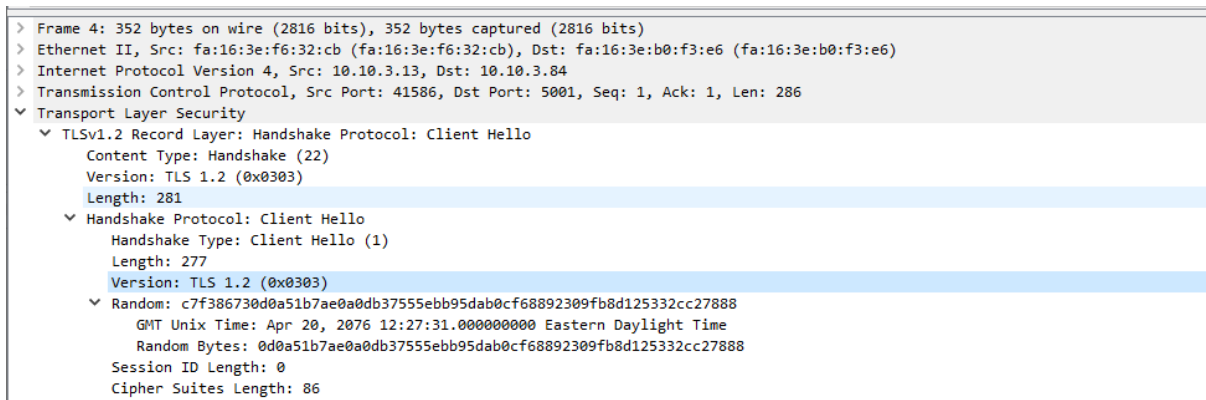
WINNF Test Requirements:

WINNF test requirements from WINNF-TS-0122-V1.0.2 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
---	--	------

Analysis of WINNF Test Requirements

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



```

> Frame 4: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits)
> Ethernet II, Src: fa:16:3e:f6:32:cb (fa:16:3e:f6:32:cb), Dst: fa:16:3e:b0:f3:e6 (fa:16:3e:b0:f3:e6)
> Internet Protocol Version 4, Src: 10.10.3.13, Dst: 10.10.3.84
> Transmission Control Protocol, Src Port: 41586, Dst Port: 5001, Seq: 1, Ack: 1, Len: 286
▼ Transport Layer Security
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 281
  ▼ Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 277
    Version: TLS 1.2 (0x0303)
  ▼ Random: c7f386730d0a51b7ae0a0db37555ebb95dab0cf68892309fb8d125332cc27888
    GMT Unix Time: Apr 20, 2076 12:27:31.00000000 Eastern Daylight Time
    Random Bytes: 0d0a51b7ae0a0db37555ebb95dab0cf68892309fb8d125332cc27888
    Session ID Length: 0
    Cipher Suites Length: 86
  
```

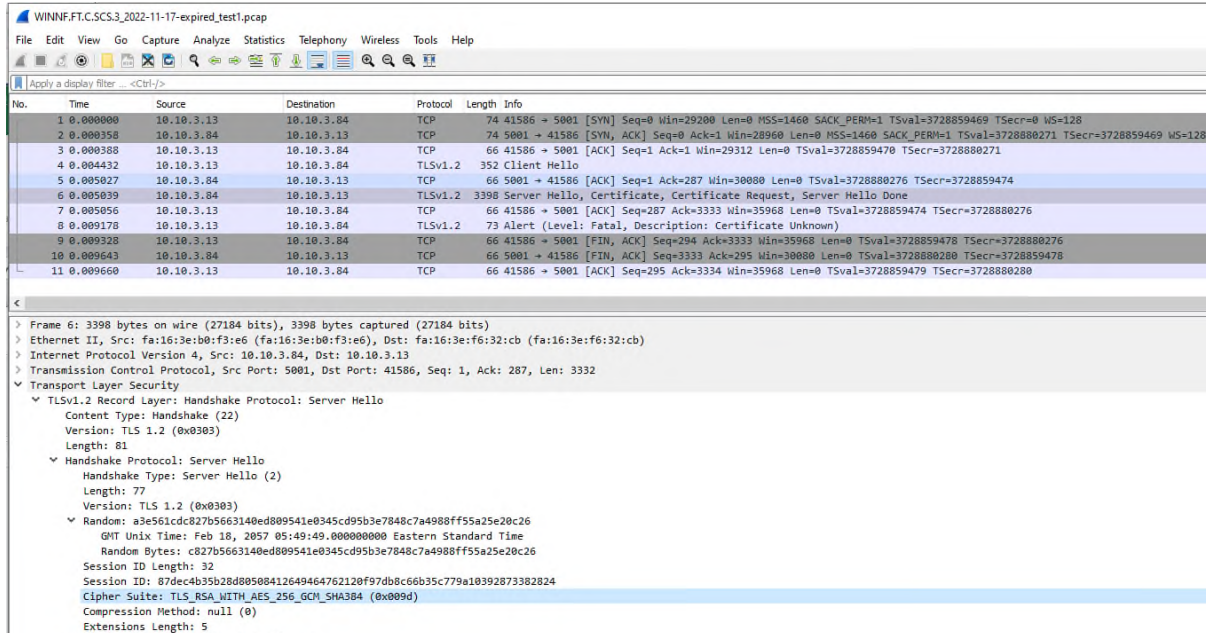
2. From Client Hello, cipher suite list is from WINNF approved list:

Cipher Suites

- Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)
- Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)
- Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

3. From Server Hello, cipher suite chosen:
 TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)



WINNFT.C.SCS.3_2022-11-17-expired_test1.pcap

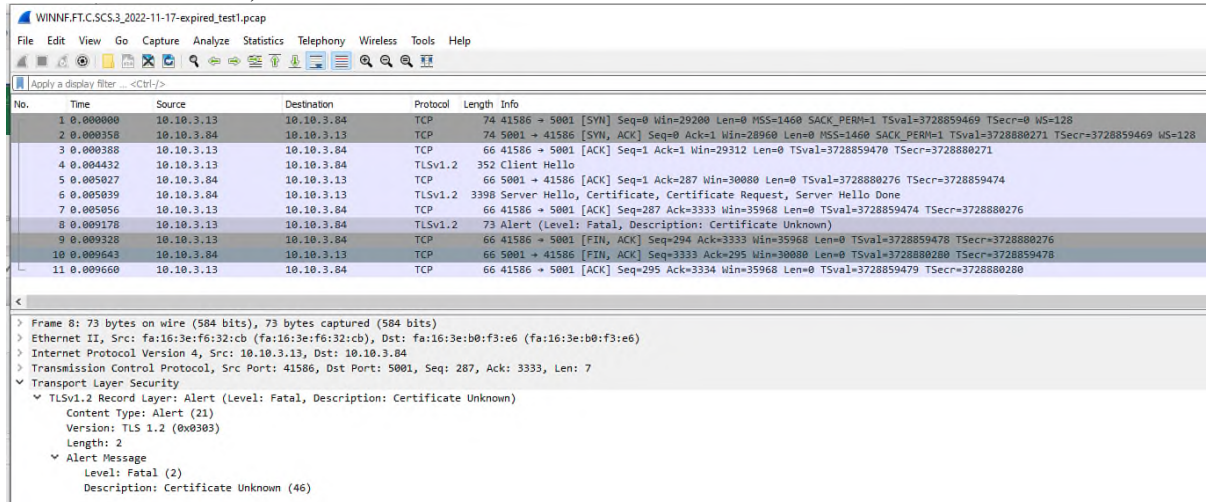
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-I>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.3.13	10.10.3.84	TCP	74	41586 → 5001 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3728859469 TSecr=0 WS=128
2	0.000358	10.10.3.84	10.10.3.13	TCP	74	5001 → 41586 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=3728880271 TSecr=3728859469 WS=128
3	0.000388	10.10.3.13	10.10.3.84	TCP	66	41586 → 5001 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3728859470 TSecr=3728880271
4	0.004432	10.10.3.13	10.10.3.84	TLSv1.2	352	Client Hello
5	0.005027	10.10.3.84	10.10.3.13	TCP	66	5001 → 41586 [ACK] Seq=1 Ack=287 Win=30080 Len=0 TSval=3728880276 TSecr=3728859474
6	0.005039	10.10.3.84	10.10.3.13	TLSv1.2	3398	Server Hello, Certificate, Certificate Request, Server Hello Done
7	0.005056	10.10.3.13	10.10.3.84	TCP	66	41586 → 5001 [ACK] Seq=287 Ack=3333 Win=35968 Len=0 TSval=3728859474 TSecr=3728880276
8	0.009178	10.10.3.13	10.10.3.84	TLSv1.2	73	Alert (Level: Fatal, Description: Certificate Unknown)
9	0.009328	10.10.3.13	10.10.3.84	TCP	66	41586 → 5001 [FIN, ACK] Seq=294 Ack=3333 Win=35968 Len=0 TSval=3728859478 TSecr=3728880276
10	0.009643	10.10.3.84	10.10.3.13	TCP	66	5001 → 41586 [FIN, ACK] Seq=3333 Ack=295 Win=30080 Len=0 TSval=3728880280 TSecr=3728859478
11	0.009660	10.10.3.13	10.10.3.84	TCP	66	41586 → 5001 [ACK] Seq=295 Ack=3334 Win=35968 Len=0 TSval=3728859479 TSecr=3728880280

> Frame 6: 3398 bytes on wire (27184 bits), 3398 bytes captured (27184 bits)
 > Ethernet II, Src: fa:16:3e:b0:f3:e6 (fa:16:3e:b0:f3:e6), Dst: fa:16:3e:f6:32:cb (fa:16:3e:f6:32:cb)
 > Internet Protocol Version 4, Src: 10.10.3.84, Dst: 10.10.3.13
 > Transmission Control Protocol, Src Port: 5001, Dst Port: 41586, Seq: 1, Ack: 287, Len: 3332
 > Transport Layer Security
 > TLSv1.2 Record Layer: Handshake Protocol: Server Hello
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 81
 > Handshake Protocol: Server Hello (2)
 Length: 77
 Version: TLS 1.2 (0x0303)
 > Random: a3e561cdc827b5663140ed809541e0345cd95b3e7848c7a4988ff55a25e20c26
 GMT Unix Time: Feb 18, 2057 05:49:49.000000000 Eastern Standard Time
 Random Bytes: c827b5663140ed809541e0345cd95b3e7848c7a4988ff55a25e20c26
 Session ID Length: 32
 Session ID: 87dec4b35b28d0805084126494647621120f97db8c66b35c779a10392873302824
 Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
 Compression Method: null (0)
 Extensions Length: 5

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



WINNFT.C.SCS.3_2022-11-17-expired_test1.pcap


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-I>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.3.13	10.10.3.84	TCP	74	41586 → 5001 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3728859469 TSecr=0 WS=128
2	0.000358	10.10.3.84	10.10.3.13	TCP	74	5001 → 41586 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=3728880271 TSecr=3728859469 WS=128
3	0.000388	10.10.3.13	10.10.3.84	TCP	66	41586 → 5001 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3728859470 TSecr=3728880271
4	0.004432	10.10.3.13	10.10.3.84	TLSv1.2	352	Client Hello
5	0.005027	10.10.3.84	10.10.3.13	TCP	66	5001 → 41586 [ACK] Seq=1 Ack=287 Win=30080 Len=0 TSval=3728880276 TSecr=3728859474
6	0.005039	10.10.3.84	10.10.3.13	TLSv1.2	3398	Server Hello, Certificate, Certificate Request, Server Hello Done
7	0.005056	10.10.3.13	10.10.3.84	TCP	66	41586 → 5001 [ACK] Seq=287 Ack=3333 Win=35968 Len=0 TSval=3728859474 TSecr=3728880276
8	0.009178	10.10.3.13	10.10.3.84	TLSv1.2	73	Alert (Level: Fatal, Description: Certificate Unknown)
9	0.009328	10.10.3.13	10.10.3.84	TCP	66	41586 → 5001 [FIN, ACK] Seq=294 Ack=3333 Win=35968 Len=0 TSval=3728859478 TSecr=3728880276
10	0.009643	10.10.3.84	10.10.3.13	TCP	66	5001 → 41586 [FIN, ACK] Seq=3333 Ack=295 Win=30080 Len=0 TSval=3728880280 TSecr=3728859478
11	0.009660	10.10.3.13	10.10.3.84	TCP	66	41586 → 5001 [ACK] Seq=295 Ack=3334 Win=35968 Len=0 TSval=3728859479 TSecr=3728880280

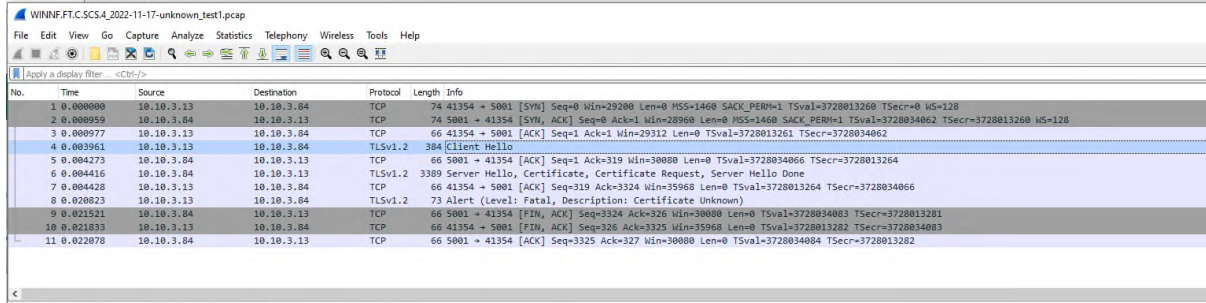
> Frame 8: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
 > Ethernet II, Src: fa:16:3e:f6:32:cb (fa:16:3e:f6:32:cb), Dst: fa:16:3e:b0:f3:e6 (fa:16:3e:b0:f3:e6)
 > Internet Protocol Version 4, Src: 10.10.3.13, Dst: 10.10.3.84
 > Transmission Control Protocol, Src Port: 41586, Dst Port: 5001, Seq: 287, Ack: 3333, 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	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

4. WINNF.FT.C.SCS.4

Packet Capture Sequence



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.3.13	10.10.3.84	TCP	74	41354 → 5001 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3728013260 TSecr=0 WS=128
2	0.000959	10.10.3.84	10.10.3.13	TCP	74	5001 → 41354 [SYN, ACK] Seq=0 Ack=1 Win=28968 Len=0 MSS=1460 SACK_PERM=1 TSval=3728034062 TSecr=3728013260 WS=128
3	0.000977	10.10.3.13	10.10.3.84	TCP	66	41354 → 5001 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3728013261 TSecr=3728034062
4	0.003961	10.10.3.13	10.10.3.84	TLSv1.2	384	Client Hello
5	0.004273	10.10.3.84	10.10.3.13	TCP	66	5001 → 41354 [ACK] Seq=1 Ack=319 Win=30080 Len=0 TSval=3728034066 TSecr=3728013264
6	0.004416	10.10.3.84	10.10.3.13	TLSv1.2	3389	Server Hello, Certificate, Certificate Request, Server Hello Done
7	0.004428	10.10.3.13	10.10.3.84	TCP	66	41354 → 5001 [ACK] Seq=319 Ack=3324 Win=35968 Len=0 TSval=3728013264 TSecr=3728034066
8	0.020823	10.10.3.13	10.10.3.84	TLSv1.2	73	Alert (Level: Fatal, Description: Certificate Unknown)
9	0.021521	10.10.3.84	10.10.3.13	TCP	66	5001 → 41354 [FIN, ACK] Seq=3324 Ack=326 Win=30080 Len=0 TSval=3728034083 TSecr=3728013261
10	0.021833	10.10.3.13	10.10.3.84	TCP	66	41354 → 5001 [FIN, ACK] Seq=326 Ack=3325 Win=35968 Len=0 TSval=3728013282 TSecr=3728034083
11	0.022078	10.10.3.84	10.10.3.13	TCP	66	5001 → 41354 [ACK] Seq=3325 Ack=327 Win=30080 Len=0 TSval=3728034084 TSecr=3728013282

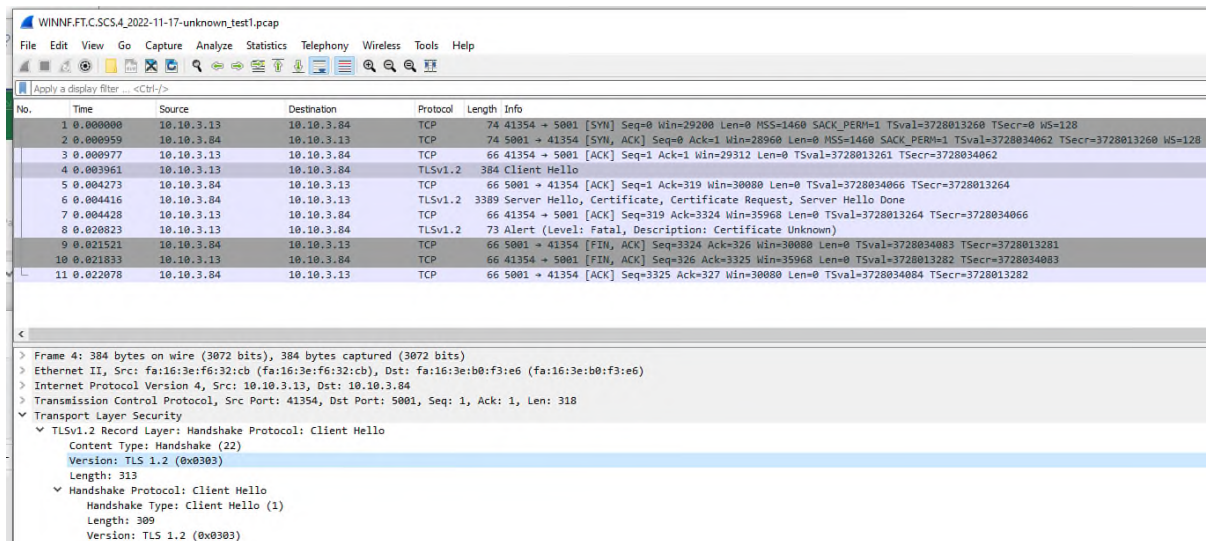
WINNF Test Requirements:

WINNF test requirements from WINNF-TS-0122-V1.0.2 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



Frame 4: 384 bytes on wire (3072 bits), 384 bytes captured (3072 bits) on interface 0
 Ethernet II, Src: fa:16:3e:f6:32:cb (fa:16:3e:f6:32:cb), Dst: fa:16:3e:b0:f3:e6 (fa:16:3e:b0:f3:e6)
 Internet Protocol Version 4, Src: 10.10.3.13, Dst: 10.10.3.84
 Transmission Control Protocol, Src Port: 41354, Dst Port: 5001, Seq: 1, Ack: 1, Len: 318
 Transport Layer Security
 TLSv1.2 Record Layer: Handshake Protocol: Client Hello
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 313
 Handshake Protocol: Client Hello
 Handshake Type: Client Hello (1)
 Length: 309
 Version: TLS 1.2 (0x0303)

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

Cipher Suites

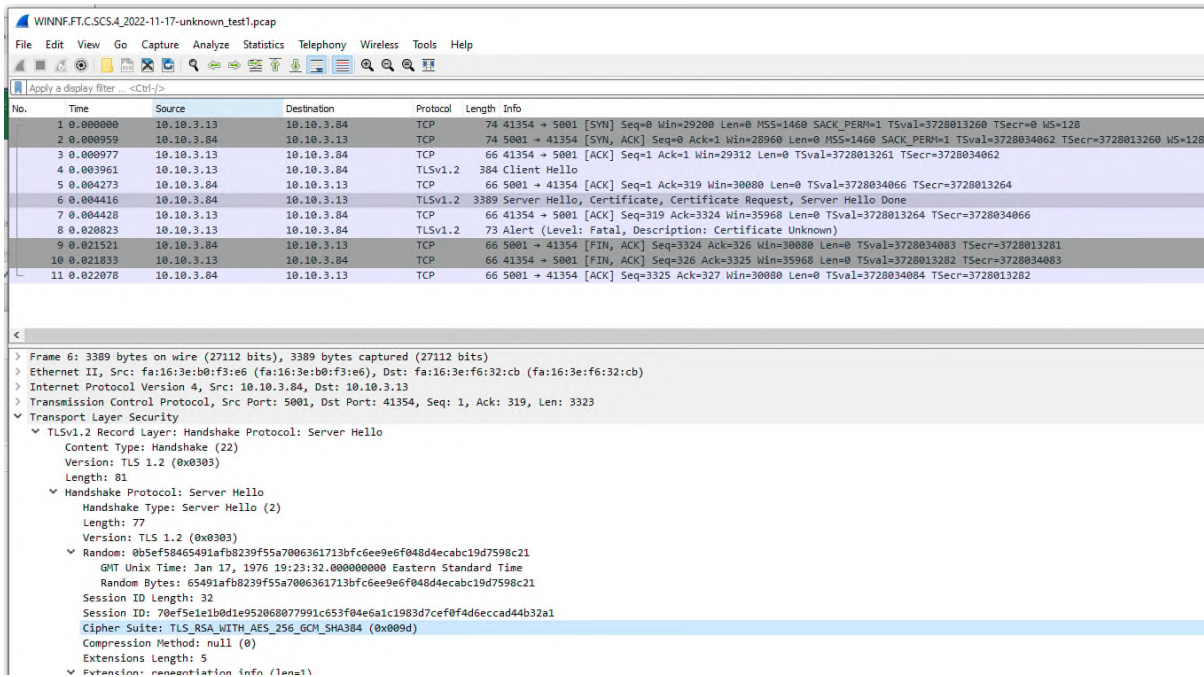
Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)

Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Cipher Suite: **TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)**
 Cipher Suite: **TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)**

3. From Server Hello, cipher suite chosen:
TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)



WINNFT.C.SCS4_2022-11-17-unknown_test1.pcap

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.3.13	10.10.3.84	TCP	74	41354 → 5001 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3728013260 TSecr=0 WS=128
2	0.000959	10.10.3.84	10.10.3.13	TCP	74	5001 → 41354 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=3728034062 TSecr=3728013260 WS=128
3	0.000977	10.10.3.13	10.10.3.84	TCP	66	41354 → 5001 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3728013261 TSecr=3728034062
4	0.003961	10.10.3.13	10.10.3.84	TLShv1.2	384	Client Hello
5	0.004273	10.10.3.84	10.10.3.13	TCP	66	5001 → 41354 [ACK] Seq=1 Ack=319 Win=30080 Len=0 TSval=3728034066 TSecr=3728013264
6	0.004416	10.10.3.84	10.10.3.13	TLShv1.2	3389	Server Hello, Certificate, Certificate Request, Server Hello Done
7	0.004428	10.10.3.13	10.10.3.84	TCP	66	41354 → 5001 [ACK] Seq=319 Ack=3324 Win=35968 Len=0 TSval=3728013264 TSecr=3728034066
8	0.020823	10.10.3.13	10.10.3.84	TLShv1.2	73	Alert (Level: Fatal, Description: Certificate Unknown)
9	0.021521	10.10.3.84	10.10.3.13	TCP	66	5001 → 41354 [FIN, ACK] Seq=3324 Ack=326 Win=30080 Len=0 TSval=3728034083 TSecr=3728013281
10	0.021833	10.10.3.13	10.10.3.84	TCP	66	41354 → 5001 [FIN, ACK] Seq=326 Ack=3325 Win=35968 Len=0 TSval=3728013282 TSecr=3728034083
11	0.022878	10.10.3.84	10.10.3.13	TCP	66	5001 → 41354 [ACK] Seq=3325 Ack=327 Win=30080 Len=0 TSval=3728034084 TSecr=3728013282

Frame 6: 3389 bytes on wire (27112 bits), 3389 bytes captured (27112 bits) on Ethernet II, Src: fa:16:3e:b0:f3:e6 (fa:16:3e:b0:f3:e6), Dst: fa:16:3e:f6:32:cb (fa:16:3e:f6:32:cb)

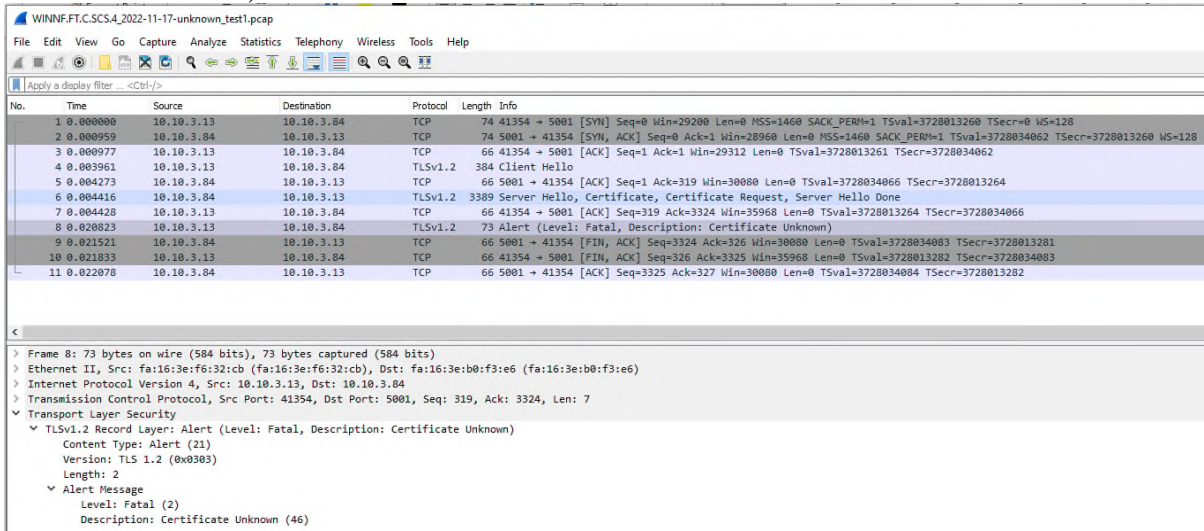
Internet Protocol Version 4, Src: 10.10.3.84, Dst: 10.10.3.13

Transmission Control Protocol, Src Port: 5001, Dst Port: 41354, Seq: 1, Ack: 319, Len: 3323

Transport Layer Security

- TLShv1.2 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: 0b5ef58465491afb8239f55a7006361713bfc6ee9e6f048d4ecabc19d7598c21
 - GMT Unix Time: Jan 17, 1976 19:23:32.000000000 Eastern Standard Time
 - Random Bytes: 65491afb8239f55a7006361713bfc6ee9e6f048d4ecabc19d7598c21
 - Session ID Length: 32
 - Session ID: 70ef5e1eb0d1e952068077991c653f04e6a1c1983d7cef0f4d6eccd44b32a1
 - Cipher Suite: **TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)**
 - Compression Method: null (0)
 - Extensions Length: 5
 - Extension: representation info (len=1)

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



WINNFT.C.SCS4_2022-11-17-unknown_test1.pcap

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.3.13	10.10.3.84	TCP	74	41354 → 5001 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3728013260 TSecr=0 WS=128
2	0.000959	10.10.3.84	10.10.3.13	TCP	74	5001 → 41354 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=3728034062 TSecr=3728013260 WS=128
3	0.000977	10.10.3.13	10.10.3.84	TCP	66	41354 → 5001 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3728013261 TSecr=3728034062
4	0.003961	10.10.3.13	10.10.3.84	TLShv1.2	384	Client Hello
5	0.004273	10.10.3.84	10.10.3.13	TCP	66	5001 → 41354 [ACK] Seq=1 Ack=319 Win=30080 Len=0 TSval=3728034066 TSecr=3728013264
6	0.004416	10.10.3.84	10.10.3.13	TLShv1.2	3389	Server Hello, Certificate, Certificate Request, Server Hello Done
7	0.004428	10.10.3.13	10.10.3.84	TCP	66	41354 → 5001 [ACK] Seq=319 Ack=3324 Win=35968 Len=0 TSval=3728013264 TSecr=3728034066
8	0.020823	10.10.3.13	10.10.3.84	TLShv1.2	73	Alert (Level: Fatal, Description: Certificate Unknown)
9	0.021521	10.10.3.84	10.10.3.13	TCP	66	5001 → 41354 [FIN, ACK] Seq=3324 Ack=326 Win=30080 Len=0 TSval=3728034083 TSecr=3728013281
10	0.021833	10.10.3.13	10.10.3.84	TCP	66	41354 → 5001 [FIN, ACK] Seq=326 Ack=3325 Win=35968 Len=0 TSval=3728013282 TSecr=3728034083
11	0.022878	10.10.3.84	10.10.3.13	TCP	66	5001 → 41354 [ACK] Seq=3325 Ack=327 Win=30080 Len=0 TSval=3728034084 TSecr=3728013282

Frame 8: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on Ethernet II, Src: fa:16:3e:f6:32:cb (fa:16:3e:f6:32:cb), Dst: fa:16:3e:b0:f3:e6 (fa:16:3e:b0:f3:e6)

Internet Protocol Version 4, Src: 10.10.3.13, Dst: 10.10.3.84


Transmission Control Protocol, Src Port: 41354, Dst Port: 5001, Seq: 319, Ack: 3324, Len: 7

Transport Layer Security

- TLShv1.2 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)

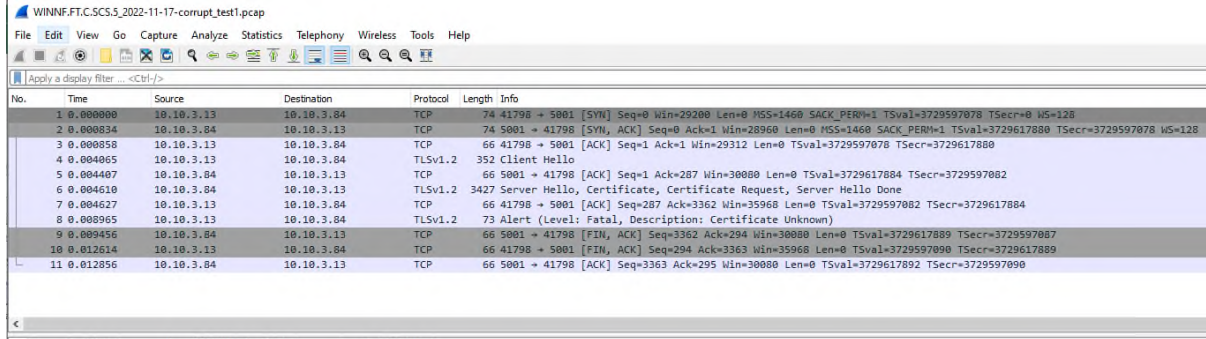
Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

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

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

5. WINNF.FT.C.SCS.5

Packet Capture Sequence



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.3.13	10.10.3.84	TCP	74	41798 → 5001 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=3729597078 TSecr=0 WS=128
2	0.000834	10.10.3.84	10.10.3.13	TCP	74	5001 → 41798 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM=1 TSval=3729617880 TSecr=3729597078 WS=128
3	0.000858	10.10.3.13	10.10.3.84	TCP	66	41798 → 5001 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=3729597078 TSecr=3729617880
4	0.004065	10.10.3.13	10.10.3.84	TLSv1.2	352	Client Hello
5	0.004407	10.10.3.84	10.10.3.13	TCP	66	5001 → 41798 [ACK] Seq=1 Ack=287 Win=30080 Len=0 TSval=3729617884 TSecr=3729597082
6	0.004610	10.10.3.84	10.10.3.13	TLSv1.2	3427	Server Hello, Certificate, Certificate Request, Server Hello Done
7	0.004627	10.10.3.13	10.10.3.84	TCP	66	41798 → 5001 [ACK] Seq=287 Ack=3362 Win=35968 Len=0 TSval=3729597082 TSecr=3729617884
8	0.009965	10.10.3.13	10.10.3.84	TLSv1.2	73	Alert (Level: Fatal, Description: Certificate Unknown)
9	0.009456	10.10.3.84	10.10.3.13	TCP	66	5001 → 41798 [FIN, ACK] Seq=3362 Ack=294 Win=30080 Len=0 TSval=3729617889 TSecr=3729597087
10	0.012614	10.10.3.13	10.10.3.84	TCP	66	41798 → 5001 [FIN, ACK] Seq=294 Ack=3363 Win=35968 Len=0 TSval=3729597090 TSecr=3729617889
11	0.012856	10.10.3.84	10.10.3.13	TCP	66	5001 → 41798 [ACK] Seq=3363 Ack=295 Win=30080 Len=0 TSval=3729617892 TSecr=3729597090

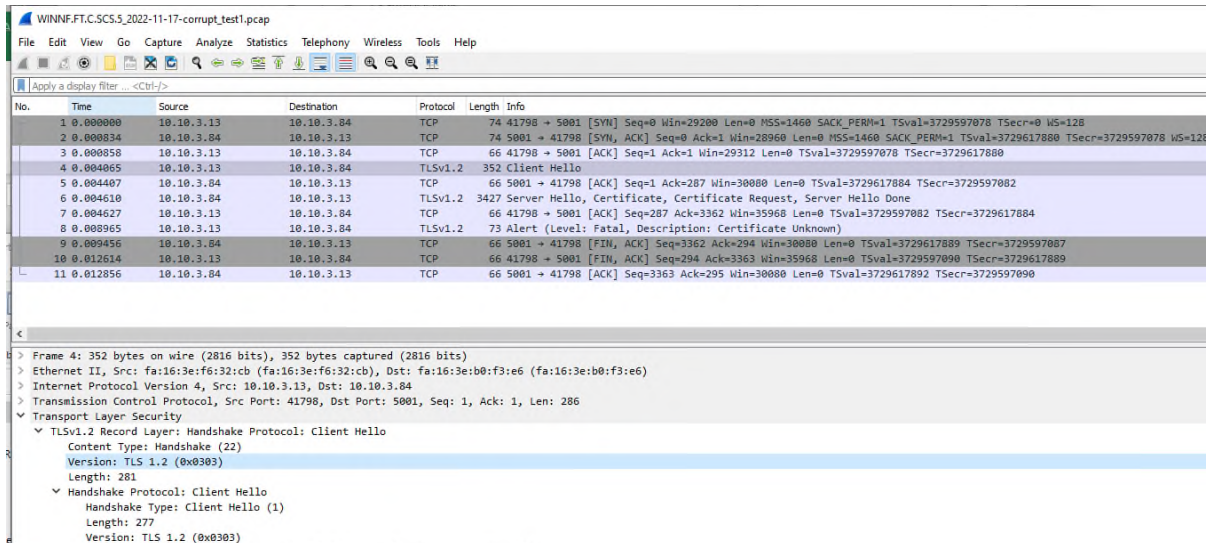
WINNF Test Requirements:

WINNF test requirements from WINNF-TS-0122-V1.0.2 CBRS CBSB 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



Frame 4: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits)

- Ethernet II, Src: fa:16:3e:f6:32:cb (fa:16:3e:f6:32:cb), Dst: fa:16:3e:b0:f3:e6 (fa:16:3e:b0:f3:e6)
- Internet Protocol Version 4, Src: 10.10.3.13, Dst: 10.10.3.84
- Transmission Control Protocol, Src Port: 41798, Dst Port: 5001, Seq: 1, Ack: 1, Len: 286
- Transport Layer Security
 - ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
 - Content Type: Handshake (22)
 - Version: TLS 1.2 (0x0303)
 - Length: 281
 - ▼ Handshake Protocol: Client Hello
 - Handshake Type: Client Hello (1)
 - Length: 277
 - Version: TLS 1.2 (0x0303)

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

Cipher Suites

Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)

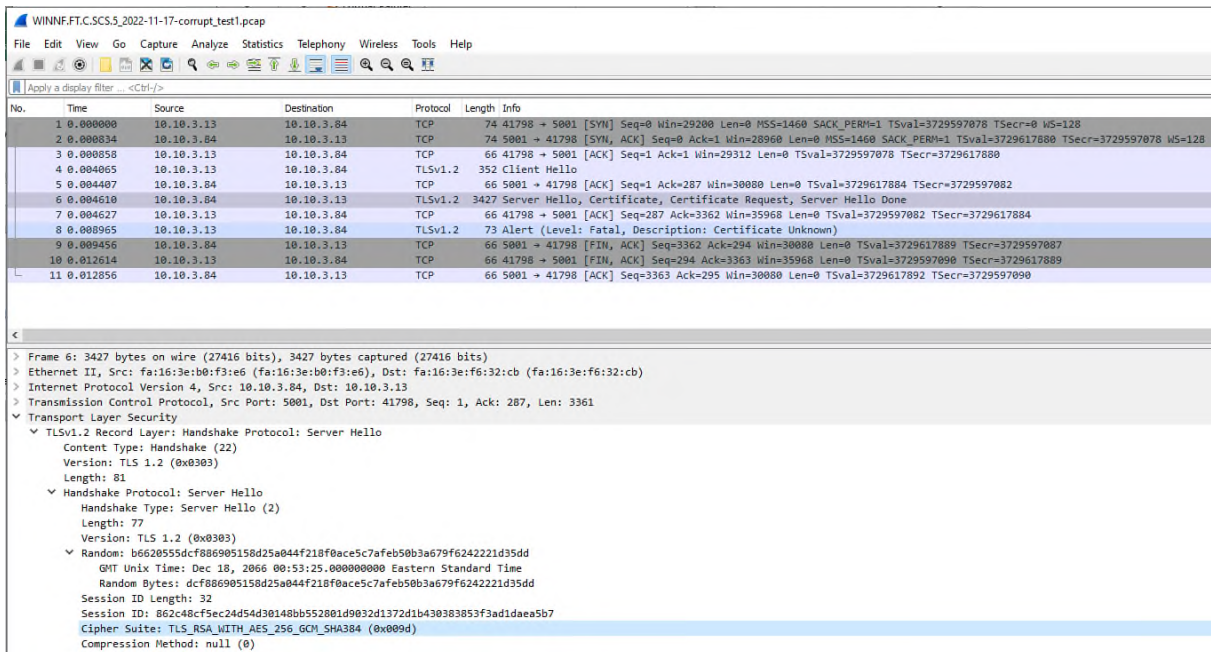
Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

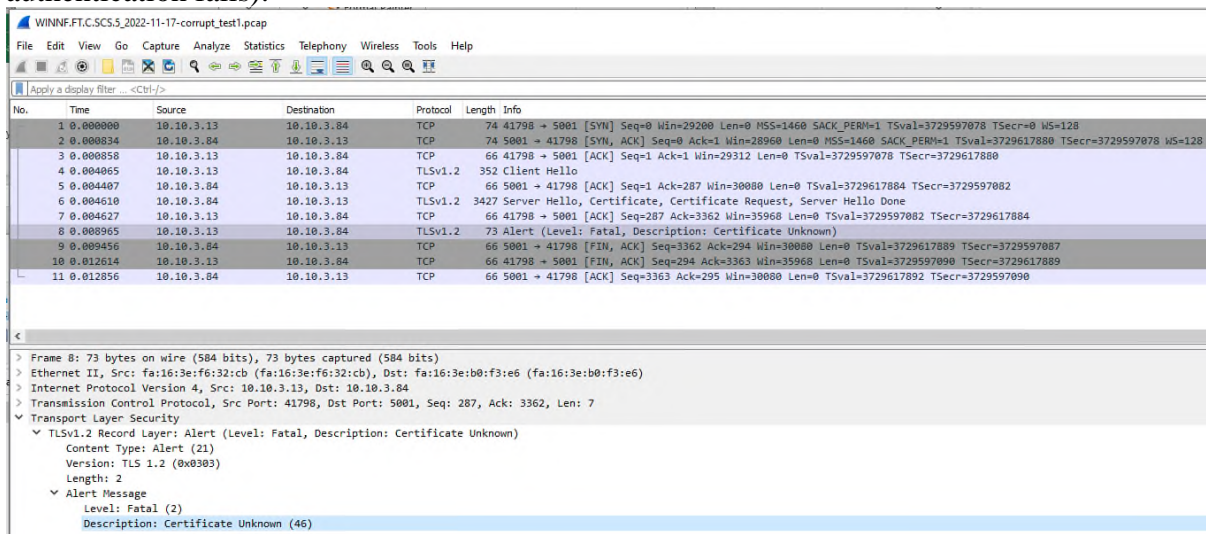
Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
 Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)

3. From Server Hello, cipher suite chosen:

TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)



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



Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

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


Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

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	24 months	2024-04-26
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	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Appendix A – EUT & Client Provided Details

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

General EUT Description

Manufacturer	Ericsson
Address	Torshamnsgatan 23 Kista SE-16480 Stockholm Sweden
Product Name	AIR 3268 B48
Product Number	KRD 901 254/1 (with antenna, security unlocked) KRD 901 254/11** (with antenna, security locked) KRD 901 254/3 (CAB/RDNB board for testing purpose, security unlocked) KRD 901 254/31* (CAB/RDNB board for testing purpose, security locked)
	Note*: Tested unit Note**: This will be the marketed, sold unit.
Serial Number(s)	E23E345115
Software Version	CXP9024418/15-R52A165_R13A190 Domain Proxy Software Version ERICdomainproxyservice_CXP9035414 2.52.6
Hardware Version	R1B
Test Specification/Issue/Date	FCC CFR 47 Part 96: 2022

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Technical Description


AIR 3268 B48 is a single-band TDD Antenna Integrated Radio unit with 32 transmitters and 32 receivers and 64 dual-polarized antenna elements supporting 3550-3700MHz. It has an enhanced Common Public Radio Interface (eCPRI) and 16/8 downlink/uplink layer multi-user MIMO supporting LTE, and is NR prepared.

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.

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Appendix B – EUT, Peripherals, and Test Setup Photos

Client	Ericsson	
Product	KRD 901 254 Air 3268 B48 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Test setup

