

Test Report

As per

FCC Part 96 SAS requirements (CBRS Test Plan)

on the
**Ericsson Radio Unit KRD 901 258 AIR
1672 B48 (3550-3700MHz)**

FCC ID(s): TA8AKRD901258



**Add value.
Inspire trust.**

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

Testing produced
for

Ericsson AB

See Appendix A for
full client & EUT
details.

Scott Drysdale.
Test Personnel

A handwritten signature in black ink, appearing to read "Scott Drysdale", written over a horizontal line.

Nour El Masri
Report Reviewer

A handwritten signature in black ink, appearing to read "Nour El Masri", written over a horizontal line.



Testing Laboratory
Certificate #2955.19

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (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	12
Applicable Standards, Specifications and Methods.....	13
Document Revision Status.....	14
Definitions and Acronyms	15
Testing Facility	16
Calibrations and Accreditations.....	16
Testing Environmental Conditions and Dates	17
Detailed Test Results Section	18
Registration.....	19
Grant	27
Heartbeat	29
Measurement.....	37
Relinquishment and Deregistration.....	40
Power Measurement.....	42
WINNF Security Test Case Analysis	49
Test Equipment	70
Appendix A – EUT & Client Provided Details	71
Technical Description	73
Appendix B – EUT, Peripherals, and Test Setup Photos.....	74

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (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 Radio Unit KRD 901 258 AIR 1672 B48 (3550-3700MHz)** 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 901 258 AIR 1672 B48 B77 (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 Radio Unit KRD 901 258 AIR 1672 B48 (3550-3700MHz)
EUT passed all tests performed	Yes
Tests conducted by	Scott Drysdale

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

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Test Results Summary

Section as per Working Document WINNF-TS-0122

Section	CBSD	DP	Test Case ID	Test Case Title	RF Measurement Requirement	Pass / Fail
6.1.4.1.1	X	--	WINNF.FT.C. REG.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. REG.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. REG.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. REG.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. REG.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. REG.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. REG.7	Registration due to change of an installation parameter	Test waits until transmission starts, then trigger an installationParam change. Record time at which transmission stops. Time must be within 60	P

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

					seconds of the installationParam change taking effect.	
6.1.4.2.1	X	--	WINNF.FT.C. REG.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. REG.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. REG.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. REG.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. REG.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. REG.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. REG.14	Blacklisted CBSD (responseCode 101)	Monitor for 60 seconds after REG message sent. No transmission during test.	N/A
6.1.4.2.8	--	X	WINNF.FT.D. REG.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. REG.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. REG.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. REG.18	Group Error (responseCode 201)	Monitor for 60 seconds after REG message	N/A

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

					sent. No transmission during test.	
6.1.4.2.12	--	X	WINNF.FT.D. REG.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. REG.20	Category A CBSD location update		N/A
6.3.4.2.1	X	X	WINNF.FT.C. GRA.1	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. GRA.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. HBT.1	Heartbeat Success Case (first Heartbeat Response)	Monitor RF from start of test. Ensure that: • 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)	N/A
6.4.4.1.2	--	X	WINNF.FT.D. HBT.2	Domain Proxy Heartbeat Success Case (first Heartbeat Response)	Monitor RF from start of test. Ensure that: • 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. HBT.3	Heartbeat responseCode=105 (DEREGISTER)	Monitor RF transmission. Ensure that: • CBSD stops transmission within	P

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

					60 seconds of the heartbeatResponse which contains responseCode = 105	
6.4.4.2.2	X	--	WINNF.FT.C. HBT.4	Heartbeat responseCode=500 (TERMINATED_GRANT)		N/A
6.4.4.2.3	X	X	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
6.4.4.2.4	X	X	WINNF.FT.C. HBT.6	Heartbeat responseCode=501 (SUSPENDED_GRANT) in Subsequent Heartbeat Response	Monitor RF transmission. Ensure: • CBSD stops transmission within 60 seconds of heartbeatResponse which contains responseCode=501	p
6.4.4.2.5	X	X	WINNF.FT.C. HBT.7	Heartbeat responseCode=502 (UNSYNC_OP_PARAMETER)	Monitor RF transmission. Ensure: • CBSD stops transmission within 60 seconds of heartbeatResponse which contains responseCode=502	p
6.4.4.2.6	--	X	WINNF.FT.D. HBT.8	Domain Proxy Heartbeat responseCode=500 (TERMINATED_GRANT)	Monitor RF transmission. CBSDs will have different behavior: • CBSD1: will continue to transmit to end of test (this is not a pass/fail criteria, but check) • CBSD2: must stop transmission within 60 seconds of being sent heartbeatResponse with responseCode = 500	P

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

6.4.4.3.1	X	X	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
6.4.4.3.2	X	X	WINNF.FT.C.HBT.10	Heartbeat Response Absent (Subsequent Heartbeat)	Monitor RF transmission. Verify: • CBSD must stop transmission within transmitExpireTime +60 seconds, where transmitExpireTime is from last successful heartbeatResponse message	P
6.5.4.2.1	X	--	WINNF.FT.C.MES.1	Registration Response contains measReportConfig	No RF monitoring	N/A
6.5.4.2.2	--	X	WINNF.FT.D.MES.2	Domain Proxy Registration Response contains measReportConfig	No RF monitoring	P
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: • 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:	P

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

					• CBSD stops transmission at any time prior to sending the relinquishmentRequest message.	
6.7.4.1.1	X	--	WINNF.FT.C.DRG.1	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)	N/A
6.7.4.1.2	--	X	WINNF.FT.D.DRG.2	Domain Proxy Successful Deregistration	Monitor RF transmission. Ensure: • CBSD stops transmission at any time prior to sending the relinquishmentRequest message or deregistrationRequest message (whichever is sent first)	P
6.8.4.1.1	X	X	WINNF.FT.C.SCS.1	Successful TLS connection between UUT and SAS Test Harness	No RF transmission during test Check the tcpdump for the TLS information	P
6.8.4.2.1	X	X	WINNF.FT.C.SCS.2	TLS failure due to revoked certificate	No RF transmission during test Check the tcpdump for the TLS information	P
6.8.4.2.2	X	X	WINNF.FT.C.SCS.3	TLS failure due to expired server certificate	No RF transmission during test Check the tcpdump for the TLS information	P
6.8.4.2.3	X	X	WINNF.FT.C.SCS.4	TLS failure when SAS Test Harness certificate is issue by unknown CA	No RF transmission during test Check the tcpdump for the TLS information	P

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

6.8.4.2.4	X	X	WINNF.FT.C.SCS.5	TLS failure when certificate at the SAS Test Harness is corrupted	No RF transmission during test Check the tcpdump for the TLS information	P
7.1.4.1.1	X	X	WINNF.PT.C.HBT	UUT RF Transmit Power Measurement	Power Spectral Density test case. Assume we use 1 carrier bandwidth (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

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 901 258 AIR 1672 B48 B77 (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 901 258/2 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-V1.0.2, 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-V1.0.2, 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-V1.0.2, 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.

Where timing of the graphs provided for less than 1 second capability of resolution between the event and the requirement, the test was additionally observed via slow-motion video where determination between the which event occurred first could be made.

Logs are kept on file.

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Applicable Standards, Specifications and Methods

ANSI C63.26:2015	American National Standard for Compliance Testing of Transmitters Used in Licensed Radio Services
CFR47 FCC Part 96	Code of Federal Regulations – Citizens Broadband Radio Service
WINNF-TS-0122 Version V1.0.2 25 November 2020	Conformance and Performance Test Technical Specification; CBSD/DP as Unit Under Test (UUT) Working Document
ISO/IEC 17025:2017	General requirements for the competence of testing and calibration laboratories

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Document Revision Status

7169016414 000 Draft release – July 14, 2025

7169016414 001 First release – July 15, 2025 – minor revisions as per customer request.

7169016414 002 Second release – July 15, 2025 – 2nd minor revisions as per customer request.

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (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.

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.

NCR – No Calibration Required

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 901 258 AIR 1672 B48 B77 (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 901 258 AIR 1672 B48 B77 (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)
July 9-11	All	SD	20-23	40-55	98-102

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Detailed Test Results Section

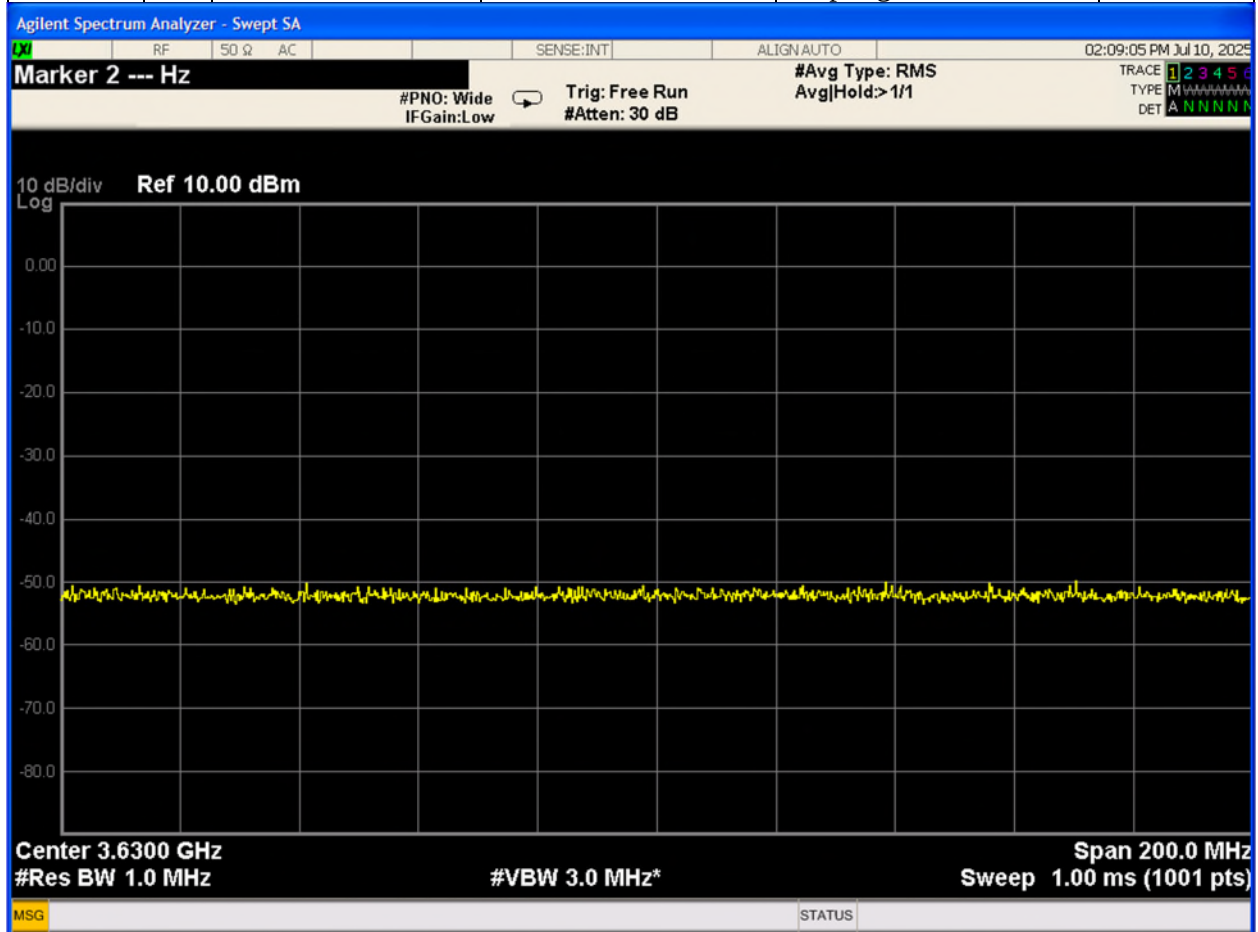
Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Registration.

D.REG.2

Authorization transmit after it receives authorization from a SAS.

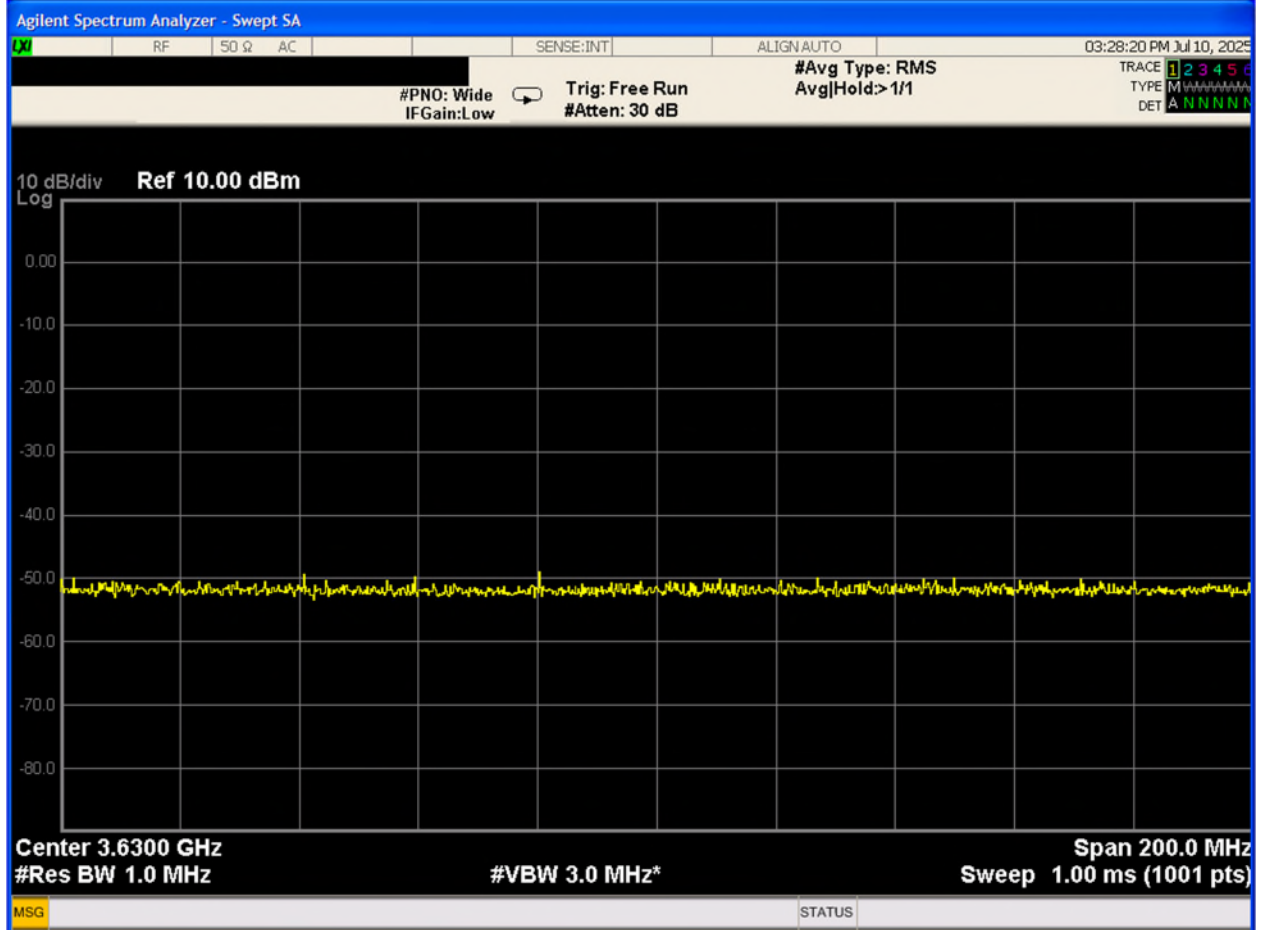
Section	DP		Test Case ID	Test Case Title	Pass / Fail
6.1.4.1.2	X		WINNF.FT.D.REG.2	Domain Proxy Multi-Step registration	P



Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

D.REG.6

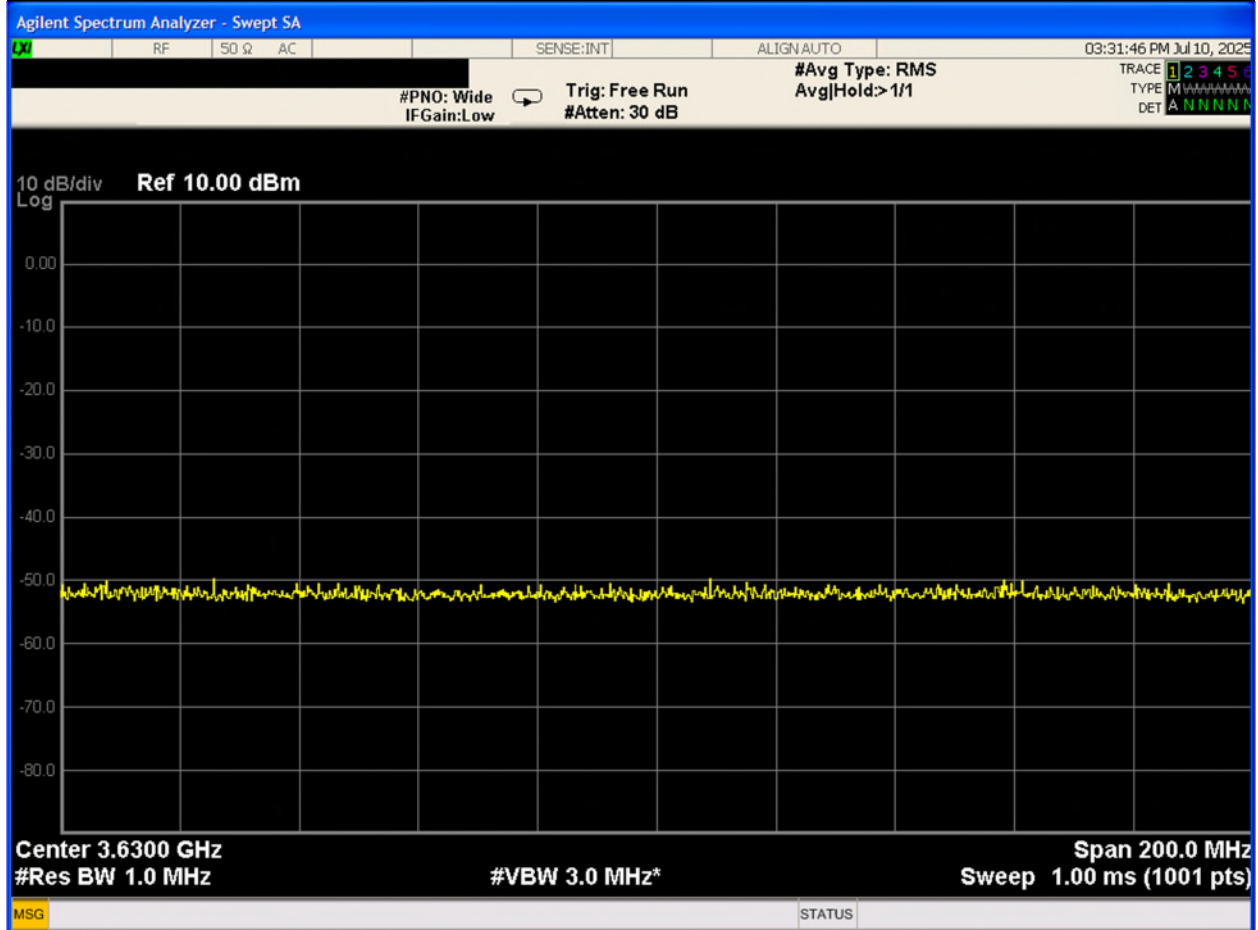
6.1.4.1.6	X	WINNF.FT.D.REG.6	Domain Proxy Single-Step registration for CBSD with CPI signed data	P
-----------	---	------------------	---	---



Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

D.REG.9

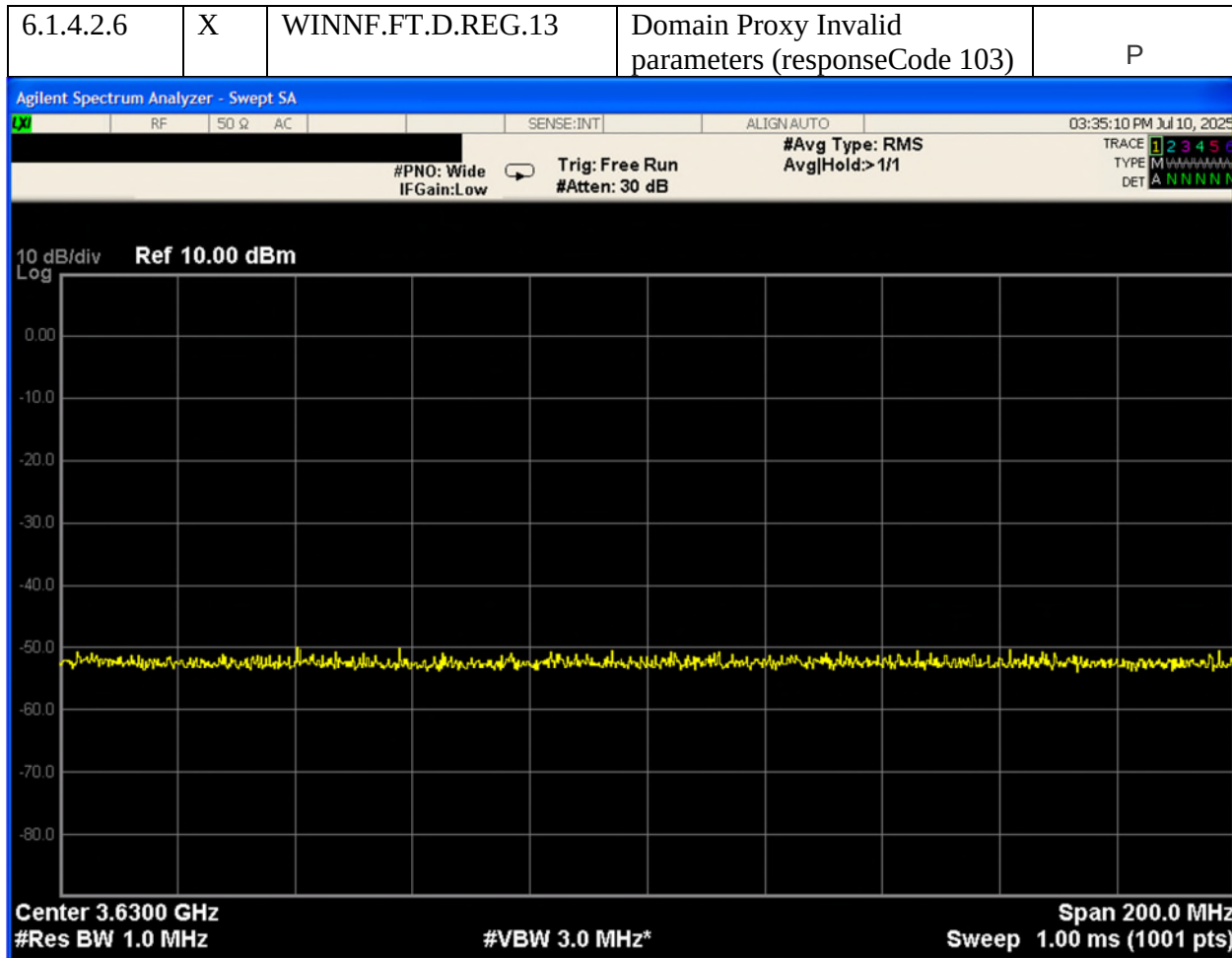
6.1.4.2.2	X	WINNF.FT.D.REG.9	Domain Proxy Missing Required parameters (responseCode 102)	P
-----------	---	------------------	---	---



Note response code verified via logs kept on file.

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

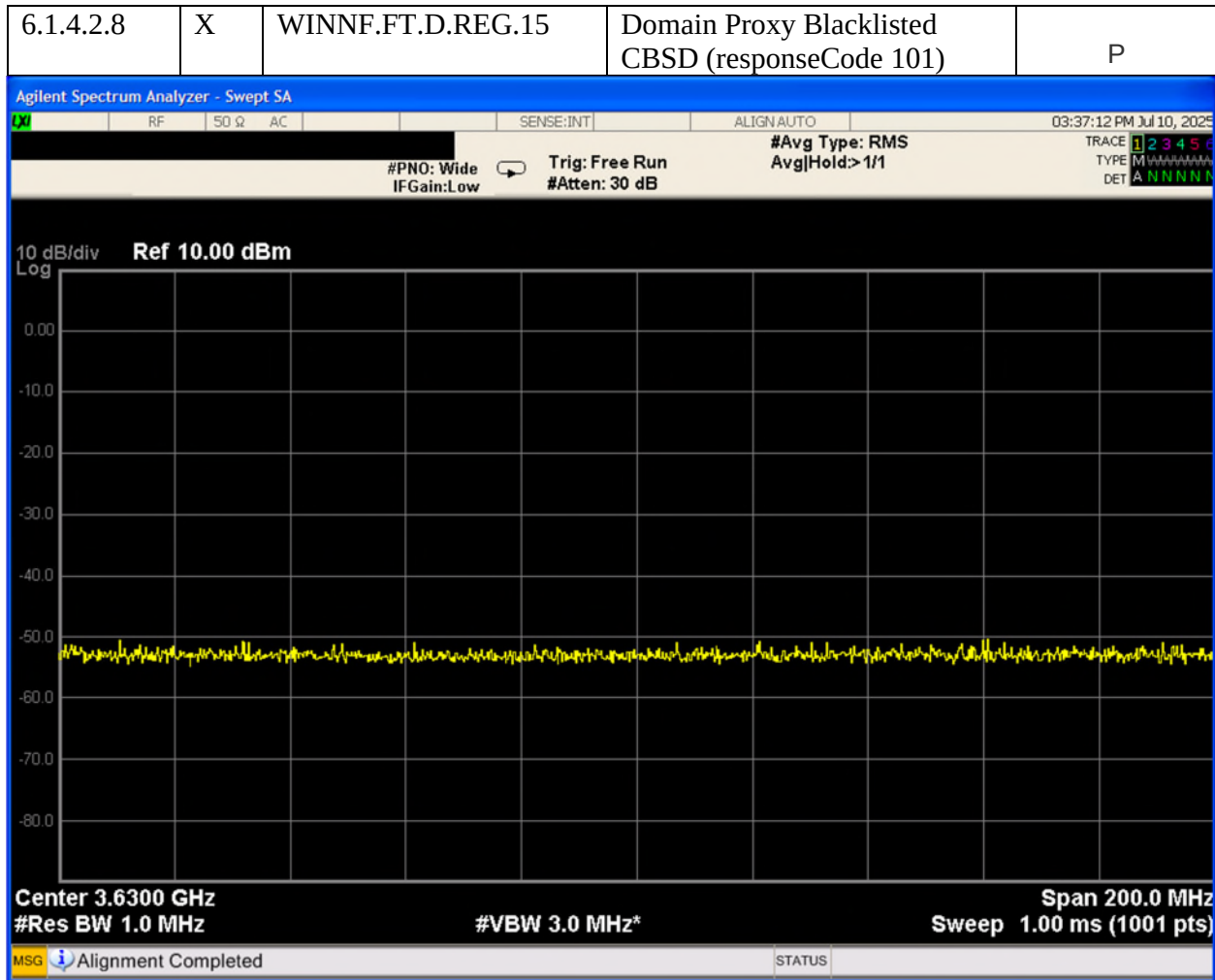
D.REG.13



Note response code verified via logs kept on file.

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

D.REG.15

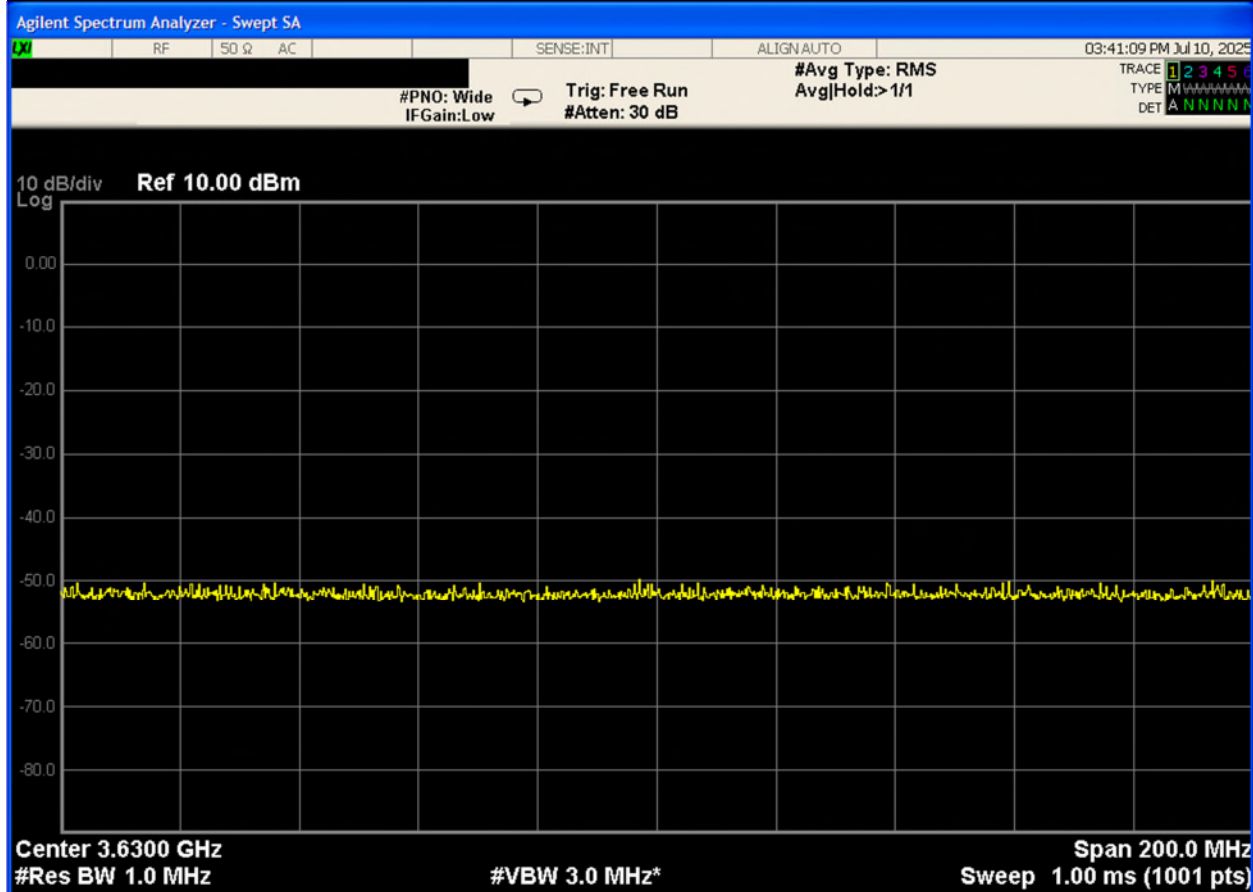


Note response code verified via logs kept on file.

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

D.REG.17

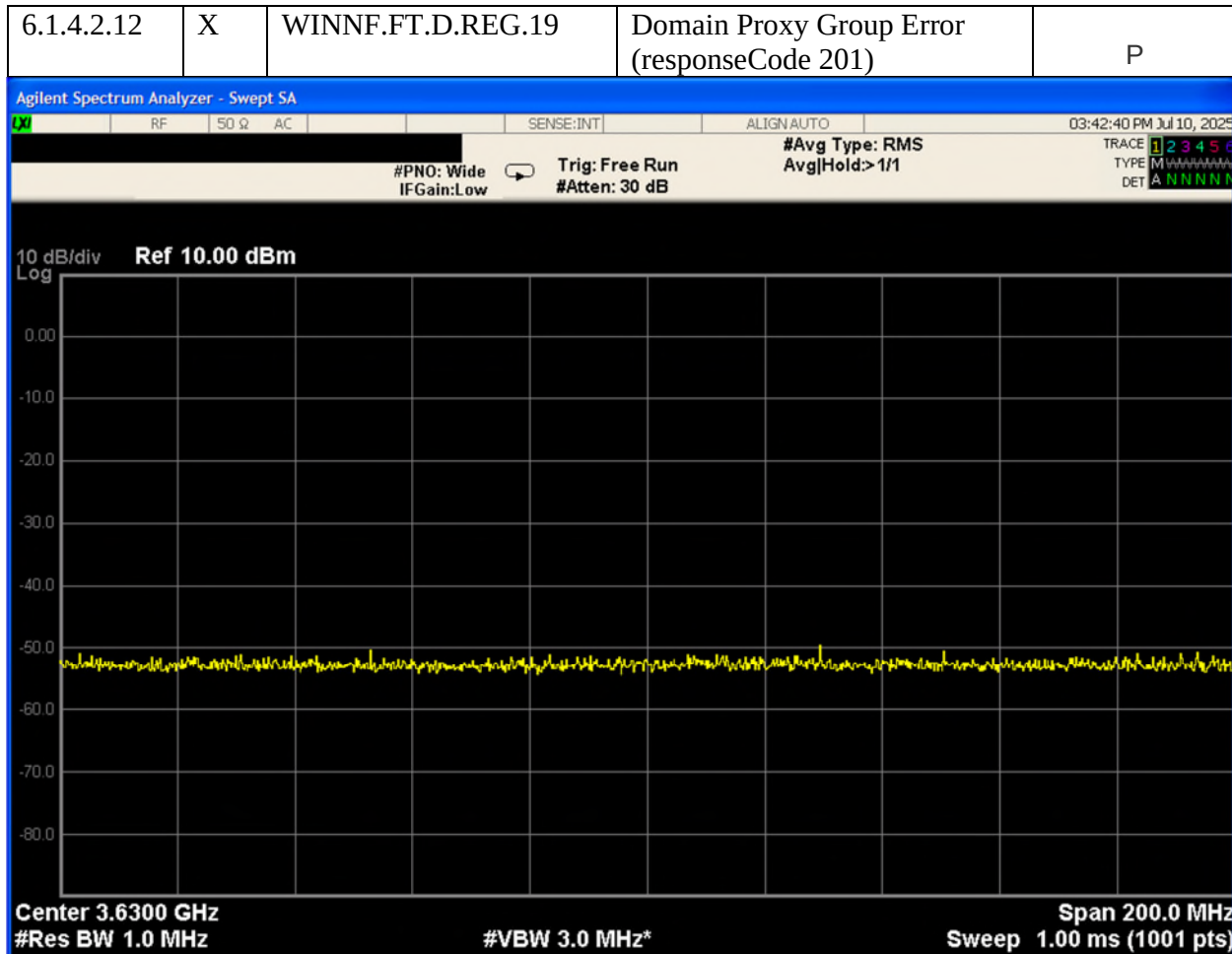
6.1.4.2.10	X	WINNF.FT.D.REG.17	Domain Proxy Unsupported SAS protocol version responseCode 100)	P
------------	---	-------------------	---	---



Note response code verified via logs kept on file.

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

D.REG.19



Note response code verified via logs kept on file.

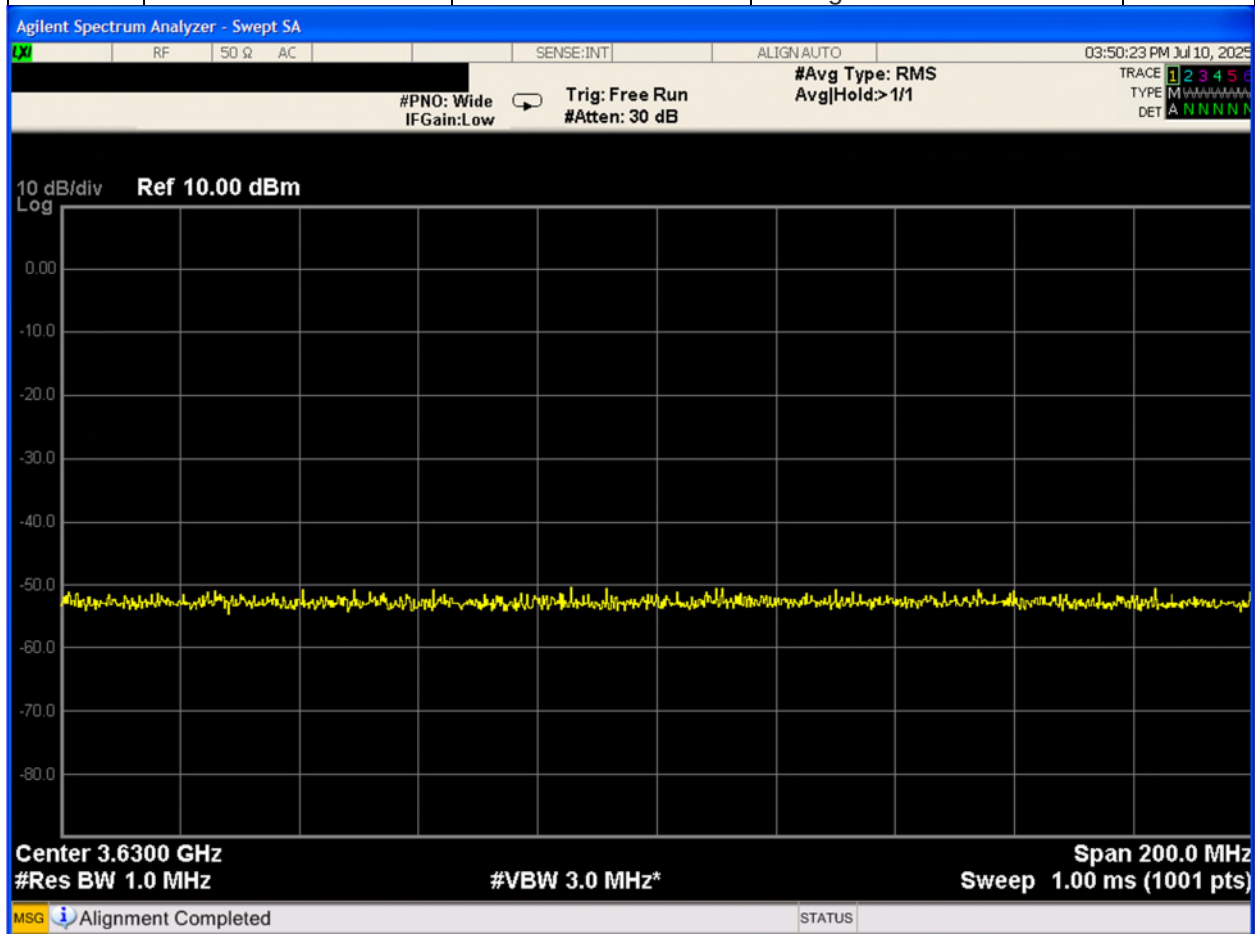
Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Grant

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.

C.GRA.1

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

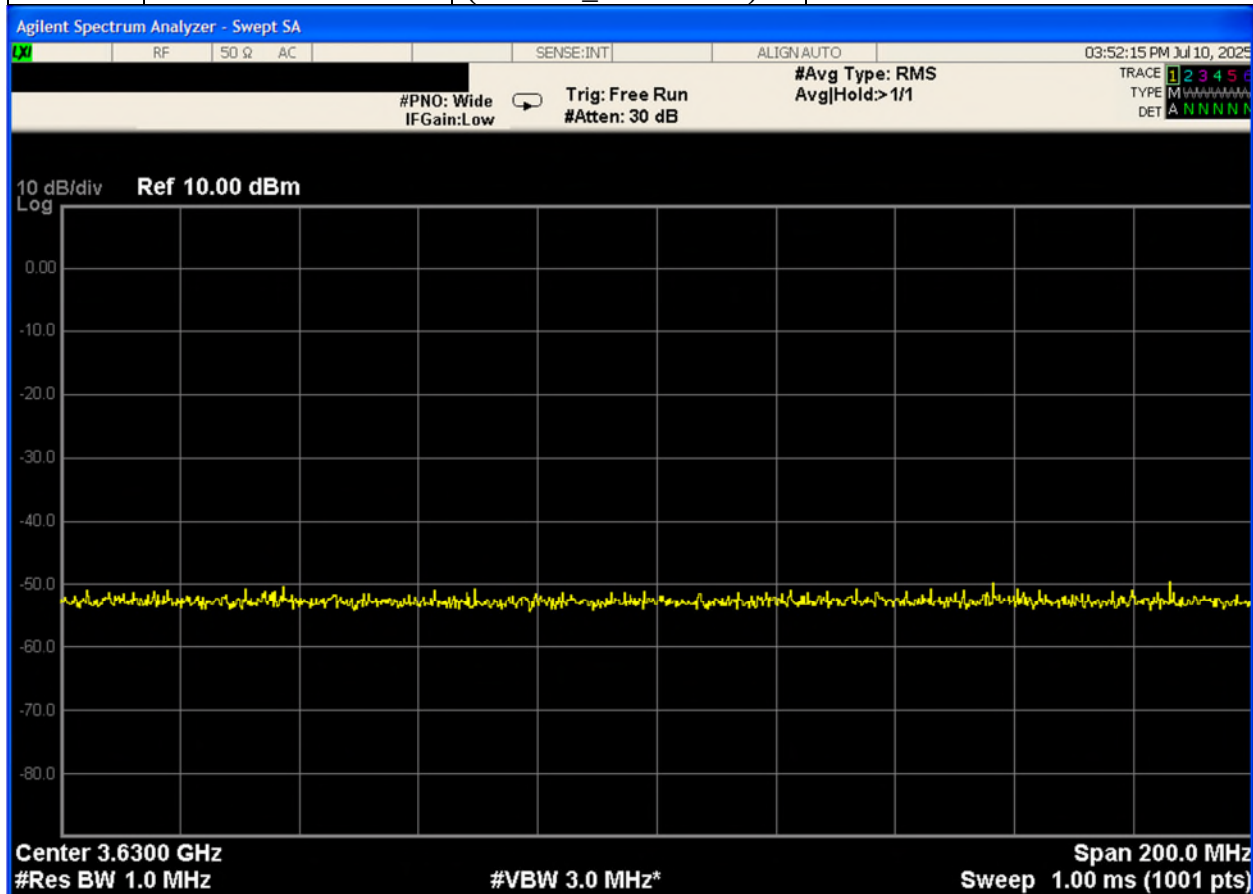


Note response code verified via logs kept on file.

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

C.GRA.2

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



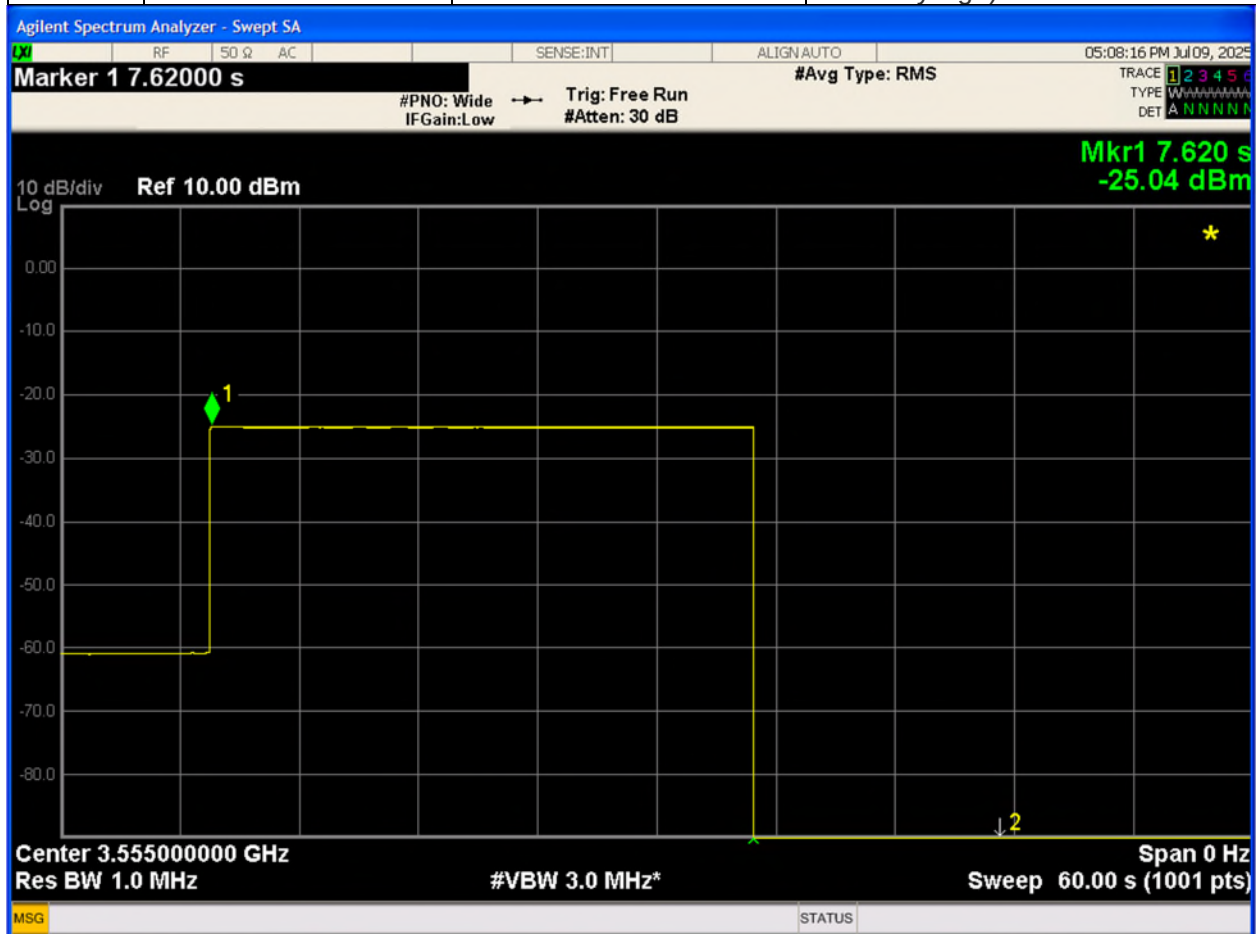
Note response code verified via logs kept on file.

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Heartbeat

D.HBT.2

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: - 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
-----------	------------------	--	---	---

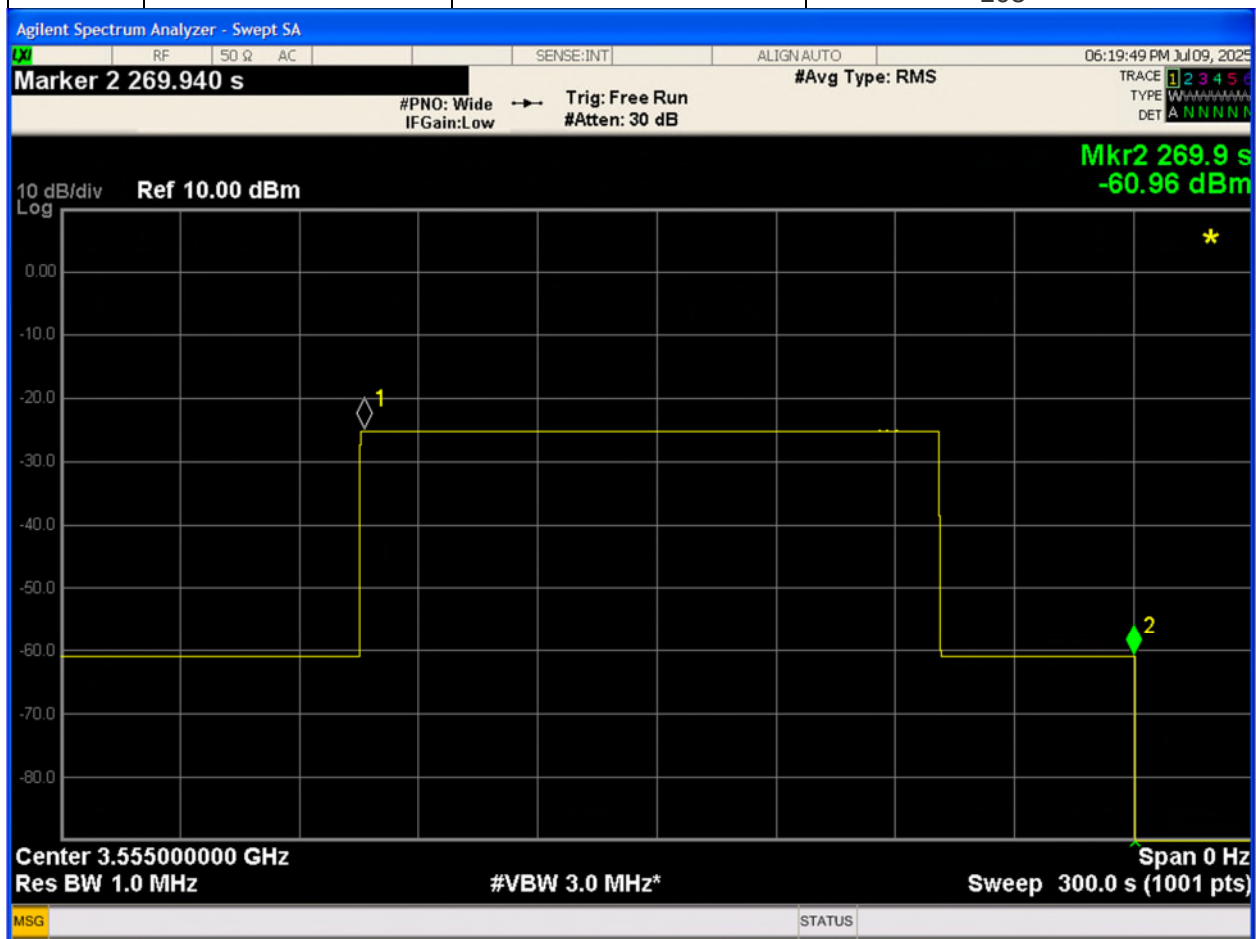


Test Harness logs and timing on graph was verified, the EUT passed the requirement.

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

C.HBT.3

6.4.4.2.1	WINNF.FT.C.HBT.3	Heartbeat responseCode=105 (DEREGISTER)	Monitor RF transmission. Ensure that: CBSD stops transmission within 60 seconds of the heartbeatResponse which contains responseCode = 105	P
-----------	------------------	---	--	---

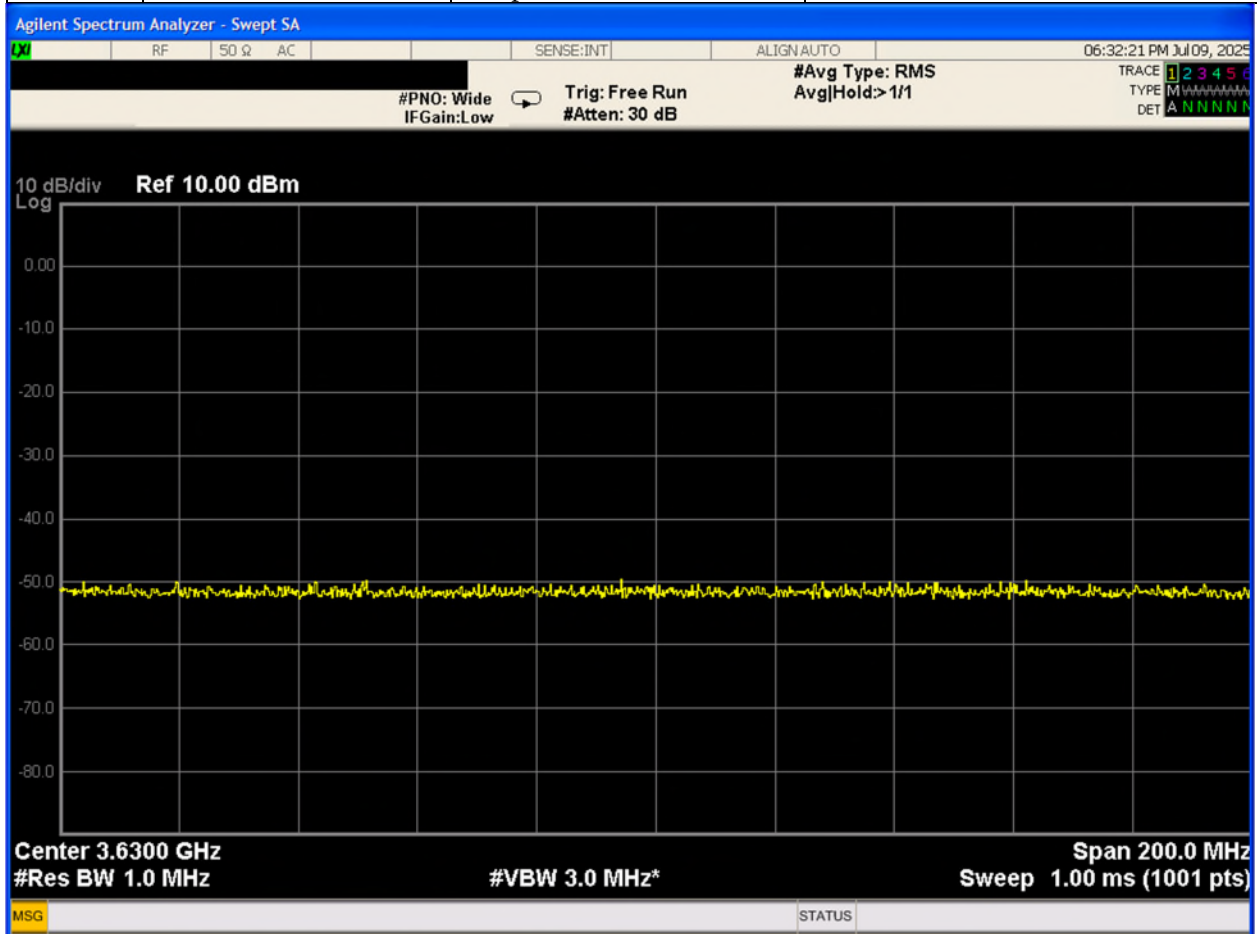


Test Harness logs and timing on graph was verified, the EUT passed the requirement.

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

C.HBT.5

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

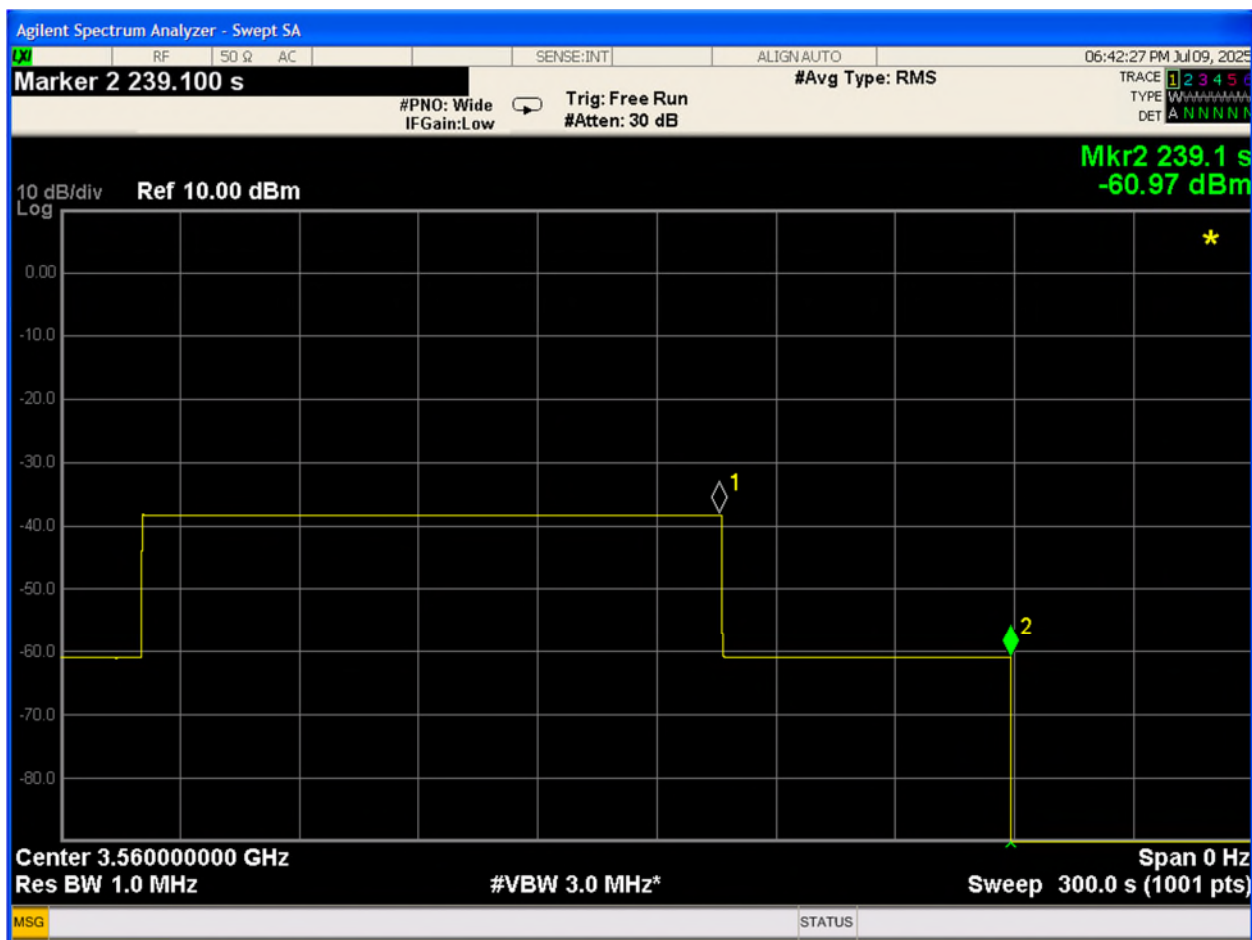


Test Harness logs and timing on graph was verified, the EUT passed the requirement.

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

C.HBT.6

6.4.4.2.4	WINNF.FT.C.HBT.6	Heartbeat responseCode=501 (SUSPENDED_GRANT) in Subsequent Heartbeat Response	Monitor RF transmission. Ensure: CBSD stops transmission within 60 seconds of heartbeatResponse which contains responseCode=501	p
-----------	------------------	---	---	---

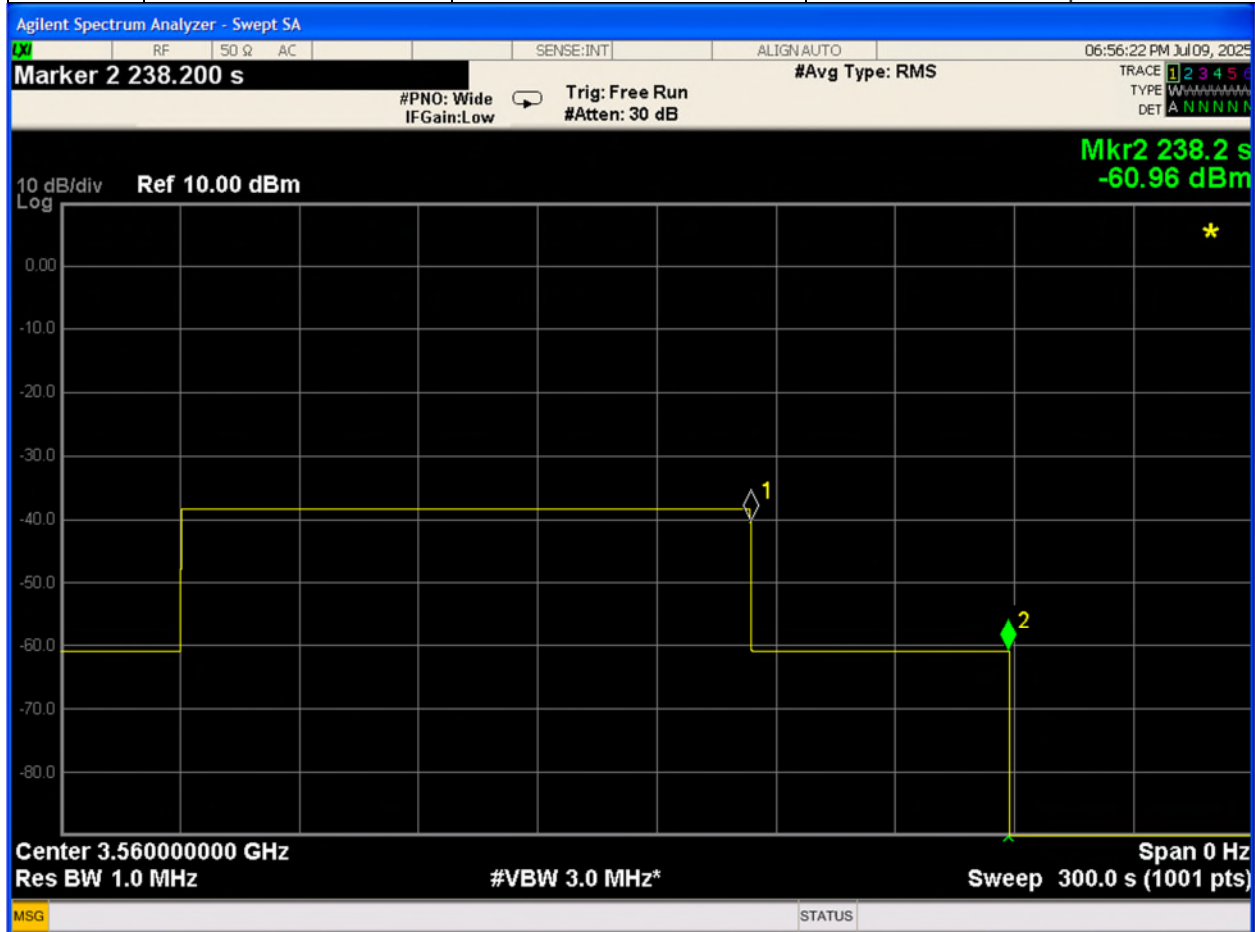


Test Harness logs and timing on graph was verified, the EUT passed the requirement.

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

C.HBT.7

6.4.4.2.5	WINNF.FT.C.HBT.7	Heartbeat responseCode=502 (UNSYNC_OP_PARAM)	Monitor RF transmission. Ensure: CBSD stops transmission within 60 seconds of heartbeatResponse which contains responseCode=502	p
-----------	------------------	--	---	---

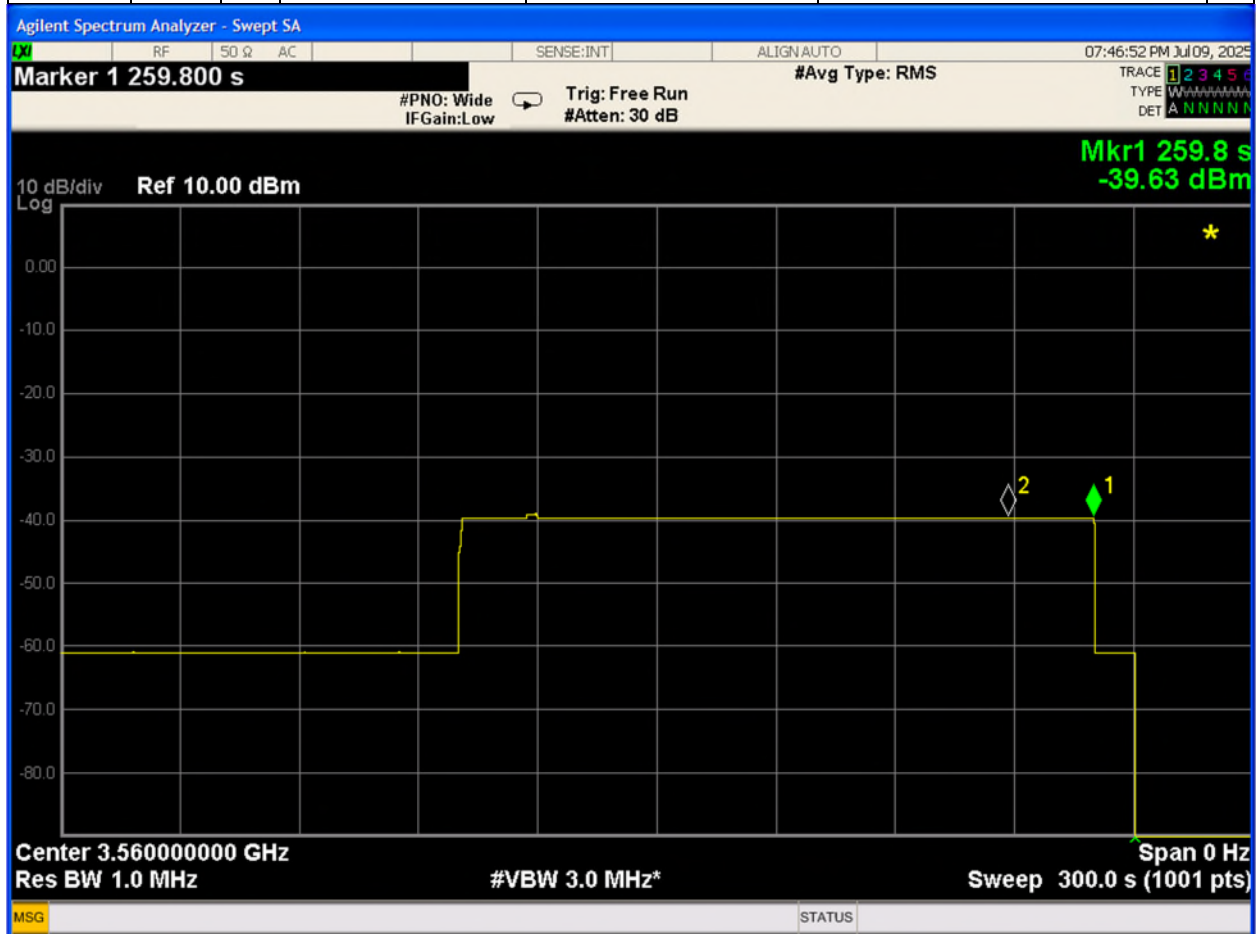


Test Harness logs and timing on graph was verified, the EUT passed the requirement.

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

D.HBT.8

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: • 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
-----------	----	---	-------------------	--	---	---

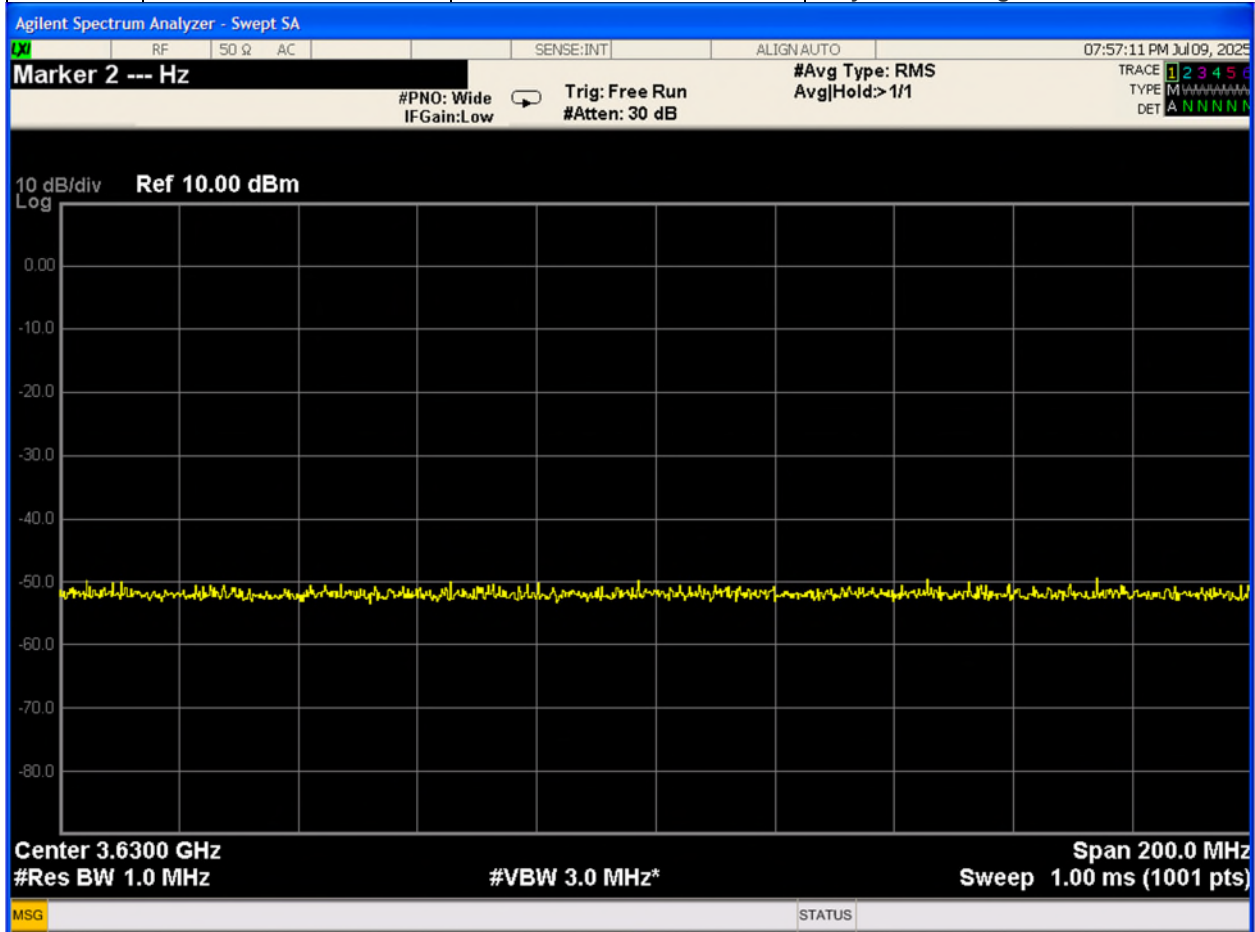


Test Harness logs and timing on graph was verified, the EUT passed the requirement.

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

C.HBT.9

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

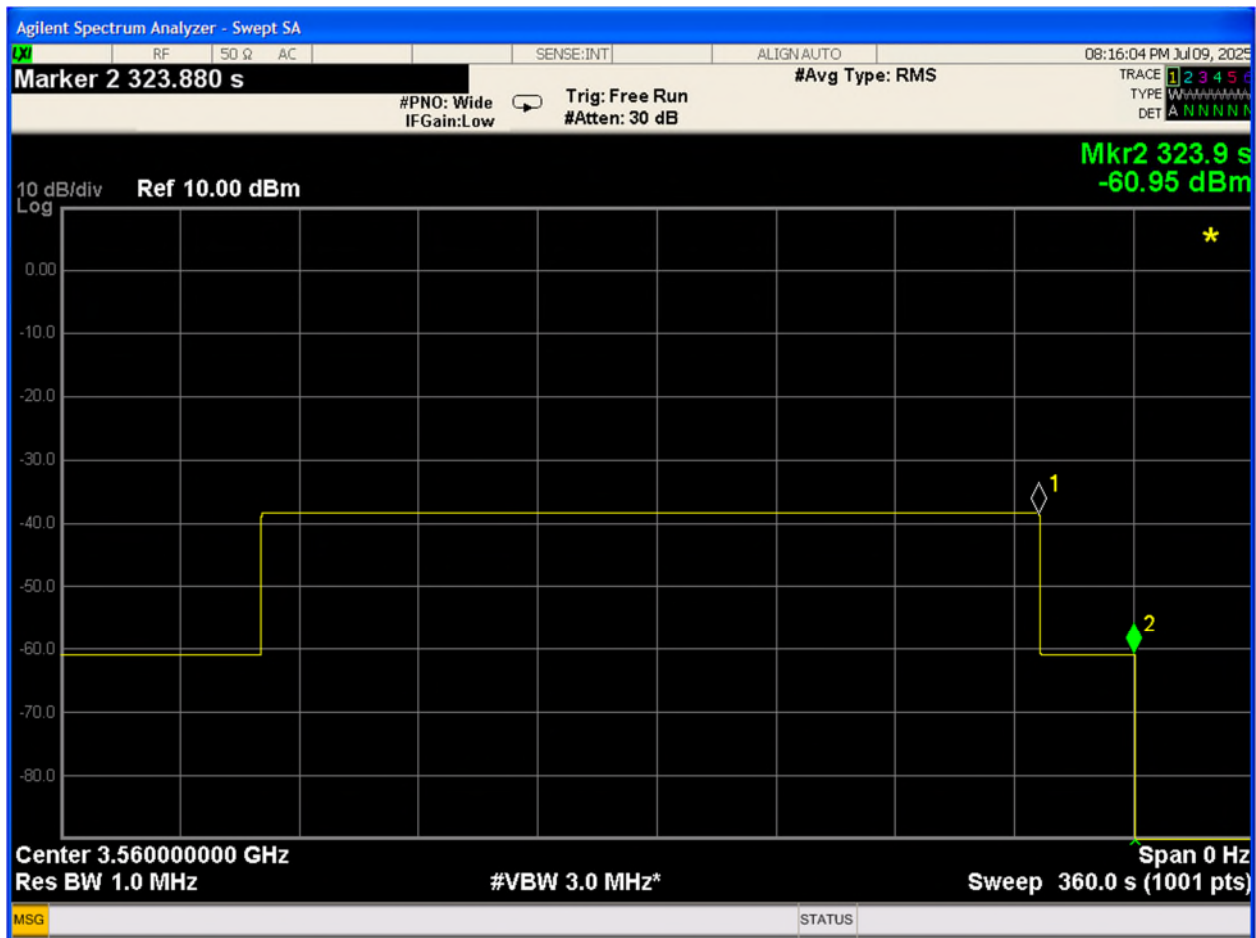


Test Harness logs and timing on graph was verified, the EUT passed the requirement.

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

C.HBT.10

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



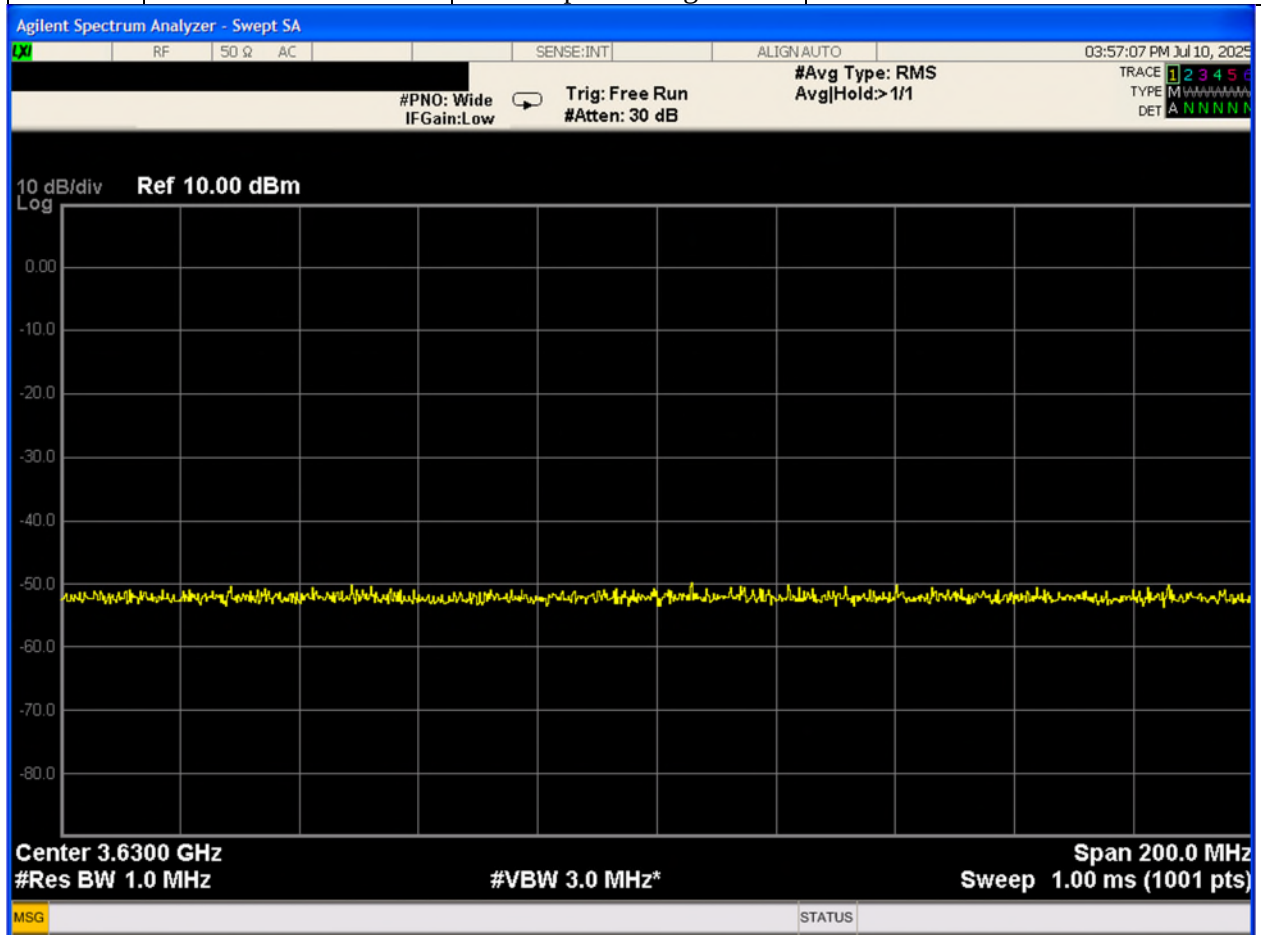
Test Harness logs and timing on graph was verified, the EUT passed the requirement.

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Measurement

D.MES.2

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

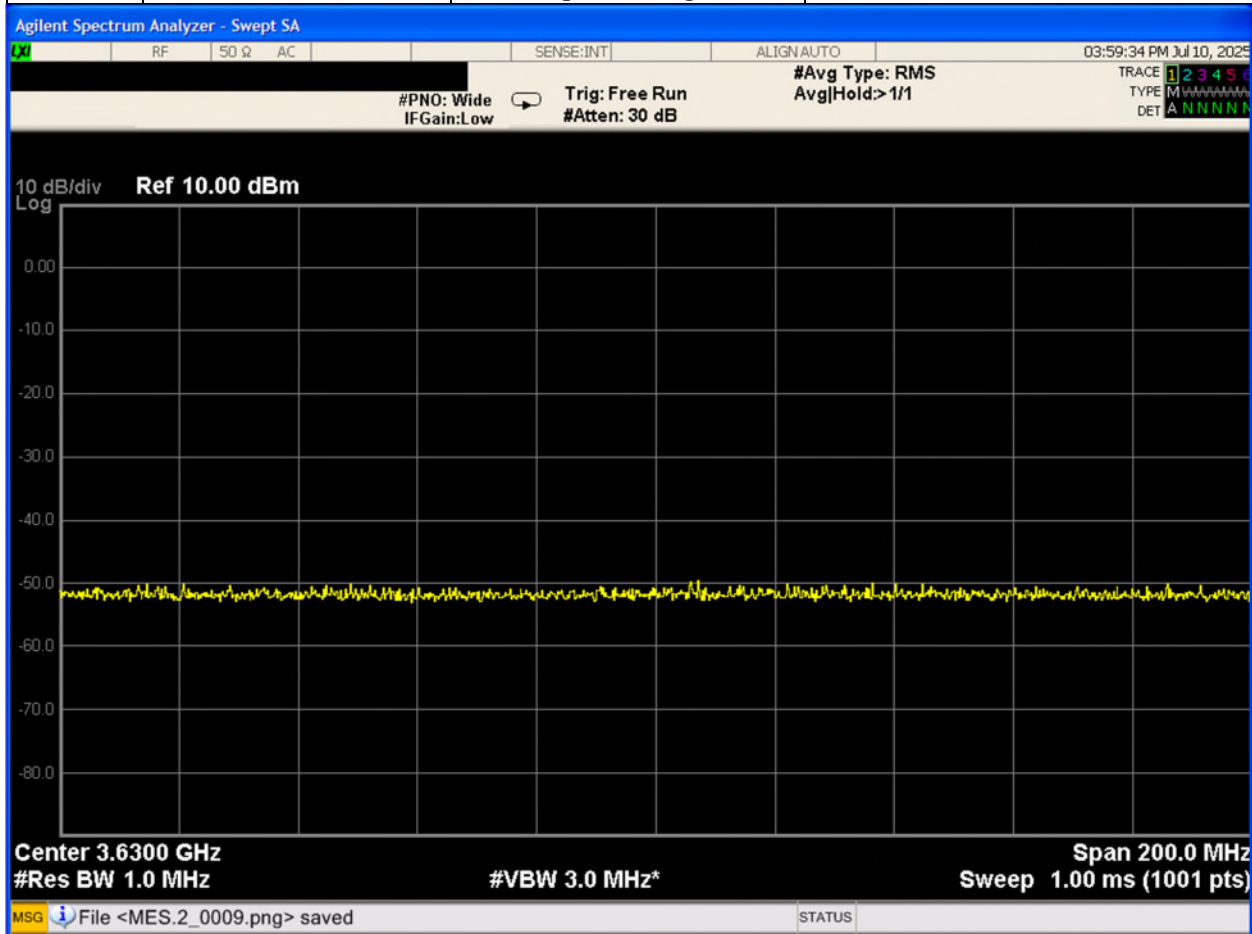


Pass. “measreportconfig” in logs. All other requirements verified.

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

C.MES.3

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

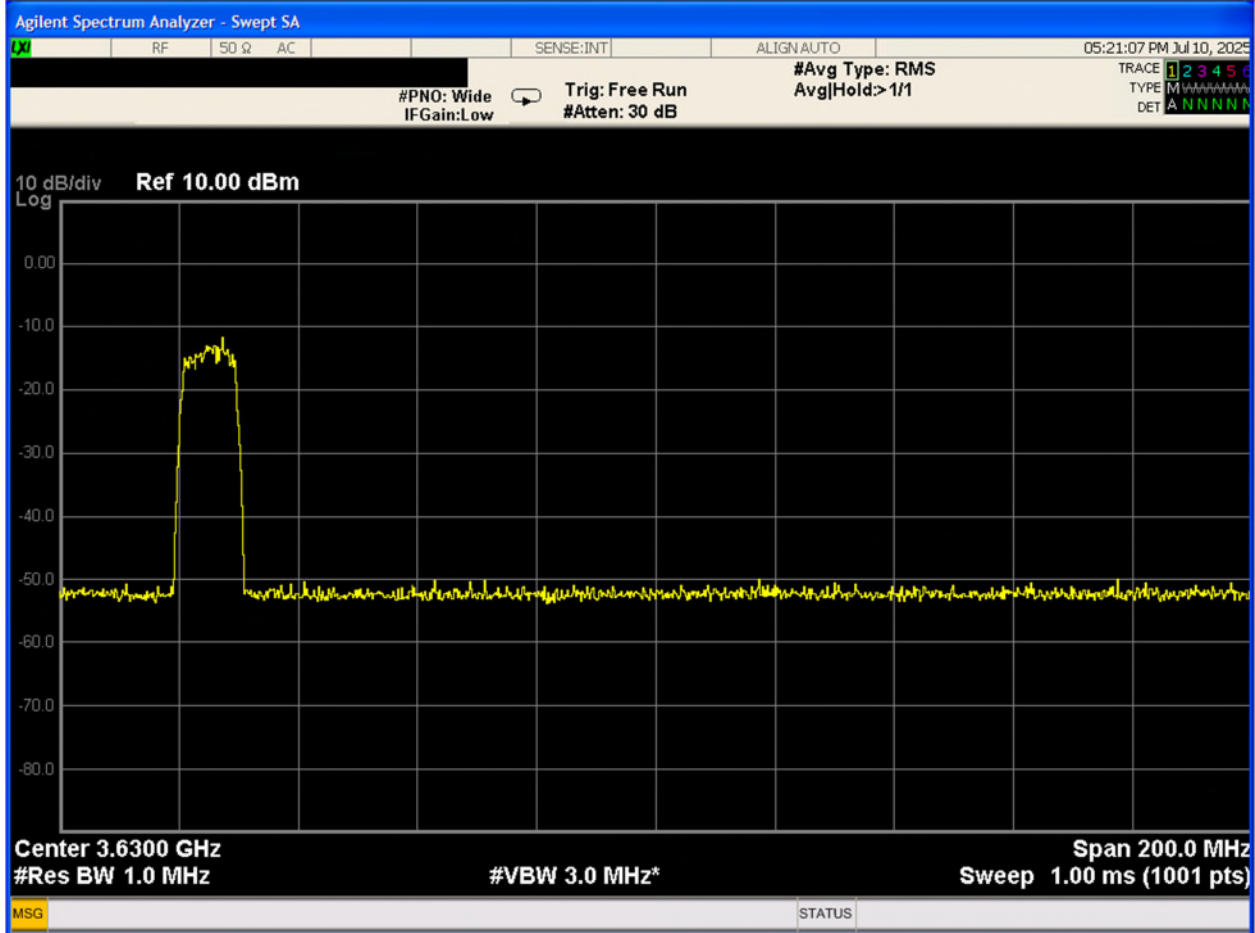


Pass. “measreportconfig” in logs. All other requirements verified.

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

D.MES.5

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



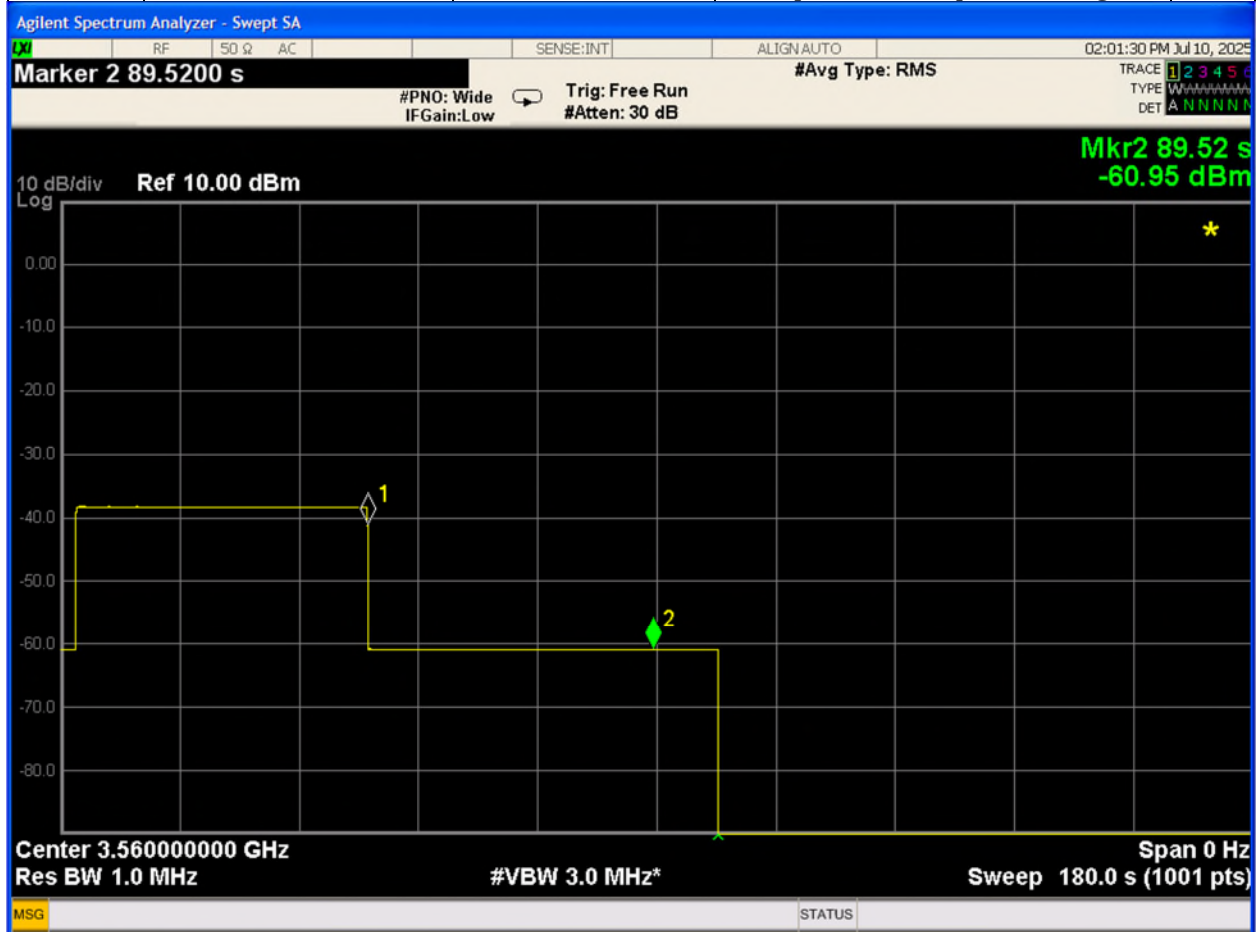
Pass. “measreportconfig” in logs. All other requirements verified.

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Relinquishment and Deregistration

D.RLQ.2

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



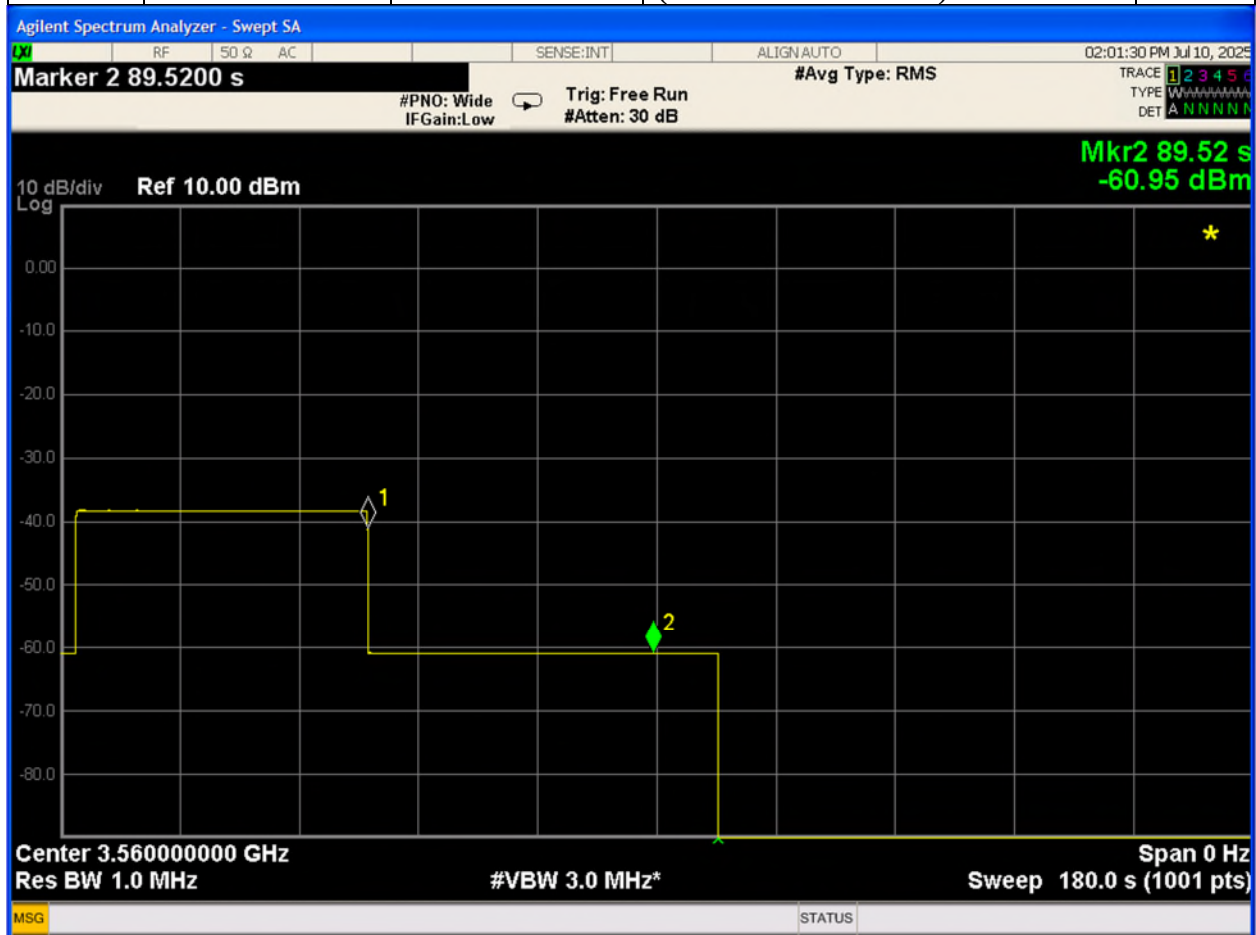
Test Harness logs and timing on graph was verified, the EUT passed the requirement.

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

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

D.DRG.2

6.7.4.1.2	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
-----------	----------------------	--	--	---



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 and video analysis

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Power Measurement

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

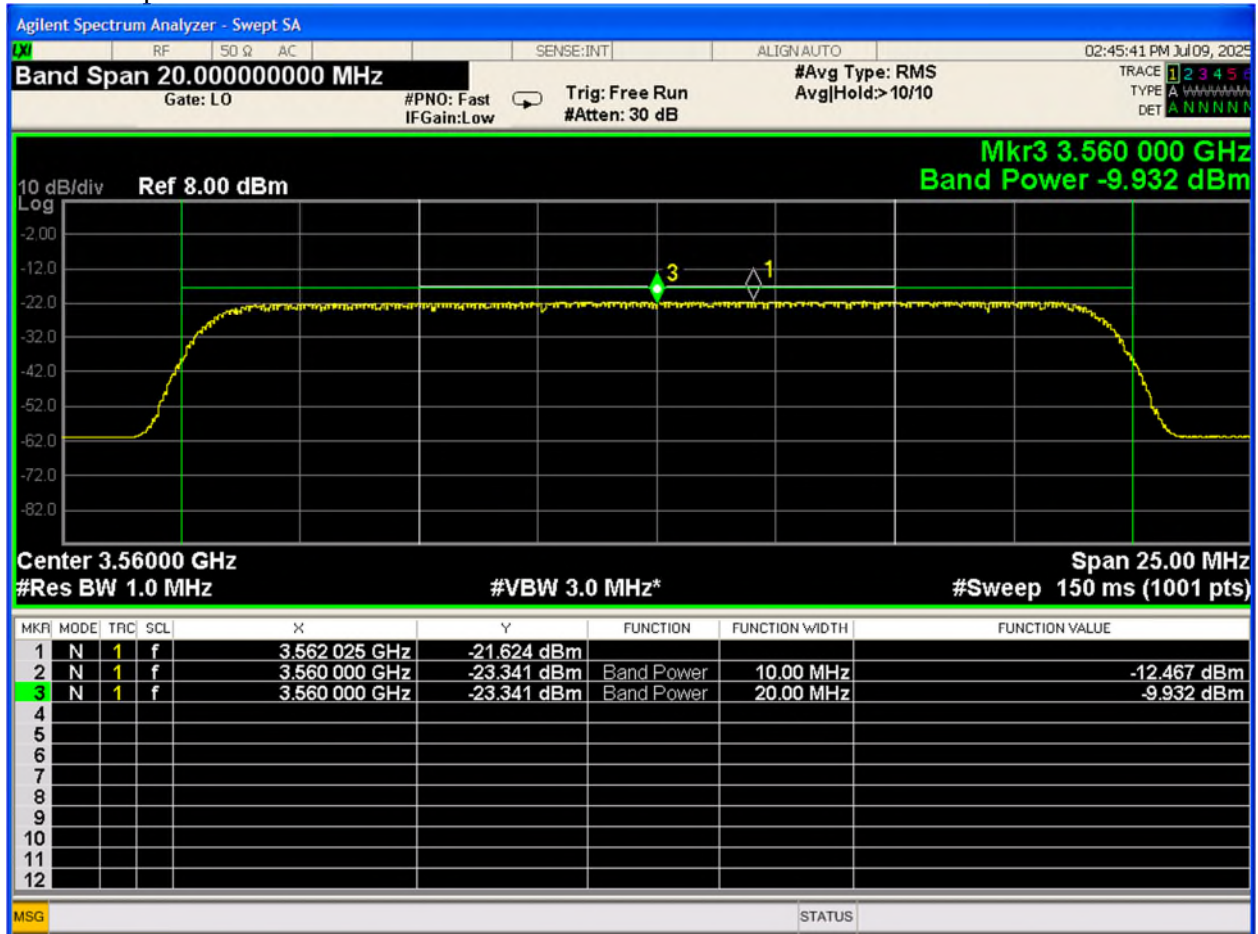
Test Table

	10MHz EIRP limit (target)	1MHz EIRP limit (target)	Raw Power	Raw	Raw	External Losses	Conducted			EIRP (Total)	EIRP 10 MHz	EIRP 1 MHz	Margin TUV SUD
Freq	dBm	dBm	dBm	dBm/10 MHz	dBm/1 MHz	(dB)	dBm/MHz	Antenna gain dBi	Port gain (dB)	dBm	dBm	dBm/MHz	
3560	44	34	-9.9	-12.4	-21.6	31.7	10.21	11	12.04	44.84	42.34	33.14	0.86
3560	47	37	-6.8	-9.4	-18.6	31.7	13.31	11	12.04	47.94	45.34	36.14	0.86
3630	44	34	-9.3	-11.9	-21.5	31.7	10.87	11	12.04	45.44	42.84	33.24	0.76
3630	47	37	-6.3	-8.9	-18.3	31.7	13.72	11	12.04	48.44	45.84	36.44	0.56
3690	44	34	-9.5	-12.1	-20.9	31.7	10.67	11	12.04	45.24	42.64	33.84	0.16
3690	47	37	-6.6	-9.2	-18	31.7	13.5	11	12.04	48.14	45.54	36.74	0.26

Note: 16 ports = $10\log(16)$ dB port gain = 12.04 dB

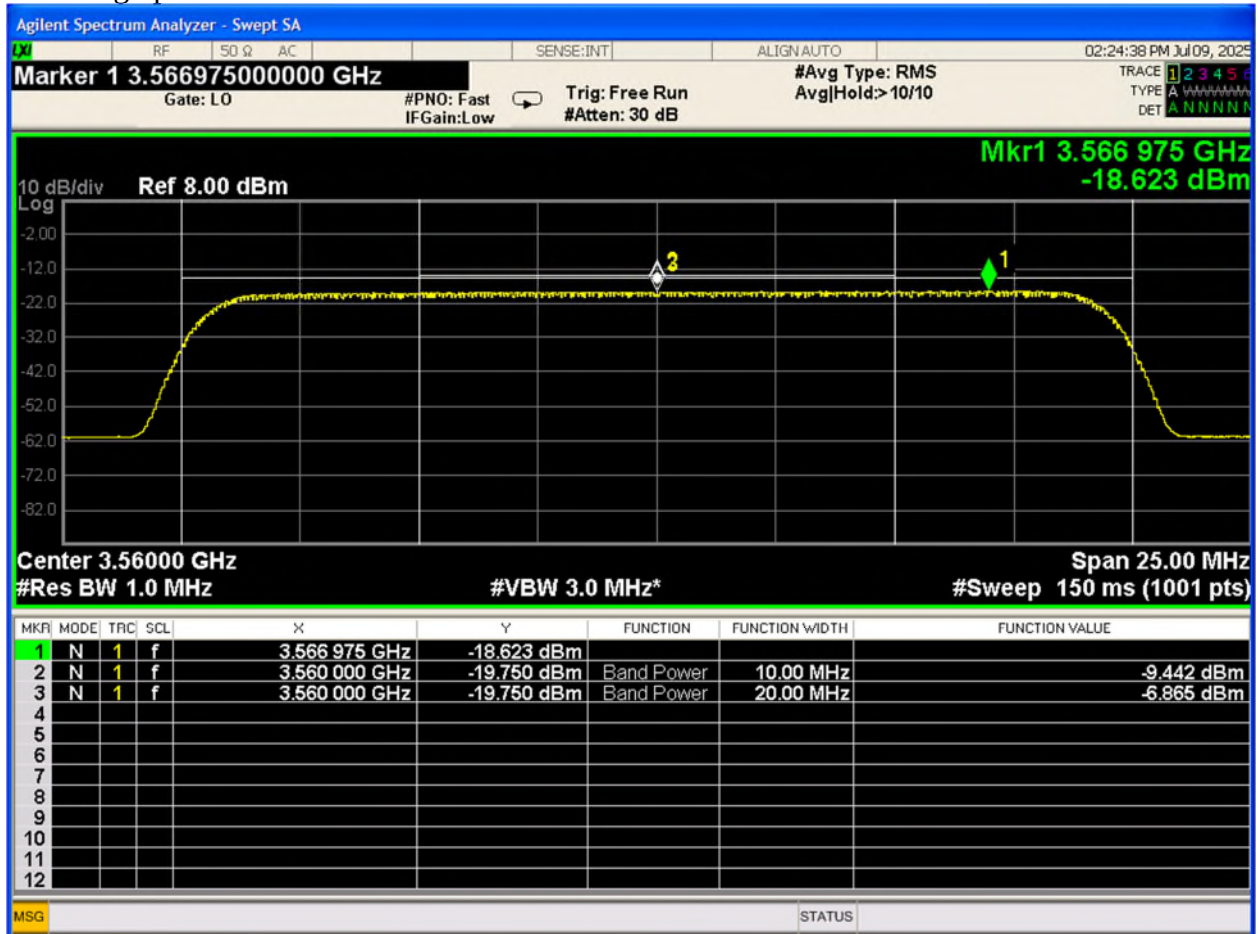
Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

3560 low power



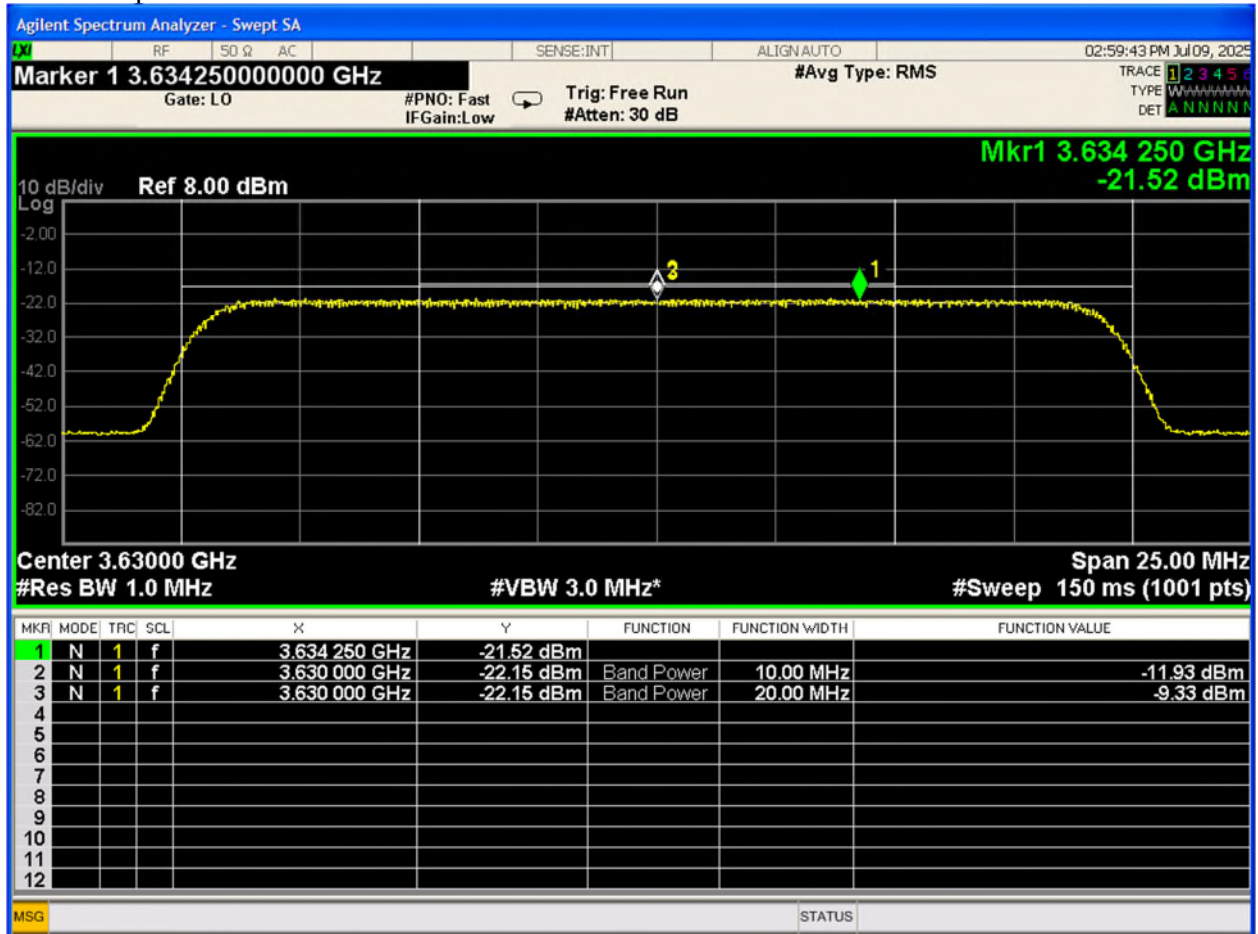
Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

3560-High power



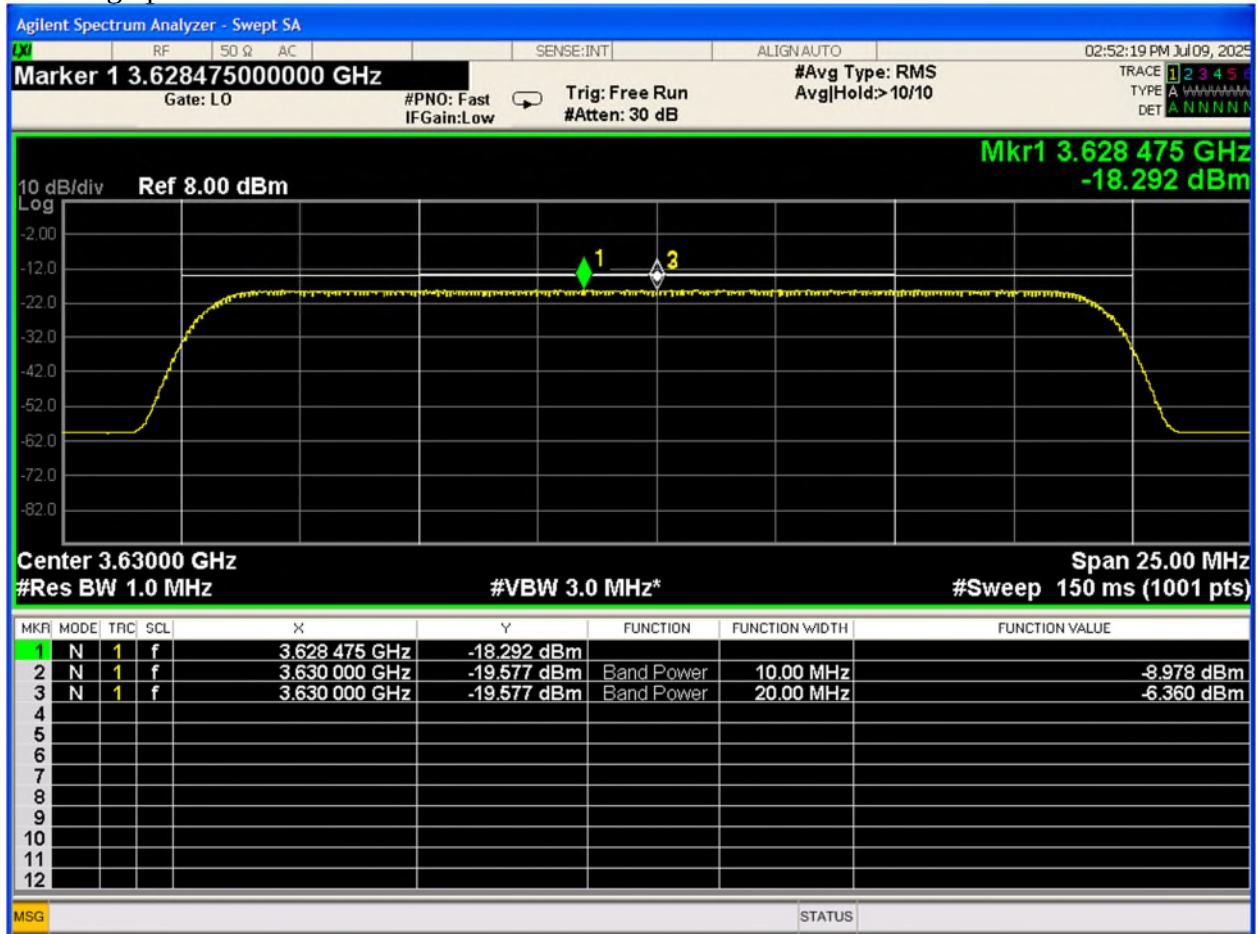
Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

3630 low power



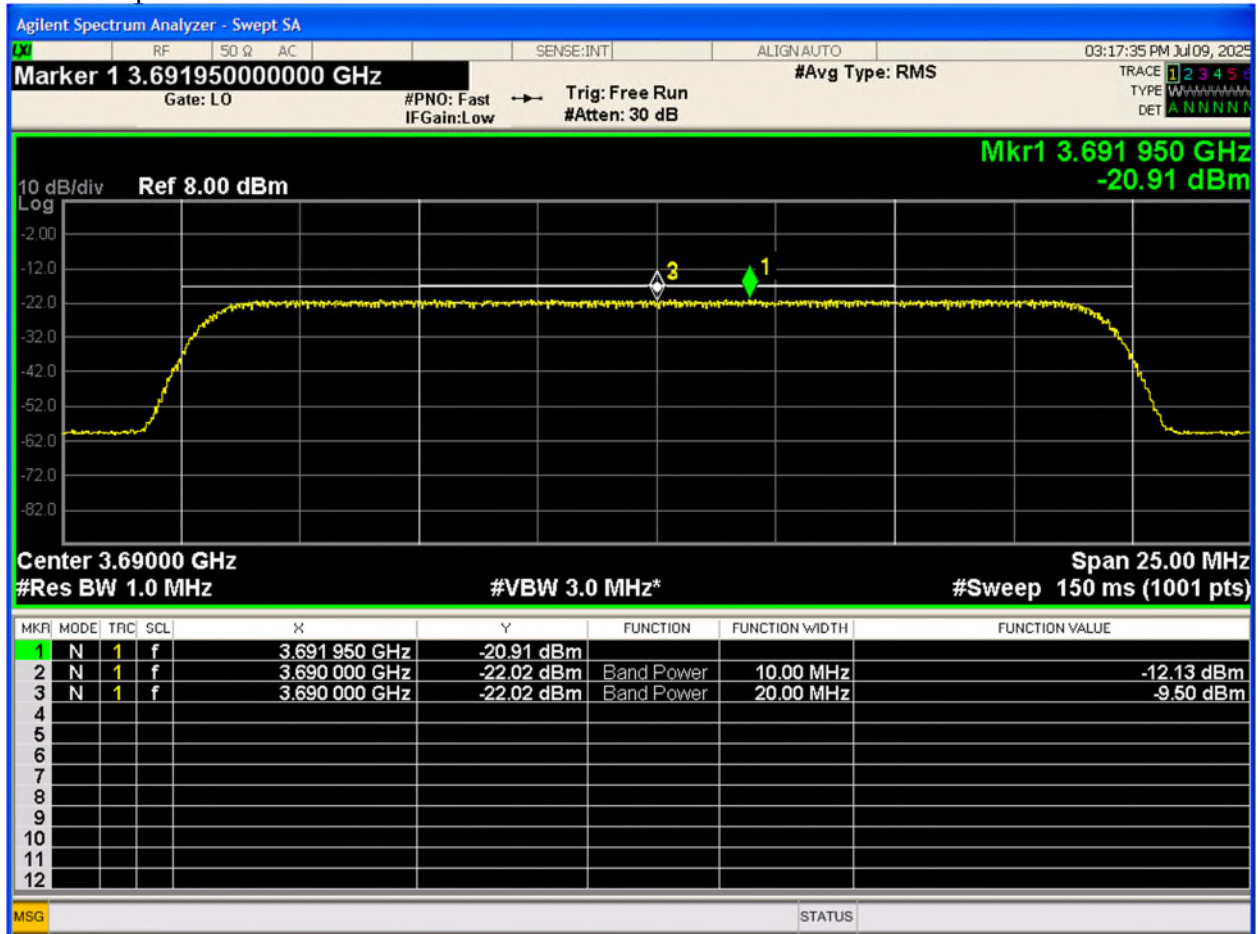
Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

3630-high power



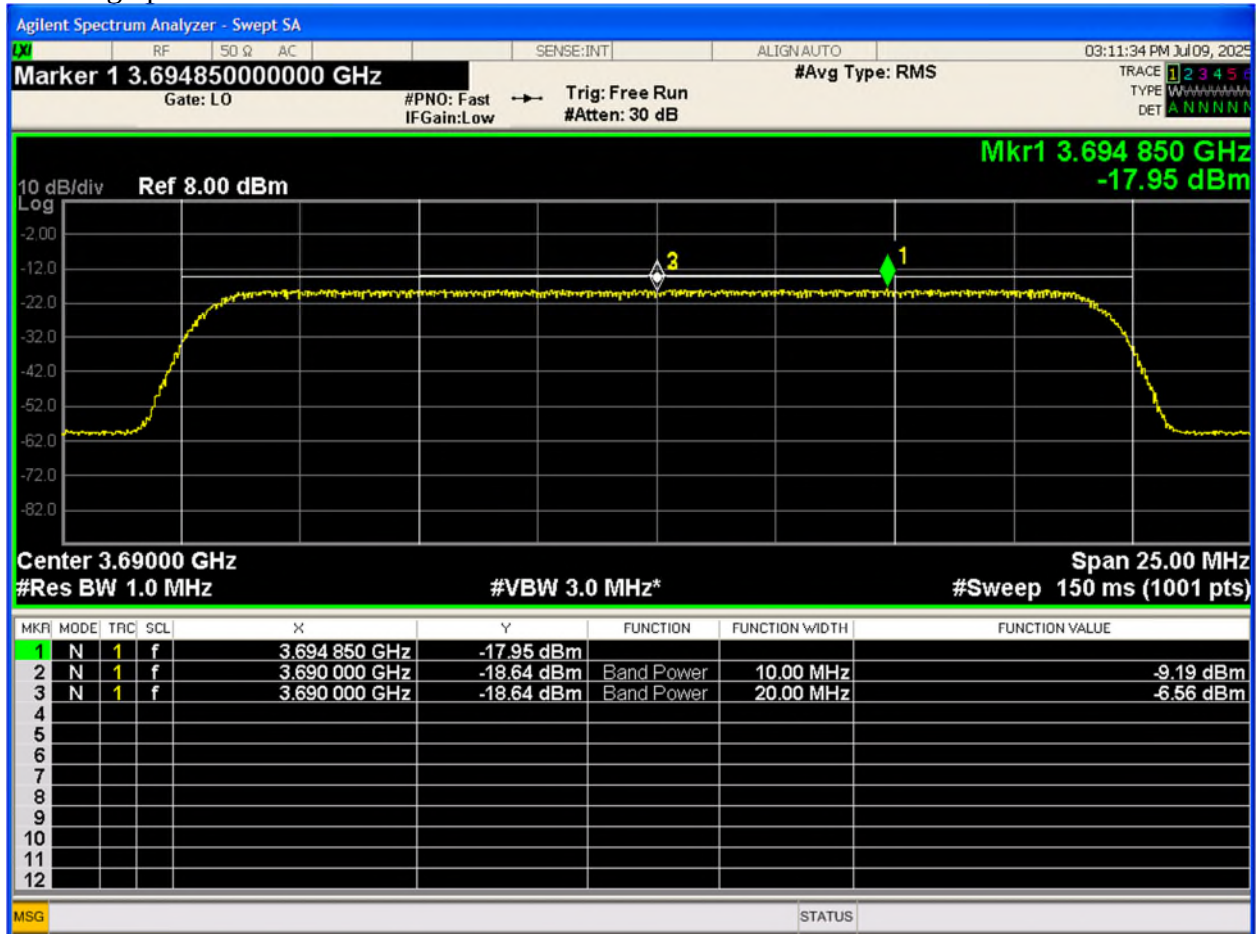
Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

3690 low power



Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

3690-high power

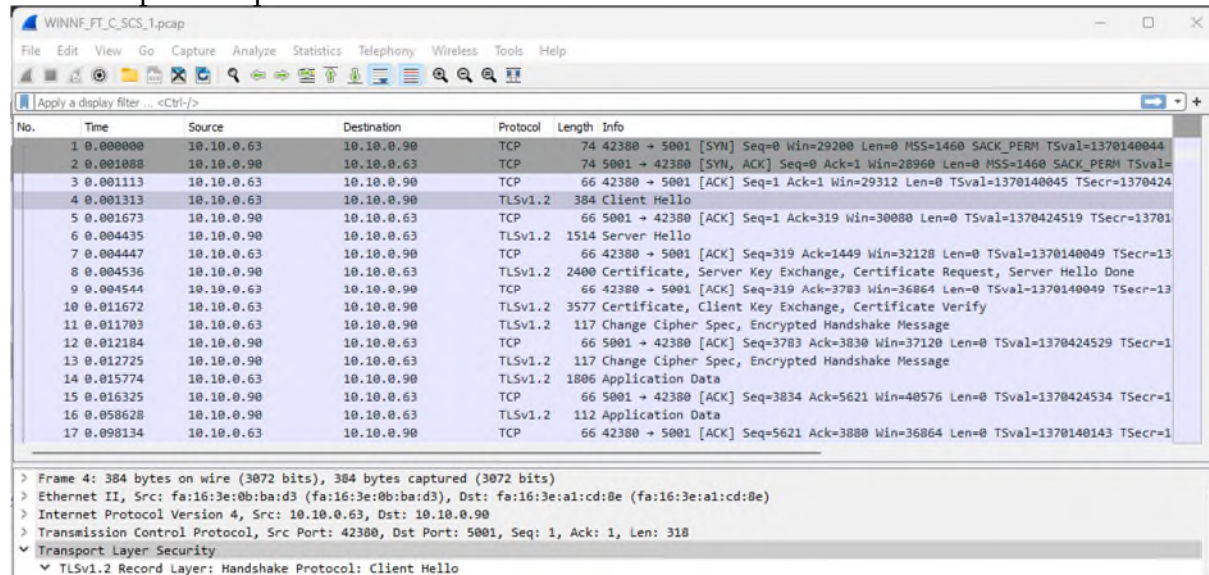


Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

WINNF Security Test Case Analysis

WINNF.FT.C.SCS.1

Packet Capture Sequence



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.0.63	10.10.0.90	TCP	74	42380 → 5001 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=1370140044
2	0.001088	10.10.0.90	10.10.0.63	TCP	74	5001 → 42380 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=
3	0.001113	10.10.0.63	10.10.0.90	TCP	66	42380 → 5001 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1370140045 TSecr=1370424
4	0.001313	10.10.0.63	10.10.0.90	TLSv1.2	384	Client Hello
5	0.001673	10.10.0.90	10.10.0.63	TCP	66	5001 → 42380 [ACK] Seq=1 Ack=319 Win=30080 Len=0 TSval=1370424519 TSecr=13701
6	0.004435	10.10.0.90	10.10.0.63	TLSv1.2	1514	Server Hello
7	0.004447	10.10.0.63	10.10.0.90	TCP	66	42380 → 5001 [ACK] Seq=319 Ack=1449 Win=32128 Len=0 TSval=1370140049 TSecr=13
8	0.004536	10.10.0.90	10.10.0.63	TLSv1.2	2400	Certificate, Server Key Exchange, Certificate Request, Server Hello Done
9	0.004544	10.10.0.63	10.10.0.90	TCP	66	42380 → 5001 [ACK] Seq=319 Ack=3783 Win=36864 Len=0 TSval=1370140049 TSecr=13
10	0.011672	10.10.0.63	10.10.0.90	TLSv1.2	3577	Certificate, Client Key Exchange, Certificate Verify
11	0.011703	10.10.0.63	10.10.0.90	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
12	0.012184	10.10.0.90	10.10.0.63	TCP	66	5001 → 42380 [ACK] Seq=3783 Ack=3830 Win=37120 Len=0 TSval=1370424529 TSecr=1
13	0.012725	10.10.0.90	10.10.0.63	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
14	0.015774	10.10.0.63	10.10.0.90	TLSv1.2	1806	Application Data
15	0.016325	10.10.0.90	10.10.0.63	TCP	66	5001 → 42380 [ACK] Seq=3834 Ack=5621 Win=40576 Len=0 TSval=1370424534 TSecr=1
16	0.058628	10.10.0.90	10.10.0.63	TLSv1.2	112	Application Data
17	0.098134	10.10.0.63	10.10.0.90	TCP	66	42380 → 5001 [ACK] Seq=5621 Ack=3880 Win=36864 Len=0 TSval=1370140143 TSecr=1

> Frame 4: 384 bytes on wire (3072 bits), 384 bytes captured (3072 bits)
 > Ethernet II, Src: fa:16:3e:0b:ba:d3 (fa:16:3e:0b:ba:d3), Dst: fa:16:3e:a1:cd:8e (fa:16:3e:a1:cd:8e)
 > Internet Protocol Version 4, Src: 10.10.0.63, Dst: 10.10.0.90
 > Transmission Control Protocol, Src Port: 42380, Dst Port: 5001, Seq: 1, Ack: 1, Len: 318
 > Transport Layer Security
 ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello

WINNF test requirements:

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

2	- Make sure that Mutual authentication happens between UUT and the SAS Test Harness. - Make sure that UUT uses TLS v1.2 - Make sure that cipher suites from one of the following is selected, - TLS_RSA_WITH_AES_128_GCM_SHA256 - TLS_RSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	PASS

Analysis of WINNF Test Requirements

1. From Client Hello: TLS version = TLS 1.2

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

```

> Frame 4: 384 bytes on wire (3072 bits), 384 bytes captured (3072 bits)
> Ethernet II, Src: fa:16:3e:0b:ba:d3 (fa:16:3e:0b:ba:d3), Dst: fa:16:3e:a1:cd:8e (fa:16:3e:a1:cd:8e)
> Internet Protocol Version 4, Src: 10.10.0.63, Dst: 10.10.0.90
> Transmission Control Protocol, Src Port: 42380, 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)
      ▼ Random: 5588b214f4bd771f8523729b1fad5b3ca54c98191173a281b71dfd29d96b623b
        GMT Unix Time: Jun 22, 2015 21:10:44.000000000 Eastern Daylight Time
        Random Bytes: f4bd771f8523729b1fad5b3ca54c98191173a281b71dfd29d96b623b
      Session ID Length: 32
      Session ID: 2b73f510971e87c02c649bfd4619a48be58cf72c8f7e0f3b76df067b2665d757
      Cipher Suites Length: 86
      ▼ 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)

```

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

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

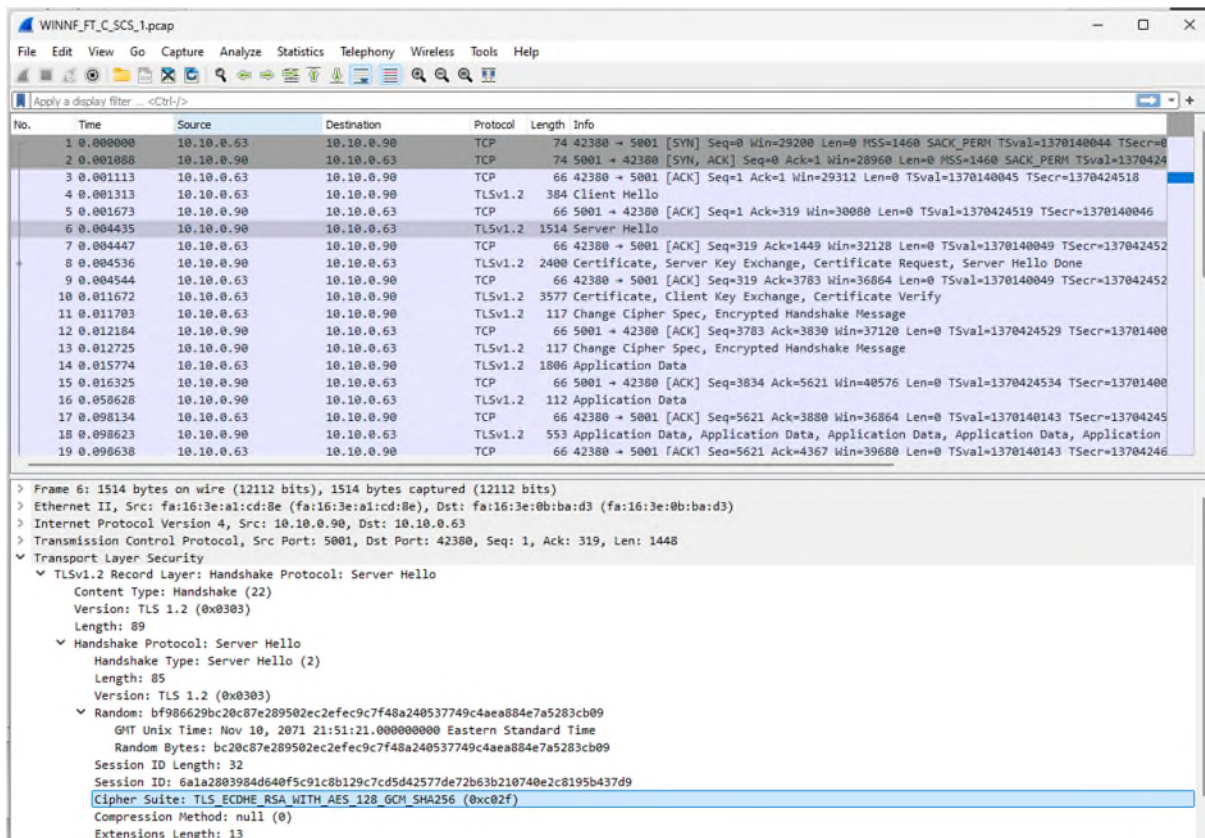
```

> Frame 4: 384 bytes on wire (3072 bits), 384 bytes captured (3072 bits)
> Ethernet II, Src: fa:16:3e:0b:ba:d3 (fa:16:3e:0b:ba:d3), Dst: fa:16:3e:a1:cd:8e (fa:16:3e:a1:cd:8e)
> Internet Protocol Version 4, Src: 10.10.0.63, Dst: 10.10.0.90
> Transmission Control Protocol, Src Port: 42380, 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)
  ▼ Random: 5588b214f4bd771f8523729b1fad5b3ca54c98191173a281b71dfd29d96b623b
    GMT Unix Time: Jun 22, 2015 21:10:44.000000000 Eastern Daylight Time
    Random Bytes: f4bd771f8523729b1fad5b3ca54c98191173a281b71dfd29d96b623b
    Session ID Length: 32
    Session ID: 2b73f510971e87c02c649bfd4619a48be58cf72c8f7e0f3b76df067b2665d757
    Cipher Suites Length: 86
  ▼ 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 (0xc009f)
    Cipher Suite: TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (0xc00a3)
    Cipher Suite: TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0xc009e)
    Cipher Suite: TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (0xc00a2)
    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 (0xc006b)
    Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (0xc006a)
    Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0xc0067)
    Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (0xc0040)
    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 (0xc000a)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc0014)
    Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc0009)
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc0013)
    Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0xc0039)
    Cipher Suite: TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0xc0038)
    Cipher Suite: TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0xc0033)
    Cipher Suite: TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0xc0032)
    Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA (0xc0005)
    Cipher Suite: TLS_ECDH_RSA_WITH_AES_256_CBC_SHA (0xc000f)
    Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA (0xc0004)
    Cipher Suite: TLS_ECDH_RSA_WITH_AES_128_CBC_SHA (0xc000e)
    Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0xc009d)
    Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0xc009c)
    Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA256 (0xc003d)
    Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA256 (0xc003c)
    Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0xc0035)
    Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0xc002f)
    Cipher Suite: TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0xc00ff)

```

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

3. Cipher suite chosen (from Server Hello):
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.0.63	10.10.0.90	TCP	74	42380 → 5001 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=1370140044 TSecr=0
2	0.001058	10.10.0.90	10.10.0.63	TCP	74	5001 → 42380 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=1370424529 TSecr=1370140044
3	0.001113	10.10.0.63	10.10.0.90	TCP	66	42380 → 5001 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1370140045 TSecr=1370424518
4	0.001313	10.10.0.63	10.10.0.90	TLSv1.2	384	Client Hello
5	0.001673	10.10.0.90	10.10.0.63	TCP	66	5001 → 42380 [ACK] Seq=1 Ack=319 Win=30080 Len=0 TSval=1370424519 TSecr=1370140046
6	0.004435	10.10.0.90	10.10.0.63	TLSv1.2	1514	Server Hello
7	0.004447	10.10.0.63	10.10.0.90	TCP	66	42380 → 5001 [ACK] Seq=319 Ack=1449 Win=32128 Len=0 TSval=1370140049 TSecr=137042452
8	0.004536	10.10.0.90	10.10.0.63	TLSv1.2	2400	Certificate, Server Key Exchange, Certificate Request, Server Hello Done
9	0.004544	10.10.0.63	10.10.0.90	TCP	66	42380 → 5001 [ACK] Seq=319 Ack=3783 Win=36864 Len=0 TSval=1370140049 TSecr=137042452
10	0.011672	10.10.0.63	10.10.0.90	TLSv1.2	3577	Certificate, Client Key Exchange, Certificate Verify
11	0.011703	10.10.0.63	10.10.0.90	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
12	0.012184	10.10.0.90	10.10.0.63	TCP	66	5001 → 42380 [ACK] Seq=3783 Ack=3830 Win=37120 Len=0 TSval=1370424529 TSecr=13701400
13	0.012725	10.10.0.90	10.10.0.63	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
14	0.015774	10.10.0.63	10.10.0.90	TLSv1.2	1806	Application Data
15	0.016325	10.10.0.90	10.10.0.63	TCP	66	5001 → 42380 [ACK] Seq=3834 Ack=5621 Win=40576 Len=0 TSval=1370424534 TSecr=13701400
16	0.050628	10.10.0.90	10.10.0.63	TLSv1.2	112	Application Data
17	0.091134	10.10.0.63	10.10.0.90	TCP	66	42380 → 5001 [ACK] Seq=5621 Ack=3880 Win=36864 Len=0 TSval=1370140143 TSecr=13704245
18	0.098623	10.10.0.90	10.10.0.63	TLSv1.2	553	Application Data, Application Data, Application Data, Application Data, Application
19	0.098638	10.10.0.63	10.10.0.90	TCP	66	42380 → 5001 [ACK] Seq=5621 Ack=4367 Win=39680 Len=0 TSval=1370140143 TSecr=13704246

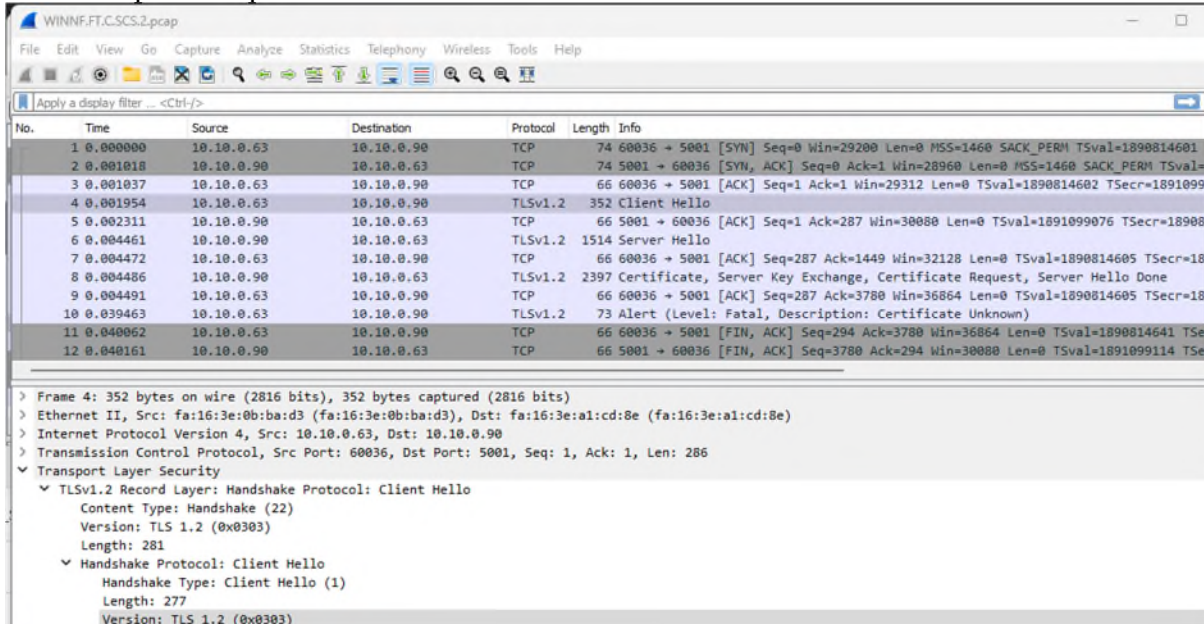
> Frame 6: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
 > Ethernet II, Src: fa:16:3e:a1:cd:8e (fa:16:3e:a1:cd:8e), Dst: fa:16:3e:0b:ba:d3 (fa:16:3e:0b:ba:d3)
 > Internet Protocol Version 4, Src: 10.10.0.90, Dst: 10.10.0.63
 > Transmission Control Protocol, Src Port: 5001, Dst Port: 42380, Seq: 1, Ack: 319, Len: 1448
 > Transport Layer Security
 > TLSv1.2 Record Layer: Handshake Protocol: Server Hello
 Content Type: Handshake (22)
 Version: TLS 1.2 (0x0303)
 Length: 89
 > Handshake Protocol: Server Hello
 Handshake Type: Server Hello (2)
 Length: 85
 Version: TLS 1.2 (0x0303)
 > Random: bf986629bc20c87e289502ec2efec9c7f48a240537749c4aea884e7a5283cb09
 GMT Unix Time: Nov 10, 2071 21:51:21.000000000 Eastern Standard Time
 Random Bytes: bc20c87e289502ec2efec9c7f48a240537749c4aea884e7a5283cb09
 Session ID Length: 32
 Session ID: 6a1a2803984d640f5c91c0b129c7cd5d42577de72b63b210740e2c8195b437d9
 Cipher Suite: **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)**
 Compression Method: null (0)
 Extensions Length: 13

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

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

WINNF.FT.C.SCS.2

Packet Capture Sequence



The image shows a Wireshark packet capture sequence for the file WINNF.FT.C.SCS.2.pcap. The interface displays a list of 12 packets. Packet 4 is selected, showing details for the Transport Layer Security (TLS) handshake. The details pane shows the following information:

- Frame 4: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits)
- Ethernet II, Src: fa:16:3e:0b:ba:d3 (fa:16:3e:0b:ba:d3), Dst: fa:16:3e:a1:cd:8e (fa:16:3e:a1:cd:8e)
- Internet Protocol Version 4, Src: 10.10.0.63, Dst: 10.10.0.90
- Transmission Control Protocol, Src Port: 60036, 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)

WINNF Test

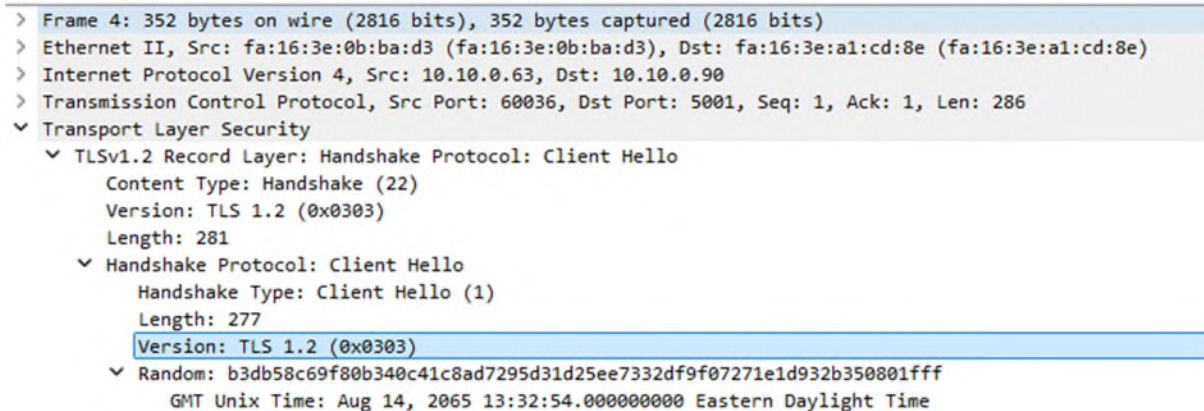
Requirements:

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

2	- Make sure that UUT uses TLS v1.2 for security establishment. - Make sure UUT selects the correct cipher suite. - UUT shall use CRL or OCSP to verify the validity of the server certificate. - Make sure that Mutual authentication does not happen between UUT and the SAS Test Harness.	PASS	FAIL
---	--	------	------

Analysis of WINNF Test Requirements

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



The image shows a Wireshark packet capture sequence for the file WINNF.FT.C.SCS.2.pcap. The interface displays a list of 12 packets. Packet 4 is selected, showing details for the Transport Layer Security (TLS) handshake. The details pane shows the following information:

- Frame 4: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits)
- Ethernet II, Src: fa:16:3e:0b:ba:d3 (fa:16:3e:0b:ba:d3), Dst: fa:16:3e:a1:cd:8e (fa:16:3e:a1:cd:8e)
- Internet Protocol Version 4, Src: 10.10.0.63, Dst: 10.10.0.90
- Transmission Control Protocol, Src Port: 60036, 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)

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

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

TLS_RSA_WITH_AES_128_GCM_SHA25

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (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:0b:ba:d3 (fa:16:3e:0b:ba:d3), Dst: fa:16:3e:a1:cd:8e (fa:16:3e:a1:cd:8e)
> Internet Protocol Version 4, Src: 10.10.0.63, Dst: 10.10.0.90
> Transmission Control Protocol, Src Port: 60036, 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: b3db58c69f80b340c41c8ad7295d31d25ee7332df9f07271e1d932b350801fff

GMT Unix Time: Aug 14, 2065 13:32:54.000000000 Eastern Daylight Time

Random Bytes: 9f80b340c41c8ad7295d31d25ee7332df9f07271e1d932b350801fff

Session ID Length: 0

Cipher Suites Length: 86

▼ 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)

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)

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

3. From Server Hello, cipher suite chosen:

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

```
> Frame 6: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
> Ethernet II, Src: fa:16:3e:a1:cd:8e (fa:16:3e:a1:cd:8e), Dst: fa:16:3e:0b:ba:d3 (fa:16:3e:0b:ba:d3)
> Internet Protocol Version 4, Src: 10.10.0.90, Dst: 10.10.0.63
> Transmission Control Protocol, Src Port: 5001, Dst Port: 60036, Seq: 1, Ack: 287, Len: 1448
▼ Transport Layer Security
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 89
    ▼ Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 85
      Version: TLS 1.2 (0x0303)
      ▼ Random: 1397b7082563030a13f0a5c6e6ad8c823b8ca88cdcbce75b2e7e4269e199aa72
        GMT Unix Time: Jun 1, 1980 08:18:16.000000000 Eastern Daylight Time
        Random Bytes: 2563030a13f0a5c6e6ad8c823b8ca88cdcbce75b2e7e4269e199aa72
        Session ID Length: 32
        Session ID: 2cb742e2876ee2486cb4e686e4f55a467b20bef18ce60781dc7532ea87611f64
        Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
        Compression Method: null (0)
        Extensions Length: 13
```

4. Read OSCP Request/Response to/from server, CRL used:

```
> Frame 3455: 2498 bytes on wire (19984 bits), 2498 bytes captured (19984 bits)
> Ethernet II, Src: fa:16:3e:0b:ba:d3 (fa:16:3e:0b:ba:d3), Dst: fa:16:3e:17:b4:ac (fa:16:3e:17:b4:ac)
> Internet Protocol Version 4, Src: 10.10.0.124, Dst: 10.10.0.61
> Transmission Control Protocol, Src Port: 8180, Dst Port: 42552, 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
        ✓ toolResponseData
          > 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: 5368021a252947538580c3c3b4c4e5f3896641
                IssuerKeyHash: 506370b6d95142e48404041547e5c8d6e5fdba
                serialNumber: 0a0f048948a78e7f50f
              > certificate: 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: 90f6f08438a1268b0d7e21cf2049842794c7f5ee489ad70b9140a771cfe3e7ec59a0..
            > certs: 1 item
              > Certificate (id-at-commonName=SAS-OCSP-EXAMPLE,id-at-organizationName=Informa SAS OSCP Responder Certi,id-at-organizationName=Test Lab for FCC PART 96,id-at-countryName=US)
                > signedCertificate
                  > algorithmIdentifier (sha256withRSAEncryption)
                    Algorithm ID: 1.2.840.113549.1.1.11 (sha256withRSAEncryption)
                    Padding: 0
                    encrypted: 88a5474077895a0804c353a0cc780ff2a307626cc2494bc12b127f0282a40f8780aee07..
```

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

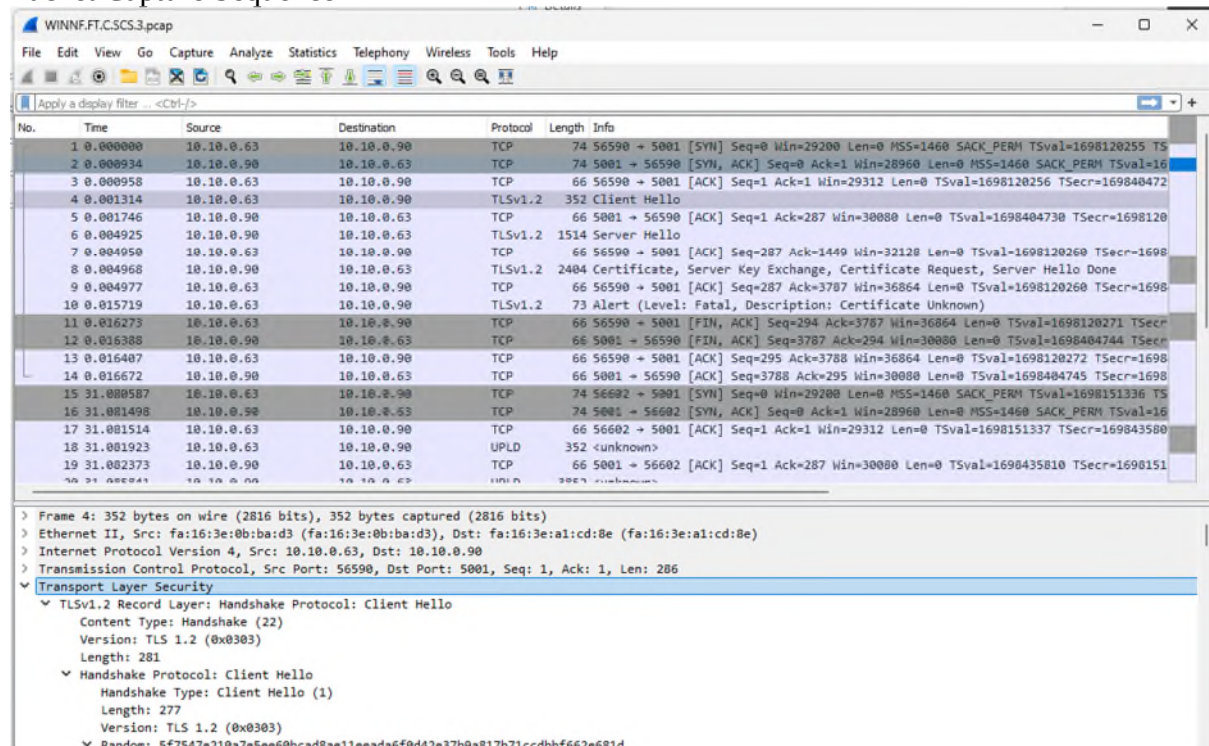
```
> Frame 10: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
> Ethernet II, Src: fa:16:3e:0b:ba:d3 (fa:16:3e:0b:ba:d3), Dst: fa:16:3e:a1:cd:8e (fa:16:3e:a1:cd:8e)
> Internet Protocol Version 4, Src: 10.10.0.63, Dst: 10.10.0.90
> Transmission Control Protocol, Src Port: 60036, Dst Port: 5001, Seq: 287, Ack: 3780, 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
```

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

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

WINNF.FT.C.SCS.3

Packet Capture Sequence



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.0.63	10.10.0.90	TCP	74	56590 → 5001 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=1698120255 TS...
2	0.000934	10.10.0.90	10.10.0.63	TCP	74	5001 → 56590 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=16...
3	0.000958	10.10.0.63	10.10.0.90	TCP	66	56590 → 5001 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1698120256 TSecr=169840472
4	0.001314	10.10.0.63	10.10.0.90	TLSv1.2	352	Client Hello
5	0.001746	10.10.0.90	10.10.0.63	TCP	66	5001 → 56590 [ACK] Seq=1 Ack=287 Win=30080 Len=0 TSval=1698404730 TSecr=1698120
6	0.004925	10.10.0.90	10.10.0.63	TLSv1.2	1514	Server Hello
7	0.004950	10.10.0.63	10.10.0.90	TCP	66	56590 → 5001 [ACK] Seq=287 Ack=1449 Win=32128 Len=0 TSval=1698120260 TSecr=1698
8	0.004968	10.10.0.90	10.10.0.63	TLSv1.2	2404	Certificate, Server Key Exchange, Certificate Request, Server Hello Done
9	0.004977	10.10.0.63	10.10.0.90	TCP	66	56590 → 5001 [ACK] Seq=287 Ack=3707 Win=36864 Len=0 TSval=1698120260 TSecr=1698
10	0.015719	10.10.0.63	10.10.0.90	TLSv1.2	73	Alert (Level: Fatal, Description: Certificate Unknown)
11	0.016273	10.10.0.63	10.10.0.90	TCP	66	56590 → 5001 [FIN, ACK] Seq=294 Ack=3787 Win=36864 Len=0 TSval=1698120271 TSecr
12	0.016388	10.10.0.90	10.10.0.63	TCP	66	5001 → 56590 [FIN, ACK] Seq=3787 Ack=294 Win=30080 Len=0 TSval=1698404744 TSecr
13	0.016407	10.10.0.63	10.10.0.90	TCP	66	56590 → 5001 [ACK] Seq=295 Ack=3788 Win=36864 Len=0 TSval=1698120272 TSecr=1698
14	0.016672	10.10.0.90	10.10.0.63	TCP	66	5001 → 56590 [ACK] Seq=3788 Ack=295 Win=30080 Len=0 TSval=1698404745 TSecr=1698
15	31.000587	10.10.0.63	10.10.0.90	TCP	74	56602 → 5001 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=1698151336 TS...
16	31.001498	10.10.0.90	10.10.0.63	TCP	74	5001 → 56602 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=16...
17	31.001514	10.10.0.63	10.10.0.90	TCP	66	56602 → 5001 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1698151337 TSecr=169843580
18	31.001923	10.10.0.63	10.10.0.90	UPLD	352	<unknown>
19	31.002373	10.10.0.90	10.10.0.63	TCP	66	5001 → 56602 [ACK] Seq=1 Ack=287 Win=30080 Len=0 TSval=1698435810 TSecr=1698151

WINNF Test Requirements:

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

2	- Make sure that UUT uses TLS v1.2 for security establishment. - Make sure UUT selects the correct cipher suite. - UUT shall use CRL or OCSP to verify the validity of the server certificate. - Make sure that Mutual authentication does not happen between UUT and the SAS Test Harness.	PASS
---	--	------

Analysis of WINNF Test Requirements

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

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (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:0b:ba:d3 (fa:16:3e:0b:ba:d3), Dst: fa:16:3e:a1:cd:8e (fa:16:3e:a1:cd:8e)
> Internet Protocol Version 4, Src: 10.10.0.63, Dst: 10.10.0.90
> Transmission Control Protocol, Src Port: 56590, 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: 5f7547e210a7e5ee60bcad8ae11eeada6f0d42e37b9a817b71ccdbbf662e681d
        GMT Unix Time: Sep 30, 2020 23:07:14.000000000 Eastern Daylight Time
        Random Bytes: 10a7e5ee60bcad8ae11eeada6f0d42e37b9a817b71ccdbbf662e681d
        Session ID Length: 0

```

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 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

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: 5f7547e210a7e5ee60bcad8ae11eeada6f0d42e37b9a817b71ccdbbf662e681d

GMT Unix Time: Sep 30, 2020 23:07:14.000000000 Eastern Daylight Time

Random Bytes: 10a7e5ee60bcad8ae11eeada6f0d42e37b9a817b71ccdbbf662e681d

Session ID Length: 0

Cipher Suites Length: 86

▼ 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)

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)

Compression Methods Length: 1

▼ Compression Methods (1 method)

Compression Method: null (0)

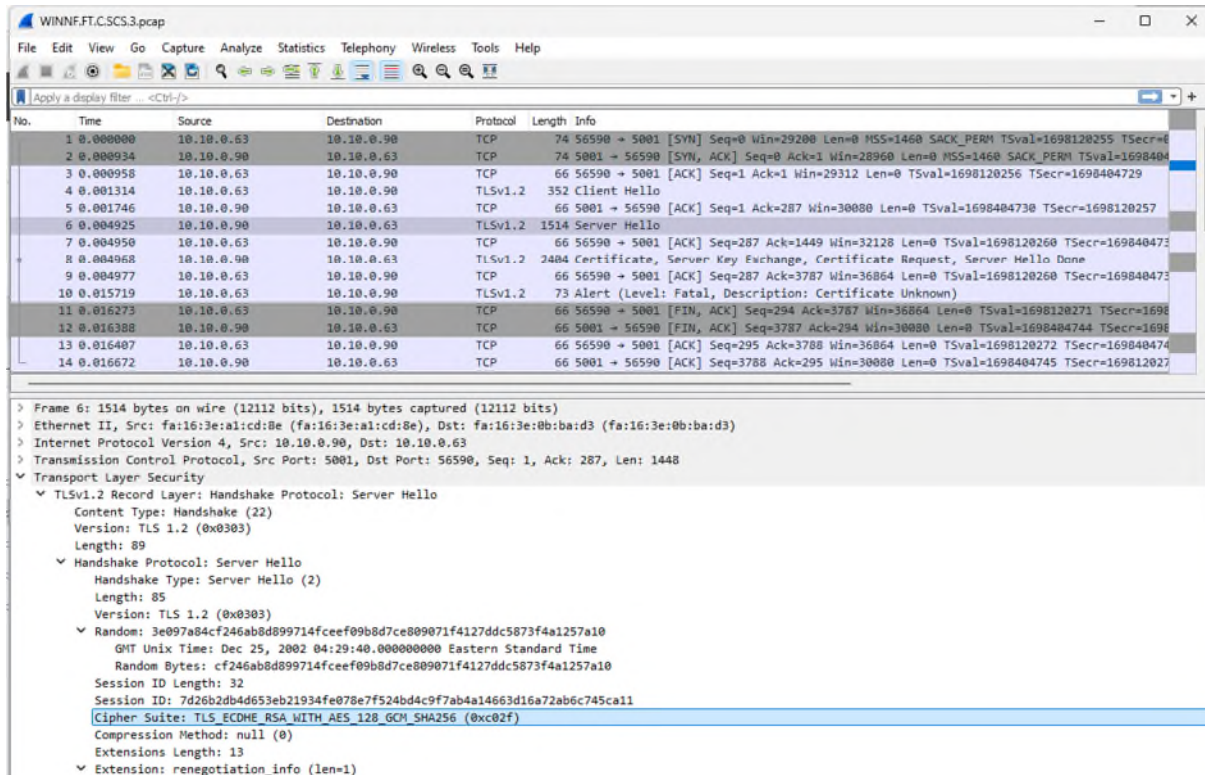
Extensions Length: 150

▼ Extension: server_name (len=15)

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

3. From Server Hello, cipher suite chosen:

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)



Wireshark packet capture showing TLS handshake details. The packet list shows a Server Hello (packet 6) and a TLS Alert (packet 14). The packet details for packet 6 show the Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f).

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

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

WINNF.TC.SCS3.pcap					
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help					
Apply a display filter ... <Ctrl-F>					
No.	Time	Source	Destination	Protocol	Length Info
1	0.000000	10.10.0.63	10.10.0.90	TCP	74 56590 → 5001 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=1698120256
2	0.000934	10.10.0.90	10.10.0.63	TCP	74 5001 → 56590 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=1698120256
3	0.000958	10.10.0.63	10.10.0.90	TCP	66 56590 → 5001 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1698120256
4	0.001314	10.10.0.63	10.10.0.90	TLShv1.2	352 Client Hello
5	0.001746	10.10.0.90	10.10.0.63	TCP	66 5001 → 56590 [ACK] Seq=1 Ack=287 Win=30080 Len=0 TSval=1698404730
6	0.004925	10.10.0.90	10.10.0.63	TLShv1.2	1514 Server Hello
7	0.004950	10.10.0.63	10.10.0.90	TCP	66 56590 → 5001 [ACK] Seq=287 Ack=1449 Win=32128 Len=0 TSval=1698120256
8	0.004968	10.10.0.90	10.10.0.63	TLShv1.2	2404 Certificate, Server Key Exchange, Certificate Request, Server Hello Done
9	0.004977	10.10.0.63	10.10.0.90	TCP	66 56590 → 5001 [ACK] Seq=287 Ack=3787 Win=36864 Len=0 TSval=1698120256
10	0.015719	10.10.0.63	10.10.0.90	TLShv1.2	73 Alert (Level: Fatal, Description: Certificate Unknown)
11	0.016273	10.10.0.63	10.10.0.90	TCP	66 56590 → 5001 [FIN, ACK] Seq=294 Ack=3787 Win=36864 Len=0 TSval=1698120256
12	0.016388	10.10.0.90	10.10.0.63	TCP	66 5001 → 56590 [FIN, ACK] Seq=3787 Ack=294 Win=30080 Len=0 TSval=1698120256
13	0.016407	10.10.0.63	10.10.0.90	TCP	66 56590 → 5001 [ACK] Seq=295 Ack=3788 Win=36864 Len=0 TSval=1698120256
14	0.016672	10.10.0.90	10.10.0.63	TCP	66 5001 → 56590 [ACK] Seq=3788 Ack=295 Win=30080 Len=0 TSval=1698404730

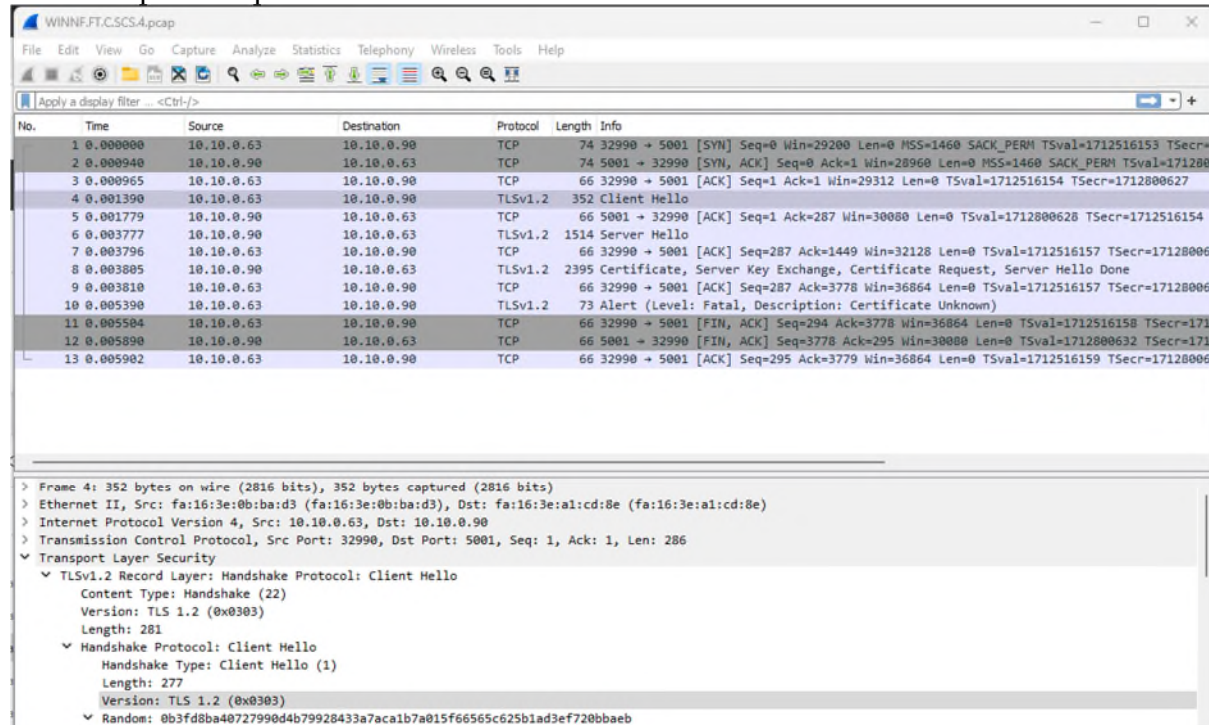
> Frame 10: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
> Ethernet II, Src: fa:16:3e:0b:ba:d3 (fa:16:3e:0b:ba:d3), Dst: fa:16:3e:a1:cd:8e (fa:16:3e:a1:cd:8e)
> Internet Protocol Version 4, Src: 10.10.0.63, Dst: 10.10.0.90
> Transmission Control Protocol, Src Port: 56590, Dst Port: 5001, Seq: 287, Ack: 3787, 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)

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

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

WINNF.FT.C.SCS.4

Packet Capture Sequence



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.0.63	10.10.0.90	TCP	74	32990 → 5001 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=1712516153 TSecr=1712800627
2	0.000940	10.10.0.90	10.10.0.63	TCP	74	5001 → 32990 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM TSval=1712800627 TSecr=1712516153
3	0.000965	10.10.0.63	10.10.0.90	TCP	66	32990 → 5001 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1712516154 TSecr=1712800627
4	0.001390	10.10.0.63	10.10.0.90	TLSv1.2	352	Client Hello
5	0.001779	10.10.0.90	10.10.0.63	TCP	66	5001 → 32990 [ACK] Seq=1 Ack=287 Win=30080 Len=0 TSval=1712800628 TSecr=1712516154
6	0.003777	10.10.0.90	10.10.0.63	TLSv1.2	1514	Server Hello
7	0.003796	10.10.0.63	10.10.0.90	TCP	66	32990 → 5001 [ACK] Seq=287 Ack=1449 Win=32128 Len=0 TSval=1712516157 TSecr=1712800632
8	0.003805	10.10.0.90	10.10.0.63	TLSv1.2	2395	Certificate, Server Key Exchange, Certificate Request, Server Hello Done
9	0.003810	10.10.0.63	10.10.0.90	TCP	66	32990 → 5001 [ACK] Seq=287 Ack=3778 Win=36864 Len=0 TSval=1712516157 TSecr=1712800632
10	0.005390	10.10.0.63	10.10.0.90	TLSv1.2	73	Alert (Level: Fatal, Description: Certificate Unknown)
11	0.005504	10.10.0.63	10.10.0.90	TCP	66	32990 → 5001 [FIN, ACK] Seq=294 Ack=3778 Win=36864 Len=0 TSval=1712516158 TSecr=1712800632
12	0.005890	10.10.0.90	10.10.0.63	TCP	66	5001 → 32990 [FIN, ACK] Seq=3778 Ack=295 Win=30080 Len=0 TSval=1712800632 TSecr=1712516158
13	0.005902	10.10.0.63	10.10.0.90	TCP	66	32990 → 5001 [ACK] Seq=295 Ack=3779 Win=36864 Len=0 TSval=1712516159 TSecr=1712800632

WINNF Test Requirements:

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

2	- Make sure that UUT uses TLS v1.2 for security establishment. - Make sure UUT selects the correct cipher suite. - UUT shall use CRL or OCSP to verify the validity of the server certificate. - Make sure that Mutual authentication does not happen between UUT and the SAS Test Harness.	PASS	FAIL
---	--	------	------

Analysis of WINNF Test Requirements

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

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (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:0b:ba:d3 (fa:16:3e:0b:ba:d3), Dst: fa:16:3e:a1:cd:8e (fa:16:3e:a1:cd:8e)
> Internet Protocol Version 4, Src: 10.10.0.63, Dst: 10.10.0.90
> Transmission Control Protocol, Src Port: 32990, 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: 0b3fd8ba40727990d4b79928433a7aca1b7a015f66565c625b1ad3ef720bbaeb
        GMT Unix Time: Dec 25, 1975 05:00:26.000000000 Eastern Standard Time
        Random Bytes: 40727990d4b79928433a7aca1b7a015f66565c625b1ad3ef720bbaeb
      Session ID Length: 0
      Cipher Suites Length: 86
      ✓ Cipher Suites (43 suites)

```

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 901 258 AIR 1672 B48 B77 (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:0b:ba:d3 (fa:16:3e:0b:ba:d3), Dst: fa:16:3e:a1:cd:8e (fa:16:3e:a1:cd:8e)
> Internet Protocol Version 4, Src: 10.10.0.63, Dst: 10.10.0.90
> Transmission Control Protocol, Src Port: 32990, 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: 0b3fd8ba40727990d4b79928433a7aca1b7a015f66565c625b1ad3ef720bbaeb
        GMT Unix Time: Dec 25, 1975 05:00:26.000000000 Eastern Standard Time
        Random Bytes: 40727990d4b79928433a7aca1b7a015f66565c625b1ad3ef720bbaeb
        Session ID Length: 0
        Cipher Suites Length: 86
        ▼ 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)
          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)

```

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

3. From Server Hello, cipher suite chosen:

Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)

```
> Frame 6: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits)
> Ethernet II, Src: fa:16:3e:a1:cd:8e (fa:16:3e:a1:cd:8e), Dst: fa:16:3e:0b:ba:d3 (fa:16:3e:0b:ba:d3)
> Internet Protocol Version 4, Src: 10.10.0.90, Dst: 10.10.0.63
> Transmission Control Protocol, Src Port: 5001, Dst Port: 32990, Seq: 1, Ack: 287, Len: 1448
▼ Transport Layer Security
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 89
  ▼ Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 85
    Version: TLS 1.2 (0x0303)
  ▼ Random: 895d58c6a1ff84b17b04c4bbfc98cf03501b485090fd26c40092bb870850a8b8
    GMT Unix Time: Jan 11, 2043 08:36:06.000000000 Eastern Standard Time
    Random Bytes: a1ff84b17b04c4bbfc98cf03501b485090fd26c40092bb870850a8b8
    Session ID Length: 32
    Session ID: 7038974fa7bdc2b13ff19ffd6f4b1b6bf5e2850e17f6bead9d1602743078bf17
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
    Compression Method: null (0)
```

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

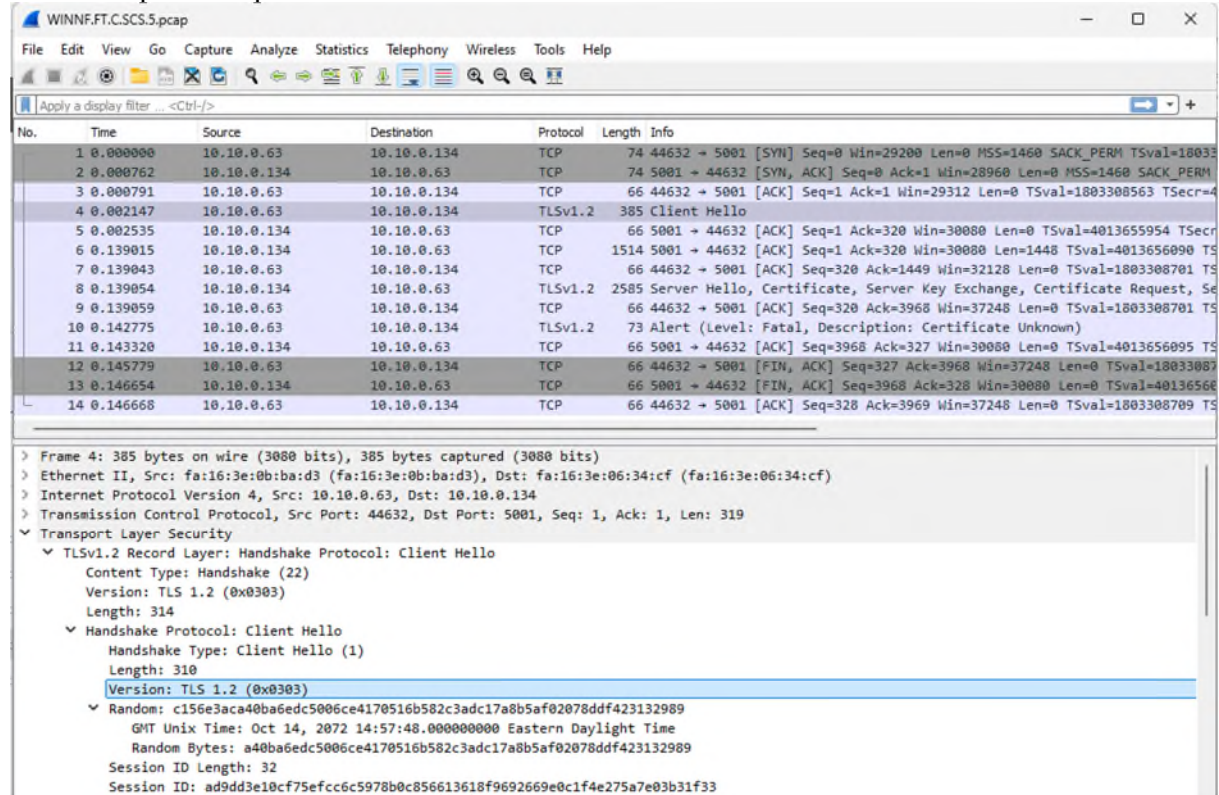
```
> Frame 10: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
> Ethernet II, Src: fa:16:3e:0b:ba:d3 (fa:16:3e:0b:ba:d3), Dst: fa:16:3e:a1:cd:8e (fa:16:3e:a1:cd:8e)
> Internet Protocol Version 4, Src: 10.10.0.63, Dst: 10.10.0.90
> Transmission Control Protocol, Src Port: 32990, Dst Port: 5001, Seq: 287, Ack: 3778, 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 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

WINNF.FT.C.SCS.5

Packet Capture Sequence



WINNF.FT.C.SCS.5.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.0.63	10.10.0.134	TCP	74	44632 → 5001 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval=1803308762
2	0.000762	10.10.0.134	10.10.0.63	TCP	74	5001 → 44632 [SYN, ACK] Seq=0 Ack=1 Win=28960 Len=0 MSS=1460 SACK_PERM
3	0.000791	10.10.0.63	10.10.0.134	TCP	66	44632 → 5001 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=1803308563 TSecr=4
4	0.002147	10.10.0.63	10.10.0.134	TLSv1.2	385	Client Hello
5	0.002535	10.10.0.134	10.10.0.63	TCP	66	5001 → 44632 [ACK] Seq=1 Ack=320 Win=30080 Len=0 TSval=4013655954 TSecr=
6	0.139015	10.10.0.134	10.10.0.63	TCP	1514	5001 → 44632 [ACK] Seq=1 Ack=320 Win=30080 Len=1448 TSval=4013656090 TS
7	0.139043	10.10.0.63	10.10.0.134	TCP	66	44632 → 5001 [ACK] Seq=320 Ack=1449 Win=32128 Len=0 TSval=1803308701 TS
8	0.139054	10.10.0.134	10.10.0.63	TLSv1.2	2585	Server Hello, Certificate, Server Key Exchange, Certificate Request, Se
9	0.139059	10.10.0.63	10.10.0.134	TCP	66	44632 → 5001 [ACK] Seq=320 Ack=3968 Win=37248 Len=0 TSval=1803308701 TS
10	0.142775	10.10.0.134	10.10.0.63	TLSv1.2	73	Alert (Level: Fatal, Description: Certificate Unknown)
11	0.143320	10.10.0.134	10.10.0.63	TCP	66	5001 → 44632 [ACK] Seq=3968 Ack=327 Win=30080 Len=0 TSval=4013656095 TS
12	0.145779	10.10.0.63	10.10.0.134	TCP	66	44632 → 5001 [FIN, ACK] Seq=327 Ack=3968 Win=37248 Len=0 TSval=18033087
13	0.146654	10.10.0.134	10.10.0.63	TCP	66	5001 → 44632 [FIN, ACK] Seq=3968 Ack=328 Win=30080 Len=0 TSval=4013656
14	0.146668	10.10.0.63	10.10.0.134	TCP	66	44632 → 5001 [ACK] Seq=328 Ack=3969 Win=37248 Len=0 TSval=1803308709 TS

Frame 4: 385 bytes on wire (3080 bits), 385 bytes captured (3080 bits)

Ethernet II, Src: fa:16:3e:0b:ba:d3 (fa:16:3e:0b:ba:d3), Dst: fa:16:3e:06:34:cf (fa:16:3e:06:34:cf)

Internet Protocol Version 4, Src: 10.10.0.63, Dst: 10.10.0.134

Transmission Control Protocol, Src Port: 44632, Dst Port: 5001, Seq: 1, Ack: 1, Len: 319

Transport Layer Security

TLShv1.2 Record Layer: Handshake Protocol: Client Hello

Content Type: Handshake (22)

Version: TLS 1.2 (0x0303)

Length: 314

Handshake Protocol: Client Hello

Handshake Type: Client Hello (1)

Length: 310

Version: TLS 1.2 (0x0303)

Random: c156e3aca40ba6edc5006ce4170516b582c3adc17a8b5af02078ddf423132989

GMT Unix Time: Oct 14, 2072 14:57:48.000000000 Eastern Daylight Time

Random Bytes: a40ba6edc5006ce4170516b582c3adc17a8b5af02078ddf423132989

Session ID Length: 32

Session ID: ad9dd3e10cf75efcc6c5978b0c856613618f9692669e0c1f4e275a7e03b31f33

WINNF Test Requirements:

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

2	- Make sure that UUT uses TLS v1.2 for security establishment. - Make sure UUT selects the correct cipher suite. - UUT shall use CRL or OCSP to verify the validity of the server certificate. - Make sure that Mutual authentication does not happen between UUT and the SAS Test Harness.	PASS	FAIL
---	--	------	------

Analysis of WINNF Test Requirements

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

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

```

> Frame 4: 385 bytes on wire (3080 bits), 385 bytes captured (3080 bits)
> Ethernet II, Src: fa:16:3e:0b:ba:d3 (fa:16:3e:0b:ba:d3), Dst: fa:16:3e:06:34:cf (fa:16:3e:06:34:cf)
> Internet Protocol Version 4, Src: 10.10.0.63, Dst: 10.10.0.134
> Transmission Control Protocol, Src Port: 44632, Dst Port: 5001, Seq: 1, Ack: 1, Len: 319
✓ Transport Layer Security
  ✓ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 314
    ✓ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 310
      Version: TLS 1.2 (0x0303)
      ✓ Random: c156e3aca40ba6edc5006ce4170516b582c3adc17a8b5af02078ddf423132989
        GMT Unix Time: Oct 14, 2072 14:57:48.000000000 Eastern Daylight Time
        Random Bytes: a40ba6edc5006ce4170516b582c3adc17a8b5af02078ddf423132989
        Session ID Length: 32
        Session ID: ad9dd3e10cf75efcc6c5978b0c856613618f9692669e0c1f4e275a7e03b31f33
        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 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

```

> Frame 4: 385 bytes on wire (3080 bits), 385 bytes captured (3080 bits)
> Ethernet II, Src: fa:16:3e:0b:ba:d3 (fa:16:3e:0b:ba:d3), Dst: fa:16:3e:06:34:cf (fa:16:3e:06:34:cf)
> Internet Protocol Version 4, Src: 10.10.0.63, Dst: 10.10.0.134
> Transmission Control Protocol, Src Port: 44632, Dst Port: 5001, Seq: 1, Ack: 1, Len: 319
▼ Transport Layer Security
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 314
  ▼ Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 310
    Version: TLS 1.2 (0x0303)
  ▼ Random: c156e3aca40ba6edc5006ce4170516b582c3adc17a8b5af02078ddf423132989
    GMT Unix Time: Oct 14, 2072 14:57:48.000000000 Eastern Daylight Time
    Random Bytes: a40ba6edc5006ce4170516b582c3adc17a8b5af02078ddf423132989
    Session ID Length: 32
    Session ID: ad9dd3e10cf75f6cc6c5978b0c856613618f9692669e0c1f4e275a7e03b31f33
    Cipher Suites Length: 86
  ▼ 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 (0x0060)
    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)
    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)

```


Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (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)

```

> Frame 8: 2585 bytes on wire (20680 bits), 2585 bytes captured (20680 bits)
> Ethernet II, Src: fa:16:3e:06:34:cf (fa:16:3e:06:34:cf), Dst: fa:16:3e:0b:ba:d3 (fa:16:3e:0b:ba:d3)
> Internet Protocol Version 4, Src: 10.10.0.134, Dst: 10.10.0.63
> Transmission Control Protocol, Src Port: 5001, Dst Port: 44632, Seq: 1449, Ack: 320, Len: 2519
> [2 Reassembled TCP Segments (3967 bytes): #6(1448), #8(2519)]
▼ Transport Layer Security
  ▼ TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 3962
  ▼ Handshake Protocol: Server Hello
    Handshake Type: Server Hello (2)
    Length: 81
    Version: TLS 1.2 (0x0303)
  ▼ Random: 6a66e101fa58e3425747af6f091daf4826414588b74eeeee444f574e47524401
    GMT Unix Time: Jul 27, 2026 00:39:29.000000000 Eastern Daylight Time
    Random Bytes: fa58e3425747af6f091daf4826414588b74eeeee444f574e47524401
    Session ID Length: 32
    Session ID: e5612d33af60968aaa3af57ec1b8abb599fbbf49fe200df378a65912f91158e9
    Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
    Compression Method: null (0)
    Extensions Length: 9
  ▼ Extension: extended_master_secret (len=0)
    Type: extended_master_secret (23)
    Length: 0

```

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

```

> Frame 10: 73 bytes on wire (584 bits), 73 bytes captured (584 bits)
> Ethernet II, Src: fa:16:3e:0b:ba:d3 (fa:16:3e:0b:ba:d3), Dst: fa:16:3e:06:34:cf (fa:16:3e:06:34:cf)
> Internet Protocol Version 4, Src: 10.10.0.63, Dst: 10.10.0.134
> Transmission Control Protocol, Src Port: 44632, Dst Port: 5001, Seq: 320, Ack: 3968, 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 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Test Equipment

Instrument	Manufacturer	Type No.	Serial No	Calibration Period (months) O/P Mon	Calibration Due
Power Supply	Xantrex	XKW 60-50	E00109863	O/P Mon	-
Signal Analyzer	Agilent	MXA	SSG013930	24 months	24.04.2026
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 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Appendix A – EUT & Client Provided Details

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (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 (for test report title)	AIR 1672 B48 B77D
Product Number	KRD 901 258/1 (with antenna, security unlocked) KRD 901 258/11** (with antenna, security locked) KRD 901 258/2* (CAB/RDNB board for testing purpose, security unlocked) KRD 901 258/21 (CAB/RDNB board for testing purpose, security locked) Note*: Tested unit Note**: This will be the marketed, sold unit
Serial Number(s)	EA8B946864
Software Version	CXP2020666/2-R32B15
Hardware Version	R1B
Domain Proxy Software Version:	ERICdomainproxyservice_CXP9035414 2.109.5

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Technical Description

The Equipment Under Test (EUT) AIR 1672 B48 B77D KRD 901 258 is an Ericsson AB dual-band TDD Antenna Integrated Radio unit with 16 transmitters and 16 receivers. It has 48 antenna elements and operates in the 3550-3700 MHz (B48) and 3700-3980 MHz (B77D) bands. It has an enhanced Common Public Radio Interface (eCPRI) and 8/4 downlink/uplink layer multi-user MIMO supporting NR. The Equipment Under Test (EUT) is shown in the photograph below. A full technical description can be found in the Manufacturer's documentation.



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

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Appendix B – EUT, Peripherals, and Test Setup Photos

Client	Ericsson	
Product	KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)	
Standard(s)	FCC Part 96 SAS requirements (CBRS Test Plan)	

Test setup

<Photos kept on file>