# Test Report

As per

# FCC Part 96 SAS requirements (CBRS Test Plan)

Add value.
Inspire trust.

on the

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

**FCC ID(s): TA8AKRD901258**


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

Nour El Masri
Report Reviewer

ACCREDITED
Testing Laboratory
Certificate #2955.19

# Table of Contents

# 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.

# 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'.

## *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.<br>• Record time at which transmission stops. Time must be within 60 | P |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | 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 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | 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:<br>• Transmission does not start until time of first heartbeat response or after.<br>• 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:<br>• Transmission does not start until time of first heartbeat response or after.<br>• 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:<br>• CBSD stops transmission within | P |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | 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:<br>• 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_PARAM) | Monitor RF transmission. Ensure:<br>• 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 (TEMINATED_GRANT) | Monitor RF transmission. CBSDs will have different behavior:<br>• CBSD1: will continue to transmit to end of test (this is not a pass/fail criteria, but check)<br>• CBSD2: must stop transmission within 60 seconds of being sent heartbeatResponse with responseCode = 500 | P |

| | | | | | | |
|---|---|---|---|---|---|---|
| 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:<br>• 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:<br>• 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 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | • 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:<br>• 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:<br>• 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<br>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<br>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<br>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<br>Check the tcpdump for the TLS information | P |

| | | | | | | |
|---|---|---|---|---|---|---|
| 6.8.4.2.4 | X | X | WINNF.FT.C.SCS.5 | TLS failure when certificate at the SAS Test Harness is corrupted | No RF transmission during test<br>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.<br><br>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.

## *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 market. 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.

# 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<br>Version V1.0.2<br>25 November 2020 | Conformance and Performance Test Technical Specification;<br>CBSD/DP as Unit Under Test (UUT)<br>Working Document |
| ISO/IEC 17025:2017 | General requirements for the competence of testing and calibration laboratories |

# 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.

# 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'.

# 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.

## *Testing Environmental Conditions and Dates*

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

| Date | Test | Initials | Temperature (ºC) | Humidity (%) | Pressure (kPa) |
|---|---|---|---|---|---|
| July 9-11 | All | SD | 20-23 | 40-55 | 98-102 |

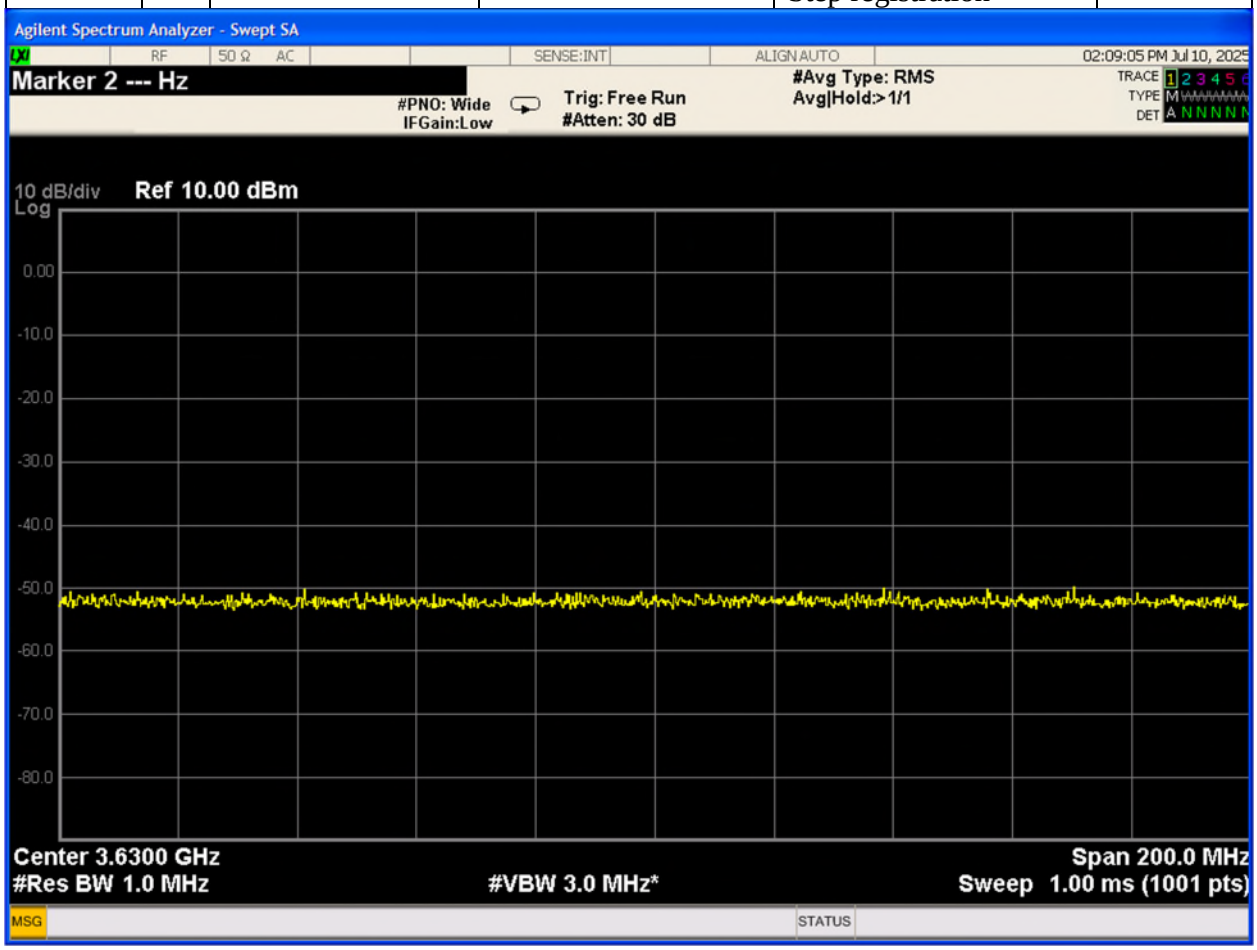
# Detailed Test Results Section

## *Registration.*

D.REG.2

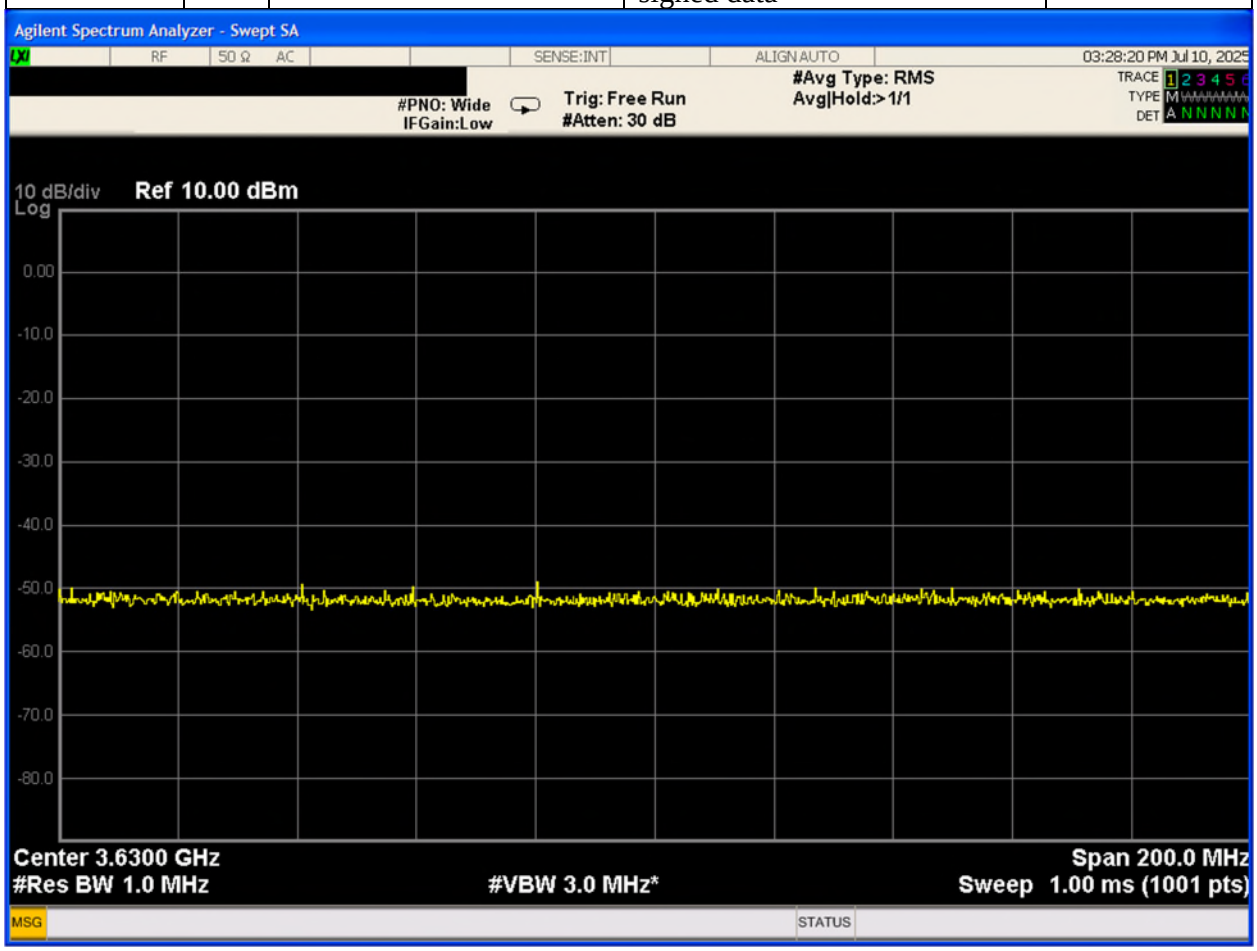
Authorization transmit after it receives authorization from a SAS.

| 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 |



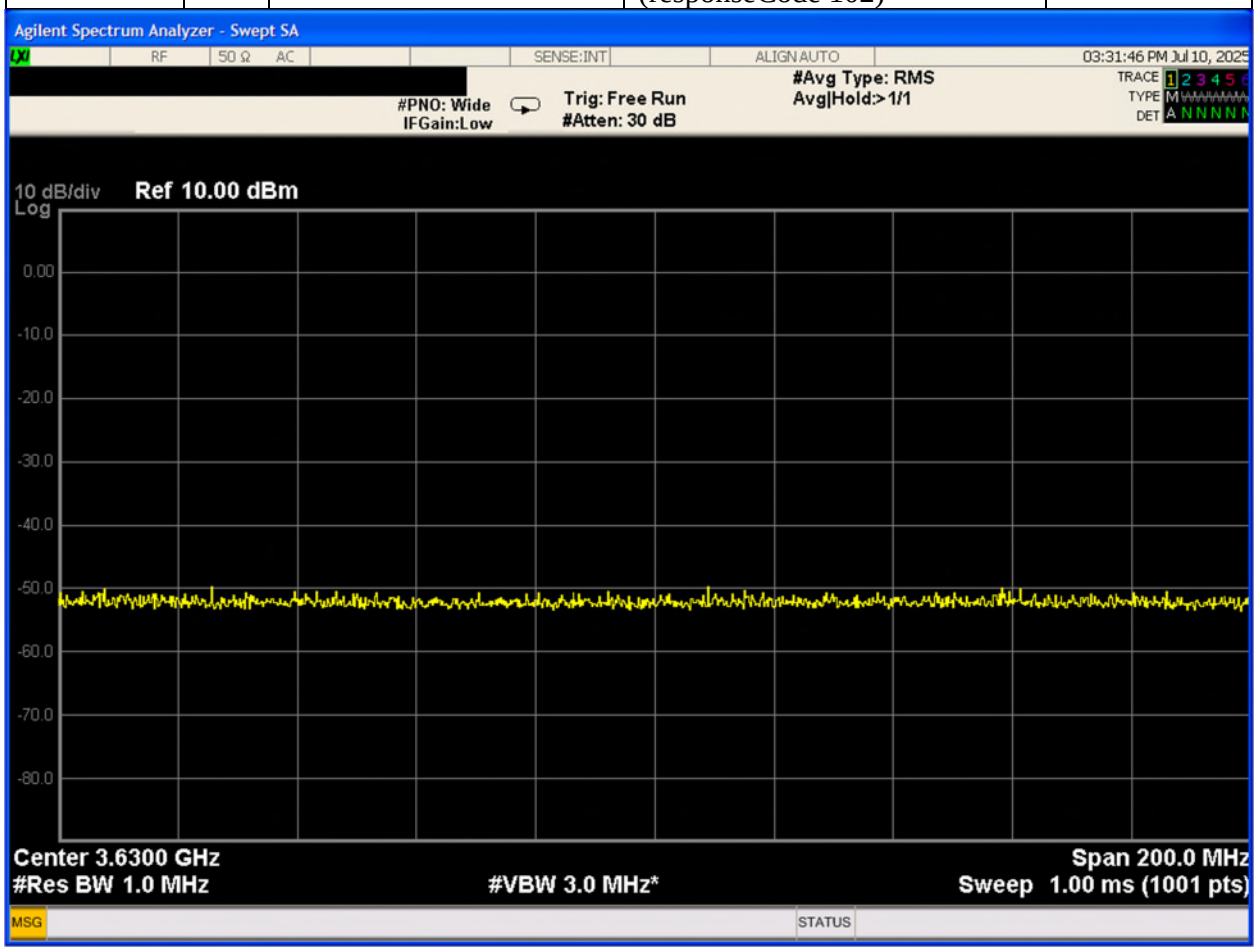
## D.REG.6

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



## D.REG.9

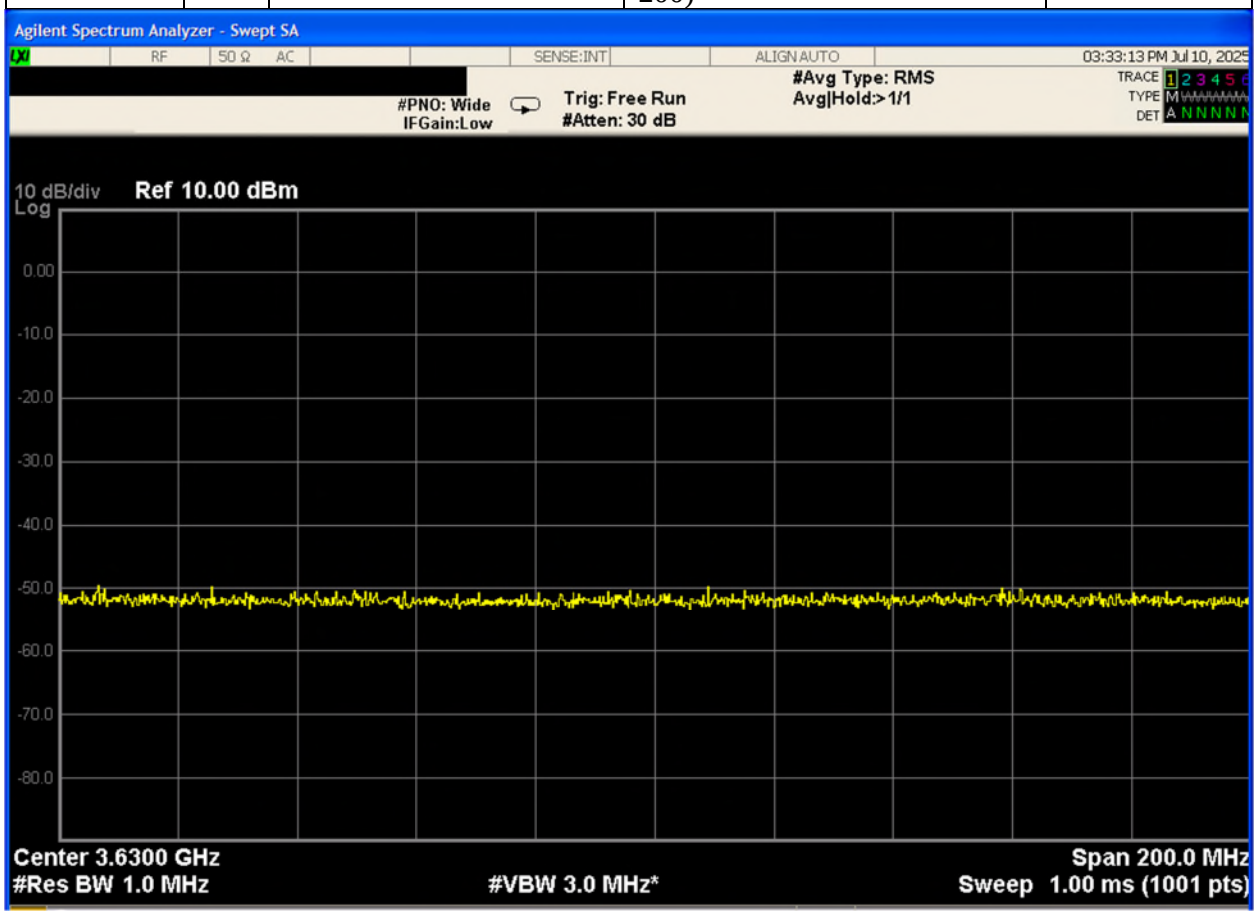
| | | | | |
|---|---|---|---|---|
| 6.1.4.2.2 | X | WINNF.FT.D.REG.9 | Domain Proxy Missing Required parameters (responseCode 102) | P |




Note response code verified via logs kept on file.

## D.REG.11

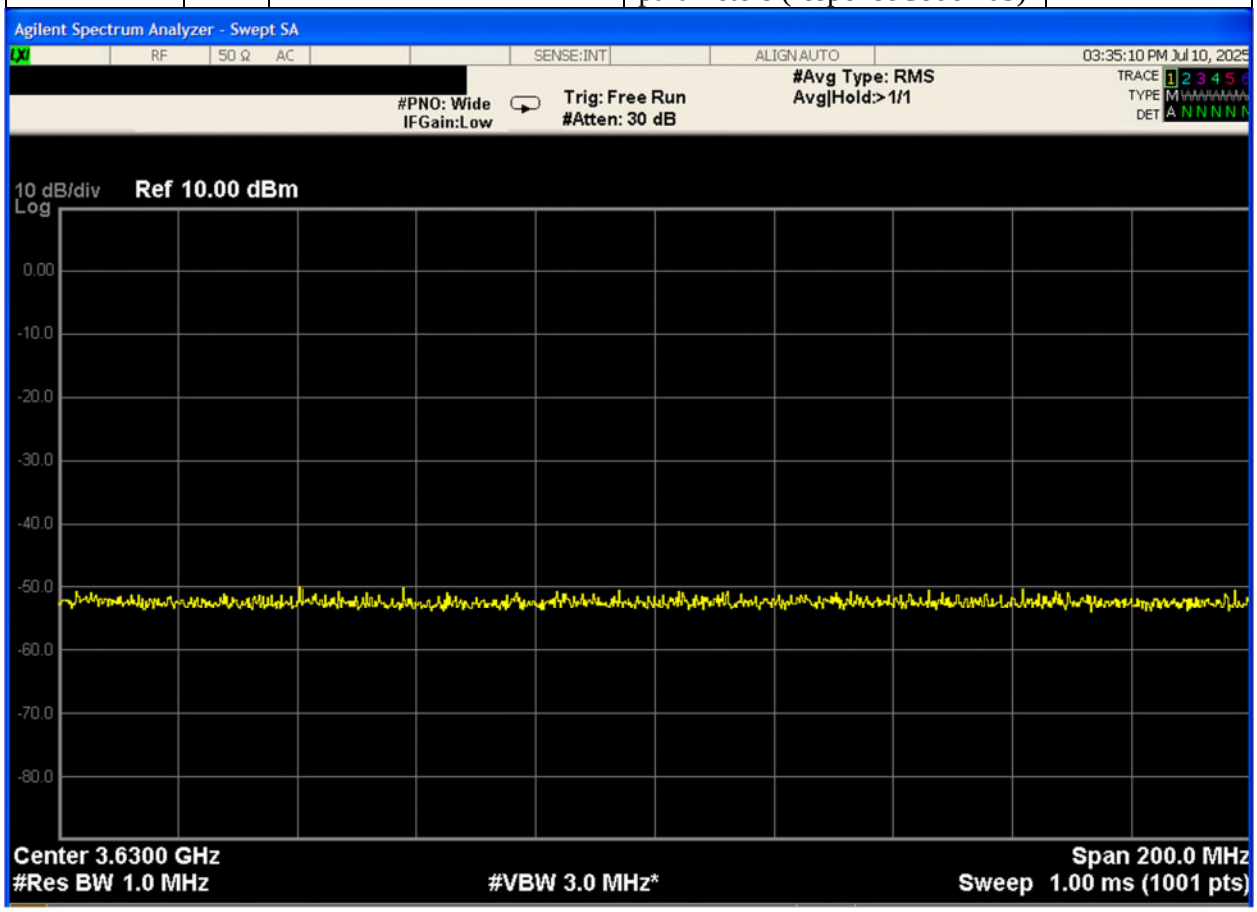
| | | | | |
|---|---|---|---|---|
| 6.1.4.2.4 | X | WINNF.FT.D.REG.11 | Domain Proxy Pending registration (responseCode 200) | P |




Note response code verified via logs kept on file.

## D.REG.13

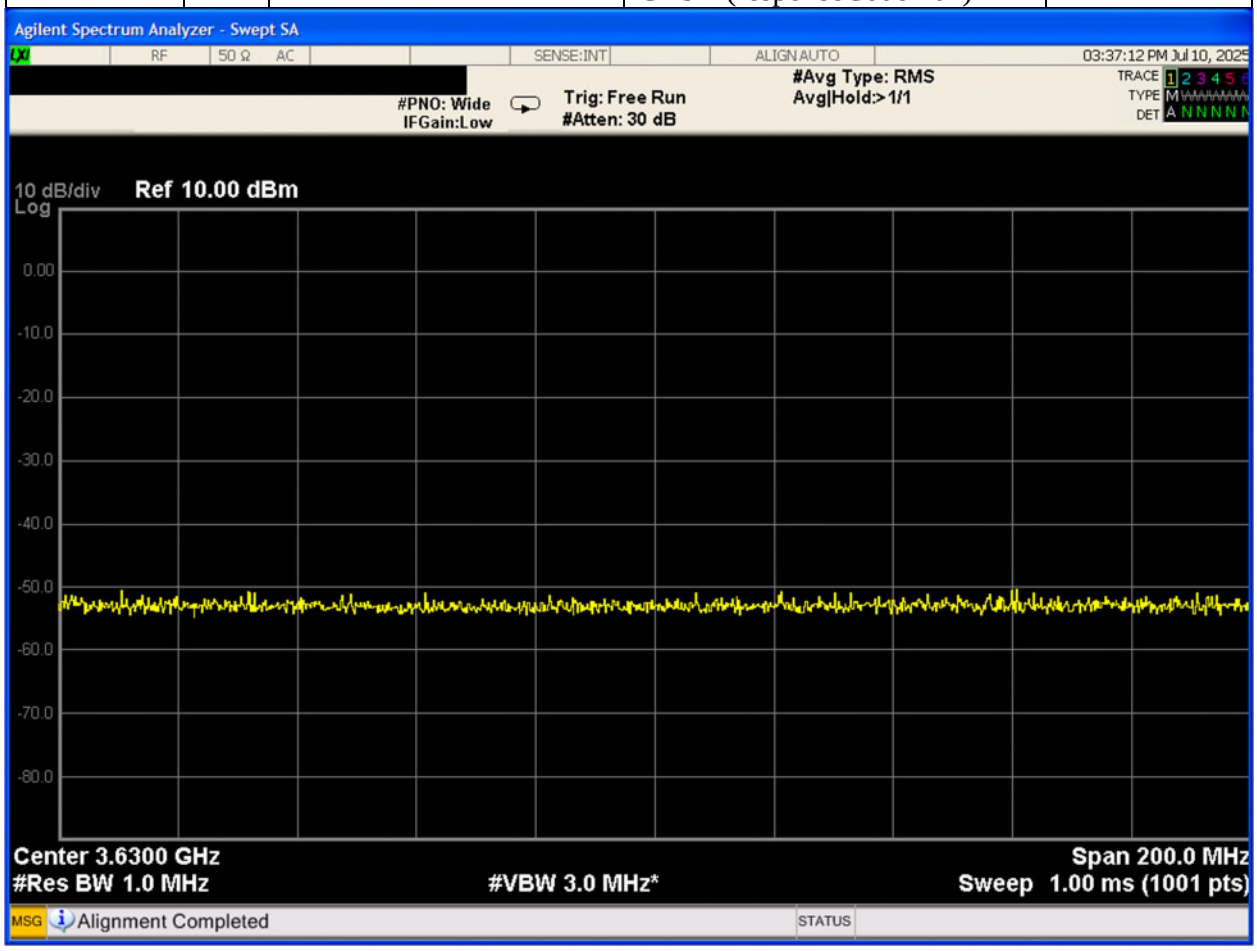
| | | | | |
|---|---|---|---|---|
| 6.1.4.2.6 | X | WINNF.FT.D.REG.13 | Domain Proxy Invalid parameters (responseCode 103) | P |




Note response code verified via logs kept on file.

## D.REG.15

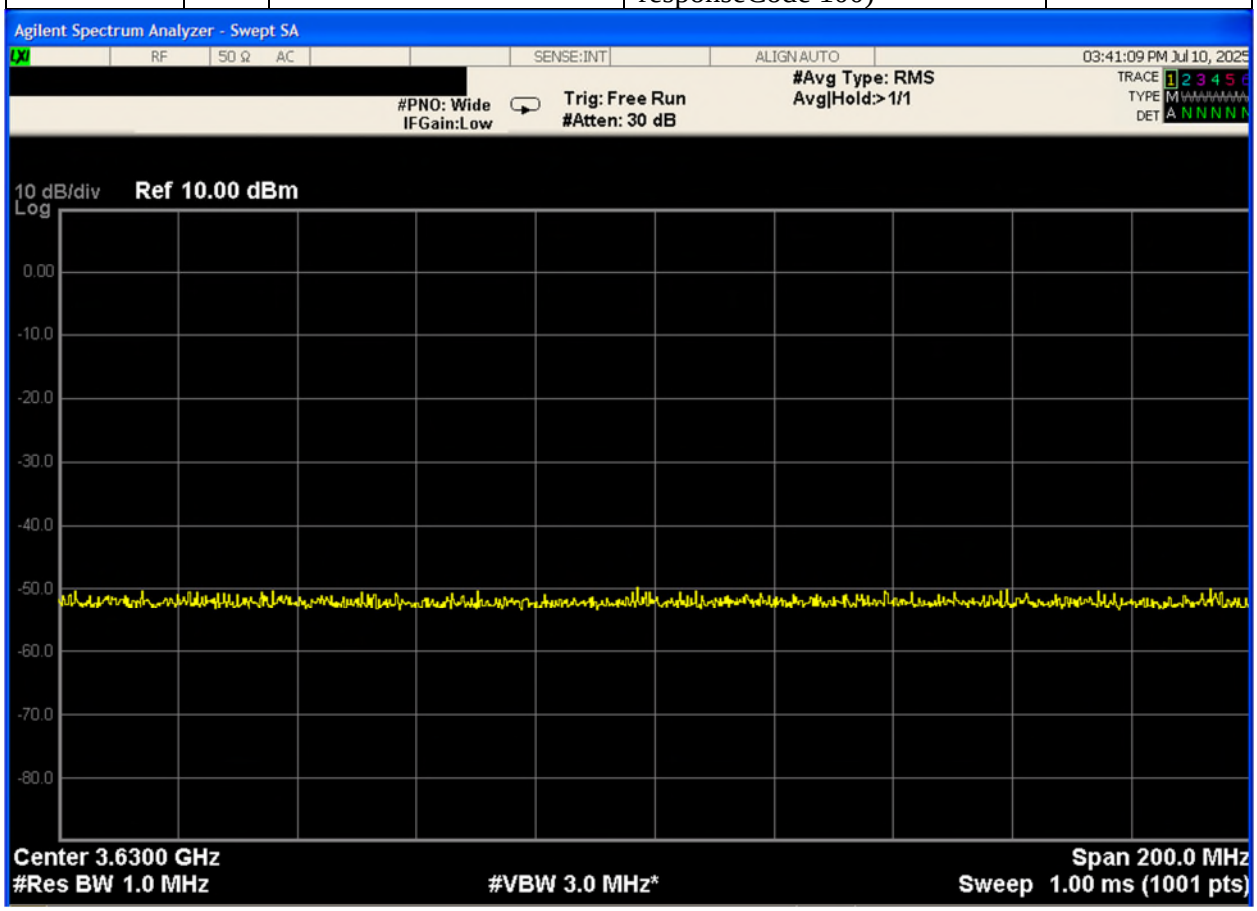
| | | | | |
|---|---|---|---|---|
| 6.1.4.2.8 | X | WINNF.FT.D.REG.15 | Domain Proxy Blacklisted CBSD (responseCode 101) | P |




Note response code verified via logs kept on file.

## D.REG.17

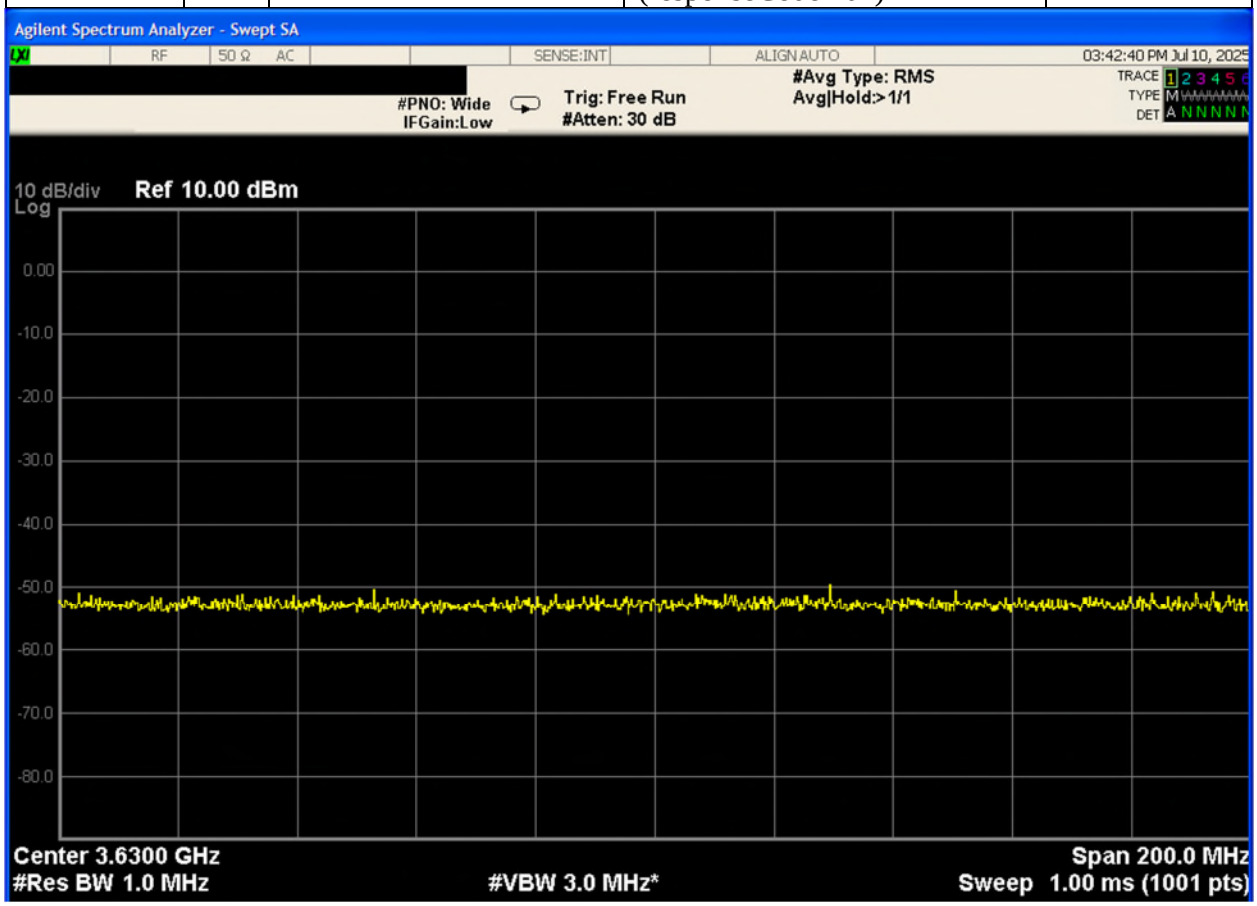
| | | | | |
|---|---|---|---|---|
| 6.1.4.2.10 | X | WINNF.FT.D.REG.17 | Domain Proxy Unsupported SAS protocol version responseCode 100) | P |




Note response code verified via logs kept on file.

## D.REG.19

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



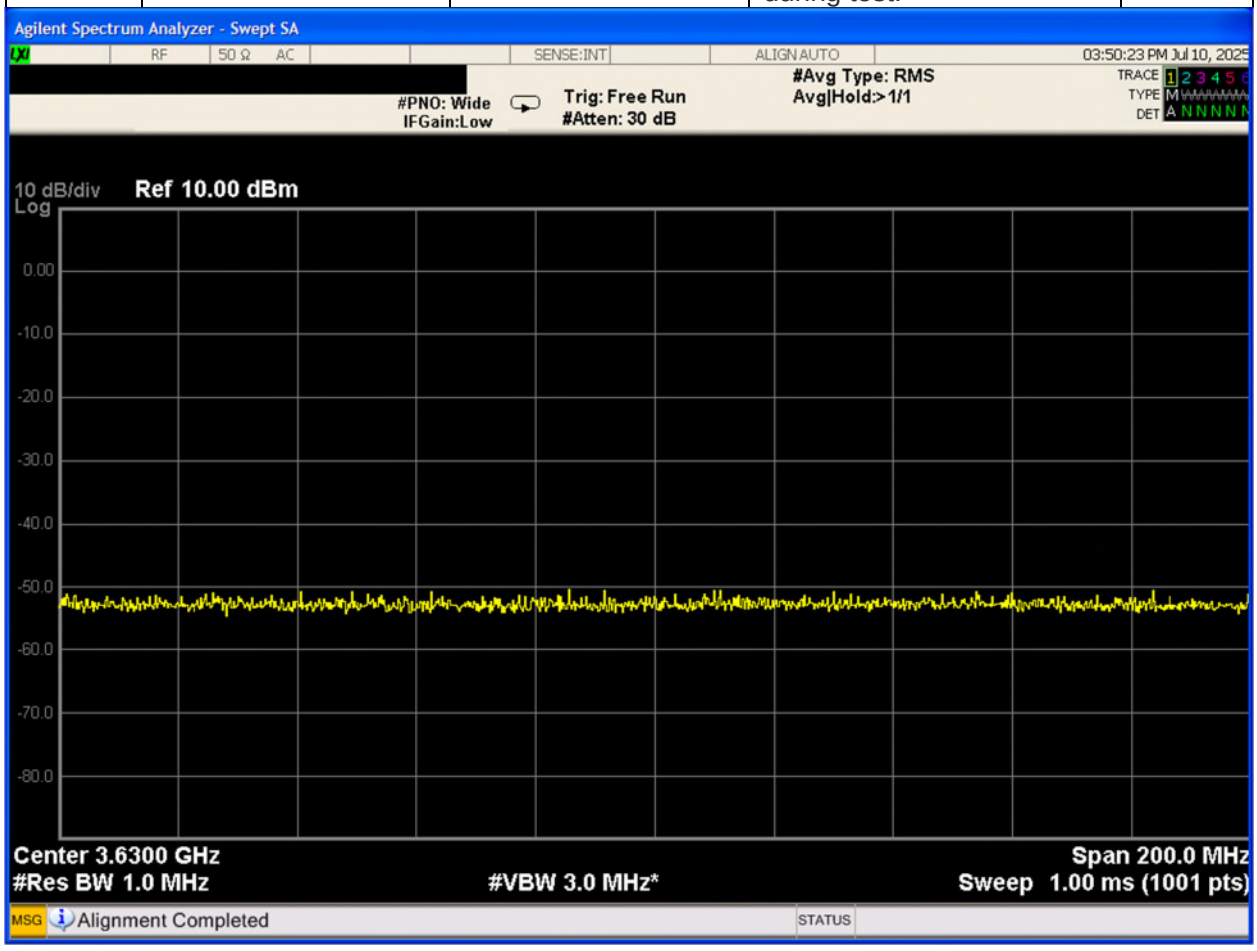

Note response code verified via logs kept on file.

## 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

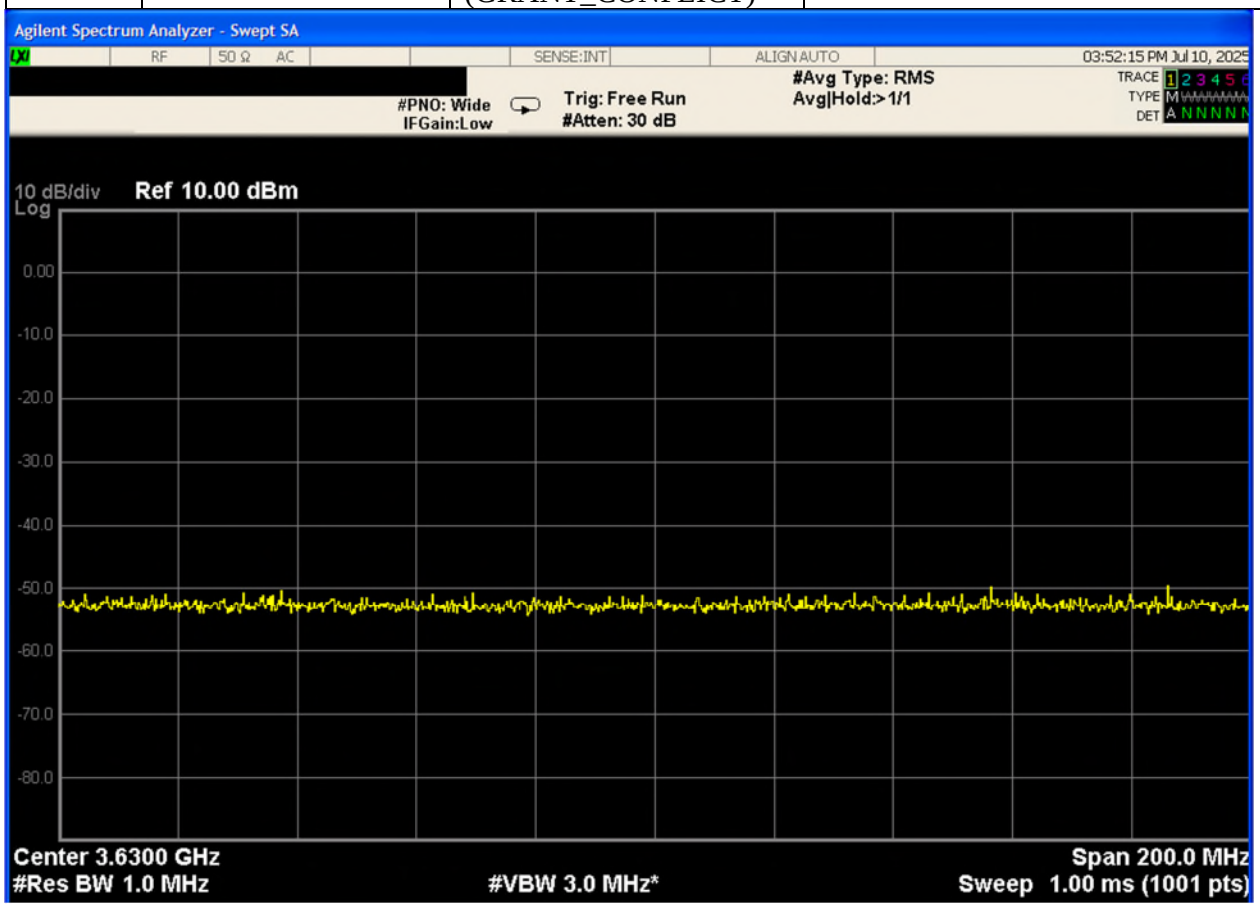
| | | | | |
|---|---|---|---|---|
| 6.3.4.2.1 | WINNF.FT.C.GRA.1 | Unsuccessful Grant responseCode=400 (INTERFERENCE) | Monitor for 60 seconds after REG message sent. No transmission during test. | P |




Note response code verified via logs kept on file.

## 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 |

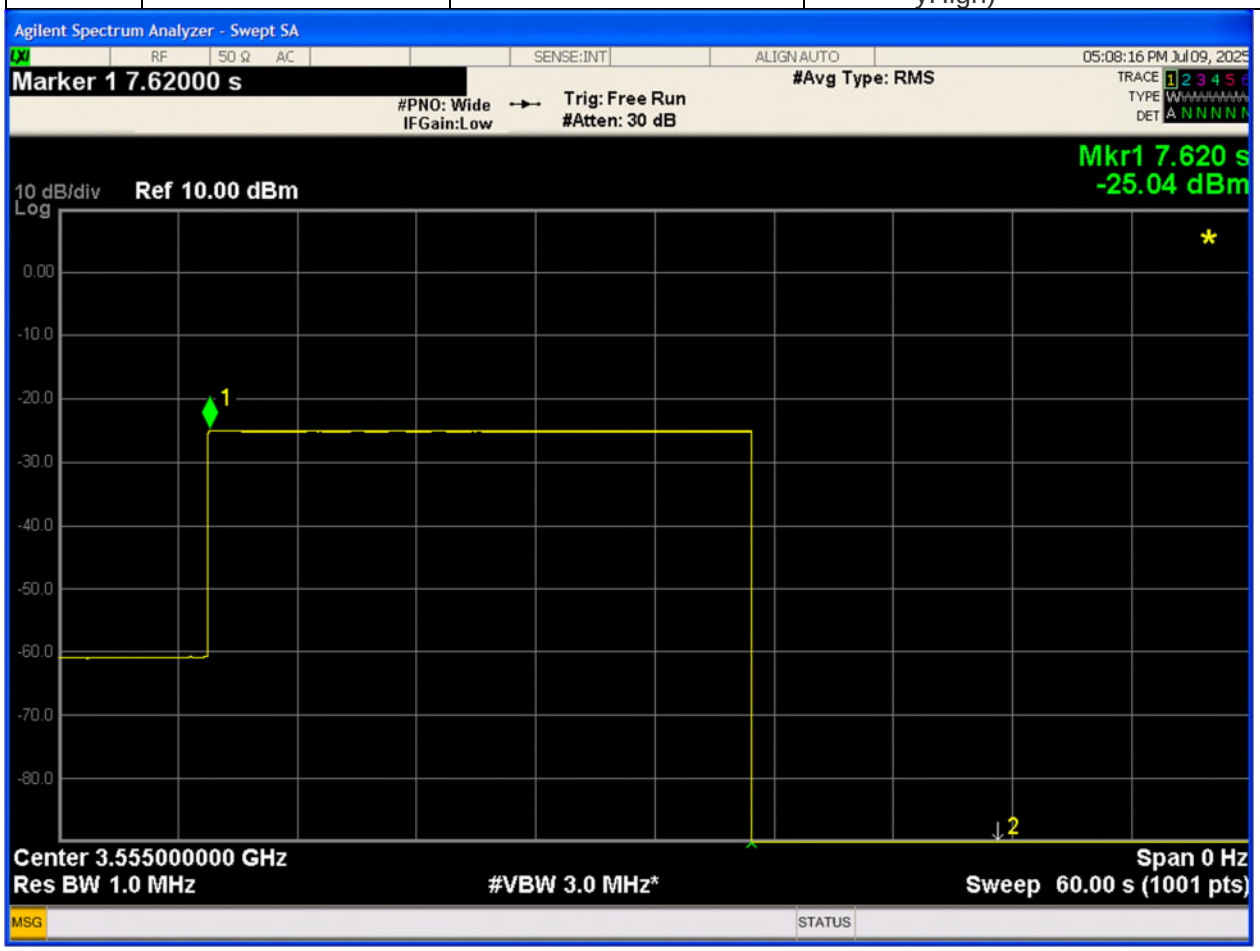



Note response code verified via logs kept on file.

## *Heartbeat*

D.HBT.2

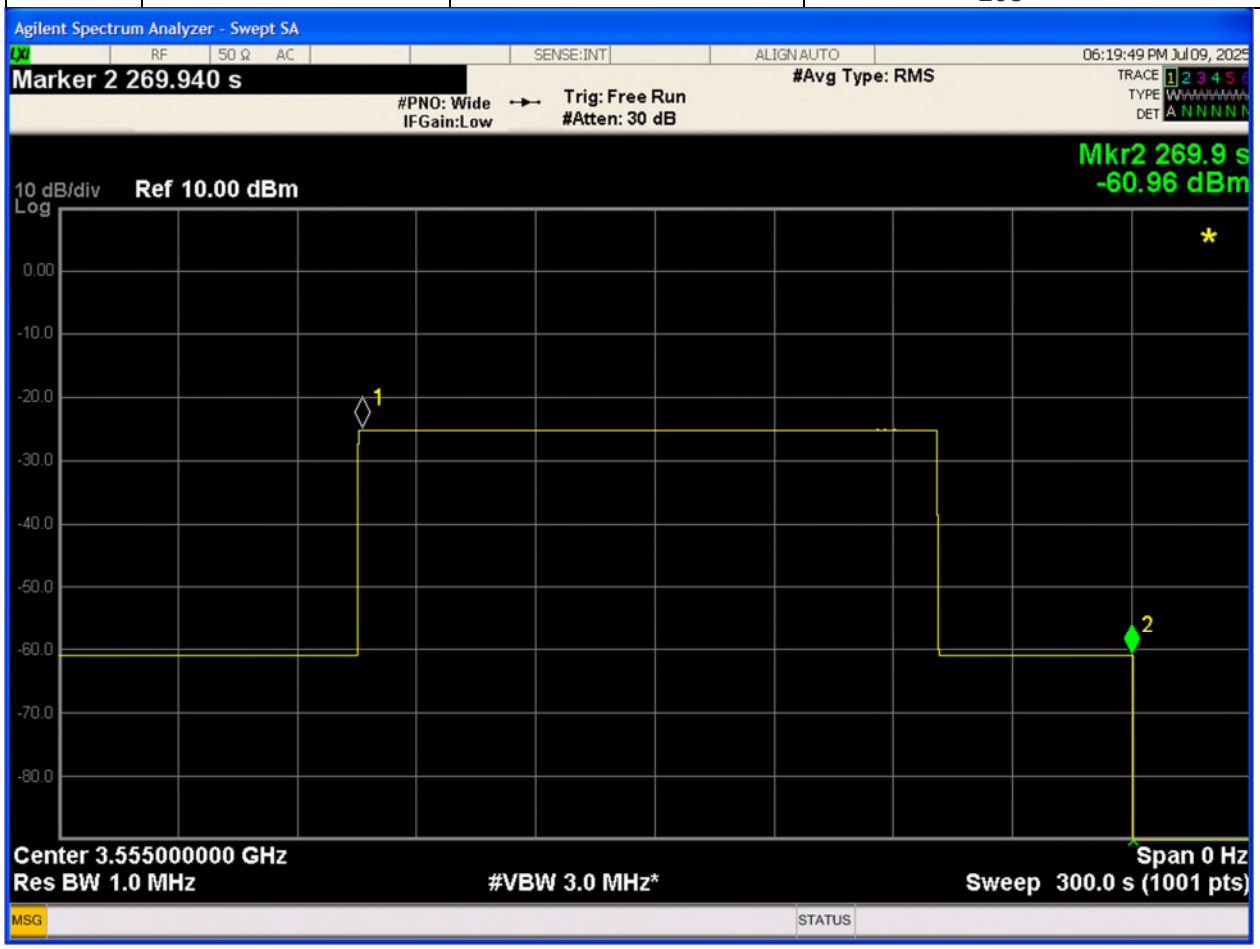
| | | | | |
|---|---|---|---|---|
| 6.4.4.1.2 | WINNF.FT.D.HBT.2 | Domain Proxy Heartbeat Success Case (first Heartbeat Response) | Monitor RF from start of test. Ensure that:<br>• Transmission does not start until time of first heartbeat response or after.<br>• After transmission starts, measure that transmission is within the granted channel (frequencyLow, frequencyHigh) | P |




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

## C.HBT.3

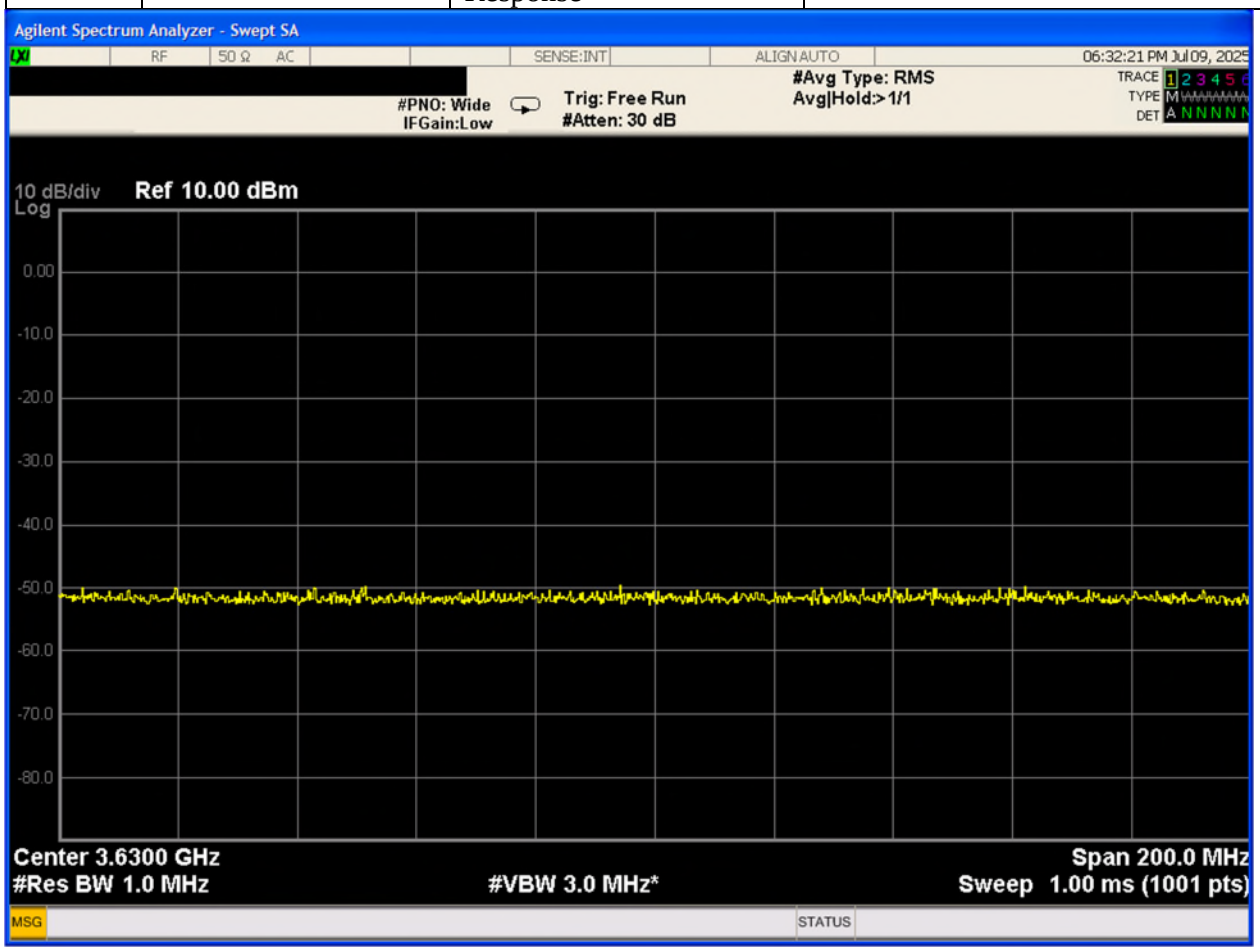
| | | | | |
|---|---|---|---|---|
| 6.4.4.2.1 | WINNF.FT.C.HBT.3 | Heartbeat responseCode=105 (DEREGISTER) | Monitor RF transmission. Ensure that:<br>• CBSD stops transmission within 60 seconds of the heartbeatResponse which contains responseCode = 105 | P |




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

## C.HBT.5

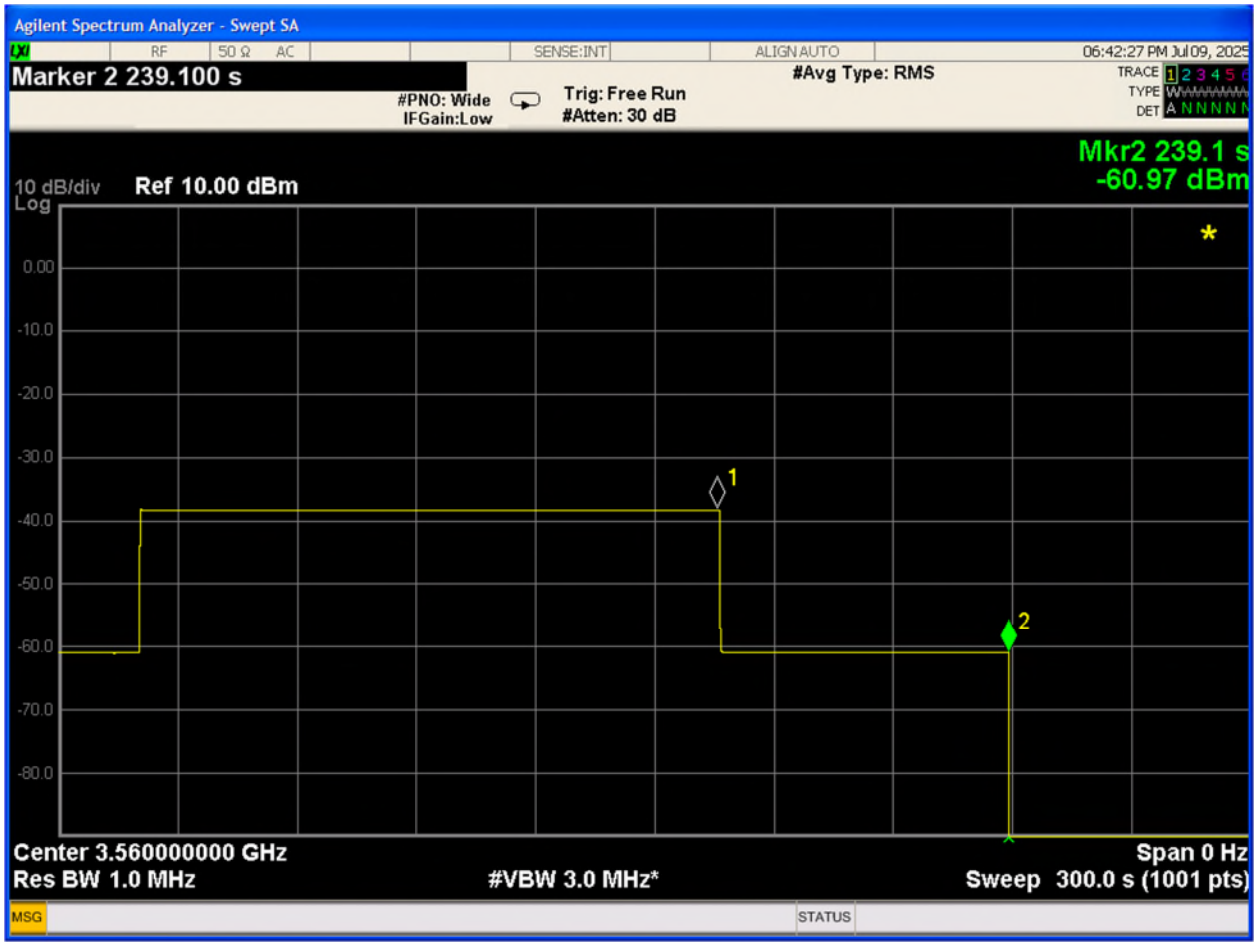
| | | | | |
|---|---|---|---|---|
| 6.4.4.2.3 | WINNF.FT.C.HBT.5 | Heartbeat responseCode=501 (SUSPENDED_GRANT) in First Heartbeat Response | Monitor RF transmission from start of test. Ensure there is no transmission during the test | p |




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

## C.HBT.6

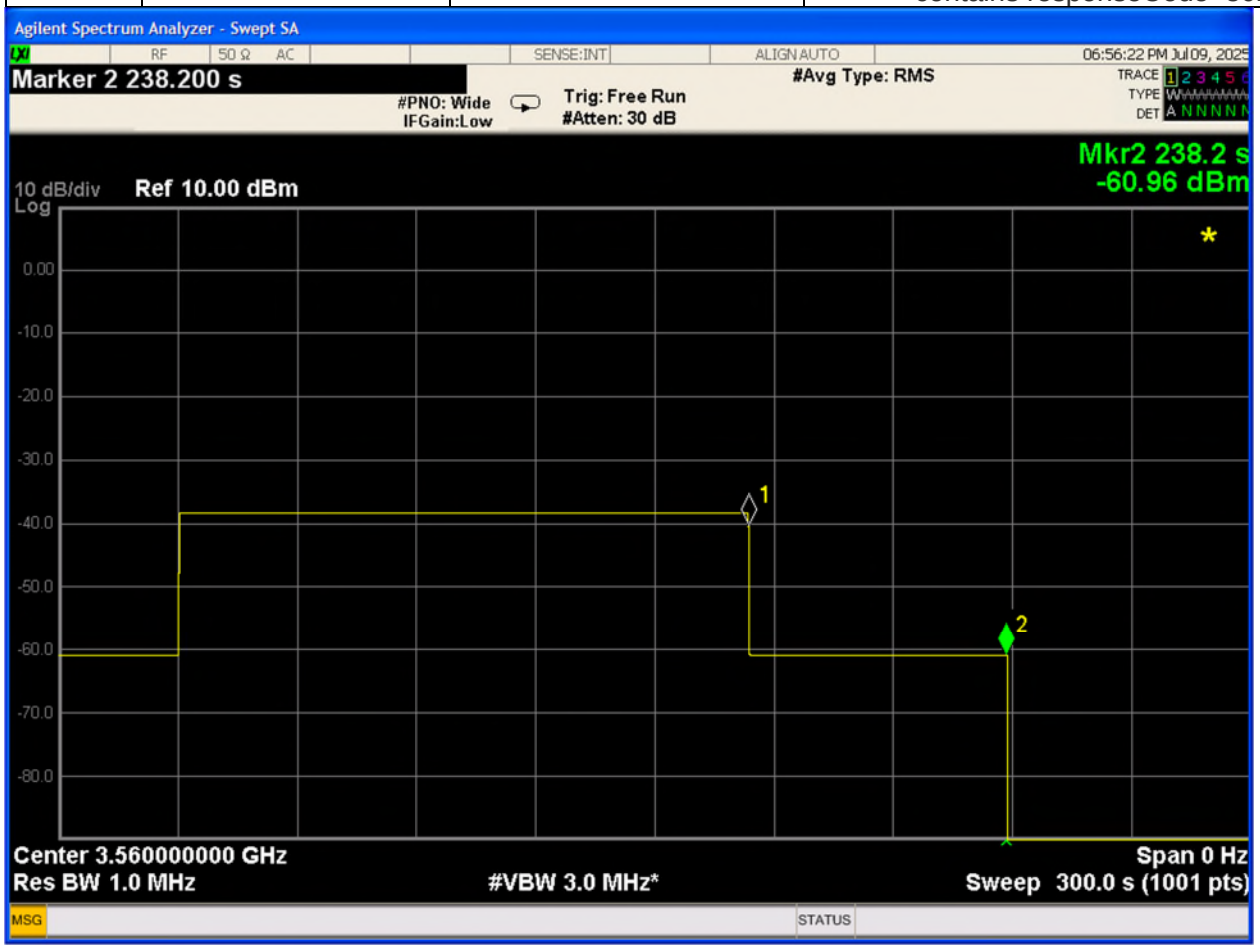
| | | | | |
|---|---|---|---|---|
| 6.4.4.2.4 | WINNF.FT.C.HBT.6 | Heartbeat responseCode=501 (SUSPENDED_GRANT) in Subsequent Heartbeat Response | Monitor RF transmission. Ensure:<br>• CBSD stops transmission within 60 seconds of heartbeatResponse which contains responseCode=501 | p |




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

## C.HBT.7

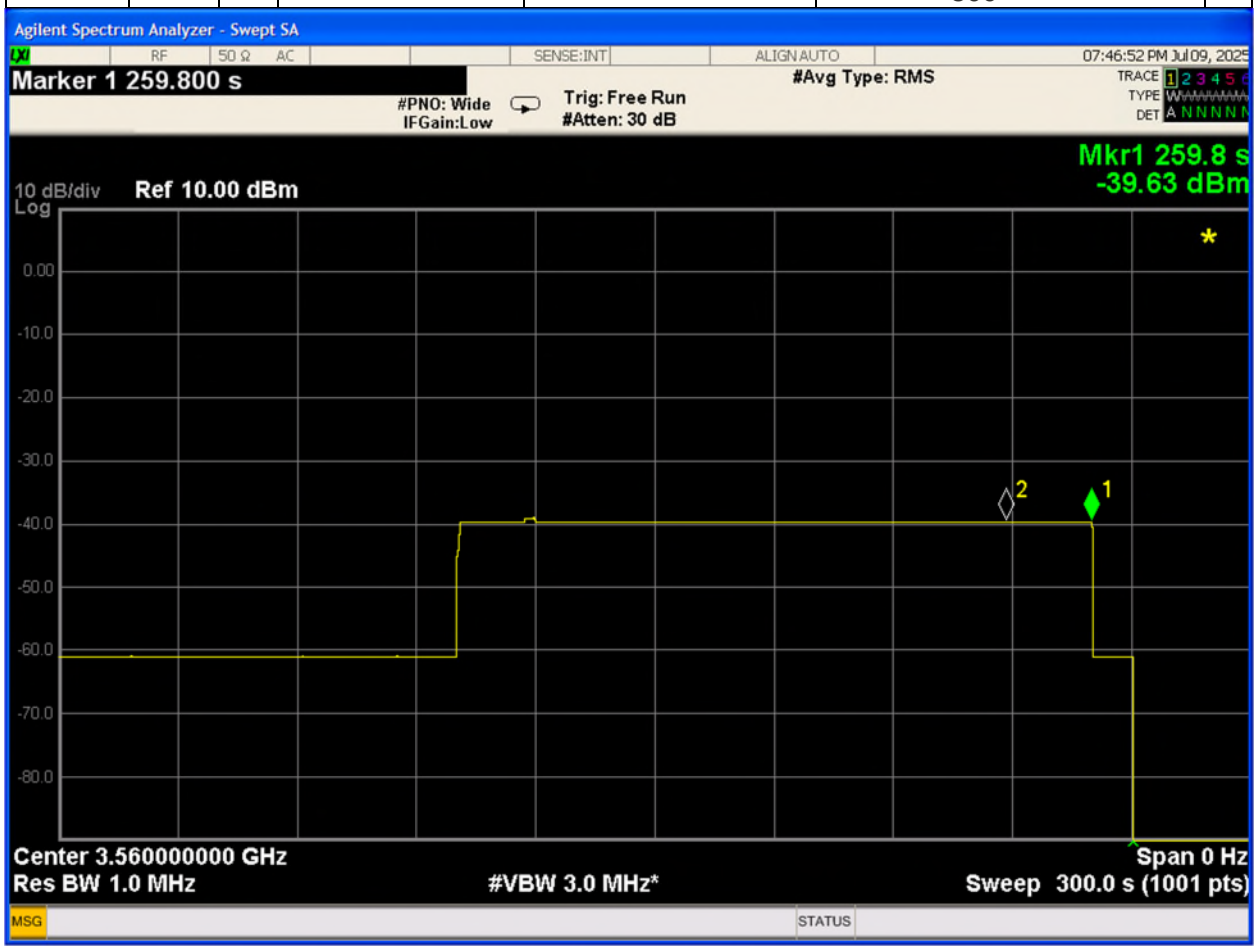
| | | | | |
|---|---|---|---|---|
| 6.4.4.2.5 | WINNF.FT.C.HBT.7 | Heartbeat responseCode=502 (UNSYNC_OP_PARAM) | Monitor RF transmission. Ensure:<br>• CBSD stops transmission within 60 seconds of heartbeatResponse which contains responseCode=502 | p |




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

## D.HBT.8

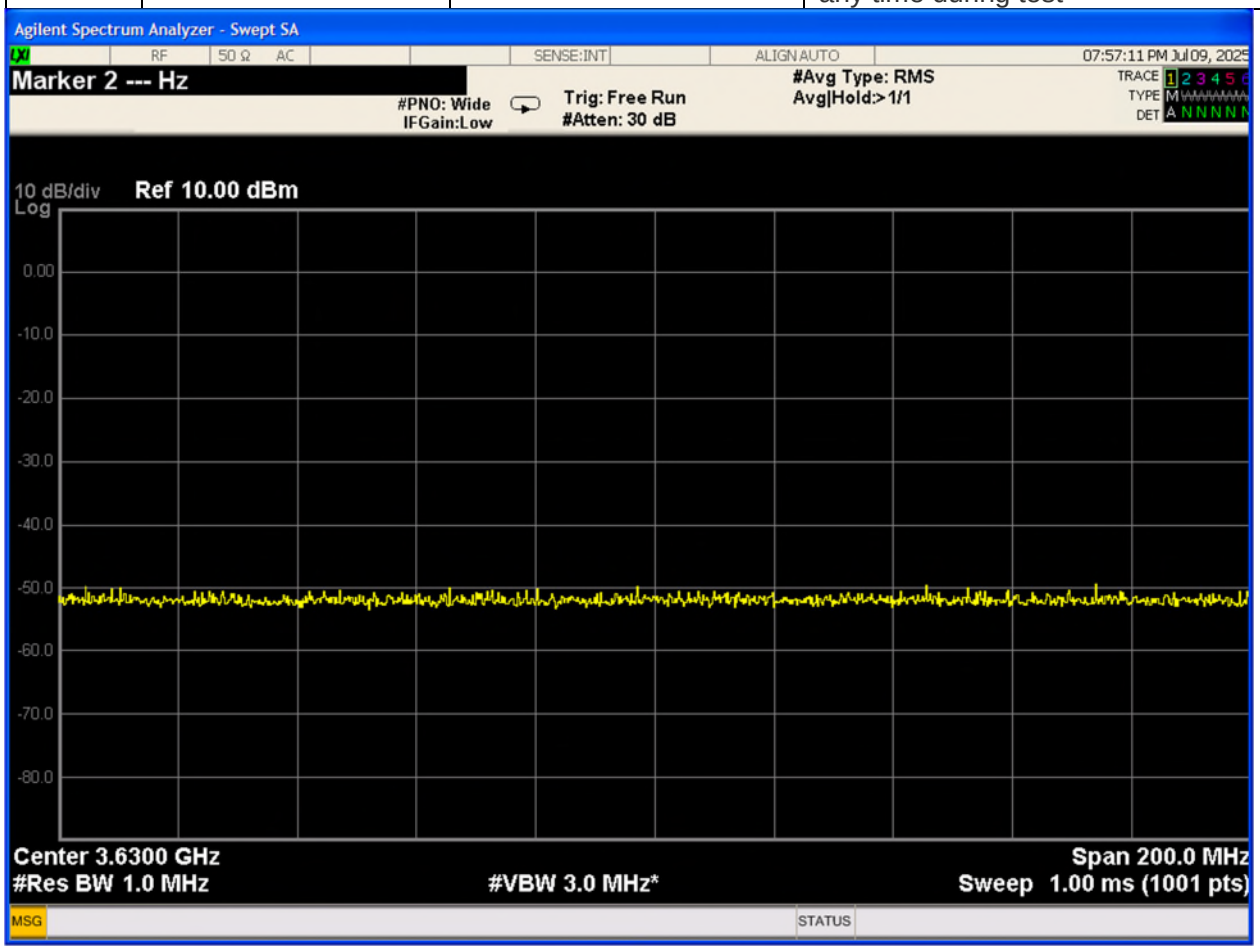
| | | | | | | |
|---|---|---|---|---|---|---|
| 6.4.4.2.6 | -- | X | WINNF.FT.D.HBT.8 | Domain Proxy Heartbeat responseCode=500 (TEMINATED_GRANT) | Monitor RF transmission. CBSDs will have different behavior:<br>• CBSD1: will continue to transmit to end of test (this is not a pass/fail criteria, but check)<br>• 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.

## C.HBT.9

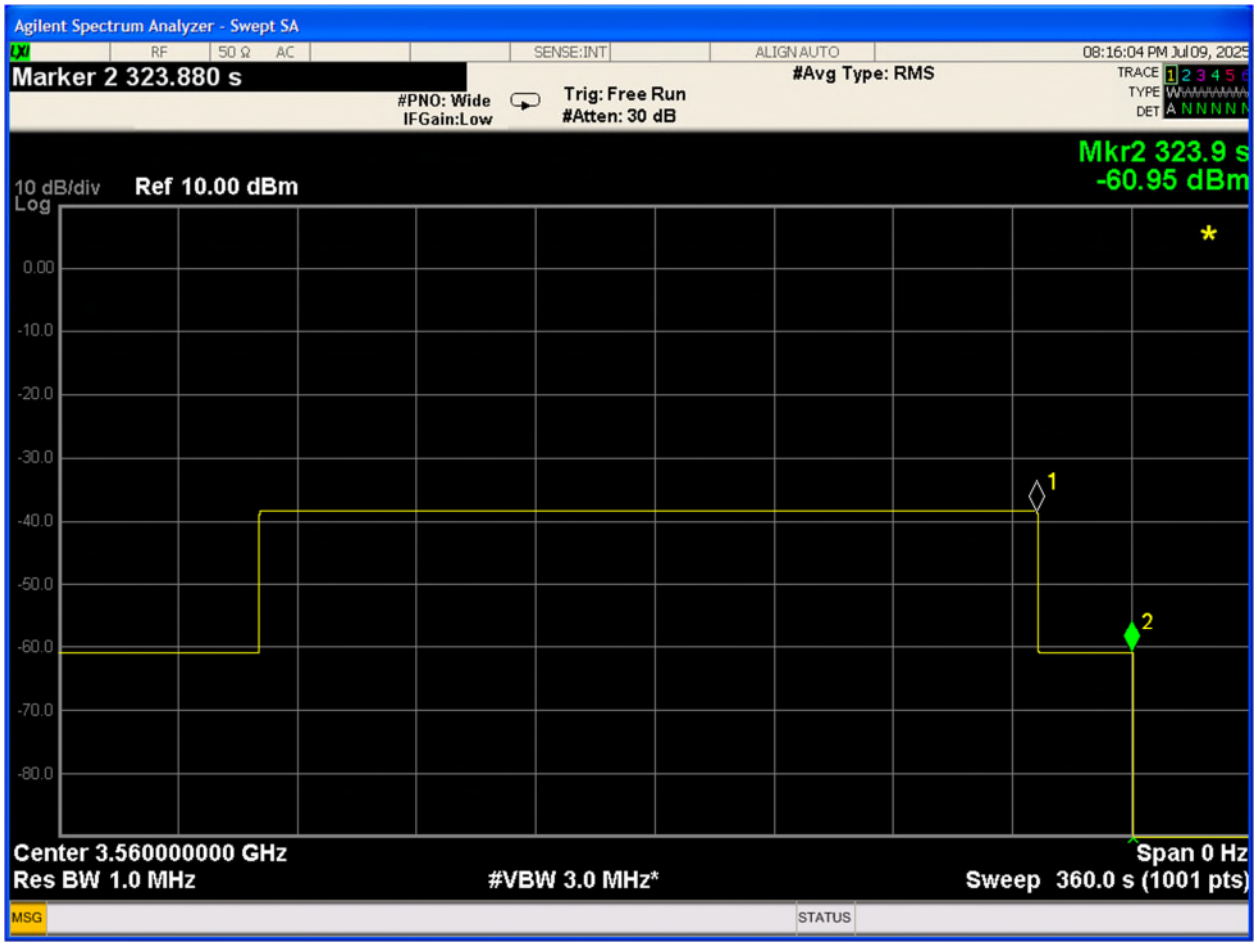
| | | | | |
|---|---|---|---|---|
| 6.4.4.3.1 | WINNF.FT.C.HBT.9 | Heartbeat Response Absent (First Heartbeat) | Monitor RF from start of test to 60 seconds after last heartbeatResponse message was sent. CBSD should not transmit at any time during test | P |




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

## C.HBT.10

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

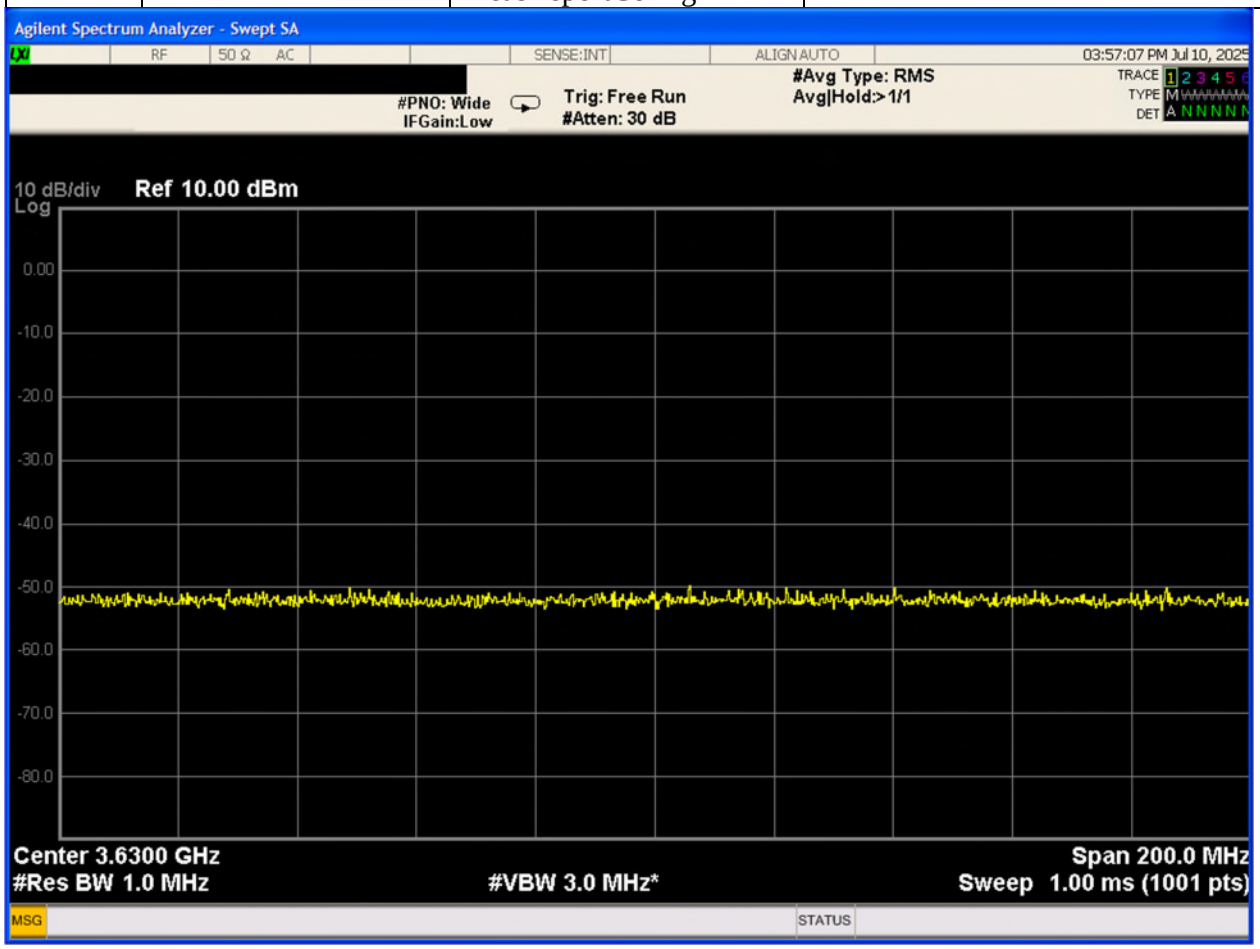



Test Harness logs and timing on graph was verified, the EUT passed the requirement.

## *Measurement*

D.MES.2

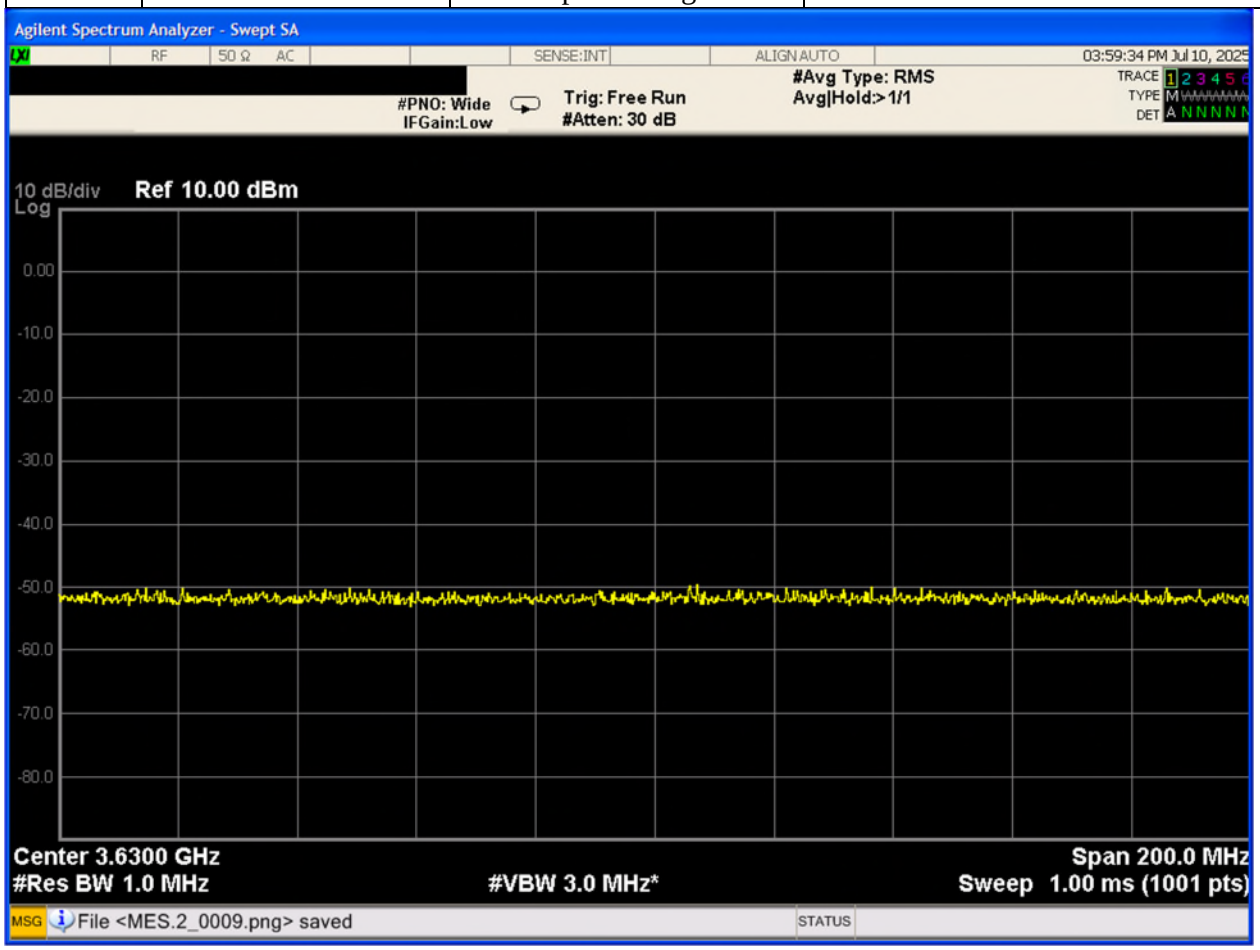
| | | | | |
|---|---|---|---|---|
| 6.5.4.2.2 | WINNF.FT.D.MES.2 | Domain Proxy Registration Response contains measReportConfig | No RF monitoring | P |




Pass. "measreportconfig" in logs. All other requirements verified.

## C.MES.3

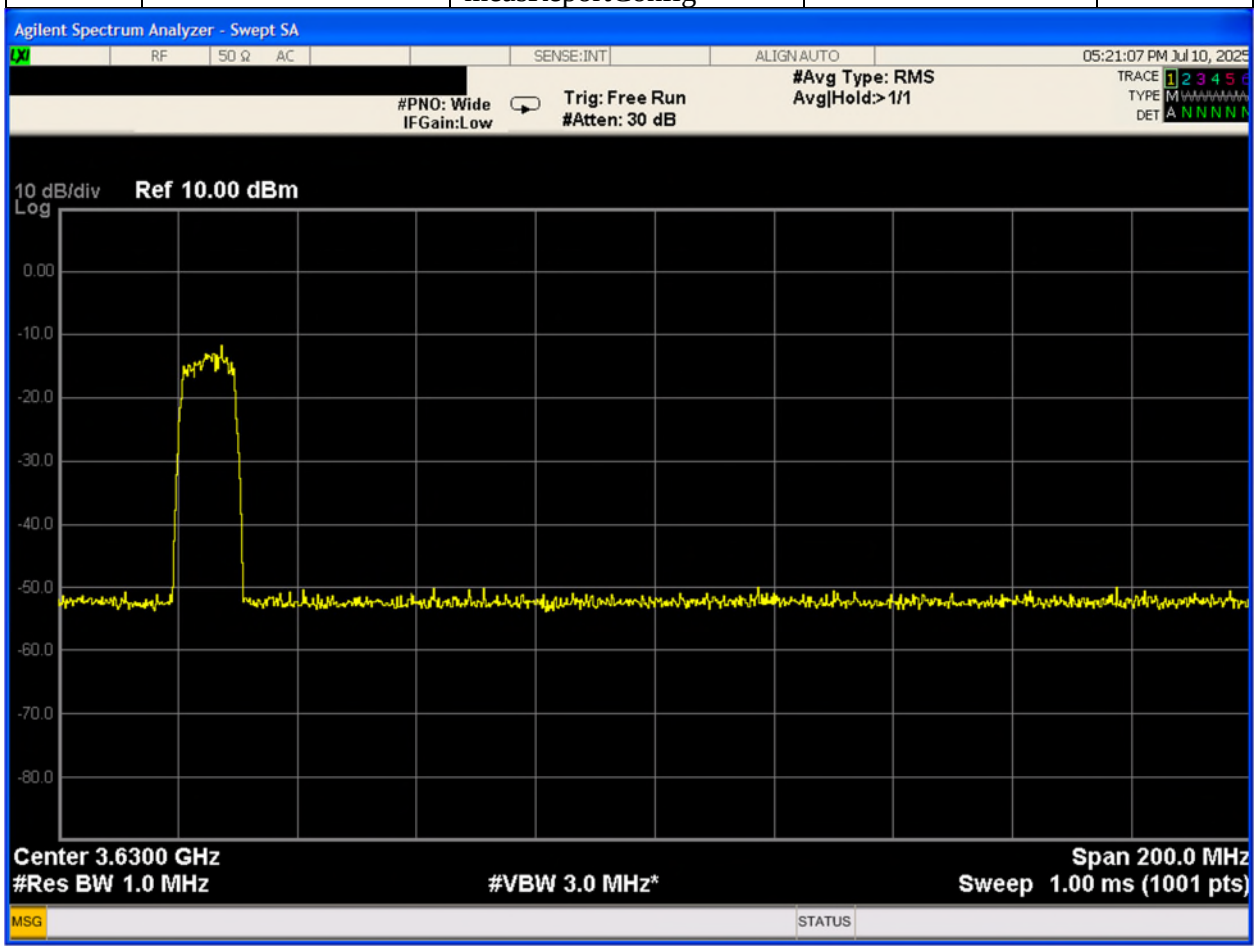
| | | | | |
|---|---|---|---|---|
| 6.5.4.2.3 | WINNF.FT.C.MES.3 | Grant Response contains measReportConfig | No RF monitoring | P |




Pass. "measreportconfig" in logs. All other requirements verified.

## D.MES.5

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

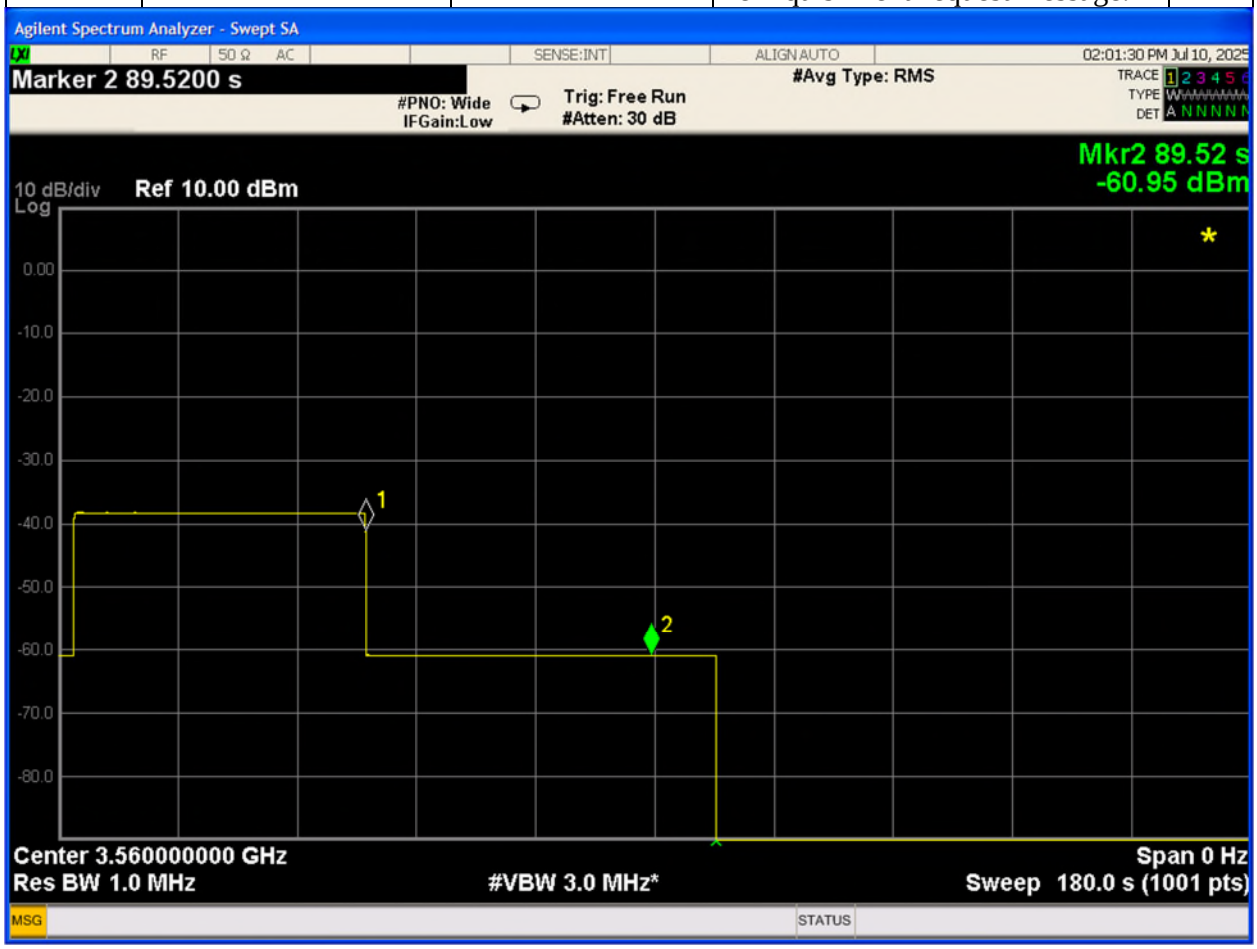



Pass. "measreportconfig" in logs. All other requirements verified.

## *Relinquishment and Deregistration*

D.RLQ.2

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

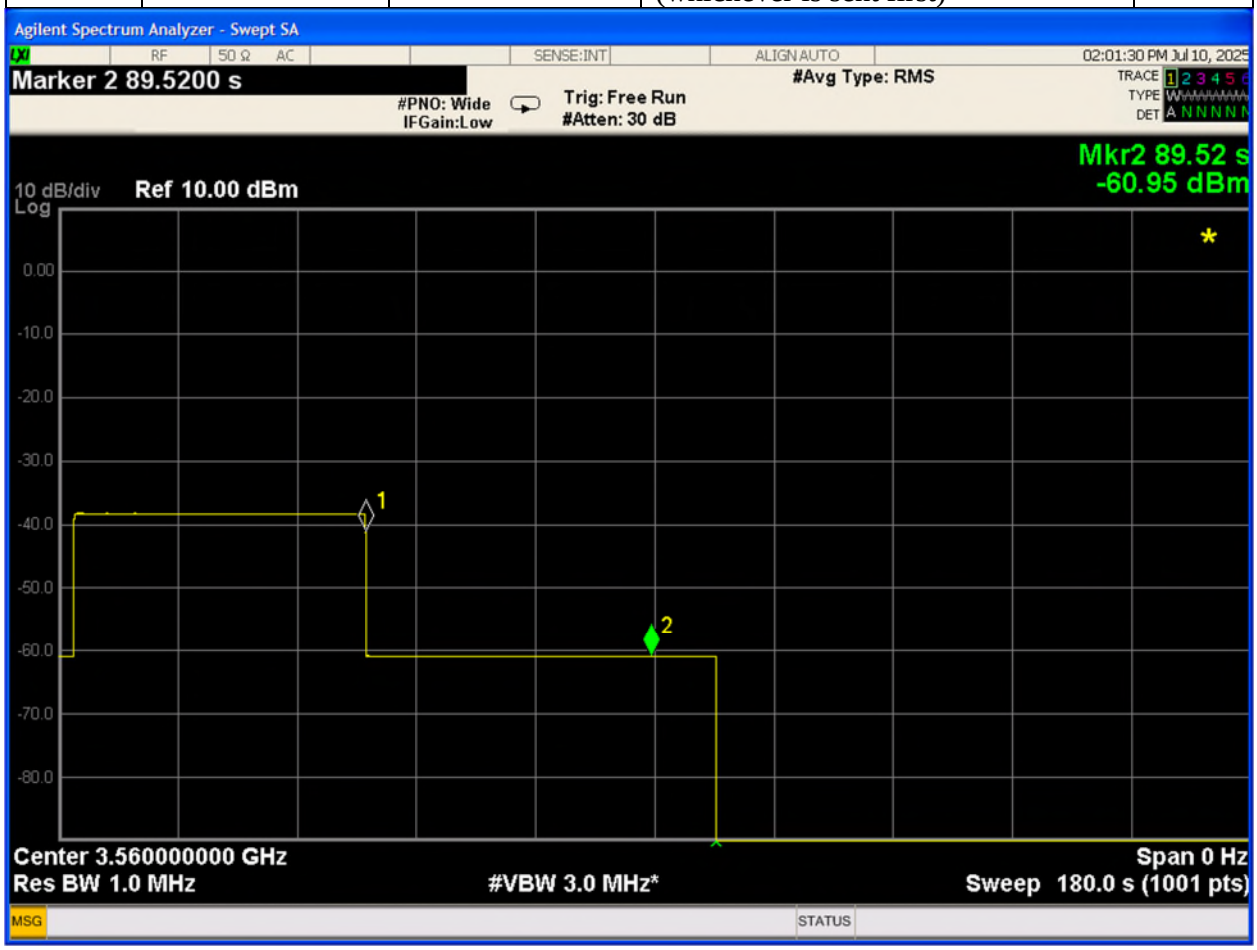



Test Harness logs and timing on graph was verified, the EUT passed the requirement.

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

## D.DRG.2

| | | | | |
|---|---|---|---|---|
| 6.7.4.1.2 | WINNF.FT.D.DRG.2 | Domain Proxy Successful Deregistration | Monitor RF transmission. Ensure:<br>• 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

## *Power Measurement*

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

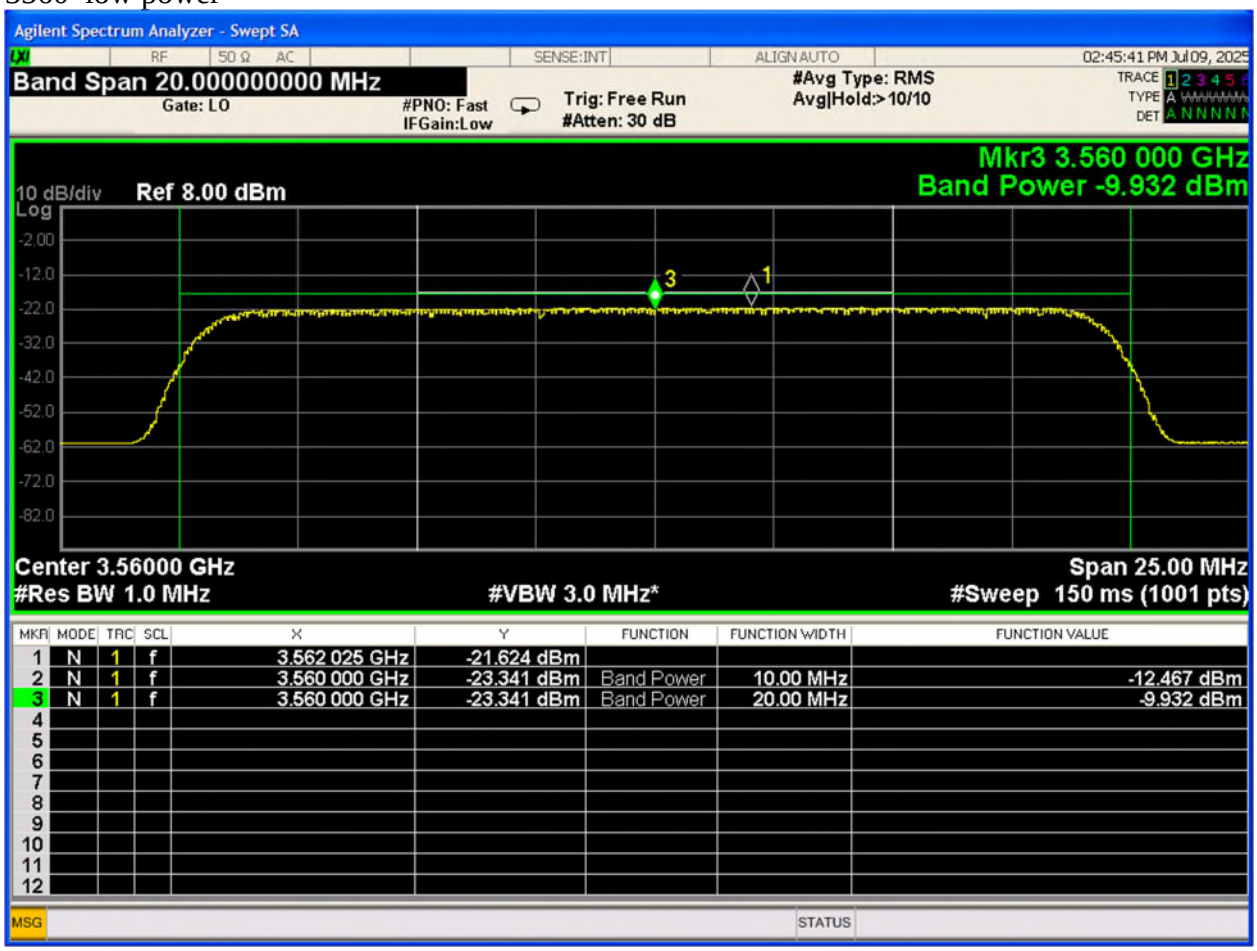
| | | | | | | |
|---|---|---|---|---|---|---|
| 7.1.4.1.1 | X | X | WINNF.PT.C.HBT | UUT RF Transmit Power Measurement | Power Spectral Density test case.<br><br>Assume we use 1 carrier bandwidth (say, 5 or 10 MHz), one frequency (say middle channel in band) for test. Measure at max transmit power, and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

Test Table

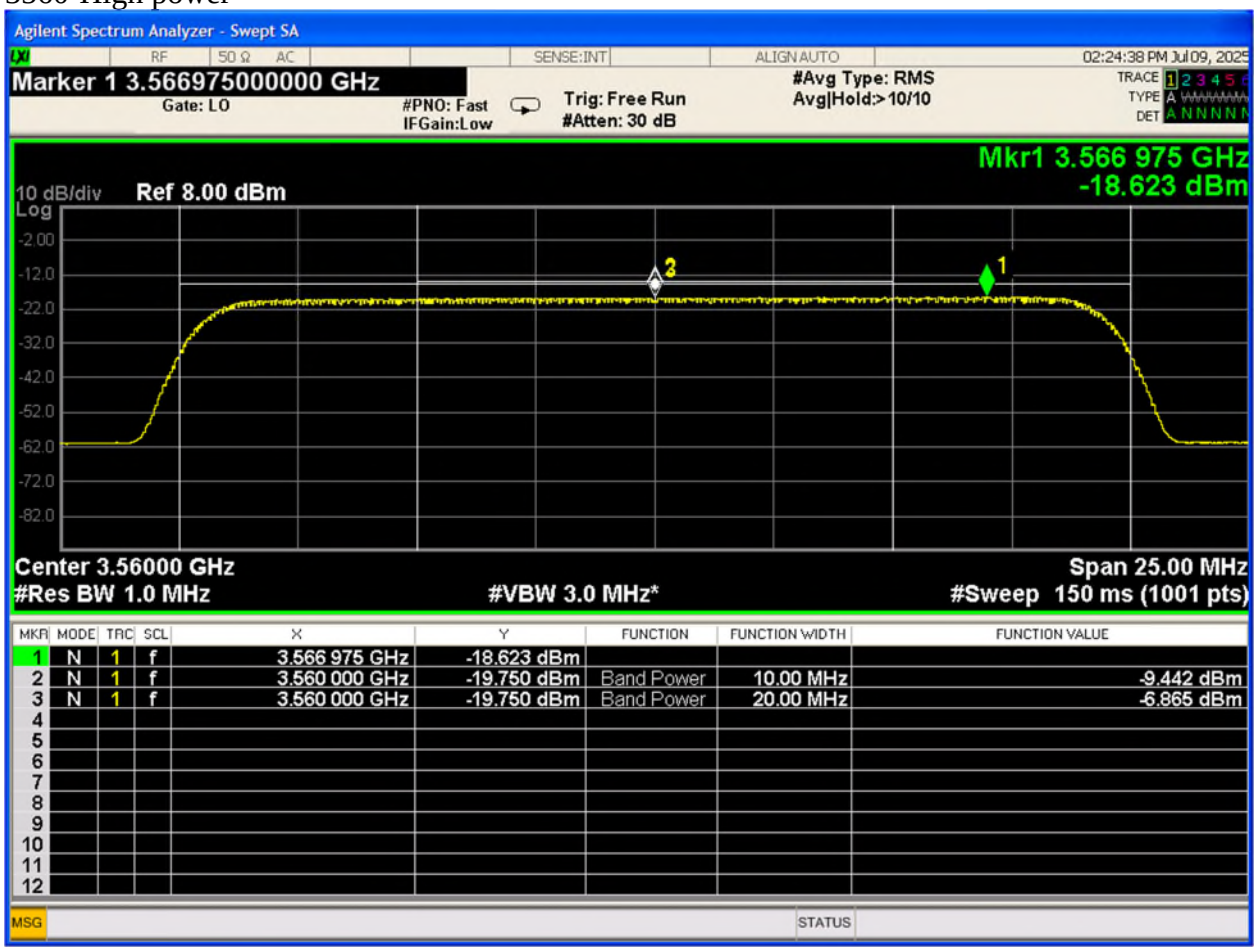
| | 10MHz EIRP limit (target) | 1MHz EIRP limit (target) | Raw Power | Raw | Raw | External Losses | Conducted | | | EIRP (Total) | EIRP 10 MHz | EIRP 1 MHz | Margin TUV SUD |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Freq | dBm | dBm | dBm | dBm/ 10 MHz | dBm/ 1 MHz | (dB) | dBm/MHz | 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 = 10log(16)dB port gain = 12.04 dB

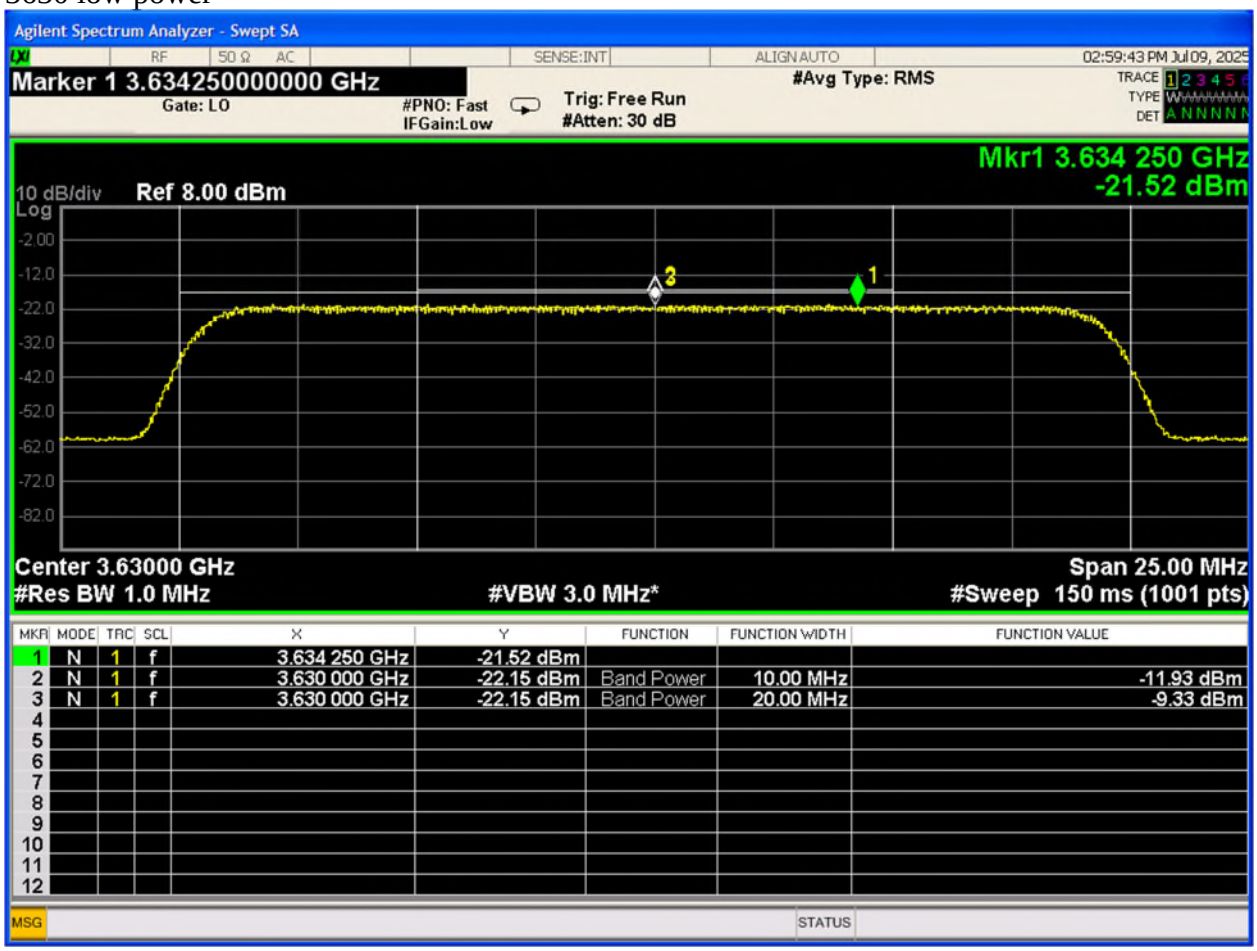
3560 low power



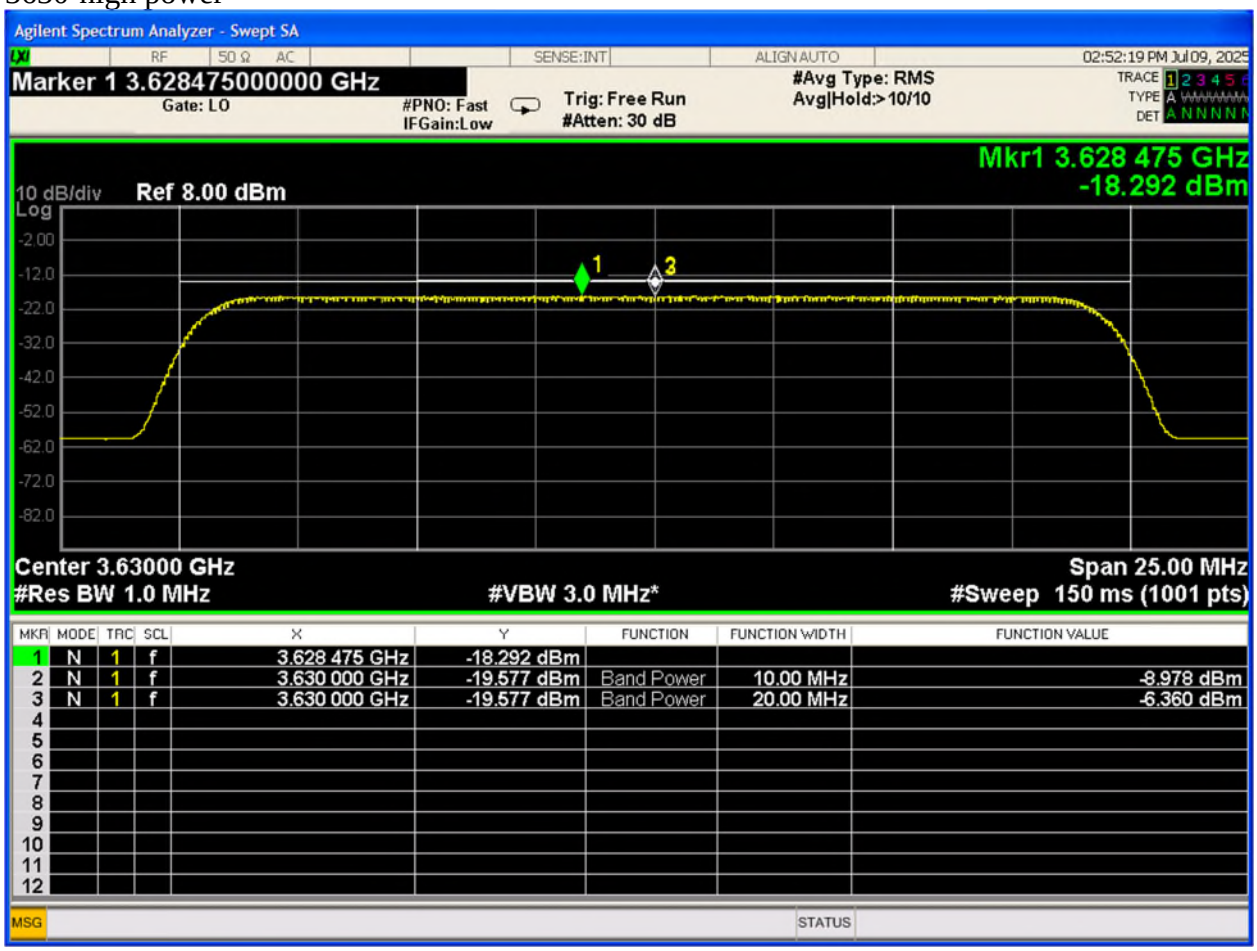
3560-High power



3630 low power

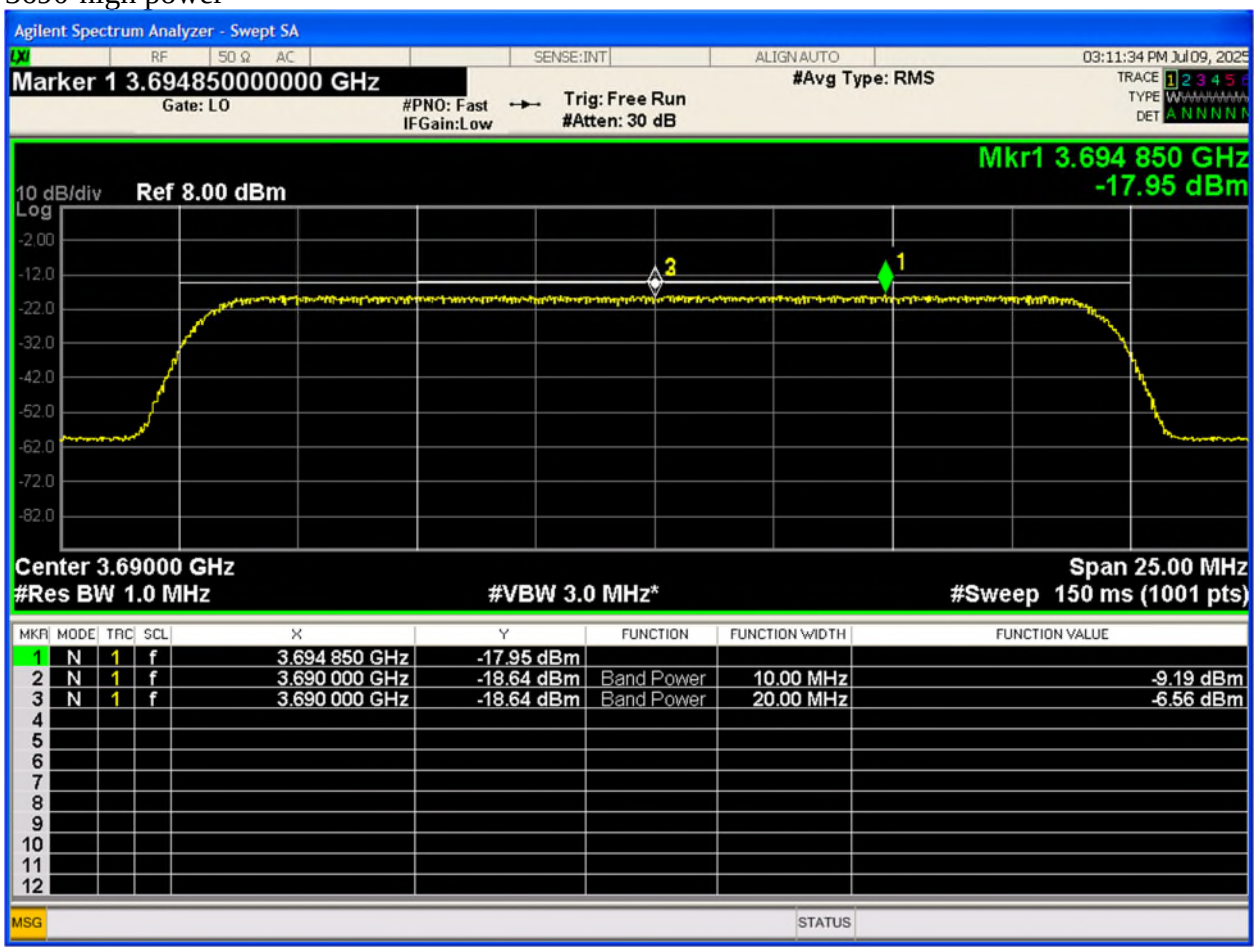


3630-high power



3690 low power

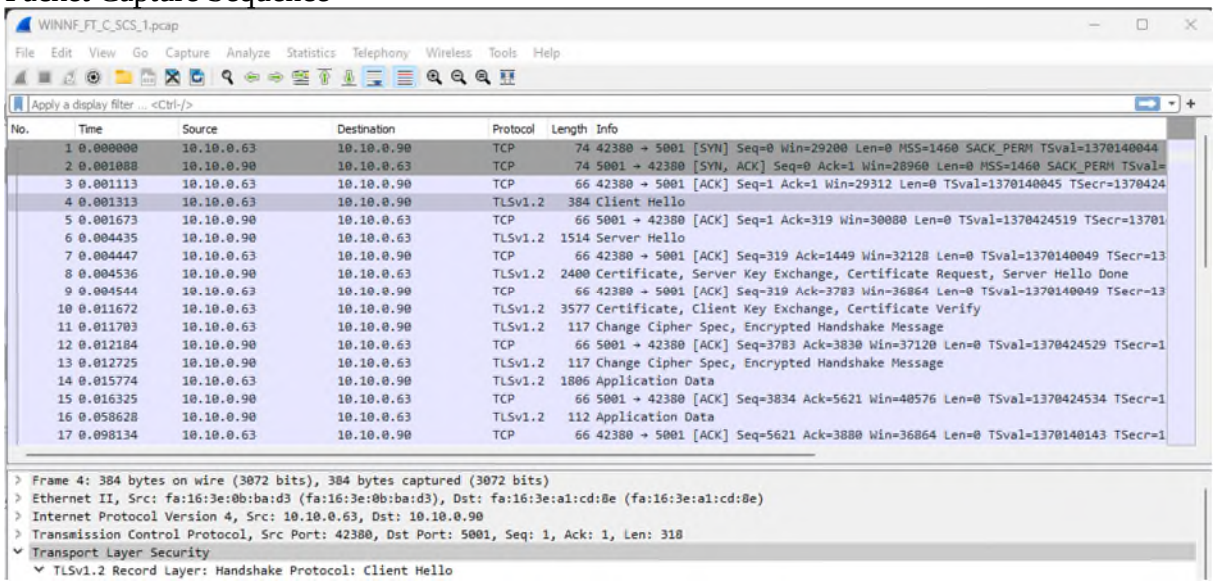
3690-high power



## *WINNF Security Test Case Analysis*

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

Packet Capture Sequence



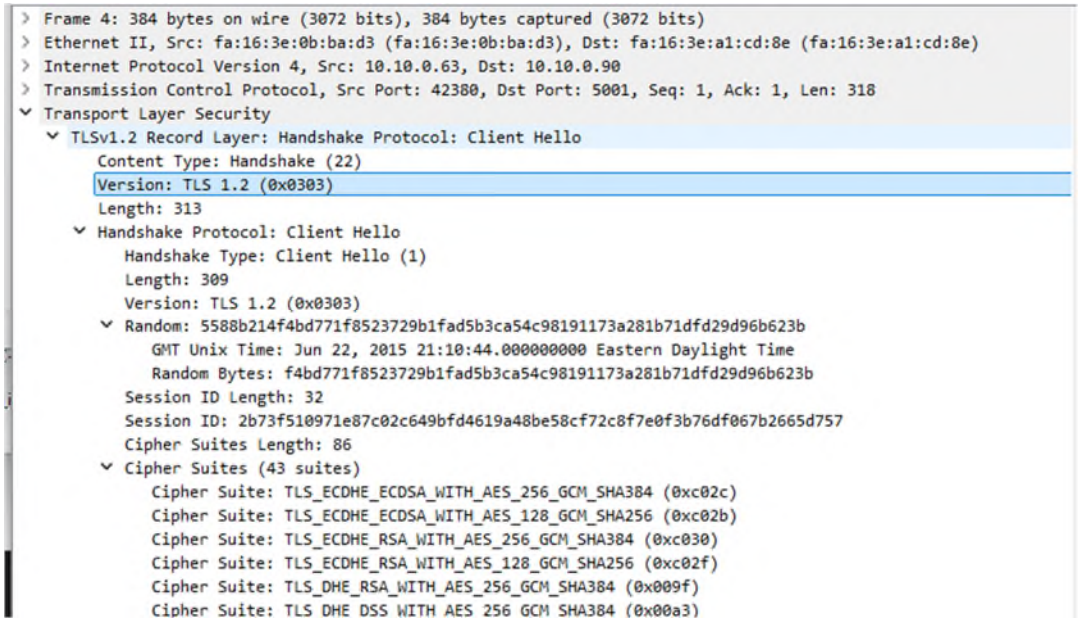

WINNF test requirements:

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

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

Analysis of WINNF Test Requirements

1. From Client Hello: TLS version = TLS 1.2



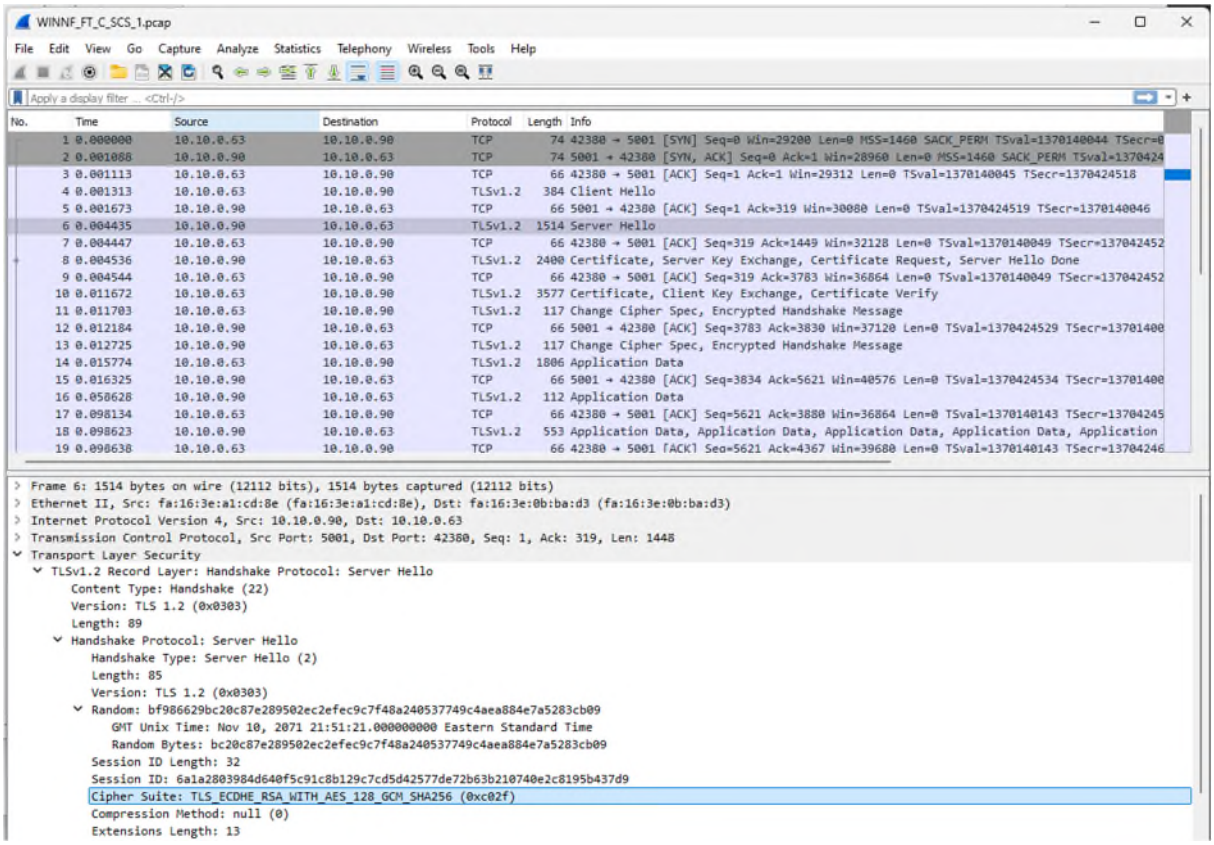

2. Cipher suite list from Client Hello is from WINNF approved list:

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

TÜV SÜD Canada

```
> 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
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 313
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 309
        Version: TLS 1.2 (0x0303)
      v 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
      v 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)
```

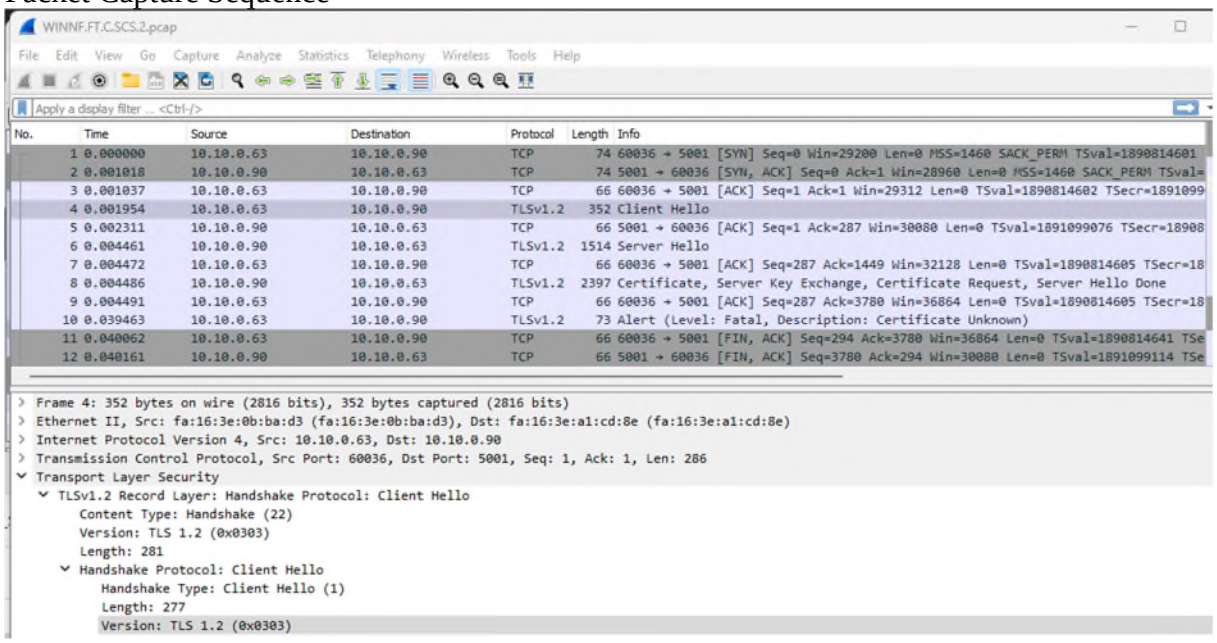
3. Cipher suite chosen (from Server Hello):
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)




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

## WINNF.FT.C.SCS.2

Packet Capture Sequence




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.<br>• Make sure UUT selects the correct cipher suite.<br>• UUT shall use CRL or OCSP to verify the validity of the server certificate.<br>• Make sure that Mutual authentication does not happen between UUT and the SAS Test Harness. | PASS | FAIL |

Analysis of WINNF Test Requirements

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

```
> Frame 4: 352 bytes on wire (2816 bits), 352 bytes captured (2816 bits)
> Ethernet II, Src: fa:16:3e: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
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 281
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 277
        Version: TLS 1.2 (0x0303)
      v Random: b3db58c69f80b340c41c8ad7295d31d25ee7332df9f07271e1d932b350801fff
          GMT Unix Time: Aug 14, 2065 13:32:54.000000000 Eastern Daylight Time
```

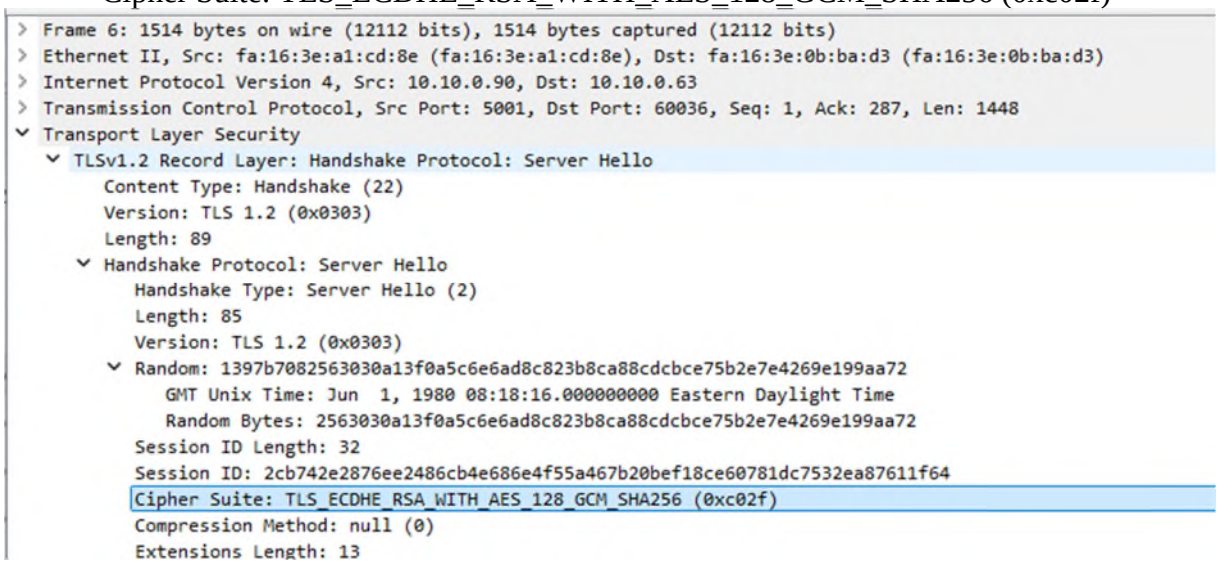
2. From Client Hello, cipher suite list is from WINNF approved list:
TLS_RSA_WITH_AES_128_GCM_SHA25
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

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

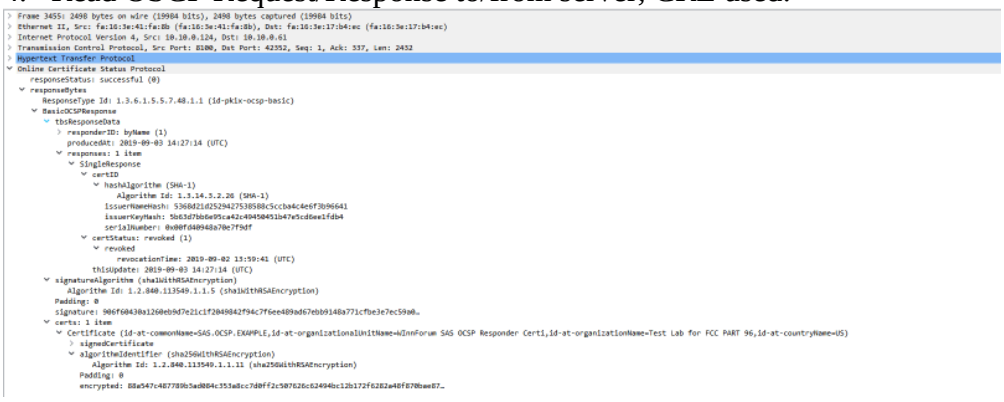
TÜV SÜD Canada

```
> 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
v Transport Layer Security
  v TLSv1.2 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 281
    v Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 277
        Version: TLS 1.2 (0x0303)
      v 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
      v 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)
```

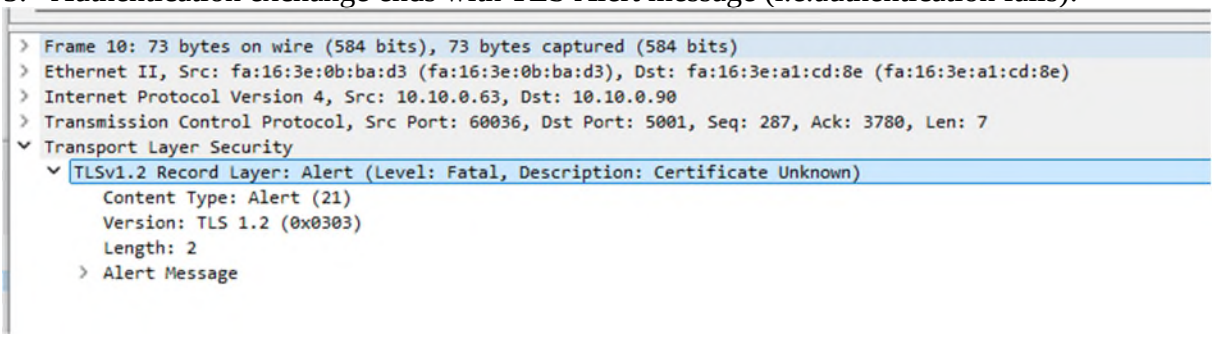
3. From Server Hello, cipher suite chosen:
   Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)




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



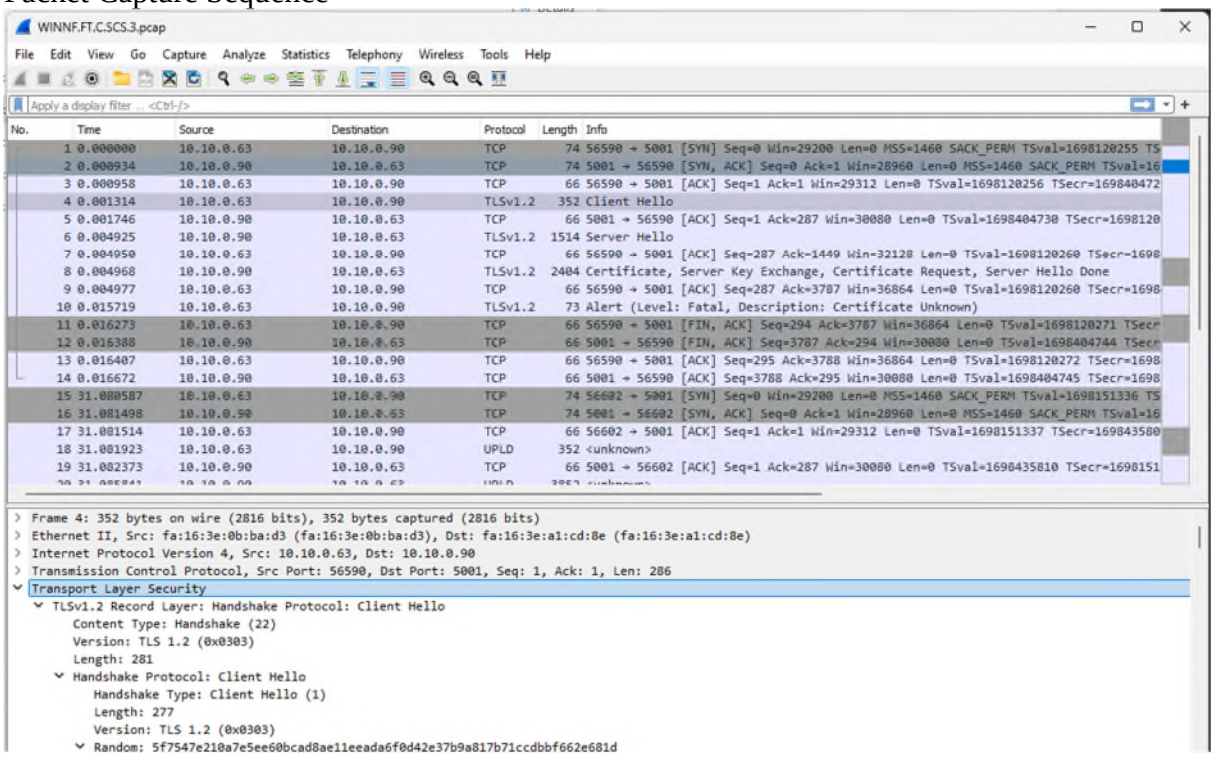
5. Authentication exchange ends with TLS Alert message (i.e.authentication fails):




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

## WINNF.FT.C.SCS.3

Packet Capture Sequence



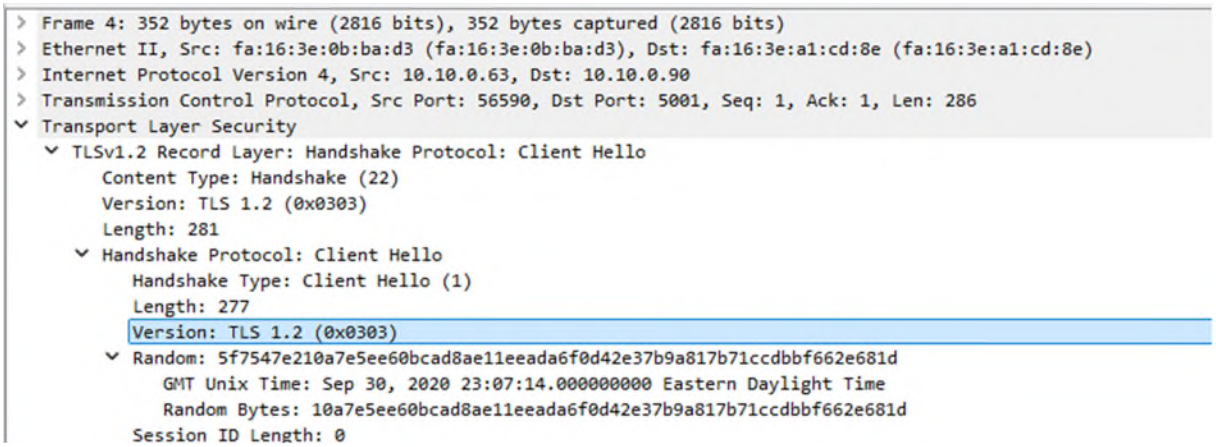

WINNF Test Requirements:

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.<br>• Make sure UUT selects the correct cipher suite.<br>• UUT shall use CRL or OCSP to verify the validity of the server certificate.<br>• Make sure that Mutual authentication does not happen between UUT and the SAS Test Harness. | PASS |

Analysis of WINNF Test Requirements

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

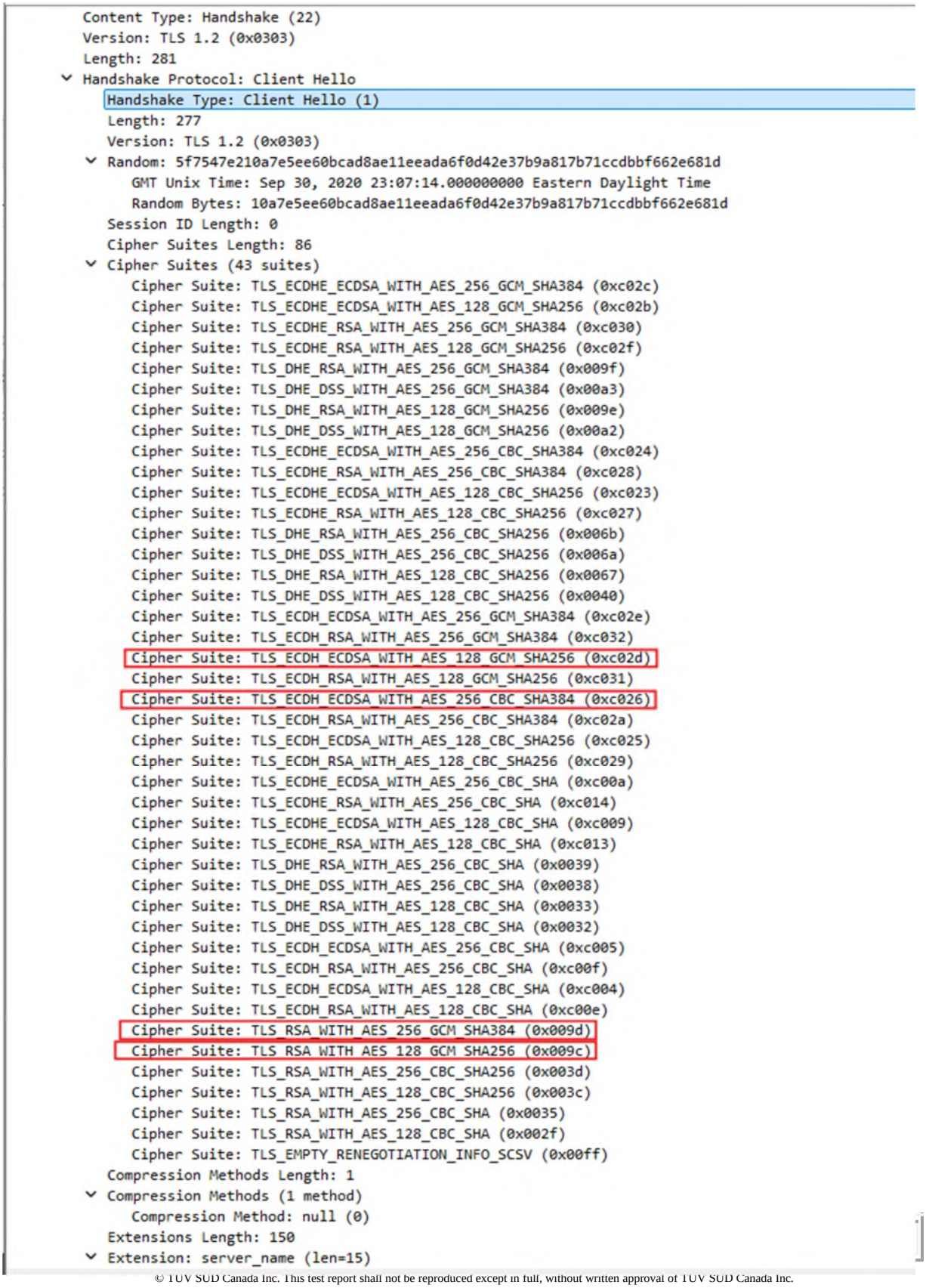



2. From Client Hello, cipher suite list is from WINNF approved list:

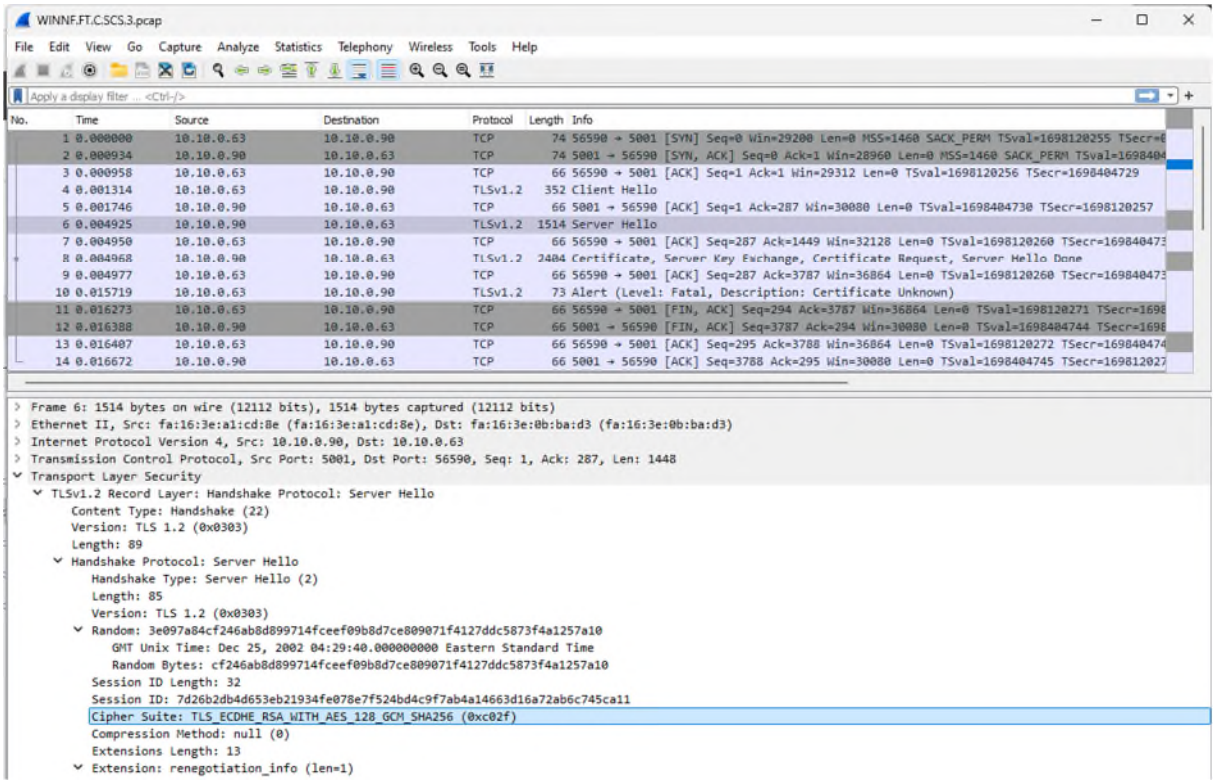
Cipher Suites

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)

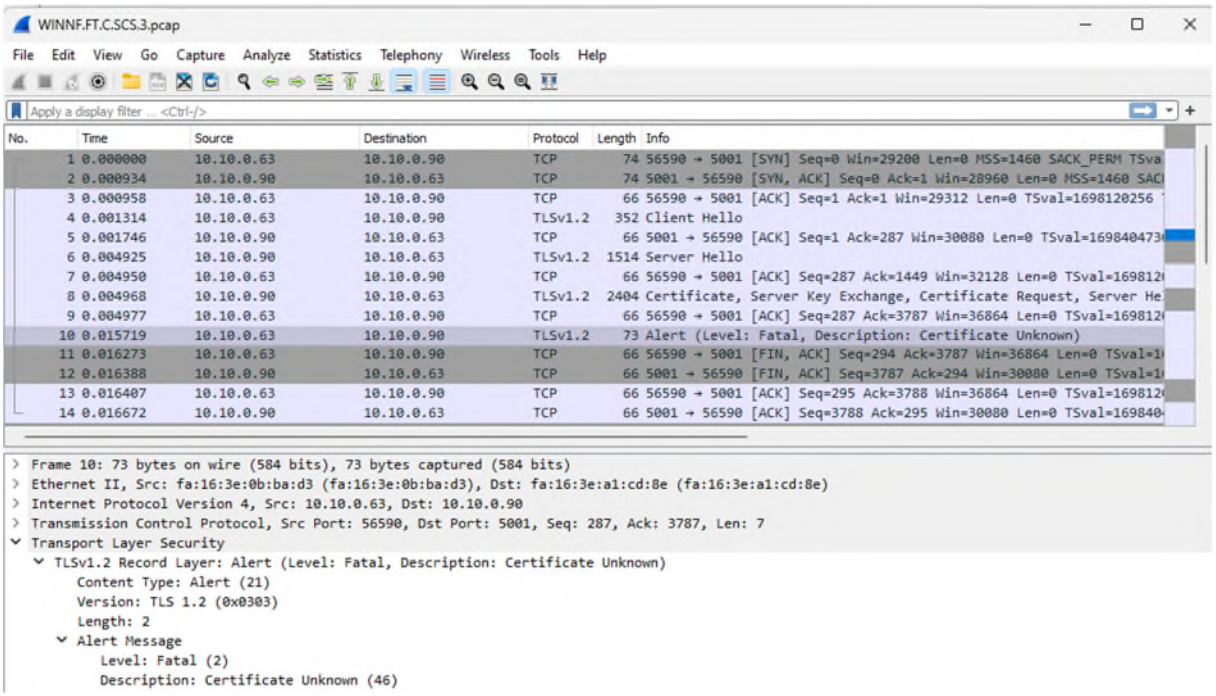
| | |
|---|---|
| Client | **Ericsson** |
| Product | **KRD 901 258 AIR 1672 B48 B77 (3550-3700MHz)** |
| Standard(s) | FCC Part 96 SAS requirements (CBRS Test Plan) |



3. From Server Hello, cipher suite chosen:
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)



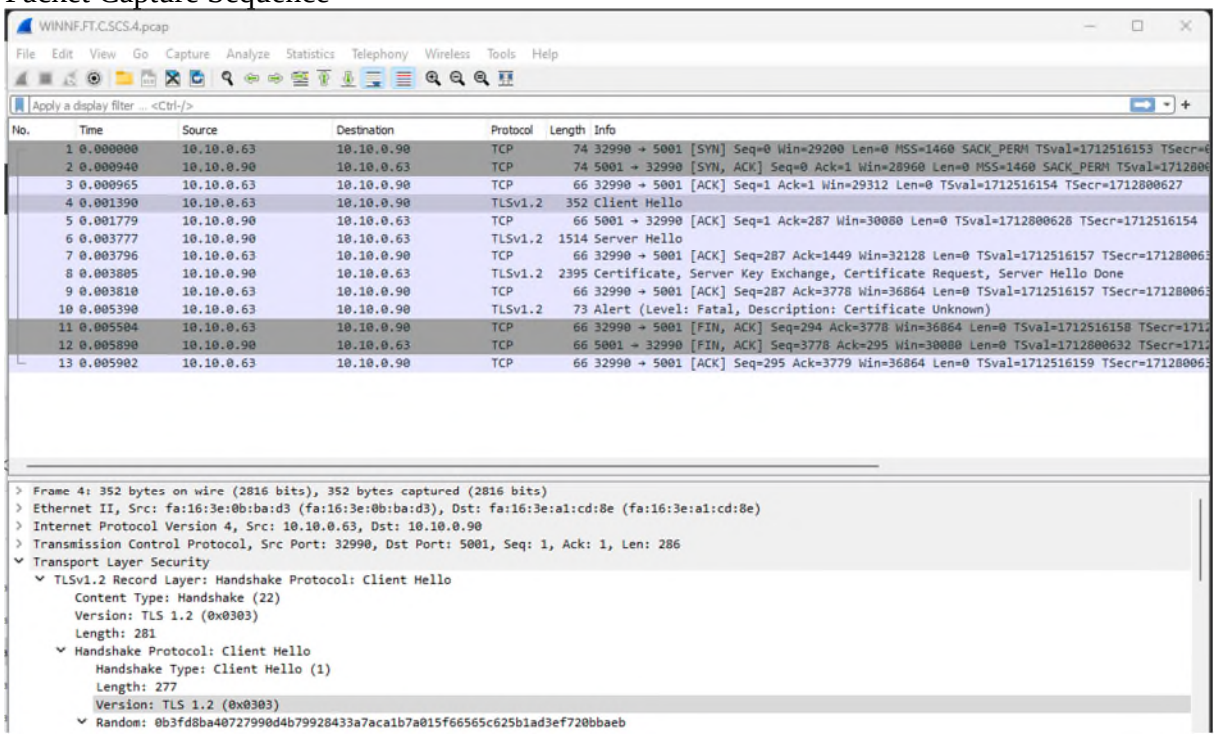

4. Authentication exchange ends with TLS Alert message (i.e. authentication fails):




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

## WINNF.FT.C.SCS.4

Packet Capture Sequence



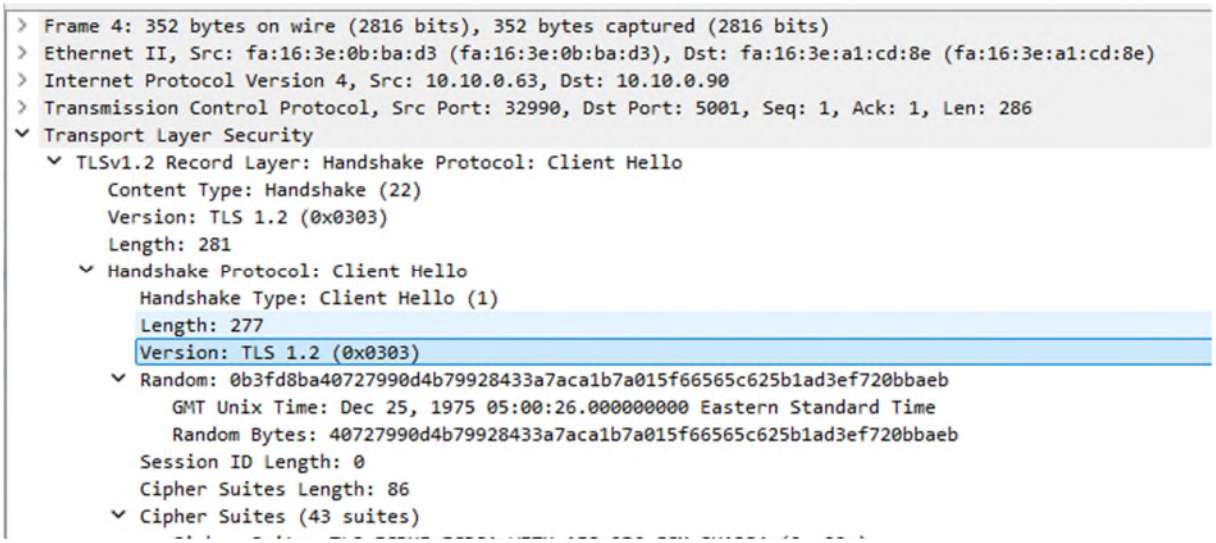

WINNF Test Requirements:

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.<br>• Make sure UUT selects the correct cipher suite.<br>• UUT shall use CRL or OCSP to verify the validity of the server certificate.<br>• Make sure that Mutual authentication does not happen between UUT and the SAS Test Harness. | PASS | FAIL |

Analysis of WINNF Test Requirements

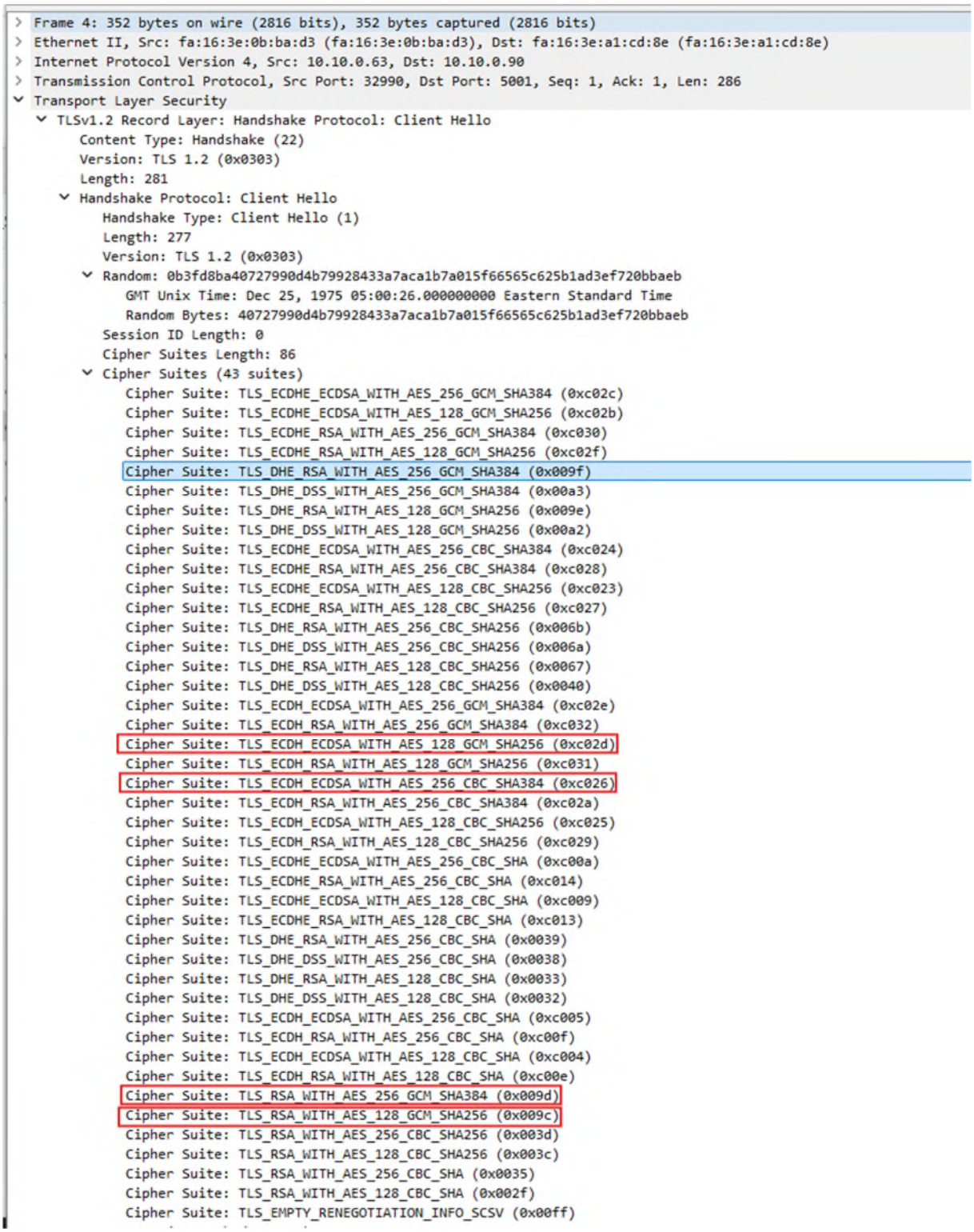
1. From Client Hello can read: TLS version = TLS 1.2



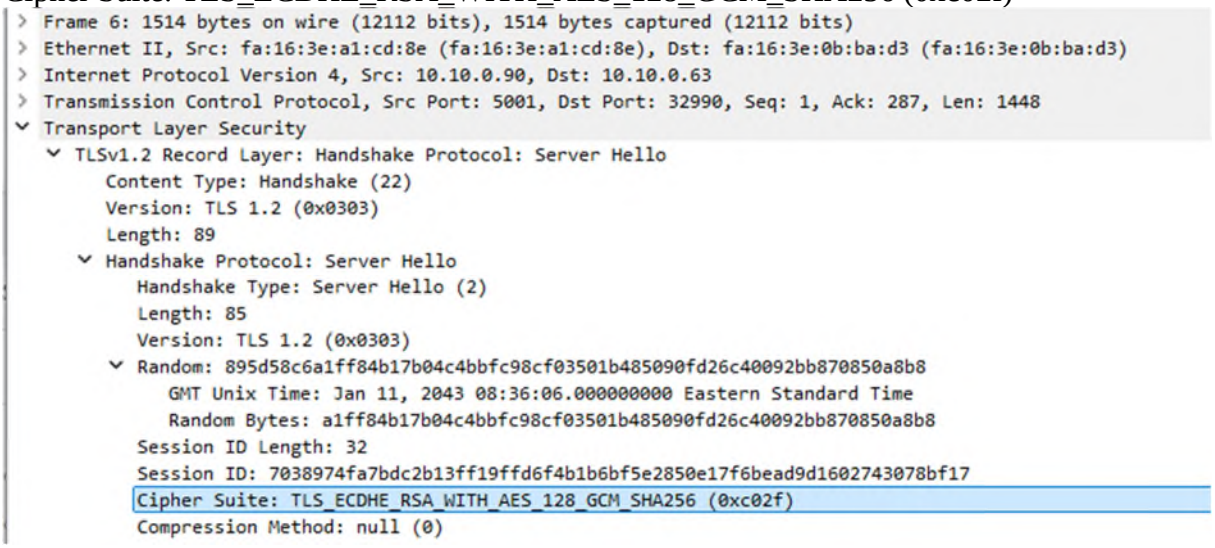

2. From Client Hello, cipher suite list is from WINNF approved list:

Cipher Suites

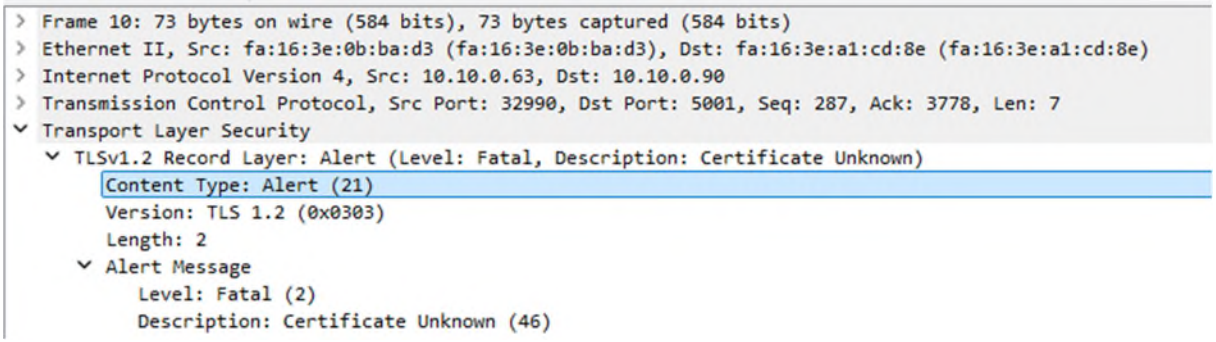
Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)
Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)
Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)



3. From Server Hello, cipher suite chosen:
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)



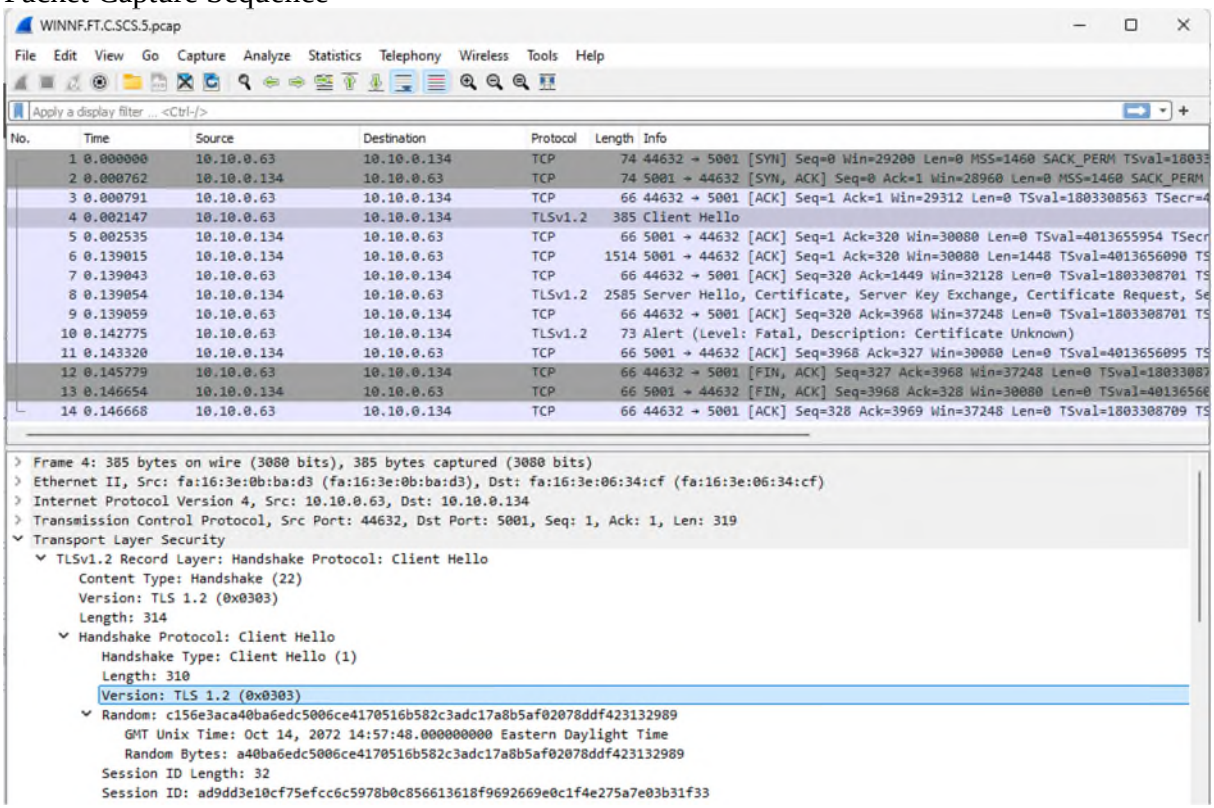

4. Authentication exchange ends with TLS Alert message (i.e. authentication fails):




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

## WINNF.FT.C.SCS.5

Packet Capture Sequence



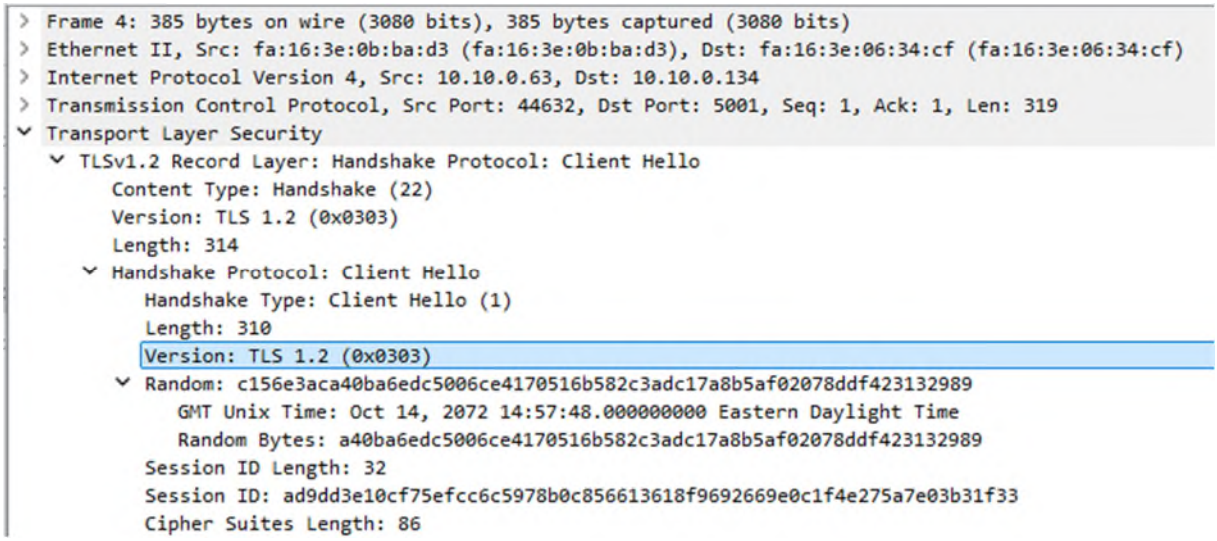

WINNF Test Requirements:

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.<br>• Make sure UUT selects the correct cipher suite.<br>• UUT shall use CRL or OCSP to verify the validity of the server certificate.<br>• Make sure that Mutual authentication does not happen between UUT and the SAS Test Harness. | PASS | FAIL |

Analysis of WINNF Test Requirements

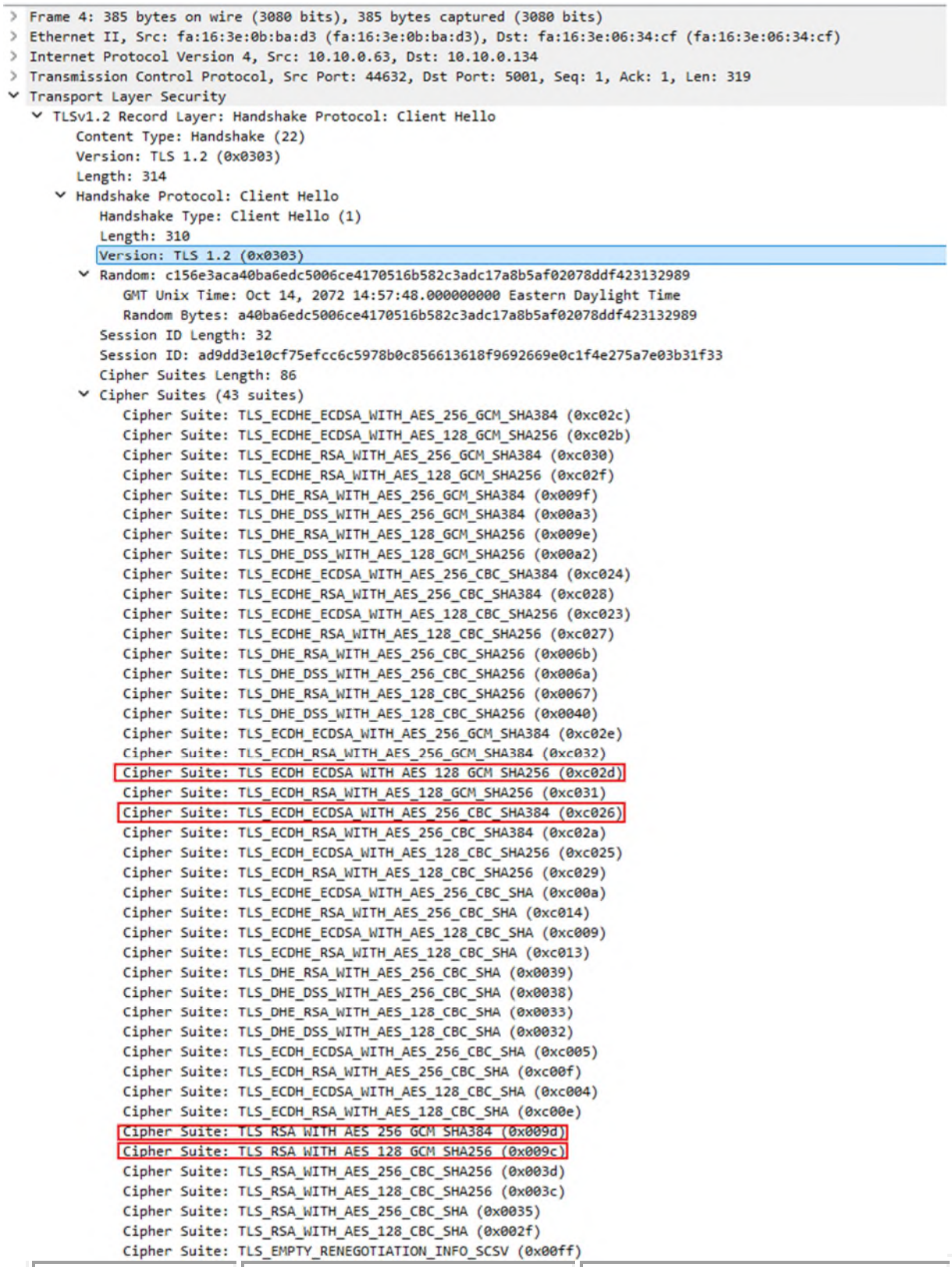
1. From Client Hello can read: TLS version = TLS 1.2



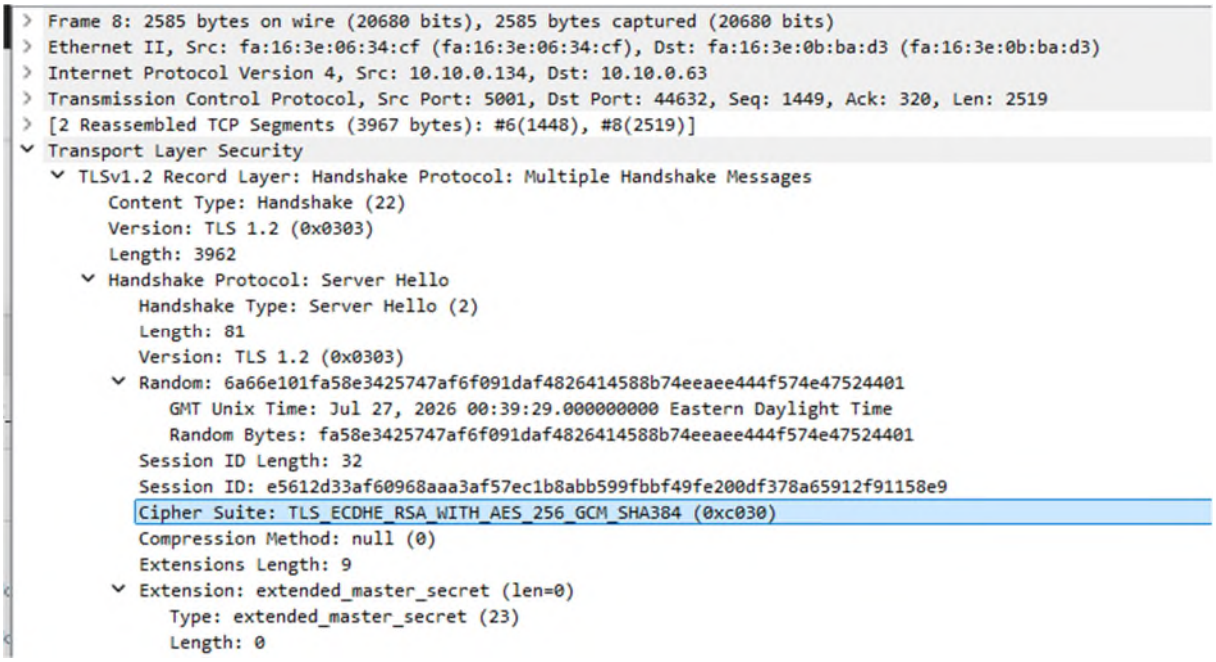

2. From Client Hello, cipher suite list is from WINNF approved list:

Cipher Suites

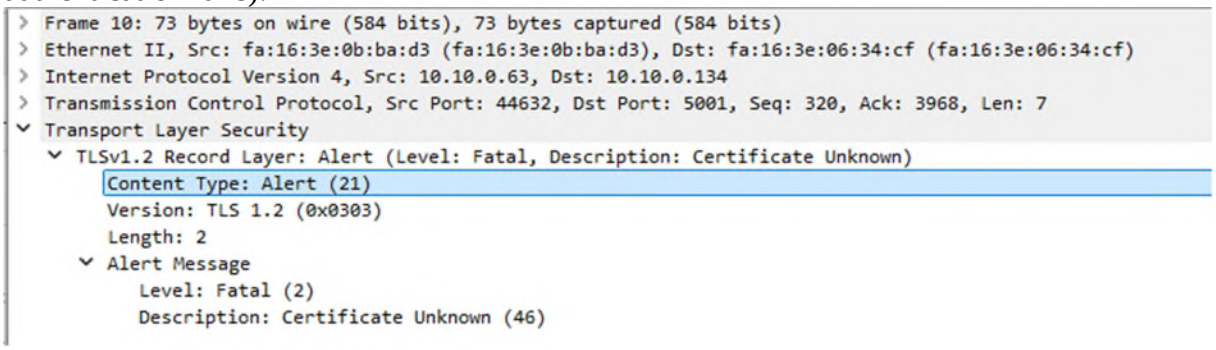
Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02d)
Cipher Suite: TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 (0xc026)
Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)



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




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




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

## *Test Equipment*

| Instrument | Manufacturer | Type No. | Serial No | Calibration Period (months) | Calibration Due |
|---|---|---|---|---|---|
| Power Supply | Xantrex | XKW 60-50 | E00109863 | O/P Mon | - |
| Signal Analyzer | Agilent | MXA | SSG013930 | 24 months | 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 | - |

# Appendix A – EUT & Client Provided Details

## General EUT Description

| | |
|---|---|
| Manufacturer | Ericsson |
| Address | Torshamnsgatan 23<br>Kista<br>SE-16480<br>Stockholm<br>Sweden |
| Product Name (for test report title) | AIR 1672 B48 B77D |
| Product Number | KRD 901 258/1 (with antenna, security unlocked)<br>KRD 901 258/11** (with antenna, security locked)<br>KRD 901 258/2* (CAB/RDNB board for testing purpose, security unlocked)<br>KRD 901 258/21 (CAB/RDNB board for testing purpose, security locked)<br>Note*: Tested unit<br>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 |

**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.

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

Test setup

<Photos kept on file>