



Wi-Fi Interoperability TEST REPORT

No. 24T04Z101045-023

for

TCL Communication Ltd.

Product Name: 9491G

Model Number: 9491G

CID: WFA131214

Wi-Fi Component Firmware: 2023-10-26-192901

Issued Date: 2024-06-17

Note:

The test results in this test report relate only to the devices specified in this report. This report shall not be reproduced except in full without the written approval of CTTL.

Test Laboratory:

CTTL-Telecommunication Technology Labs, CAICT

No. 52, Huayuan North Road, Haidian District, Beijing, P. R. China 100191.

Tel: +86(0)10-62304633-2512, Fax: +86(0)10-62304633-2504

Email: cttl_terminals@caict.ac.cn, website: www.chinattl.com



No. 24T04Z101045-023

REPORT HISTORY

Report Number	Revision	Description	Issue Date
24T04Z101045-023	Rev.0	1st edition	2024-06-17

Note: the latest revision of the test report supersedes all previous version.

CONTENTS

1. TEST LABORATORY	4
1.1. TESTING LOCATION	4
1.2. TESTING ENVIRONMENT	4
1.3. PROJECT DATA	4
1.4. SIGNATURE	4
2. CLIENT INFORMATION	5
2.1. APPLICANT INFORMATION	5
2.2. MANUFACTURER INFORMATION	5
3. EQUIPMENT UNDER TEST (EUT) AND ANCILLARY EQUIPMENT (AE)	6
3.1. ABOUT EUT	6
3.2. PRODUCT DESIGNATORS	6
3.3. PRODUCT CAPABILITIES	7
4. REFERENCE DOCUMENTS	8
4.1. DOCUMENTS SUPPLIED BY APPLICANT	8
4.2. REFERENCE DOCUMENTS FOR TESTING	8
5. TEST RESULTS	9
5.1. SUMMARY OF MEASUREMENT RESULTS	9
5.2. STATEMENTS	16
6. TEST FACILITIES UTILIZED	17
ANNEX A: EUT PHOTOGRAPH	18
ANNEX B: EUT PARAMETERS	18
B.1. MEASUREMENT METHOD	19
B.2 MEASUREMENT RESULT	20
ANNEX C: TEST LAYOUT	33
ANNEX D: ACCREDITATION CERTIFICATE	34

1. Test Laboratory

1.1. Testing Location

Location 1: CTTL(CuiHu)

Address: CuiHu Cloud Center, No. 1 Gaolizhang Road, Wenquan
Town, Haidian District, Beijing, China

1.2. Testing Environment

Normal Temperature: 20-22℃

Relative Humidity: 40-60%

1.3. Project data

Testing Start Date: 2024-05-21

Testing End Date: 2024-06-17

1.4. Signature



Zhen Bowei
(Prepared this test report)



Xie Fangfang
(Reviewed this test report)



Hu Xiaoyu
(Approved this test report)

2. Client Information

2.1. Applicant Information

Company Name: TCL Communication Ltd.
Address /Post: 5/F, Building 22E, 22 Science Park East Avenue, Hong Kong Science
Park, Shatin, NT, Hong Kong
City: /
Postal Code: /
Country: /
Contact: Annie Jiang
Email: nianxiang.jiang@tcl.com
Telephone: +86 755 3661 1621
Fax: +86 755 3661 2000-81722

2.2. Manufacturer Information

Company Name: TCL Communication Ltd.
Address /Post: 5/F, Building 22E, 22 Science Park East Avenue, Hong Kong Science
Park, Shatin, NT, Hong Kong
City: /
Postal Code: /
Country: /
Contact: Annie Jiang
Email: nianxiang.jiang@tcl.com
Telephone: +86 755 3661 1621
Fax: +86 755 3661 2000-81722

3. Equipment Under Test (EUT) and Ancillary Equipment (AE)

3.1. About EUT

Series Number	E88F6F7EE43D
CID	WFA131214
Product Name	9491G
Model Number	9491G
Wi-Fi Component Firmware Version	2023-10-26-192901
Wireless Chipset	MT6631N/B
Operating System	Android
OS Version	Android

Note: Photographs of EUT are shown in ANNEX A of this test report.

3.2. Product Designators

Device Type	Enterprise
Product Type	STA
Primary Product Category	Tablet (Wi-Fi and other)
Additional Category of Product	N/A
Does this product want be designate as a Source	Yes
Is this product an Application Specific Device	No
Does this product support Wi-Fi Test Suite	Yes
Is 802.11a Device:	Yes
Is 802.11b Device:	Yes
Is 802.11g Device:	Yes
Is 802.11n Device:	Yes
Is 802.11ac Device:	Yes
Is 802.11ax Device:	No
Spatial Streams	

Band	Transmit	Receive
2.4GHz	1	1
5GHz	1	1

*EUT ID: is used to identify the test sample in the lab internally.

3.3. Product Capabilities

No	Item	Product Capability Description	Value
1	WPA2	Open Security	Yes
		WPA2™ - Personal	Yes
		WPA2™ - Enterprise	Yes
		WPA/WPA2-Personal	Yes
		WPA/WPA2-Enterprise	Yes
		WEP	Yes
		Pre-Authentication	No
		EAP-TLS	Yes
		EAP-TTLS/MSCHAPv2	Yes
		EAP-PEAPv0/EAP-MSCHAPv2	Yes
		EAP-PEAPv1/EAP-GTC	Yes
		EAP-SIM	Yes
		EAP-FAST MSCHAPv2	No
		EAP-FAST GTC	No
		EAP-AKA	Yes
		EAP-AKA Prime	Yes
2	Spectrum	802.11h	No
3	WMM	WMM supported	Yes
4	11n	Short Guard Interval - 20 MHz (2.4 GHz)	Yes
		Short Guard Interval - 40 MHz (2.4 GHz)	No
		Short Guard Interval - 20 MHz (5 GHz)	Yes
		Short Guard Interval - 40 MHz (5 GHz)	Yes
		STBC Receive (2.4 GHz)	Yes
		STBC Receive (5 GHz)	Yes
		STBC Rx- support 1ss or can be configured to 1ss?	Yes
		Tx A-MPDU (2.4 GHz)	Yes
		Tx A-MPDU (5 GHz)	Yes
		HT Duplicate (MCS 32) (2.4 GHz)	Yes
		HT Duplicate (MCS 32) (5 GHz)	Yes
		40 MHz operation in 2.4 GHz, with coexistence mechanisms	No
		40 MHz operation in 5 GHz	Yes
		OBSS on Extension Channel	Yes
		STAUT Power Management	No

Note: The test samples listed above were selected and prepared by the applicant.

4. Reference Documents

4.1. Documents supplied by applicant

EUT feature information is supplied by the applicant or manufacturer, which is the basis of testing.

4.2. Reference Documents for testing

The following documents listed in this section are referred for testing.

Wi-Fi CERTIFIED n System Interoperability Test Plan v2.21

Wi-Fi CERTIFIED WPA2 Test Plan v1.18

5. Test Results

5.1. Summary of Measurement Results

No	Standard Sub-clause	Test Cases	Verdict
1	Configurability of Tests	Clause 5.1.1	P
2	AP & STA Association & Throughput, Honoring NAV	Clause 5.2.3	P
3	Mixed 802.11b/g Interoperability STA Testing	Clause 5.2.5	P
4	AP & STA Association & Throughput with Replay Counter Processing	Clause 5.2.11	P
5	Group Traffic Transmission/Reception with WPA/WPA2-PSK Mixed Mode	Clause 5.2.14	P
6	802.11h Testing - Spectrum Management Bit	Clause 5.2.22	NA
7	802.11h Testing - Channel Switch Test	Clause 5.2.23	NA
8	Roaming Test for Single & Dual Band STAs with WPA-PSK	Clause 5.2.26	P
9	Traffic Differentiation in Single BSS with 802.11n STA	Clause 5.2.27	P
10	Traffic Differentiation in Single BSS with 2 802.11n STAs	Clause 5.2.28	P
11	Traffic Differentiation in Single BSS with WMM STA	Clause 5.2.29	P
12	Traffic Differentiation in Single BSS with Legacy non-WMM STA	Clause 5.2.30	P
13	Test ACM Bit Conformance	Clause 5.2.31	P
14	Test the AC Parameter Modification	Clause 5.2.32	P
15	TXOP Limit Test	Clause 5.2.33	P
16	Basic Association in 802.11n Environment	Clause 5.2.35	P
17	Ability to Receive 1 and 2 Spatial Streams	Clause 5.2.36	P
18	A-MPDU Aggregation when the STA is the Recipient with and without WPA2-PSK	Clause 5.2.37	P
19	A-MSDU Aggregation when the STA is the Recipient	Clause 5.2.38	P
20	Overlapping BSS – 2.4 GHz	Clause 5.2.39	P
21	Overlapping BSS – 5 GHz	Clause 5.2.40	P
22	Short GI Operation	Clause 5.2.42	P
23	Overlapping BSS on the Extension Channel	Clause 5.2.43	P
24	HT Duplicate Mode (MCS Index = 32)	Clause 5.2.44	P
25	STBC Receive Test	Clause 5.2.46	P
26	A-MPDU Aggregation when the STA is the Transmitter	Clause 5.2.47	P
27	STA 20/40 MHz Coexistence	Clause 5.2.48	NA
28	STAUT Transmitting to AP using Supported Number of Spatial Streams	Clause 5.2.50	P

No	Standard Sub-clause	Test Cases	Verdict
WPA2-Personal STA tests			
29	STAUT user interface verification test	Clause 5.1	P
30	STAUT handles RSNE unexpected values test	Clause 5.2.1	NA
31	STAUT verification of RSN Capabilities test	Clause 5.2.2	NA
32	STAUT RSNE bounds verification test	Clause 5.2.3	NA
33	This test case verifies that the STAUT does not use HT/VHT/HE rates when using WEP40 as the encryption cipher	CT_Security_WEP-PHY_STA_Disallow-HT_10110_1 [6]	P
34	This test verifies that the STAUT does not use HT/VHT/HE rates when using TKIP as the encryption cipher	CT_Security_WPAPersonal-PHY_STA_Disallow-HT_10112_2 [6]	P
35	This test verifies that the STAUT configured with WPA2-Personal associates with an AP configured with WPA2-Personal	CT_Security_WPA2Personal_STA_Association_WPA2Personal_10332_1 [6]	P
36	This test verifies that the STAUT configured with WPA2-Personal does not associate with an AP configured with no security (open mode)	CT_Security_WPA2Personal_STA_NoAssociation_NoSecurityMode_10153_1 [6]	P
37	This test verifies that the STAUT configured with WPA2-Personal does not associate with an AP configured with WEP	CT_Security_WPA2Personal_STA_NoAssociation_WEP_10160_1 [6]	P
38	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	CT_Security_WPA2Personal_STA_RSNEBoundsVerification-AbsentGrpMgmtCipher_10275_1 [6]	P
39	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	CT_Security_WPA2Personal_STA_RSNEBoundsVerification-AbsentPMKIDCount_10274_1 [6]	P
40	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	CT_Security_WPA2Personal_STA_RSNEBoundsVerification-AbsentRSNCap_10273_1 [6]	P
41	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	CT_Security_WPA2Personal_STA_RSNEBoundsVerification-AllOptional_10276_1 [6]	P
42	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	CT_Security_WPA2Personal_STA_RSNEBoundsVerification-FTPSKAKM_10280_1 [6]	P

No	Standard Sub-clause	Test Cases	Verdict
43	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	CT_Security_WPA2Personal_STA_RSNEBoundsVerification-MultiAKM_10278_1 [6]	P
44	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	CT_Security_WPA2Personal_STA_RSNEBoundsVerification-UndefElem_10277_1 [6]	P
45	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	CT_Security_WPA2Personal_STA_RSNEBoundsVerification-UnknownAKM_10279_1 [6]	P
46	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	CT_Security_WPA2Personal_STA_UnexpectedRSNEIncompleteAKM_10323_1 [6]	P
47	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	CT_Security_WPA2Personal_STA_UnexpectedRSNEIncompletePairwise_10322_1 [6]	P
48	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	CT_Security_WPA2Personal_STA_UnexpectedRSNENoAKM_10315_1 [6]	P
49	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	CT_Security_WPA2Personal_STA_UnexpectedRSNENoPairwise_10314_1 [6]	P
50	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	CT_Security_WPA2Personal_STA_UnexpectedRSNENoPairwiseAKM_10316_1 [6]	P

No	Standard Sub-clause	Test Cases	Verdict
51	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	CT_Security_WPA2Personal_STA_UnexpectedRSNE_PMKIDPresent_10324_1 [6]	P
52	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	CT_Security_WPA2Personal_STA_UnexpectedRSNE_RSNProtoVer_10313_1 [6]	P
53	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	CT_Security_WPA2Personal_STA_UnexpectedRSNE_TruncatedAKM_10319_1 [6]	P
54	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	CT_Security_WPA2Personal_STA_UnexpectedRSNE_TruncatedGrpCipher_10317_1 [6]	P
55	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	CT_Security_WPA2Personal_STA_UnexpectedRSNE_TruncatedPairwise_10318_1 [6]	P
56	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	CT_Security_WPA2Personal_STA_UnexpectedRSNE_TruncatedPMKID_10321_1 [6]	P
57	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	CT_Security_WPA2Personal_STA_UnexpectedRSNE_TruncatedRSNCap_10320_1 [6]	P
58	This test verifies that the STAUT successfully associates, authenticates and passes data traffic when reserved bit 15 in the RSN Capabilities field is set to one instead of zero	CT_Security_WPA2Personal_STA_RSNCapabilitiesVerification-ReservedBit-15_10485_1 [6]	P

No	Standard Sub-clause	Test Cases	Verdict
59	This test verifies that the STAUT does not set optional feature bits to one in the RSN Capabilities field on transmission when unsupported and ignores them on reception	CT_Security_WPA2Personal_STA_RSNCapabilitiesVerification-OptionalBits_10486_2 [6]	P
60	This test verifies that the STAUT configured with WPA2-Personal Mixed Mode associates with an AP configured with WPA2-Personal	CT_Security_WPA2PersonalMixedMode_STA_Association-WPA2Personal_10058_1 [6]	P
61	This test verifies that the STAUT configured with WPA/WPA2-Personal mixed mode associates with an AP configured with WPA2-Personal Mixed Mode	CT_Security_WPA2PersonalMixedMode_STA_Association_WPA2PersonalMixedMode_10061_1 [6]	P
62	This test verifies that the STAUT configured with WPA2-Personal Mixed Mode associates with an AP configured with WPA-Personal	CT_Security_WPA2PersonalMixedMode_STA_Association-WPA2Personal_10064_1 [6]	P
WPA2-Enterprise STA tests			
63	STAUT Pre-authentication test	Clause 5.3.1	NA
64	STAUT PMK Caching test	Clause 5.3.2	P
65	STAUT Multiple authentication servers test	Clause 5.3.3.1_HostapdServer	P
66	STAUT Multiple authentication servers test	Clause 5.3.3.1_MicrosoftServer	P
67	STAUT Multiple authentication servers test	Clause 5.3.3.1_RadiatorServer	P
68	STAUT Expired server certificate test	Clause 5.3.3.2	P
69	STAUT EAP SIM IMSI not contained within the AS Database test	Clause 5.3.3.3	P
70	STAUT EAP AKA Sequence number resynchronization test	Clause 5.3.3.4	P
71	STAUT No USIM record for EAP AKA test	Clause 5.3.3.5	P
72	STAUT Protected success indication and EAP AKA fast reconnect using roaming test	Clause 5.3.3.6	P
73	STAUT Authenticated provisioning and EAP FAST-GTC inner authentication test	Clause 5.3.3.7	NA
74	STAUT Authenticated provisioning and EAP FAST-MSCHAPv2 inner authentication test	Clause 5.3.3.8	NA
75	STAUT EAP AKA' incorrect username prefix test	Clause 5.3.3.9	P
76	STAUT RSNE bounds verification test	Clause 5.3.4	NA

No	Standard Sub-clause	Test Cases	Verdict
77	STAUT unknown Root CA detection test	Clause 5.3.5	NA
78	This test verifies that the STAUT associates with an AP when both devices are configured with WPA2-Enterprise with EAP AKA	CT_Security_EAP-AKA_STA_EAP-AKA_10118_1 [6]	P
79	This test verifies that the STAUT associates with an AP when both devices are configured with WPA2-Enterprise with EAP AKA'	CT_Security_EAP-AKA'_STA_EAP-AKA'_10119_1 [6]	P
80	This test verifies that the STAUT associates with an AP when both devices are configured with WPA2-Enterprise with EAP FAST-GTC	CT_Security_EAP-FAST-GTC_STA_EAP-FAST-GTC_10120_1 [6]	NA
81	This test verifies that the STAUT associates with an AP when both devices are configured with WPA2-Enterprise with EAP FAST-MSCHAPv2	CT_Security_EAP-FAST-MSCHAPv2_STA_EAP-FAST-MSCHAPv2_10121_1 [6]	NA
82	This test verifies that the STAUT associates with an AP when both devices are configured with WPA2-Enterprise with PEAPv0	CT_Security_EAP-PEAPv0_STA_EAP-PEAPv0_10122_1 [6]	P
83	This test verifies that the STAUT associates with an AP when both devices are configured with WPA2-Enterprise with PEAPv1	CT_Security_EAP-PEAPv1_STA_EAP-PEAPv1_10124_1 [6]	P
84	This test verifies that the STAUT associates with an AP when both devices are configured with WPA2-Enterprise with EAP SIM	CT_Security_EAP-SIM_STA_EAP-SIM_10470_1 [6]	P
85	This test verifies that the STAUT associates with an AP when both devices are configured with WPA2-Enterprise with EAP TLS	CT_Security_EAP-TLS_STA_EAP-TLS_10126_1 [6]	P
86	This test verifies that the STAUT associates with an AP when both devices are configured with WPA2-Enterprise with EAP TTLS	CT_Security_EAP-TTLS_STA_EAP-TTLS_10128_1 [6]	P
87	This test verifies that the STAUT correctly performs server certificate validation during an EAP exchange	CT_Security_SCV_STA_WPA2ServerCertificateValidation_10334_1 [6]	P
88	This test verifies that the STAUT configured with WPA2-Enterprise does not associate with an AP configured with WPA2-Personal	CT_Security_WPA2Enterprise_STA_NoAssociation-WPA2Personal_10166_1 [6]	P
89	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	CT_Security_WPA2Enterprise_STA_RSNEBoundsVerificationAbsentAKMSuite_10260_1 [6]	P

No	Standard Sub-clause	Test Cases	Verdict
90	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	CT_Security_WPA2Enterprise_STA_RSNEBoundsVerification AbsentGrpCipher_10258_1 [6]	P
91	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	CT_Security_WPA2Enterprise_STA_RSNEBoundsVerification AbsentGrpMgmtCipher_10263_1 [6]	P
92	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	CT_Security_WPA2Enterprise_STA_RSNEBoundsVerification AbsentPairwise_10259_1 [6]	P
93	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	CT_Security_WPA2Enterprise_STA_RSNEBoundsVerification AbsentPMKIDCount_10262_1 [6]	P
94	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	CT_Security_WPA2Enterprise_STA_RSNEBoundsVerification AbsentRSNCap_10261_1 [6]	P
95	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	CT_Security_WPA2Enterprise_STA_RSNEBoundsVerification AllOptional_10264_1 [6]	P
96	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	CT_Security_WPA2Enterprise_STA_RSNEBoundsVerification MultiPairwiseAKM_10266_1 [6]	P
97	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	CT_Security_WPA2Enterprise_STA_RSNEBoundsVerification UndefElem_10265_1 [6]	P
98	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	CT_Security_WPA2Enterprise_STA_UnexpectedRSNE-AbsentPMKID_10298_1 [6]	P

No	Standard Sub-clause	Test Cases	Verdict
99	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	CT_Security_WPA2Enterprise_STA_UnexpectedRSNE-InvalidPMKID_10297_1 [6]	P

Please refer to **ANNEX B2** for details. Terms used in Verdict column

P	Pass, The EUT complies with the essential requirements in the standard.
NA	Not Applicable, The test was not applicable
F	Fail, The EUT does not comply with the essential requirements in the standard

5.2. Statements

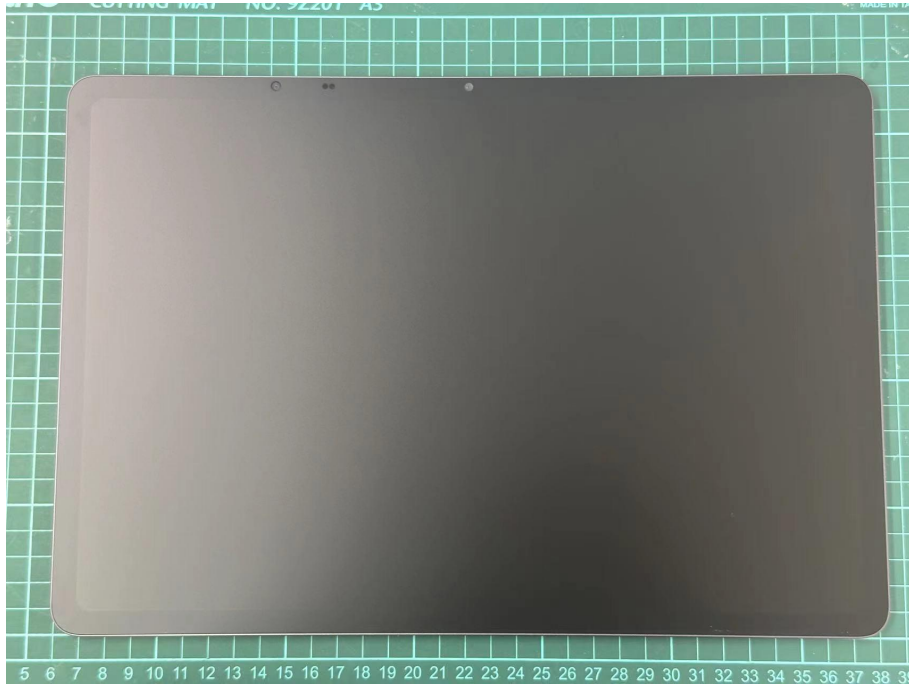
The test cases as listed in section 5.1 of this report for the EUT specified in section 3 was performed by CTTL according to the standards or reference documents listed in section 4.2

The EUT met all requirements of the standards or reference documents, and only the WLAN function was tested.

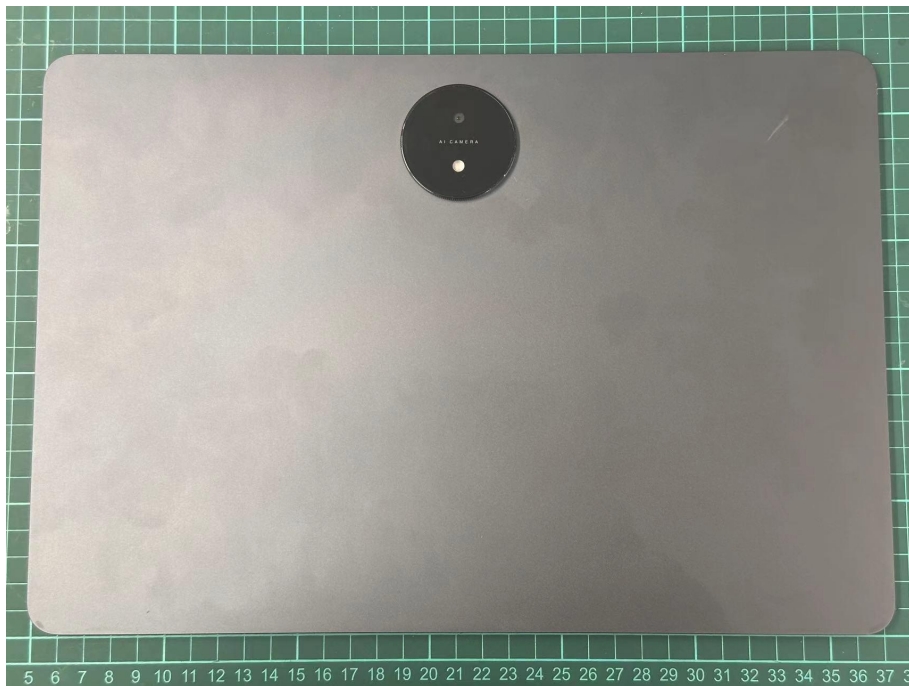
6. Test Facilities Utilized

No.	Equipment	Model	Version	Manufacturer	Serial No.
1	Realtek 802.11n Card	RTL8812BU	WTS-10.9.1222.20 16Driver-1030.14.9 20.2016 Windows 10 64-bit	Realtek	/
2	Broadcom 802.11a/b/g/n Card	BCM94360MC_1	6.30.190.17 Wi-Fi Test Suite version: 1.139.1	Broadcom	/
3	Intel 802.11a/b/g/n MiniPCI Express	AX210.NGWG.NV (Linux)	WTS-1.0.15-6r2 Linux_Core_build_ 19147:211d325039 d6- 65.1eed1396.0	Intel	/
4	Marvell 802.11a/b/g/n Card	RDW8997P-WF-S0	WTS-11N(20:56:54 Jun232020),11N Tested 1.05a Driver - PCIE8997 - 16.68.17.p1-C3X16 C202.p1-GPL-(FP6 8)	NXP	/
5	Qualcomm 802.11a/b/g/n Access Point	CA-65-Y9345-LCT	IPQ8064.ILQ.3.2.r3 -000000014-P-1	Qualcomm	/
6	Broadcom 802.11a/b/g/n Access Point	BCM94912R6715W6E R2	803876 17.10.210.2	Broadcom	/
7	Mediatek 802.11a/b/g/n Access Point	AP - MT7615 R2TBV2	1.3.5.9	Mediatek	/
8	Quick track test tool	/	/	/	/

ANNEX A: EUT photograph



EUT Photo (Front view)



EUT Photo (Back view)

ANNEX B: EUT parameters

B.1. Measurement Method

The basic test configuration for infrastructure tests is depicted in the following figure and is a physical connection diagram (note there are two logical networks to separate chariot traffic from configuration traffic for STAs only).

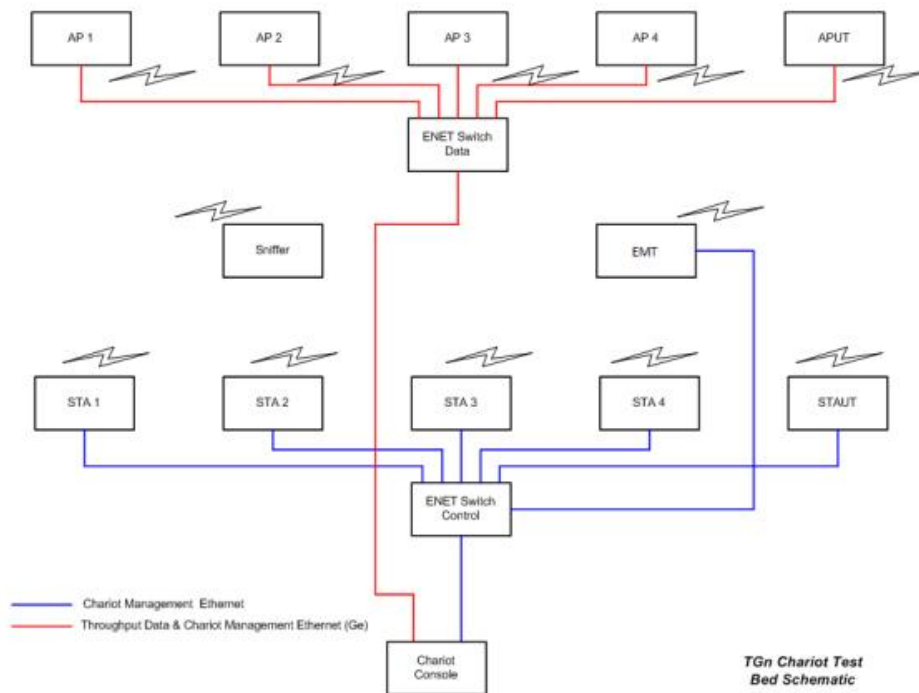


Fig.1 Basic System Test

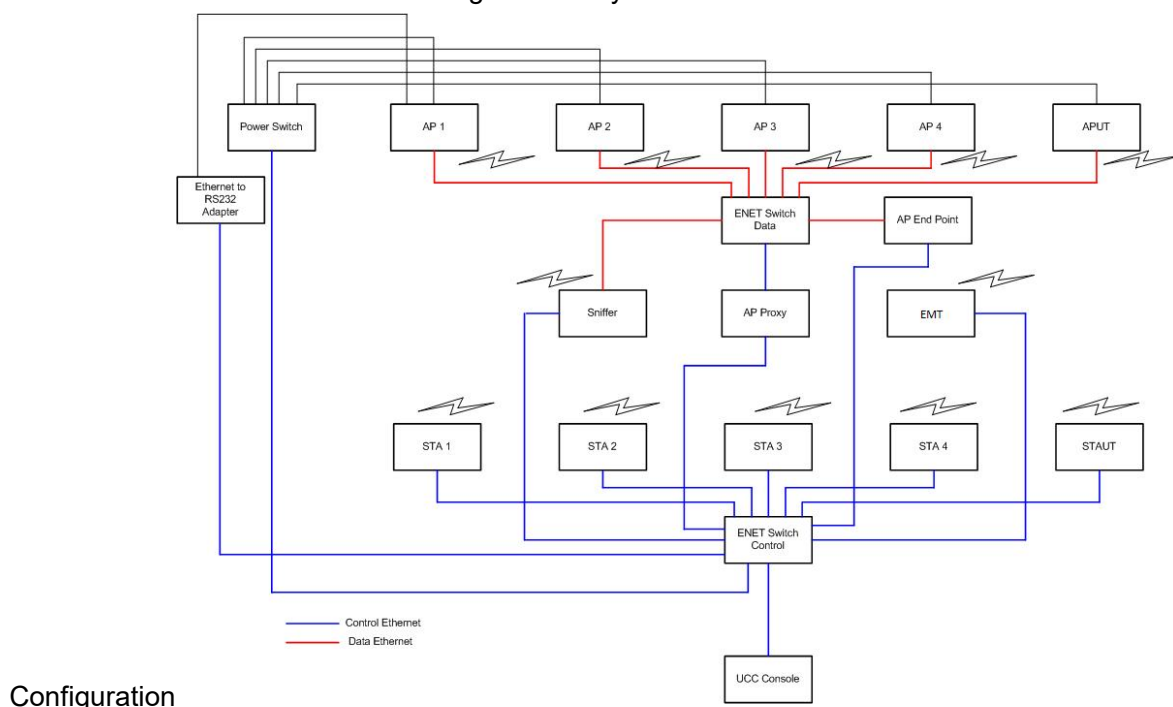


Fig.2 Wi-Fi Test Suite System Test Configuration

Figure 3 depicts the basic system test configuration for testing and certifying interoperability among WPA2 devices.

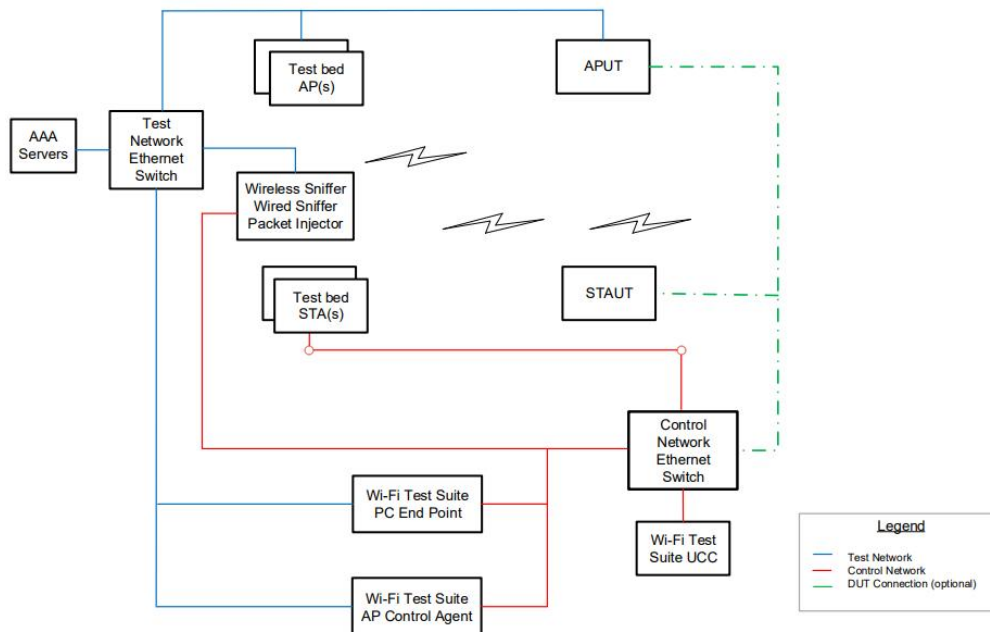


Fig.3 Interoperability system test configuration

Figure 4 depicts the basic system test configuration for testing and certifying compliance among WPA2 devices.

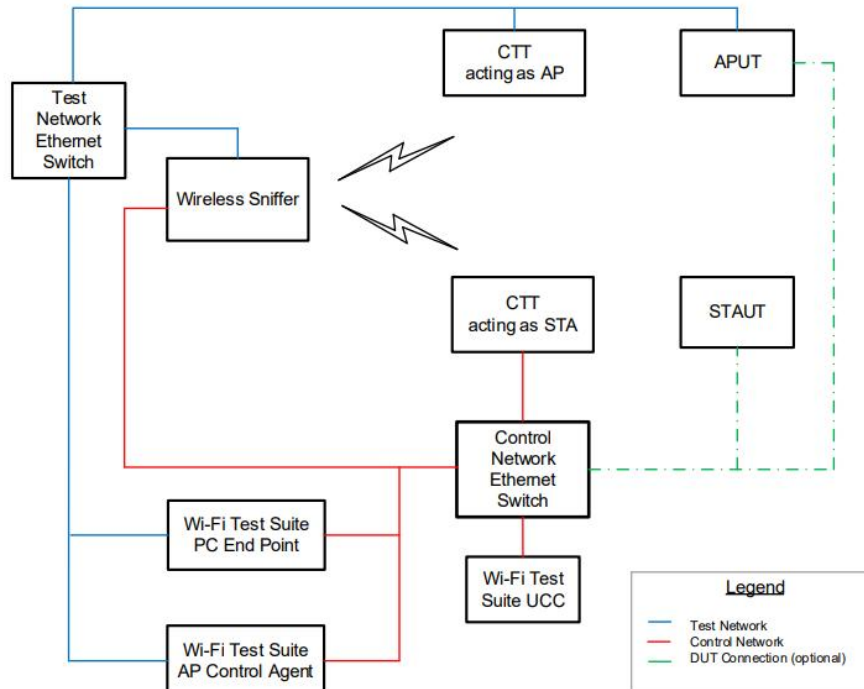


Fig.4 Compliance system test configuration

B.2 Measurement Result

No	Test Item	Standard Requirement	Test Result	Conclusion
1	Clause 5.1.1	General Configurability Tests	Pass	P
2	Clause 5.2.3	AP & STA Association and Throughput, Honoring NAV	Pass	P
		5.2.3S1DT1 throughput in Mbps	23.52	
		5.2.3S1DT2 throughput in Mbps	23.11	
		5.2.3S1DT3 throughput in Mbps	2.50	
3	Clause 5.2.5	Mixed 802.11b/g Interoperability STA Testing	Pass	P
		5.2.5MS8GDT1 throughput in Mbps	3.02	
		5.2.5MS8BDT1 throughput in Mbps	3.01	
		5.2.5MS8GDT2 throughput in Mbps	3.85	
		5.2.5MS8BDT2 throughput in Mbps	1.55	
		5.2.5MS8GDT3 throughput in Mbps	2.52	
		5.2.5MS8BDT3 throughput in Mbps	0.97	
4	Clause 5.2.11	AP & STA Association & Throughput with Replay Counter Processing	Pass	P
		Bytes received exceeds 6.6 Megabytes	Pass	
5	Clause 5.2.14	Group Traffic Transmission/Reception with WPA/WPA2-PSK Mixed Mode	Pass	P
		MCS DT1	Pass	
		MCS DT2	Pass	
6	Clause 5.2.22	802.11h Testing - Spectrum Management Bit	Not Tested	NA
7	Clause 5.2.23	802.11h Testing - Channel Switch Test	Not Tested	NA
8	Clause 5.2.26	Dual Band Roaming Test for Dual Band STAs with WPA-PSK	Pass	P

No	Test Item	Standard Requirement	Test Result	Conclusion
9	Clause 5.2.27	Traffic Differentiation in Single BSS with 802.11n STA	Pass	P
		T02 and T03: Sniffer check - Probe Request and Association Request	Pass	
		T04 result in %	100.000%	
		T05 result in % and sniffer check	100.000%	
		T06 result in %	100.000%	
		T07 result in % and sniffer check	100.000%	
		T08 result in %	98.200%	
10	Clause 5.2.28	Traffic Differentiation in Single BSS with 2 802.11n STAs	Pass	P
		T02 and T03: Sniffer check - Probe Request and Association Request	Pass	
		T04 result in %	100.010%	
		T05 result in %	100.000%	
		T06 result in %	100.000%	
		T07 result in %	100.100%	
11	Clause 5.2.29	Traffic Differentiation in Single BSS with WMM STA	Pass	P
		T02 and T03: Sniffer check - Probe Request and Association Request	Pass	
		T04 result in %	96.064%	
		T05 result in %	100.000%	
		T06 result in %	100.200%	
		T07 result in %	95.679%	
12	Clause 5.2.30	Traffic Differentiation in Single BSS with Legacy non-WMM STA	Pass	P
		T02 and T03: Sniffer check - Probe Request and Association Request	Pass	
		T04 result in %	89.648%	
		T05 result in %	106.820%	
		T06 result in %	173.540%	
13	Clause 5.2.31	Test ACM Bit Conformance	Pass	P
		T04 - 2 results in %	100.000%	
			36.234%	
14	Clause 5.2.32	Test the AC Parameter Modification	Pass	P
		T04 - 2 results in %	44.596%	
			100.000%	
15	Clause 5.2.33	TXOP Limit Test	Pass	P
		T02 result in %	142.850%	
		T04 result in %	142.850%	
		T06 result in %	125.000%	

No	Test Item	Standard Requirement	Test Result	Conclusion
16	Clause 5.2.35	Basic Association in 802.11n Environment	Pass	P
		HT Capability IE – 20/40 MHz supported in 2.4G	No	
		HT Capability IE – SGI 20MHz supported in 2.4G	Yes	
		HT Capability IE – SGI 40MHz supported in 2.4G	No	
		HT Capability IE – Tx STBC supported in 2.4G	Yes	
		HT Capability IE – Rx STBC supported in 2.4G	Yes	
		HT Capability IE – Supported MCS set in 2.4G	1ss	
		HT Capability IE – MCS 32 supported in 2.4G	Yes	
		HT Capability IE – Tx A-MPDU supported in 2.4G	Yes	
		HT Capability IE – 20/40 MHz supported in 5G	Yes	
		HT Capability IE – SGI 20MHz supported in 5G	Yes	
		HT Capability IE – SGI 40MHz supported in 5G	Yes	
		HT Capability IE – Tx STBC supported in 5G	Yes	
		HT Capability IE – Rx STBC supported in 5G	Yes	
		HT Capability IE – Supported MCS set in 5G	1ss	
		HT Capability IE – MCS 32 supported in 5G	Yes	
		HT Capability IE – Tx A-MPDU supported in 5G	Yes	
17	Clause 5.2.36	Ability to Receive 1 and 2 Spatial Streams	Pass	P
		Supported MCS set field in the HT Capability IE contains 1 in the bitmap indexes	Pass	
		20 MHz MCS 7 in 2.4 GHz	Pass	
		20 MHz MCS 15 in 2.4 GHz	Not Tested	
		20 MHz MCS 23 in 2.4 GHz	Not Tested	
		20 MHz MCS 7 in 5.0 GHz	Pass	
		20 MHz MCS 15 in 5.0 GHz	Not Tested	
		20 MHz MCS 23 in 5.0 GHz	Not Tested	
		20/40 MHz MCS 7 in 2.4 GHz	Not Tested	
		20/40 MHz MCS 15 in 2.4 GHz	Not Tested	
		20/40 MHz MCS 23 in 2.4 GHz	Not Tested	
		20/40 MHz MCS 7 in 5.0 GHz	Pass	
		20/40 MHz MCS 15 in 5.0 GHz	Not Tested	
		20/40 MHz MCS 23 in 5.0 GHz	Not Tested	
18	Clause 5.2.37	A-MPDU Aggregation when the STA is the Recipient with and without WPA2-PSK	Pass	P
		5.2.37T4DT1 throughput in Mbps	54.87	
19	Clause 5.2.38	A-MSDU Aggregation when the STA is the Recipient	Pass	P
		5.2.38T4DT1 throughput in Mbps and AP1 packets are > 2346	43.18	

No	Test Item	Standard Requirement	Test Result	Conclusion
20	Clause 5.2.39	Overlapping BSS - 2.4 GHz	Pass	P
		5.2.39T4DT2A throughput in Mbps	5.60	
		5.2.39T4DT2B throughput in Mbps	7.71	
21	Clause 5.2.40	Overlapping BSS - 5 GHz	Pass	P
		5.2.40T4DT2A throughput in Mbps	8.03	
		5.2.40T4DT2B throughput in Mbps	8.37	
22	Clause 5.2.42	Short GI Operation	Pass	P
23	Clause 5.2.43	Overlapping BSS on the Extension Channel	Pass	P
		5.2.43T4DT2A throughput in Mbps	70.39	
		5.2.43T4DT2B throughput in Mbps	9.44	
24	Clause 5.2.44	HT Duplicate Mode (MCS Index = 32)	Pass	P
25	Clause 5.2.46	STBC Receive	Pass	P
26	Clause 5.2.47	A-MPDU Aggregation when the STA in the transmitter	Pass	P
		5.2.47T3DT1 throughput in Mbps and uplink traffic is aggregated	56.33	
		5.2.47T6DT1 throughput in Mbps and uplink traffic is aggregated	Not Tested	
		5.2.47T9DT1 throughput in Mbps and uplink traffic is aggregated	Not Tested	
27	Clause 5.2.48	STA 20/40 MHz Coexistence	Not Tested	NA
28	Clause 5.2.50	STAUT Transmitting to AP using Supported Number of Spatial Streams	Pass	P
		T04 - equal to or greater than 52 Mbps (MCS = 5) in 2.4 GHz, OR, equal to or greater than 104 Mbps (MCS = 13) in 2.4 GHz	Not Tested	
		T04 - equal to or greater than 52 Mbps (MCS = 5) in 5 GHz, OR, equal to or greater than 104 Mbps (MCS = 13) in 5 GHz	Pass	
		T06 – equal to or greater than 156 Mbps(MCS=21) in 2.4 GHz	Not Tested	
		T06 – equal to or greater than 156 Mbps(MCS=21) in 5 GHz	Not Tested	

No	Test Item	Standard Requirement	Test Result	Conclusion
WPA2-Personal STA tests				
29	Clause 5.1	STAUT user interface verification test	Pass	P
30	Clause 5.2.1	STAUT handles RSNE unexpected values test	Not Tested	NA
31	Clause 5.2.2	STAUT verification of RSN Capabilities test	Not Tested	NA
32	Clause 5.2.3	STAUT RSNE bounds verification test	Not Tested	NA
33	CT_Security_WEP-PHY_STA_Disallow-HT_10110_1 [6]	This test case verifies that the STAUT does not use HT/VHT/HE rates when using WEP40 as the encryption cipher	Pass	P
34	CT_Security_WPA2Personal-PHY_STA_Disallow-HT_10112_1 [6]	This test verifies that the STAUT does not use HT/VHT/HE rates when using TKIP as the encryption cipher	Pass	P
35	CT_Security_WPA2Personal_STA_Association WPA2Personal_10332_1 [6]	This test verifies that the STAUT configured with WPA2-Personal associates with an AP configured with WPA2-Personal	Pass	P
36	CT_Security_WPA2Personal_STA_NoAssociation NoSecurityMode_10153_1 [6]	This test verifies that the STAUT configured with WPA2-Personal does not associate with an AP configured with no security (open mode)	Pass	P
37	CT_Security_WPA2Personal_STA_NoAssociation WEP_10160_1 [6]	This test verifies that the STAUT configured with WPA2-Personal does not associate with an AP configured with WEP	Pass	P
38	CT_Security_WPA2Personal_STA_RSNEBoundsVerification-AbsentGrpMgmtCipher_10275_1 [6]	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	Pass	P
39	CT_Security_WPA2Personal_STA_RSNEBoundsVerification-AbsentPMKIDCount_10274_1 [6]	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	Pass	P

No	Test Item	Standard Requirement	Test Result	Conclusion
40	CT_Security_WP A2Personal_STA _RSNEBoundsV erificatio n-AbsentRSNCa p_10273_1 [6]	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	Pass	P
41	CT_Security_WP A2Personal_STA _RSNEBoundsV erificatio n-AllOptional_10 276_1 [6]	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	Pass	P
42	CT_Security_WP A2Personal_STA _RSNEBoundsV erificatio n-FTPSKAKM_1 0280_1 [6]	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	Pass	P
43	CT_Security_WP A2Personal_STA _RSNEBoundsV erificatio n-MultiAKM_102 78_1 [6]	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	Pass	P
44	CT_Security_WP A2Personal_STA _RSNEBoundsV erificatio n-UndefElem_10 277_1 [6]	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	Pass	P
45	CT_Security_WP A2Personal_STA _RSNEBoundsV erificatio n-UnknownAKM_ 10279_1 [6]	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	Pass	P
46	CT_Security_WP A2Personal_STA _UnexpectedRS NE IncompleteAKM_ 10323_1 [6]	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	Pass	P

No	Test Item	Standard Requirement	Test Result	Conclusion
47	CT_Security_WP A2Personal_STA _UnexpectedRS NE IncompletePairwi se_10322_1 [6]	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	Pass	P
48	CT_Security_WP A2Personal_STA _UnexpectedRS NE NoAKM_10315_ 1 [6]	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	Pass	P
49	CT_Security_WP A2Personal_STA _UnexpectedRS NE NoPairwise_103 14_1 [6]	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	Pass	P
50	CT_Security_WP A2Personal_STA _UnexpectedRS NE NoPairwiseAKM_ 10316_1 [6]	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	Pass	P
51	CT_Security_WP A2Personal_STA _UnexpectedRS NE PMKIDPresent_1 0324_1 [6]	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	Pass	P
52	CT_Security_WP A2Personal_STA _UnexpectedRS NE RSNProtoVer_10 313_1 [6]	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	Pass	P
53	CT_Security_WP A2Personal_STA _UnexpectedRS NE TruncatedAKM_1 0319_1 [6]	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	Pass	P

No	Test Item	Standard Requirement	Test Result	Conclusion
54	CT_Security_WP A2Personal_STA _UnexpectedRS NE TruncatedGrpCip her_10317_1 [6]	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	Pass	P
55	CT_Security_WP A2Personal_STA _UnexpectedRS NE TruncatedPairwis e_10318_1 [6]	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	Pass	P
56	CT_Security_WP A2Personal_STA _UnexpectedRS NE TruncatedPMKID _10321_1 [6]	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	Pass	P
57	CT_Security_WP A2Personal_STA _UnexpectedRS NE TruncatedRSNC ap_10320_1 [6]	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	Pass	P
58	CT_Security_WP A2Personal_STA _RSNCapabilitiesVerifica tion-ReservedBit- 15_10485_1 [6]	This test verifies that the STAUT successfully associates, authenticates and passes data traffic when reserved bit 15 in the RSN Capabilities field is set to one instead of zero	Pass	P
59	CT_Security_WP A2Personal_STA _RSNCapabilitiesVerifica tion-OptionalBits _10486_2 [6]	This test verifies that the STAUT does not set optional feature bits to one in the RSN Capabilities field on transmission when unsupported and ignores them on reception	Pass	P
60	CT_Security_WP A2Personal MixedMode_STA _Association-WP A2Personal_100 58_1 [6]	This test verifies that the STAUT configured with WPA2-Personal Mixed Mode associates with an AP configured with WPA2-Personal	Pass	P

No	Test Item	Standard Requirement	Test Result	Conclusion
61	CT_Security_WP A2Personal MixedMode_STA _Association WPA2PersonalMi xedMode_10061 _1 [6]	This test verifies that the STAUT configured with WPA/WPA2-Personal mixed mode associates with an AP configured with WPA2-Personal Mixed Mode	Pass	P
62	CT_Security_WP A2Personal MixedMode_STA _Association-WP APersonal_1006 4_1 [6]	This test verifies that the STAUT configured with WPA2-Personal Mixed Mode associates with an AP configured with WPA-Personal	Pass	P
WPA2-Enterprise STA tests				
63	Clause 5.3.1	STAUT Pre-authentication test	Not Tested	NA
64	Clause 5.3.2	STAUT PMK Caching test	Pass	P
65	Clause 5.3.3.1_Hostapd Server	STAUT Multiple authentication servers test	Pass	P
66	Clause 5.3.3.1_Microsoft Server	STAUT Multiple authentication servers test	Pass	P
67	Clause 5.3.3.1_Radiator Server	STAUT Multiple authentication servers test	Pass	P
68	Clause 5.3.3.2	STAUT Expired server certificate test	Pass	P
69	Clause 5.3.3.3	STAUT EAP SIM IMSI not contained within the AS Database test	Pass	P
70	Clause 5.3.3.4	STAUT EAP AKA Sequence number resynchronization test	Pass	P
71	Clause 5.3.3.5	STAUT No USIM record for EAP AKA test	Pass	P
72	Clause 5.3.3.6	STAUT Protected success indication and EAP AKA fast reconnect using roaming test	Pass	P
73	Clause 5.3.3.7	STAUT Authenticated provisioning and EAP FAST-GTC inner authentication test	Not Tested	NA
74	Clause 5.3.3.8	STAUT Authenticated provisioning and EAP FAST-MSCHAPv2 inner authentication test	Not Tested	NA
75	Clause 5.3.3.9	STAUT EAP AKA' incorrect username prefix test	Pass	P
76	Clause 5.3.4	STAUT RSNE bounds verification test	Not Tested	NA
77	Clause 5.3.5	STAUT unknown Root CA detection test	Not Tested	NA

No	Test Item	Standard Requirement	Test Result	Conclusion
78	CT_Security_EA P-AKA_STA_EA P-AKA_10118_1 [6]	This test verifies that the STAUT associates with an AP when both devices are configured with WPA2-Enterprise with EAP AKA	Pass	P
79	CT_Security_EA P-AKA'_STA_EA P-AKA'_10119_1 [6]	This test verifies that the STAUT associates with an AP when both devices are configured with WPA2-Enterprise with EAP AKA'	Pass	P
80	CT_Security_EA P-FAST-GTC_STA_EA P-FAST-GTC_10120_1 [6]	This test verifies that the STAUT associates with an AP when both devices are configured with WPA2-Enterprise with EAP FAST-GTC	Not Tested	NA
81	CT_Security_EA P-FAST-MSCHAPv2_STA_EA P-FAST-MSCHAPv2_10121_1 [6]	This test verifies that the STAUT associates with an AP when both devices are configured with WPA2-Enterprise with EAP FAST-MSCHAPv2	Not Tested	NA
82	CT_Security_EA P-PEAPv0_STA_EA P-PEAPv0_10122_1 [6]	This test verifies that the STAUT associates with an AP when both devices are configured with WPA2-Enterprise with PEAPv0	Pass	P
83	CT_Security_EA P-PEAPv1_STA_EA P-PEAPv1_10124_1 [6]	This test verifies that the STAUT associates with an AP when both devices are configured with WPA2-Enterprise with PEAPv1	Pass	P
84	CT_Security_EA P-SIM_STA_EA P-SIM_10470_1 [6]	This test verifies that the STAUT associates with an AP when both devices are configured with WPA2-Enterprise with EAP SIM	Pass	P
85	CT_Security_EA P-TLS_STA_EA P-TLS_10126_1 [6]	This test verifies that the STAUT associates with an AP when both devices are configured with WPA2-Enterprise with EAP TLS	Pass	P
86	CT_Security_EA P-TTLS_STA_EA P-TTLS_10128_1 [6]	This test verifies that the STAUT associates with an AP when both devices are configured with WPA2-Enterprise with EAP TTLS	Pass	P
87	CT_Security_SC V_STA_WPA2ServerCertificateValidation_10334_1 [6]	This test verifies that the STAUT correctly performs server certificate validation during an EAP exchange	Pass	P

No	Test Item	Standard Requirement	Test Result	Conclusion
88	CT_Security_WP A2Enterprise_ST A_NoAssociation -WPA2Personal_ 10166_1 [6]	This test verifies that the STAUT configured with WPA2-Enterprise does not associate with an AP configured with WPA2-Personal	Pass	P
89	CT_Security_WP A2Enterprise_ST A_RSNEBounds Verification AbsentAKMSuite _10260_1 [6]	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	Pass	P
90	CT_Security_WP A2Enterprise_ST A_RSNEBounds Verification AbsentGrpCipher _10258_1 [6]	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	Pass	P
91	CT_Security_WP A2Enterprise_ST A_RSNEBounds Verification AbsentGrpMgmt Cipher_10263_1 [6]	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	Pass	P
92	CT_Security_WP A2Enterprise_ST A_RSNEBounds Verification AbsentPairwise_ 10259_1 [6]	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	Pass	P
93	CT_Security_WP A2Enterprise_ST A_RSNEBounds Verification AbsentPMKIDCo unt_10262_1 [6]	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	Pass	P
94	CT_Security_WP A2Enterprise_ST A_RSNEBounds Verification AbsentRSNCap_ 10261_1 [6]	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	Pass	P

No	Test Item	Standard Requirement	Test Result	Conclusion
95	CT_Security_WP A2Enterprise_STA_RSNEBounds Verification AllOptional_10264_1 [6]	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	Pass	P
96	CT_Security_WP A2Enterprise_STA_RSNEBounds Verification MultiPairwiseAKM_10266_1 [6]	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	Pass	P
97	CT_Security_WP A2Enterprise_STA_RSNEBounds Verification UndefElem_10265_1 [6]	This test verifies that the STAUT correctly performs bounds verification on the received RSNE from the test bed AP in Beacon and/or Probe Response frames	Pass	P
98	CT_Security_WP A2Enterprise_STA_UnexpectedRSNE-AbsentPMKID_10298_1 [6]	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	Pass	P
99	CT_Security_WP A2Enterprise_STA_UnexpectedRSNE-InvalidPMKID_10297_1 [6]	This test verifies that the STAUT correctly handles unexpected values in the RSNE from the test bed AP and appropriately requests association	Pass	P

ANNEX C: TEST LAYOUT



Wi-Fi Certification Test Laboratory

ANNEX D: Accreditation Certificate



The image shows a template for a Laboratory Accreditation Certificate. It features the ILAC-MRA and CNAS logos at the top. The text identifies the China National Accreditation Service for Conformity Assessment as the accrediting body. The certificate is for Telecommunication Technology Labs, CAICT, located at No.52, Huayuan North Road, Haidian District, Beijing, China. It states that the lab is accredited in accordance with ISO/IEC 17025: 2017 General Requirements for the Competence of Testing and Calibration Laboratories (CNAS-CL01 Accreditation Criteria for the Competence of Testing and Calibration Laboratories) for the competence to undertake the service described in the schedule attached to this certificate. The scope of accreditation is detailed in the attached schedule bearing the same registration number as above. The certificate is signed on behalf of the China National Accreditation Service for Conformity Assessment by Zhang Chao Hua. The effective date is 2023-06-20 and the expiry date is 2029-06-19. A footer note states that the validity of the certificate can be checked on the CNAS website at <http://www.cnas.org.cn/english/findanaccreditedbody/index.shtml>.

China National Accreditation Service for Conformity Assessment
LABORATORY ACCREDITATION CERTIFICATE
(Registration No. CNAS L0570)

Telecommunication Technology Labs, CAICT
(Legal Entity: *China Academy of Information and Communications Technology*)
No.52, Huayuan North Road, Haidian District, Beijing, China

is accredited in accordance with ISO/IEC 17025: 2017 General Requirements for the Competence of Testing and Calibration Laboratories(CNAS-CL01 Accreditation Criteria for the Competence of Testing and Calibration Laboratories) for the competence to undertake the service described in the schedule attached to this certificate.

The scope of accreditation is detailed in the attached schedule bearing the same registration number as above. The schedule forms an integral part of this certificate.

Effective Date: 2023-06-20
Expiry Date: 2029-06-19

Signed on behalf of China National Accreditation Service for Conformity Assessment 

China National Accreditation Service for Conformity Assessment (CNAS) is authorized by Certification and Accreditation Administration of the People's Republic of China (CNCA) to operate the national accreditation schemes for conformity assessment. CNAS is a signatory of the International Laboratory Accreditation Cooperation Mutual Recognition Arrangement (ILAC MRA) and the Asia Pacific Accreditation Cooperation Mutual Recognition Arrangement (APAC MRA). The validity of the certificate can be checked on CNAS website at <http://www.cnas.org.cn/english/findanaccreditedbody/index.shtml>.

END OF REPORT