Wi-Fi Interoperability TEST REPORT

No. 24T04Z101045-024

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

REPORT HISTORY

Report Number	Revision	Description	Issue Date
24T04Z101045-024	Rev.0	1st edition	2024-06-17

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

CONTENTS

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℃

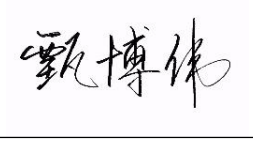
Relative Humidity: 40-60%

1.3. Project data

Testing Start Date: 2024-05-21

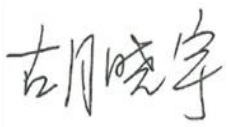
Testing End Date: 2024-06-17

1.4. Signature



Zhen Bowei
(Reviewed 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.

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 WPA3 Test Plan v3.5

5. Test Results

5.1. Summary of Measurement Results

No	Test Cases Standard Sub-clause	Test Cases	Verdict
WPA3-Personal STAUT tests			
1	STAUT configuration requirements validation test	Clause 5.1	P
2	STAUT SAE connectivity and PMK caching test	Clause 5.2.1.1	P
3	STAUT SAE connectivity and PMK caching test	Clause 5.2.1.2	P
4	STAUT SAE connectivity and PMK caching test	Clause 5.2.1.3	P
5	STAUT Anti-clogging test	Clause 5.2.2.1	P
6	STAUT Anti-clogging test	Clause 5.2.2.2	P
7	STAUT reflection attack test	Clause 5.2.3	P
8	STAUT WPA2-Personal compatibility test	Clause 5.2.4	P
9	STAUT support for additional finite cyclic groups test	Clause 5.2.5.1	P
10	STAUT support for additional finite cyclic groups test	Clause 5.2.5.2	P
11	STAUT negative test	Clause 5.2.6	P
12	STAUT SAE confirmaiton exchange variation test	Clause 5.2.7	P
13	STAUT does not request unsuitable Diffie-Hellman groups for SAE test	Clause 5.3	P
14	STAUT Rejected Groups element test	Clause 5.4.1	P
15	STAUT aborts 4-way handshake with RSNXE mismatch test	Clause 5.4.2	P
16	STAUT SAE Transition Disable test	Clause 5.6.1	P
17	STAUT SAE-PK connectivity and PMK caching test	Clause 5.7.1.1	NA
18	STAUT SAE-PK connectivity and PMK caching test	Clause 5.7.1.2	NA
19	STAUT SAE-PK connectivity and PMK caching test	Clause 5.7.1.3	NA
20	STAUT SAE-PK connectivity and PMK caching test	Clause 5.7.1.4	NA
21	STAUT SAE-PK connectivity and PMK caching test	Clause 5.7.1.5	NA
22	STAUT SAE-PK connectivity and PMK caching test	Clause 5.7.1.6	NA
23	STAUT SAE-PK connectivity and PMK caching test	Clause 5.7.1.7	NA
24	STAUT SAE-PK connectivity and PMK caching test	Clause 5.7.1.8	NA
25	STAUT SAE-PK connectivity and PMK caching test	Clause 5.7.1.9	NA
26	STAUT SAE-PK connectivity and PMK caching test	Clause 5.7.1.10	NA
27	STAUT SAE-PK connectivity and PMK caching test	Clause 5.7.1.11	NA
28	STAUT SAE-PK validation failure test	Clause 5.7.2.1	NA
29	STAUT SAE-PK validation failure test	Clause 5.7.2.2	NA
30	STAUT SAE-PK validation failure test	Clause 5.7.2.3	NA
31	STAUT SAE-PK validation failure test	Clause 5.7.2.4	NA
32	STAUT SAE-PK downgrade mitigation test	Clause 5.7.3	NA
33	STAUT SAE-PK password not in correct form or incorrect Sec encoding test	Clause 5.7.4.1	NA
34	STAUT SAE-PK password not in correct form or incorrect Sec encoding test	Clause 5.7.4.2	NA
35	STAUT SAE-PK password not in correct form or incorrect Sec encoding test	Clause 5.7.4.3	NA
36	STAUT SAE-PK password not in correct form or incorrect Sec encoding test	Clause 5.7.4.4	NA
37	STAUT SAE-PK password not in correct form or incorrect Sec encoding test	Clause 5.7.4.5	NA
38	STAUT SAE-PK password not in correct form or incorrect Sec encoding test	Clause 5.7.4.6	NA

No	Test Cases Standard Sub-clause	Test Cases	Verdict
39	STAUT SAE-PK password not in correct form or incorrect Sec encoding test	Clause 5.7.4.7	NA
40	STAUT connect to WPA3-Personal only AP, roam to WPA3-Personal transition mode AP	Clause 5.8.1	NA
41	STAUT connect to WPA3-Personal Transition Mode AP and roam to WPA3-Personal Only AP	Clause 5.8.2	NA
42	STAUT connect to WPA2-Personal only AP, roam to WPA3-Personal transition mode AP	Clause 5.8.3	NA
43	STAUT connect to WPA3-Personal only AP, roam to WPA2-Personal Only AP then roam to WPA3-Personal transition mode AP	Clause 5.8.4	NA
44	STAUT connect to WPA2-Personal only AP, roam to WPA3-Personal only AP then roam to WPA3-Personal transition mode AP	Clause 5.8.5	NA
45	STAUT WPA3-Personal manual roaming test	Clause 5.8.6	NA
46	STAUT WPA3-Personal manual roaming test	Clause 5.8.6_6G	NA
47	STAUT connect to WPA3-Personal Transition Mode AP in 2.4/5 GHz and roam to WPA3-Personal Only AP in 6 GHz	Clause 5.8.7_6G	NA
48	STAUT Group Key Handshake Key Rotation Test	Clause 5.9.1	P
WPA3-Enterprise 192-bit security STAUT tests			
49	STAUT configuration requirements validation test - Configure STAUT for 192-bit security on a BSSID	Clause 19.1.1	NA
50	STAUT IPv4 connectivity using 192-bit security ECC p384 test	Clause 19.2.1	NA
51	STAUT IPv6 connectivity using 192-bit security ECC p384 test	Clause 19.2.2	NA
52	STAUT IPv4 connectivity test using 192-bit security RSA 3K and TLS_ECDHE_RSA_AES_256_GCM_SHA384 cipher test	Clause 19.3.1	NA
53	STAUT IPv6 connectivity using 192-bit security RSA 3K and TLS_ECDHE_RSA_AES_256_GCM_SHA384 cipher test	Clause 19.3.2	NA
54	STAUT IPv4 connectivity using 192-bit security RSA 3K and TLS_DHE_RSA_AES_256_GCM_SHA384 cipher test	Clause 19.4.1	NA
55	STAUT IPv6 connectivity using 192-bit security RSA 3K and TLS_DHE_RSA_AES_256_GCM_SHA384 cipher test	Clause 19.4.2	NA
56	STAUT response to incorrect RSNE received from AP test	Clause 19.5.1	NA
57	STAUT response to AAA server TLS authentication parameters test	Clause 19.5.2	NA
58	STAUT PMK Caching test	Clause 19.6.1	NA
QuickTrack			
59	This test validates that the STAUT uses the supported DH group 15 to successfully complete SAE authentication	CT_Security_WPA3Personal_STA_AcceptOptionalDHgroups-DHgroup15_10015_2 [12]	NA
60	This test validates that the STAUT uses the supported DH group 15 to successfully complete SAE authentication using Hash-to-element mechanism for PWE derivation	CT_Security_WPA3Personal_STA_AcceptOptionalDHgroups-DHgroup15-HnPandH2E_10365_1 [12]	NA
61	This test validates that the STAUT uses the supported DH group 20 to successfully complete SAE authentication	CT_Security_WPA3Personal_STA_AcceptOptionalDHgroups-DHgroup20_10019_2 [12]	P

No	Test Cases Standard Sub-clause	Test Cases	Verdict
62	This test validates that the STAUT uses the supported DH group 20 to successfully complete SAE authentication using Hash-to-element mechanism for PWE derivation	CT_Security_WPA3Personal_STA_AcceptOptionalDHgroups-DHgroup20-HnPandH2E_10369_1 [12]	P
63	This test validates that the STAUT uses the supported DH group 21 to successfully complete SAE authentication	CT_Security_WPA3Personal_STA_AcceptOptionalDHgroups-DHgroup21_10020_2 [12]	P
64	This test validates that the STAUT uses the supported DH group 21 to successfully complete SAE authentication using Hash-to-element mechanism for PWE derivation	CT_Security_WPA3Personal_STA_AcceptOptionalDHgroups-DHgroup21-HnPandH2E_10370_1 [12]	P
65	This test verifies that the STAUT correctly includes the Rejected Groups elements in the subsequent SAE Commit message(s) and successfully completes the SAE authentication with the AP when the AP rejects offered group(s) by the STAUT	CT_Security_WPA3Personal_STA_Association-RejectedGroupElem_10345_1 [12]	P
66	This test verifies that the STAUT is able to connect to an AP that has exceeded its Anticlogging Threshold value	CT_Security_WPA3Personal_STA_DoS-AttackResponse_101172 [12]	P
67	This test verifies that the STAUT is able to connect to a test bed AP that has exceeded its Anticlogging Threshold value when H2E is used for PWE derivation	CT_Security_WPA3Personal_STA_DoS-AttackResponse-HnPandH2E_10364_1 [12]	P
68	This test verifies that the STAUT supporting both Hunting-and-Pecking and Hash-to-element successfully performs SAE authentication with an AP that is configured to use hash-to-element only	CT_Security_WPA3Personal_STA_HnPandH2E-auth-H2Eonly_10362_1 [12]	P
69	This test verifies that the STAUT supporting both Hunting-and-Pecking and Hash-to-element successfully performs SAE authentication with an AP that is configured to also support both Hunting-and-Pecking and hash-to-element	CT_Security_WPA3Personal_STA_HnPandH2E-auth-HnPandH2E_10363_1 [12]	P
70	This test verifies that the STAUT supporting both Hunting-and-Pecking and Hash-to-element successfully performs SAE authentication with an AP that is configured to use Hunting-and-Pecking only	CT_Security_WPA3Personal_STA_HnPandH2E-auth-HnPonly_10361_1 [12]	P
71	This test verifies that the STAUT does not associate to test bed AP when configured to use PWE derivation as Hunting-and-Pecking with WPA3-SAE security in 6 GHz	CT_Security_WPA3Personal_STA_NoAssociation-HnPOnly_10468_1 [12]	NA
72	This test verifies that a WPA3 only STAUT cannot be connected to a testbed AP with open security	CT_Security_WPA3Personal_STA_NoAssociation-NoSecurityMode_10155_1 [12]	P
73	This test verifies that the STAUT aborts 4-way handshake when it detects a mismatch in the RSNXE in EAPOL Message 3 and Beacon (or Probe Response) frames from an AP	CT_Security_WPA3Personal_STA_NoAssociation-RSNXEMismatch_10346_2 [12]	P

No	Test Cases Standard Sub-clause	Test Cases	Verdict
74	This test verifies that a WPA3 only STAUT cannot be connected to a testbed AP with only WEP enabled	CT_Security_WPA3Personal_STA_NoAssociation-WEP_10162_1 [12]	P
75	This test verifies that the STAUT does not associate to test bed AP when configured for WEP security in 6 GHz	CT_Security_WPA3Personal_STA_NoAssociation-WEP_10463_1 [12]	NA
76	This test verifies that a WPA3 only STAUT cannot be connected to a WPA2 testbed AP	CT_Security_WPA3Personal_STA_NoAssociation-WPA2Personal_10165_1 [12]	P
77	This test verifies that the STAUT does not associate to test bed AP when configured for WPA2 Personal with PMF required and SHA 256 security in 6 GHz	CT_Security_WPA3Personal_STA_NoAssociation-WPA2Personal-PMFRequired-SHA256_10467_1 [12]	NA
78	This test verifies that the STAUT does not associate to test bed AP when configured for WPA Personal security in 6 GHz	CT_Security_WPA3Personal_STA_NoAssociation-WPAPersonal_10466_1 [12]	NA
79	This test verifies that the STAUT saves the PMK from the initial SAE authentication to perform a successful reconnection using PMKSA caching	CT_Security_WPA3Personal_STA_PMK-caching_10202_2 [12]	P
80	This test case verifies that the STAUT correctly handles a reflection attack during SAE commitment exchange.	CT_Security_WPA3Personal_STA_Reflection-AttackResponse_10214_1 [12]	P
81	This test verifies that the STAUT correctly rejects improper elements received from the test bed STA	CT_Security_WPA3Personal_STA_RejectionImproperElements-InvalidElem_10221_1 [12]	P
82	This test verifies that the STAUT correctly rejects invalid order received from the test bed STA	CT_Security_WPA3Personal_STA_RejectionImproperElements-InvalidOrder_10224_1 [12]	P
83	This test verifies that the STAUT correctly rejects an invalid scalar value set to one in the SAE Commit message received from the test bed STA	CT_Security_WPA3Personal_STA_RejectionImproperElements-OneScalar_10223_1 [12]	P
84	This test verifies that the STAUT correctly rejects an invalid scalar value set to zero in the SAE commit message received from the test bed STA	CT_Security_WPA3Personal_STA_RejectionImproperElements-ZeroScalar_10222_1 [12]	P
85	This test validates that the STAUT initiating SAE authentication never requests, in the SAE Commit message, a DH group marked as unsuitable	CT_Security_WPA3Personal_STA_RejectionUnsuitableDHgroups_10248_1 [12]	P

No	Test Cases Standard Sub-clause	Test Cases	Verdict
86	This test verifies that the STAUT can successfully complete the SAE protocol with the test bed AP when the testbed AP initiates the SAE confirmation exchange by transmitting an SAE Confirm message immediately after sending its SAE Commit message to the STAUT during the SAE authentication exchange	CT_Security_WPA3Personal_STA_SAEConfirmationExchangeVariation_10371_2 [12]	P
87	This test verifies that, if the network indicates Transition Disable for WPA3-Personal Transition mode, the STAUT applies the policy and does not attempt to associate with an AP that only supports WPA2-Personal	CT_Security_WPA3Personal-transition_STA_TransitionDisable_10347_2 [12]	P
88	This test verifies that the STAUT configured for WPA3-Personal transition mode prefers SAE to connect to an AP advertising WPA3-Personal transition mode support	CT_Security_WPA3Personal-transition_STA_WPA3-PersonalTransitionMode_10335_2 [12]	P
89	This test verifies that the STAUT correctly performs server certificate validation with an explicitly configured server certificate during an EAP exchange	CT_Security_SCVConfigured_STA_BadServerCert-UOSCDisabled_10195_1 [12]	NA
90	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server certificate during an EAP exchange	CT_Security_SCVConfigured_STA_BadServerCert-UOSCEnabled_10289_1 [12]	P
91	This test verifies that the STAUT correctly performs server certificate validation during an EAP exchange	CT_Security_SCVConfigured_STA_Match_10143_1 [12]	P
92	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server certificate during an EAP exchange	CT_Security_SCVConfigured_STA_NonMatch-TODSTRICTClient_10184_1 [12]	P
93	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server certificate during an EAP exchange	CT_Security_SCVConfigured_STA_NonMatch-TODSTRICTServer-UOSCDisabled_10182_1 [12]	NA
94	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server certificate during an EAP exchange	CT_Security_SCVConfigured_STA_NonMatch-TODSTRICTServer-UOSCEnabled_10183_1 [12]	P
95	This test verifies that the STAUT correctly performs server certificate validation during an EAP exchange	CT_Security_SCVConfigured_STA_NonMatch-UOSCDisabled_10168_1 [12]	NA
96	This test verifies that the STAUT correctly performs server certificate validation with an explicitly configured server certificate during an EAP exchange	CT_Security_SCVConfigured_STA_NonMatch-UOSCEnabled_10169_1 [12]	P
97	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA during an EAP exchange	CT_Security_SCVFQDNRootCA_STA_Match_10145_1 [12]	P

No	Test Cases Standard Sub-clause	Test Cases	Verdict
98	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA during an EAP exchange	CT_Security_SCVFQDN RootCA_STA_Match-TODSTRICTServer_10146_1 [12]	P
99	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA during an EAP exchange	CT_Security_SCVFQDN RootCA_STA_NonMatch FQDN-UOSCDisabled_10174_1 [12]	NA
100	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA during an EAP exchange	CT_Security_SCVFQDN RootCA_STA_NonMatch FQDN-UOSCEnabled_10175_1 [12]	P
101	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA during an EAP exchange	CT_Security_SCVFQDN RootCA_STA_NonMatch RootCA-UOSCDisabled_10148_1 [12]	NA
102	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA during an EAP exchange	CT_Security_SCVFQDN RootCA_STA_NonMatch RootCA-UOSCEnabled_10149_1 [12]	P
103	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA in trust store during an EAP exchange	CT_Security_SCVFQDN RootStore_STA_BadPublicCA-UOSCDisabled_10185_1 [12]	NA
104	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA in trust store during an EAP exchange	CT_Security_SCVFQDN RootStore_STA_BadPublicCA-UOSCEnabled_10194_1 [12]	P
105	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA in trust store during an EAP exchange	CT_Security_SCVFQDN RootStore_STA_Match_10150_1 [12]	P
106	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA in trust store during an EAP exchange	CT_Security_SCVFQDN RootStore_STA_NonMatchFQDN-UOSCDisabled_10176_1 [12]	NA
107	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA in trust store during an EAP exchange	CT_Security_SCVFQDN RootStore_STA_NonMatchFQDN-UOSCEnabled_10177_1 [12]	P
108	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA in trust store during an EAP exchange	CT_Security_SCVFQDN RootStore_STA_NonMatchSuffix-UOSCDisabled_10172_1 [12]	NA

No	Test Cases Standard Sub-clause	Test Cases	Verdict
109	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA in trust store during an EAP exchange	CT_Security_SCVFQDNRootStore_STA_NonMatchSuffix-UOSCEnabled_10173_1 [12]	P
110	This test verifies that, when the STAUT is in unconfigured state (do not explicitly disable server validation), the STAUT does not successfully complete the 802.1X EAP exchange	CT_Security_SCVNetworkProfileConfig_STA_NoEAPAuth_10440_1 [12]	NA
111	This test verifies that, when the STAUT is configured to explicitly disable server validation (select "Don't validate" or similar in STAUT UI), the STAUT does not successfully complete the 802.1X EAP exchange	CT_Security_SCVNetworkProfileConfig_STA_NoValidate_10441_1 [12]	NA
112	This test verifies that, when the STAUT is configured to use system trust store only (do not explicitly disable server validation), the STAUT does not successfully complete the 802.1X EAP exchange	CT_Security_SCVNetworkProfileConfig_STA_TrustStoreonly_10442_1 [12]	NA
113	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured root CA during an EAP exchange	CT_Security_SCVRootCA_STA_BadRootCA-UOSCDisabled_10438_1 [12]	NA
114	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured root CA during an EAP exchange	CT_Security_SCVRootCA_STA_BadRootCA-UOSCEnabled_10439_1 [12]	P
115	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured root CA during an EAP exchange	CT_Security_SCVRootCA_STA_Match_10144_1 [12]	P
116	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured root CA during an EAP exchange	CT_Security_SCVRootCA_STA_NonMatch-TODSTRICTServer-UOSCDisabled_10178_1 [12]	NA
117	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured root CA during an EAP exchange	CT_Security_SCVRootCA_STA_NonMatch-TODSTRICTServer-UOSCEnabled_10179_1 [12]	P
118	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured root CA during an EAP exchange	CT_Security_SCVRootCA_STA_NonMatch-TODTOFU-UOSCDisabled_10180_1 [12]	NA
119	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured root CA during an EAP exchange	CT_Security_SCVRootCA_STA_NonMatch-TODTOFU-UOSCEnabled_10181_1 [12]	P
120	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) suffix and root CA during an EAP exchange	CT_Security_SCVSuffixRootCA_STA_BadRootCA-UOSCDisabled_10291_1 [12]	NA

No	Test Cases Standard Sub-clause	Test Cases	Verdict
121	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) suffix and root CA during an EAP exchange	CT_Security_SCVSuffixRootCA_STA_BadRootCA-UOSCEnabled_10292_1 [12]	P
122	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) suffix and root CA during an EAP exchange	CT_Security_SCVSuffixRootCA_STA_Match_10151_1 [12]	P
123	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) suffix and root CA during an EAP exchange	CT_Security_SCVSuffixRootCA_STA_NonMatchSuffix-UOSCDisabled_10170_1 [12]	NA
124	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) suffix and root CA during an EAP exchange	CT_Security_SCVSuffixRootCA_STA_NonMatchSuffix-UOSCEnabled_10171_1 [12]	P
125	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) suffix and root store during an EAP exchange	CT_Security_SCVSuffixRootStore_STA_BadPublicCA-UOSCDisabled_10443_1 [12]	NA
126	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) suffix and root store during an EAP exchange	CT_Security_SCVSuffixRootStore_STA_BadPublicCA-UOSCEnabled_10444_1 [12]	P
127	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) suffix and root store during an EAP exchange	CT_Security_SCVSuffixRootStore_STA_Match_10147_1 [12]	P
128	This test verifies that the STAUT does not associate to test bed AP when configured for WPA2 Enterprise security in 6 GHz	CT_Security_WPA3Enterprise_STA_NoAssociation-WPA2Enterprise_104652 [12]	NA
129	This test verifies that the STAUT does not associate to test bed AP when configured for WPA Enterprise security in 6 GHz	CT_Security_WPA3Enterprise_STA_NoAssociation-WPAEnterprise_10464_2 [12]	NA
130	This test verifies that the STAUT successfully associates, authenticates and passes data traffic when reserved bits in the RSN Capabilities and Extended RSN Capabilities fields are set to one instead of zero, and when the RSNXE is extended. This test also verifies that the STAUT does not set optional feature bits to one in the RSN Capabilities and Extended RSN Capabilities fields on transmission when unsupported and ignores them on reception.	CT_Security_RSN_STA_CapabilitiesVerification-ReservedBits-31_10603_1 [12]	P

No	Test Cases Standard Sub-clause	Test Cases	Verdict
131	This test verifies that the STAUT successfully associates, authenticates and passes data traffic when reserved bits in the RSN Capabilities and Extended RSN Capabilities fields are set to one instead of zero, and when the RSNXE is extended. This test also verifies that the STAUT does not set optional feature bits to one in the RSN Capabilities and Extended RSN Capabilities fields on transmission when unsupported and ignores them on reception.	CT_Security_RSN_STA_CapabilitiesVerification-ReservedBits-SAE-PK_10604_1 [12]	P
132	This test verifies that the STAUT successfully associates, authenticates and passes data traffic when reserved bits in the RSN Capabilities and Extended RSN Capabilities fields are set to one instead of zero, and when the RSNXE is extended. This test also verifies that the STAUT does not set optional feature bits to one in the RSN Capabilities and Extended RSN Capabilities fields on transmission when unsupported and ignores them on reception.	CT_Security_RSN_STA_CapabilitiesVerification-ReservedBits-Extra_10605_1 [12]	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

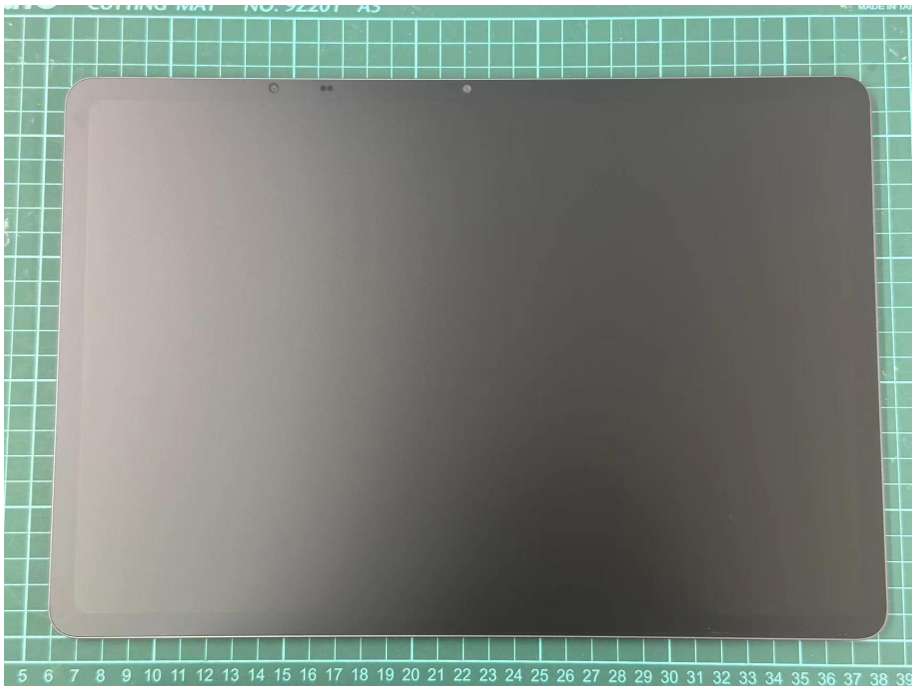
The test cases as listed in section 5.1 of this report for the EUT specified in section 3 was performed by CTTL according to the standards or reference documents listed in section 4.2

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

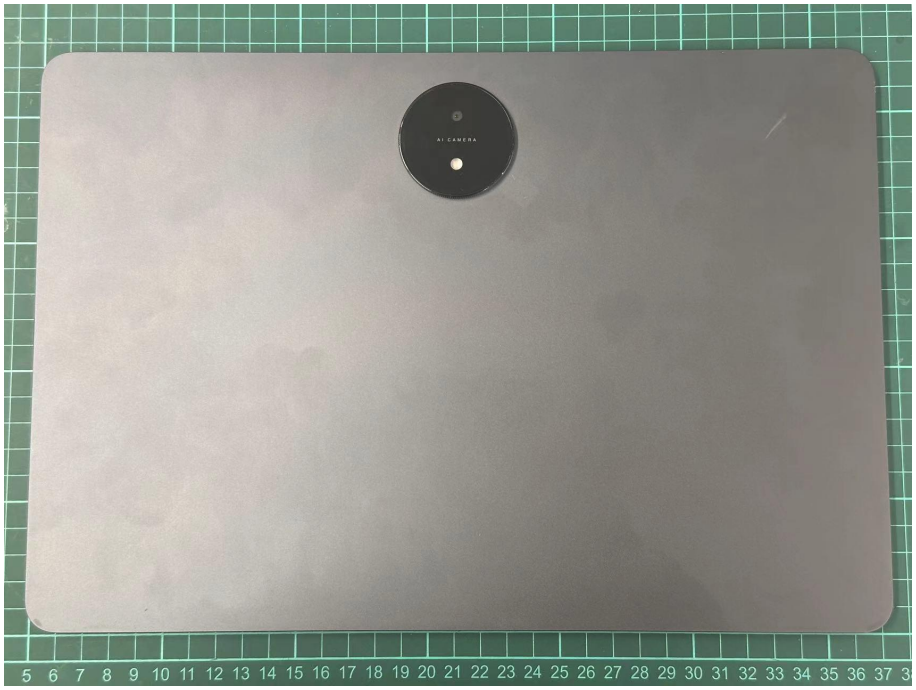
6. Test Facilities Utilized

No	Name	Model	manufacturer	version
1.	Shielding Room	S81	ETS	/
2.	MTK-AP-3	MT7915-AP-WPA3	MediaTek	7.2.18.0
3.	QCA-AP-2	CA-65-YC633-1000-WPA3R3	Qualcomm	IPQ8074.WFA.11.3-00028-P-1
4.	QCA-AP-4	CA-65-YE079-HE	Qualcomm	IPQ8074.WFA.11.3-00028-P-1
5.	BCM-STA-3	BCM94391FCPAESL	Broadcom	993233 87.12.100
6.	INT-STA-3	AX210.NGWG.NV	Intel	2022-10-24T08
7.	QuickTrack tool	/	/	/

ANNEX A: EUT photograph



EUT Photo (Front view)



EUT Photo (Back view)

ANNEX B: EUT parameters

B.1. Measurement Method

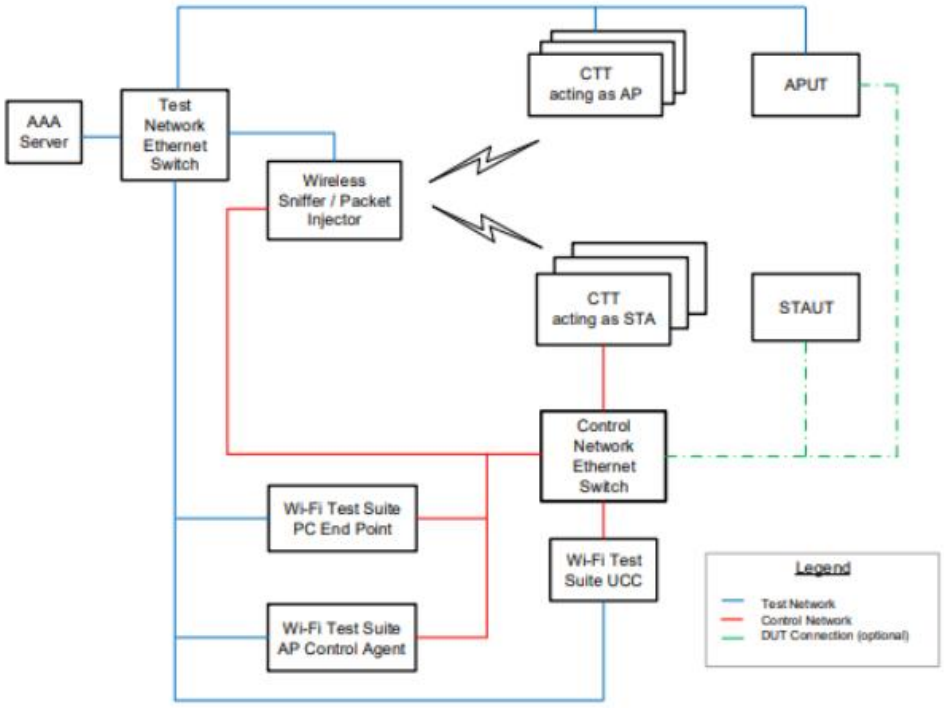


Fig.1 WPA3 Test Bed Schematic

1). The WFA Sigma Automation Suite will be used as much as possible. This tool suite provides configuration, test control, traffic generation, and results analysis services. The test plan, in its entirety, can be executed in a fully automated manner through the WFA distributed Sigma Command Scripts and the Sigma Unified CAPI Console.

B.2 Measurement Result

No	Test Cases	Test Item	Test Result	Conclusion
WPA3-Personal STAUT tests				
1	Clause 5.1	STAUT configuration requirements validation test	Pass	P
2	Clause 5.2.1.1	STAUT SAE connectivity and PMK caching test	Pass	P
3	Clause 5.2.1.2	STAUT SAE connectivity and PMK caching test	Pass	P
4	Clause 5.2.1.3	STAUT SAE connectivity and PMK caching test	Pass	P
5	Clause 5.2.2.1	STAUT Anti-clogging test	Pass	P
6	Clause 5.2.2.2	STAUT Anti-clogging test	Pass	P
7	Clause 5.2.3	STAUT reflection attack test	Pass	P
8	Clause 5.2.4	STAUT WPA2-Personal compatibility test	Pass	P
9	Clause 5.2.5.1	STAUT support for additional finite cyclic groups test	Pass	P
10	Clause 5.2.5.2	STAUT support for additional finite cyclic groups test	Pass	P
11	Clause 5.2.6	STAUT negative test	Pass	P
12	Clause 5.2.7	STAUT SAE confirmaiton exchange variation test	Pass	P
13	Clause 5.3	STAUT does not request unsuitable Diffie-Hellman groups for SAE test	Pass	P
14	Clause 5.4.1	STAUT Rejected Groups element test	Pass	P
15	Clause 5.4.2	STAUT aborts 4-way handshake with RSNXE mismatch test	Pass	P
16	Clause 5.6.1	STAUT SAE Transition Disable test	Pass	P
17	Clause 5.7.1.1	STAUT SAE-PK connectivity and PMK caching test	Not tested	NA
18	Clause 5.7.1.2	STAUT SAE-PK connectivity and PMK caching test	Not tested	NA
19	Clause 5.7.1.3	STAUT SAE-PK connectivity and PMK caching test	Not tested	NA
20	Clause 5.7.1.4	STAUT SAE-PK connectivity and PMK caching test	Not tested	NA
21	Clause 5.7.1.5	STAUT SAE-PK connectivity and PMK caching test	Not tested	NA
22	Clause 5.7.1.6	STAUT SAE-PK connectivity and PMK caching test	Not tested	NA
23	Clause 5.7.1.7	STAUT SAE-PK connectivity and PMK caching test	Not tested	NA
24	Clause 5.7.1.8	STAUT SAE-PK connectivity and PMK caching test	Not tested	NA
25	Clause 5.7.1.9	STAUT SAE-PK connectivity and PMK caching test	Not tested	NA
26	Clause 5.7.1.10	STAUT SAE-PK connectivity and PMK caching test	Not tested	NA
27	Clause 5.7.1.11	STAUT SAE-PK connectivity and PMK caching test	Not tested	NA
28	Clause 5.7.2.1	STAUT SAE-PK validation failure test	Not tested	NA
29	Clause 5.7.2.2	STAUT SAE-PK validation failure test	Not tested	NA
30	Clause 5.7.2.3	STAUT SAE-PK validation failure test	Not tested	NA
31	Clause 5.7.2.4	STAUT SAE-PK validation failure test	Not tested	NA
32	Clause 5.7.3	STAUT SAE-PK downgrade mitigation test	Not tested	NA

No	Test Cases	Test Item	Test Result	Conclusion
33	Clause 5.7.4.1	STAUT SAE-PK password not in correct form or incorrect Sec encoding test	Not tested	NA
34	Clause 5.7.4.2	STAUT SAE-PK password not in correct form or incorrect Sec encoding test	Not tested	NA
35	Clause 5.7.4.3	STAUT SAE-PK password not in correct form or incorrect Sec encoding test	Not tested	NA
36	Clause 5.7.4.4	STAUT SAE-PK password not in correct form or incorrect Sec encoding test	Not tested	NA
37	Clause 5.7.4.5	STAUT SAE-PK password not in correct form or incorrect Sec encoding test	Not tested	NA
38	Clause 5.7.4.6	STAUT SAE-PK password not in correct form or incorrect Sec encoding test	Not tested	NA
39	Clause 5.7.4.7	STAUT SAE-PK password not in correct form or incorrect Sec encoding test	Not tested	NA
40	Clause 5.8.1	STAUT connect to WPA3-Personal only AP, roam to WPA3-Personal transition mode AP	Not tested	NA
41	Clause 5.8.2	STAUT connect to WPA3-Personal Transition Mode AP and roam to WPA3-Personal Only AP	Not tested	NA
42	Clause 5.8.3	STAUT connect to WPA2-Personal only AP, roam to WPA3-Personal transition mode AP	Not tested	NA
43	Clause 5.8.4	STAUT connect to WPA3-Personal only AP, roam to WPA2-Personal Only AP then roam to WPA3-Personal transition mode AP	Not tested	NA
44	Clause 5.8.5	STAUT connect to WPA2-Personal only AP, roam to WPA3-Personal only AP then roam to WPA3-Personal transition mode AP	Not tested	NA
45	Clause 5.8.6	STAUT WPA3-Personal manual roaming test	Not tested	NA
46	Clause 5.8.6_6G	STAUT WPA3-Personal manual roaming test	Not tested	NA
47	Clause 5.8.7_6G	STAUT connect to WPA3-Personal Transition Mode AP in 2.4/5 GHz and roam to WPA3-Personal Only AP in 6 GHz	Not tested	NA
48	Clause 5.9.1	STAUT Group Key Handshake Key Rotation Test	Pass	P
WPA3-Enterprise 192-bit security STAUT tests				
49	Clause 19.1.1	STAUT configuration requirements validation test - Configure STAUT for 192-bit security on a BSSID	Not tested	NA
50	Clause 19.2.1	STAUT IPv4 connectivity using 192-bit security ECC p384 test	Not tested	NA
51	Clause 19.2.2	STAUT IPv6 connectivity using 192-bit security ECC p384 test	Not tested	NA
52	Clause 19.3.1	STAUT IPv4 connectivity test using 192-bit security RSA 3K and TLS_ECDHE_RSA_AES_256_GCM_SHA384 cipher test	Not tested	NA
53	Clause 19.3.2	STAUT IPv6 connectivity using 192-bit security RSA 3K and TLS_ECDHE_RSA_AES_256_GCM_SHA384 cipher test	Not tested	NA
54	Clause 19.4.1	STAUT IPv4 connectivity using 192-bit security RSA 3K and TLS_DHE_RSA_AES_256_GCM_SHA384 cipher test	Not tested	NA

No	Test Cases	Test Item	Test Result	Conclusion
55	Clause 19.4.2	STAUT IPv6 connectivity using 192-bit security RSA 3K and TLS_DHE_RSA_AES_256_GCM_SHA384 cipher test	Not tested	NA
56	Clause 19.5.1	STAUT response to incorrect RSNE received from AP test	Not tested	NA
57	Clause 19.5.2	STAUT response to AAA server TLS authentication parameters test	Not tested	NA
58	Clause 19.6.1	STAUT PMK Caching test	Not tested	NA
59	CT_Security_WPA3Personal_STA_AcceptOptionalDHgroups-DHgroup15_10015_2 [12]	This test validates that the STAUT uses the supported DH group 15 to successfully complete SAE authentication	Not tested	NA
60	CT_Security_WPA3Personal_STA_AcceptOptionalDHgroups-DHgroup15-HnPandH2E_10365_1 [12]	This test validates that the STAUT uses the supported DH group 15 to successfully complete SAE authentication using Hash-to-element mechanism for PWE derivation	Not tested	NA
61	CT_Security_WPA3Personal_STA_AcceptOptionalDHgroups-DHgroup20_10019_2 [12]	This test validates that the STAUT uses the supported DH group 20 to successfully complete SAE authentication	Pass	P
62	CT_Security_WPA3Personal_STA_AcceptOptionalDHgroups-DHgroup20-HnPandH2E_10369_1 [12]	This test validates that the STAUT uses the supported DH group 20 to successfully complete SAE authentication using Hash-to-element mechanism for PWE derivation	Pass	P
63	CT_Security_WPA3Personal_STA_AcceptOptionalDHgroups-DHgroup21_10020_2 [12]	This test validates that the STAUT uses the supported DH group 21 to successfully complete SAE authentication	Pass	P
64	CT_Security_WPA3Personal_STA_AcceptOptionalDHgroups-DHgroup21-HnPandH2E_10370_1 [12]	This test validates that the STAUT uses the supported DH group 21 to successfully complete SAE authentication using Hash-to-element mechanism for PWE derivation	Pass	P
65	CT_Security_WPA3Personal_STA_Association-RejectedGroupElem_10345_1 [12]	This test verifies that the STAUT correctly includes the Rejected Groups elements in the subsequent SAE Commit message(s) and successfully completes the SAE authentication with the AP when the AP rejects offered group(s) by the STAUT	Pass	P
66	CT_Security_WPA3Personal_STA_DoS-AttackResponse_10117_2 [12]	This test verifies that the STAUT is able to connect to an AP that has exceeded its Anticlogging Threshold value	Pass	P

No	Test Cases	Test Item	Test Result	Conclusion
67	CT_Security_WPA3Personal_STA_DoS-AttackResponse-HnPandH2E_10364_1 [12]	This test verifies that the STAUT is able to connect to a test bed AP that has exceeded its Anticlogging Threshold value when H2E is used for PWE derivation	Pass	P
68	CT_Security_WPA3Personal_STA_HnPandH2E-auth-H2Eonly_10362_1 [12]	This test verifies that the STAUT supporting both Hunting-and-Pecking and Hash-to-element successfully performs SAE authentication with an AP that is configured to use hash-to-element only	Pass	P
69	CT_Security_WPA3Personal_STA_HnPandH2E-auth-HnPandH2E_10363_1 [12]	This test verifies that the STAUT supporting both Hunting-and-Pecking and Hash-to-element successfully performs SAE authentication with an AP that is configured to also support both Hunting-and-Pecking and hash-to-element	Pass	P
70	CT_Security_WPA3Personal_STA_HnPandH2E-auth-HnPonly_10361_1 [12]	This test verifies that the STAUT supporting both Hunting-and-Pecking and Hash-to-element successfully performs SAE authentication with an AP that is configured to use Hunting-and-Pecking only	Pass	P
71	CT_Security_WPA3Personal_STA_NoAssociation-HnPOnly_10468_1 [12]	This test verifies that the STAUT does not associate to test bed AP when configured to use PWE derivation as Hunting-and-Pecking with WPA3-SAE security in 6 GHz	Not tested	NA
72	CT_Security_WPA3Personal_STA_NoAssociation-NoSecurityMode_10155_1 [12]	This test verifies that a WPA3 only STAUT cannot be connected to a testbed AP with open security	Pass	P
73	CT_Security_WPA3Personal_STA_NoAssociation-RSNXEMismatch_10346_2 [12]	This test verifies that the STAUT aborts 4-way handshake when it detects a mismatch in the RSNXE in EAPOL Message 3 and Beacon (or Probe Response) frames from an AP	Pass	P
74	CT_Security_WPA3Personal_STA_NoAssociation-WEP_10162_1 [12]	This test verifies that a WPA3 only STAUT cannot be connected to a testbed AP with only WEP enabled	Pass	P
75	CT_Security_WPA3Personal_STA_NoAssociation-WEP_10463_1 [12]	This test verifies that the STAUT does not associate to test bed AP when configured for WEP security in 6 GHz	Not tested	NA
76	CT_Security_WPA3Personal_STA_NoAssociation-WPA2Personal_10165_1 [12]	This test verifies that a WPA3 only STAUT cannot be connected to a WPA2 testbed AP	Pass	P
77	CT_Security_WPA3Personal_STA_NoAssociation-WPA2Personal-PMFRequired-SHA256_10467_1 [12]	This test verifies that the STAUT does not associate to test bed AP when configured for WPA2 Personal with PMF required and SHA 256 security in 6 GHz	Not tested	NA

No	Test Cases	Test Item	Test Result	Conclusion
78	CT_Security_WPA3Personal_STA_NoAssociation-WPAPersonal_10466_1 [12]	This test verifies that the STAUT does not associate to test bed AP when configured for WPA Personal security in 6 GHz	Not tested	NA
79	CT_Security_WPA3Personal_STA_PMK-caching_10202_2 [12]	This test verifies that the STAUT saves the PMK from the initial SAE authentication to perform a successful reconnection using PMKSA caching	Pass	P
80	CT_Security_WPA3Personal_STA_Reflection-AttackResponse_10214_1 [12]	This test case verifies that the STAUT correctly handles a reflection attack during SAE commitment exchange.	Pass	P
81	CT_Security_WPA3Personal_STA_RejectionImproperElements-InvalidElem_10221_1 [12]	This test verifies that the STAUT correctly rejects improper elements received from the test bed STA	Pass	P
82	CT_Security_WPA3Personal_STA_RejectionImproperElements-InvalidOrder_10224_1 [12]	This test verifies that the STAUT correctly rejects invalid order received from the test bed STA	Pass	P
83	CT_Security_WPA3Personal_STA_RejectionImproperElements-OneScalar_10223_1 [12]	This test verifies that the STAUT correctly rejects an invalid scalar value set to one in the SAE Commit message received from the test bed STA	Pass	P
84	CT_Security_WPA3Personal_STA_RejectionImproperElements-ZeroScalar_10222_1 [12]	This test verifies that the STAUT correctly rejects an invalid scalar value set to zero in the SAE commit message received from the test bed STA	Pass	P
85	CT_Security_WPA3Personal_STA_RejectionUnsuitableDHgroups_10248_1 [12]	This test validates that the STAUT initiating SAE authentication never requests, in the SAE Commit message, a DH group marked as unsuitable	Pass	P
86	CT_Security_WPA3Personal_STA_SAEConfirmationExchangeVariation_10371_2 [12]	This test verifies that the STAUT can successfully complete the SAE protocol with the test bed AP when the testbed AP initiates the SAE confirmation exchange by transmitting an SAE Confirm message immediately after sending its SAE Commit message to the STAUT during the SAE authentication exchange	Pass	P
87	CT_Security_WPA3Personal-transition_STA_TransitionDisable_10347_2 [12]	This test verifies that, if the network indicates Transition Disable for WPA3-Personal Transition mode, the STAUT applies the policy and does not attempt to associate with an AP that only supports WPA2-Personal	Pass	P

No	Test Cases	Test Item	Test Result	Conclusion
88	CT_Security_WPA3Personal-transition_STA_WPA3-PersonalTransitionMode_10335_2 [12]	This test verifies that the STAUT configured for WPA3-Personal transition mode prefers SAE to connect to an AP advertising WPA3-Personal transition mode support	Pass	P
89	CT_Security_SCVConfigured_STA_BadServerCert-UOSCDisabled_10195_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with an explicitly configured server certificate during an EAP exchange	Not tested	NA
90	CT_Security_SCVConfigured_STA_BadServerCert-UOSCEnabled_10289_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server certificate during an EAP exchange	Pass	P
91	CT_Security_SCVConfigured_STA_Match_10143_1 [12]	This test verifies that the STAUT correctly performs server certificate validation during an EAP exchange	Pass	P
92	CT_Security_SCVConfigured_STA_NonMatch-TODSTRICTClient_10184_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server certificate during an EAP exchange	Pass	P
93	CT_Security_SCVConfigured_STA_NonMatch-TODSTRICTServer-UOSCDisabled_10182_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server certificate during an EAP exchange	Not tested	NA
94	CT_Security_SCVConfigured_STA_NonMatch-TODSTRICTServer-UOSCEnabled_10183_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server certificate during an EAP exchange	Pass	P
95	CT_Security_SCVConfigured_STA_NonMatch-UOSCDisabled_10168_1 [12]	This test verifies that the STAUT correctly performs server certificate validation during an EAP exchange	Not tested	NA
96	CT_Security_SCVConfigured_STA_NonMatch-UOSCEnabled_10169_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with an explicitly configured server certificate during an EAP exchange	Pass	P
97	CT_Security_SCVFQDNRootCA_STA_Match_10145_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA during an EAP exchange	Pass	P
98	CT_Security_SCVFQDNRootCA_STA_Match-TODSTRICTServer_10146_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA during an EAP exchange	Pass	P

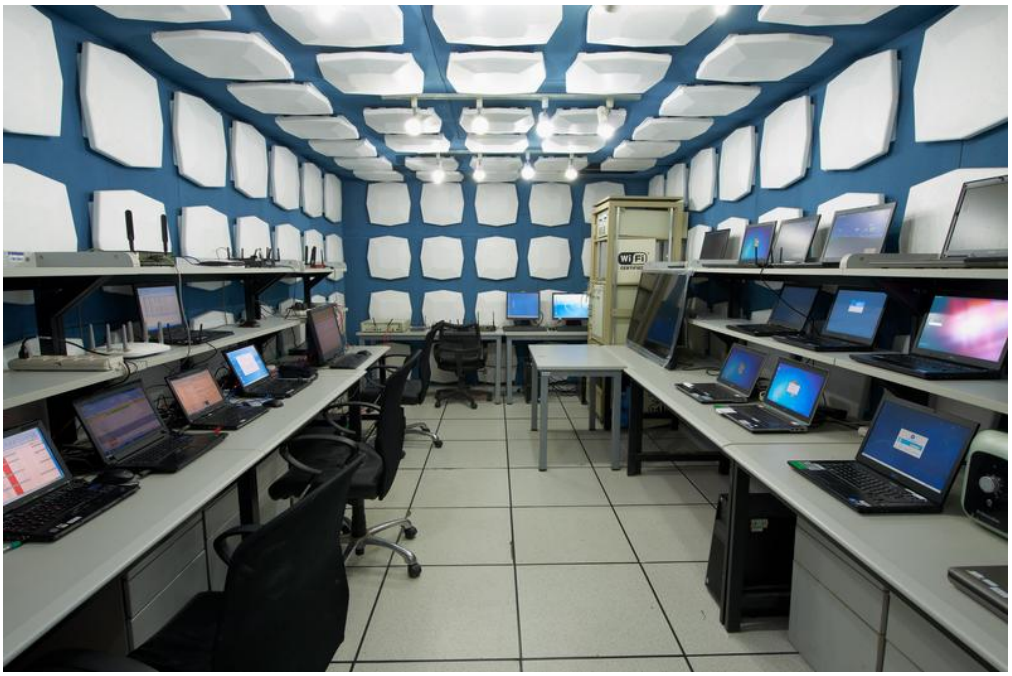
No	Test Cases	Test Item	Test Result	Conclusion
99	CT_Security_SCVFQDNRootCA_STA_NonMatchFQDN-UOSCDisabled_10174_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA during an EAP exchange	Not tested	NA
100	CT_Security_SCVFQDNRootCA_STA_NonMatchFQDN-UOSCEnabled_10175_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA during an EAP exchange	Pass	P
101	CT_Security_SCVFQDNRootCA_STA_NonMatchRootCA-UOSCDisabled_10148_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA during an EAP exchange	Not tested	NA
102	CT_Security_SCVFQDNRootCA_STA_NonMatchRootCA-UOSCEnabled_10149_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA during an EAP exchange	Pass	P
103	CT_Security_SCVFQDNRootStore_STA_BadPublicCA-UOSCDisabled_10185_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA in trust store during an EAP exchange	Not tested	NA
104	CT_Security_SCVFQDNRootStore_STA_BadPublicCA-UOSCEnabled_10194_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA in trust store during an EAP exchange	Pass	P
105	CT_Security_SCVFQDNRootStore_STA_Match_10150_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA in trust store during an EAP exchange	Pass	P
106	CT_Security_SCVFQDNRootStore_STA_NonMatchFQDN-UOSCDisabled_10176_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA in trust store during an EAP exchange	Not tested	NA
107	CT_Security_SCVFQDNRootStore_STA_NonMatchFQDN-UOSCEnabled_10177_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA in trust store during an EAP exchange	Pass	P
108	CT_Security_SCVFQDNRootStore_STA_NonMatchSuffix-UOSCDisabled_10172_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA in trust store during an EAP exchange	Not tested	NA

No	Test Cases	Test Item	Test Result	Conclusion
109	CT_Security_SCVFQDNRootStore_STA_NonMatchSuffix-UOSCEnabled_10173_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) and root CA in trust store during an EAP exchange	Pass	P
110	CT_Security_SCVNetworkProfileConfig_STA_NoEAPAuth_10440_1 [12]	This test verifies that, when the STAUT is in unconfigured state (do not explicitly disable server validation), the STAUT does not successfully complete the 802.1X EAP exchange	Not tested	NA
111	CT_Security_SCVNetworkProfileConfig_STA_NoValidate_10441_1 [12]	This test verifies that, when the STAUT is configured to explicitly disable server validation (select "Don't validate" or similar in STAUT UI), the STAUT does not successfully complete the 802.1X EAP exchange	Not tested	NA
112	CT_Security_SCVNetworkProfileConfig_STA_TrustStoreonly_10442_1 [12]	This test verifies that, when the STAUT is configured to use system trust store only (do not explicitly disable server validation), the STAUT does not successfully complete the 802.1X EAP exchange	Not tested	NA
113	CT_Security_SCVRootCA_STA_BadRootCA-UOSCDisabled_10438_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured root CA during an EAP exchange	Not tested	NA
114	CT_Security_SCVRootCA_STA_BadRootCA-UOSCEnabled_10439_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured root CA during an EAP exchange	Pass	P
115	CT_Security_SCVRootCA_STA_Match_10144_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured root CA during an EAP exchange	Pass	P
116	CT_Security_SCVRootCA_STA_NonMatch-TODSTRICTServer-UOSCDisabled_10178_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured root CA during an EAP exchange	Not tested	NA
117	CT_Security_SCVRootCA_STA_NonMatch-TODSTRICTServer-UOSCEnabled_10179_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured root CA during an EAP exchange	Pass	P
118	CT_Security_SCVRootCA_STA_NonMatch-TODTOFU-UOSCDisabled_10180_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured root CA during an EAP exchange	Not tested	NA
119	CT_Security_SCVRootCA_STA_NonMatch-TODTOFU-UOSCEnabled_10181_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured root CA during an EAP exchange	Pass	P

No	Test Cases	Test Item	Test Result	Conclusion
120	CT_Security_SCVSuffixRootCA_STA_BadRootCA-UOSCDisabled_10291_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) suffix and root CA during an EAP exchange	Not tested	NA
121	CT_Security_SCVSuffixRootCA_STA_BadRootCA-UOSCEnabled_10292_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) suffix and root CA during an EAP exchange	Pass	P
122	CT_Security_SCVSuffixRootCA_STA_Match_10151_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) suffix and root CA during an EAP exchange	Pass	P
123	CT_Security_SCVSuffixRootCA_STA_NonMatchSuffix-UOSCDisabled_10170_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) suffix and root CA during an EAP exchange	Not tested	NA
124	CT_Security_SCVSuffixRootCA_STA_NonMatchSuffix-UOSCEnabled_10171_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) suffix and root CA during an EAP exchange	Pass	P
125	CT_Security_SCVSuffixRootStore_STA_BadPublicCA-UOSCDisabled_10443_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) suffix and root store during an EAP exchange	Not tested	NA
126	CT_Security_SCVSuffixRootStore_STA_BadPublicCA-UOSCEnabled_10444_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) suffix and root store during an EAP exchange	Pass	P
127	CT_Security_SCVSuffixRootStore_STA_Match_10147_1 [12]	This test verifies that the STAUT correctly performs server certificate validation with explicitly configured server domain (FQDN) suffix and root store during an EAP exchange	Pass	P
128	CT_Security_WPA3Enterprise_STA_NoAssociation-WPA2Enterprise_104652 [12]	This test verifies that the STAUT does not associate to test bed AP when configured for WPA2 Enterprise security in 6 GHz	Not tested	NA
129	CT_Security_WPA3Enterprise_STA_NoAssociation-WPAEnterprise_10464_2 [12]	This test verifies that the STAUT does not associate to test bed AP when configured for WPA Enterprise security in 6 GHz	Not tested	NA

No	Test Cases	Test Item	Test Result	Conclusion
130	CT_Security_RSN_STA_CapabilitiesVerification-ReservedBits-31_10603_1 [12]	This test verifies that the STAUT successfully associates, authenticates and passes data traffic when reserved bits in the RSN Capabilities and Extended RSN Capabilities fields are set to one instead of zero, and when the RSNXE is extended. This test also verifies that the STAUT does not set optional feature bits to one in the RSN Capabilities and Extended RSN Capabilities fields on transmission when unsupported and ignores them on reception.	Pass	P
131	CT_Security_RSN_STA_CapabilitiesVerification-ReservedBits-SAE-PK_10604_1 [12]	This test verifies that the STAUT successfully associates, authenticates and passes data traffic when reserved bits in the RSN Capabilities and Extended RSN Capabilities fields are set to one instead of zero, and when the RSNXE is extended. This test also verifies that the STAUT does not set optional feature bits to one in the RSN Capabilities and Extended RSN Capabilities fields on transmission when unsupported and ignores them on reception.	Pass	P
132	CT_Security_RSN_STA_CapabilitiesVerification-ReservedBits-Extra_10605_1 [12]	This test verifies that the STAUT successfully associates, authenticates and passes data traffic when reserved bits in the RSN Capabilities and Extended RSN Capabilities fields are set to one instead of zero, and when the RSNXE is extended. This test also verifies that the STAUT does not set optional feature bits to one in the RSN Capabilities and Extended RSN Capabilities fields on transmission when unsupported and ignores them on reception.	Pass	P

ANNEX C: TEST LAYOUT



Wi-Fi Certification Test Laboratory

ANNEX D: Accreditation Certificate

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 张朝华

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*****