CONFIDENTIAL TRADE SECRET

FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE® MEMBERS

– DO NOT COPY –

WPA2™ Security Improvements

Test Plan

Version 1.1

10900-B Stonelake Boulevard, Suite 126
Austin, TX 78759

Phone: 512.498.9434 • Fax: 512.498.9435 • Email: support@wi-fi.org
www.wi-fi.org

Latest version available at: https://www.wi-fi.org/members/task-group-resources

WI-FI ALLIANCE PROPRIETARY AND CONFIDENTIAL – SUBJECT TO CHANGE WITHOUT NOTICE

Table of contents

List of tables

List of figures

1 Overview

1.1 Scope and purpose

A primary goal of Wi-Fi Alliance is to ensure interoperability among Wi-Fi CERTIFIED products from multiple manufacturers, and to promote this technology within both the business and consumer markets. To this end, the following compliance test plan was developed. Working in conjunction with authorized test labs, these tests will be executed on vendor products for the WPA2™ Security Improvements feature.

The scope of this test plan is governed by the Wi-Fi Alliance Security Enhancements Marketing Requirements Document (MRD) [1].

1.2 Definition of devices under test

The device under test (DUT) may be an Access Point (APUT) or Station (STAUT) that will be tested for the WPA2 Security Improvements feature using this test plan. The general characteristics of the DUT are entered in the Wi-Fi Alliance website registration system and are summarized in Table 1 and Table 2 respectively.

Prior to submission to the authorized test labs, the implementer shall complete the following capabilities declaration tables for use in performing this certification testing.

Table 1. APUT general capabilities declaration

Item	Question	Test case	Vendor response
1	Does the APUT support WPA2™-Enterprise?	4.2.1	Yes/No
2	Does the APUT support Joint Multi-band RSNA?	4.2.3	Yes/No
3	Does the APUT support PeerKey handshake?	4.2.3	Yes/No
4	Does the APUT support signaling and payload protected (SPP) A-MSDU's transmission and reception?	4.2.3	Yes/No
5	Does the APUT only allow SPP A-MSDU's transmission and reception?	4.2.3	Yes/No
6	Does the APUT support protected block ack agreement capability (PBAC)?	4.2.3	Yes/No
7	Does the APUT support Extended Key ID for individually addressed frames?	4.2.3	Yes/No

Table 2. STAUT general capabilities declaration

Item	Question	Test case	Vendor response
1	Does the STAUT support WPA2-Enterprise?	5.2.1, 5.2.5	Yes/No
2	Does the STAUT support WEP default key 0 simultaneously with a pairwise key in a TSN network?	5.2.3	Yes/No
3	Does the STAUT support Joint Multi-band RSNA?	5.2.3	Yes/No
4	Does the STAUT support PeerKey handshake?	5.2.3	Yes/No

Item	Question	Test case	Vendor response
5	Does the STAUT support signaling and payload protected (SPP) A-MSDU's transmission and reception?	5.2.3	Yes/No
6	Does the STAUT only allow SPP A-MSDU's transmission and reception?	5.2.3	Yes/No
7	Does the STAUT support protected block ack agreement capability (PBAC)?	5.2.3	Yes/No
8	Does the STAUT support Extended Key ID for individually addressed frames?	5.2.3	Yes/No
9	Provide the list of EAP methods supported by the STAUT.	5.2.5	Value

1.3 References

The documents listed in this section are included in requirements made in the body of this test plan. Knowledge of their contents is required for the understanding and implementation of this test plan. If a listing includes a date or a version identifier, only that specific version of the document is required. If the listing includes neither a date nor a version identifier, the latest version of the document is required.

[1] Security Enhancements Marketing Requirements Document, v1.21, https://www.wi-fi.org/file-member/security-enhancements-mrd

[2] IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," IEEE Std 802.11-2016, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6178212&isnumber=6178210

[3] IEEE 802.1X-2010 - IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control

[4] Wi-Fi Alliance 60 GHz Technical Specification, https://www.wi-fi.org/members/certification-programs

1.4 Acronyms and definitions

1.4.1 Acronyms and abbreviations

Table 3 defines the acronyms and abbreviations used throughout this document. Some acronyms and abbreviations are commonly used in publications and standards defining the operation of wireless local area networks, while others have been generated by Wi-Fi Alliance. Refer to the Wi-Fi Alliance Acronyms Terms Definitions document for a complete list of approved acronyms and abbreviations.

Table 3. Acronyms and abbreviations

Acronyms	Definition
A-BFT	Association Beamforming Training
AKM	Authentication Key Management
AP	Access Point

Acronyms	Definition
APUT	Access Point under test
BRP	Beam refinement protocol
CA	Certification authority
CBAP	Contention-based Access Period
CCMP	Counter Mode CBC-MAC Protocol
CTT	Compliance test tool
DMG	Directional multi-gigabit
DUT	Device Under Test
EAP	Extensible Authentication Protocol
EDCA	Enhanced distributed channel access
GCMP	Galois/Counter Mode Protocol
MFPC	Management frame protection capable
MFPR	Management frame protection required
PMF	Protected Management Frames
PMK	Pairwise Master Key
PSK	Pre-Shared Key
PTK	Pairwise Transient Key
QoS	Quality of service
RSNE	Robust Security Network Element
RSS	Responder sector sweep
SLS	Sector-level sweep
SPP	Signaling and payload protected
SSID	Service Set Identifier
SSW	Sector sweep
STA	Station
STAUT	Station under test
TPTK	Temporary Pairwise Transient Key

Acronyms	Definition
TSN	Transition Security Network

1.4.2 Definitions

There are no special definitions for this test plan.

2 Test tools, methodology and approach

This section defines the tools, methodology, and approach for testing devices for WPA2 Security Improvements.

2.1 Sniffer

A sniffer test tool is required to be used for test cases throughout this test plan. The sniffer test tool requirements are:

- Supports 802.11 a/b/g/n/ac
- Supports 802.11 ad
  - Capture and decode DMG frames
  - Capture and decode 60 GHz specific elements
- Ability to parse IEEE 802.1x EAPOL key frames used in the 4-way handshake

2.2 Wi-Fi Test Suite software

The Wi-Fi Alliance's Wi-Fi Test Suite provides configuration, test control, traffic generation, and results analysis services. Unless otherwise noted, the entire test plan may be executed in a fully automated manner using Wi-Fi Alliance-distributed Wi-Fi Test Suite Command Scripts and the Wi-Fi Test Suite Unified CAPI Console. Additional information is available through the member website https://www.wi-fi.org/members/certification-testing/wi-fi-test-suite.

2.3 Basic system test configuration

Figure 1 depicts the basic system test configuration for testing compliance among WPA2 Security Improvements devices.

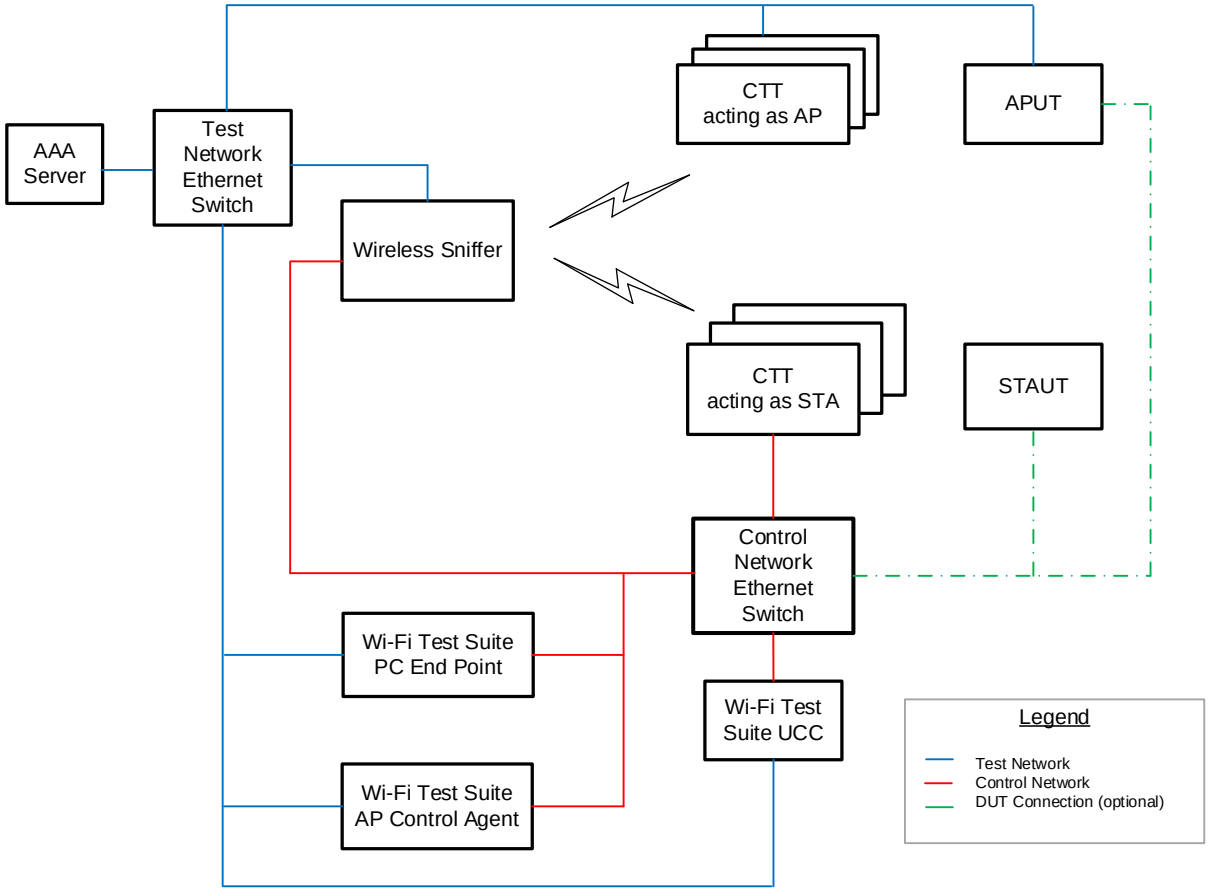

Figure 1. System test configuration

2.3.1 Test bed layout for Wi-Fi CERTIFIED WiGig testing

The test bed layout shall meet the following requirements:

1. Place all APs on a bench at the same height where the STAs are positioned.
2. Ensure a line of sight between devices participating in the test procedure.
3. The distance between APs and STAs shall not exceed four feet and shall not be less than one foot.
4. Tests shall be conducted in an RF chamber.

2.4 Test bed/CTT capability requirements

2.4.1 2.4 GHz and 5 GHz testing

2.4.1.1 Test bed AP requirements

Table 4 defines the WPA2 Security Improvements default parameters for the test bed AP. If required, these default parameter values are modified for specific test cases.

Table 4. Test bed AP default parameters

Parameter	Default value
SSID	Wi-Fi
Operating channel	44 (if dual band STAUT, else 6)
Security	WPA2™-Personal (CCMP-128)
Passphrase	12345678
PMF	Enabled MFPR (bit 6) set to 0 and MFPC (bit 7) bit set to 1 in RSN Capabilities field

2.4.1.2 Test bed STA requirements

Table 5 defines the WPA2 Security Improvements default parameters for the test bed STA. If required, these default parameter values are modified for specific test cases.

Table 5. Test bed STA default parameters

Parameter	Default value
Security	WPA2-Personal (CCMP-128)
Passphrase	12345678
PMF	Enabled MFPR (bit 6) set to 0 and MFPC (bit 7) bit set to 1 in RSN Capabilities field

2.4.2 60 GHz testing

2.4.2.1 Test bed AP requirements

Table 6 defines the WPA2 Security Improvements default parameters for the test bed AP. If required, these default parameter values are modified for specific test cases.

Table 6. Test bed AP default parameters

Parameter/Mode Name	Default value	Notes
SSID	Wi-Fi	
Operating channel	2	
Cipher Suite Type	8 (GCMP-128)	
Passphrase	12345678	
PHY Mode – SC	On	MCSs 5 to 12 disabled if supported
TX A-MSDU	Off	
TX A-MPDU	Off	
BRP Training	Off	

2.4.2.2 Test bed STA requirements

Table 7 defines the WPA2 Security Improvements default parameters for the test bed STA. If required, these default parameter values are modified for specific test cases.

Table 7. Test bed STA default parameters

Parameter/Mode Name	Default value	Notes
Cipher Suite Type	8 (GCMP-128)	
Passphrase	12345678	
PHY Mode – SC	On	MCSs 5 to 12 disabled if supported
TX A-MSDU	Off	
TX A-MPDU	Off	
BRP Training	Off	

3 Requirements for Wi-Fi Alliance certification

The following items describe the necessary features that are required for a DUT to pass WPA2 Security Improvements feature testing.

3.1 General requirements

3.1.1 Prerequisite certification requirements

There are no prerequisite certification requirements for the APUT and STAUT.

3.1.2 Testing requirements

For 60GHz testing, a DUT may disable Wi-Fi Simple Configuration functionality for executing WPA2 Security Improvements test plan.

3.2 Applicability of tests

The applicable tests for certification are the tests of mandatory features and tests of optional features that a vendor chooses to declare or that are indicated by the DUT as described in the underlying technical specifications. Table 8 and Table 9 list the applicable tests for the APUT and STAUT respectively.

“Applicability” indicates whether a feature and its associated tests are either mandatory or optional to implement. Mandatory (M) tests are required for certification.

Optional (O) tests are performed if the vendor declares the feature, or the DUT indicates the feature as described in the underlying technical specifications via transmitted frames or transmitted messages or user interfaces. If the optional feature is declared and if that test fails, the DUT shall fail the WPA2 Security Improvements feature testing. Conditional (C) tests are mandatory if certain specified conditions pertain to the DUT (again, as declared by the vendor during the submission or indicated by the DUT), and are optional otherwise.

If the feature requires information, in particular if the vendor implements or supports an optional feature, the fourth column contains a “Y” and the vendor shall provide information in the DUT Information spreadsheet. (A copy of the spreadsheet is accessible through the online Wi-Fi Alliance Certification System.)

If a vendor declares an optional feature, that feature shall be indicated by the DUT as described in the underlying technical specifications. Declaration of an optional feature by a vendor comprises inclusion of the feature in the appropriate Wi-Fi Alliance registration and DUT Information spreadsheet at the time of submission. An optional feature that was not declared, but is indicated within an associated capabilities field(s), IE’s, or any transmitted frames comprises inclusion of the feature.

Each vendor shall fill out the DUT Information spreadsheet completely. Test labs will verify that the list of optional features declared by the vendor matches the list indicated by the DUT; each optional feature for which any test exists in this test plan and that appears in one list shall also appear in the other. The information determines which tests and which test parameters apply to the certification.

A “Y” in the last column indicates the certain subset of optional capabilities that will be indicated on the interoperability certificate if they are declared by the vendor.

3.2.1 APUT tests

Table 8 summarizes the APUT tests for WPA2 Security Improvements certification.

Table 8. APUT test applicability

Test case description	Test plan section	Applicability: Mandatory (M) / Optional (O) / Conditional (C)	Should feature be listed in the Capabilities Form? (Y/N)	If implemented, displayed in certificate? (Y/N)
APUT RSNE bounds verification using WPA2-Enterprise test	4.2.1	C	Y, refer to Table 1	N
APUT handles RSNE unexpected value test	4.2.2	M		N
APUT verification of RSN Capabilities test	4.2.3	M		N
APUT RSNE bounds verification using WPA2-PSK test	4.2.4	M		N

3.2.2 STAUT tests

Table 9 summarizes the STAUT tests for WPA2 Security Improvements certification.

Table 9. STAUT test applicability

Test case description	Test plan section	Applicability: Mandatory (M) / Optional (O) / Conditional (C)	Should feature be listed in the Capabilities Form? (Y/N)	If implemented, displayed in certificate as? (Y/N)
STAUT RSNE bounds verification using WPA2-Enterprise test	5.2.1	C	Y, refer to Table 2	N
STAUT handles RSNE unexpected values test	5.2.2	M		N
STAUT verification of RSN Capabilities test	5.2.3	M		N
STAUT RSNE bounds verification using WPA2-PSK test	5.2.4	M		N
STAUT unknown Root CA detection test	5.2.5	C	Y, refer to Table 2	N
STAUT replay protection test	5.2.6	M		N

3.3 Configuration requirements

The DUT parameters that require manual configuration are listed below.

5. SSID
6. Wireless operational mode (a/n/ac/ad)

7. Channel
8. Local IP address and subnet mask

If any of the above items cannot be configured through the user interface, then the DUT test fails.

3.3.1 2.4 GHz and 5 GHz testing

3.3.1.1 APUT configuration requirements

Table 10 lists the default APUT configuration values that a technician shall set within a test procedure. Specific test cases may impose additional configuration requirements.

Table 10. APUT default configuration requirements

Item	Configuration requirement	Default value
1	SSID	Wi-Fi
2	Operating channel	44 (if dual band APUT, else 6)
3	Security	WPA2-Personal (CCMP-128)
4	Passphrase	12345678
5	PMF	Out-of-the-box

3.3.1.2 STAUT configuration requirements

Table 11 lists the default STAUT configuration values that a technician shall set within a test procedure. Specific test cases may impose additional configuration requirements.

Table 11. STAUT default configuration requirements

Item	Configuration requirement	Default value
1	Security	WPA2-Personal (CCMP-128)
2	Passphrase	12345678
3	PMF	Out-of-the-box

3.3.2 60 GHz testing

3.3.2.1 APUT configuration requirements

Table 12 lists the default APUT configuration values that a technician shall set within a test procedure. Specific test cases may impose additional configuration requirements.

Table 12. APUT default mode configuration

Item	Mode name	Default
1	SSID	Wi-Fi
2	Operating channel	2
3	Cipher Suite Type	8 (GCMP-128)
4	Passphrase	12345678
5	TX A-MSDU	On (If supported)
6	TX A-MPDU	On (If supported)
7	BRP Training	On (If supported)
8	Wi-Fi Simple Config	Enabled

3.3.2.2 STAUT configuration requirements

Table 13 lists the default STAUT configuration values that a technician shall set within a test procedure. Specific test cases may impose additional configuration requirements.

Table 13. STAUT default mode configuration

Item	Mode name	Default
1	Cipher Suite Type	8 (GCMP-128)
2	Passphrase	12345678
3	TX A-MSDU	On (If supported)
4	TX A-MPDU	On (If supported)
5	BRP Training	On (If supported)
6	Wi-Fi Simple Config feature	Enabled
7	Wi-Fi Peer-to-Peer feature	Enabled

3.4 Testing rules

1. If the DUT fails any tests, no further testing will be performed until the vendor addresses the problems and has updated the device.
2. The default DUT parameters shall be configured on devices at the start of each test case unless otherwise noted.

4 WPA2 Security Improvements APUT tests

4.1 APUT configuration requirements validation test

This section is not applicable to an APUT undergoing Security Improvements testing.

4.2 APUT test cases

For a WiGig APUT device, Table 14 lists the initial test configuration steps that shall be completed between a test bed STA and the APUT when referred by test cases in this section as an initial test configuration.

Table 14. APUT and test bed STA initial test configuration

Step	APUT	CTT acting as a test bed STA	Expected result
1		Disassociate if already associated.	
2	Starts transmission of DMG Beacon frames.		SN: If the DMG Privacy subfield in the DMG Parameters field is set to 1, then CONTINUE else FAIL. SN: Verify that IF RSNE is present in the captured DMG Beacon frame, the following fields of the RSNE are set accordingly: 1. Version field is set to 01 00. 2. Group Data Cipher Suite is set to 00-0F-AC:8. 3. Pairwise Cipher Suite Count is set to 0x 01 00. 4. Pairwise Cipher Suite List is set to GCMP 00-0F-AC:8. 5. AKM Suite Count is set to 0x 01 00. 6. AKM Suite List is set to 00-0F-AC:1. 7. PMKID Count is set to 0 or is not present. 8. PMKID List is not present. If all the conditions above are met, then CONTINUE, else FAIL.
3		Receives DMG Beacon and performs SLS with the APUT during the A-BFT or during DTI period when offered by the APUT.	NOTE – The RSS component of the SLS is a Responder TXSS if the value of the IsResponderTXSS subfield of the Beacon Interval Control field is equal to 1.
4	Responds to each received Probe Request frame with ACK, and follows by transmitting a Probe Response frame.	Optionally, sends a Probe Request frame with the Address 1 (RA) field set to the APUT MAC address, and the Address 3 (BSSID) field set to the APUT MAC address or wildcard BSSID.	If the APUT does not respond with ACK and then a Probe Response frame to each individually-addressed Probe Request frame then FAIL. Otherwise CONTINUE. SN: Verify that the RSNE is present in the captured Probe Response frame and that the following fields of the RSNE are set accordingly: 1. Version field is set to 01 00. 2. Group Data Cipher Suite is set to 00-0F-AC:8. 3. Pairwise Cipher Suite Count is set to 0x 01 00.

Step	APUT	CTT acting as a test bed STA	Expected result
			4. Pairwise Cipher Suite List is set to GCMP 00-0F-AC:8. 5. AKM Suite Count is set to 0x 01 00. 6. AKM Suite List is set to 00-0F-AC:1. 7. PMKID Count is set to 0 or is not present. 8. PMKID List is not present. If all the conditions above are true, then CONTINUE, else FAIL.
5	During a CBAP, any device (Test bed STA or APUT) with channel access rights can perform further transmit or receive training using one or more of the following methods: BRP with receive or transmit training, in any order, including both • Transmission of a Grant frame signaling TXSS • Transmission of an SSW frame signaling TXSS		

4.2.1 APUT RSNE bounds verification using WPA2-Enterprise test

Objective

This test verifies that the APUT correctly handles unexpected RSNE termination, and then successfully associates to the STA and passes data traffic,

Applicability: Conditional. This test case is only required if the APUT declared support for WPA2-Enterprise in Table 1.

References

Section 9.4.2.25 [2]

Section 3.1 [4]

Test environment

- APUT
- CTT acting as a test bed STA
- Wireless Sniffer
- AAA server

Test configuration

Table 15, Table 16 and Table 17 define the specific parameter values required for this test case.

Table 15. APUT RSNE bounds verification using WPA2-Enterprise test configuration

Parameter	APUT value	CTT acting as a test bed STA value	AAA server
Test bed vendor	N/A	For 2.4 or 5 GHz: Intel For 60 GHz: Qualcomm	HostAPD

Parameter	APUT value	CTT acting as a test bed STA value	AAA server
SSID	Wi-Fi	N/A	N/A
Operating channel	For dual band 2.4 and 5 GHz: 6 or For 5 GHz only: 44 For 60 GHz: 2	N/A	N/A
Security	WPA2-Enterprise (EAP-TLS)	WPA2-Enterprise (EAP-TLS)	EAP-TLS
PMF configuration (2.4 and 5 GHz)	Scenario A - F, H - J: Out-of-the-box Scenario G: MFPR (bit 6) and MFPC (bit 7) bits set to 0 in RSN Capabilities field	Scenario E - J: MFPC (bit 7) set to 1	N/A
PMF configuration (60 GHz)	Out-of-the-box	Disable PMF configuration in the RSNE for all scenarios	N/A

Table 16. RSNE configuration on CTT for test case 4.2.1 (for 2.4 GHz or 5 GHz)

Scenario	RSNE format (in hex)	Description
Scenario A	30 (Element ID) 02 (Length in octets) 01 00 (Version 1)	None of the optional fields are included in the RSNE
Scenario B	30 (Element ID) 06 (length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite)	The following optional field is included in the RSNE • Group Data Cipher Suite
Scenario C	30 (Element ID) 0C (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List
Scenario D	30 (Element ID) 12 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List

Scenario	RSNE format (in hex)	Description
Scenario E	30 (Element ID) 14 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 80 00 (management frame protection is enabled but not required)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities
Scenario F	30 (Element ID) 16 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 80 00 (management frame protection is enabled but not required) 00 00 (No PMKIDs)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count
Scenario G	30 (Element ID) 1A (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 80 00 (management frame protection is enabled but not required) 00 00 (No PMKIDs) 00 0F AC 06 (BIP-CMAC-128 as group management cipher suite)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count • Group Management Cipher Suite
Scenario H	30 (Element ID) 1F (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count • Group Management Cipher Suite

Scenario	RSNE format (in hex)	Description
	00 0F AC 01 (IEEE Std 802.1X authentication) 80 00 (management frame protection is enabled but not required) 00 00 (No PMKIDs) 00 0F AC 06 (BIP-CMAC-128 as group management cipher suite) 04 00 01 02 03 (Undefined subfield)	• RSNE extensible element (5 octets)
Scenario I	30 (Element ID) 2A (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 80 00 (management frame protection is enabled but not required) 01 00 (PMK ID count 1) 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 (PMK ID) 00 0F AC 06 (BIP-CMAC-128 as group management cipher suite)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMK ID Count and Invalid PMK ID • Group Management Cipher Suite
Scenario J	30 (Element ID) 16 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 80 00 (management frame protection is enabled but not required) 01 00 (PMKID Count)	PMK ID count is 1 but no PMK ID present in the List field

Table 17. RSNE configuration on CTT for test case 4.2.1 (for 60 GHz)

Scenario	RSNE format (in hex)	Description
Scenario A	30 (Element ID) 02 (Length in octets) 01 00 (Version 1)	None of the optional fields are included in the RSNE
Scenario B	30 (Element ID) 06 (length in octets) 01 00 (Version 1)	The following optional field is included in the RSNE • Group Data Cipher Suite

Scenario	RSNE format (in hex)	Description
	00 0F AC 08 (GCMP-128 as group data cipher suite)	
Scenario C	30 (Element ID) 0C (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List
Scenario D	30 (Element ID) 12 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List
Scenario E	30 (Element ID) 14 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities
Scenario F	30 (Element ID) 16 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 00 00 (No PMKIDs)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count
Scenario G	30 (Element ID) 1A (Length in octets) 01 00 (Version 1)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List

Scenario	RSNE format (in hex)	Description
	00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 00 00 (No PMKIDs) 00 0F AC 0B (BIP-GMAC-128 as group management cipher suite)	• AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count • Group Management Cipher Suite
Scenario H	30 (Element ID) 1F (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 00 00 (No PMKIDs) 00 0F AC 0B (BIP-GMAC-128 as group management cipher suite) 04 00 01 02 03 (Undefined subfield)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count • Group Management Cipher Suite • RSNE extensible element (5 octets)
Scenario I	30 (Element ID) 2A (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 01 00 (PMK ID count 1) 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 (PMK ID) 00 0F AC 0B (BIP-GMAC-128 as group management cipher suite)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMK ID Count and Invalid PMK ID • Group Management Cipher Suite
Scenario J	30 (Element ID) 16 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication)	PMK ID count is 1 but no PMK ID present in the List field

Scenario	RSNE format (in hex)	Description
	01 00 (PMKID Count)	

Test procedure and expected results

Table 18 provides the test procedure and expected results for this test case for 2.4 or 5 GHz capable APUT.

Table 18. APUT RSNE bounds verification using WPA2-Enterprise test procedure and expected results

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
1	Power on the APUT. Reset the device to its default configuration as specified in Table 10 Configure the APUT to transmit Beacon frames.			SN: Verify that the RSNE is present in the captured Beacon frame and that the following fields of the RSNE are set accordingly: 1. Version field is set to 01 00. 2. Group Data Cipher Suite is set to 00-0F-AC:4. 3. Pairwise Cipher Suite Count is set to 0x 01 00. 4. Pairwise Cipher Suite List is set to CCMP 00-0F-AC:4. 5. AKM Suite Count is set to 0x 01 00. 6. AKM Suite List is set to 00-0F-AC:1. 7. PMKID Count is set to 0 or is not present. 8. PMKID List is not present. If all the conditions above are met, then CONTINUE, else FAIL.
2	The APUT transmits a Probe Response frame.	Reset the STA to its default configuration as specified in Table 5. Configure the STA to perform an active scan in the APUT's operating channel. The STA transmits a Probe Request frame.	Verify that a broadcast Probe Request frame with SSID set to wildcard is transmitted in the APUT's operating channel.	SN: Verify that the RSNE is present in the captured Probe Response frame and that the following fields of the RSNE are set accordingly: 1. Version field is set to 01 00. 2. Group Data Cipher Suite is set to 00-0F-AC:4. 3. Pairwise Cipher Suite Count is set to 0x 01 00. 4. Pairwise Cipher Suite List is set to CCMP 00-0F-AC:4. 5. AKM Suite Count is set to 0x 01 00. 6. AKM Suite List is set to 00-0F-AC:1. 7. PMKID Count is set to 0 or is not present. 8. PMKID List is not present. If all the conditions above are true, then CONTINUE, else FAIL.
3		Configure the device as per Table 16.		

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
4	The APUT transmits an Association Response frame.	The STA transmits an Association Request frame.	Verify that an Association Request frame is transmitted by the STA containing an RSNE as per the configuration in Table 16.	SN: For all scenarios except G and J: If the Association Response frame contains SUCCESS (Status Code field set to 0) then CONTINUE, else FAIL. For scenario G and J: If the Association Response frame is transmitted by APUT and contains a SUCCESS (Status Code field set to 0), then CONTINUE. Else if the Association Response frame is transmitted by APUT and does not contain a SUCCESS then PASS, else FAIL.
5	The APUT and STA complete: • EAP authentication • 4-way handshake • DHCP exchange			SN: If the APUT successfully completes EAP authentication followed by 4-way handshake, then CONTINUE, else FAIL.
6		Configure the STA to ping the console IP address. <ping CONSOLE_IP_ADDR>, COUNT = 3, FRAME_RATE = 1		If the ping is successful, then PASS else FAIL.
Repeat Steps 3 - 6 for each scenario specified in Table 16.				

Table 19 provides the test procedure and expected results for this test case 60 GHz capable APUT.

Table 19. APUT RSNE bounds verification using WPA2-Enterprise test procedure and expected results

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
1	Turn on the APUT. Reset the device to its default configuration as specified in Table 12.	Reset the test bed STA to its default configuration as specified in Table 7.		
2	Perform the APUT and test bed STA initial configuration as described in Table 14.			
3		Configure the device as per Table 17.		
4	The APUT transmits an Association Response frame.	The STA transmits an Association Request frame.	Verify that an Association Request frame is transmitted by the STA containing an RSNE as per the configuration in Table 17.	SN: For all scenarios except G and J: If the Association Response frame contains SUCCESS (Status Code field set to 0) then CONTINUE, else FAIL.

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
				a. If the Association Response frame contains the 60 GHz IE, then CONTINUE else FAIL. b. If the EDCA Parameter Set element, DMG Capabilities element and DMG Operation element are present in the Association Response frame, then CONTINUE else FAIL. For scenario G and J: If the Association Response frame is transmitted by APUT and contains a SUCCESS (Status Code field set to 0), then CONTINUE. a. If the Association Response frame contains the 60 GHz IE, then CONTINUE else FAIL. b. If the EDCA Parameter Set element, DMG Capabilities element and DMG Operation element are present in the Association Response frame, then CONTINUE else FAIL. Else if the Association Response frame is transmitted by APUT and does not contain a SUCCESS then PASS, Else FAIL.
5	The APUT and STA complete: • EAP authentication • 4-way handshake • DHCP exchange			SN: If the APUT successfully completes EAP authentication followed by 4-way handshake, then CONTINUE, else FAIL.
6		Configure the STA to ping the console IP address. <ping CONSOLE_IP_ADDR>, COUNT = 20, FRAME_RATE = 1		If more than 5 consecutive ping timeouts occur in any of the ping tests, then FAIL. If more than 10% ping failures in any of the ping tests, then FAIL. If no fail messages are received, then PASS.
Repeat Steps 3 - 6 for each scenario specified in Table 17.				

4.2.2 APUT handles RSNE unexpected value test

Objective

This test verifies that the APUT correctly handles unexpected values in the RSN element and appropriately accepts or rejects an association request.

Applicability: Mandatory

References

Section 9.4.2.25 [2]

Test environment

- APUT
- CTT acting as a test bed STA
- Wireless Sniffer

Test configuration

Table 20, Table 21 and Table 22 define the specific parameter values required for this test case.

Table 20. APUT handles RSNE unexpected value test configuration

Parameter	APUT value	CTT acting as a test bed STA value
Test bed vendor	N/A	For 2.4 or 5 GHz: Qualcomm For 60 GHz: Qualcomm
SSID	Wi-Fi	N/A
Operating channel	For dual band 2.4 and 5 GHz: 6 or For 5 GHz only: 44 For 60 GHz: 2	N/A
Security	WPA2-PSK	WPA2-PSK
PMF configuration (2.4 and 5 GHz)	Out-of-the-box	MFPC
PMF configuration (60 GHz)	Out-of-the-box	Disable PMF configuration in the RSNE for all scenarios

Table 21. RSNE configuration on CTT for test case 4.2.2 (for 2.4 and 5 GHz)

Scenario	RSNE format (in hex)	Description
Scenario A	30 (Element ID) 16 (Length in octets) 02 00 (Version 2) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count)	RSN protocol Version field is set to value 2

Scenario	RSNE format (in hex)	Description
	00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 00 (management frame protection is enabled but not required) 00 00 (No PMKIDs)	
Scenario B	30 (Element ID) 12 (Length in octets) 01 00, (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 00 00, (pairwise cipher suite count) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 00 (management frame protection is enabled but not required) 00 00 (No PMKIDs)	Pairwise Cipher Suite Count field value is set to 0 (Pairwise Cipher Suite List field is not present)
Scenario C	30 (Element ID) 10 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 00 00 (AKM suite count) 80 00 (management frame protection is enabled but not required)	AKM Suite Count field value is set to 0 (AKM Suite List field is not present)
Scenario D	30 (Element ID) 0C (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 00 00 (pairwise cipher suite count) 00 00 (AKM suite count) 80 00 (management frame protection is enabled but not required)	Pairwise Cipher Suite Count field value is set to 0 (Pairwise Cipher Suite List field is not present) AKM Suite Count field value is set to 0 (AKM Suite List field is not present)
Scenario E	30 (Element ID) 16 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count)	Preauthentication subfield of the RSN Capabilities field is set to 1

Scenario	RSNE format (in hex)	Description
	00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 81 00 (preauthentication is supported) 00 00 (No PMKIDs)	
Scenario F	30 (Element ID) 01 (Length in octets) 01 (Version 1) - truncated to 1 octet	RSN Version field is truncated to 1 octet
Scenario G	30 (element id, 48 in hex) 05 (length in octets in hex) 01 00 (Version 1) 00 0F AC (truncated)	Group Data Cipher Suite truncated
Scenario H	30 (Element ID) 0B (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC (truncated)	Pairwise Cipher Suite List truncated
Scenario I	30 (Element ID) 11 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC (truncated)	AKM Suite List truncated
Scenario J	30 (Element ID) 13 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 (truncated)	RSN Capabilities truncated
Scenario K	30 (Element ID) 15 (Length in octets)	PMKID count truncated

Scenario	RSNE format (in hex)	Description
	01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 00 (management frame protection is enabled but not required) 00 (truncated)	
Scenario L	30 (Element ID) 0C (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 02 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite)	Pairwise Cipher count is 2 but only 1 present in the List field
Scenario M	30 (Element ID) 12 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 02 00 (AKM suite count) 00 0F AC 02 (PSK)	AKM Suite count is 2 but only 1 present in the List field
Scenario N	30 (Element ID) 16 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 00 (management frame protection is enabled but not required) 01 00 (PMKID Count)	PMK ID count is 1 but no PMK ID present in the List field
Scenario O	30 (Element ID) 1A (Length in octets) 01 00 (Version 1)	Multiple pairwise ciphers and AKMs present

Scenario	RSNE format (in hex)	Description
	00 0F AC 04 (CCMP-128 as group data cipher suite) 02 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 02 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 00 0F AC 02 (PSK)	

Table 22. RSNE configuration on CTT for test case 4.2.2 (for 60 GHz)

Scenario	RSNE format (in hex)	Description
Scenario A	30 (Element ID) 16 (Length in octets) 02 00 (Version 2) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 00 00 (No PMKIDs)	RSN protocol Version field is set to value 2
Scenario B	30 (Element ID) 12 (Length in octets) 01 00, (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 00 00, (pairwise cipher suite count) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 00 00 (No PMKIDs)	Pairwise Cipher Suite Count field value is set to 0 (Pairwise Cipher Suite List field is not present)
Scenario C	30 (Element ID) 10 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 00 00 (AKM suite count)	AKM Suite Count field value is set to 0 (AKM Suite List field is not present)

Scenario	RSNE format (in hex)	Description
Scenario D	30 (Element ID) 0C (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 00 00 (pairwise cipher suite count) 00 00 (AKM suite count)	Pairwise Cipher Suite Count field value is set to 0 (Pairwise Cipher Suite List field is not present) AKM Suite Count field value is set to 0 (AKM Suite List field is not present)
Scenario E	30 (Element ID) 16 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 81 00 (preauthentication is supported) 00 00 (No PMKIDs)	Preauthentication subfield of the RSN Capabilities field is set to 1
Scenario F	30 (Element ID) 01 (Length in octets) 01 (Version 1) - truncated to 1 octet	RSN Version field is truncated to 1 octet
Scenario G	30 (element id, 48 in hex) 05 (length in octets in hex) 01 00 (Version 1) 00 0F AC (truncated)	Group Data Cipher Suite truncated
Scenario H	30 (Element ID) 0B (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC (truncated)	Pairwise Cipher Suite List truncated
Scenario I	30 (Element ID) 11 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count)	AKM Suite List truncated

Scenario	RSNE format (in hex)	Description
	00 0F AC (truncated)	
Scenario J	30 (Element ID) 13 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 (truncated)	RSN Capabilities truncated
Scenario K	30 (Element ID) 15 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 00 (truncated)	PMKID count truncated
Scenario L	30 (Element ID) 0C (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 02 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite)	Pairwise Cipher count is 2 but only 1 present in the List field
Scenario M	30 (Element ID) 12 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 02 00 (AKM suite count) 00 0F AC 02 (PSK)	AKM Suite count is 2 but only 1 present in the List field
Scenario N	30 (Element ID) 16 (Length in octets) 01 00 (Version 1)	PMK ID count is 1 but no PMK ID present in the List field

Scenario	RSNE format (in hex)	Description
	00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 01 00 (PMKID Count)	
Scenario O	30 (Element ID) 1A (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 02 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 02 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 00 0F AC 02 (PSK)	Multiple pairwise ciphers and AKMs present

Test procedure and expected results

Table 23 provides the test procedure and expected results for this test case for 2.4 or 5 GHz capable APUT.

Table 23. APUT handles RSNE unexpected value test procedure and expected results

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
1	Power on the APUT. Reset the device to its default configuration as specified in Table 10. Configure the APUT to transmit Beacon frames.	Reset the STA to its default configuration as specified in Table 5.		
2	The APUT transmits a Probe Response frame.	Configure the STA to perform active scan in the APUT's operating channel. The STA transmits a Probe Request frame.	Verify that a broadcast Probe Request frame with SSID set to wildcard is transmitted in the APUT's operating channel.	
3		Configure the STA as per Table 21.		
4	The APUT transmits an Association Response frame.	Configure the STA to associate with the APUT. The STA transmits an Association Request frame.	Verify that an Association Request frame is transmitted by the STA containing an	SN: For Scenarios A, F, G, H, I, N:

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
			RSNE as per the configuration in Table 21.	If the Association Response frame from the APUT does not contain SUCCESS (Status Code field set to 0), then PASS, else FAIL. For Scenarios B, C, D, E, J, K, L, M, O: If the Association Response frame is transmitted by APUT and contains a SUCCESS (Status Code field set to 0), then CONTINUE. Else if the Association Response frame is transmitted by APUT and does not contain a SUCCESS then PASS, Else FAIL.
5	The APUT and STA complete: • 4-way handshake • DHCP exchange			
6		The STA pings the console IP address. <ping CONSOLE_IP_ADDR>, COUNT = 3, FRAME_RATE = 1		If the ping is successful, then PASS else FAIL.
Repeat Steps 3 - 6 for each scenario specified in Table 21.				

Table 24 provides the test procedure and expected results for this test case for 60 GHz capable APUT.

Table 24. APUT handles RSNE unexpected value test procedure and expected results

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
1	Turn on the APUT. Reset the device to its default configuration as specified in Table 12.	Reset the test bed STA to its default configuration as specified in Table 7.		
2	Perform the APUT and test bed STA initial configuration as described in Table 14.			
3		Configure the STA as per Table 22.		
4	The APUT transmits an Association Response frame.	Configure the STA to associate with the APUT. The STA transmits an Association Request frame.	Verify that an Association Request frame is transmitted by the STA containing an RSNE as per the configuration in Table 22.	SN: For Scenarios A, F, G, H, I, N: If the Association Response frame from the APUT does not contain SUCCESS (Status Code field set to 0), then PASS, else FAIL. For Scenarios B, C, D, E, J, K, L, M, O: If the Association Response frame is transmitted by APUT and contains a SUCCESS (Status Code field set to 0), then CONTINUE. Else if the Association Response frame is transmitted by APUT and does not contain a SUCCESS then PASS,

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
				Else FAIL.
5	The APUT and STA complete: • 4-way handshake • DHCP exchange			
6		The STA pings the console IP address. <ping CONSOLE_IP_ADDR>, COUNT = 20, FRAME_RATE = 1		If more than 5 consecutive ping timeouts occur in any of the ping tests, then FAIL. If more than 10% ping failures in any of the ping tests, then FAIL. If no fail messages are received, then PASS.
Repeat Steps 3 - 6 for each scenario specified in Table 22.				

4.2.3 APUT verification of RSN Capabilities test

Objective

This test verifies that the APUT successfully associates, authenticates and passes data traffic when reserved bits 15 and 14 in the RSN Capabilities field are set to one instead of zero. This test also verifies that the APUT does not set the optional feature bits to one in the RSN Capabilities field on transmission when unsupported and ignores the optional bits on reception.

Applicability: Mandatory

References

Section 9.4.2.25.4 [2]

Test environment

- APUT
- CTT acting as a test bed STA
- Wireless Sniffer

Test configuration

Table 25, Table 26 and Table 27 define the specific parameter values required for this test case.

Table 25. APUT verification of RSN Capabilities test configuration

Parameter	APUT value	CTT acting as a test bed STA value
Test bed vendor	N/A	For 2.4 or 5 GHz: Marvell For 60 GHz: Qualcomm
SSID	Wi-Fi	N/A
Operating channel	For dual band 2.4 and 5 GHz: 6 or For 5 GHz only: 44 For 60 GHz: 2	N/A
Security	WPA2-PSK	WPA2-PSK
PMF configuration (2.4 and 5 GHz)	Out-of-the-box	MFPC
PMF configuration (60 GHz)	Out-of-the-box	Disable PMF configuration in the RSNE for all scenarios

Table 26. RSNE configuration on CTT for test case 4.2.3 (for 2.4 and 5 GHz)

Scenario	RSNE format	Description
Scenario A	30 (Element ID) 16 (Length in octets) 01 00 (Version 1)	Reserved bits (bit-14 and bit-15) in RSN Capabilities field are set to 1

Scenario	RSNE format	Description
	00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 C0 (bit-14 and bit-15 set to 1) 00 00 (No PMKIDs)	
Scenario B	30 (Element ID) 16 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) xx xx, (RSN Capabilities field) 00 00 (No PMKIDs)	RSN Capabilities field is based on the vendor declaration in Table 1 such that a logical negation is configured only if the STAUT does not support a particular capability. For example; if a STAUT declaration indicates no support for Joint Multi-Band RSNA, then bit 8 (B8) is set to 1 on CTT. If the STAUT declaration indicates no support for PBAC, then bit 12 (B12) is set to 1 on CTT.

Table 27. RSNE configuration on CTT for test case 4.2.3 (for 60 GHz)

Scenario	RSNE format	Description
Scenario A	30 (Element ID) 16 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 C0 (bit-14 and bit-15 set to 1) 00 00 (No PMKIDs)	Reserved bits (bit-14 and bit-15) in RSN Capabilities field are set to 1
Scenario B	30 (Element ID) 16 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as group data cipher suite)	RSN Capabilities field is based on the vendor declaration in Table 1 such that a logical negation is configured only if the STAUT does not support a particular capability. For example; if a STAUT declaration indicates no support for Joint Multi-Band RSNA, then bit 8 (B8) is set to 1 on CTT. If the STAUT declaration indicates no support for PBAC, then bit 12 (B12) is set to 1 on CTT.

Scenario	RSNE format	Description
	01 00 (AKM suite count) 00 0F AC 02 (PSK) xx xx, (RSN Capabilities field) 00 00 (No PMKIDs)	

Test procedure and expected results

Table 28 provides the test procedure and expected results for this test case for 2.4 or 5 GHz capable APUT.

Table 28. APUT verification of RSN Capabilities test procedure and expected results

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
1	Power on the APUT. Reset the device to its default configuration as specified in Table 10. Configure the APUT to transmit Beacon frames.	Reset the device to its default configuration as specified in Table 5.		SN: Verify the following subfields in the RSN Capabilities field in the Beacon frame from the APUT: 1. No Pairwise subfield is set to 0. 2. Joint Multi-Band RSNA. 3. PeerKey enabled. 4. SPP A-MSDU Capable. 5. SPP A-MSDU Required. 6. PBAC (MFPR and MFPC subfields shall be set to 1 if PBAC subfield is set to 1). 7. Extended Key ID for Individually Addressed frames. If the values of these subfields match with the vendor declaration in Table 1, then CONTINUE, else FAIL.
2	The APUT transmits a Probe Response frame.	Configure the STA to perform an active scan in the APUT's operating channel. The STA transmits a Probe Request frame.	Verify that a broadcast Probe Request frame with SSID set to wildcard is transmitted in the APUT's operating channel.	SN: Verify the following subfields in the RSN Capabilities field in the Probe Response frame from the APUT: 1. No Pairwise subfield is set to 0. 2. Joint Multi-Band RSNA. 3. PeerKey enabled. 4. SPP A-MSDU Capable. 5. SPP A-MSDU Required. 6. PBAC (MFPR and MFPC subfields shall be set to 1 if PBAC subfield is set to 1). 7. Extended Key ID for Individually Addressed Frames. If the values of these subfields match with the vendor declaration in Table 1, then CONTINUE, else FAIL.
3		Configure the STA as per Table 26.		
4	The APUT transmits an Association Response frame.	Configure the STA to associate with the APUT.	Verify that an Association Request frame is	SN:

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
		The STA transmits an Association Request frame.	transmitted by the STA containing an RSNE as per the configuration in Table 26.	If the Association Response frame contains SUCCESS (Status Code field set to 0), then CONTINUE, else FAIL.
5	The APUT and STA complete: • 4-way handshake • DHCP exchange			SN: If the APUT successfully completes a 4-way handshake, then CONTINUE, else FAIL.
6		The STA pings the console IP address. <ping CONSOLE_IP_ADDR>, COUNT = 3, FRAME_RATE = 1		If the ping is successful, then PASS else FAIL.
Repeat Steps 3 - 6 for each scenario specified in Table 26.				

Table 29 provides the test procedure and expected results for this test case for 60 GHz capable APUT.

Table 29. APUT verification of RSN Capabilities test procedure and expected results

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
1	Power on the APUT. Reset the device to its default configuration as specified in Table 12. Configure the APUT to transmit DMG Beacon frames.	Reset the test bed STA to its default configuration as specified in Table 7.		SN: IF RSNE is present in the DMG Beacon frame transmitted by the APUT, then verify the following subfields in the RSN Capabilities field: 1. No Pairwise subfield is set to 0. 2. Joint Multi-Band RSNA. 3. PeerKey enabled. 4. SPP A-MSDU Capable. 5. SPP A-MSDU Required. 6. PBAC (MFPR and MFPC subfields shall be set to 1 if PBAC subfield is set to 1). 7. Extended Key ID for Individually Addressed frames. If the values of these subfields match with the vendor declaration in Table 1, then CONTINUE, else FAIL.
2	Perform the APUT and test bed STA initial configuration as described in Table 14.			
3	The APUT transmits a Probe Response frame.	Configure the STA to perform an active scan in the APUT's operating channel. The STA transmits a Probe Request frame.	Verify that a broadcast Probe Request frame with SSID set to wildcard is transmitted in the APUT's operating channel.	SN: Verify the following subfields in the RSN Capabilities field in the Probe Response frame from the APUT: 1. No Pairwise subfield is set to 0. 2. Joint Multi-Band RSNA. 3. PeerKey enabled. 4. SPP A-MSDU Capable. 5. SPP A-MSDU Required.

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
				6. PBAC (MFPR and MFPC subfields shall be set to 1 if PBAC subfield is set to 1). 7. Extended Key ID for Individually Addressed Frames. If the values of these subfields match with the vendor declaration in Table 1, then CONTINUE, else FAIL.
4		Configure the STA as per Table 27.		
5	The APUT transmits an Association Response frame.	Configure the STA to associate with the APUT. The STA transmits an Association Request frame.	Verify that an Association Request frame is transmitted by the STA containing an RSNE as per the configuration in Table 27.	SN: If the Association Response frame contains SUCCESS (Status Code field set to 0), then CONTINUE, else FAIL.
6	The APUT and STA complete: • 4-way handshake • DHCP exchange			SN: If the APUT successfully completes a 4-way handshake, then CONTINUE, else FAIL.
7		The STA pings the console IP address. <ping CONSOLE_IP_ADDR>, COUNT = 20, FRAME_RATE = 1		If more than 5 consecutive ping timeouts occur in any of the ping tests, then FAIL. If more than 10% ping failures in any of the ping tests, then FAIL. If no fail messages are received, then PASS.
Repeat Steps 4 - 7 for each scenario specified in Table 27.				

4.2.4 APUT RSNE bounds verification using WPA2-PSK test

Objective

This test verifies that the APUT correctly handles unexpected RSNE termination, and then successfully associates to the STA and passes data traffic.

Applicability: Mandatory

References

Section 9.4.2.25 [2]

Test environment

- APUT
- CTT acting as a test bed STA
- Wireless Sniffer

Test configuration

Table 30, Table 31 and Table 32 define the specific parameter values required for this test case.

Table 30. APUT RSNE bounds verification using WPA2-PSK test configuration

Parameter	APUT value	CTT acting as a test bed STA value
Test bed vendor	N/A	For 2.4 or 5 GHz: Intel For 60 GHz: Qualcomm
SSID	Wi-Fi	N/A
Operating channel	For dual band 2.4 and 5 GHz: 6 or For 5 GHz only: 44 For 60 GHz: 2	N/A
Security	WPA2-PSK	WPA2-PSK
PMF configuration (2.4 and 5 GHz)	Scenario A - C, E - F: Out-of-the-box Scenario D: MFPR (bit 6) and MFPC (bit 7) bits set to 0 in RSN Capabilities field	Scenario B - F: MFPC (bit 7) set to 1
PMF configuration (60 GHz)	Out-of-the-box	Disable PMF configuration in the RSNE for all scenarios

Table 31. RSNE configuration on CTT for test case 4.2.4 (for 2.4 and 5 GHz)

Scenario	RSNE format	Description
Scenario A	30 (Element ID) 12 (Length in octets) 01 00, (Version 1)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List

Scenario	RSNE format	Description
	00 0F AC 04, (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK)	• AKM Suite Count and AKM Suite List
Scenario B	30 (Element ID) 14 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 00 (management frame protection is enabled but not required)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities
Scenario C	30 (Element ID) 16 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 00 (management frame protection is enabled but not required) 00 00 (No PMKIDs)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count
Scenario D	30 (Element ID) 1A (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 00, (management frame protection is enabled but not required) 00 00 (No PMKIDs) 00 0F AC 06 (BIP-CMAC-128 as group management cipher suite)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count • Group Management Cipher Suite
Scenario E	30 (Element ID) 1F (Length in octets)	The following optional fields are included in the RSNE • Group Data Cipher Suite

Scenario	RSNE format	Description
	01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 00, (management frame protection is enabled but not required) 00 00 (No PMKIDs) 00 0F AC 06 (BIP-CMAC-128 as group management cipher suite) 04 00 01 02 03 (Undefined subfield)	• Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count • Group Management Cipher Suite • RSNE extensible element (5 octets)
Scenario F	30 (Element ID) 2A (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 00 (management frame protection is enabled but not required) 01 00 (PMK ID count 1) 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 (PMK ID) 00 0F AC 06 (BIP-CMAC-128 as group management cipher suite)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMK ID Count and Invalid PMK ID • Group Management Cipher Suite

Table 32. RSNE configuration on CTT for test case 4.2.4 (for 60 GHz)

Scenario	RSNE format	Description
Scenario A	30 (Element ID) 12 (Length in octets) 01 00, (Version 1) 00 0F AC 08, (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List
Scenario B	30 (Element ID) 14 (Length in octets) 01 00 (Version 1)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List

Scenario	RSNE format	Description
	00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK)	• AKM Suite Count and AKM Suite List • RSN Capabilities
Scenario C	30 (Element ID) 16 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 00 00 (No PMKIDs)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count
Scenario D	30 (Element ID) 1A (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 00 00 (No PMKIDs) 00 0F AC 0B (BIP-GMAC-128 as group management cipher suite)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count • Group Management Cipher Suite
Scenario E	30 (Element ID) 1F (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 00 00 (No PMKIDs) 00 0F AC 0B (BIP-GMAC-128 as group management cipher suite) 04 00 01 02 03 (Undefined subfield)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count • Group Management Cipher Suite • RSNE extensible element (5 octets)
Scenario F	30 (Element ID)	The following optional fields are included in the RSNE

Scenario	RSNE format	Description
	2A (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 01 00 (PMK ID count 1) 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 (PMK ID) 00 0F AC 0B (BIP-GMAC-128 as group management cipher suite)	• Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMK ID Count and Invalid PMK ID • Group Management Cipher Suite

Test procedure and expected results

Table 33 provides the test procedure and expected results for this test case.

Table 33. APUT RSNE bounds verification using WPA2-PSK test procedure and expected results

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
1	Power on the APUT. Reset the device to its default configuration as specified in Table 10. Configure the APUT to transmit Beacon frames.			SN: Verify that the RSNE is present in the captured Beacon frame and that the following fields of the RSNE are set accordingly: 1. Version field is set to 01 00. 2. Group Data Cipher Suite is set to 00-0F-AC:4. 3. Pairwise Cipher Suite Count is set to 0x 01 00. 4. Pairwise Cipher Suite List is set to CCMP 00-0F-AC:4. 5. AKM Suite Count is set to 0x 01 00. 6. AKM Suite List is set to 00-0F-AC:2. 7. PMKID Count is set to 0 or is not present. 8. PMKID List is not present. If all the conditions above are met, then CONTINUE, else FAIL.
2	The APUT transmits a Probe Response frame.	Reset the STA to its default configuration as specified in Table 5. Configure the STA to perform an active scan in the APUT's operating channel. The STA transmits a Probe Request frame.	Verify that a broadcast Probe Request frame with SSID set to wildcard is transmitted in the APUT's operating channel.	SN: Verify that the RSNE is present in the captured Probe Response frame and that the following fields of the RSNE are set accordingly: 1. Version field is set to 01 00. 2. Group Data Cipher Suite is set to 00-0F-AC:4. 3. Pairwise Cipher Suite Count is set to 0x 01 00. 4. Pairwise Cipher Suite List is set to CCMP 00-0F-AC:4. 5. AKM Suite Count is set to 0x 01 00. 6. AKM Suite List is set to 00-0F-AC:2. 7. PMKID Count is set to 0 or is not present.

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
				8. PMKID List is not present. If all the conditions above are met, then CONTINUE, else FAIL.
3		Configure the STA as per Table 31.		
4	The APUT transmits an Association Response frame.	The STA transmits an Association Request frame.	Verify that an Association Request frame is transmitted by the STA containing an RSNE as per the configuration in Table 31.	SN: For all scenarios except D, E and F: If the Association Response frame contains SUCCESS (Status Code field set to 0), then CONTINUE, else FAIL. For scenario D and E: If the Association Response frame is transmitted by APUT and contains a SUCCESS (Status Code field set to 0), then CONTINUE. Else if the Association Response frame is transmitted by APUT and does not contain a SUCCESS then PASS, else FAIL. For scenario F: If the Association Response frame is transmitted by APUT and does not contain a SUCCESS (Status Code field set to 0), then PASS else FAIL.
5	The APUT and STA complete: • 4-way handshake • DHCP exchange			SN: If the APUT successfully completes a 4-way handshake, then CONTINUE, else FAIL.
6		The STA pings the console IP address. <ping CONSOLE_IP_ADDR>, COUNT = 3, FRAME_RATE = 1		If the ping is successful, then PASS, else FAIL.
Repeat Steps 3 - 6 for each scenario specified in Table 31.				

Table 34 provides the test procedure and expected results for this test case.

Table 34. APUT RSNE bounds verification using WPA2-PSK test procedure and expected results

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
1	Power on the APUT. Reset the device to its default configuration as specified in Table 12. Configure the APUT to transmit DMG Beacon frames.	Reset the test bed STA to its default configuration as specified in Table 7.		

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
2	Perform the APUT and test bed STA initial configuration as described in Table 14.			
3	The APUT transmits a Probe Response frame.	Configure the STA to perform an active scan in the APUT's operating channel. The STA transmits a Probe Request frame.	Verify that a broadcast Probe Request frame with SSID set to wildcard is transmitted in the APUT's operating channel.	
4		Configure the STA as per Table 32.		
5	The APUT transmits an Association Response frame.	The STA transmits an Association Request frame.	Verify that an Association Request frame is transmitted by the STA containing an RSNE as per the configuration in Table 32.	SN: For all scenarios except D and F: If the Association Response frame contains SUCCESS (Status Code field set to 0), then CONTINUE, else FAIL. a. If the Association Response frame contains the 60 GHz IE, then CONTINUE else FAIL. b. If the EDCA Parameter Set element, DMG Capabilities element and DMG Operation element are present in the Association Response frame, then CONTINUE else FAIL. For scenario D: If the Association Response frame is transmitted by APUT and contains a SUCCESS (Status Code field set to 0), then CONTINUE. a. If the Association Response frame contains the 60 GHz IE, then CONTINUE else FAIL. b. If the EDCA Parameter Set element, DMG Capabilities element and DMG Operation element are present in the Association Response frame, then CONTINUE else FAIL. Else if the Association Response frame is transmitted by APUT and does not contain a SUCCESS then PASS, Else FAIL. For scenario F: If the Association Response frame is transmitted by APUT and does not contain a SUCCESS (Status Code field set to 0), then PASS else FAIL.
6	The APUT and STA complete: • 4-way handshake • DHCP exchange			SN: If the APUT successfully completes a 4-way handshake, then CONTINUE, else FAIL.
7		The STA pings the console IP address.		If more than 5 consecutive ping timeouts occur in any of the ping tests, then FAIL.

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
		<ping CONSOLE_IP_ADDR>, COUNT = 20, FRAME_RATE = 1		If more than 10% ping failures in any of the ping tests, then FAIL. If no fail messages are received, then PASS.
Repeat Steps 4 - 7 for each scenario specified in Table 32.				

5 WPA2 Security Improvements STAUT tests

5.1 STAUT configuration requirements validation test

This section is not applicable to an STAUT undergoing Security Improvements testing.

5.2 STAUT test cases

For a WiGig STAUT device, Table 35 lists the initial test configuration steps that shall be completed between a test bed AP and the STAUT when referred by test cases in this section as an initial test configuration.

Table 35. STAUT and test bed AP initial test configuration

Step	STAUT	Test bed AP	Expected result
1	Disassociate if already associated.		
2		The test bed AP starts transmission of DMG Beacon frames with the default configuration of DMG Beacon frame fields plus possible exceptions as noted by each test case.	
3	The STAUT receives the DMG Beacon frames and performs SLS with the AP during the A-BFT or during DTI period when offered by the AP. NOTE – The RSS component of the SLS is a Responder TXSS if the value of the IsResponderTXSS subfield of the Beacon Interval Control field is equal to one.		
4	Optionally, the STAUT sends a Probe Request frame with the Address 1 (RA) field set to the AP MAC address, and the Address 3 (BSSID) field set to the AP MAC address or wildcard BSSID.	The AP responds to each received Probe Request frame with an ACK, and then transmits a Probe Response frame.	
5	During a CBAP, any device (STAUT or AP) with channel access rights can perform further transmit or receive training using one or more of the following methods: BRP with receive or transmit training, in any order, including both • Transmission of a Grant frame signaling TXSS • Transmission of an SSW frame signaling TXSS		

5.2.1 STAUT RSNE bounds verification using WPA2-Enterprise test

Objective

This test verifies that the STAUT correctly handles unexpected RSNE termination, and then successfully connects to the AP and passes data traffic.

Applicability: Conditional. This test case is only required if the STAUT declared support for WPA2-Enterprise in Table 2.

References

Section 9.4.2.25 [2]

Section 3.1 [4]

Test environment

- STAUT
- CTT acting as a test bed AP
- Wireless Sniffer
- AAA server

Test configuration

Table 36, Table 37 and Table 38 define the specific parameter values required for this test case.

Table 36. STAUT RSNE bounds verification using WPA2-Enterprise test configuration

Parameter	STAUT value	CTT acting as a test bed AP value	AAA server
Test bed vendor	N/A	For 2.4 and 5 GHz: Qualcomm For 60 GHz: Qualcomm	HostAPD
SSID	N/A	Wi-Fi	N/A
Operating channel	N/A	For dual band 2.4 and 5 GHz: 6 or For 5 GHz only: 44 For 60 GHz: 2	N/A
Security	WPA2-Enterprise (EAP-TLS)	WPA2-Enterprise (EAP-TLS)	EAP-TLS
PMF configuration (2.4 and 5 GHz)	Scenario A - F, H: Out-of-the-box Scenario G: MFPR (bit 6) and MFPC (bit 7) bits set to 0 in RSN Capabilities field	Scenario E - H: MFPC (bit 7) set to 1	N/A
PMF configuration (60 GHz)	Out-of-the-box	Disable PMF configuration in the RSNE for all scenarios	N/A

Table 37. RSNE configuration on CTT for test case 5.2.1 (for 2.4 and 5 GHz)

Scenario	RSNE format	Description
Scenario A	30 (Element ID) 2 (Length in octets) 01 00 (Version 1)	None of the optional fields are included in the RSNE
Scenario B	30 (Element ID) 6 (length in octets in hex) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite)	The following optional field is included in the RSNE • Group Data Cipher Suite
Scenario C	30 (Element ID) 0C (Length in octets) 01 00 (Version 1)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List

Scenario	RSNE format	Description
	00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite)	
Scenario D	30 (Element ID) 12 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List
Scenario E	30 (Element ID) 14 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 80 00 (management frame protection is enabled but not required)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities
Scenario F	30 (Element ID) 16 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 80 00 (management frame protection is enabled but not required) 00 00 (No PMKIDs)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count
Scenario G	30 (Element ID) 1A (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04, (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count • Group Management Cipher Suite

Scenario	RSNE format	Description
	00 0F AC 01 (IEEE Std 802.1X authentication) 80 00 (management frame protection is enabled but not required) 00 00 (No PMKIDs) 00 0F AC 06 (BIP-CMAC-128 as group management cipher suite)	
Scenario H	30 (Element ID) 1F (Length in octets) 01 00, (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 80 00 (management frame protection is enabled but not required) 00 00 (No PMKIDs) 00 0F AC 06 (BIP-CMAC-128 as group management cipher suite) 04 00 01 02 03 (Undefined subfield)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count • Group Management Cipher Suite • RSNE extensible element (5 octets)
Scenario I	30 (Element ID) 2A (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 80 00 (management frame protection is enabled but not required) 01 00 (PMK ID count 1) 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10, (PMK ID) 00 0F AC 06 (BIP-CMAC-128 as group management cipher suite)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMK ID Count and PMK ID • Group Management Cipher Suite
Scenario J	30 (Element ID) 16 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 80 00 (management frame protection is enabled but not required)	PMK ID count is 1 but no PMK ID present in the List field

Scenario	RSNE format	Description
	01 00 (PMKID Count)	
Scenario K	30 (Element ID) 1A (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 02 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 02 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 00 0F AC 02 (PSK)	Multiple pairwise ciphers and AKMs present

Table 38. RSNE configuration on CTT for test case 5.2.1 (for 60 GHz)

Scenario	RSNE format	Description
Scenario A	30 (Element ID) 2 (Length in octets) 01 00 (Version 1)	None of the optional fields are included in the RSNE
Scenario B	30 (Element ID) 6 (length in octets in hex) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite)	The following optional field is included in the RSNE • Group Data Cipher Suite
Scenario C	30 (Element ID) 0C (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List
Scenario D	30 (Element ID) 12 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List

Scenario	RSNE format	Description
Scenario E	30 (Element ID) 14 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities
Scenario F	30 (Element ID) 16 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 00 00 (No PMKIDs)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count
Scenario G	30 (Element ID) 1A (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08, (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 00 00 (No PMKIDs) 00 0F AC 0B (BIP-GMAC-128 as group management cipher suite)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count • Group Management Cipher Suite
Scenario H	30 (Element ID) 1F (Length in octets) 01 00, (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 00 00 (No PMKIDs)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count • Group Management Cipher Suite • RSNE extensible element (5 octets)

Scenario	RSNE format	Description
	00 0F AC 0B (BIP-GMAC-128 as group management cipher suite) 04 00 01 02 03 (Undefined subfield)	
Scenario I	30 (Element ID) 2A (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 01 00 (PMK ID count 1) 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10, (PMK ID) 00 0F AC 0B (BIP-GMAC-128 as group management cipher suite)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMK ID Count and PMK ID • Group Management Cipher Suite
Scenario J	30 (Element ID) 16 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 01 00 (PMKID Count)	PMK ID count is 1 but no PMK ID present in the List field
Scenario K	30 (Element ID) 1A (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 02 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 02 00 (AKM suite count) 00 0F AC 01 (IEEE Std 802.1X authentication) 00 0F AC 02 (PSK)	Multiple pairwise ciphers and AKMs present

Test procedure and expected results

Table 39 provides the test procedure and expected results for this test case for 2.4 or 5 GHz capable STAUT.

Table 39. STAUT RSNE bounds verification using WPA2-Enterprise test procedure and expected results

Step	STAUT	CTT acting as a test bed AP	CTT validation check	Expected Result
1	Reset the STAUT to its default configuration as specified in Table 11.			
2	Configure the STAUT as per Table 36.	Reset the AP to its default configuration as specified in Table 4. Configure the AP as per Table 36.		
3	Configure the STAUT to perform an active scan in the AP's operating channel. The STAUT transmits a Probe Request frame.	The AP transmits Beacon and Probe Response frames as per the configuration in Table 37.	Verify that the AP transmits Beacon and Probe Response frames per the configuration in Table 37.	
4	The STAUT transmits an Association Request frame.	The AP transmits an Association Response frame.	For all scenarios except I and J: Verify that the AP transmits an Association Response frame to the STAUT with Status Code set to 0 (SUCCESS). For scenarios I and J: If the Association Request frame is transmitted by the STAUT, verify that the AP transmits Association Response frame with status Code set to 0 (SUCCESS).	SN: For all scenarios except I and J: If the Association Request frame is transmitted by the STAUT, then CONTINUE, else FAIL. For scenarios I and J: If the Association Request frame is transmitted by STAUT, then CONTINUE. Else if the Association Request frame is not transmitted by STAUT then PASS, else FAIL.
5	The STAUT and AP complete: • EAP authentication • 4-way handshake • DHCP exchange			SN: If the STAUT successfully completes EAP authentication followed by a 4-way handshake, then CONTINUE, else FAIL.
6		The AP pings the STAUT IP address. <ping STAUT_IP_ADDR>, COUNT = 3, FRAME_RATE = 1		If the ping is successful, then PASS, else FAIL.
Repeat Step 2 - 6 for each scenario specified in Table 37.				

Table 40 provides the test procedure and expected results for this test case for 60 GHz capable STAUT.

Table 40. STAUT RSNE bounds verification using WPA2-Enterprise test procedure and expected results

Step	STAUT	CTT acting as a test bed AP	CTT validation check	Expected Result
1	Reset the STAUT to its default configuration as specified in Table 13.			

Step	STAUT	CTT acting as a test bed AP	CTT validation check	Expected Result
2	Configure the STAUT as per Table 36.	Reset the AP to its default configuration as specified in Table 6. Configure the AP as per Table 36.		
3	Perform STAUT and test bed AP initial test configuration as defined in Table 35.			
4	Configure the STAUT to perform an active scan in the AP's operating channel. The STAUT transmits a Probe Request frame.	The AP transmits DMG Beacon and Probe Response frames as per the configuration in Table 38.	Verify that the AP transmits DMG Beacon and Probe Response frames per the configuration in Table 38.	
5	The STAUT transmits an Association Request frame.	The AP transmits an Association Response frame.	For all scenarios except I and J: Verify that the AP transmits an Association Response frame to the STAUT with Status Code set to 0 (SUCCESS). For scenarios I and J: If the Association Request frame is transmitted by the STAUT, verify that the AP transmits Association Response frame with status Code set to 0 (SUCCESS).	SN: For all scenarios except I and J: If the Association Request frame is transmitted by the STAUT, then CONTINUE, else FAIL. • If the DMG Capabilities element and QoS Capability element are present in the Association Request frame from STAUT, then CONTINUE else FAIL. For scenarios I and J: If the Association Request frame is transmitted by STAUT, then CONTINUE. • If the DMG Capabilities element and QoS Capability element are present in the Association Request frame from STAUT, then CONTINUE else FAIL. Else if the Association Request frame is not transmitted by STAUT then PASS, Else FAIL.
6	The STAUT and AP complete: • EAP authentication • 4-way handshake • DHCP exchange			SN: If the STAUT successfully completes EAP authentication followed by a 4-way handshake, then CONTINUE, else FAIL.
7		The AP pings the STAUT IP address. <ping STAUT_IP_ADDR>, COUNT = 20, FRAME_RATE = 1		If more than 5 consecutive ping timeouts occur in any of the ping tests, then FAIL. If more than 10% ping failures in any of the ping tests, then FAIL. If no fail messages are received, then PASS.

Step	STAUT	CTT acting as a test bed AP	CTT validation check	Expected Result
Repeat Step 2 - 7 for each scenario specified in Table 38.				

5.2.2 STAUT handles RSNE unexpected values test

Objective

This test verifies that the STAUT correctly handles unexpected values in the RSNE and appropriately requests association.

Applicability: Mandatory

References

Section 9.4.2.25 [2]

Test environment

- STAUT
- CTT acting as a test bed AP
- Wireless Sniffer

Test configuration

Table 41, Table 42 and Table 43 define the specific parameter values required for this test case.

Table 41. STAUT handles RSNE unexpected values test configuration

Parameter	STAUT value	CTT acting as a test bed AP value
Test bed vendor	N/A	For 2.4 and 5 GHz: Marvell For 60 GHz: Qualcomm
SSID	N/A	Wi-Fi
Operating channel	N/A	For dual band 2.4 and 5 GHz: 6 or For 5 GHz only: 44 For 60 GHz: 2
Security	WPA2-PSK	WPA2-PSK
PMF configuration (2.4 and 5 GHz)	Out-of-the-box	MFPC
PMF configuration (60 GHz)	Out-of-the-box	Disable PMF configuration in the RSNE for all scenarios

Table 42. RSNE configuration on CTT for test case 5.2.2 (for 2.4 and 5 GHz)

Scenario	RSNE format	Description
Scenario A	30 (Element ID) 16 (Length in octets) 02 00 (Version 2) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count)	RSN protocol Version field is set to value 2

Scenario	RSNE format	Description
	00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 00 (management frame protection is enabled, but not required) 00 00 (No PMKIDs)	
Scenario B	30 (Element ID) 12 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 00 00 (pairwise cipher suite count) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 00 (management frame protection is enabled but not required) 00 00 (No PMKIDs)	Pairwise Cipher Suite Count field value is set to 0 (Pairwise Cipher Suite List field is not present)
Scenario C	30 (Element ID) 10 (Length in octets) 01 00 (Version 1) 00 0F AC 04, (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 00 00 (AKM suite count) 80 00 (management frame protection is enabled but not required)	AKM Suite Count field value is set to 0 (AKM Suite List field is not present)
Scenario D	30 (Element ID) 0C (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 00 00 (pairwise cipher suite count) 00 00 (AKM suite count) 80 00 (management frame protection is enabled but not required)	Pairwise Cipher Suite Count field value is set to 0 (Pairwise Cipher Suite List field is not present) AKM Suite Count field value is set to 0 (AKM Suite List field is not present)
Scenario F	30 (Element ID) 01 (Length in octets) 01 (Version 1) - truncated to 1 octet	RSN Version field is truncated to 1 octet
Scenario G	30 (Element ID) 05 (Length in octets) 01 00 (Version 1) 00 0F AC (truncated)	Group Data Cipher Suite truncated

Scenario	RSNE format	Description
Scenario H	30 (Element ID) 0B (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC (truncated)	Pairwise Cipher Suite List truncated
Scenario I	30 (Element ID) 11 (length in octets in hex) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC (truncated)	AKM Suite List truncated
Scenario J	30 (Element ID) 13 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 (truncated)	RSN Capabilities truncated
Scenario K	30 (Element ID) 15 (Length in octets) 01 00 (Version 1) 00 0F AC 04, (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 00 (management frame protection is enabled but not required) 00 (truncated)	PMKID count truncated
Scenario L	30 (Element ID) 0C (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite)	Pairwise Cipher count is 2, but only 1 present in the List field

Scenario	RSNE format	Description
	02 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite)	
Scenario M	30 (Element ID) 12 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 02 00 (AKM suite count) 00 0F AC 02 (PSK)	AKM Suite count is 2 but only 1 present in the List field

Table 43. RSNE configuration on CTT for test case 5.2.2 (for 60 GHz)

Scenario	RSNE format	Description
Scenario A	30 (Element ID) 16 (Length in octets) 02 00 (Version 2) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 00 00 (No PMKIDs)	RSN protocol Version field is set to value 2
Scenario B	30 (Element ID) 12 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 00 00 (pairwise cipher suite count) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 00 00 (No PMKIDs)	Pairwise Cipher Suite Count field value is set to 0 (Pairwise Cipher Suite List field is not present)
Scenario C	30 (Element ID) 10 (Length in octets) 01 00 (Version 1) 00 0F AC 08, (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite)	AKM Suite Count field value is set to 0 (AKM Suite List field is not present)

Scenario	RSNE format	Description
	00 00 (AKM suite count)	
Scenario D	30 (Element ID) 0C (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 00 00 (pairwise cipher suite count) 00 00 (AKM suite count)	Pairwise Cipher Suite Count field value is set to 0 (Pairwise Cipher Suite List field is not present) AKM Suite Count field value is set to 0 (AKM Suite List field is not present)
Scenario F	30 (Element ID) 01 (Length in octets) 01 (Version 1) - truncated to 1 octet	RSN Version field is truncated to 1 octet
Scenario G	30 (Element ID) 05 (Length in octets) 01 00 (Version 1) 00 0F AC (truncated)	Group Data Cipher Suite truncated
Scenario H	30 (Element ID) 0B (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC (truncated)	Pairwise Cipher Suite List truncated
Scenario I	30 (Element ID) 11 (length in octets in hex) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC (truncated)	AKM Suite List truncated
Scenario J	30 (Element ID) 13 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count)	RSN Capabilities truncated

Scenario	RSNE format	Description
	00 0F AC 02 (PSK) 80 (truncated)	
Scenario K	30 (Element ID) 15 (Length in octets) 01 00 (Version 1) 00 0F AC 08, (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 00 (truncated)	PMKID count truncated
Scenario L	30 (Element ID) 0C (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 02 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite)	Pairwise Cipher count is 2, but only 1 present in the List field
Scenario M	30 (Element ID) 12 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 02 00 (AKM suite count) 00 0F AC 02 (PSK)	AKM Suite count is 2 but only 1 present in the List field

Test procedure and expected results

Table 44 provides the test procedure and expected results for this test case for 2.4 and 5 GHz STAUT.

Table 44. STAUT handles RSNE unexpected values test procedure and expected results

Step	STAUT	CTT acting as a test bed AP	CTT validation check	Expected Result
1	Reset the STAUT to its default configuration as specified in Table 11.			
2		Reset the AP to its default configuration as specified in Table 4.		

Step	STAUT	CTT acting as a test bed AP	CTT validation check	Expected Result
		Configure the AP as per Table 42.		
3	Configure the STAUT to perform an active scan in the AP's operating channel. The STAUT transmits a Probe Request frame.	The AP transmits a Probe Response frame.	Verify that the AP transmits Beacon and Probe Response frames per the configuration in Table 42.	
4	Configure the STAUT to associate with the AP. The STAUT transmits an Association Request frame.	The AP transmits an Association Response frame.	For scenarios B, C, D, J, K, L, M: If the Association Request frame is transmitted by the STAUT, verify that the AP transmits Association Response frame with status Code set to 0 (SUCCESS).	SN: For scenarios A, F, G, H, I: If the Association Request frame is not transmitted by the STAUT, then PASS, else FAIL. For scenarios B, C, D, J, K, L, M: If the Association Request frame is transmitted by STAUT, then CONTINUE. Else if the Association Request frame is not transmitted by STAUT then PASS, else FAIL.
5	The STAUT and AP complete: • 4-way handshake • DHCP exchange			SN: If the STAUT successfully completes a 4-way handshake, then CONTINUE, else FAIL.
6		The AP pings the STAUT IP address. <ping STAUT_IP_ADDR>, COUNT = 3, FRAME_RATE = 1		If the ping is successful, then PASS, else FAIL.
Repeat Steps 2 - 6 for each scenario specified in Table 42.				

Table 45 provides the test procedure and expected results for this test case for 60 GHz STAUT.

Table 45. STAUT handles RSNE unexpected values test procedure and expected results

Step	STAUT	CTT acting as a test bed AP	CTT validation check	Expected Result
1	Reset the STAUT to its default configuration as specified in Table 13.			
2		Reset the AP to its default configuration as specified in Table 6. Configure the AP as per Table 43.		
3	Perform STAUT and test bed AP initial test configuration as defined in Table 35.			
4	Configure the STAUT to perform an active scan in the AP's operating channel.	The AP transmits a Probe Response frame.	Verify that the AP transmits DMG Beacon and Probe Response frames per the configuration in Table 43.	

Step	STAUT	CTT acting as a test bed AP	CTT validation check	Expected Result
	The STAUT transmits a Probe Request frame.			
5	Configure the STAUT to associate with the AP. The STAUT transmits an Association Request frame.	The AP transmits an Association Response frame.	For scenarios B, C, D, J, K, L, M: If the Association Request frame is transmitted by the STAUT, verify that the AP transmits Association Response frame with status Code set to 0 (SUCCESS).	SN: For scenarios A, F, G, H, I: If the Association Request frame is not transmitted by the STAUT, then PASS, else FAIL. For scenarios B, C, D, J, K, L, M: If the Association Request frame is transmitted by STAUT, then CONTINUE. Else if the Association Request frame is not transmitted by STAUT then PASS, else FAIL.
6	The STAUT and AP complete: • 4-way handshake • DHCP exchange			SN: If the STAUT successfully completes a 4-way handshake, then CONTINUE, else FAIL.
7		The AP pings the STAUT IP address. <ping STAUT_IP_ADDR>, COUNT = 20, FRAME_RATE = 1		If more than 5 consecutive ping timeouts occur in any of the ping tests, then FAIL. If more than 10% ping failures in any of the ping tests, then FAIL. If no fail messages are received, then PASS.
Repeat Steps 2 - 7 for each scenario specified in Table 43.				

5.2.3 STAUT verification of RSN Capabilities test

Objective

This test verifies that the STAUT successfully associates, authenticates and passes data traffic when reserved bits 15 and 14 in the RSN Capabilities field are set to one instead of zero. This test also 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.

Applicability: Mandatory

References

Section 9.4.2.25.4 [2]

Test environment

- STAUT
- CTT acting as a test bed AP
- Wireless Sniffer

Test configuration

Table 46, Table 47 and Table 48 define the specific parameter values required for this test case.

Table 46. STAUT verification of RSN Capabilities test configuration

Parameter	STAUT value	CTT acting as a test bed AP value
Test bed vendor	N/A	For 2.4 and 5 GHz: Qualcomm For 60 GHz: Qualcomm
SSID	N/A	Wi-Fi
Operating channel	N/A	For dual band 2.4 and 5 GHz: 6 or For 5 GHz only: 44 For 60 GHz: 2
Security	WPA2-PSK	WPA2-PSK
PMF configuration (2.4 and 5 GHz)	Out-of-the-box	MFPC
PMF configuration (60 GHz)	Out-of-the-box	Disable PMF configuration in the RSNE for all scenarios

Table 47. RSNE configuration on CTT for test case 5.2.3 (for 2.4 and 5 GHz)

Scenario	RSNE format	Description
Scenario A	30, (Element ID) 16, (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 C0 (bit-14 and bit-15 set to 1) 00 00 (No PMKIDs)	Reserved bits (bit-14 and bit-15) in RSN Capabilities field are set to 1
Scenario B	30 (Element ID) 16 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) xx xx, (RSN Capabilities field) 00 00 (No PMKIDs)	RSN Capabilities field is based on the vendor declaration in Table 2 such that a logical negation is configured only if the DUT does not support a particular capability. For example; if a DUT declaration indicates no support for Joint Multi-Band RSNA, then bit 8 (B8) is set to 1 on CTT. If the DUT declaration indicates no support for PBAC, then bit 12 (B12) is set to 1 on CTT.

Table 48. RSNE configuration on CTT for test case 5.2.3 (for 60 GHz)

Scenario	RSNE format	Description
Scenario A	30, (Element ID) 16, (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 C0 (bit-14 and bit-15 set to 1) 00 00 (No PMKIDs)	Reserved bits (bit-14 and bit-15) in RSN Capabilities field are set to 1
Scenario B	30 (Element ID) 16 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) xx xx, (RSN Capabilities field) 00 00 (No PMKIDs)	RSN Capabilities field is based on the vendor declaration in Table 2 such that a logical negation is configured only if the DUT does not support a particular capability. For example; if a DUT declaration indicates no support for Joint Multi-Band RSNA, then bit 8 (B8) is set to 1 on CTT. If the DUT declaration indicates no support for PBAC, then bit 12 (B12) is set to 1 on CTT.

Test procedure and expected results

Table 49 provides the test procedure and expected results for this test case for 2.4 and 5 GHz STAUT.

Table 49. STAUT verification of RSN Capabilities test procedure and expected results

Step	STAUT	CTT acting as a test bed AP	CTT validation check	Expected Result
1	Reset the STAUT to its default configuration as specified in Table 11.	Reset the AP to its default configuration as specified in Table 4.		
2		Configure the AP as per Table 47	Verify that the AP transmits Beacon and Probe Response frames per the configuration in Table 47.	
3	Configure the STAUT to perform an active scan in the AP's operating channel. The STAUT transmits a Probe Request frame.	The AP transmits a Probe Response frame.		

Step	STAUT	CTT acting as a test bed AP	CTT validation check	Expected Result
4	Configure the STAUT to associate with the AP. The STAUT transmits an Association Request frame.	The AP transmits an Association Response frame.	Verify that the AP transmits an Association Response frame to the STAUT with Status Code set to 0 (SUCCESS).	SN: Verify the following subfields in the RSN Capabilities field in the Association Request frame from the STAUT: 1. No Pairwise subfield is set to 0. 2. Joint Multi-Band RSNA. 3. PeerKey enabled. 4. SPP A-MSDU Capable. 5. SPP A-MSDU Required. 6. PBAC (MFPR and MFPC subfields shall be set to 1 if PBAC subfield is set to 1). 7. Extended Key ID for Individually Addressed Frames. If the values of these subfields match with the vendor declaration in Table 2, then CONTINUE, else FAIL. If the Association Request frame is transmitted by the STAUT, then CONTINUE, else FAIL.
5	The STAUT and AP complete: • 4-way handshake • DHCP exchange			SN: If the STAUT successfully completes a 4-way handshake, then CONTINUE, else FAIL.
6		The AP pings the STAUT IP address. <ping STAUT_IP_ADDR>, COUNT = 3, FRAME_RATE = 1		If the ping is successful, then PASS else FAIL.
Repeat Steps 2 - 6 for each scenario specified in Table 47.				

Table 50 provides the test procedure and expected results for this test case for 60 GHz STAUT.

Table 50. STAUT verification of RSN Capabilities test procedure and expected results

Step	STAUT	CTT acting as a test bed AP	CTT validation check	Expected Result
1	Reset the STAUT to its default configuration as specified in Table 13.	Reset the AP to its default configuration as specified in Table 6.		
2		Configure the AP as per Table 48.	Verify that the AP transmits DMG Beacon and Probe Response frames per the configuration in Table 48.	
3	Perform STAUT and test bed AP initial test configuration as defined in Table 35.			

Step	STAUT	CTT acting as a test bed AP	CTT validation check	Expected Result
4	Configure the STAUT to perform an active scan in the AP's operating channel. The STAUT transmits a Probe Request frame.	The AP transmits a Probe Response frame.		
5	Configure the STAUT to associate with the AP. The STAUT transmits an Association Request frame.	The AP transmits an Association Response frame.	Verify that the AP transmits an Association Response frame to the STAUT with Status Code set to 0 (SUCCESS).	SN: Verify the following subfields in the RSN Capabilities field in the Association Request frame from the STAUT: 8. No Pairwise subfield is set to 0. 9. Joint Multi-Band RSNA. 10. PeerKey enabled. 11. SPP A-MSDU Capable. 12. SPP A-MSDU Required. 13. PBAC (MFPR and MFPC subfields shall be set to 1 if PBAC subfield is set to 1). 14. Extended Key ID for Individually Addressed Frames. If the values of these subfields match with the vendor declaration in Table 2, then CONTINUE, else FAIL. If the Association Request frame is transmitted by the STAUT, then CONTINUE, else FAIL.
6	The STAUT and AP complete: • 4-way handshake • DHCP exchange			SN: If the STAUT successfully completes a 4-way handshake, then CONTINUE, else FAIL.
7		The AP pings the STAUT IP address. <ping STAUT_IP_ADDR>, COUNT = 20, FRAME_RATE = 1		If more than 5 consecutive ping timeouts occur in any of the ping tests, then FAIL. If more than 10% ping failures in any of the ping tests, then FAIL. If no fail messages are received, then PASS.
Repeat Steps 2 - 7 for each scenario specified in Table 48.				

5.2.4 STAUT RSNE bounds verification using WPA2-PSK test

Objective

This test verifies that the STAUT correctly handles unexpected RSNE termination, and then successfully connects to the AP and passes data traffic.

Applicability: Mandatory

References

Section 9.4.2.25 [2]

Test environment

- STAUT
- CTT acting as a test bed AP
- Wireless Sniffer

Test configuration

Table 51, Table 52 and Table 53 define the specific parameter values required for this test case.

Table 51. STAUT RSNE bounds verification using WPA2-PSK test configuration

Parameter	STAUT value	CTT acting as a test bed AP value
Test bed vendor	N/A	For 2.4 and 5 GHz: Marvell For 60 GHz: Qualcomm
SSID	N/A	Wi-Fi
Operating channel	N/A	For dual band 2.4 and 5 GHz: 6 or For 5 GHz only: 44 For 60 GHz: 2
Security	WPA2-PSK	WPA2-PSK
PMF configuration (2.4 and 5 GHz)	Scenario A - C, E: Out-of-box Scenario D: MFPR (bit 6) and MFPC (bit 7) bits set to 0 in RSN Capabilities field	Scenario B - E: MFPC (bit 7) set to 1
PMF configuration (60 GHz)	Out-of-the-box	Disable PMF configuration in the RSNE for all scenarios

Table 52. RSNE configuration on CTT for test case 5.2.4 (for 2.4 and 5 GHz)

Scenario	RSNE format	Description
Scenario A	30 (Element ID) 12 (Length in octets) 01 00 (Version 1)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List

Scenario	RSNE format	Description
	00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK)	• AKM Suite Count and AKM Suite List
Scenario B	30 (Element ID) 14 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 00 (management frame protection is enabled but not required)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities
Scenario C	30 (Element ID) 16 (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 00, (management frame protection is enabled but not required) 00 00 (No PMKIDs)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count
Scenario D	30 (Element ID) 1A (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 00 (management frame protection is enabled but not required) 00 00 (No PMKIDs) 00 0F AC 06 (BIP-CMAC-128 as group management cipher suite)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count • Group Management Cipher Suite
Scenario E	30 (Element ID) 1F (Length in octets)	The following optional fields are included in the RSNE • Group Data Cipher Suite

Scenario	RSNE format	Description
	01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 00 (management frame protection is enabled but not required) 00 00 (No PMKIDs) 00 0F AC 06 (BIP-CMAC-128 as group management cipher suite) 04 00 01 02 03 (Undefined subfield)	• Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count • Group Management Cipher Suite • RSNE extensible element (5 octets)
Scenario F	30 (Element ID) 2A (Length in octets) 01 00 (Version 1) 00 0F AC 04 (CCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 04 (CCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 80 00 (management frame protection is enabled, but not required) 01 00 (PMK ID count 1) 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 (PMK ID) 00 0F AC 06 (BIP-CMAC-128 as group management cipher suite)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMK ID Count and PMK ID • Group Management Cipher Suite

Table 53. RSNE configuration on CTT for test case 5.2.4 (for 60 GHz)

Scenario	RSNE format	Description
Scenario A	30 (Element ID) 12 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List
Scenario B	30 (Element ID) 14 (Length in octets) 01 00 (Version 1)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List

Scenario	RSNE format	Description
	00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK)	• AKM Suite Count and AKM Suite List • RSN Capabilities
Scenario C	30 (Element ID) 16 (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 00 00 (No PMKIDs)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count
Scenario D	30 (Element ID) 1A (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 00 00 (No PMKIDs) 00 0F AC 0B (BIP-GMAC-128 as group management cipher suite)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count • Group Management Cipher Suite
Scenario E	30 (Element ID) 1F (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 00 00 (No PMKIDs) 00 0F AC 0B (BIP-GMAC-128 as group management cipher suite) 04 00 01 02 03 (Undefined subfield)	The following optional fields are included in the RSNE • Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMKID Count • Group Management Cipher Suite • RSNE extensible element (5 octets)
Scenario F	30 (Element ID)	The following optional fields are included in the RSNE

Scenario	RSNE format	Description
	2A (Length in octets) 01 00 (Version 1) 00 0F AC 08 (GCMP-128 as group data cipher suite) 01 00 (pairwise cipher suite count) 00 0F AC 08 (GCMP-128 as pairwise cipher suite) 01 00 (AKM suite count) 00 0F AC 02 (PSK) 01 00 (PMK ID count 1) 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 (PMK ID) 00 0F AC 0B (BIP-GMAC-128 as group management cipher suite)	• Group Data Cipher Suite • Pairwise Cipher Suite Count and Pairwise Cipher Suite List • AKM Suite Count and AKM Suite List • RSN Capabilities • PMK ID Count and PMK ID • Group Management Cipher Suite

Test procedure and expected results

Table 54 provides the test procedure and expected results for this test case for 2.4 and 5 GHz STAUT.

Table 54. STAUT RSNE bounds verification using WPA2-PSK test procedure and expected results

Step	STAUT	CTT acting as a test bed AP	CTT validation check	Expected Result
1	Reset the STAUT to its default configuration as specified in Table 11.			
2	Configure the STAUT as per Table 51.	Reset the AP to its default configuration as specified in Table 4. Configure the AP as per Table 52.		
3	Configure the STAUT to perform an active scan in the AP's operating channel. The STAUT transmits a Probe Request frame.	The AP transmits a Probe Response frame.	Verify that the AP transmits Beacon and Probe Response frames per the configuration in Table 52.	
4	Configure the STAUT to associate with the AP. The STAUT transmits an Association Request frame.	The AP transmits an Association Response frame.	For all scenarios except F: Verify that the AP transmits an Association Response frame to the STAUT with Status Code set to 0 (SUCCESS). For scenario F: If the Association Request frame is transmitted by the STAUT, verify that the AP transmits Association Response frame with status Code set to 0 (SUCCESS).	SN: For all scenarios except F: If the Association Request frame is transmitted by the STAUT, then CONTINUE, else FAIL. For scenario F: If the Association Request frame is transmitted by STAUT, then CONTINUE. Else if the Association Request frame is not transmitted by STAUT then PASS, else FAIL.
5	The STAUT and AP complete:			SN:

Step	STAUT	CTT acting as a test bed AP	CTT validation check	Expected Result
	• 4-way handshake • DHCP exchange			If the STAUT successfully completes a 4-way handshake, then CONTINUE, else FAIL.
6		The AP pings the STAUT IP address. <ping STAUT_IP_ADDR>, COUNT = 3, FRAME_RATE = 1		If the ping is successful, then PASS else FAIL.
Repeat Steps 2 - 6 for each scenario specified in Table 52.				

Table 55 provides the test procedure and expected results for this test case for 60 GHz STAUT.

Table 55. STAUT RSNE bounds verification using WPA2-PSK test procedure and expected results

Step	STAUT	CTT acting as a test bed AP	CTT validation check	Expected Result
1	Reset the STAUT to its default configuration as specified in Table 13.			
2	Configure the STAUT as per Table 51.	Reset the AP to its default configuration as specified in Table 6. Configure the AP as per Table 53.		
3	Perform STAUT and test bed AP initial test configuration as defined in Table 35.			
4	Configure the STAUT to perform an active scan in the AP's operating channel. The STAUT transmits a Probe Request frame.	The AP transmits a Probe Response frame.	Verify that the AP transmits DMG Beacon and Probe Response frames per the configuration in Table 53.	
5	Configure the STAUT to associate with the AP. The STAUT transmits an Association Request frame.	The AP transmits an Association Response frame.	For all scenarios except F: Verify that the AP transmits an Association Response frame to the STAUT with Status Code set to 0 (SUCCESS). For scenario F: If the Association Request frame is transmitted by the STAUT, verify that the AP transmits Association Response frame with status Code set to 0 (SUCCESS).	SN: For all scenarios except F: If the Association Request frame is transmitted by the STAUT, then CONTINUE, else FAIL. For scenario F: If the Association Request frame is transmitted by STAUT, then CONTINUE. Else if the Association Request frame is not transmitted by STAUT then PASS, else FAIL.
6	The STAUT and AP complete: • 4-way handshake • DHCP exchange			SN: If the STAUT successfully completes a 4-way handshake, then CONTINUE, else FAIL.

Step	STAUT	CTT acting as a test bed AP	CTT validation check	Expected Result
7		The AP pings the STAUT IP address. <ping STAUT_IP_ADDR>, COUNT = 20, FRAME_RATE = 1		If more than 5 consecutive ping timeouts occur in any of the ping tests, then FAIL. If more than 10% ping failures in any of the ping tests, then FAIL. If no fail messages are received, then PASS.
Repeat Steps 2 - 7 for each scenario specified in Table 53.				

5.2.5 STAUT unknown Root CA detection test

Objective

This test verifies that the STAUT correctly performs server certification validation during an EAP exchange and aborts an 802.1X EAP exchange when the server certificate does not chain up to the Trusted Root CA certificate installed on the STAUT.

A server certificate signed by an unknown CA is required for this test and shall be configured on the AAA server.

This test is repeated for all the EAP methods listed in Table 56 that are supported by the STAUT.

Applicability: Conditional. This test case is only required if the STAUT declared support for WPA2-Enterprise in Table 2.

References

IEEE 802.1X-2010 [3]

Test environment

- STAUT
- CTT acting as a test bed AP
- Wireless Sniffer
- AAA server

Test configuration

Table 56 defines the specific parameter values required for this test case.

Table 56. STAUT unknown Root CA detection test configuration

Parameter	STAUT value	CTT acting as a test bed AP value
Test bed vendor	N/A	For 2.4 and 5 GHz: Marvell For 60 GHz: Qualcomm
SSID	N/A	Wi-Fi
Operating channel	N/A	For dual band 2.4 and 5 GHz: 6 or For 5 GHz only: 44 For 60 GHz: 2
Security	WPA2-Ent	WPA2-Ent
EAP method	EAP-TLS EAP-TTLS EAP-PEAPv0 EAP-PEAPv1	EAP-TLS EAP-TTLS EAP-PEAPv0 EAP-PEAPv1

Test procedure and expected results

Table 57 provides the test procedure and expected results for this test case for 2.4 and 5 GHz STAUT.

Table 57. STAUT unknown Root CA detection test procedure and expected results

Step	STAUT	CTT acting as a test bed AP	AAA server	CTT validation check	Expected Result
1	Reset the STAUT to its default configuration as specified in Table 11.	Reset the AP to its default configuration as specified in Table 4. Configure the AP as per Table 56.	Configure a server certificate signed by an unknown CA on the AAA server.		
2	Configure the STAUT to perform an active scan in the AP's operating channel. The STAUT transmits a Probe Request frame.	The AP transmits a Probe Response frame.		Verify that the AP transmits Beacon and Probe Response frames per the configuration in Table 56.	
3	Configure the STAUT to associate with the AP.			Verify that during the 802.1X EAP exchange, the AP sends the server certificate signed by an unknown CA to the STAUT.	SN: If the STAUT indicates that 802.1X authentication has not been successful, then CONTINUE, Else if the STAUT completes EAP exchange and associates successfully with the AP, then FAIL.
4		The AP pings the STAUT IP address. <ping STAUT_IP_ADDR>, COUNT = 3, FRAME_RATE = 1			If the ping is successful, then FAIL else CONTINUE.
5			Configure a server certificate signed by a trusted CA on the AAA server.		
6	Trigger the STAUT to associate with the AP.				
7	The STAUT and AP complete: • Association exchange • 4-way handshake				SN: If the STAUT successfully completes 4-way handshake, then CONTINUE, else FAIL.
8		The AP pings the STAUT IP address. <ping STAUT_IP_ADDR>, COUNT = 3, FRAME_RATE = 1			If the ping is successful, then PASS else FAIL.

Table 58 provides the test procedure and expected results for this test case for 60 GHz STAUT.

Table 58. STAUT unknown Root CA detection test procedure and expected results

Step	STAUT	CTT acting as a test bed AP	AAA server	CTT validation check	Expected Result
1	Reset the STAUT to its default configuration as specified in Table 13.	Reset the AP to its default configuration as specified in Table 6. Configure the AP as per Table 56.	Configure a server certificate signed by an unknown CA on the AAA server.		
2	Perform STAUT and test bed AP initial test configuration as defined in Table 35.				
3	Configure the STAUT to perform an active scan in the AP's operating channel. The STAUT transmits a Probe Request frame.	The AP transmits a Probe Response frame.		Verify that the AP transmits Beacon and Probe Response frames per the configuration in Table 56.	
4	Configure the STAUT to associate with the AP.			Verify that during the 802.1X EAP exchange, the AP sends the server certificate signed by an unknown CA to the STAUT.	SN: If the STAUT indicates that 802.1X authentication has not been successful, then CONTINUE, Else if the STAUT completes EAP exchange and associates successfully with the AP, then FAIL.
5		The AP pings the STAUT IP address. <ping STAUT_IP_ADDR>, COUNT = 3, FRAME_RATE = 1			If the ping is successful, then FAIL else CONTINUE.
6			Configure a server certificate signed by a trusted CA on the AAA server.		
7	Trigger the STAUT to associate with the AP.				
8	The STAUT and AP complete: • Association exchange • 4-way handshake				SN: If the STAUT successfully completes 4-way handshake, then CONTINUE, else FAIL.
9		The AP pings the STAUT IP address.			If more than 5 consecutive ping timeouts occur in any of the ping tests, then FAIL.

Step	STAUT	CTT acting as a test bed AP	AAA server	CTT validation check	Expected Result
		<ping STAUT_IP_ADDR>, COUNT = 20, FRAME_RATE = 1			If more than 10% ping failures in any of the ping tests, then FAIL. If no fail messages are received, then PASS.

Appendix A (Normative) Test bed products

A.1 Approved test bed vendors

All test bed equipment is available exclusively from:

Tessco Technologies

11126 McCormick Road

Hunt Valley, Maryland 21031

wifialliance@tessco.com

Note that the distributor does not supply technical support and cannot answer technical questions regarding this equipment. A contact person for each device is listed herein that may be able to direct technical questions to the correct resource.

The current list of all approved test bed equipment for all Wi-Fi Alliance test beds may be accessed at the ftp site: https://www.wi-fi.org/members/certification-testing/test-bed-information.

A.2 Approved test bed equipment

Table 61, Table 62 and Table 63 provide the approved test bed equipment for the DUTs listed in this test plan.

Table 59. Approved test bed AP

Vendor	Product	Software version(s)	Band supported	Contact
Marvell	RD-88W-AP-8964-WIFI-R0	version,9.1.1.8-wpa3.p8-W8964 firmware,9.3.1.4	2.4 and 5 GHz	wifilab-support@marvell.com
Qualcomm	CA-65-Y9345-DPP	IPQ8064.ILQ.6.1.r2-00000008-P-1	2.4 and 5 GHz	wfa.security.support@qti.qualcomm.com
Qualcomm	CA-65-YA181	AP181_Nand-IPQ8064_SPF-5.2.0.1-May-2019_11AD	60 GHz	WFA_60G_Support_Group@qti.qualcomm.com

Table 60. Approved test bed STA

Vendor	Product	Software version(s)	Band supported	Contact
Intel	9260.NGWG.NV	Linux_Core_build_12993:f4a943c/39.6081708d.0 / build:497/commit:256abd7	2.4 and 5 GHz	wfa.external.support@intel.com
Marvell	RD-88W-8997P-WIFI-S0	PCIE8997-3.28.18.p1-C4X16C518-GPL-(FP68)/ Mrvl-WFASigma_ver_Security_R0.1(14:44:30 Apr 5 2018)	2.4 and 5 GHz	wifilab-support@marvell.com
Qualcomm	QC-DB-L00003_1	Q835/1.0 (OpenQ-835_Android-N_WFA-DPP-WPA3_v1.4-ITC-JFlash)	2.4 and 5 GHz	wfa.security.support@qti.qualcomm.com
Qualcomm	CA-65-YA181	AP181_Nand-IPQ8064_SPF-5.2.0.1-May-2019_11AD	60 GHz	WFA_60G_Support_Group@qti.qualcomm.com

Table 61. Approved test tools

Vendor	Product	Software version(s)	Band supported	Contact
Qualcomm	Sniffer/ CA-65-Y9345-LCT (OpenWrt Chaos Calmer 15.05.1)	UnKnown_4.12.0-rc6+	2.4 and 5 GHz	support@wi-fi.org
Intel	Packet Injector/ 8260.NGWMG.NVL	Ubuntu 16.04, Kernel: 4.4.0-21	2.4 and 5 GHz	support@wi-fi.org
Peraso Sniffer	PRSW120	A.1.1804.004600	60 GHz	support-wifi60ghz@perasotech.com

Appendix B (Informative) Document revision history

Table 62. Document revision history

Version	Date YYYY-MM-DD	Remarks
1.0	2018-04-09	Initial release.
1.1	2019-05-22	Added WiGig test requirements. Removed 5.2.6 as it is moved to KRACK test plan v2.3