CONFIDENTIAL TRADE SECRET

FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE® MEMBERS

– DO NOT COPY –

WPA3™-SAE

Test Plan

Version 1.4

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/certification-programs

© 2020 Wi-Fi Alliance. All Rights Reserved.
This document contains confidential trade secrets intended solely for use by only authorized Wi-Fi Alliance members.
For the latest up-to-date information, please refer to the Wi-Fi Alliance website's members-only area.

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

Wi-Fi Alliance owns the copyright in this document and reserves all rights therein. This document and any related materials may only be used by Wi-Fi Alliance members for their internal use, such as quality assurance and pre-certification activities, and for their participation in approved Wi-Fi Alliance activities, such as the Wi-Fi Alliance certification program, unless otherwise permitted by Wi-Fi Alliance through prior written consent. A user of this document may duplicate and distribute copies of the document in connection with the authorized uses described above, provided any duplication in whole or in part includes the copyright notice and the disclaimer text set forth herein. Unless prior written permission has been received from Wi-Fi Alliance, any other use of this document and all other duplication and distribution of this document are prohibited. Wi-Fi Alliance regards the unauthorized use, duplication or distribution of this document by a member as a material breach of the member's obligations under the organization's rules and regulations, which may result in the suspension or termination of Wi-Fi Alliance membership. Unauthorized use, duplication, or distribution by nonmembers is an infringement of the Wi-Fi Alliance's copyright. Distribution of this document to persons or organizations who are not members of Wi-Fi Alliance is strictly prohibited. TO PREVENT UNAUTHORIZED ACCESS, DO NOT STORE ON COMPUTER ANY LONGER THAN REQUIRED.

THIS DOCUMENT IS PROVIDED "AS IS" AND WITHOUT WARRANTY OF ANY KIND. TO THE GREATEST EXTENT PERMITTED BY LAW, WI-FI ALLIANCE DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF TITLE, NONINFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. WI-FI ALLIANCE DOES NOT WARRANT THAT THIS DOCUMENT IS COMPLETE OR WITHOUT ERROR AND DISCLAIMS ANY WARRANTIES TO THE CONTRARY. NOTHING IN THIS DOCUMENT CREATES ANY WARRANTIES WHATSOEVER REGARDING THE SUITABILITY OR NON-SUITABILITY OF A PRODUCT OR A SERVICE FOR CERTIFICATION UNDER ANY CERTIFICATION PROGRAM OF WI-FI ALLIANCE OR ANY THIRD PARTY.

© 2020 Wi-Fi Alliance. All Rights Reserved.

Table of contents

1 OVERVIEW 7
1.1 Scope and purpose 7
1.2 Definition of devices under test 7
1.3 References 7
1.4 Acronyms and definitions 8
1.4.1 Acronyms and abbreviations 8
1.4.2 Definitions 8

2 TEST TOOLS, METHODOLOGY AND APPROACH 9
2.1 Sniffer 9
2.2 Wi-Fi Test Suite software 9
2.3 Basic system test configuration 9
2.4 Test bed capability requirements 10
2.4.1 CTT/Test bed AP requirements 10
2.4.2 CTT/Test bed STA requirements 11

3 REQUIREMENTS FOR WI-FI ALLIANCE CERTIFICATION 12
3.1 General requirements 12
3.1.1 Prerequisite certification requirements 12
3.1.2 Testing requirements 12
3.2 Applicability of tests 12
3.2.1 APUT tests 13
3.2.2 STAUT tests 14
3.3 Configuration requirements 14
3.3.1 DUT configuration requirements 14
3.4 Testing rules 15

4 WPA3-SAE APUT TESTS 16
4.1 APUT configuration requirements validation test 16
4.2 APUT WPA3-SAE tests 18
4.2.1 APUT initial configuration test 18
4.2.2 APUT connectivity and PMK caching test 20
4.2.3 APUT Anti-clogging test 22
4.2.4 APUT WPA2-Personal transition test 23
4.2.5 APUT support for additional finite cyclic groups test 26
4.2.6 APUT negative test 28
4.2.7 APUT WPA2-Personal transition negative test 31
4.2.8 APUT correct handling of PMKID during initial WPA3-SAE association test 32
4.3 APUT rejecting unsuitable Diffie-Hellman groups for SAE tests 34

5 WPA3-SAE STAUT TESTS 37
5.1 STAUT configuration requirements validation test 37
5.2 STAUT WPA3-SAEtests 39
5.2.1 STAUT SAE connectivity and PMK caching test 39

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

5.2.2 STAUT Anti-clogging test 42
5.2.3 STAUT reflection attack test 45
5.2.4 STAUT WPA2-Personal compatibility test 47
5.2.5 STAUT support for additional finite cyclic groups test 49
5.2.6 STAUT negative test 51
5.2.7 STAUT SAE confirmation exchange variation test 53
5.3 STAUT does not request unsuitable Diffie-Hellman groups for SAE tests 56
APPENDIX A (NORMATIVE) TEST BED PRODUCTS 58
A.1 Approved test bed vendors 58
A.2 Approved test bed equipment 58
APPENDIX B (INFORMATIVE) DOCUMENT REVISION HISTORY 60

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

List of tables

Table 1. General capabilities declaration 7
Table 2. Acronyms and abbreviations 8
Table 3. CTT/Test bed AP default parameters 11
Table 4. CTT/Test bed STA default parameters 11
Table 5. APUT test applicability 13
Table 6. STAUT test applicability 14
Table 7. APUT default parameters 15
Table 8. STAUT default parameters 15
Table 9. APUT configuration requirements validation test procedure and expected results 16
Table 10. APUT initial configuration test configuration 18
Table 11. APUT initial configuration test procedure and expected results 19
Table 12. APUT connectivity and PMK caching test configuration 20
Table 13. APUT connectivity and PMK caching test procedure and expected results 21
Table 14. APUT Anti-clogging test configuration 22
Table 15. APUT Anti-clogging test procedure and expected results 22
Table 16. APUT WPA2-Personal transition test configuration 24
Table 17. APUT WPA2-Personal transition test procedure and expected results 24
Table 18. APUT support for additional finite cyclic groups test configuration 26
Table 19. APUT support for additional finite cyclic groups test procedure and expected results 27
Table 20. APUT negative test configuration 28
Table 21. APUT negative test procedure and expected results 29
Table 22. APUT WPA2-Personal transition negative test configuration 31
Table 23. APUT WPA2-Personal transition negative test procedure and expected results 32
Table 24. APUT correct handling of PMKID during initial WPA3-SAE association test configuration 32
Table 25. APUT correct handling of PMKID during initial WPA3-SAE association test procedure and expected results 33
Table 26. Test configuration 35
Table 27. DH group list and suitability for SAE 35
Table 28. Test procedure and expected results 36
Table 29. STAUT configuration requirements validation test configuration 37
Table 30. STAUT configuration requirements validation test procedure and expected results 37
Table 31. STAUT SAE connectivity and PMK caching test configuration 39
Table 32. STAUT SAE connectivity and PMK caching test procedure and expected results 40
Table 33. STAUT Anti-clogging test configuration 42
Table 34. STAUT Anti-clogging test procedure and expected results 42
Table 35. STAUT reflection attack test configuration 45
Table 36. STAUT reflection attack test procedure and expected results 46
Table 37. STAUT WPA2-Personal compatibility test configuration 47
Table 38. STAUT WPA2-Personal compatibility test procedure and expected results 48
Table 39. STAUT support for additional finite cyclic groups test configuration 49
Table 40. STAUT support for additional finite cyclic groups test procedure and expected results 50
Table 41. STAUT negative test configuration 51
Table 42. STAUT negative test procedure and expected results 52

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Table 43. SAE confirmation exchange variation configuration 54
Table 44. SAE confirmation exchange variation procedure and expected results 54
Table 45. Test configuration 56
Table 46. Test procedure and expected results 56
Table 47. Approved test bed access points 58
Table 48. Approved test bed stations 58
Table 49. Approved test tools 59
Table 50. Document revision history 60

List of figures

Figure 1. System test configuration 10

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

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 has been developed. Working in conjunction with authorized test labs, these tests are executed on vendor products for the WPA3™-SAE feature. Products that successfully pass all certification requirements listed in the Wi-Fi CERTIFIED WPA3™ Test Plan [1] shall be granted Wi-Fi CERTIFIED WPA3 certification.

The scope of this test plan is governed by the Wi-Fi Alliance Security Enhancements Marketing Requirements Document [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 WPA3-SAE 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.

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. General capabilities declaration

Item	Question	Test case	Vendor response
1	Does the APUT support AP-generated unique password? If Yes, the APUT vendor shall provide instructions to the user to fetch this password using UI or automation.	4.2.1	Yes/No
2	Does the APUT have the ability to enable SAE separately without provisioning a password?	4.2.1	Yes/No
3	What is the default value of the AntiCloggingThreshold on the APUT?	4.2.3	Value
4	Provide a list of finite cyclic groups supported by the APUT.	4.1, 4.2.5, 4.3	Value
5	Provide a list of finite cyclic groups supported by the STAUT.	5.1, 5.2.5, 5.3	Value
6	Does the STAUT support PMKSA caching when the disconnect command is triggered on the STAUT?	5.2.1	Yes/No

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] Wi-Fi CERTIFIED WPA3™ Test Plan, https://www.wi-fi.org/members/certification-programs

[2] Security Enhancements Marketing Requirements Document, v1.21, https://www.wi-fi.org/members/certification-programs

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

[3] IEEE Std 802.11™-2016 - IEEE Standard for Local and Metropolitan Area Networks -Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

[4] WPA3 Specification, https://www.wi-fi.org/members/certification-programs

1.4 Acronyms and definitions

1.4.1 Acronyms and abbreviations

Table 2 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.

Table 2. Acronyms and abbreviations

Acronyms	Definition
AKM	Authentication and key management
CCMP	CTR with CBC-MAC Protocol
DH	Diffie–Hellman
DUT	Device Under Test
EAPoL	Extensible Authentication Protocol over LANs (IEEE Std 802.1X-2010)
ECDH	Elliptic curve Diffie–Hellman
PMK	Pairwise master key
PMKID	Pairwise master key identifier
RSNE	Robust Security Network element
SAE	Simultaneous authentication of equals
WPA2™-PSK	Wi-Fi Protected Access® 2 - Pre-Shared Key

1.4.2 Definitions

There are no special definitions for this document.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

2 Test tools, methodology and approach

This section defines the tools, methodology, and approach for testing devices for the WPA3-SAE feature.

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
- Ability to parse SAE 802.11 Authentication frames
- Ability to parse 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 WPA3-SAE devices.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

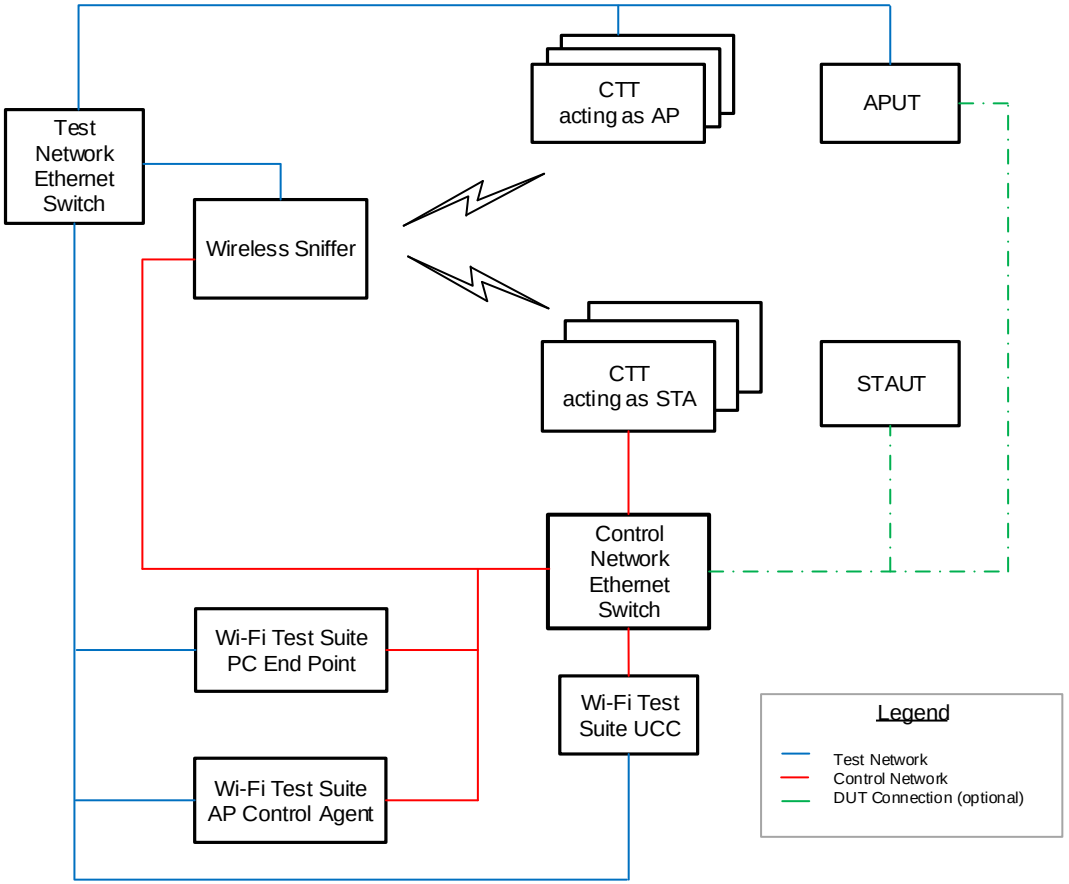

Figure 1. System test configuration

2.4 Test bed capability requirements

2.4.1 CTT/Test bed AP requirements

The following capabilities are required of the CTT/test bed AP.

- Able to open, and keep open, multiple simultaneous SAE connections with the STAUT

Table 3 defines the WPA3-SAE default parameters for the test bed AP. If required, the following parameter values are modified for specific test cases.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Table 3. CTT/Test bed AP default parameters

Parameter	Description	Default value
SSID	Service Set Identifier	Wi-Fi
Operating channel	Primary channel used for the test	44 (if dual band STAUT, else 6)
Security / AKM Suite	802.11 Security method	SAE / 00-0F-AC:8
Cipher Suite Type	Cipher suite	4 (CCMP-128) For 2.4 GHz and 5 GHz STAUT
PMF	Protected management frame	Required
Passphrase	Key used for encryption	12345678

2.4.2 CTT/Test bed STA requirements

The following capabilities are required of the CTT/test bed STA.

- Able to open, and keep open, multiple simultaneous SAE connections with a SAE-capable APUT (Anti-clogging device)

Table 4 defines the WPA3-SAE default parameters for the test bed STA. If required, the following parameter values are modified for specific test cases.

Table 4. CTT/Test bed STA default parameters

Parameter	Description	Default value
Security / AKM Suite	802.11 Security method	SAE / 00-0F-AC:8
Cipher Suite Type	Cipher suite	4 (CCMP-128) For 2.4 GHz and 5 GHz APUT
PMF	Protected management frame	Required
Passphrase	Key used for encryption	12345678

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

3 Requirements for Wi-Fi Alliance certification

The following items describe the necessary features that are required for a DUT to pass WPA3-SAE feature testing.

3.1 General requirements

The DUT shall comply with all the following general requirements.

3.1.1 Prerequisite certification requirements

An WPA3-SAE APUT device shall implement and pass the following Wi-Fi Alliance certifications as a prerequisite:

- A Wi-Fi CERTIFIED PHY (11a/b/g/n/ac)
- Wi-Fi CERTIFIED WPA2™ with Protected Management Frames

An WPA3-SAE STAUT device shall implement and pass the following Wi-Fi Alliance certifications as a prerequisite:

- A Wi-Fi CERTIFIED PHY (11a/b/g/n/ac)
- Wi-Fi CERTIFIED WPA2 with Protected Management Frames

3.1.2 Testing requirements

This section lists the DUT requirements that are necessary to execute the test cases in this test plan.

- The DUT shall be able to be configured with a password/phrase/key/code to be used to establish link layer security.
- A STAUT shall support at least one cached PMK. An SAE-capable STA can retain in its cache the PMKs it established as a result of a successful SAE authentication. This test plan validates that at least one cached PMK is supported.
- This test plan is only applicable for DUTs that support 2.4 GHz and/or 5 GHz.
- If the DUT was previously certified for WPA3-Personal certification using WPA3-SAE test plan v1.0, supports ECP group 25 and/or ECP group 26 from Table 27, and is submitted for recertification, contact staff (support@wi-fi.org) to request a waiver to continue to support ECP group 25 and/or ECP group 26.

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 5 and Table 6 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

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

the WPA3-SAE 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 5 summarizes the APUT tests for WPA3-SAE feature certification.

Table 5. 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 configuration requirements validation test	4.1	M		
APUT initial configuration test	4.2.1	M		
APUT connectivity and PMK caching test	4.2.2	M		
APUT Anti-clogging test	4.2.3	M		
APUT WPA2-Personal transition test	4.2.4	M		
APUT support for additional finite cyclic groups test	4.2.5	C	Y [refer to Table 1]	N
APUT negative test	4.2.6	M		
APUT WPA2-Personal transition negative test	4.2.7	M		
APUT correct handling of PMKID during initial WPA3-SAE association test	4.2.8	M		
APUT rejecting unsuitable Diffie-Hellman groups for SAE tests	4.3	M		

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

3.2.2 STAUT tests

Table 6 summarizes the STAUT tests for WPA3-SAE feature certification.

Table 6. 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? (Y/N)
STAUT configuration requirements validation test	5.1	M		
STAUT SAE connectivity and PMK caching test	5.2.1	M		
STAUT Anti-clogging test	5.2.2	M		
STAUT reflection attack test	5.2.3	M		
STAUT WPA2-Personal compatibility test	5.2.4	M		
STAUT support for additional finite cyclic groups test	5.2.5	C	Y [refer to Table 1]	N
STAUT negative test	5.2.6	M		
STAUT SAE confirmation exchange variation test	5.2.7	M		
STAUT does not request unsuitable Diffie-Hellman groups for SAE tests	5.3	M		

3.3 Configuration requirements

The DUT parameters that require manual configuration are listed below.

1. SSID
2. Wireless operational mode (a/b/g/n/ac)
3. Channel
4. SAE support
5. Password/phrase/code/key

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

3.3.1 DUT configuration requirements

Table 7 lists the default APUT configuration values that a technician shall set within a test procedure. Specific test cases may impose additional configuration requirements.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Table 7. APUT default parameters

Parameter	Description	Default value
SSID	Service Set Identifier	Wi-Fi
Operating channel	Primary channel used for the test	44 (if dual band APUT, else 6)
Security / AKM Suite	802.11 Security method	SAE / 00-0F-AC:8
Cipher Suite Type	Cipher suite	4 (CCMP-128) For 2.4 GHz and 5 GHz APUT
PMF	Protected management frame	Required
Passphrase	Key used for encryption	12345678

Table 8 lists the default STAUT configuration values that a technician shall set within a test procedure. Specific test cases may impose additional configuration requirements.

Table 8. STAUT default parameters

Parameter	Description	Default value
Security / AKM Suite	802.11 Security method	SAE / 00-0F-AC:8
Cipher Suite Type	Cipher suite	4 (CCMP-128) For 2.4 GHz and 5 GHz APUT
PMF	Protected management frame	Required
Passphrase	Key used for encryption	12345678

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.
3. By default, PMK caching capability is enabled on the APUT and the STAUT.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

4 WPA3-SAE APUT tests

4.1 APUT configuration requirements validation test

Objective

This test verifies that the APUT is configurable with the parameters required for the test cases in section 4. In addition to basic wireless configuration (SSID, operational mode, channel) there is a password/phrase/code/key that shall be configured, and optionally additional finite cyclic groups may be configured.

The configuration parameters are defined in section 3.3. Note that this test case is not automated by a Wi-Fi Test Suite script. The technician shall manually configure the required parameters through the user interface.

Applicability: Mandatory

References

None

Test environment

- APUT

Test procedure and expected results

Table 9 provides the specific test procedure and expected results for this test case.

Table 9. APUT configuration requirements validation test procedure and expected results

Step	DUT	Expected result
1	Configure support for SAE.	If able to configure support for SAE, then CONTINUE, else FAIL.
2	Configure the password/phrase/code/key.	If able to configure password/phrase/code/key, then CONTINUE, else FAIL.
3	If the APUT supports multiple finite cyclic groups, configure each supported group (one at a time) on the APUT.	If able to configure the supported finite cyclic groups, then CONTINUE, else FAIL. If the APUT allows configuration of any unsuitable DH group (as per Table 27) using the end user interface, then FAIL, else CONTINUE.
4	Enable SAE and WEP support on the APUT.	If able to configure WEP when SAE is enabled, then FAIL, else CONTINUE.
5	Enable SAE and TKIP support on the APUT.	If able to configure TKIP when SAE is enabled, then FAIL, else CONTINUE.
6	Enable both SAE and WPA2-Personal on the APUT for the same BSS.	If able to configure SAE and WPA2-Personal for the same BSS, then CONTINUE, else FAIL.
7	Configure WPA Version 1 on the same BSS where SAE is enabled.	If able to configure WPA Version 1 with SAE enabled for the same BSS, then FAIL, else CONTINUE.
8	Configure WPA2-Personal with TKIP with SAE enabled for the same BSS.	If the APUT can be configured in the transition mode for SAE when WPA2-Personal is configured with TKIP, then FAIL, else CONTINUE.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Step	DUT	Expected result
9	Configure the APUT in transition mode with WPA2-Personal with CCMP and attempt to enter SAE passphrase that is > 63 characters.	If the APUT is unable to be provisioned with the passphrase then PASS, else FAIL.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

4.2 APUT WPA3-SAE tests

The following tests verify SAE support on an APUT device.

4.2.1 APUT initial configuration test

Objective

This test verifies that the APUT is able to be properly configured to support SAE.

Applicability: Mandatory

References

Section 12.4.5 [1]

Test environment

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

Test configuration

Table 10 defines the specific parameter values required for this test case.

Table 10. APUT initial configuration test configuration

Parameter	APUT value	CTT acting as a test bed STA value
Test bed vendor	N/A	Marvell
SSID	Wi-Fi	N/A
Operating channel	44 (if dual band APUT, else 6)	N/A
AKM Suite Type	8 (SAE)	8 (SAE)
Cipher Suite Type	4 (CCMP-128) for 2.4 GHz and 5 GHz APUT	4 (CCMP-128) for 2.4 GHz and 5 GHz APUT
Password	12345678	12345678

Test procedure and expected results

Table 11 provides the test procedure and expected results for this test case.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Table 11. APUT initial configuration test procedure and expected results

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
1	Reset the APUT to its default configuration as specified in Table 7. If the APUT has the ability to enable SAE separately without provisioning a password, then enable SAE, otherwise go to Step 4.			
2	Change the SAE AKM selector configuration from disabled to enabled on the APUT.			SN: Wait 10 seconds. If the APUT does not transmit Beacon frames with SAE AKM (00-0F-AC:8) in the RSNE, then CONTINUE, else FAIL.
3		Reset the STA to its default configuration as specified in Table 4. Trigger the STA to perform SAE authentication with the APUT.	Verify that the STA transmits an Authentication frame with Authentication Algorithm Number field set to 3. to the APUT.	SN: If the APUT refuses SAE authentication attempts from the STA then CONTINUE, else FAIL.
4	Configure the password in Table 10 on the APUT. The APUT starts transmitting Beacon frames.			SN: Verify that the captured Beacon frame contains an RSNE with the following: 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 01 00 4. Pairwise Cipher Suite List is set to CCMP 00-0F-AC:4 5. AKM Suite Count is set to 01 00 6. AKM Suite List is set to 00-0F-AC:8 7. PMKID Count is set to 0 or is not present 8. PMKID List is not present 9. MFPR bit (bit 6) in RSN Capabilities field set to 1 If all conditions are true, then CONTINUE else FAIL.
5		Reset the STA to its default configuration as specified in Table 4. Trigger the STA to perform active scan on the operating channel of the APUT.	Verify that the STA sends Probe Request frame to the APUT.	SN: Verify that the captured Probe Response frame contains an RSNE with the following: 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 01 00 4. Pairwise Cipher Suite List is set to CCMP 00-0F-AC:4 5. AKM Suite Count is set to 01 00 6. AKM Suite List is set to 00-0F-AC:8 7. PMKID Count is set to 0 or is not present 8. PMKID List is not present 9. MFPR bit (bit 6) in RSN Capabilities field set to 1 If all conditions are true, then PASS else FAIL.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

4.2.2 APUT connectivity and PMK caching test

Objective

This test verifies that the APUT is able to perform an SAE handshake with the test bed STA.

Applicability: Mandatory

References

Sections 12.4.5, 12.6.10.3 [1]

Test environment

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

Test configuration

Table 12 defines the specific parameter values required for this test case.

Table 12. APUT connectivity and PMK caching test configuration

Parameter	APUT value	CTT acting as a test bed STA value
Test bed vendor	N/A	Intel
SSID	Wi-Fi	N/A
Operating channel	44 (if dual band APUT, else 6)	N/A
AKM Suite Type	8 (SAE)	8 (SAE)
Cipher Suite Type	4 (CCMP-128) For 2.4 GHz and 5 GHz APUT:	4 (CCMP-128) For 2.4 GHz and 5 GHz APUT
Password	0123456789abcdef0123456789abcdef	0123456789abcdef0123456789abcdef

Test procedure and expected results

Table 13 provides the test procedure and expected results for this test case.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Table 13. APUT connectivity and PMK caching test procedure and expected results

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
1	Reset the APUT to its default configuration as specified in Table 7. Configure the APUT as specified in Table 12.	Reset the STA to its default configuration as specified in Table 4.		
2	The APUT starts transmitting Beacon frames.			SN: If the APUT includes SAE AKM (00-0F-AC:8) in the RSNE in Beacon frames, then CONTINUE, else FAIL.
3		Configure the STA as specified in Table 12. Trigger the STA to perform SAE authentication with the APUT.	SN: Verify that the STA transmits an Authentication frame with Authentication Algorithm Number field set to 3.	SN: Verify the following behavior between the APUT and STA: 1. Exchanges SAE authentication frames with Authentication Transaction Sequence number set to 1. 2. Exchanges SAE authentication frames with Authentication Transaction Sequence number set to 2. 3. Performs 4-way handshake. If all conditions are true, then CONTINUE, else FAIL.
4		Configure the STA to ping the APUT's console IP address. <ping CONSOLE_IP_ADDR>, COUNT = 3, FRAME_RATE = 1		If the ping is successful, then CONTINUE, else FAIL.
5		Trigger the STA to disconnect from the APUT.		
6		Trigger the STA to re-associate with the APUT	SN: Verify that the STA transmits an Authentication frame with Authentication Algorithm Number field set to 0. SN: Inspect the sniffer capture and verify that the PMKID is included in the (Re)Association Request frame from the STA to the APUT.	SN: If the PMKID in EAPOL message 1 from APUT and the PMKID in (Re)Association Request frame from STA matches then CONTINUE, else FAIL.
7		Configure the STA to ping the APUT's console IP address. <ping CONSOLE_IP_ADDR>, COUNT = 3, FRAME_RATE = 1		If the ping resumes within 15 seconds, then PASS, else FAIL.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

4.2.3 APUT Anti-clogging test

Objective

This test verifies that the APUT is able to detect and appropriately respond to a distributed denial of service attack.

Applicability: Mandatory

References

Section 12.4.6 [1]

Test environment

- APUT
- CTT acting as a test bed STA
- Wireless Sniffer
- Packet Injector acting as a clogging device,

Test configuration

Table 14 defines the specific parameter values required for this test case.

Table 14. APUT Anti-clogging test configuration

Parameter	APUT value	CTT acting as a test bed STA value	Packet Injector value
Test bed vendor	N/A	Qualcomm	N/A
SSID	Wi-Fi	N/A	N/A
Operating channel	44 (if dual band APUT, else 6)	N/A	Same as APUT
AKM Suite Type	8 (SAE)	8 (SAE)	N/A
Cipher Suite Type	4 (CCMP-128)	4 (CCMP-128)	N/A
Password	12345678	12345678	N/A

Test procedure and expected results

Table 15 provides the test procedure and expected results for this test case.

Table 15. APUT Anti-clogging test procedure and expected results

Step	APUT	CTT acting as a test bed STA	Packet Injector	CTT validation check	Expected Result
1	Reset the APUT to its default configuration as specified in Table 7.	Reset the STA to its default configuration as specified in Table 4.			

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Step	APUT	CTT acting as a test bed STA	Packet Injector	CTT validation check	Expected Result
	Configure the APUT as specified in Table 14.				
2	The APUT starts transmitting Beacon frames.		Trigger the packet injector to transmit SAE Commit messages from different MAC addresses.		Note: The APUT has more than N simultaneous open connections
3		Configure the STA as specified in Table 14. Trigger the STA to perform SAE authentication with the APUT.		SN: The STA attempts to connect to the AP using SAE by transmitting an SAE Commit message with: • Authentication Algorithm Number = 3 • Authentication Transaction Sequence number = 1	SN: Verify the APUT transmits an Authentication frame with the following: 1. Authentication Algorithm Number = 3. 2. Authentication Transaction Sequence number = 1. 3. Status Code = 76 (Anti-Clogging Token Requested). 4. Anti-Clogging Token present. If all conditions are true, then CONTINUE, else FAIL.
4				SN: STA sends a subsequent SAE Commit message and includes the received Anti-Clogging Token in the Authentication frame.	SN: Verify the following behavior between the APUT and STA: 1. Accepts STA SAE frame with Anti-Clogging Token by responding with an SAE Commit message with Authentication Transaction Sequence number set to 1. 2. Exchanges SAE Authentication frames with Authentication Transaction Sequence number set to 2. 3. Performs 4-way handshake. If all conditions are true, then CONTINUE, else FAIL.
5		Configure the STA to ping the APUT's console IP address. <ping CONSOLE_IP_ADDR>, COUNT = 3, FRAME_RATE = 1			If the ping is successful then PASS, else FAIL.

4.2.4 APUT WPA2-Personal transition test

Objective

This test verifies that the APUT is able to support SAE and WPA2-Personal on a single SSID.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Applicability: Mandatory

References

Sections 12.4, 12.5 [1]

Test environment

- APUT
- CTT acting as test bed STA1
- CTT acting as test bed STA2
- Wireless Sniffer

Test configuration

Table 16 defines the specific parameter values required for this test case.

Table 16. APUT WPA2-Personal transition test configuration

Parameter	APUT value	CTT acting as a test bed STA1 value	CTT acting as a test bed STA1 value
Test bed vendor	N/A	Qualcomm	Marvell
SSID	Wi-Fi	N/A	N/A
Operating channel	44 (if dual band APUT, else 6)	N/A	N/A
AKM Suite Type	Transitional compatibility mode 2 (PSK) and 8 (SAE)	8 (SAE)	2 (PSK)
Cipher Suite Type	4 (CCMP-128)	4 (CCMP-128)	4 (CCMP-128)
PMF	Enabled	Enabled	Enabled
Password	12345678123456781234567812345678	12345678123456781234567812345678	12345678123456781234567812345678

Test procedure and expected results

Table 17 provides the test procedure and expected results for this test case.

Table 17. APUT WPA2-Personal transition test procedure and expected results

Step	APUT	CTT acting as a test bed STA1	CTT acting as a test bed STA2	CTT validation check	Expected Result
1	Reset the APUT to its default configuration as specified in Table 7.	Reset STA1 to its default configuration as specified in Table 4.	Reset STA2 to its default configuration as specified in Table 4.		
2	Configure the APUT as specified in Table 16 for both SAE and PSK on a single SSID.				SN: If the Beacon frames from the APUT advertise support for both SAE and PSK as an AKM

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Step	APUT	CTT acting as a test bed STA1	CTT acting as a test bed STA2	CTT validation check	Expected Result
					Suite type, then CONTINUE, else FAIL.
3		Configure STA1 as specified in Table 16. Trigger STA1 to perform SAE authentication with the APUT.		SN: Verify that the STA transmits an Authentication frame with Authentication Algorithm Number field set to 3 and sends Association Request frame for SAE.	SN: Verify the following behavior between the APUT and STA1: 1. SAE authentication completes successfully. 2. Successful 4-way handshake. If all conditions are true, then CONTINUE else FAIL.
4		Configure STA1 to ping the APUT's console IP address. <ping CONSOLE_IP_ADDR>, COUNT = 3, FRAME_RATE = 1			If the ping is successful, then CONTINUE, else FAIL.
5			Configure STA2 as specified in Table 16. Trigger STA2 to perform WPA2-Personal association with the APUT.	SN: Verify that the STA transmits an Authentication frame with Authentication Algorithm Number field set to 0 and sends Association Request frame for WPA2-Personal	SN: Verify the following behavior between the APUT and STA2: 1. WPA2-Personal association is successful. 2. Successful 4-way handshake. If all conditions are true, then CONTINUE else FAIL.
6			Configure STA2 to ping the APUT's console IP address. <ping CONSOLE_IP_ADDR>, COUNT = 3, FRAME_RATE = 1		If the ping is successful then PASS, else FAIL.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

4.2.5 APUT support for additional finite cyclic groups test

Objective

This test verifies that the APUT is able to support additional (EC)DH finite cyclic groups.

This test shall be repeated for all finite cyclic groups supported by the APUT.

Applicability: Conditional mandatory. This test case is required if the APUT declared support for (EC)DH finite cyclic groups in Table 1.

References

Section 12.4.4 [1]

Test environment

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

Test configuration

Table 18 defines the specific parameter values required for this test case.

Table 18. APUT support for additional finite cyclic groups test configuration

Parameter	APUT value	CTT acting as a test bed STA value
Test bed vendor	N/A	Qualcomm
SSID	Wi-Fi	N/A
Operating channel	44 (if dual band APUT, else 6)	N/A
AKM Suite Type	8 (SAE)	8 (SAE)
Cipher Suite Type	4 (CCMP-128)	4 (CCMP-128)
Password	12345678	12345678
(EC)DH finite cyclic group	As supported	As supported by APUT

Test procedure and expected results

Table 19 provides the test procedure and expected results for this test case.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Table 19. APUT support for additional finite cyclic groups test procedure and expected results

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
1	Reset the APUT to its default configuration as specified in Table 7. Configure the APUT as specified in Table 18. The APUT starts transmitting Beacon frames.	Reset the STA to its default configuration as specified in Table 4.		SN: If the Beacon frames from the APUT advertise support for SAE, then CONTINUE, else FAIL.
2		Configure the STA as specified in Table 18 and configure the (EC)DH finite cyclic group to a value other than 19 that is supported by the APUT.		
3		Trigger the STA to associate with the APUT.	Verify that the STA is using the correct group in the SAE Commit message.	SN: Verify that the APUT: 1. Performs SAE using an (EC)DH finite cyclic group provisioned on the STA. 2. Performs 4-way handshake with the STA. If all conditions are true, then CONTINUE, else FAIL.
4		Configure the STA to ping the APUT's console IP address. <ping CONSOLE_IP_ADDR>, COUNT = 3, FRAME_RATE = 1		If the ping is successful then CONTINUE, else FAIL.
5	Repeat steps 2-4 for all other (EC)DH finite cyclic groups supported by the APUT.			If all supported (EC)DH finite cyclic groups pass, then PASS, else FAIL.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

4.2.6 APUT negative test

Objective

This test verifies that the APUT correctly rejects improper elements received from the test bed STA.

Applicability: Mandatory

References

Section 12.4 [1]

Test environment

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

Test configuration

Table 20 defines the specific parameter values required for this test case.

Table 20. APUT negative test configuration

Parameter	APUT value	CTT acting as a test bed STA value
Test bed vendor	N/A	Intel
SSID	Wi-Fi	N/A
Operating channel	44 (if dual band APUT, else 6)	N/A
AKM Suite Type	8 (SAE)	8 (SAE)
Cipher Suite Type	4 (CCMP-128)	4 (CCMP-128)
DH group	Group 19	Group 19
Password	12345678	12345678
Scalar value	N/A	Step 4: 0000000000000000000000000000000000000000000000000000000000000000 Step 6: 0000000000000000000000000000000000000000000000000000000000000001 Step 8: ffffffff00000000ffffffffffffffffbce6faada7179e84f3b9cac2fc632551

Test procedure and expected results

Table 21 provides the test procedure and expected results for this test case.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Table 21. APUT negative test procedure and expected results

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
1	Reset the APUT to its default configuration as specified in Table 7. Configure the APUT as specified in Table 20. The APUT starts transmitting Beacon frames.	Reset the STA to its default configuration as specified in Table 4.		SN: If the Beacon frames from the APUT advertise support for SAE, then CONTINUE, else FAIL.
2		Configure the STA as specified in Table 20. Trigger the STA to associate with the APUT using an invalid COMMIT-ELEMENT in the SAE Commit message.	Verify that the STA sends an invalid COMMIT-ELEMENT in the SAE Commit message to the APUT.	
3				SN: Wait for 30 seconds. If the APUT either does not respond, or responds with an Authentication frame with Authentication Transaction Sequence number set to 1 with a non-zero status code, then CONTINUE; else FAIL.
4		Configure the STA as specified in Table 20. Trigger the STA to associate with the APUT using an invalid scalar value set to zero in the SAE Commit message.	Verify that the STA sends a scalar value set to zero in the SAE Commit message to the APUT.	
5				SN: Wait for 30 seconds. If the APUT either does not respond or responds with an Authentication frame with Authentication Transaction Sequence number set to 1 with a non-zero status code, then CONTINUE; else FAIL.
6		Configure the STA as specified in Table 20. Trigger the STA to associate with the APUT using an invalid scalar value set to one in the SAE Commit message.	Verify that the STA sends a scalar value set to one in the SAE Commit message to the APUT.	
7				SN: Wait for 30 seconds. If the APUT either does not respond or responds with an Authentication frame with Authentication Transaction Sequence number set to 1 with a non-zero status code, then CONTINUE; else FAIL.
8		Configure the STA as specified in Table 20.	Verify that the STA sends a scalar value set to q, where q is the order	

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
		Trigger the STA to associate with the APUT using an invalid scalar value set to q, where q is the order of the elliptic curve being used (group 19) in the SAE Commit message.	of the elliptic curve being used in the SAE Commit message to the APUT.	
9				SN: Wait for 30 seconds. If the APUT either does not respond or responds with an Authentication frame with Authentication Transaction Sequence number set to 1 with a non-zero status code, then PASS; else FAIL.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

4.2.7 APUT WPA2-Personal transition negative test

Objective

This test verifies that the APUT configured to operate in WPA2-Personal transition mode correctly rejects an association request with PMF set to disabled received from an SAE STA.

Applicability: Mandatory

References

Section 12.4, 12.5 [1]

Test environment

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

Test configuration

Table 22 defines the specific parameter values required for this test case.

Table 22. APUT WPA2-Personal transition negative test configuration

Parameter	APUT value	CTT acting as a test bed STA value
Test bed vendor	N/A	Marvell
SSID	Wi-Fi	N/A
Operating channel	6 or 44	N/A
AKM Suite Type	Transitional compatibility mode 2 (PSK) and 8 (SAE)	8 (SAE)
Cipher Suite Type	4 (CCMP-128)	4 (CCMP-128)
PMF	Enabled	Disabled
Password	12345678	12345678

Test procedure and expected results

Table 23 provides the test procedure and expected results for this test case.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Table 23. APUT WPA2-Personal transition negative test procedure and expected results

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
1	Reset the APUT to its default configuration as specified in Table 7.	Reset STA to its default configuration as specified in Table 4.		
2	Configure the APUT as specified in Table 22 for both SAE and PSK on a single SSID.			SN: If the Beacon frames from the APUT advertise support for both SAE and PSK as an AKM Suite type, then CONTINUE, else FAIL.
3		Configure STA as specified in Table 22. Trigger STA to perform SAE authentication with the APUT.	SN: Verify that the STA transmits an Authentication frame with Authentication Algorithm Number field set to 3 and sends Association Request frame with MFPR and MFPC bits set to 0.	SN: Verify the following behavior between the APUT and test bed TA: 1. SAE authentication completes successfully. 2. APUT sends Association Response frame with Status Code field set to non-zero value. If all conditions are true, then PASS else FAIL.

4.2.8 APUT correct handling of PMKID during initial WPA3-SAE association test

Objective

This test verifies that the APUT, after a successful SAE authentication, is able to associate with a STA that

- Includes PMKID in initial Association Request frame
- Does not include PMKID in the initial Association Request frame

Applicability: Mandatory

References

Section 12.4.5 [3]

Test environment

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

Test configuration

Table 24 defines the specific parameter values required for this test case.

Table 24. APUT correct handling of PMKID during initial WPA3-SAE association test configuration

Parameter	APUT value	CTT acting as a test bed STA value
Test bed vendor	N/A	Intel

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Parameter	APUT value	CTT acting as a test bed STA value
SSID	Wi-Fi	N/A
Operating channel	6 or 44. If dual band, use 6	N/A
AKM Suite Type	8 (SAE)	8 (SAE)
Cipher Suite Type	4 (CCMP-128) For 2.4 GHz and 5 GHz APUT	4 (CCMP-128) For 2.4 GHz and 5 GHz APUT
Password	12345678	12345678

Test procedure and expected results

Table 25 provides the test procedure and expected results for this test case.

Table 25. APUT correct handling of PMKID during initial WPA3-SAE association test procedure and expected results

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
1	Reset the APUT to its default configuration as specified in Table 7 Configure the APUT as specified in Table 24	Reset the STA to its default configuration as specified in Table 4		
2	The APUT starts transmitting Beacon frames.			SN: If the APUT includes SAE AKM (00-0F-AC:8) in the RSNE in Beacon frames, then CONTINUE, else FAIL.
3		Configure the STA as specified in Table 8. Configure the STA to include the PMKID from the established PMK in the RSNE in the Association Request frame. Trigger the STA to associate with the APUT.	SN: Verify that the STA transmits Authentication frames with Authentication Algorithm Number field set to 3. SN: Verify that the STA includes the PMKID in the RSNE in the Association Request frame.	SN: Verify the following behavior between the APUT and STA: 1. Exchanges SAE authentication frames with Authentication Transaction Sequence number set to 1. 2. Exchanges SAE authentication frames with Authentication Transaction Sequence number set to 2. 3. Association Response frame with Status Code set to 0. 4. Performs 4-way handshake. If all the above conditions are true, then CONTINUE, else FAIL.
4		Configure the STA to ping the APUT's console IP address. <ping CONSOLE_IP_ADDR>, COUNT = 3, FRAME_RATE = 1		If the ping is successful, then CONTINUE, else FAIL.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Step	APUT	CTT acting as a test bed STA	CTT validation check	Expected Result
5		Reset the STA to its default configuration as specified in Table 4.		
6		Configure the STA as specified in Table 8. Configure the STA to NOT include PMKID from the established PMK in the RSNE in the Association Request frame. Trigger the STA to associate with the APUT.	SN: Verify that the STA transmits Authentication frames with Authentication Algorithm Number field set to 3. SN: Verify that the STA does not include the PMKID in the RSNE in the Association Request frame.	SN: Verify the following behavior between the APUT and STA: 1. Exchanges SAE authentication frames with Authentication Transaction Sequence number set to 1. 2. Exchanges SAE authentication frames with Authentication Transaction Sequence number set to 2. 3. Association Response frame with Status Code set to 0. 4. Performs 4-way handshake. If all conditions are true, then CONTINUE, else FAIL.
7		Configure the STA to ping the APUT's console IP address. <ping CONSOLE_IP_ADDR>, COUNT = 3, FRAME_RATE = 1		If the ping is successful, then PASS, else FAIL.

4.3 APUT rejecting unsuitable Diffie-Hellman groups for SAE tests

Objective

This test validates that the APUT rejects DH group marked as unsuitable per Table 27 offered for SAE authentication.

Applicability: Mandatory.

References

None

Test environment

- APUT
- Wireless sniffer
- STA
- RF shielded room

Test configuration

Table 26 define the specific parameter values required for this test case.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Table 26. Test configuration

Parameter	APUT value	STA value
Test bed vendor	N/A	Qualcomm, Intel
SSID	TestSAE	N/A
Operating channel	6 for 2.4 GHz only APUT and 36 for 5 GHz only APUT Dual band APUT choose 6 or 36	N/A
AKM Suite Type	8 (SAE)	8 (SAE)
Cipher Suite Type	4 (CCMP-128)	4 (CCMP-128)

Table 27. DH group list and suitability for SAE

Group Number	Description	Suitability
1	768-bit MODP group	Unsuitable
2	1024-bit MODP group	Unsuitable
3	EC2N group on GP[2^155]	Unsuitable
4	EC2N group on GP[2^185]	Unsuitable
5	1536-bit MODP group	Unsuitable
6	Random EC2N group over GF[2^163]	Unsuitable
7	Koblitz EC2N group over GF[2^163]	Unsuitable
8	Random EC2N group over GF[2^163]	Unsuitable
9	Koblitz EC2N group over GF[2^163]	Unsuitable
10	Random EC2N group over GF[2^163]	Unsuitable
11	Koblitz EC2N group over GF[2^163]	Unsuitable
12	Random EC2N group over GF[2^163]	Unsuitable
13	Koblitz EC2N group over GF[2^163]	Unsuitable
14	2048-bit MODP group	Unsuitable
15	3072-bit MODP group	Suitable
16	4096-bit MODP group	Suitable
17	6144-bit MODP group	Suitable
18	8192-bit MODP group	Suitable
19	256-bit random ECP group (NIST)	Suitable (Mandatory)
20	384-bit random ECP group (NIST)	Suitable
21	521-bit random ECP group (NIST)	Suitable

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

22	1024-bit MODP group (160-bit order)	Unsuitable
23	2048-bit MODP group (224-bit order)	Unsuitable
24	2048-bit MODP group (256-bit order)	Unsuitable
25	192-bit Random ECP group	Unsuitable
26	224-bit Random ECP group (NIST)	Unsuitable
27	224-bit Random ECP group (Brainpool)	Unsuitable
28	256-bit Random ECP group (Brainpool)	Unsuitable
29	384-bit Random ECP group (Brainpool)	Unsuitable
30	512-bit Random ECP group (Brainpool)	Unsuitable

Test procedure and expected results

Table 28 provides the test procedure and expected results for this test case.

Table 28. Test procedure and expected results

Step	APUT	STA	Expected Result
1	Configure the APUT with the parameters listed in Table 26.	Configure the STA with the parameters listed in Table 26.	
2	The APUT starts to transmit Beacon frames.	Trigger the STA to initiate SAE authentication with the APUT using DH groups specified in Table 27. One group at a time marked as unsuitable is chosen and the STA is configured to offer this group during the SAE Commit message to the APUT.	.
3		The STA transmits an SAE Commit message offering an unsuitable DH group to the AP.	SN: If the APUT rejects the offered group by transmitting Commit message with Status Code set to "UNSUPPORTED_FINITE_CYCLIC_GROUP" (0x004d), then CONTINUE else FAIL.
4	The STA is configured to repeat Step 3 until no other groups marked as “Unsuitable” are left to choose from Table 27.		SN: If all the groups marked as "Unsuitable" have been offered by the STA and the APUT has rejected all of them, then PASS else FAIL.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

5 WPA3-SAE STAUT tests

5.1 STAUT configuration requirements validation test

Objective

This test verifies that the STAUT is configurable with the parameters required for the test cases in section 5. In addition to basic wireless configuration (SSID, operational mode, channel) there is a password/phrase/code/key that shall be configured and optionally additional finite cyclic groups may be configured. The configuration parameters are defined in section 3.3. Note that this test case is not automated by a Wi-Fi Test Suite script. The technician shall manually configure the required parameters through the user interface.

Applicability: Mandatory

References

N/A

Test environment

- STAUT

Test configuration

Table 29 defines the specific parameter values required for this test case.

Table 29. STAUT configuration requirements validation test configuration

Parameter	DUT value	Test bed device 1 value	Test bed device 2 value
SAE configuration	Enable/disable	Enabled	Disabled

Test procedure and expected results

Table 30 provides the specific test procedure and expected results for this test case.

Table 30. STAUT configuration requirements validation test procedure and expected results

Step	STAUT	Expected result
1	Configure the SSID and password/phrase/code/key for SAE	If the STAUT UI is capable of being provisioned with the input, then CONTINUE else FAIL.
2	Configure SAE in transitional mode with WPA2-Personal using CCMP with a passphrase > 63 characters	If the STAUT UI is unable to be provisioned with the passphrase then CONTINUE, else FAIL.
3	If the STAUT supports multiple finite cyclic groups and provides an end user interface for configuration of these groups, configure each supported group (one at a time) on the STAUT.	If the STAUT allows configuration of any unsuitable DH group (as per Table 27) using the end user interface, then FAIL, else PASS.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

5.2 STAUT WPA3-SAEtests

5.2.1 STAUT SAE connectivity and PMK caching test

Objective

This test verifies that the STAUT can successfully complete the SAE protocol with the test bed AP.

Applicability: Mandatory

References

Sections 12.4.5, 12.6.10.3 [1]

Test environment

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

Test configuration

Table 31 defines the specific parameter values required for this test case.

Table 31. STAUT SAE connectivity and PMK caching test configuration

Parameter	STAUT value	CTT acting as a test bed AP value
Test bed vendor	N/A	Qualcomm
SSID	N/A	Wi-Fi
Operating channel	N/A	6 or 44 (dual band use 6)
AKM Suite Type	8 (SAE)	8 (SAE)
Cipher Suite Type	4 (CCMP-128)	4 (CCMP-128)
Password	0123456789abcdef0123456789abcdef	0123456789abcdef0123456789abcdef

Test procedure and expected results

Table 32 provides the test procedure and expected results for this test case.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Table 32. STAUT SAE connectivity and PMK caching 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 8. Configure the STAUT as specified in Table 31.	Reset the AP to its default configuration as specified in Table 3. Configure the AP as specified in Table 31.		
2	Trigger the STAUT to associate with the AP.	The AP starts transmitting Beacon frames.	Verify that captured Beacon frame contains an RSNE with the following: 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 01 00 4. Pairwise Cipher Suite List is set to CCMP 00-0F-AC:4 5. AKM Suite Count is set to 01 00 6. AKM Suite List is set to 00-0F-AC:8 7. PMKID Count is set to 0 or is not present 8. PMKID List is not present 9. MFPR bit (bit 6) in RSN Capabilities field is set to 1	SN: Verify the following conditions are true: 1. STAUT initiates SAE authentication with the AP by transmitting an SAE Commit message. 2. STAUT successfully completes SAE authentication with the AP. 3. STAUT sets MFPR bit (bit 6) of the RSN Capabilities field in the Association Request frame to 1. 4. STAUT performs 4-way handshake with the AP. If all the conditions are true, then CONTINUE else FAIL.
3	Configure the STAUT to ping the AP's console IP address. <ping CONSOLE_IP_ADDR>, COUNT = 3, FRAME_RATE = 1			If the ping is successful, then CONTINUE, else FAIL.
4	If the STAUT supports PMKSA caching when the disconnect is triggered on the STAUT (see item 6 in Table 1), then trigger the STAUT to disconnect from the AP.	If the STAUT cannot support PMKSA caching when the disconnect is triggered on the STAUT, trigger the AP to deauthenticate the STAUT.		
5	Trigger the STAUT to re-associate with the AP.		SN: Verify that the PMKID in EAPOL message 1 from the AP matches the PMKID in the (Re)Association Request frame from the STAUT.	SN: Verify the following conditions are true: 1. The STAUT transmits an Authentication frame with the Authentication Algorithm Number field set to 0 2. The (Re)Association Request frame sent from the STAUT to the AP includes PMKID If all the conditions are true, then CONTINUE else FAIL.
6	Configure the STAUT to ping the AP's console IP address. <ping CONSOLE_IP_ADDR>, COUNT = 3, FRAME_RATE = 1			If the ping is successful then PASS, else FAIL.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

5.2.2 STAUT Anti-clogging test

Objective

This test verifies that the STAUT is able to connect to an AP that has exceeded its AntiCloggingThreshold value.

Applicability: Mandatory

References

Section 12.4.6 [1]

Test environment

- STAUT
- CTT acting as a test bed AP
- Wireless Sniffer
- Packet injector acting as a clogging device

Test configuration

Table 33 defines the specific parameter values required for this test case.

Table 33. STAUT Anti-clogging test configuration

Parameter	STAUT value	CTT acting as a test bed AP value	Packet injector
Test bed vendor	N/A	Qualcomm	N/A
SSID	N/A	Wi-Fi	N/A
Operating channel	N/A	44 (if dual band APUT, else 6)	Same as AP
AKM Suite Type	8 (SAE)	8 (SAE)	N/A
Cipher Suite Type	4 (CCMP-128)	4 (CCMP-128)	N/A
Password	12345678	12345678	N/A

Test procedure and expected results

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

Table 34. STAUT Anti-clogging test procedure and expected results

Step	STAUT	CTT acting as a test bed AP	Packet injector	CTT validation check	Expected Result
1	Reset the STAUT to its default configuration as specified in Table 8.	Reset the AP to its default configuration as specified in Table 3.		SN: Verify that the AP sends a Beacon frame that advertises	

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Step	STAUT	CTT acting as a test bed AP	Packet injector	CTT validation check	Expected Result
	Configure the STAUT as specified in Table 33.	Configure the AP as specified in Table 33. The AP starts transmitting Beacon frames.		AKM Suite Type as 8 in the RSNE.	
2		The AP accepts connections until its Anti-Clogging threshold has been reached and then issues Authentication frames with the Authentication Transaction Sequence number set to 1 and also contains the Anti-Clogging Token.	Trigger the packet injector to transmit SAE Commit messages from different MAC addresses.	SN: Verify that the AP transmits an Authentication frame with the following: 1. Authentication Algorithm Number = 3. 2. Authentication Transaction Sequence number = 1. 3. Status Code = 76 (Anti-Clogging Token Requested). 4. Anti-Clogging Token present.	
3	Trigger the STAUT to associate with the AP.				SN: Verify that the STAUT: 1. Initially issues an Authentication frame with Authentication Transaction Sequence number set to 1 with no Anti-Clogging Tokens. 2. Receives an Authentication frame from the AP with Authentication Transaction Sequence number set to 1 that contains an Anti-Clogging Token. 3. Transmits an Authentication frame with Authentication Transaction Sequence number set to 1 with the Anti-Clogging Token received in the aforementioned Authentication frame from the AP. 4. Completes the SAE protocol with the AP. If all conditions are true then CONTINUE, else FAIL
4	Configure the STAUT to ping the AP's console IP address. <ping CONSOLE_IP_ADDR>, COUNT = 3, FRAME_RATE = 1				If the ping is successful then PASS, else FAIL.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

5.2.3 STAUT reflection attack test

Objective

This test verifies that the STAUT properly handles a reflection attack.

Applicability: Mandatory

References

Section 12.4.8.6.4 [1]

Test environment

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

Test configuration

Table 35 defines the specific parameter values required for this test case.

Table 35. STAUT reflection attack test configuration

Parameter	STAUT value	CTT acting as a test bed AP value
Test bed vendor	N/A	Qualcomm
SSID	N/A	Wi-Fi
Operating channel	N/A	44 (if dual band APUT, else 6)
AKM Suite Type	8 (SAE)	8 (SAE)
Cipher Suite Type	4 (CCMP-128)	4 (CCMP-128)
Password	12345678	12345678
Reflection attack	N/A	Enabled

Test procedure and expected results

Table 36 provides the test procedure and expected results for this test case.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Table 36. STAUT reflection attack 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 8. Configure the STAUT as specified in Table 35.	Reset the AP to its default configuration as specified in Table 3. Configure AP as specified in Table 35. The AP starts transmitting Beacon frames.		
2	Trigger the STAUT to associate with the AP.		Verify that the AP sends SAE Commit message with Authentication Transaction Sequence number set to 1 and with scalar and element values set identical to the values sent by STAUT in the SAE Commit message to the AP.	SN: Verify that the STAUT: 1. Issues an Authentication frame to the AP with Authentication Transaction Sequence number set to 1. 2. Does not transmit an Authentication frame with Authentication Transaction Sequence number set to 2. If all conditions are true, then PASS, else FAIL

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

5.2.4 STAUT WPA2-Personal compatibility test

Objective

This test verifies that the STAUT is able to connect to an AP with SAE and WPA2-Personal.

Applicability: Mandatory

References

Sections 12.4, 12.5 [1]

Test environment

- STAUT
- CTT acting as a test bed AP1
- CTT acting as a test bed AP2
- Wireless Sniffer

Test configuration

Table 37 defines the specific parameter values required for this test case.

Table 37. STAUT WPA2-Personal compatibility test configuration

Parameter	STAUT value	CTT acting as a test bed AP1 value	CTT acting as a test bed AP2 value
Test bed vendor	N/A	Qualcomm	Marvell
SSID	N/A	Wi-Fi	Wi-Fi
Operating channel	N/A	44 (if dual band APUT, else 6)	44 (if dual band APUT, else 6)
AKM Suite Type	8 (SAE) and 2(PSK)	Transitional compatibility mode 8 (SAE) and 2 (PSK)	2 (PSK)
Cipher Suite Type	4 (CCMP-128)	4 (CCMP-128)	4 (CCMP-128)
PMF	Enabled	Enabled	Enabled
Password	12345678123456781234567812345678	12345678123456781234567812345678	12345678123456781234567812345678

Test procedure and expected results

Table 38 provides the test procedure and expected results for this test case.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Table 38. STAUT WPA2-Personal compatibility test procedure and expected results

Step	STAUT	CTT acting as a test bed AP1	CTT acting as a test bed AP2	CTT validation check	Expected Result
1	Reset the STAUT to its default configuration as specified in Table 8. Configure the STAUT as specified in Table 37.	Reset the AP1 to its default configuration as specified in Table 3. Configure AP1 as specified in Table 37. AP1 starts transmitting Beacon frames.			SN: If AP1 sends a Beacon frame with support for SAE and WPA2-Personal, then CONTINUE, else FAIL.
2	Trigger the STAUT to associate with AP1. The STAUT pings AP1's IP address. <ping AP1_IP_ADDR>, COUNT = 3, FRAME_RATE = 1				SN: Verify that the STAUT: 1. Initiates SAE to AP1. 2. Successfully completes SAE with AP1. 3. Performs 4-way handshake with AP1. 4. Ping is successful. If all the conditions are true, then CONTINUE; else FAIL
3			Reset AP2 to its default configuration as specified in Table 3. Configure AP2 as specified in Table 37. AP2 starts transmitting Beacon frames.		
4		Turn off AP1.			SN: Verify that the STAUT: 1. Performs 4-way handshake with AP2. If all the conditions are true, then CONTINUE, else FAIL.
5	Configure the STAUT to ping AP2's console IP address. <ping CONSOLE_IP_ADDR>, COUNT = 3, FRAME_RATE = 1				If the ping is successful, then PASS, else FAIL.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

5.2.5 STAUT support for additional finite cyclic groups test

Objective

This test verifies that the STAUT supports additional finite cyclic groups.

This test shall be repeated for all finite cyclic groups supported by the STAUT.

Applicability: Conditionally mandatory. This test case is required if the STAUT declared support for (EC)DH finite cyclic groups in Table 1.

References

Section 12.4.4 [1]

Test environment

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

Test configuration

Table 39 defines the specific parameter values required for this test case.

Table 39. STAUT support for additional finite cyclic groups test configuration

Parameter	STAUT value	CTT acting as a test bed AP value
Test bed vendor	N/A	Qualcomm
SSID	N/A	Wi-Fi
Operating channel	N/A	44 (if dual band APUT, else 6)
AKM Suite Type	8 (SAE)	8 (SAE)
Cipher Suite Type	4 (CCMP-128)	4 (CCMP-128)
Password	12345678	12345678
(EC)DH finite cyclic group	All supported	As supported by STAUT

Test procedure and expected results

Table 40 provides the test procedure and expected results for this test case.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Table 40. STAUT support for additional finite cyclic groups 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 8. Configure the STAUT as specified in Table 39 with a supported (EC)DH finite cyclic group other than 19.	Reset the AP to its default configuration as specified in Table 3. Configure the AP as specified in Table 39 and allow all (EC)DH finite cyclic groups claimed to be supported by the STAUT. The AP starts transmitting Beacon frames.		
2	Trigger the STAUT to associate with the AP.			SN: Verify that the STAUT: 1. Performs SAE using (EC)DH finite cyclic group provisioned to AP. 2. Performs 4-way handshake with the AP. If all conditions are true, then CONTINUE; else FAIL.
3	Configure the STAUT to ping the AP's console IP address. <ping CONSOLE_IP_ADDR>, COUNT = 3, FRAME_RATE = 1			If the ping is successful, then CONTINUE, else FAIL.
4	Repeat steps 2 and 3 for all other (EC)DH finite cyclic groups supported by STAUT.			If all supported (EC)DH finite cyclic groups pass, then PASS, else FAIL.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

5.2.6 STAUT negative test

Objective

This test verifies that the STAUT correctly rejects improper elements and finite cyclic group values received from the test bed AP.

Applicability: Mandatory

References

Section 12.4 [1]

Test environment

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

Test configuration

Table 41 defines the specific parameter values required for this test case.

Table 41. STAUT negative test configuration

Parameter	STAUT value	CTT acting as a test bed AP value
Test bed vendor	N/A	Qualcomm
SSID	N/A	Wi-Fi
Operating channel	N/A	44 (if dual band APUT, else 6)
AKM Suite Type	8 (SAE)	8 (SAE)
Cipher Suite Type	4 (CCMP-128)	4 (CCMP-128)
DH group	Group 19	Group 19
Password	12345678	12345678
Scalar value	N/A	Step 5: 0000000000000000000000000000000000000000000000000000000000000000 Step 7: 0000000000000000000000000000000000000000000000000000000000000001 Step 9: ffffffff00000000ffffffffffffffffbce6faada7179e84f3b9cac2fc632551

Test procedure and expected results

Table 42 provides the test procedure and expected results for this test case.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Table 42. STAUT negative 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 8. Configure the STAUT as specified in Table 41.	Reset the AP to its default configuration as specified in Table 3. Configure the AP as specified in Table 41 and with an invalid COMMIT-ELEMENT in the SAE Commit message. The AP starts transmitting Beacon frames.		
2	Trigger the STAUT to associate with the AP.			SN: Wait for 30 seconds. Verify that the STAUT: 1. Initiates an SAE authentication exchange with the AP. 2. Does not respond with an Authentication frame with Authentication Transaction Sequence number set to 2. If all conditions are met, then CONTINUE else FAIL.
3	Reset the STAUT to its default configuration as specified in Table 8. Configure the STAUT as specified in Table 41.	Reset the AP to its default configuration as specified in Table 3. Configure the AP as specified in Table 41 and to an EC(DH) finite cyclic group which the STAUT does not support during the SAE authentication exchange. The AP starts transmitting Beacon frames.		
4	Trigger the STAUT to associate with the AP.			SN: Wait for 30 seconds. Verify that the STAUT: 1. Initiates an SAE authentication exchange with the AP. 2. Does not respond with an Authentication frame with Authentication Transaction Sequence number set to 2. If all conditions are true, then CONTINUE; else FAIL.
5	Reset the STAUT to its default configuration as specified in Table 8. Configure the STAUT as specified in Table 41.	Reset the AP to its default configuration as specified in Table 3. Configure the AP as specified in Table 41 and with an invalid all zero scalar value in the SAE Commit message. The AP starts transmitting Beacon frames.		
6	Trigger the STAUT to associate with the AP.			SN: Wait for 30 seconds. Verify that the STAUT: 1. Initiates an SAE authentication exchange with the AP.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Step	STAUT	CTT acting as a test bed AP	CTT validation check	Expected Result
				2. Does not respond with an Authentication frame with Authentication Transaction Sequence number set to 2. If all conditions are met, then CONTINUE else FAIL.
7	Reset the STAUT to its default configuration as specified in Table 8. Configure the STAUT as specified in Table 41.	Reset the AP to its default configuration as specified in Table 3. Configure the AP as specified in Table 41 and with an invalid scalar value set to one in the SAE Commit message. The AP starts transmitting Beacon frames.		
8	Trigger the STAUT to associate with the AP.			SN: Wait for 30 seconds. Verify that the STAUT: 1. Initiates an SAE authentication exchange with the AP. 2. Does not respond with an Authentication frame with Authentication Transaction Sequence number set to 2. If all conditions are met, then CONTINUE else FAIL.
9	Reset the STAUT to its default configuration as specified in Table 8. Configure the STAUT as specified in Table 41.	Reset the AP to its default configuration as specified in Table 3. Configure the AP as specified in Table 41 and with an invalid scalar value set to q, where q is the order of the elliptic curve being used (group 19) in the SAE Commit message. The AP starts transmitting Beacon frames.		
10	Trigger the STAUT to associate with the AP.			SN: Wait for 30 seconds. Verify that the STAUT: 1. Initiates an SAE authentication exchange with the AP. 2. Does not respond with an Authentication frame with Authentication Transaction Sequence number set to 2. If all conditions are met, then PASS else FAIL.

5.2.7 STAUT SAE confirmation exchange variation test

Objective

This test verifies that the STAUT can successfully complete the SAE protocol with the test bed AP. This testbed AP initiates the SAE confirmation exchange by transmitting an SAE Confirm message immediately after sending its SAE Commit message to the STAUT during the SAE authentication exchange.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Applicability: Mandatory

References

Section 12.4 [3]

Test environment

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

Test configuration

Table 43 defines the specific parameter values required for this test case.

Table 43. SAE confirmation exchange variation configuration

Parameter	STAUT value	CTT acting as a test bed AP value
Test bed vendor	N/A	Marvell
SSID	N/A	Wi-Fi
Operating channel	N/A	6 or 44. If dual band, use 6
AKM Suite Type	8 (SAE)	8 (SAE)
Cipher Suite Type	4 (CCMP-128)	4 (CCMP-128)
Password	12345678	12345678

Test procedure and expected results

Table 44 provides the test procedure and expected results for this test case.

Table 44. SAE confirmation exchange variation 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 8. Configure the STAUT as specified in Table 43	Reset the AP to its default configuration as specified in Table 3 Configure the AP as specified in Table 43. Configure the AP to initiate SAE confirmation exchange by transmitting an SAE Confirm message immediately after sending its SAE Commit message to the STAUT.		

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Step	STAUT	CTT acting as a test bed AP	CTT validation check	Expected Result
2		The AP starts transmitting Beacon frames.	Verify that captured Beacon frame contains an RSNE with the following: 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 01 00 4. Pairwise Cipher Suite List is set to CCMP 00-0F-AC:4 5. AKM Suite Count is set to 01 00 6. AKM Suite List is set to 00-0F-AC:8 7. PMKID Count is set to 0 or is not present 8. PMKID List is not present 9. MFPR bit (bit 6) and MFPC bit (bit 7) in RSN Capabilities field is set to 1	
3	Trigger the STAUT to associate with the AP.			SN: If the STAUT initiates SAE authentication with the AP by transmitting an SAE Commit message, then CONTINUE else FAIL.
4	STAUT and AP successfully completes SAE commitment exchange.			
5		AP transmits SAE Confirm message to the STAUT with authentication transaction sequence number 2.	Verify that the AP transmits SAE Confirm message immediately after sending its SAE Commit message to the STAUT.	
6	STAUT transmits SAE Confirm message to the AP.			SN: If the STAUT successfully completes SAE authentication with the AP, then CONTINUE else FAIL.
7	STAUT and AP completes association and 4-way handshake.			SN: If the STAUT successfully completes 4-way handshake with the AP, then CONTINUE else FAIL.
8	Configure the STAUT to ping the AP's console IP address. <ping CONSOLE_IP_ADDR>, COUNT = 3, FRAME_RATE = 1			If the ping is successful, then PASS, else FAIL.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

5.3 STAUT does not request unsuitable Diffie-Hellman groups for SAE tests

Objective

This test validates that the STAUT initiating SAE authentication never requests for a DH group marked as unsuitable per Table 27 in the commit message.

Applicability: Mandatory.

References

None

Test environment

- STAUT
- Wireless sniffer
- AP
- RF shielded room

Test configuration

Table 45 define the specific parameter values required for this test case.

Table 45. Test configuration

Parameter	STAUT value	AP value
Test bed vendor	N/A	Qualcomm
SSID	N/A	testSAE
Operating channel	N/A	6 for 2.4 GHz only STAUT and 36 for 5 GHz only STAUT Dual band STAUT choose 6 or 36
AKM Suite Type	8 (SAE)	8 (SAE)
Cipher Suite Type	4 (CCMP-128)	4 (CCMP-128)

Test procedure and expected results

Table 46 provides the test procedure and expected results for this test case.

Table 46. Test procedure and expected results

Step	STAUT	AP	Expected Result
1	Configure the STAUT with the parameters listed in Table 45.	Configure the AP with the parameters listed in Table 45.	

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Step	STAUT	AP	Expected Result
		Configure the AP to reject any DH group including the mandatory Group 19.	
2	Trigger the STAUT to associate to the AP.	The AP starts to transmit Beacon frames.	
3	The STAUT transmits an SAE Commit message offering one of the supported DH Group to the AP.	The AP rejects the offered group by transmitting Commit message with Status Code set to "UNSUPPORTED_FINITE_CYCLIC_GROUP" (0x004d).	SN: If the STAUT offers an unsuitable group in SAE Commit message per Table 27, then FAIL else CONTINUE.
4	The STAUT chooses another supported group and repeats Step 3 until there are no other groups to choose. Note: The STAUT can offer a suitable DH group multiple times even when the AP is rejecting it.		SN: If no new group is used OR if a previously attempted group is used in the SAE Commit message, then PASS else FAIL.

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

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 47, Table 48 and Table 49 provide the approved test bed equipment for the DUTs listed in this test plan.

Table 47. Approved test bed access points

Vendor	Product	Software version(s)	Contact
Marvell	RD-88W-AP-8964-WIFI-R0	version, 9.1.2.8-wpa3.p6-W8964 firmware,9.3.2.5	Wifilab.support@nxp.com
Qualcomm	CA-65-YC633-1000-WPA3	IPQ8074.ILQ.10.1.6-00012-P-1	wfa.security.support@qti.qualcomm.com

Table 48. Approved test bed stations

Vendor	Product	Software version(s)	Contact
Intel	AX200 NGWG NV	5.3/ build:2707;commit:62afe85;date:2019-12-04T09:06:52-08:00 ax200	wfa.external.support@intel.com
Marvell	RD-88W-8997P-WIFI-S0	PCIE8997-16.68.1.p195-C4X16C623-GPL-(FP68)/ Mrvl-WFASigma_ver_Security_R0.1(14:44:30 Apr 5 2018)	Wifilab.support@nxp.com
Qualcomm	QC-DB-L00003_1	WFA-FR2019-2.0 eng.git.20191017.163144 8.1.0r00008.2a_LA.UM.6.4.r1-06900-8x98.0 drv=/hapd=v2.10-devel-8.1.0/sigma=framework-(OpenQ-835_Android_O_WFA-FR2019-2.0-ITC-JFlash.zip)	wfa.security.support@qti.qualcomm.com

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Table 49. Approved test tools

Vendor	Product	Software version(s)	Contact
Qualcomm	Sniffer/ CA-65-Y9345-LCT (OpenWrt Chaos Calmer 15.05.1)	UnKnown_4.12.0-rc6+	support@wi-fi.org
Intel	Packet Injector/ 8260.NGWMG.NVL	Ubuntu 16.04, , Kernel: 4.8.0.36-generic	support@wi-fi.org

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.

Appendix B (Informative) Document revision history

Table 50. Document revision history

Version	Date YYYY-MM-DD	Remarks
1.0	2018-04-09	Initial release.
1.1	2019-04-10	Added test cases 4.3 and 5.3 to validate that APUT and STAUT do not offer/accept unsuitable DH groups for SAE authentication. Additional steps for configuration requirements validation tests (4.1 and 5.1) to validate that APUT and STAUT do not allow configuration of unsuitable groups through end user UI. Additional steps for negative tests (4.2.6 and 5.2.6) to validate that APUT and STAUT aborts SAE authentication when invalid scalar value is received from the peer in the SAE Commit message.
1.2	2019-04-23	Removed various PMF setting rows from non-transitional mode cases as default setting for both APUT, STAUT and testbed (AP and STA) is PMF=Required Added PSK to STAUT AKM in test 5.2.4 Removed PSK from testbed AP AKM in test case 5.2.5 Rephrased configuration table in 4.3 and 5.3 to be consistent with rest of the cases Changed password for test case 4.2.2 and 5.2.1 for CAPI acceptable password
1.3	2019-08-01	Updated table 25 DH group list and suitability for SAE, to identify Groups 28, 29, and 30 as unsuitable.
1.4	2020-02-14	Added test cases 4.2.8 for PMK ID and 5.2.7 for SAE authentication variation Updated test case 5.2.1 step 4 for PMKSA caching

WI-FI ALLIANCE CONFIDENTIAL TRADE SECRET. FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE MEMBERS – DO NOT COPY

© 2020 Wi-Fi Alliance. All Rights Reserved.