**CONFIDENTIAL TRADE SECRET**

**FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE® MEMBERS**

**– DO NOT COPY –**

# Wi-Fi CERTIFIED WPA3™

# Test Plan

## Version 2.1

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/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

© 2020 Wi-Fi Alliance. All Rights Reserved.

## List of tables

## List of figures

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 WPA3™ products from multiple manufacturers, and to promote this technology within both the business and consumer markets. To this end, the following test plan has been developed. Working in conjunction with authorized test labs, these tests are executed on vendor products to grant products Wi-Fi CERTIFIED WPA3 certification upon successful test completion.

The scope of this test plan is governed by the Wi-Fi Alliance Security Marketing Requirements Documents [2] and [10].

## 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 features 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 |
|---|---|---|---|
| | Questions for APUT | | |
| Q1 | Does the APUT support over-the-air FT on WPA3-Personal only mode? | FT-8.1.1; FT-8.2.1 | Yes/No |
| Q2 | Does the APUT support over-the-air FT on WPA3-Personal transition mode? | FT-8.1.7, FT-8.1.8, FT-8.1.9; FT-8.2.7, FT-8.2.8, FT-8.2.9 | Yes/No |
| Q3 | Does the APUT support over-the-air FT on WPA3-Enterprise only mode? | FT-8.1.4; FT-8.2.4 | Yes/No |
| Q4 | Does the APUT support over-the-air FT on WPA3-Enterprise transition mode? | FT-8.1.5, FT-8.1.6; FT-8.2.5, FT-8.2.6 | Yes/No |
| Q5 | Does the APUT support over-the-DS FT on WPA3-Personal only mode? | FT-8.1.1_DS; FT-8.2.1_DS | Yes/No |
| Q6 | Does the APUT support over-the-DS FT on WPA3-Enterprise only mode? | FT-8.1.4_DS; FT-8.2.4_DS | Yes/No |
| | Questions for STAUT | | |
| Q1 | Does the STAUT support over-the-air FT on WPA3-Personal only mode? | FT-9.1.1 | Yes/No |
| Q2 | Does the STAUT support over-the-air FT on WPA3-Personal transition mode? | FT-9.1.7, FT-9.1.8, FT-9.1.9, FT-9.1.10 | Yes/No |
| Q3 | Does the STAUT support over-the-air FT on WPA3-Enterprise only mode? | FT-9.1.4 | Yes/No |
| Q4 | Does the STAUT support over-the-air FT on WPA3-Enterprise transition mode? | FT-9.1.5, FT-9.1.6 | Yes/No |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| Item | Question | Test case | Vendor response |
|---|---|---|---|
| Q5 | Does the STAUT support over-the-DS FT on WPA3-Personal only mode? | FT-9.1.1_DS | Yes/No |
| Q6 | Does the STAUT support over-the-DS FT on WPA3-Enterprise only mode? | FT-9.1.4_DS | Yes/No |
| Q7 | Which of the following EAP methods does the STAUT support (list all): EAP-TLS, EAP-TTLS, PEAPv0, PEAPv1 | | |
| Q8 | Does the STAUT support EAP credential configuration: (a) explicitly-configured server certificate? | SCV-11.1_eap_UOSC_Choice,<br>SCV-11.6_eap_UOSC_Choice,<br>SCV-11.10_eap_UOSC_Choice,<br>SCV-11.11_eap_UOSC_Choice | 1. With UOSC=enabled only<br>2. With UOSC=disabled only<br>3. With both UOSC=enabled and UOSC=disabled<br>4. Not Supported |
| Q9 | Does the STAUT support EAP credential configuration: (b) server domain (FQDN) + root CA? | SCV-11.1.2_eap_UOSC_Choice<br>SCV-11.1.7_eap_UOSC_Choice,<br>SCV-11.1.9_eap_UOSC_Choice<br>SCV-11.1.14_eap_UOSC_Choice | 5. With UOSC=enabled only<br>6. With UOSC=disabled only<br>7. With both UOSC=enabled and UOSC=disabled<br>8. Not Supported |
| Q10 | Does the STAUT support EAP credential configuration: (c) server domain suffix + root CA? | SCV-11.1.3_eap_UOSC_Choice,<br>SCV-11.1.8_eap_UOSC_Choice | 9. With UOSC=enabled only<br>10. With UOSC=disabled only<br>11. With both UOSC=enabled and UOSC=disabled<br>12. Not Supported |
| Q11 | Does the STAUT support EAP credential configuration: (d) root CA only? | SCV-11.1.4_eap_UOSC_Choice,<br>SCV-11.1.13_eap_UOSC_Choice,<br>SCV-11.1.15_eap_UOSC_Choice | 13. With UOSC=enabled only<br>14. With UOSC=disabled only<br>15. With both UOSC=enabled and UOSC=disabled<br>16. Not Supported |
| Q12 | Does the STAUT support EAP credential configuration: (e) server domain (FQDN) + root store? | SCV-11.1.16_eap_UOSC_Choice,<br>SCV-11.1.18_eap_UOSC_Choice,<br>SCV-11.1.19_eap_UOSC_Choice | 17. With UOSC=enabled only<br>18. With UOSC=disabled only<br>19. With both UOSC=enabled and UOSC=disabled<br>20. Not Supported |
| Q13 | Does the STAUT support EAP credential configuration: (f) server domain suffix + root store? | SCV-11.1.17_eap_UOSC_Choice | 21. With UOSC=enabled only<br>22. With UOSC=disabled only<br>23. With both UOSC=enabled and UOSC=disabled<br>24. Not Supported |
| Q14 | Does the STAUT supports configuration of a network profile through its UI: run 1: Unconfigured (do not explicitly disable server validation)? | SCV-11.2.1_eap | Yes/No |
| Q15 | Does the STAUT supports configuration of a network profile through its UI, run 2: Explicitly disable server validation (select "Don't validate" or similar)? | SCV-11.2.2_eap | Yes/No |
| Q16 | Does the STAUT supports configuration of a network profile through its UI, run 3: Configure use of system trust store only (do not explicitly disable server validation)? | SCV-11.2.3_eap | Yes/No |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| Item | Question | Test case | Vendor response |
|---|---|---|---|
| Notes:<br>• The STAUT needs to pass all applicable tests in EAP method(s) supported<br>• eap can take the value of one or more of (TLS, TTLS, PEAP0, PEAP1) per declared support in Q7<br>• UOSC_Choice can be one of: UOSC-A (UOSC enabled), UOSC-DA (UOSC disabled).<br>• Vendor should only select one response from Q7 through Q15 in vendor response column<br>• For STAUT that supports both UOSC-A and UOSC-DA, only applicable UOSC-A tests need to be run<br>• Vendor response on UOSC is applicable to all test cases in respective test case column, e.g., in Q11, if a vendor choice is With UOSC=enabled only, then SCV-11.1.16_eap_UOSC-A,SCV-11.1.18_eap_UOSC-A,SCV-11.1.19_eap_UOSC-A are tested with all supported EAP methods as indicated in Q7 | | | |

## 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] IEEE Draft 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, REVmd/D3.0, Oct 2019

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

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

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

[5] WPA3-Enterprise 192-bit Security Test Plan, https://www.wi-fi.org/members/certification-programs

[6] WPA2 Security Improvements Test Plan, https://www.wi-fi.org/members/certification-programs

[7] Key Reinstallation Vulnerability Detection Test Plan, https://www.wi-fi.org/members/certification-programs

[8] IEEE 802.1X-2010 - IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control, https://ieeexplore.ieee.org/document/5409813

[9] IETF RFC 5216, The EAP-TLS Authentication Protocol, https://tools.ietf.org/html/rfc5216

[10] Security R2 Marketing Requirements Document, 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 |
|---|---|
| AAA | Authentication, authorization, and accounting |
| AKM | Authentication and key management |
| ANonce | Authenticator nonce |
| AP | Access point |
| API | Application programming interface |
| APUT | AP under test |
| BSSID | Basic service set identifier |
| CA | Control agent |
| CCMP | CTR with CBC-MAC Protocol |
| CN | Common Name |
| CTT | Compliance test tool |
| DH | Diffie–Hellman |
| DS | Distribution system |
| DUT | Device Under Test |
| EAP | Extensible Authentication Protocol |
| EAPOL | Extensible Authentication Protocol over LANs (IEEE Std 802.1X-2010) |
| ECDH | Elliptic curve Diffie–Hellman |
| FQDN | Fully qualified domain name |
| FT | Fast BSS Transition |
| FTE | Fast BSS Transition element |
| MDE | Mobility Domain element |
| MFPC | Management frame protection capable |

| Acronyms | Definition |
|---|---|
| MFPR | Management frame protection required |
| MIC | message integrity check |
| PHY | Physical layer |
| PMF | Protected Management Frames |
| PMK | Pairwise master key |
| PMKID | Pairwise master key identifier |
| R0KH | PMK-R0 key holder |
| R1KH | PMK-R1 key holder |
| RSN | Robust security network |
| RSNE | Robust Security Network element |
| SAE | Simultaneous Authentication of Equals |
| SNonce | Supplicant nonce |
| SSID | Service set identifier |
| STA | Station |
| TOD | Trust Override Disable |
| TOFU | Trust-On-First-Use |
| UOSC | User Override of Server Certificate |
| WPA3™ | Wi-Fi Protected Access® 3 |

### 1.4.2 Definitions

There are no special definitions for this test plan.

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

For WPA3-Personal only and WPA3-Enterprise 192-bit Security tests, refer to the corresponding test plans listed in section 1.2 for the tools, methodology, and approach for testing and certifying devices for WPA3 certification.

## 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 MAC/PHY per certification need
- Ability to parse frames per test case requirements in this test plan
- 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 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.

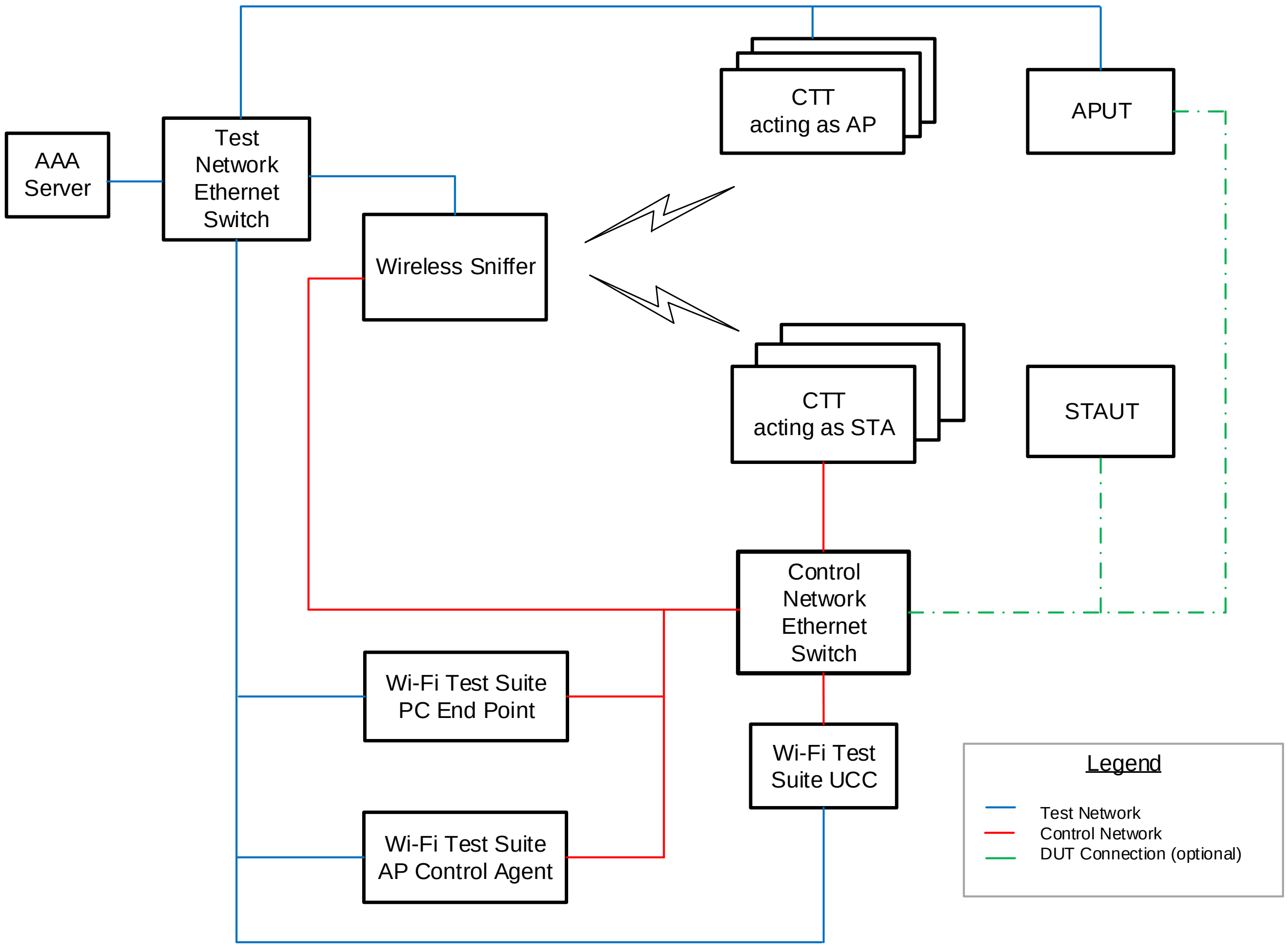
AAA Server
Test Network Ethernet Switch
Wireless Sniffer
CTT acting as AP
APUT
CTT acting as STA
STAUT
Control Network Ethernet Switch
Wi-Fi Test Suite PC End Point
Wi-Fi Test Suite AP Control Agent
Wi-Fi Test Suite UCC
Legend
Test Network
Control Network
DUT Connection (optional)

**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 operate in Enterprise and Personal Modes

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

© 2020 Wi-Fi Alliance. All Rights Reserved.

**Table 3. CTT/Test bed AP general configuration parameters**

| Parameter | Description | Default value |
|---|---|---|
| SSID | Service Set Identifier | Wi-Fi |
| Operating channel | Primary channel used for the test | 6 or 44 (dual band use 6) |
| Cipher Suite Type | Cipher suite | Group cipher suite: 00-0F-AC 4 (CCMP-128)<br>Pairwise cipher suite: 00-0F-AC 4 (CCMP-128)<br>Group management cipher suite: 00-0F-AC:6 (BIP-CMAC-128), when management frame protection is enabled |
| FT Mobility Domain | FT Mobility Domain used for tests | 0101 |
| FT Resource Request Protocol | Support for FT Resource Request Protocol | Disabled |
| PMKSA Caching | PMKSA Caching Capability | Disabled |

### 2.4.2 CTT/Test bed STA requirements

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

- Able to connect in Enterprise and Personal Modes

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

**Table 4. CTT/Test bed STA general configuration parameters**

| Parameter | Description | Default value |
|---|---|---|
| Cipher Suite Type | Cipher suite | • Group cipher suite: 00-0F-AC 4 (CCMP-128)<br>• Pairwise cipher suite: 00-0F-AC 4 (CCMP-128)<br>• Group management cipher suite: 00-0F-AC:6 (BIP-CMAC-128), when management frame protection is enabled |
| FT Resource Request Protocol | Support for FT Resource Request Protocol | Disabled |
| PMKSA Caching | PMKSA Caching Capability | Disabled |

© 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 certification.

## 3.1 General requirements

### 3.1.1 Prerequisite certification requirements

WPA3-Personal devices 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
    - WPA2 Security Improvements [6]
    - Key Reinstallation Vulnerability Detection [7]

WPA3-Enterprise devices shall implement and pass the following Wi-Fi Alliance certifications as a prerequisite:

- A Wi-Fi CERTIFIED PHY (11a/b/g/n/ac)
- WPA2-Enterprise with all supported EAP methods
    - If WPA3-Enterprise 192-bit Security [5] certification is desired, then EAP-TLS shall be tested as a prerequisite
- WPA2 with
    - Protected Management Frames
    - WPA2 Security Improvements [6]
    - Key Reinstallation Vulnerability Detection [7]

### 3.1.2 Testing requirements

#### 3.1.2.1 WPA3-Personal testing requirements

The latest version of the following Wi-Fi Alliance test plan shall be passed in order to receive WPA3-Personal certification.

- WPA3-SAE Test Plan [4]

A STAUT may support Fast BSS Transition.

An APUT may support Fast BSS Transition. If an APUT supports Fast BSS Transition, then:

- The corresponding vendor shall submit two APs. One serves as the APUT; the other serves as an AP.
- Note: If an APUT is supporting FT in the same box for different bands, then it is not required to pass the FT tests. The reason is that such new device capability has not been validated and will be addressed in the future.

© 2020 Wi-Fi Alliance. All Rights Reserved.

#### 3.1.2.2 WPA3-Enterprise testing requirements

The latest version of the following Wi-Fi Alliance test plan shall be passed in order to receive WPA3-Enterprise certification.

- WPA3-SAE Test Plan [4]

WPA3-Enterprise devices may implement and pass the following Wi-Fi Alliance test plan.

- WPA3-Enterprise 192-bit Security Test Plan [5]

A STAUT may support Fast BSS Transition.

An APUT may support Fast BSS Transition. If an APUT supports Fast BSS Transition, then:

- The corresponding vendor shall submit two APs - one serves as the APUT the other serves as a testbed AP
- Note: If an APUT is supporting FT in the same box for different bands, then it is not required to pass the FT tests. The reason is that such new device capability has not been validated and it will be addressed in future.

A STAUT shall support Server Certificate Validation, if it supports one or more of the following EAP methods: TTLS, TLS, PEAPv0, PEAPv1.

## 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 the 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.

© 2020 Wi-Fi Alliance. All Rights Reserved.

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 Fast BSS Transition certification.

For WPA3-SAE and WPA3-Enterprise 192-bit Security features, please refer to the corresponding test plans as follows:

- WPA3-SAE Test Plan [4]
- WPA3-Enterprise 192-bit Security Test Plan [5]

**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) |
|---|---|---|---|---|
| CTT STA Roam from APUT to AP and back | 8.1 | | | |
| APUT in WPA3-Personal only Mode | FT-8.1.1 | O | Y | Y |
| APUT in WPA3-Personal only Mode, over the-DS | FT-8.1.1_DS | O | Y | Y |
| APUT in WPA3-Enterprise only mode, interoperating with PMF required CTT STA | FT-8.1.4 | O | Y | Y |
| APUT in WPA3-Enterprise only mode, interoperating with PMF required CTT STA, over-the-DS | FT-8.1.4_DS | O | Y | Y |
| APUT in WPA3-Enterprise transition mode, interoperating with PMF required CTT STA | FT-8.1.5 | O | Y | Y |
| APUT in Enterprise Transition mode, interoperating with PMF disabled CTT STA | FT-8.1.6 | O | Y | Y |
| APUT in WPA3-Personal transition mode, interoperating with PMF required CTT STA | FT-8.1.7 | O | Y | Y |
| APUT in WPA3-Personal transition mode, interoperating with PMF disabled CTT STA | FT-8.1.8 | O | Y | Y |
| APUT in WPA3-Personal transition mode, interoperating with PMF required CTT STA | FT-8.1.9 | O | Y | |
| CTT STA Roam from AP to APUT and back | 8.2 | | | |
| APUT in WPA3-Personal only Mode | FT-8.2.1 | O | Y | Y |
| APUT in WPA3-Personal only Mode, over the-DS | FT-8.2.1_DS | O | Y | Y |
| APUT in WPA3-Enterprise only mode, interoperating with PMF required CTT STA | FT-8.2.4 | O | Y | Y |
| APUT in WPA3-Enterprise only mode, interoperating with PMF required CTT STA, over-the-DS | FT-8.2.4_DS | O | Y | Y |
| APUT in WPA3-Enterprise transition mode, interoperating with PMF required CTT STA | FT-8.2.5 | O | Y | Y |
| APUT in Enterprise Transition mode, interoperating with PMF disabled CTT STA | FT-8.2.6 | O | Y | Y |
| APUT in WPA3-Personal transition mode, interoperating with PMF required CTT STA | FT-8.2.7 | O | Y | Y |
| APUT in WPA3-Personal transition mode, interoperating with PMF disabled CTT STA | FT-8.2.8 | O | Y | Y |
| APUT in WPA3-Personal transition mode, interoperating with PMF required CTT STA | FT-8.2.9 | O | Y | Y |

### 3.2.2 STAUT tests

Table 6 summarizes for WPA3 Fast BSS Transition and Server Certificate Validation feature certification.

For WPA3-Personal only Mode and WPA3-Enterprise 192-bit Security features, refer to the corresponding test plans as follows:

- WPA3-SAE Test Plan [4]
- WPA3-Enterprise 192-bit Security Test Plan [5]

**Table 6. STAUT test applicability**

| Test Case Description | Test plan section | Applicability: Mandatory (M) / Optional (O) / Conditional © | Should feature be listed in the Capabilities Form? (Y/N) | If implemented, displayed in certificate? (Y/N) |
|---|---|---|---|---|
| STAUT roam from CTT AP1 to AP2 and back | 9.1 | | | |
| STAUT in WPA3-Personal only Mode | FT-9.1.1 | O | Y | Y |
| STAUT in WPA3-Personal only Mode, Over-the-DS | FT-9.1.1_DS | O | Y | Y |
| STAUT in WPA3-Enterprise only mode, interoperating with PMF required CTT APs | FT-9.1.4 | O | Y | Y |
| STAUT in WPA3-Enterprise only mode, interoperating with PMF required CTT APs, Over-the-DS | FT-9.1.4_DS | O | Y | Y |
| STAUT in WPA3-Enterprise transition mode, interoperating with PMF required CTT APs | FT-9.1.5 | O | Y | Y |
| STAUT in Enterprise Transition Mode, interoperating with PMF disabled CTT APs | FT-9.1.6 | O | Y | Y |
| STAUT in WPA3-Personal transition mode, interoperating with PMF required CTT APs | FT-9.1.7 | O | Y | Y |
| STAUT in WPA3-Personal transition mode, interoperating with PMF disabled CTT APs | FT-9.1.8 | O | Y | Y |
| STAUT in WPA3-Personal transition mode, interoperating with PMF required CTT APs | FT-9.1.9 | O | Y | Y |
| STAUT in WPA3-Personal transition mode, with multiple AKMs | FT-9.1.10 | O | Y | Y |
| | | | | |
| Server Certificate Validation Tests | 11.1 | | | |
| EAP Method: TLS | | | | |
| STAUT configured with exactly-matching server certificate<br>AAA server certificate is signed by private CA | SCV-11.1.1_TLS | C | N | N |
| STAUT configured with matching FQDN and root cert<br>AAA server certificate is signed by private CA | SCV-11.1.2_TLS | | | |
| STAUT configured with matching FQDN-suffix and root cert<br>AAA server certificate is signed by private CA | SCV-11.1.3_TLS | | | |
| STAUT configured with matching root cert but no FQDN<br>AAA server certificate is signed by private CA | SCV-11.1.4_TLS | | | |
| STAUT configured with non-matching server certificate signed by different CA to certificate presented by server<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=enabled | SCV-11.1.6_TLS_UOSC-A | | | |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| | | | | |
|---|---|---|---|---|
| STAUT configured with non-matching server certificate signed by different CA to certificate presented by server<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=disabled only | SCV-11.1.6_TLS_UOSC-DA | | | |
| STAUT configured with non-matching FQDN prefix but matching root cert<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=enabled | SCV-11.1.7_TLS_UOSC-A | | | |
| STAUT configured with non-matching FQDN prefix but matching root cert<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=disabled only | SCV-11.1.7_TLS_UOSC-DA | | | |
| STAUT configured with non-matching FQDN suffix but matching root cert<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=enabled | SCV-11.1.8_TLS_UOSC-A | | | |
| STAUT configured with non-matching FQDN suffix but matching root cert<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=disabled only | SCV-11.1.8_TLS_UOSC-DA | | | |
| STAUT configured with matching FQDN but non-matching root cert<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=enabled | SCV-11.1.9_TLS_UOSC-A | | | |
| STAUT configured with matching FQDN but non-matching root cert<br>AAA server certificate is signed by private CA | SCV-11.1.9_TLS_UOSC-DA | | | |
| STAUT configured with non-matching server certificate containing TOD-STRICT policy, signed by a different CA to the certificate presented by server but indicating the same domain name<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=enabled | SCV-11.1.10_TLS_UOSC-A | | | |
| STAUT configured with non-matching server certificate containing TOD-STRICT policy, signed by a different CA to the certificate presented by server but indicating the same domain name<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=disabled only | SCV-11.1.10_TLS_UOSC-DA | | | |
| STAUT configured with non-matching server certificate (without TOD policy).<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy.<br>STAUT supports UOSC=enabled | SCV-11.1.11_TLS_UOSC-A | | | |
| STAUT configured with non-matching server certificate (without TOD policy).<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy. | SCV-11.1.11_TLS_UOSC-DA | | | |
| STAUT is configured with a non-matching root certificate (without TOD policy), and no FQDN<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy<br>STAUT supports UOSC=enabled | SCV-11.1.13_TLS_UOSC-A | | | |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| | | | | |
|---|---|---|---|---|
| STAUT is configured with a non-matching root certificate (without TOD policy), and no FQDN<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy<br>STAUT supports UOSC=disabled only | SCV-11.1.13_TLS_UOSC-DA | | | |
| STAUT configured with matching FQDN and root cert<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy. | SCV-11.1.14_TLS | | | |
| STAUT is configured with a non-matching root certificate (without TOD policy), and no FQDN<br>AAA server certificate is signed by private CA and contains TOD-TOFU policy<br>STAUT supports UOSC=enabled | SCV-11.1.15_TLS_UOSC-A | | | |
| STAUT is configured with a non-matching root certificate (without TOD policy), and no FQDN<br>AAA server certificate is signed by private CA and contains TOD-TOFU policy<br>STAUT supports UOSC=disabled only | SCV-11.1.15_TLS_UOSC-DA | | | |
| STAUT configured with matching FQDN<br>AAA server certificate is signed by well-known root CA | SCV-11.1.16_TLS | | | |
| STAUT configured with matching FQDN-suffix<br>AAA server certificate is signed by well-known root CA | SCV-11.1.17_TLS | | | |
| STAUT configured with non-matching FQDN<br>AAA server certificate is signed by well-known root CA<br>STAUT supports UOSC=enabled | SCV-11.1.18_TLS_UOSC-A | | | |
| STAUT configured with non-matching FQDN<br>AAA server certificate is signed by well-known root CA<br>STAUT supports UOSC=disabled only | SCV-11.1.18_TLS_UOSC-DA | | | |
| STAUT configured with non-matching FQDN suffix<br>AAA server certificate is signed by well-known root CA<br>STAUT supports UOSC=enabled | SCV-11.1.19_TLS_UOSC-A | | | |
| STAUT configured with non-matching FQDN suffix<br>AAA server certificate is signed by well-known root CA<br>STAUT supports UOSC=disabled only | SCV-11.1.19_TLS_UOSC-DA | | | |
| EAP Method: TTLS | | | | |
| STAUT configured with exactly-matching server certificate<br>AAA server certificate is signed by private CA | SCV-11.1.1_TTLS | C | N | N |
| STAUT configured with matching FQDN and root cert<br>AAA server certificate is signed by private CA | SCV-11.1.2_TTLS | | | |
| STAUT configured with matching FQDN-suffix and root cert<br>AAA server certificate is signed by private CA | SCV-11.1.3_TTLS | | | |
| STAUT configured with matching root cert but no FQDN<br>AAA server certificate is signed by private CA | SCV-11.1.4_TTLS | | | |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| | | | | |
|---|---|---|---|---|
| STAUT configured with non-matching server certificate signed by different CA to certificate presented by server<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=enabled | SCV-11.1.6_TTLS_UOSC-A | | | |
| STAUT configured with non-matching server certificate signed by different CA to certificate presented by server<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=disabled only | SCV-11.1.6_TTLS_UOSC-DA | | | |
| STAUT configured with non-matching FQDN prefix but matching root cert<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=enabled | SCV-11.1.7_TTLS_UOSC-A | | | |
| STAUT configured with non-matching FQDN prefix but matching root cert<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=disabled only | SCV-11.1.7_TTLS_UOSC-DA | | | |
| STAUT configured with non-matching FQDN suffix but matching root cert<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=enabled | SCV-11.1.8_TTLS_UOSC-A | | | |
| STAUT configured with non-matching FQDN suffix but matching root cert<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=disabled only | SCV-11.1.8_TTLS_UOSC-DA | | | |
| STAUT configured with matching FQDN but non-matching root cert<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=enabled | SCV-11.1.9_TTLS_UOSC-A | | | |
| STAUT configured with matching FQDN but non-matching root cert<br>AAA server certificate is signed by private CA | SCV-11.1.9_TTLS_UOSC-DA | | | |
| STAUT configured with non-matching server certificate containing TOD-STRICT policy, signed by a different CA to the certificate presented by server but indicating the same domain name<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=enabled | SCV-11.1.10_TTLS_UOSC-A | | | |
| STAUT configured with non-matching server certificate containing TOD-STRICT policy, signed by a different CA to the certificate presented by server but indicating the same domain name<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=disabled only | SCV-11.1.10_TTLS_UOSC-DA | | | |
| STAUT configured with non-matching server certificate (without TOD policy).<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy.<br>STAUT supports UOSC=enabled | SCV-11.1.11_TTLS_UOSC-A | | | |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| | | | | |
|---|---|---|---|---|
| STAUT configured with non-matching server certificate (without TOD policy).<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy. | SCV-11.1.11_TTLS_UOSC-DA | | | |
| STAUT is configured with a non-matching root certificate (without TOD policy), and no FQDN<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy<br>STAUT supports UOSC=enabled | SCV-11.1.13_TTLS_UOSC-A | | | |
| STAUT is configured with a non-matching root certificate (without TOD policy), and no FQDN<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy<br>STAUT supports UOSC=disabled only | SCV-11.1.13_TTLS_UOSC-DA | | | |
| STAUT configured with matching FQDN and root cert<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy. | SCV-11.1.14_TTLS | | | |
| STAUT is configured with a non-matching root certificate (without TOD policy), and no FQDN<br>AAA server certificate is signed by private CA and contains TOD-TOFU policy<br>STAUT supports UOSC=enabled | SCV-11.1.15_TTLS_UOSC-A | | | |
| STAUT is configured with a non-matching root certificate (without TOD policy), and no FQDN<br>AAA server certificate is signed by private CA and contains TOD-TOFU policy<br>STAUT supports UOSC=disabled only | SCV-11.1.15_TTLS_UOSC-DA | | | |
| STAUT configured with matching FQDN<br>AAA server certificate is signed by well-known root CA | SCV-11.1.16_TTLS | | | |
| STAUT configured with matching FQDN-suffix<br>AAA server certificate is signed by well-known root CA | SCV-11.1.17_TTLS | | | |
| STAUT configured with non-matching FQDN<br>AAA server certificate is signed by well-known root CA<br>STAUT supports UOSC=enabled | SCV-11.1.18_TTLS_UOSC-A | | | |
| STAUT configured with non-matching FQDN<br>AAA server certificate is signed by well-known root CA<br>STAUT supports UOSC=disabled only | SCV-11.1.18_TTLS_UOSC-DA | | | |
| STAUT configured with non-matching FQDN suffix<br>AAA server certificate is signed by well-known root CA<br>STAUT supports UOSC=enabled | SCV-11.1.19_TTLS_UOSC-A | | | |
| STAUT configured with non-matching FQDN suffix<br>AAA server certificate is signed by well-known root CA<br>STAUT supports UOSC=disabled only | SCV-11.1.19_TTLS_UOSC-DA | | | |
| EAP Method: PEAPv0 | | | | |
| STAUT configured with exactly-matching server certificate<br>AAA server certificate is signed by private CA | SCV-11.1.1_PEAP0 | C | N | N |

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.

| | | | | |
|---|---|---|---|---|
| STAUT configured with matching FQDN and root cert<br>AAA server certificate is signed by private CA | SCV-11.1.2_PEAP0 | | | |
| STAUT configured with matching FQDN-suffix and root cert<br>AAA server certificate is signed by private CA | SCV-11.1.3_PEAP0 | | | |
| STAUT configured with matching root cert but no FQDN<br>AAA server certificate is signed by private CA | SCV-11.1.4_PEAP0 | | | |
| STAUT configured with non-matching server certificate signed by different CA to certificate presented by server<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=enabled | SCV-11.1.6_PEAP0_UOSC-A | | | |
| STAUT configured with non-matching server certificate signed by different CA to certificate presented by server<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=disabled only | SCV-11.1.6_PEAP0_UOSC-DA | | | |
| STAUT configured with non-matching FQDN prefix but matching root cert<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=enabled | SCV-11.1.7_PEAP0_UOSC-A | | | |
| STAUT configured with non-matching FQDN prefix but matching root cert<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=disabled only | SCV-11.1.7_PEAP0_UOSC-DA | | | |
| STAUT configured with non-matching FQDN suffix but matching root cert<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=enabled | SCV-11.1.8_PEAP0_UOSC-A | | | |
| STAUT configured with non-matching FQDN suffix but matching root cert<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=disabled only | SCV-11.1.8_PEAP0_UOSC-DA | | | |
| STAUT configured with matching FQDN but non-matching root cert<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=enabled | SCV-11.1.9_PEAP0_UOSC-A | | | |
| STAUT configured with matching FQDN but non-matching root cert<br>AAA server certificate is signed by private CA | SCV-11.1.9_PEAP0_UOSC-DA | | | |
| STAUT configured with non-matching server certificate containing TOD-STRICT policy, signed by a different CA to the certificate presented by server but indicating the same domain name<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=enabled | SCV-11.1.10_PEAP0_UOSC-A | | | |

| | | | | |
|---|---|---|---|---|
| STAUT configured with non-matching server certificate containing TOD-STRICT policy, signed by a different CA to the certificate presented by server but indicating the same domain name<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=disabled only | SCV-11.1.10_PEAP0_UOSC-DA | | | |
| STAUT configured with non-matching server certificate (without TOD policy).<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy.<br>STAUT supports UOSC=enabled | SCV-11.1.11_PEAP0_UOSC-A | | | |
| STAUT configured with non-matching server certificate (without TOD policy).<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy. | SCV-11.1.11_PEAP0_UOSC-DA | | | |
| STAUT is configured with a non-matching root certificate (without TOD policy), and no FQDN<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy<br>STAUT supports UOSC=enabled | SCV-11.1.13_PEAP0_UOSC-A | | | |
| STAUT is configured with a non-matching root certificate (without TOD policy), and no FQDN<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy<br>STAUT supports UOSC=disabled only | SCV-11.1.13_PEAP0_UOSC-DA | | | |
| STAUT configured with matching FQDN and root cert<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy. | SCV-11.1.14_PEAP0 | | | |
| STAUT is configured with a non-matching root certificate (without TOD policy), and no FQDN<br>AAA server certificate is signed by private CA and contains TOD-TOFU policy<br>STAUT supports UOSC=enabled | SCV-11.1.15_PEAP0_UOSC-A | | | |
| STAUT is configured with a non-matching root certificate (without TOD policy), and no FQDN<br>AAA server certificate is signed by private CA and contains TOD-TOFU policy<br>STAUT supports UOSC=disabled only | SCV-11.1.15_PEAP0_UOSC-DA | | | |
| STAUT configured with matching FQDN<br>AAA server certificate is signed by well-known root CA | SCV-11.1.16_PEAP0 | | | |
| STAUT configured with matching FQDN-suffix<br>AAA server certificate is signed by well-known root CA | SCV-11.1.17_PEAP0 | | | |
| STAUT configured with non-matching FQDN<br>AAA server certificate is signed by well-known root CA<br>STAUT supports UOSC=enabled | SCV-11.1.18_PEAP0_UOSC-A | | | |
| STAUT configured with non-matching FQDN<br>AAA server certificate is signed by well-known root CA<br>STAUT supports UOSC=disabled only | SCV-11.1.18_PEAP0_UOSC-DA | | | |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| | | | | |
|---|---|---|---|---|
| STAUT configured with non-matching FQDN suffix<br>AAA server certificate is signed by well-known root CA<br>STAUT supports UOSC=enabled | SCV-11.1.19_PEAP0_UOSC-A | | | |
| STAUT configured with non-matching FQDN suffix<br>AAA server certificate is signed by well-known root CA<br>STAUT supports UOSC=disabled only | SCV-11.1.19_PEAP0_UOSC-DA | | | |
| EAP Method: PEAPv1 | | | | |
| STAUT configured with exactly-matching server certificate<br>AAA server certificate is signed by private CA | SCV-11.1.1_PEAP1 | C | N | N |
| STAUT configured with matching FQDN and root cert<br>AAA server certificate is signed by private CA | SCV-11.1.2_PEAP1 | | | |
| STAUT configured with matching FQDN-suffix and root cert<br>AAA server certificate is signed by private CA | SCV-11.1.3_PEAP1 | | | |
| STAUT configured with matching root cert but no FQDN<br>AAA server certificate is signed by private CA | SCV-11.1.4_PEAP1 | | | |
| STAUT configured with non-matching server certificate signed by different CA to certificate presented by server<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=enabled | SCV-11.1.6_PEAP1_UOSC-A | | | |
| STAUT configured with non-matching server certificate signed by different CA to certificate presented by server<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=disabled only | SCV-11.1.6_PEAP1_UOSC-DA | | | |
| STAUT configured with non-matching FQDN prefix but matching root cert<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=enabled | SCV-11.1.7_PEAP1_UOSC-A | | | |
| STAUT configured with non-matching FQDN prefix but matching root cert<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=disabled only | SCV-11.1.7_PEAP1_UOSC-DA | | | |
| STAUT configured with non-matching FQDN suffix but matching root cert<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=enabled | SCV-11.1.8_PEAP1_UOSC-A | | | |
| STAUT configured with non-matching FQDN suffix but matching root cert<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=disabled only | SCV-11.1.8_PEAP1_UOSC-DA | | | |
| STAUT configured with matching FQDN but non-matching root cert<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=enabled | SCV-11.1.9_PEAP1_UOSC-A | | | |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| | | | | |
|---|---|---|---|---|
| STAUT configured with matching FQDN but non-matching root cert<br>AAA server certificate is signed by private CA | SCV-11.1.9_PEAP1_UOSC-DA | | | |
| STAUT configured with non-matching server certificate containing TOD-STRICT policy, signed by a different CA to the certificate presented by server but indicating the same domain name<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=enabled | SCV-11.1.10_PEAP1_UOSC-A | | | |
| STAUT configured with non-matching server certificate containing TOD-STRICT policy, signed by a different CA to the certificate presented by server but indicating the same domain name<br>AAA server certificate is signed by private CA<br>STAUT supports UOSC=disabled only | SCV-11.1.10_PEAP1_UOSC-DA | | | |
| STAUT configured with non-matching server certificate (without TOD policy).<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy.<br>STAUT supports UOSC=enabled | SCV-11.1.11_PEAP1_UOSC-A | | | |
| STAUT configured with non-matching server certificate (without TOD policy).<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy. | SCV-11.1.11_PEAP1_UOSC-DA | | | |
| STAUT is configured with a non-matching root certificate (without TOD policy), and no FQDN<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy<br>STAUT supports UOSC=enabled | SCV-11.1.13_PEAP1_UOSC-A | | | |
| STAUT is configured with a non-matching root certificate (without TOD policy), and no FQDN<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy<br>STAUT supports UOSC=disabled only | SCV-11.1.13_PEAP1_UOSC-DA | | | |
| STAUT configured with matching FQDN and root cert<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy. | SCV-11.1.14_PEAP1 | | | |
| STAUT is configured with a non-matching root certificate (without TOD policy), and no FQDN<br>AAA server certificate is signed by private CA and contains TOD-TOFU policy<br>STAUT supports UOSC=enabled | SCV-11.1.15_PEAP1_UOSC-A | | | |
| STAUT is configured with a non-matching root certificate (without TOD policy), and no FQDN<br>AAA server certificate is signed by private CA and contains TOD-TOFU policy<br>STAUT supports UOSC=disabled only | SCV-11.1.15_PEAP1_UOSC-DA | | | |
| STAUT configured with matching FQDN<br>AAA server certificate is signed by well-known root CA | SCV-11.1.16_PEAP1 | | | |
| STAUT configured with matching FQDN-suffix<br>AAA server certificate is signed by well-known root CA | SCV-11.1.17_PEAP1 | | | |

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.

| | | | | |
|---|---|---|---|---|
| STAUT configured with non-matching FQDN<br>AAA server certificate is signed by well-known root CA<br>STAUT supports UOSC=enabled | SCV-11.1.18_PEAP1_UOSC-A | | | |
| STAUT configured with non-matching FQDN<br>AAA server certificate is signed by well-known root CA<br>STAUT supports UOSC=disabled only | SCV-11.1.18_PEAP1_UOSC-DA | | | |
| STAUT configured with non-matching FQDN suffix<br>AAA server certificate is signed by well-known root CA<br>STAUT supports UOSC=enabled | SCV-11.1.19_PEAP1_UOSC-A | | | |
| STAUT configured with non-matching FQDN suffix<br>AAA server certificate is signed by well-known root CA<br>STAUT supports UOSC=disabled only | SCV-11.1.19_PEAP1_UOSC-DA | | | |
| | | | | |
| STAUT server certificate configuration requirements test | 11.2 | | | |
| STAUT server certificate configuration requirements test, EAP=TTLS<br>Run 1: Unconfigured | SCV-11.2.1_TTLS | C | N | N |
| STAUT server certificate configuration requirements test, EAP=TTLS<br>Run 2: Explicitly disable server validation | SCV-11.2.2_TTLS | | | |
| STAUT server certificate configuration requirements test, EAP=TTLS<br>Run 3: Configure use of system trust store only | SCV-11.2.3_TTLS | | | |
| STAUT server certificate configuration requirements test, EAP=TLS<br>Run 1: Unconfigured | SCV-11.2.1_TLS | | | |
| STAUT server certificate configuration requirements test, EAP=TLS<br>Run 2: Explicitly disable server validation | SCV-11.2.2_TLS | | | |
| STAUT server certificate configuration requirements test, EAP=TLS<br>Run 3: Configure use of system trust store only | SCV-11.2.3_TLS | | | |
| STAUT server certificate configuration requirements test, EAP=PEAPv0<br>Run 1: Unconfigured | SCV-11.2.1_PEAP0 | | | |
| STAUT server certificate configuration requirements test, EAP=PEAPv0<br>Run 2: Explicitly disable server validation | SCV-11.2.2_PEAP0 | | | |
| STAUT server certificate configuration requirements test, EAP=PEAPv0<br>Run 3: Configure use of system trust store only | SCV-11.2.3_PEAP0 | | | |
| STAUT server certificate configuration requirements test, EAP=PEAPv1<br>Run 1: Unconfigured | SCV-11.2.1_PEAP1 | | | |
| STAUT server certificate configuration requirements test, EAP=PEAPv1<br>Run 2: Explicitly disable server validation | SCV-11.2.2_PEAP1 | | | |
| STAUT server certificate configuration requirements test, EAP=PEAPv1<br>Run 3: Configure use of system trust store only | SCV-11.2.3_PEAP1 | | | |

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.

## 3.3 Configuration requirements

The DUT parameters that require manual configuration are listed below.

1. SSID
2. Channel
3. Support for cipher suites
4. Password/phrase/code/key
5. User Interface to enter the network configurations for Server Certificate Validation, if supported by STAUT

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 APUT general configuration values that a technician shall set within a test procedure. Specific test cases may impose additional configuration requirements.

**Table 7. APUT general configuration parameters**

| Parameter | Description | Default value |
|---|---|---|
| SSID | Service Set Identifier | Wi-Fi |
| Operating channel | Primary channel used for the test | 6 or 44 (dual band use 6) |
| FT Mobility Domain | FT Mobility Domain | Hex 0101 |

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

**Table 8. STAUT general configuration parameters**

| Parameter | Description | Default value |
|---|---|---|
| SSID | Service Set Identifier | Wi-Fi |

## 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 and general DUT parameters shall be configured on devices at the start of each test case unless otherwise noted.

© 2020 Wi-Fi Alliance. All Rights Reserved.

# 4 WPA3-Personal only Mode APUT tests

Refer to WPA3-SAE Test Plan [4] for this category of tests.

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-Personal only Mode STAUT tests

Refer to WPA3-SAE Test Plan [4] for this category of tests.

© 2020 Wi-Fi Alliance. All Rights Reserved.

# 6 WPA3 192-bit Security APUT tests

Refer to WPA3-Enterprise 192-bit Security Test Plan [5] for this category of tests.

© 2020 Wi-Fi Alliance. All Rights Reserved.

# 7 WPA3 192-bit Security STAUT tests

Refer to WPA3-Enterprise 192-bit Security Test Plan [5] for this category of tests.

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.

# 8 WPA3 Fast BSS Transition APUT tests

## 8.1 CTT STA Roam from APUT to AP1 and back

### Objective

The following tests verify that the APUT can support over-the-air FT protocol with AKM suites as indicated in the following scenarios when the CTT STA associates to the APUT first then roams to the AP.

If APUT supports Over-the-DS, the test is repeated in Over-the-DS mode per Table 9 .

**Applicability:** Optional. Respective test scenarios are only required if the APUT declared support in Table 1.

### References

Section 13.5,13.7,13.8 [1]

### Test environment

- APUT
- CTT STA acting as a test bed STA
- An AP acting as AP1, which is from same vendor that provides APUT
- Wireless Sniffer
- Authentication Server
- Network Ping Endpoint: A test bed laptop that is on the same subnet and is accessible from APUT and AP1

### Test configuration

Table 9 defines the specific parameter values required for this test case. Each scenario (i.e., entry in the table) shall be exercised as an independent run.

**Table 9. CTT STA Roam from APUT to AP1 and back: Scenarios and Configuration Settings**

| Test case number | APUT Fast BSS Transition Test Case | APUT, AP1 PMF setting | CTT STA PMF setting | APUT, AP1 AKM Suite(s) | CTT STA AKM Suites configuration and in (Re)association Request SN check | FT Protocol configuration in APUT, AP1 and CTT STA | Other Configuration Settings |
|---|---|---|---|---|---|---|---|
| FT-8.1.1 | APUT in WPA3-Personal only Mode | Required | Required | 8,9 | 9 | Over the Air | Passphrase: 12345678<br>PMKSA caching enabled for both STA and APs |
| FT-8.1.1_DS | APUT in WPA3-Personal only Mode, over the-DS | Required | Required | 8,9 | 9 | Over-the-DS | Passphrase: 12345678 |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| Test case number | APUT Fast BSS Transition Test Case | APUT, AP1 PMF setting | CTT STA PMF setting | APUT, AP1 AKM Suite(s) | CTT STA AKM Suites configuration and in (Re)association Request SN check | FT Protocol configuration in APUT, AP1 and CTT STA | Other Configuration Settings |
|---|---|---|---|---|---|---|---|
| | | | | | | | PMKSA caching enabled for both STA and APs |
| FT-8.1.4 | APUT in WPA3-Enterprise only mode, interoperating with PMF required CTT STA | Required | Required | 5, 3 | 3 | Over the Air | AS: hostapd<br>EAP: EAP-TTLS |
| FT-8.1.4_DS | APUT in WPA3-Enterprise only mode, interoperating with PMF required CTT STA | Required | Required | 5, 3 | 3 | Over-the-DS | AS: hostapd<br>EAP: EAP-TTLS |
| FT-8.1.5 | APUT in WPA3-Enterprise transition mode, interoperating with PMF required CTT STA | Capable | Required | 1, 3,5 | 3 | Over the Air | AS: hostapd<br>EAP: EAP-TTLS |
| FT-8.1.6 | APUT in Enterprise Transition mode, interoperating with PMF disabled CTT STA | Capable | Disabled | 1, 3,5 | 3 | Over the Air | AS: hostapd<br>EAP: EAP-TTLS |
| FT-8.1.7 | APUT in WPA3-Personal transition mode, interoperating with PMF required CTT STA | Capable | Required | 2,4,6,8,9 | 9 | Over the Air | Passphrase: 12345678 |
| FT-8.1.8 | APUT in WPA3-Personal transition mode, interoperating with PMF disabled CTT STA | Capable | Disabled | 2,4,6,8,9 | 4 | Over the Air | Passphrase: 12345678 |
| FT-8.1.9 | APUT in WPA3-Personal transition mode, interoperating with PMF required CTT STA | Capable | Required | 2,4,6,8,9 | 4 | Over the Air | Passphrase: 12345678 |

### Test procedure and expected results

Table 10 provides the specific test procedure and expected results for this test case.

**Table 10. CTT STA Roam from APUT to AP1 and back: test procedure and expected results**

| Step | APUT | Test bed AP1 | CTT acting as a test bed STA1 | AAA Server<br>Applicable to WPA3-Enterprise | CTT STA validation check and AP1 validation check | Expected Result |
|---|---|---|---|---|---|---|
| 1 | Reset APUT. Configure the APUT per Table 7, and Table 9 according | Reset and configure the AP1 per Table 3, and Table 9 according | Delete any cached security information on STA1. Reset and configure STA1 per | Configure the Authentication | Record the actual AKM Suite Count and AKM Suite List from the RSNE from APUT and AP1 Beacon | |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| Step | APUT | Test bed AP1 | CTT acting as a test bed STA1 | AAA Server<br>Applicable to WPA3-Enterprise | CTT STA validation check and AP1 validation check | Expected Result |
|---|---|---|---|---|---|---|
| | to the test mode being verified | to the test scenario being verified | Table 4, and Table 9 according to the test mode being verified | server per Table 9.<br>Revoke any active security context for STA1 and then configure STA1 with fresh security credentials | | |
| 2 | APUT starts to transmit Beacon frames. | AP1 starts to transmit Beacon frames. | | | SN: Verify that AP1 transmits a correctly formatted Beacon frame with the Mobility Domain element (MDE) with:<br>1. MDID is present and valid<br>2. Fast BSS Transition over DS field is set according to the test mode configured (0 for over-the-air, 1 for over-the-DS)<br>3. A RSNE with AKM Suite List field includes the AKM list per Scenario in Table 9 depending on the test mode configured.<br>a. Record the actual AKM Suite Count and AKM Suite List from the RSNE from AP1 Beacon<br>b. Contains correct MFPR/MFPC settings depending on test mode | SN: Verify that APUT transmits a correctly formatted Beacon frame with the Mobility Domain element (MDE) with:<br>1. MDID is present and valid<br>2. Fast BSS Transition over DS field is set according to the test mode configured (0 for over-the-air, 1 for over-the-DS)<br>3. A RSNE with AKM Suite List field includes the AKM list per scenario in Table 9 depending on the test mode configured.<br>a. Record the actual AKM Suite Count and AKM Suite List from the RSNE from APUT Beacon<br>b. Contains correct MFPR/MFPC settings depending on test mode<br>If all the above conditions are true, then CONTINUE else FAIL |
| 3 | | | Configure CTT STA to send a Probe Request frame. | | | SN: Verify that APUT transmits a correctly formatted Probe Response frame with RSNE including correct AKM suite(s)<br>If all the above conditions are true, then CONTINUE else FAIL |
| 4 | | | Configure CTT STA to connect to APUT BSSID. | | Verify that for CTT STA: in Authentication Request frame:<br>1. For SAE:<br>a. authentication type =3 | |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| Step | APUT | Test bed AP1 | CTT acting as a test bed STA1 | AAA Server<br>Applicable to WPA3-Enterprise | CTT STA validation check and AP1 validation check | Expected Result |
|---|---|---|---|---|---|---|
| | | | The CTT STA associates to the APUT BSSID using FT in the corresponding test mode. The STA sends an Association Request frame to the APUT. | | 2. For others:<br>a. authentication type =0 (open)<br>In initial mobility domain Association Request frame:<br>1. MDE is present<br>2. AKM suite is as in Table 9<br>3. MFPC/MFPR are as in Table 9 | |
| 5 | APUT sends an Association Response Frame | | | | | SN: Verify that the APUT transmits a correctly formatted Association Response frame to STA, containing:<br>1. Fast BSS Transition IE (FTE) containing the R1KH-ID and R0KH-ID and having<br>a. MIC element count set to 0<br>b. ANonce set to 0<br>c. SNonce set to 0<br>d. MIC set to 0<br>2. MDE as advertised in the Beacon<br>If all the above conditions are true, then CONTINUE else FAIL |
| 6 | Wait for 4-way handshake to occur. | | | | | |
| 7 | | | PING_IP_ADDRESS = IP_ADDR of Network Ping Endpoint<br>Configure CTT STA to start a continuous ping to the Network Ping Endpoint<br><ping PING__IP_ADDR>, COUNT = 10, FRAME_RATE = 1 | | | If ping is successful through APUT then CONTINUE, else FAIL |
| 8 | | | Trigger CTT STA to roam (reassociate) to | | SN:<br>In FT Over-the-air case, verify that the CTT STA transmits a correctly | SN: |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| Step | APUT | Test bed AP1 | CTT acting as a test bed STA1 | AAA Server<br>Applicable to WPA3-Enterprise | CTT STA validation check and AP1 validation check | Expected Result |
|---|---|---|---|---|---|---|
| | | | AP1 BSSID via FT protocol<br>Allow the STA to authenticate and reassociate to AP1 BSSID using FT protocol in the corresponding test mode. | | formatted Authentication Request frame with Authentication type = 2<br>In FT Over-the-DS case, verify that the CTT STA does not transmit an Authentication frame.<br>1. In WPA3-Enterprise run, verify that the CTT STA transmits a FT Request frame to APUT where STA Address field is set to the MAC address of the CTT STA, and the Target AP Address field is set to BSSID ofAP1 and MDE/FTE/RSNE are present.<br>Verify that the CTT STA transmits a correctly formatted Reassociation Request frame to the AP1:<br>1. MDE/FTE/RSNE are present<br>2. AKM suite is as in Table 9<br>3. MFPC/MFPR are as in Table 9<br>In FT over-the-air case, verify that the AP1 transmits a correctly formatted authentication Response frame with:<br>1. FTE with ANonce, SNonce, R1KH-ID and R0KH-ID<br>2. MDE<br>3. RSNE with PMKR0Name<br>4. Authentication type = 2 (FT)<br>Verify that the AP1 transmits a correctly formatted Reassociation Response frame to the test bed STA, containing:<br>1. FTE with MIC, ANonce, SNonce, R1KH-ID and R0KH-ID<br>2. MDE | In FT Over-the-DS case: Verify that APUT does not transmit an Authentication frame.<br>1. In WPA3-Enterprise run, verify that APUT transmits an FT Response frame to CTT STA where STA Address field is set to the MAC address of the CTT STA, Target AP Address field is set to BSSID of AP1, Status Code field indicates SUCCESS, and MDE/FTE/RSNE are present.<br>If all the conditions are satisfied, 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 | Test bed AP1 | CTT acting as a test bed STA1 | AAA Server<br>Applicable to WPA3-Enterprise | CTT STA validation check and AP1 validation check | Expected Result |
|---|---|---|---|---|---|---|
| | | | | | 3. RSNE with PMKR1Name, RSN version set to 1, and AKM Suite Count field and AKM Suite List field exactly matching those in recorded AP1 Beacon in Step 2 | |
| 9 | | | PING_IP_ADDRESS = IP_ADDR of Network Ping Endpoint<br>Configure CTT STA to start a continuous ping to the Network Ping Endpoint<br><ping PING__IP_ADDR>, COUNT = 10, FRAME_RATE = 1 | | Ensure that ping packets are sent to Network Ping Endpoint via AP1 and that the ping is successful. | If ping is successful through AP1 then CONTINUE, else FAIL |
| 10 | | | Trigger CTT STA to roam (reassociate) to APUT BSSID via FT protocol | | SN:<br>In FT Over-the-air case, verify that the CTT STA transmits a correctly formatted Authentication Request frame with Authentication type = 2<br>In FT Over-the-DS case, verify that the CTT STA does not transmit an Authentication frame.<br>1. In the WPA3-Enterprise run, verify that the CTT STA transmits a FT Request frame to AP1, where the STA Address field is set to the MAC address of the CTT STA, the Target AP Address field is set to BSSID of APUT, and MDE/FTE/RSNE are present.<br>In FT Over-the-DS case,<br>1. in the WPA3-Enterprise run, verify thatAP1 transmits an FT | |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| Step | APUT | Test bed AP1 | CTT acting as a test bed STA1 | AAA Server<br>Applicable to WPA3-Enterprise | CTT STA validation check and AP1 validation check | Expected Result |
|---|---|---|---|---|---|---|
| | | | | | Response frame to CTT STA where:<br>a. The STA Address field is set to the MAC address of the CTT STA<br>b. The Target AP Address field is set to BSSID of the APUT<br>c. The Status Code field indicates SUCCESS<br>d. MDE/FTE/RSNE are present | |
| 11 | APUT responds with an Authentication Response Frame (in Over-the-air case) | | | | | SN:<br>In FT Over-the-air case, verify that the APUT transmits a correctly formatted Authentication Response frame to the STA, containing:<br>1. FTE with ANonce, SNonce, R1KH-ID and R0KH-ID<br>2. MDE<br>3. RSNE with PMKR0Name<br>4. Authentication type = 2 (FT)<br>If all the above conditions are true, then CONTINUE else FAIL |
| 12 | | | The CTT STA sends a Reassociation Request frame to the APUT containing FTE, MDE and RSNE, where RSNE indicates support for the tested FT mode by setting AKM Suite Count field to 1 and AKM Suite | | Verify that the CTT STA transmits a correctly formatted Reassociation Request frame to the APUT as follows:<br>1. MDE/FTE/RSNE are present<br>2. AKM suite is as in Table 9<br>3. MFPC/MFPR are as in Table 13. | |
| 13 | The APUT responds to the Reassociation Request frame by sending a Reassociation Response frame. | | | | | SN:<br>Verify that the APUT transmits a correctly formatted Reassociation Response frame to the STA, containing: |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| Step | APUT | Test bed AP1 | CTT acting as a test bed STA1 | AAA Server<br>Applicable to WPA3-Enterprise | CTT STA validation check and AP1 validation check | Expected Result |
|---|---|---|---|---|---|---|
| | | | | | | 1. the FTE with MIC, ANonce, SNonce, R1KH-ID and R0KH-ID<br>2. MDE<br>3. RSNE with PMKR1Name, RSN version set to 1, and AKM Suite Count field and AKM Suite List field exactly matching those in the recorded APUT Beacon in step 2<br>If all the above conditions are true, then CONTINUE else FAIL |
| 14 | | | PING_IP_ADDRESS = IP_ADDR of Network Ping Endpoint<br>Configure STA1 to ping Network Ping Endpoint<br><ping PING__IP_ADDR>, COUNT = 10, FRAME_RATE = 1 | | Ensure that ping packets are sent to the Network Ping Endpoint via the APUT and that the ping is successful. | For test 8.1.1. and 8.1.1_DS:<br>If ping is successful then CONTINUE, else FAIL<br>For others:<br>If ping is successful then PASS, else FAIL |
| 15 | | | Trigger CTT STA1 to disassociate from the APUT | | SN:<br>Verify that the CTT STA sends Disassociation or Deauthentication frame to APUT | |
| 16 | | | Wait 5 seconds. Trigger CTT STA1 to connect to APUT BSSID<br>The CTT STA1 sends an Association Request frame to the APUT | | SN:<br>Verify that the CTT STA sends Authentication Request frame with authentication type =0 (open)<br>In the initial mobility domain Association Request:<br>1. MDE is present<br>2. AKM suite is as in Table 13<br>3. PMKID is present<br>4. MFPC/MFPR are as in Table 13 | SN: Verify that the APUT transmits a correctly formatted Association Response frame to STA, containing:<br>1. Fast Transition IE (FTE) containing the R1KH-ID and R0KH-ID and having<br>a. MIC element count set to 0<br>b. ANonce set to 0<br>c. SNonce set to 0<br>d. MIC set to 0<br>2. MDE as advertised in the Beacon frame in step 2 |

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 | Test bed AP1 | CTT acting as a test bed STA1 | AAA Server<br>Applicable to WPA3-Enterprise | CTT STA validation check and AP1 validation check | Expected Result |
|---|---|---|---|---|---|---|
| | | | | | | If all the above conditions are true, then CONTINUE else FAIL |
| 17 | Wait for 4-way handshake to occur. | | | | SN:<br>Verify that RSNE with PMKR1Name is present in message 2 | SN:<br>Verify that APUT transmits message 1 containing the same PMKID as indicated by CTT STA1 in Association Request in step 16 |
| 18 | Repeat steps 7 thru 14 | | | | | Same as steps 7 -14 except step 14:<br>If ping is successful in step 14 then PASS, else FAIL |

## 8.2 CTT STA Roam from AP1 to APUT and back

### Objective

The following tests verify that the APUT can support over-the-air FT protocol with AKM suites as indicated in the following scenarios when the CTT STA roams from an AP to the APUT.

If APUT supports Over-the-DS, the test is repeated in Over-the-DS mode per Table 11.

**Applicability:** Optional. Respective test scenarios are only required if the APUT declared support in Table 1.

### References

Section 13.5,13.7,13.8 [1]

### Test environment

- APUT
- CTT acting as a test bed STA
- An AP acting as AP1, which is from same vendor that provides APUT
- Wireless Sniffer
- Authentication Server
- Network Ping Endpoint: A test bed laptop that is on the same subnet and is accessible from APUT and AP1

### Test configuration

Table 11 defines the specific parameter values required for this test case. Each scenario (i.e., entry in the table) shall be exercised as an independent run.

© 2020 Wi-Fi Alliance. All Rights Reserved.

**Table 11. CTT STA Roam from AP1 to APUT and back: Scenarios and Configuration Settings**

| Test case number | APUT Fast BSS Transition Test Case | APUT, AP1 PMF setting | CTT STA PMF setting | APUT, AP1 AKM Suite(s) | CTT STA AKM Suite(s) configuration and in (Re)association Request SN check | FT Protocol configuration in APUT, AP1 and CTT STA | Other Configuration Settings |
|---|---|---|---|---|---|---|---|
| FT-8.2.1 | APUT in WPA3-Personal only Mode | Required | Required | 8,9 | 9 | Over the Air | Passphrase: 12345678 |
| FT-8.2.1_DS | APUT in WPA3-Personal only Mode, Over-the-DS | Required | Required | 8,9 | 9 | Over-the-DS | Passphrase: 12345678 |
| FT-8.2.4 | APUT in WPA3-Enterprise only mode, interoperating with PMF required CTT STA | Required | Required | 5, 3 | 3 | Over the Air | AS: hostapd<br>EAP: EAP-TTLS |
| FT-8.2.4_DS | APUT in WPA3-Enterprise only mode, interoperating with PMF required CTT STA, Over-the-DS | Required | Required | 5, 3 | 3 | Over-the-DS | AS: hostapd<br>EAP: EAP-TTLS |
| FT-8.2.5 | APUT in WPA3-Enterprise transition mode, interoperating with PMF required CTT STA | Capable | Required | 1, 3,5 | 3 | Over the Air | AS: hostapd<br>EAP: EAP-TTLS |
| FT-8.2.6 | APUT in Enterprise Transition mode, interoperating with PMF disabled CTT STA | Capable | Disabled | 1, 3,5 | 3 | Over the Air | AS: hostapd<br>EAP: EAP-TTLS |
| FT-8.2.7 | APUT in WPA3-Personal transition mode, interoperating with PMF required CTT STA | Capable | Required | 2,4,6,8, 9 | 9 | Over the Air | Passphrase: 12345678 |
| FT-8.2.8 | APUT in WPA3-Personal transition mode, interoperating with PMF disabled CTT STA | Capable | Disabled | 2,4,6,8, 9 | 4 | Over the Air | Passphrase: 12345678 |
| FT-8.2.9 | APUT in WPA3-Personal transition mode, interoperating with PMF required CTT STA | Capable | Required | 2,4,6,8, 9 | 4 | Over the Air | Passphrase: 12345678 |

### Test procedure and expected results

Table 12 provides the specific test procedure and expected results for this test case.

**Table 12. CTT STA Roam from AP1 to APUT and back: test procedure and expected result**

| Step | Test bed AP1 | APUT | CTT acting as a test bed STA1 | AAA Server<br>Applicable to WPA3-Enterprise | CTT STA validation check and AP1 validation check | Expected Result |
|---|---|---|---|---|---|---|
| 1 | Reset and configure the AP1 per Table 3, and Table 11, according to | Reset and configure the APUT per Table 7, and Table 11 according to | Delete any cached security information on STA1. Configure STA1 | Configure the Authentication server per Table 11. | | |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| Step | Test bed AP1 | APUT | CTT acting as a test bed STA1 | AAA Server<br>Applicable to WPA3-Enterprise | CTT STA validation check and AP1 validation check | Expected Result |
|---|---|---|---|---|---|---|
| | the test mode being verified | the test mode being verified | per Table 4, and Table 11 according to the test mode being verified | Revoke any active security context for STA1 and then configure STA1 with fresh security credentials | | |
| 2 | AP1 starts to transmit Beacon frames. | APUT starts to transmit Beacon frames. | | | SN:<br>1. Verify that AP1 transmits a correctly formatted Beacon with:<br>2. the Mobility Domain element (MDE) with:<br>a. MDID is present and valid<br>3. Fast BSS Transition over DS field is set according to the test mode configured (0 for over-the-air, 1 for over-the-DS)<br>4. RSNE with AKM Suite List field includes the AKM list in Table 11, depending on the test mode configured.<br>a. Record the actual AKM Suite Count and AKM Suite List from the RSNE<br>b. Contains correct MFPR/MFPC settings depending on test mode | SN:<br>1. Verify that APUT transmits a correctly formatted Beacon:<br>a. with the Mobility Domain element (MDE) with MDID is present and valid<br>2. Fast BSS Transition over DS field is set according to the test mode configured (0 for over-the-air, 1 for over-the-DS)<br>3. RSNE with AKM Suite List field includes the AKM list in Table 11, depending on the test mode configured.<br>a. Record the actual AKM Suite Count and AKM Suite List from the RSNE<br>b. Contains correct MFPR/MFPC settings depending on test mode<br>If all the above conditions are true, then CONTINUE else FAIL |
| 3 | | | Configure CTT STA to send a Probe Request frame. | | SN: Verify that AP1 transmits a correctly formatted Probe Response frame with RSNE including correct AKM suite(s) as in its Beacon | |
| 4 | | | Configure CTT STA to connect to AP1 BSSID<br>The CTT STA associates to the AP1 BSSID using FT in the corresponding test | | Verify that for CTT STA:<br>In Authentication Request:<br>1. For SAE:<br>a. authentication type =3<br>2. For others: | |

| Step | Test bed AP1 | APUT | CTT acting as a test bed STA1 | AAA Server<br>Applicable to WPA3-Enterprise | CTT STA validation check and AP1 validation check | Expected Result |
|---|---|---|---|---|---|---|
| | | | mode. The STA sends an Association Request frame to the AP1. | | a. authentication type =0 (open)<br>In the initial mobility domain Association Request frame:<br>b. MDE is present<br>c. AKM suite is as in Table 11<br>d. MFPC/MFPR are as in Table 11 | |
| 5 | AP1 sends an Association Response Frame | | | | SN:<br>Verify that the AP1 transmits a correctly formatted Association Response frame to the STA, containing:<br>1. Fast BSS Transition IE (FTE) containing the R1KH-ID and R0KH-ID and having<br>a. MIC element count set to 0<br>b. ANonce set to 0<br>c. SNonce set to 0<br>d. MIC set to 0<br>2. MDE as advertised in the Beacon | |
| 6 | Wait for 4-way handshake to occur. | | | | | |
| 7 | | | PING_IP_ADDRESS = IP_ADDR of Network Ping Endpoint<br>Configure CTT STA to start a continuous ping to the Network Ping Endpoint<br><ping PING__IP_ADDR>, COUNT = 10, FRAME_RATE = 1 | | If ping is successful through AP1 then CONTINUE, else FAIL | |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| Step | Test bed AP1 | APUT | CTT acting as a test bed STA1 | AAA Server<br>Applicable to WPA3-Enterprise | CTT STA validation check and AP1 validation check | Expected Result |
|---|---|---|---|---|---|---|
| 8 | | | Trigger CTT STA to roam to APUT BSSID via CAPI<br>Allow the STA to authenticate and reassociate to the APUT BSSID using FT in the corresponding test mode. | | SN:<br>In FT Over-the-air case, verify that the CTT STA transmits a correctly formatted Authentication Request frame with Authentication type = 2<br>In FT Over-the-DS case, verify that the CTT STA does not transmit an Authentication frame. In WPA3-Enterprise run, verify that the CTT STA transmits a FT Request frame to AP1 where:<br>1. STA Address field is set to the MAC address of the CTT STA,<br>2. Target AP Address field is set to BSSID of APUT,<br>3. MDE/FTE/RSNE are present.<br>In FT Over-the-DS case: in WPA3-Enterprise run, verify that AP1 transmits an FT Response frame to CTT STA where:<br>1. STA Address field is set to the MAC address of the CTT STA,<br>2. Target AP Address field is set to BSSID of APUT<br>3. Status Code field indicates SUCCESS,<br>4. MDE/FTE/RSNE are present.<br>Verify that the CTT STA transmits a correctly formatted Reassociation Request frame to APUT:<br>1. MDE/FTE/RSNE are present<br>2. AKM suite is as in Table 11 | SN:<br>In FT Over-the-air case: Verify that the APUT transmits a correctly formatted authentication Response frame with:<br>1. FTE with ANonce, SNonce, R1KH-ID and R0KH-ID<br>2. MDE<br>3. RSNE with PMKR0Name<br>4. Authentication type = 2 (FT)<br>Verify that the APUT transmits a correctly formatted Reassociation Response frame to the test bed STA, containing<br>1. FTE with MIC, ANonce, SNonce, R1KH-ID and R0KH-ID<br>2. MDE<br>3. RSNE with PMKR1Name, RSN version set to 1, and AKM Suite Count field and AKM Suite List field exactly matching those in recorded APUT Beacon in Step 2<br>If all the conditions are satisfied, then CONTINUE else FAIL. |

| Step | Test bed AP1 | APUT | CTT acting as a test bed STA1 | AAA Server<br>Applicable to WPA3-Enterprise | CTT STA validation check and AP1 validation check | Expected Result |
|---|---|---|---|---|---|---|
| | | | | | 3. MFPC/MFPR are as in Table 11 | |
| 9 | | | PING_IP_ADDRESS = IP_ADDR of Network Ping Endpoint<br>Configure CTT STA to start a continuous ping to the Network Ping Endpoint<br>ping <PING__IP_ADDR>, COUNT = 10, FRAME_RATE = 1 | | | If ping is successful through APUT then CONTINUE, else FAIL |
| 10 | | | Trigger CTT STA to roam to AP1 BSSID via FT protocol | | SN:<br>In FT Over-the-air case: Verify that the CTT STA transmits a correctly formatted Authentication Request frame with Authentication type = 2<br>In FT Over-the-DS case:<br>Verify that the CTT STA does not transmit an Authentication frame.<br>1. In WPA3-Enterprise run, verify that the CTT STA transmits a FT Request frame to APUT where:<br>a. STA Address field is set to the MAC address of the CTT STA<br>b. Target AP Address field is set to BSSID of AP1<br>c. MDE/FTE/RSNE are present. | SN:<br>In FT Over-the-DS case:<br>1. In WPA3-Enterprise run, verify that the APUT transmits an FT Response frame to CTT STA where:<br>a. STA Address field is set to the MAC address of the CTT STA<br>b. Target AP Address field is set to BSSID of AP1,<br>c. Status Code field indicates SUCCESS, and<br>d. MDE/FTE/RSNE are present.<br>If all the conditions are satisfied, then CONTINUE else FAIL. |
| 11 | AP1 responds with an Authentication Response Frame (in Over-the-air case) | | | | SN:<br>In FT Over-the-air case, verify that AP1 transmits a correctly formatted Authentication | |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| Step | Test bed AP1 | APUT | CTT acting as a test bed STA1 | AAA Server<br>Applicable to WPA3-Enterprise | CTT STA validation check and AP1 validation check | Expected Result |
|---|---|---|---|---|---|---|
| | | | | | Response frame to the STA, containing<br>1. FTE with ANonce, SNonce, R1KH-ID and R0KH-ID<br>2. MDE<br>3. RSNE with PMKR0Name<br>4. Authentication type = 2 (FT)<br>If all the above conditions are true, then CONTINUE else FAIL | |
| 12 | | | The CTT STA sends a Reassociation Request frame to AP1 containing FTE, MDE and RSNE, where RSNE indicates support for the tested FT mode by setting AKM Suite Count field to 1 and AKM Suite | | Verify that the CTT STA transmits a correctly formatted Reassociation Request frame to the AP1, such that:<br>1. MDE/FTE/RSNE are present<br>2. AKM suite is as in Table 11<br>3. MFPC/MFPR are as in Table 11 | |
| 13 | The AP1 responds to the Reassociation Request frame by sending a Reassociation Response frame. | | | | SN: Verify that the AP1 transmits a correctly formatted Reassociation Response frame to the CTT STA, containing<br>1. FTE with MIC, ANonce, SNonce, R1KH-ID and R0KH-ID<br>2. MDE<br>3. RSNE with PMKR1Name, RSN version set to 1<br>4. AKM Suite Count field and AKM Suite List field exactly matching the those in recorded AP1 Beacon in step 2 | |
| 14 | | | PING_IP_ADDRESS = IP_ADDR of Network Ping Endpoint<br>Configure CTT STA to start a continuous ping | | Ensure that ping packets are sent between CTT STA and to the Network Ping Endpoint via AP1.<br>If ping is successful then PASS, else FAIL | |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| Step | Test bed AP1 | APUT | CTT acting as a test bed STA1 | AAA Server<br>Applicable to WPA3-Enterprise | CTT STA validation check and AP1 validation check | Expected Result |
|---|---|---|---|---|---|---|
|  |  |  | to the Network Ping Endpoint<br>ping <PING__IP_ADDR>, COUNT = 10, FRAME_RATE = 1 |  |  |  |

© 2020 Wi-Fi Alliance. All Rights Reserved.

# 9 WPA3 Fast BSS Transition STAUT tests

## 9.1 STAUT Roam from CTT AP1 to AP2 and back

### Objective

These tests verify that the STAUT can support FT protocol with AKM suites as indicated in the following scenarios.

If STAUT supports Over-the-DS, the test is repeated in Over-the-DS mode per Table 13.

**Applicability:** Optional. Respective test scenarios are only required if the STAUT declared support in Table 1.

### References

Section 13.5,13.7,13.8 [1]

### Test environment

- STAUT
- CTTs acting as a test bed AP1 and AP2 from same vendor
- Wireless Sniffer
- Authentication Server
- Network Ping Endpoint: A test bed laptop that is on the same subnet and is accessible from the testbed APs

### Test configuration

Table 13 defines the specific parameter values required for this test case. Each scenario (i.e., entry in the table) shall be exercised as an independent run.

**Table 13. STAUT Roam from CTT AP1 to AP2 and back: Scenarios and Configuration Settings**

| Test case number | STAUT Fast BSS Transition Test Case | STAUT PMF setting | CTT AP1 AP2 PMF setting | STAUT AKM Suite(s) configuration | CTT AP1, AP2 AKM Configuration | AKM in (Re)association Request SN check | FT Protocol configuration in AP1, AP2 and STAUT | Other Configuration Settings |
|---|---|---|---|---|---|---|---|---|
| FT-9.1.1 | STAUT in WPA3-Personal only Mode | Required | Required | 8,9 | 9 | 9 | Over the Air | Passphrase: 12345678<br>PMKSA caching enabled for STAUT and APs |
| FT-9.1.1_DS | STAUT in WPA3-Personal only Mode | Required | Required | 8,9 | 9 | 9 | Over-the-DS | Passphrase: 12345678<br>PMKSA caching enabled for |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | STAUT and APs |
| FT-9.1.4 | STAUT in WPA3-Enterprise only mode, interoperating with PMF required CTT APs | Required | Required | 1, 3 | 3 | 3 | Over the Air | AS: hostapd<br>EAP: EAP-TTLS |
| FT-9.1.4_DS | STAUT in WPA3-Enterprise only mode, interoperating with PMF required CTT APs, Over-the-DS | Required | Required | 1, 3 | 3 | 3 | Over-the-DS | AS: hostapd<br>EAP: EAP-TTLS |
| FT-9.1.5 | STAUT in WPA3-Enterprise transition mode, interoperating with PMF required CTT APs | Capable | Required | 1, 3,5 | 3 | 3 | Over the Air | AS: hostapd<br>EAP: EAP-TTLS |
| FT-9.1.6 | STAUT in Enterprise Transition Mode, interoperating with PMF disabled CTT APs | Capable | Disabled | 1, 3,5 | 3 | 3 | Over the Air | AS: hostapd<br>EAP: EAP-TTLS |
| FT-9.1.7 | STAUT in WPA3-Personal transition mode, interoperating with PMF required CTT APs | Capable | Required | 2,4,6,8,9 | 9 | 9 | Over the Air | Passphrase: 12345678 |
| FT-9.1.8 | STAUT in WPA3-Personal transition mode, interoperating with PMF disabled CTT APs | Capable | Disabled | 2,4,6,8,9 | 4 | 4 | Over the Air | Passphrase: 12345678 |
| FT-9.1.9 | STAUT in WPA3-Personal transition mode, interoperating with PMF required CTT APs | Capable | Required | 2,4,6,8,9 | 4 | 4 | Over the Air | Passphrase: 12345678 |
| FT-9.1.10 | STAUT in WPA3-Personal transition mode with multiple AKMs | Capable | Capable | 2,4,6,8,9 | 2,4,6,8,9 | 9 | Over the Air | Passphrase: 12345678 |

### Test procedure and expected results

Table 14 provides the specific test procedure and expected results for this test case.

**Table 14. STAUT Roam from CTT AP1 to AP2 and back: test procedure and expected results**

| Step | STAUT | CTT acting as a test bed AP1 | CTT acting as a test bed AP2 | AAA Server<br>Applicable to WPA3-Enterprise | CTT validation check | Expected Result |
|---|---|---|---|---|---|---|
| 1 | Delete any cached security information on STA1. Reset and configure STAUT per Table 8, and Table 13 | Reset and configure the AP1 per Table 3 and Table 13 | Reset and configure the AP2 per Table 3, and Table 13 | Configure the Authentication server per Table 13.<br>Revoke any active security context for STAUT and then | SN: Verify that AP1 and AP2 transmit a correctly formatted Beacon frame with the:<br>1. Mobility Domain element (MDE) with MDID is present and valid<br>2. Fast BSS Transition over DS field is set according to the test mode configured (0 for over-the-air, 1 for over-the-DS)<br>3. RSNE with AKM Suite List field includes the AKM list per scenario in Table 13. | |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | configure STAUT with fresh security credentials | a. Record the actual AKM Suite Count and AKM Suite List from the RSNE for both AP1 and AP2<br>b. Contain correct MFPR/MFPC settings depending on test scenario | |
| 2 | Configure STAUT to send a Probe Request frame to AP1, if supported | | | | | |
| 3 | Configure STAUT to connect to AP1 BSSID<br>The STAUT associates to the CTT AP1 BSSID using FT in the corresponding test mode. The STAUT sends an Association Request frame to the CTT AP1. | | | | SN:<br>Verify that the CTT AP1 transmits a correctly formatted Association Response frame to STA, containing:<br>1. Fast BSS Transition IE (FTE) containing the R1KH-ID and R0KH-ID and having<br>a. MIC element count set to 0<br>b. ANonce set to 0<br>c. SNonce set to 0<br>d. MIC set to 0<br>2. MDE as advertised in the Beacon frame of AP1 | SN:<br>Verify that for STAUT:<br>In the Authentication Request frame:<br>1. For SAE: authentication type =3<br>2. For others:<br>3. authentication type =0 (open)<br>In initial mobility domain Association Request frame:<br>1. MDE is present<br>2. AKM suite is as in Table 13<br>If all the above conditions are true, then CONTINUE else FAIL |
| 4 | Wait for 4-way handshake to complete | | | | | |
| 5 | PING_IP_ADDRESS = IP_ADDR of Network Ping Endpoint<br>Configure STAUT to ping Network Ping Endpoint:<br>ping <PING_IP_ADDR>, COUNT = 10, FRAME_RATE = 1 | | | | | If ping is successful then CONTINUE, else FAIL |
| 6 | Trigger STAUT to roam (reassociate) to the BSSID of AP2. via FT protocol | | | | SN:<br>In FT Over-the-air case: Verify that the AP2 transmits a correctly formatted authentication Response frame with:<br>1. FTE with ANonce, SNonce, R1KH-ID and R0KH-ID<br>2. MDE<br>3. RSNE with PMKR0Name<br>4. Authentication type = 2 (FT) | SN:<br>In FT Over-the-air case: Verify that the STAUT transmits a correctly formatted Authentication Request frame with Authentication type = 2<br>In FT Over-the-DS case:<br>1. Verify that STAUT does not transmit an Authentication frame. |

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.

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | In FT Over-the-DS case: in WPA3-Enterprise run, verify that AP1 transmits an FT Response frame to STAUT where:<br>1. STA Address field is set to the MAC address of STAUT<br>2. Target AP Address field is set to BSSID of testbed AP2,<br>3. Status Code field indicates SUCCESS<br>4. MDE/FTE/RSNE are present<br><br>Verify that the AP2 transmits a correctly formatted Reassociation Response frame to the test bed STA, containing<br>1. FTE with MIC, ANonce, SNonce, R1KH-ID and R0KH-ID<br>2. MDE<br>3. RSNE with PMKR1Name, RSN version set to 1, and AKM Suite Count field and AKM Suite List field exactly matching those in the recorded AP2 Beacon in step 1 | 2. In WPA3-Enterprise run, verify that the STAUT transmits a FT Request frame to AP1 where STA Address field is set to the MAC address of the STAUT, Target AP Address field is set to BSSID of testbed AP2, MDE/FTE/RSNE are present.<br><br>Verify that the STAUT transmits a correctly formatted Reassociation Request frame to the test bed AP2:<br>1. MDE/FTE/RSNE are present<br>2. AKM suite is as in Table 13<br>3. MFPC is set to 1 except in runs where CTT PMF configuration is disabled<br><br>If all the above conditions are true, then CONTINUE else FAIL |
| 7 | PING_IP_ADDRESS = IP_ADDR of Network Ping Endpoint<br><br>Configure STAUT to ping the Network Ping Endpoint<br>ping <PING_IP_ADDR>, COUNT = 10, FRAME_RATE = 1 | | | | | If ping is successful and packets are sent between AP2 and STAUT then PASS, else FAIL |
| 8 | Trigger STAUT to roam (reassociate) to the BSSID of AP1 via FT protocol | | | | SN:<br>In FT Over-the-air case, verify that the CTT AP1 transmits a correctly formatted authentication Response frame with:<br>1. FTE with ANonce, SNonce, R1KH-ID and R0KH-ID<br>2. MDE<br>3. RSNE with PMKR0Name<br>4. Authentication type = 2 (FT)<br><br>In FT Over-the-DS case: in WPA3-Enterprise run, verify that AP2 transmits an FT Response frame to STAUT where:<br>1. STA Address field is set to the MAC address of STAUT | SN:<br>In FT Over-the-air case: Verify that the STAUT transmits a correctly formatted Authentication Request frame with Authentication type = 2<br><br>In FT Over-the-DS case: Verify that the STAUT does not transmit an Authentication frame.<br>1. In WPA3-Enterprise run, verify that the STAUT transmits a FT Request frame to AP2 where STA Address field is set to the MAC address of the STAUT, Target AP Address field is set to BSSID of CTT AP1, MDE/FTE/RSNE are present. |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | 2. Target AP Address field is set to BSSID of CTT AP1<br>3. Status Code field indicates SUCCESS,<br>4. MDE/FTE/RSNE are present.<br><br>Verify that the AP1 transmits a correctly formatted Reassociation Response frame to the test bed STA, containing<br>1. FTE with MIC, ANonce, SNonce, R1KH-ID and R0KH-ID<br>2. MDE<br>3. RSNE with PMKR1Name, RSN version set to 1, and AKM Suite Count field and AKM Suite List field exactly matching those in recorded AP1 Beacon in step 1 | Verify that the STAUT transmits a correctly formatted Reassociation Request frame to the test bed AP1:<br>2. MDE/FTE /RSNE are present<br>3. AKM suite is as in Table 13<br>4. MFPC is set to 1 except in runs where CTT PMF configuration is disabled<br><br>Verify that EAP or EAPOL messages are not transmitted after the Re-Association Response frame<br><br>If all the above conditions are true, then CONTINUE else FAIL |
| 9 | PING_IP_ADDRESS = IP_ADDR of Network Ping Endpoint<br><br>Configure STAUT to ping the Network Ping Endpoint<br>ping <PING_IP_ADDR>, COUNT = 10, FRAME_RATE = 1 | | | | | For case: 9.1.1 and 9.1.1_DS, if ping is successful then CONTINUE, else FAIL<br><br>For others, if ping is successful then PASS, else FAIL. |
| 10 | Trigger STAUT to disassociate from the AP1. | | | | | SN:<br>Verify that the STAUT sends Disassociation or Deauthentication frame to AP1<br><br>If all the above conditions are true, then CONTINUE else FAIL |
| 11 | Wait 5 seconds.<br>Trigger STAUT to connect to CTT AP1 BSSID<br>The STAUT sends an Association Request to the CTT AP1. | | | | SN:<br>Verify that the CTT AP1 transmits a correctly formatted Association Response frame to STA, containing:<br>1. Fast BSS Transition IE (FTE) containing the R1KH-ID and R0KH-ID and having<br>a. MIC element count set to 0<br>b. ANonce set to 0<br>c. SNonce set to 0<br>d. MIC set to 0<br>2. MDE as advertised in the Beacon frame in step 1 | SN:<br>Verify that for STAUT:<br>1. In Authentication Request, authentication type =0 (open) (PMKSA caching).<br>2. In initial mobility domain Association Request:<br>a. MDE is present<br>b. AKM suite is as in Table 13<br>c. PMKID is present<br>d. MFPC is set to 1 except in runs where CTT PMF configuration is disabled |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | 3. If all the above conditions are true, then CONTINUE else FAIL |
| 12 | Wait for 4-way handshake to complete | | | | SN:<br>Verify that the CTT AP1 transmits message 1 containing the same PMKID as indicated by STAUT in Association Request in step 11 | SN:<br>Verify that for STAUT:<br>RSNE with PMKR1Name is present in message 2 |
| 13 | Repeat steps 5 thru 9 | | | | | Same as steps 5 -9 except step 9:<br>If ping is successful in step 9 then PASS, else FAIL |

# 10 Reserved for future Use

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.

# 11 WPA3 Server Certificate Validation STAUT test cases

## 11.1 STAUT server certificate validation test

### Objective

This test verifies that the STAUT correctly performs server certification validation during an 802.1X EAP exchange and aborts an EAP exchange when validation of the server certificate fails in each of a variety of security configurations.

This test comprises multiple runs as defined in Table 15 where different combinations of the AAA server certificate and the STAUT server certificate validation configuration are used. These runs are conditionally run depending on vendor-declared configuration capabilities in Table 1 as follows:

- If STAUT supports configuration (a) "explicitly configured server certificate", runs 1, 6, 10 and 11 are executed.
- If STAUT supports configuration (b) "server domain (FQDN) + root CA", runs 2, 7, 9 and 14 are executed.
- If STAUT supports configuration (c) "server domain suffix + root CA", runs 3 and 8 are executed.
- If STAUT supports configuration (d) "root CA only", runs 4, 13 and 15 are executed.
- If STAUT supports configuration (e) "server domain (FQDN) + root store", runs 16, 18 and 19 are executed.
- If STAUT supports configuration (f) "server domain suffix + root store", run 17 is executed.

This test is repeated for all the EAP methods listed in Table 15 that are supported by the STAUT per vendor declaration.

The vendor is required to declare support for all configuration values that the DUT is capable of supporting.

There are multiple authentication attempts within each run. If authentication fails, or times-out on the first attempt and the STAUT presents a dialog or notification to the user (for example, asking if the user accepts trust in the certificate presented by the server), any such dialogs/notifications are accepted and the second authentication attempt is made. Then, the server certificate is changed on the AAA server, to a different certificate with the same domain name but signed by a different CA with the same name (simulating an attempted attack), and the authentication steps are repeated. The expected results for each attempt depend on the configuration for that run.

### Applicability

Conditional. This test case is only required if the STAUT declared support for WPA3-Enterprise in Table 1 and supports at least one of the EAP methods listed in Table 15.

### References

IEEE 802.1X-2010 [8], IETF RFC 5216 [9]

### Test environment

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

Network Ping Endpoint: A test bed laptop that is on the same subnet and is accessible from testbed AP.

© 2020 Wi-Fi Alliance. All Rights Reserved.

### Test configuration

Table 15 defines the specific parameter values required for this test case.

**Table 15. STAUT server certificate validation 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 see Table 23 | |
| Security (AKM, PMF | WPA3-Ent Transition Mode | WPA3-Ent Transition Mode<br>AKM = 1 and 5 (802.1X, SHA-1 and SHA-256)<br>MFPC=1, MFPR=0 (PMF Capable) | |
| PMKSA caching | Disabled | Disabled | |
| User Override of Server Certificate (UOSC) | Enabled in all runs for which UOSC is supported by STAUT (per vendor capabilities declaration). | N/A | N/A |
| Network profile: | | | |
| EAP method | EAP-TLS<br>EAP-TTLS<br>EAP-PEAPv0<br>EAP-PEAPv1 | N/A | EAP-TLS<br>EAP-TTLS<br>EAP-PEAPv0<br>EAP-PEAPv1 |
| Server | See Table 16 | N/A | See Table 16 |
| Client credentials | For all runs with EAP-TTLS and EAP-PEAP: identity: wifi-user; password: test%11<br>For all runs with EAP-TLS: rsa_user1_w1_fi.pem<br>rsa_user1_cert.pem client certificate is signed by a CA that is not expected to be in the STAUT trust store out-of-box. | N/A | For all runs with EAP-TTLS and EAP-PEAP: identity: wifi-user; password: test%11 |

Table 16 defines the security configuration parameters that are specific to each run in this test case, where the following notation is used:

- ca_cert (STAUT and AAA): CA certificate
- For STAUT, ca_cert=DEFAULT indicates STAUT uses default out-of-box trust store
- server_cert_sta (STAUT): server certificate
- server_cert (AAA): server certificate
- private_key (AAA): private key of server certificate
- domain_suffix_match (STAUT): Suffix match requirement for domain name (if not configured, then wildcard match)
- domain_match (STAUT): FQDN match requirement for domain name (if not configured, then wildcard match)

### Table 16. STAUT server certificate validation test runs

| Run | Description | STAUT configuration (network profile) | AAA server configuration | <RES-INIT > | <RES-TOD1> | <RES-TOD2> |
|---|---|---|---|---|---|---|
| 1 | STAUT configured with exactly matching server certificate<br>AAA server certificate is signed by private CA<br>Validation is expected to succeed in step 3 | Configuration (a):<br>server_cert_sta= rsa_server1_w1_fi.pem | ### CONFIG 1 ###<br>ca_cert=rsa_ca1_w1_fi.pem<br>server_cert= rsa_server1_w1_fi.pem private_key=rsa_server1_w1_fi.key<br>rsa_server1_w1_fi.pem server certificate is signed by ca1.w1-fi.org, and has SubjectAltName dNSName and SubjectName CN equal to server1.w1-fi.org<br>### CONFIG 2 ###<br>ca_cert=rsa_ca1BAD_w1_fi.pem<br>server_cert= rsa_server1BAD_w1_fi.pem<br>private_key=rsa_server1BAD_w1_fi.key<br>rsa_Server1BAD_w1_fi.pem server certificate is signed by ca1BAD.w1-fi.org, and has SubjectAltName dNSName and SubjectName CN equal to server1.w1-fi.org<br>rsa_ca1_w1_fi.pem and rsa_ca1BAD_w1_fi.pem root certificates have Subject and Issuer CN equal to ca1.w1-fi.org and are not in STAUT trust store out-of-box. | SUCCESS | N/A | N/A |
| 2 | STAUT configured with matching FQDN and root cert<br>AAA server certificate is signed by private CA<br>Validation is expected to succeed in step 3 | Configuration (b):<br>ca_cert=rsa_ca1_w1_fi.pem<br>domain_match=server1.w1-fi.org | | SUCCESS | N/A | N/A |
| 3 | STAUT configured with matching FQDN-suffix and root cert<br>AAA server certificate is signed by private CA<br>Validation is expected to succeed in step 3 | Configuration (c):<br>ca_cert= rsa_ca1_w1_fi.pem<br>domain_suffix_match= w1-fi.org | | SUCCESS | N/A | N/A |
| 4 | STAUT configured with matching root cert but no FQDN<br>AAA server certificate is signed by private CA<br>Validation is expected to succeed in step 3 | Configuration (d):<br>ca_cert=rsa_ca1_w1_fi.pem | | SUCCESS | N/A | N/A |
| 6 | STAUT configured with non-matching server certificate signed by different CA to certificate presented by server<br>AAA server certificate is signed by private CA<br>Validation is expected to fail in step 3 due to untrusted CA (and non-matching server cert), and succeed in step 6 only if UOSC is enabled | Configuration (a):<br>server_cert_sta= rsa_server2_w1_fi.pem<br>server certificate is signed by ca2.w1-fi.org (different CA to ca1.w1-fi.org), and has SubjectAltName dNSName and SubjectName CN equal to server2.w1-fi.org | | FAILURE | N/A | N/A |
| 7 | STAUT configured with non-matching FQDN prefix but matching root cert<br>AAA server certificate is signed by private CA<br>Validation is expected to fail in step 3 due to non-matching domain name configuration, and succeed in step 6 only if UOSC is enabled | Configuration (b):<br>ca_cert=rsa_ca1_w1_fi.pem<br>domain_match= server2.w1-fi.org | | FAILURE | N/A | N/A |

| Run | Description | STAUT configuration (network profile) | AAA server configuration | <RES-INIT > | <RES-TOD1> | <RES-TOD2> |
|---|---|---|---|---|---|---|
| 8 | STAUT configured with non-matching FQDN suffix but matching root cert<br>AAA server certificate is signed by private CA<br>Validation is expected to fail in step 3 due to non-matching domain suffix configuration (despite trusted configured CA), and succeed in step 6 only if UOSC is enabled | Configuration (c):<br>ca_cert=rsa_ca1_w1_fi.pem<br>domain_suffix_match= w1-fi2.org | | FAILURE | N/A | N/A |
| 9 | STAUT configured with matching FQDN but non-matching root cert<br>AAA server certificate is signed by private CA<br>Validation is expected to fail in step 3 due to untrusted (non-matching) CA, and succeed in step 6 only if UOSC is enabled | Configuration (b):<br>ca_cert=rsa_ca2_w1_fi.pem<br>domain_match = server1.w1-fi.org | | FAILURE | N/A | N/A |
| 10 | STAUT configured with non-matching server certificate containing TOD-STRICT policy, signed by a different CA to the certificate presented by server but indicating the same domain name<br>AAA server certificate is signed by private CA<br>Validation is expected to fail in step 3 due to non-matching server cert, and also fail in step 6 because TOD policy in the configured certificate prevented UOSC (if enabled). In addition, TOD policy in the configured certificate prevents UOSC (if enabled) in step 9, | Configuration (a):<br>server_cert_sta= rsa_server1ALT_w1_fi.pem<br>The server certificate is signed by ca2.w1-fi.org (different CA to ca1.w1-fi.org), has SubjectAltName dNSName and SubjectName CN equal to server1.w1-fi.org, and has a Certificate Policies entry indicating the TOD-STRICT policy. | | FAILURE | TOD | TOD |
| 11 | STAUT configured with non-matching server certificate (without TOD policy).<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy.<br>Validation is expected to fail in step 3 due to untrusted (non-matching) server cert, and also fail in step 6 because TOD policy in AAA server certificate prevented UOSC, UOSC (if enabled) is not prevented in step 9 because the TOD policy was only present in the CONFIG 1 server certificate, | Configuration (a):<br>server_cert_sta= rsa_server1_w1_fi.pem | ### CONFIG 1 ###<br>ca_cert=rsa_ca2_w1_fi.pem<br>server_cert= rsa_server4_w1_fi.pem<br>private_key=rsa_server4_w1_fi.key<br>rsa_server4_w1_fi.pem server certificate is signed by ca2.w1-fi.org, has SubjectAltName dNSName and SubjectName CN equal to server4.w1-fi.org, and has a Certificate Policies entry indicating the TOD-STRICT policy | FAILURE | TOD | N/A |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| Run | Description | STAUT configuration (network profile) | AAA server configuration | <RES-INIT > | <RES-TOD1> | <RES-TOD2> |
|---|---|---|---|---|---|---|
| | and that certificate was never successfully validated | | rsa_ca2_w1_fi.pem root certificate has Subject and Issuer CN equal to ca2.w1-fi.org and is not in STAUT trust store out-of-box.<br>### CONFIG 2 ###<br>Same as CONFIG 2 above | | | |
| 13 | STAUT is configured with a non-matching root certificate (without TOD policy), and no FQDN<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy<br>Validation is expected to fail in step 3 due to untrusted (non-matching) CA, and also fail in step 6 because TOD policy in AAA server certificate prevented UOSC. UOSC (if enabled) is not prevented in step 9 because the TOD policy was only present in the CONFIG 1 server certificate, and that certificate was never successfully validated | Configuration (d):<br>ca_cert= rsa_ca1_w1_fi.pem | | FAILURE | TOD | N/A |
| 14 | STAUT configured with matching FQDN and root cert<br>AAA server certificate is signed by private CA and contains TOD-STRICT policy.<br>Validation is expected to succeed in step 3. TOD policy in the server certificate that was successfully validated in step 3 prevents UOSC (if enabled) in step 9, | Configuration (b):<br>ca_cert=rsa_ca2_w1_fi.pem<br>domain_match= server4.w1-fi.org | | SUCCESS | N/A | TOD |
| 15 | STAUT is configured with a non-matching root certificate (without TOD policy), and no FQDN<br>AAA server certificate is signed by private CA and contains TOD-TOFU policy<br>Validation is expected to fail in step 3 due to untrusted (non-matching) CA and succeed in step 6 only if UOSC is enabled. If UOSC is enabled, TOD policy in the server certificate that was successfully validated due to UOSC in step 6 prevents UOSC in step 9; if UOSC is disabled then UOSC will not occur in step 9 anyway, | Configuration (d):<br>ca_cert= rsa_ca2_w1_fi.pem | ### CONFIG 1 ###<br>ca_cert=rsa_ca1_w1_fi.pem<br>server_cert= rsa_server5_w1_fi.pem<br>private_key=rsa_server5_w1_fi.key<br>rsa_server5_w1_fi.pem server certificate is signed by ca1.w1-fi.org, and has SubjectAltName dNSName and SubjectName CN equal to server5.w1-fi.org, and has a Certificate Policies entry indicating the TOD-TOFU policy<br>### CONFIG 2 ###<br>Same as CONFIG 2 above | FAILURE | N/A | TOD |
| 16 | STAUT configured with matching FQDN<br>AAA server certificate is signed by well-known root CA<br>Validation is expected to succeed in step 3 | Configuration (e):<br>ca_cert=DEFAULT<br>domain_match=testserver.wfatestorg.org | ### CONFIG 1 ###<br>ca_cert=ca_publicca.pem<br>server_cert=testserver_wfatestorg_org.pem | SUCCESS | N/A | N/A |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| Run | Description | STAUT configuration (network profile) | AAA server configuration | <RES-INIT > | <RES-TOD1> | <RES-TOD2> |
|---|---|---|---|---|---|---|
| 17 | STAUT configured with matching FQDN-suffix<br>AAA server certificate is signed by well-known root CA<br>Validation is expected to succeed in step 3 | Configuration (f):<br>ca_cert=DEFAULT<br>domain_suffix_match=wfatestorg.org | private_key=testserver_wfatestorg_org.key<br>testserver_wfatestorg_org.pem contains a server certificate and its intermediate certificate that is signed by ca_publicca.pem, and the server certificate has SubjectAltName dNSName and SubjectName CN equal to testserver.wfatestorg.org<br>### CONFIG 2 ###<br>ca_cert=caBAD_publicca.pem<br>server_cert=testserverBAD_wfatestorg_org.pem<br>private_key=testserverBAD_wfatestorg_org.key<br>testserverBAD_wfatestorg_org.pem contains a server certificate and its intermediate certificate that is signed by caBAD_publicca.pem, and the server certificate has SubjectAltName dNSName and SubjectName CN equal to testserver.wfatestorg.org<br>ca_publicca.pem root certificate is expected to be in STAUT trust store out-of-box.<br>caBAD_publicca.pem root certificate and its intermediate certificate are privately generated (i.e. not in STAUT trust store out-of-box), and have all attributes other than Public Key (i.e. including Subject and Issuer CN) equal to the same values as those of ca_publicca.pem and its intermediate certificate, respectively | SUCCESS | N/A | N/A |
| 18 | STAUT configured with non-matching FQDN<br>AAA server certificate is signed by well-known root CA<br>Validation is expected to fail in step 3 due to non-matching domain name configuration (despite trusted CA), and succeed in step 6 only if UOSC is enabled | Configuration (e):<br>ca_cert=DEFAULT<br>domain_match=testserver2.wfatestorg.org |  | FAILURE | N/A | N/A |
| 19 | STAUT configured with non-matching FQDN suffix<br>AAA server certificate is signed by well-known root CA<br>Validation is expected to fail in step 3 due to non-matching domain name configuration (despite trusted CA), and succeed in step 6 only if UOSC is enabled | Configuration (e):<br>ca_cert=DEFAULT<br>domain_match=testserver.wfatestorg2.org |  | FAILURE | N/A | N/A |
|  |  |  |  |  |  |  |

### Test procedure and expected results

Table 17 provides the test procedure and expected results for this test case for 2.4 and 5 GHz STAUT.

**Table 17. STAUT server certificate validation 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 and configure to the general settings as specified in Table 8 and Table 16. | Reset the AP to its default configuration and configure general settings as specified | Configure the server certificate for this run on the AAA server as specified in Table 16 for CONFIG 1. |  |  |

| Step | STAUT | CTT acting as a test bed AP | AAA server | CTT validation check | Expected Result |
|---|---|---|---|---|---|
| | | in Table 3Configure the AP as per Table 16 | | | |
| 2 | Configure the STAUT to perform an active scan in the AP's operating channel (if supported). | The AP transmits a Probe Response frame. | | Verify that the AP transmits Beacon and (if the STAUT sends a Probe Request frame) Probe Response frames per the configuration in Table 16.and that MFPC and MFPR in RSNE are equal to 1. | |
| 3 | Configure the STAUT with the client security configuration as specified in Table 16 and trigger STAUT to associate with the SSID "Wi-Fi". | | | Verify that during the 802.1X EAP exchange, the AP sends a TLS server_hello message containing a certificate that matches the server certificate configured on the AAA server for CONFIG 1.<br>In runs where an intermediate certificate exists, verify that the server certificate is followed by the intermediate certificate. | For runs where <RES-INIT>==SUCCESS, if the EAP exchange successfully completes within 10 seconds, then CONTINUE, else FAIL<br>For other runs, if the STAUT does not send any TLS Application Data message and the AP does not send any EAP Success message within 10 seconds, then CONTINUE, else FAIL<br>Note. See Table 16 for the values of <RES-INIT> for each run. |
| 4 | PING_IP_ADDRESS = IP_ADDR of Network Ping Endpoint<br>Configure STAUT to ping Network Ping Endpoint<br>ping <PING__IP_ADDR>, COUNT = 3, FRAME_RATE = 1 | | | | For runs where <RES-INIT>==SUCCESS, if ping is successful then GOTO STEP 8, else FAIL<br>For other runs, if ping fails then CONTINUE, else FAIL |
| 5 | Within 10 secs since the STAUT was triggered in step 3, if UOSC is enabled then follow indicated steps to accept trust in the server certificate.<br>Note. The instructions to accept trust might include (re)entering the client credentials. | | | | For runs where <RES-TOD1>==TOD or STAUT does not support UOSC for the run's EAP credential configuration:<br>1. If a dialog or notification to accept trust was shown to user then FAIL, else GOTO STEP 8.<br>For other runs, if no dialog or notification to accept trust was |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| Step | STAUT | CTT acting as a test bed AP | AAA server | CTT validation check | Expected Result |
|---|---|---|---|---|---|
| | | | | | shown to end user then FAIL, else CONTINUE |
| 6 | STAUT autonomously continues or restarts the EAP exchange.<br>Note: For this test case, STAUT is expected to autonomously continue or restart (for example, by reassociating) the EAP exchange once the user accepts trust in a server certificate. | | | | SN:<br>If the EAP exchange successfully completes within 10 seconds then CONTINUE, else FAIL |
| 7 | PING_IP_ADDRESS = IP_ADDR of Network Ping Endpoint<br>Configure STAUT to ping Network Ping Endpoint<br>ping <PING__IP_ADDR>, COUNT = 3, FRAME_RATE = 1 | | | | If ping is successful then CONTINUE, else FAIL |
| 8 | Trigger the STAUT to deauthenticate from the AP.<br>Wait 5 secs. | | Reconfigure AAA server per Table 16 for CONFIG 2. | | |
| 9 | Trigger the STAUT (without any other reconfiguration) to associate with the SSID "Wi-Fi". | | | Verify that during the 802.1X EAP exchange, the AP sends a TLS server_hello message containing a certificate that matches the server certificate configured on the AAA server for CONFIG 2.<br>In runs where an intermediate certificate exists, verify that the server certificate is followed by the intermediate certificate. | SN:<br>If the STAUT does not send any TLS Application Data message and the AP does not send any EAP Success message within 10 seconds, then CONTINUE, else FAIL |
| 10 | PING_IP_ADDRESS = IP_ADDR of Network Ping Endpoint<br>Configure STAUT to ping Network Ping Endpoint<br>ping <PING__IP_ADDR>, COUNT = 3, FRAME_RATE = 1 | | | | If ping fails then CONTINUE, else FAIL |
| 11 | Wait 10 secs since the STAUT was triggered in step 9. | | | | For runs where <RES-TOD2>==TOD or STAUT does not support UOSC for the run's EAP credential configuration, if a |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| Step | STAUT | CTT acting as a test bed AP | AAA server | CTT validation check | Expected Result |
|---|---|---|---|---|---|
| | | | | | dialog or notification to accept trust was shown to the end user, then FAIL, else PASS<br>For other runs, if no dialog or notification to accept trust was shown to the end user then FAIL, else PASS |

## 11.2 STAUT server certificate configuration requirements test

### Objective

This test verifies that, when the STAUT is manually configured through its UI with a network profile, the STAUT does not successfully complete an 802.1X EAP exchange without performing server certificate validation.

This test is repeated for each of the runs specified in Table 15. In addition, this test is repeated for all the EAP methods listed in Table 15 for which the STAUT can be configured with a network profile through its UI per vendor declaration.

### Applicability

Conditional. This test case is only required if the STAUT declared support for WPA3-Enterprise in Table 1 and supports configuration of a network profile through its UI for at least one of the EAP methods listed in Table 18.

### References

IEEE 802.1X-2010 [8], IETF RFC 5216 [9]

### Test environment

- STAUT
- CTT acting as a test bed AP
- Wireless Sniffer
- AAA server
- Network Ping Endpoint: A test bed laptop that is on the same subnet and is accessible from the testbed AP.

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

**Table 18. STAUT server certificate validation 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 see Table 23 | |
| Security (AKM, PMF) | WPA3-Ent Transition Mode | WPA3-Ent Transition Mode | |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| Parameter | STAUT value | CTT acting as a test bed AP value | AAA server |
|---|---|---|---|
| | | AKM = 1 and 5 (802.1X, SHA-1 and SHA-256)<br>MFPC=1, MFPR=0 (PMF Capable) | |
| Network profile: | Note: Configured through STAUT's UI | | |
| EAP method | EAP-TLS<br>EAP-TTLS<br>EAP-PEAPv0<br>EAP-PEAPv1 | N/A | EAP-TLS<br>EAP-TTLS<br>EAP-PEAPv0<br>EAP-PEAPv1 |
| Server | • Run 1: Unconfigured (do not explicitly disable server validation)<br>• Run 2: Explicitly disable server validation (select "Don't validate" or similar<br>• Run 3: Configure use of system trust store only (do not explicitly disable server validation)<br>In all the above runs, do not explicitly configure a server certificate, a root CA certificate or a domain name. | N/A | ca_cert=rsa_ca1_w1_fi.pem<br>server_cert= rsa_server1_w1_fi.pem<br>private_key=rsa_server1_w1_fi.key<br>rsa_server1_w1_fi.pem server certificate is signed by rsa_ca1.w1-fi.org, and has SubjectAltName dNSName and SubjectName CN equal to server1.w1-fi.org |
| Client credentials | • For all runs with EAP-TTLS and EAP-PEAP:<br>identity: wifi-user; password: test%11<br>• For all runs with EAP-TLS: rsa_user1_cert.pem<br>rsa_user1_cert.pem client certificate is signed by a CA that is not expected to be in the STAUT trust store out-of-box. | N/A | • For all runs with EAP-TTLS and EAP-PEAP:<br>identity: wifi-user; password:test%11 |

### Test procedure and expected results

Table 19 provides the test procedure and expected results for this test case for 2.4 and 5 GHz STAUT.

**Table 19. STAUT server certificate validation test procedure and expected results**

| Step | STAUT | CTT acting as a test bed AP | AAA server | CTT validation check | Expected Result |
|---|---|---|---|---|---|
| 1 | Follow vendor instruction to reset and configure the STAUT per Table 18 for manual testing | Reset the AP to its default configuration and configure as specified in Table 3. Configure the AP as per Table 18. | Configure the server certificate for this run on the AAA server as specified in Table 18 | | |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| Step | STAUT | CTT acting as a test bed AP | AAA server | CTT validation check | Expected Result |
|---|---|---|---|---|---|
| 2 | Follow vendor instructions to configure a network profile on STAUT through its UI for the corresponding EAP method in Table 18, and trigger the STAUT to associate with the CTT AP | | | If it is possible to configure a network profile on the STAUT through its UI, then verify that:<br>during the 802.1X EAP exchange, the AP sends a TLS server_hello message containing a certificate that matches the server certificate configured on the AAA server. | If it is not possible to configure a network profile on the STAUT through its UI with the configuration in Table 18, then PASS, else CONTINUE<br>SN:<br>If the STAUT does not send any TLS Application Data message and the AP does not send any EAP Success message within 10 seconds, then PASS, else FAIL |

© 2020 Wi-Fi Alliance. All Rights Reserved.

# Appendix A 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 following ftp site: https://www.wi-fi.org/members/certifications-testing/testing-information. Contact Wi-Fi Alliance to obtain a username and password for the FTP site.

## A.2 Approved test bed equipment

This section provides the approved test bed equipment for all DUT listed in this test plan.

**Table 20. Approved test bed Access Points**

| Vendor | Product | Software version(s) | Contact |
|---|---|---|---|
| Qualcomm | CA-65-YC633-1000-WPA3 | IPQ8074.ILQ.10.1.6-00010-P-1<br>1.0 | wfa.external.support@qti.qualcomm.com |

**Table 21. Approved test bed Stations**

| Vendor | Product | Software version(s) | Contact |
|---|---|---|---|
| Intel | AX200 NGWG NV | 3.0;build:2604;commit:a3b5339;date:2019-10-02T10:16:12-07:00<br>ax200 | wfa.external.support@intel.com |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| Vendor | Product | Software version(s) | Contact |
|---|---|---|---|
| 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<br>drv=/hapd=v2.10-devel-8.1.0/sigma=framework-<br>(OpenQ-835_Android_O_WFA-FR2019-2.0-ITC-JFlash.zip) | wfa.external.support@qti.qualcomm.com |

Table 22. Approved test tools

| Vendor | Product | Software version(s) | Contact |
|---|---|---|---|
| Qualcomm | Sniffer/ CA-65-Y9345-LCT | UnKnown_4.12.0-rc6+ | support@wi-fi.org |

© 2020 Wi-Fi Alliance. All Rights Reserved.

**Table 23. Test bed assignment**

| Test Case Number | Vendor (CTT) |
|---|---|
| FT APUT test cases | |
| FT-8.1.1 | Qualcomm Android STA |
| FT-8.1.1_DS | Intel STA |
| FT-8.1.4 | Qualcomm Android STA |
| FT-8.1.4_DS | Intel STA |
| FT-8.1.5 | Qualcomm Android STA |
| FT-8.1.6 | Qualcomm Android STA |
| FT-8.1.7 | Intel STA |
| FT-8.1.8 | Qualcomm Android STA |
| FT-8.1.9 | Intel STA |
| FT-8.2.1 | Qualcomm Android STA |
| FT-8.2.1_DS | Intel STA |
| FT-8.2.4 | Qualcomm Android STA |
| FT-8.2.4_DS | Intel STA |
| FT-8.2.5 | Intel STA |
| FT-8.2.6 | Qualcomm Android STA |
| FT-8.2.7 | Intel STA |
| FT-8.2.8 | Qualcomm Android STA |
| FT-8.2.9 | Qualcomm Android STA |
| | |
| FT STAUT | |
| FT-9.1.1 | Qualcomm AP |
| FT-9.1.4 | Qualcomm AP |
| FT-9.1.4_DS | Qualcomm AP |
| FT-9.1.5 | Qualcomm AP |
| FT-9.1.6 | Qualcomm AP |

© 2020 Wi-Fi Alliance. All Rights Reserved.

| | |
|---|---|
| FT-9.1.7 | Qualcomm AP |
| FT-9.1.8 | Qualcomm AP |
| FT-9.1.9 | Qualcomm AP |
| FT-9.1.10 | Qualcomm AP |
| | |
| SCV Test Cases | |
| All SCV test cases are using Qualcomm AP as CTT | |

# Appendix B (Informative) Document revision history

Table 24. Document revision history

| Version | Date YYYY-MM-DD | Remarks |
|---|---|---|
| 1.0 | 2018-04-09 | Initial release. |
| 2.0 | 2019-12-20 | Updated to include Fast BSS Transition test cases in sections 8 and 9 and Server Certificate Validation test cases in section 11 |
| 2.1 | 2020-02-14 | Added test bed vendor software versions in Appendix A.1 |