# WPA3™
# Specification

## Version 1.0

**WI-FI ALLIANCE PROPRIETARY – SUBJECT TO CHANGE WITHOUT NOTICE**

This document may be used with the permission of Wi-Fi Alliance under the terms set forth herein.

By your use of the document, you are agreeing to these terms. Unless this document is clearly designated as an approved specification, this document is a work in process and is not an approved Wi-Fi Alliance specification. This document is subject to revision or removal at any time without notice. Information contained in this document may be used at your sole risk. Wi-Fi Alliance assumes no responsibility for errors or omissions in this document. This copyright permission does not constitute an endorsement of the products or services. Wi-Fi Alliance trademarks and certification marks may not be used unless specifically allowed by Wi-Fi Alliance.

Wi-Fi Alliance has not conducted an independent intellectual property rights ("IPR") review of this document and the information contained herein, and makes no representations or warranties regarding IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions.

Wi-Fi Alliance owns the copyright in this document and reserves all rights therein. A user of this document may duplicate and distribute copies of the document in connection with the authorized uses described herein, 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. Unauthorized use, duplication, or distribution is an infringement of Wi-Fi Alliance's copyright.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY WI-FI ALLIANCE AND WI-FI ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF THIS DOCUMENT AND ANY INFORMATION CONTAINED IN THIS DOCUMENT.

# Document revision history

| Version | Date YYYY-MM-DD | Remarks |
|---|---|---|
| 1.0 | 2018-04-09 | Initial release. |

# Table of contents

# List of tables

# 1 Introduction

This document is the technical specification for the Wi-Fi CERTIFIED WPA3™ certification program and defines a subset of functionality for WPA3 devices that achieve Wi-Fi CERTIFIED WPA3 certification. Only devices that complete the certification program test requirements for Wi-Fi CERTIFIED WPA3 shall be designated as Wi-Fi CERTIFIED WPA3.

## 1.1 Scope

The content of this specification addresses the solution requirements for the following feature modes:

- WPA3™-SAE Mode
- WPA3-SAE Transition Mode
- WPA3™-Enterprise 192-bit Mode

## 1.2 References

Knowledge of the documents listed in this section is required for understanding this technical specification. If a reference 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, then the latest version of the document is required. In the event of a conflict between this specification and the following referenced documents, the contents of this specification take precedence.

[1] IEEE Standard for Information Technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2016.

## 1.3 Definitions and acronyms

### 1.3.1 Shall/should/may/might word usage

The words shall, should, and may are used intentionally throughout this document to identify the requirements for the WPA3 program. The words can and might shall not be used to define requirements.

The word *shall* indicates a mandatory requirement. All mandatory requirements must be implemented to assure interoperability with other WPA3 products.

The word *should* denotes a recommended approach or action.

The word *may* indicates a permitted approach or action with no implied preference.

The words *might* and *can* indicate a possibility or suggestion and should be used sparingly.

### 1.3.2 Conventions

The ordering of bits and bytes in the fields within information elements, attributes and action frames shall follow the conventions in Section 8.2.2 of IEEE Standard 802.11-2016 [1] unless otherwise stated.

The word *ignored* shall be used to describe bits, bytes, fields or parameters whose values are not verified by the recipient.

The word *reserved* shall be used to describe objects (bits, bytes, or fields or their assigned values) whose usage and interpretation will be defined in the future by this specification or by other technical specifications/bulletins. A reserved object shall be set to zero unless otherwise stated. The recipient of a reserved object shall ignore its value unless that object becomes defined at a later date. The sender of an object defined by this technical specification shall not use a reserved code value.

### 1.3.3 Definitions

There are no special definitions in this specification.

### 1.3.4 Abbreviations and acronyms

Table 1 defines the acronyms used throughout this document. Some acronyms 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 1. Abbreviations and acronyms**

| Acronyms | Definition |
|---|---|
| BSS | Basic service set |
| MFPC | Management frame protection capable |
| MFPR | Management frame protection required |
| PMF | Protected Management Frame |
| PSK | Preshared key |
| RSN | Robust Security Network |
| RSNE | RSN element |
| SAE | Simultaneous Authentication of Equals |
| SSID | Service set identifier |
| WPA2™-PSK | Wi-Fi Protected Access® 2-Preshared Key |
| WPA3™-SAE | Wi-Fi Protected Access® 3-SAE |
| WPA3™-Enterprise | Wi-Fi Protected Access® 3-Enterprise |

# 2 WPA3-SAE

WPA3-SAE applies to personal network settings.

## 2.1 Modes of operation

### 2.1.1 WPA3-SAE Mode

- When a BSS is configured in WPA3-SAE Mode, PMF shall be set to required (MFPR bit in the RSN Capabilities field shall be set to 1 in the RSNE transmitted by the AP)
- A WPA3-SAE STA shall negotiate PMF when associating to an AP using WPA3-SAE Mode

### 2.1.2 WPA3-SAE Transition Mode

- When WPA2-PSK and WPA3-SAE are configured on the same BSS (mixed mode), PMF shall be set to capable (MFPC bit shall be set to 1, and MFPR bit shall be set to 0 in the RSN Capabilities field in the RSNE transmitted by the AP)
- When WPA2-PSK and WPA3-SAE are configured on the same BSS (mixed mode), the AP shall reject an association for SAE if PMF is not negotiated for that association
- A WPA3-SAE STA shall negotiate PMF when associating to an AP using WPA3-SAE Transition Mode

# 3 WPA3-Enterprise 192-bit Mode

WPA3-Enterprise 192-bit Mode may be deployed in sensitive enterprise environments to further protect Wi-Fi networks with higher security requirements such as government, defense, and industrial.

## 3.1 WPA3-Enterprise 192-bit Mode requirements

1. When WPA3-Enterprise 192-bit Mode is used by an AP, PMF shall be set to required (MFPR bit in the RSN Capabilities field shall be set to 1 in the RSNE transmitted by the AP).
2. When WPA3-Enterprise 192-bit Mode is used by a STA, PMF shall be set to required (MFPR bit in the RSN Capabilities field shall be set to 1 in the RSNE transmitted by the STA).
3. Permitted EAP cipher suites for use with WPA3-Enterprise 192-bit Mode are:
   - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

     - ECDHE and ECDSA using the 384-bit prime modulus curve P-384
   - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

     - ECDHE using the 384-bit prime modulus curve P-384

     - RSA ≥ 3072-bit modulus
   - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

     - RSA ≥ 3072-bit modulus

     - DHE ≥ 3072-bit modulus