WPA3™ Specification

Version 2.0

WI-FI ALLIANCE PROPRIETARY – SUBJECT TO CHANGE WITHOUT NOTICE

By your use of the document and any information contained herein, you are agreeing to these terms. If you do not agree to these terms, you may not use this document or any information contained herein. 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. You may need to obtain licenses from third parties before using the information contained in this document for any purpose.

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.

If you provide comments, feedback, suggestions or other ideas to Wi-Fi Alliance related to the subject matter of this document, unless otherwise agreed to in writing by Wi-Fi Alliance, you agree that such comments, feedback, suggestions and other ideas are not confidential and that Wi-Fi Alliance may freely use such comments, feedback, suggestions or other ideas without providing any additional consideration to you.

These terms are governed by the laws of the state of California, U.S., without regard to any conflict of laws principles. In the event of any dispute under these terms, you agree to resolve such dispute by binding arbitration in English pursuant to the Rules of Arbitration of the International Chamber of Commerce in San Francisco, California, U.S.

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.
2.0	2019-12-20	Updated to include Fast BSS Transition, Server Certificate Validation, WPA3-Personal only and transition mode definition, WPA3-Enterprise only and transition mode definition

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-Personal only Mode
- WPA3-Personal transition Mode
- WPA3-Enterprise only Mode
- WPA3-Enterprise transition Mode
- WPA3-Enterprise 192-bit Mode
- WPA3 Fast BSS Transition
- WPA3-Enterprise Server Certificate Validation

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

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
AKM	Authentication and Key Management
BSS	Basic service set
CN	Common Name
EAP	Extensible Authentication Protocol
FQDN	Fully qualified domain name
FT	Fast BSS transition
MFPC	Management frame protection capable
MFPR	Management frame protection required
OID	Object Identifier
PMF	Protected Management Frame
PSK	Preshared key
RSN	Robust Security Network
RSNE	RSN element
SAE	Simultaneous Authentication of Equals
SSID	Service set identifier
TOD	Trust Override Disable
TOFU	Trust-On-First-Use
UOSC	User Override of Server Certificate
WPA3	Wi-Fi Protected Access® 3

2 WPA3-Personal

WPA3-Personal applies to personal network settings.

2.1 Modes of operation

WPA3-Personal modes are defined as follows:

- WPA3-Personal only Mode
- WPA3-Personal transition Mode

2.2 WPA3-Personal only Mode

When operating in WPA3-Personal only Mode:

1. An AP shall enable at least AKM suite selector 00-0F-AC:8 in the BSS
2. A STA shall allow at least AKM suite selector 00-0F-AC:8 to be selected for an association
3. An AP shall not enable AKM suite selector: 00-0F-AC:2, 00-0F-AC:6
4. A STA shall not allow AKM suite selector: 00-0F-AC:2, 00-0F-AC:6 to be selected for an association
5. An AP shall set MFPC to 1, MFPR to 1
6. A STA shall set MFPC to 1, MFPR to 1
7. A STA shall not enable WEP and TKIP

2.3 WPA3-Personal transition Mode

When operating in WPA3-Personal transition Mode:

1. An AP shall enable at least AKM suite selectors 00-0F-AC:2 and 00-0F-AC:8 in the BSS
2. A STA shall allow at least AKM suite selectors 00-0F-AC:2 and 00-0F-AC:8 to be selected for an association
3. An AP should enable AKM suite selector: 00-0F-AC:6
4. A STA should allow AKM suite selector: 00-0F-AC:6 to be selected for an association
5. An AP shall set MFPC to 1, MFPR to 0
6. A STA shall set MFPC to 1, MFPR to 0
7. An AP shall reject an association for SAE if PMF is not negotiated for that association
8. A STA shall negotiate PMF when associating to an AP using SAE

2.4 Additional Requirements on WPA3-Personal Modes

The following additional requirements apply to all WPA3-Personal Modes:

1. An AP shall not enable WPA version 1 on the same BSS with WPA3-Personal
2. An AP shall not enable WEP and TKIP on the same BSS as WPA3-Personal
3. When connecting to an AP that supports both SAE and PSK, a STA shall connect using SAE
4. On an AP, whenever any PSK AKM (00-0F-AC:2 or 00-0F-AC:6) is enabled, the WPA3-Personal Transition Mode shall be enabled by default, unless explicitly overridden by the administrator to operate in WPA2-Personal only Mode

3 WPA3-Enterprise

WPA3-Enterprise applies to enterprise network settings.

3.1 Modes of operation

WPA3-Enterprise modes are defined as follows:

- WPA3-Enterprise only Mode
- WPA3-Enterprise transition Mode
- WPA3-Enterprise 192-bit Mode

3.2 WPA3-Enterprise only Mode

- When a BSS is configured in WPA3-Enterprise only 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-Enterprise STA shall negotiate PMF when associating to an AP using WPA3-Enterprise only mode

3.3 WPA3-Enterprise transition Mode

- When WPA2-Enterprise and WPA3-Enterprise transition Mode are configured on the same BSS (mixed mode), PMF shall be set to capable (MFPC bit shall be set to 1, and MFPR bit is by default set to 0 in the RSN Capabilities field in the RSNE transmitted by the AP)
- A WPA3-Enterprise STA shall negotiate PMF when associating to an AP using WPA3-Enterprise transition mode

3.4 Additional Requirements on WPA3-Enterprise Modes

The following additional requirements apply to all WPA3-Enterprise Modes:

1. An AP shall not enable WPA version 1 on the same BSS with WPA3-Enterprise
2. An AP shall not enable WEP and TKIP on the same BSS as WPA3-Enterprise

3.5 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.

When operating in WPA3-Enterprise 192-bit Mode:

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

4 WPA3 Fast BSS Transition

The content of this section addresses the Fast BSS Transition requirements for the following feature modes:

- Fast BSS Transition for WPA3-Personal transition Mode
- Fast BSS Transition for WPA3-Enterprise transition Mode
- Fast BSS Transition for WPA3-Personal only Mode
- Fast BSS Transition for WPA3-Enterprise only Mode

4.1 STA AKM preference order

When a WPA3 STA needs to choose between multiple AKMs on a BSS, the STA shall select the AKM in priority order from the applicable list in the subclauses below. AKM selections not listed are out of scope of this specification.

4.1.1 Personal Modes

1. FT Authentication using SAE 00-0F-AC:9
2. SAE Authentication 00-0F-AC:8
3. FT Authentication using PSK 00-0F-AC:4
4. PSK using SHA-256 00-0F-AC:6
5. PSK 00-0F-AC:2

4.1.2 Enterprise Modes

1. FT Authentication using IEEE Std 802.1X (SHA 256) 00-0F-AC:3
2. Authentication using IEEE Std 802.1X (SHA256) 00-0F-AC:5
3. Authentication using IEEE Std 802.1X 00-0F-AC:1

5 Server Certificate Validation

5.1 Failure Conditions for Server Certificate Validation

A WPA3 STA shall perform server certificate validation when using EAP-TTLS, EAP-TLS, EAP-PEAPv0 or EAP-PEAPv1 EAP methods.

A WPA3 STA shall, when performing an EAP exchange with one of the above EAP methods, determine that server certificate validation has failed if none of the following are true:

1. The STA is configured with EAP credentials that include a server certificate that is exactly equal to the certificate in the received Server Certificate message.
2. The STA is configured with EAP credentials that explicitly specify a CA root certificate that matches the root certificate in the received Server Certificate message and, if the EAP credentials also include a domain name (FQDN or suffix-only), it matches the domain name (SubjectAltName dNSName if present, otherwise SubjectName CN) of the certificate [2] in the received Server Certificate message.
3. The STA is configured with EAP credentials that include a domain name (FQDN or suffix-only) that matches the domain name (SubjectAltName dNSName if present, otherwise SubjectName CN) of the certificate [2] in the received Server Certificate message, and the root certificate of that certificate is present in the STA's trust root store.

The standards that define each EAP method specify additional conditions under which server certificate validation is required to fail, e.g. see Section 5.3 of [2].

If a WPA3 STA's validation of a server certificate fails during an EAP exchange with EAP-TTLS, EAP-PEAPv0 or EAP-PEAPv1, the STA shall not enter into Phase 2 of the EAP exchange.

5.2 Support for User Override of Server Certificate

A WPA3 STA may support User Override of Server Certificate (UOSC) for a given EAP credential configuration. If UOSC is supported and enabled for a given EAP credential configuration then, if the STA's validation of a server certificate received in the Server Certificate message of an EAP exchange for that configuration fails and UOSC is not disabled for the EAP exchange by TOD policy (see below), the STA provides a means (e.g. dialog/notification UI) by which a user can accept trust in that certificate. If the user accepts trust in UOSC, the STA configures its EAP credentials such that validation of the server certificate succeeds, and automatically continues or reattempts the EAP exchange. If UOSC is disabled (by TOD policy or otherwise) or not supported for a given EAP credential configuration, the STA does not provide such means of user override of server certificate validation.

A WPA3 STA that supports UOSC shall support the Trust Override Disable (TOD) policies. TOD policies provide the network operator with a means to disable UOSC for certain networks with stronger security requirements; this makes it harder for users to configure untrusted server credentials for those networks. A TOD policy is indicated in the Certificate Policies extension of an X.509 v3 server certificate by including exactly one of the defined OIDs.

Two TOD policies, TOD-STRICT and TOD-TOFU, are defined with OIDs as follows:

- TOD-STRICT: "1.3.6.1.4.1.40808.1.3.1"
- TOD-TOFU: "1.3.6.1.4.1.40808.1.3.2"

5.3 Criteria to disable UOSC

5.3.1 TOD Policies

The WPA3 STA shall disable UOSC in an EAP exchange if any of the following are true:

1. The STA is using configured EAP credentials for the EAP exchange that were previously used to successfully validate a server certificate, and the server certificate that was most recently successfully validated using those credentials included the TOD-STRICT or TOD-TOFU policy OID.

2. The STA is using configured EAP credentials for the EAP exchange that include an explicitly configured server certificate, and that configured certificate includes the TOD-STRICT or TOD-TOFU policy OID.
3. The certificate in the received Server Certificate message contains the TOD-STRICT policy OID.

In the first two conditions above, the STA typically selects the EAP credential configuration (aka network profile) to be used for the EAP exchange based on the network SSID or Interworking parameters (e.g. Home Realm, Roaming Consortium). The two conditions above apply to the selected configured EAP credentials irrespective of the values of the attributes in the received Server Certificate message (e.g. irrespective of whether or not the dNSName or CN matches a domain name specified in the selected EAP credentials).

All three conditions above apply to the TOD-STRICT policy. Therefore, the TOD-STRICT policy disallows UOSC in all EAP exchanges with the network, including first-use connection to that network. This policy might, for example, be used to help enforce user behavior to obtain EAP credentials via a trusted out-of-band mechanism.

Only the first two conditions above apply to the TOD-TOFU policy. Therefore, the TOD-TOFU policy does not disallow UOSC in scenarios where neither of those two conditions apply, such as first-use connection to a network without pre-configured credentials. This policy might, for example, be used to allow UOSC for Trust-On-First-Use (TOFU), while helping avoid users inadvertently accepting trust via UOSC in an adversary's certificate in subsequent connections to the network.

5.3.2 Additional Consideration on TOD Policies

STA implementations may differ in terms of how EAP credentials are configured when trust in a server certificate is accepted by the user by UOSC. This may impact whether or not those configured credentials will successfully validate the server at some future time once its certificate has been renewed by the network operator. If the renewed certificate is not successfully validated, the TOD policy in the original server certificate would disallow UOSC in that renewed certificate. Therefore, the configured EAP credentials would need to be updated manually or by other out-of-band means or deleted (at which point TOD policy would no longer apply) and reconfigured by UOSC.

Unless the STA is a-priori configured with EAP credentials that include an explicitly configured server certificate with TOD policy (per condition (2) in section 5.3.1), none of the conditions in section 5.3.1 will apply in the event that an adversary attacks an EAP exchange on first-use connection to a network; hence the STA might allow UOSC of the adversary's server certificate in such first-use connection scenario unless UOSC is disabled by other means.

A TOD policy does not imply any restrictions with regard to deletion of configured EAP credentials (network profiles) for which the TOD policy applies, nor to the modification of such network profiles with EAP credentials obtained by out-of-band mechanisms (e.g. mobile device management, manual configuration). It is assumed that the EAP credentials configured using such mechanisms are obtained from a trusted source such as the network operator.

Appendix A Examples of recommended warning dialog messages in Server Certificate Validation

If a STA allows the user to accept trust in a server certificate that has failed validation (UOSC), it is recommended that the STA strongly warns the user of the potential security consequences of doing so. The following are examples of recommended warning dialog / notification messages corresponding to some validation failure scenarios:

- Untrusted root CA: Warning: Attackers might be trying to steal your information (for example, passwords, messages, or credit cards). Authentication of the Wi-Fi® network "Wi-Fi" failed because the Certificate Authority that signed the network's certificate is not trusted by this device. Do not accept trust in this network unless you have verified the certificate's SHA-1 fingerprint "4e 7d e4 cd e8 5f 32 60 d6 fc 32 4d 0d 30 07 f7 bd 2d 14 17" presented by the network with your network administrator or service provider.
- Trusted root CA but host name mismatch: Warning: Attackers might be trying to steal your information (for example, passwords, messages, or credit cards). Authentication of the Wi-Fi network "Wi-Fi" failed because the host name configured on this device does not match the host name presented by the network. Do not accept trust in this network unless you have verified the host name "server1.wi_fi" presented by the network with your network administrator or service provider.
- Trusted public root CA (in trust store) but no host name configuration: Warning: Attackers might be trying to steal your information (for example, passwords, messages, or credit cards). Authentication of the Wi-Fi network "Wi-Fi" failed because this device is not configured with a host name for the network. Do not accept trust in this network unless you have verified the host name "server.operator.org" presented by the network with your network administrator or service provider.