Opportunistic Wireless Encryption Specification

Version 1.1

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.
1.1	2020-11-21	Clarification on PTK calculation in section 2.1

Table of contents

List of tables

1 Introduction

This document is the technical specification for Wi-Fi CERTIFIED Enhanced Open™, the Wi-Fi Alliance certification program for Opportunistic Wireless Encryption (OWE).

Whether home use, commercial, guest access/captive portal or device onboarding, the use of open unencrypted wireless networks presents a huge security risk from passive packet capture and sniffing. The purpose of OWE is to mitigate attacks on open unencrypted wireless networks that present significant security threats to users.

1.1 Scope

This specification, along with [1] and [2], define the feature requirements for OWE devices.

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.

[2] IETF RFC 8110, Opportunistic Wireless Encryption, March 2017, https://tools.ietf.org/html/rfc8110.

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 OWE 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 OWE 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

The definitions listed in Table 1 are applicable to this specification.

Table 1. Definitions

Term	Definition
OWE AP	An AP that implements the OWE protocol defined in [2]
OWE STA	A STA that implements the OWE protocol defined in [2]

1.3.4 Abbreviations and acronyms

Table 2 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 2. Abbreviations and acronyms

Acronyms	Definition
BSS	Basic service set
OWE	Opportunistic Wireless Encryption
MFPC	Management frame protection capable
MFPR	Management frame protection required
PMF	Protected Management Frame
RSN	Robust Security Network
RSNE	RSN element
SSID	Service set identifier

2 Opportunistic Wireless Encryption

2.1 OWE requirements

This section describes the specific requirements for OWE.

- When OWE is used by an AP, Protected Management Frame (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)
- When OWE 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)
- OWE PTK derivation shall use the key derivation type defined in IEEE Std 802.11-2016, subclause 12.7.1.7.2 [1]

2.2 OWE Transition Mode support

OWE Transition Mode enables a seamless transition from Open unencrypted WLANs to OWE WLANs without adversely impacting the end user experience.

An OWE AP implementation should provide the ability for OWE STAs and non-OWE STAs to connect to the same distribution system simultaneously. This is referred to as OWE Transition Mode.

All OWE STAs shall connect to an OWE AP operating in OWE Transition Mode using OWE with the procedure defined in [2].

When OWE penetration has reached a sufficient level, it is recommended that Open and the OWE Transition Mode be deprecated and at that time the method of unauthenticated wireless access shall be OWE per RFC 8110 [2]. The time between the current implementation of OWE Transition Mode and the deprecation of OWE Transition Mode is referred to as the Transition Period.

2.2.1 OWE Transition Mode requirements

1. An OWE AP device that supports the OWE Transition Mode shall support more than one BSS.
2. An OWE AP shall use two different SSIDs, one for OWE and one for Open. Both BSSs shall be advertised in their respective Beacon frames. Both SSIDs shall either operate in the same band and channel, or the OWE Transition Mode element as defined in section 2.3.1 shall include the band and channel information of the other SSID.
3. The Open BSS shall include support for Open in all Beacon and Probe Response frames and shall include a OWE Transition Mode element to encapsulate the BSSID and SSID of the OWE BSS.
4. The OWE BSS shall include the OWE Transition Mode element in all Beacon and Probe Response frames to encapsulate the BSSID and SSID of the Open BSS.
5. Beacon frames from the OWE BSS shall have a zero length SSID and the RSNE shall indicate support for OWE [2].
6. An OWE STA shall only display to the user in the list of available networks the SSID of the Open BSS of an OWE AP operating in OWE Transition Mode, and shall suppress the display of the OWE BSS SSID of that OWE AP. An OWE STA shall only associate with the OWE BSS of an OWE AP in OWE Transition Mode and shall associate using the procedure defined in [2].
7. An AP in OWE Transition Mode that receives an Association Request frame on its OWE BSS shall process it and respond using the procedure defined in [2].
8. No additional AP management user interface is needed to support OWE Transition Mode; however, one may be provided per vendor discretion.
9. An AP supporting OWE Transition Mode shall automatically enter OWE Transition Mode when an Open SSID is provisioned. At instantiation, the SSID for the OWE BSS shall be selected in a manner that ensures the OWE SSID is unique among networks within radio range of the AP in OWE Transition Mode. The non-security operating characteristics of the OWE BSS should be identical to those of the corresponding Open BSS.

10. After the Transition Period, it is recommended that a single OWE BSS be used, and that the SSID of that single OWE BSS be the SSID name of the no longer used corresponding Open BSS. An OWE AP shall also support OWE per [2] and allow for separate provisioning of OWE without an accompanying Open BSS.

    Note: An OWE STA's network profile matching algorithm should recognize the post-Transition Period time. During the Transition Period, the open and paired OWE network names may be stored. When only an OWE network with the indicated open name is present, the STA connects using OWE to the advertised OWE network.

11. An AP operating in OWE Transition Mode may bridge broadcast or multicast traffic between the Open and OWE BSSs, for example to support discovery of devices while in OWE Transition Mode. Support of such bridging is determined by the vendor implementation.
12. An AP in OWE Transition Mode shall instantiate both the OWE and Open SSIDs with the same operating policies. For example, if client isolation is enabled on one of the SSIDs, it shall be enabled on the other SSID as well; if broadcast or multicast traffic is disabled on one SSID, it shall be disabled on the other.

2.3 Elements, attributes and frame formats

2.3.1 OWE Transition Mode element definition

The Vendor Specific element format (as defined in section 9.4.2.26 of [1]) is used to define the OWE Transition Mode element in this specification. The format of the OWE Transition Mode element is shown in Table 3.

Table 3. OWE Transition Mode element format

Field	Size (octets)	Value (Hex)	Description
Element ID	1	0xDD	IEEE 802.11 Vendor Specific element. A one octet field set to the value 221 (0xDD) [1]
Length	1	Variable	Length of the following fields in the element in octets. The Length field is variable, and set to 4 plus the total length of the OWE Transition Mode fields. [1].
Organizationally unique identifier	3	0x 50 6F 9A	The Wi-Fi Alliance specific OUI (refer to section 9.4.1.32 of [1])
Organization Identifier (OI) Type	1	0x1C	Value assigned by Wi-Fi Alliance
BSSID	6	Variable	Contains the BSSID of the other virtual AP. which is the Open BSSID for the OWE BSS and the OWE BSSID for the Open BSS.
SSID Length	1	Variable	The length, in octets, of the SSID field which indicates the SSID of the other virtual AP.
SSID	Variable	Variable	SSID of the other virtual AP
Band Info	1	Variable	Contains the Global Operating Class number of the other virtual AP. It is present when the two SSIDs operate in a different band/channel.
Channel Info	1	Variable	Contains the operating channel number of the other virtual AP. It is present when the two SSIDs operate in a different band/channel.

Band Info and Channel Info are optional fields. If configured, both fields shall be included in an OWE Transition Mode element. OWE Transition Mode Band Info and Channel Info field combinations:

- Both Band Info and Channel Info fields are not present
- Both Band Info and Channel Info fields are present

Other combinations of Band Info and Channel Info fields are not valid.