WPA3™
Specification
Version 3.4

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
3.0	2020-12-14	Update to include SAE-PK, WIFI URI, Transition Disable indication, and Privacy Extension mechanisms
3.1	2022-11-23	Update to Transition Disable indication section to clarify the use of the mechanism and to add a requirement prohibiting an AP from enabling Transition Disable indication by default.
3.2	2023-12-18	Updates to STA AKM Preference Order, updates to Modes of operation for WPA3-Personal and WPA3-Enterprise, updates to Transition Disable Indication for AKM 24 and AKM 25, updates to Authentication using SAE-PK for AKM 24 and AKM 25 and added section for MLD Security.
3.3	2024-02-16	Updates to add section on AKM Constraints on Wi-Fi Alliance Generational PHYs and Bands, and clarify various requirements and terminology
3.4	2024-10-30	Add a section to define RSN overriding and describe WPA3-Personal Compatibility Mode

Table of contents

List of tables

1 Introduction

This document is the 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 WPA3 features.

Additional recommendations and guidance for deployment of WPA3 networks and implementation of WPA3 devices can be found in [12].

1.2 References

Knowledge of the documents listed in this section is required for understanding this 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, 2020

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

[3] IETF RFC 3972, Cryptographically Generated Addresses (CGA), https://tools.ietf.org/html/rfc3972

[4] NIST SP 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-89.pdf

[5] NIST SP 800-107 Revision 1, Recommendations for Applications using Approved Hash Functions, https://csrc.nist.gov/publications/detail/sp/800-107/rev-1/final

[6] IETF RFC 4648, The Base16, Base32 and Base64 Data Encodings, https://tools.ietf.org/html/rfc4648

[7] IETF RFC 3986, Uniform Resource Identifier (URI): Generic Syntax, https://tools.ietf.org/html/rfc3986

[8] IETF RFC 5480, ECC SubjectPublicKeyInfo Format, https://tools.ietf.org/html/rfc5480

[9] IETF RFC 3279, Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, https://tools.ietf.org/html/rfc3279

[10] IETF RFC 7664, Dragonfly https://tools.ietf.org/html/rfc7664

[11] Verhoeff, J, "Error Detecting Decimal Codes", Mathematisch Centrum

[12] WPA3 and Wi-Fi Enhanced Open Deployment and Implementation Guide, <REF>

[13] IEEE 802.11-2020, Amendment 1: Enhancements for High-Efficiency WLAN, 2021 (IEEE Std. 802.11ax-2021)

[14] IEEE P802.11-REVme/D7.0, https://standards.ieee.org/ieee/802.11/10548/

[15] IEEE P802.11be/D7.0, https://standards.ieee.org/ieee/802.11be/7516/

[16] Wi-Fi Alliance Opportunistic Wireless Encryption Specification Version 1.1, https://www.wi-fi.org/file/opportunistic-wireless-encryption-specification

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 9.2.2 of IEEE Standard 802.11 [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 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 specification shall not use a reserved code value.

1.3.3 Definitions

Term	Definition
BSS Configuration	The collection of credentials and allowed security parameters that are configured on an AP for a specific BSS. NOTE: For a (Wi-Fi 7) AP MLD, each affiliated 802.11 AP (link) has its own BSS Configuration. However, certain security parameters must be allowed across the BSS Configurations of all affiliated 802.11 APs (links) of the AP MLD, since they apply at the MLD level.
Network Profile	The collection of credentials and allowed security parameters for a particular network name (SSID) that a STA uses when connecting to any AP in that network.
Wi-Fi Enhanced Open Only Mode	AP: operating a BSS configured to support Wi-Fi Enhanced Open connections but not using Wi-Fi Enhanced Open Transition Mode to support (legacy) Open System authentication connections STA: configured to connect to BSSs in a given network using Wi-Fi Enhanced Open but not using (legacy) Open System authentication
Wi-Fi Enhanced Open Transition Mode	AP: operating multiple BSSs (using OWE SSID and Open SSID, advertised in OWE Transition Mode element) configured to support Wi-Fi Enhanced Open and non Wi-Fi Enhanced Open STAs to connect to the same distribution system simultaneously STA: configured to connect to BSSs in a given network using either Wi-Fi Enhanced Open or, if an AP does not support Wi-Fi Enhanced Open, (legacy) Open System authentication
WPA3-Enterprise 192-bit Mode	AP: operating a BSS configured to support WPA3-Enterprise 192-bit connections, but not support WPA3-Enterprise without 192-bit or WPA2-Enterprise connections

Term	Definition
	STA: configured to connect to BSSs in a given network (SSID) using WPA3-Enterprise 192-bit mode, but not WPA3-Enterprise without 192-bit or WPA2-Enterprise
WPA3-Enterprise Only Mode	AP: operating a BSS configured to support WPA3-Enterprise connections but not support WPA2-Enterprise connections STA: configured to connect to BSSs in a given network (SSID) using WPA3-Enterprise but not WPA2-Enterprise
WPA3-Enterprise Transition Mode	AP: operating a BSS configured to support WPA3-Enterprise and WPA2-Enterprise connections simultaneously STA: configured to connect to BSSs in a given network (SSID) using WPA3-Enterprise or, if the BSS does not support WPA3-Enterprise, WPA2-Enterprise
WPA3-Personal Compatibility Mode	AP: operating a BSS configured to support WPA3-Personal and WPA2-Personal connections simultaneously, using RSN overriding signaling as defined in 2.4 to avoid interoperability issues with some legacy STAs STA: N/A
WPA3-Personal Only Mode	AP: operating a BSS configured to support WPA3-Personal connections but not support WPA2-Personal connections STA: configured to connect to BSSs in a given network (SSID) using WPA3-Personal but not WPA2-Personal
WPA3-Personal SAE-PK Mode	AP: operating a BSS configured to support WPA3-Personal with SAE-PK and WPA3-Personal without SAE-PK connections simultaneously, but not support WPA2-Personal connections STA: configured to connect to BSSs in a given network (SSID) using WPA3-Personal with SAE-PK (or, if the BSS does not support SAE-PK, without SAE-PK if allowed by local policy), but not WPA2-Personal
WPA3-Personal Transition Mode	AP: operating a BSS configured to support WPA3-Personal and WPA2-Personal connections simultaneously STA: configured to connect to BSSs in a given network (SSID) using WPA3-Personal or, if the BSS does not support WPA3-Personal, WPA2-Personal
WPA3 STA	A STA capable of operating in WPA3-Personal and/or WPA3-Enterprise modes NOTE: A (Wi-Fi 7) STA that supports EHT and MLO can operate as an (IEEE 802.11) non-AP MLD [15]. In IEEE 802.11 terminology, a non-AP MLD has one or more affiliated "non-AP STAs". However, in the context of EHT and MLO operation, the usage of "STA" in this document refers to the non-AP MLD including its affiliated non-AP STAs (not only to the affiliated non-AP STA(s)), unless otherwise stated.

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
ANQP	Access Network Query Protocol

Acronyms	Definition
BSS	Basic Service Set
CN	Common Name
EAP	Extensible Authentication Protocol
EHT	Extremely High Throughput (Wi-Fi 7 PHY/MAC)
ESS	Extended Service Set
FILS	Fast Initial Link Setup
FQDN	Fully Qualified Domain Name
FT	Fast BSS Transition
GAS	Generic Advertisement Service
MFPC	Management Frame Protection Capable
MFPR	Management Frame Protection Required
MLD	Multi-Link Device (Wi-Fi 7)
MLO	Multi-Link Operation (Wi-Fi 7)
OCV	Operating Channel Validation
OID	Object Identifier
PMF	Protected Management Frames
PSK	Preshared Key
RSN	Robust Security Network
RSNE	RSN element
SAE	Simultaneous Authentication of Equals
SAE-PK	SAE Public Key
SSID	Service Set Identifier
TOD	Trust Override Disable
TOFU	Trust-On-First-Use
UOSC	User Override of Server Certificate
URI	Uniform Resource Identifier
WPA3	Wi-Fi Protected Access® 3

2 Requirements on Configuration and Operation of WPA3-Personal

WPA3-Personal applies to personal network settings.

2.1 Modes of operation

WPA3-Personal modes are enumerated as follows:

- WPA3-Personal Only Mode
- WPA3-Personal Transition Mode
- WPA3-Personal Compatibility Mode
- WPA3-Personal SAE-PK Only Mode (see section 6)
- WPA3-Personal SAE-PK Transition Mode (see section 6)

2.2 WPA3-Personal Only Mode

When an AP's BSS is operating in WPA3-Personal Only Mode:

1. The AP's BSS Configuration shall enable at least one of the following AKMs:
    a. AKM suite selector 00-0F-AC:8 (SAE)
    b. AKM suite selector 00-0F-AC:24 (SAE using group-dependent hash)

    If the AP's BSS Configuration enables AKM suite selector 00-0F-AC:24, it should also enable 00-0F-AC:8 for interoperability.
2. The AP's BSS Configuration shall not enable AKM suite selectors 00-0F-AC:2 (PSK), 00-0F-AC:4 (FT over PSK), 00-0F-AC:6 (PSK using SHA-256), 00-0F-AC:19 (FT over PSK using SHA-384) or 00-0F-AC:20 (PSK using SHA-384).
3. The AP's BSS Configuration shall be PMF Required, i.e., AP sets MFPC to 1 and MFPR to 1 in beacons and probe responses of the BSS.
    NOTE: The AP should not reject an association on the basis of the value of MFPR indicated by the STA in its (Re)Association Request frame.
4. The AP shall also follow the additional requirements in Section 2.5.

When a STA's Network Profile is in WPA3-Personal Only Mode:

1. The STA's Network Profile shall allow at least one of the following AKMs to be selected:
    a. AKM suite selector 00-0F-AC:8
    b. AKM suite selector 00-0F-AC:24
    If the STA's Network Profile allows AKM suite selector 00-0F-AC:24 to be selected, it should also allow AKM suite selector 00-0F-AC:8 to be selected for interoperability.
    NOTE: Per 12.12.9 of [15], AKM suite selector 00-0F-AC:8 is not used in an association that negotiates use of EHT or MLO.
2. The STA's Network Profile shall not allow AKM suite selectors 00-0F-AC:2, 00-0F-AC:4, 00-0F-AC:6, 00-0F-AC:19 or 00-0F-AC:20 to be selected.
    NOTE: This means a STA operating in WPA3-Personal Only Mode will not connect to an AP that advertises only PSK AKMs.
3. The STA's Network Profile shall be PMF Required, i.e., STA sets MFPC to 1 and MFPR to 1 in all (re)association requests to APs in that network.
    NOTE: This means a STA operating in WPA3-Personal Only Mode will not connect to an AP that does not advertise support for PMF.
4. The STA shall also follow the additional requirements in Section 2.5.

2.3 WPA3-Personal Transition Mode

When an AP's BSS is operating in WPA3-Personal Transition Mode:

1. The AP's BSS Configuration shall enable at least AKM suite selectors 00-0F-AC:2 (PSK) and 00-0F-AC:8 (SAE).
2. The AP's BSS Configuration should enable AKM suite selectors 00-0F-AC:6 (PSK using SHA-256) and 00-0F-AC:24 (SAE using group-dependent hash).
3. The AP's BSS Configuration shall be PMF Capable, i.e., AP sets MFPC to 1 and MFPR to 0 in beacons and probe responses of the BSS.
4. The AP shall reject an association for SAE if PMF is not negotiated for that association.
5. The AP shall also follow the additional requirements in Section 2.5.

   NOTE: Per Sections 11.2 and 11.4, an AP does not operate a BSS in WPA3-Personal Transition Mode in the 6 GHz band or Sub 1 GHz band.

When a STA's Network Profile is in WPA3-Personal Transition Mode:

1. The STA's Network Profile shall allow at least AKM suite selectors 00-0F-AC:2, 00-0F-AC:6 and 00-0F-AC:8 to be selected.
   NOTE: Per 12.12.9 of [15] and Section 11.3, AKM suite selectors 00-0F-AC:2, 00-0F-AC:6 and 00-0F-AC:8 are not used in an association that negotiates use of EHT or MLO (see also Section 2.5).
   NOTE: Per 12.12.2 of [13] and Sections 11.2 and 11.4, AKM suite selectors 00-0F-AC:2 and 00-0F-AC:6 are not used in an association in the 6 GHz band or Sub 1 GHz band.
2. The STA's Network Profile should allow AKM suite selector 00-0F-AC:24 to be selected.
3. The STA's Network Profile shall be PMF Capable, i.e., STA sets MFPC to 1 and MFPR to 0 in all (re)association requests to APs in that network.
4. If the STA negotiates SAE when associating to an AP, the STA shall negotiate PMF.
5. The STA shall also follow the additional requirements in Section 2.5.

2.4 WPA3-Personal Compatibility Mode

When an AP's BSS is operating in WPA3-Personal Compatibility Mode:

1. The AP's BSS Configuration shall, if the BSS is in 2.4 GHz or 5 GHz band, enable AKM suite selector 00-0F-AC:2. The AP's BSS Configuration shall, irrespective of the band the BSS is operating on, enable AKM suite selector 00-0F-AC:8. If the AP's BSS Configuration enables EHT or MLO it shall, irrespective of the band the BSS is operating on, also enable AKM suite selector 00-0F-AC:24 in the BSS Configuration. The AP advertises this configuration as follows:
   a. The AP shall advertise the single AKM suite selector 00-0F-AC:2 in the RSNE in the 2.4 GHz and 5 GHz bands. The AP shall advertise the single AKM suite selector 00-0F-AC:8 in the RSNE in the 6 GHz band.
   b. The AP shall advertise the single AKM suite selector 00-0F-AC:8 in the RSNE Override element in the 2.4 and 5 GHz bands. The RSNE Override element is not advertised in the 6 GHz band.
   c. The AP shall, if the BSS enables EHT or MLO, irrespective of the band the BSS is operating on, advertise the single AKM suite selector 00-0F-AC:24 in the RSNE Override 2 element.
   d. The AP shall set SAE Hash-to-element to 1 in the RSNXE Override element in the 2.4 and 5 GHz bands. The RSNXE is not advertised in the 2.4 and 5 GHz bands.

e. The AP shall set SAE Hash-to-element to 1 in the RSNXE in the 6 GHz band. In addition, the AP shall, if the BSS is in the 6 GHz band and enables EHT or MLO, set SAE Hash-to-element to 1 in the RSNXE Override element.

NOTE: Other AKM suites, including FT, are disallowed in WPA3-Personal Compatibility Mode (but might be allowed in other modes that use RSN overriding).

2. The AP's BSS Configuration shall enable at least CCMP-128 as a pairwise cipher. NOTE: If the BSS enables EHT or MLO, it also enable GCMP-256 as a pairwise cipher per Section 2.5. The AP advertises this configuration as follows:
    a. The AP shall advertise the single pairwise cipher CCMP-128 in the RSNE on all bands and in the RSNE Override element in the 2.4 and 5 GHz bands.
    b. The AP shall, if the BSS enables EHT or MLO, irrespective of the band the BSS is operating on, advertise the single pairwise cipher GCMP-256 in the RSNE Override 2 element.
3. An AP's BSS Configuration shall, irrespective of the band the BSS is operating on, enable CCMP-128 as the group data cipher suite and BIP-CMAC-128 as the group management cipher suite. The AP advertises this configuration as follows:
    a. The AP shall advertise CCMP-128 in the RSNE as the group data cipher.
    b. The AP shall advertise CCMP-128 as the group data cipher and BIP-CMAC-128 as the group management cipher suite in the RSNE Override element.
    c. The AP shall, if the BSS enables EHT or MLO, advertise CCMP-128 as the group data cipher and BIP-CMAC-128 as the group management cipher suite in the RSNE Override 2 element.
4. The AP's BSS Configuration shall enable PMF as follows:
    a. The AP shall set MFPC in the RSNE in the 2.4 and 5 GHz bands to 1 if it has enabled functionality that requires PMF to be enabled with WPA2-Personal (e.g. Wi-Fi Agile Multiband), or to 0 otherwise. The AP shall set MFPR to 0 in the RSNE in the 2.4 and 5 GHz bands. The AP shall set MFPC to 1 and MFPR to 1 in the RSNE in the 6 GHz band.
    NOTE: An AP might set MFPC to 0 in the RSNE in the 2.4 and 5 GHz bands when using RSN overriding even if it has enabled functionality that requires PMF to be enabled with WPA2-Personal, but such a combination is not called WPA3-Personal Compatibility Mode.
    b. The AP shall set MFPC to 1 and MFPR to 1 in the RSNE Override element in the 2.4 and 5 GHz bands.
    c. The AP shall, if the BSS enables EHT or MLO, irrespective of the band the BSS is operating on, set MFPC to 1 and MFPR to 1 in the RSNE Override 2 element.
5. The AP shall reject a (re)association for SAE if PMF is not negotiated for that (re)association.
6. The AP shall also follow the additional requirements in Section 2.5.

NOTE: There is no separate WPA3-Personal Compatibility Mode for STAs. A STA in WPA3-Personal Transition Mode or a WPA2-Personal mode can, irrespective of whether it supports RSN overriding, connect with an AP in WPA3-Personal Compatibility Mode; if the STA does not support RSN overriding, it would connect using WPA2-Personal. A STA in WPA3-Personal Only Mode can, if it supports RSN overriding, connect with an AP in WPA3-Personal Compatibility Mode.

2.5 Additional Requirements on WPA3-Personal modes

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

1. An AP's BSS Configuration shall not enable WPA version 1 on the same BSS with WPA3-Personal.
2. An AP's BSS Configuration shall not enable WEP and TKIP on the same BSS as WPA3-Personal.
3. If an AP's BSS Configuration enables any PSK AKM (e.g., 00-0F-AC:2, 00-0F-AC:4, 00-0F-AC:6, 00-0F-AC:19 or 00-0F-AC:20), an SAE AKM shall also be enabled in the BSS Configuration unless explicitly overridden by the

administrator to operate in WPA2-Personal Only Mode. NOTE: Examples of modes in which both PSK and SAE AKMs are enabled include WPA3-Personal Transition Mode and WPA3-Personal Compatibility Mode.

4. If an AP's BSS Configuration enables EHT or MLO, it shall enable AKM suite selector 00-0F-AC:24.
5. If an AP's BSS Configuration enables EHT or MLO. It shall enable GCMP-256 as a pairwise cipher.
6. An AP's BSS Configuration shall only enable Diffie-Hellman groups 15-21, inclusive, for use with SAE.

7. A STA shall connect using the AKM preference order defined in Section 4.1.
8. A STA's Network Profile shall not enable WEP and TKIP.
9. A STA that enables EHT or MLO shall, in its Network Profile, allow AKM suite selector 00-0F-AC:24 to be selected.
10. A STA that enables EHT or MLO shall, in its Network Profile, allow GCMP-256 to be selected as a pairwise cipher.
11. A STA's Network Profile shall only use Diffie-Hellman groups 15-21, inclusive, with SAE.

12. An AP's and STA's SAE implementation shall, when using SAE Hunting-and-Pecking algorithm, set the security parameter k defined in Section 3.2 of [10] to a value of at least forty (40).
13. An AP's and STA's SAE implementation shall avoid differences in code execution that allow side channel information collection through the cache.

NOTE: The rules used to evaluate the suitability of SAE groups, and guidance on achieving the above SAE implementation requirements, are detailed in Appendix B.

3 Requirements on Configuration and Operation of WPA3-Enterprise

WPA3-Enterprise applies to enterprise network settings.

3.1 Modes of operation

WPA3-Enterprise modes are enumerated as follows:

- WPA3-Enterprise Only Mode
- WPA3-Enterprise Transition Mode
- WPA3-Enterprise 192-bit Mode

3.2 WPA3-Enterprise Only Mode

When an AP's BSS is operating in WPA3-Enterprise Only Mode:

1. The AP's BSS Configuration shall enable at least AKM suite selector 00-0F-AC:5 (IEEE 802.1X with SHA-256).
2. The AP's BSS Configuration shall not enable AKM suite selector: 00-0F-AC:1 (IEEE 802.1X with SHA-1).
3. The AP's BSS Configuration shall be PMF Required, i.e., AP sets MFPC to 1 and MFPR to 1 in beacons and probe responses of the BSS.
   NOTE: The AP should not reject an association on the basis of the value of MFPR indicated by the STA in its (Re)Association Request frame.
4. The AP shall also follow the additional requirements in Section 3.4.

When a STA's Network Profile is in WPA3-Enterprise Only Mode:

1. The STA's Network Profile shall allow at least AKM suite selector 00-0F-AC:5 to be selected.
2. The STA's Network Profile shall not allow AKM suite selector 00-0F-AC:1 to be selected.
   NOTE: This means a STA operating in WPA3-Enterprise Only Mode will not connect to an AP that advertises only AKM suite selector 00-0F-AC:1 (IEEE 802.1X with SHA-1 AKM).
3. The STA's Network Profile shall be PMF Required, i.e., STA sets MFPC to 1 and MFPR to 1 in all (re)association requests to APs in that network.
   NOTE: This means a STA operating in WPA3-Enterprise Only Mode will not connect to an AP that does not advertise support for PMF.
4. The STA shall also follow the additional requirements in Section 3.4.

3.3 WPA3-Enterprise Transition Mode

When an AP's BSS is operating in WPA3-Enterprise Transition Mode:

1. The AP's BSS Configuration shall enable at least AKM suite selectors 00-0F-AC:1 (IEEE 802.1X with SHA-1) and 00-0F-AC:5 (IEEE 802.1X with SHA-256) in the BSS.
2. The AP's BSS configuration shall be PMF Capable, i.e., AP sets MFPC to 1 and MFPR to 0.
3. The AP shall also follow the additional requirements in Section 3.4.

NOTE: Per Section 11.2, an AP does not operate a BSS in WPA3-Enterprise Transition Mode in the 6 GHz band.

When a STA's Network Profile is in WPA3-Enterprise Transition Mode:

1. The STA's Network Profile shall allow at least AKM suite selectors 00-0F-AC:1 and 00-0F-AC:5 to be selected.
   NOTE: Per Sections 11.2 and 11.3, AKM suite selector 00-0F-AC:1 (IEEE 802.1X with SHA-1) is not used in an association that negotiates use of EHT or MLO, nor in an association in the 6 GHz band.
2. The STA's Network Profile shall be PMF Capable, i.e., STA sets MFPC to 1 and MFPR to 0 in all (re)association requests to APs in that network.
3. The STA shall also follow the additional requirements in Section 3.4.

3.4 Additional Requirements on (non-192-bit) WPA3-Enterprise modes

The following additional requirements apply to all (non-192-bit) WPA3-Enterprise modes:

1. An AP's BSS Configuration shall not enable WPA version 1 with WPA3-Enterprise.
2. An AP's BSS Configuration shall not enable WEP and TKIP with WPA3-Enterprise.
3. If an AP's BSS Configuration enables EHT or MLO, it shall enable GCMP-256 as a pairwise cipher.
4. A STA shall connect using the AKM preference order defined in Section 4.2.
5. A STA's Network Profile shall not enable WEP and TKIP.
6. A STA that enables EHT or MLO shall, in its Network Profile, allow GCMP-256 to be selected as a pairwise cipher.
7. If a STA supports EAP-pwd, the implementation shall:
   a. only use Diffie-Hellman groups 15-21, inclusive, with EAP-pwd, and
   b. set the security parameter k defined in Section 3.2 of [10] to a value of at least forty (40), and
   c. avoid differences in code execution that allow side channel information collection through the cache.

3.5 WPA3-Enterprise 192-bit mode

WPA3-Enterprise 192-bit mode is well suited for deployments in sensitive enterprise environments to further protect Wi-Fi® networks with higher security requirements such as government, defense, and industrial.

When an AP's BSS is operating in WPA3-Enterprise 192-bit mode:

1. The AP's BSS Configuration shall enable AKM suite selector 00-0F-AC:12 (Suite B 192b) and shall not enable any other AKM suite selector.
   Note: WPA3-Enterprise 192-bit mode does not interoperate with any other security mode.
2. The AP's BSS Configuration shall be PMF Required, i.e., AP sets MFPC to 1 and MFPR to 1 in beacons and probe responses of the BSS.
3. The AP's BSS Configuration shall enable the pairwise cipher GCMP-256 and shall not enable any other pairwise cipher.

When a STA's Network Profile is in WPA3-Enterprise 192-bit mode:

1. The STA's Network Profile shall allow AKM suite selector 00-0F-AC:12 (Suite B 192b) to be selected, and shall not allow any other AKM suite selector to be selected.
2. The STA's Network Profile shall be PMF Required, i.e., STA sets MFPC to 1 and MFPR to 1 in all (re)association requests to APs in that network.
3. The STA's Network Profile shall allow GCMP-256 to be selected as the pairwise cipher, and shall not allow any other pairwise cipher to be selected.
4. 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 STA AKM Selection Preference Order

When a WPA3 STA needs to choose between multiple AKMs advertised on a BSS, the STA shall select the first AKM in preference order from the applicable list in the subclauses below. No preference order is defined for AKMs that are not specified in this section.

NOTE: This preference order applies when the STA selects between the set of AKMs that are both advertised on a given BSS and enabled in the STA's Network Profile. It does not imply any requirements on the AKMs enabled in the STA's Network Profile and does not imply any preference regarding the STA's selection between multiple BSSs.

4.1 Personal modes

1. FT Authentication over SAE using group-dependent hash 00-0F-AC:25
2. SAE Authentication using group-dependent hash 00-0F-AC:24
3. FT Authentication over SAE 00-0F-AC:9
4. SAE Authentication 00-0F-AC:8
5. FT Authentication over PSK 00-0F-AC:4
6. PSK using SHA-256 00-0F-AC:6
7. PSK 00-0F-AC:2

4.2 Enterprise modes

1. FT Authentication over IEEE Std 802.1X using SHA-256 00-0F-AC:3
2. Authentication using IEEE Std 802.1X using SHA-256 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 (within a 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.

6 SAE-PK

6.1 Background

Some public Wi-Fi networks use a group-level password for link-layer authentication. A password can be conveniently distributed to a group of users in various scenarios, e.g., displayed on public signage, distributed in written materials, or even verbally exchanged if necessary. Users are familiar with reading a password, sometimes from a distance, and entering it into their personal client devices.

The deployment and provisioning of a Wi-Fi network using a group-level password is straightforward and is attractive in use cases where the technical skill, infrastructure, and maintenance that would be required to deploy strong authentication using, for example, a preinstalled PKI trust root, provisioned certificates, or unique per-user secret credentials is not available.

The password is usually intended to provide, at a minimum, a simple means of (group-level) network access control. Depending on the use case, the size of the user group to which the password is distributed might be large, there might be no mutual trust relationship between users in the group, and the secrecy of the password from third parties outside the intended group might be only weakly protected. Therefore, in many such deployments, it is not difficult for a potential adversary to gain knowledge of the password.

Authentication between an AP and a STA using a regular password as a symmetric credential is vulnerable to insider impersonation attack - i.e., an adversary with knowledge of the password can launch a man-in-the-middle attack on client STAs by impersonating an AP. This is sometimes known as an "evil twin AP" attack. The tools required to enable such attacks are becoming more sophisticated and easier to obtain. Once a client STA connects to the adversary's AP, the adversary is able to inspect, modify, and forge any data exchanged with the client STA.

SAE Public Key (SAE-PK) authentication is an extension of SAE that is intended for use cases where authentication is based on a password that might be distributed to or obtained by a potential adversary. With SAE-PK, the AP in an infrastructure network is additionally authenticated based on a static public/private key pair, in order to provide protection against impersonation attacks as described above.

The SAE-PK password is set equal to a representation of a fingerprint of the AP's public key, and therefore serves both as a secret by which the AP authenticates STAs for network access, and also as a means to bootstrap trust in the AP's static public key for STAs to authenticate the AP. There is some (parameterized) trade-off between the security of the public key fingerprint and the convenience of using a password of moderate length.

6.2 SAE-PK overview

SAE-PK is an extension to SAE authentication. The additional signaling required for SAE-PK is carried in the same IEEE 802.11 Authentication frames that carry SAE Commit and Confirm messages.

When an AP sends an SAE Confirm message to a STA, the frame contains the AP's public key, a Modifier value (wrapped using a Key Encryption Key derived from the SAE keyseed), and a digital signature where the input data comprises the SAE public values used by both AP and STA, the AP’s public key and Modifier, and the MAC addresses of both AP and STA signed with the private key analog of the AP’s public key.

The STA verifies trust in the AP’s public key using a fingerprint encoded in the password. Base32 encoding of the fingerprint, and the addition of separator characters and a checksum character, helps manual entry of the password by the user (case-invariant, avoidance of special and commonly confused characters). An example password (for λ=12) is as follows: a2bc-de3f-ghi4.

The digital signature sent by the AP allows the STA to authenticate the SAE key exchange transcript with the AP (see [4] Section 6.3.1.1) using the trusted public key of the AP.

If the STA fails to validate trust in the received AP public key, or fails to verify the digital signature, authentication does not proceed. Otherwise, if the SAE authentication procedures succeed, the established PMKSA is used for IEEE 802.11 (re)association in accordance with [1].

Resistance to second preimage attack on the fingerprint represented in the password is enhanced using the hash-extension technique utilized in [3]. The fingerprint is the truncated output of a hash function, the input to which comprises

the AP's public key prepended by the SSID (to mitigate rainbow preimage attacks) and a 16-octet Modifier value. The Modifier is found randomly by one-time brute-force search (when the password is initially generated) and is a value that results in the first 8*Sec bits of the fingerprint being equal to zero. This allows a fingerprint of effective length (8*Sec + 19*λ/4 - 5)-bits to be represented in only 5λ bits (where base32 encoding results in a λ-character password excluding separators), using λ/4 bits to redundantly encode Sec and one of the characters (5 bits) for the checksum. Further details and recommendations for these values are found in Section 6.6.2.

6.3 Credential generation procedure

This section describes how SAE-PK credentials are generated. These credentials comprise:

- A public/private key pair K_AP / k_AP
- A corresponding 128-bit Modifier value M, found for a specified value of Sec
- A corresponding SAE-PK Password
- Optionally, an SAE Password Identifier, which identifies the above credentials

The same set of credentials (and, therefore, the same public/private key pair) are configured on all APs in a given network (SSID).

NOTE: At a minimum, the SAE-PK Password (and, if used, the SAE Password Identifier) is distributed to client STAs. If the QR-code representation is used (see WIFI URI defined in Section 7), client STAs additionally obtain the full public key (K_AP).

The private key shall not be divulged outside the APs in the infrastructure network. If the network comprises multiple APs, the means by which the key pair and Modifier are securely distributed and managed between those APs is out of scope of this specification.

The same key pair K_AP / k_AP can be used for multiple passwords that are generated for use on the same network (i.e., by randomly finding new Modifiers).

A device that supports SAE-PK shall support SAE-PK with an ECDSA P-256 AP public key. Support for SAE-PK with other ECDSA keys that have prime length equal to or greater than 256 bits is optional.

A device that supports SAE-PK with an ECDSA key with prime length greater than 256 bits shall support, and should enable, SAE group 20. A device that supports SAE-PK with an ECDSA key pair with prime length greater than 384 bits shall support, and should enable, SAE group 21.

An AP that is configured for SAE-PK to use an ECDSA key with prime length greater than 256 should disable SAE groups that have strength estimate (per Table 11 [10] in Appendix B) less than 192 bits unless those groups are needed for use with other passwords configured on the BSS. An AP that is configured for SAE-PK to use an ECDSA key with prime length greater than 384 should disable SAE groups that have strength estimate (per Table 11 in Appendix B) less than 256 bits unless those groups are needed for use with other passwords configured on the BSS.

A device shall not reject an SAE group, or reject an SAE Confirm message, purely on the basis that the strength estimates of the SAE-PK and SAE groups do not match.

NOTE: The above requirements and recommendations are intended to promote consistency between the strength estimate of the negotiated SAE group and the SAE-PK signing key.

NOTE: The AP public key curve and prime length are established when the SAE-PK credentials are generated, and therefore have to be supported by all APs and STAs in that network.

A 128-bit unsigned integer Modifier value M shall be found by initially setting M to a random value and (as necessary) incrementing M by one until a value of M is found for which the first Sec octets of Fingerprint are equal to zero:

$$\text{Fingerprint} = L(\text{Hash}(\text{SSID} \,||\, M \,||\, K\_AP), 0, 8*\text{Sec} + 19*\lambda/4 - 5)$$

where:

- L(S, F, N) is the function that extracts bits F to F+N–1 of the bit string S starting from the left
- Hash() is the function implementing the hash algorithm defined in Table 12-1 of [1], depending on the length of the AP's public key K_AP, using the ECC column for the prime length of ECDSA keys

- Sec is the hash extension security parameter, equal to an integer value of 3 or 5
  - λ shall be chosen such that λ =4*n, where n is an integer equal to or greater than 3, and 8*Sec + 19*λ/4 - 5 <= HashLen, where HashLen is the output length of the hash function Hash()
- SSID is a variable length sequence of octets equal to the network SSID
- K_AP is the AP's public key, represented as the DER of ASN.1 SubjectPublicKeyInfo. The encoding is as defined in RFC 5480 [8] for ECDSA, where subjectPublicKey is the compressed format. The ASN.1 representation for an ECDSA P-256 key is as follows:

```
AlgorithmIdentifier ::= SEQUENCE {
   algorithm         ecPublicKey,
   parameters        secp256r1 }
SubjectPublicKeyInfo ::= SEQUENCE {
   algorithm         AlgorithmIdentifier,
   subjectPublicKey    BIT STRING }
```

The password shall then be determined as follows:

PasswordBase = Base32(P(0) || P(1) || … || P(λ/4-1))

Password = AddSeparators(PasswordBase || ChkSum)

where:

- When i< (λ/4-1), P(i) = Sec_1b || L(Fingerprint, 8*Sec+(19*i), 19)
- When i=(λ/4-1), P(i) = Sec_1b || L(Fingerprint, 8*Sec+(19*i), 14)
- Sec_1b is a 1-bit integer equal to 1 when Sec=3, and equal to 0 when Sec=5
- Base32() is the base32 encoding function (5 bits per character) as defined in [6] with lowercase US-ASCII alphabet
- ChkSum is a base32 character equal to the output of the Verhoeff algorithm [11] where:
  - The input is PasswordBase, comprising lowercase base32 characters that encode values as defined in [6]
  - The dihedral group is of order 32 and degree 16 (D16) and the permutation is (1 2)(7 11 13 5 20 23 9 6 27 15 21 25 14 10 8 31 26 4 16 22 12 29 18 24 28 17 3 30 19 0)
  - NOTE: The multiplication (group) operation d(j, k) in this dihedral group can be calculated by the formula:
    d(j, k) = (j + k) mod 16 when j<16 and k<16
    d(j, k) = ((j + k) mod 16) + 16 when j<16 and k≥16
    d(j, k) = ((j - k) mod 16) + 16 when j≥16 and k<16
    d(j, k) = (j - k) mod 16 when j≥16 and k≥16
  - NOTE: The inverse operation inv(j) in this dihedral group can be calculated by the formula:
    inv(j) = 16 - j when j<16
    inv(j) = j when j≥16
- AddSeparators() is the function that inserts a hyphen character (ASCII 0x2D) after every four characters of the US-ASCII input string, except that a trailing hyphen character is not inserted

NOTE: The length of the input to the base32 encoding function is not in general an integer number of octets. An implementation might need to zero-pad the input and truncate the output so that a 5λ-bit input always results in a λ-character output.

6.4 Authentication using SAE-PK

SAE-PK uses the SAE authentication exchange as defined in [1], using a password generated per Section 6.3, except where specified below.

When SAE-PK is used, the value SAE_PK (127) is used in the Status Code field of SAE Commit messages to indicate success. This also implicitly indicates use of the Hash-to-Element technique [1].

When SAE-PK is enabled on a BSS, an AP that supports SAE-PK shall:

- Advertise one or more SAE AKMs in RSNE of Beacon and Probe Response frames

- Advertise support for SAE-PK by setting the SAE-PK bit (6) to 1 in RSNXE (which is sent in Beacon, Probe Response, and certain other frames as defined in [1])
- Use SAE-PK with a peer STA that indicates SAE_PK status code in its SAE Commit message.
- Use one or more SAE passwords generated using the SAE-PK credential generation procedure defined in Section 6.3

When SAE-PK is used, the key derivation from keyseed and context (as defined in 12.4.5.4 of [1]) is expanded to additionally derive a Q-bit KEK, as follows:

Length = 2Q + PMK_bits

kck_pmk_kek = KDF-Hash-Length(keyseed, “SAE-PK keys”, context)

KCK = L(kck_ pmk_kek, 0, Q)

PMK = L(kck_pmk_kek, Q, PMK_bits)

KEK = L(kck_pmk_kek, Q+PMK_bits, Q)

where:

- Q is the length of the digest of the hash function H() depending on the SAE group, as defined in 12.4.2 of [1]
- PMK_bits is the length of the PMK in bits, e.g., 256 for AKM suite selectors 00-0F-AC:8 and 00-0F-AC:9, or equal to Q for AKM suite selectors 00-0F-AC:24 and 00-0F-AC:25

NOTE: The KCK and KEK above are unrelated to the EAPOL-Key KCK and KEK obtained from the PTK in a subsequent 4-way handshake.

When SAE-PK is used, an AP that supports SAE-PK that sends an SAE Confirm message with status of Success shall include an SAE-PK element (as defined in Section 6.7), a FILS Public Key element and a FILS Key Confirmation element in the Authentication frame, where:

- The EncryptedModifier field of the SAE-PK element contains the output of the AES-SIV-Q algorithm, where Q ∈ {256, 384, 512} is as defined above and KEK is the key. The plaintext passed to the AEAD algorithm is the 16-octet Modifier M, with no AAD
- The FILS Public Key field of the FILS Public Key element (as defined in [1]) contains the AP's public key K_AP (represented as the DER of ASN.1 SubjectPublicKeyInfo), and the Key Type field is set to 2 (for ECDSA, encoded according to RFC 5480 [8])
- The KeyAuth field of the FILS Key Confirmation element (as defined in [1]) is set equal to:

  KeyAuth = Sig_AP(eleAP || eleSTA || scaAP || scaSTA || M || K_AP || AP-MAC || STA-MAC)

where:

- Sig_AP() is a function that generates the digital signature of the hash of the input using the AP's private key k_AP (see Section 6.3). The hash algorithm depends on the prime length of the AP's public key K_AP, and is the same as the hash function Hash() defined in Section 6.3. The form of signature is as defined in ISO/IEC 14888-3 for ECDSA, and the signature value is encoded as DER of ASN.1 according to RFC 5480 [8] and RFC 3279 [9]. A constant-time algorithm shall be used to generate the digital signature. The ASN.1 representation for an ECDSA signature value is as follows:

```
Ecdsa-Sig-Value ::= SEQUENCE {
    r         INTEGER,
    s         INTEGER }
```

- eleAP and eleSTA are equal to the SAE element sent by the AP and STA, respectively, in the current authentication sequence, converted to octet strings per 12.4.7.4 (Encoding and decoding of SAE Commit messages) of [1]
- scaAP and scaSTA are equal to the SAE scalar sent by the AP and STA, respectively, in the current authentication sequence, converted to octet strings per 12.4.7.4 (Encoding and decoding of SAE Commit messages) of [1]
- M and K_AP are the Modifier and AP public key, respectively, as defined in Section 6.3. M and K_AP are identified by the SAE Password Identifier, if negotiated during the SAE Commit exchange

- AP-MAC and STA-MAC are the MAC addresses of the AP and STA, respectively. Between two MLDs, they are the MLD MAC addresses.

If required, the FILS Public Key and FILS Key Confirmation elements are fragmented per 10.28.11 (Element Fragmentation) of [1]. The FILS Public Key element (and any associated Fragment elements) and FILS Key Confirmation element (and any associated Fragment elements) appear, in that order, immediately prior to all Vendor Specific elements (including the SAE-PK element) in the Authentication frame.

If a STA that supports SAE-PK in "Confirmed" state is using SAE-PK and receives an SAE Confirm message then, per 12.4.8.6.5 of [1], it processes the SAE Confirm message in accordance with 12.4.5.6 of [1]. If this processing is successful and the SAE Confirm message is verified, then, prior to proceeding further, the STA shall verify an SAE-PK element, FILS Public Key element, and FILS Key Confirmation element are also present in the Authentication frame, unwrap the Modifier, validate the public key, verify the signature and complete authentication per the following steps:

1. Unwrapping

- The STA attempts to unwrap the Modifier in the SAE-PK element using the KEK

2. Public key validation

- If the STA has a stored trusted public key that corresponds to the same SSID, password, and (if used) password identifier (e.g., from scanning a QR code containing SAE-PK password and public key, or from a previous successful authentication):
  - If the public key K_AP in the FILS Public Key element matches the stored key, the STA determines that K_AP is trusted; else (i.e., if it does not match, or a valid public key could not be parsed) it determines that K_AP is not trusted
- Otherwise (i.e., if the STA does not have a corresponding stored trusted public key), the STA calculates the expected (8*Sec + 19*λ/4 - 5)-bit fingerprint Fingerprint_Expected from the configured Password as defined below, and generates Fingerprint of the unwrapped Modifier and public key K_AP (from the FILS Public Key element) as defined in Section 6.3. If they exactly match, the STA determines that K_AP is trusted; else it determines K_AP is not trusted:
  - PasswordBase || ChkSum = RemSeparators(Password)
  - λ = Len(Password) - Floor(Len(Password) / 5))
  - PW = Base32d(PasswordBase)
  - Sec is 3 when L(PW, 0, 1) is equal to 1, or is 5 when L(PW, 0, 1) is equal to 0
  - Fingerprint_Expected = 0^(8*Sec) || F(0) || F(1) || … || F(λ/4-1)

  where:

  - Password is identified by the SAE Password Identifier, if negotiated during the SAE Commit exchange
  - RemSeparators() is the function that removes a hyphen character (ASCII 0x2D) every fifth character of the US-ASCII input string
  - Len() is the function returning the length of the input string in characters
  - Floor() is the function defined in 1.5 of [1]
  - Base32d() is the base32 decoding function, outputting 5λ bits
  - 0^(8*Sec) is the bit string comprising Sec octets of the value zero
  - When i< (λ/4-1), F(i) = L(PW, 20*i+1, 19)
  - When i=(λ/4-1), F(i) = L(PW, 20*i+1, 14)

  NOTE: The length of the output of the base32 decoding function is not in general an integer number of octets. An implementation might need to pad the input and correctly truncate the output so that a λ-character input always results in a 5λ-bit output.

  NOTE: Per Section 6.5.3, a password that is not in the correct form for SAE-PK (including a valid checksum character, and consistency of redundant Sec encoding) is not used in the SAE-PK authentication exchange.

3. Signature verification

- If the STA has successfully validated trust in the public key K_AP, the STA attempts to verify the digital signature in the FILS Key Confirmation element using K_AP. The digital signature verification procedure is as defined in

ISO/IEC 14888-3 for ECDSA, where the hash algorithm and input data are specified in the definition of Sig_AP() above

4. Authentication confirmation

- If the STA has successfully validated trust in the public key K_AP, and successfully verified the signature in the FILS Key Confirmation element, and the SAE Confirm message was successfully verified, then the STA should store the trusted public key (if not already stored), and shall proceed per 12.4.8.6.5 of [1], resulting in transition to "Accepted" state. Otherwise (i.e., if the SAE-PK element, FILS Public Key element, or FILS Key Confirmation element were absent or invalid, or public key validation failed, or signature verification failed, or the SAE Confirm message was not verified), the STA shall remain in "Confirmed" state

NOTE: If a client STA is reconfigured with a new password for a given network, any stored trusted public key for that network pertaining to the old password might no longer be valid and so should be deleted.

When the STA performs (re)association using SAE-PK, it shall include RSNXE with SAE-PK bit (6) set to 1 in the (Re)Association Request frame.

6.5 SAE-PK Modes of operation

A device that supports SAE-PK shall support WPA3-Personal.

A device that supports SAE-PK can enable SAE-PK in any mode where an SAE AKM is enabled, e.g., WPA3-Personal Only Mode or WPA3-Personal Transition Mode.

The term "WPA3-Personal SAE-PK Only Mode" is used to refer to a WPA3-Personal mode in which a STA's Network Profile enables SAE-PK but does not allow:

- WEP
- TKIP
- PSK AKM
- SAE AKM without SAE-PK

NOTE: A PMK derived using SAE-PK can be used with PMKSA caching using the same PMKSA caching association exchanges as when a PMK derived using regular SAE authentication is used. An (M)PMK derived using SAE-PK (during FT Initial Mobility Domain Association) can be used for FT authentication using the same FT key hierarchy derivation and FT authentication exchanges as when an (M)PMK derived using regular SAE authentication is used.

6.5.1 SAE-PK AP operation

An AP that supports SAE-PK that is configured with an SAE-PK password (with corresponding key pair and modifier) shall use the same SAE-PK password (including hyphen separator characters) with SAE AKM irrespective of whether or not SAE-PK is negotiated. If the AP enables SAE Password Identifiers, this applies for each password identifier.

If every password configured for use with SAE AKM (in dot11RSNAConfigPasswordValueTable) and/or PSK AKM on a BSS is an SAE-PK password, an AP that supports SAE-PK shall set the "SAE-PK Passwords Used Exclusively" bit (88) in the Extended Capabilities element to 1, otherwise set to 0.

An AP that supports SAE-PK shall prevent configuration of a password with a value that would be misidentified by STAs as an SAE-PK Password Format (see Section 6.5.3) in both of the following cases:

- The password is configured for use with PSK AKM on a BSS that has SAE-PK enabled, and has a value that is not equal to the value of an SAE-PK Password Format (with corresponding key pair and modifier) configured for use with SAE AKM (in dot11RSNAConfigPasswordValueTable) on the same BSS
- The password is configured for use with SAE AKM (in dot11RSNAConfigPasswordValueTable) on a BSS that has SAE-PK enabled, and does not have a corresponding SAE-PK key pair and modifier configured

An AP that supports SAE-PK shall support the Transition Disable mechanism defined in Section 8. The AP should, by default, indicate Transition Disable for SAE-PK when SAE-PK authentication is performed.

NOTE: If an AP that supports SAE-PK does not indicate Transition Disable for SAE-PK, STAs that are not explicitly configured to only use SAE-PK remain vulnerable to downgrade attack even after first connection to the network, as

described in Section 6.6.3. It is strongly recommended that APs indicate Transition Disable for SAE-PK when SAE-PK authentication is performed, if all APs in the network support SAE-PK. This recommendation also applies even if only a subset of the APs in the network support SAE-PK, unless the coverage area of that subset of APs would be insufficient. If the QR-code representation of SAE-PK credentials is used, the "trdisable" attribute should be specified accordingly (see Section 7).

6.5.2 SAE-PK Password Format

A password is in the correct form for SAE-PK Password Format if all the following are true:

- Every fifth octet in the octet string of the password is equal to 0x2D (ASCII hyphen)
- All other octets correspond to values in the base32 lowercase US-ASCII alphabet
- The number of base32 characters (λ) is at least 12, and an integer multiple of 4
- The MSBs corresponding to the i=(4*n+1)th base32 characters have the same value for all integer values of n between 0 and λ/4-1
- The λth (i.e., final) base32 character is a valid checksum character for the preceding base32 characters per the Verhoeff algorithm as defined in Section 6.3

6.5.3 SAE-PK STA operation

When a STA that supports SAE-PK has SAE-PK enabled for a Network Profile, the STA shall use SAE-PK authentication when connecting to an AP in that network that indicates support for SAE-PK.

A STA that supports SAE-PK shall not initiate SAE-PK authentication using a password that is not in the correct SAE-PK Password Format (see Section 6.5.3).

A STA that supports SAE-PK should, if the user manually enters a password for a network:

- If the password is not in the correct SAE-PK Password Format, but the STA has identified at least one AP in the network that advertises "SAE-PK Passwords Used Exclusively" bit set to one:
  - Confirm with the user that the password is correctly entered, before using it with any other (non-SAE-PK) authentication protocol allowed by the configured mode of operation
- If the password is in the correct SAE-PK Password Format:
  - Enable SAE-PK by default for that Network Profile

NOTE: If a STA that supports SAE-PK identifies a network for which all SAE and PSK passwords in use are SAE-PK passwords (i.e., where at least one AP sets the "SAE-PK Passwords Used Exclusively" bit to 1), and the STA provides a UI for manual input of passwords, the STA implementation can assist manual entry by, for example, rejecting or auto-correcting invalid characters (that are not in the base32 character set or are in uppercase) and pre-populating hyphen separator characters (ASCII 0x2D) every fifth non-trailing character.

A STA that supports SAE-PK shall support the Transition Disable mechanism defined in Section 8.

NOTE: If a STA that supports SAE-PK receives Transition Disable indication for SAE-PK, the STA uses WPA3-Personal SAE-PK Only Mode for the corresponding network (see Section 6.5).

When a STA has SAE-PK enabled for a Network Profile, and is selecting between discovered APs in that Network Profile (SSID) that it considers suitable candidates for association, it shall attempt to authenticate with an AP that advertises support for SAE-PK, before attempting to authenticate with any AP that is not advertising support for SAE-PK.

NOTE: How a STA determines whether an AP is a suitable candidate for association is out of scope of this specification. A STA might determine that an AP is not suitable if it predicts an acceptable level of link quality will not be achieved.

6.6 Security considerations

6.6.1 General

As described in Section 6.1, SAE-PK is intended for use cases where authentication is based on a password that might be distributed to or obtained by a potential adversary. An adversary that has knowledge of the password (but not the private key analog of the AP's public key) is able to gain network access but is not able to impersonate an AP when SAE-PK is used. The security properties of SAE, such as pairwise link confidentiality and integrity protection, even when an adversary knows the password, also apply to SAE-PK.

Since an adversary that has knowledge of the password can still gain network access with SAE-PK, the security of (genuine) client devices connected to the network also relies on the network enabling client filtering/isolation to prevent insider attacks.

It is assumed that the mechanism(s) used to distribute the password to client STAs are sufficiently resistant to subversion by an adversary, so that client STAs can reasonably trust the veracity of the public key fingerprint (encoded in the password) or the public key itself (in the QR code) as a means to authenticate a legitimate AP. For example, in a public venue Wi-Fi network, the password might be distributed using venue signage, menus, receipts and so on, and it is assumed difficult for an adversary to modify or replace the password (or QR code) displayed on these materials in a way that is not detected by users of client STAs. The integrity of the input mechanism (e.g., QR code scanning application) on the client STA is also assumed. The redundant encoding of Sec across multiple characters in the password, and the requirement (see Section 6.5.3) that a STA does not initiate SAE-PK authentication using a password with inconsistent encoding of Sec, mitigates the possibility that malicious modifications to a small number of characters of the password could result in the value of Sec decoded by the STA being less than the actual value, which could facilitate a second-preimage attack (see Section 6.6.2).

In addition, the checksum character allows a STA to detect accidental typos or malicious modifications to single characters of an SAE-PK password. The recommendation (see Section 6.5.3) that a STA implementation confirms with the user that the password has been correctly entered if it identifies a network where at least one AP sets the SAE-PK Passwords Exclusively bit set to one, but the entered password is not in the correct form for SAE-PK, is intended to enhance usability and also mitigate the possibility that predictable typos or malicious modifications to single characters of the password could facilitate a downgrade attack (if the STA is not already configured in WPA3-Personal SAE-PK Only Mode for the network) (see Section 6.6.3).

It is assumed that the KEK (the pairwise secret extracted from the SAE keyseed that is used to encrypt the Modifier sent in the SAE-PK element) is not compromised, and that the Modifier is generated using a random number generator with high entropy. If a third party were able to decrypt or guess the Modifier value (and passively observe the AP's public key K_AP and SSID), it could reconstruct the password (see Section 6.3).

The integrity of the mechanism used to generate SAE-PK credentials (as defined in Section 6.3) is assumed. If the private key is compromised, all security assurances associated with that private key are void. In addition, even if the private key is not compromised, an adversary that somehow has control over the mechanism by which a valid Modifier value M and corresponding password are found might be able to find values of M that result in identical passwords for both the genuine public key and the adversary's public key (i.e., a hash collision attack) with substantially reduced computational complexity compared to the second preimage attacks described in Section 6.6.2. To avoid the possibility that a network administrator inadvertently uses a compromised or malicious (third party) password generation mechanism, it is recommended that AP implementations provide network administrators with a secure tool or service for SAE-PK credential generation.

It is assumed that constant time operations are correctly implemented for digital signature generation, and nonces are generated from a high-quality source of entropy, in order to prevent attacks that could compromise the AP's private key.

6.6.2 Resistance to preimage attacks

If the STA has not a-priori stored the full AP public key (e.g., from a previous authentication to the same network, or from being provisioned with a QR code), the resistance of SAE-PK to active attacks by an adversary impersonating a legitimate AP is dependent on the public key fingerprint represented in the password being sufficiently resistant to second preimage attacks.

There is a trade-off between the second preimage security strength and the effective fingerprint length, which depends on the password length (λ characters, excluded separators) and the value of Sec (where larger values of Sec require more computation resources to find a value of Modifier on initial credential generation).

In order to launch such an attack, an adversary with its own public key pair would need to find a value for Modifier for which the fingerprint is identical to that represented in the password. A conventional (non-quantum) brute-force attack would require an average of 2^S trials, where S = 8*Sec + 19*λ/4 - 5 is the length of the truncated hash fingerprint, and is equal to the preimage strength (see [5]).

The feasibility of a second preimage attack depends both on the time and monetary cost required to execute the attack. Assuming integrity of the password, the average time required for an adversary using (for example) a high-speed accelerated "hash miner" capable of 50 TeraHashes/sec to find a Modifier value by brute-force search that results in a second preimage of the fingerprint, for various combinations of λ and Sec, is shown in Table 2. There is a small probability that the adversary can find a second preimage in much less than the average time. The average time required might be substantially reduced using a faster hash miner, e.g., with additional parallelization of local or cloud-based compute resources comprising ASICs with a very large number of cores. The monetary cost of the attack (including cost of consumed power) scales with the number of trials required.

Table 2. Examples of average time required to find a second preimage

λ	Sec	S	Average time required to find a second preimage at 50 TH/sec (years)
12	3	76	48
12	5	92	3.1 million
16	3	95	25.1 million
16	5	111	1.6 trillion

Passwords with the lowest supported security strength (λ=12, Sec=3) are attractive in terms of usability (shorter password) and deployment (short time required to generate the password). However, in the case of network deployments with stronger security requirements, it is recommended that passwords with security strength of at least S=92 bits are used.

NOTE: If a STA has stored the full (trusted) AP public key - either following successful authentication to the network using SAE-PK or by being provisioned using the QR code - a preimage attack on that STA on subsequent authentication does not apply since the STA will verify that the full AP public key matches.

6.6.3 Resistance to downgrade

An adversary that knows the password might attempt a downgrade attack on a STA, by which it could obtain a man-in-the-middle position, using an "evil twin AP" that only advertises support for symmetric password-based authentication algorithms (e.g., SAE without SAE-PK, PSK AKM, or IEEE 802.1X AKM with a password-based phase 2 method).

A STA that supports SAE-PK that is configured to use WPA3-Personal SAE-PK Only Mode for a given network is fully resistant to such downgrade attack when connecting to that network. A STA will use WPA3-Personal SAE-PK Only Mode for a given network (while the corresponding Network Profile remains configured) if it has already received a Transition Disable indication for SAE-PK for that network (i.e., received from an AP in a previous SAE-PK authentication, or obtained from provisioning using an SAE-PK QR code), or if manually configured by the user (e.g., based on an indication on signage displaying the password that it is an SAE-PK password).

A STA that supports SAE-PK that is configured to use SAE-PK in some other mode for a given network (e.g., the STA also allows SAE without SAE-PK, PSK and/or other password-based authentication algorithms) is potentially vulnerable to downgrade attack. This might typically be the case when a user manually enters the password on first connection to the network and would continue to be the case on subsequent connections to the network if the network is not advertising Transition Disable for SAE-PK (or the user subsequently deletes the Network Profile). Some degree of resistance to such attack is provided by the AP selection rule defined in Section 6.5.3. However, the STA might still be vulnerable if it is unable to discover and successfully connect to a suitable AP that supports SAE-PK in the genuine network - e.g., if the STA is at the edge of usable coverage of the genuine network, as a consequence of a denial-of-service attack where the

adversary blocks or manipulates frames to prevent successful connection to the genuine network, or if the user inputs an incorrect password containing typos that are predictable by the adversary (e.g., omitted hyphen separators) or that has been maliciously modified (see Section 6.6.1).

Similarly, if a network had previously been using a non-SAE-PK password and is subsequently reconfigured to enable SAE-PK with a new SAE-PK password, STAs that had previously connected to the network with the old password might retain a profile containing that password. If the user does not update the profile with the new SAE-PK password, the STA might connect to an adversary's AP that is configured with the old password.

A STA that does not support SAE-PK does not have protection against downgrade attack when connecting to an SAE-PK network. In addition, a legacy STA that does not support SAE (and, therefore, uses PSK) does not have meaningful confidentiality or integrity protection against an adversary that knows the password.

6.7 SAE-PK element

This section defines the SAE-PK element.

The SAE-PK element is in the Vendor Specific format as defined in 9.4.2.25 of [1]. Its format is shown in Table 3. The element is extensible.

Table 3. SAE-PK element format

Field	Size (Octets)	Value (Hex)	Description
Element ID	1	0xDD	IEEE 802.11 vendor specific element
Length	1		Length of the following fields in the IE in octets.
OUI	3	0x50-6F-9A	Wi-Fi Alliance specific OUI (refer to sub-clause 9.4.1.31 of [1])
OUI Type	1	0x1F	Identifying the type and version of the SAE-PK element
EncryptedModifier	32	Variable	Encrypted Modifier M

7 WIFI URI

This section defines the URI representation for Wi-Fi credentials using the "WIFI" URI scheme. The URI can be encoded in a QR code to provide a convenient means to provisioning the credentials to devices.

7.1 URI format

The URI is defined by [7] and formatted by the WIFI-qr ABNF rule:

```
WIFI-qr = “WIFI:” [type “;”] [trdisable “;”] ssid “;” [hidden “;”] [id “;”] [password “;”] [public-key “;”] “;”
type = “T:” *(unreserved) ; security type
trdisable = “R:” *(HEXDIG) ; Transition Disable value
ssid = “S:” *(printable / pct-encoded) ; SSID of the network
hidden = “H:true” ; when present, indicates a hidden (stealth) SSID is used
id = “I:” *(printable / pct-encoded) ; UTF-8 encoded password identifier, present if the password has an SAE password identifier
password = “P:” *(printable / pct-encoded) ; password, present for password-based authentication
public-key = “K:” *PKCHAR ; DER of ASN.1 SubjectPublicKeyInfo in compressed form and encoded in “base64” as per [6], present when the network supports SAE-PK, else absent
printable = %x20-3a / %x3c-7e ; semi-colon excluded
PKCHAR = ALPHA / DIGIT / %x2b / %x2f / %x3d
```

In this version of the specification, the URI supports provisioning of credentials for Wi-Fi networks using password-based authentication, and for unauthenticated (open and Wi-Fi Enhanced Open™ [16]) Wi-Fi networks.

If the "type" is present, its value is set to "WPA" and it indicates password-based authentication is used.

If the "type" is absent, it indicates an unauthenticated network (open or Wi-Fi Enhanced Open).

NOTE: This specification does not define usage of the WIFI URI with WEP shared key.

The value of "trdisable", if present, is set to a hexadecimal representation of the Transition Disable bitmap field (defined in Section 8).

NOTE: "trdisable" allows transition modes to be disabled at initial configuration of a Network Profile, and therefore provides protection against downgrade attack on a first connection (e.g., before a Transition Disable indication is received from an AP).

The values of "ssid", "password", and "id" are, in general, octet strings. Octets that do not correspond to characters in the printable set defined in this ABNF rule are percent-encoded.

NOTE: The semi-colon is excluded from the printable set as defined in this ABNF rule, and therefore is percent-encoded.

NOTE: When the password is used with WPA2-Personal (including WPA3-Personal Transition Mode), it comprises only ASCII-encoded characters. When the password is used with only SAE, it comprises octets with arbitrary values. The SAE password identifier is a UTF-8 string.

Devices parsing this URI shall ignore semicolon separated components that they do not recognize in the WIFI-qr instantiation. Ignoring unknown components allows devices to be forward compatible with future extensions to this specification

7.2 WIFI URI device support

A STA that supports the WIFI URI and is capable of scanning a QR code shall, when a WIFI QR code indicating a supported mode is scanned and subject to user confirmation (if applicable to the STA's implementation), configure a Network Profile with the specified parameters.

If the URI contains Transition Disable indication (trdisable), the STA shall disable algorithms in the configured Network Profile in accordance with the rules defined in Section 8 (Transition Disable indication).

If the URI does not contain Transition Disable indication, the STA should by default enable algorithms in the configured Network Profile corresponding to the transition modes that are supported by the STA (e.g., WPA3-Personal Transition Mode when a password is specified, or Wi-Fi Enhanced Open Transition Mode when no password is specified).

7.3 URI examples

Some examples of the WIFI URI format are as follows:

1. WIFI:T:WPA;S:MyNet;P:MyPassword;;
   - STA that supports WPA3-Personal might use SAE or PSK (WPA3-Personal Transition Mode)
   - STA that does not support WPA3-Personal uses PSK (WPA2-Personal)
2. WIFI:T:WPA;R:1;S:MyNet;P:MyPassword;;
   - STA that supports WPA3-Personal and Transition Disable uses SAE only (WPA3-Personal Only Mode)
   - STA that supports WPA3-Personal but not Transition Disable might use SAE or PSK (WPA3-Personal Transition Mode)
   - STA that does not support WPA3-Personal uses PSK (WPA2-Personal)
3. WIFI:T:WPA;R:3; S:MyNet;P:a2bc-de3f-ghi4;K:MDkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDIgADURzxmttZoIRIPWGoQMV00XHWCAQIhXruVWOz0NjlkIA=;;
   - STA that supports SAE-PK (and, therefore, Transition Disable) uses SAE-PK only (WPA3-Personal SAE-PK Only Mode)
   - STA that supports WPA3-Personal and Transition Disable but not SAE-PK uses SAE without SAE-PK only (WPA3-Personal Only Mode)
   - STA that supports WPA3-Personal but not Transition Disable or SAE-PK might use SAE or PSK (WPA3-Personal Transition Mode)
   - STA that does not support WPA3-Personal uses PSK (WPA2-Personal)
4. WIFI: S:MyNet;;
   - STA that supports Wi-Fi Enhanced Open might use Wi-Fi Enhanced Open or legacy open (Wi-Fi Enhanced Open Transition Mode)
   - STA that does not support Wi-Fi Enhanced Open uses legacy open

8 Transition Disable

8.1 Transition Disable Overview

Transition Disable is an indication from an AP to a STA, that the STA is to not allow certain security parameters in the STA's Network Profile (such that the Network Profile is no longer configured in certain transition modes) for subsequent (re)associations to the AP's network.

A Network Profile configured on a STA might be configured in certain transition modes (possibly also with other legacy security algorithms enabled). For example, a WPA3-Personal STA implementation might have a Network Profile configured in WPA3-Personal Transition Mode by default, which enables a legacy PSK algorithm. However, at such time that (all) BSSs in the network have WPA3-Personal enabled, APs in, that network can use the Transition Disable indication to cause the STA to reconfigure its Network Profile to WPA3-Personal Only Mode, and therefore provide protection against subsequent downgrade attacks.

8.2 Transition Disable Deployment Guide

Since misconfiguration of Transition Disable on a given BSS can impact a STA’s ability to subsequently connect to other BSSs in the same network (which might have different security configurations) during the lifetime of the Network Profile, it is important that the decision to enable Transition Disable on a given BSS is made based on knowledge of its impact at the network level.

When a BSS is configured on an AP, the AP shall not enable Transition Disable on that BSS by default.

NOTE: In some deployments, the decision to enable Transition Disable on a given BSS might be made by a centralized entity (e.g., WLAN controller) that manages the security configuration of other BSSs in the network, and therefore has knowledge of the impact at the network level. In other implementations, alternative means might be used to gain knowledge of the impact at the network level; the decision to enable Transition Disable might not necessarily involve explicit configuration by a network administrator.

NOTE: An AP that enables Transition Disable on a BSS is not required to disable the corresponding transition mode(s) on that BSS. For example, the APs in a WPA3-Personal network might enable Transition Disable on their BSSs to ensure that all STAs that support WPA3-Personal are protected against downgrade attack, but while still enabling WPA3-Personal Transition Mode on those BSSs so that legacy STAs can connect.

Transition Disable is indicated in the Transition Disable KDE, which is in the format defined in 12.7.2 of [1]. Little endian encoding is used for multi-byte fields and subfields. Its format is shown in Table 4. The length of the Transition Disable field is variable.

8.3 Transition Disable Requirements

8.3.1 AP Requirements

If an AP supports Transition Disable and Transition Disable is enabled in a BSS Configuration, an AP shall include a Transition Disable KDE (Table 4) in the Key Data field of Message 3 of all 4-way handshakes, or in the Key Delivery element of (Re)association Response frames when FILS authentication is used, for all WPA3 and Wi-Fi Enhanced Open associations in that BSS.

The AP shall not include the Transition Disable KDE in 4-way handshakes for WPA2 or WPA associations.

NOTE: This is to avoid potential interoperability issues with legacy STAs.

NOTE: Transition Disable is not indicated during FT authentication; however, it is indicated in the 4-way handshake of the FT Initial Mobility Domain Association.

8.3.2 STA Requirements

If all the following conditions are true:

- A STA supports Transition Disable, and
- The STA received a protected Transition Disable KDE from its associated AP, and
- The STA has obtained user confirmation (if applicable to the STA's implementation)

the STA's Network Profile for that SSID:

- Shall disable use of WEP and TKIP
- Shall disable association without negotiation of PMF
- Shall, for each bit other than bit 3 in the Transition Disable Bitmap field (Table 5) that is equal to 1 (one):
  - If the STA connected to the AP using one of the algorithms listed for the corresponding bit in the Most Secure Algorithms column of Table 5, disable all algorithms listed for the corresponding bit in the Transition Algorithms column
- May, if bit 3 in the Transition Disable bitmap is equal to 1 (one) and the STA connected to the AP using OWE AKM, disable use of Open system authentication without encryption.
  - NOTE: This action is potentially vulnerable to an active denial-of-service attack since the connection using OWE AKM is unauthenticated.

The STA shall not take any action for bits in the Transition Disable Bitmap field that are equal to 0 (zero), or for bits equal to 1 (one) where the above conditions do not apply.

NOTE: Notwithstanding other requirements defined in this specification, other security algorithms that are not listed in either column for the corresponding bit are not required to be disabled. NOTE: For the lifetime of a Network Profile, a Transition Disable policy shall apply to all subsequent (re)associations to all BSSs with the corresponding SSID.

Table 4. Transition Disable KDE format

Field	Size (Octets)	Value (Hex)	Description
Element ID	1	0xDD	IEEE 802.11 KDE type
Length	1	Variable	Length of the following fields in the IE in octets.
OUI	3	0x50-6F-9A	Wi-Fi Alliance specific OUI (refer to sub-clause 9.4.1.31 of [1])
OUI Type	1	0x20	Identifying the type and version of the Transition Disable KDE
Transition Disable Bitmap	Variable	Variable	Bit field indicating transition modes (see Table 5).

Table 5. Transition Disable Bitmap field index values

Bit	Name	Most secure algorithms	Transition algorithms
0	WPA3-Personal Only	AKM suite selector 00-0F-AC:8 (SAE) or 00-0F-AC:24 (SAE using group-dependent hash)	All PSK and FT over PSK AKM suite selectors (i.e., 00-0F-AC:2, 00-0F-AC:4. 00-0F-AC:6, 00-0F-AC:19 and 00-0F-AC:20)
1	SAE-PK Only	AKM suite selectors 00-0F-AC:8 or 00-0F-AC:24 when using SAE-PK	All SAE and FT over SAE AKM suite selectors when **not** using SAE-PK (i.e., 00-0F-AC:8, 00-0F-AC:9, 00-0F-AC:24, 00-0F-AC:25) All PSK and FT over PSK AKM suite selectors
2	WPA3-Enterprise	AKM suite selector 00-0F-AC:5 (IEEE 802.1X using SHA-256)	AKM suite selector 00-0F-AC:1 (IEEE 802.1X using SHA-1)
3	Wi-Fi Enhanced Open	AKM suite selector 00-0F-AC:18 (OWE)	Open system authentication without encryption

9 Privacy Extension mechanisms

This section defines various mechanisms for protecting and maintaining privacy on Wi-Fi networks. A STA that supports Privacy Extension mechanisms shall enable the following features out of the box.

9.1 Randomized MAC address

The factory provisioned MAC address of a client is a stable, globally unique device identifier that uniquely identifies a client in a LAN environment. Without MAC privacy enhancements, it is used in each frame the station transmits while connected to a BSS, but also in each frame transmitted while disconnected, for example, during an active scanning, or upon detection of Passpoint capable APs, thus notifying about its existence.

MAC privacy enhancements are specified in IEEE Std. 802.11 [1] to mitigate passive tracking based on MAC address.

9.1.1 Composition of a randomized MAC address

A STA shall construct a randomized MAC address as specified in Section 12.2.10 of [1]. Additionally, the randomized bits in the MAC address shall be generated using a Pseudo-Random Number Generator (PRNG) or a cryptographically stronger implementation. If an AP does not advertise a MAC address policy, described in Section 11.23.3.3.16 of [1], then 46 bits of the MAC address shall be randomized. The U/L bit shall be set to 1 and the I/G bit shall be set to 0.

9.1.2 Authentication and Association

When a STA uses the same MAC address for association to multiple ESSs, user location fingerprinting becomes more possible.

A STA shall construct a uniquely randomized MAC address per SSID, following the requirements given in Section 12.2.10 of [1] unless a saved Wi-Fi Network Profile explicitly requires using its globally unique MAC address. The STA may construct a new randomized MAC address for an SSID at its discretion.

9.1.3 Active Scanning Procedures

When performing active scanning procedures, the STA shall construct a randomized MAC address following the requirements defined in in Section 12.2.10 of [1], for transmission of Probe Request frames. The STA shall use a randomized MAC address for scanning while the STA is not associated to a BSS. The STA shall construct a new randomized MAC address for each active scanning instance.

9.1.4 ANQP Procedures

For each ANQP exchange, a STA shall use a new randomized MAC address following the requirements defined in Section 12.2.10 of [1], while the STA is not associated to a BSS.

9.2 Sequence Numbers

Sequence numbers are a predictable identifier that can allow multiple MAC addresses to be associated with each other, which allows an attacker to identify a particular device regardless of a random MAC address.

A STA shall follow the procedures defined in Section 12.2.10 of [1] when changing its MAC address to a new random address.

9.3 Scrambler Seed

The 802.11 scrambler is a 7-bit Linear-Feedback Shift Register (LFSR) with an initial state of a pseudo random non-zero value, which is XORed with the frame payload when OFDM is used. Implementations that reseed the scrambler using the previous frame's data allow multiple MAC addresses to be associated with each other, which allows an attacker to identify a particular device regardless of a random MAC address.

A STA shall follow the scrambler seed procedures defined in Section 12.2.10 of [1] when changing its MAC address to a new random address.

9.4 GAS

GAS queries reveal the existence of a STA in the environment. The dialog token is a predictable identifier that can lead to user identification in every location the client sends GAS queries, regardless of a randomized MAC address.

A STA shall use a randomized dialog token for every new GAS exchange.

10 MLD security

For the (Re)Association Request frame sent by a non-AP MLD to an AP MLD:

- The A2 field shall be the same as the A2 field of the latest Authentication frame(s) sent from the non-AP MLD to the AP MLD that leads to a successful authentication to set the state to State 2
- The A1 field shall be the same as the A1 field of the latest Authentication frame(s) sent from the non-AP MLD to the AP MLD that leads to a successful authentication to set the state to State 2

NOTE: If non-AP MLD has performed a successful authentication beforehand with an AP MLD to save time for the later association, and the non-AP MLD cannot transmit to the AP affiliated with the AP MLD that responds to the Authentication frame sent from the non-AP MLD that leads to successful authentication (for example, due to the reason that AP MLD removes the affiliated AP), then the non-AP MLD might initiate another authentication exchange with AP MLD through any AP affiliated with the AP MLD using PMKSA caching.

11 Security Constraints on Wi-Fi Alliance Generational PHYs and Bands

11.1 Overview

Security constraints for Wi-Fi Alliance Generational PHYs and Bands are defined in the following clauses of the IEEE 802.11 standard and the subsections below.

- Clause 12.12 of IEEE 802.11ax-2021 amendment [13] (basis for Wi-Fi 6)
- Clause 12.12 of IEEE 802.11 REVme [14]
- Clause 12.12 of IEEE 802.11be draft amendment [15] (basis for Wi-Fi 7)

11.2 Constraints in the 6 GHz band

A WPA3 AP or STA operating in the 6 GHz band shall abide by the constraints defined in subclause 12.12.2 of [13] and additionally:

- When an AP is operating a BSS in the 6 GHz band:
    a. The AP's BSS Configuration shall not allow TKIP
    b. The AP's BSS Configuration shall not be configured in WPA3-Personal Transition Mode
    c. The AP's BSS Configuration shall not allow 802.1X SHA-1 AKM (and therefore the BSS shall not be configured in WPA3-Enterprise Transition Mode)
    d. The AP's BSS Configuration shall be PMF Required, i.e., AP shall set MFPC to 1 and MFPR to 1 in beacons and probe responses of the BSS
    e. The AP's BSS Configuration shall not allow the SAE Hunting and Pecking mechanism
    f. The AP's BSS Configuration shall not allow Wi-Fi Enhanced Open Transition Mode (i.e., where the OWE Transition Mode element is included in Beacons and Probe responses)
- When a WPA3 STA is connecting to an AP in the 6 GHz band:
    a. The STA shall not allow: WEP, TKIP, any PSK (or FT PSK) AKM, 802.1X SHA-1 AKM, or the SAE Hunting and Pecking mechanism
    b. The STA shall always negotiate PMF
    c. The STA shall not allow Open System authentication without encryption

11.3 Constraints for EHT or MLO (Wi-Fi 7)

When an AP is operating a BSS with EHT or MLO enabled, the AP shall abide by the constraints for that BSS defined in subclause 12.12.9 of [15] and additionally:

- The AP's BSS Configuration shall not allow any PSK AKM or 802.1X SHA-1 AKM to be used in an association that negotiates use of EHT or MLO
  NOTE: The AP's BSS Configuration is still allowed to advertise these AKMs and might still enable these AKMs for backwards interoperability with STAs in an association that does not negotiate use of EHT nor MLO.
- The AP's BSS Configuration shall not enable legacy open
  NOTE: Wi-Fi Enhanced Open might be used for unauthenticated access with EHT or MLO.
- The AP's BSS Configuration shall not allow Wi-Fi Enhanced Open Transition Mode (i.e., where the OWE Transition Mode element is included in Beacons and Probe responses).

When a STA associates to an AP with EHT or MLO enabled, the STA shall abide by the constraints defined in subclause 12.12.9 of [15] and additionally:

- The STA shall not negotiate any PSK AKM or 802.1X SHA-1 AKM in an association that negotiates use of EHT or MLO
  NOTE: If the AP does not advertise any AKM that would be allowed with EHT or MLO, the STA might associate with EHT and MLO disabled, i.e., fall back to HE (Wi-Fi 6) functionality and select one of the advertised AKMs.
- The STA shall not allow Open System authentication without encryption in an association that negotiates use of EHT or MLO.

11.4 Constraints in the Sub 1 GHz band

A WPA3 AP or STA operating in the Sub 1 GHz band shall abide by the constraints defined in subclause 12.12.6 of [14] and additionally:

- When an AP is operating a BSS in the Sub 1 GHz band:
  d. The AP's BSS Configuration shall not allow TKIP
  e. The AP's BSS Configuration shall not be configured in WPA3-Personal Transition Mode
  f. The AP's BSS Configuration shall be PMF Required, i.e., AP shall set MFPC to 1 and MFPR to 1 in beacons and probe responses of the BSS
  g. The AP's BSS Configuration shall not allow the SAE Hunting and Pecking mechanism
  h. The AP's BSS Configuration shall not allow Wi-Fi Enhanced Open Transition Mode (i.e., where the OWE Transition Mode element is included in Beacons and Probe responses)
- When a WPA3 STA is connecting to an AP in the Sub 1 GHz band:
  a. The STA shall not allow: WEP, TKIP, any PSK (or FT PSK) AKM, or the SAE Hunting and Pecking mechanism
  b. The STA shall always negotiate PMF
  c. The STA shall not allow Open System authentication without encryption

12 Operating Channel Validation

Operating Channel Validation (OCV) is defined in [14].

An AP shall not enable OCV in its BSS Configuration if PMF is not enabled in that BSS Configuration.

A STA shall not use OCV for an association if PMF is not used for that association.

13 Requirements on data packet handling

The requirements in this section apply to all WPA3 APs and STAs when operating in all modes.

Failure to implement these requirements correctly may expose the vendor implementation to attack and/or compromise the network.

13.1 Fragments encrypted with different keys

Requirement:

A device shall not assemble fragments encrypted with different keys into the same MSDU/MMPDU.

Background:

This vulnerability stems from different keys being used to protect MSDUs. Although it is a good security practice to ensure using one key for all fragments of a frame, it is not strictly followed in some existing device implementations, especially in the midst of a transitional period such as key renewal. An adversary can exploit this to inject additional fragments for attack with different keys when a key renewal happens. Thus, a receiving device shall check that only one key is used for decryption of all fragments of an MSDU/MMPDU. A receiving device may implement this requirement by discarding a fragmented MSDU/MMPDU if its fragments are encrypted with different keys.

13.2 Cache attacks on frame fragments

Requirement:

If a new association or reassociation happens, a receiving device shall discard any fragments from an incomplete MSDU/MMPDU from previous association.

Background:

If a receiving device retains previous fragments upon a new association or reassociation, an adversary can inject malicious fragments into memory to be included with new fragments after a new association. A device can effectively stop this type of attack by clearing incomplete fragments from memory upon a new association or reassociation.

13.3 Non-consecutive PN fragments

Requirement:

During defragmentation, a receiving device shall check that PN (packet number) increments by exactly 1 for consecutive fragments. If not, the receiving device shall discard any fragment that does not follow this requirement.

Background:

If a device reassembles fragments during the defragmentation process, it shall check that fragments of an MSDU/MMPDU have PNs that are ordered with an increment of exactly 1. If a device cannot observe this order from the assembly of the fragments, then the device shall discard the unexpected fragment(s). Without stringent detection of non-consecutive packet numbered fragments, an adversary can abuse this vulnerability by adding intentional fragments in between to achieve the goal of exfiltration.

13.4 Plaintext fragments in a protected network

Requirement:

When an MSDU or MMPDU is encrypted, a receiving device shall verify that every fragment from the respective MSDU/MMPDU is encrypted. Otherwise, the device shall discard the unencrypted fragments.

Background:

Some existing devices in a protected network do not differentiate plaintext fragments from that of encrypted ones for an MSDU/MMPDU during defragmentation. This offers an attacker a possible way to mix intended plaintext fragments with the normal encrypted ones. To avoid such a situation, a receiving device shall not accept plaintext fragments when the corresponding MSDU/MMPDU is expected to be encrypted.

13.5 Accepting plaintext broadcast or multicast fragments

Requirement:

Broadcast or multicast frames shall not be fragmented, and a receiving device shall discard such fragments upon reception.

Background:

Broadcast or multicast frames shall not be fragmented. However, research has found that vulnerable existing devices accept plaintext broadcast fragments. This allows an adversary to inject arbitrary plaintext fragments into the network during and after the 4-way handshake.

13.6 Accepting plaintext A-MSDU frames that start with an EAPOL LLC/SNAP header

Requirement:

A device shall apply the frame protection rules to all the A-MSDU subframes individually. A receiving device shall discard subframes with EtherType other than EAPOL from a plaintext A-MSDU if the network uses encryption.

Background:

Due to the fact that initial plaintext 4-way handshake frames are accepted, an attacker can disguise a plaintext A-MSDU under a valid EAPOL LLC/SNAP header, i.e., the first 8 bytes correspond to a valid RFC1042 (EAPOL LLC/SNAP) header. A vulnerable existing device might process subsequent plaintext subframes, allowing an adversary to inject arbitrary plaintext data and to bypass secured state of the connection.

13.7 Plaintext frame attack in a protected network

Requirement:

A receiving device shall discard plaintext Data frames in a protected network, except for EAPOL frames during the initial 4-way handshake. A receiving device shall discard plaintext robust Management frames when PMF is enabled.

Background:

Vulnerable existing devices accept plaintext Data frames and plaintext robust Management frames even though security is negotiated, which undermines the security provided by RSN.

13.8 Plaintext fragmented frames in a protected network

Requirement:

When an MSDU or MMPDU is expected to be encrypted, a receiving device shall discard any unencrypted fragments.

Background:

Vulnerable existing devices accept plaintext fragmented frames even though a secure connection is established. This allows an attacker to inject intended plaintext frames and ignore the protected state of the network. Therefore, a device shall not accept plaintext fragments when the corresponding MSDU/MMPDU is encrypted.

13.9 Forwarding EAPOL frames

Requirement:

An AP shall not forward EAPOL frames.

Background:

This attack is only applicable to existing Access Points (APs) that forward EAPOL frames. An adversary can launch denial-of-service attacks by flooding the connected network clients with such frames. This also allows the attacker to further exploit other vulnerabilities in clients connected to the vulnerable APs.

13.10 TKIP MIC of fragmented frames

Requirement:

A receiving device shall perform TKIP MIC check and if it fails at the MSDU level, the device shall discard the MSDU and invoke countermeasures as appropriate.

Background:

Although use of TKIP is disallowed in all WPA3 modes, WPA3 devices might enable TKIP when operating in certain legacy modes.

Some existing devices do not perform MIC (message integrity code) check for fragmented TKIP frames. Such a vulnerability can be abused by injecting frames and facilitating further attacks in a network that supports TKIP. A device shall not skip MIC verification and shall discard affected MSDU(s) upon failure and perform appropriate countermeasures.

13.11 Treating fragmented frames as full frames

Requirement:

A device shall support defragmentation of a frame according to the 802.11 standard [14]. During defragmentation, if a device detect errors in processing any of the fragments of an MSDU or MMPDU then it shall discard the invalid fragments.

Background:

Some existing devices treat fragments from a frame independently as full frames, by ignoring the More Fragments subfield in the Frame Control field of the 802.11 MAC header of a frame. In addition, some existing devices do not support the (de)fragmentation process. These devices can still process received fragmented frames by treating them as independent full frames. This opens up a possibility for an attacker to inject malicious data in retained fragments. Thus, devices shall implement the defragmentation correctly. They shall also keep track of all the fragments belonging to an MSDU/MMPDU.

14 RSN overriding

14.1 General

Extensions to the RSNE and RSNXE have resulted in issues with previously deployed STAs being unable to complete connection with an AP that is enabling newer functionality, e.g., when advertising multiple AKM suite selectors. Since software updates to fix these issues might not be available for some previously deployed STAs, some network deployments depend on other mechanisms to avoid known interoperability issues. RSN overriding provides such a mechanism in a manner that allows an AP to advertise limited RSN parameters in the RSNE and the RSNXE (or fully omitting the RSNXE), so that the deployed STAs would not be exposed to the extensions that have resulted in issues. The extended set of RSN parameters is advertised in new elements to allow STAs that support the override mechanism to use newer RSN options. Previously deployed STAs that are not updated to support this mechanism are assumed to ignore the new elements.

Since the RSN overriding mechanism hides the full set of available RSN options from STAs that do not support the mechanism and might result in them not being able to use the strongest commonly enabled option, the mechanism should be used only in cases where STAs are expected to have issues connecting to an AP with an RSNE that would advertise all the enabled options.

The RSN overriding mechanism has two components - the RSNE overriding mechanism and the RSNXE overriding mechanism. The RSNXE overriding mechanism cannot be used without the RSNE overriding mechanism.

The RSNE overriding mechanism uses three elements to allow the set of indicated AKM and pairwise cipher suite selectors in each element to be minimized. This is done to reduce the risk of interoperability issues with parsing and processing of the payload of the elements, and to reduce the need to modify the elements used by deployed STAs when introducing new capabilities. The RSNE is expected to be used to indicate a WPA2-only configuration in the 2.4 and 5 GHz bands for maximum compatibility, while the RSNE in the 6 GHz band and the RSNE Override element and the RSNE Override 2 element are expected to indicate WPA3 or Wi-Fi Enhanced Open configurations. The RSNE Override element is used to advertise a more secure set of parameters than the ones in the RSNE in cases where inclusion of those parameters in the RSNE could cause interoperability issues with deployed STAs. The RSNE Override 2 element is used to advertise a more secure set of parameters than the ones in the RSNE Override element (if present) when the administrator of the AP wants to minimize the number of advertised AKM and pairwise cipher suite selectors in each of the elements. (Wi-Fi 7) AP MLDs use the RSNE Override 2 element to advertise common parameters for all affiliated links.

The RSNXE overriding mechanism uses two elements to allow an AP to advertise different sets of extended RSN capabilities. This is done to reduce the risk of interoperability issues with parsing and processing of the payload of the elements. This specification defines the RSN overriding mechanism as an extension to IEEE Std 802.11-2020. For the clarity of the definition, a virtual dot11 MIB variable dot11RSNOverrideActivated is used to manage when the mechanism is activated. How this MIB variable is implemented is outside the scope of this specification.

14.2 RSN overriding mechanism

The Payload field of the RSNE Override element and the RSNE Override 2 element uses the same format, as described in Section 14.4, as the Information field of the RSNE. The RSNE Override element and RSNE Override 2 element override the Pairwise Cipher Suite Count, Pairwise Cipher Suite List, AKM Suite Count, AKM Suite List, and RSN Capabilities fields of the RSNE in the same frame. The RSNE Override element and RSNE Override 2 element may also specify the Group Management Cipher Suite field in cases where that field is not included in the RSNE. The RSNE Override element and the RSNE Override 2 element shall indicate (either explicitly or implicitly by default) the same Group Data Cipher Suite field as the Group Data Cipher Suite field in the RSNE. If the group management cipher suite is indicated in the RSNE (either explicitly or implicitly by default), the RSNE Override element and the RSNE Override 2 element shall indicate the same group management cipher suite as the group management cipher suite indicated in the RSNE. If the RSNE does not indicate a group management cipher suite, the RSNE Override element and the RSNE Override 2 element shall indicate the same group management cipher suite.

The RSNE Override element and the RSNE Override 2 element shall not include the AKM suite selectors 00-0F-AC:1 (IEEE 802.1X using SHA-1), 00-0F-AC:2 (PSK using SHA-1), 00-0F-AC:4 (FT over PSK), 00-0F-AC:6 (PSK using SHA-256), 00-0F-AC:19 (FT over PSK using SHA-384), or 00-0F-AC:20 (PSK using SHA-384).

If the RSN Capabilities field is present in the RSNE and any of the MFPR, MFPC, Joint Multi-band RSNA, Extended Key ID for Individually Addressed Frames, or OCVC bits in that field are set to 1, the corresponding bits in the RSNE Override element and the RSNE Override 2 element shall be set to 1. If any of these bits in the RSNE are set to 0 or the RSN Capabilities field is not present in the RSNE, the corresponding bits in the RSN Capabilities field in the RSNE Override element and the RSNE Override 2 element may be set to 1. If any of these bits in the RSNE Override element are set to 1, the corresponding bits in the RSNE Override 2 element shall be set to 1. Other bits in the RSN Capabilities field of the RSNE shall not be overridden.

The method of an AP selecting which parameters to include in the RSNE and RSNXE versus the RSNE Override element, the RSNE Override 2 element, and the RSNXE Override element is outside the scope of this standard. For the specific case of WPA3-Personal Compatibility Mode, the set of parameters included in each element is defined in Section 2.4.

The Payload field of the RSNXE Override element, as described in Section 14.4, uses the same format as the Information field of the RSNXE. It overrides values in the RSNXE (if present) or the omission of the RSNXE. If the RSNXE is included, all advertised extended RSN capabilities in that element shall also be advertised in the RSNXE Override element.

An AP shall include the RSNE Override element in Beacon and Probe Response frames for a given BSS when dot11RSNAActivated and dot11RSNOverrideActivated are true at the AP for that BSS, and the Payload field of the RSNE Override element differs from the Information field of the RSNE. An AP shall include the RSNE Override 2 element in Beacon and Probe Response frames for a given BSS when dot11RSNAActivated and dot11RSNOverrideActivated are true at the AP for that BSS, and the Payload field of the RSNE Override 2 element differs from the Payload field of the RSNE Override element and the Information field of the RSNE. An AP shall include the RSNXE Override element in Beacon and Probe Response frames for a given BSS when dot11RSNAActivated and dot11RSNOverrideActivated are true at the AP for that BSS, any subfield of the Extended RSN Capabilities field in this element is nonzero, except the Field Length subfield, and either the RSNXE is not included or the Payload field of the RSNXE Override element differs from the Information field of the RSNXE.

A (Wi-Fi 7) AP MLD with dot11RSNOverrideActivated set to true shall include an identical RSNE Override 2 element in Beacon and Probe Response frames on all affiliated links as a common set of parameters for multi-link associations. A (Wi-Fi 7) AP MLD with dot11RSNOverrideActivated set to true shall include an identical RSNXE Override element in Beacon and Probe Response frames on all affiliated links as a common set of parameters for multi-link associations if the AP includes an RSNXE Override element on any affiliated link.

NOTE: A (Wi-Fi 7) AP MLD includes an identical RSNXE in Beacon and Probe Response frames on all affiliated links as a common set of parameters for multi-link associations if the AP MLD includes an RSNXE on any affiliated link (see 12.6.2 of IEEE Std 802.11be-2024).

An AP shall not include the RSNXE Override element in Beacon and Probe Response frames if neither the RSNE Override element nor the RSNE Override 2 element are included.

NOTE: IEEE 802.11 might extend the RSNXE in the future by adding new fields after the Extended RSN Capabilities field. If that is done, the same extension would apply to the RSNXE Override element.

A STA with dot11RSNAActivated and dot11RSNOverrideActivated set to true shall use the Payload field of either the RSNE Override element or the RSNE Override 2 element, instead of the Information field of the RSNE, when processing Beacon and Probe Response frames that include an RSNE Override element or an RSNE Override 2 element, where that Payload field advertises a combination of parameters that the STA supports. When a (Wi-Fi 7) STA (i.e. non-AP MLD) with dot11RSNAActivated and dot11RSNOverrideActivated set to true establishes a multi-link association with a (Wi-Fi 7) AP MLD that uses RSN overriding, it shall use the Payload field of the RSNE Override 2 element when processing Beacon and Probe Response frames that include that element from all affiliated APs.

NOTE 1—A STA that is not establishing a multi-link association might need to select the RSNE Override element over the RSNE Override 2 element if it does not support any combination of the pairwise ciphers and AKM suites advertised in the RSNE Override 2 element. The STA might need to select the RSNE over the RSNE Override element and the RSNE Override 2 element if it does not support any combination of the pairwise ciphers and AKM suites advertised in the RSNE Override element nor any combination of the pairwise ciphers and AKM suites advertised in the RSNE Override 2 element.

A STA with dot11RSNAActivated and dot11RSNOverrideActivated set to true shall use the contents of the RSNXE Override element instead of the contents of the RSNXE when processing Beacon and Probe Response frames that

include both elements. A STA with dot11RSNAActivated and dot11RSNOverrideActivated set to true shall use the contents of the RSNXE Override element when processing Beacon and Probe Response frames that include the RSNXE Override element and do not include the RSNXE. A STA with dot11RSNAActivated and dot11RSNOverrideActivated set to true shall use the contents of the RSNXE (if present) when processing Beacon and Probe Response frames that do not include the RSNXE Override element.

A STA with dot11RSNAActivated and dot11RSNOverrideActivated set to true shall include the RSN Selection element with the Variant field set to 0 in (Re)Association Request frames when (re)associating with an AP using that AP's RSNE in Beacon and Probe Response frames to determine enabled RSN parameters if that AP advertises RSNE Override element or RSNE Override 2 element in its Beacon frames.

A STA with dot11RSNAActivated and dot11RSNOverrideActivated set to true shall include the RSN Selection element with the Variant field set to 1 in (Re)Association Request frames when (re)associating with an AP using that AP's RSNE Override element in Beacon and Probe Response frames to determine enabled RSN parameters.

A STA with dot11RSNAActivated and dot11RSNOverrideActivated set to true shall include the RSN Selection element with the Variant field set to 2 in (Re)Association Request frames when (re)associating with an AP using that AP's RSNE Override 2 element in Beacon and Probe Response frames to determine enabled RSN parameters.

In case of MLO, the RSN Selection element shall indicate which RSNE variant advertised by the AP was used on the link on which the (Re)Association Request frame was sent. The value in the RSN Selection element is not applicable to other links, e.g., due to inheritance for per-STA profiles, and STAs are not required to include this element for other requested links.

The RSNE Override element and the RSNE Override 2 element shall not be present in (Re)Association Request frames.

If the AP includes the RSNE Override element or the RSNE Override 2 element, the STA shall indicate its selected RSN parameters in the RSNE included in the (Re)Association Request frame even if the selection is based on the AP’s RSNE Override element or the AP's RSNE Override 2 element instead of the RSNE. The STA shall indicate its extended RSN capabilities in the RSNXE included in the (Re)Association Request frame if any subfield of the Extended RSN Capabilities field in this element is nonzero, except the Field Length subfield.

NOTE 2—The RSNXE Override element is not present in the (Re)Association Request frame.

NOTE 3—The RSNE Override element, the RSNE Override 2 element, and the RSNXE Override element are not present in the (Re)Association Response frame.

Two elements are defined for overriding the RSNE, to allow a minimum number of AKM and pairwise cipher suite selectors to be included in each element (RSNE, RSNE Override element, and RSNE Override 2 element) for simplicity to reduce risk of implementation issues. APs and STAs that support RSN overriding shall support both the RSNE Override and RSNE Override 2 elements. A STA that supports at least one possible combination of the parameters in an RSNE Override 2 element advertised by an AP selects and uses that element instead of the RSNE or the RSNE Override element. A STA that did not select the RSNE Override 2 element and that supports at least one possible combination of the parameters in an RSNE Override element advertised by an AP selects and uses the RSNE Override element instead of the RSNE.

A STA with dot11RSNAActivated and dot11RSNOverrideActivated set to true shall select only a single element from the set of the RSNE, the RSNE Override element, and the RSNE Override 2 element that the AP advertises and use that in all (re)associations with that AP. The STA shall indicate the element that it selected to be used for a (re)association in the RSN Selection element in the (Re)Association Request frame.

NOTE 4—The STA selecting a single element from the set of RSNE, RSNE Override element, and RSNE Override 2 element implies that the STA cannot selectively pick components from multiple elements (e.g., a pairwise cipher from the RSNE Override element and an AKM from the RSNE).

NOTE 5—The STA selecting a single element from the set of RSNXE and RSNXE Override element implies that the STA cannot selectively pick components from multiple elements (e.g., one extended RSN capability bit from the RSNXE and another one from the RSNXE Override element).

14.3 Downgrade protection

A STA indicates support for RSN overriding by using a special construction of its SNonce value. This is done for all (re)associations regardless of whether RSN overriding is used for the (re)association. This allows the AP to determine that all the RSNE and RSNXE combinations from Beacon and Probe Response frames can safely be included in the frames that enable protected validation of the elements that STAs use during AP discovery and selection. In addition, the STA that uses this construction of its SNonce value shall ignore any unknown KDE or element in the Key Data field of EAPOL-Key frames. This allows the AP to determine that additional data can be added to message 3 of the 4-way handshake and message 1 of the group key handshake.

An AP with dot11RSNAActivated and dot11RSNOverrideActivated set to true shall be capable of processing any length of the RSNXE that is smaller than or equal to 257 octets and greater than or equal to 3 octets, included in the Key Data field of message 2 to calculate the MIC to validate that message even if the RSNXE indicates support of a feature that is not supported by the AP.

An AP with dot11RSNAActivated and dot11RSNOverrideActivated set to true shall ignore any unknown KDE or element in the Key Data field of EAPOL-Key frames.

NOTE 1—This mechanism based on SNonce is used to allow the capability indication to be provided in a manner that is protected due to the existing binding to the derived PTK while not introducing any new changes in either the RSNE or the RSNXE to avoid interoperability issues with deployed STAs.

A STA that supports RSN overriding constructs its SNonce for the 4-way handshake by setting the last six octets to be the SNonce cookie. This is used in message 2 to allow the AP to detect the special case and as the SNonce in derivation of the PTK.

If an AP with which an RSN overriding capable STA is associated does not enable RSN overriding and does not advertise support for some of the extended RSN capabilities that the STA supports, the STA may omit the RSNXE completely, or may omit indication of the extended RSN capabilities that the AP does not support, in the (Re)Association Request frame and in message 2 of the 4-way handshake.

A STA that included an RSN Selection element in the (Re)Association Request frame shall include the same element in message 2 of the 4-way handshake.

An AP that receives a (Re)Association Request frame with an RSN Selection element shall use that element in combination with the RSNE and the RSNXE, if present, when verifying that the STA selected a valid combination of RSN parameters for the BSS. In case of MLO, the AP shall ignore the contents of the RSN Selection element and its omission (e.g., through non-inheritance for a per-STA profile) for links other than the association link.

When an AP with dot11RSNAActivated and dot11RSNOverrideActivated set to true receives message 2 of the 4-way handshake with a valid Key MIC field, it shall verify that either (1) the RSN Selection element is included in the (Re)Association Request frame the same element with the same contents is included in message 2, or (2) the RSN Selection element is included in neither the (Re)Association Request frame nor message 2. If this verification indicates a mismatch, the AP shall abandon the 4-way handshake and disconnect the STA.

When an AP with dot11RSNAActivated and dot11RSNOverrideActivated set to true receives message 2 of the 4-way handshake, it shall check the last six octets of the SNonce. If the last six octets are the SNonce cookie, the AP shall include all RSNE and RSNXE variants it advertised in Beacon and Probe Response frames in message 3. Specifically, these variants are the RSNE, the RSNE Override element, the RSNE Override 2 element, the RSNXE, and the RSNXE Override element. These are carried directly in the non-multi-link association case and encapsulated in the MLO Link and RSN Override Link KDEs (i.e., one of each KDE per link) in the multi-link association case.

A STA that supports RSN overriding shall verify that message 3 of the 4-way handshake contains all the RSNE and RSNXE variants that it has received from AP, or the affiliated APs in case of multi-link association, in Beacon and Probe Response frames. Validation of each such element follows the rules described in 12.7.6 (4-way handshake) of [1] for the RSNE and RSNXE. If any of these verification steps indicates a mismatch, the STA shall disassociate or deauthenticate.

When using the FT protocol, a STA that supports RSN overriding shall construct its SNonce with the last six octets set to be the SNonce cookie.

When an AP with dot11RSNAActivated and dot11RSNOverrideActivated set to true receives a Reassociation Request frame for the FT protocol with the last six octets of the SNonce being the SNonce cookie and the AP accepts the

reassociation request, it shall include all RSNE and RSNXE variants it advertised in Beacon and Probe Response frames in the Reassociation Response frame. Specifically, these variants are the RSNE, the RSNE Override element, the RSNE Override 2 element, the RSNXE, and the RSNXE Override element. These are carried directly in the non-multi-link association case and encapsulated in the Per-STA Profile subelement of the Basic Multi-Link element in the multi-link association case.

When RSN overriding is used with the FT protocol, the RSN Selection element shall be included in the Element Count subfield of the MIC Control field in the FTE in the Reassociation Request frame. The MIC for this FTE in the Reassociation Request frame shall be calculated on the concatenation of the data described in 13.8.4 of [1] followed by the RSN Selection element.

When an AP that supports RSN overriding verifies the FTE in the Reassociation Request frame, it shall follow the rules described in 13.8.4 of [1] with the extensions described above.

When RSN overriding is used with the FT protocol, all the RSNE and RSNXE variants (the RSNE, the RSNXE, the RSNE Override element, the RSNE Override 2 element, and the RSNXE Override element) that the AP advertises in the Beacon frames and Probe Response frames shall be included in the Element Count subfield of the MIC Control field in the FTE in the Reassociation Response frame. The MIC for this FTE in the Reassociation Response frame shall be calculated on the concatenation of the data described in 13.8.5 of [1] followed by the elements in the following order: (1) if the Basic Multi-Link element is not included in the Reassociation Response frame: the RSNE Override element, the RSNE Override 2 element, the RSNXE Override element (each included if present in the Beacon and Probe Response frames); or (2) if the Basic Multi-Link element is included in the Reassociation Response frame: RSNE Override elements (if present) corresponding to all requested links that exist in increasing order of link ID, RSNE Override 2 elements (if present) corresponding to all requested links that exist in increasing order of link ID, RSNXE Override elements (if present) corresponding to all requested links that exist in increasing order of link ID.

When a STA that supports RSN overriding verifies the FTE in the Reassociation Response frame, it shall follow the rules described in 13.8.5 of [1] with the extensions described above.

14.4 Information elements, KDEs, and definitions for RSN overriding

This section defines the RSNE Override, RSNE Override 2, RSNXE Override, and RSN Selection elements; a KDE for encapsulating these (on a per-link basis, for MLO); and an SNonce identifying octets for RSN overriding capability.

These elements are in the Vendor Specific format as defined in 9.4.2.25 of [1]. Their formats are shown in Table 6, Table 8, and Table 8.

Table 6. RSNE Override element format

Field	Size (Octets)	Value (Hex)	Description
Element ID	1	0xDD	IEEE 802.11 vendor specific element
Length	1	Variable	Length of the following fields in the element in octets.
OUI	3	0x50-6F-9A	Wi-Fi Alliance specific OUI (refer to 9.4.1.31 of [1])
OUI Type	1	0x29	Identifying this as an RSNE Override element
Payload	Variable	Variable	Information field (see 9.4.2.1 of [1]) of the RSNE as defined in 9.4.2.24 of [1].

Table 7. RSNE Override 2 element format

Field	Size (Octets)	Value (Hex)	Description
Element ID	1	0xDD	IEEE 802.11 vendor specific element
Length	1	Variable	Length of the following fields in the element in octets.
OUI	3	0x50-6F-9A	Wi-Fi Alliance specific OUI (refer to 9.4.1.31 of [1])

Field	Size (Octets)	Value (Hex)	Description
OUI Type	1	0x2A	Identifying this as an RSNE Override 2 element
Payload	variable	Variable	Information field (see 9.4.2.1 of [1]) of the RSNE as defined in 9.4.2.24 of [1].

Table 8. RSNXE Override element format

Field	Size (Octets)	Value (Hex)	Description
Element ID	1	0xDD	IEEE 802.11 vendor specific element
Length	1	Variable	Length of the following fields in the element in octets.
OUI	3	0x50-6F-9A	Wi-Fi Alliance specific OUI (refer to 9.4.1.31 of [1])
OUI Type	1	0x2B	Identifying this as an RSNXE Override element
Payload	variable	Variable	Information field (see 9.4.2.1 of [1]) of the RSNXE as defined in 9.4.2.241 of [1])

Table 9. RSN Selection element format

Field	Size (Octets)	Value (Hex)	Description
Element ID	1	0xDD	IEEE 802.11 vendor specific element
Length	1	5	Length of the following fields in the element in octets.
OUI	3	0x50-6F-9A	Wi-Fi Alliance specific OUI (refer to 9.4.1.31 of [1])
OUI Type	1	0x2C	Identifying this as an RSN Selection element
Variant	1	Variable	Indication of the RSNE variant that is used for an association: 0 = RSNE 1 = RSNE Override element 2 = RSNE Override 2 element

Table 10. RSN Override Link KDE format

Field	Size (Octets)	Value (Hex)	Description
Element ID	1	0xDD	IEEE 802.11 KDE
Length	1	Variable	Length of the following fields in the KDE in octets.
OUI	3	0x50-6F-9A	Wi-Fi Alliance specific OUI (refer to 9.4.1.31 of [1])
OUI Type	1	0x2D	Identifying this as an RSN Override Link KDE
Link ID	1	Variable	The link identifier for the affiliated STA link.
Elements	Variable	Variable	The set of RSNE Override, RSNE Override 2, and/or RSNXE Override elements that are advertised in Beacon frames for the link. These elements can be in any order.

SNonce cookie: The following six octets (in hex) are used by a STA to advertise support for RSN overriding in the last six octets of its SNonce: 50 6F 9A 00 00 29.

NOTE—SNonce is a sequence of octets with the most significant octet first. The last six octets of an SNonce refer to the six least significant octets (0x29 being the value of the last and the least significant octet). Those octets are the last six octets of a field that contains an SNonce.

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

Appendix B SAE implementation details

B.1 Rules used to evaluate the suitability of SAE groups

SAE performs public key cryptography using named Diffie-Hellman groups. The IKEv1 (RFC 2409) group registry maintained by the Internet Assigned Numbers Authority (IANA) maps the group's complete domain parameter set to a reference number. Not all registered groups are suitable for use with SAE.

The rules used to evaluate the suitability of groups are:

- No binary elliptic curve (EC2N) groups
- No groups defined over a prime field (MODP) with a prime less than 3072 bits
- No groups defined over a prime field (MODP) with a small sub-group of prime order
- No elliptic curve group with a prime less than 256-bits
- No elliptic curve group that might expose detectible timing differences when used in conjunction with the SAE.

The following table indicates the groups to be used with SAE. All other groups must not be used with SAE.

Group Number	Description	Strength Estimate (*)	Suitability
15	3072-bit MODP group	128	Suitable
16	4096-bit MODP group	152	Suitable
17	6144-bit MODP group	176	Suitable
18	8192-bit MODP group	200	Suitable
19	256-bit random ECP group (NIST)	128	Suitable (Mandatory to implement)
20	384-bit random ECP group (NIST)	192	Suitable
21	521-bit random ECP group (NIST)	256	Suitable

Table 11. Diffie-Hellman Group Suitability for SAE

(*) Strength estimate is a maximum value and can be decreased based on entropy estimates (Implementation Guidance for FIPS140-2 and the Cryptographic Module Validation Program)

NOTE: This requirement disallows use of MODP groups with a prime less than 3072 bits with SAE. The Hunting and Pecking algorithm for MODP groups is affected by timing side-channels, and the obtained information can later be used to recover the password. MODP groups 22, 23, and 24 have a small sub-group and are known to be weak; refer to "Measuring small sub-group attacks against Diffie-Hellman" by Valeta et al, 2017.

B.2 Avoiding differences in code execution

SAE implementations must avoid differences in code execution that allow side channel information collection through the cache.

Two methods exist:

- Implement SAE in such a way to use constant time operations that use the same memory access pattern regardless of the values derived from the password.
- Reduce the visibility of side channel information, for instance, by preventing sharing of cache lines between processes if efficiently supported by the hardware architecture.

An attack based on differences in code execution requires monitoring of cache access patterns on a compromised machine, one running the attacker's software. The obtained information can later be used to recover the password. When the attack is on the Hash-to-Element algorithm, the goal is to learn if the quadratic residue (QR) test in the first iteration of the Hash-to-Element algorithm succeeded or not. This information can be used in the offline password partitioning attack to recover the target's password. The implementation of the Hash-to-Element algorithm for elliptic-curve cryptography (ECC) groups does include mitigations against side channel attacks. Those mitigations include performing extra dummy iterations on random data and blinding of the underlying cryptographic calculation of the quadratic residue test. Preventing the installation of malicious software may be an effective additional mitigation approach for some device categories.