WPA3™
Specification
Version 3.1

WI-FI ALLIANCE PROPRIETARY – SUBJECT TO CHANGE WITHOUT NOTICE

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

Wi-Fi Alliance has not conducted an independent intellectual property rights ("IPR") review of this document and the information contained herein, and makes no representations or warranties regarding IPR, including without limitation patents, copyrights or trade secret rights. You may need to obtain licenses from third parties before using the information contained in this document for any purpose.

Wi-Fi Alliance owns the copyright in this document and reserves all rights therein. A user of this document may duplicate and distribute copies of the document in connection with the authorized uses described herein, provided any duplication in whole or in part includes the copyright notice and the disclaimer text set forth herein. Unless prior written permission has been received from Wi-Fi Alliance, any other use of this document and all other duplication and distribution of this document are prohibited. Unauthorized use, duplication, or distribution is an infringement of Wi-Fi Alliance’s copyright.

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

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

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

Document revision history

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

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 the following features:

- WPA3-Personal only mode
- WPA3-Personal transition mode
- WPA3-Enterprise only mode
- WPA3-Enterprise transition mode
- WPA3-Enterprise 192-bit mode
- WPA3 Fast BSS Transition
- WPA3-Enterprise Server Certificate Validation
- SAE-PK
- SAE-PK only mode
- WIFI URI
- Transition Disable indication

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 Draft Standard for Information technology -- Telecommunications and information exchange between systems Local and metropolitan area networks -- Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 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] Wi-Fi Alliance WPA3 Security Considerations, https://www.wi-fi.org/file/wpa3-security-considerations

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

1.3 Definitions and acronyms

1.3.1 Shall/should/may/might word usage

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

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

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

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

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

1.3.2 Conventions

The ordering of bits and bytes in the fields within information elements, attributes and action frames shall follow the conventions in Section 8.2.2 of IEEE Standard 802.11 [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

There are no special definitions in this specification.

1.3.4 Abbreviations and acronyms

Table 1 defines the acronyms used throughout this document. Some acronyms are commonly used in publications and standards defining the operation of wireless local area networks, while others have been generated by Wi-Fi Alliance®.

Table 1. Abbreviations and acronyms

Acronyms	Definition
AKM	Authentication and Key Management
ANQP	Access Network Query Protocol
BSS	Basic service set
CN	Common Name
EAP	Extensible Authentication Protocol
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

Acronyms	Definition
OID	Object Identifier
PMF	Protected Management Frame
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 WPA3-Personal

WPA3-Personal applies to personal network settings.

2.1 Modes of operation

WPA3-Personal modes are defined as follows:

- WPA3-Personal only mode
- WPA3-Personal transition mode

2.2 WPA3-Personal only mode

When operating in WPA3-Personal only mode:

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

2.3 WPA3-Personal transition mode

When operating in WPA3-Personal transition mode:

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

2.4 Additional Requirements on WPA3-Personal modes

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

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

3 WPA3-Enterprise

WPA3-Enterprise applies to enterprise network settings.

3.1 Modes of operation

WPA3-Enterprise modes are defined as follows:

- WPA3-Enterprise only mode
- WPA3-Enterprise transition mode
- WPA3-Enterprise 192-bit mode

3.2 WPA3-Enterprise only mode

When operating in WPA3-Enterprise only mode:

- An AP shall enable at least AKM suite selector 00-0F-AC:5 (IEEE 802.1X with SHA-256) in the BSS
- A STA shall allow at least AKM suite selector 00-0F-AC:5 to be selected for an association
- An AP shall not enable AKM suite selector: 00-0F-AC:1 (IEEE 802.1X with SHA-1)
- A STA shall not allow AKM suite selector 00-0F-AC:1 to be selected for an association
- An AP shall set MFPC to 1, MFPR to 1
- A STA shall set MFPC to 1, MFPR to 1
- A STA shall not enable WEP and TKIP

3.3 WPA3-Enterprise transition mode

When operating in WPA3-Enterprise transition mode:

- An AP 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
- A STA shall allow at least AKM suite selectors 00-0F-AC:1 and 00-0F-AC:5 to be selected for an association
- An AP shall set MFPC to 1, MFPR to 0
- A STA shall set MFPC to 1, MFPR to 0

3.4 Additional Requirements on WPA3-Enterprise modes

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

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

3.5 WPA3-Enterprise 192-bit mode

WPA3-Enterprise 192-bit mode 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 operating in WPA3-Enterprise 192-bit mode:

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

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

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - ECDHE using the 384-bit prime modulus curve P-384
  - RSA ≥ 3072-bit modulus
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - RSA ≥ 3072-bit modulus
  - DHE ≥ 3072-bit modulus

4 WPA3 Fast BSS Transition

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

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

4.1 STA AKM preference order

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

4.1.1 Personal modes

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

4.1.2 Enterprise modes

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

5 Server Certificate Validation

5.1 Failure Conditions for Server Certificate Validation

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

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

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

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

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

5.2 Support for User Override of Server Certificate

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

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

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

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

5.3 Criteria to disable UOSC

5.3.1 TOD Policies

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

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

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

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

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

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

5.3.2 Additional Consideration on TOD Policies

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

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

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

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 password (and, if used, the 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 1 of [10]) 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 1 of [10]) 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:

Fingerprint = L(Hash(SSID || M || K_AP), 0, 8*Sec + 19*λ/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.

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

- Advertise the SAE AKM 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 + 256

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

KCK = L(kck_ pmk_kek, 0, Q)

PMK = L(kck_pmk_kek, Q, 256)

KEK = L(kck_pmk_kek, Q+256, 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]

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-BSSID || 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-BSSID is the BSSID of the AP, and STA-MAC is the MAC address of the STA

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 6.5.2, 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 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 "SAE-PK only mode" is used to refer to a mode in which a STA enables SAE-PK but does not allow WEP or TKIP, or a PSK AKM, or an SAE AKM without SAE-PK, to be used for association.

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 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 (see Section 6.5.2) 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 (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 STA operation

When a STA that supports SAE-PK has SAE-PK enabled for a network, the STA shall use SAE-PK 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 form for SAE-PK. A password is in the correct form for SAE-PK 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

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 form (see above) for SAE-PK, but the STA has identified at least one AP in the network that advertises "SAE-PK Passwords Used Exclusively":
  - 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 form for SAE-PK:
  - Enable SAE-PK by default for that network

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 an 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 SAE-PK only mode for the corresponding network (see Section 6.5).

When a STA has SAE-PK enabled for a network, and is selecting between discovered APs in that network (SSID) that it considers suitable candidates for association, it shall attempt to authenticate with those APs that are advertising support for SAE-PK, before attempting to authenticate with any of those APs that are 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 6.5.2) 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 6.5.2) that a STA implementation confirms with the user that the password has been correctly entered if it identifies a network where SAE-PK passwords are used exclusively, 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 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

λ	Sec	S	Average time required to find a second preimage at 50 TH/sec (years)
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 SAE-PK only mode for a given network is fully resistant to such downgrade attack when connecting to that network. A STA will use 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 6.5.2. 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™) 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 (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:R:4;S:MyNet;;
   - STA that supports Wi-Fi Enhanced Open and Transition Disable uses Wi-Fi Enhanced Open only mode
   - STA that supports Wi-Fi Enhanced Open but not Transition Disable 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 indication

Transition Disable is an indication from an AP to a STA, that the STA is to disable certain transition modes for subsequent (re)associations to the AP's network.

A network profile configured on a STA might have certain transition modes (and possibly other legacy security algorithms) enabled. For example, a WPA3-Personal STA implementation might enable WPA3-Personal transition mode in a network profile, which enables a legacy PSK algorithm. However, when a network (fully) supports the most secure algorithm defined in a transition mode, that network can use the Transition Disable indication to cause the STA to disable transition modes for that network profile, and therefore provide protection against subsequent downgrade attacks.

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 implementations, 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.

When Transition Disable is enabled on a BSS, an AP that supports Transition Disable shall include a Transition Disable KDE 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. 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.

A STA that supports Transition Disable shall, if all the following conditions are true:

- The STA received a protected Transition Disable KDE from an AP, and
- The STA authenticated using an algorithm that the KDE does not indicate is to be disabled (see below), and
- The STA has obtained user confirmation (if applicable to the STA's implementation),

disable security algorithms in its network profile corresponding to the AP's SSID as follows:

- Disable use of WEP and TKIP
- Disallow association without negotiation of PMF
- For each bit in the Transition Disable Bitmap field that is equal to 1, if the STA supports at least 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.
    - 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.
- The STA does not take any action for bits in the Transition Disable Bitmap field that are equal to 0 (zero).

NOTE: A network profile is assumed to be stateful on a STA, and hence a Transition Disable policy applies to all subsequent (re)associations to all BSSs with the corresponding SSID, for the lifetime of the network profile.

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	AKM suite selector 00-0F-AC:8 (SAE)	AKM suite selectors 00-0F-AC:2 and 00-0F-AC:6 (PSK), and any other PSK AKMs AKM suite selector 00-0F-AC:4 (FT over PSK), and any other FT over PSK AKMs
1	SAE-PK	AKM suite selector 00-0F-AC:8 (SAE) using SAE-PK	AKM suite selector 00-0F-AC:8 (SAE) when not using SAE-PK, and 00-0F-AC:9 (FT over SAE) when not using SAE-PK AKM suite selectors 00-0F-AC:2 and 00-0F-AC:6 (PSK), and any other PSK AKMs AKM suite selector 00-0F-AC:4 (FT over PSK), and any other FT over PSK AKMs
2	WPA3-Enterprise	AKM suite selector 00-0F-AC:5 (IEEE 802.1X with SHA-256)	AKM suite selector 00-0F-AC:1 (IEEE 802.1X with 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.

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