WPA3™ Specification Addendum for WPA3 R3

(Based on WPA3™ Specification Version 2.0)

Draft Version 0.0.3

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
V0.0.1	2020-03-09	Initial draft of addendum, incorporating contribution approved by TG 3/3/20: - SAE-PK-TS_v0.0.0 20200207a.docx
V0.0.2	2020-04-21	Incorporated contributions approved by TG on 4/21/20: - WPA3_Specification_for_WPA3-R3_v0.0.1 0413a.docx, which included clarification text for Transition Disable per Proposed changes to WPA3 Specification for WPA3-R3 v0.0.1.docx, and WFA KDE/VSIE OUI type values
V0.0.3	2020-04-28	Editorial review

Table of contents

List of tables

1 Introduction

No changes.

1.1 Scope

Insert bullets as shown below.

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

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

1.2 References

Add references 3-10.

[1] IEEE Draft Standard for Information technology -- Telecommunications and information exchange between systems Local and metropolitan area networks -- Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, REVmd/D3.0, Oct. 2019

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

[3] IEEE Draft Standard for Information technology -- Telecommunications and information exchange between systems Local and metropolitan area networks -- Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, REVmd Draft 3.1

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

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

[6] 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

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

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

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

[10]Wi-Fi Alliance WPA3 Security Considerations, https://www.wi-fi.org/file/wpa3-security-considerations

2 WPA3-Personal

No changes.

3 WPA3-Enterprise

No changes.

4 WPA3 Fast BSS Transition

No changes.

5 Server Certificate Validation

No changes.

Insert new sections 6-8.

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 SAE-PK element included in 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, 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 [5] 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 [3].

Resistance to second preimage attack on the fingerprint represented in the password is enhanced using the hash-extension technique utilized in [4]. 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 + 5λ - 2)-bits to be represented in only 5λ bits (where base32 encoding results in a λ-character password excluding separators), using 2 bits to represent Sec followed by the remaining (5λ - 2) bits of the fingerprint. 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 key pair K_AP / k_AP shall be randomly and uniquely generated. The same key pair can be reused if a new password is generated for the same network (i.e., by randomly finding a new Modifier), but should not be reused otherwise.

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, or DSA or RSA keys that have prime length equal to or greater than 2048 bits, is optional. A device that supports SAE-PK with an ECDSA key with prime length greater than 256, or an RSA or DSA key with prime length greater than 2048, shall support an SAE group indicated as suitable in Table 1 of [10] that has a strength estimate equal to or greater than 192. A device that supports SAE-PK with an ECDSA key pair with prime length greater than 384, or an RSA key with prime length greater than 3072, shall support an SAE group indicated as suitable that has a strength estimate equal to or greater than 256.

NOTE: The AP public key type 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 + 5λ - 2)

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 [3], depending on the prime length of the AP's public key K_AP (ECC for ECDSA, or FFC for RSA and DSA)
- Sec is the hash extension security parameter, equal to an integer value between 2 and 5 inclusive
  - Sec and λ shall be chosen such that the following inequality holds: 8*Sec + 5λ - 2 <= 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 depends on the AP's public key type ([4] for RSA and DSA, and [9] for ECDSA). For ECDSA, 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(Sec_2b || L(Fingerprint, 8*Sec, 5λ-2)))

Password = AddSeparators(PasswordBase)

where:

- Sec_2b is a 2-bit unsigned integer where Sec_2b = Sec - 2
- Base32() is the base32 encoding function (5 bits per character) as defined in [7] with lowercase US-ASCII alphabet
- 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 [3], 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 and Probe Response frames)
- Use SAE-PK with a peer STA that indicates SAE_PK status code in its SAE Commit message.
- Use SAE password(s) 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 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 depending on the group, as defined in [3]

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) in the Authentication frame, where:

- The EncryptedModifier field contains the output of the AEAD-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 [3]) 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 RSA or DSA) or 3 (for ECDSA).
- The KeyAuth field of the FILS Key Confirmation element (as defined in [3]) 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 group, as defined in [3]. The form of signature depends on the type of the AP's public key (IETF RFC 3447 for RSA, FIPS 186-4 for DSA, and ISO/IEC 14888-3 for ECDSA). A constant-time algorithm shall be used to generate the digital signature.
- 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 Section 12.4.7.4 (Encoding and decoding of SAE Commit messages) of [3]
- 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 Section 12.4.7.4 (Encoding and decoding of SAE Commit messages) of [3]
- 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 a STA that supports SAE-PK in "Confirmed" state is using SAE-PK and receives an SAE Confirm message then, per Section 12.4.8.6.5 of [3], it processes the SAE Confirm message in accordance with Section 12.4.5.6 of [3]. 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 is also present in the Authentication frame, unwrap the Modifier, validate the public key, verify the signature and complete authentication per the following steps:

a) Unwrapping

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

b) 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 SAE-PK 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 + 5λ - 2)-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 SAE-PK 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 = RemSeparators(Password)
  - λ = Len(Password) - Floor(Len(Password) / 5))
  - PW = Base32d(PasswordBase)
  - Sec = L(PW, 0, 2) + 2
  - Fingerprint_Expected = 08*Sec || L(PW, 2, 5λ - 2)

  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 Section 1.5 of [3]
  - Base32d() is the base32 decoding function, outputting 5λ bits
  - 08*Sec is the bit string comprising Sec octets of the value zero

  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.

c) 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 SAE-PK element using K_AP. The digital signature verification procedure depends on the form of signature, which depends on the AP public key type. The form of signature and input data are as defined above.

d) Authentication confirmation

- If the STA has successfully validated trust in the public key K_AP, and successfully verified the signature in the SAE-PK 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 Section 12.4.8.6.5 of [3], resulting in transition to "Accepted" state. Otherwise (i.e., if the SAE-PK element was 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.

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 SAE AKM is enabled, e.g., WPA3-Personal only Mode or WPA3-Personal transition Mode.

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 Extended Capabilities element to 1, otherwise set to 0.

An AP that supports SAE-PK that enables SAE-PK on a BSS and is configured with one or more passwords that are not SAE-PK passwords, shall prevent configuration of those passwords with values that would be misidentified by STAs as SAE-PK passwords (see Section 6.5.2).

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.

NOTE: If a STA is configured with a password for a network for which the use of SAE-PK has not been explicitly configured, the STA can use the following logic to auto-enable SAE-PK: If every fifth octet in the octet string of the password is equal to 0x2D (ASCII hyphen), and all other octets correspond to values in the base-32 lowercase US-ASCII alphabet, enable SAE-PK for that network; otherwise do not enable SAE-PK 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), pre-populating hyphen separator characters (ASCII 0x2D) every fifth non-trailing character, and auto-enabling SAE-PK for that network.

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 does not allow a PSK AKM to be selected for an association and does not allow AKM suite selector 00-0F-AC:8 to be selected for an association unless SAE-PK was used.

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.

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).

It is assumed that constant time operations are correctly implemented for digital signature generation, in order to prevent timing or cache side-channel 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 + 5λ - 2 is the length of the truncated hash fingerprint, and is equal to the preimage strength (see [6]).

Minimum preimage strength values, with example corresponding parameters, are given in Table 1.

Table 1. Minimum preimage strength values

Description	Preimage strength (S)	Example corresponding parameters
Minimum required	74	λ=12, Sec=2
Minimum recommended	82	λ=12, Sec=3

With the minimum required preimage strength (74 bits), an adversary using a high-speed accelerated "hash miner" capable of 50 TeraHashes/sec would require on average ~12 years to find a Modifier value by brute-force search that results in a second preimage of the fingerprint. With the minimum recommended preimage strength (82 bits), the average time required with the same "hash miner" increases to ~3000 years.

The minimum required and minimum recommended preimage strength values may increase in future revisions of this specification.

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 only use SAE-PK for a given network is fully resistant to such downgrade attack when connecting to that network. A STA will only use SAE-PK 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 the SAE-PK logo).

A STA that supports SAE-PK that is not configured to only use SAE-PK 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 mistakenly inputs an incorrect password containing errors that are predictable by the adversary (e.g., omitted hyphen separators).

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 Section 9.4.2.25 of [3]). Little endian encoding is used for multi-byte fields and subfields. Its format is shown in Table 2.

An SAE-PK element may be fragmented as described in Section 10.28.11 (Element Fragmentation) of [3] if required.

Table 2. SAE-PK 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 IE in octets.
OUI	3	0x50-6F-9A	Wi-Fi Alliance specific OUI (refer to sub-clause 9.4.1.32 of [3])
OUI Type	1	0x1F	Identifying the type and version of the SAE-PK element
Modifier Length	1	Variable	Length of the EncryptedModifier field
EncryptedModifier	Variable	Variable	Encrypted Modifier M
FILS Public Key	Variable	Variable	FILS Public Key element
FILS Key Confirmation	Variable	Variable	FILS Key Confirmation element

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.

7.1.1 URI format

The URI is defined by [8] 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
public-key = "K:" *PKCHAR ; DER of ASN.1 SubjectPublicKeyInfo encoded in "base64" as per [5], 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 password-based credentials.

The value of "type" takes the following values in this version of the specification:

- "WPA": if the STA can use the password with WPA2-Personal (possibly also with WPA3-Personal)
- "WPA3": if the STA can only use the password with WPA3-Personal

NOTE: If "id" is present, the value of "type" is "WPA3".

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 should ignore unknown semicolon separated components in the WIFI-qr instantiation in order to be forward compatible with future extensions to this specification.

7.1.2 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).

7.1.3 URI examples

Some examples of the WIFI URI format are as follows:

WPA3-Personal Transition Mode password without Transition Disable (SAE STA will use SAE or PSK depending on AP support, PSK STA will use PSK):

WIFI:T:WPA;S:MyNet;P:MyPassword;;

WPA3-Personal Transition Mode password with Transition Disable for SAE (SAE STA will only use SAE, PSK STA will use PSK):

WIFI:T:WPA;R:1;S:MyNet;P:MyPassword;;

WPA3-Personal only Mode (SAE STA will only use STA, PSK STA will not connect):

WIFI:T:WPA3;R:1;S:MyNet;P:MyPassword;;

WPA3-Personal Password Identifier password (SAE STA only, does not apply to PSK STA):

WIFI:T:WPA3;R:1;S:MyNet;I:MyIdentifier;P:MyPassword;;

WPA3-Personal Transition Mode with Transition Disable for SAE-PK and SAE (STA that supports SAE-PK will only use SAE-PK, SAE STA will only use SAE, PSK STA will use PSK):

WIFI:T:WPA;R:3; S:MyNet;P:a2bc-de3f-ghi4;K:MDkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDIgADURzxmttZoIRIPWGoQMV00XHWCAQIhXruVWOz0NjlkIA=;;

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 connections to the AP's network.

A STA implementation might enable certain transition modes (and possibly other legacy security algorithms) in a network profile. For example, a WPA3-Personal STA might by default enable WPA3-Personal Transition Mode in a network profile, which enables WPA2-PSK algorithm. However, when a network (fully) supports the most secure algorithm defined in a transition mode, the Transition Disable indication can be used to disable transition modes for that network on a STA, and therefore provide protection against downgrade attacks.

NOTE: A network administrator might, in order to mitigate risk of downgrade attack, use Transition Disable indication even when only a subset of APs in the corresponding network support the most secure algorithm. In such case, the STA would only connect to the APs in the network that support the most secure algorithm.

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

Transition Disable is indicated in the Transition Disable KDE, which is in the format defined in Section 12.7.2 of [3]). Little endian encoding is used for multi-byte fields and subfields. Its format is shown in Table 3. The length of the Transition Disable field is variable.

An AP that supports Transition Disable shall, when configured to do so, 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.

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 it receives a protected Transition Disable KDE in a frame as described above from an AP it has authenticated using an algorithm that the KDE does not indicate is to be disabled (see below) and subject to user confirmation (if applicable to the STA's implementation), disable security algorithms in its network profile for the corresponding network 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 4, 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).

Table 3. 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 9.4.1.32 of [3])

Field	Size (Octets)	Value (Hex)	Description
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 4).

Table 4. Transition Disable Bitmap 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) not using SAE-PK, and 00-0F-AC:9 (FT over SAE) 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 selectors 00-0F-AC:1 and 00-0F-AC:5 (IEEE 802.1X)	None
3	Enhanced Open	AKM suite selector 00-0F-AC:18 (OWE)	Open System authentication without encryption