Wi-Fi Protected Setup™ Specification

Version 2.0.8

Document history

Version	Date	Status	Comments
2.0.0.51	2010-09-01	Draft	Draft release version to public
2.0.0	2010-12-20	Final	Public release version
2.0.1	2011-08-11	Final	Public release version - Added tablet PC to table 41
2.0.2	2012-01-30	Final	Public release version - Change Headless Devices section to mandate implementation of strong mitigation against a brute force attack on the AP that uses a static PIN.
2.0.2.1.21	2014-01-27	Draft	Draft release version to public - Updated to support NFC - Updated to incorporate the Wi-Fi Peer-to-Peer Services default configuration method - Updated to incorporate 60GHz_WPS_SRD_1.0 - Minor editorial corrections/clarifications
2.0.3		Draft	Internal Draft, not publicly released
2.0.4	2014-03-21	Final	Public release version - Clarifications on NFC sections - Minor editorial corrections/clarifications
2.0.5	2014-08-04	Final	Public release version - Editorial updates to clarify references to Wi-Fi Peer-to-Peer Services Specification
2.0.6	2018-04-26	Final	Added Multi-AP identifier to Table 29.
2.0.7	2019-12-09	Final	Added Multi-AP subelements to Table 29 Added attributes in Encrypted Settings of M2, M8 if Enrollee is STA to Table 21 Added attribute types and sizes to Table 28 (for IBSS with Wi-Fi Protected Setup Specification) Added Response Type to Table 43
2.0.8	2020-12-01	Final	Public release version - Editorial update

Table of contents

List of tables

List of figures

1 Introduction

Although home Wi-Fi® networks have become very popular, the industry continues to be plagued by a high rate of support calls and retail equipment returns due primarily to the complexity of initial network setup. Furthermore, most (by some estimates, 60-70%) of those who successfully set up their wireless networks never configure security features and are highly vulnerable to network attacks. This document contains a specification for easy, secure setup and introduction of devices into WPA2™-enabled 802.11 networks. The terms “Wi-Fi Simple Configuration” and “WSC” are interchangeable with “Wi-Fi Protected Setup”.

1.1 Scope

The primary goal of the Wi-Fi Simple Configuration protocol is to simplify the security setup and management of wireless networks. The goal of this specification is to provide users with a method that their wireless networks can be easily protected against unauthorized access and disclosure of private information.

The protocol defined in this specification supports WPA2-Personal networks and Open (no security) networks. Note that wherever WPA2 or AES is referenced in this document, those references include both CCMP and GCMP. It also defines a few elements specific for WPA2-Enterprise networks. This specification is aimed primarily at home and small business wireless networks and Peer-to-Peer (P2P) groups.

1.2 Supported Usage Models

Wi-Fi Simple Configuration addresses the following primary usage models.

1.2.1 Primary Usage Models

1. Setting up a new secure WLAN, which includes Out of Box (Infrastructure mode only)
2. Adding new Member devices to the WLAN

1.2.2 Secondary Usage Models

1. Removing Members from the WLAN
2. Guest access (temporary or otherwise restricted access compared to regular member devices)
3. Re-keying credentials
4. Expanding the network - Adding additional APs or Routers
5. Changing Network Name (SSID), radio channels, other parameters outside of security & initial connectivity settings
6. Out-of-band exchange of credentials with NFC interface or tag

1.3 Design Approach

The fundamental design approach in this specification is to define a structured and layered set of OS-independent and extensible protocols that enable both basic and advanced WLAN setup scenarios. Wi-Fi certification is expected to require support only for basic scenarios, but the architecture is extensible and able to support a range of advanced features. In this specification, primary emphasis is placed on the basic setup scenarios.

Although Wi-Fi Simple Configuration offers a broad range of choices to device vendors, the architecture is unified around two core elements. The first is a common data representation for device description and WLAN configuration that is used with all Wi-Fi Simple Configuration methods. The second is a protocol called the Registration Protocol, which is used with all methods that utilize 2-way communication channels such as WLAN, Ethernet, or the 2-way direct mode of near-field communications (NFC). Wi-Fi Simple Configuration can be easily extended to support additional communication channels by defining an encapsulation of the Registration Protocol messages over additional network types.

1.4 Solution Flexibility

The core protocols described in this specification can enable configuration using a wide variety of hardware choices, including both in-band and out-of-band communication channels. Although it would be simpler to choose just a single method, it is unrealistic to expect all devices to have the same I/O capabilities. Therefore, this specification provides a range of choices. Wi-Fi Alliance may choose to specify a subset of these choices for its compliance certification program.

The following types of devices are supported by this specification:

- Both WPA2/WPA-Personal and WPA2/WPA-Enterprise devices
- Access Points with per-device or shared WPA2/WPA keys
- Access Points able to add new devices to the network as a standalone function or through a trusted external device called a Registrar
- Access Points, Registrars, or Client devices with a physical or virtual Pushbutton used for in-band setup using the optional Pushbutton configuration (PBC) method
- Access Points, Registrars, or Client devices that support optional hardware-based out-of-band channel such as Ethernet, Near-Field Communication (NFC) interface, and/or an NFC Tag.
- Client devices with only a simple display or a fixed label containing a setup password
- Rich UI devices such as PCs, cell phones, and TV sets and Set top boxes, suitable for hosting WLAN Manager Registrar functions
- Registrar devices that support only optional setup methods

1.5 User Experience

The most important characteristic of any initial setup solution is the user experience. This section introduces two scenarios to illustrate the Wi-Fi Simple Configuration user experience. Sections 5, 6, 10 and 11 contain a more detailed specification of these and other scenarios.

1.5.1 In-band Setup

Context 1: the user has a cell phone that he wants to use to set up a newly-purchased AP. This AP's only communication channels are Ethernet and WLAN.

Setup steps

1. User turns on the AP.
2. Software on the cell phone automatically detects the AP and asks the user if he wants to configure the AP.
3. The phone prompts the user for the AP's PIN, found on a label attached to the device. The user keys in the PIN, accepts the default settings, and receives confirmation that the AP is successfully configured.

Now, the user brings home a wireless printer and turns it on.

4. The phone detects the new wireless device and prompts the user to add it to the network. The user reads the printer's PIN number from its display and enters it into the cell phone.
5. Both the cell phone and printer provide visual confirmation when the printer joins the network.

Context 2: the user has a portable game console that he wants to connect to the existing WLAN for online gaming. This user prioritizes convenience over security, so he decides to use the Pushbutton configuration method for setting up the portable game console.

Setup steps

1. User presses the PBC button on the game console.
2. User presses the PBC button on the Registrar.
3. The game console and Registrar display the progress of the PBC method on their respective user interfaces. Upon completion of the protocol, both indicate "connection success."

1.5.2 Out-of-Band Setup

Context: The user purchases a Wi-Fi Simple Configuration AP and a wireless printer that includes an NFC Tag for setup. The AP also includes an integrated NFC interface.

Setup steps

1. User plugs in the AP. The AP automatically chooses an SSID and a WPA2-Personal PSK.
2. User turns on the printer and touches the printer's NFC Tag to the AP's NFC interface.
3. AP configures the printer and the printer provides visual confirmation (using an LED) that it has joined the network.

2 References

[1] IEEE Std 802.1X, Port-Based Network Access Control, 2001

[2] NFC Forum Data Exchange Format (NDEF) Specification, NFC Forum, 2006

[3] NFC Forum Type 1 Tag Operation Specification, NFC Forum, 2007

[4] NFC Forum Type 2 Tag Operation Specification, NFC Forum, 2007

[5] NFC Forum Type 3 Tag Operation Specification, NFC Forum, 2007

[6] NFC Forum Type 4 Tag Operation Specification, NFC Forum, 2007

[7] NFC Forum Logical Link Control Protocol Specification, NFC Forum, 2009

[8] NFC Forum Connection Handover Specification 1.2, NFC Forum, 2010

[9] RFC 2104, HMAC: Keyed-Hashing for Message Authentication, 1997

[10] RFC 2511, Internet X.509 Certificate Request Message Format, 1999

[11] RFC 3526, More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), 2003

[12] RFC 3748, Extensible Authentication Protocol (EAP), 2004

[13] RFC 4122, A Universally Unique IDentifier (UUID) URN Namespace, 2005

[14] Wi-Fi Protected Setup Protocol and Usability Best Practices, Wi-Fi Alliance,

[15] WFA WLANConfig Service 1.0, Wi-Fi Alliance, Version 1.01 2006

[16] WFA Device 1.0, Wi-Fi Alliance, Version 1.01, 2006

[17] IEEE Std 802.11-2012, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2012

[18] Wi-Fi Alliance, “Wi-Fi Direct Specification”, 2013

[19] Wi-Fi Alliance, “Wi-Fi Peer-to-Peer Services Technical Specification”, 2014

3 Definitions

AP: An infrastructure-mode 802.11 Access Point.

Credential: A data structure issued by a Registrar to an Enrollee, allowing the latter to gain access to the network.

Device: An independent physical or logical entity capable of communicating with other Devices across a LAN or WLAN.

Device Password: A shared secret that may be used to authenticate the in-band exchange between the Registrar and Enrollee.

Discovery Protocol: A protocol informing the Enrollee and the Registrar of each others presence and capabilities.

DMG (Directional Multi-Gigabit): A frequency band wherein the operating channel center frequency is above 45 GHz.

Domain: A set of one or more Devices governed by a common authority for the purpose of gaining access to one or more WLANs.

Enrollee: A Device seeking to join a WLAN Domain. Once an Enrollee obtains a valid credential, it becomes a Member.

External Registrar: A Registrar for an AP's Domain that runs on a device separate from the AP.

Guest: A Member with credentials that provide only temporary or otherwise limited access to a WLAN.

In-band: Data transfer using the WLAN communication channel, including WLAN multiband devices (e.g. 2.4GHz, 5GHz, and 60GHz).

Internal Registrar: A Registrar that is embedded in an AP. All APs shall include an Internal Registrar.

Member: A WLAN Device possessing Domain credentials.

NFC Device: NFC Forum compliant contactless device that support the following Modus Operandi: Initiator, Target, and Reader/Writer. It may also support card emulator.

NFC Interface: Contactless interface of an NFC Device.

NFC LLCP: The Logical Link Control Protocol (LLCP) specification between two NFC Forum Devices [7].

NFC Tag: NFC Forum compliant contactless memory card that can be read or written by an NFC Device and may be powered by the RF field.

Out-of-Band: Data transfer using a communication channel other than the WLAN.

PIN (Personal Identification Number): A 4 or 8 digit device password.

Registration Protocol: A Registration Protocol is a (logically) three party in-band protocol to assign a Credential to the Enrollee. The protocol operates between the Enrollee and the Registrar and may receive support through a proxy.

Registrar: An entity with the authority to issue and revoke Domain Credentials. A Registrar may be integrated into an AP, or it may be separate from the AP. A Registrar may not have WLAN capability. A given Domain may have multiple Registrars.

PCP: A Personal basic service set (PBSS) Control Point, peer-to-peer functionality in a 60GHz device, mandatory for all Wi-Fi CERTIFIED 60GHz Stations.

Pushbutton configuration (PBC): A configuration method triggered by pressing a physical or logical button on the Enrollee and on the Registrar.

Stand-Alone External Registrar (SAER): An External Registrar that is not embedded in a wireless STA. For example, may be embedded in an Ethernet connected device, or may be software installed on any networking device.

Station (STA): An 802.11 non-AP station or client.

WLAN: A wireless (802.11) network.

4 Core Architecture

4.1 Components and Interfaces

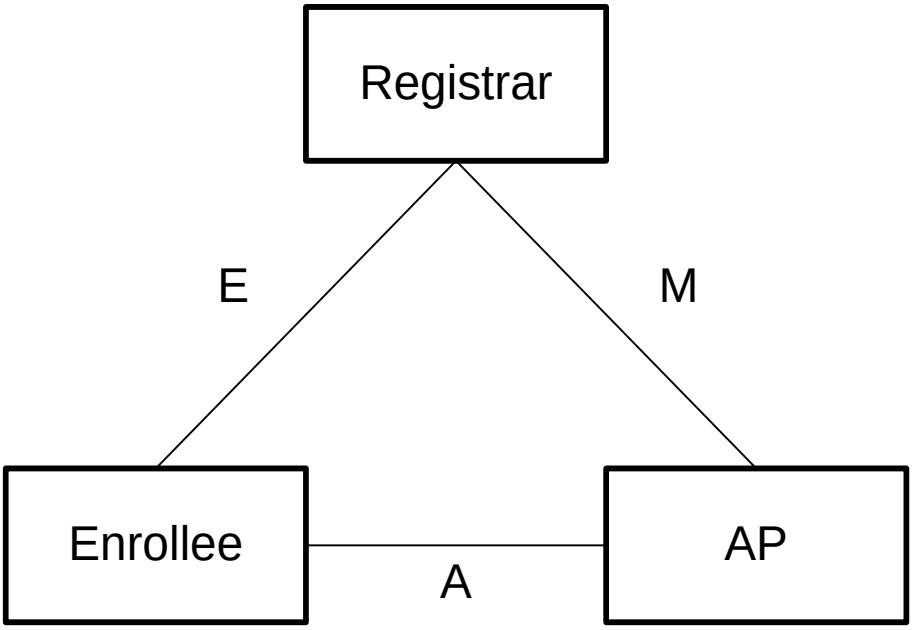

Figure 1 – Components and Interfaces

Figure 1 illustrates the major components and their interfaces as defined by the Wi-Fi Simple Configuration Protocol. There are three logical components involved in Wi-Fi Simple Configuration: the Registrar, the AP, and the Enrollee. In some cases these logical components may be co-located. For example, an AP may include a built-in Registrar to add Enrollees in a standalone fashion either with or without a web browser.

4.1.1 Architectural Overview

A new WLAN is established by turning on the AP and optionally attaching its external network connectivity (typically by connecting the AP to a DSL or cable modem, or equivalent). At this point in time, there are no other devices on the network. The next step is to add an Enrollee or Registrar device to the network. This is accomplished by running the Registration Protocol between the AP and the new device. If the new device is added as an external Registrar, then future Enrollees can be added using that Registrar.

Wi-Fi Simple Configuration defines new 802.11 information elements (IE) that are included in beacons, probe requests and probe responses. The purpose of these IEs is to advertise the presence of devices that are capable of performing Wi-Fi Simple Configuration operations. Note that the information obtained from these IEs is not authenticated.

4.1.2 Interface E

This interface is logically located between the Enrollee and the Registrar (physically, the AP can work as a proxy to convey the messages). The purpose of Interface E is to enable the Registrar to discover and issue WLAN Credentials to the Enrollee. Interface E may include only WLAN communication or it may also include communication across an out-of-band channel.

Enrollee

The Enrollee implements Interface E by:

1. Including a Wi-Fi Simple Configuration IE in 802.11 probe request messages.
2. Including a unique, randomly generated device password on a display or printed label. The device password is used to authenticate the in-band exchange between the Registrar and Enrollee.
3. Optionally supporting one or more out-of-band channels for easier and more secure configuration.
4. Implementing the “Enrollee” part of the Registration Protocol (for more details, refer to section 7)

Registrar

The Registrar implements Interface E by:

1. Processing Enrollee (device or AP) Discovery data in Probe messages (for wireless Registrars) and/or UPnP (for IP-based Registrars).
2. Implementing the “Registrar” part of the Registration Protocol (for more details, see section 7).
3. Optionally supporting one or more out-of-band channels for easier and more secure configuration
4. Configuring the AP with the Enrollee’s MAC address and Credential using Interface M if necessary
5. Responding to Enrollee Probe-Requests through Probe-Responses if Registrar is an AP.

4.1.3 Interface M

Interface M is the interface between the AP and the Registrar. It enables an external Registrar to manage a Wi-Fi Simple Configuration AP. Wi-Fi Simple Configuration uses the same protocol for setting up the AP Management interface as for issuing Credentials to Enrollee devices.

AP

The AP implements Interface M by:

1. Acting as the Enrollee in the Registration Protocol, sending its own Discovery message across both 802.11 and UPnP. Support for at least three external Registrars is required.
2. Implementing the Management Interface described in the WFADevice and WFAWLANConfiguration Service documents. The AP is required to be a UPnP device that includes support for the Wi-Fi Simple Configuration proxy service.
3. Monitoring 802.11 probe request and EAP messages from Enrollees and converting them to UPnP Event messages. It also accepts UPnP actions and converts them to EAP messages according to the proxy function described in the WFAWLANConfiguration Service document.

Registrar

The Registrar implements Interface M by:

1. Processing AP Discovery messages across 802.11 and/or UPnP.
2. Subscribing to proxy events, receiving and processing Enrollee Discovery and Registration messages from the UPnP proxy and continuing the Registration protocol message exchange via UPnP actions.
3. Implementing the Registrar side of the Registration Protocol to gain management rights over the AP or to issue WLAN credentials to Enrollees
4. Configuring the AP with the MAC address and/or the per-device Credential of the Enrollee.
5. Implementing the Management Interface described in the WFADevice and WFAWLANConfiguration Service documents. This implementation requires the Registrar to function as a UPnP control point.

4.1.4 Interface A

Interface A is between the Enrollee and the AP. The function of Interface A is to enable discovery of the Wi-Fi Simple Configuration WLAN and to enable communication between the Enrollee and IP-only Registrars.

AP

The AP implements Interface A by

1. Sending out 802.11 beacons indicating support for Wi-Fi Simple Configuration and generating Probe Response messages containing a description of the AP.
2. Implementing an 802.1X authenticator and the Wi-Fi Simple Configuration EAP method.
3. Proxying 802.11 probe request and EAP messages between Enrollees and external Registrars as described in the WFADevice and WFAWLANConfiguration Service documents.

Enrollee

The Enrollee implements Interface A by:

1. Discovering a Wi-Fi Simple Configuration AP and/or wireless external Registrar and sending it 802.11 probe requests including the Enrollee Discovery data.
2. Implementing an 802.1X supplicant and the Wi-Fi Simple Configuration EAP method.

4.2 Registration Protocol

The Registration Protocol accomplishes the following purposes:

1. It helps to troubleshoot basic connectivity problems with the wireless channel
2. It provides demonstrative identification of the Enrollee to the Registrar and the Registrar to the Enrollee using out-of-band information, enabling the credential configuration function.
3. It establishes the roles of each device (AP, Registrar, or Enrollee).
4. It securely conveys WLAN settings and other configuration from the Registrar to the Enrollee.
5. It establishes an Extended Master Session Key EMSK, which can be used to secure additional application-specific configuration functions.

The Registration Protocol can be run entirely in-band, entirely out-of-band, or with a combination of in-band and out-of-band communication. This flexibility allows the protocol to be easily adaptable to take advantage of a variety of different out-of-band mechanisms.

The Registration Protocol operates in two phases. The first phase of the Registration Protocol, also known as the discovery phase, is used to exchange descriptive information between the Registrar and the Enrollee.

The discovery phase of the Registration Protocol is mandatory.

In the case of a station enrollee the discovery phase serves two purposes:

- allows the Enrollee to discover Registrars available for enrollment
- allows the Enrollee to make itself discoverable such that Registrars can discover prospective candidates for enrollment

The station Enrollee may choose either of the following two methods to run the discovery phase:

- during the scanning procedure the station enrollee may use active scans to send probe requests including the WSC IE to the AP. The AP will respond with probe responses including the WSC IE; considering that the WSC IE in the probe response includes information from one or more Registrars (as a union) this method is recommended only if the Enrollee intends to make itself discoverable but does not intend to also discover detailed information about external Registrars. Note : The station enrollee may choose not to associate for WSC provisioning if the AuthorizedMACs subelement containing the station's MAC address or wildcard MAC address (ff:ff:ff:ff:ff:ff) is not present in the Beacon or the Probe Response frames.
- the station enrollee may decide to associate to a WSC-enabled AP and initiate the Registration Protocol by sending message M1 to the Registrar; assuming that the Registrar is not yet prepared to enroll the candidate enrollee it will respond with message M2D; this method is recommended if the Enrollee intends to discover available Registrars in addition to making itself discoverable

In the case of an AP acting as an enrollee the discovery phase is started from the Registrar:

- a wireless external Registrar sends probe requests including the WSC IE with Request Type attribute set to Registrar or WLAN Manager Registrar. The AP responds with probe responses including the WSC IE with Response Type attribute set to AP (i.e. Access Point)
- a wired external Registrar uses appropriate UPnP discovery mechanism to identify the AP

During the discovery phase the Enrollee may exchange messages with multiple APs and/or Registrars on the network.

After the discovery phase if both the Enrollee and the Registrar decide to proceed with the enrollment procedure, the second phase of the Registration Protocol will follow. The second phase culminates with the Credential provisioning.

The Registration Protocol operates in lock-step fashion, terminating with M2, M2D, or with M8. The termination cases follow:

- M2D – this message indicates that the Registrar is unable to authenticate with the Enrollee, but it is willing to provide descriptive information about the Registrar to the Enrollee.
- M2 – this message may optionally carry ConfigData from the Registrar, in which case it terminates the Registration Protocol. The connection of the physical channel implicitly authenticates the data sent across this channel. In this case, the first and second phases of the Registration Protocol are combined, and only one round trip is needed.
- M8 – this message is the culmination of the third round trip of the second phase of the Registration Protocol. The three round trips of the second phase are used to gradually perform mutual authentication of the Enrollee and the Registrar based on the Enrollee's device password. WLAN Credentials are delivered to the Enrollee in message M8.

The Registration protocol may also terminate if errors or timeouts occur during execution.

A detailed description of the Registration Protocol can be found in Section 7.

4.3 Security Overview

Wi-Fi Simple Configuration offers a variety of choices for device manufacturers, and each choice has different security implications. The security of a system is only as strong as its weakest component. Therefore, the effective security strength when using Wi-Fi Simple Configuration to set up a given WLAN corresponds to the strength of the least secure method used for setting up any of the devices on that WLAN. Users who want strong security should be encouraged to purchase products that support the higher-security Wi-Fi Simple Configuration options. There are two major modes of operation of Wi-Fi Simple Configuration: in-band configuration and out-of-band configuration.

With in-band configuration, a Diffie-Hellman key exchange is performed and authenticated using a shared secret called a "device password." The device password is either obtained from the Enrollee and entered into the Registrar, or obtained from the Registrar and entered into the Enrollee. Entry of the device password may be either manual entry or via NFC using a Wi-Fi Simple Configuration NFC Password Token. If NFC is used to enter the device password, the Registrar is also provided the hash of the Enrollee's Diffie-Hellman public key. This significantly strengthens the authentication of the Enrollee to the Registrar and reduces risks associated with attackers stealing NFC Tags used for wireless setup.

With out-of-band configuration, WLAN Credentials are sent across an out-of-band channel to the Enrollee. The Credentials and configuration are optionally encrypted on the out-of-band channel. The out-of-band channel currently supported by this specification is NFC using a Wi-Fi Simple Configuration NFC Configuration Token.

4.3.1 In-band Configuration

The Wi-Fi Simple Configuration in-band Registration protocol is designed to provide strong protection against passive eavesdropping attacks and also to detect and to protect the system from an attempt to perform an active brute force attack. This means that if a Registrar engages an attacker that it believes is the legitimate Enrollee, it first detects that the attacker does not know the password. This detection occurs before it has given enough information to expose the password to brute force attack. However, if the Registrar runs the Registration Protocol multiple times with an attacker using the same PIN, the attacker will be able to discover the PIN through brute force offline attack and run the protocol again to obtain the network settings. To address this vulnerability, if a PIN authentication or communication error occurs after sending message M6, the Registrar SHALL warn the user and SHALL NOT automatically reuse the PIN. Furthermore, if the Registrar detects this situation and prompts the user for a new PIN from the Enrollee device, it SHALL NOT accept the same PIN again without warning the user of a potential attack. If a strong device password (such as an Out-of-Band Device Password or a Machine-specified password) with at least 32 bytes of randomness is used instead of a PIN, the Registrar is permitted to use this password multiple times without warning the user when failures occur. The requirements regarding PIN reuse do not apply to the PBC (Pushbutton) method.

Device Password

All devices supporting Wi-Fi Simple Configuration shall provide at least one numeric Device Password (PIN) for initial setup that is unique and randomly generated per device. Although it is possible and permitted for two devices to have the same Device Password, a group of devices should not intentionally be assigned the same Device Password, and the Device Password SHALL not be based on other characteristics of the device, such as MAC address or serial number.

Headless Devices

Headless devices (i.e., those without a display) are required by Wi-Fi Simple Configuration to include an 8-digit device password called a PIN (A PIN on a headless device is typically printed on a sticker or otherwise physically inscribed on the device). The PIN value of a headless device shall also be configured into the device itself. This would typically be done during the manufacturing process.

PIN-based device passwords are the basic security level for Wi-Fi Simple Configuration. Since one of the digits in the 8-digit PIN is used as a checksum, the PIN contains approximately 23 bits of entropy. This in itself is not the biggest limitation, however. The biggest limitation is that this PIN may be a fixed value (when it is static, usually displayed on a label). Because a fixed PIN value is able to be reused, it is susceptible to active attack. The protocol permits a user to override the default device password with a new value, which can help security-conscious users reduce this vulnerability.

Probably the most significant class of headless devices in a WLAN is the AP itself. If possible, each time the Registration Protocol is run, an AP should generate and display a new, temporary PIN (one time use) for establishing external Registrars (with the AP acting as an Enrollee). However, if a static PIN is used, the AP shall track multiple

failed attempts to authenticate an external Registrar and then enter a lock-down state (This state is signified by setting the attribute AP Setup Locked to TRUE). After at most 10 failed, consecutive attempts, with no time limitation, from any number of external Registrars, the AP shall revert to a locked down state, and the AP shall remain in the locked down state indefinitely (i.e., until the user intervenes to unlock AP's PIN for use by external Registrars)..

In this state, the AP SHALL refuse to run the Registration Protocol in initial AP setup mode with any external Registrars. This technique protects the AP's PIN against brute force attack by an attacker posing as new external Registrar(s). During the AP Setup Locked state, it is still possible to add new Enrollee devices to the WLAN, but it is not possible to add new external Registrars using the AP's PIN.

The AP may include additional means to enter the locked state. For example, an AP may implement an incremental and/or temporary lockout process that extends the lockout time between failed PIN attempts. However, even if these additional methods are implemented, an AP still shall enter an indefinite locked down state as described above.

The AP shall include means to leave the locked state by user intervention. For example removing the locked state using the AP's administrative Web page or power cycling the AP (turn off the AP then turn it back on) are means for the user to intervene and reset the use of PINs by external Registrars.

In addition to the PIN method, headless devices may implement the Pushbutton configuration method (Devices with richer UIs may also optionally implement the PBC method). The PBC method has zero bits of entropy and only protects against passive eavesdropping attacks. The PBC method should only be used if no PIN-capable Registrar is available and the WLAN user is willing to accept the security risks associated with PBC.

Although the security properties of these methods are weaker than the other options, they are included in this specification to accommodate devices without displays or other out-of-band channels.

Devices with Displays

If an Enrollee device advertises support for the Display Configuration Method, it is required to generate a fresh 4 or 8-digit PIN each time it runs the Registration Protocol and show this PIN on a display. This has two significant advantages. First, because the password is single-use, it is not susceptible to the brute force attack described above. Second, it is simpler to manufacture devices that dynamically generate keys than to have them pre-configured and printed on stickers at the factory. There is also no risk that a display will fall off or get lost, which is possible with a sticker.

Devices with NFC

If the Registrar supports the same out-of-band channel as the Enrollee, that channel can be used to deliver strong device passwords (such as 256 bit random values) to the

Registrar. The hash of the Enrollee's public key is also included. As far as the WLAN is concerned, this approach resists even attackers that succeed in reading the data sent across the out-of-band channel. However, if the attacker is able to read the device's NFC Tag before completion of the enrollment process, then it may be possible for them to perform a rogue network attack against the Enrollee.

4.3.2 Guidelines and Requirements for PIN values

The PIN requirements for the two main classes of devices are:

- Headless devices (devices without display) shall use an 8-digit PIN, e.g. a PIN printed on a label attached to the device. The last digit of this 8-digit PIN is used as the checksum of the first 7 digits. Section 7.4.1 specifies how the checksum is generated.
- Devices that use a display to show the PIN and can generate a new PIN shall use either a 4-digit or 8-digit PIN. The last digit of an 8-digit PIN is used as the checksum of the first 7 digits. Section 7.4.1 specifies how the checksum is generated. A 4-digit PIN does not include a checksum digit.

Note: If a device can generate a dynamic PIN and show it on a display but also has a label with a static PIN, it is recommended to use the dynamic PIN shown on the display although it is allowed to use the PIN from the label.

The recommended length for a manually entered device password is an 8-digit numeric PIN. This length does not provide a large amount of entropy for strong mutual authentication, but the design of the Registration Protocol protects against dictionary attacks on PINs if a fresh PIN or a rekeying key is used each time the Registration Protocol is run.

PIN values should be randomly generated, and they SHALL NOT be derivable from any information that can be obtained by an eavesdropper or active attacker. The device's serial number and MAC address, for example, are easily eavesdropped by an attacker on the in-band channel. Furthermore, if a device includes multiple PIN values, these values SHALL be cryptographically separate from each other. If, for example, a device includes both a label-based PIN and a Device Password on an integrated NFC Tag, the two Device Passwords SHALL be different and uncorrelated.

A Registrar may be preconfigured with a set of Enrollee PIN and UUID-E pairs as part of a packaged solution or a Registrar may choose to store PIN values. PINs stored on the Registrar may remain valid for an indeterminate amount of time, but Registrars should invalidate a PIN if a registration attempt results in a failed PIN authentication. PINs that are stored on the Registrar should be cryptographically protected and should not be read-accessible via an interface on the Registrar.

4.3.3 Out-of-Band Configuration

There are three options for using out-of-band channels for configuration in this specification.

Unencrypted Settings

The first option places the WLAN Credential unencrypted onto the out-of-band media. Using this option is based on the assumption that the user will maintain physical control over the out-of-band media (such as an NFC Tag). This control shall be maintained even after the enrollment process is complete. The primary advantage of this option is convenience: the out-of-band media can be reused with new Enrollees without requiring the Registrar to be running at the time of introduction. Another important advantage of this option is that it works well with legacy APs that do not forward messages containing Enrollee public keys to the Registrar. The disadvantage is that if an attacker gains access to the out-of-band media, they will immediately obtain valid WLAN Credentials.

Encrypted Settings

This option uses a key derived from the Diffie-Hellman public key of the Enrollee obtained over the in-band channel, along with that of the Registrar, to encrypt settings for that specific Enrollee. Although the settings are encrypted, it is still advisable to physically guard the out-of-band media from being read by an attacker.

NFC Interfaces Operating in Peer-to-peer Mode

This mode has the strongest security properties supported by this specification because practical man-in-the-middle attacks against NFC are not feasible. In this mode, a 1536-bit Diffie-Hellman exchange is performed over the NFC interface, and WLAN settings are encrypted using 128-bit AES and delivered over the same interface. The Diffie-Hellman public keys and WLAN settings are implicitly authenticated by both the Registrar and the Enrollee, because they are received over the NFC channel.

5 Initial WLAN Setup

There are two primary scenarios for initial WLAN setup with Wi-Fi Simple Configuration. The first case is a standalone AP that supports Wi-Fi Simple Configuration. A "standalone AP" is one that includes a built-in Registrar and does not use an external Registrar. The second case is where a Wi-Fi Simple Configuration AP operates with one or more external Registrars. External Registrars are granted authority by the AP to issue Credentials to Enrollees and to manage the AP's configuration.

A Wi-Fi Simple Configuration enabled AP shall broadcast its SSID in beacons. If the user manually disables broadcasting of the SSID the AP shall automatically disable WSC as well. When WSC is disabled the WSC IE is not include in the Beacon or management frames. No WSC protocol frames are exchanged.

If WSC is enabled, an AP shall not prevent enrollment or block communications based on other access control mechanisms (like MAC Address filtering).

5.1 Standalone AP

The simplest configuration for initial WLAN setup with Wi-Fi Simple Configuration is a standalone AP. In this case, the user simply plugs in the AP and optionally attaches its Internet connection. When initializing in a standalone mode, a Wi-Fi Simple Configuration AP shall automatically choose an SSID (preferably a random SSID) and channel. It should also by default turn on WPA2-Personal with a strong, randomly generated PSK. If backwards compatibility needs to be provided to clients that do not support WPA2-Personal, the AP may optionally get configured for Mixed Mode. A standalone AP should include a Wi-Fi Simple Configuration Registrar, issuing keys to Enrollees via the Registration Protocol. A standalone AP may also include an option to turn security on or off. An AP should also include a factory reset option that erases any configuration and keys that have been established by the user and returns the AP to the state it had when originally purchased.

If an AP includes a built-in Registrar that uses a Web-based interface to input Enrollee passwords or perform other Registrar functions, the following suggestions are recommended:

- The AP's Registrar pages should be protected with TLS
- HTTP Basic Authentication shall not be used, even over TLS. At minimum, Digest Authentication over TLS with the "response-auth" option should be used.
- It should be possible to disable the AP's Registrar Web interface for adding Enrollees.

If the AP ships with a built-in device password for web page access and for setting up an external Registrar, this password shall be unique to that individual device. Furthermore, the user shall be permitted to change this password to a stronger value. If the default password is changed, then the original password shall be deactivated unless the AP is reset to its original factory settings.

Security Considerations

There are several security and usability challenges when using a standalone AP as a Registrar. These challenges stem primarily from the limitations of the user interface and storage capabilities of an AP. Ideally, the Registrar should guide the user step-by-step through the setup process and explain any errors or problems that have been encountered. However, a standalone AP without a display will have difficulty providing this level of feedback to the user unless it is operated through a browser interface. It is important to understand that these usability issues also have an impact on security. A user might not be able to make correct security decisions unless the system can provide sufficient information to inform those decisions.

5.2 AP With an External Registrar

It is ultimately the responsibility of the AP to perform link layer access control on a wireless network in infrastructure mode. Wi-Fi Simple Configuration was developed based on the presumption that a person in physical possession of the AP during the setup process is the de facto owner who is authorized to extend Domain membership to other devices. If wireless security is enabled, each member device shall first be given a Credential (in home networks, this Credential is typically a passphrase using WPA2-Personal). This enrollment function can be performed by a standalone AP and it can also be delegated to one or more external Registrar devices. If an external Registrar is used, then the external Registrar may also establish a secure Management Interface with the AP. The Management Interface is specified in the WFADevice and WFAWLANConfiguration Service documents.

An external Registrar issues Credentials to Enrollees and configures APs in the Domain to accept those Credentials. It also provides diagnostic feedback to help the user resolve problems with the network and to lead users through the device enrollment process. Secondary usage models such as guest access and Credential revocation can also be facilitated by an external Registrar.

A user may want to use an external Registrar for any of the following reasons:

- The external Registrar may have a greater ability to store and display a comprehensive log of network setup events.
- An external Registrar may have a richer UI that can help explain and resolve problems encountered during setup.
- The external Registrar may support multiple out-of-band channels, so it is capable of easily introducing a greater variety of Enrollee devices.
- It may be possible to restrict operation of the external Registrar to specific user accounts, thus providing an additional level of control over the process.

The external Registrar device may also be more convenient for the user to operate than the Registrar built into the AP. APs are not always located conveniently for user interaction. For example, if the external Registrar is a cell phone, the portability of the Registrar may improve the user's setup experience, especially if an out-of-band method such as NFC is used.

Although a Registrar may be a WLAN device, it is not required to be. The defining characteristic of a Registrar is that it verifies and issues WLAN Credentials to Enrollees. On a WPA2-Personal network with a single shared WLAN key, any device that has IP connectivity to the AP and that already knows the WLAN key can act as a Registrar to provision new Enrollees.

If the Registrar is external to the AP and the AP supports per-device WLAN keys, however, the Registrar shall also be able to configure the AP with the Enrollee's new Credential. In this case, a secure WLAN Management Interface shall be established between the Registrar and any compliant APs in its Domain. Configuring keys to secure the Management Interface is very similar to establishing trust and shared keys between an Enrollee and a Registrar. The AP Management Interface is also needed if the external Registrar wants to subsequently manage AP settings such as the SSID, channel, and other parameters. Registrars that establish AP Management keys are called WLAN Managers.

To ensure interoperability and satisfy the ease-of-use requirements of Wi-Fi Simple Configuration, Wi-Fi Simple Configuration APs *shall simultaneously support at least three* external Registrars. Note that an AP could continue to function as a standalone Registrar even after it is configured to support one or more external Registrars. This is a policy decision left to the AP implementation. If the AP's standalone Registrar function can be disabled, it is recommended that the AP include a factory reset capability to restore its default operation.

When an AP has a new WLAN Manager Registrar associated by the Wi-Fi Simple Configuration protocol, it may need to replace a previously established WLAN Manager Registrar relationship based on the capacity of the AP. An AP may permit a new WLAN Manager Registrar relationship to be established once knowledge of the AP's shared secret has been demonstrated. Any additional conditions (if it shall be in a configuration mode, for example) that are required for adding an external WLAN Manager Registrar are left up to the AP implementation. Once successfully added, the Management Interface permits any WLAN Manager Registrar to revoke the Registrar privileges of any other WLAN Manager Registrar.

The sections below describe the process for setting up an AP with an external Registrar.

Note that in all discovery diagrams described in this section, the following remarks apply when the discovery takes place in a DMG network (e.g a network in 60 GHz).

1. Message exchanges related to the DMG beamforming procedure are omitted.
2. Authentication frames are not transmitted.
3. The term "beacon" refers to the "DMG Beacon frame".

5.2.1 EAP-based Setup of External Registrar

Figure 2 illustrates the process to register an external Registrar to a Wi-Fi Simple Configuration AP. The message flow and logical transitions in this and other such diagrams in this specification correspond to the state machines in Section 7.7.3 and Section 7.7.4.

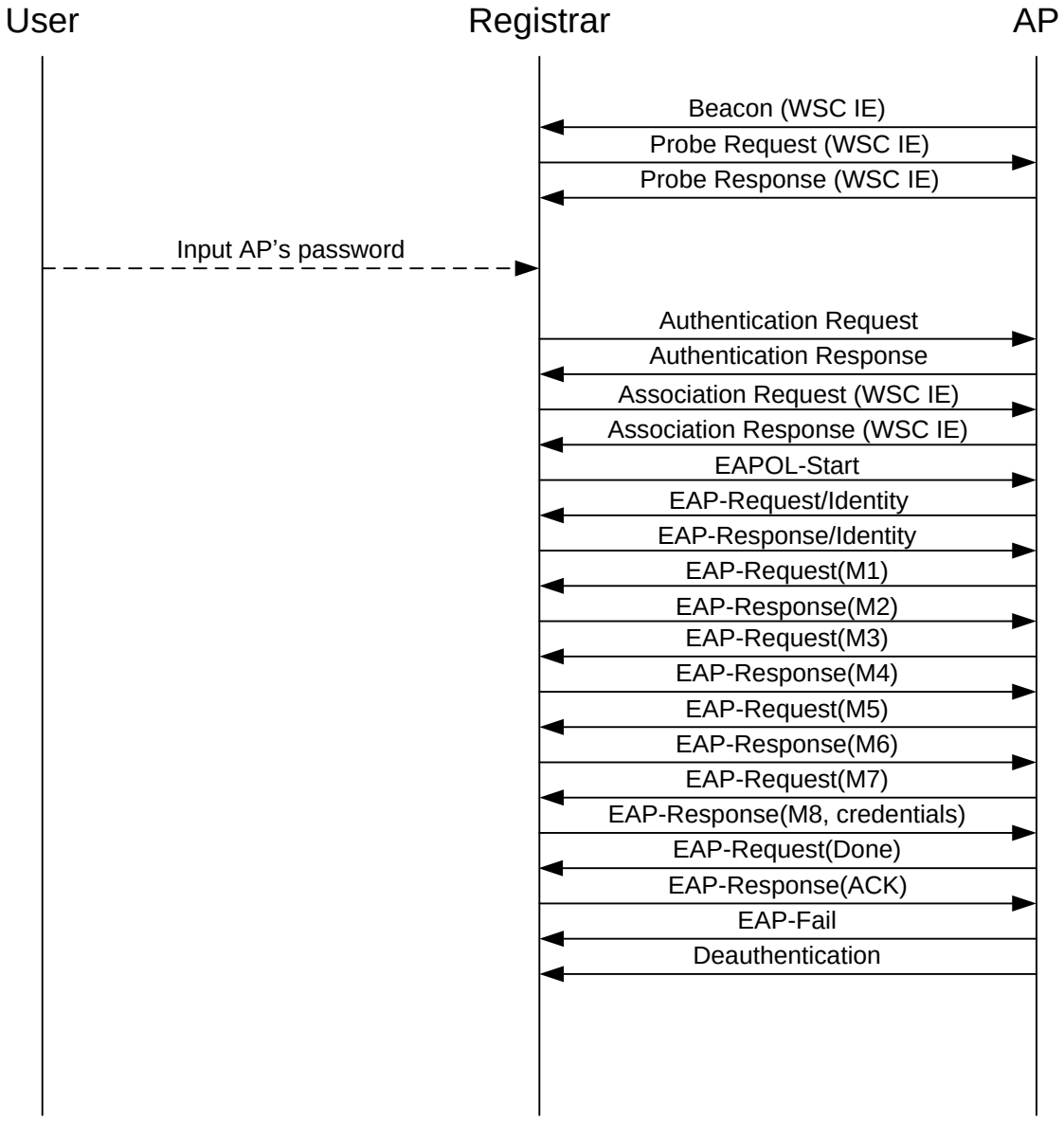

Figure 2 – EAP-based Setup of an External Registrar

1. The AP sends out a beacon that includes an Information Element indicating it supports the Wi-Fi Simple Configuration capability (C).
2. The Registrar sends a Wi-Fi Simple Configuration probe request to the WLAN with Request Type set to Registrar or WLAN Manager Registrar.
3. The AP sends a Wi-Fi Simple Configuration probe response to the Registrar with Response Type set to AP (i.e. Access Point).
4. The user obtains a device password from the AP by reading a label or display on the AP (or its Web page) and enters the password into the Registrar. Alternatively, if both the AP and Registrar support NFC, the user may enter the device password by touching the AP's NFC Tag to the Registrar's NFC reader.
5. The external Registrar initiates an 802.1X connection using the name "WFA-SimpleConfig-Registrar-1-0" as its EAP-Response/Identity.
6. The AP and Registrar exchange messages M1-M8, in accordance with the Registration Protocol. Message M7 includes the current settings of the AP. Message M8 optionally includes new wireless settings specified by the Registrar.
7. The AP sends EAP-Done, the Registrar sends EAP-ACK, and the AP sends EAP-Failure to indicate the end of the Registration Protocol session.
8. The Registrar and AP set their configuration according to the settings delivered in M7 or M8. The Registrar then disassociates and re-associates with the AP and authenticates using its new Credential with the authentication method supported by the AP.

For security reasons, it is recommended for the in-band setup to only be enabled when the AP is in a time-limited setup mode. The AP's device password is unlikely to be very strong, and the system will be more susceptible to attack if the AP remains in its setup mode. Users should be advised to override the default AP password with a stronger secret, but they may not comply.

Mental model mapping

Wi-Fi Simple Configuration provides an easy way to transfer wireless settings and security keys to new devices. The Registrar needs the password of the Enrollee to make sure it gives the WLAN keys to the intended device.

5.2.2 Ethernet-based Setup of External Registrar

Figure 3 illustrates how UPnP can be used for introducing an External Registrar to a Wi-Fi Simple Configuration AP over Ethernet. The goal is to allow the external Registrar to obtain the WLAN settings and/or establish keys that can be subsequently used to secure the AP Management Interface.

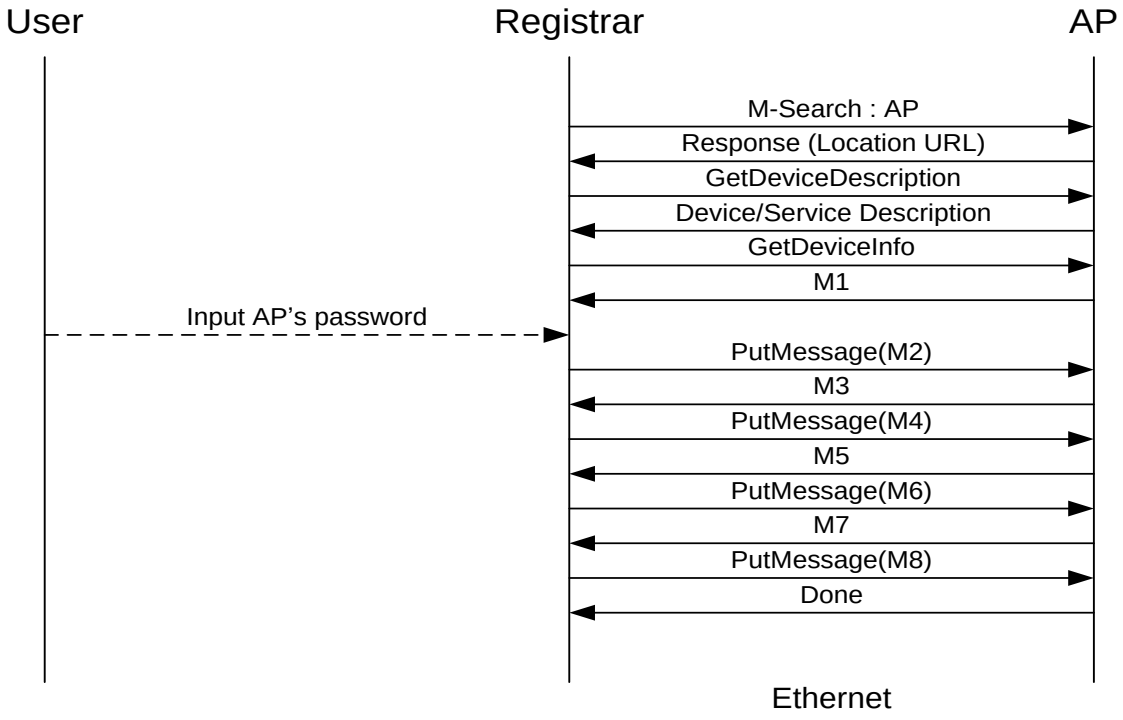

Figure 3 – UPnP-based Setup of an External Registrar

1. The user causes the Registrar to search for the AP using UPnP.
2. The Registrar retrieves the AP's M1 message using the UPnP action GetDeviceInfo.
3. The user obtains a device password from the AP by reading a label or display on the AP (or its Web page) and enters the password into the Registrar.
4. The Registrar and AP exchange M2-M8 using the PutMessage action. As with the EAP-based method, configuration settings are exchanged in M7 and M8.

6 Adding Member Devices

Ideally, a Wi-Fi Simple Configuration AP should support multiple keys such that each Enrollee in a typical home network can be given its own independent Credential. However, it is permitted for the AP to support only a single WPA2-Personal key shared by all devices.

The first scenario in this section applies for adding Enrollees to APs with built-in Registrar capabilities as well as wireless external Registrars.

An Enrollee only shall support a single configuration session at any time. If a Registrar attempts to proceed with configuration of an Enrollee that is engaged in a session with another Registrar, the Enrollee should return a NACK message to the new Registrar. The first Registrar will ignore the NACK, because it will contain different Nonce values.

When an Enrollee is initialized, it looks for Beacons from APs and sends probe requests with the WSC IE into either selected networks or into each network sequentially. It may also send probe requests in each 802.11 channel with the WSC IE included. It looks for the WSC IE in probe responses that it receives and can engage with one or more Registrars to further discover Registrar capabilities and to see if the user has selected a Registrar. The Enrollee should continue looking for Selected Registrar flags in Beacons, probe responses and any M2 messages and should cease scanning when it finds a Registrar indicating that it is prepared to configure it.

When an AP is provisioning an Enrollee and the AP's Wi-Fi Simple Configuration State is set to Configured, the AP shall not change its configuration (except for the use of a per device key).

6.1 In-band Setup Using a Standalone AP/Registrar

This scenario applies both for adding Enrollees with APs with built-in Registrar capabilities as well as wireless external Registrars.

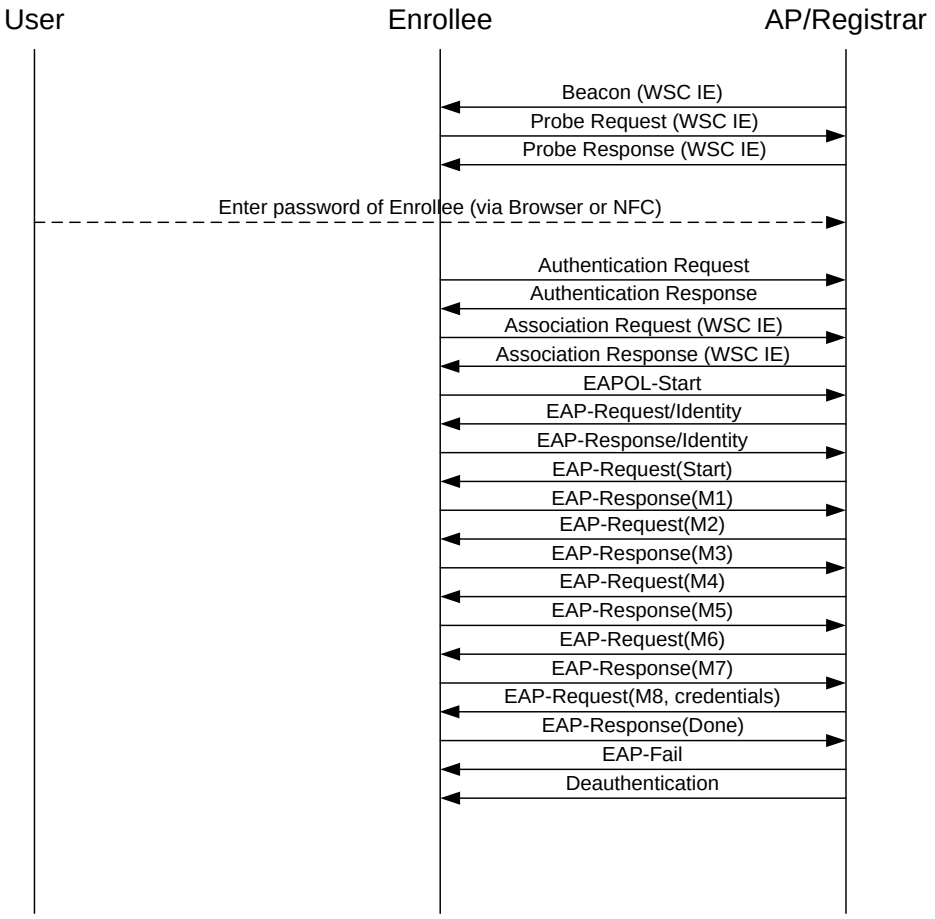

Figure 4 – In-band Setup Using a Standalone AP/Registrar

Setup steps

The following procedure describes an in-band approach for adding Member devices using a Standalone AP/Registrar. This method requires the user to convey the Enrollee's device password to the AP/Registrar using keyboard entry or an out-of-band channel. This example does not show the exchange of M1 and M2D that may take place after the probe message exchange because the Enrollee is waiting for the user to configure the AP/Registrar with the Enrollee's device password.

1. The Enrollee sends its Discovery data in a probe request to a Wi-Fi Simple Configuration AP. The AP or wireless Registrar responds with its own Discovery data in the probe response.
2. The user is prompted to enter the Enrollee's device password into the AP/Registrar using a keypad interface or an out-of-band channel.

3. The Enrollee connects and initiates 802.1X using the identity “WFA-SimpleConfig-Enrollee-1-0”.
4. The Enrollee and Registrar exchange messages M1-M8 to provision the Enrollee.
5. The Enrollee disassociates and reconnects, using its new WLAN authentication Credential.

6.2 In-band Setup Using an External Registrar

This section describes an In-band setup procedure using an External Registrar. The sections 6.2.1 and 6.2.2 explain an example of the user actions and relative protocol sequences for the case where a user triggers a registration protocol at the External Registrar device first. The cases where a user triggers a registration protocol at the Enrollee device first are shown in the sections 6.2.3 and 6.2.4.

6.2.1 PIN based setup - External Registrar trigger first

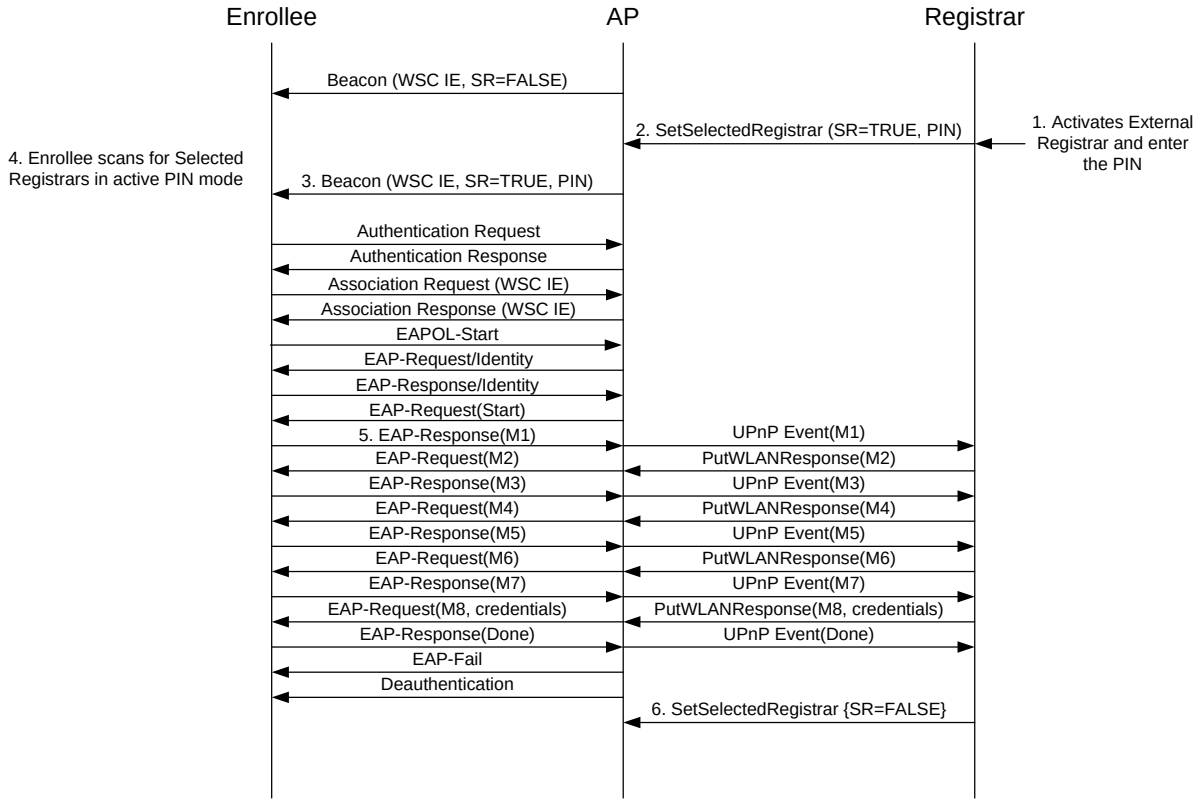

Figure 5 – PIN based setup – External Registrar trigger first

1. User activates PIN based configuration and obtains PIN from the Enrollee by reading a label or display on the Enrollee (or its UI) and enters PIN into the External Registrar

2. External Registrar notifies the AP when it becomes active by setting the Selected Registrar attribute to TRUE using SetSelectedRegistrar UPnP action. The Registrar shall include the wildcard MAC Address (FF:FF:FF:FF:FF:FF) if the Registrar doesn't know the authorized Enrollee MAC Address.
3. After an AP receives a SetSelectedRegistrar UPnP action with Selected Registrar TRUE, AP incorporates Selected Registrar flag set to TRUE in its Beacons and Probe Response. The AP shall also add the MAC addresses from the received AuthorizedMACs subelement in
   an AuthorizedMACs subelement in Beacon and Probe Response frames. If the External Registrar is WSC version 1.0 it will not have included an AuthorizedMACs subelement. In this case the AP shall add the wildcard MAC Address (FF:FF:FF:FF:FF:FF) in an AuthorizedMACs subelement in Beacon and Probe Response frames.
4. Enrollee starts PIN based registration protocol and scans for an AP in active PIN mode
5. Enrollee associates with target AP in active PIN mode and sends M1 message. M1 message is proxied to the External Registrar(s) registered to receive UPnP events.
6. The AP shall update its Selected Registrar attribute based on the state of all active Registrars. This attribute may need to be changed when an External Registrar notifies the AP about the change with the SetSelectedRegistrar UPnP action or becomes disconnected.

6.2.2 PBC based setup – External Registrar trigger first

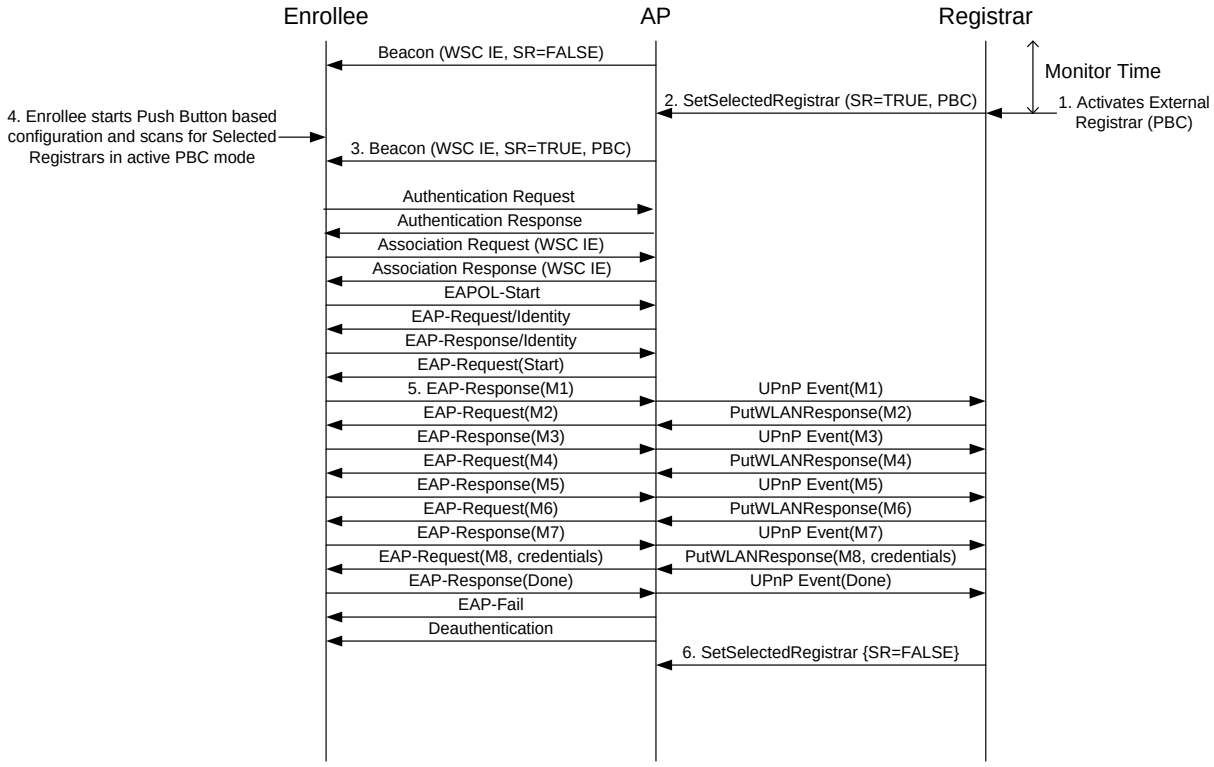

Figure 6 – PBC based setup – External Registrar trigger first

1. User activates Pushbutton based configuration on the External Registrar device
2. External Registrar notifies the AP when it becomes active by setting the Selected Registrar attribute to TRUE using SetSelectedRegistrar UPnP action. The Registrar shall include the wildcard MAC Address (FF:FF:FF:FF:FF:FF) if the Registrar doesn't know the authorized Enrollee MAC Address.
3. After an AP receives a SetSelectedRegistrar UPnP action with Selected Registrar TRUE, AP incorporates Selected Registrar flag set to TRUE in its Beacons and Probe Responses. The AP shall also add the MAC addresses from the received AuthorizedMACs subelement in
an AuthorizedMACs subelement in Beacon and Probe Response frames. If the External Registrar is WSC version 1.0 it will not have included an AuthorizedMACs subelement. In this case the AP shall add the wildcard MAC Address (FF:FF:FF:FF:FF:FF) in an AuthorizedMACs subelement in Beacon and Probe Response frames.
4. Enrollee starts Pushbutton based configuration and scans for AP in active PBC mode
5. Enrollee associates with target AP in active PBC mode and sends M1 message. M1 message is proxied to the External Registrar(s) subscribed to receive UPnP events.

6. The AP shall update its Selected Registrar attribute based on the state of all active Registrars. This attribute may need to be changed when an External Registrar notifies the AP about the change with the SetSelectedRegistrar UPnP action or becomes disconnected.

6.2.3 PIN based setup – Enrollee trigger first

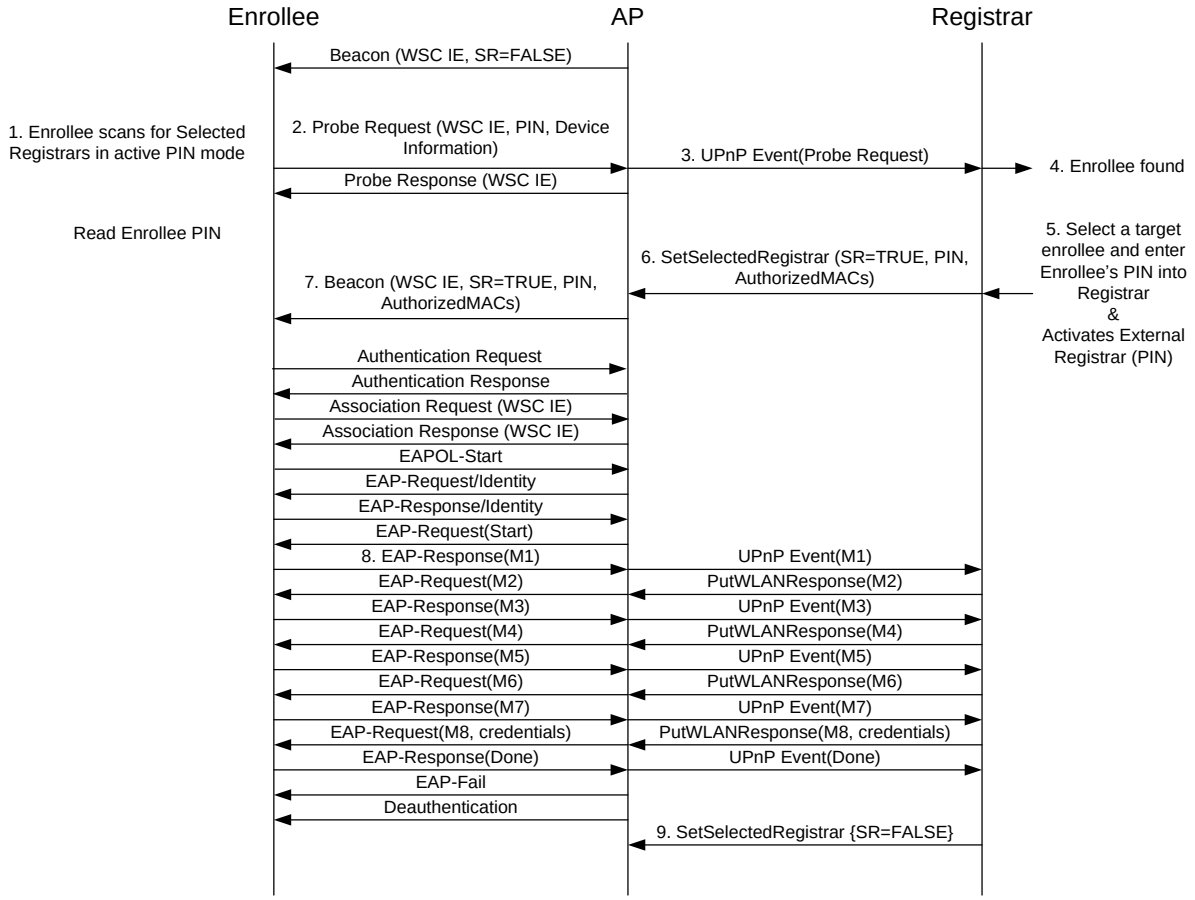

Figure 7 – PIN based setup – Enrollee trigger first

1. User starts PIN based configuration at Enrollee device
2. Enrollee sends a Probe Request with WSC IE
3. AP proxies the Probe Request from Enrollee to the External Registrar(s) subscribed to receive UPnP events
4. External Registrar(s) obtains the device information of the Enrollee
5. User selects a target Enrollee from the device list and enters the Enrollee's PIN into the External Registrar. The optional "Request to Enroll" subelement in the WSC IE

of the Probe Request should be used to indicate which Enrollee device is requesting to start a registration protocol.

6. External Registrar notifies the AP when it becomes active by setting the Selected Registrar attribute to TRUE using SetSelectedRegistrar UPnP action. The External Registrar also shall include AuthorizedMACs subelement in SetSelectedRegistrar UPnP action to notify the AP of the authorized enrollees.
7. After an AP receives a SetSelectedRegistrar UPnP action with Selected Registrar TRUE, AP incorporates Selected Registrar flag set to TRUE in its Beacons and Probe Responses. The AP shall also add the MAC addresses from the received AuthorizedMACs subelement in
an AuthorizedMACs subelement in Beacon and Probe Response frames. If the External Registrar is WSC version 1.0 it will not have included an AuthorizedMACs subelement. In this case the AP shall add the wildcard MAC Address (FF:FF:FF:FF:FF:FF) in an AuthorizedMACs subelement in Beacon and Probe Response frames.
8. Once an Enrollee detects the AP that is in active PIN mode it sends M1 to that AP. If the Enrollee cannot find such an AP, it may follow the fallback procedure written in the Best Practice Document (3.4 “Fallback Wi-Fi Simple Configuration AP detection method”)
9. The AP shall update its Selected Registrar attribute based on the state of all active Registrars. This attribute may need to be changed when an External Registrar notifies the AP about the change with the SetSelectedRegistrar UPnP action or becomes disconnected.

6.2.4 PBC based setup – Enrollee trigger first

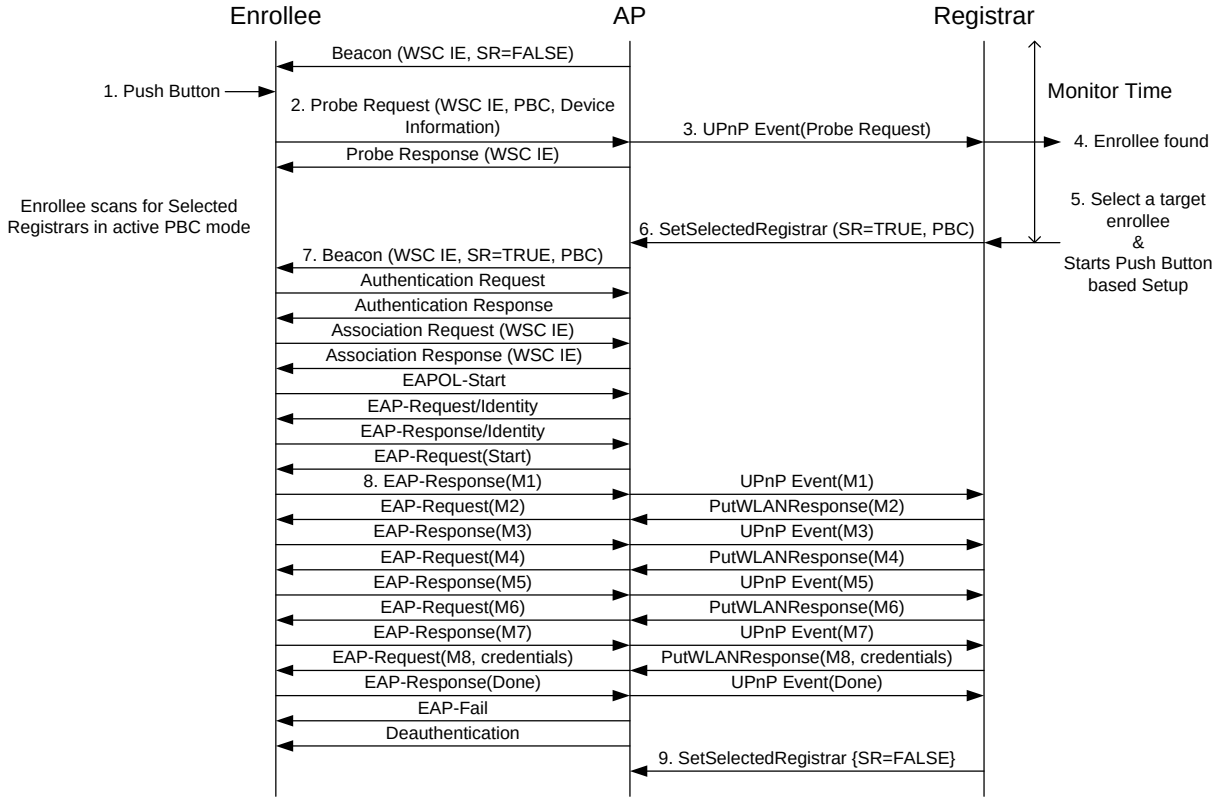

Figure 8 – PBC based setup – Enrollee trigger first

1. User starts PBC based configuration
2. Enrollee sends a Probe Request to AP with WSC IE
3. AP proxies the Probe Request from Enrollee to the External Registrar(s). Probe Request is proxied to the External Registrar(s) subscribed to receive UPnP events
4. External Registrar(s) obtains the device information of the Enrollee
5. User selects a target Enrollee from the device list and activates PBC based External Registrar functionality. The optional “Request to Enroll” subelement in the WSC IE of the Probe Request should be used to indicate which Enrollee device is requesting to start a registration protocol.
6. External Registrar notifies the AP when it becomes active by setting the Selected Registrar attribute to TRUE using SetSelectedRegistrar UPnP action. The External Registrar also shall include AuthorizedMACs subelement in SetSelectedRegistrar UPnP action to notify the AP of the authorized enrollees.
7. After an AP receives a SetSelectedRegistrar UPnP action with Selected Registrar TRUE, AP incorporates Selected Registrar flag set to TRUE in its Beacons and Probe Responses. The AP shall also add the MAC addresses from the received AuthorizedMACs subelement in
an AuthorizedMACs subelement in Beacon and Probe Response frames. If the

External Registrar is WSC version 1.0 it will not have included an AuthorizedMACs subelement. In this case the AP shall add the wildcard MAC Address (FF:FF:FF:FF:FF:FF) in an AuthorizedMACs subelement in Beacon and Probe Response frames.

8. Once an Enrollee detects the AP that is in active PBC mode it sends M1 to that AP.
9. The AP shall update its Selected Registrar attribute based on the state of all active Registrars. This attribute may need to be changed when an External Registrar notifies the AP about the change with the SetSelectedRegistrar UPnP action or becomes disconnected.

6.3 In-band Setup Using Multiple External Registrars

This section describes advanced use cases such as Enrollee introduction with multiple external Registrars using a PIN-based configuration method. It illustrates how the Enrollee can discover multiple external Registrars and suggests how guidance to the user may be provided through a user interface hosted by either the Enrollee or one of the Registrars.

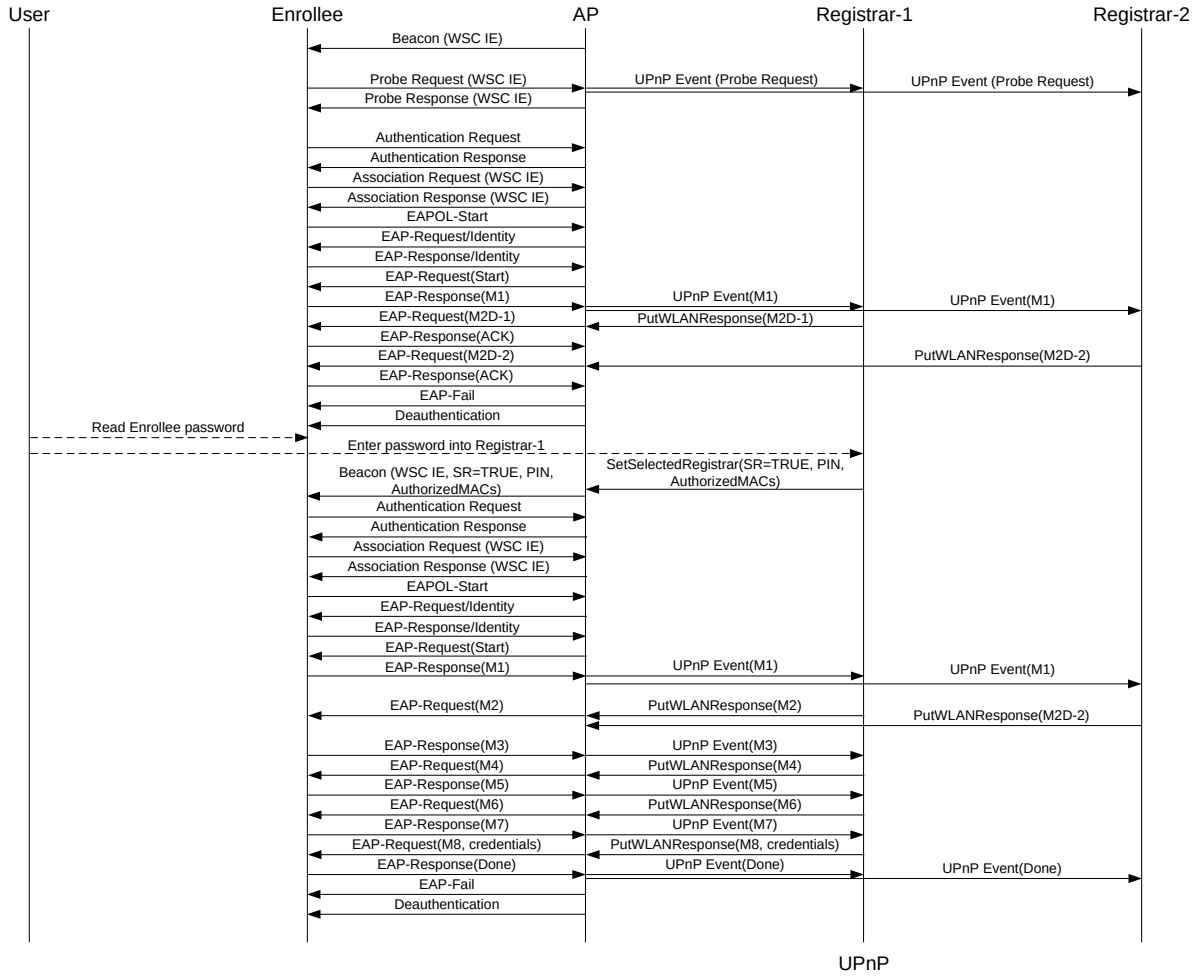

Figure 9 – In-band Setup Using Multiple External Registrars

The scenario shown in this section is the most complex considered so far. This scenario shows discovery of multiple Registrars and subsequent in-band Registration with one of them.

1. The Enrollee sends its Discovery message using an 802.11 probe request. The Discovery message is broadcast by the AP to all external Registrars using UPnP events.
2. The AP responds to the probe request with its own Discovery data.
3. The Enrollee connects to the AP and initiates 802.1X.
4. The Enrollee's M1 message is proxied to all External Registrars as UPnP events. Each active Registrar (Internal Registrar, if enabled, and all the External Registrars that have subscribed to receive UPnP events from the AP) should send M2 or M2D.
5. The two external Registrars send M2D messages to the AP. The AP queues these up for delivery to the Enrollee.

6. The AP sequentially delivers the M2D messages to the Enrollee, which responds with ACK messages to each one. After the last M2D has been delivered without a WSC_MSG response, the AP sends EAP-Failure to terminate the 802.1X connection.
7. The user reads the Enrollee's device password and enters it into the Registrar-1, prompted by either the Enrollee user interface or Registrar-1's user interface.
8. Registrar-1 notifies the AP when it becomes active by setting the Selected Registrar attribute to TRUE using SetSelectedRegistrar UPnP action. Registrar-1 also shall include AuthorizedMACs subelement in SetSelectedRegistrar UPnP action to notify the AP of the authorized enrollees.
9. After the AP receives a SetSelectedRegistrar UPnP action with Selected Registrar TRUE, AP incorporates Selected Registrar flag set to TRUE in its Beacons and Probe Responses. The AP shall also add the MAC addresses from the received AuthorizedMACs subelement in an AuthorizedMACs subelement in Beacon and Probe Response frames. If Registrar-1 is WSC version 1.0 it will not have included an AuthorizedMACs subelement. In this case the AP shall add the wildcard MAC Address (FF:FF:FF:FF:FF:FF) in an AuthorizedMACs subelement in Beacon and Probe Response frames.
10. Enrollee reconnects and restarts the 802.1X authentication. This time, Registrar-1 sends an M2 message rather than an M2D message.
11. The first M2 transmitted from Registrar-1 to the Enrollee locks the Registrar for this protocol run. Potentially remaining M2/M2D messages from Registrar-2 should not be transmitted to the Enrollee
12. The Enrollee and Registrar engage in the complete Registration Protocol until the Enrollee is provisioned with its Credential.

If necessary, the Registrar configures the AP to accept the new Enrollee's Credential before sending M8 to the Enrollee. If the Registrar is managing multiple APs in the same Domain, it may configure all of them with the new Credential at this point.

6.4 Secure Setup with Legacy Enrollee

Context: the user has already configured a Wi-Fi Simple Configuration AP with an external Registrar as previously described.

Setup steps

1. Consult the Registrar UI to obtain the SSID and WPA2-Personal pass phrase to use for the legacy Enrollee.
2. Enter these values into the Enrollee using whatever method that the product supports.

If the pass phrase chosen by the Registrar is a strong secret, it may be very difficult for the user to configure it manually into a legacy Enrollee. The choice of a WPA2-Personal pass phrase is an implementation decision of the Registrar. If a weak pass phrase is used, the WLAN will be susceptible to brute force attacks against the pass phrase. If a strong pass phrase is used, the user may have difficulty configuring legacy devices. If the Registrar and most or all of the Enrollees support re-keying, the WPA2-Personal pass code can be changed dynamically with minimal disruption to the WLAN. This provides an opportunity to strengthen the security of the WLAN once legacy devices are replaced.

6.4.1 Mental model mapping

Wi-Fi Simple Configuration allows keys to be entered manually into devices that do not support advanced key transfer methods.

7 Registration Protocol Definition

This section provides a detailed specification of the Registration Protocol. If the in-band method is chosen, then the user is prompted to enter the device password (typically obtained from a display or label) into the Registrar. While waiting for the password, the Registrar sends an M2D message containing the Registrar's description to the Enrollee. This enables Enrollees with rich user interfaces to give appropriate instructions to the user and direct them to use the correct Registrar. Registration Protocol messages M3-M7 incrementally demonstrate mutual knowledge of the device password. Once both sides have proven knowledge of the password, encrypted configuration data is exchanged. Cryptographic protection for the messages is based on a key derivation key (KDK) that is computed from the Diffie-Hellman secret, nonces, and Enrollee MAC address.

7.1 Registration Protocol Initiation

The initiation of Registration may occur automatically when an Enrollee is powered on. Alternatively, an Enrollee may choose not to attempt Registration unless explicitly directed to do so by some user action. Whether or not the Enrollee automatically initiates Registration, Registrars shall not proceed with the Registration protocol beyond exchange of Discovery (that is, up to M2D) data without the explicit supervision and intervention of the user operating the Registrar.

Messages of a particular instance of the Registration Protocol are identified by nonces and Authenticator attributes. If a message is received with either an invalid nonce or an invalid Authenticator attribute, the recipient shall silently ignore this message. When using UPnP transport, the sender in this case may retransmit the message a few times until its per-message timeout limit is reached, at which point the session is aborted. When using EAP transport, only the IEEE 802.1X authenticator is responsible for retransmitting the messages. Recommended timeout values are: retransmission timeout = 5 seconds, individual message processing timeout = 15 seconds, overall timeout for the entire protocol to complete = 2 minutes.

If a per-message or overall timeout occurs before a valid message is received, both sides shall discard all state information corresponding to the Registration Protocol instance. The only exception to this rule is any error logs that may be kept and when using UPnP transport, sending a WSC_NACK message to the other side with the associated configuration error. If either side of the UPnP transport fails to receive a response or acknowledgement message, it should retransmit the previous message with no modifications.

One common concern with in-band protocols that require expensive computation (such as a Diffie-Hellman exponentiation) is that an attacker may flood a victim with requests that induce it to consume all available computational resources and thus deny service to legitimate users. To mitigate this threat, implementations may choose to respond only to Registration Protocol requests when the device and/or Registrar is in an explicit "Registration Mode" according to the implementation of each device. Enrollee or Registrar policy can yield further improvements. For example, if manual input of a device password is used for authentication, a Registrar should strictly limit the number of times the Registration Protocol is run per user input.

It is permitted for the Device Password ID in the M2 message to differ from the Device Password ID included in M1. This may occur if the Registrar wants to use a different Device Password than originally proposed by the Enrollee. For example, an Enrollee may attempt to run the Pushbutton configuration method by setting M1's Device Password ID to the Pushbutton value. The Registrar may detect multiple Enrollees in PBC mode and may therefore decide that the PIN method should be used instead. It would indicate this to the Enrollee by setting the Device Password ID in M2 to indicate PIN rather than Pushbutton.

7.2 Registration Protocol Messages

Enrollee → Registrar: M_1 = Version || N1 || Description || PK_E

Enrollee ← Registrar: M_2 = Version || N1 || N2 || Description || PK_R [|| ConfigData] || $HMAC_{AuthKey}(M_1 || M_2^*)$

Enrollee → Registrar: M_3 = Version || N2 || E-Hash1 || E-Hash2 || $HMAC_{AuthKey}(M_2 || M_3^*)$

Enrollee ← Registrar: M_4 = Version || N1 || R-Hash1 || R-Hash2 || $ENC_{KeyWrapKey}$(R-S1) || $HMAC_{AuthKey}$ ($M_3 || M_4^*$)

Enrollee → Registrar: M_5 = Version || N2 || $ENC_{KeyWrapKey}$(E-S1) || $HMAC_{AuthKey}$ ($M_4 || M_5^*$)

Enrollee ← Registrar: M_6 = Version || N1 || $ENC_{KeyWrapKey}$(R-S2) || $HMAC_{AuthKey}$ ($M_5 || M_6^*$)

Enrollee → Registrar: M_7 = Version || N2|| $ENC_{KeyWrapKey}$(E-S2 [||ConfigData]) || $HMAC_{AuthKey}$ ($M_6 || M_7^*$)

Enrollee ← Registrar: M_8 = Version || N1 || [$ENC_{KeyWrapKey}$(ConfigData)] || $HMAC_{AuthKey}$ ($M_7 || M_8^*$)

- || this symbol means concatenation of parameters to form a message
- Subscripts when used in the context of a cryptographic function such as $HMAC_{Key}$ refer to the key used by that function.
- M_n^* is message M_n excluding the HMAC-SHA-256 value.
- Version identifies the type of Registration Protocol message.
- N1 is a 128-bit random number (nonce) specified by the Enrollee. A new N1 random number shall be generated for each Registration Protocol instance. The Registrar shall use the N1 value included in the latest M1 from the corresponding enrollee.
- N2 is a 128-bit random number (nonce) specified by the Registrar. A new N2 random number shall be generated for each Registration Protocol instance. Enrollee shall use the N2 value included in the latest M2D/M2 message from the corresponding registrar.
- Description contains a human-readable description of the sending device (UUID, manufacturer, model number, MAC address, etc.) and device capabilities such as supported algorithms, I/O channels, Registration Protocol role, etc.

Description data is also included in 802.11 probe request and probe response messages. Data elements included in the Description for each message are specified in Section 8.

- PK_E and PK_R are Diffie-Hellman public keys of the Enrollee and Registrar, respectively. If support for other cipher suites (such as elliptic curve) is added in the future, a different protocol Version number will be used.
- AuthKey is an authentication key derived from the Diffie-Hellman secret $g^{AB} \bmod p$, the nonces N1 and N2, and the Enrollee's MAC address. If M1 and M2 are both transported over a channel that is not susceptible to man-in-the-middle attack, the Enrollee's device password may be omitted from the key derivation.
- E-Hash1, E-Hash2 are pre-commitments made by the Enrollee to prove knowledge of the two halves of its own device password.
- R-Hash1, R-Hash2 are pre-commitments made by the Registrar to prove knowledge of the two halves of the Enrollee's device password.
- $ENC_{KeyWrapKey}(...)$ This notation indicates symmetric encryption of the values in parentheses using the key KeyWrapKey. The encryption algorithm is AES-CBC per FIPS 197, with PKCS#5 v2.0 padding.
- R-S1, R-S2 are secret 128-bit nonces that, together with R-Hash1 and R-Hash2, can be used by the Enrollee to confirm the Registrar's knowledge of the first and second half of the Enrollee's device password, respectively.
- E-S1, E-S2 are secret 128-bit nonces that, together with E-Hash1 and E-Hash2, can be used by the Registrar to confirm the Enrollee's knowledge of the first and second half of the Enrollee's device password, respectively.
- $HMAC_{AuthKey}(...)$ This notation indicates an Authenticator attribute that contains a HMAC keyed hash over the values in parentheses and using the key AuthKey. The keyed hash function is HMAC-SHA-256 per FIPS 180-2 and RFC-2104. To reduce message sizes, only 64 bits of the 256-bit HMAC output are included in the Authenticator attribute.
- ConfigData contains WLAN settings and Credentials for the Enrollee. Additional settings for other networks and applications may also be included in ConfigData. Although ConfigData is shown here as always being encrypted, encryption is only mandatory for keys and key bindings. Encryption is optional for other configuration data. It is the sender's decision whether or not to encrypt a given part of the ConfigData.

7.2.1 Optional Parameters

Since the Registration Protocol is used for a variety of scenarios, there are a few variants in terms of optional parameters used in different scenarios.

M2 – ConfigData

If M2 is sent to the Enrollee across an out-of-band channel, then ConfigData from the Registrar is included in M2. Encryption of ConfigData on the out-of-band channel is optional.

When setting up an AP over in-band, an External Registrar needs to securely retrieve the current settings from the AP in M7 before deciding whether to keep or override any of them in M8.

If M2 is sent in-band to the Enrollee when both a Handover Request and Handover Select Message have been exchanged over NFC, then ConfigData from the Registrar shall be included in M2. ConfigData shall be encrypted using the KeyWrapKey. The Enrollee shall not respond with M3, but with Response(Done) or Response(NACK), dependent on whether the Enrollee accepts the ConfigData received, see section 10.1.3.

M2D – Registrar Discovery Message

Registrars may respond to Enrollees in-band through M2D rather than M2 if they do not know the Enrollee's Device Password. M2D is used to provide the Enrollee with information about the Registrar. An Enrollee would send an M3 message and continue with the Registration Protocol exchange only if it receives an M2 message from a Registrar.

M7 – ConfigData

If the Enrollee is an AP running the Registration Protocol over in-band with a Registrar that is requesting to be added as an external Registrar, the current WLAN settings and keys of the AP are included in a ConfigData parameter in M7. This allows the Registrar to either keep or override the current settings in M8. Enrollees may also include an X.509 Certificate Request in M7 if the Registrar supports this feature. If ConfigData is included in M7 or M8, it shall be encrypted using the KeyWrapKey.

M8 – ConfigData

If the Enrollee is an AP running the Registration Protocol over the in-band channel with a Registrar that is requesting to be added as an external Registrar, the current WLAN settings and keys of the AP are included in a ConfigData parameter in M7.

The inclusion of AP settings and keys allows the Registrar to either keep or override the current settings in M8. Enrollees may also include an X.509 Certificate Request in M7 if the Registrar supports this feature. If ConfigData is included in M7 or M8, it shall be encrypted using the KeyWrapKey.

Note: An unauthenticated method such as PBC cannot be used to establish an external Registrar.

7.2.2 Validation of Configuration Data

When processing ConfigData from M8 (or M2) received from a Registrar that is using WSC version 2.0 or newer, the Enrollee shall verify that the MAC Address attribute inside each Credential attribute (if the Enrollee is a STA) or the MAC Address attribute inside the encrypted settings (if the Enrollee is an AP) matches with its own MAC Address. If an address mismatch is found, the ConfigData shall not be used and the protocol run shall be terminated with an error. In case the ConfigData was received in M8, the Enrollee shall reply with WSC_NACK using Configuration Error value 13 (Rogue activity suspected).

If the optional Network Key Sharable attribute is included in a Credential attribute, the Registrar is explicitly indicating to the Enrollee whether the Network Key can be shared with other devices. If the Network Key Sharable attribute has value 0 (FALSE), the Enrollee shall not share the Network Key with other devices. This may indicate that the Network Key is a per-STA key or that the Registrar policy does not allow the key to be shared.

Note: Existing Registrar implementations based on specification 1.0h might not use the Enrollee's MAC address as the value of the MAC Address attribute in ConfigData. For backwards compatibility, the contents of this attribute are ignored when the Registrar is not using protocol version 2.0 or newer.

7.3 Key Derivation

Upon receipt of M1, the Registrar has enough information to determine whether to use the in-band method or out-of-band method for enrollment. If M2 is sent over a physically secure out-of-band channel, then ConfigData can be sent in M2, and the Registration Protocol can be terminated at that point. Depending upon the physical security of the out-of-band channel and the Registrar's policy, the Registrar can choose whether to encrypt ConfigData that is sent in an out-of-band M2. Encrypting this data provides an additional measure of security.

1536-bit MODP Group for Diffie-Hellman Exchange

The 1536 bit MODP group used by Wi-Fi Simple Configuration is taken from RFC 3526.

The prime is: 2^1536 - 2^1472 - 1 + 2^64 * { [2^1406 pi] + 741804 }

Its hexadecimal value is:

FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B 80DC1CD1
29024E08 8A67CC74 020BBEA6 3B139B22 514A0879 8E3404DD
EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D 6D51C245
E485B576 625E7EC6 F44C42E9 A637ED6B 0BFF5CB6 F406B7ED
EE386BFB 5A899FA5 AE9F2411 7C4B1FE6 49286651 ECE45B3D
C2007CB8 A163BF05 98DA4836 1C55D39A 69163FA8 FD24CF5F
83655D23 DCA3AD96 1C62F356 208552BB 9ED52907 7096966D

670C354E 4ABC9804 F1746C08 CA237327 FFFFFFFF FFFFFFFF

The generator is: 2.

Derivation of KDK

KDK = HMAC-SHA-256$_{DHKey}$ (N1 || EnrolleeMAC || N2)

DHKey is defined as SHA-256 (zeropad($g^{AB} \bmod p$, 192)) , where zeropad(value, 192) means that the binary presentation of the value is padded with zeros from left to the length of 192 octets. PK_E is $g^A \bmod p$ and PK_R is $g^B \bmod p$. The Enrollee and Registrar know the secret values A and B, respectively. EnrolleeMAC is the 6-byte 802.11 MAC address of the Enrollee. The Enrollee's MAC address is included in the Description data sent in M1.

Derivation of AuthKey, KeyWrapKey, and EMSK

Additional keys are derived from KDK using a key derivation function (kdf). The function prf used in kdf is the keyed hash HMAC-SHA-256.

```
kdf(key, personalization_string, total_key_bits) :
        result := ""
        iterations = (total_key_bits + prf_digest_size – 1)/prf_digest_size
        for i = 1 to iterations do
                result := result || prf(key, i || personalization_string || total_key_bits)
         return 1st total_key_bits of result and destroy any bits left over
```

In the pseudocode, key is the 256-bit KDK, i and total_key_bits are 32-bit unsigned integers, and personalization_string is a UTF-8 string without NULL termination. Concatenation is big endian.

Given KDK and this key derivation function, the Registration Protocol session keys are derived as follows:

AuthKey || KeyWrapKey || EMSK = kdf(KDK, "Wi-Fi Easy and Secure Key Derivation", 640)

- **AuthKey** (256 bits) used to authenticate the Registration Protocol messages.
- **KeyWrapKey** (128 bits) used to encrypt secret nonces and ConfigData.
- **EMSK** (256 bits) an Extended Master Session Key that is used to derive additional keys used by Wi-Fi Simple Configuration and possibly other applications.

This notation means that 640 bits are generated by the kdf function using the seed value KDK. These 640 bits are split into three parts corresponding to the three symmetric session keys AuthKey, KeyWrapKey, and EMSK.

Application-specific master session keys

Application-specific master session keys (AMSK) used to bootstrap trust for other applications can be derived from the EMSK using the previously described kdf. If, for example, an external Registrar being introduced to an AP specifies WLAN Manager Registrar as its Request Type, then the EMSK is used to derive symmetric keys for the AP Management Interface:

MgmtAuthKey || MgmtEncKey = kdf(EMSK, N1 || N2 || "WFA-WLAN-Management-Keys", 384)

- **MgmtAuthKey** (256 bits) is used to authenticate AP management messages.
- **MgmtEncKey** (128 bits) is used to encrypt AP management messages.

When using these keys in UPnP processing, the key identifiers are:

MgmtAuthKeyID = first 128 bits of SHA-256 (N1 || N2 || "WFA-WLAN-Management-MgmtAuthKey")

MgmtEncKeyID = first 128 bits of SHA-256 (N1 || N2 || "WFA-WLAN-Management-MgmtEncKey")

7.4 Proof-of-possession of Device Password

E-Hash1 is derived from the session parameters and the device password as follows. First, the device password is converted to two 128-bit PSK values as follows:

PSK1 = first 128 bits of $HMAC_{AuthKey}$(1st half of DevicePassword)

PSK2 = first 128 bits of $HMAC_{AuthKey}$(2nd half of DevicePassword)

If the selected configuration method is PIN (label or display), then DevicePassword consists of the ASCII representation of the PIN's decimal values (without NULL termination). For example, if the PIN value is 39358448, DevicePassword would be expressed as the eight ASCII characters "39358448". PSK1 would then be derived from the HMAC of "3935" and PSK2 from the HMAC of "8448".

If an out-of-band mechanism is used as the configuration method, the device password is expressed in hexadecimal using ASCII characters (two characters per octet, uppercase letters only). For example, an Out-of-Band Device Password with a 16-byte Device Password value of 0x100a200b300c400d500e600f70018002 would be expressed as the 32 ASCII characters "100A200B300C400D500E600F70018002".

In case the UTF8 representation of the DevicePassword length is an odd number (N), the first half of DevicePassword will have length of N/2+1 and the second half of the DevicePassword will have length of N/2.

The Enrollee creates two 128-bit secret nonces, E-S1, E-S2 and then computes

$$\text{E-Hash1} = \text{HMAC}_{\text{AuthKey}}(\text{E-S1} \,||\, \text{PSK1} \,||\, \text{PK}_E \,||\, \text{PK}_R)$$

$$\text{E-Hash2} = \text{HMAC}_{\text{AuthKey}}(\text{E-S2} \,||\, \text{PSK2} \,||\, \text{PK}_E \,||\, \text{PK}_R)$$

The Registrar creates two 128-bit secret nonces, R-S1, R-S2 and then computes

$$\text{R-Hash1} = \text{HMAC}_{\text{AuthKey}}(\text{R-S1} \,||\, \text{PSK1} \,||\, \text{PK}_E \,||\, \text{PK}_R)$$

$$\text{R-Hash2} = \text{HMAC}_{\text{AuthKey}}(\text{R-S2} \,||\, \text{PSK2} \,||\, \text{PK}_E \,||\, \text{PK}_R)$$

The hash values are gradually exchanged and verified in messages M3-M7. If a verification check of one of the Device Password parts fails, the receiving side shall acknowledge the message with a failure indication, and the Enrollee and Registrar shall stop the protocol and discard all keys and nonces associated with the session.

If the Enrollee supports multiple device passwords (one on a label and one on an NFC Tag, for example), it determines the password known to the Registrar from the Device Password ID transferred with M2. If the Enrollee supports a display capable of showing a dynamic device password, the Enrollee SHALL discard the prior device password and choose a new one before each instance of the Registration Protocol. This technique prevents an attacker from using a brute force attack to crack the first half of the device password in one round of the Registration Protocol and then use that value to crack the second half in a second round of the protocol.

7.4.1 PIN Checksums

If the Device Password ID is Default (value = 0), this means that the device password is a PIN. For 8-digit numeric PINs, the last digit in the PIN is used as a checksum of the other digits. This has the disadvantage of reducing the entropy of the PIN. It has the advantage, however, of enabling errors in user input of the PIN to be detected and potentially corrected before the PIN is actually used in the Registration Protocol. The algorithm to validate the checksum is given in C code below.

```
bool ValidateChecksum(unsigned long int PIN)
{
   unsigned long int accum = 0;
        accum += 3 * ((PIN / 10000000) % 10);
        accum += 1 * ((PIN / 1000000) % 10);
        accum += 3 * ((PIN / 100000) % 10);
        accum += 1 * ((PIN / 10000) % 10);
        accum += 3 * ((PIN / 1000) % 10);
        accum += 1 * ((PIN / 100) % 10);
        accum += 3 * ((PIN / 10) % 10);
        accum += 1 * ((PIN / 1) % 10);
```

```
    return (0 == (accum % 10));
}
```

The corresponding algorithm to compute the checksum digit given the other seven random PIN digits is:

```
int ComputeChecksum(unsigned long int PIN)
{
        unsigned long int accum = 0;
        PIN *= 10;
        accum += 3 * ((PIN / 10000000) % 10);
        accum += 1 * ((PIN / 1000000) % 10);
        accum += 3 * ((PIN / 100000) % 10);
        accum += 1 * ((PIN / 10000) % 10);
        accum += 3 * ((PIN / 1000) % 10);
        accum += 1 * ((PIN / 100) % 10);
        accum += 3 * ((PIN / 10) % 10);

        int digit = (accum % 10);
        return (10 - digit) % 10;
}
```

Users of course are not expected to compute checksums for passwords they choose, so user-specified Device Passwords do not include a checksum digit. Other types of Device Passwords, such as those transferred using NFC, are not manually entered by the user, so there is no need to include a checksum in these types of device passwords. Checksum digits are only included and validated for the Default (PIN) device password type, and only if an 8-digit PIN is used.

7.4.2 Device Password Splitting

If a Device Password length is an odd number of bytes, the extra byte is included in PSK1.

7.4.3 Device Password Usage in M1 and M2

The following are recommendations on the use of the Device Password ID (DPID) in M1 and M2. See section 8.2.1 for the Device Password usage in Beacons and section 8.2.5 for usage in probe responses.

1. In M1, Enrollee sends DPID=Default, Configuration Methods does not include Display bit. Registrar accepts user input of 8-digit PIN. Registrar checks the checksum digit and warns user if checksum does not match. Registrar sends M2 with DPID=Default to Enrollee.

2. In M1, Enrollee sends DPID=Default, Configuration Methods has Display bit set. Registrar accepts user input of 4- or 8-digit PIN. If 8-digit, Registrar checks the checksum digit and warns user if checksum does not match. Registrar sends M2 with DPID=Default to Enrollee.
3. In M1, Enrollee sends DPID=User-specified. Registrar accepts user input of 8-digit PIN. Registrar does not check the checksum digit. Registrar sends M2 with DPID=User-specified to Enrollee.
4. In M1, Enrollee sends DPID=Machine-specified. Registrar checks to see if it knows the machine-specified password for the Enrollee (based on Enrollee UUID). If so, it sends M2 with DPID=Machine-specified. If not, it sends M2D.
5. In M1, Enrollee sends DPID=Rekey. Registrar checks to see if it knows the rekey password for the Enrollee (based on Enrollee UUID). If so, it sends M2 with DPID=Rekey. If not, it sends M2D.
6. In M1, Enrollee sends DPID=Pushbutton. If Registrar supports Pushbutton method, it gives user the option of activating the Registrar with that method. If PBC is active on the Registrar, it sends M2 with DPID=Pushbutton. If not, and if no other password for that Enrollee is known, it sends M2D. If the Registrar knows a Machine-specified password for the Enrollee, the Registrar shall send M2 with DPID=Machine-specified. If the Registrar does not know a Machine-specified password, but the user has provided the Registrar with the Enrollee's PIN, then the Registrar shall send M2 with DPID=Default.
7. In M1, Enrollee sends DPID=Registrar-specified. Registrar checks to see if it knows the Registrar-specified password for the Enrollee (based on Enrollee UUID). If so, it sends M2 with DPID=Registrar-specified. If not, it sends M2D.
8. In M1, Enrollee sends DPID=NFC-Connection-Handover. Registrar checks to see if it has received a public key hash value in an NFC Connection Handover message that matches the hash of the Enrollee’s public key from M1. If so it sends M2. If not, it sends M2D.
9. In any of above cases, if Registrar has received a device password via an out-of-band channel with a public key hash matching the Enrollee public key given in M1, then the Registrar sends M2 with DPID=Password ID taken from Out-of-Band Device Password attribute.

In any of above cases, a Registrar shall accept only numeric digits as input for the PIN. As examples, user inputs of 12345678 or 1234-5678 would be interpreted identically as 12345678. To meet this requirement, an implementation of a Registrar may either reject non-numeric input (i.e., require user to re-enter the PIN by identifying non-numeric input) or may allow non-numeric characters (but subsequently ignore such characters and only use the digits from the user input).

7.5 Key Wrap Algorithm

The following algorithm is used to perform the key wrap function that protects the secret nonces and the ConfigData.

1. First compute **KWA** = 1st 64 bits of $HMAC_{AuthKey}$(**DataToEncrypt**)
2. Generate random 128-bit **IV**.
3. Compute **WrappedData** = **AES-Encrypt-CBC**$_{KeyWrapKey}$**(DataToEncrypt || KWA, IV)**
4. **IV** is included along with **WrappedData** in the Encrypted Settings attribute.

To decrypt, use the following algorithm.

1. **Data** || **KWA** = **AES-Decrypt-CBC**$_{KeyWrapKey}$(**WrappedData**, **IV**)
2. If **KWA** = 1st 64 bits of $HMAC_{AuthKey}$(**Data**), then output **Data**, else output "failure"

Note: IV shall be random, and it shall not be copied from any keying material used for other purposes. A freshly-generated random nonce shall be used. KWA is the Key Wrap Authenticator attribute.

7.6 Key Summary and Classification

The table in this section summarizes the different keys created and used by Wi-Fi Simple Configuration. For security reasons, it is important to use keys for specific purposes. A key used for bulk data encryption, for instance, should not be used for key wrapping. Likewise, a key used for message signing (authentication) should not be used for encryption.

Table 1 – Key Types and Lifetimes

Key Name	Type	Known by	Used for
PK_E	Authentication and key derivation, Long-lived or Temporary	Enrollee, Registrar	Generating session keys
PK_R	Authentication and key derivation, Long-lived or Temporary	Enrollee, Registrar	Generating session keys
Device password	Authentication, Temporary if shown on display, may be Long-lived if on label or NFC Tag	Enrollee, Registrar	Authenticating Diffie-Hellman exchange
$g^{AB} \bmod p$	Authentication and key derivation, Temporary	Enrollee, Registrar	Generating session keys

Key Name	Type	Known by	Used for
KDK	Key derivation, Temporary	Enrollee and Registrar	Generating session keys
AuthKey	Authentication, Temporary	Enrollee and Registrar	Mutual authentication of Enrollee and Registrar
KeyWrapKey	Key wrap, Temporary	Enrollee and Registrar	Encrypting WLAN Configuration for Enrollee
PSK1	Authentication, Temporary	Enrollee and Registrar	Proof-of-possession of device password
PSK2	Authentication, Temporary	Enrollee and Registrar	Proof-of-possession of device password
EMSK	Key derivation, Temporary	Enrollee and Registrar	Derivation of AMSK keys
MgmtAuthKey	Authentication, Long-lived	Registrar and AP	Authentication and authorization of AP Management Interface
MgmtEncKey	Encryption, Long-lived	Registrar and AP	Privacy for AP Management Interface

7.7 EAP Transport of Registration Protocol

Wi-Fi Simple Configuration uses 802.1X and EAP to transport in-band Registration Protocol messages, with attributes transported with big endian byte ordering. This protocol is mapped onto a custom EAP method described below. Wi-Fi Simple Configuration does not require the AP to support RADIUS, and the network need not include an authentication server. In fact, many Wi-Fi Simple Configuration APs may support 802.1X only to configure WPA2-Personal Credentials using Wi-Fi Simple Configuration. Enrollees using Wi-Fi Simple Configuration are not granted direct access to the WLAN through the Wi-Fi Simple Configuration custom EAP method. The EAP method is used to configure the Enrollee with a Credential that can be used subsequently with whatever access method is supported by that WLAN. For example, if the AP only supports WPA2-Personal with a network-wide shared PSK, then the Enrollee would run the 802.1X exchange to obtain the PSK, disassociate, and then reconnect and use WPA2-Personal to access the WLAN. Alternatively, if the AP supports 802.1X authentication, the Enrollee may first run the Wi-Fi Simple Configuration EAP method to obtain a shared secret Credential and then reconnect using that secret in conjunction with another EAP method to access the WLAN.

The Wi-Fi Simple Configuration EAP method (EAP-WSC) can be used for Registrar and Enrollee discovery and for Credential establishment. The first time the Enrollee encounters a new WLAN, it sends out its Discovery information and executes the EAP-WSC method. In both the Discovery message and in M1, the Enrollee provides information about itself to the WLAN. The M2 and M2D messages sent to the Enrollee likewise provide information about the available Registrars. When the Enrollee first discovers and attempts to connect to the WLAN, the WLAN's Registrar(s) may not yet

know the Enrollee's device password. Therefore, Registrars without the device password respond with M2D messages. Although these M2D messages are unauthenticated, they can help Enrollees with rich user interfaces to guide the user through the enrollment process and can also help a headless Enrollee select a particular Registrar that may support optional or vendor extended functions.

As the Enrollee scans over the M2D messages sent by the network, it may discover that none of them possesses its device password. At this point, the Enrollee has an opportunity to prompt the user to perform a trust bootstrapping operation such as connecting an available out-of-band channel or entering a device password into one of the available Registrars. If the user decides to enter the Enrollee's device password into the Registrar, the Enrollee can reconnect and run the EAP method once more to perform the complete Registration Protocol. If the Enrollee has no user interface to lead the user through the enrollment, it is likely that one or more of the WLAN's Registrars can do this. Both the Registrar and the Enrollee are given sufficient information about each others' capabilities through the EAP method to successfully lead the user through the enrollment. If the user decides to use an out-of-band channel for registration, then M2 is implicitly authenticated by the channel and can carry the network configuration data.

7.7.1 EAP Message Framing

The AP functions as the EAP authenticator on the WLAN. Thus, the AP generates EAP Request messages, and Enrollees and Registrars generate EAP Responses. If the Registrar is external to the AP, then it uses UPnP (rather than RADIUS) to exchange Registration Protocol messages with the AP. A Registrar may also function in the role of an 802.1X authenticator. This latter mode is useful for networks with legacy APs.

The following text presents a brief summary of the Wi-Fi Simple Configuration EAP method. The EAP packet format for Request and Response messages is depicted in Figure 10. The Wi-Fi Simple Configuration EAP method uses EAP as specified in RFC 3748 and EAPOL as specified in IEEE 802.1X-2001, but does not represent a network authentication protocol. Rather Wi-Fi Simple Configuration utilizes the 802.1X data connection for acquiring settings necessary for connecting to the network and the resulting EAP exchange shall always terminate with EAP-Failure.

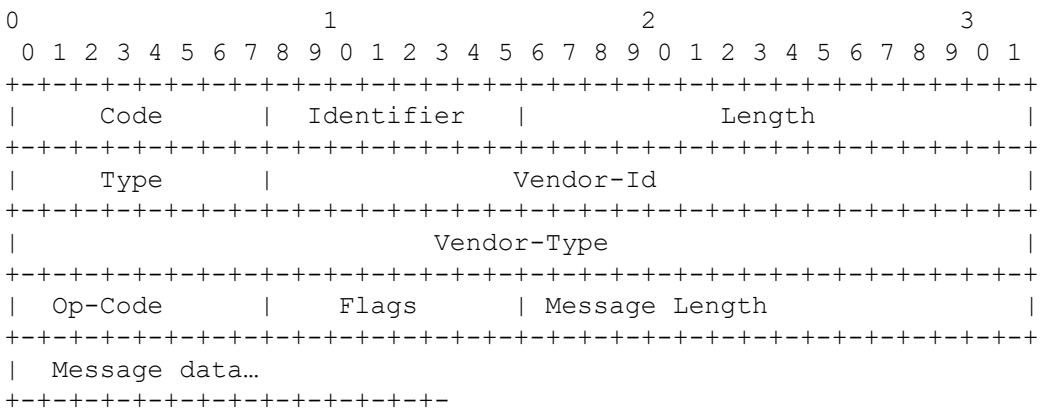

Figure 10 – EAP Packet Format

The Code field is set to 1 for EAP-Request messages and to 2 for EAP-Response messages. The Identifier field is used to correlate Request and Response messages. The Length gives the overall length of the EAP packet. The Type indicates the EAP method type. For Wi-Fi Simple Configuration, it is set to 254 (expanded type).

The Vendor-Id is the WFA SMI code 0x00372A, and the Vendor-Type is: 0x0000 0001 (SimpleConfig).

The Op-Code field is one of the following values:

- 0x01 : WSC_Start
- 0x02 : WSC_ACK
- 0x03 : WSC_NACK
- 0x04 : WSC_MSG
- 0x05 : WSC_Done
- 0x06 : WSC_FRAG_ACK

The sequence of the messages corresponding to these Op-Code values is defined by the appropriate state machine associated with the scenario (adding an Enrollee or adding an external Registrar).

The Flags field is a bit-wise OR of flags.

- 0x01 : more fragments (MF)
- 0x02 : Length field (LF)
- 0x04 – 0x80 : reserved

The Message Length field, if included, contains the total length of the WSC TLV attributes in the WSC message.

The Message Data field contains the WSC TLV attributes. The WSC message may be fragmented and placed in multiple EAP packets.

Fragmentation and Reassembly

If the MF flag is set, the original packet required fragmentation, and additional fragments still need to be transmitted. The MF flag is not set if no additional packet fragments are expected. After receiving each packet with MF set, the receiving party responds with a WSC_FRAG_ACK message. The Message Data parts of each fragment are concatenated together by the receiving party to reassemble the original packet.

If the LF flag is set, the Message Length field is included in the header to indicate the number of bytes of the entire WSC message data being conveyed. If the LF is not set, the Message Length field is omitted. The LF flag and Message Length field shall be included in the first EAP packet for a fragmented EAP message. The LF flag shall not be set for later fragments.

EAP fragmentation is specific to the EAP connection. If a message is fragmented for transmission over EAP, the supplicant and authenticator shall handle fragmentation and reassembly of the frame. The proxy function shall provide a completely assembled message to the UPnP interface.

EAP Identity

If the supplicant intends to add itself as an external Registrar, it shall use the EAP Identity “WFA-SimpleConfig-Registrar-1-0”. If it intends to acquire WLAN credentials as an Enrollee, it shall use the EAP Identity “WFA-SimpleConfig-Enrollee-1-0”.

7.7.2 EAP Messages

WSC_Start

The AP sends WSC_Start when it receives an EAP Response/Identity containing the NAI “WFA-SimpleConfig-Enrollee-1-0”. The Message Data field of this message is empty.

WSC_ACK

WSC_ACK is sent by the Enrollee or Registrar when it successfully processes a message but does not have a message to send in response. For example, WSC_ACK is sent in response to M2D messages. The Message Data field is indicated in 8.3.10.

WSC_NACK

WSC_NACK is sent by the supplicant or the authenticator if it encounters an error authenticating or processing a message. If the supplicant is an Enrollee, this message is sent by the AP to all external Registrars that have subscribed to receive UPnP events. The Message Data field of this message is specified in Section 8.3.11.

WSC_MSG

The supplicant or authenticator may send a WSC_MSG. Its MessageData payload contains a Registration Protocol message. The authenticator state machine does not look into these messages to determine their contents. It simply passes them along to the Registrar or Enrollee.

WSC_Done

WSC_Done is sent by the Enrollee after it has successfully processed a WSC M8 message. It indicates that the Enrollee believes it has correctly received a Credential for the WLAN. The Message Data field is indicated in 8.3.12.

WSC_FRAG_ACK

WSC_FRAG_ACK is sent by the supplicant or the authenticator when it successfully processes a fragment of an EAP message and is ready for the next fragment.

7.7.3 EAP State Machine for Enrollee Registration

Figure 11 illustrates an EAP state machine on the AP (802.1X authenticator) for adding Enrollees. Registrar and Enrollee state machines are not specified in this document, but they should be constructed so that they operate in accordance with the AP's state machine and the Registration Protocol. Dotted line transitions represent messages sent by the authenticator on the AP. Solid line transitions represent messages sent by the Enrollee. Comma-separated lists indicate that the message may be one of those in the list. The lock-step sequence of the Registration Protocol shall be preserved in this machine. Once M5 is sent, for example, if anything but M6 is received, the Enrollee will respond with a NACK message.

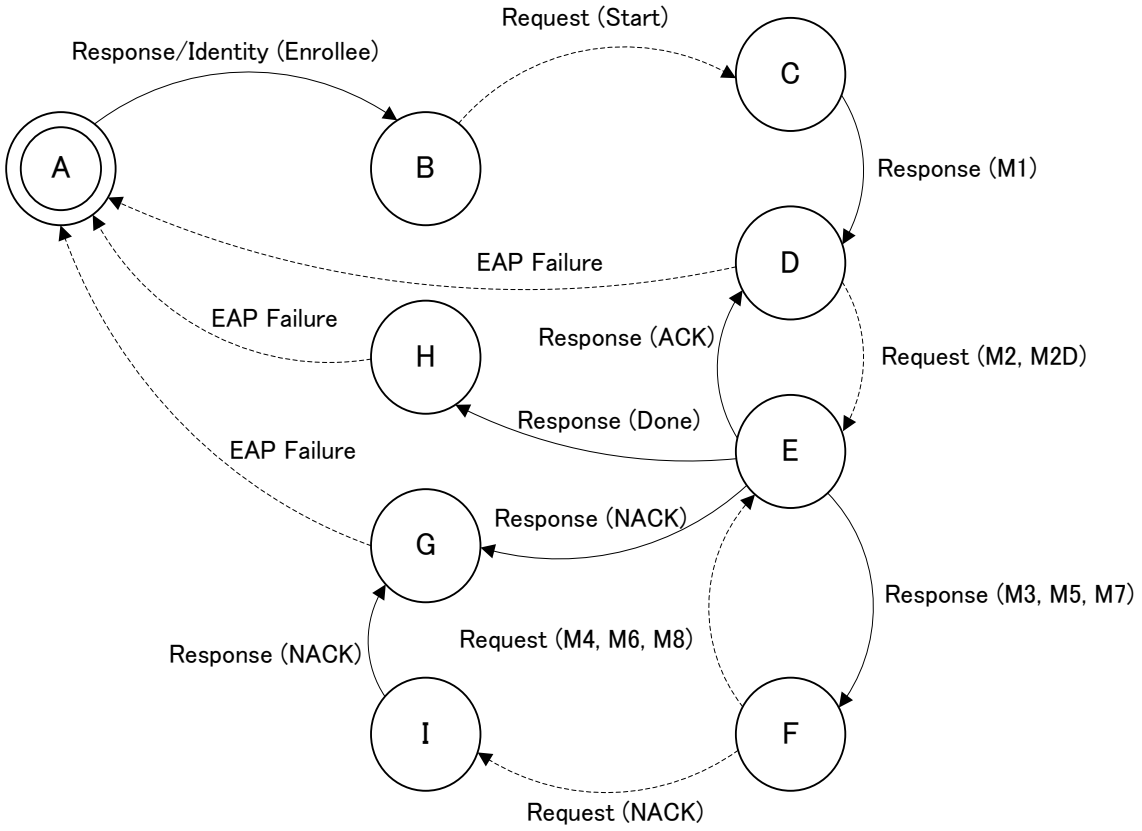

Figure 11 – EAP State Machine for Enrollee Registration

When the Enrollee decides to connect to the network and run the Wi-Fi Simple Configuration EAP method, it associates with the AP and sends an EAPoL-Start message. The AP responds with an EAP-Request/Identity. The Enrollee sends an EAP-Response/Identity containing the defined Wi-Fi Alliance name for a Simple Configuration Enrollee ("WFA-SimpleConfig-Enrollee-1-0"). This causes the AP to start running the Simple Configuration EAP method. The Registration Protocol messages are exchanged until M8 is received and validated by the Enrollee. If it successfully processes M8, the Enrollee sends an EAP-Response/Done message to the authenticator, which events the WSC_Done message to any External Registrar and the authenticator returns an EAP-Failure message to the Enrollee. An Enrollee should

assume that the received credentials are valid after successfully processing message M2 that includes ConfigData or M8 and sending the WSC_Done message. The Enrollee then disassociates and reconnects with the Credential obtained from M2's or M8's ConfigData. If M2D is received by the Enrollee, it should respond with an ACK message so that the AP can continue to send it discovery messages from other Registrars. After the AP sends an EAP-Failure to the Enrollee, the Enrollee can do one of two things (given that the AP did not de-authenticate the Enrollee after sending the EAP-Failure): it can disconnect from the AP and reconnect some time later to rerun the Wi-Fi Simple Configuration EAP method by sending an EAPoL-Start message OR it can stay connected to the AP and rerun the Wi-Fi Simple Configuration EAP method by sending another EAPoL-Start message.

Once the Enrollee sends an M3 message, both the Registrar and the Enrollee shall proceed in lock-step fashion until either a failure or until success occurs (indicated by the Done response message). If the Enrollee (802.1X supplicant) detects any errors in these later phases, it responds by sending a NACK message and transitioning to state G to terminate the connection. At this point, it is required for the Enrollee to compute a fresh device password for use in the next instance of the Registration Protocol. If the same password is reused with multiple instances of the protocol, it will be susceptible to active attack.

7.7.4 EAP State Machine for Adding an External Registrar

The Figure 12 below illustrates an EAP state machine on the AP (802.1X authenticator) for adding external Registrars. The corresponding Registrar state machine is not specified in this document, but it should be constructed so that it operates in accordance with the AP's state machine and the Registration Protocol.

Dotted line transitions represent messages sent by the authenticator on the AP. Solid line transitions represent messages sent by the supplicant on the Registrar. Comma-separated lists indicate that the message may be one of those in the list. The lock-step sequence of the Registration Protocol shall be preserved in this machine. Once M4 is sent by the Registrar, for example, if anything but M5 is sent by the AP, the Registrar will respond with a NACK message and enter state F. Likewise, if the Registrar encounters an authentication error in processing a message, it shall respond with a WSC_NACK.

Similarly, if the AP detects an authentication error in processing a message sent by the Registrar, it shall respond with a WSC_NACK, after which the Registrar (802.1X supplicant) sends WSC_NACK and AP replies with EAP-Failure. Upon successful processing of M8, the AP sends a WSC_Done message, and the Registrar responds with WSC_ACK to enter state G. The AP then sends EAP-Failure to end the protocol session.

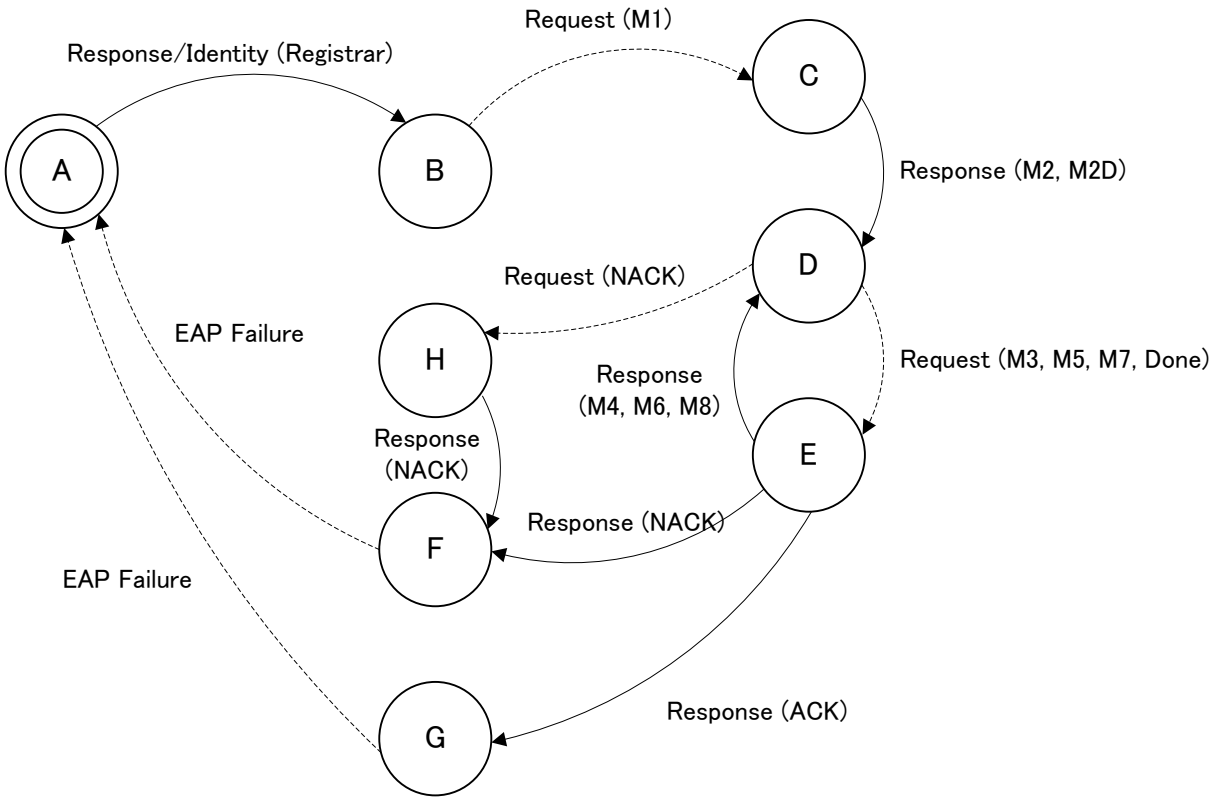

Figure 12 – EAP State Machine for Adding a Registrar

In this use case, the first message sent by the AP's 802.1X authenticator contains M1. If the Registrar has already been configured with the AP's device password, it responds with M2. Otherwise, it responds with M2D. If the AP receives M2D from the Registrar, it sends WSC_NACK. The Registrar (802.1X supplicant) then sends WSC_NACK and the AP replies with EAP-Failure and both of the devices enter state A. At this point, the Registrar can prompt the user to enter the AP device password and then restart the Registration Protocol or use an out-of-band channel.

7.8 UPnP Transport of Registration Protocol

If the Enrollee and Registrar are connected using an Ethernet connection, the Registration Protocol may be transported over UPnP. UPnP is also used to transport Registration Protocol messages between an Access Point and its external Registrars. Details pertaining to the encapsulation of Registration Protocol messages in UPnP can be found in the WFAWLANConfiguration Service documents.

7.9 Version Negotiation

Wi-Fi Simple Configuration protocol messages include information about the version of the protocol supported by the transmitter of the message. This allows the protocol to be extended in the future without breaking backwards compatibility with deployed devices that use an older version of the protocol.

Version 1.0h of the specification did not describe exact rules for processing received messages with the Version attribute that indicates a version that differs from the local implementation. To avoid potential interoperability issues with deployed implementations with unknown behavior with any other value than 0x10 (1.0), the Version attribute is now deprecated and shall be included with the fixed value 0x10 in the messages. A new subelement, Version2, is used to indicate the version of the protocol based on the following rules. Implementations based on version 2.0 or newer are required to include the new Version2 subelement in messages. If this subelement is not included, the message is assumed to be from an implementation that is based on the 1.0h version of the protocol.

Received messages should not be rejected based on a version number mismatch. The transmitter of protocol messages is responsible for generating messages in the format supported by the receiver. The receiver can thus process the message based on the rules described in the specification it was implemented with regardless of which version the transmitter indicated. Where backwards compatibility requires different message contents, the newer specification version defines rules for generating the message based on the version number of the other end. New protocol versions can modify the contents of the messages that follow version negotiation (M2..M8, WSC_ACK, WSC_NACK, WSC_Done) freely when the other end is determined to support the protocol version that introduces the changes. The messages that can be transmitted before version negotiation (Beacon, Probe Request, (Re)Association Request, UPnP messages that initiate the connection) can only be extended by adding new attributes that implementations based on older specification will ignore as optional attributes.

8 Message Encoding

The protocols presented in section 7 can be mapped onto a variety of underlying networks or transports. Because most messages include cryptographic hashes of prior messages, it is very important to establish an invariant binary representation for each message. Registration Protocol messages can be encapsulated and transported inside other messages such as EAP or UPnP. In each encapsulation, the binary BLOB that constitutes the message is well defined. For example, in EAP each Registration Protocol message is placed in the message data portion of the EAP packet described in Section 7.7.1. In UPnP, these same binary messages are base 64 encoded and passed as parameters to SOAP actions.

The ordering of the attributes in messages described in this section SHALL match the order given in the tables the subsequent subsections contain. Attributes that are listed as required (R) shall be included. Attributes that are listed in each table as optional (O) shall be recognized and handled if they are provided. Attributes that are marked as conditional (C) shall be included when the associated condition indicated for the attribute is TRUE. The attribute designation <other…> in a table indicates that any non-required attributes, including vendor extensions may be used. A device that receives a non-required attribute that it does not recognize shall ignore it.

Attributes with data fields defined as an ASCII or UTF-8 string, and which are not directly involved in security calculations or negotiation, may have a zero length data field, but this is not recommended. Devices shall be able to receive such attributes.

8.1 Wi-Fi Simple Configuration TLV Data Format

Wi-Fi Simple Configuration encodes information as attributes in a binary type identifier, length and value (TLV) format. The TLV format uses fields as defined in TLV Format Table. TLVs are transmitted and/or saved in big endian byte order.

Table 2 – Type, Length, Value (TLV) format for Wi-Fi Simple Configuration binary data

Byte Offset	Field Length	Field Name	Description
0	2 Bytes	AttributeType	Type identifier for the attribute
2	2 Bytes	DataLength	Length in bytes of the attribute's data field
4	0-0xFFFF Bytes	Data	Attribute Data

Most Wi-Fi Simple Configuration attributes are simple data structures, but some are nested data structures that contain other TLV attributes. For example, the Encrypted Data attribute contains sub-attributes Key ID and Cyphertext. The cleartext (unencrypted) form of the Cyphertext Data field is itself a set of Wi-Fi Simple Configuration attributes encoded in TLV format. The Credential attribute is another example of a compound attribute.

8.2 802.11 Management Frames

Initial discovery of Wi-Fi Simple Configuration devices is accomplished using 802.11 Information Elements in management frames (Beacon, Probe Request, and Probe Response). If the Enrollee decides to pursue a connection to the network, it initiates an 802.1X/EAP connection for the EAP-based Registration Protocol. The information exchanged in beacons and probe messages is not secure and should be considered only as hints.

Wi-Fi Simple Configuration Information Element

The Wi-Fi Simple Configuration Information Element complies with the IEEE 802.11 Information Element format and indicates specific data necessary for network information, capabilities and modes, to configure an Enrollee for the wireless network and to report problems with the Enrollee associating with a specified wireless network with the supplied settings.

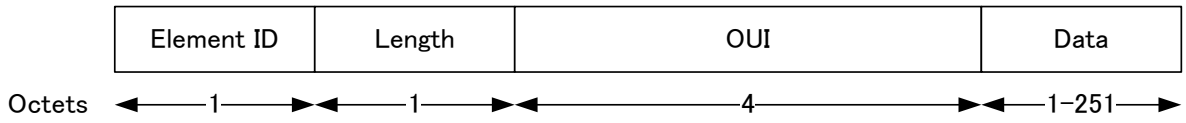

Figure 13 – Wi-Fi Simple Configuration Information Element

There may be more than one instance of the Wi-Fi Simple Configuration Information Element in a single 802.11 management frame. If multiple Information Elements are present, the Wi-Fi Simple Configuration data consists of the concatenation of the Data components of those Information Elements (the order of these elements in the original packet shall be preserved when concatenating Data components).

Access Points shall provide the Wi-Fi Simple Configuration IE in all Beacon and Probe Response frames to indicate support for WSC. Stations shall provide the Wi-Fi Simple Configuration IE in all Probe Request frames to indicate support for WSC.

A station that intends to use the EAP-WSC method with a WSC enabled AP shall include a WSC IE in its 802.11 (re)association request in addition to other information elements as specified by the IEEE 802.11 Standard. Note that during the WSC association the Privacy subfield of the Capability information field, the RSN IE and the WPA IE are irrelevant and shall be ignored by both the station and AP. However, both the station and AP shall continue to comply with any other protocol (for instance WMM). Therefore if a WSC IE is present in the (re)association request, the AP shall engage in EAP-WSC with the station and shall not attempt any other security handshake.

On successful association, the station will then send an EAPOL-Start to the AP and wait for EAP-Request/Identity. The AP is allowed to send EAP-Request/Identity to the station before EAPOL-Start is received if a WSC IE is included in the (re)association request and the WSC IE is version 2.0 or higher. When the station receives an EAP-

Request/Identity, it will respond with EAP-Response/Identity to indicate if it intends to be an Enrollee or a Registrar.

Note: For backwards compatibility with version 1.0 implementations an AP hosting a WPA2-Personal network and supporting WSC would need to permit the association exchange with a station intending to engage in EAP-WSC where there is no RSN IE or WPA IE in the association request frames even if there is no WSC IE either. The AP shall only permit the exchange of EAP-WSC messages with a station that associates in this manner and only after receiving the EAPOL-Start frame. The WSC IE may or may not be present in the association requests from WSC version 1.0 devices.

In the Wi-Fi Simple Configuration Information Element, the Element ID has a value of 221 and OUI is hex 00 50 F2 04.

Data placed in Wi-Fi Simple Configuration Information Elements should be constrained by the sender to avoid exceeding the space available in an 802.11 frame.

8.2.1 Beacon Frame (C)

The Wi-Fi Simple Configuration Information Element shall be included in a beacon frame, and contain attributes presented and described in the table in this section. If AP has locked its PIN such as due to too many authentication failures, AP Setup Locked shall be included.

Table 3 – Attributes in WSC IE in the Beacon Frame

Attribute	R/O/C	Allowed Values
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Wi-Fi Simple Configuration State	R	0x01 (Not Configured), 0x02 (Configured).
AP Setup Locked	C	Shall be included if value is TRUE.
Selected Registrar	C	Indicates if the user has recently activated a Registrar to add an Enrollee. If Selected Registrar is TRUE, then the Selected Registrar attribute SHALL be included.
Device Password ID	C	Device Password ID indicates the method or identifies the specific password that the selected Registrar intends to use. If any of the active registrars are in PBC mode this value shall be 0x0004 (Pushbutton). Note that WSC 1.0 devices may use other values. If Selected Registrar is TRUE, then the Device Password ID attribute SHALL be included.
Selected Registrar Configuration Methods	C	This attribute contains the Configuration methods active on all of the selected Registrars. This attribute shall be the union of the Selected Registrar Configuration Methods from all active registrars (internal and external). If Selected Registrar is TRUE, then the Selected Registrar Configuration Methods attribute SHALL be included.

Attribute	R/O/C	Allowed Values
UUID-E	C	The AP's UUID shall be provided when the AP is a dual-band AP in Pushbutton mode and indicating Pushbutton mode on both radios.
RF Bands	C	Indicates all RF bands available on the AP. A dual-band AP shall provide this attribute.
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
AuthorizedMACs (inside WFA Vendor Extension)	C	List of enrollee MAC addresses that have been registered to start WSC. The AP includes this field in beacons so enrollees can tell if they have been registered to start WSC. There may be multiple enrollees active on the network, but not all of them have been registered to start WSC. This element allows an enrollee to detect if they should start WSC or not. The AP shall include this attribute if any of the Registrars provides a list of authorized MAC addresses.
Registrar Configuration Methods (inside WFA Vendor Extension)	C	The Configuration Methods supported by the internal Registrar of the AP. If the AP is an NFC Device then the Registrar Configuration Methods subelement SHALL be included, otherwise it MAY be included.
<other…>	O	Multiple attributes are permitted.

8.2.2 Association Request and Reassociation Request

If the station intends to use Wi-Fi Simple Configuration, the Wi-Fi Simple Configuration Information Element shall be included in an association request or reassociation request to indicate the use of the WSC protocol. Note: WSC 1.0 stations may not include WSC IE in these frames.

The IE contains the following attributes:

Table 4 – Attributes in WSC IE in the Association/Reassociation Request frame

Attribute	R/O/C	Allowed Values
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Request Type	R	
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
<other…>	O	Multiple attributes are permitted.

8.2.3 Association Response and Reassociation Response

If the station indicated the use of WSC, the WSC Information Element shall be included in an association response or reassociation response, and contain the following device attributes:

Table 5 – Attributes in WSC IE in the Association/Reassociation Response frame

Attribute	R/O/C	Allowed Values
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Response Type	R	
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
<other…>	O	Multiple attributes are permitted.

8.2.4 Probe Request (D-E or D-R)

If the station intends to use Wi-Fi Simple Configuration protocol, the Wi-Fi Simple Configuration Information Element shall be included in a probe request, and contain the following device attributes (Enrollee or Registrar):

Table 6 – Attributes in WSC IE in the Probe Request frame

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Request Type	R	
Configuration Methods	R	
UUID-(E or R)	R	
Primary Device Type	R	
RF Bands	R	Specific RF band used for this message.
Association State	R	
Configuration Error	R	
Device Password ID	R	If the device is in PBC mode this value shall be 0x0004 (Pushbutton).
Manufacturer	C	Shall be included in protocol version 2.0 and higher.
Model Name	C	Shall be included in protocol version 2.0 and higher.
Model Number	C	Shall be included in protocol version 2.0 and higher.
Device Name	C	User-friendly description of device. Shall be included in protocol version 2.0 and higher.

Attribute	R/O/C	Notes
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
Request to Enroll (inside WFA Vendor Extension)	O	Indicates the desire to enroll in the network. If the Registrar gets this attribute it can use this as a trigger that a device wants to enroll.
Requested Device Type	O	When a device receives a Probe Request containing a WSC IE with the Requested Device Type attribute it will only respond with a Probe Response if the devices Primary Device Type or Secondary Device Type matches the Requested Device Type contained in the Probe Request.
<other…>	O	Multiple attributes are permitted.

8.2.5 Probe Response (D-AP/Registrar)

The Wi-Fi Simple Configuration Information Element shall be included in a probe response, and contain the following attributes corresponding to the AP. If AP has locked its PIN, such as due to too many authentication failures, AP Setup Locked shall be included.

Table 7 – Attributes in WSC IE in the Probe Response frame

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Wi-Fi Simple Configuration State	R	0x01 (Not Configured), 0x02 (Configured).
AP Setup Locked	C	Shall be included if value is TRUE
Selected Registrar	C	Indicates if the user has recently activated a Registrar to add an Enrollee. If Selected Registrar is TRUE, then the Selected Registrar shall be included.
Device Password ID	C	Device Password ID indicates the method or identifies the specific password that the selected Registrar intends to use. If any of the active registrars are in PBC mode this value shall be 0x0004 (Pushbutton). Note that WSC 1.0 devices may use other values. If Selected Registrar is TRUE, then the Device Password ID shall be included.
Selected Registrar Configuration Methods	C	This attribute contains the Configuration methods active on all of the selected Registrars. This attribute shall be the union of the Selected Registrar Configuration Methods from all active registrars (internal and external). If Selected Registrar is TRUE, then the Selected Registrar Configuration Methods shall be included.
Response Type	R	

Attribute	R/O/C	Notes
UUID-E	R	Unique identifier of the AP.
Manufacturer	R	
Model Name	R	
Model Number	R	
Serial Number	R	
Primary Device Type	R	
Device Name	R	User-friendly description of device.
Configuration Methods	R	Configuration Methods corresponds to the methods the AP supports as an Enrollee for adding external Registrars.
RF Bands	C	Indicates all RF bands available on the AP. A dual-band AP shall provide this attribute.
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
AuthorizedMACs (inside WFA Vendor Extension)	C	List of enrollee MAC addresses that have been registered to start WSC. The AP includes this field in probe. responses so enrollees can tell if they have been registered to start WSC. There may be multiple enrollees active on the network, but not all of them have been registered to start WSC. This element allows an enrollee to detect if they should start WSC or not. The AP shall include this attribute if any of the Registrars provides a list of authorized MAC addresses.
Registrar Configuration Methods (inside WFA Vendor Extension)	C	The Configuration Methods supported by the internal Registrar of the AP. If the AP is an NFC Device then the Registrar Configuration Methods subelement SHALL be included, otherwise it MAY be included.
<other…>	O	Multiple attributes are permitted.

8.3 Registration Protocol Message Definitions

This section lists attributes that appear in Registration Protocol messages and in AP Management interface parameters.

8.3.1 Message M1

Table 8 – Attributes in the Message M1

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Message Type	R	Value is 0x04 for M1.
UUID-E	R	
MAC Address	R	Enrollee's MAC address.
Enrollee Nonce	R	
Public Key	R	Diffie-Hellman key of Enrollee. Key size and Group are implied by the attribute data size.
Authentication Type Flags	R	Bit field of authentication types supported by the Enrollee.
Encryption Type Flags	R	Bit field of encryption types supported by the Enrollee.
Connection Type Flags	R	
Configuration Methods	R	
Wi-Fi Simple Configuration State	R	For a STA Enrollee set always to 0x01 'Not Configured'. For an AP Enrollee see Section 12.
Manufacturer	R	
Model Name	R	
Model Number	R	
Serial Number	R	
Primary Device Type	R	
Device Name	R	
RF Bands	R	Specific RF band used for this message.
Association State	R	
Device Password ID	R	
Configuration Error	R	
OS Version	R	
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
Request to Enroll (inside WFA Vendor Extension)	O	Indicates the desire to enroll in the network. If the Registrar gets this attribute it can use this as a trigger that a device wants to enroll.
<other…>	O	Multiple attributes are permitted.

8.3.2 Message M2

Table 9 – Attributes in the Message M2

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Message Type	R	Value is 0x05 for M2.
Enrollee Nonce	R	
Registrar Nonce	R	
UUID-R	R	
Public Key	R	Diffie-Hellman key of Registrar. Key size and Group are implied by the attribute data size.
Authentication Type Flags	R	Bit field of authentication types supported by the Registrar.
Encryption Type Flags	R	Bit field of encryption types supported by the Registrar.
Connection Type Flags	R	
Configuration Methods	R	
Manufacturer	R	
Model Name	R	
Model Number	R	
Serial Number	R	
Primary Device Type	R	
Device Name	R	
RF Bands	R	Specific RF band used for this message.
Association State	R	
Configuration Error	R	
Device Password ID	R	The Device Password ID indicated by the Registrar may be different than the ID sent by the Enrollee in M1.
OS Version	R	
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
<other…>	O	Multiple attributes are permitted.
Authenticator	R	

8.3.3 Message M2D

Message M2D is a discovery-only variant of M2. Its purpose is to enable Registrars to advertise their existence to Enrollees without requiring either side to perform expensive cryptographic operations.

Table 10 – Attributes in the Message M2D

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Message Type	R	Value is 0x06 for M2D.
Enrollee Nonce	R	
Registrar Nonce	R	
UUID-R	R	
Authentication Type Flags	R	Bit field of authentication types supported by the Registrar.
Encryption Type Flags	R	Bit field of encryption types supported by the Registrar.
Connection Type Flags	R	
Configuration Methods	R	
Manufacturer	R	
Model Name	R	
Model Number	R	
Serial Number	R	
Primary Device Type	R	
Device Name	R	
RF Bands	R	Specific RF band used for this message.
Association State	R	
Configuration Error	R	
OS Version	R	
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
<other…>	O	Multiple attributes are permitted.

8.3.4 Message M3

Table 11 – Attributes in the Message M3

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Message Type	R	Value is 0x07 for M3.
Registrar Nonce	R	
E-Hash1	R	Hash of first half of device password, DH secret, and secret nonce 1.
E-Hash2	R	Hash of second half of device password, DH secret, and secret nonce 2.
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
<other…>	O	Multiple attributes are permitted.
Authenticator	R	

8.3.5 Message M4

Table 12 – Attributes in the Message M4

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Message Type	R	Value is 0x08 for M4.
Enrollee Nonce	R	
R-Hash1	R	Hash of first half of device password, DH secret, and secret nonce 1.
R-Hash2	R	Hash of second half of device password, DH secret, and secret nonce 2.
Encrypted Settings	R	Encrypted Secret Nonce attribute containing Registrar's secret nonce 1.
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
<other…>	O	Multiple attributes are permitted.
Authenticator	R	

Table 13 – Attributes in Encrypted Settings Data in the M4

Attribute	R/O	Notes
R-SNonce1	R	
<other…>	O	Multiple attributes are permitted.
Key Wrap Authenticator	R	

Encrypted Settings Data in M5 and M6 also follow this pattern.

8.3.6 Message M5

Table 14 – Attributes in the Message M5

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Message Type	R	Value is 0x09 for M5.
Registrar Nonce	R	
Encrypted Settings	R	Encrypted Secret Nonce attribute containing Enrollee's secret nonce 1.
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
<other…>	O	Multiple attributes are permitted.
Authenticator	R	

8.3.7 Message M6

Table 15 – Attributes in the Message M6

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Message Type	R	Value is 0x0a for M6.
Enrollee Nonce	R	
Encrypted Settings	R	Encrypted Secret Nonce attribute containing Registrar's secret nonce 2.
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
<other…>	O	Multiple attributes are permitted.
Authenticator	R	

8.3.8 Message M7

Table 16 – Attributes in the Message M7

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Message Type	R	Value is 0x0b for M7.
Registrar Nonce	R	
Encrypted Settings	R	Encrypted Secret Nonce attribute containing Enrollee's secret nonce 2 and current wireless settings if Enrollee is an AP.
Setting Delay Time (inside WFA Vendor Extension)	O	An estimate of the time in seconds required by the Device to apply the changes.
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
<other…>	O	Multiple attributes are permitted.
Authenticator	R	

If the Enrollee is a WLAN station, the following attributes are encrypted in the Encrypted Settings.

Table 17 – Enrollee Settings Attributes in Encrypted Settings of M7

Attribute	R/O	Notes
E-Snonce2	R	
Identity Proof	O	
<other…>	O	Multiple attributes are permitted.
Key Wrap Authenticator	R	

If the Enrollee is an AP setting up an external Registrar, the attributes included in Encrypted Settings are specified in the following table.

Table 18 – AP Settings Attributes in Encrypted Settings of M7

Attribute	R/O	Notes
E-SNonce2	R	
SSID	R	
MAC Address	R	AP's BSSID
Authentication Type	R	The configured authentication type.
Encryption Type	R	The configured encryption type.
Network Key Index	O	Deprecated. Only included by WSC 1.0 devices. Ignored by WSC 2.0 or newer devices.
Network Key	R	Just one instance is allowed.
<other…>	O	Multiple attributes are permitted.
Key Wrap Authenticator	R	

8.3.9 Message M8

Table 19 – Attributes in the Message M8

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Message Type	R	Value is 0x0c for M8.
Enrollee Nonce	R	
Encrypted Settings	R	Encrypted wireless settings for Enrollee. This attribute may also include a digital Certificate.
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
<other…>	O	Multiple attributes are permitted.
Authenticator	R	

Table 20 – Attributes in Encrypted Settings of M2, M8 if Enrollee is AP

Attribute	R/O	Notes
SSID	R	
Authentication Type	R	The authentication type to be used by the AP.
Encryption Type	R	The encryption type to be used by the AP.
Network Key Index	O	Deprecated. Only included by WSC 1.0 devices. Ignored by WSC 2.0 or newer devices.
Network Key	R	
MAC Address	R	AP's MAC Address (BSSID).
New Password	O	
Device Password ID	O	Required if New Password is included.
<other…>	O	Multiple attributes are permitted.
Key Wrap Authenticator	R	

Table 21 – Attributes in Encrypted Settings of M2, M8 if Enrollee is STA

Attribute	R/O	Notes
Credential	R	May include multiple instances of Credential
New Password	O	
Device Password ID	O	Required if New Password is included.
IP Address Configuration Method	R	Specified mechanism selected by Registrar
Registrar IPv4 Address	O	Must be included when Registrar supports WSC_IP
IPv4 Subnet Mask	O	Must be included when Registrar supports WSC_IP
Enrollee IPv4 Address	O	Must be included when WSC_IP is selected
Available IPv4 Submask List	O	A list of address submasks that may be used by the Enrollee.
<other…>	O	Multiple attributes are permitted.
Key Wrap Authenticator	R	

8.3.10 WSC_ACK Message

The following table lists the attributes that are included in the WSC_ACK message data.

Table 22 – Attributes in the WSC_ACK Message

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Message Type	R	Value is 0xD for WSC_ACK Message.
Enrollee Nonce	R	
Registrar Nonce	R	
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
<other…>	O	Multiple attributes are permitted.

8.3.11 WSC_NACK Message

The following table lists the attributes that are included in the WSC_NACK message data.

Table 23 – Attributes in the WSC_NACK Message

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Message Type	R	Value is 0xE for WSC_NACK Message.
Enrollee Nonce	R	
Registrar Nonce	R	
Configuration Error	R	
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
<other…>	O	Multiple attributes are permitted.

8.3.12 WSC_Done Message

The following table lists the attributes that are included in the WSC_Done message data.

Table 24 – Attributes in the WSC_Done Message

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Message Type	R	Value is 0xF for WSC_Done Message.
Enrollee Nonce	R	
Registrar Nonce	R	
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
<other…>	O	Multiple attributes are permitted.

8.4 AP Settings Message Definitions

This section describes messages that are carried within UPnP actions as described in the WFAWLANConfiguration Service. The messages are not protected in any way at the SOAP level.

8.4.1 SetSelectedRegistrar Message

The following table lists the attributes that can be set using the UPnP action SetSelectedRegistrar(). This action is unauthenticated, and it can be called by any UPnP control point on the network capable of operating as a Registrar, even if it does not have keys for the AP Management Interface. External Registrars shall notify the AP when they become active by setting the Selected Registrar attribute to TRUE using this UPnP action.

After an AP receives a SetSelectedRegistrar UPnP action with Selected Registrar TRUE, it shall include the Selected Registrar set to TRUE in its Beacon and Probe Response messages. The AP shall also add the MAC addresses from the received AuthorizedMACs subelement in an AuthorizedMACs subelement in Beacon and Probe Response frames. The addresses listed in Beacon and Probe Response frames are a combination of authorized Enrollee MAC addresses received from all Registrars. If there is not enough room for all the authorized Enrollee MACs, only the most recently added ones are listed.

The Selected Registrar, Selected Registrar Configuration Methods, and AuthorizedMACs subelement in Beacon and Probe Response frames are a union of information received from all Registrars. The AP is responsible for updating these attributes when the Registrar notifies the AP that changes associated with the SetSelectedRegistrar UPnP action have occurred or it becomes disconnected. An

internal Registrar can become inactive when the user cancels out or navigates away from the internal Registrar UI used for enrolling a device.

Table 25 – Attributes in the SetSelectedRegistrar Message

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Selected Registrar	R	If FALSE, the rest of the parameters are ignored, and the AP immediately revokes data associated with the prior SetSelectedRegistrar call as if the Walk Time interval had expired.
Device Password ID	R	Device Password ID indicates the method or identifies the specific password that the selected Registrar intends to use. If any of the active registrars are in PBC mode this value shall be 0x0004 (Pushbutton).
Selected Registrar Configuration Methods	R	This attribute contains the Configuration methods active by the selected Registrar.
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
AuthorizedMACs (inside WFA Vendor Extension)	C	List of enrollee MAC addresses for which the Registrar has suitable information (e.g., PIN) to complete registration protocol. Shall be included in protocol version 2.0 and higher.
UUID-R	C	Registrars based on version 2.0 or higher are required to include their Registrar UUID in SetSelectedRegistrar to provide the AP a unique identifier for the source of this action if the AP is using version 2.0 or higher.
<other…>	O	Multiple attributes are permitted.

9 Security Configuration Requirements

Version 2.0 of the WSC specification deprecates the use of WEP and WPA (TKIP) with the WSC protocol. An AP with WSC enabled may only advertise support for WPA-Personal if also WPA2-Personal (AES-CCMP) is enabled (Mixed Mode).

By default, an AP shall get configured for WPA2-Personal by a Registrar (either its Internal Registrar or an External Registrar). The AP may be configured for Mixed Mode.

If the AP is in the Configured state (Wi-Fi Simple Configuration State set to 0x02), the AP shall either have no security enabled or shall have WPA2 enabled (with Mixed Mode as an optional alternative). Support for WSC will be disabled if the AP is configured for WEP or WPA-only security (WPA2 is not enabled). In this case, if possible, an appropriate message should be shown to the user. If the AP is capable of hosting multiple networks (multiple-SSID/BSSID capable), WSC shall be disabled on the network (SSID/BSSID) that has WEP or WPA-only enabled.

Registrars shall not provision Enrollees with WEP or WPA credentials. Registrars supporting WSC version 1.0 only, might configure an AP for WPA-Personal. In this scenario, the AP shall enable Mixed Mode instead. If a Registrar that only supports WSC version 1.0 tries to configure an AP for WEP then that process shall fail gracefully and if possible an appropriate message should be shown to the user.

A STA that has been provisioned using the WSC protocol shall use WPA2 to connect to an AP with Mixed Mode enabled. If a STA gets provisioned with WPA-Personal credentials (by a Registrar that only supports WSC version 1.0), the STA will have to look at the AP's beacon (as the AP might have gone through initial configuration); if the AP advertises WPA2-Personal the STA shall use WPA2-Personal to connect otherwise if the AP advertises WPA-Personal the STA shall use the received WPA-Personal credentials. If a STA gets provisioned with WEP credentials (by a Registrar that only supports WSC version 1.0) that process shall fail and if possible an appropriate message should be shown to the user.

If a STA gets provisioned with multiple credentials (either by a Registrar that supports WSC version 2.0 or a Registrar that supports WSC version 1.0 only), it shall apply the rules as outlined above for each credential separately and only ignore the credentials for WEP. If no valid credentials are found, the WSC protocol run shall fail.

10 NFC Out-of-Band Interface Specification

This section details the specifications for using NFC as an out-of-band channel for Wi-Fi Simple Configuration.

10.1 NFC Usage Models

The NFC out-of-band interface provides three different usage models for WLAN configuration provisioning with Wi-Fi Simple Configuration.

Password Token

An NFC Tag provided with the Enrollee device is used to physically transmit a device password from the Enrollee to an NFC-enabled Registrar. The device password will then be used with the in-band registration protocol to provision the Enrollee with WLAN configuration data. The device password is considerably longer than the user would be expected to type (e.g. a 32 byte random value instead of 8 digits).
An NFC Password Token may be integrated into the device if the device is portable and the manufacturer assumes no practical difficulty for the user to physically move the device close to the Registrar NFC Device. Integration of an NFC Password Token into a device can be realized either physically (into the device housing) or virtually (emulated by an integrated NFC Device).

Configuration Token

An NFC Tag is used to physically transmit WLAN configuration from an NFC-enabled Registrar to the NFC-enabled Enrollee. The user first touches the NFC Interface of the Registrar with the NFC Tag to retrieve WLAN configuration data, then touches the NFC Interface of the Enrollee to provision the Enrollee. If the same WLAN configuration is used for all Enrollees, the NFC Tag may be re-used for provisioning further Enrollees without touching the Registrar's NFC Interface.

Connection Handover
An Enrollee NFC Device may directly exchange public key hashes with a Registrar NFC Device if both are brought into close proximity, i.e. literally touched, to establish near field communication. This usage model requires at least one of the devices to be portable. The public key hashes allow each of the devices involved in the Registration Protocol to verify that they are communicating with the same device that was involved in the near field communication.

10.1.1 Password Token

An NFC Password Token shall contain an NDEF record with the payload shown in table 26, where the attributes are encoded TLV elements as defined in section 8.1 and 12. The NDEF record type name shall be the MIME media type "application/vnd.wfa.wsc" and the record shall be formatted as a standalone NDEF message on the NFC Tag.

Table 26 – NDEF Record Payload of the NFC Password Token

Attribute	R/O/C	Notes
Out-of-Band Device Password	R	As defined in section 12
Version2 (inside WFA Vendor Extension)	C	As defined in section 12
<other…>	O	Multiple attributes are permitted

The Registrar detects the availability of an NFC Out-of-Band Device Password Token from the content of the Configuration Methods parameter provided in M1 or in the Probe-Response (from AP) or Probe-Request (from Enrollee). This allows the Registrar to prompt or otherwise guide the user to provide the Password Token. If an Enrollee indicates support of an external or integrated NFC Token, this shall be an NFC Password Token containing an Out-of-Band Device Password.

10.1.2 Configuration Token

An NFC Configuration Token shall contain an NDEF record with the payload shown in table 27, where the attributes are encoded TLV elements as defined in section 8.1 and 12. The NDEF record type name shall be the MIME media type "application/vnd.wfa.wsc" and the record shall be formatted as a standalone NDEF message on the NFC Tag.

Table 27 – NDEF Record Payload of the NFC Configuration Token

Attribute	R/O/C	Notes
Credential	R	As defined in section 12
RF Bands	O	As defined in section 12
AP Channel	O	As defined in section 12
MAC Address	O	As defined in section 12
Version2 (inside WFA Vendor Extension)	C	As defined in section 12
<other…>	O	Multiple attributes are permitted

The Credential attribute shall contain unencrypted WLAN configuration data.

Optionally the RF Bands attribute, the AP Channel attribute and the MAC Address attribute may be included as hints to help the Station/Enrollee to find the AP without a full scan. The RF Bands attribute is used to indicate the operating RF band of the AP, the AP Channel attribute also includes the operating channel of the AP and the MAC Address attribute describes the BSSID of the AP. It is recommended to include those attributes if known. If the RF Bands attribute and AP Channel attribute are both included then the RF Bands attribute indicates the band that the channel specified by the AP Channel attribute is in. If the RF Bands attribute is included without the AP Channel

attribute then it indicates the RF Bands in which the AP is operating with the SSID specified in the SSID in Credential attribute.

To facilitate user guidance by the Enrollee when an NFC Configuration Token is available, the Registrar shall set the External NFC Token bit in its Configuration Methods attribute. This attribute may be conveyed via M2/M2D or in beacons or probe responses in the Selected Registrar Configuration Methods attribute.

Vendors may provide an empty NFC Configuration Token, to be filled at any point in time by a Registrar that is an NFC Device when it is triggered to write the current network configuration data onto the NFC Tag. Subsequently, this NFC Tag can be used to configure Enrollees without any further Registrar involvement. Vendors may also provide a pre-configured NFC Configuration Token containing a (random) configuration to setup a new network, allowing immediate usage of the NFC Tag to configure Enrollees. For static and reusable NFC Configuration Tokens, the wild-card MAC Address (FF:FF:FF:FF:FF:FF) shall be used in the Credential Attributes (see Table 36).

10.1.3 Connection Handover

When two NFC Devices are brought into close proximity, they will establish NFC communication based on the NFC Forum Logical Link Control Protocol (LLCP) specification[7]. If one of the devices has intention to activate a further (wireless) communication method, it may then use the NFC Forum Connection Handover protocol to announce possible communication means (potentially including configuration data) and request the other device to respond with a selection of matching technologies, including necessary configuration data.

If an Enrollee NFC Device has established NFC LLCP communication with a Registrar NFC Device, the Enrollee shall send a handover request message indicating Wi-Fi communication capability by using “application/vnd.wfa.wsc” as the carrier type name.

Figure 14 shows a handover request message where the only available alternative carrier is Wi-Fi, but in practice there may be multiple choices depending on the device capabilities. Multiple Alternative Carrier Records should be listed in order of priority (see [8] for further details). Also the carrier power state may have one of the other values defined in the Connection Handover specification if the Wi-Fi radio is not yet active at the time of sending.

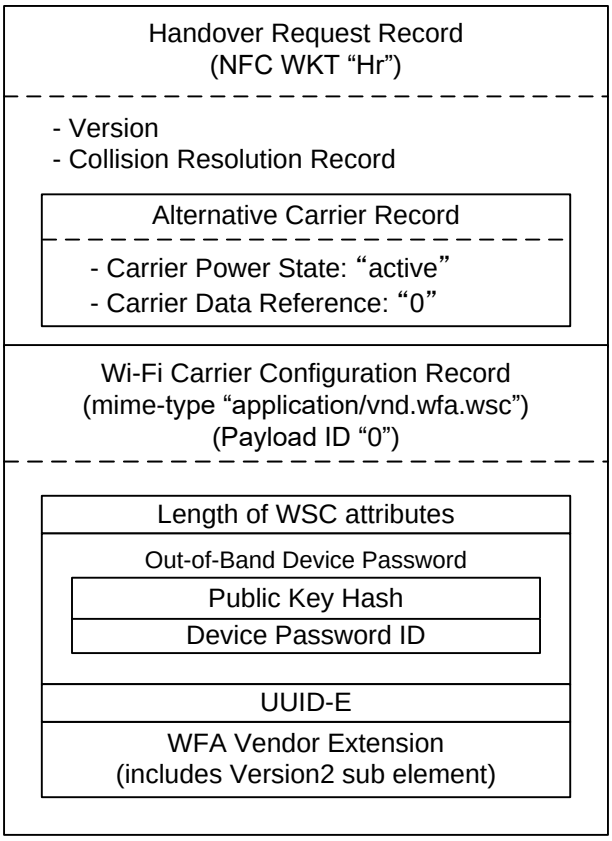

Figure 14 – Wi-Fi Handover Request Message

A Registrar NFC Device shall respond to a Handover Request Message with a Handover Select Message that provides WLAN configuration data according to table 27 within an NDEF record of MIME media type “application/vnd.wfa.wsc”.

Figure 15 shows a Handover Select Message where the only available alternative carrier is Wi-Fi, but in practice there may be multiple choices depending on the device capabilities and the options provided with the handover request. Multiple Alternative Carrier Records should be listed in order of priority (see [8] for further details). Also the carrier power state may have one of the other values defined in the Connection Handover specification if the Wi-Fi radio is not yet active at the time of sending.

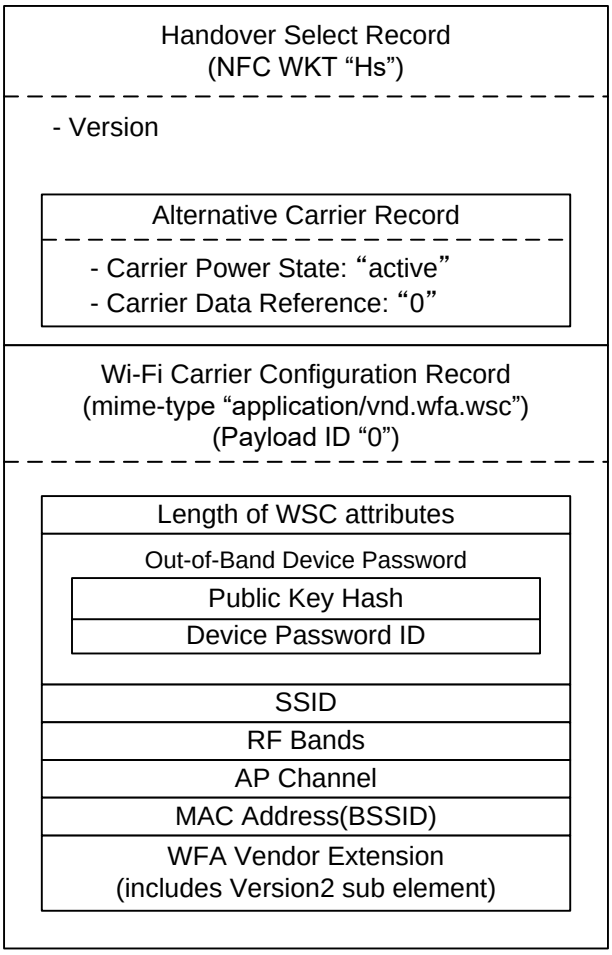

Figure 15 – Wi-Fi Handover Select Message

In both the handover request and select messages, at the head of the WSC attributes the Length of WSC attributes field shall be included. The size of the Length of WSC attributes field shall be 2 octets. The value held by the Length of WSC attributes field shall be the total length of the following WSC attributes in octets, using big-endian byte ordering.

The UUID-E attribute is included in the Handover Request Message and the SSID attribute is included in the Handover Select Message to assist with the discovery over 802.11 that follows the exchange of the connection handover messages. Optionally the RF Bands attribute, the AP Channel attribute and the MAC Address attribute may be included as hints to help the Station/Enrollee to find the AP without a full scan. The RF Bands attribute is used to indicate the operating RF band of the AP, the AP Channel attribute also includes the operating channel of the AP and the MAC Address attribute describes the BSSID of the AP. It is recommended to include those attributes if known. If the RF Bands attribute and AP Channel attribute are both included then the RF Bands attribute indicates the band that the channel specified by the AP Channel attribute is in. If the RF Bands attribute is included without the AP Channel attribute then it indicates the RF Bands in which the AP is operating with the SSID specified in the SSID attribute.

The Registrar shall detect the presence of an NFC Device on the Enrollee from the content of the Configuration Methods parameter provided in M1 or in the Probe Response (from AP) or Probe Request (from Enrollee) frames. With this information the Registrar can prompt or otherwise guide the user to touch the devices together. To avoid misleading instructions to the user to "touch devices" when this is not possible or practical, the Registrar should only choose the Connection Handover method if either the Registrar itself is portable or if the Enrollee includes the attribute Portable Device is TRUE in its probe request and/or M1 message.

Alternatively, the NFC data exchange may be implemented independent of the in-band device discovery. In this case, provisioning is also possible if the WLAN interface is unpowered. This enables very simple Registrars in terms of user interface and procedures (no rich user interface required, the user can directly proceed without waiting for Registrar guidance).

In both Handover Select and Handover Request Messages, and in the related M1 and M2 messages that follow the NFC Connection Handover, the Device Password ID shall be set to NFC-Connection-Handover. The Device Password shall have zero length when the Device Password ID is set to NFC Connection-Handover.

For Enrollee provided Public Key Hash Data fields in a Handover Message, the Public Key Hash Data field shall correspond to the first 160 bits of a SHA-256 hash of the Enrollee's public key. If the hash does not match that of the Enrollee's Public Key attribute in M1, then the Registrar shall send M2D with the Configuration Error value set to Public Key Hash Mismatch.

If the Enrollee Public Key test specified in the previous paragraph was successful and both a Handover Request and an Handover Select Message have been exchanged over NFC, then the Registrar shall include an encrypted ConfigData in M2 when sending M2 over Wi-Fi and skip M3-M8 of the WPS protocol.

For Registrar provided Public Key Hash Data fields in a Handover Message, the Public Key Hash Data field corresponds to the first 160 bits of a SHA-256 hash of the Registrar's public key. This hash shall match that of the Registrar's Public Key attribute in M2. If this value does not match, then the Enrollee sends WSC_NACK with the Configuration Error value set to Public Key Hash Mismatch.

10.2 Requirements for NFC Out-of-Band Support

10.2.1 Enrollee Requirements

A Wi-Fi Simple Configuration NFC-enabled Enrollee shall provide at least one of:

- an NFC Password Token in one of the mandatory NFC Forum tag formats; and/or
- an NFC Interface with the ability to:
    - read NFC Configuration Tokens of the mandatory NFC Forum tag formats; and

- exchange NFC Connection Handover messages in NFC peer mode with a Registrar NFC Device.

10.2.2 Registrar Requirements

A Wi-Fi Simple Configuration NFC-enabled Registrar shall be an NFC Device with the ability to:

- read NFC Password Tokens of the mandatory NFC Forum tag formats; and
- write NFC Configuration Tokens in the mandatory NFC Forum tag formats; and
- exchange NFC Connection Handover messages in NFC peer mode with an Enrollee NFC Device.

10.2.3 P2P Registrar Requirements

A Wi-Fi Peer to Peer Group Owner shall provide one of the following:

- An NFC Forum tag format containing an NDEF message with an NDEF record containing the Out-of-Band Device Password attribute using mechanisms defined in the P2P specification [18].
- An NFC Interface with the ability to:
  - read NFC Password Tokens of the mandatory NFC Forum tag formats; and
  - write NFC Configuration Tokens in the mandatory NFC Forum tag formats; and
  - exchange NFC Connection Handover messages in NFC peer mode with an Enrollee NFC Device

11 Pushbutton Configuration

11.1 Introduction

This section specifies an optional method called Pushbutton configuration that allows a Registrar with a very simple user interface (for example, a button and a LED) and no additional out-of-band channel to provide Credentials to PBC-capable Enrollee devices. PBC Enrollees may also have very simple user interfaces. PBC requires only a single button press on the Enrollee and on the Registrar, in arbitrary order.

PBC can be implemented in a variety of ways. On a limited-UI Registrar such as an AP, it could be implemented using only a button and a LED. On a richer UI device such as a DTV, it could be implemented using a button and messages on a user display. For a rich UI device such as a PC, it could be implemented using a virtual button and a rich series of displayed messages guiding the user. To simplify the discussion, this section uses the term *button* to describe the trigger element that initiates the PBC method on the Enrollee and Registrar.

Since the PBC method is unauthenticated, it is not permitted to use this method to manage AP settings, either through M8 or through the Management Interface. This implies that an AP SHALL NOT support using PBC to add an external Registrar or to derive keys for subsequent AP management.

11.2 User Experience

The PBC method requires the user to press a button on both the Enrollee and on the Registrar within a two-minute interval called the Walk Time. Figure 16 illustrates an example of the user actions and relative timings of PBC for the case where the Enrollee button is pressed first. The case where the Registrar button is pressed first is similar, and is shown in Figure 17. Section 11.3 contains a more detailed explanation of the protocol.

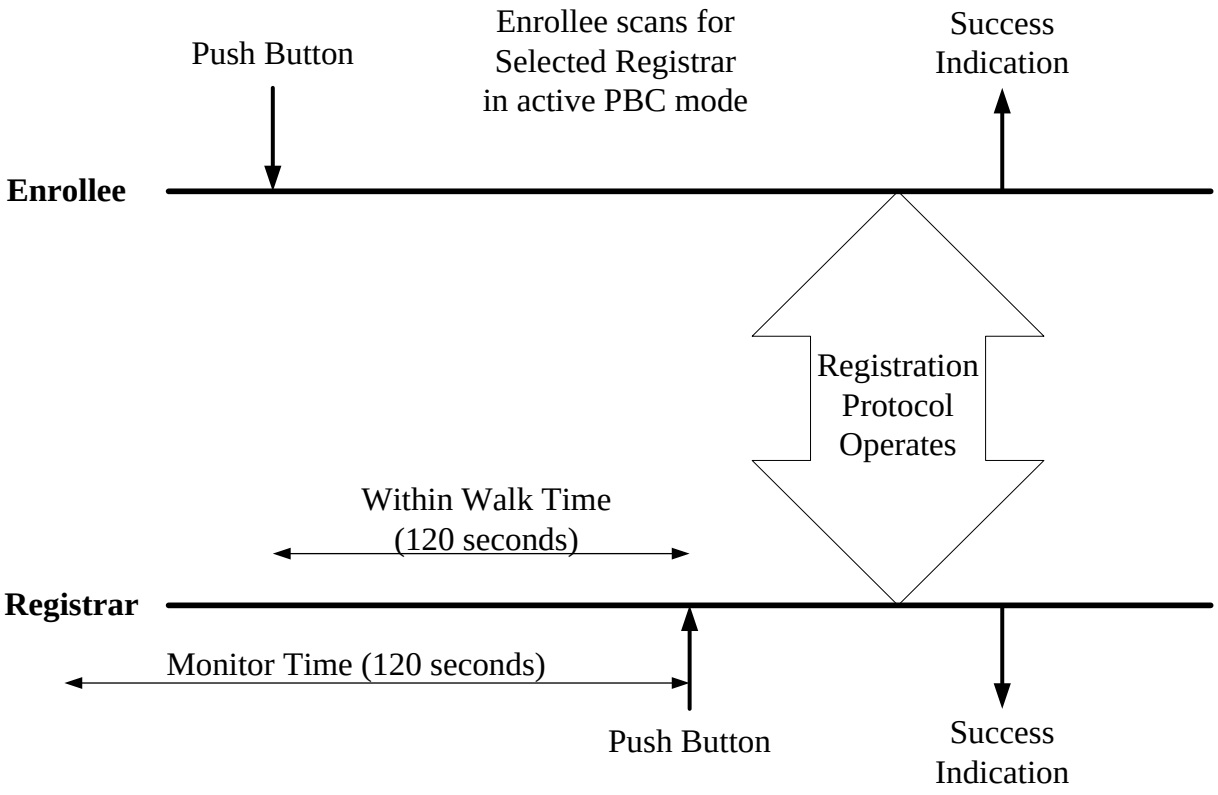

Figure 16 – PBC User Actions – Enrollee PB first

In this example, the user first pushes the button on the Enrollee and then goes to the Registrar to push the Registrar's button. The user shall complete the second button push within Walk Time**,** a maximum of 120 seconds, or the Enrollee times-out and indicates failure.

Similarly, if the user first pushes the Registrar button, the Enrollee button shall be pushed within Walk Time or the Registrar will indicate failure (refer to Figure 17).

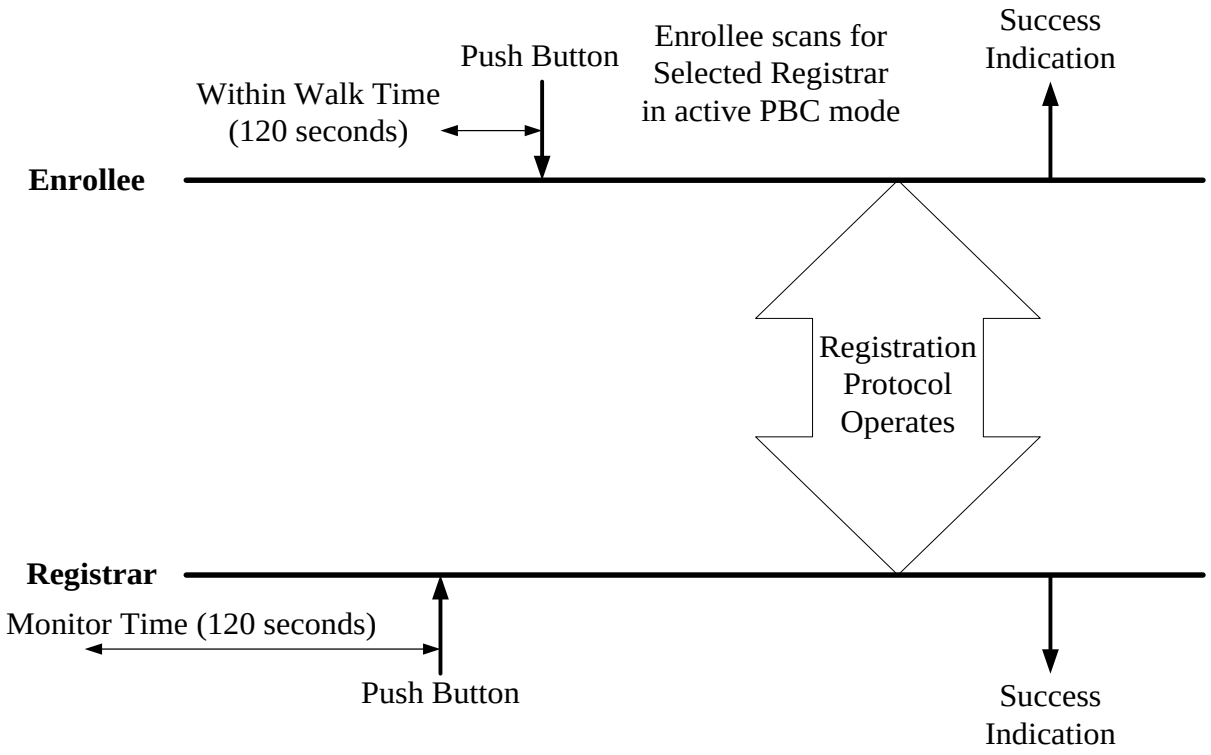

Figure 17 – User Actions – Registrar PB first

When the user pushes the Registrar button, the Registrar informs the AP using the UPnP action SetSelectedRegistrar that it is the Selected Registrar and that it is actively using PBC mode. The AP informs Enrollees that the Selected Registrar is in active PBC mode using Beacons and Probe Response frames.

11.3 PBC Technical Description

As shown in Figure 16, Figure 17, and Figure 18, the button press or equivalent trigger event on the Enrollee (B_E) causes it to actively search for a Registrar in PBC mode. However, the Enrollee SHALL not proceed immediately with the Registration Protocol when it first discovers a Registrar in active PBC mode. Instead, the Enrollee SHALL complete a scan of all 802.11 channels that it supports to discover if any other nearby Registrars are in active PBC mode.

The Enrollee performs this scan by sending out probe requests with a Device Password ID indicating that the Enrollee is in PBC mode and receiving probe responses indicating a Selected Registrar with a PBC Device Password ID. The probe request and the probe response shall include the WSC IE. During this scan, if the Enrollee discovers more than one Registrar in active PBC mode then the Enrollee SHALL abort its connection attempt and signal a “session overlap” error to the user. If a session overlap error occurs, the user should be advised through the Enrollee or Registrar UI or product literature to wait some period of time before trying again. Note: In the case of a dual-band AP and a dual-band station, the station may discover more than one Registrar in active PBC mode. If the dual-band station does discover more than one Registrar in

active PBC mode, one on each RF band, and the UUID in the Beacon and Probe-Response are the same for all RF bands, then the station shall not consider this to be a session overlap.

Alternatively, the user may use a different method such as the PIN method to resolve this problem, if a Registrar capable of PIN input is available.

If only one Registrar in active PBC mode is found after a complete scan, the Enrollee can immediately begin running the Registration Protocol with the Registrar in active PBC mode. The station shall receive the Wi-Fi Simple Configuration IE from the Registrar, with active PBC mode, in order to engage with the Registrar using the PBC method.

The button press or equivalent trigger event on the Registrar (B_R) causes it to first check whether PBC probe requests from more than one Enrollee have been received by the Registrar. The Registrar shall examine whether probe requests have been received within a 120 second window prior to the PBC button press on the Registrar. This window is called the PBC Monitor Time. Within the PBC Monitor Time, if the Registrar receives PBC probe requests from more than one Enrollee, or if the Registrar receives an M1 message from an Enrollee with a UUID-E that does not match the UUID-E received in a probe request, then the Registrar SHALL signal a “session overlap” error. As a result, the Registrar shall refuse to enter active PBC mode and shall also refuse to perform a PBC-based Registration Protocol exchange until both of the following conditions are met:

- The user presses the Registrar’s PBC button again.
- Only one PBC Enrollee has been seen within the prior Monitor Time window of the new button press.

If the Registrar is engaged in PBC Registration Protocol exchange with an Enrollee and receives a Probe Request or M1 Message from another Enrollee, then the Registrar should signal a “session overlap” error. In this case, the Registrar would reply with a WSC_NACK upon reception of the next M1-M8 message received from the Enrollee that it is engaged with.

If the Registrar has been running for less than Monitor Time (that is, it is freshly booted), it is not required to wait until Monitor Time has elapsed before entering active PBC mode.

If the Registrar successfully runs the PBC method to completion with an Enrollee, that Enrollee’s probe requests are removed from the Monitor Time check the next time the Registrar’s PBC button is pressed. This permits multiple PBC Enrollees to be added sequentially without requiring a 120 second delay between each one.

An Enrollee or Registrar shall only remain in active PBC mode for the duration of Walk Time after its PBC button (or equivalent trigger) has been pressed before reverting to non-active PBC mode. Multiple presses of the button are permitted. If a PBC button on an Enrollee or Registrar is pressed again during Walk Time, the timers for that device are restarted at that time and the other actions that occur at the first button press are performed again (sending out probes or scanning for example). The effect is the same

as if the device's PBC button has been pressed for the first time. Walk Time timer expiration during the protocol run does not terminate the protocol for PBC mode. If PBC is completed successfully, the configuration received during negotiation shall be used.

When an AP receives a Selected Registrar and Device Password ID indicating active PBC mode from a Registrar, it shall either automatically remove this information and no longer include Selected Registrar or set it to FALSE in probe response and beacon frames after an interval of Walk Time has elapsed.

Before the Registrar's button is pushed, the AP shall not advertise any active PBC mode. Further, any M1 messages from an Enrollee specifying the PBC method (using the Device Password ID) shall result either in an M2D message or M2 message with different Device Password ID from Registrars that are not in PBC mode. Until a single Registrar in active PBC mode is found, or until Walk Time elapses, the Enrollee shall continue scanning for a Registrar in active PBC mode.

When the PBC Registrar's button is pushed, it shall send a UPnP SetSelectedRegistrar message to the AP which will cause the AP to advertise a Selected Registrar with active PBC mode. When in active PBC mode, the Registrar shall respond to a PBC M1 message with an M2 message but only if the UUID-E value in the PBC M1 message matches the UUID-E from the PBC probe request message (i.e., if the UUID-E of the PBC M1 message does not match the UUID-E from the PBC probe request message, then the PBC M1 message shall be rejected by the Registrar with M2D using Configuration Error 12 - Multiple PBC sessions detected). The M2 message denotes via the Device Password ID attribute that the Registrar is in the active PBC mode. Upon receiving the M2 message, the Enrollee engages that Registrar with messages M3-M8, with both the Registrar and Enrollee using a value of '00000000' for the PBC Device Password (i.e., PIN = all zeroes).

Figure 18 illustrates the message flow for an external Registrar, an AP, and an Enrollee using PBC. The B_E event is when the Enrollee button is pressed and the B_R event is the Registrar's button press. When the order is reversed and the Registrar's button is pressed first, the behavior is similar.

The AP will be instructed by the Registrar to advertise the Registrar's active PBC mode. As long as the Enrollee's button is pressed before the Walk Time timeout, the protocol proceeds in the same manner as when the buttons are pressed in the opposite order. Note that if the Registrar is internal to the AP, the UPnP messages may become simple library calls.

During implementation, the primary difference between the PBC method and the authenticated device password method is whether the Trigger event of the session comes from user's Pushbutton action or from device password (PIN) input. The protocol after M1 shall be identical. This protocol consistency reduces the implementation burden for Enrollee devices that support the optional PBC method in addition to the mandatory PIN method.

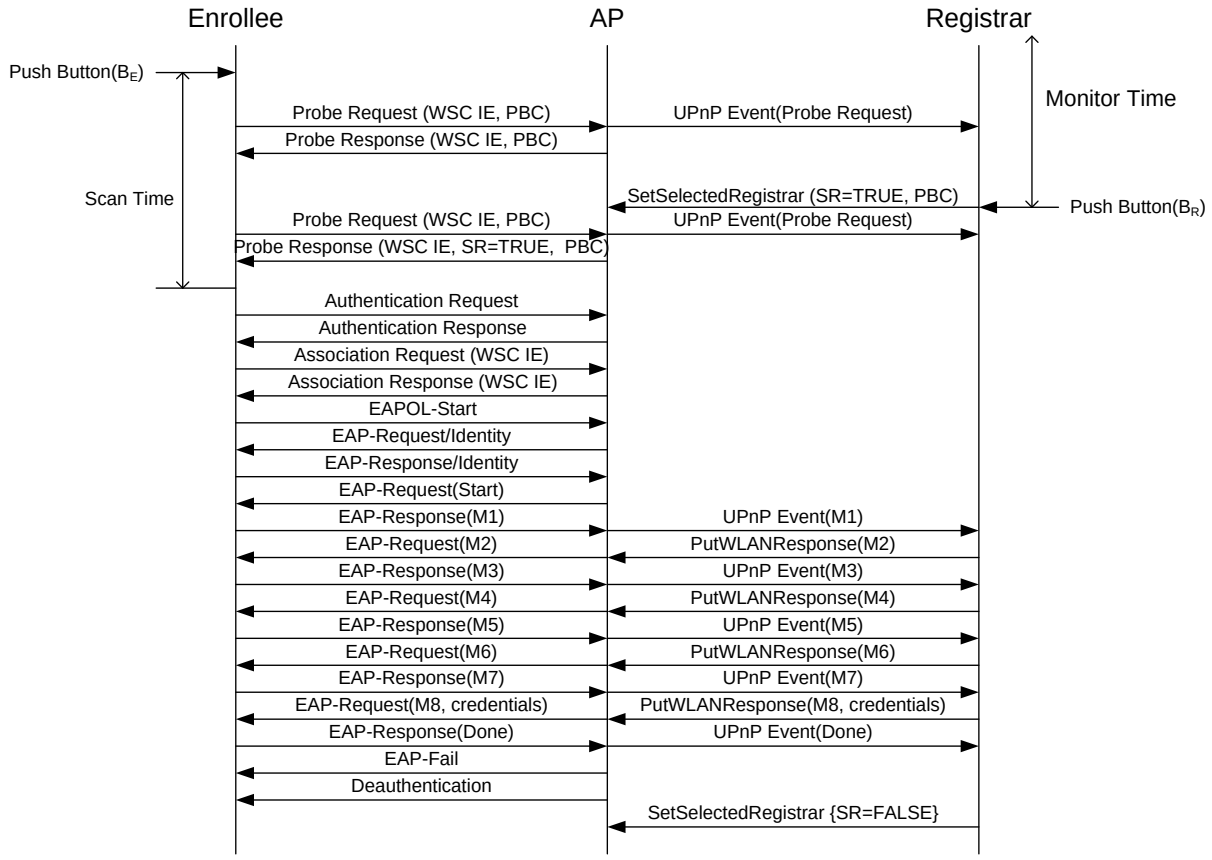

Figure 18 – PBC message exchange

11.4 PBC Security Considerations

PBC protects against eavesdropping attacks and takes measures to prevent a device from joining a network that was not selected by the device owner. The absence of authentication, however, means that PBC does not protect against active attack.

PBC is susceptible to an active attack where the attacker makes the intended AP completely undetectable. This attack is possible by jamming the channel and offering an AP in the active PBC mode on another channel to induce an Enrollee to connect to a rogue network. It is also possible for an active attacker to gain access to the end user's WLAN. If, for example, the end user presses the Registrar button first, the attacker has an opportunity to connect to the AP before the intended Enrollee's button is pressed.

The end user should be instructed to check the LED(s) on both the Registrar and the Enrollee in case there is a success indication on one and a failure indication on the other. Users should also verify that the device is connected to the correct network when PBC is used. The user may, for example, print a page on the newly connected printer from another network device, or view content on a media device.

If the attacker combines an attack to capture an Enrollee with an attack that gains access to the user's WLAN the LED(s) will indicate success. If the attacker

subsequently routes traffic between the Enrollee that it has captured and the user's WLAN, the attack would be virtually undetectable.

Because of the vulnerabilities to active attack, users who are concerned about the security of their network should be advised to use one of the other Wi-Fi Simple Configuration methods rather than PBC. Client devices are required to support the PIN-based method. Therefore, as long as the network includes at least one Registrar capable of PIN entry, users have a viable option of setting up the network securely.

12 Data Element Definitions

The following table enumerates the various attribute types defined for Wi-Fi Simple Configuration. The sizes given in Length correspond to the Data part of the attribute. The overall size occupied by each attribute will include an additional 4 bytes (2 bytes of ID, 2 bytes of Length). Boolean attributes (identified with 'Bool' as the Length in the following table) have the Length of one byte (1B) and have two valid values: 0 = FALSE, 1 = TRUE. The variable length string attributes, e.g., Device Name, are encoded without null-termination, i.e., no 0x00 octets added to the end of the value. If the string is empty, the attribute length is set to zero. Note: Some existing implementations based on v1.0h use zero padding on some of the attributes. For backwards compatibility, implementations should be able to parse such values in received attributes by ignoring the extra 0x00 octet(s), but new implementations shall not add this type of padding when generating string attributes. Note: Unrecognized attributes in messages shall be ignored; they shall not cause the message to be rejected.

Table 28 – Attribute types and sizes defined for Wi-Fi Simple Configuration

Description	ID (Type)	Length
802.1X Enabled	0x1062	Bool
AP Channel	0x1001	2B
AP Setup Locked	0x1057	Bool
Application Extension	0x1058	<= 512B
AppSessionKey	0x1063	<=128B
Association State	0x1002	2B
Authentication Type	0x1003	2B
Authentication Type Flags	0x1004	2B
Authenticator	0x1005	8B
Available IPv4 Submask List	0x1072	N*4B
Configuration Error	0x1009	2B
Configuration Methods	0x1008	2B
Confirmation URL4	0x100A	<=64B
Confirmation URL6	0x100B	<=76B
Connection Type	0x100C	1B
Connection Type Flags	0x100D	1B
Credential	0x100E	unlimited
Device Name	0x1011	<= 32B
Device Password ID	0x1012	2B
EAP Identity	0x104D	<= 64B
EAP Type	0x1059	<= 8B

Description	ID (Type)	Length
E-Hash1	0x1014	32B
E-Hash2	0x1015	32B
Encrypted Settings	0x1018	unlimited
Encryption Type	0x100F	2B
Encryption Type Flags	0x1010	2B
Enrollee IPv4 Address	0x1071	4B
Enrollee Nonce	0x101A	16B
Entry Acceptable (only for IBSS)	0x106D	1B
E-SNonce1	0x1016	16B
E-SNonce2	0x1017	16B
Feature ID	0x101B	4B
Identity	0x101C	<= 80B
Identity Proof	0x101D	unlimited
Initialization Vector	0x1060	32B
IP Address Configuration Methods	0x1073	2B
IPv4 Subnet Mask	0x1070	4B
Key Identifier	0x101F	16B
Key Lifetime	0x1051	4B
Key Provided Automatically	0x1061	Bool
Key Wrap Authenticator	0x101E	8B
MAC Address	0x1020	6B
Manufacturer	0x1021	<= 64B
Message Counter	0x104E	8B
Message Type	0x1022	1B
Model Name	0x1023	<= 32B
Model Number	0x1024	<= 32B
Network Index	0x1026	1B
Network Key	0x1027	<= 64B
Network Key Index (reserved)	0x1028	1B
New Device Name	0x1029	<= 32B
New Password	0x102A	<= 64B
Out-of-Band Device Password	0x102C	<= 58B
OS Version	0x102D	4B
Permitted Configuration Methods	0x1052	2B

Description	ID (Type)	Length
Portable Device	0x1056	Bool
Power Level	0x102F	1B
Primary Device Type	0x1054	8B
PSK Current	0x1030	1B
PSK Max	0x1031	1B
Public Key	0x1032	192B
Public Key Hash	0x104F	20B
Radio Enabled	0x1033	Bool
Reboot	0x1034	Bool
Registrar Current	0x1035	1B
Registrar Established	0x1036	Bool
Registrar IPv4 Address	0x106F	4B
Registrar List	0x1037	<=512B
Registrar Max	0x1038	1B
Registrar Nonce	0x1039	16B
Registration Ready (only for IBSS)	0x106E	1B
Rekey Key	0x1050	32B
Request Type	0x103A	1B
Requested Device Type	0x106A	8B
Response Type	0x103B	1B
RF Bands	0x103C	1B
R-Hash1	0x103D	32B
R-Hash2	0x103E	32B
R-SNonce1	0x103F	16B
R-SNonce2	0x1040	16B
Secondary Device Type List	0x1055	<= 128B
Selected Registrar	0x1041	Bool
Selected Registrar Configuration Methods	0x1053	2B
Serial Number	0x1042	<= 32B
SSID	0x1045	<= 32B
Total Networks	0x1046	1B
UUID-E	0x1047	16B
UUID-R	0x1048	16B

Description	ID (Type)	Length
Vendor Extension	0x1049	<= 1024B
Version	0x104A	1B (int)
WEPTransmitKey	0x1064	1B
Wi-Fi Simple Configuration State	0x1044	1B
X.509 Certificate	0x104C	unlimited
X.509 Certificate Request	0x104B	unlimited
<Reserved - not allowed>	0x0000 to 0x1000	n/a
<Reserved - not allowed>	0x1006	n/a
<Reserved - not allowed>	0x1007	n/a
<Reserved - not allowed>	0x1013	n/a
<Reserved - not allowed>	0x1019	n/a
<Reserved - not allowed>	0x1025	n/a
<Reserved - not allowed>	0x102B	n/a
<Reserved - not allowed>	0x102E	n/a
<Reserved - not allowed>	0x1043	n/a
<Reserved - not allowed>	0x105A to 0x105F	n/a
<Reserved for future WSC use>	0x1065 to 0x1069 and 0x106B, 0x106C, and 0x1074 to 0x1FFF	n/a
<Reserved - not allowed>	0x2000 to 0xFFFF	n/a

The following table defines the subelement values used in WFA Vendor Extension attribute. This attribute is used to encode new information in a way that avoids some backwards compatibility issues with deployed implementations that are based on previous specification versions, but do not comply with requirements to ignore new attributes.

WFA Vendor Extension attribute is a Vendor Extension attribute (ID 0x1049) that uses Vendor ID 0x00372A and contains one or more subelements. Each subelement starts with a header consisting of one-octet ID field (the subelement ID value from the following table) and one-octet length field (number of octets in the payload of this subelement).

Table 29 – WFA Vendor Extension Subelements

Description	ID	Length
Version2	0x00	1B
AuthorizedMACs	0x01	<=30B
Network Key Shareable	0x02	Bool
Request to Enroll	0x03	Bool
Settings Delay Time	0x04	1B
Registrar Configuration Methods	0x05	2B
Multi-AP Identifier	0x06	1B
Multi-AP Profile	0x07	1B
Multi-AP Default 802.1Q Setting	0x08	2B
Reserved for future use	0x09 to 0xFF	

802.1X Enabled

This variable specifies if the network uses 802.1X for network authentication.

AP Channel

This variable specifies the 802.11 channel the AP is hosting.

AP Setup Locked

This variable indicates that the AP has entered a state in which it will refuse to allow an external Registrar to attempt to run the Registration Protocol using the AP's PIN (with the AP acting as Enrollee). The AP SHALL enter this state after 3 failed PIN authentication attempts within 60 seconds. An AP shall stay in the lock-down state for 60 seconds. When the AP is in this state, it SHALL continue to allow other Enrollees to connect and run the Registration Protocol with any external Registrars or the AP's built-in Registrar (if any). It is only the use of the AP's PIN for adding external Registrars that is disabled in this state.

If AP allows operation as an Enrollee to be started by sending M1 even if AP Setup is locked (e.g., to provide manufacturer information), and Registrar(station) continues negotiation, Enrollee(AP) will reject the request to add a new external Registrar by replying to M2 with WSC_NACK with the configuration error value for Setup Locked.

The AP Setup Locked state can be reset to FALSE through an authenticated call to SetAPSettings. APs may provide other implementation-specific methods of resetting the AP Setup Locked state as well.

AppSessionKey

The AppSessionKey attribute allows the exchange of application specific session keys and may be used as an alternative to calculating AMSKs.

Application Extension

The Application Extension attribute is used to pass parameters for enabling applications during the WSC exchange. It is similar to the Vendor Extension attribute except that instead of a 3-byte Vendor ID prefix to the Vendor Data field, a 16-byte UUID (as defined in RFC 4122) is used. This provides a virtually unlimited application ID space with a regular structure that can be easily mapped onto a generic application extension API. Furthermore, the 16-byte UUID value can be used to derive application-specific AMSKs as described in Section 7.3 or pass any necessary keying directly.

The Enrollee may, for example, send two Application Extension attributes to the Registrar in the Encrypted Settings of M7, one with UUID-A and one with UUID-X. If the Registrar supports the application corresponding to UUID-X but not UUID-A, the Registrar may indicate to the Enrollee that it also supports application X by sending an Application Extension with UUID-X in the Encrypted Settings of M8. Given this exchange, the Enrollee and Registrar can exchange application-specific information in the Data field such as application specific keying, and/or they can derive an AMSK for application X as follows:

AMSK = kdf(EMSK, N1 || N2 || UUID-X, 256)

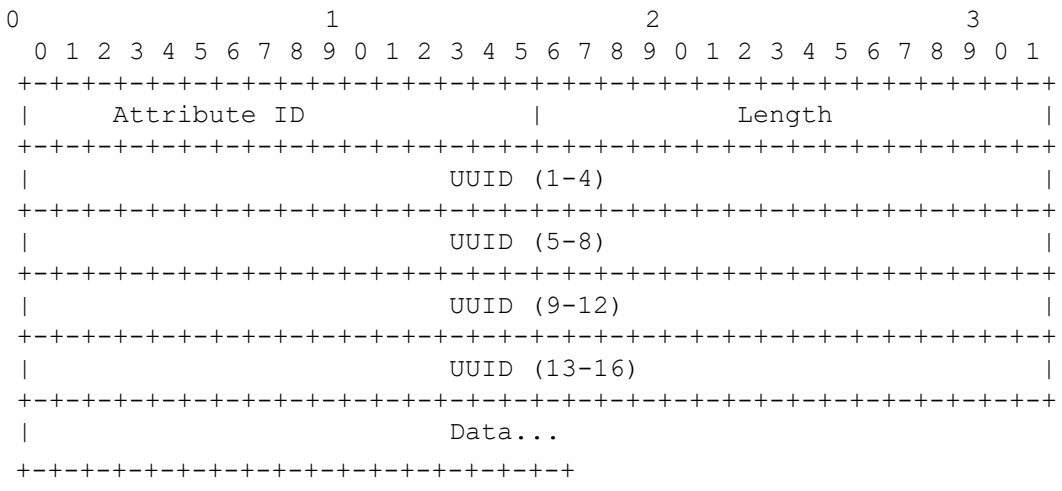

Figure 19 – Application Extension

One use of this Application Extension mechanism is to permit a Wi-Fi Simple Configuration exchange to simultaneously set up connections for multiple wireless technologies (Wi-Fi, Bluetooth, etc.). To accomplish this, each network type would specify a UUID value for this purpose and define a corresponding Data element (to exchange data such as the device's MAC address on the other network). A network

setup application on each device would exchange the Application Extension data using the Wi-Fi Simple Configuration Registration Protocol and then set up the other network connections using that data with the native pairing mechanisms of the other networks.

Furthermore, if device pairing takes place first with another network type, it is possible to use the other network pairing mechanism as an out-of-band channel comparable to UFD or NFC. If this is done, the UUID and Data value to use for Wi-Fi Simple Configuration are:

UUID=0xA6F6D81FB26941e2A72EC0B702248E90

Data=TLV attribute list below:

Table 30 – Attributes in the Data field (out-of-band channel)

Attribute	R/O/C	Notes
Version	R	As defined in section 12
Out-of-Band Device Password	O	May be omitted if Out-of-Band Device Password has already been received from peer device.
SSID	O	Included if SSID is known by sender.
Version2 (inside WFA Vendor Extension)	C	As defined in section 12
<other…>	O	

Note that this approach passes the Out-of-Band Device Password directly in the Data field or can be used to pass transport specific parameters and keying directly to eliminate the need to re-run the Registration protocol a second time.

Association State

The Association State component shows the configuration and previous association state of the wireless station when sending a Discovery request.

Table 31 – Association State Values

Association State	Description
0	Not Associated
1	Connection Success
2	Configuration Failure
3	Association Failure
4	IP Failure

Authentication Type

This variable contains the selected value from the Authentication Types table for the Enrollee (AP or station) to use. When both the Registrar and the Enrollee are using

protocol version 2.0 or newer, this variable can use the value 0x0022 to indicate mixed mode operation (both WPA-Personal and WPA2-Personal enabled). Protocol version 1.0h did not describe a value for mixed mode operation and for backwards compatibility, only a single value, 0x0020 WPA2-Personal, should be used when communicating with version 1.0 devices. 0x0022 is the only allowed case where multiple authentication types are set; all other values are required to have only a single bit set to one in this attribute value.

Authentication Type Flags

This variable indicates the network authentication capabilities of the Enrollee (AP or station). It provides a bitwise OR of the fields in the Authentication Types table.

Table 32 – Authentication Types

Value	Authentication Type	Notes
0x0001	Open	
0x0002	WPA-Personal	Deprecated in version 2.0
0x0004	Shared	Deprecated in version 2.0
0x0008	WPA-Enterprise	Deprecated in version 2.0
0x0010	WPA2-Enterprise	Includes both CCMP and GCMP
0x0020	WPA2-Personal	Includes both CCMP and GCMP
0x0040	Reserved for Multi-AP use	

Authenticator

The Message Authenticator component is a keyed hash of data. The specific data included in the hash calculation depends upon the processing context. The hash algorithm for Wi-Fi Simple Configuration versions 1.0 and 2.0 is HMAC-SHA-256. In the context of the Registration Protocol, the default key used in the HMAC is AuthKey. If a non-default key is used, the key is specified in the Key Identifier attribute immediately preceding the Authenticator attribute. To reduce message payload size, the Authenticator attribute's Data component includes only the first 64 bits of the HMAC-SHA-256 output.

AuthorizedMACs

This subelement contains a list of Enrollee MAC addresses (each being six bytes in length) that have been registered to start WSC. The AP includes this field in Beacon and Probe Response frames so Enrollees can tell if they have been registered to start WSC. There may be multiple Enrollees active on the network, but not all of them have been registered to start WSC. This element allows an Enrollee to detect if they should start WSC with the AP. The AuthorizedMACs field augments the use of the Selected Registrar.

External Registrars include this subelement in the SetSelectedRegistrar UPnP action to notify the AP of the authorized Enrollees. The AP merges the lists of authorized

Enrollee MAC addresses received from all Registrars into the AuthorizedMACs subelement in Beacon and Probe Response frames. The AP updates this information whenever a Registrar indicates a new set of authorized addresses. The AP is also responsible for removing addresses from this subelement whenever an external Registrar is disconnected from the AP in case that Registrar had not removed its list of authorized addresses with SetSelectedRegistrar.

Registrars (both internal and external) shall add the AuthorizedMACs subelement, this applies to all Configuration Methods, including PIN, PBC and NFC. Registrars (both internal and external) shall include the authorized Enrollee MAC address into the AuthorizedMACs subelement when they receive provisioning information (such as PIN value associated with MAC address). The Registrar shall include the wildcard MAC Address (FF:FF:FF:FF:FF:FF) if the Registrar doesn't have enough information to specify target Enrollee (e.g. In the case where the Registrar does not have a user interface to let users to select a target Enrollee from the list). APs are required to include a merged list of authorized Enrollee MAC addresses in Beacon and Probe Response frames.

APs shall include the wildcard MAC Address in the AuthorizedMACs subelement that is added to Beacon and Probe Response frames in the case where they receive a SetSelectedRegistrar UPnP action with SelectedRegistrar flag equal to TRUE from a WSC version 1.0 External Registrar. An AP that included the wildcard MAC Address in the AuthorizedMACs subelement in Beacon and Probe Response frames on behalf of a WSC 1.0 External Registrar will remove the wildcard MAC address if it receives a SetSelectedRegistrar UPnP action with a SelectedRegistrar flag equal to FALSE from that Registrar, or if that Registrar is disconnected from the AP, if no other Registrar has caused the wildcard MAC address to be added and therefore requires its presence.

Configuration Methods

The Configuration Methods Data component lists the configuration methods the Enrollee or Registrar supports. The list is a bitwise OR of values from the table below. In addition to Configuration Methods, APs and STAs that support the UPnP Management Interface shall support the Permitted Configuration Methods attribute, which is used to control the Configuration Methods that are enabled on that AP.

Table 33 – Configuration Methods

Value	Configuration Method	Description
0x0001	USBA (Flash Drive)	Deprecated
0x0002	Ethernet	Deprecated
0x0004	Label	8 digit static PIN typically available on device.
0x0008	Display	A dynamic 4 or 8 digit PIN is available from a display. Version 2.0 devices shall qualify the display as Virtual (0x2008) or Physical (0x4008)
0x0010	External NFC Token	An NFC Tag is used to transfer the configuration or device password.
0x0020	Integrated NFC Token	The NFC Tag is integrated in the device.
0x0040	NFC Interface	The device contains an NFC interface.
0x0080	Pushbutton	The device contains either a physical or virtual Pushbutton. Version 2.0 devices shall qualify the Pushbutton as Virtual (0x0280) or Physical (0x0480)
0x0100	Keypad	Device is capable of entering a PIN
0x0280	Virtual Pushbutton	Pushbutton functionality is available through a software user interface.
0x0480	Physical Pushbutton	A physical Pushbutton is available on the device.
0x0880	(Reserved)	Reserved (for IBSS with Wi-Fi Protected Setup Specification)
0x1000	P2Ps Default Configuration Method	Reserved for Wi-Fi Peer-to-Peer Services Specification [19]
0x2008	Virtual Display PIN	The dynamic 4 or 8 digit PIN is displayed through a remote user interface. For example using the management html page of an AP to obtain the dynamic PIN.
0x4008	Physical Display PIN	The dynamic 4 or 8 digit PIN is shown on a display/screen that is part of the device. For example obtaining the dynamic PIN from the LCD screen on a printer.

Configuration Error

The Configuration Error component shows the result of the device attempting to configure itself and to associate with the WLAN.

Table 34 – Configuration Error

Configuration Error	Description	Comments
0	No Error	Used whenever protocol run is still proceeding without errors. - only valid option for Probe Request WSC IE, M1, M2 - not valid for WSC_NACK except when a station acts as an External Registrar (to learn the current AP settings after M7 with configuration error = 0)
1	Out-of-Band Interface Read Error	Used in M2 when failing to read out-of-band information
2	Decryption CRC Failure	Used as indication of failed decryption of Encrypted Settings attribute (invalid PKCS#5 v2.0 pad string).
3	2.4 channel not supported	Indicate that the 2.4 RF band is not supported when receiving new settings with optional RF bands attribute.
4	5.0 channel not supported	Indicate that the 5.0 RF band is not supported when receiving new settings with optional RF bands attribute.
5	Signal too weak	Deprecated – do not use.
6	Network auth failure	Deprecated – do not use.
7	Network association failure	Deprecated – do not use.
8	No DHCP response	Deprecated – do not use.
9	Failed DHCP config	Deprecated – do not use.
10	IP address conflict	Deprecated – do not use.
11	Couldn’t connect to Registrar	AP: sent in WSC_NACK as a response to M1 (or WSC_ACK after M2D in case multiple Registrars are used) if the AP cannot connect to an External Registrar that has been registered with the AP

Configuration Error	Description	Comments
12	Multiple PBC sessions detected	Enrollee/Registrar: if session overlap is detected during protocol run, WSC_NACK with this value is used to indicate that (if WSC_NACK is allowed to be sent at that time in the protocol run).
13	Rogue activity suspected	Report suspected rogue activity (based on vendor-specific mechanism to detect this, e.g., based on a burst of failed protocol run)
14	Device busy	Used if a device is unable to respond due to some internal conflict or resource contention issue; for example, if a device is only capable of performing a single instance of the Registration Protocol at a time, it may return this error in response to attempts to start another instance in the middle of an active session.
15	Setup locked	Enrollee(AP): if the AP allows operation as an Enrollee to be started by sending M1 even if AP Setup is locked (e.g., to provide manufacturer information), and Registrar(station) continues negotiation, Enrollee(AP) will reject the request to add a new external Registrar by replying to M2 with WSC_NACK with this configuration error value
16	Message Timeout	Deprecated – do not use.
17	Registration Session Timeout	Deprecated – do not use.
18	Device Password Auth Failure	- Enrollee: if R-Hash1 derived from R-S1 does not match with the pre-committed value in M4 - Enrollee: if R-Hash2 derived from R-S2 does not match with the pre-committed value in M6 - Registrar: if E-Hash1 derived from E-S1 does not match with the pre-committed value in M5 - Registrar: if E-Hash2 derived from E-S2 does not match with the pre-committed value in M7
19	60 GHz channel not supported	Indicate that the 60 GHz RF band is not supported when receiving new settings with optional RF bands attribute.

Configuration Error	Description	Comments
20	Public Key Hash Mismatch	Indicate that a public key hash value does not match a public key.

Confirmation URL4

The Registrar may provide a URL (IPv4 address based) for the Enrollee to use to post a confirmation once settings have been successfully applied and the Enrollee has joined the network. This configuration parameter is optional for a Registrar and it is optional for the Enrollee to post to the URL if the Registrar includes it. The Enrollee shall not connect to a Confirmation URL that is on a different subnet. Details regarding how to perform the confirmation are not yet specified.

Confirmation URL6

The Registrar may provide a URL (IPv6 address based) for the Enrollee to use to post a confirmation once settings have been successfully applied and the Enrollee has completed joining the network. This is an optional configuration parameter for a Registrar and it is optional for the Enrollee to post to the URL if the Registrar includes it. The Enrollee shall not connect to a Confirmation URL that is on a different subnet. Details regarding how to perform the confirmation are not yet specified.

Connection Type

This attribute contains a specific value from the Connection Type Flags table for the Enrollee (AP or station) to use.

Connection Type Flags

This variable represents the capabilities of the Enrollee.

Table 35 – Connection Types

Value	Description	Required/Optional
0x1	ESS	R
0x2	IBSS	R

Credential

This is a compound attribute containing a single WLAN Credential. There can be multiple instances of the Credential attribute. The following table lists the attributes in Credential:

Table 36 – Credential Attributes

Attribute	R/O	Notes, Allowed Values
Network Index	R	Deprecated – use fixed value 1 for backwards compatibility.
SSID	R	SSID of network.
Authentication Type	R	The authentication type used in this network.
Encryption Type	R	The encryption type used in this network.
Network Key Index	O	Deprecated. Only included by WSC 1.0 devices. Ignored by WSC 2.0 or newer devices.
Network Key	R	
MAC Address	R	Member device's MAC address.
EAP Type	O	
EAP Identity	O	
Key Provided Automatically	O	
802.1X Enabled	O	
Network Key Shareable (inside WFA Vendor Extension)	O	If present, this attribute indicates whether the Network Key can be shared or not with other devices.
<other…>	O	Multiple attributes are permitted.

Device Name

This component is a user-friendly description of the device encoded in UTF-8. Typically, the component would be a unique identifier that describes the product in a way that is recognizable to the user.

Device Password ID

This attribute is used to identify a device password. There are seven predefined values and seven reserved values. If the Device Password ID is Default, the Enrollee should use its PIN password (from the label or display). This password may correspond to the label, display, or a user-defined password that has been configured to replace the original device password.

User-specified indicates that the user has overridden the password with a manually selected value. Machine-specified indicates that the original PIN password has been overridden by a strong, machine-generated device password value. The Rekey value indicates that the device's 256-bit rekeying password will be used. The Pushbutton value indicates that the PIN is the all-zero value reserved for the Pushbutton configuration method.

The Registrar-specified value indicates a PIN that has been obtained from the Registrar (via a display or other out-of-band method). This value may be further augmented with the optional "Identity" attribute in M1. This augmentation is useful when multiple predefined UserID/PIN pairs have been established by a Registrar such as an authenticator used for Hotspot access. If the Device Password ID in M1 is not one of the predefined or reserved values, it corresponds to a password given to the Registrar as an Out-of-Band Device Password.

The NFC-Connection-Handover value indicates that the Registrar and Enrollee have exchanged NFC Connection Handover messages containing hashes of their respective public keys over NFC, and that WLAN configuration data will be delivered in M2.

P2Ps value indicates that P2Ps Default Configuration method PIN as specified by Wi-Fi Peer-to-Peer Services Specification [19] shall be used.

Table 37 – Device Password ID

Value	Description
0x0000	Default (PIN)
0x0001	User-specified
0x0002	Machine-specified
0x0003	Rekey
0x0004	Pushbutton
0x0005	Registrar-specified
0x0006	Reserved (for IBSS with Wi-Fi Protected Setup Specification)
0x0007	NFC-Connection-Handover
0x0008	P2Ps (Reserved for Wi-Fi Peer-to-Peer Services Specification [19])
0x0009 – 0x000F	Reserved
0x0010 - 0xFFFF	Randomly generated value for Password given to the Enrollee or Registrar via an Out-of-Band Device Password attribute.

EAP Identity

This attribute contains an ASCII representation of the NAI to be used with a Credential.

EAP Type

This attribute contains the binary representation of an EAP type as found in an EAP packet. If it is a standard EAP Type, it is only a single byte. Extended EAP types, such as the Wi-Fi Simple Configuration Registration Protocol (refer to section 7.7.1), may be up to eight bytes (one-byte Type, three-byte Vendor-Id, and four-byte Vendor-Type).

E-Hash1

This is the HMAC-SHA-256 hash of the first half of the device password and the Enrollee's first secret nonce.

E-Hash2

This is the HMAC-SHA-256 hash of the second half of the device password and the Enrollee's second secret nonce.

E-SNonce1

This is the first nonce used by the Enrollee with the first half of the device password

E-SNonce2

This is the second nonce used by the Enrollee with the second half of the device password.

Encrypted Settings

The Data field of the Encrypted Settings attribute includes an initialization vector (IV) followed by a set of encrypted Wi-Fi Simple Configuration TLV attributes. The last attribute in the encrypted set is a Key Wrap Authenticator computed according to the procedure described in section7.5.

In the context of the Registration Protocol, the default key used for the encryption is the KeyWrapKey. The encryption algorithm is AES in CBC mode in accordance with FIPS 197. In other contexts, the key is specified in a Key Identifier attribute immediately preceding the Encrypted Settings attribute. The data structure of the Encrypted Settings attribute follows.

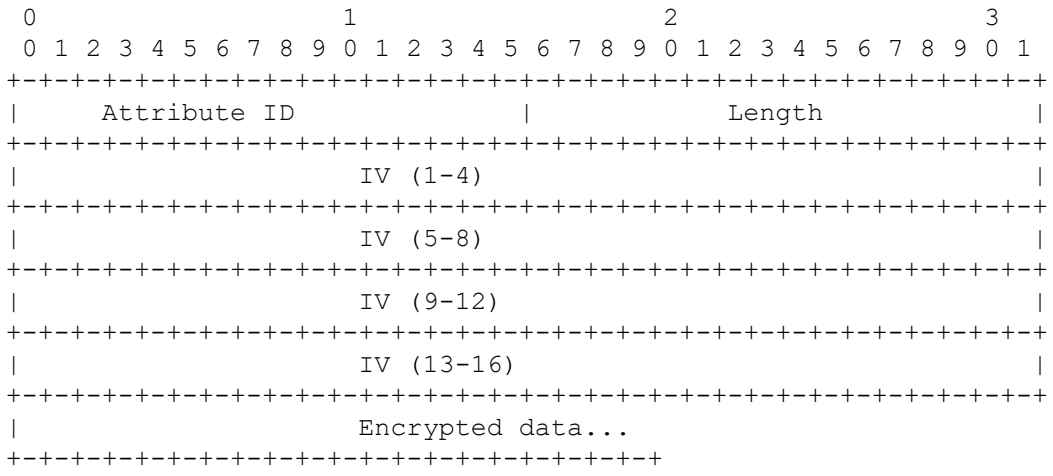

Figure 20 – Encrypted Settings data structure

If an alternative key wrap algorithm is supported in the future, it can be added by defining a new attribute with a different Attribute ID. The Key Wrap Authenticator is 96 bits long (32 bits of Attribute ID and Length, 64 bits of the HMAC-SHA-256 output). This implies that the total overhead for an Encrypted Settings attribute is 256 bits (32 bits of Attribute ID and Length, 128 bits of IV, and 96 bits of Key Wrap Authenticator).

Encryption Type

This attribute contains a specific value from the Encryption Type Flags table for the Enrollee (AP or station) to use. When both the Registrar and the Enrollee are using protocol version 2.0 or newer, this variable can use the value 0x000c to indicate mixed mode operation (both WPA-Personal with TKIP and WPA2-Personal with AES enabled). Protocol version 1.0h did not describe a value for mixed mode operation and for backwards compatibility, only a single value, 0x0008 AES, should be used when communicating with version 1.0 devices. 0x000c is the only allowed case where multiple encryption types are set; all other values are required to have only a single bit set to one in this attribute value.

Encryption Type Flags

This attribute contains a binary OR set of WLAN encryption types supported by the Enrollee (one or more from the Encryption Types table).

Table 38 – Encryption Types

Value	Encryption Type	Notes
0x0001	None	
0x0002	WEP	Deprecated in version 2.0
0x0004	TKIP	Deprecated in version 2.0. TKIP can only be advertised on the AP when Mixed Mode is enabled (Encryption Type is 0x000c).
0x0008	AES	Includes both CCMP and GCMP
0x000c	AES/TKIP	Mixed Mode

Enrollee Nonce

The Enrollee Nonce component is a randomly generated binary value that is created by the Enrollee for setup.

Feature ID

This attribute indicates a particular feature build for an OS running on the device. It is a four byte field, the most significant bit is reserved and always set to one.

Identity

This attribute holds a user identity value encoded as an ASCII string. It can be used by the Enrollee to declare that the Enrollee device corresponds to an existing user or

device identity that has been previously established in a separate authentication domain known by the Registrar.

Identity Proof

This attribute holds a proof of the claimed identity. If the in-band method is used, Identity Proof can be included in M7. Because the authentication of the Registrar is completed in M6, by M7 the Enrollee can share its Identity Proof in the Encrypted Settings attribute and thereby avoid exposure of this proof to an attacker.

Key Identifier

This attribute contains a 128-bit key identifier. If this attribute immediately precedes an Encrypted Data or Authenticator attribute, then the key corresponding to the 128-bit identifier should be used to decrypt or verify the Data field.

Key Lifetime

This attribute contains the number of seconds until the Credential expires.

Key Provided Automatically

This variable specifies whether the key is provided by the network.

Key Wrap Authenticator

This attribute contains the first 64 bits of the HMAC-SHA-256 computed over the data to be encrypted with the key wrap algorithm. It is appended to the end of the ConfigData prior to encryption as described in section 7.5.

MAC Address

The MAC Address is six byte value that contains the 48 bit value of the MAC Address.

Example: 0x00 0x07 0xE9 0x4C 0xA8 0x1C

Manufacturer

The Manufacturer component is an ASCII string that identifies the manufacturer of the device. Generally, this field should allow a user to make an association with a device with the labeling on the device.

Message Counter

This variable contains a 64-bit counter that is included in certain messages to prevent replay attacks. It is not needed in Registration Protocol messages, but it is used in many of the UPnP-based Management Interface messages.

Message Type

This variable identifies the specific message being sent by the Enrollee or Registrar, in accordance with the Message Type table.

Table 39 – Message Type

Message Type Value	Description
0x01	Beacon
0x02	Probe Request
0x03	Probe Response
0x04	M1
0x05	M2
0x06	M2D
0x07	M3
0x08	M4
0x09	M5
0x0A	M6
0x0B	M7
0x0C	M8
0x0D	WSC_ACK
0x0E	WSC_NACK
0x0F	WSC_DONE

Model Name

The Model Name attribute is an ASCII string that identifies the model of the device. Generally, this field should allow a user to create an association of a device with the labeling on the device.

Model Number

The Model Number provides additional description of the device to the user.

Network Index

This variable is deprecated. Value 1 is used for backwards compatibility when the attribute is required in a message.

Network Key

This variable specifies the wireless encryption key to be used by the Enrollee. This field is interpreted in accordance with the Network Key Table. The Network Key attribute value shall not include zero padding, i.e., when WPA2-Personal (Passphrase) option is used, the length of this attribute shall match with the length of the ASCII passphrase. Note: Some existing implementations based on v1.0h null-terminate the passphrase value, i.e., add an extra 0x00 octet into the end of the value. For backwards compatibility, implementations shall be able to parse such a value in received attributes by ignoring the extra 0x00 octet, but new implementations shall not add this padding when generating the Network Key attribute.

Table 40 – Network Key

Authentication	Encryption	Network Key Type	Comment
Open	None	0 ASCII characters	
WPA2-Personal (Passphrase)	TKIP/AES	8 – 63 ASCII characters	
WPA2-Personal	TKIP/AES	64 Hex characters	
Shared/Open	WEP	5 or 13 ASCII characters 10 or 26 Hex characters	Deprecated in version 2.0

Network Key Sharable

This variable is used within Credential attributes. It specifies whether the Network Key included in this Credential can be shared or not with other devices. A TRUE value indicates that the Network Key can be shared.

New Device Name

This variable is used to change the friendly description of the device.

New Password

This variable is used to set a new password on the Enrollee.

Out-of-Band Device Password

The Out-of-Band Device Password attribute contains a fixed data structure intended to be compact enough to fit into small-capacity out-of-band channels. The Out-of-Band Device Password attribute is defined below.

The Password ID of an Out-of-Band Device Password should be chosen at random, but it shall not be one of the predefined or reserved Device Password ID values, except when NFC negotiated handover is used in which case the Password ID is set to NFC-Connection-Handover (0x0007).

The Device Password is (Length – 22) bytes long, with a maximum size of 32 bytes. A 32-byte password implies a total size of 58 bytes for the Out-of-Band Device Password attribute (including the Attribute ID and Length) when written to an NFC Tag, for example. Note that an Out-of-Band Device Password is written to an out-of-band channel in binary format but represented in ASCII format when it is validated (see

Section 7.4). If the out-of-band channel has sufficient capacity, it is recommended that Device password be 32 bytes. Otherwise, it can be any size with a minimum length of sixteen bytes, except when the Device Password ID is equal to NFC-Connection-Handover in which case the Device password shall have zero length. For Enrollee provided Device Passwords, the Public Key Hash Data field corresponds to the first 160 bits of a SHA-256 hash of the Enrollee's public key. This hash shall match that of the Enrollee's Public Key attribute in M1. If this value does not match, then the Registrar SHALL NOT use the Device Password or proceed with M2 of the Registration Protocol (even if the Device Password ID in M1 is a match). When constructing M2 in a Registration Protocol exchange using this password, the Registrar shall copy the Password ID value into the Device Password ID attribute of M2.

For Registrar provided Device Passwords, the Public Key Hash Data field corresponds to the first 160 bits of a SHA-256 hash of the Registrar's public key. This hash shall match that of the Registrar's Public Key attribute in M2. If this value does not match, then the Enrollee SHALL NOT use the Device Password or proceed with M3 of the Registration Protocol (even if the Device Password ID in M2 is a match). When constructing M1 in a Registration Protocol exchange using this password, the Enrollee shall copy the Password ID value into the Device Password ID attribute of M1.

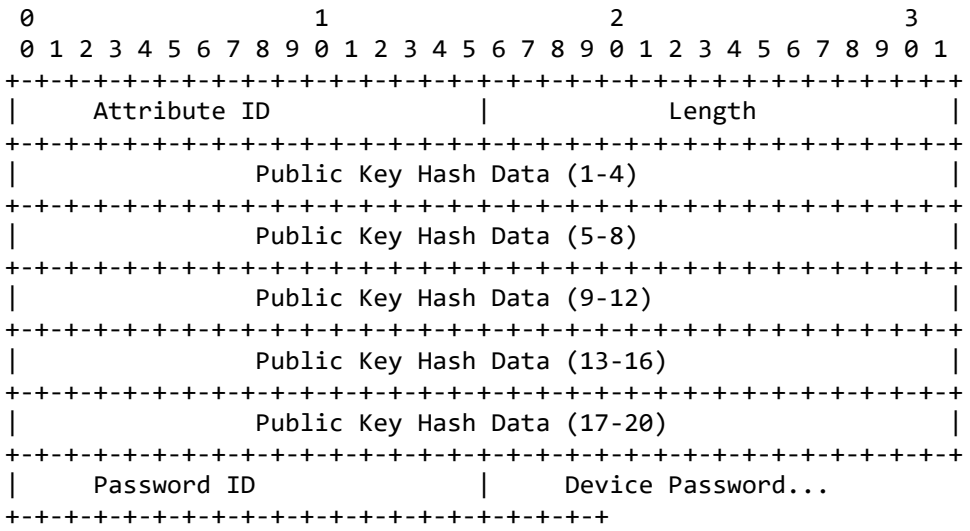

Figure 21 – Out-of-Band Device Password

OS Version

The OS Version component indicates what operating system is running on the device. It is a four-byte field. The most significant bit is reserved and always set to one.

Permitted Configuration Methods

This variable contains the same data structure as Configuration Methods, but it indicates which of the Configuration Methods supported by the device are enabled.

Setting this attribute on an AP or STA through the UPnP Management Interface can be used to disable or re-enable a particular method for that device.

If the bit in Permitted Configuration Methods corresponding to a particular method is set to zero, the device SHALL signal an error rather than participate in a Registration Protocol exchange using that method. This setting has no effect on the use of that method by external Registrars when the device is an AP. If a Configuration Method is disabled using Permitted Configuration Methods, only the enabled methods are reported in the discovery messages (probe request, probe response, M1, and M2).

Portable Device

This variable indicates that the device is portable. It may be used to help determine if it will be possible to perform actions such as touching devices together for NFC-based configuration.

Power Level

This variable indicates the power level in mW that the radio on the device is set to transmit. Power Level has a range of 1-100.

Primary Device Type

This attribute contains the primary type of the device. Its format follows:

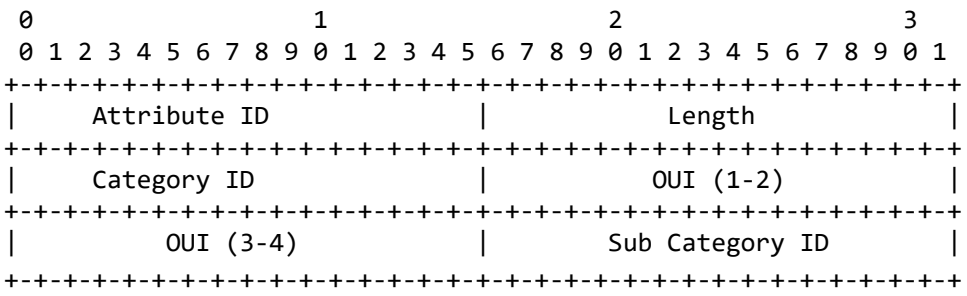

Figure 22 – Primary Device Type format

Vendor-specific sub-categories are designated by setting the OUI to the value associated with that vendor. Note that a four-byte subdivided OUI is used. For the predefined values, the Wi-Fi Alliance OUI of 00 50 F2 04 is used. The predefined values for Category ID and Sub Category ID are provided in the next table. There is no way to indicate a vendor-specific main device category. The OUI applies only to the interpretation of the Sub Category. If a vendor does not use sub categories for their

OUI, the three-byte OUI occupies the first three bytes of the OUI field and the fourth byte is set to zero.

Table 41 – Primary Device Type

Category	ID Value	Sub Category	ID Value
Computer	1	PC	1
		Server	2
		Media Center	3
		Ultra-mobile PC	4
		Notebook	5
		Desktop	6
		MID (Mobile Internet Device)	7
		Netbook	8
		Tablet	9
		Ultrabook	10
Input Device	2	Keyboard	1
		Mouse	2
		Joystick	3
		Trackball	4
		Gaming controller	5
		Remote	6
		Touchscreen	7
		Biometric reader	8
		Barcode reader	9
Printers, Scanners, Faxes and Copiers	3	Printer or Print Server	1
		Scanner	2
		Fax	3
		Copier	4
		All-in-one (Printer, Scanner, Fax, Copier)	5
Camera	4	Digital Still Camera	1
		Video Camera	2
		Web Camera	3
		Security Camera	4
Storage	5	NAS	1

Category	ID Value	Sub Category	ID Value
Network Infrastructure	6	AP	1
		Router	2
		Switch	3
		Gateway	4
		Bridge	5
Displays	7	Television	1
		Electronic Picture Frame	2
		Projector	3
		Monitor	4
Multimedia Devices	8	DAR	1
		PVR	2
		MCX	3
		Set-top box	4
		Media Server/Media Adapter/Media Extender	5
		Portable Video Player	6
Gaming Devices	9	Xbox	1
		Xbox360	2
		Playstation	3
		Game Console/Game Console Adapter	4
		Portable Gaming Device	5
Telephone	10	Windows Mobile	1
		Phone – single mode	2
		Phone – dual mode	3
		Smartphone – single mode	4
		Smartphone – dual mode	5
Audio Devices	11	Audio tuner/receiver	1
		Speakers	2
		Portable Music Player (PMP)	3
		Headset (headphones + microphone)	4
		Headphones	5
		Microphone	6
		Home Theater Systems	7

Category	ID Value	Sub Category	ID Value
Docking Devices	12	Computer docking station	1
		Media kiosk	2
Others	255		

PSK Current

This variable represents the number of allocated PSKs on the AP.

PSK Max

This variable represents the maximum number of PSKs supported by the AP.

Public Key

This variable represents the sender's Diffie-Hellman public key. The Length of the attribute indicates the size of the key as well as the specific generator and prime. For 1536-bit Diffie-Hellman (the default), these values are specified in Section 7.3. The binary presentation of the Public Key value is padded with zeros from the left, so that the attribute length is the maximum length for the specific DH group, i.e., in the case of the default 1536-bit group, the Public Key attribute length is 192.

Public Key Hash

This variable contains the first 160 bits of the SHA-256 hash of a public key.

R-Hash1

This is the HMAC-SHA-256 hash of the first half of the device password and the Registrar's first secret nonce.

R-Hash2

This is the HMAC-SHA-256 hash of the second half of the device password and the Registrar's second secret nonce.

R-SNonce1

This is the first nonce used by the Registrar with the first half of the device password

R-SNonce2

This is the second nonce used by the Registrar with the second half of the device password.

Radio Enabled

This variable indicates the status of the radio interface on the device.

Reboot

This variable is a request to reboot the device.

Registrar Configuration Methods

This subelement contains the Configuration Methods supported by a Registrar. An AP includes this field in Beacon and Probe Response frames so that Enrollees can discover

the Configuration Methods supported by the AP's internal Registrar without performing discovery by use of messages M1 and M2.

Registrar Current

This variable gives the number of Registrars that have an association with the device (typically the AP).

Registrar Established

This variable gives an indication if the device has previously created an association with a Registrar. The typical application would be for an Access Point to indicate that the configuration has been accepted or set. This field is TRUE if it has an external Registrar association established.

Registrar List

This variable is a list of Registrar UUIDs and associated Device Names. Each entry in the list begins with the binary UUID (16 bytes) of a Registrar followed by its Null-terminated Device Name.

Registrar Max

This variable indicates the capacity of associated Registrars for the device (typically an AP).

Registrar Nonce

The Registrar Nonce component is a randomly generated binary value that is created by the Registrar for setup.

Rekey Key

This variable contains a 256-bit key used for rekeying. When the Device Password ID is set to Rekey, it means that the Registrar should use the rekeying key of the Enrollee as the device password rather than the PIN.

Request Type

The Request Type component specifies the mode in which the device will operate in for this setup exchange. If the device is an Enrollee, it may send only discovery messages or it may also request that the Registrar proceed with opening a data connection. This protocol allows Enrollees to more efficiently discover devices on the network.

If the device indicates that it intends to engage setup either as a Registrar or an Enrollee, the Access Point continues to indicate that it will operate as an AP in the response. The Request Type attribute is carried throughout the 802.1X data channel setup process in the Wi-Fi Simple Configuration IE.

There are two sub-types of Registrars: WLAN Manager Registrar indicates that this Registrar intends to manage the AP or STA settings using UPnP. It will derive a UPnP AP or STA Management key. The ordinary Registrar type indicates that this Registrar does not intend to subsequently manage the Enrollee's settings. APs shall not derive AP Management Keys for an ordinary Registrar. If a Registrar does not intend to be a WLAN Manager Registrar, it should set the Request Type to Registrar. Doing so avoids needlessly consuming resources on the AP.

Table 42 – Request Type

Request Type Value	Description
0x00	Enrollee, Info only
0x01	Enrollee, open 802.1X
0x02	Registrar
0x03	WLAN Manager Registrar

Request to Enroll

This optional subelement in the WSC IE in Probe Request or M1 indicates the desire to enroll in the network by setting its value to TRUE. If the Registrar gets this subelement it can use this as a trigger that a device wants to enroll (maybe an indication can be shown to the user). The device shall set it to FALSE after the registration protocol completion.

Requested Device Type

This attribute contains the requested device type of a P2P device.

This attribute allows a device to specify the Primary Device Type or the Secondary Device Type of other devices it is interested in. Only a device that receives a Probe Request containing a WSC IE with this attribute and with a Primary Device Type or Secondary Device Type that matches the Requested Device Type will respond with a Probe Response.

Its format and contents is identical to the ‘Primary Device Type’ attribute.

Both the Category ID and Sub Category ID can be used as a filter. If only looking for devices with a certain Category ID, the OUI and Sub Category ID fields will have to be set to zero.

Response Type

The Response Type component specifies the operational mode of the device for this setup exchange. The Response Type IE is carried throughout the 802.1X data channel setup process.

Table 43 – Response Type

Response Type Value	Description
0x00	Enrollee, Info only
0x01	Enrollee, open 802.1X
0x02	Registrar
0x03	AP
0x04	Reserved (for IBSS with Wi-Fi Protected Setup Specification)

RF Bands

This attribute is used to indicate a specific RF band that is utilized during message exchange to permit end points and proxies to communicate over a consistent radio interface. It is also used in Beacons and Probe Responses to indicate all RF Bands that an AP supports, in which case it is a bitwise OR of the values in the table below. It may also be used as an optional attribute in a Credential or Encrypted Settings to indicate a specific (or group) of RF bands to which a setting applies, or as an optional attribute in an out-of-band provisioning method such as NFC to indicate the RF Band relating to a channel or the RF Bands in which an AP is operating with a particular SSID.

Table 44 – RF Bands

RF Band Value	Description
0x01	2.4GHz
0x02	5.0GHz
0x04	60GHz

Secondary Device Type List

This attribute contains a list of secondary device types supported by the device. OUI and standard values for Category ID and Sub Category ID fields are defined in the Primary Device Type attribute. The Secondary Device Type List format follows:

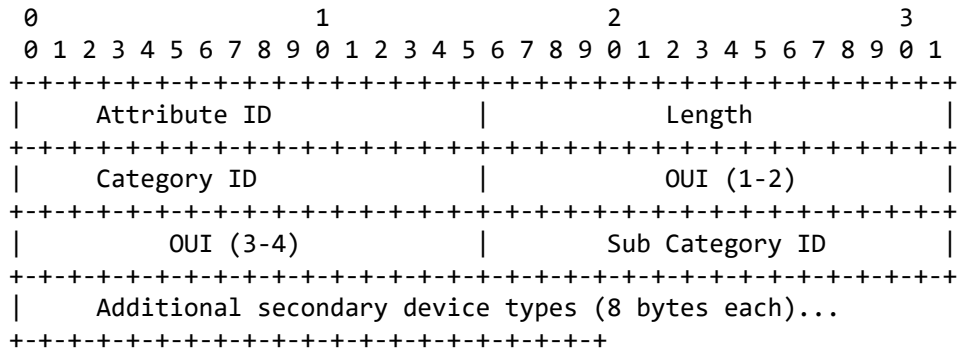

Figure 23 – Secondary Device Type List

Selected Registrar

This field indicates that a Registrar has been selected by a user.

Examples of selecting a registrar include:

- Navigating to an embedded UI on the AP to enroll a device
- Pushing the button on the AP
- Navigating to a UI on an External Registrar to enroll a device.

If a user selects an Internal Registrar in AP and activates the registration protocol to accept new Enrollee, the Internal Registrar shall set the Selected Registrar attributes in the beacon and probe response frame to TRUE. In the case of External Registrar, External Registrar shall send a SetSelectedRegistrar UPnP action to AP with Selected Registrar attribute TRUE when the user has expressed an interest in adding a device. An example of this would be navigating to a UI on an External Registrar to enroll a device. After the AP receives said SetSelectedRegistrar UPnP action with Selected Registrar TRUE, the AP incorporates Selected Registrar attribute set to TRUE in its beacons and probe responses.

The AP shall update its Selected Registrar attribute based on the state of all active Registrars. This attribute may need to be changed when an External Registrar notifies the AP with the SetSelectedRegistrar UPnP action or becomes disconnected.

Selected Registrar Configuration Methods

This attribute has the same values that Configuration Methods have. It is used in Probe Response messages to convey the Configuration Methods of the selected Registrar.

Serial Number

The Serial Number component identifies the serial number of the Enrollee.

Setting Delay Time

Estimate of the time (in seconds) the device will take to apply the settings and connect to the network after receiving the settings in message M8.

SSID

This attribute represents the Service Set Identifier or network name. This is used by the client to connect to the wireless network. The SSID attribute value shall match with the value of the SSID, i.e., it does not include zero padding and the length of the attribute is the same as that of the SSID used in the network.

Symmetric Key

This attribute contains a symmetric key.

Total Networks

This attribute contains the number of WLAN networks supported by the device.

UUID-E

The universally unique identifier (UUID) element is a unique GUID generated by the Enrollee. It uniquely identifies an operational device and should survive reboots and resets. The UUID is provided in binary format. If the device also supports UPnP, then the UUID corresponds to the UPnP UUID.

UUID-R

The universally unique identifier (UUID) element is a unique GUID generated by the Registrar. It uniquely identifies an operational device and should survive reboots and resets. The UUID is provided in binary format. If the device also supports UPnP, then the UUID corresponds to the UPnP UUID.

Vendor Extension

This variable permits vendor extensions in the Wi-Fi Simple Configuration TLV framework. The Vendor Extension figure illustrates the implementation of vendor extensions. Vendor ID is the SMI network management private enterprise code.

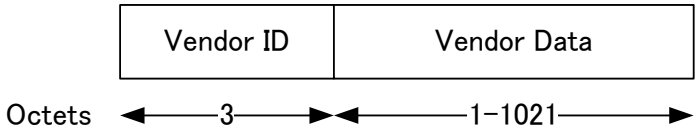

Figure 24 – Vendor Extension Encapsulation

Version

Deprecated Version mechanism. This attribute is always set to value 0x10 (version 1.0) for backwards compatibility. Version 1.0h of the specification did not fully describe the version negotiation mechanism and version 2.0 introduced a new subelement (Version2) for indicating the version number to avoid potential interoperability issues with deployed 1.0h-based devices.

Version2

The Version2 field specifies the version Wi-Fi Simple Configuration implemented by the device sending this attribute. The one-byte field is broken into a four-bit major part using the top MSBs and four-bit minor part using the LSBs. As an example, version 3.2 would be 0x32. This subelement was added in the specification version 2.0 and if the subelement is not included in a message, the transmitter of the message is assumed to use version 1.0.

WEP Transmit Key

This attribute identifies the Key Index that is used as the AP transmit key for WEP configurations.

Wi-Fi Simple Configuration State

For a Station Enrollee the 'Wi-Fi Simple Configuration State' attribute in WSC IE contained in Message M1 shall always have the value 'Not Configured' (0x01).

For an Access Point, the Wi-Fi Simple Configuration State attribute in WSC IEs contained in beacon, probe response and message M1 indicates if the device is configured. If an AP is shipped from the factory in the “Not Configured” state (Wi-Fi Simple Configuration State set to 0x01), then the AP shall transition to the “Configured” state (Wi-Fi Simple Configuration State set to 0x02) if any of the following occur:

1. Configuration by an External Registrar.

The AP sends the WSC_Done message in the External Registrar configuration process.

2. Automatic configuration by Internal Registrar.

The AP receives the WSC_Done response in the Enrollee Registration Process from the first Enrollee.

Note: The Internal Registrar waits until successful completion of the protocol before applying the automatically generated credentials to avoid an accidental transition from “Not Configured” to “Configured” in the case that a neighboring device tries to run WSC before the real enrollee, but fails. A failed attempt does not change the configuration of the AP, nor the Wi-Fi Simple Configuration State.

3. Manual configuration by user.

A user manually configures the AP using whatever interface(s) it provides to modify any one of the following:

- the SSID,
- the encryption algorithm
- the authentication algorithm
- any key or pass phrase

If the AP is shipped from the factory in the “Not Configured” state (Wi-Fi Simple Configuration State set to 0x01), then a factory reset shall revert the Wi-Fi Simple Configuration State to “Not Configured”.

If the AP is shipped from the factory pre-configured with WPA2-Personal or Mixed Mode and a randomly generated key, the Wi-Fi Simple Configuration State may be set to “Configured” (0x2) to prevent an External Registrar from overwriting the factory settings. A factory reset shall restore the unit to the same configuration as when it was shipped.

Note that a Station acting as an Enrollee should proceed with the Registration Protocol regardless if the Access Point is in ‘Configured’ state or ‘Not Configured’ state (for instance in out of the box mode if the AP is shipped from the factory in the ‘Not Configured’ state). In other words the STA Enrollee may ignore the actual value of the Wi-Fi Simple Configuration State attribute received in beacons or probe responses as long as the value is valid.

Table 45 – Wi-Fi Simple Configuration State

Value	Description
0x00	Reserved
0x01	Not configured
0x02	Configured
0x03-0xFF	Reserved

X.509 Certificate Request

This attribute contains an X.509 certificate request payload as specified in RFC 2511.

X.509 Certificate

This attribute contains an X.509 certificate.

13 Protocol Implementation Conformance Specification (PICS)

The following table summarizes the potential features of an implementation of WSC and defines the mandatory and optional set of these features. The following notation is used

M – Mandatory Feature

O – Optional Feature

n/a – Not applicable to the specific device type

d – Deprecated Feature with possible negative testing; shall not be supported

nt – Deprecated and not tested

The Conditional column in WSC – Core WSC Feature which shall be implemented for WPS certification

AP-Web – A HTTP interface to the AP Internal Registrar

AP-ER – A AP supporting an External Registrar

NFC – Support for Near Field Communications

Table 46 is used for conditional features. Conditional features are dependent on the higher level inclusion of an optional feature (like NFC) and then define the implementation requirements for the dependent features. The following notation is used for the conditional features:

WSC – Core WSC Feature which shall be implemented for WPS certification

AP-Web – A HTTP interface to the AP Internal Registrar

AP-ER – A AP supporting an External Registrar

NFC – Support for Near Field Communications

Table 46 – WSC PICS

Requirement	WSC 2.0 Section	Condition	AP	STA	STA+ER	ER Only
WSC 2.0 Core Features (WSC)		**WSC**	**O**	**O**	**O**	**n/a**
Support Registrar Function	4	WSC	**M**	**O**	**M**	**M**
Support Enrollee Function	4	WSC	**M**	**M**	**n/a**	**n/a**
Support Internal Registrar or External Registrar	4	WSC	**M**	**n/a**	**n/a**	**n/a**
Support WSC 2.0 and WSC 1.0	7.9	WSC	**M**	**M**	**M**	**M**
Pushbutton Configuration:	6.2.4, 11	WSC	**M**	**O**	**O**	**O**
PIN Configuration:	6.2.1, 6.2.3,	WSC	**M**	**M**	**M**	**M**
8 Digit PIN	4.3.2	WSC	**M**	**M**	**M**	**M**
4 Digit PIN	4.3.2	WSC	**M**	**M**	**M**	**M**
AP Initial Out-of-Box Setup	5.1	**WSC**	**M**	**n/a**	**n/a**	**n/a**
Unique Initial SSID	5.1	WSC	**O**	**n/a**	**n/a**	**n/a**

Requirement	WSC 2.0 Section	Condition	AP	STA	STA+ER	ER Only
WSC Enabled Out-of-Box	5.1	WSC	**M**	**n/a**	**n/a**	**n/a**
WPA2-AES Default for WSC	5.1	WSC	**M**	**n/a**	**n/a**	**n/a**
WPA2-AES Enabled Out-of-Box	5.1	WSC	**O**	**n/a**	**n/a**	
Able to turn WPA2 on/off	5.1	WSC	**O**	**n/a**	**n/a**	**n/a**
Able to configure WSC for Mixed Mode	5.1	WSC	**O**	**n/a**	**n/a**	**n/a**
Able to configure WSC for WPA/TKIP	5.1	WSC	**d**	**n/a**	**n/a**	**n/a**
Able to configure WSC for WEP	5.1	WSC	**d**	**n/a**	**n/a**	**n/a**
Able to set MAC filtering and use WSC	5.1	WSC	**d**	**n/a**	**n/a**	**n/a**
Support of User Reset to Defaults	5.1	WSC	**O**	**n/a**	**n/a**	**n/a**
HTTP Interface to Internal Registrar in AP (AP-WEB)	5.1	**WSC**	**O**	**n/a**	**n/a**	**n/a**
Registrar Pages protected by TLS	5.1	AP-Web	**M**	**n/a**	**n/a**	**n/a**
HTTP Basic Auth for Registrar	5.1	AP-Web	**d**	**n/a**	**n/a**	**n/a**
Digest Auth with response-auth	5.1	AP-Web	**M**	**n/a**	**n/a**	**n/a**
AP Device Unique Password	5.1	AP-Web	**O**	**n/a**	**n/a**	**n/a**
AP With an External Registrar (AP-ER)	5.2	**WSC**	**M**	**n/a**	**n/a**	**n/a**
Secure Management Interface to AP	5.2	AP-ER	**M**	**n/a**	**M**	**M**
Support 3 External Registrars	5.2	AP-ER	**M**	**n/a**	**M**	**M**
Add new External Registrars	5.2	AP-ER	**M**	**n/a**	**M**	**M**
Revoke other External Registrar	5.2	AP-ER	**O**	**n/a**	**O**	**O**
Support of UPnP WFADevice:1	5.2	AP-ER	**M**	**n/a**	**M**	**M**
EAP setup of External Registrar	5.2.1	AP-ER	**M**	**n/a**	**n/a**	**n/a**
External Registrar introduction even after AP Configuration	5.2.1	AP-ER	**M**	**n/a**	**n/a**	**n/a**
In-Band Setup Using Multiple Registrars	6.3	AP-ER	**M**	**M**	**M**	**M**
UPnP WFAWLANConfig:1 (UPnP-C)	5.2	**AP-ER**	**M**	**n/a**	**M**	**M**
UPnP Transport of Registration Protocol	5.2, 6.2, 6.3	AP-ER	**M**	**n/a**	**M**	**M**
UPnP ER Setup of an AP	5.2	AP-ER	**M**	**n/a**	**M**	**M**
UPnP ER Setup of a STA	6.2, 6.3	AP-ER	**M**	**n/a**	**M**	**M**
GetDeviceInfo	UPNP-C	AP-ER	**M**	**n/a**	**M**	**M**
PutMessage	UPNP-C	AP-ER	**M**	**n/a**	**M**	**M**
SetSelectedRegistrar	UPNP-C	AP-ER	**M**	**n/a**	**M**	**M**
PutWLANResponse	UPNP-C	AP-ER	**M**	**n/a**	**M**	**M**

Requirement	WSC 2.0 Section	Condition	AP	STA	STA+ER	ER Only
In-band STA Setup using Standalone AP/Registrar:	6.1	WSC	**M**	**n/a**	**n/a**	**n/a**
Secure Setup of Legacy Enrollee	6.4	WSC	**M**	**n/a**	**M**	**M**
Registrar Display of SSID and Passphrase	6.4	WSC	**M**	**n/a**	**O**	**O**
WSC Registration Protocol	7	**WSC**	**M**	**M**	**M**	**M**
Key Derivation:KDK:	7.3	WSC	**M**	**M**	**M**	**M**
Key Derivation:AuthKey:	7.3	WSC	**M**	**M**	**M**	**M**
Key Derivation:KeyWrapKey:	7.3	WSC	**M**	**M**	**M**	**M**
Key Derivation:EMSK:	7.3	WSC	**O**	**O**	**O**	**O**
Key Derivation:MgmtAuthKey:	7.3	WSC	**O**	**O**	**O**	**O**
Key Derivation:MgmtEncKey:	7.3	WSC	**O**	**O**	**O**	**O**
Proof-of-possession of Device Password:	7.4	WSC	**M**	**M**	**M**	**M**
PIN Checksums:	7.4.1	WSC	**M**	**M**	**M**	**M**
Key Wrap Algorithm:	7.5	WSC	**M**	**M**	**M**	**M**
Rekeying:	Annex E	WSC	**O**	**O**	**O**	**O**
EAP Transport of Registration Protocol:	7.7	WSC	**M**	**M**	**M**	**n/a**
Beacon Frame:	8.2.1	WSC	**M**	**M**	**M**	**n/a**
Association Request and Reassociation Request:	8.2.2	WSC	**M**	**M**	**M**	**n/a**
Association Response and Reassociation Response:	8.2.3	WSC	**M**	**M**	**M**	**n/a**
Active Probe for PBC	8.2.4, 11.3	WSC	**n/a**	**M**	**M**	**n/a**
Active Probe for PIN Mode	8.2.4	WSC	**n/a**	**O**	**O**	**n/a**
WSC IE Processing in Probe Request (PBC)	8.2.4	WSC	**M**	**M**	**M**	**M**
WSC IE Processing in Probe Request (PIN)	8.2.4	WSC	**M**	**M**	**M**	**M**
WSC IE Processing in Probe Response	8.2.5	WSC	**M**	**M**	**M**	**M**
Message M1:	8.3.1	WSC	**M**	**M**	**M**	**M**
Message M2:	8.3.2	WSC	**M**	**M**	**M**	**M**
Message M2D:	8.3.3	WSC	**M**	**M**	**M**	**M**
Message M3:	8.3.4	WSC	**M**	**M**	**M**	**M**
Message M4:	8.3.5	WSC	**M**	**M**	**M**	**M**
Message M5:	8.3.6	WSC	**M**	**M**	**M**	**M**
Message M6:	8.3.7	WSC	**M**	**M**	**M**	**M**
Message M7:	8.3.8	WSC	**M**	**M**	**M**	**M**
Message M8:	8.3.9	WSC	**M**	**M**	**M**	**M**
WSC_ACK Message:	8.3.10	WSC	**M**	**M**	**M**	**M**
WSC_NACK Message:	8.3.11	WSC	**M**	**M**	**M**	**M**
WSC_Done Message:	8.3.12	WSC	**M**	**M**	**M**	**M**
Reassembly of WSC IE	7.7.1	WSC	**M**	**M**	**M**	**n/a**
Reassembly of EAP Fragments	7.7.1	WSC	**M**	**M**	**M**	**n/a**
Fragmentation of EAP Frames	7.7.1	WSC	**O**	**O**	**O**	**n/a**
SetSelectedRegistrar Message:	8.4.1	WSC	**M**	**n/a**	**M**	**M**
AuthorizedMACs subelement	8.4.1, 12	WSC	**M**	**O**	**M**	**M**
Support for Near Field Communications (NFC)	10	**WSC**	**O**	**O**	**O**	**O**
NFC Interface	10.1	NFC	**M**	**O**	**M**	**M**
Password Token Usage Model	10.1.1	NFC	**M**	**O**	**M**	**M**
Configuration Token Usage Model	10.1.2	NFC	**M**	**O**	**M**	**M**

Requirement	WSC 2.0 Section	Condition	AP	STA	STA+ER	ER Only
Connection Handover Usage Model	10.1.3	NFC	**M**	**O**	**M**	**M**
In-band Setup using a Standalone AP/Registrar	6.1	NFC	**M**	**n/a**	**n/a**	**n/a**
Deprecated Features		--	**nt**	**nt**	**nt**	**nt**
Secure Setup with Legacy AP	--	WSC	**nt**	**n/a**	**nt**	**nt**
No-Security Out-of-Box Setup - Standalone AP	--	WSC	**nt**	**n/a**	**nt**	**nt**
Removing Members from the WLAN:	Annex E	WSC	**nt**	**n/a**	**nt**	**nt**
Guest access	Annex E	WSC	**nt**	**n/a**	**nt**	**nt**
Re-keying credentials	Annex E	WSC	**nt**	**n/a**	**nt**	**nt**
Adding additional AP or Router	Annex E	WSC	**nt**	**n/a**	**nt**	**nt**
Change SSID, radio channels, etc. (UPnP)	Annex E	WSC	**nt**	**n/a**	**nt**	**nt**
In-Band M2	Annex A	WSC	**nt**	**n/a**	**nt**	**nt**
Out-of-Band M2	Annex A	WSC	**nt**	**n/a**	**nt**	**nt**
USB Based Configuration	Annex G	WSC	**nt**	**n/a**	**nt**	**nt**
GetAPSettings	UPNP-C	UPnP-C	**nt**	**n/a**	**nt**	**nt**
SetAPSettings	UPNP-C	UPnP-C	**nt**	**n/a**	**nt**	**nt**
DelAPSettings	UPNP-C	UPnP-C	**nt**	**n/a**	**nt**	**nt**
GetSTASettings	UPNP-C	UPnP-C	**nt**	**n/a**	**nt**	**nt**
SetSTASettings	UPNP-C	UPnP-C	**nt**	**n/a**	**nt**	**nt**
DelSTASettings	UPNP-C	UPnP-C	**nt**	**n/a**	**nt**	**nt**
RebootAP	UPNP-C	UPnP-C	**nt**	**n/a**	**nt**	**nt**
RebootSTA	UPNP-C	UPnP-C	**nt**	**n/a**	**nt**	**nt**
ResetAP	UPNP-C	UPnP-C	**nt**	**n/a**	**nt**	**nt**
ResetSTA	UPNP-C	UPnP-C	**nt**	**n/a**	**nt**	**nt**

Annex A - Out-of-Band Channel Considerations

This section provides guidelines and suggestions relating to the use of out-of-band channels with Wi-Fi Simple Configuration. Its purpose is to highlight important security issues related to the properties of various channel types that can be used in the Wi-Fi Simple Configuration architecture.

Out-of-band channels can be used to deliver one or both of Registration Protocol messages M1 and M2. Depending upon the Registrar policy and the data privacy characteristics of the out-of-band channel, configuration provided in M2 may or may not be encrypted. Unless both M1 and M2 are sent over a write-protected out-of-band channel, it is assumed that the out-of-band channel provides strong assurance of data privacy. If the out-of-band channel is bidirectional, it is strongly recommended to use the channel for both M1 and M2. Table A1 and the discussion in this section examines the implications of using an out-of-band channel for either M1, M2, or both.

Table 47 – Out-of-Band Channels Use Cases

	In-band M1	M1
In-band M2	Case A	Case B
Out-of-band M2	Case C	Case D

- Case A: this is the in-band case. It requires that the user type (or otherwise convey) a device password known by the Enrollee into the Registrar. If the attacker has sent M1 and it subsequently eavesdrops the corresponding M2, it can attempt a brute force attack against the Enrollee's device password (half at a time).

  If this password is a fixed value printed on a label, it will be susceptible to an active attacker that runs the Registration Protocol multiple times to incrementally discover the entire device password through brute force attack. Therefore, it is strongly recommended that the password be randomly generated by the Enrollee for each Registration. This implies that Enrollees without an out-of-band channel should include a display or equivalent mechanism for showing the dynamic password. Nevertheless, fixed, label-based passwords may be used for low-cost devices.

  It is also possible to use a hybrid solution for Case A, where an out-of-band channel is used to configure a long fixed or dynamic device password. Once the device password is configured, the in-band protocol can be run using that password. If the Out-of-Band Device Password attribute is used in this case, the hash of the Enrollee's public key is conveyed along with the device password on the out-of-band channel.

  This significantly strengthens the security of the solution, because the Registrar will not send M2 unless M1's public key matches the hash. If an attacker is able to eavesdrop the Out-of-Band Device Password, the public key hash prevents

them from masquerading as the Enrollee and thereby gaining access to the WLAN.

- Case B: The Registrar is given M1 over the out-of-band channel, so it has a basis for trusting the Enrollee and sending a response encrypted with the Enrollee's public key. Because M2 is sent over the in-band channel, however, the Enrollee has no basis for validating M2 unless it is authenticated by a device password. Therefore, this case should be handled the same as Case A.

  Case B can also include a hybrid mode, where the Enrollee sends its password along with M1 (embedded within M1 or sent separately) across the private out-of-band channel. If bandwidth limitations preclude sending the entire M1 message across the out-of-band channel, then the Out-of-Band Device Password attribute can be sent instead. If the password is sent over the out-of-band channel, the Registrar can proceed with M2 through M8 without requiring the user to manually enter the password.

  The Out-of-Band Device password attribute also includes a hash of the Enrollee device's public key, which the Registrar can use to strongly authenticate the Enrollee regardless of the privacy of the out-of-band channel.

- Case C: In this case, M1 could have come from an attacker, but M2 is protected from the attacker by the out-of-band channel. There is no need for the user to manually enter a device password, because the out-of-band channel provides a basis for trust between the Registrar and Enrollee.

  The Registrar trusts the Enrollee because it knows that only the Enrollee has received M2. The Enrollee trusts the Registrar because it receives M2 across the private channel. In this case, the Registrar delivers configuration data in M2, and the Registration Protocol terminates at that point. Encryption of the configuration and Credential in M2 is optional when it is delivered across the private out-of-band channel.

- Case D: In this case, both M1 and M2 are authenticated by the out-of-band channel. There is no need for the user to enter a device password in this case, and the Registration Protocol terminates with M2. Furthermore, in this case the out-of-band channel need not provide data privacy, because the ConfigData can be encrypted using keys derived from the Diffie-Hellman exchange.

Annex B - Security Analysis of Registration Protocol

The Registration Protocol is believed to be secure against both eavesdropping and active attacks, if the device password is used only for a single instance of the Registration Protocol. This fact implies that the Enrollee should be capable of displaying a freshly generated random password.

If a fixed, label-based password is used, this protocol is vulnerable to a brute force or dictionary attack on the password by an active attacker posing as an Enrollee. Susceptibility to this attack will depend upon the length of the device password. To perform the attack, the active attacker can induce the Registrar to perform the Diffie-Hellman exchange with it and send R-Hash1 and ENC(R-S1) in M4. Given this reality, the attacker can discover PSK1 by brute-force calculation if the first half of the device password is relatively short. By running a second round of the protocol with the same password, the attacker can discover the rest of the device password (provided that the password is relatively short).

Devices with label-based passwords will have limited security unless those passwords are quite long (and thus inconvenient to enter manually). Therefore, devices with label-based passwords are strongly encouraged to also support another out-of-band channel such as NFC.

Wi-Fi Simple Configuration assumes that a person in physical possession of the Registrar during the setup process is the de facto owner who is authorized to extend Domain membership to other devices. Wi-Fi Simple Configuration also assumes that a person in physical possession of the Enrollee device is the de facto owner of that device and is authorized to use it. The registration protocol uses the MAC address that the Enrollee includes in message M1 for key derivation and also in message M8 for credential binding. Successful completion of the registration protocol proves that both the Enrollee and the Registrar have used the same Device Password and it becomes the basis for the Enrollee to claiming ownership of the MAC address. It is a well-known fact that a MAC address can be easily spoofed. This weakness could be exploited in the form of an insider attack where an otherwise legitimate user may impersonate another user with the purpose of getting someone else’s credential. For networks hosting a shared credential – for instance WPA2-Personal as used in many home environments – this does not present any concern. However for networks hosting unique per-station credentials – for instance WPA2-Enterprise networks – this may become a concern. The countermeasure is fairly simple if the network administrators ensure that the Enrollee’s MAC address is not used as a substitute for identifying the user and if the assumption stated above that the person in physical possession of the Enrollee device is the de facto owner of the device is confirmed to be true.

Out-Of-Band Channels

Wi-Fi Simple Configuration can use multiple types of out-of-band channels. This section discusses important characteristics of out-of-band channels and how to use them. The Wi-Fi Simple Configuration architecture is easily extensible to support a variety of out-of-band channels. However, it should be noted that interoperability

increases if the number of out-of-band channels used by Wi-Fi Simple Configuration is kept small.

Out-of-band Channel Characteristics

Resistance to man-in-the-middle attack

This is a mandatory security property of any out-of-band channel. If an Adversary can intercept and replace messages on the out-of-band channel without detection, that channel should be considered equivalent to an in-band channel for security purposes.

Physical proximity

Another important characteristic of a good out-of-band channel is that it allows the user to unambiguously indicate which two devices are engaged in the Wi-Fi Simple Configuration exchange.

Resistance to eavesdropping

Out-of-band channels have differing degrees of resistance to eavesdropping (privacy). For example, physical wires are more resistant to eavesdropping attacks than are infrared, near-field communications (NFC), or RFID. Out-of-band channels shall be highly resistant to eavesdropping because the public key provided by the Enrollee in M1 is vulnerable to spoofing.

Channel data capacity

Channels such as point-to-point wired connections typically have ample capacity to transmit large quantities of data. Others, such as RFID or consumer IR, may have very limited capacity. The out-of-band channel shall have sufficient data capacity and transfer rates to accommodate the Wi-Fi Simple Configuration data exchange with minimal user experience impact.

Annex C - Out-of-band Setup Using a Standalone AP/Registrar

Note the Registrar has knowledge about the matching out-of-band capabilities from the Discovery data and is thus capable of guiding the user accordingly.

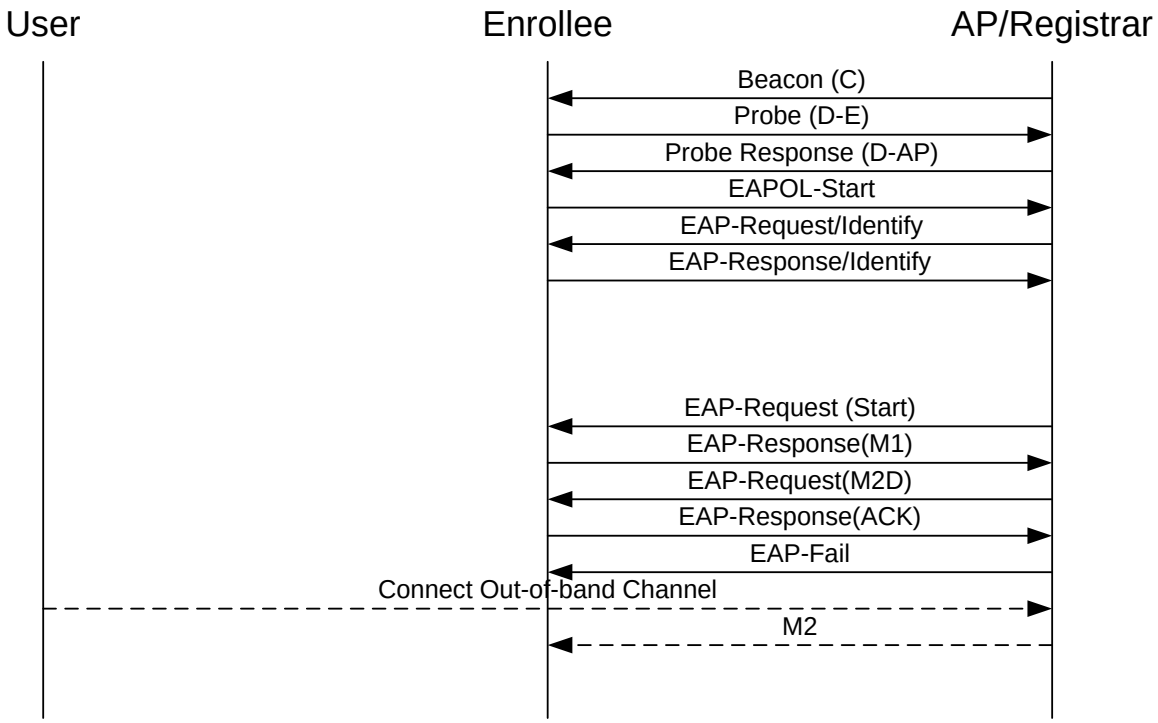

Figure 25 – Out-of-band Setup Using an AP/Registrar

Setup steps

1. The Enrollee discovers a Wi-Fi Simple Configuration AP sends its Discovery data in a probe request. The Registrar/AP responds with its own Discovery data in the probe response.
2. The Enrollee sends M1 using 802.1X.
3. The AP/Registrar responds with an M2D message.
4. The Enrollee acknowledges M2D, and the AP/Registrar sends EAP-Failure.
5. The user connects the out-of-band channel.
6. The AP/Registrar sends M2 with ConfigData to the Enrollee across the out-of-band channel.

Annex D - Out-of-band Setup Using an External Registrar

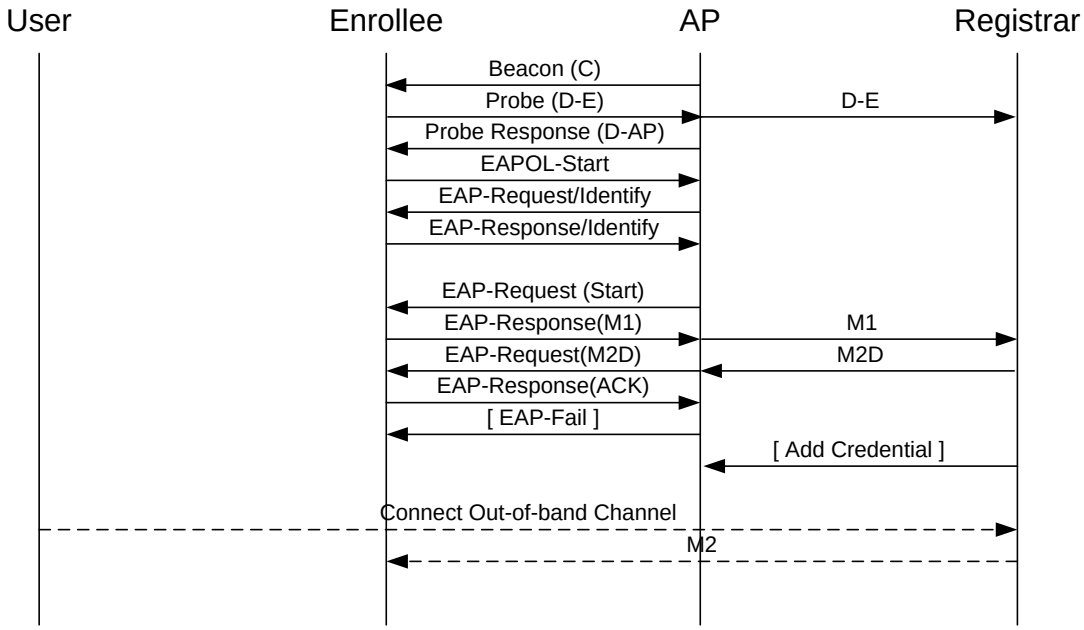

Figure 26 – Out-of-band Setup Using External Registrar

Figure 26 illustrates an external Registrar Registering an Enrollee via an out-of-band channel into a network with a Wi-Fi Simple Configuration AP.

1. The Enrollee sends its Discovery data in a probe request to a Wi-Fi Simple Configuration AP. The AP sends its own Discovery data in the probe response and forwards the Enrollee's Discovery message on to the external Registrar.
2. The Enrollee initiates 802.1X authentication and exchanges M1 and M2D with the external Registrar.
3. The Registrar displays information about the Enrollee extracted from the M1 message sent during the Discovery procedure and awaits confirmation before proceeding with the Invitation.
4. The user establishes the out-of-band channel. The Registrar may provide guidance concerning the channel to use based on information from the Discovery message.
5. If the WLAN requires separate keys for different clients, the Registrar needs to use the Management Interface to add a Credential for the Enrollee to the AP. This requirement implies that the Registrar shall be a WLAN Manager Registrar. If the WLAN Manager Registrar is managing multiple APs in the same Domain, it may configure all of them with the new Credential at this point.
6. The Registrar sends the Credential and configuration to the Enrollee in M2 across the selected out-of-band channel.

Annex E - Secondary Usage Models

This section describes secondary usage models that are not currently supported by certification testing.

Removing Members from the WLAN

If the AP supports per-device WPA keys, the Registrar can invoke the UPnP action DelAPSettings to remove a Member device from the WLAN. If a shared WPA key is configured, re-keying can be used.

Guest access

To establish guest access, a guest device should be given a unique Credential that can be revoked by the Registrar using DelAPSettings without disrupting the connections of other devices. It is also possible to assign a Key Lifetime to have the Credential automatically expire. It is necessary for guest devices to have separate WPA-Personal keys from other Member devices for this approach to work. Re-keying can also be used to support guest access scenarios (refer to the next paragraph).

Re-keying credentials

“Rekeying” paragraph in this section describes how to re-key credentials without requiring the user to go through a manual re-introduction process. This method can be used to support certain guest access scenarios and individual removal of Member devices without requiring the AP to support multiple WPA-Personal keys. The Registrar simply deletes the Rekey-PSK corresponding to the guest device whose access needs to be revoked. The Registrar next changes the AP’s WPA2-PSK through the Management Interface (this requires the Registrar to be a WLAN Manager Registrar). This technique results in breaking all existing connections of Enrollees that support re-keying to automatically re-authenticate and receive the new PSK Credential based on their Rekey-PSK. Manual intervention is required only to reconfigure the keys in those devices that do not support the re-keying option.

Of course, a temporary disruption in the network will occur during the transition time. A smoother guest access experience without such disruption is best achieved through multiple PSK support on the AP.

Expanding the network - Adding additional AP or Router

A Registrar would discover the new AP through UPnP or the 802.11 Beacon and Probe Response. Once the Registrar becomes established as an external WLAN Manager Registrar for the new AP, it can retrieve the current Credentials from an existing AP and transfer them to the new AP using the AP Management Interfaces of those APs.

Changing Network Name (SSID), radio channels, etc.

A WLAN Manager Registrar can set the non-security related parameters (SSID, radio channel, for example) on the AP through the UPnP AP Management Interface. Prior to doing so, however, it is necessary to configure the WLAN clients with the new

parameters as well. Some of these parameters, such as the radio channel, can be discovered automatically, but the SSID is an exception to this rule. One approach to updating these parameters would be to force rekeying for all of the current devices, give them new Credentials, including the new SSID, and then change the AP to the new SSID as well. Unfortunately, this method can cause a disruption in the operation of the network as some clients switched to the new SSID. Ideally, they would simply store an additional WLAN profile for the new SSID and only switch over to it after the AP changes. This would allow them to maintain their current connection to the AP for the maximum possible time.

Rekeying

If a Member device shall be rekeyed, it should re-run the in-band Registration Protocol using a Device Password derived from the previous session as follows. Note that the EMSK, N1, and N2 in the DevicePassword derivation all correspond to the previous instance of the Registration Protocol. In other words, the DevicePasswords for rekeying should be derived and stored by the Enrollee immediately after successful completion of the Registration Protocol. This is important, because the Enrollee and Registrar should discard the KDK and EMSK soon after completion of the protocol. Registrars should store DevicePasswords for rekeying along with either the Enrollee's MAC address or its UUID, both of which will be present in the Description data sent by the Enrollee when it runs the Registration Protocol for rekeying. Registrars can pass rekeying Device Passwords to APs after they complete the Registration Protocol. This enables the rekeying operation to be performed by the AP rather than requiring the Registrar to be online when rekeying occurs. Storing rekeying keys in APs also allows a Registrar to revoke Credentials issued by another Registrar without requiring the Enrollee to get another key from the original Registrar by rekeying.

DevicePassword = kdf(EMSK, N1 || N2 || "WFA-Rekey-PSK", 256)

A Member device that becomes disconnected by the WLAN and is unable to reauthenticate using its current WLAN Credential should attempt in-band rekeying before prompting the user for intervention. Support for the rekeying feature is optional. If either the Member device or the Registrar does not support rekeying, then a fresh registration using the regular device password or out-of-band channel will be required if the Credential becomes invalid.

Annex F - Management Interface Message Definitions

This section describes Management Interface messages that are carried within UPnP actions as described in the WFAWLANConfiguration Service. This messages are deprecated and not part of any certification testing.

The messages are not protected in any way at the SOAP level, but they contain their own internal protection through the Message Counter, Enrollee Nonce, Registrar Nonce, and Authenticator attributes.

When a Registrar establishes AP management keys using the Registration Protocol, the keys are identified by the Enrollee Nonce and the Registrar Nonce used in the Registration Protocol. The Message Counter is a 64-bit counter that is maintained by the Registrar (the UPnP control point). Each time a message containing a Message Counter attribute is sent by a Registrar, the Message Counter is incremented.

When an AP responds to the UPnP action, it SHALL include the same Message Counter value in its reply. Because the entire message, including the Message Counter and nonces are included in the computation of the Authenticator, this mechanism guards against replay attacks. To prevent these attacks, the AP SHALL also store the most recently seen value of the Message Counter from a given Registrar. It is permitted for Message Counters to increment by more than a single count per message, but APs SHALL reject messages containing Message Counters that are numerically lower than the most recently known Message Counter value for that pair of nonces.

GetAPSettings Input Message

The following table lists the attributes that are passed in the input parameter of the UPnP action GetAPSettings.

Table 48 – GetAPSettings Input Message

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Message Counter	R	
Enrollee Nonce	R	
Registrar Nonce	R	
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
<other…>	O	Multiple attributes are permitted.
Authenticator	R	

GetAPSettings Output Message

The following table lists the attributes that can be retrieved using the UPnP action GetAPSettings. In GetAPSettings, the Encrypted Settings attribute is the same as specified in Section 8.3.8 except without E-SNonce2. .

Table 49 – GetAPSettings Output Message

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Message Counter	R	SHALL be a copy of the Message Counter passed in the input parameter.
Enrollee Nonce	R	
Registrar Nonce	R	
Authentication Type	R	
Configuration Methods	R	
Connection Type	R	
Connection Type Flags	R	
Encryption Type Flags	R	
Primary Device Type	R	
Encrypted Settings	R	
MAC Address	R	
Manufacturer	R	
Authentication Type Flags	R	
New Device Name	R	
PSK Current	R	
PSK Max	R	
Registrar Current	R	
Registrar List	R	
Registrar Max	R	
Selected Registrar	R	
SSID	R	
Total Networks	R	
UUID-E	R	
AP Setup Locked	O	Shall be included if value is TRUE
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
<other…>	O	Multiple attributes are permitted.

Attribute	R/O/C	Notes
Authenticator	R	

SetAPSettings Message

The following table lists the attributes that can be set using the UPnP action SetAPSettings. In SetAPSettings, the Encrypted Settings attribute is the same as specified in Section 8.3.9.

If the AP receives an AP Settings Message indicating a new Power Level or AP Channel, the AP should make those changes without rebooting.

Table 50 – SetAPSettings Message

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Message Counter	R	
Enrollee Nonce	R	
Registrar Nonce	R	
AP Setup Locked	O	Shall be included if value is TRUE
Authentication Type	O	
Encrypted Settings	O	
New Device Name	O	
SSID	O	
AP Channel	O	
Power Level	O	
Radio Enabled	O	
Permitted Configuration Methods	O	
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
<other…>	O	Multiple attributes are permitted.
Authenticator	R	

DelAPSettings Message

The following table lists the attributes that can be used to remove network settings and Credentials using the UPnP action DelAPSettings. The scope of the removed settings depends upon how many of the optional attributes are specified. If only SSID is

specified, all settings associated with that SSID are removed. If MAC Address is specified, then only the Credential associated with that MAC Address is removed. If X.509 Certificate is included, then trust in that Certificate is revoked.

Note that the Encrypted Settings in DelAPSettings does not have the same requirements of 7.3.9 (M2 and M8 Encrypted Settings) and may be used as needed by an implementation.

Table 51 – DelAPSettings Message

Attribute	R/O/C	Notes, Allowed Values
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Message Counter	R	
Enrollee Nonce	R	
Registrar Nonce	R	
Encrypted Settings	O	
Network Index	R	Deprecated – use fixed value 1 for backwards compatibility.
SSID	O	SSID of network.
MAC Address	O	Member device's MAC address.
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
<other…>	O	Multiple attributes are permitted
Authenticator	R	

ResetAP and RebootAP Messages

The following table lists the attributes that are passed in the input parameter of the UPnP actions ResetAP and RebootAP:

Table 52 – ResetAP and RebootAP Messages

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Message Counter	R	
Enrollee Nonce	R	
Registrar Nonce	R	
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.

Attribute	R/O/C	Notes
<other…>	O	Multiple attributes are permitted.
Authenticator	R	

STA Settings Message Definitions

See the introduction of this Annex for information regarding the Message Counter attribute.

GetSTASettings Input Message

The following table lists the attributes that are passed in the input parameter of the UPnP action GetSTASettings:

Table 53 – GetSTASettings Input Message

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Message Counter	R	
Enrollee Nonce	R	
Registrar Nonce	R	
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
<other…>	O	Multiple attributes are permitted.
Authenticator	R	

GetSTASettings Output Message

The following table lists the attributes that can be retrieved using the UPnP action GetSTASettings. Attributes included in Encrypted Settings are the same as those specified in Section 8.3.8, except omitting E-SNonce2.

Table 54 – GetSTASettings Output Message

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Message Counter	R	SHALL be a copy of the Message Counter passed in the input parameter.
Enrollee Nonce	R	
Registrar Nonce	R	
Configuration Methods	R	

Attribute	R/O/C	Notes
Connection Type	R	
Connection Type Flags	R	
Encryption Type	R	
Encryption Type Flags	R	
Primary Device Type	R	
Encrypted Settings	R	
MAC Address	R	
Manufacturer	R	
New Device Name	R	
Authentication Type Flags	R	
Registrar Established	R	
Selected Registrar	R	
Association State	R	
Configuration Error	R	
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
<other…>	O	Multiple attributes are permitted.
Authenticator	R	

SetSTASettings Message

The following table lists the attributes that can be retrieved and set using the UPnP action SetSTASettings. Attributes included in Encrypted Settings are specified in Section 8.3.9.

Table 55 – SetSTASettings Message

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Message Counter	R	
Enrollee Nonce	R	
Registrar Nonce	R	
Encryption Type	R	
Encrypted Settings	R	
New Device Name	O	
AP Channel	O	

Attribute	R/O/C	Notes
Power Level	O	
Radio Enabled	O	
Reboot	O	
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
<other…>	O	Multiple attributes are permitted.
Authenticator	R	

DelSTASettings Message

The following table lists the attributes that can be used to remove network settings and Credentials using the UPnP action DelSTASettings. The scope of the removed settings depends upon how many of the optional attributes are specified. If only SSID is specified, all settings associated with that SSID are removed.

Table 56 – DelSTASettings Message

Attribute	R/O/C	Notes, Allowed Values
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Message Counter	R	
Enrollee Nonce	R	
Registrar Nonce	R	
Encrypted Settings	O	
Network Index	R	Deprecated – use fixed value 1 for backwards compatibility.
SSID	O	SSID of network.
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
<other…>	O	Multiple attributes are permitted.
Authenticator	R	

ResetSTA and RebootSTA Messages

The following table lists the attributes that are passed in the input parameter of the

UPnP actions ResetSTA and RebootSTA:

Table 57 – ResetSTA and RebootSTA Messages

Attribute	R/O/C	Notes
Version	R	Deprecated. Always set to 0x10 for backwards compatibility. See Version2 for current version negotiation mechanism.
Message Counter	R	
Enrollee Nonce	R	
Registrar Nonce	R	
Version2 (inside WFA Vendor Extension)	C	0x20 = version 2.0, 0x21 = version 2.1, etc. Shall be included in protocol version 2.0 and higher.
<other…>	O	Multiple attributes are permitted.
Authenticator	R	

Annex G - USBA (USB Host) Out-of-Band Interface Specification

This section details the specifications for using a USB-based flash drive for the out-of-band wireless configuration channel. This mode of configuration is deprecated and should not be used.

Requirements for USB Flash Drives (UFD)

Wi-Fi Simple Configuration devices should work with a variety of USB Flash Drives (UFD's) to ensure compatibility. To date there have been many variations of UFD's that have a variety of different characteristics (Drive type, Master Boot Record, Capacity, etc). The follow list is the recommended configuration of a UFD to maintain broad compliance with WCN devices:

- USB Interface Class 0x8
- USB Mass Storage Subclass 0x6
- USB Interface Protocol 0x50
- USB Mass Storage INQUIRY RMB Bit value of 0x1
- Raw capacity between 200k and 10gig
- FAT 16/32
- Master Boot Record Present
- Maximum current sink 150mA
- Single Partition

Enrollee Requirements for USBA out-of-band Interfaces

Wi-Fi Simple Configuration devices shall support the following hardware requirements to ensure interoperability with UFD devices:

- Easily accessible USB Host Port (USB version 1.1 or higher)
- Support WPA2-Personal 64 byte HEX Network Keys
- Support standard UFD's
    - Support for USB Mass Storage Subclass 0x6
    - Support for USB Interface Protocol 0x50
    - Support UFD's with USB Mass Storage INQUIRY RMB Bit value of 0x1 or 0x0
    - Support UFD's with raw capacity between 200k and 10gig
    - Support UFD's with FAT 16/32 format
    - Support UFD's with or without Master Boot Record Present
- Source up to 200mA on USB Host port.
- Support UFD's with multiple partitions. The WSC device should scan each partition of the UFD looking for the WSC configuration files.

When a Wi-Fi Simple Configuration Enrollee has been successfully configured, including connection to the network and IP connectivity, it should confirm configuration by flashing the appropriate LEDs three times with a 1 Hz cycle as defined in the following:

- 0.5 sec ON, 0.5 sec OFF, 0.5 sec ON, 0.5 sec OFF, 0.5 sec ON, then OFF
- XXXXX____XXXXX____XXXXX

When a Wi-Fi Simple Configuration device is unsuccessful at reading or writing the configuration file or connecting to the network and obtaining an IP address, it should respond with a sequence of flashes – 2 short flashes (0.3 sec ON duration) and one long flash (1 sec ON duration) with a 0.3 sec delay between all flashes -- and then repeat until the WFD is removed (or for at least three full cycles). See example below:

- 0.3 sec ON, 0.3 sec OFF, 0.3 sec ON, 0.3 sec OFF, 1 sec ON, 0.3 sec OFF
- XXX__XXX__XXXXXXXXXXX__XXX__XXX__XXXXXXXXXXX__XXX_
  __XXX__XXXXXXXXXXX__XXX__XXX__XXXXXXXXXXX....

Firmware and Software Requirements

Wi-Fi Simple Configuration compliant devices will need the ability to parse the optionally encrypted M2 TLV based configuration files stored on the UFD and extract settings.

Encrypted Settings File (xxxxxxxx.WSC)

The xxxxxxxx.WSC file is used to describe the wireless settings of the WLAN. This is a binary file containing the TLVs specified in the M2 message of the Registration protocol. The WLAN settings and keys in this file shall be encrypted in an Encrypted Settings attribute using the KeyWrapKey. The TLV data set contains the configuration options for each individual station. The xxxxxxxx.WSC file is located in the \SMRTNTKY\WFAWSC\ directory on the UFD. The file name will be derived from the last 4 bytes of the MAC address of the wireless network adapter that is being configured represented in ASCII-HEX. If, for example, the MAC address of the network adapter is 00-08-0D-1A-DE-67, the corresponding device configuration filename is: 0D1ADE67.WSC. The xxxxxxxx.WSC file may be provided along with the 00000000.WSC file. The 00000000.WSC file may contain settings for any device to use to associate with the WLAN. The xxxxxxxx.WSC file contains settings for a specific station/AP.

Unencrypted Settings File (00000000.WSC)

The 00000000.WSC file is used to transfer unencrypted wireless settings of the WLAN. The TLV data set contains the configuration options for Access Points and wireless stations. The 00000000.WSC file is located in the \SMRTNTKY\WFAWSC\ directory on the UFD. It is a policy decision left to the Enrollee and the Registrar whether or not to support unencrypted settings.

Table 58 – Payload of the UFD Unencrypted Settings File

Attribute	R/O/C	Notes
Version	R	As defined in section 12
Credential	R	As defined in section 12
Version2 (inside WFA Vendor Extension)	C	As defined in section 12
<other…>	O	Multiple attributes are permitted

The main advantage of unencrypted settings is that they can be reused across multiple Enrollees and in the future without the requirement of running the Registrar again to generate Enrollee-specific settings. The usability advantages of this feature, however, come at a potential cost to the security of the system. If an attacker is able to gain access to the UFD, they will be able to gain access to the network by reading the data from the drive.

Enrollee devices shall first try to use the Encrypted Settings File and only use the unencrypted settings file if the Encrypted Settings File is not found. If the Encrypted Settings File is present, but the Enrollee is unable to use it, the Enrollee may choose to use the unencrypted settings file as a fallback measure.

Enrollee Device Password and Key Hash (xxxxxxxx.WFA)

The xxxxxxxx.WFA file is used to transfer the Enrollee's device password and public key hash to the Registrar. The data in the file is the Out-of-Band device password attribute. The xxxxxxxx.WFA file is located in the \SMRTNTKY\WFAWSC\ directory on the UFD. The file name will be derived from the last 4 bytes of the MAC address of the wireless network adapter that is being configured, represented in ASCII-HEX. For example, if the MAC address of the network adapter is 00-08-0D-1A-DE-67, the corresponding device configuration filename is: 0D1ADE67.WFA.

The 00000000.WFA file may also be present on the UFD. This file is provided by a Registrar (Registrar specified password) and indicates a Device Password for an Enrollee to use to connect. The Device Password ID in this file shall be set to 0x0005 (Registrar-specified). In this case, the Enrollee shall set the Device Password ID attribute in M1 to 0x0005 (Registrar-specified) and verify that the Public Key sent by the Registrar in a corresponding M2 matches the Public Key Hash provided in the

00000000.WFA file on the UFD prior to sending M3.

Table 59 – Payload of the Enrollee Device Password and Key Hash File

Attribute	R/O/C	Notes
Version	R	As defined in section 12
Out-of-Band Device Password	R	As defined in section 12
Version2 (inside WFA Vendor Extension)	C	As defined in section 12
<other…>	O	Multiple attributes are permitted