Wi-Fi Protected Setup Specification

Version 1.0h

December 2006

This document contains a proposal for easy, secure setup and introduction of devices into WPA-enabled 802.11 networks. It is intended to meet the requirements determined by the Wi-Fi Protected Setup working group in the Wi-Fi Alliance.

Table of Contents

1. Introduction

1.1. Purpose

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. Responding to this clear and compelling need, many vendors have developed proprietary solutions for WLAN setup. The proliferation of setup solutions is causing confusion and cross-vendor incompatibility that threatens to make things worse for the end user. Therefore, the Wi-Fi Alliance Wi-Fi Protected Setup working group has issued a call for proposals to standardize an easy and secure setup solution for Wi-Fi networks. This Specification has been developed in response to this call for proposals. For convenience, the remainder of this document uses the term "Wi-Fi Protected Setup" to describe the proposed solution.

1.2. Scope

The primary goal of Wi-Fi Protected Setup is to simplify the security setup and management of Wi-Fi networks. The goal of this specification is to provide users with the assurance that their wireless networks are protected against unauthorized access and disclosure of private information.

The scope of this document is limited to that outlined by the Wi-Fi Protected Setup Specification Requirements Document.

1.3. Related Documents

Related documents and locations are listed in the following table

Document	Location
WFADevice.doc	
WFAWLANConfig Service.doc	

1.4. Supported Usage Models

According to the Specification Requirements Document, Wi-Fi Protected Setup proposals must address all of the primary usage models and should also support as many secondary usage models as possible. The primary factors for evaluation of proposed solutions are support for usage models, cost, ease-of-use, security, and compatibility with legacy devices.

Primary Usage Models

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

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 AP or Router

5. Changing Network Name (SSID), radio channels, other parameters outside of security & initial connectivity settings

The solution outlined in this specification can support all of these usage models.

1.5. Mental Model

End users require an appropriate mental model before they can successfully accomplish a task. If a new technology can leverage a familiar mental model, it has a much higher chance of success. The Wi-Fi Protected Setup Specification Requirements Document requires proposals to include a suitable mental model and suggests using "lock and key". This metaphor is widely understood, and it effectively conveys the ideas of ownership and security. This specification uses the recommended "lock and key" mental model. Setting up an AP is analogous to installing or changing locks. Permitting a new member device to access the WLAN is analogous to giving someone a key. As required in the Specification Requirements Document, this document includes a mapping of user actions associated with the Wi-Fi Protected Setup usage models onto the mental model. Each use case section in this document includes a brief section describing the mapping.

1.6. Design Approach

The fundamental design approach in this proposal 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 Protected Setup 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 Protected Setup 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 Protected Setup can be easily extended to support additional communication channels by defining an encapsulation of the Registration Protocol messages over additional network types.

1.7. 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. The 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 WPA-Personal and WPA-Enterprise devices
- Access Points with per-device or shared 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 push button used for in-band setup using the optional PushButton Configuration method

- Access Points, Registrars, or Client devices that support optional hardware-based out-of-band channel such as Ethernet, USB flash drive, Near-Field Communication (NFC) interface, and/or an NFC Contactless Token.
- 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

1.8. 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 Protected Setup user experience. Sections 3, 8, 9 and 10 contain a more detailed specification of these and other scenarios.

1.8.1. 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 install 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 push button 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."

1.8.2. Out-of-band Setup

Context: The user purchases a Wi-Fi Protected Setup AP and a wireless printer that includes an NFC contactless token (card) 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 WPA Personal PSK.
2. User turns on the printer and touches the printer's NFC contactless token to the AP's NFC interface.
3. The printer is configured by the AP and provides visual confirmation (using an LED) that it has joined the network.

2. Core Architecture

2.1. 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
- Discovery Protocol. A protocol informing the Enrollee and the Registrar of each others presence and capabilities.
- 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.
- 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
- Out-of-band: Data transfer using a communication channel other than the WLAN
- Member: A WLAN Device possessing Domain credentials
- NFC interface: Contactless interface compliant to NFC specification (see section 9 for details).
- NFC Contactless Token: Contactless passive token according to the NFC specification (see section 9 for details).
- NFC Device: Any device that supports an NFC interface and protocols according to the NFC specification (see section 9 for details).
- 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.
- External Registrar: A Registrar for an AP's Domain that runs on a device separate from the AP
- PushButton Configuration (PBC): A configuration method triggered by pressing a physical or logical button on the Enrollee and on the Registrar.
- WLAN: A Wi-Fi network

2.2. Components and Interfaces

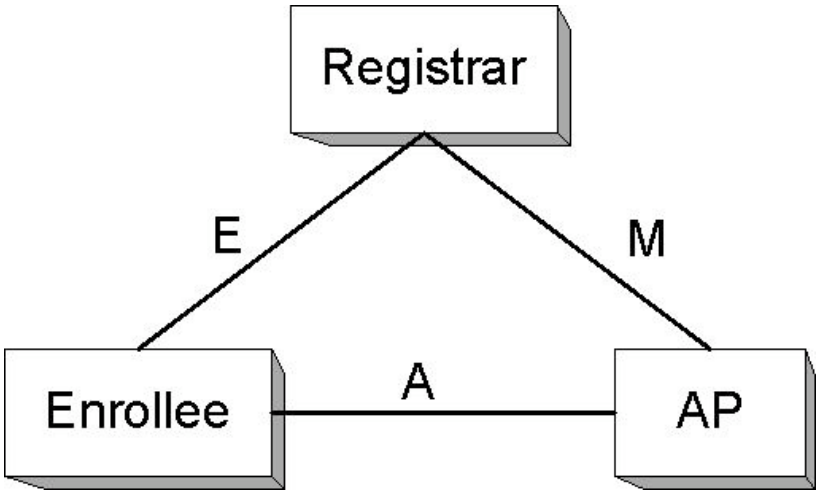


Figure 1: Components and Interfaces

Figure 1 illustrates the major components and their interfaces as defined by the Wi-Fi Protected Setup Proposal. There are three logical components involved in Wi-Fi Protected Setup: 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.

2.2.1. 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 Protected Setup 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 Protected Setup operations. Information obtained from these IEs should be considered to be merely a hint. It is never authenticated, so it should not be trusted.

2.2.2. 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 Protected Setup 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 2.3).
5. Optionally receiving ad-hoc probe-responses from wireless Registrars.

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 2.3).
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 or operating in ad-hoc mode.

2.2.3. Interface M

Interface M is the interface between the AP and the Registrar. It enables an external Registrar to manage a Wi-Fi Protected Setup AP. Wi-Fi Protected Setup 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 WFAWLANConfig Service documents. The AP is required to be a UPnP device that includes support for the Wi-Fi Protected Setup 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 WFAWLANConfig 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. Optionally receiving and processing Enrollee Discovery and Registration messages sent in ad hoc mode.
4. Implementing the Registrar side of the Registration Protocol to gain management rights over the AP or to issue WLAN credentials to Enrollees
5. Configuring the AP with the MAC address and/or the per-device Credential of the Enrollee.
6. Implementing the Management Interface described in the WFADevice and WFAWLANConfig Service documents. This implementation requires the Registrar to function as a UPnP control point.

2.2.4. Interface A

Interface A is between the Enrollee and the AP. The function of Interface A is to enable discovery of the Wi-Fi Protected Setup 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 Protected Setup and generating Probe Response messages containing a description of the AP.
2. Implementing an 802.1X authenticator and the Wi-Fi Protected Setup EAP method.
3. Proxying 802.11 probe request and EAP messages between Enrollees and external Registrars as described in the WFADevice and WFAWLANConfig Service documents.

Enrollee

The Enrollee implements Interface A by

1. Discovering a Wi-Fi Protected Setup 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 Protected Setup EAP method.

2.3. 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. For interoperability reasons, however, it is recommended that the Wi-Fi Alliance choose only a small number of suitable out-of-band channels and scenarios for its certification tests.

The Registration Protocol operates in two phases. The first round trip of the Registration Protocol is used to exchange public keys and other descriptive information between the Registrar and the Enrollee using messages named M1 and M2D or M2. The Enrollee sends M1, and the Registrar sends M2D or M2. The primary role of the first round trip is to enable presence and feature discovery and to exchange public keys.

If both the Registrar and Enrollee decide to proceed with the second phase of the Registration Protocol, three additional round trips may be performed to complete authentication and Credential provisioning. When an Enrollee is in the first phase of the Registration Protocol, it may exchange messages with multiple Registrars on the network. If there is more than one Registrar, the user may choose which one to use.

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 only terminates the Registration Protocol if it is delivered using an out-of-band channel such as a USB flash drive or NFC interface. 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 may be found in Section 6.

2.4. Security Overview

Wi-Fi Protected Setup 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 Protected Setup 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 Protected Setup options. There are two major modes of operation of Wi-Fi Protected Setup: 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 obtained from the Enrollee and entered into the Registrar either manually using a keypad entry or using a USB flash drive or NFC. If the USB or NFC are 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 USB flash drives or NFC tokens 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 two out-of-band channels currently supported by this specification are USB flash drive and NFC.

It is worth noting that the Wi-Fi Alliance may choose to eliminate one or more of the options supported by this specification from the compliance tests that will eventually be used for Wi-Fi Protected Setup certification. If this occurs, then the minimum security strength of the standardized solution may be increased beyond what is claimed in this section.

2.4.1. In-band Configuration

.

The Wi-Fi Protected Setup 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 MUST warn the user and MUST 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 MUST NOT accept the same PIN again without warning the user of a potential attack. If a strong device password (such as an OOB 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 Protected Setup must 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 MUST 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 Protected Setup 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 must 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 Protected Setup. Since one of the digits in the 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 on a label). Because a fixed PIN value is very likely 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, an AP should generate and display a fresh PIN for establishing external Registrars each time the Registration Protocol is run in the initial AP setup mode. However, if a sticker-based PIN is used, the AP should track multiple failed attempts to authenticate as an external Registrar and then enter a lock-down state (This state is signified by setting the attribute AP Setup Locked to TRUE).

In this state, the AP MUST refuse to run the Registration Protocol in initial AP setup mode (with the AP acting as an Enrollee) with any external Registrars. This technique protects the AP's PIN against brute force attack by an attacker posing as a new external Registrar. 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 Setup Locked state can be reset to FALSE through the SetAPSettings action (The SetAPSettings action can only be invoked by a previously authorized external Registrar) or through some other AP-specific method. The AP may include, for example, a way to reset this state using the AP's administrative Web page. It is up to the AP implementation to decide when to enter the AP Setup Locked state.

In addition to the PIN method, headless devices may implement the push button configuration (PBC) method (Devices with richer UIs may also optionally implement the PBC method). The PBC method has zero bits of entropy and only protects only 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 is capable of displaying either four or eight numeric digits, it is required to generate a fresh device password each time it runs the Registration Protocol. 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 displays may display either 4 or 8 digit PINs. The last digit of an 8-digit PIN is a checksum of the first 7 digits. Section 6.4.1 specifies how the checksum is generated. Four-digit PINs do not include a checksum digit.

Devices with NFC or USB

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 USB flash drive or the device's NFC token before completion of the enrollment process, then it may be possible for them to perform a rogue network attack against the Enrollee.

2.4.2. Guidelines and Requirements for PIN values

The recommended length for a manually entered device password is an eight 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 MUST 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 MUST 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 Contactless Token, the two Device Passwords MUST 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.

2.4.3. Out-of-band Configuration

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

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 token or USB flash drive). This control must 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 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.

3. Initial WLAN Setup

There are three primary scenarios for initial WLAN setup with Wi-Fi Protected Setup. The first case is a standalone AP that supports Wi-Fi Protected Setup. A "standalone AP" is one that includes a built-in Registrar and does not use an external Registrar. The second case is a WLAN with a legacy AP that does not support Wi-Fi Protected Setup. In this case, an external Registrar issues Credentials directly to Enrollees, but the AP does not participate in this process. The third case is where a Wi-Fi Protected Setup 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, WPA keys, and Registrar list.

3.1. Standalone AP

The simplest configuration for initial WLAN setup with Wi-Fi Protected Setup 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 Protected Setup AP must automatically choose an SSID (preferably a random SSID) and channel. It should also by default turn on WPA or WPA2 with a strong, randomly generated PSK. A standalone AP should include a Wi-Fi Protected Setup 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 must 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 must be unique to that individual device. Furthermore, the user must be permitted to change this password to a stronger value. If the default password is changed, then the original password must 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 not be able to make correct security decisions unless the system can provide sufficient information to inform those decisions.

3.2. Legacy AP

Even if the AP does not support Wi-Fi Protected Setup, other devices on the network can still benefit from supporting Wi-Fi Protected Setup. In this case, an external Registrar must be manually configured with the key(s) and SSID that have been established for the WLAN via some proprietary method. The

method for entering this legacy AP configuration data will depend on the implementation of the AP and of the Registrar. Given this information, the Registrar can use Wi-Fi Protected Setup to provide Enrollees with WLAN Credentials.

In the legacy AP case, a wireless Registrar receives Discovery frames from an Enrollee through Probe Requests and may respond back to the Enrollee through an ad-hoc Probe Response. If both the Enrollee and the Registrar support ad hoc connections, they may proceed directly to the rest of the Wi-Fi Protected Setup protocol exchange over 802.1X using a point-to-point ad-hoc connection. If either the Registrar or the Enrollee do not support the in-band protocol in ad hoc mode, then the Registrar still may use the Enrollee's Probe Request to help guide the user through the setup process. If the Registrar and the Enrollee share a common out-of-band configuration method, then that method can be used to set up the Enrollee even with a legacy AP.

This mode of operation will naturally have some limitations. The user experience of manually configuring the Registrar, for example, may vary according to the AP implementation. Furthermore, it may be difficult to configure strong keys for the network with this method because the keys would need to be entered by hand. The legacy AP may also support only single shared key (no per-device keys). Another potential limitation is that with a legacy AP, a wired Registrar may not be able to receive Discovery messages sent by Enrollees in 802.11 frames. This means the user may have to invoke the out-of-band Registrar function manually.

Security Considerations

The primary security problem with a legacy AP is that without Wi-Fi Protected Setup to distribute strong keys between the Registrar and the AP, the user is likely to configure a weak WPA Personal pass phrase that is susceptible to offline dictionary or brute force attack.

3.3. AP With an External Registrar

It is ultimately the responsibility of the AP to perform link layer access control on a Wi-Fi network in infrastructure mode. Wi-Fi Protected Setup 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 must first be given a Credential (in home networks, this Credential is typically a WPA-Personal PSK). 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 must also establish a secure Management Interface with the AP. The Management Interface is specified in the WFADevice and WFAWLANConfig 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 WPA-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 must also be able to configure the AP with the Enrollee's new Credential. In this case, a secure WLAN Management Interface must 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 Protected Setup, Wi-Fi Protected Setup APs *must simultaneously support at least three* external WLAN Manager Registrars. Note that an AP could continue to function as a standalone Registrar even after it is configured to support one or more external WLAN Manager 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 Protected Setup protocol, it may need to replace a previously established WLAN Manager Registrar relationship based on the capacity of the AP. An AP must 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 must 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 ManagerRegistrar.

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

3.3.1. EAP-based Setup of External Registrar

Figure 2 illustrates the process to register an external Registrar to a Wi-Fi Protected Setup AP. The message flow and logical transitions in this and other such diagrams in this specification correspond to the state machines in Section 6.10.3 and Section 6.10.4.

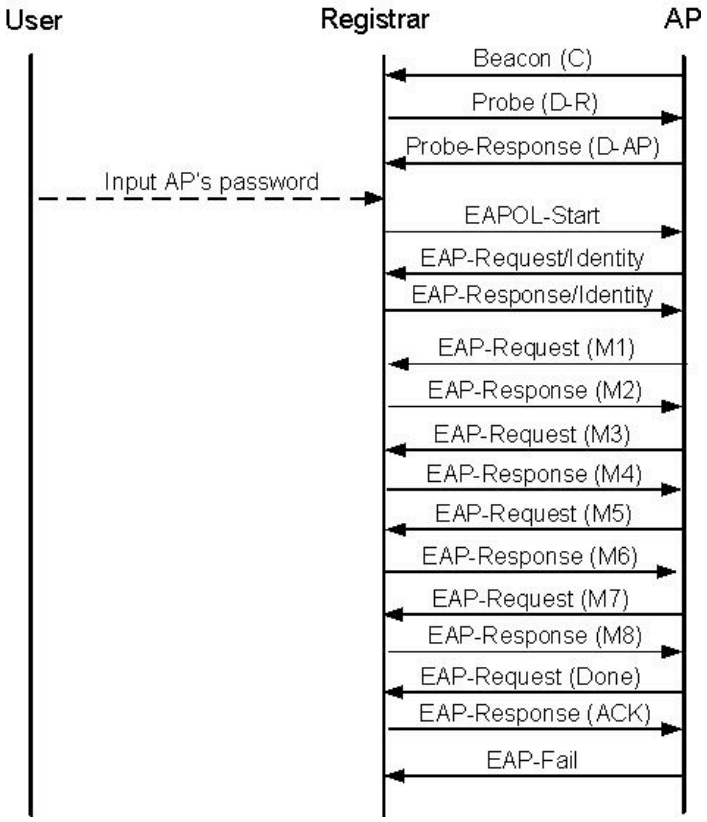


Figure 2: EAP-based Setup of an External Registrar

1. The AP sends out a beacon that includes an Information Element indicating it supports the Wi-Fi Protected Setup capability (C).
2. The Registrar sends a Wi-Fi Protected Setup probe request to the WLAN with Request Type set to Registrar or WLAN Manager Registrar.
3. The AP sends a Wi-Fi Protected Setup probe response to the Registrar with Response Type set to Enrollee.
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 token 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-Fail 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. Note that it must be possible to place the AP into setup mode for introducing a new external Registrar even after the AP has been configured.

Mental model mapping

Wi-Fi Protected Setup 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.

3.3.2. Ethernet-based Setup of External Registrar

Figure 3 illustrates how UPnP can be used for introducing an External Registrar to a Wi-Fi Protected Setup 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.

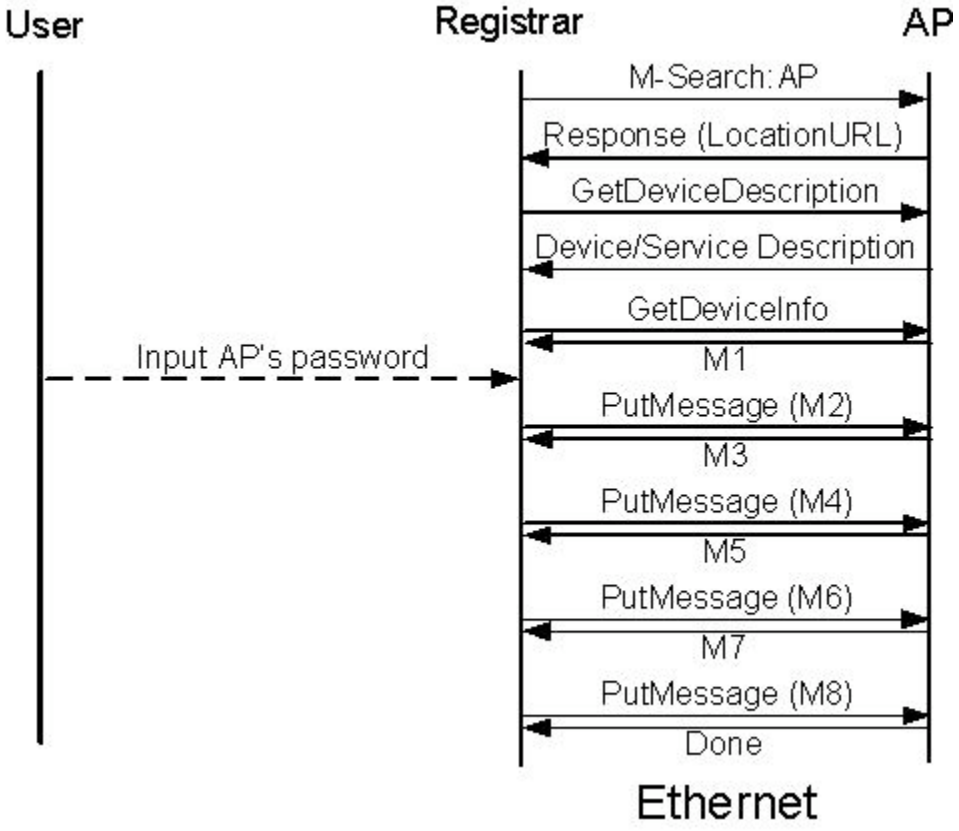


Figure 3: UPnP-based Setup of an External Registrar

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.

4. Adding Member Devices

Ideally, a Wi-Fi Protected Setup 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 WPA-Personal key shared by all devices.

The first two scenarios in this section apply both for adding Enrollees to APs with built-in Registrar capabilities as well as wireless external Registrars that support direct Registration of Enrollees using an ad hoc 802.11 connection. The latter approach is especially useful for WLANs with legacy APs.

An Enrollee only must 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 to 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.

4.1. 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 that support direct Registration of Enrollees using an ad hoc 802.11 connection. The latter approach is especially useful for WLANs with legacy APs.

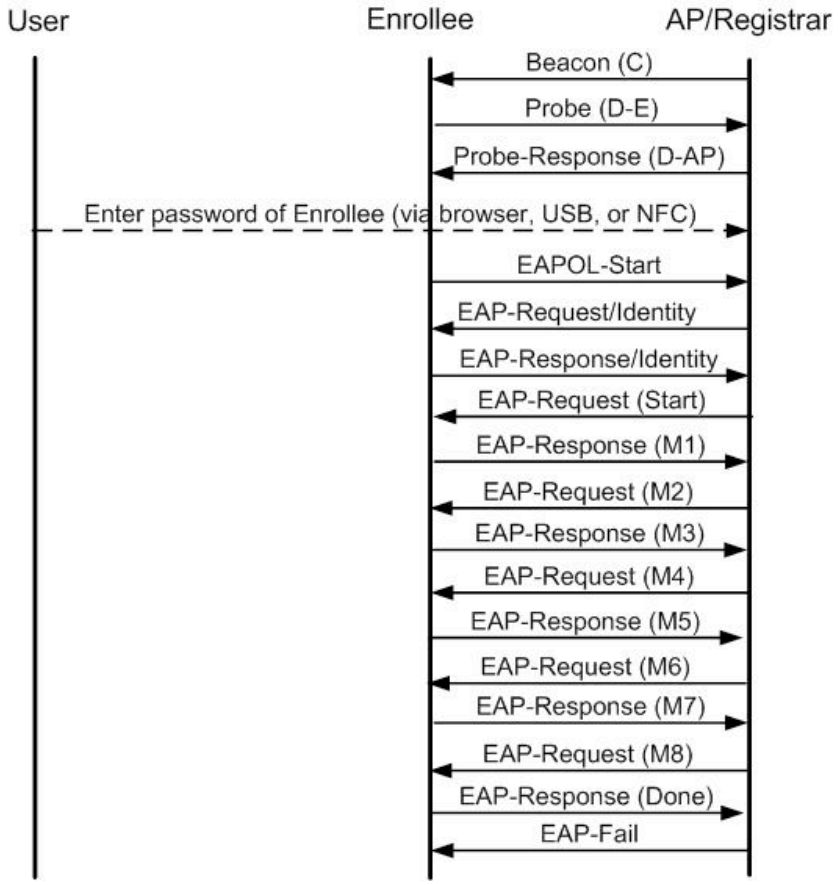


Figure 4: In-band Setup Using a Standalone AP/Registrar

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 Protected Setup AP or ad hoc wireless Registrar. 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.

4.2. 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.

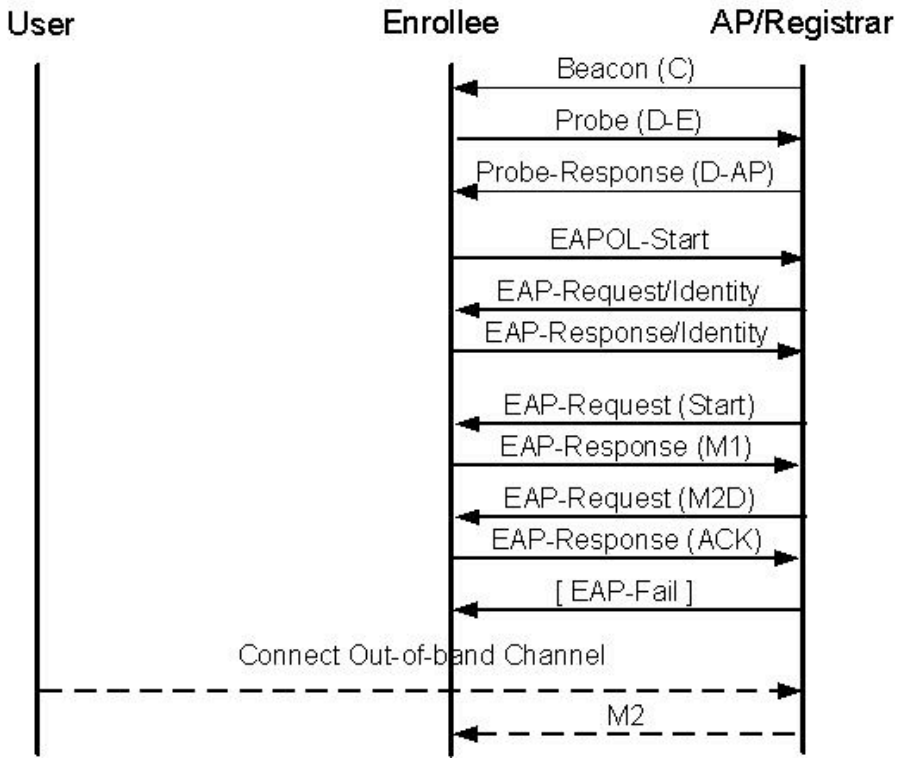


Figure 5: Out-of-band Setup Using an AP/Registrar

Setup steps

1. The Enrollee discovers a Wi-Fi Protected Setup AP or ad hoc wireless Registrar and 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-Fail.
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.

4.3. Out-of-band Setup Using an External Registrar

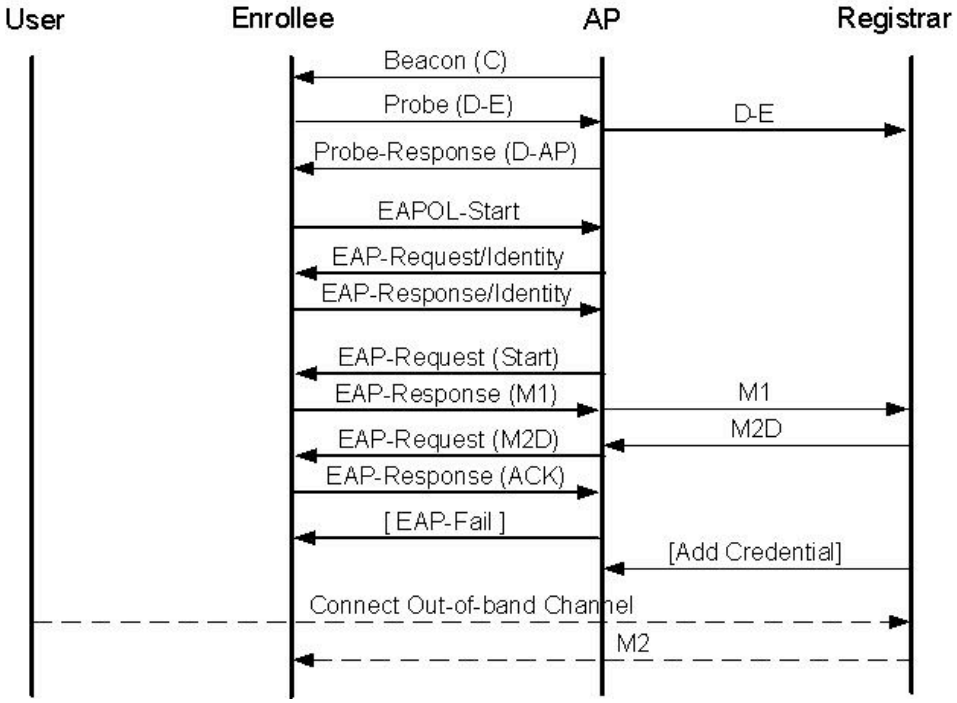


Figure 6: Out-of-band Setup Using External Registrar

Figure 6 illustrates an external Registrar Registering an Enrollee via an out-of-band channel into a network with a Wi-Fi Protected Setup AP.

1. The Enrollee sends its Discovery data in a probe request to a Wi-Fi Protected Setup 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 must 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.

4.4. Secure Setup with Legacy AP

When a legacy AP is used, the AP itself by definition does not support Wi-Fi Protected Setup. This reality implies that it cannot operate as a Registrar, and it does not support the Management Interface used by an external Registrar. If the user is somehow able to configure a wireless external Registrar with knowledge of Credentials accepted by the legacy AP, however, then the external Registrar can in turn issue those Credentials to Enrollees using the Wi-Fi Protected Setup protocols. The protocols between the wireless external Registrar and the Enrollee have already been described in Section 4.2 and Section 4.1. The means by which a Registrar is configured with the settings of a legacy AP are not specified by WiFi Wi-Fi Protected Setup.

4.5. Secure Setup with Legacy Enrollee

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

Setup steps

1. Consult the Registrar UI to obtain the SSID and WPA-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 WPA-Personal pass code 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 WPA-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.

4.5.1. Mental model mapping

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

4.6. No-Security Out-of-band Setup Using a Standalone AP

Context: the user purchases a new AP and another wireless device (a headless media player like an Internet radio), both supporting Wi-Fi Protected Setup. For some reason, the user wants the network to be unsecured.

Setup steps

1. Set AP to unlock mode (possibly using a small toggle switch labeled lock/unlock)
2. Insert a flash drive into the AP.
3. Remove the drive from the AP and then insert it into the Enrollee.

Note that the user experience for setting up an insecure network is virtually identical to setting up a secure network. This is important, because it demonstrates that adding security need not impose any additional user inconvenience.

4.6.1. Mental model mapping

The same simple steps used for adding a device to a locked network are also used for adding a device to an unlocked network. In this case, only the name of the network is given to the new device. This is like telling someone your address and deliberately leaving the door unlocked so they can enter without a key.

5. Secondary Usage Models

This section describes the way in whichthe Wi-Fi Protected Setup architecture can be applied to achieve the secondary usage models discussed in the Specification Requirements Document.

5.1. 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 (see Section 5.3) can be used.

5.2. 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 Section 5.3).

5.3. Re-keying credentials

Section 6.5 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 WPA-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.

5.4. 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.

5.5. 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.

6. 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.

6.1. 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 must 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 must silently ignore this message. 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. 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 must 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 sending a WSC_Nack message to the other side with the associated configuration error. If either side 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.

6.2. 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.
- N2 is a 128-bit random number (nonce) specified by the 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 7.
- 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.

6.2.1. 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, because that channel is presumed to be inherently secure from eavesdropping attacks. However, if the out-of-band channel stores M2, encryption of ConfigData using the KeyWrapKey is strongly recommended.

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.

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 must 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 must be encrypted using the KeyWrapKey.

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

6.3. 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 Protected Setup 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($g^{AB} \bmod p$). 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 Protected Setup 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”)

6.4. 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 OOB 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

$$\text{E-Hash1} = HMAC_{AuthKey}(\text{E-S1} \,||\, \text{PSK1} \,||\, PK_E \,||\, PK_R)$$
$$\text{E-Hash2} = HMAC_{AuthKey}(\text{E-S2} \,||\, \text{PSK2} \,||\, PK_E \,||\, PK_R)$$

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

$$\text{R-Hash1} = HMAC_{AuthKey}(\text{R-S1} \,||\, \text{PSK1} \,||\, PK_E \,||\, PK_R)$$
$$\text{R-Hash2} = HMAC_{AuthKey}(\text{R-S2} \,||\, \text{PSK2} \,||\, PK_E \,||\, PK_R)$$

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 must acknowledge the message with a failure indication, and the Enrollee and Registrar must 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 Contactless Token, 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 MUST 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.

6.4.1. 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.

6.4.2. Device Password Splitting

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

6.4.3. Device Password Usage

The following are recommendations on the use of the Device Password ID (DPID).

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

2) In M1, Enrollee sends DPID=Default, Config Methods has Display bit set. Registrar accepts user input of 4- or 8-digit PIN. If 8-digit, Registrar checks the checksum bit 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 must 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 must send M2 with DPID=Default.

[note: there is still some ambiguity around how the Enrollee will interpret DPID=Default in this case if the user has configured a user-specified PIN on it. Probably the best alternative is to have the Enrollee give precedence to the user-specified PIN. However, the Registrar will not know whether or not to verify the checksum digit.]

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 any of above cases, if Registrar has received a device password via an OOB 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 OOB Device Password attribute.

6.5. 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**$_{\text{KeyWrapKey}}$(**WrappedData**, **IV**)
2. If **KWA** = 1st 64 bits of HMAC$_{\text{AuthKey}}$(**Data**), then output **Data**, else output "failure"

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

6.6. Rekeying

If a Member device must 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.

6.7. Key Summary and Classification

The table in this section summarizes the different keys created and used by Wi-Fi Protected Setup. 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.

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	Enrollee, Registrar	Authenticating Diffie-Hellman exchange

	on display, may be Long-lived if on label or NFC Contactless Token		
g^{AB}mod p	Authentication and key derivation, Temporary	Enrollee, Registrar	Generating session keys
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

Table 1: Key Types and Lifetimes

6.8. Security Analysis

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 USBA (refer to Section 8) or NFC (refer to Section 9).

6.9. Out-Of-Band Channels

Wi-Fi Protected Setup 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 Protected Setup 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 Protected Setup is kept small.

6.9.1. 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 Protected Setup exchange.

Resistance to eavesdropping

Out-of-band channels have differing degrees of resistance to eavesdropping (privacy). For example, physical wires and USB flash drives are more resistant to eavesdropping attacks than are infrared, near-field communications (NFC), or RFID. Out-of-band channels must 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 USB flash drives and 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 must have sufficient data capacity and transfer rates to accommodate the Wi-Fi Protected Setup data exchange with minimal user experience impact.

6.10. EAP Transport of Registration Protocol

Wi-Fi Protected Setup 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 Protected Setup does not require the AP to support RADIUS, and the network need not include an authentication server. In fact, many Wi-Fi Protected Setup APs may support 802.1X only to configure WPA-Personal Credentials using Wi-Fi Protected Setup. Enrollees using Wi-Fi Protected Setup are not granted direct access to the WLAN through the Wi-Fi Protected Setup 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 WPA-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 WPA-Personal to access the WLAN. Alternatively, if the AP supports 802.1X authentication, the Enrollee may first run the Wi-Fi Protected Setup 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 Protected Setup 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.

6.10.1. 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 in ad hoc mode. This latter mode is useful for networks with legacy APs.

Figure 7 and the following text presents a brief summary of the Wi-Fi Protected Setup EAP method. The EAP packet format for Request and Response messages is depicted in Figure 7. The Wi-Fi Protected Setup 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 Protected Setup utilizes the 802.1X data connection for acquiring settings necessary for connecting to the network & the resulting EAP exchange must always terminate with EAP-Fail.

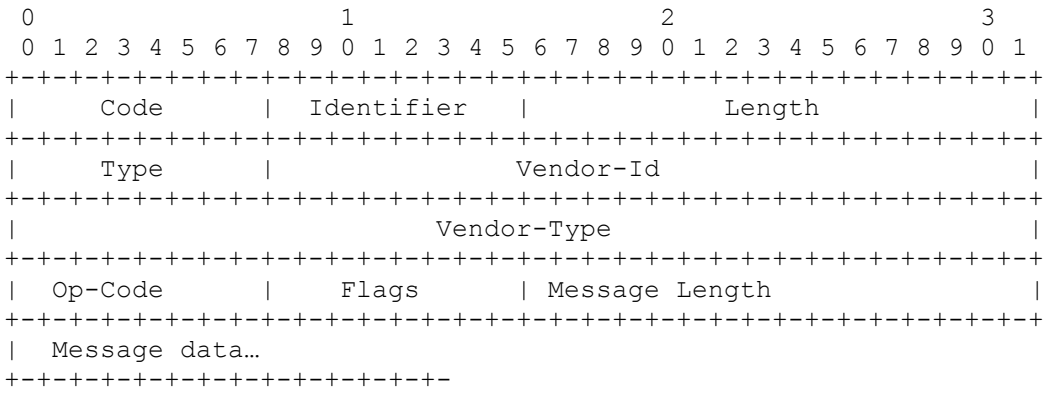


Figure 7: EAP Packet Format

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 Protected Setup, 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).

Fragmentation and Reassembly

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

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

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 MessageData 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 message data being conveyed. If the LF is not set, the Message Length field is omitted. The LF flag and Message Length field are included only in the first EAP packet for a fragmented EAP message. The LF flag must 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 must handle fragmentation and reassembly of the frame. The proxy function must provide a completely assembled message to the UPnP interface.

EAP Identity

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

6.10.2. 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 7.3.10.

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 through a UPnP event. The Message Data field of this message is specified in Section 7.3.11.

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 7.3.12.

WSC_FRAG_ACK

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

6.10.3. EAP State Machine for Enrollee Registration

Figure 8 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 must 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.

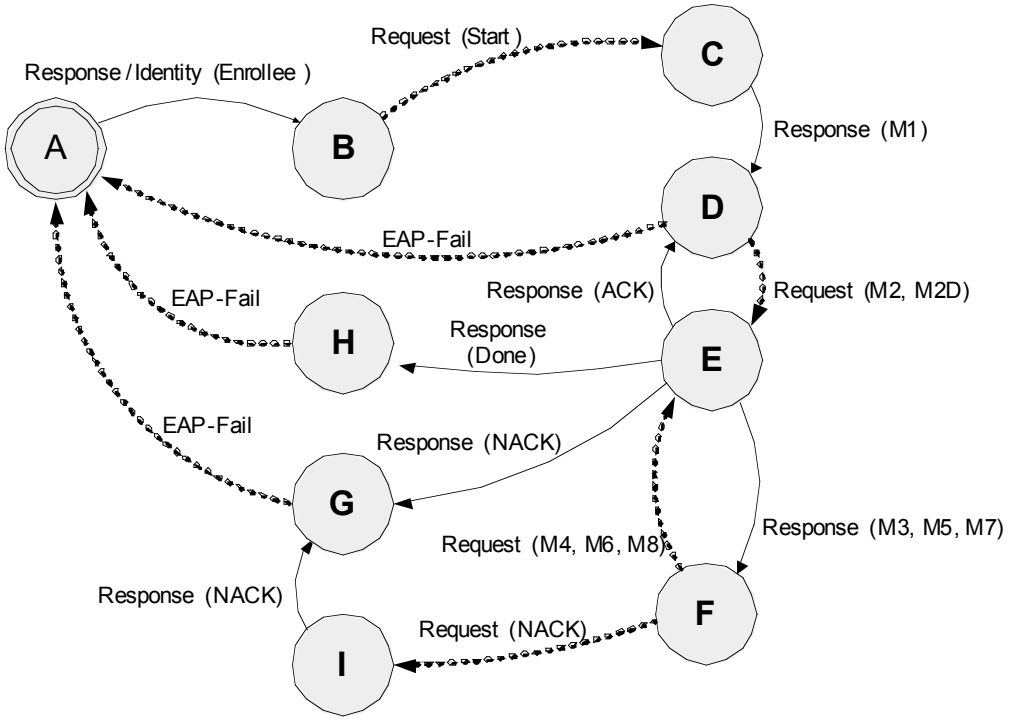


Figure 8: State Machine for Enrollee Registration

When the Enrollee decides to connect to the network and run the Wi-Fi Protected Setup EAP method, it associates with the AP or ad hoc Registrar 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 SimpleConfig Enrollee ("WFA-SimpleConfig-Enrollee-1-0"). This causes the AP to start running the SimpleConfig 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 a EAP-Response/Done message to the authenticator, which events the WSC_Done message to any external registrars and the authenticator returns an EAP-Fail message to the Enrollee. The Enrollee then disassociates and reconnects with the Credential obtained from 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.

Once the Enrollee sends an M3 message, both the Registrar and the Enrollee must proceed in lock-step fashion until either a failure or until success occurs (indicated by the Done response message). If the Enrollee detects any errors or timeouts 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.

6.10.4. EAP State Machine for Adding an External Registrar

The diagram 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 Registrar. Comma-separated lists indicate that the message may be one of those in the list. The lock-step sequence of the Registration Protocol must 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 must respond with a WSC_NACK.

Similarly, if the AP detects an authentication error in processing a message sent by the Registrar, it must respond with a WSC_NACK, after which the Registrar sends EAP-Fail. 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-FAIL to end the protocol session.

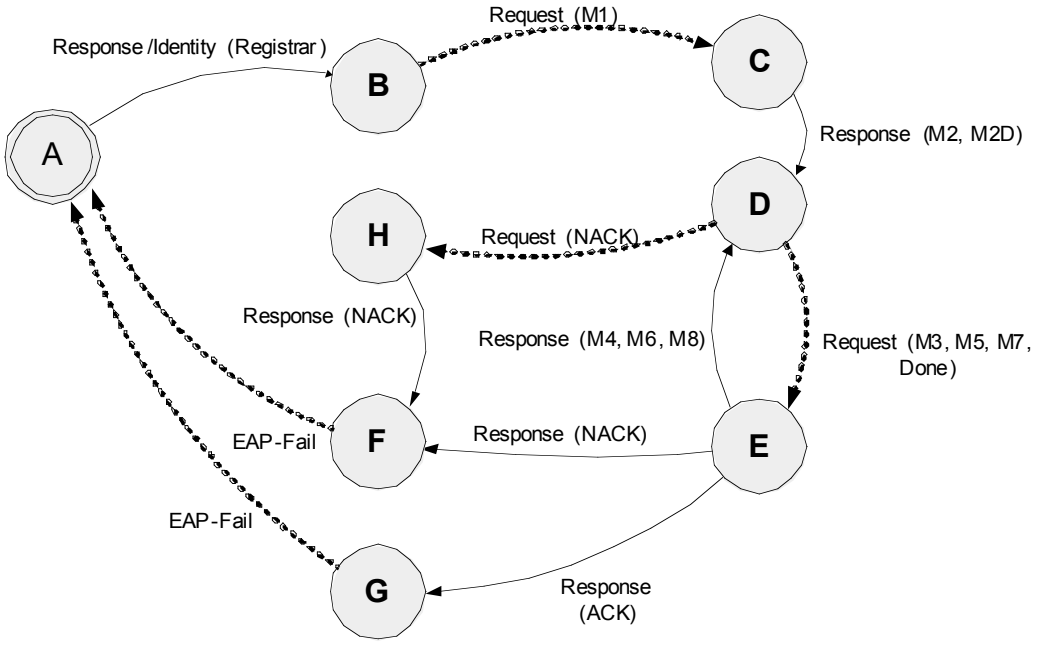


Figure 9: State Machine for Adding a Registrar

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 then sends EAP-Fail and enters 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 OOB channel.

6.11. 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 WFAWLANConfig Service documents.

7. Message Encoding

The protocols presented in section 6 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 6.10.1. 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 MUST match the order given in the tables the subsequent subsections contain. Attributes that are listed in each table as optional (O) must be recognized and handled if they are provided. 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 must ignore it.

7.1. Wi-Fi Protected Setup TLV Data Format

Wi-Fi Protected Setup 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.

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

Table 1: Type, Length, Value (TLV) format for Wi-Fi Protected Setup binary data

Most Wi-Fi Protected Setup 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 Protected Setup attributes encoded in TLV format. The Credential attribute is another example of a compound attribute.

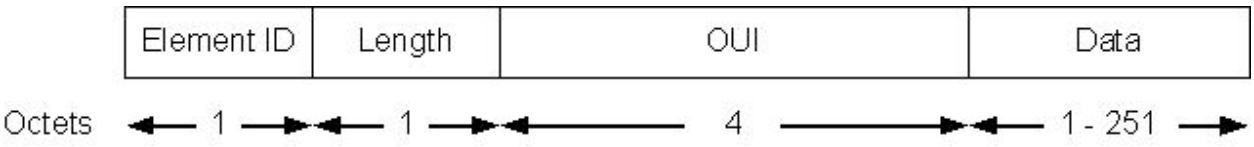
7.2. 802.11 Management Frames

Initial discovery of Wi-Fi Protected Setup 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 unsecured and should be considered only as hints.

Wi-Fi Protected Setup Information Element

The Wi-Fi Protected Setup 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



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

Access Points must provide the Wi-Fi Protected Setup IE in all beacon and probe-response frames. Stations may provide the Wi-Fi Protected Setup IE in all probe-request frames, but an AP must not require that a Station include the IE in probe-request frames in order to engage with EAP-WSC.

The presence of the Wi-Fi Protected Setup IE in Beacons and probe-responses indicates support for the EAP-WSC method over 802.1X.

A client that intends to use the EAP-WSC method with a WSC enabled AP may include a WSC IE in its 802.11 (re)association request. If a WSC IE is present in the (re)association request, the AP shall engage in EAP-WSC with the station and must not attempt other security handshake. If the client does not include a WSC IE in its 802.11 (re)association request, it must send its 802.11 Authentication frame with Authentication set to open and an 802.11 Association Request frame without an RSN IE or SSN IE, regardless of the network type that is hosted by the AP. On successful association, the client will then send an EAPOL-Start to the AP and wait for EAP-Request/Identity. When the client receives an EAP-Request/Identity, it will respond with EAP-Response/Identity and the appropriate WSC string to indicate if it is an Enrollee or Registrar.

When a WSC enabled AP receives an 802.11 Authentication frame with Authentication set to open, it will send an 802.11 Authentication frame with Authentication set to open. After the authentication exchange, if the WSC AP receives an 802.11 Association request frame without an RSN or SSN, it will send an 802.11 Association response frame without an RSN IE or SSN IE. The AP will then allow 802.1X connections and wait for the EAPOL-Start from the client. When the AP receives an EAPOL-Start frame from the client, it will send an EAP-Request/Identity and wait for an EAP-Response/Identity. The EAP-Response/Identity will indicate if the station intends to be an Enrollee or a Registrar. Note: an AP must ignore EAPOL-Start frames received from clients that associated to the AP with an RSN IE or SSN IE indicating a WPA2-PSK/WPA-PSK authentication method in the association request.

Note: An AP hosting a WPA-PSK or WPA2-PSK network and supporting WPS would need to permit the association exchange with a client where there is no RSN or SSN IE in the association frames. The AP must only permit the exchange of EAP messages with a station that associates in this manner.

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

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

7.2.1. Beacon Frame (C)

If the Wi-Fi Protected Setup Information Element is included in a beacon frame, it contains 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 must be included. If Selected Registrar is TRUE, then the Selected Registrar, Device Password ID, and Selected Registrar Config Methods attributes MUST be included. Otherwise, they are omitted.

Attribute	R/O	Allowed Values
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Wi-Fi Protected Setup State	R	1 = unconfigured, 2 = configured
AP Setup Locked	O	Must be included if value is TRUE
Selected Registrar	O	BOOL: indicates if the user has recently activated a Registrar to add an Enrollee.
Device Password ID	O	Device Password ID indicates the method or identifies the specific password that the selected Registrar intends to use.
Selected Registrar Config Methods	O	This attribute contains the config methods active on the selected Registrar.
UUID-E	O	The AP's UUID is provided only when the AP is a dual-band AP in push button mode and indicating push button mode on both radios
RF Bands	O	Indicates all RF bands available on the AP. A dual-band AP must provide this attribute.
<other…>	O	Multiple attributes are permitted

7.2.2. Association Request and Reassociation Request

If the Wi-Fi Protected Setup Information Element is included in an association request or reassociation request, it contains the following attributes:

Attribute	R/O	Allowed Values
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Request Type	R	
<other…>	O	Multiple attributes are permitted

7.2.3. Association Response and Reassociation Response

If the Wi-Fi Protected Setup Information Element is included in an association response or reassociation response, it contains the following attributes:

Attribute	R/O	Allowed Values
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Response Type	R	
<other…>	O	Multiple attributes are permitted

7.2.4. Probe Request (D-E or D-R)

If the Wi-Fi Protected Setup Information Element is included in a probe request, it contains the following Enrollee device attributes:

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Request Type	R	
Config 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	
<other…>	O	Multiple attributes are permitted

7.2.5. Probe Response (D-AP/Registrar)

If the Wi-Fi Protected Setup Information Element is included in a probe response, it contains the following attributes corresponding to the AP or Registrar using 802.11 ad hoc mode. If AP has locked its PIN, such as due to too many authentication failures, AP Setup Locked must be included. If Selected Registrar is TRUE, then the Selected Registrar, Device Password ID, and Selected Registrar Config Methods attributes MUST be included. Otherwise, they are omitted.

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Wi-Fi Protected Setup State	R	1 = unconfigured, 2 = configured.
AP Setup Locked	O	Must be included if value is TRUE
Selected Registrar	O	BOOL: indicates if the user has recently activated a Registrar to add an Enrollee.
Device Password ID	O	Device Password ID indicates the method or identifies the specific password that the selected Registrar intends to use..
Selected Registrar	O	This attribute contains the Config Methods

Config Methods		active on the selected Registrar.
Response Type	R	
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.
Config Methods	R	Config Methods corresponds to the methods the AP supports as an Enrollee for adding external Registrars.
RF Bands	O	Indicates all RF bands available on the AP. A dual-band AP must provide this attribute.
<other…>	O	Multiple attributes are permitted

7.3. Registration Protocol Message Definitions

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

7.3.1. Message M1

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Message Type	R	Value is 0x04 for M1.
UUID-E	R	
MAC Address	R	
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	
Encryption Type Flags	R	
Connection Type Flags	R	
Config Methods	R	
Wi-Fi Protected Setup State	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	
Device Password ID	R	
Configuration Error	R	
OS Version	R	
<other…>	O	Multiple attributes are permitted

7.3.2. Message M2

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
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	
Encryption Type Flags	R	
Connection Type Flags	R	
Config 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	
<other…>	O	Multiple attributes are permitted
Authenticator	R	

7.3.3. 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. The only differences between M2 and M2D are in the Message Type value and in the omission of the Public Key, Encrypted Data, and Authenticator attributes in the M2D message.

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Message Type	R	Value is 0x06 for M2D.
…		Same as M2, except no Public Key, no Encrypted Data, no Device Password ID and no Authenticator attribute.

7.3.4. Message M3

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
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.
<other…>	O	Multiple attributes are permitted
Authenticator	R	

7.3.5. Message M4

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
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.
<other…>	O	Multiple attributes are permitted .
Authenticator	R	

Encrypted Settings Data in 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.

7.3.6. Message M5

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Message Type	R	Value is 0x09 for M5.
Registrar Nonce	R	
Encrypted Settings	R	Encrypted Secret Nonce attribute containing Enrollee's secret nonce 1.
<other…>	O	Multiple attributes are permitted .
Authenticator	R	

7.3.7. Message M6

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Message Type	R	Value is 0x0a for M6.
Enrollee Nonce	R	
Encrypted Settings	R	Encrypted Secret Nonce attribute containing Registrar's secret nonce 2.
<other…>	O	Multiple attributes are permitted .
Authenticator	R	

7.3.8. Message M7

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
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.
<other…>	O	Multiple attributes are permitted .
Authenticator	R	

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

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. If more than one Network Key is included, then all of them are required to be prefixed by a Network Key Index.

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	
Encryption Type	R	
Network Key Index	O	If omitted, the Network Key Index defaults to 1.
Network Key	R	Multiple instances of Network Key and its preceding Network Key Index may be included.
<other…>	O	Multiple attributes are permitted .
Key Wrap Authenticator	R	

7.3.9. Message M8

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
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.
<other…>	O	Multiple attributes are permitted .
Authenticator	R	

The Encrypted Settings attribute in M2 or M8 sent to APs may contain multiple network keys and associated binding information (SSID, MAC Address, Authentication Type, and Encryption Type). If the optional Network Index attribute is present, the attributes in the following table apply to that network index. Similarly, multiple network keys can be specified, each optionally preceded by a Network Key Index. If more than one Network Key is included, then all of them are required to be prefixed by a Network Key Index. Note: There may be multiple instances of Network Key Index and associated bindings following a given SSID in the Encrypted Settings attribute or there may be multiple instances of Network Index and associated groupings in the Encrypted Settings attribute.

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

Attribute	R/O	Notes
Network Index	O	This attribute is only used if the Enrollee is an AP and the Registrar wants to configure settings for a non-default network interface. If omitted, the Network Index defaults to 1.
SSID	R	
Authentication Type	R	
Encryption Type	R	
Network Key Index	O	If omitted, the Network Key Index defaults to 1.
Network Key	R	Multiple instances of Network Key and its preceding Network Key Index may be included.
MAC Address	R	
New Password	O	
Device Password ID	O	Required if New Password is included.
<other…>	O	Multiple attributes are permitted .
Key Wrap Authenticator	R	

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.
<other…>	O	Multiple attributes are permitted .
Key Wrap Authenticator	R	

7.3.10. WSC_ACK Message

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

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Message Type	R	Value is 0xD for WSC_ACK Message.
Enrollee Nonce	R	
Registrar Nonce	R	
<other…>	O	Multiple attributes are permitted .

7.3.11. WSC_NACK Message

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

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Message Type	R	Value is 0xE for WSC_NACK Message.
Enrollee Nonce	R	
Registrar Nonce	R	
Configuration Error	R	
<other…>	O	Multiple attributes are permitted .

7.3.12. WSC_Done Message

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

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Message Type	R	Value is 0xF for WSC_Done Message.
Enrollee Nonce	R	
Registrar Nonce	R	
<other…>	O	Multiple attributes are permitted .

7.4. AP Settings Message Definitions

This section and Section 7.4.5 describe messages that are carried within UPnP actions as described in the WFAWLANConfig Service. 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 MUST 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 MUST 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 MUST reject messages containing Message Counters that are numerically lower than the most recently known Message Counter value for that pair of nonces.

7.4.1. GetAPSettings Input Message

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

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Message Counter	R	
Enrollee Nonce	R	
Registrar Nonce	R	
<other…>	O	Multiple attributes are permitted .
Authenticator	R	

7.4.2. 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 7.3.8 except without E-SNonce2. .

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Message Counter	R	MUST be a copy of the Message Counter passed in the input parameter.
Enrollee Nonce	R	
Registrar Nonce	R	
Authentication Type	R	
Config 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	Must be included if value is TRUE
<other…>	O	Multiple attributes are permitted .
Authenticator	R	

7.4.3. 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 7.3.9.

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

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Message Counter	R	
Enrollee Nonce	R	
Registrar Nonce	R	
AP Setup Locked	O	Must 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 Config Methods	O	
<other…>	O	Multiple attributes are permitted .
Authenticator	R	

7.4.4. 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 Network Index and SSID are specified, all settings associated with that SSID and network index are removed. If Network Key Index is also specified, then only that key is removed. If MAC Address is specified, then only the Credential associated with that Network Key Index or 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.

Attribute	R/O	Notes, Allowed Values
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Message Counter	R	
Enrollee Nonce	R	
Registrar Nonce	R	
Encrypted Settings	O	
Network Index	R	
SSID	O	SSID of AP or ad hoc network.
Network Key Index	O	
MAC Address	O	Member device's MAC address.
<other…>	O	Multiple attributes are permitted
Authenticator	R	

7.4.5. 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. Registrars that support the PBC method are required to advertise when this mode is active by calling SetSelectedRegistrar(). For other Registrars, calling this action is optional but strongly recommended, because it enables Enrollees to optimize their Wi-Fi Protected Setup network selection behavior.

After an AP receives a SetSelectedRegistrar action with Selected Registrar TRUE, it MUST include this information in its Probe Response messages until a SetSelectedRegistrar action has set SelectedRegistrar to FALSE or a timeout interval equal to the PBC method Walk Time has elapsed (whichever occurs first). During the time the Selected Registrar information is active, it is included in Probe Response messages and Beacons.

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
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.
Selected Registrar Config Methods	R	This attribute contains the config methods active by the selected Registrar.
<other…>	O	Multiple attributes are permitted

7.4.6. ResetAP and RebootAP Messages

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

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Message Counter	R	
Enrollee Nonce	R	
Registrar Nonce	R	
<other…>	O	Multiple attributes are permitted .
Authenticator	R	

7.5. STA Settings Message Definitions

See the introduction of Section 0 for information regarding the Message Counter attribute.

7.5.1. GetSTASettings Input Message

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

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Message Counter	R	
Enrollee Nonce	R	
Registrar Nonce	R	
<other…>	O	Multiple attributes are permitted .
Authenticator	R	

7.5.2. 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 7.3.8, except omitting E-SNonce2.

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Message Counter	R	MUST be a copy of the Message Counter passed in the input parameter.
Enrollee Nonce	R	

Registrar Nonce	R	
Config Methods	R	
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	
<other…>	O	Multiple attributes are permitted .
Authenticator	R	

7.5.3. 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 7.3.9.

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Message Counter	R	
Enrollee Nonce	R	
Registrar Nonce	R	
Encryption Type	R	
Encrypted Settings	R	
New Device Name	O	
AP Channel	O	
Power Level	O	
Radio Enabled	O	

Reboot	O	
<other…>	O	Multiple attributes are permitted .
Authenticator	R	

7.5.4. 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 Network Index and SSID are specified, all settings associated with that SSID and network index are removed. If Network Key Index is also specified, then only that key is removed.

Attribute	R/O	Notes, Allowed Values
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Message Counter	R	
Enrollee Nonce	R	
Registrar Nonce	R	
Encrypted Settings	O	
Network Index	R	
SSID	O	SSID of AP or ad hoc network.
Network Key Index	O	
<other…>	O	Multiple attributes are permitted .
Authenticator	R	

7.5.5. ResetSTA and RebootSTA Messages

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

Attribute	R/O	Notes
Version	R	0x10 = version 1.0, 0x11 = version 1.1, etc.
Message Counter	R	
Enrollee Nonce	R	
Registrar Nonce	R	
<other…>	O	Multiple attributes are permitted .
Authenticator	R	

8. 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.

8.1. Requirements for USB Flash Drives (UFD)

Wi-Fi Protected Setup 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

8.2. Enrollee Requirements for USBA OOB Interfaces

Wi-Fi Protected Setup devices must support the following hardware requirements to ensure interoperability with UFD devices:

- Easily accessible USB Host Port (USB version 1.1 or higher)
- Support WPA-PSK 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 Protected Setup 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 Protected Setup 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__XXXXXXXXXXXX__XXX__XXX__XXXXXXXXXXXX__XXX__XXX__XXXXXXXXXXXX___XXX__XXX__XXXXXXXXXXXX....

8.3. Firmware and Software Requirements

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

8.3.1. 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 must 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.

8.3.2. 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.

Payload of the UFD Unencrypted Settings File

Attribute	R/O	Notes
Version	R	As defined in section 11
Credential	R	As defined in section 11
<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 must 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.

8.3.3. 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 OOB 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 must be set to 0x0005 (Registrar-specified). In this case, the Enrollee must 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.

Payload of the Enrollee Device Password and Key Hash File

Attribute	R/O	Notes
Version	R	As defined in section 11
OOB Device Password	R	As defined in section 11
<other…>	O	Multiple attributes are permitted

9. NFC Out-of-Band Interface Specification

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

9.1. Disclaimer

As the referenced NFC Forum specifications may be updated or changed in the future by the NFC Forum, the current specification may be updated to reflect these changes. If there are any conflicts between the NFC section of the Wi-Fi Protected Setup specification and the relevant NFC Forum specifications, the NFC Forum specifications are the normative reference.

If not otherwise stated, the data formats and protocols used for the data exchange between and with NFC devices and for storing data on NFC compatible memory cards shall be specified in documents released by the NFC Forum.

The Near Field Communication (NFC) Forum is a non-profit industry association to advance the use of NFC short-range wireless interaction in consumer electronics, mobile devices and PCs.

The NFC Forum is promoting implementation and standardization of NFC technology to ensure interoperability between devices and services. The NFC technology is standardized in ISO/IEC18092.

9.2. Overview

NFC stands for "Near Field Communication". It is a contactless technology designed for very short-range operation – approximately 10cm or less. NFC is compliant with today's field proven contactless smart card technology.

The main aspects that make NFC different and complementary to any (wireless) network technology are:

1. **Short distance:** NFC is designed on purpose to work up to a distance of approximately 10cm or less. This is to ensure that the intentional action of the user - bringing two NFC devices close to each other - is needed to trigger/initiate the communication.
2. **Communication with NFC Tokens:** NFC works in the conventional way between powered devices and additionally allows communication to non self-powered devices (without battery) like contactless smart cards.

The following terms will be used throughout this section

- **NFC Interface**
  Contactless interface of an NFC Device.
- **NFC Token**
  A physical entity compliant with one of the mandatory NFC Forum tag specifications. An NFC Token cannot communicate with other NFC Tokens, but its content can be read or written by an NFC Device.

  The shape of an NFC Token is not defined. It can have any shape, e.g. card-shape, tag-shape or coin-shape, or can be integrated into a device housing.
- **NFC Device**
  A device that acts as a contactless reader/writer. NFC Devices can communicate directly with each other and/or with NFC Tokens.

An NFC Device can have its NFC Interface permanently activated or not. If the NFC Interface is not permanently on it may be implicitly or explicitly activated.

9.3. NFC Use Cases

NFC can be deployed in different ways for simple WLAN configuration.

From a user interaction point of view, the user has to deal with two main situations:

- using an external NFC NFC Token
- deploying direct NFC communication between Enrollee and Registrar (i.e. "touching" the devices).

From an implementation point of view, device vendors have the following opportunities:

- Hardware implementation
  - NFC device
  - integrated NFC Token
  - external NFC Token
- The NFC capabilities can be exploited for simple WLAN configuration in two ways:
  - provide the Enrollee device password out-of-band
  - provide the configuration information out-of-band

9.3.1. NFC Password Token

Device vendors can decide to provide their device with an external NFC Token storing an OOB Device Password as specified in section 11. This password is considerably longer than the user would be expected to type (e.g. a 32B random value instead of 8 digits).

The Registrar detects the availability of an NFC OOB Device Password Token from the content of the "Config Methods" parameter (specified in section 11) provided in M1 or in the Probe-Responses (from AP) or Probe-Request (from Enrollee). This allows the Registrar to prompt or otherwise guide the user to provide the token. If an Enrollee indicates it supports an (external or integrated) NFC Token, this is assumed to be an NFC Password Token (containing an OOB Device Password).

9.3.2. Touching Devices

Vendors of portable devices may want to deploy the intuitive NFC user interaction of touching devices. Assuming that the Registrar includes an NFC Interface, implementation options for the "Touching Devices" use case are:

- NFC Password Token integrated into the device housing (protocol behavior analogous to section **Error! Reference source not found.**), which is touched to the Registrar to convey the OOB Device Password.

  The Registrar can detect the presence of an integrated NFC Password Token from the "Config Methods" attribute of the Enrollee (specified in section 11). If this method is chosen, the Registrar prompts (or otherwise guides) the user to touch the devices.

- NFC Device.

  If both the Enrollee and the Registrar are NFC Devices, the configuration data can be exchanged over the NFC Interface. In this case, the messages M1 and M2 are exchanged via NFC, and the encrypted configuration data is included in M2.

The Registrar can detect the presence of an NFC Interface on both sides from the content of the "Config Methods" parameter (specified in section 11) provided in M1 or in the Probe-Responses (from AP) or Probe-Request (from Enrollee). Given this discovery information the Registrar can prompt or otherwise guide the user to touch the devices together.

The NFC exchange may be implemented independently of the in-band device discovery. In this case configuration is also possible if the WLAN interface is off. 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). Note that the Probe-Request messages should still be sent to allow fallback to the in-band configuration method.

To avoid misleading instructions to the user to "touch devices" in cases where this is not possible or practical, the Registrar should only choose the "touching devices" method if the Registrar itself is portable or if the Enrollee includes the attribute Portable Device = TRUE in its probe request and/or M1 message.

9.3.3. NFC Configuration Token

An NFC NFC Configuration Token contains unencrypted configuration data for a WLAN. Enrollees with an NFC Interface can be configured by a simple touch with the NFC Configuration Token.

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 token. Subsequently, this token can be used to directly 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 token to configure Enrollees.

The use of an NFC Configuration Token will allow the SimpleConfig method to be used with legacy APs (with neither NFC nor in-band support for SimpleConfig).

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

9.4. Generic Requirements for NFC OOB Support

9.4.1. New Devices (Enrollee or AP) Requirements

An Enrollee or AP can support the use of NFC for SimpleConfig with the following options.

1. The Enrollee or AP uses a (long) password for the Registration Protocol, stored in an NFC Password Token.The NFC Password Token is either integrated in the device housing or is physically separated.

   This option does not require the presence of an NFC Interface in the Enrollee or AP.

2. The Enrollee or AP is an NFC Device capable of communicating directly with an NFC-enabled Registrar and capable of reading an NFC Token. After being touched, the Enrollee or AP must be able to exchange M1/M2 with the Registrar via the NFC Interface. The Enrollee or AP must also be capable of reading the configuration data from an NFC Configuration Token.

9.4.2. Registrar Requirements

In case the Registrar shall support the use of NFC for Wi-Fi Protected Setup, it must be an NFC Device.

- If the use case "NFC Password Token" is supported, the Registrar must be capable of reading a password from an NFC Password Token.
- If the use case "NFC Configuration Token" is supported, the Registrar must be able to write configuration data to an NFC Configuration `Token`
- If the use case "Touching Devices" is supported, the Registrar must be able to exchange M1/M2 directly with Enrollee being an NFC Device

9.5. Hardware Requirements

9.5.1. Requirements for NFC Tokens

The following hardware requirements must be fulfilled by an NFC Password Token or an NFC Configuration Token, if used for SimpleConfig as outlined in this proposal:

- It must be compatible to at least one of the mandatory tag formats defined by the NFC Forum.
- The NFC Password Token or NFC Configuration Token needs enough memory space to store the data files (Note: the values below are indicative and have to be extended by protocol overhead of the lower layers)
    - For the NFC Password Token (see **Error! Reference source not found.**): the Enrollee public key hash and device password (e.g. ~ 58 bytes)
    - For the NFC Configuration Token (see **Error! Reference source not found.**): unencrypted configuration data (e.g. ~ 108 bytes)

9.5.2. Requirements for an NFC Device

The following hardware requirements must be fulfilled by an NFC Device, if used for SimpleConfig.

- It must be able to read at least one of the mandatory tag formats defined by the NFC Forum.

9.6. Firmware and Software Requirements

9.6.1. NFC Password Token

The TLV encoded data (as defined in section 7) must be embedded into an NDEF record using the MIME type ‘application/vnd.wfa.wsc’.

The NDEF data is stored on the NFC Password Token following the corresponding NFC Forum tag specification.

Payload of the NDEF record in case of an NFC Password Token

Attribute	R/O	Notes
Version	R	As defined in section 11
OOB Device Password	R	As defined in section 11

9.6.2. NFC Configuration Token

The TLV encoded data (as defined in section 7) must be embedded into a NDEF record using the MIME type ‘application/vnd.wfa.wsc’.

The NDEF data is stored on the NFC Token following the corresponding NFC Forum tag specification.

Payload of the NDEF record in case of an NFC Configuration Token

Attribute	R/O	Notes
Version	R	As defined in section 11
Credential	R	As defined in section 11

9.6.3. NFC Device

The following requirements have to be fulfilled by an NFC Device, if used for SimpleConfig.

- For the use case "NFC Password Token" it must be able to read NDEF records as specified in section 9.6.1.
- For the use case "NFC Configuration Token" it must be able to read and write NDEF records as specified in section 9.6.2.
- For the use case "Touching Devices", the WLAN configuration data is requested by the Enrollee (device or AP) by sending an M1 message as binary data in TLV format (specified in section 7.3.1) over the NFC interface as described in the specifications of the NFC Forum. The data are transferred as binary data in TLV format as specified in Section 7.1.

  In response, an M2 message (as binary data in TLV format, specified in section 7.1) is transferred by the Registrar.

  If the NFC Device is an AP, it may send the encrypted configuration data within an M7 message (as binary data in TLV format, specified in section 7.3.8) back to an NFC-enabled Registrar. This option can be used if the AP is already configured and shall keep its configuration (e.g. if adding a second Registrar). In this case, the Registrar may not send configuration data in M2.

9.7. Informative: NFC Forum specifications

The information in this paragraph is intended to give an overview of the relevant NFC Forum specifications. The normative reference is available at the NFC Forum.

9.7.1. NFC Data Exchange Format (NDEF)

The **NFC Data Exchange Format (NDEF)** is a data format to ensure interoperability between NFC devices. NDEF is specified by the NFC Forum.

The NDEF defines the data structure framework to exchange application or service specific data in an interoperable way.

An NDEF packet may include a set of NDEF records. Each record contains a type, length and value (TLV) component.

9.7.2. NDEF mapping documents

The NFC Forum selected a range of different NFC contactless tokens, which have to be supported by compliant NFC devices. The NDEF mapping documents describe how NDEF packets are stored on these different tokens in order to guarantee an interoperable ecosystem.The ‘NDEF Mapping documents’ are available at the NFC Forum.

10. PushButton Configuration

10.1. Introduction

This section specifies an optional method called PushButton Configuration (PBC) 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 MUST NOT support using PBC to addian external Registrar or to derive keys for subsequent AP management.

10.2. 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 10 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, but not shown here. Section 10.3 contains a more detailed explanation of the protocol.

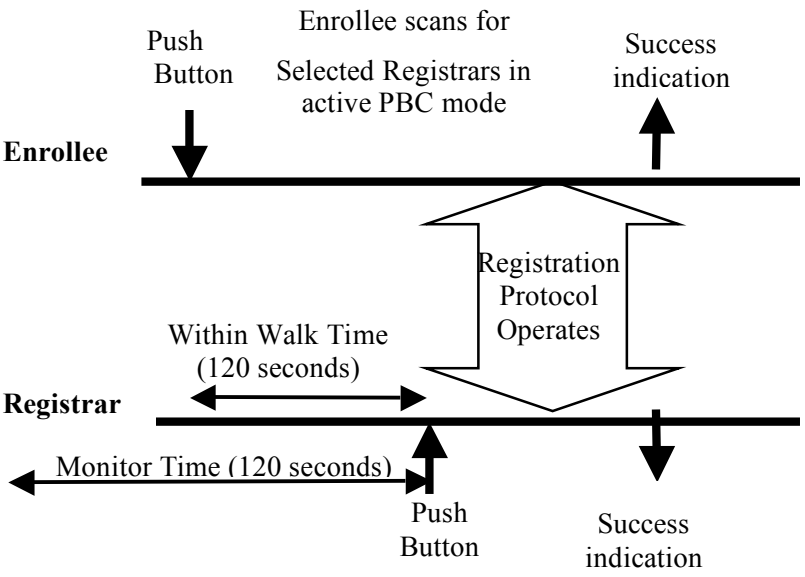


Figure 10 PBC User Actions

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 must 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 must be pushed within Walk Time or the Registrar will indicate failure.

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 using PBC mode. The AP informs Enrollees that the Selected Registrar is in PBC mode using Probe Response messages.

10.3. PBC Technical Description

The button press or equivalent trigger event on the Enrollee causes it to actively search for a Registrar in PBC mode. However, the Enrollee MUST not proceed immediately with the Registration Protocol when it first discovers a Registrar. Instead, the Enrollee MUST complete a scan of all 802.11 channels that it supports to discover if any other nearby Registrars are in 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. During this scan, the Enrollee MUST abort its connection attempt and signal a "session overlap" error to the user if it discovers more than one Registrar in PBC mode. 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 PBC mode. If the dual-band station does discover more than one Registrar in PBC mode, one 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 PBC mode is found after a complete scan, the Enrollee can immediately begin running the Registration Protocol with it in PBC mode. The station must receive the Wi-Fi Protected Setup IE from the Registrar in order to engage with the Registrar using the PBC method.

The button press or equivalent trigger event on the Registrar causes it to first check whether more than one Enrollee PBC probe request has been received by the Registrar. The Registrar must examine whether such a request has been received within 120 seconds prior to the PBC button press on the Registrar. This window is called the PBC Monitor Time. If more than one Enrollee PBC probe request has been received within the Monitor Time interval, the Registrar MUST signal a session overlap" error and refuse to enter PBC mode or 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 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 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 must only remain in PBC mode for the duration of Walk Time after its PBC button (or equivalent trigger) has been pressed before reverting to non-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.

When an AP receives a Selected Registrar and Device Password ID indicating PBC mode from a Registrar, it MUST automatically remove this information and no longer include it in probe responses after an interval of Walk Time has elapsed.

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

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 PBC active. When in PBC mode, the Registrar shall respond to PBC M1 messages with UUID-E values matching the UUID-E from the PBC probe request message. The Registrar's response is an M2 message denoting via the DevicePassword ID attribute that it is in the active PBC state. 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 (PIN).

Figure 11 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 its active PBC state. As long as the Enrollee's button is pressed before the Walk Time timeout, then 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 push button 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 PBC method in addition to the mandatory PIN method.

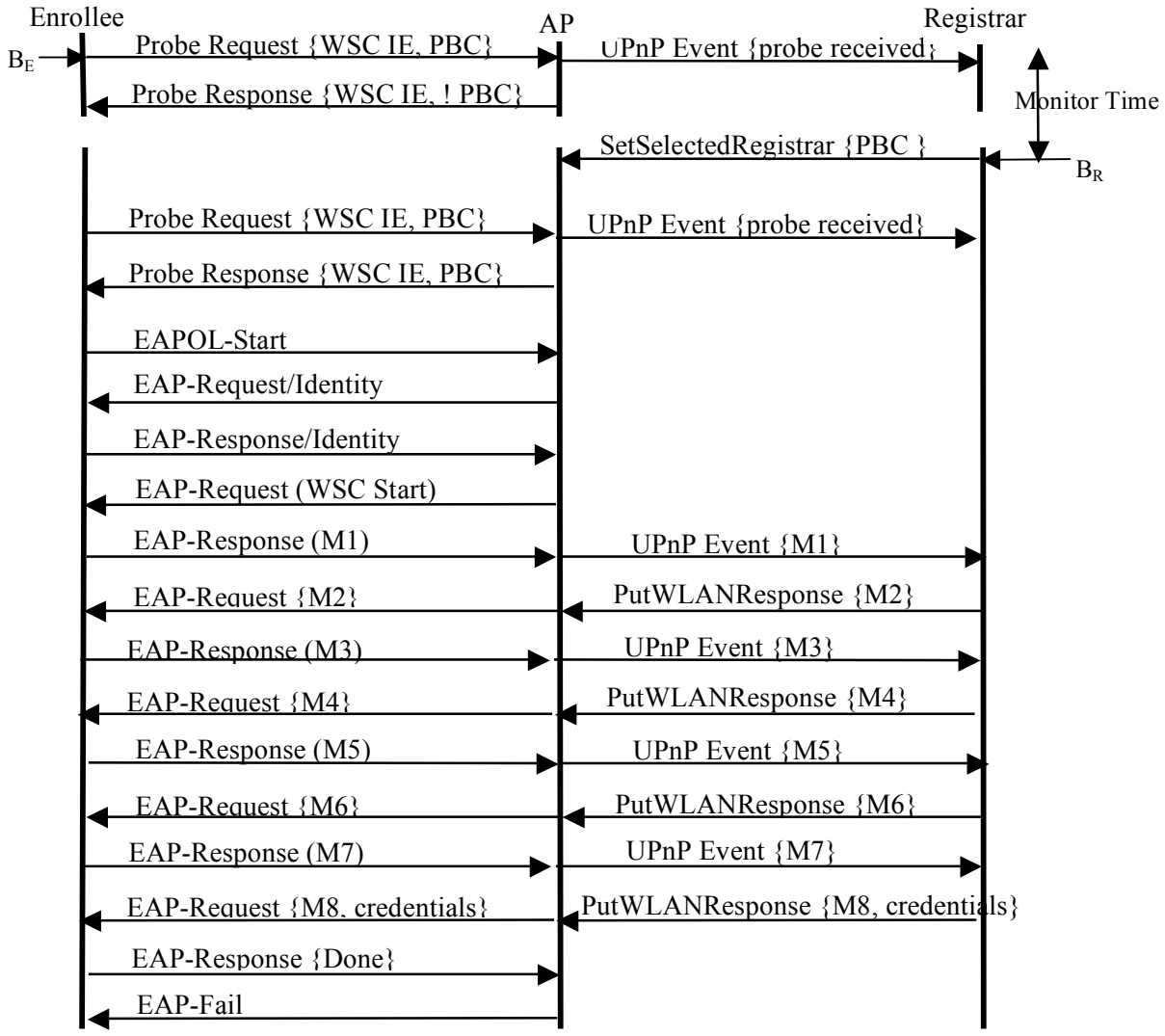


Figure 11 PBC message exchange

10.4. User Feedback

The PBC device shall indicate the status of PBC to the user through a UI. The minimum set of PBC status information is described in this section. For devices without a rich UI, such as a Registrar built into an AP or a media converter device, the minimum required UI is a single color LED. For a richer user experience, multicolor or multiple LED, or a small LCD panel is recommended. The Registrar or Enrollee with a rich UI should have the capability to indicate more detailed status information to user(s) than the minimum set described here.

When PBC is used, user feedback must be provided to communicate the following conditions.

- InProgress
    - Condition: the protocol is searching for a partner, connecting, or exchanging network parameters
    - Recommended user action: wait for protocol to finish
- Error
    - Condition: some error occurred which was not related to security, such as failed to find any partner or protocol prematurely aborted.
    - Recommended user action: push buttons to start protocol again
- Session Overlap Detected
    - Condition: protocol detected overlapping operation: could be a security risk
    - Recommended user action: wait, then re-attempt. If the condition recurs, refer the user to PIN-based or OOB channel configuration method(s) in user manual or Registrar's screen.
- Success
    - Condition: protocol is finished: no uncorrectable errors occurred. Normally after guard time period.
    - Recommended user action: If seen on both Registrar and Enrollee, the user may immediately use devices for their intended application(s)

The user is not **required** to observe the user feedback in order for the protocol to be complete. The user should, however, be encouraged to verify user feedback on both the Registrar and on the Enrollee to confirm that the setup operation succeeded.

If LEDs are used to provide user feedback, the following timing and color patterns (if multi-color) must be followed.

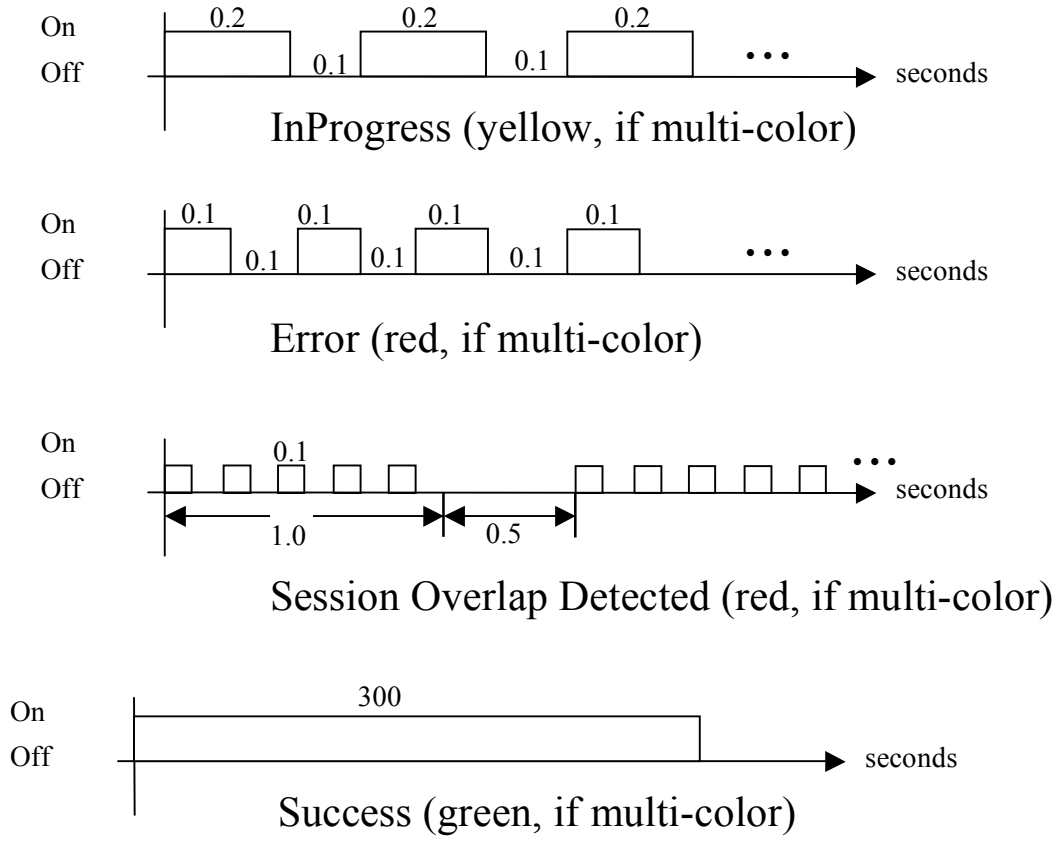


Figure 12 LED Feedback Patterns

10.5. 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 PBC state 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 Protected Setup 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.

11. Data Element Definitions

The following table enumerates the various attribute types defined for Wi-Fi Protected Setup. 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).

Description	ID (Type)	Length
AP Channel	0x1001	2B
Association State	0x1002	2B
Authentication Type	0x1003	2B
Authentication Type Flags	0x1004	2B
Authenticator	0x1005	8B
Config Methods	0x1008	2B
Configuration Error	0x1009	2B
Confirmation URL4	0x100A	<=64B
Confirmation URL6	0x100B	<=76B
Connection Type	0X100C	1B
Connection Type Flags	0X100D	1B
Credential	0X100E	
Device Name	0x1011	<= 32B
Device Password ID	0x1012	2B
E-Hash1	0x1014	32B
E-Hash2	0x1015	32B
E-SNonce1	0x1016	16B
E-SNonce2	0x1017	16B
Encrypted Settings	0x1018	
Encryption Type	0X100F	2B
Encryption Type Flags	0x1010	2B
Enrollee Nonce	0x101A	16B
Feature ID	0x101B	4B
Identity	0X101C	<= 80B
Identity Proof	0X101D	
Key Wrap Authenticator	0x101E	8B
Key Identifier	0X101F	16B

MAC Address	0x1020	6B
Manufacturer	0x1021	<= 64B
Message Type	0x1022	1B
Model Name	0x1023	<= 32B
Model Number	0x1024	<= 32B
Network Index	0x1026	1B
Network Key	0x1027	<= 64B
Network Key Index	0x1028	1B
New Device Name	0x1029	<= 32B
New Password	0x102A	<= 64B
OOB Device Password	0X102C	<= 58
OS Version	0X102D	4B
Power Level	0X102F	1B
PSK Current	0x1030	1B
PSK Max	0x1031	1B
Public Key	0x1032	192B
Radio Enabled	0x1033	Bool
Reboot	0x1034	Bool
Registrar Current	0x1035	1B
Registrar Established	0x1036	Bool
Registrar List	0x1037	<=512B
Registrar Max	0x1038	1B
Registrar Nonce	0x1039	16B
Request Type	0x103A	1B
Response Type	0x103B	1B
RF Bands	0X103C	1B
R-Hash1	0X103D	32B
R-Hash2	0X103E	32B
R-SNonce1	0X103F	16B
R-SNonce2	0x1040	16B
Selected Registrar	0x1041	Bool
Serial Number	0x1042	<= 32B
Wi-Fi Protected Setup State	0x1044	1B

SSID	0x1045	<= 32B
Total Networks	0x1046	1B
UUID-E	0x1047	16B
UUID-R	0x1048	16B
Vendor Extension	0x1049	<= 1024B
Version	0x104A	1B (int)
X.509 Certificate Request	0x104B	
X.509 Certificate	0x104C	
EAP Identity	0x104D	<= 64B
Message Counter	0x104E	8B
Public Key Hash	0x104F	20B
Rekey Key	0x1050	32B
Key Lifetime	0x1051	4B
Permitted Config Methods	0x1052	2B
Selected Registrar Config Methods	0x1053	2B
Primary Device Type	0x1054	8B
Secondary Device Type List	0x1055	<= 128B
Portable Device	0x1056	Bool
AP Setup Locked	0x1057	Bool
Application Extension	0x1058	<= 512B
EAP Type	0x1059	<= 8B
Initialization Vector	0x1060	32B
Key Provided Automatically	0x1061	Bool
802.1X Enabled	0x1062	Bool
AppSessionKey	0x1063	<=128B
WEPTransmitKey	0x1064	1B
<Reserved for WFA>	0x1065 – 0x1FFF	
<Unavailable>	0x000 – 0x0FFF, 0x2000 – 0xFFFF	

Table 2: Master Table – Data Component Set

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 should enter this state if it believes a brute force attack is underway against the AP's PIN.

When the AP is in this state, it MUST 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.

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

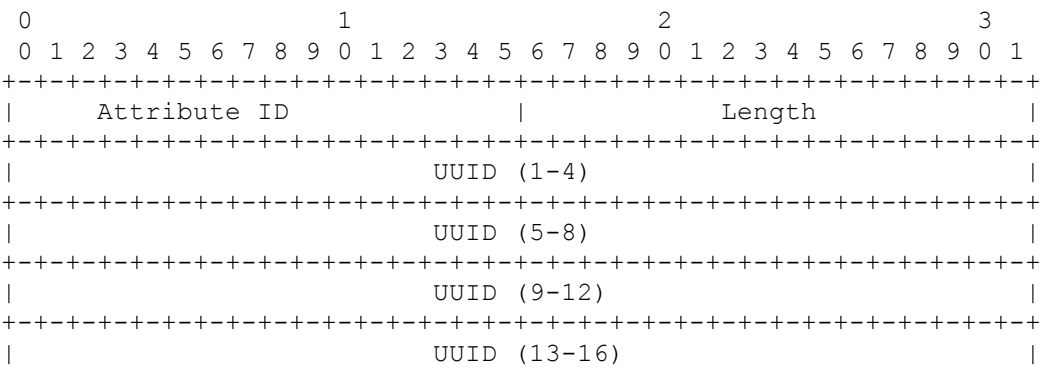
The AppSessionKey attribute allows the exchange of application specific session keys and may be used as an alternative to calculating AMSKs.

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 6.3 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)



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                            Data...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

One use of this Application Extension mechanism is to permit a Wi-Fi Protected Setup 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 Protected Setup 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 Protected Setup are:

UUID=0xA6F6D81FB26941e2A72EC0B702248E90

Data=TLV attribute list below:

Attribute	R/O	Notes
Version	R	As defined in section 11
OOB Device Password	O	May be omitted if OOB Device Password has already been received from peer device.
SSID	O	Included if SSID is known by sender.
<other…>	O	

Note that this approach passes the OOB 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.

Association State Values

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

Authentication Type

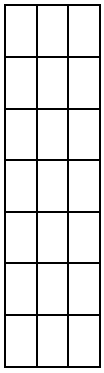
This variable contains a specific value from the Authentication Types table for the Enrollee (AP or station) to use.

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 – Authentication Types

Value	Description
0x0001	Open
0x0002	WPAPSK
0x0004	Shared
0x0008	WPA
0x0010	WPA2
0x0020	WPA2PSK



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 Easy Setup version 1.0 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.

Config Methods

The Config 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 Config Methods, APs and STAs that support the UPnP Management Interface must support the Permitted Config Methods attribute, which is used to control the Config Methods that are enabled on that AP.

Table – Config Methods

Value	Hardware Interface
0x0001	USBA (Flash Drive)
0x0002	Ethernet
0x0004	Label
0x0008	Display

0x0010	**External NFC Token**
0x0020	**Integrated NFC Token**
0x0040	**NFC Interface**
0x0080	**PushButton**
0x0100	**Keypad**

Configuration Error

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

Configuration Error	**Description**
0	**No Error**
1	**OOB Interface Read Error**
2	**Decryption CRC Failure**
3	**2.4 channel not supported**
4	**5.0 channel not supported**
5	**Signal too weak**
6	**Network auth failure**
7	**Network association failure**
8	**No DHCP response**
9	**Failed DHCP config**
10	**IP address conflict**
11	**Couldn't connect to Registrar**
12	**Multiple PBC sessions detected**
13	**Rogue activity suspected**
14	**Device busy**
15	**Setup locked**
16	**Message Timeout**
17	**Registration Session Timeout**
18	**Device Password Auth Failure**

The Device busy error is returned if the sending device is unable to respond to the request 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.

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 must 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 must 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 – Connection Types

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

Credential

This is a compound attribute containing a single WLAN Credential. Note: There can be multiple Network Keys in a single Credential attribute by repeating the Network Key Index and attributes that follow it. Alternatively, there can be multiple instances of the Credential attribute. Generally, multiple keys in a single Credential for a single SSID should be used, and multiple Credential attributes for separate SSIDs should be used. The following table lists the attributes in Credential:

Table – Credential Attributes

Attribute	R/O	Notes, Allowed Values
Network Index	R	
SSID	R	SSID of AP or ad hoc network.
Authentication Type	R	
Encryption Type	R	

Network Key Index	O	
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	
<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 six predefined values and ten 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 OOB Device Password.

Value	**Description**
0x0000	**Default (PIN)**
0x0001	**User-specified**
0x0002	**Machine-specified**
0x0003	**Rekey**
0x0004	**PushButton**
0x0005	**Registrar-specified**
0x0006 – 0x000F	**Reserved**

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 Protected Setup Registration Protocol (refer to section 6.10.1), 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

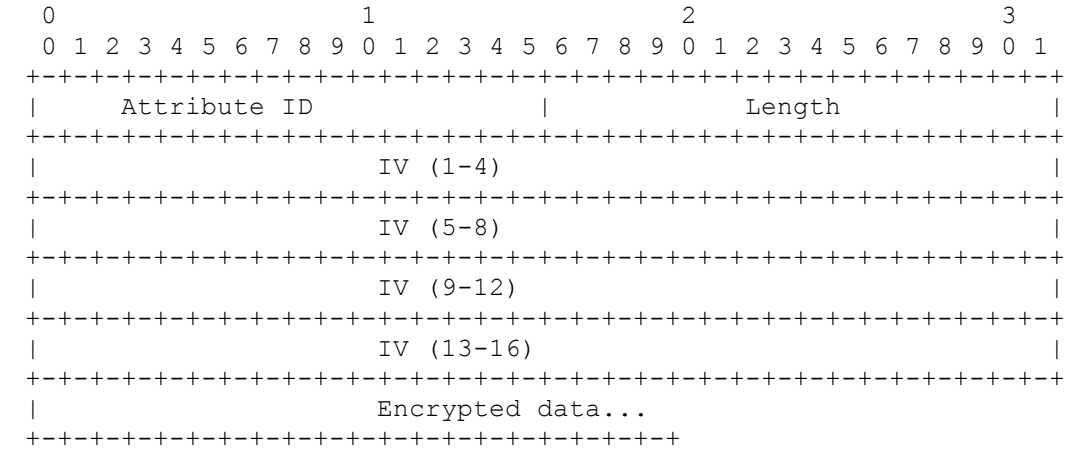
E-SNonce2

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 Protected Setup TLV attributes. The last attribute in the encrypted set is a Key Wrap Authenticator computed according to the procedure described in section 6.5.

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.



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

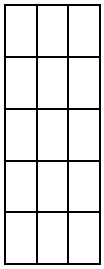
This attribute contains a specific value from the Encryption Type Flags table for the Enrollee (AP or station) to use.

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 –Encryption Types

Value	Description
0x0001	None
0x0002	WEP
0x0004	TKIP
0x0008	AES



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 6.5.

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 – 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 used to get and set network settings for devices that host more than one network. The default value is 1 and refers to the primary WLAN network on the device.

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.

Network Key

Authentication	Encryption	Network Key Type
None	None	0 ASCII characters
WPAPSK (Passphrase)	TKIP/AES	8 – 63 ASCII characters
WPAPSK	TKIP/AES	64 Hex characters

Shared/Open	**WEP**	**5 or 13 ASCII characters** **10 or 26 Hex characters**

Network Key Index

This variable specifies a particular Network Key instance.

New Device Name

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

New Password

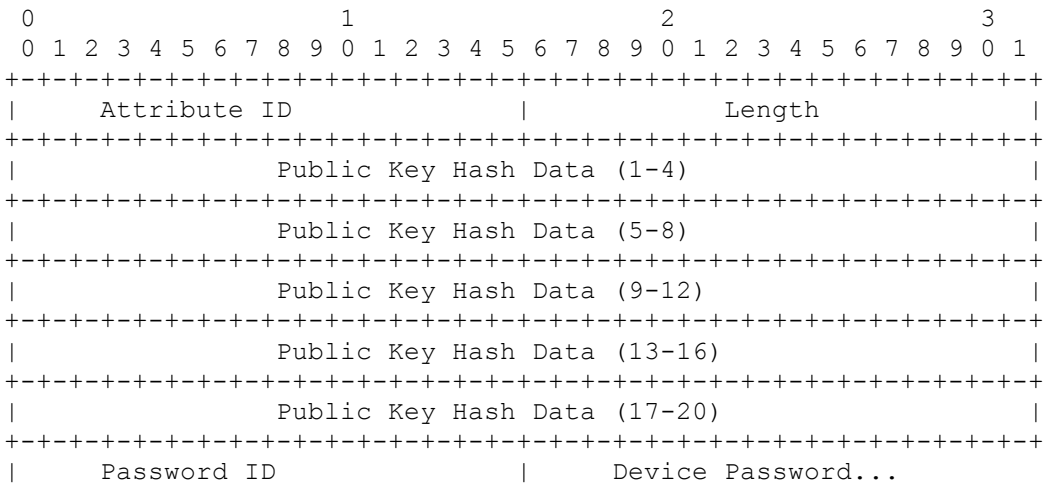
This variable is used to set a new password on the Enrollee.

OOB Device Password

The OOB Device Password attribute contains a fixed data structure intended to be compact enough to fit into small-capacity out-of-band channels. The OOB Device Password attribute is defined below. 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 OOB Device Password attribute (including the Attribute ID and Length). 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. The Password ID of an OOB Device Password should be chosen at random, but it must not be one of the predefined or reserved Device Password ID values.

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 must match that of the Enrollee's Public Key attribute in M1. If this value does not match, then the Registrar MUST 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 must 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 must match that of the Registrar's Public Key attribute in M2. If this value does not match, then the Enrollee MUST 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 must copy the Password ID value into the Device Password ID attribute of M1.



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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 Config Methods

This variable contains the same data structure as Config Methods, but it indicates which of the Config 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 Config Methods corresponding to a particular method is set to zero, the device MUST 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 Config Method is disabled using Permitted Config Methods, only the enabled methods are reported in the discovery messages (probe request, probe response, M1, and M2).

Portable Device

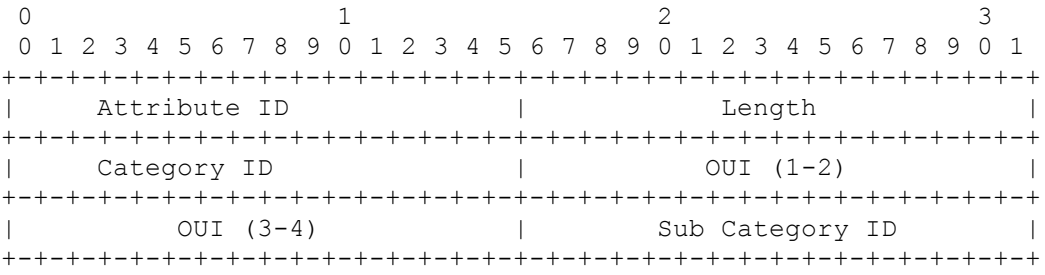
This variable indicates that the device is portable. It may be used to help determine if it will be possible to perform actions such as touching devices together for NFC-based configuration.

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:



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.

Category	ID Value	Sub Category	ID Value
Computer	1	PC	1
		Server	2

		Media Center	3
Input Device	2		
Printers, Scanners, Faxes and Copiers	3	Printer	1
		Scanner	2
Camera	4	Digital Still Camera	1
Storage	5	NAS	1
Network Infrastructure	6	AP	1
		Router	2
		Switch	3
Displays	7	Television	1
		Electronic Picture Frame	2
		Projector	3
Multimedia Devices	8	DAR	1
		PVR	2
		MCX	3
Gaming Devices	9	Xbox	1
		Xbox360	2
		Playstation	3
Telephone	10	Windows Mobile	1

PSK Current

This variable represents the number of allocated PSKs on the AP for a particular Network Index.

PSK Max

This variable represents the maximum number of PSKs supported by the AP for a particular Network Index.

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 6.3.

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 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 Protected Setup 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 must 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.

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

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.

Response Type Value	Description
0x00	**Enrollee, Info only**
0x01	**Enrollee, open 802.1X**
0x02	**Registrar**
0x03	**AP**

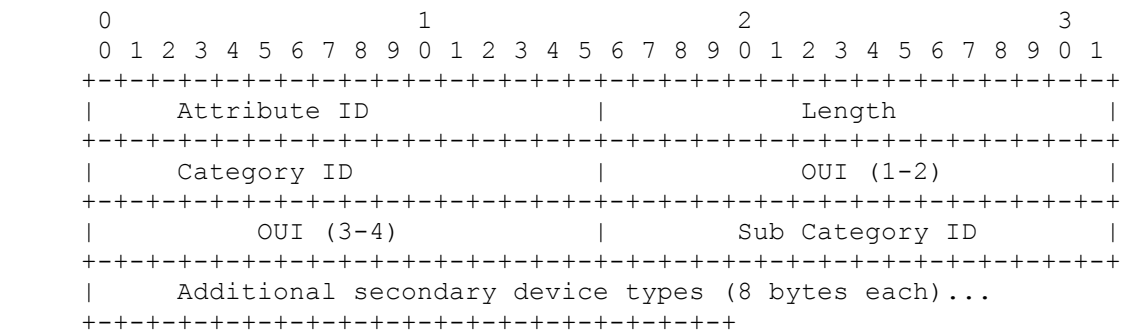
RF Bands

This attribute is **Table 6.1.3 – RF Band** sage exchange to permit end points and proxies to communicate over a consistent radio interface. 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.

RF Band Value	Description
0x01	**2.4GHz**
0x02	**5.0GHz**

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:



Selected Registrar

This field indicates that a Registrar has been selected by a user and that an Enrollee should proceed with setting up an 802.1X uncontrolled data port with the Registrar.

Selected Registrar Config Methods

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

Serial Number

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

Wi-Fi Protected Setup State

The 'Wi-Fi Protected Setup State' attribute in WSC IEs contained in beacon and probe response indicates if a device is configured.If an AP is shipped from the factory in the Not-Configured state (Wi-Fi Protected Setup State set to 0x01), then the AP must transition to the Configured state (Wi-Fi Protected Setup 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 (Figure 9).

2. Automatic configuration by internal registrar.
The AP receives the WSC_Done response in the Enrollee Registration Process (Figure 8) 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 unconfigured to configured in the case that a neighbouring 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 Protected Setup 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 Protected Setup State set to 0x01), then a factory reset must revert the Wi-Fi Protected Setup State to Not Configured.

If the AP is shipped from the factory pre-configured with WPA2-Personal mixed mode and a randomly generated key, the Wi-Fi Protected Setup State may be set to 'Configured' (0x2) to prevent an external registrar from overwriting the factory settings. A factory reset must restore the unit to the same configuration as when it was shipped.

Table - Wi-Fi Protected Setup State

Wi-Fi Protected Setup State Value	Description
0x00	**Reserved**
0x01	**Not configured**
0x02	**Configured**
0x03-0xFF	**Reserved**

SSID

This variable represents the Service Set Identifier or network name. This is used by the client to connect to the wireless network. This variable is read/write.

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

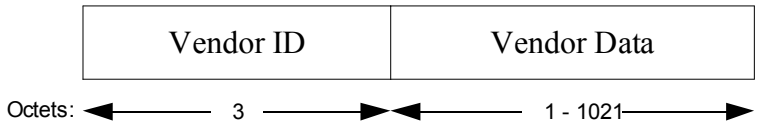
The universally unique identifier (UUID) element is a unique GUID generated by the Registrar. It uniquely identifies an operational device and should survive reboots and resets. The UUID is provided in binary format. If the device also supports UPnP, then the UUID corresponds to the UPnP UUID.

Vendor Extension

This variable permits vendor extensions in the Wi-Fi Protected Setup TLV framework. The Vendor Extension figure illustrates the implementation of vendor extensions. Vendor ID is the SMI network

management private enterprise code. Note: For a Vendor Extension in 802.11 management frames, the Vendor Data field must not exceed 246 Bytes.

Vendor Extension Encapsulation



Version

Version specifies the Easy Setup version. 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.

WEP Transmit Key

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

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.

12. Conclusion

Wi-Fi Protected Setup is a framework for securely introducing wireless devices. Instead of glossing over the problem of initial trust bootstrapping, Wi-Fi Protected Setup focuses squarely on this problem. Achieving a good user experience without sacrificing security are the two primary goals of Wi-Fi Protected Setup. The framework also supports subsequent bootstrapping of applications and other network credentials based on the initial credential established during registration. Multiple different out-of-band and in-band communication channels can be used, so the existing I/O capabilities of devices can be used as much as possible.

Definitions and Acronyms

Unique terms, acronyms, and associated definitions are listed in the table below.

Term	Definition
AES	Advanced Encryption Standard
AES CBC	AES “Counter with CBC-MAC”, a mode that provides both authentication and encryption

13. Appendix: Additional Setup Scenarios

This section describes advanced use cases such as Enrollee introduction with multiple external Registrars. 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.

In-band Setup Using Multiple External Registrars

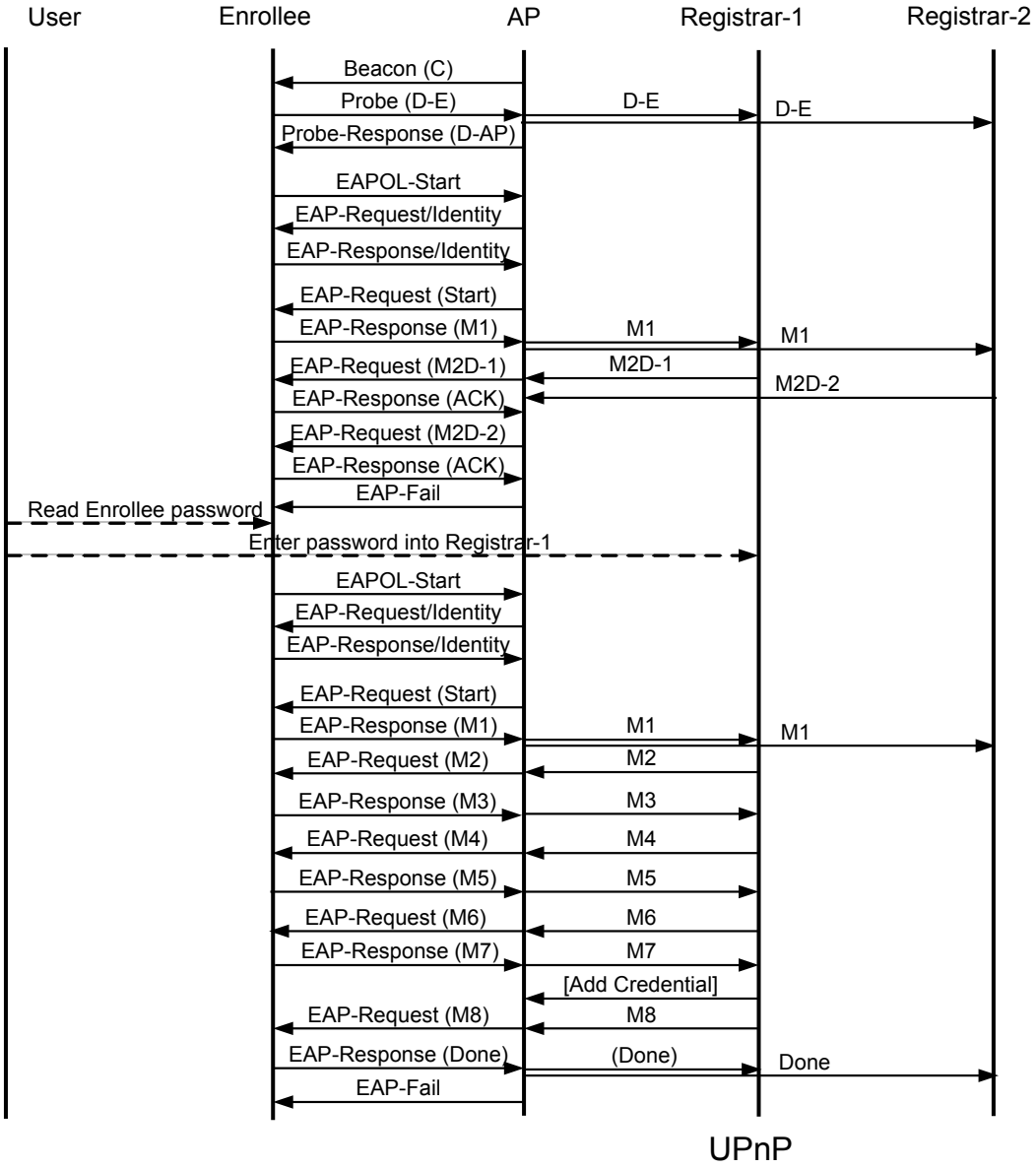


Figure 13: In-band Setup Using Multiple External Registrars

Setup steps

The scenario shown in Figure 13 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 a UPnP event.
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 broadcast to all external Registrars as a UPnP event.
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-Fail 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. Enrollee reconnects and restarts the 802.1X authentication. This time, Registrar 1 sends an M2 message rather than an M2D message.
9. 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.

14. Appendix: Out-of-Band Channel Considerations

This section provides guidelines and suggestions relating to the use of out-of-band channels with Wi-Fi Protected Setup. Its purpose is to highlight important security issues related to the properties of various channel types that can be used in the Wi-Fi Protected Setup 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 3 and the discussion in this section examines the implications of using an out-of-band channel for either M1, M2, or both.

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

Table 3: Out-of-band Channels Use Cases

- 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 OOB 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 OOB 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 OOB

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 OOB 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.