SCTE•ISBE CABLE-TEC EXPO® VIRTUAL EXPERIENCE » OCTOBER 12-15 2020

2020 Fall Technical Forum SCTE·ISBE • NCTA • CABLELABS®

# Wi-Fi Passwords

## The Evolving Battle Between Usability and Security

A Technical Paper prepared for SCTE•ISBE by

**Craig Pratt**
Lead Software Engineer, Security Technologies
CableLabs
858 Coal Creek Circle, Louisville, CO 80027
+1 303.661.3408
c.pratt@cablelabs.com

**Darshak Thakore**
Principal Software Architect, Security Technologies
CableLabs
858 Coal Creek Circle, Louisville, CO 80027
d.thakore@cablelabs.com

**Jacob Gladish**
Director of Software Development
Comcast
1701 JFK Boulevard, Philadelphia, PA 19103
jacob_gladish@comcast.com

 

# Table of Contents



## List of Figures



 

# 1. Introduction

By all measures, Wi-Fi is a phenomenal success. As broadband availability and capacity increased, the speed of Wi-Fi also increased. As the number and nature of devices supported by Wi-Fi expanded, the range and capabilities also expanded. And when Wi-Fi entered the corporate/enterprise workspace, accommodations were added to allow for Wi-Fi credentials to be provided via integration with enterprise-level user authentication systems.

## 1.1. One Password to Rule Them All…

For most Wi-Fi networks, credential provisioning comes down to the question: "What's the Wi-Fi password?", followed by the tedious task of verifying the spelling and punctuation. And while there have been various mechanisms created to share Wi-Fi passwords across devices, the vast majority of Wi-Fi networks utilize a single shared password.

The implications of having a single credential for a Wi-Fi network have been known for years. With the first version of Wi-Fi security (Wired Equivalent Privacy or WEP), the fact that there was a single persistent key for the network (among other issues) led to a serious security vulnerability that would allow the key to be derived by simply observing a sufficient amount of network traffic. WEP password cracking was addressed in WFA Wi-Fi Protected Access 2 (WPA2) [3]. But even in WPA2, one authorized Station can observe the traffic of any other Station by observing its authentication exchange. And one issue is inescapable: once a password is shared, it cannot be unshared. The only remedy today for revoking a station's credentials on a single-password networks is to change the password and reprovisioning all devices that need access with the new password.

While reprovisioning all Stations on a Wi-Fi network might have been a practical (if not tedious) task in the past - with perhaps a half-dozen interactive devices on the network (laptops, smart phones, etc.) - today it is a virtual impossibility. IoT devices in particular have proliferated enormously in recent years and are notorious for having inconsistent means of provisioning Wi-Fi credentials. And their interfaces and documentation workflows are geared for initial "quick start" setup, not reprovisioning. Many devices even require a complete factory reset to be provisioned – leading to a cascade of issues with device reconfiguration, updating apps, and reassociating devices with their various cloud services.

## 1.2. The Evolution of Wi-Fi Credentials

There have been a variety of solutions proposed and implemented to help mitigate the single password issue: Multi-zone networks (e.g. "guest" networks) allow for one password to be used for resident users/devices and another for non-resident users/devices. However, the way guest networks are implemented requires multiple Wi-Fi networks (SSIDs) to be configured on a wireless Access Point (AP) – which either dedicates separate Wi-Fi channels to the guest network or increases the amount of overhead on shared channels. And as soon as the password for the resident zone is shared with a device or user, the zone can be compromised.

WPA2/3 Enterprise was designed to support the integration of enterprise environments utilizing centralized user provisioning systems with Wi-Fi provisioning. These user-level authentication systems were tailored for interactive enterprise devices (e.g. laptops and mobile devices). This allowed the use of enterprise management systems to manage Wi-Fi access. The same aspects that make WPA2/3 Enterprise well suited to enterprise environments, however, make it difficult to use for home/SOHO environments. For instance, while it can be natural to provision interactive devices such as laptops and mobile devices with user credentials, IoT devices are not as easily associated with a single user – and almost universally

lack support for WPA2/3 Enterprise. And the infrastructure required for WPA2/3 Enterprise support is too complex for the average user to configure and manage.

MAC address filtering solutions attempt to provide per-device in a different way: While a user/device may gain access to the network using a shared password credential, other components of the Wi-Fi Access Point can filter traffic based on the MAC address of individual device(s). Revoking "access" to a device can be done at-will and based on various criteria – such as time of day, the internet host(s) being accessed, or metering criteria (e.g. time on-line or data usage). These solutions are currently employed by many network providers and are the bane of teenagers across the Internet. But they are also easily defeated by credential sharing and MAC spoofing – and they don't prevent the observation of network traffic using the shared credential.

### 1.3. Goals for the Next Generation of Wi-Fi Authentication and Security

Ultimately what is needed for truly manageable Wi-Fi networks is a mechanism that allows each device to have a unique, verifiable identity and allows for the provisioning of credentials which are cryptographically strong, unique and revocable. And to help ensure adoption and make everyone's life easier, provisioning of devices should be as easy – if not easier – than the single-password method. Once individual identities and credentials can be associated with Wi-Fi devices, a new world of possibilities opens up for Wi-Fi network management and device/network security.

One solution that has been in development in the Wi-Fi Alliance is the Device Provisioning Protocol (DPP) specification – also referred to as "WFA Easy Connect". The DPP specification enables the secure transfer of device credentials and metadata on both home and enterprise networks using a variety of provisioning mediums and mechanisms without complex infrastructure and without entering password/pre-shared keys (PSKs). In this paper we describe how DPP/Easy Connect works, the context and justification for it, and how it can be built upon to provide more safe and secure Wi-Fi networks while also enabling the advanced networking features we need in the future.

## 2. Wifi Device Authentication and Key Establishment

### 2.1. WPA2 (802.11i-2004)

The first generation of Wi-Fi security (WEP) required all the wireless-enable devices ("Stations") to share a common 40- or 104-bit encryption key. The Access Point and Stations were all manually configured with the same 10- or 26-digit hex-coded key. This key was used directly to encrypt every payload packet sent across the network. Fatal security issues were discovered in WEP that led to it being deprecated – and replaced by WPA. But security issues aside, there was also a need for more flexible per-Station key establishment methods than either WEP and WPA could provide in order for Wi-Fi to be adopted in more environments.

To allow for more flexibility in how keys are associated with Stations, the WPA2 specification (802.11i-2004) introduced "pairwise" and "group" keys. Specifically, WPA2 defines the following keys:

- **The Pairwise Transient Key (PTK)**: This key is used to encrypt all unicast (non-broadcast/multicast) traffic between one Station and the Access Point. The PTK is established using the "4-Way Handshake"
- **The Group Transient Key (GTK)**: This key is used to encrypt all broadcast and multicast traffic on the network attached to the AP. The GTK is established and distributed using the "Group Key Handshake"

- **The Pairwise Master Key (PMK)**: This key is used, along with other parameters, to establish the PTK. The method for establishing the PMK varies according to the authentication method.

All Wi-Fi key establishment methods use the 4-way handshake to establish the PTK and GTK for a Station. What varies between the methods is the establishment of the PMK, which will be described in later sections.

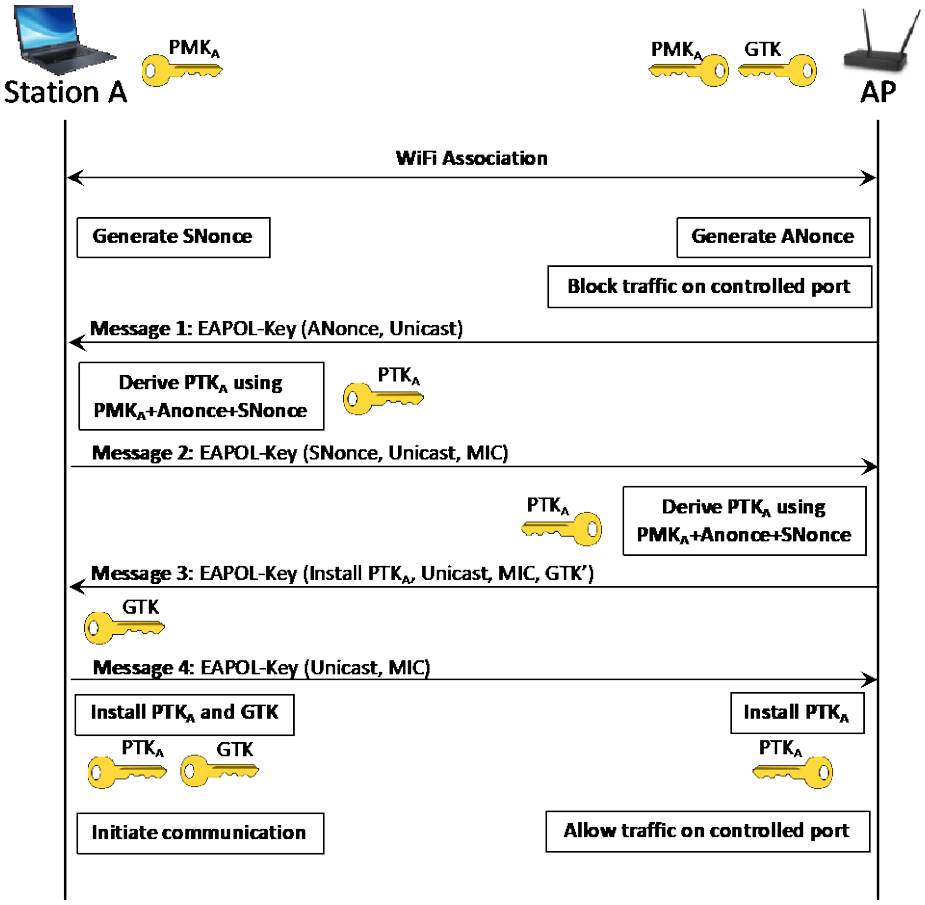


**Figure 1: The Wi-Fi/EAPOL 4-Way Handshake**

### *2.1.1. WPA2 Personal*

Residential, small/home office (SOHO) networks often use the WPA-Personal profile – which utilizes a shared password to determine the PMK. All that is required to establish a WPA-Personal Wi-Fi network is to configure the AP with an SSID and password and configure all the Stations with the same password.

The 4-Way Handshake allows the Station and the AP to establish that they both have the same password and allows for the establishment of a per-Station PTK.

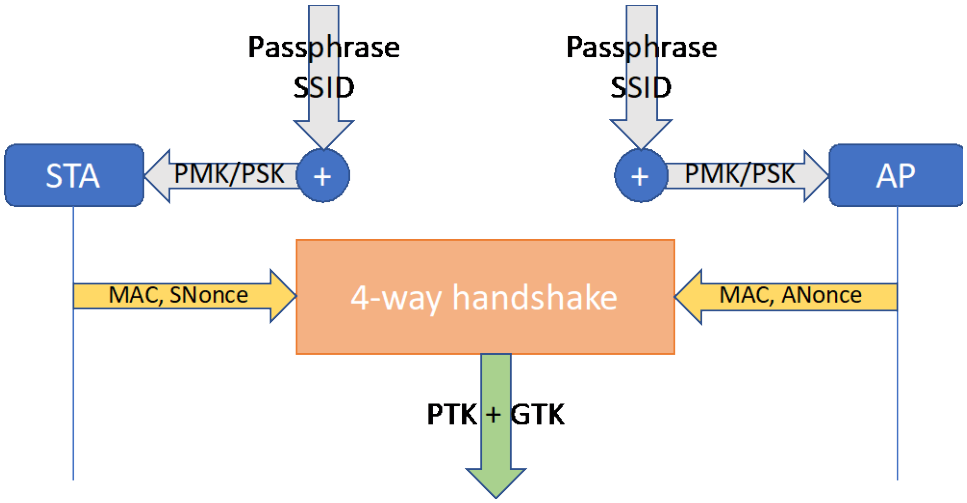


**Figure 2: PTK establishment in WPA-Personal**

What's notable here is that – while each Station and the AP will have the same PMK (by virtue of using the same password) – the 4-Way Handshake ensures that each Station has a *unique* PTK (by virtue of the fact that the Snonce and Anonce are randomly generated). The GTK, on the other hand, is the same for all entities on the network so that shared traffic (such as broadcast and multicast) can be decrypted by all parties on the network.

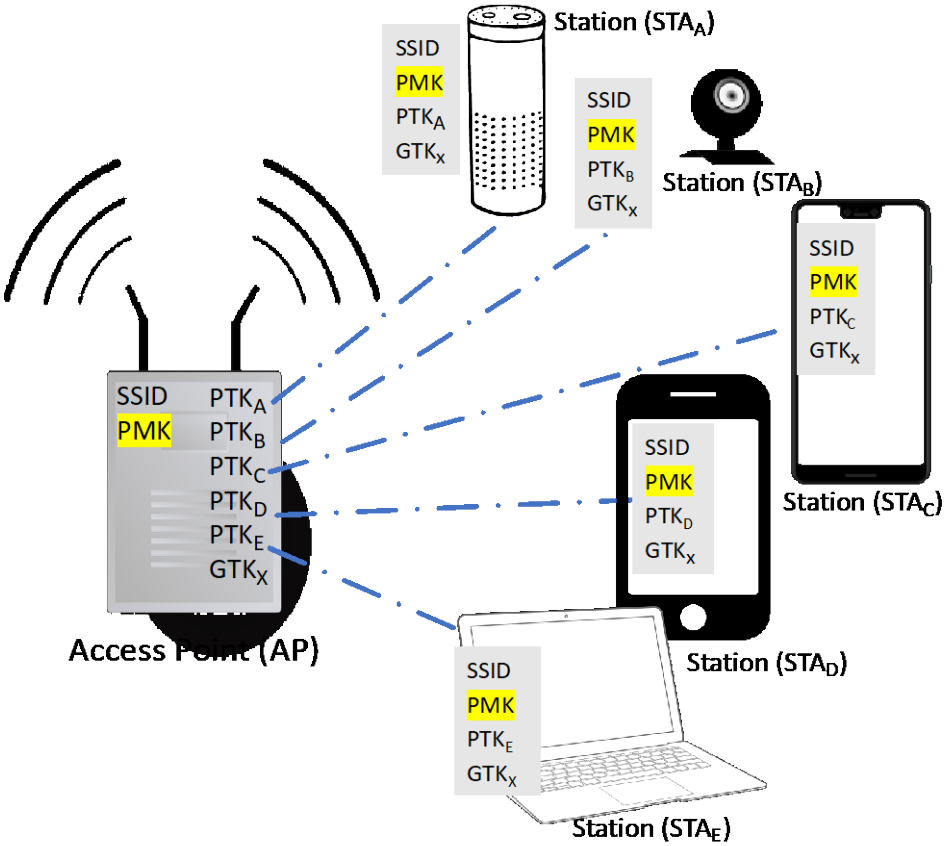


**Figure 3: Key Usage in WPA2-Personal**

 

Note that every time a Station reauthenticates, a new PTK is generated. And any time a Station leaves the network, a new GTK is generated by the AP and distributed to the currently authentication Stations to ensure that Stations which have been removed from the network cannot decrypt group traffic using a previously derived GTK.

While WPA2 Personal is simple to setup – and simple to authenticate – this simplicity comes with a price: any Station(s) with the active password can authenticate. And the only way to prevent an unwanted Station from authenticating is to manually change the password on the AP and all the Stations – which is highly disruptive, especially with IoT devices. Additionally, any Station with knowledge of the Password/PMK can derive the encryption key of any other Station by observing the authentication exchange of that Station and the AP.

### *2.1.2. WPA2/WPA3 Enterprise*

As mentioned previously, shared passwords are not an appropriate authentication solution for environments where user/Station access needs to be tightly controlled. Specifically:

1. In enterprise environments, there is typically already an authentication system in place – and corporations wishing to deploy Wi-Fi want to use their existing systems to authenticate Stations using existing user credentials.
2. The level of access to an enterprise network is often user-dependent. A shared password does not allow for differentiated or revocable Wi-Fi service. Some form of user identity is required. E.g. The user ID can be used to establish which VLAN (Virtual Local Area Network) and other resources the Station will have access to.
3. Revoking access to certain users/Stations should not require disrupting the Wi-Fi network and/or reconfiguring other Stations – as is the case with WPA2-Personal.

WPA2-Enterprise addresses the limitations of WPA2-Personal by providing a means of user-level authentication prior to the 4-Way Handshake using EAP-based (Extensible Authentication Protocol) authentication with a AAA server implementing the RADIUS/Diameter protocol. WPA3-Enterprise utilizes the same authentication methods and protocol as WPA2-Enterprise while updating the security profile of the various authentication methods and management messages. For example, WPA3-Enterprise requires Wi-Fi management frames to be protected and deprecates the use of cipher suites that are now considered insecure.

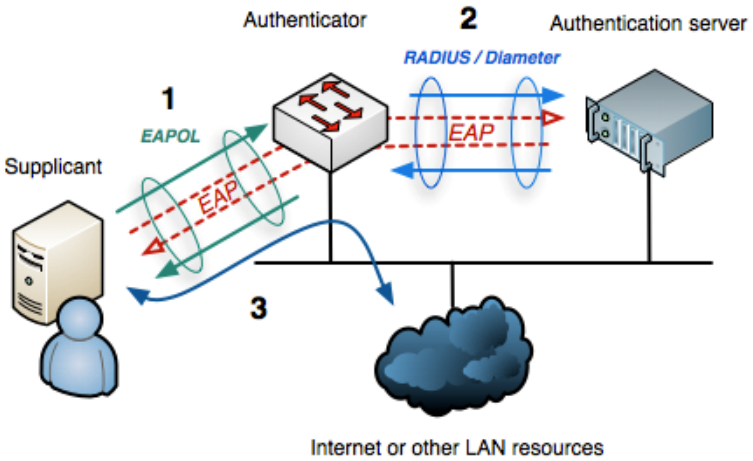


**Figure 4: WPA2-Enterprise Authentication**

 

Once the Station ("Supplicant") and Authentication Server agree on an EAP method, they can exchange an arbitrary set of EAP messages to perform authentication. If authentication is successful, the Authentication Server and Station derive a shared key and the Authentication Server provides the derived key to the Authenticator. The Authenticator uses the EAP-derived PMK to drive the 4-way handshake with the Station.

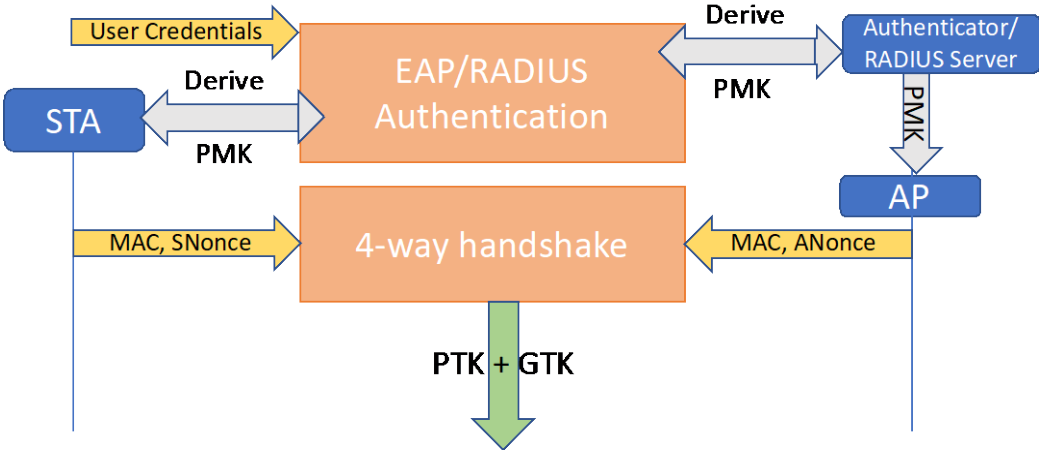


**Figure 5: PTK Establishment in WPA2-Enterprise**

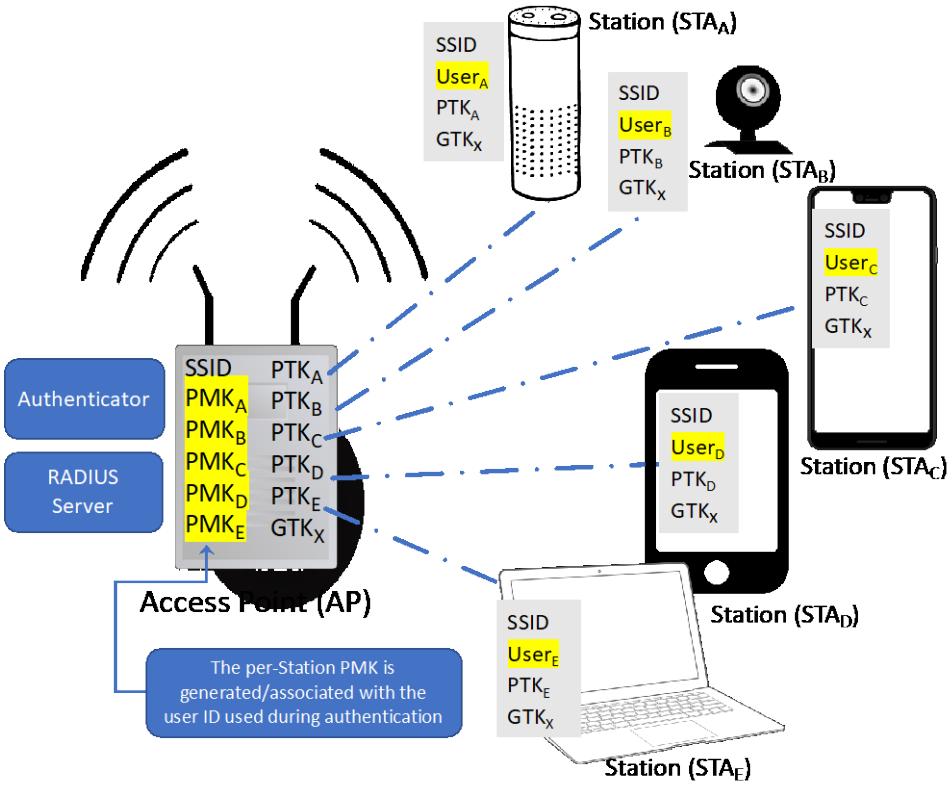


**Figure 6: Key Usage in WPA2-Enterprise**

WPA2-Enterprise addresses the single-password shortcomings of WPA2-Personal – and can satisfy the common enterprise requirements listed above when properly deployed and configured. But it does so at

the cost of additional infrastructure, user/credential provisioning, and additional configuration. In particular, WPA2-Enterprise solutions are often tailored for user-based authentication using enterprise credentials. While this is well-suited to enterprise environments with interactive clients and a centralized user credential database, it's less suited for IoT and other dedicated-use devices.

User or device-level authentication can alternatively be performed in WPA2/3 Enterprise by using X.509 certificates. This form of authentication requires installing certificates and keys into the devices. However WPA2/3 Enterprise by itself does not provide a standardized mechanism to provision certificates/credentials and associated CA certificates into device trust stores.

### *2.1.3. Other WPA2 PMK Establishment Methods*

As noted in section 2.1.1, the simplicity of using a shared password in WPA2-Personal is also its main deficiency. And while WPA2-Enterprise enables per-device credentials, it introduces other issues. But as might be clear by now, any method that provides a per-station PMK can enable per-Station credentials, Station-specific policy, and Station revocability.

The key to deriving a unique per-station PMK is to determine an identity for a Station. The simplest form of identification for a Station is the MAC address of its Wi-Fi interface. Each Station can be configured with a unique WPA2-Personal password and the AP can associate a password with the MAC of the station. When the Station attempts authentication, the AP can look up the password associated with the MAC address of the authentication frames and initiate the WPA2 4-Way Handshake. The same MAC association can be used to establish per-Station policy (e.g. VLAN association, access policies, etc.).

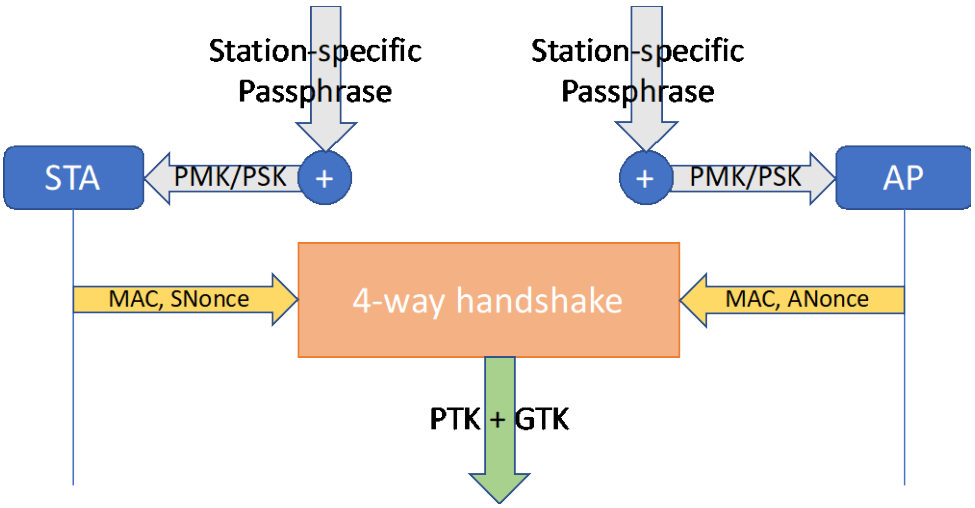


**Figure 7: PTK Establishment Using MAC-associated Password/PMK**

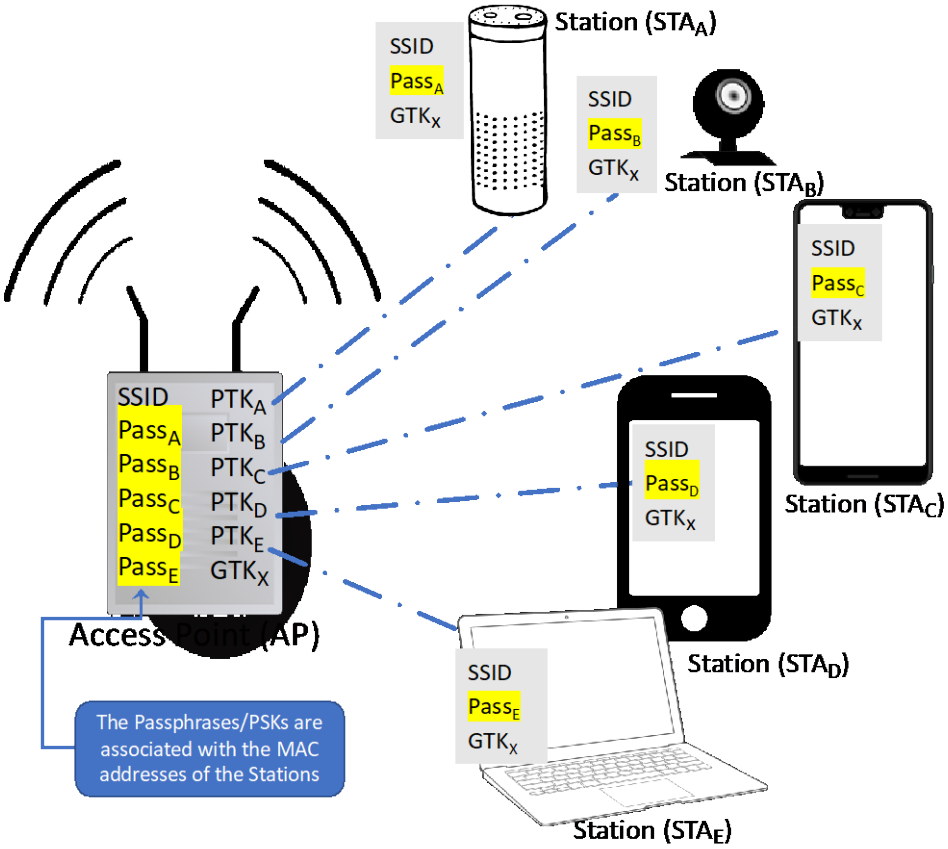


**Figure 8: PMK Distribution using MAC-associated Password/PMK**

This MAC association method is supported by the reference Wi-Fi AP implementation *HostAPD* as well as a variety of commercial products/offerings.

There are some issues with this method however:

- The first time a Station connects with a password, the MAC isn't known by the AP. If the password/PSK is a single-station credential, the AP will learn the MAC address of the first Station that connects with the Password/PSK – which may not be the intended Station.
- If the password/PSKs are auto-generated, they may be cumbersome to enter by the user. If they're user-generated, it can become tedious – potentially leading to poorly chosen passwords.
- For a multi-station password/PSK credential, there's no reliable way to control which Station(s) are allowed to use the credential.
- Some devices use MAC address randomization prior to AP association for privacy protection. This can prevent the methods used for establishing initial MAC-to-PSK associations from working.

What is needed is a form of Station identification and credential that is nontransferable and attestable. In other words, Stations need an identifier that can be proven using secure methods and cannot be easily transferred from one Station to another. One such method will be discussed in Section 3.

 

## 2.2. WPA3-Personal

As discussed in Section 2.1.2, the basic messaging and authentication of WPA3-Enterprise is identical to WPA2-Enterprise – and the method to exchange the PMK is unchanged. WPA3-Personal, however, uses a dramatically different method than WPA2-Personal for mutually deriving the PMK. Rather than using the password/PSK (and SSID) to derive the PMK, WPA3-Personal uses an exchange called "Simultaneous Authentication of Equals" (SAE). SAE is a PAKE-based (Password Authenticated Key Exchange) cryptographic exchange that can derive a cryptographically strong shared secret from a low-entropy password.

This method solves one of the largest issues with WPA2-Personal shared passwords: the ability to derive and Station's PTK and decrypt all the traffic on the network – including traffic captured before the PTK was known. Here's an illustration of the SAE exchange:

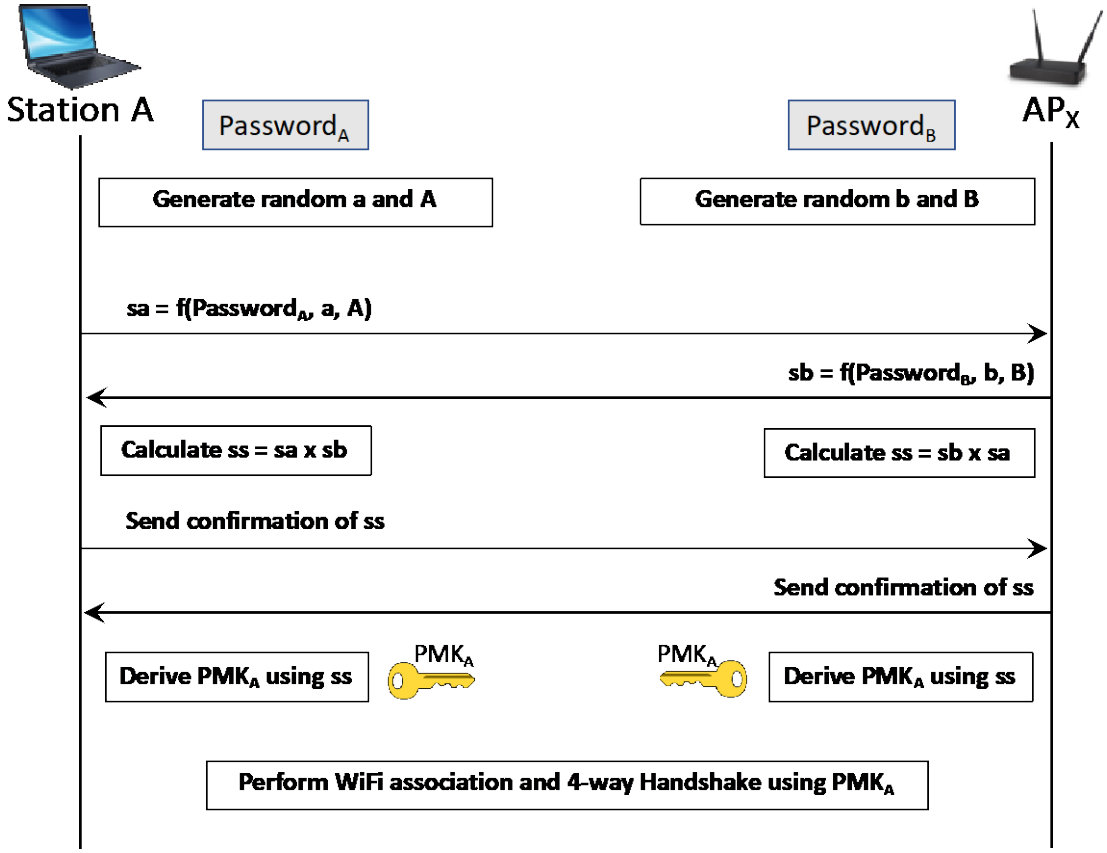


**Figure 9: WPA3 Personal SAE Exchange**

Some advantages of the SAE exchange:

- Both parties can calculate and send their components independently
- The computations used to derive the shared secret/PMK ensure that the password and the PMK cannot be determined
- Ensures perfect forward secrecy

 

# 3. Provisioning Station Credentials using DPP

The Wi-Fi Alliance Easy Connect ™ specification defines mechanisms for provisioning a Station with Wi-Fi network credentials without user entry of passwords/keys or installation of enterprise certificates. While simplifying the task of device onboarding, Easy Connect also provides stronger security methods, per-device credentials, revocation, mutual authentication, and reliable/secure device- and group-level identification.

## 3.1. DPP Provisioning

There are a variety of means in Easy Connect by which a device can be discovered and authenticated for provisioning. Figure 10 and Figure 11 illustrate the provisioning of a DPP "Connector" and PSK, respectively, on devices using a scanned QR code to provide network authentication and connectivity.

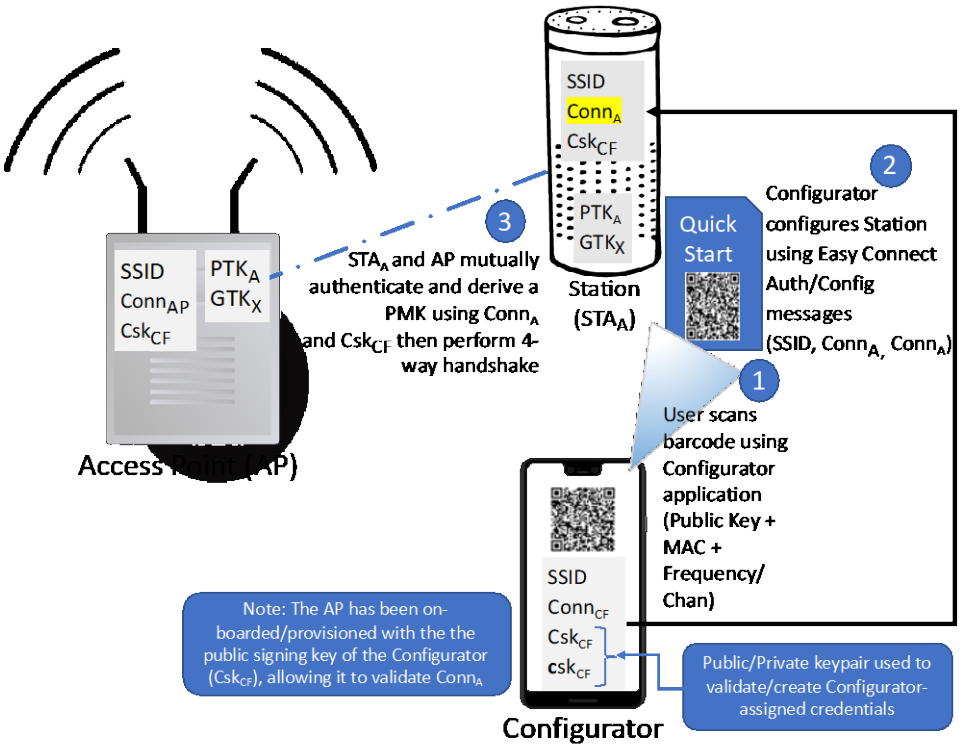


**Figure 10: DPP Direct Provisioning of Connector Using QR Code**

 

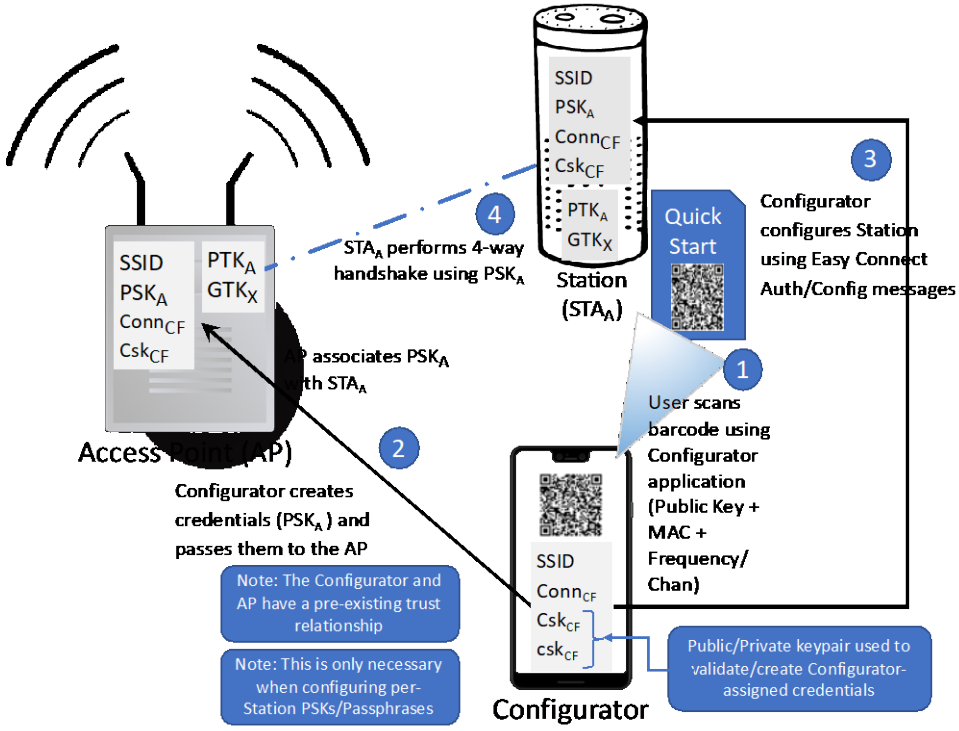


**Figure 11: DPP Direct Provisioning of PSK Using QR Code**

Figure 10 and Figure 11 illustrate a stand-alone Configurator directly provisioning the on-boarded Station ($STA_A$). But it can often be advantageous to have the Configurator co-located on the AP. This model ensures that (a) the Configurator is always accessible (which simplifies the discovery/initiation process) and (b) ensures that credentials stored by the Configurator are not easily lost (e.g. if the device with the Configurator is lost or the application is deleted). Figure 12 illustrates a Configurator which operates on the AP.

 

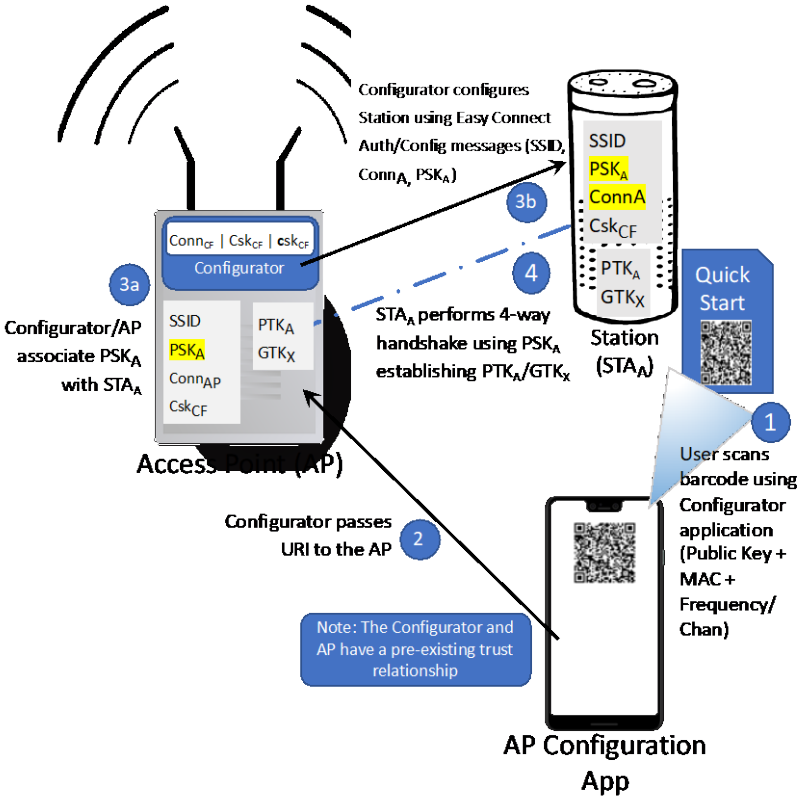


**Figure 12: DPP AP-based Provisioning of PSK using QR code**

Regardless of how provisioning is performed, all Stations can be provisioned with a PSK, WPA2 password, Enterprise credentials (certificate), WPA3/SAE Password, and/or DPP Connector credentials. The Configurator can offer more than one type of credential to a Station. And a Station can accept more than one credential. A network can be provisioned with a combination of credentials depending upon the

 

credential types supported on the AP, the credential types supported on the Stations, and what credentials the Configurator creates/supplies.

Below is an illustration showing Stations provisioned with a combination of different credential types:

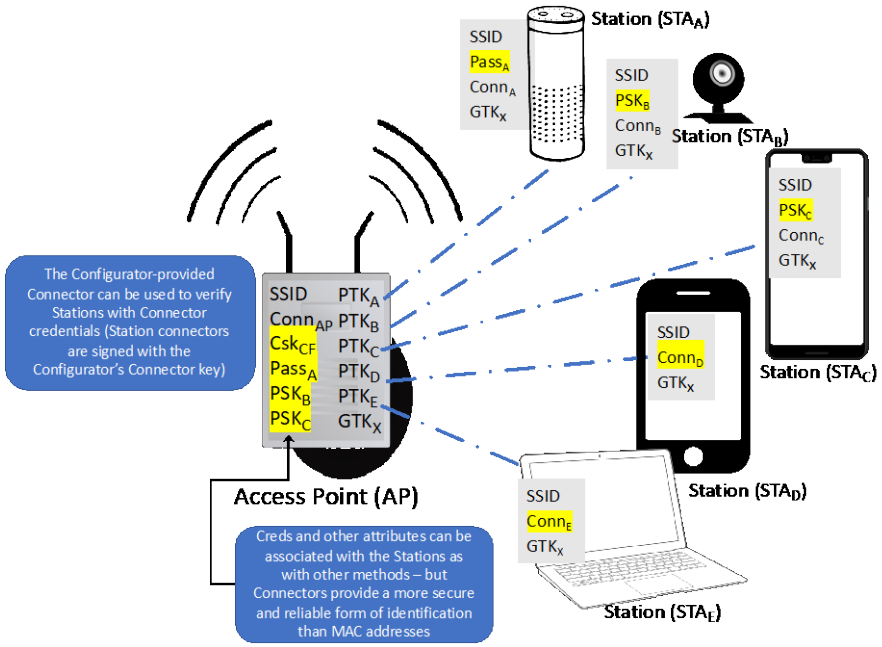


**Figure 13: DPP Provisioning of PSKs**

The DPP onboarding process also provides the opportunity for the Configurator application (or its proxy) to interact with the user and configure the Station and the AP/Wi-Fi network according to user interaction/direction or other technologies. For example, during the onboarding process, the user may designate that a Station may only connect to the Internet and not to other devices on the home network, that a device should not be able to use more than a particular bitrate of uplink bandwidth, or that a Station should not be able to use the uplink during particular hours of the day

## 3.2. DPP/EasyConnect Connectors

Many of the solutions currently deployed to provide device/Station-level policy depend upon MAC addresses to identify devices and associate per-device and per-group policy, as described in section 2.1.3. There are a number of issues using MAC addresses as identifiers:

1. MAC addresses are easily observable via traffic monitoring – even by parties that are not part of the Wi-Fi network (since every Wi-Fi packet contains a MAC address),
2. The MAC address of an adapter is changeable. This is especially problematic when an AP/gateway with shared password credentials attempts to assign policy based on MAC address. It is trivial for one Station to take on another Station's MAC-associated policy by simply cloning the MAC address. E.g. A child in a household can circumvent MAC-associated network time or usage restrictions by stealing a parent's MAC address or assigning a random MAC address.
3. Due to (1), MAC addresses have become a privacy concern. Device manufacturers have announced initiatives to use randomized MAC addresses to avoid device/identity tracking.

 

Today's systems that utilize MAC-based policy assignment will likely encounter issues as these privacy initiatives are implemented. [4][5]

DPP solves the issue of identification with *Connectors*. Connectors provide a secure and durable identity for a Station while also enabling mutual authentication and verifiable metadata. Connectors are JSON Objects created by the Configurator at the time of onboarding, cryptographically signed using the private key of the Configurator ($\mathbf{c}sk_{CF}$), and encoded using JWS (JSON Web Signature) serialization.

Here is an example of a Connector, prior to encoding and signing using JWS:

```
{
  "groups": [
      {
         "groupId": "home",
         "netRole": "sta"
      },
      {
         "groupId": "cottage",
         "netRole": "sta"
      }
   ],
   "expiry": "2019-01-31T22:00:00+02:00",
   "netAccessKey": {
      "kty": "EC",
      "y": "LUsDBmn7nv-LCnn6fBoXKsKpLGJiVpY_knTckGgsgeU",
      "x": "Xj-zV2iEiH8XwyA9ijpsL6xyLvDiIBthrHO8ZVxwmpA",
      "crv": "P-256"
   }
}
```

**Figure 14: DPP Connector Example**

Once encoded and signed, the same Connector appears as three base64-encoded fields separated by "." characters – with the first group being JWS "protected" header values, then the encoded Connector, followed by a signature of the two fields. The signature (or hash of the signature) can be used to identify the Connector. Here's an example of a JWS-encoded and signed Connector:

```
eyJ0eXAiOiJkcHBDb24iLCJraWQiOiJrTWNlZ0RCUG1OWlZha0FzQlpPek9vQ3N2UWprcl9uRUFwOXVGLUVEbVZFIiwiYWxnIjoiRVMyNTYifQ
.
eyJncm91cHMiOlt7Imdyb3VwSWQiOiJob21lIiwibmV0Um9sZSI6InN0YSJ9LHsiZ3JvdXBJZCI6ImNvdHRhZ2UiLCJuZXRSb2x
lIjoic3RhIn1dLCJuZXRBY2Nlc3NLZXkiOnsia3R5IjoiRUMiLCJjcnYiOiJQLTI1NiIsIngiOiJYai16VjJpRWlIOFh3eUE5aW
pwc0w2eHlMdkRpSUJ0aHJITzhaVnh3bXBBIiwieSI6IkxVc0RCbW43bnYtTENubjZmQm9YS3NLcExHSmlWcFlfa25UY2tHZ3NnZ
VUifSwiZXhwaXJ5IjoiMjAxOS0wMS0zMVQyMjowMDowMCswMjowMCJ9
.
8fJSNCpDjv5BEFfmlqEbBNTaHx2L6c_22Uvr9KYjtAw88VfvEUWiruECUSJCUVFqv1yDEE4RJVdTIw3aUDhlMw
```

**Figure 15: Encoded DPP Connector Example**

As part of the Wi-Fi authorization process, a Station supporting DPP can authenticate with the Access Point using the Connector supplied to the Station during provisioning. Figure 16 illustrates the mutual authentication and derivation of the PMK using Connectors.

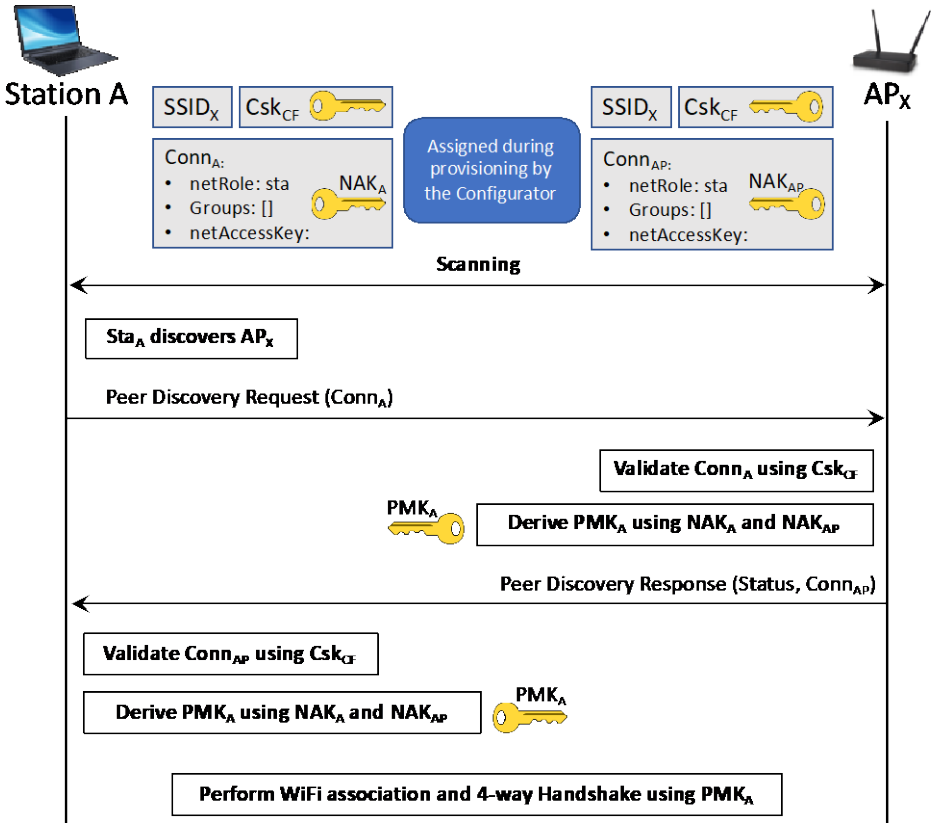


**Figure 16: DPP Connector-based Authentication**

Note that Connector-based authentication addresses the major issues of WPA2-Personal described in Section 2.1.1 – by utilizing a PMK/PSK that's device-specific and non-transferrable. And they also address the major issues of WPA2/3-Enterprise described in Section 2.1.2 – since Connectors are easily generated and easily validated without the need for enterprise infrastructure and provisioning.

## 3.3. Applications of DPP Connectors

As reliable identifiers, Connectors allow for the association of metadata with a Station. During the DPP device onboarding process, arbitrary metadata can be associated with a newly onboarded Station by associating the metadata with the Station's connector (Specifically, the Connector signature or a hash of the signature).

For instance, during the provisioning process, a user could designate that a device should only operate during particular hours. Or a Station can provide, via the DPP Configuration Request object, a MUD (Manufacturer Usage Description) URL that – when processed – indicates that a Station/Device should only connect to a particular host. These provisioning attributes can be stored on the AP by associating them with the Station's Connector.

Connectors also solve the issues related with MAC address reassignment described in Section 2.1.3. When the device authenticates – as shown in Figure 16 – the MAC address of the Station can be associated with the Station's Connector after mutual authentication is completed. MAC-based policies/ACLs can be implemented on an AP/gateway without any requirement on MAC addresses being immutable across Station associations.

 

For example, the application of time-based Internet access restrictions for a Station "kidtab" for 10pm to 6am can be implemented by an AP/gateway using DPP Connectors via the following steps:

1. The Configurator onboarded "kidtab" and assigned it Connector C
2. The Configurator (or proxy application) is used to configure an access restriction for "kidtab" from 10pm to 6am
3. The Configurator adds a time-based policy attribute for 10pm to 6am (daily) and associates it with Connector C on the AP/gateway (using previously established credentials).
4. When "kidtab" authenticates/associates with the network using Connector C, the AP/gateway associates the MAC address with Connector C (the "kidtab" Connector).
5. Once "kidtab" is fully connected, the AP/gateway looks up the policies for "kidtab", finds an associated time-based policy, and sets a timer for 10pm.
6. When the timer goes off at 10pm, the AP/gateway sets packet blocking rules that prevent any traffic with the source MAC address associated with "kidtab" (determined in step 3) and a destination IP outside the local network.

With MAC-associated policy (as is the case with Wi-Fi policy systems today) steps (3) and (4) can fail if/when endpoints utilize MAC randomization – even when per-Station passwords are used. And when shared passwords are used, these kinds of policies can be easily defeated by simply cloning the MAC address of another authorized Station.

Another application of DPP Connectors is reprovisioning. Since all DPP-provisioned Stations and APs are configured with both a Connector and the public key of its Configurator (enabling mutual authentication), the Stations and/or AP can be dynamically and securely reprovisioned at any time by the Configurator using the Connector-based trust relationship. Reconfiguration can be used to update the network configuration of a Station without user intervention – for example to change the SSID of the network. DPP reconfiguration can also be used to provision new Connectors (with new attributes) based on changes made in the Configurator application.

## 4. Wireless Network Segmentation

The number and nature of wireless devices connected to home/SOHO networks has changed dramatically since Wi-Fi was introduced. Smart TVs/speakers, set-top boxes, and streaming devices interact with both the local area network and cloud-based services, while IoT devices such as doorbells, lightbulbs, thermostats, security cameras, and appliances interact and integrate exclusively with cloud-based services.

Additionally, the single- or limited-purpose nature of IoT devices makes them more commoditizable. For instance, to many people, most brands of smart plugs, switches, and bulbs are inconsequential. The considerations are (a) are they compatible with the smart speaker/home automation system that people use and recognize (e.g. "Alexa-Compatible", "Google Home Compatible", "Apple HomeKit Compatible", etc.) and (b) purchase cost. Each device – and its associated (and necessary) cloud-based controller – represent a distinct risk to the user's network and even to networks/systems outside the home. One compromised cloud-based controller can be used to facilitate a botnet-based DDoS (Distributed Denial of Service) attack.

With more devices there's also more demand for shared resources. Most notably, Wi-Fi bandwidth and Internet uplink bandwidth can become strained. And there may be a desire to prioritize traffic to reduce latency for applications such as interactive gaming and video conferencing.

 

One solution to address the current needs of the modern Wi-Fi network and devices – and to provide capabilities for future network requirements – is *network segmentation*. Network segmentation can be implemented in AP/gateways using a combination of virtual bridges and SDN (software-defined networking). But this form of network segmentation can only be reliably and securely implemented when there's a solid means of attestation for a device's identity and layer 2 (MAC) addresses – as described in Section 3.

Network segmentation can enable:

- The separation of Stations by risk category and/or function. E.g. Home automation (HA)/security devices can be allowed to connect to the Internet but cannot initiate connections to devices in other segments. Or devices with a higher quality of credential (e.g. a DPP Connector) can be separated from those with lower-quality credentials (e.g. a PSK).
- Segment-level access controls. Stations in some segments can discover/initiate connections to devices in other segments, but not vice-versa. E.g. Interactive devices such as smart phones and tablets can initiate connections with home automation/security devices, but those HA/security devices cannot access non-HA/security devices
- The "quarantine" of Stations that are suspected of being compromised – either explicitly via user direction or automatically, based on behavior/AI or external threat notifications
- The application segment-level policies – such as usage and time quotas.

Figure 17 illustrates an example network segmentation.

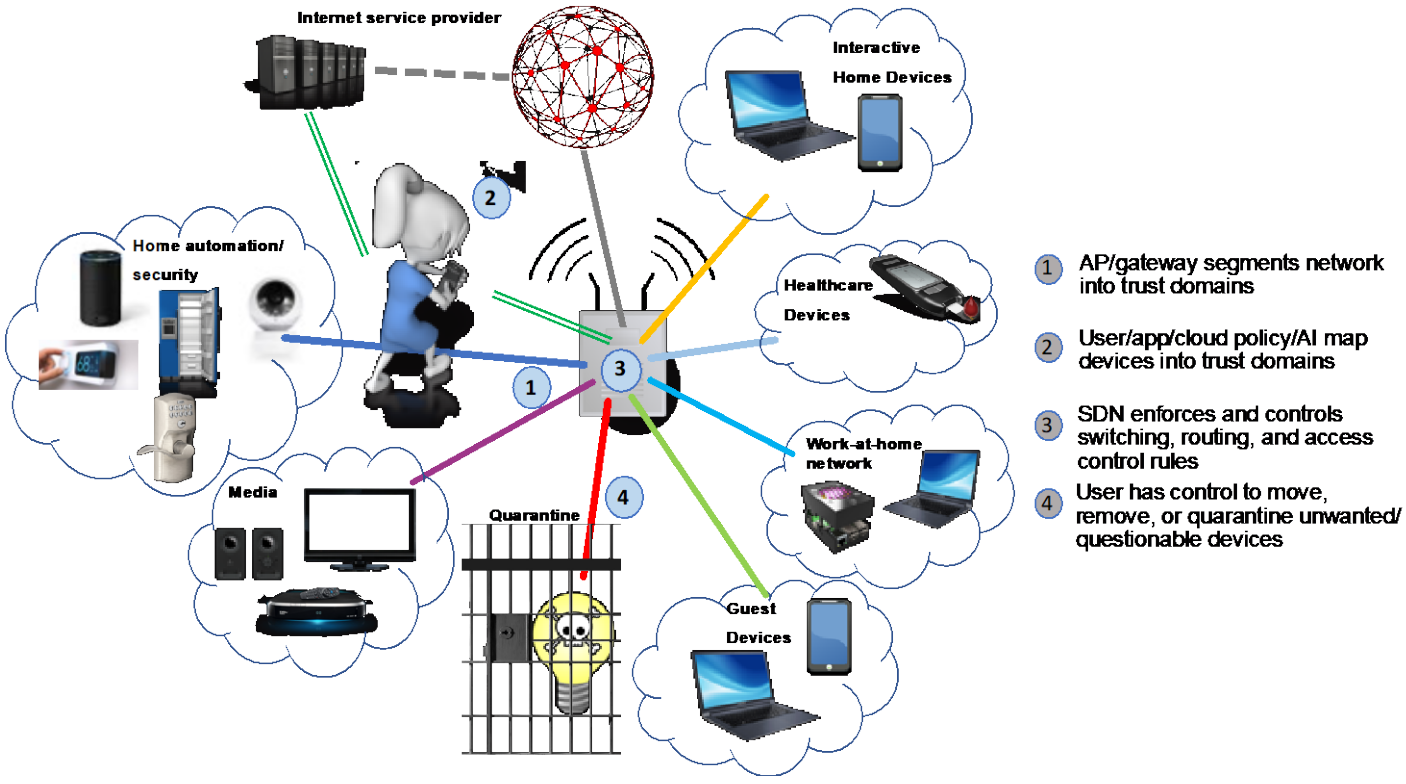


**Figure 17: Example Network Segmentation**

 

### 4.1. Network Segmentation using DPP Connectors

The disposition of Stations into particular segments can be done initially during onboarding – based on Station information provided in the DPP Config Request, initial or historical profiling of the Station (e.g. via device fingerprinting), and/or user direction (e.g. the user choosing a segment from a drop-down on the Configurator UI). A Station can also be moved from one segment to another, based on preference changes or updated information. E.g. If an advisory is published about a particular device, the AP/Gateway could move the Station into a "Quarantine" segment until its software is updated.

To implement segmentation using SDN an AP/Gateway minimally requires:

1. Each Station to have a unique identity – which allows a Station to be associated with a segment.
2. Each Station to have its own security credentials which are associated with the identity and non-transferrable.
3. The MAC address of each Station – which allows SDN rules to be applied to the Station's traffic.

As outlined in Section 3.2, DPP provides (1) and (2) directly. And as described in Section 3.3, it indirectly provides (3) in a way that is much more robust than today's methods that presume immutable MAC addresses.

For example, the provisioning of Station "kidtab" into the network segment "Home-Secure" (a segment designated for laptops, tablets, and smartphones for household residents) could be accomplished with the following steps:

1. The Configurator (or proxy application) is used to onboard "kidtab". The Configurator creates Connector C for it with a "groups" containing "net-seg" and provides Connector C and an SSID of "HomeNet" in the DPP exchange.
2. The Configurator adds a "net-seg" attribute with the value "Home-Secure" and associates the attribute with the Connector C on the AP/Gateway (using previously established credentials)
3. When "kidtab" mutually authenticates with the "HomeNet" AP/gateway using Connector C, the AP/gateway associates the MAC address in the message exchange with "kidtab".
4. Once "kidtab" is fully associated, the AP/gateway looks up the "net-seg" policy for "kidtab", finds the name "Home-Secure" and:
    a. allocates an IP address for "kidtab" in an IP subnet associated with the "Home-Secure" network segment.
    b. Ensures that SDN rules are written appropriately for "kidtab" to be in the "Home-Secure" segment – and to enforce any segment- or Station-specific policy – using the MAC address for "kidtab" (determined in Step 3).
5. If/when "kidtab" disassociates from "HomeNet", the AP/gateway removes the MAC association for "kidtab", the IP address assignment, and all SDN rules associated with its MAC address. This effectively removes it from the "Home-Secure" network.

There are, of course, many ways to implement segmentation. But invariably there will be both Layer 2 and Layer 3 processing required to implement segmentation – especially for Station-specific rule enforcement.

## 5. Conclusion

The amazing success of Wi-Fi now presents its greatest challenge: Supporting the security, scaling, and privacy needs that are required going forward while still supporting the successful Wi-Fi technologies that we're all using today.

 

DPP bridges that gap by supporting the provisioning of current WPA2 and WPA3 credentials while also supporting advanced credentials that allow for mutual authentication and identification. And by integrating with the existing Wi-Fi 4-way handshake protocol, DPP is able to provide that support without introducing new hardware requirements on APs or Stations.

The features of DPP in and of themselves make a compelling case for the protocol. But when you take into consideration the security issues with IoT devices, the need to provide per-Station policies for managing/prioritizing access for non-IoT devices, and the privacy concerns related to MAC addresses, the importance and value of having a non-spoofable Station and AP identity becomes obvious. And the application of per-Station policies and network segmentation – built on the foundation of DPP – can ensure that Wi-Fi will be able to meet the evolving needs of users and devices.

# Abbreviations

| | |
|---|---|
| AAA | Authentication Authorization and Accounting |
| ACL | Access control list |
| AP | Access point |
| bps | Bits per second |
| DDoS | Distributed denial of service |
| DPP | Device provisioning protocol |
| EAP | Extensible authentication protocol |
| EAPoL | Extensible authentication protocol (EAP) over LAN |
| GTK | Groupwise temporal key |
| IEEE | Institute of Electrical and Electronics Engineers |
| JWS | JSON Web Signature |
| MAC | media access control |
| MUD | Manufacturer usage description |
| PAKE | Password authenticated key exchange |
| PMK | Pairwise master key |
| PSK | Pre-shared key |
| PTK | Pairwise temporal key |
| QR | Quick Response (code) |
| RADIUS | Remote Authentication Dial-In User Service |
| SAE | Simultaneous authentication of equals |
| SCTE | Society of Cable Telecommunications Engineers |
| SDN | Software Defined Networking |
| SOHO | Small office home office |
| SSID | Service Set Identifier |
| VLAN | Virtual local area network |
| WEP | Wired Equivalent Privacy |
| WPA | Wi-Fi Protected Access |
| WPA2 | Wi-Fi Protected Access 2 |

# Bibliography & References

[1] Device Provisioning Protocol Version 1.2; Wi-Fi Alliance
[2] WPA3™ Specification Version 2.0; Wi-Fi Alliance

 

[3] IEEE 802.11i-2004: *IEEE Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area network - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*; Institute of Electrical and Electronics Engineers
[4] Apple Knowledge Base Article 211227: *Use private Wi-Fi addresses in iOS 14, iPadOS 14, and watchOS 7*; https://support.apple.com/en-us/HT211227
[5] Android 10 Privacy and location/Privacy Changes: *MAC Address Randomization*; https://developer.android.com/about/versions/10/privacy/changes#randomized-mac-addresses

 