NGH Provisioning Standardization

Secure Inline Provisioning Solution for HS2.0 R1/R2 NGH & Legacy 802.1X Deployments

Source: NGH Provisioning Standardization Working Group
Author(s): WBA Members
Issue date: 3 November 2017
Document status: 1.0

WIRELESS BROADBAND ALLIANCE
DRIVING NEXT WIRELESS EXPERIENCE

ABOUT THE WIRELESS BROADBAND ALLIANCE

Founded in 2003, the mission of the Wireless Broadband Alliance (WBA) is to champion the development of the converged wireless broadband ecosystem through seamless, secure and interoperable unlicensed wireless broadband services for delivering outstanding user experience. Building on our heritage of NGH and carrier Wi-Fi, WBA will continue to drive and support the adoption of Next Generation Wi-Fi services need coexistence and convergence of unlicensed and licensed networks across the entire public Wi-Fi ecosystem, including IoT, Big Data, Converged Services, Smart Cities, 5G, etc. Today, membership includes major fixed operators such as BT, Comcast and Time Warner Cable; seven of the top 10 mobile operator groups (by revenue) and leading technology companies such as Cisco, Microsoft, Huawei Technologies, Google and Intel. WBA member operators collectively serve more than 3 billion subscribers and operate more than 30 million hotspots globally.

The WBA Board includes AT&T, Boingo Wireless, BT, China Telecom, Cisco Systems, Comcast, Intel, KT Corporation, Liberty Global, NTT DOCOMO, Orange and Ruckus Wireless. For a complete list of current WBA members, please click here.

Wi-Fi is aimed to take an important role in 5G development, and on-going convergence developments between licensed and unlicensed wireless will have a significant impact on the future of wireless communications.

Follow Wireless Broadband Alliance at:

http://www.twitter.com/wballiance

http://www.facebook.com/WirelessBroadbandAlliance

http://www.linkedin.com/groups?mostPopular=&gid=50482

https://plus.google.com/106744820987466669966/posts

UNDERTAKINGS AND LIMITATION OF LIABILITY

This Document and all the information contained in this Document is provided on an 'as is' basis without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for particular purpose, or non-infringement.

In addition, the WBA (and all other organizations who may have contributed to this document) makes no representations or warranties about the accuracy, completeness, or suitability for any purpose of the information. The information may contain technical inaccuracies or typographical errors. All liabilities of the WBA (and all other organizations who may have contributed to this document) howsoever arising for any such inaccuracies, errors, incompleteness, suitability, merchantability, fitness and non-infringement are expressly excluded to the fullest extent permitted by law. None of the contributors make any representation or offer to license any of their intellectual property rights to the other, or to any third party. Nothing in this information or communication shall be relied on by any recipient.

The WBA also disclaims any responsibility for identifying the existence of or for evaluating the applicability of any claimed copyrights, patents, patent applications, or other intellectual property rights, and will take no position on the validity or scope of any such rights. The WBA takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any effort to identify any such rights.

Neither the WBA nor any of the other organizations who may have contributed to this document will be liable for loss or damage arising out of or in connection with the use of this information. This is a comprehensive limitation of liability that applies to all damages of any kind, including (without limitation) compensatory, direct, indirect or consequential damages, loss of data, income or profit, loss of or damage to property and claims of third-parties.

CONTENTS

Figures

Tables

Executive Summary

This whitepaper outlines a framework that enables the inline provisioning of BYOD and Wi-Fi-only devices on NGH Wi-Fi or legacy 802.1X (Enterprise) Wi-Fi networks. Provisioning these devices for secure network access has been one of the biggest barriers to widespread implementation of Secure SSID and NGH networks in the Multi-System Operators (MSO) and Wi-Fi hotspot provider space. The requirement to provision the devices through a separate, dedicated open/secure (OSEN) SSID, or the need to pre-provision via a 3rd party network, represent friction points that make it difficult for users to discover and use the provider network and services in an intuitive and seamless manner. The challenges this experience presents to ubiquitous deployment and adoption of NGH and secure Wi-Fi networks is amply illustrated in the *Benchmarking & Gap Analysis* sections of this document. Even though Hotspot 2.0 (HS2.0) standards (R1/R2) have been published and ratified for several years, the MSO and hotspot provider landscape has not fundamentally changed – most providers continue to operate open (unsecure) Wi-Fi networks, heavily biased towards "ease-of-use" at the expense of providing a truly secure and seamless experience. Providers that allow manual connections to their secure networks, in the hopes of reducing some of the onboarding friction for their users, leave these users vulnerable to "evil twin" attacks since user devices do not always authenticate the network.

We believe the inline provisioning challenge is solvable, by extending the existing standards and specifications that constitute the NGH and Enterprise Wi-Fi services. However, this require a paradigm shift in the industry thinking around allowing *unauthenticated associations* to occur in conjunction with *mutually authenticated associations* on production SSIDs/networks.

This whitepaper defines the exact framework, use cases, call-flows, and specific element-level requirements that enable the capability for Bring-your-own-device (BYOD) and Wi-Fi-only devices to discover, provision, and use provider Wi-Fi networks (NGH or legacy 802.1X). All without pre-provisioning, obtaining credentials ahead of time, and minimal user intervention.

With the right support from OS vendors – Apple, Alphabet, and Microsoft – it is possible to envision a "user journey" where the ability to discover, setup, and use Wi-Fi networks anywhere in the world is no more difficult than answering a few yes/no question to prove that the subscriber is authorized for service or interested in pay-per-use access. Thereby, truly realizing the stated goal of the HS2.0 initiative – *to make the experience of discovering and using Wi-Fi no more complicated than cellular roaming.*

1 Introduction

While the HS2.0 R2 specification includes stipulations for managing the provisioning and credentials required for access to NGH Networks, the industry appears to be stuck in a seemingly perpetual state of waiting for all the necessary components to become HS2.0 ready, and the actual number of production HS2.0 networks remains relatively small. Meanwhile, market demand for secure Wi-Fi networks is imminent and expanding, resulting in a challenge for MSOs who do not directly sell devices and provide Wi-Fi services largely to customers with Wi-Fi-only or BYOD types. These device types lack pre-known identity definitions, like the EAP-SIM and EAP-AKA credentials common to cellular carriers, which makes it challenging for MSOs to deliver the appropriate profile/configuration necessary for connecting to the secure network (SSID) in a seamless manner.

The focus of this white paper is to define a framework for provisioning BYOD and Wi-Fi-only devices, in line with the secure production network (SSID) for HS2.0 and legacy 802.1X network. This will reduce the friction to NGH adoption and simplify deployments, by leveraging and extending existing WFA, IEEE, and WBA specifications. Wi-Fi users will be able to discover an NGH network and related services, associate automatically, complete provisioning with network access credentials, and use the services – all on a single, secure network.

1.1 Use Cases In Scope

- Onboarding existing customer using first time device
- Onboarding roaming customer for the first time
- Onboarding Pay-per-use customer

1.2 Goals

- Identify gaps in the onboarding and provisioning process in networks (NGH and legacy 802.1X) and devices (Passpoint™ certified and legacy) and the resulting impact to the "customer journey" of users trying to discover and use these network services.
- Define a framework that eliminates the need to use a separate provisioning SSID (open or secure) for online sign-up or provisioning in NGH networks.
- Extend the framework to support inline provisioning of devices trying to use legacy 802.1X networks.
- Define real world use-cases for onboarding and provisioning new devices, roaming devices, and pay-per-use devices and provide next steps for the industry and WBA.
- Accelerate deployments of NGH networks by enabling new methods to provision HS2.0 enabled devices in line with the target NGH network customers want to use.

2 Benchmark of Provisioning Process of Current NGH Deployments 1Q 2017

To benchmark the current state of provisioning in existing NGH deployments, the WBA team has evaluated test results derived from the NGH Phase 4 trial results (WIP), as well as feedback from WBA members with real word deployments of NGH and managed Wi-Fi networks. Benchmarking was used to identify any planning gaps that may exist when comparing the specification state to the actual state of real world NHG network deployments. Test results of the NHG Phase 4 trial were also used to benchmark the current NGH R1/R2 onboarding process for Passpoint™ certified devices.

2.1 Storyboard of 2017 Mobile World Congress NGH Network Provisioning Process

There are a few methods for notifying users that an NGH Wi-Fi network is available for use. Advertising the network prior to the event and marketing during the event was used to notify users of the MWC-NGH SSID.

1) Pre-provisioned users could install the NGH profile before attending Mobile World Congress.
2) Time of use sign-up and provisioning process of an iOS device via Open OSU SSID for users who do not install the profile before attending Mobile Word Congress 2017. It takes 12 screens/clicks to get the NGH profile configured.

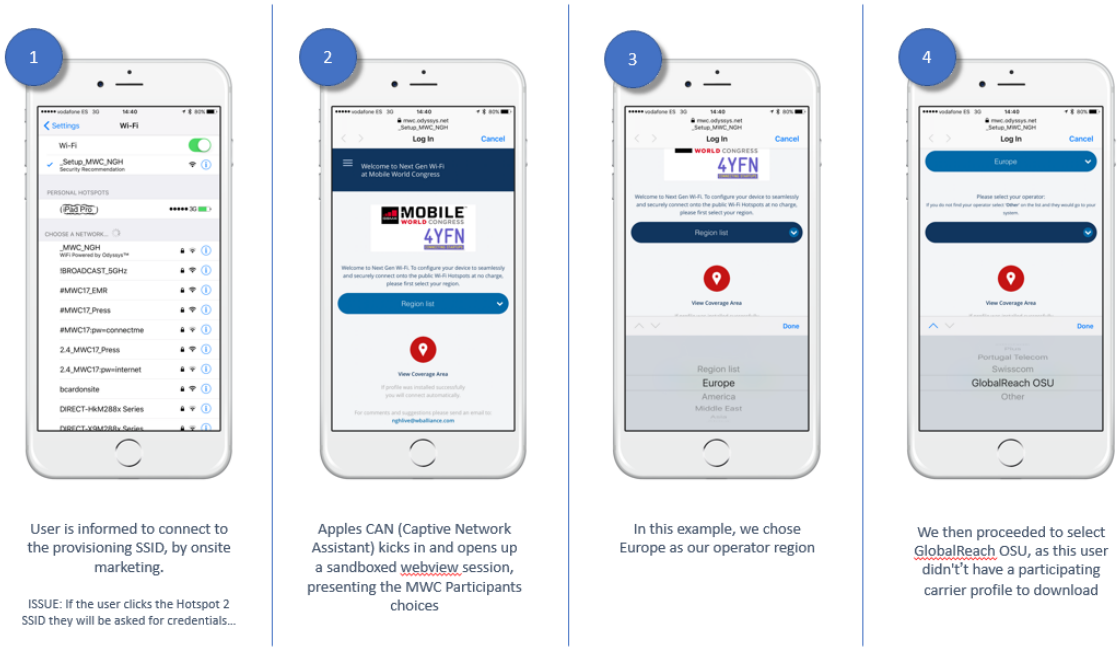
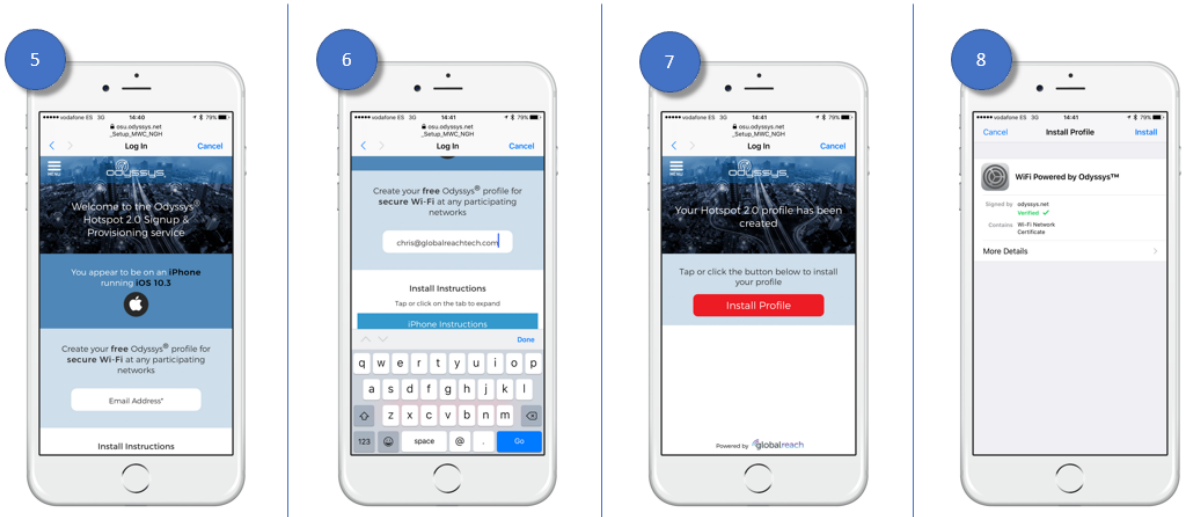


Figure-1. MWC Current State Provisioning User Journey



GlobalReach OSU loads and requires an email address before generating a AAA profile in the platform

NOTE: Typically this is the entry point to an OPS, MWC wanted a micro portal before the OSU in this case.

User enters email address and clicks Go

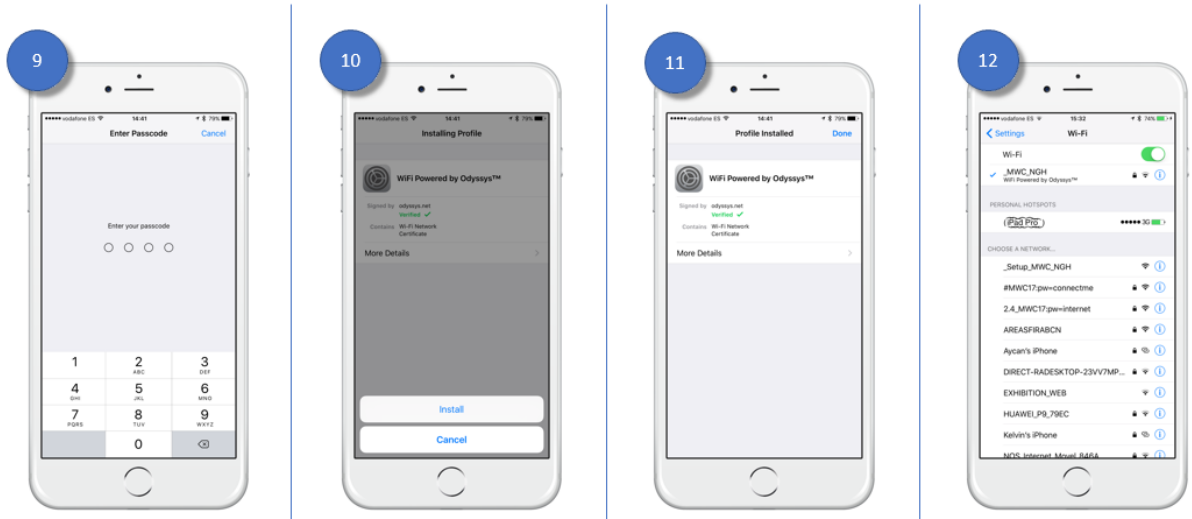
NOTE: Different calls to action maybe presented to the client depending on the needs of the carrier

The OSU then generates a AAA profile and a mobile configuration file for an Apple device. User initiation is required to click the Install Profile button to activate the profile download

Apple then takes the user through a number of steps

User must click install (top right).

Figure-2. Current State Provisioning User Journey (contd.)



User must enter their personal device security code.

User is asked again they wish to install.

Profile is installed and a Done button is presented (top right)

ISSUE: User is returned to their devices settings page, with no idea what to do..

If the device recognises the ANQP packets it will auto connect.

ISSUE: Devices often have to be told to forget the provisioning SSID, or they have a tendency to stay connected to the open provisioning SSID

Figure-3. Current State Provisioning User Journey (conclusion)

3 Gap Analysis of NGH Provisioning Process

Gap analysis was used to determine if the current state of NGH network provisioning is achieving the best use of current technology, available methods, and resources. The following planning gaps and issues are used to identify areas that should be improved. The current HS2.0 R2 specification requires the use of a separate OSU SSID to support time of use provisioning. Once the device is provisioned, users typically toggle the Wi-Fi radio to disconnect from the provisioning SSID and connect to the secure NGH network. Device operating systems are not currently compliant with the R2 specification and in many cases, have implemented new features like iOS Captive Network assistant and Androids Automatic VPN that prevent users from being able to utilize the Open or OSEN OSU SSID for provisioning or interfere with the functioning of the provisioning flows.

3.1 Identified Gaps, Impacts, and Recommendations

During both the NGH Phase 4 Trials and real world deployments, many gaps have been identified. The table below outlines several of these gaps and includes the impacts followed by recommendations. While not all of the noted gaps apply to the provisioning of the device, the inclusion of the gaps is critical as they do affect the performance of a device once provisioned - which could be seen as a provisioning issue.

APPLIES TO	GAP	IMPACTS	RECOMMENDATION
Hotspot 2.0 Release 2 - Time of use onboarding process currently requires a separate Open or Secure SSID to accomplish registration from Online Sign Up (OSU).	• Associate and sign-up via separate provisioning SSID: the subscriber device often connects or remains connected to the provisioning SSID instead of connecting or moving to the production SSID once provisioning completes. • Provisioning SSID remains in the list of "known networks" causing unpredictable – device behavior on an ongoing basis – until the user manually goes in and forgets the provisioning SSID.	**Operating Systems Impacted** • Android (all Versions) • iOS (all versions) • Mac OS • Windows 10 (More testing needed) **Other Impacts** • Resources consumed to radiate additional provisioning-only SSID on AP • Spectrum pollution – the current state requires the creation of another interference source in addition to the multitude of SSIDs that are present almost anywhere today.	Create a new provisioning solution to allow users to sign-up directly inline with the production NGH SSID and eliminate the need for dedicated provisioning SSID.
Hotspot 2.0 Release 2 - Network Selection	• Random selection of either SSID	**Operating Systems Impacted**	• Enforce mandatory

APPLIES TO	GAP	IMPACTS	RECOMMENDATION
varies for OS	when both Home and Visited HS2.0 SSIDs are present. • Policy is currently optional for service providers. • OS network selection varies from release to release and undocumented. • Devices select HS2.0 over home/private SSID when both are on same gateway.	• Android (all Versions) • iOS (all versions)	network selection policy. • Publish OS Wi-Fi network selection methods of each OS.
Access Network Query Protocol (ANQP)	• Time to decode ANQP responses takes too long in busy conditions. During gap analysis testing at the MWC, devices could take between 10-15 seconds to receive and decode ANQP packets delaying the connection to the network. • Clicking the SSID before the ANQP has been detected will prompt the user to enter a	**Operating Systems Impacted** • Android (all Versions) • iOS (all versions) • Mac OS • Windows 10 (More testing needed)	Prioritize and improve ANQP query and response mechanisms to ensure device is quickly able to identify and associate with available NGH networks.

APPLIES TO	GAP	IMPACTS	RECOMMENDATION
	username/ password they don't know.		
Apple Devices	iOS Captive Network Assistant: When opening social media links to the online sign up server that have been shared within IOS apps, (for example Twitter) the link opens the OSU within a windowed WebView within the app and not the native browser. Within WebView the provisioning profile the device does not detect download. Prohibiting the promotion of the OSU via any form of social media apps (Facebook, LinkedIn, Tumblr, Twitter etc.)	**Operating Systems Impacted** • iOS (all versions) • MAC OS	Consistent implementation for downloading mobile config file (profile) from within stand-alone or embedded browsers.
Android Devices	• A growing number of Auto VPN solutions like Google Nexus/Pixel solutions are preventing the	**Operating Systems Impacted** Android (variable)	Implement consistent installation mechanism for profile on Android devices.

APPLIES TO	GAP	IMPACTS	RECOMMENDATION
	ability to reach a captive portal and OSU by redirecting traffic back to the VPN instead of the OSU. • Variable methods for installing/ configuring the device for NGH or legacy 802.1X access – from requiring 3rd party app, using cred.conf file that needs to be moved to the *root* of the device, or completely seamless install as in Android Nougat.		
All Devices	If more than one profile present on the device (EAP-SIM, TTLS, or TLS) then no current way for the user on any device to prioritize which profile to use. The subscriber device lacks any type of user prioritization of profiles.	**Operating Systems Impacted** • Android (all Versions) • iOS (all versions) • Mac OS • Windows 10 (More testing needed)	Implement a mechanism to be able to prioritize the profiles to be used at the time of provisioning (if more than one profile is detected) or at-time-of-use.

Table 1 - Current State Gap Analysis

4 Use Case Definitions

The following use cases define the secure inline provisioning standardization framework for NGH and legacy 802.1X networks. These will illustrate necessary changes required to optimize the process for devices when they attempt to provision at time-of-use with no previously existing credentials or configurations.

The three specific use cases and associated call flows covered are -

- Onboarding a new device for an existing customer
- Onboarding a roaming customer for the first time
- Onboarding a pay-per-use customer

Detailed call flows and requirements are documented for each of the use cases in the context of HS2.0 and Legacy 802.1X networks.

4.1 Onboarding a New Device for an Existing Customer on HS2.0 Networks

The call flow for onboarding a new device with no prior credentials, belonging to a customer of the service provider, and on the service provider's network is shown below. The flow is divided into three states that are described in sections following the call flow diagram.

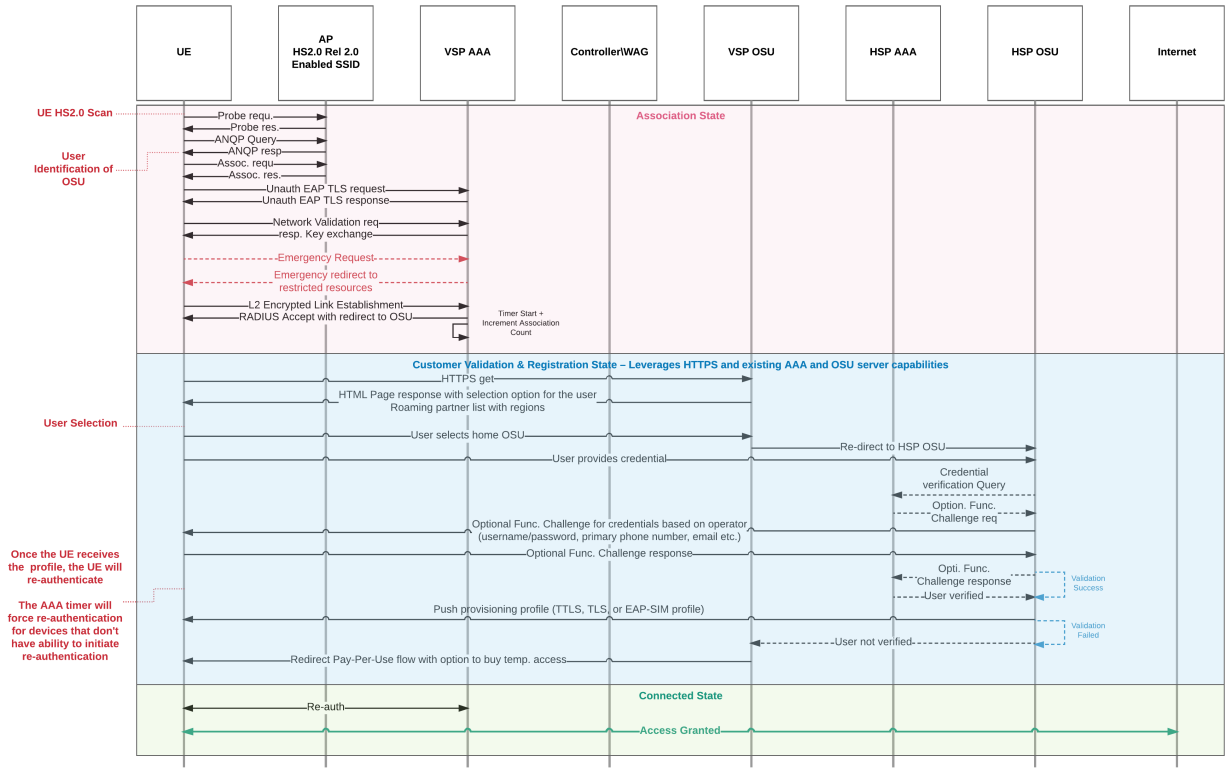


Figure-4. New customer device onboarding on HS2.0 Networks

Note: The call flow depicted above is intended to support all secure inline provisioning use cases for HS2.0 networks. The VSP and HSP AAA servers and OSU servers may be one-and-the-same when the user attempting to provision is a subscriber of the provider instead of a roamer.

4.1.1 Association State

The framework proposes extending a specific EAP-TLS variant that was originally defined to support Wi-Fi emergency calling – UNAUTH EAP-TLS (IETF RFC 5216) – to allow NGH and, potentially, legacy user devices to associate with and establish a secure encrypted Layer-2 tunnel with Wi-Fi Access Points providing NGH or legacy 802.1X service - without the need to present any credentials.

The framework proposes leveraging the same mechanism that was referenced for the emergency calling associations to enable the provisioning association to occur while preserving the ability to detect if the device association was made with the intent to place an emergency call using Emergency NAI string from the ANQP response (Ref. 802.11-2012 section 8.4.4.17). This ability to distinguish the session type is essential to ensure that the user intent is detected accurately and the session is handled properly.

The exact mechanism for enabling UNAUTH EAP-TLS to be used as the protocol to enable unauthenticated associations for *both emergency calling and provisioning* will need to be defined in collaboration with entities that own the standards/specifications that will require updates (*IETF – RFC5216, IEEE – 802.11aq, WFA HS2.0*)

4.1.1(i) The UE scans for HS2.0 capable networks and performs a discovery ANQP-element exchange to determine the home SP network is available and the capabilities of the network to enable the end-user to identify network availability prior to the IEEE 802.11 association (please refer to WFA Hotspot 2.0 Rel2 section 6.1. An example flowchart of possible steps for a UE connection manager, based on the assumptions and procedures described in WFA Hotspot 2.0 Rel2 Technical specification, Annex C.1. The device then indicates to the user that an NGH network is available for selection.

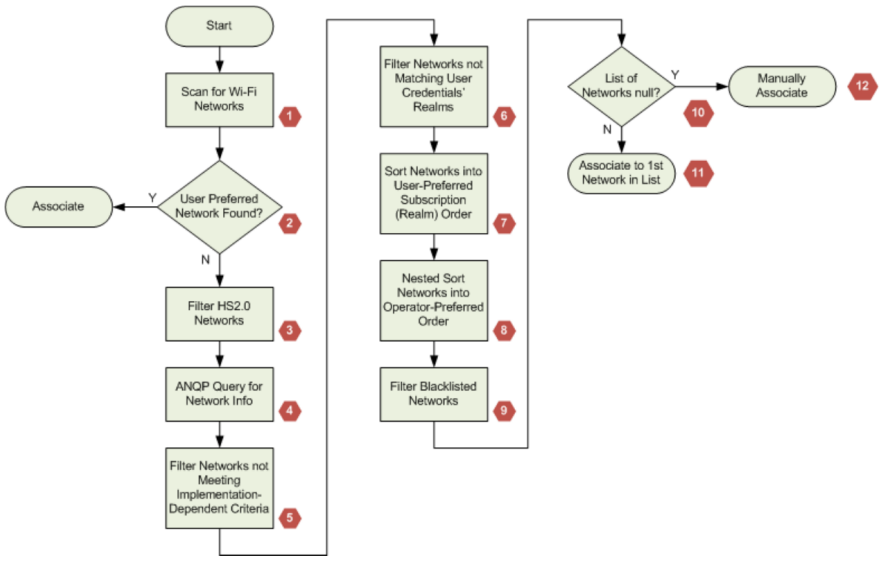


Figure-5. Connection manager steps for association (Example)

Note: Users associating manually, as depicted in step 12 of the above flow, will be doing so with the intent of provisioning their device for access using the online provisioning capability defined in this document.

4.1.1(ii) The UE begins an UNAUTH EAP-TLS association attempt, which must be user initiated (including by user attempting to place an emergency call via the native dialer, in which case the device should follow the emergency call service process as advertised in the ANQP).

4.1.1(iii) The VNP AAA server accepts the UE request to associate and presents the server certificate for validation by the UE. The UE uses root certificates[1] available locally to validate the certificate trust chain and, optionally, queries the NGH roaming consortium DB or uses locally available data to validate the *common name* and *domain name* on the that the presented certificate matches the network operator realm –

4.1.1(iii)-a If the server identify is valid the UE proceeds to key exchange and the establishment of the encrypted Layer-2 tunnel for further communications. The AAA then responds with PERMIT with REDIRECT to the WAG/controller. The WAG/controller assigns a specific VLAN identifier to the session to keep the traffic originating from the unauthenticated but associated UE separate from the traffic generated by mutually authenticated UEs.

4.1.1(iii)-b The WAG/controller must be configured to redirect all traffic originating from UEs tagged to the provisioning VLAN to the appropriate OSU server to ensure UEs are only permitted to provisioning access and otherwise restricted from having access to other network services.

4.1.1(iii)-c If the server identify cannot be validated the UE terminates the session.

4.1.1(iv) The network elements (AP, WAG/Controller) must be capable of distinguishing between UEs that associate with the network using UAUTH EAP-TLS for the purposes of provisioning and those that associate for emergency calling through the presence of the Emergency NAI string in the ANQP response provided by the UE (Ref. 802.11-2012 section 8.4.4.17) which, if present, will indicate that the user is attempting to make an emergency call enabling the routing of the user session to appropriate network resources to maintain compatibility with NGH Wi-Fi Calling standard. (Please refer to WBA NGH Wi-Fi Calling white paper). These mechanisms will need to be codified as the details of Wi-Fi emergency calling are defined in the future.

[1] The AAA must present a certificate chained to well-known Root CAs to ensure the UE can validate the legitimacy of the network provider and the AAA server. The AAA server certificate does not need to be sourced from a WFA approved CA. However, the certificate on the OSU server MUST be sourced from a WFA approved CA as this will serve as the mechanism for ensuring un-provisioned devices cannot be compromised by rogue networks/servers when they associate with the intent of provisioning for access.

4.1.1(v) UEs that do not have the Emergency NAI string present in the ANQP response are redirected to the appropriate Online Sign-Up (OSU) server using the URL provided by the AAA in the redirect message.

4.1.1(vi) The AAA also starts a session timer and increments the association counter to limit time spent in UNAUTH EAP-TLS association for the user and prevent a UE from repeatedly making UNAUTH EAP-TLS associations without completing the provisioning process.

4.1.2 Customer Validation/Registration State

This state leverages HTTPS and the OSU server capability to enable the user to complete the process of registering/validating against the network and receiving a specific profile (including appropriate credentials) that the device can use for subsequent connection attempts.

4.1.2(i) The UE initiates an HTTPS GET that is redirected to the appropriate OSU server. The OSU server responds with a HTML page containing selection options for the user (New customer PPU, existing customer, local partner or Roaming partner from registration server).

4.1.2(ii) The user follows the navigation prompts on the OSU portal for requesting a Passpoint subscription from the provider in this use case.

4.1.2(iii) If the OSU server so decides, it then delivers the appropriate Passpoint subscription to the UE for installation.

> **4.1.2(iii)-a** Optionally, at the discretion of the operator, iIf the user identity cannot be verified the user may be redirected to the pay-per-use option on the OSU to allow the user to buy network access, if desired. The user must also be presented with the option to disconnect from the network and terminate the session at this point.

4.1.2(iv) The UE natively installs the profile and configures the device for mutually authenticated network access and sends a notification to the OSU server of having completed the configuration process. This can be done, for example, via a HTTP/HTTPS GET Request to a specific URL. However, the exact mechanism for this will need to be

defined within the HS2.0 specification. If the device is able to reinitialize the EAP session, a flag will be set in the OSU server indicating this.

4.1.2(v) If the OSU server receives UE notification of successful completion of configuration steps with no indication that the device will reinitialize the EAP session, the server will notify the AAA to initiate a COA-disconnect for the user session to trigger a re-association using the newly provisioned credentials/profile. Alternatively, following successful provisioning, if the device is able to reinitialize the EAP session, the device will do so terminating the initial session and start a new session using the provisioned credentials. This will prevent that device from having to re-associate to the SSID. Otherwise, in the event of rejection of service, failure to provision, or on the expiration of a timer the AAA server will issue a COA-disconnect for the provisioning session.

4.1.3 Connected State

4.1.3(i) UE completes mutual authentication and is fully online with access to all network resource and services.

4.2 Roaming Partner Customer Provisioning on HS2.0 Networks

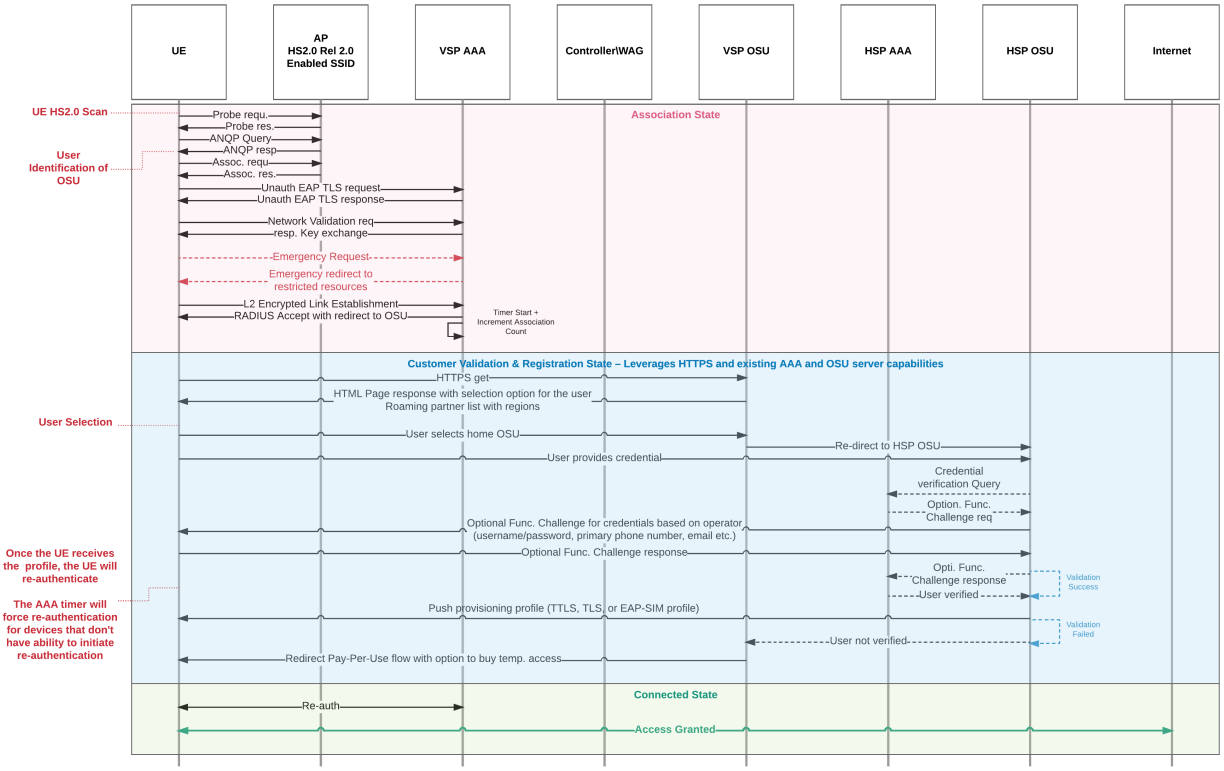


Figure-6. Roaming device onboarding on HS2.0 Networks

4.2.1 Association State

The Association State for devices belonging to roaming customers is the same as described in section 4.1.1 of this document. The initial association and determination of whether the device associated with the intent to provision or make an emergency call occur using the exact same mechanisms and standards.

4.2.2 Customer Validation/Registration State

4.2.2(i) The UE initiates a HTTP/HTTPS GET that is redirected to the OSU server. The OSU server responds with a HTML page containing selection options for the user (New customer PPU, existing customer, local partner or Roaming partner from registration server).

4.2.2(ii) The user follows the navigation prompts on the VSP OSU portal for self-identifying home provider from the list of available providers and registering as a roaming subscriber of one of the provider partners. At this point, the VSP OSU redirects the user session to the HSP OSU, directly or via a 3rd-party hub provider, to allow the provisioning process to continue further while preserving CPNI compliance by not requiring the user to disclose any personally identifiable information to the VSP OSU. Optionally, the home provider may implement additional verification of the user identify through means such as one-time code verification (the exact implementation for validating the user identify is left to the discretion of the provider).

4.2.2(iii) The HSP OSU server initiates the challenge/response process to validate the identity of its roaming subscriber using the mechanisms implemented by the HSP. The HSP AAA validates the user's identity.

4.2.2(iv) Once the user identity and authorization to use the network services is successfully verified through the challenge\response process the Home OSU server delivers the appropriate profile the UE using templates provided by the home service provider of the subscriber attempting to provision.

> **4.2.2(iv)-a** Optionally, at the discretion of the operator, if the user identity cannot be verified the Home OSU may redirect the user to the VSP OSU to allow the user the opportunity to buy pay-per-use network access, if desired. The user must also be presented with the option to disconnect from the network and terminate the session at this point.

4.2.2(v) The UE natively installs the profile and configures the device for mutually authenticated network access and sends a notification to the OSU server of having completed the configuration process. This can be done, for example, via a HTTP/HTTPS GET Request to a specific URL. However, the exact mechanism for this will need to be defined within the HS2.0 specification.

4.2.2(vi) If the OSU server receives UE notification of successful completion of configuration steps with no indication that the device will reinitialize the EAP session, the server will notify the AAA to initiate a COA-disconnect for the user session to trigger a re-association using the newly provisioned credentials/profile. Alternatively, following successful provisioning, if the device is able to reinitialize the EAP session, the device will do so terminating the initial session and start a new session using the provisioned credentials. This will prevent that device from having to re-associate to the

SSID. Otherwise, in the event of rejection of service, failure to provision, or on the expiration of a timer the AAA server will issue a COA-disconnect for the provisioning session.

4.2.3 Connected State

4.2.3(i) UE completes mutual authentication and is fully online with access to all network resource and services.

4.3 Pay-per-Use Provisioning on HS2.0 Networks

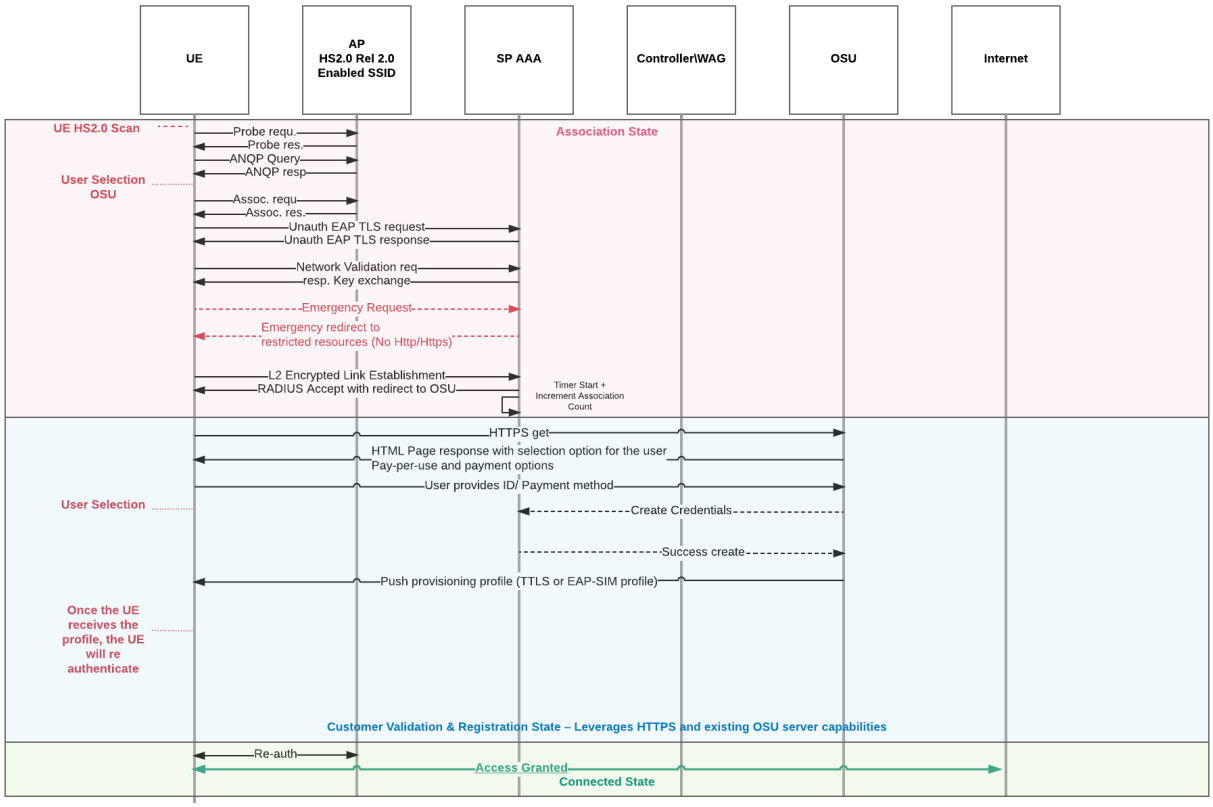


Figure-7. Pay-per-use (PPU) device onboarding on HS2.0 Networks

4.3.1 Association State

The Association State for devices belonging to pay-per-use customers is the same as described in section 4.1.1 of this document. The initial association and determination of whether the device associated with the intent to provision or make an emergency call occur using the exact same mechanisms and standards.

4.3.2 Customer Validation/Registration State

4.3.2(i) The UE initiates a HTTP/HTTPS GET that is redirected to the OSU server. The OSU server responds with a HTML page containing selection options for the user (New customer PPU, existing customer, local partner or Roaming partner from registration server).

4.3.2(ii) The user follows the navigation prompts on the OSU portal for self-identifying and registering as a pay-per-use (PPU) subscriber of one of the provider partners.

4.3.2(iii) The user follows the OSU prompts to create a new PPU account, select desired service, and complete payment.

4.3.2(iv) Once the PPU transaction is completed the OSU server generates credentials and delivers them to the UE.

4.3.2(v) The UE natively installs the profile and configures the device for mutually authenticated network access and sends a notification to the OSU of having completed the configuration process. This can be done, for example, via a HTTP/HTTPS GET Request to a specific URL. However, the exact mechanism for this will need to be defined within the HS2.0 specification.

4.3.2(vi) If the OSU server receives UE notification of successful completion of configuration steps with no indication that the device will reinitialize the EAP session, the server will notify the AAA to initiate a COA-disconnect for the user session to trigger a re-association using the newly provisioned credentials/profile. Alternatively, following successful provisioning, if the device is able to reinitialize the EAP session, the device will do so terminating the initial session and start a new session using the provisioned credentials. This will prevent that device from having to re-associate to the SSID. Otherwise, in the event of rejection of service, failure to provision, or on the expiration of a timer the AAA server will issue a COA-disconnect for the provisioning session..

4.3.3 Connected State

4.3.3(i) UE completes mutual authentication and is fully online with access to all network resource and services.

4.4 Onboarding a New Device for an Existing Customer on Legacy 802.1X Networks

The call flow for onboarding a new device, with no prior credentials, belonging to a customer of the service provider, and on the server provider's legacy 802.1X network is shown below. The flow is divided into three states that are described in sections following the call flow diagram.

Legacy 802.1X network operators should enable 802.11u support on their networks, if supported by the existing infrastructure, to enable the communication between the network and ANQP compatible devices. This is an optional add-on that operators might implement to provide the end-users with information about the available networks that support in-line provisioning in an intuitive and easy-to-use format.

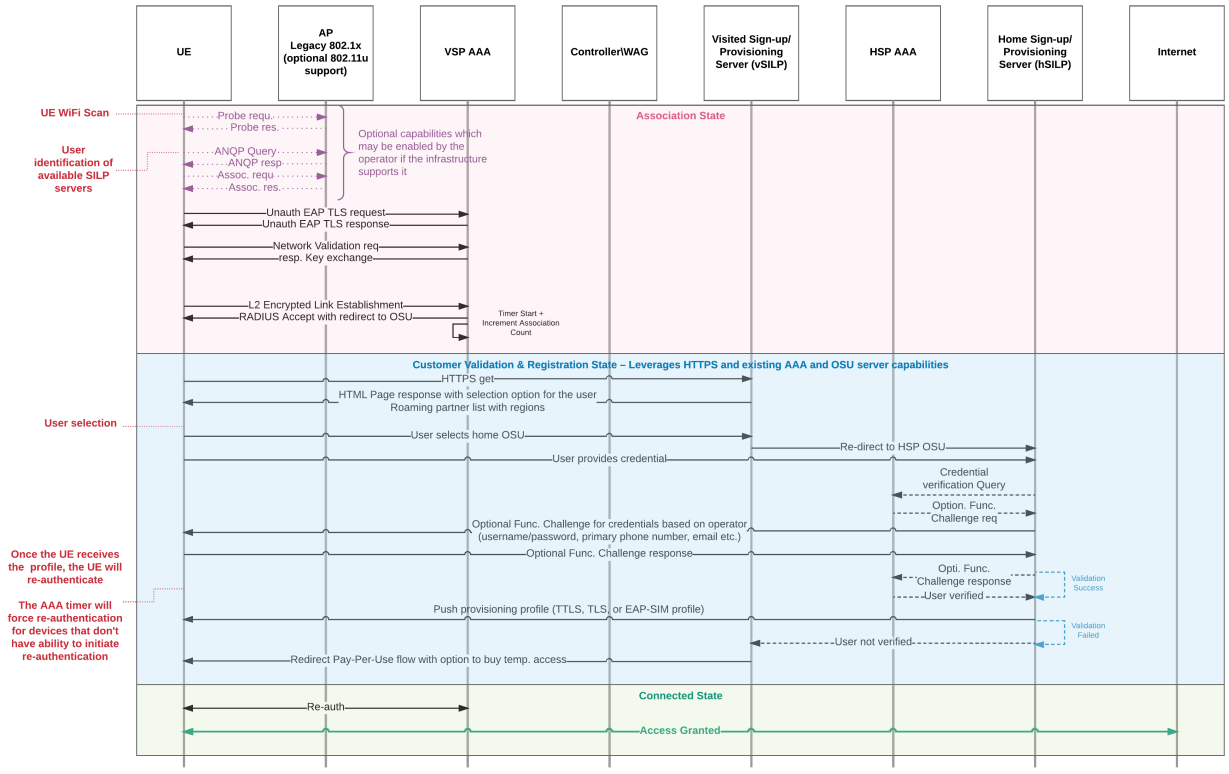


Figure 8 - New device onboarding on legacy 802.1X networks

Note: The call flow depicted above is intended to support all secure inline provisioning use cases for Legacy 802.1X networks. The VSP and HSP AAA servers and SILP servers may be one-and-the-same when the user attempting to provision is a subscriber of the provider instead of a roamer.

While the secure in-line functionality is not dependent on 802.11u enabling these features along with the appropriate changes in the device OS will remove the onus of knowing the various SSIDs from the end-users and improve the overall experience.

4.4.1 Association State

4.4.1(i) The UE scans for available Wi-Fi networks and, if capable, performs a discovery ANQP-element exchange to determine the availability of provider network the user may have access to and the capabilities of these networks prior to IEEE 802.11 association. ANQP capable devices can display well-known brand names and icons for available networks to enable the user to easily identify the networks that the user may have access to. Legacy devices will display SSIDs – in this scenario, the users will need to be aware of well-known SSIDs in order to select networks they can attempt to provision against.

4.4.1(ii) The UE begins an UNAUTH EAP-TLS association attempt, which may be automatic, or user initiated based on the capability of the specific UE.

4.4.1(iii) The AAA server accepts the UE request to associate and presents the server certificate for validation by the UE. The UE uses root certificates[2] available locally to validate the certificate trust chain and, optionally, queries the NGH roaming consortium DB or uses locally available data to validate the *common name* and *domain name* on the presented certificate matches the network operator realm –

4.4.1(iii)-a If the server identify is valid the UE proceeds to key exchange and the establishment of the encrypted Layer-2 tunnel for further communications. The AAA then responds with PERMIT with REDIRECT to the WAG/controller. The WAG/controller assigns a specific VLAN identifier to the session to keep the traffic originating from the unauthenticated but associated UE separate from the traffic generated by mutually authenticated UEs.

4.4.1(iii)-b The WAG/controller must be configured to redirect all traffic originating from UEs tagged to the provisioning VLAN to the OSU server to ensure UEs are only permitted to provisioning access and otherwise restricted from having access to other network services.

4.4.1(iii)-c If the server identify cannot be validated the UE terminates the session.

[2] The AAA must present a certificate chained to well-known Root CAs to ensure the UE can validate the legitimacy of the network provider and the AAA server. The AAA server certificate does not need to be sourced from a WFA approved CA. However, the certificate on the OSU server MUST be sourced from a WFA approved CA as this will serve as the mechanism for ensuring un-provisioned devices cannot be compromised by rogue networks/servers when they associate with the intent of provisioning for access.

4.4.1(iv) If WAG/Controller redirects all traffic originating from the UE after it associates using UNAUTH EAP-TLS to the Secure In-Line Provisioning (SILP) server using the URL provided by the AAA in the redirect message. The SILP server is a new element that is being introduced as part of this whitepaper. However, it is very similar in functionality to a captive portal and can leverage HTTPS to implement the communication and delivery of configuration profiles to the UE.

4.4.1(v) The AAA also starts a session timer and increments the association counter to limit time spent in UNAUTH EAP-TLS association for the user and prevent a UE from repeatedly making UNAUTH EAP-TLS associations without completing the provisioning process.

4.4.2 Customer Validation/Registration State

This state leverages HTTPS and the SILP server capability to enable the user to complete the process of registering/validating against the network and receiving a specific profile (including appropriate credentials) that the device can use for subsequent connection attempts.

4.4.2(i) The UE initiates a HTTPS GET that is redirected to the SILP server. The SILP server responds with a HTML page containing selection options for the user (New customer PPU, existing customer, local partner or Roaming partner from registration server).

4.4.2(ii) The user follows the navigation prompts on the SILP portal for registering as a customer/subscriber of the provider in this use case. This step will include the capability for challenge/verification of the user's identity through the SILP server. Optionally, the provider may implement additional verification of the user identify through means such as one-time code verification (the exact implementation for validating the user identify is left to the discretion of the provider).

4.4.2(iii) Once the user identity and authorization to use the network services is successfully verified through the challenge\response process the SILP server delivers the appropriate profile to the UE for installation.

4.4.2(iii)-a If the user identity cannot be verified the user should be redirected to the pay-per-use option on the SILP to allow the user the option to buy network access.

4.4.2(iv) The UE natively installs the credentials and configures the device for mutually authenticated network access and sends a notification to the SILP server of having completed the configuration process. This can be done, for example, via a HTTP/HTTPS GET Request to a specific URL.

4.4.2(v) If the SILP server receives UE notification of successful completion of configuration steps with no indication that the device will reinitialize the EAP session, the server will notify the AAA to initiate a COA-disconnect for the user session to trigger a re-association using the newly provisioned credentials/profile. Alternatively, the AAA server will issue a COA-disconnect for the session based on the expiration of the timer it initiates for the session when the UE first associates to trigger re-association using provisioned credentials. Or if the device is able to reinitialize the EAP session, the device will do so terminating the initial session and start a new session using the provisioned credentials. This will prevent that device from having to re-associate to the SSID.

4.4.3 Connected State

4.4.3(i) UE completes mutual authentication and is fully online with access to all network resource and services.

4.5 Roaming Partner Customer Provisioning on Legacy 802.1X Networks

The call flow for onboarding a device belonging to a roaming partner customer onto a legacy 802.1X network operated by the visited network operator is shown below.

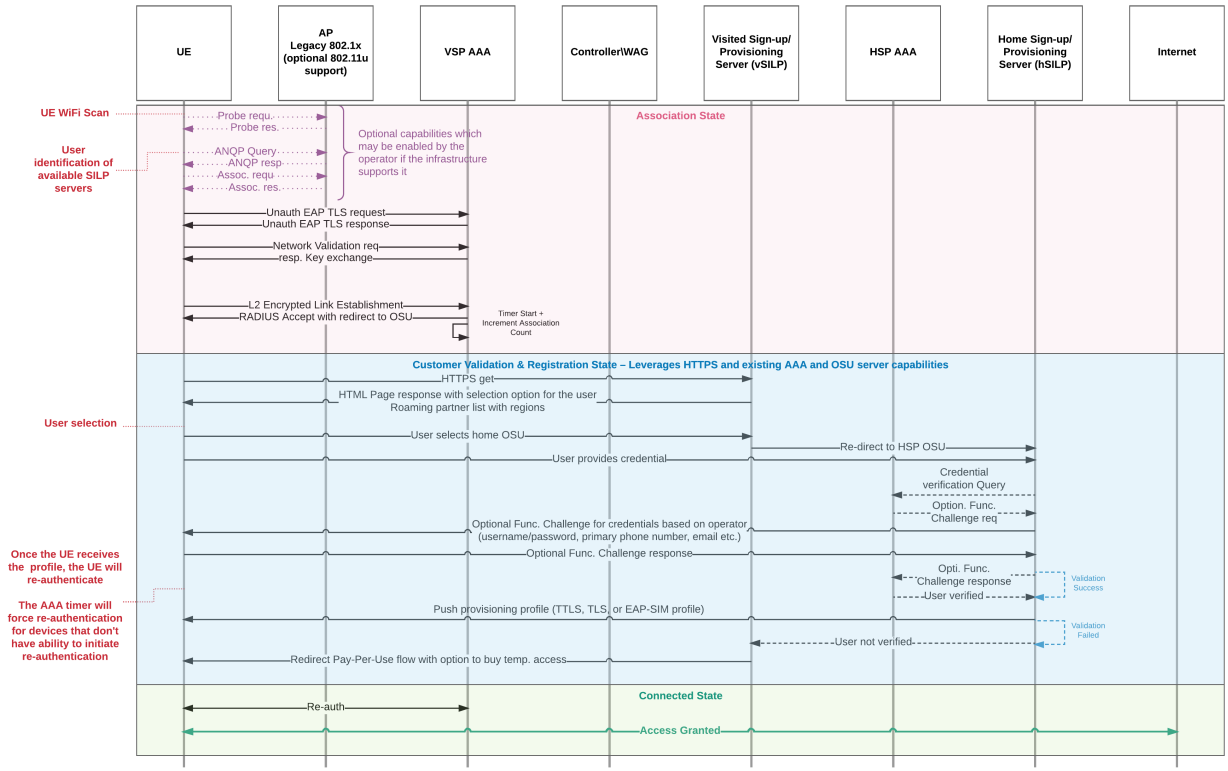


Figure 9 – Roaming partner customer onboarding on legacy 802.1X networks

4.5.1 Association State

The Association State for devices belonging to roaming customers is the same as described in section 4.4.1 of this document. The initial association on legacy 802.1X networks using the UNAUTH EAP-TLS mechanism is assumed to be for the purposes of device provisioning as Emergency calling over Wi-Fi has been defined as a HS2.0 network capability. Extending the Emergency calling over Wi-Fi to legacy 802.1X networks will need to be defined by the NGH Wi-Fi workgroup, if desired, and is outside the scope of this document.

4.5.2 Customer Validation/Registration State

4.5.2(i) The UE initiates a HTTP/HTTPS GET that is redirected to the vSILP server. The vSILP server responds with a HTML page containing selection options for the user (New customer PPU, existing customer, local partner or Roaming partner from registration server).

4.5.2(ii) The user follows the navigation prompts on the SILP portal for self-identifying home provider from the list of available providers and registering as a roaming subscriber of one of the provider partners. The vSILP server redirects the user request to the appropriate hSILP based on the home provider selected by the user. The communication between the vSILP and hSILP servers may be achieved through a direct peering setup between the visited operator and the home operator or it may be implemented through a 3rd party hub provider. The interconnection can use any suitable point-to-point secure communication technology such as L2TPv3, GRE, etc. but the communication between the end-user device, vSILP, and hSILP will be over HTTPS. Redirecting the user to the home SILP once the user has indicated the home operator eliminates the need for the vSILP to collect any personal identity data (CPNI) for the roaming subscriber. Optionally, the home provider may implement additional verification of the user identify through means such as one-time code verification (the exact implementation for validating the user identify is left to the discretion of the provider).

4.5.2(iii) The hSILP server initiates the challenge/response process to validate the roaming user's identity once the user provides the credentials to the hSILP server. The hSILP server forwards the credentials to the local AAA for authentication.

4.5.2(iv) Once the user identity and authorization to use the network services is successfully verified through the challenge/response process the hSILP server delivers the appropriate profile the UE.

4.5.2(v) If the user identity cannot be verified the user should be redirected to the pay-per-use option on the vSILP to allow the user the option to buy network access. This is an optional implementation for operators. It is also acceptable to simply provide the user with the option to disconnect and look for other methods for wireless broadband access if user validation is unsuccessful.

4.5.2(v) The UE natively installs the profile and configures the device for mutually authenticated network access and sends a notification to the hSILP server of having completed the configuration process. This can be done, for example, via a HTTP/HTTPS GET Request to a specific URL. The hSILP redirects the UE to a specific URL hosted on the vSILP server once the specific URL trigger is received from the UE indicating successful completion of device provisioning steps.

4.5.2(vi) When the vSILP server receives the redirect from the hSILP server for the UE it will notify the visited AAA to initiate a COA-disconnect for the user session to trigger a re-association using the newly provisioned credentials/profile. Alternatively, the AAA server will issue a COA-disconnect for the session based on the expiration of the timer it initiates for the session when the UE first associates to trigger re-association using provisioned credentials.

4.5.3 Connected State

4.5.3(i) UE completes mutual authentication and is fully online with access to all network resource and services.

4.6 Pay-per-Use Provisioning on Legacy 802.1X Networks

The call flow for registering pay-per-use customers on legacy 802.1X networks is shown below.

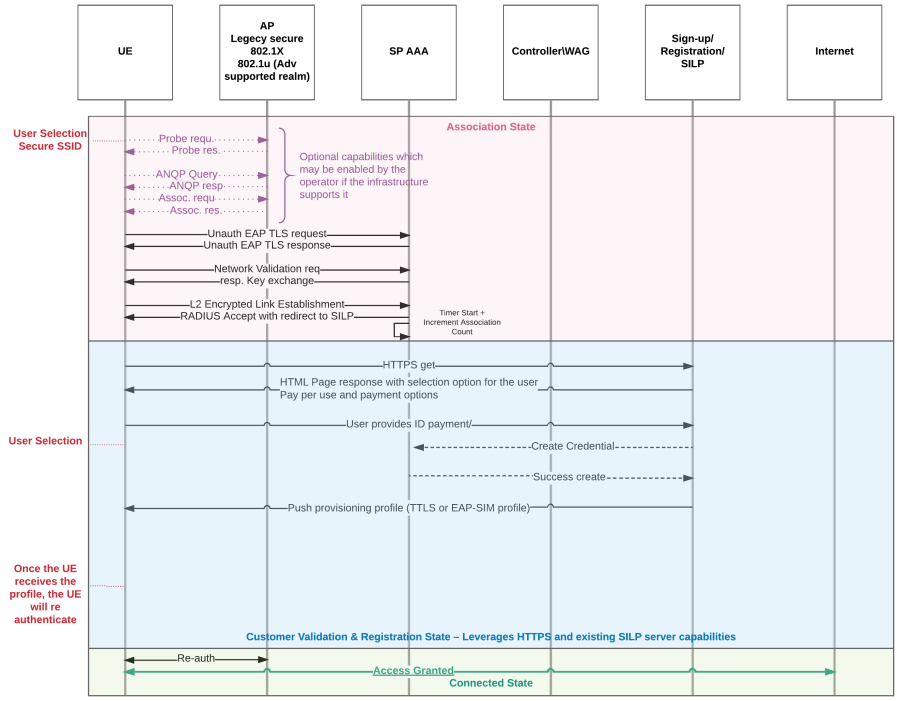


Figure 10 – Pay-per-use customer onboarding on legacy 802.1X networks

4.6.1 Association State

The Association State for devices belonging to roaming customers is the same as described in section 4.4.1 of this document. The initial association on legacy 802.1X networks using the UNAUTH EAP-TLS mechanism is assumed to be for the purposes of device provisioning as Emergency calling over Wi-Fi has been defined as a HS2.0 network capability. Extending the Emergency calling over Wi-Fi to legacy 802.1X networks will need to be defined by the NGH Wi-Fi workgroup, if desired, and is outside the scope of this document.

4.6.2 Customer Validation/Registration State

4.6.2(i) The UE initiates a HTTP/HTTPS GET that is redirected to the SILP server. The SILP server responds with a HTML page containing selection options for the user (New

customer PPU, existing customer, local partner or Roaming partner from registration server).

4.6.2(ii) The user follows the navigation prompts on the SILP portal for self-identifying and registering as a pay-per-use (PPU) subscriber of one of the provider partners.

4.6.2(iii) The user follows the SILP prompts to create a new PPU account, select desired service, and complete payment.

4.6.2(iv) Once the PPU transaction is completed the SILP server generates credentials and delivers them to the UE.

4.6.2(v) The UE natively installs the profile and configures the device for mutually authenticated network access and sends a notification to the SILP of having completed the configuration process. This can be done, for example, via a HTTP/HTTPS GET Request to a specific URL.

4.6.2(vi) If the SILP receives UE notification of successful completion of configuration steps it will notify the AAA to initiate a COA-disconnect for the user session to trigger a re-association using the newly provisioned credentials/profile. Alternatively, the AAA server will issue a COA-disconnect for the session based on the expiration of the timer it initiates for the session when the UE first associates to trigger re-association using provisioned credentials.

4.6.3 Connected State

4.6.3(i) UE completes mutual authentication and is fully online with access to all network resource and services.

5 Requirements

The specific requirements and updates required to the underlying standards, user equipment, and network elements to operationalize the *secure inline-provisioning* framework are defined in this section. The requirements and updates are classified as *must* and *should* to differentiate between the ones that are essential for enabling the base-level functionality. The changes and requirements that are classified as *should* enable capabilities to deliver an optimized user experience.

5.1 Standards Updates

STANDARD	CHANGE/REQUIREMENT	CLASSIFICATION
HS2.0	Eliminate the need for a separate dedicated provisioning SSIDs (Open and Secure) for online sign-up.	Must
	Update supported association methods to include UNAUTH EAP-TLS based associations for provisioning purposes.	Must
	Update the HS2.0 architecture to support the implementation of separate Layer-2 VLANs on the NGH network to separate *unauthenticated provisioning and emergency services* sessions from *mutually authenticated* sessions.	Must
	Define a mechanism to mitigate attacks against mutually authenticated and unauthenticated users launched by malicious actors using broadcast and multicast capabilities after they associate using the UAUTH EAP-TLS mechanism – possible options for addressing these threats could entail restricting *provisioning associations* to UNICAST communications only or, alternatively, extending the EAP-TLS specification to support *separate Group Temporal Key (GTK)* for each broadcast domain (VLAN) to minimize the potential impact of such attacks.	Must
	Define a mechanism for identifying UEs associating to the network with the intent of making an Emergency call when the Emergency NAI string is not present in the ANQP response provided by the UE.	Must
	Extend HS2.0 to define a framework for preventing UEs from associating repeatedly using the UNAUTH EAP-TLS mechanism with no intent of provisioning credentials but as a potential method for launching DOS attacks – this should consider methods to identify such associations without relying on UE MAC ID since it is easy to spoof MAC IDs.	Must

5.2 User Equipment Requirements

UE TYPE	CHANGE/REQUIREMENT	CLASSIFICATION
All	Extend EAP-TLS supplicant to support UNAUTH EAP-TLS association type – the actual association, will be manually triggered by the user. When such an association is association with a secure NGH, the UE should fallback to UNAUTH EAP-TLS as the association mechanism when it detects no available credentials for the target network. The default prompt for credentials that is currently displayed when a user attempts to associate with a legacy 802.1X SSID must be modified to allow the user to choose between – 1) providing credentials to attempt authentication against the network or 2) associate for secure inline provisioning. If the user chooses the second option the device must associate using UNAUTH EAP-TLS as the EAP method.	Must
	Extend broadcast/multicast packet decryption mechanism to discard group-addressed packets that either a) Don't match the GTK for unauthenticated associations, if implemented or b) All group-addressed packets when GTK is not assigned to the provisioning session – i.e., UE is limited to UNICAST only.	Must
	Validate *Network Operator, OSU/Secure In-line Provisioning Server (SILP)*[3], and *AAA* server identities using root CA certs available locally on the device - and optional queries to the NGH roaming consortium DB to ensure that the association attempt is being made on a legitimate provider network – trigger UE side disassociation if provider identity cannot be validated.	Must
	Ability to disassociate from a provider network after completion of credentials provisioning and re-authenticate using the installed credentials for full network access.	Must
	Enhance the "Wi-Fi networks are in range" message to intelligently identify partner networks and provide user-friendly prompt via an enhanced UI when provider or	Should

[3] The OSU and SILP server certificates must be sourced from WFA approved CA to ensure operator identity and authenticity is validated. The UE must disassociate from any network that doesn't present a certificate signed by an approved CA to prevent the compromise of any personally identifiable information about the subscriber in transacting with the OSU/SILP servers.

UE TYPE	CHANGE/REQUIREMENT	CLASSIFICATION
	partner networks are in range.	
All	Mechanism to allow user-selected invocation of anonymous TLS for provisioning purposes as alternative to current behavior – manual entry of 802.1X credentials.	Must
All	Mechanism for "native provisioning" of 802.1X credentials as described in 4.4.2(iv).	Must
All	Ability to generate a HTTPS request to specific URLs provided as a value-attribute pair by the AAA after the installation of credentials supplied by the OSU/SILP server is completed to indicate completion of device provisioning.	Should
All	Ability to re-initiate an the UNAUTH EAP-TLS session after the credentials supplied by the OSU/SILP server are installed to re-authenticate with the provider network using the credentials that were received during the provisioning process.	Should
iOS	Simplify the profile installation process to minimize the number of steps involved or make it zero-touch similar to the experience available on Android Nougat.	Should
Android	Add an additional feature to the profile installation module to remove the initial association with the target SSID from the list of "user networks" to ensure the device subsequently connects to the SSID using the credentials that are configured as part of the provisioning process and to prevent repeated connections using UNAUTH EAP-TLS.	Must

5.3 Access Point

CHANGE/REQUIREMENT	CLASSIFICATION
Ability to perform VLAN tagging at the session level – specifically the ability to assign and enforce separate VLANs for unauthenticated provisioning associations made using UNAUTH EAP-TLS and mutually authenticated unrestricted associations based on direction from the AAA as part of the EAP response.	Must
Ability to redirect HTTP/HTTPS requests originating from UEs associating using UNAUTH EAP-TLS to the Provisioning Server – this function is required in architectures that employ local breakout for internet traffic on the APs.	Must
Support for separate Group Temporal Key (GTK) for the VLANs to ensure separation of broadcast/multicast traffic for each domain.	Must – pending confirmation from WFA security reviews
Rule based blacklist enforcement for UE MAC IDs based on AAA response for abusive UEs that repeatedly associate using UNAUTH EAP-TLS (e.g., timed blacklisting, etc.).	Must

5.4 Controller/WAG:

CHANGE/REQUIREMENT	CLASSIFICATION
Ability to perform VLAN tagging at the session level – specifically the ability to assign and enforce separate VLANs for unauthenticated provisioning associations made using UNAUTH EAP-TLS and mutually authenticated unrestricted associations based on direction from the AAA as part of the EAP response.	Must
Ability to redirect HTTP/HTTPS requests originating from UEs associating using UNAUTH EAP-TLS to the Provisioning Server – this function is required in architectures that employ local breakout for internet traffic on the APs.	Must
Rule based blacklist enforcement for UE MAC IDs based on AAA response for abusive UEs that repeatedly associate using UNAUTH EAP-TLS (e.g., timed blacklisting, etc.).	Must

5.5 AAA Server

CHANGE/REQUIREMENT	CLASSIFICATION
Support for UNAUTH EAP-TLS as a supported EAP authentication method including the ability to assign a configurable VLAN tag and configurable redirect URL that will be assigned to each UNAUTH EAP-TLS session.	Must
Implementation of timer for UNAUTH EAP-TLS associations to terminate sessions after a configurable amount to time.	Must
New secure (mutually authenticated via shared secret/certificate) web service to accept Provisioning Server (OSU or SILP) notification to terminate the specified provisioning session based on device MAC ID or SESSION ID when a provisioning session has successfully completed based on user input regardless of whether the session timer has expired or not.	Must
Ability to issue a COA-disconnect for a specific session based on input received from the Provisioning server.	Must
Implementation of an association counter based on a unique device identifier (potentially MAC ID or another attribute that is harder to spoof) to maintain a count of repeated association attempts by a device using UNAUTH EAP-TLS.	Must
Ability to identify abusive UEs based on the association counter and blacklisting such UEs based on business rules defined by the service provider (e.g., blacklist UE AA:BB:CC:DD:EE: FF for 5 minutes/indefinitely etc.).	Must

5.6 Secure In-line Provisioning Server

This whitepaper introduces a new network element, Secure In-line Provisioning Server (SILP), for enabling in-line provisioning capabilities in legacy 802.1X networks. The details of this platform including technical specifications, capabilities & features, communication protocols, etc., will be detailed in a future version of this whitepaper. However, the base set of functionality that the SILP server must be capable of supporting is listed below and are similar in nature to the functions performed by a Captive Portal Server in an open network.

CHANGE/REQUIREMENT	CLASSIFICATION
A web server that the users will be redirected to after association to select from a list of available network operators – users should be choose from a list that includes the network operator and all supported roaming partners. The communications must be over HTTPS to ensure all client/server communications are encrypted and secure.	Must
Ability for SILP to collect user identification information such as *username, registered phone number, account number,* etc., along with challenge-response token such as a *password, PIN, single-use code,* etc., in a secure and encrypted manner.	Must
Ability to forward the user provided identity elements to the local AAA server for further treatment.	Must
Ability to receive and act on AAA response to the provided user identity elements. The SILP server must proceed to provisioning flow if the user identity is validated and the user is authorized for service. If the user identity is invalid or the user is not authorized for service then the SILP server must redirect the user into a pay-per-use flow (if supported) or trigger a disconnection message for the user.	Must
Ability to build and deliver a profile/configuration to the target end-user device in a format compatible with the type of device attempting to provision (e.g. mobile config for iOS and cred.conf for Android)	Must
Ability to support pay-per-use flow to enable non-subscribers to buy paid access, if supported by the operator. – See comment updates.	Must

6 Liaison Statements

6.1 WFA Liaison Request

The Next Generation Hotspot (NGH) Provisioning Standardization team would like to share with the WFA Hotspot 2.0 Technical, Marketing, and Security Task Groups the scope of use cases and concept of in-line provisioning for HS2.0 and 802.1X Wi-Fi networks. The goal is to *improve the user experience* by allowing users to discover, associate, and get their device provisioned for use in-line with first-time use over a single SSID. Use cases in scope:

1. Onboarding new device for an existing customer
2. Onboarding roaming customer for the first time
3. Onboarding pay-per-use customer

*Specific request: Modify the existing security standards for HS2.0 and 802.1X networks to allow UNAUTH-EAP-TLS associations to occur in conjunction with mutually authenticated associations on the same production SSID/network while ensuring co-existence does not open security risk or interruption of authenticated users. Additionally, to extend the existing standards to prevent devices associating without credentials on the secure SSIDs from disrupting services for mutually authenticated users by consuming resources repeatedly without the intent of provisioning credentials for authenticated access to the network.

REFERENCES

- Wi-Fi CERTIFIED Passpoint™ (Release 2) Deployment Guidelines Rev 1.1 December 7, 2016 - https://www.wi-fi.org/download.php?file=/sites/default/files/private/Passpoint_R2_Deployment_Guidelines-v1.1.pdf
- Hotspot 2.0 (Release 2) Technical Specification Package v1.2 - http://www.wi-fi.org/downloads-registered-guest/Hotspot_2-0_%2528R2%2529_Technical_Specification_Package_v1-2.zip/29728
- Open Secure Wireless 2.0 (June 8th, 2014) by Christopher Bryd - http://www.riosec.com/articles/open-secure-wireless-20
- Linux WPA/WPA2/IEEE 802.1X Supplicant - https://w1.fi/wpa_supplicant/
- RFC 5216 EAP-TLS Authentication Protocol - https://www.ietf.org/rfc/rfc5216.txt
- IEEE 802.11U – 2011 - https://standards.ieee.org/findstds/standard/802.11u-2011.html

ACRONYMS AND ABBREVIATIONS

ACRONYM / ABBREVIATION	DEFINITION
*	Wildcard
AAA	Authentication, Authorization and Accounting [server]
ANQP	Access Network Query Protocol
AP	Access Point
APC	Access Point Controller
CA	Certificate Authority
CN	Common Name
CoA	Change of Authorization
CUI	Chargeable User Identity
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
EAP-AKA	EAP Authentication and Key Agreement
EAP-AKA'	EAP AKA prime
EAP-TLS	EAP Transport Layer Security
EAP-TTLS	EAP Tunneled TLS
ESS	Extended Service Set
FQDN	Fully Qualified Domain Name
HS2.0	Hotspot 2.0
HNP	Home Network Provider (a network provider onto which a subscriber of an HSP can roam. The VNP may or may not have subscribers. Example of a non-subscriber VNP could be a business such as a hotel or event center)
HSP	Home Service Provider (a provider that offers subscriptions to users. A HSP may or may not have their own network)
HTTP	Hyper Text Transfer Protocol
IP	Internet Protocol
IPv4	IP version 4
IPv6	IP version 6
LAN	Local Area Network
MAC	Media Access Control
MCC	Mobile Country Code
MNC	Mobile Network Code
MO	Management Object
MSCHAP	Microsoft Challenge-Handshake Authentication Protocol
N/A	Not Applicable
NAI	Network Access Identifier
NAS	Non-Access Stratum
NGH	Next Generation Hotspot

OCSP	Online Certificate Status Protocol
OI	Organizational Identifier
OSEN	OSU server-only authenticated layer 2 encryption network
OSU	Online Sign Up [server]
PAP	Password Authentication Protocol
PLMN	Public Land Mobile Network
PMF	Protected Management Frames
PPS	Per Provider Subscription [MO]
PPSMO	PPS MO
R1	Release 1
R2	Release 2
RADIUS	Remote Authentication Dial In User Service
RFC	Request For Comments
RSN	Robust Security Network
SIM	Subscriber Identity Module
SILP	Secure In-Line Provisioning Server
SOAP-XML	Simple Object Access Protocol – Extensible Markup Language
SP	Service Provider
SSID	Service Set Identifier
UE	User Equipment
UI	User Interface
URL	Universal Resource Locator
UTC	Coordinated Universal Time
VNP	Visited Network Provider (a network provider onto which a subscriber of an HSP can roam. The VNP may or may not have subscribers. Example of a non-subscriber VNP could be a business such as a hotel or event center)
WBA	Wireless Broadband Association
WLC	Wireless LAN Controller
WFA	Wi-Fi Alliance
WPA2-PSK	Wi-Fi Protected Access® version 2

REVIEW AND APPROVAL

VERSION	TYPE	DATE	REVIEWED / APPROVED BY	REVIEW / APPROVAL FEEDBACK
1.0	Guidelines	03 November 2017	WBA Members – NGH Provisioning Standardization Workgroup	

PARTICIPANT LIST

COMPANY	NAME	ROLE
Comcast	Sundeep Goswami	Project Leader & Chief Editor
Comcast	Brent Daniel	Project Co-Leader & Editorial Team Member
Comcast	Toufic Kourbeh	Project Co-Leader & Editorial Team Member
CableLabs	Josh Redmore	Project Co-Leader & Editorial Team Member
GlobalReach	Chris Spencer	Project Co-Leader & Editorial Team Member
BT	Steve Dyett	Editorial Team Member
BT	Simon Ringland	Editorial Team Member
BT	Tim Twell	Editorial Team Member
CableLabs	Luther Smith	Editorial Team Member
Accuris Networks	Andrea Baccolini	Project Participant
AT&T	Irene Morvey	Project Participant
AT&T	Erinn Hall	Project Participant
Boingo Wireless	Akhil Sreenatha	Project Participant
BSG Wireless	Charlie Allgrove	Project Participant
BSG Wireless	Betty Cockrell	Project Participant
BSG Wireless	Michael Sym	Project Participant
Charter Communications	Loay Kreishan	Project Participant
GlobalReach	Thomas Locke	Project Participant
iBwave	Vladan Jevremovic	Project Participant
Orange	Nigel Bird	Project Participant
Ruckus Wireless	Mark Hamilton	Project Participant
Shaw Communications	Hussam Radman	Project Participant
Shaw Communications	Christian Saunders	Project Participant
Smith Micro Inc.	Dzung Tran	Project Participant
WBA	Bruno Tomas	Project Participant
WBA	Tiago Rodrigues	Project Participant