CONFIDENTIAL TRADE SECRET

FOR USE ONLY BY AUTHORIZED WI-FI ALLIANCE® MEMBERS

– DO NOT COPY –

Marketing Requirements Document for Passpoint 2024 FR

Version 1.0

10900-B Stonelake Boulevard, Suite 126
Austin, TX 78759

Phone: 512.498.9434 • Fax: 512.498.9435 • Email: certifications@wi-fi.org

www.wi-fi.org

Latest version available at: insert link

WI-FI ALLIANCE PROPRIETARY AND CONFIDENTIAL – SUBJECT TO CHANGE WITHOUT NOTICE

Table of Contents

1 EXECUTIVE SUMMARY 6
2 REFERENCES 7
2.1 Definitions, Acronyms and Abbreviations 7
2.1.1 Definitions 7
2.1.2 Acronyms and Abbreviations 7
3 MARKET AND MOTIVATION 9
3.1 Technology Overview 9
3.2 Market Segment and Window 9
3.3 Defining Use Cases 9
3.3.1 Subscription provisioning 9
3.3.1.1 Standard provisioning format 10
3.3.1.2 Provisioning from anywhere 10
• Purchase of a new Wi-Fi enabled device 10
• User Preparing for Travel 11
• Over the Top (OTT) Service Provider 11
3.3.2 Deauthentication Imminent 11
3.3.3 IoT Devices on Passpoint Networks 11
3.3.3.1 IoT Devices in Carpeted Enterprise 12
3.3.3.2 IoT Devices in Industrial Warehouse 12
3.3.3.3 IoT Devices that roam across healthcare settings 12
3.4 Competing and Substitute Technologies 13
3.5 Dependencies & Risks 13
3.5.1 Internal Dependencies 13
3.5.2 External Dependencies 13
3.5.3 Ecosystem Dependencies (Only for non-MAC/PHY Programs) 13
3.5.4 Wi-Fi Alliance Portfolio Alignment 13
3.5.5 Regulatory Considerations 13
3.6 Naming Recommendation 14
4 NEW PROGRAM DEVELOPMENT READINESS RESULTS 15

5 SCOPE OF INTEROPERABILITY CERTIFICATION 16
6 REQUIREMENTS 17
6.1 Prerequisites 17
6.2 Out-of-the-Box Requirements 17
6.3 Mandatory Features 17
6.3.1 Standard subscription format 17
6.3.2 Deauthentication imminent 17
6.4 Optional Features 17
6.5 Conditional Mandatory 17
6.6 Legacy Interoperability 18
APPENDIX A DOCUMENT REVISION HISTORY 19

List of Tables

Table 1. Definitions 7
Table 2. Acronyms and Abbreviations 7
Table 3. Document Revision History 19

1 Executive Summary

The Online Sign Up (OSU) solution provided in Passpoint “release 2” (2015) was intended to address the challenges of onboarding devices. However, OSU is being discontinued, due primarily to lack of market adoption and resulting challenge with business model to support the technology. Market adoption of Passpoint – both adoption within devices, especially client devices, and breadth of deployment of infrastructure –continues to be significantly limited due to the lack of a standardized mechanism for onboarding devices. With the loss of OSU, it is critical to find an onboarding mechanism for Passpoint that is simpler and will gain adoption.

The Passpoint MTG believes that this replacement needs to simplify the onboarding procedures for Passpoint to encourage broad use of Passpoint in the market, and to continue our drive to move away from captive portals toward secure Passpoint networks. Such simplification is also being considered, for example, by the Wireless Broadband Alliance (WBA) for their OpenRoaming technology, and it is crucial that we do not encourage a division of technical solutions, but rather that we address the onboarding challenges directly in the Passpoint program itself.

Such simplification might include: using only existing standard protocols or methods to provide a Passpoint-defined format “subscription” to a client; addressing user interaction challenges for headless devices; allowing onboarding from “anywhere” (not only at the Passpoint venue); and other similar technical approaches.

By making Passpoint onboarding generally supported across clients, and easier to deploy for network operators, we will broaden the appeal and remove barriers to Passpoint adoption and deployment.

The Wi-Fi Alliance (WFA) Passpoint Marketing Task Group recommends that the WFA Board of Directors approve this Marketing Requirements Document (MRD) for a Maintenance Release of Passpoint and that the Passpoint Technical Task Group use it as the basis to develop a Passpoint Maintenance Release specification and certification test plan.

2 References

[1] Wi-Fi Alliance Passpoint Specification v3.2.21

[2] IEEE Std 802.11-2020: https://standards.ieee.org/standard/802_11-2020.html

2.1 Definitions, Acronyms and Abbreviations

2.1.1 Definitions

The following definitions are applicable to this document.

Table 1. Definitions

Term	Definition

2.1.2 Acronyms and Abbreviations

This section defines the acronyms and abbreviations used throughout this document. Some acronyms and abbreviations are commonly used in publications and standards defining the operation of wireless local area networks, while others have been generated by Wi-Fi Alliance. Refer to the Wi-Fi Alliance Acronyms Terms Definitions document for a complete list of approved acronyms and abbreviations.

Table 2. Acronyms and Abbreviations

Acronyms	Definition
AAA	Authentication, Authorization and Accounting
AP	Access Point
APUT	Access Point Under Test
CA	Certificate Authority
HTTP(S)	Hypertext Transfer Protocol (Secure)
MAC	Medium Access Control
OS	Operating System
OSU	Online Sign-Up
OTT	Over The Top
PHY	Physical
SIM	Subscriber Identity/Identification Module
STA	Station
STAUT	Station Under Test

Acronyms	Definition
UI	User Interface
URL	Uniform Resource Locator
USD	Unsynchronized Service Discovery
WBA	Wireless Broadband Alliance
WFA	Wi-Fi Alliance

3 Market and Motivation

3.1 Technology Overview

In “Version 2” (the 2015 release) of Passpoint, a facility to onboard/provision client devices for Passpoint network authorization was added to the program – the Online Sign-Up (OSU) Server. However, the Passpoint program has struggled with both certifications as well as getting market deployment and implementation traction, ever since the OSU feature was made mandatory. The combination of implementation complexity and other concerns for device vendors, plus the complexity of deploying and operating OSU Servers on hotspot networks, have led to very slow (nearly non-existent) adoption of the technology. And, of course, that leads to a lack of WFA certifications, as well.

To compound this (and largely due to the above), recently the last remaining Certificate Authority (CA) that offers signed certificates for OSU Servers, is in the process of exiting the business. This leaves no way to authenticate new OSU Servers, and therefore the limited existing use of these servers will soon cease completely.

In order to support and bolster deployment of Passpoint networks and encourage Passpoint certifications, an alternative mechanism for onboarding/provisioning clients is offered in this Feature Release.

The core of this mechanism is a standardized format for a “subscription” that contains the information that needs to be stored on the client, to allow future discovery and attachment to Passpoint networks. This format will be defined in the Passpoint Specification, and standard methods for providing a client/mobile device with the information will be described. This method differs from the existing OSU solution by not requiring Passpoint-specific communications methods and by not requiring specific protocol-triggered actions by the client device, but instead letting device implementations leverage existing procedures for installing and managing such profiles within the device’s existing security regimes, thus simplifying implementation.

3.2 Market Segment and Window

The market segments for this update to the Passpoint program mirror the entire spectrum of existing Passpoint deployments, as well as the expected expanded market enabled by addressing headless devices, and supporting Passpoint onboarding from anywhere and not limited to the Passpoint venue.

3.3 Defining Use Cases

The following defining use cases are intended to be examples of deployments of the requirements specified in Section 6, and are not intended to exhaustively represent the scope of possible deployments of the features.

3.3.1 Subscription provisioning

Before an end-user’s device can connect to a Passpoint network, it needs to be provisioned with subscription metadata and matching credentials, such as username and password, or certificates. There are two main use cases to consider:

- Remote sign-up – where the user provisions their device out of range of the Passpoint network. Example: when booking a hotel room through a website, a user clicks on a link to provision their phone to automatically connect to the hotel’s Wi-Fi network upon arrival.
- Venue sign-up – where the user arrives at the venue without pre-configured subscription metadata and credentials. In this case, an additional sign-up process is needed to provision the device. Example: a user arrives at an airport they haven’t been to before and wants to connect their laptop to the airport’s free Wi-Fi.

The current Passpoint specification does not address remote sign-up scenarios, which are partially solved by the most popular operating systems (OS) today using proprietary formats. From the perspective of network providers, this requires additional work to maintain different subscription formats and delivery methods. From the perspective of end users, this contributes to an inconsistent experience where some of their devices may be able to connect to the Passpoint network, while others are relegated to traditional captive portal network.

The Passpoint specification covers the venue sign-up scenarios with the Online Sign-Up (OSU) functionality, which is being discontinued. Unfortunately, OSU network deployments did not gain traction since the feature was introduced in 2016. OSU was significantly complex to implement on both OS and the Network side. As a result, there was inconsistent support across the most popular operating systems, which ranged from partial to non-existent. That, in turn, puts network providers in a position where they could not solely rely on OSU to provide a solid and consistent experience for end-users.

Considering the status quo outlined above, subscription provisioning continues to significantly impact Passpoint adoption. There is a need for a simpler provisioning story that can address both remote and venue sign-up scenarios.

3.3.1.1 Standard provisioning format

Defining a standard subscription format in the Passpoint specification, which can be delivered using industry standard mechanisms (such as HTTP), rather than requiring a custom provisioning protocol like OSU, would:

- Significantly reduce the implementation cost for OS vendors, who will focus on translating the standard format into existing OS functionality, potentially leading to more consistent Passpoint functionality across the most popular operating systems.
- Simplify implementation and maintenance for network providers, as, over time, they would only need to focus on a single subscription metadata and credential package that would work on most devices, covering both username and password, and certificate-based authentication scenarios.
- Allow network providers to innovate and deploy provisioning flows that best fit their scenarios. For example, these might include captive portal networks that bootstrap provisioning and lead more users to the Passpoint connection, QR codes, or even leveraging other WFA provisioning protocols.

3.3.1.2 Provisioning from anywhere

The current specification restricts Online Signup (OSU) servers to reside within the host network. This limits where a Passpoint profile can be installed onto a device. By allowing access to provisioning from anywhere, a Passpoint profile could be downloaded and installed anywhere not requiring a connection to the subscribing operator's network as well allowing subscriber provider operators that do not have a network to provide Passpoint profiles without having agreements or partnerships with a network operator. This could be achieved by leveraging the new standard provisioning format proposed above.

These are some of the use cases that would be addressed by enabling subscription provisioning from anywhere:

- **Purchase of a new Wi-Fi enabled device**

A user has just purchased a new Wi-Fi enabled device and is a subscriber to several service providers that offer Passpoint. The user wishes to have their Passpoint profiles installed before leaving the store. The user may, or may not, know how to install the Passpoint profiles, and could solicit the help of the salesperson for help if does not know how to install a profile. The user/salesperson navigates an internet connection to the user's subscription provider's provisioning server and enters all the required information which triggers the Passpoint profile download. The device then either

disconnects from the Wi-Fi connected network if connected or proceeds with the normal selection process making use of the newly downloaded Passpoint profile.

- **User Preparing for Travel**

A user is preparing to take a trip and knows that their service provider does not offer roaming at the airports, on the airplanes, or at the hotels/resorts. However, the user has subscription to several travel memberships that will allow the user access to the networks either free or at reduced cost through credential and making use of Passpoint of ease of connections. Before the user leaves home, the user visits the travel memberships' website(s) to download the Passpoint profiles. Now the user is ready to travel knowing that they will not have to enter different credentials as they transition through the trip.

- **Over the Top (OTT) Service Provider**

An Over the Top (OTT) Service Provider (i.e. Google, Meta) that do not own or operate their own network could not provide an OSU server without having an agreement with a network provider. By enabling provisioning from anywhere, a user that has a subscription with an OTT Service Provider can access the OTT provisioning server from any network to download and install the OTT provider's Passpoint profile.

3.3.2 Deauthentication Imminent

A Passpoint network can provide an indication to an attached mobile device that is about to be deauthenticated from the Passpoint hotspot. This indication is carried in a Deauthentication Imminent Notice subelement in a WNM-Notification Request frame.

For example, this can occur during operation, if the client has run out of allocated time on the network or network conditions have changed and the client needs to be dropped. Also, the indication is used immediately after the device has connected, to indicate that although the EAP authentication succeeded, the client is no longer authorized for service at the time and/or location, or the hotspot network or core network is congested and the device cannot be supported.

The Deauthentication Imminent Notice might carry further information for the client, as a Reason URL to a webpage explaining the deauthorization action. To allow time for the client to access this webpage, the network may allow some time before the client is deauthenticated from the network. However, typically, if the Deauthentication Imminent Notice is used immediately upon connection, the network cannot or does not intend to allow any access to network resources to reach such a webpage, and no such URL will be provided. In that case, there is no reason for any time before the client is deauthenticated. In fact, it is highly desirable for the network to deauthenticate the client immediately to protect any unauthorized accesses, or to preserve already near exhaustion resources.

Currently (through recent clarification) the Passpoint Specification states that the network "should" deauthenticate the client immediately in these scenarios. It will better serve both the network and the clients if each has clarity that the network will ("shall") do the Deauthentication immediately.

3.3.3 IoT Devices on Passpoint Networks

A Passpoint network has various features and functions that could be beneficial and advantageous to IoT devices. As Passpoint networks become more popular and prevalent, it would be beneficial for the Wi-Fi Alliance and its member companies to make enhancements to the Passpoint program and standard to better accommodate IoT devices.

Passpoint enables new IoT use cases for devices without display and/or input interfaces. For example, enterprise IoT, industrial IoT, healthcare IoT.

IoT devices can benefit from the following features and functions provided by the Passpoint standard and networks:

- WPA3 Enterprise Security mode
- Support for different EAP-Types: EAP-SIM, EAP-AKA, EAP-TLS, and EAP-TTLS, etc.
- Agnostic of Wi-Fi SSIDs/Network Names, Domain Names, NAI Realms, and RCOIs
- Automatic and Seamless connection without user intervention (for example, headless IoT devices)
- Seamless roaming between access networks for IoT devices

In order to better support IoT devices on Passpoint networks, one requirement that arises is better provisioning and onboarding. Wi-Fi Alliance over the years has created provisioning and onboarding technologies that could be re-used and leveraged for IoT devices.

There are other opportunities and innovations that could also be developed by the Passpoint program to better serve these devices without a display and/or input interfaces in Enterprise and Industrial environments.

The following paragraphs illustrate some use cases for consideration.

3.3.3.1 IoT Devices in Carpeted Enterprise

There are several IoT devices that exist in a “carpeted enterprise” deployment. If a given “carpeted enterprise” environment has deployed a Passpoint network, then it would be useful to have Enterprise IoT devices seamless and securely connect to a Passpoint network and roam within that network.

Enterprise sensors, cameras, lighting systems, curtains/blinds, HVACs, printers/scanners, etc. could be provisioned to seamlessly and automatically connect to an Enterprise Passpoint network, for example, using an ANQP Domain Name and EAP-TLS.

3.3.3.2 IoT Devices in Industrial Warehouse

An industrial warehouse or environment could also benefit from the features and functions offered by the Passpoint standard. Industrial IoT devices could be provisioned and configured by a warehouse IT department to automatically and securely connect to the Passpoint network using Domain Name, NAI Realm, and/or RCOI. Different IoT devices in the industrial warehouse could be provisioned with different ANQP parameters for inventory and management purposes. In addition, different EAP types supported by the Passpoint standard could be leveraged for the various Industrial IoT devices in a warehouse environment. If the Industrial IoT device is mobile, then it would roam within the provisioned Passpoint network.

Some examples of Industrial IoT devices that could benefit from the Passpoint technology are motion sensors, cameras, lighting systems, temperature control/monitoring systems, inventory tracking devices, autonomous robots, etc.

3.3.3.3 IoT Devices that roam across healthcare settings

A healthcare based IoT device can be deployed in a nursing home (or private home) setting, using the Wi-Fi network locally available in that environment. This IoT device could be streaming telemetry to healthcare systems, across the Internet. If the patient encounters increasing difficulties, they could be transported to a nearby hospital. In this case, the IoT telemetry is still needed and the same device (already attached to the patient) could be used upon arrival at the hospital, if the device can use Passpoint to “roam” to the partner Wi-Fi network, similarly to how mobile phones and laptops can use Passpoint for roaming. This scenario needs the IoT device to have a similar “network agnostic” profile/configuration, like that currently available to UI-based devices like mobile phones and laptops.

3.4 Competing and Substitute Technologies

Due to the lack of market adoption of OSU, many current hotspot networks still use a captive portal for access. This results in an "open" network connection and resulting security vulnerabilities for both the client devices and potentially for the network. Also because of the lack of onboarding solutions, Passpoint networks are currently being used primarily by devices that are pre-provisioned, such as through use of a SIM credential, and this is limiting the broad adoption of Passpoint's promise of secure access to Wi-Fi networks.

The WBA program for "Federated Onboarding Service" is also trying to solve the onboarding problem, specifically for OpenRoaming networks, but that includes the underlying Passpoint support. However, their solution (so far) has limitations/simplifications, to help speed time-to-market. A general solution is still needed that supports use outside of OpenRoaming, supports settled (paid) access, and has clear/verifiable security around the onboarding process.

3.5 Dependencies & Risks

There are no dependencies on other in-flight programs, and no special risks are anticipated.

3.5.1 Internal Dependencies

The use of the Wi-Fi Easy Connect, Wi-Fi Aware USD or equivalent methodology for provisioning Passpoint credentials to a client device will create a dependency between this Passpoint program and activities in the Wi-Fi Easy Connect, Wi-Fi Aware TGs or equivalent entities, respectively, to add Passpoint support.

An internal dependency on Passpoint is the Vantage designation. It is anticipated that these improvements will expand Passpoint adoption, and the Vantage program is likely to benefit.

3.5.2 External Dependencies

There are no known dependencies on any external technology, and no special risks are anticipated.

3.5.3 Ecosystem Dependencies (Only for non-MAC/PHY Programs)

The benefits to be gained by this program will be enjoyed only by those devices or hotspots which choose to implement and deploy the features. In many cases, this includes enhancements to client "network selection" menus and operation, generally built into the OS.

3.5.4 Wi-Fi Alliance Portfolio Alignment

This program introduces enhancements to the Passpoint program, which remains within its current scope within the Wi-Fi Alliance portfolio.

The updates in this program include leveraging Wi-Fi Easy Connect, Wi-Fi Aware USD or an equivalent, for Passpoint onboarding. This is not really an "overlap", but a valuable leveraging of Wi-Fi Easy Connect, Wi-Fi Aware USD or equivalent features (some of which will be Passpoint-specific) within the Passpoint technology.

As this program enhances Passpoint deployments, it might be considered in a future Vantage designation update.

3.5.5 Regulatory Considerations

No regulatory impacts are anticipated.

3.6 Naming Recommendation

The Passpoint Marketing Task Group recommends that this program be marketed under the existing hero brand of Wi-Fi CERTIFIED Passpoint.

4 New Program Development Readiness Results

N/A

5 Scope of Interoperability Certification

This program scope includes STAs and infrastructure APs.

This program is expected to be tested in 2.4 and 5 GHz bands. Whether testing is needed in 6 GHz or HaLow is TBD.

6 Requirements

6.1 Prerequisites

DUTs submitted for certification for this program shall have the Wi-Fi CERTIFIED Passpoint certification, and its pre-requisite requirements.

6.2 Out-of-the-Box Requirements

N/A

6.3 Mandatory Features

6.3.1 Standard subscription format

The relevant use cases are listed in section 3.3.1.

A standardized format for the needed information about a subscription will be defined in the Passpoint Specification, which includes necessary credential(s) information and metadata, covering both username/password and certificate-based authentication scenarios.

The APUT shall demonstrate that this subscription format can be delivered to clients using one or more standard methods (such as HTTPS, Wi-Fi Easy Connect, Wi-Fi Aware USD or an equivalent protocols).

The (non-headless) STAUT shall demonstrate that it can process this subscription format using one or more of the same standard method(s) for provisioning the communicated subscription such that it will be used to select and authenticate to a Passpoint network in the future.

The Passpoint TGs will collaborate on identification of the standard methods for subscription provisioning, to determine a common interoperable method required for APUTs and STAUTs, for a given device type (headless/non-headless).

6.3.2 Deauthentication imminent

The relevant use case is described in section 3.3.2.

APUT, when it receives an Access-Accept from the AAA Server that includes a HS2.0 Deauthentication Request with no URL included, shall complete EAP authentication and then immediately deauthenticate the mobile device.

6.4 Optional Features

For headless STAUTs a non-UI based user interaction model method (for example, an extension to the Wi-Fi Easy Connect configuration exchange, messages defined for Wi-Fi Aware USD, or an equivalent as determined by the TTG) will be defined. A headless STAUT shall be tested if this method is implemented, to use this defined method(s) to provision a subscription such that it will be used to select and authenticate to a Passpoint network when at the Passpoint venue.

6.5 Conditional Mandatory

None.

6.6 Legacy Interoperability

Devices certified for this program shall maintain interoperability with all previously certified Wi-Fi CERTIFIED a/g/n/ac/Wi-Fi 6 and Wi-Fi CERTIFIED Passpoint devices.

Appendix A Document Revision History

Table 3. Document Revision History

Version	Date dd/mm/yy	Remarks
0.0.1	24/02/23	Initial draft with “Passpoint FR2024 MRD - StandardProvisioningFormat OSUAnywhere - v0.0.0.docx” and “Passpoint FR2024 MRD - Use Case Deauth Imminent v2.docx”
0.0.2	18/04/23	Merged in “Passpoint FR2024 MRD v0.0.1-mah-general-r3.docx” and “Passpoint FR2024 MRD v0.0.1-Provisioning use case revisions post OSU discontinuation.docx”
0.0.3	21/04/23	Merged in “Passpoint-FR2024-MRD-IoTUseCases r2.docx” together with some editorial corrections.
0.0.4	28/04/23	Editorial updates and corrections made on the April 27th 2023 teleconference.
0.0.5	04/05/23	Additional clarification in Requirements section, per May 4th 2023 teleconference.
1.0	06/05/23	Board approved