htng

MOVING HOSPITALITY FORWARD

MAC ADDRESS RANDOMIZATION IMPACT ON HOSPITALITY

1 February 2021

Version 1.00

About HTNG

Hospitality Technology Next Generation (HTNG) is a non-profit association with a mission to foster, through collaboration and partnership, the development of next-generation systems and solutions that will enable hoteliers and their technology vendors to do business globally in the 21st century. HTNG is recognized as the leading voice of the global hotel community, articulating the technology requirements of hotel companies of all sizes to the vendor community. HTNG facilitate the development of technology models for hospitality that will foster innovation, improve the guest experience, increase the effectiveness and efficiency of hotels, and create a healthy ecosystem of technology suppliers.

Copyright 2021, Hospitality Technology Next Generation

All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owner.

For any software code contained within this specification, permission is hereby granted, free-of-charge, to any person obtaining a copy of this specification (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the above copyright notice and this permission notice being included in all copies or substantial portions of the Software.

Manufacturers and software providers shall not claim compliance with portions of the requirements of any HTNG specification or standard, and shall not use the HTNG name or the name of the specification or standard in any statements about their respective product(s) unless the product(s) is (are) certified as compliant to the specification or standard.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES, OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF, OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Permission is granted for implementers to use the names, labels, etc. contained within the specification. The intent of publication of the specification is to encourage implementations of the specification.

This specification has not been verified for avoidance of possible third-party proprietary rights. In implementing this specification, usual procedures to ensure the respect of possible third-party intellectual property rights should be followed. Visit http://htng.org/ip-claims to view third-party claims that have been disclosed to HTNG. HTNG offers no opinion as to whether claims listed on this site may apply to portions of this specification.

The names Hospitality Technology Next Generation and HTNG, and logos depicting these names, are trademarks of Hospitality Technology Next Generation. Permission is granted for implementers to use the aforementioned names in technical documentation for the purpose of acknowledging the copyright and including the notice required above. All other use of the aforementioned names and logos requires the permission of Hospitality Technology Next Generation, either in written form or as explicitly permitted for the organization’s members through the current terms and conditions of membership.

TABLE OF CONTENTS

1 Introduction

1.1 What is MAC Address Randomization and Why is it Used?

MAC address randomization is the increasing trend of device operating systems using a random, anonymous device identifier instead of the real address when connecting to wireless networks. The goal of using randomization is to increase user privacy by preventing anyone from being able track devices using the real address as a consistent identifier.

1.2 What is a MAC Address?

Let's back up a little bit. The MAC address (short for media access control address) is the worldwide unique hardware address of a single network adapter. The physical address is used to identify a device in computer networks. Since MAC addresses are assigned directly by the hardware manufacturer, they are also referred to as hardware addresses. MAC addresses are written as six sets of hexadecimal expressions. Some devices have more than one MAC address; for example, a notebook will have separate MAC addresses for wired ethernet and Wi-Fi interfaces. In short, think of a VIN number for your ethernet ports.

1.3 How are MAC Addresses Used for Wi-Fi Networks Today?

The assumption and practice of having a static MAC address results in many networks leveraging it for a variety of purposes. There are well-known hospitality brands that have implemented automatic authentication programs for loyalty customers based on storing and recognizing a device's static MAC address. In the hospitality and multifamily markets, the use of a static MAC address is far reaching in current network architectures. The notion of a dynamic MAC address changing through time by virtue of a device's operating system will significantly alter the connectivity experience unless solutions that plan and address this are adopted.

For many years now, most operating systems (iOS 8+, Android 8+, Windows 10, etc.) have implemented some form of MAC randomization. However, most of these operating systems only use a randomized MAC address when scanning for access points and SSIDs (known as probe requests), but still have used a consistent, genuine MAC address when actually connecting to networks. This has successfully mitigated some forms of tracking (for example, footfall tracking in retail stores), but more advanced tracking methods have surfaced since these changes were introduced. In late 2019, Google released Android 10 which made MAC randomization the default behavior when both scanning for wireless networks and connecting to them. This was a major change that was intended to prevent tracking across networks.

Historically, MAC addresses have been a reliable identifier. However, as we learn more about privacy and security, we now know that spoofing other people's MAC addresses has been a serious network vulnerability on visitor-based Wi-Fi for some time. These changes by handset manufacturers are going to force everyone to fix this, which is ultimately a really good thing for everyone.

1.4 Impact Notes

- Maintaining a MAC address database will consume more compute resources (for example, running out of space in an ARP table)
- Maintaining larger DHCP pools will complicate networks
- Troubleshooting random MAC addresses in a network will be troublesome

- A MAC address tied to a user may be PII in some jurisdictions, which may be subject to additional requirements
- Some countries require additional step-up authentications with text messages, adding more costs for each authentication

.

2 Hospitality Use Cases

2.1 Use Case #1 – Multi-location Hotel Brand Provides Guests Internet Access Across Locations

A multi-location hotel brand wants to provide guests with instant and seamless Internet connectivity at any of their participating locations after the guest signs up for Internet service at one location. A guest who is staying at a hotel for more than 24 hours signs on to the hotel Wi-Fi network and elects to use the Internet for multiple days until checkout so they can have continuous Internet connectivity without having to go through the same process every day.

Alternate Scenarios:

- The guest may have elected a paid premium package or a free tier for Internet services.
- The device used may be a laptop or mobile device in possession of the guest

2.2 Use Case #2 – Guest Roam Between Hotel SSIDs

A hotel has previously provided guests with the ability to roam from a “Guest” SSID in the guest bedroom area to a “Public” SSID in the public areas, or conference areas.

Alternate Scenario:

- A conference attendee might be moving from the “Conference” SSID to the “Guest” SSID.

2.3 Use Case #3 – Guest Cast Personal Video Content to Hotel Room TV

A guest who is staying at a hotel for more than 24 hours signs on to the hotel Wi-Fi network and elects to use the Internet for multiple days until checkout so they can have continuous Internet connectivity without having to go through the same process every day. This guest wants to cast video content from a device to the hotel television.

Alternate Scenarios:

- The guest may have elected a paid premium package or a free tier for Internet services.
- The device used may be a laptop or mobile device in possession of the guest.

2.4 Use Case #4 – A Guest Selects a Multi-day Internet Package

A guest who is staying at a hotel for more than 24 hours signs on to the hotel Wi-Fi network and elects to use the Internet for multiple days until checkout so they can have continuous Internet connectivity without having to go through the same process every day.

2.5 Use Case #5 – Staff Connect Provided Mobile Devices to Wi-Fi (single hotel)

Hotel staff member connects to Back of House SSID. Hotel operations need to be aware in advance to configure Mobile Device Management so it ensures that the MAC address does not randomize for that particular SSID.

2.6 Use Case #6 – Multi-property Staff Connect Provided Mobile Devices to Wi-Fi (where BoH SSID differs between hotels)

Hotel staff member connects to multiple Back of House SSIDs. Hotel operations need to be aware in advance to configure Mobile Device Management so it ensures that the MAC address does not randomize for the range of potential SSIDs.

2.7 Use Case #7 – Hotel Operators Connect Hotel Headless (e.g. IoT) Devices to Wi-Fi Network

Guest attempts to connect headless device to Wi-Fi network. As most of these devices do not have a browser to accept terms and conditions and authenticate appropriately, this is usually done by whitelisting the MAC address.

2.8 Use Case #8 – Hotel Management Provides Device Identifiers and Activity to Authorities Upon Request

Government authorities may ask for information on sites visited by a particular user. The request could be for sites visited by a particular MAC address or for sites visited by a named guest. In some countries, the proposed user also has to verify their identity before accessing the Internet.

2.9 Use Case #9 – A Guest Wants to be Recognized by the Corporate Brand that Operates a Venue

Many hoteliers recognize and reward loyal guests. Some guests appreciate this and will want to ensure it continues to happen despite the MAC randomization from many operating systems.

Use Case	Description	Impacted by randomization by SSID	Impacted by randomization over time
1) Multi-location Hotel Brand Provides Guests Internet Access Across Locations	Inter-hotel roaming guest	Yes, if SSID varies	Not specifically
2) Guest Roam Between Hotel SSIDs	Intra-hotel	Yes, if SSID varies	Not specifically
3) Guest Cast Personal Video Content to Hotel Room TV	Guest casts personal content	Depends on casting solution	Not specifically
4) A Guest Selects a Multi-day Internet Package	Guest multi-day purchase	No	Yes
5) Staff Connect Provided Mobile Devices to Wi-Fi (single hotel)	Staff connect mobile device	Should be OK with MDM	Depends on authentication method
6) Multi-property Staff Connect Provided Mobile Devices to Wi-Fi (where BoH SSID differs between hotels)	Multi-property staff connect mobile device	Depends on authentication method and whether SSID varies. MDM could mitigate but might	Depends on authentication method
7) Hotel Operators Connect Hotel Headless (e.g. IoT) Devices to Wi-Fi Network	Connect headless device	Yes in theory, but OS is not yet pushing randomization	Yes in theory, but OS is not yet pushing randomization
8) Low Priority – Hotel Management Provides Device Identifiers and Activity to Authorities Upon Request	Request from authorities	Yes, if guest is new visitor	Yes, in most situations
9) Low Priority – A Guest Wants to be Recognized by the Corporate Brand that Operates a Venue	Guest wants to be recognized	Yes, unless guest takes action	Depends on authentication method

Scenario	Utilization of MAC address	Impact	Mitigation	Alternatives
Inter-hotel roaming guest	MAC address is used by centralized system to recognize a guest Recognition can be used to provide access or simply a welcome	If the hotel chain has different SSIDs in different hotels, the MAC address will only be recognized where the guest has utilized that SSID before (and the OS doesn't randomize MAC for known networks) OR If MAC randomizations by day is operable then the guest will have to re-authenticate on the second day	Guest could disable MAC randomization for this network/these networks	Use Hotspot 2.0/Passpoint certificates for laptops or SIM authentication for mobile phones to identify guests
Intra-hotel roaming guest	MAC address is used by authentication system to identify a guest and enable access across different SSIDs within the hotel (e.g. conference area to guest area, guest area to lobby area, etc.)	The guest would need to re-authenticate when moving between different areas of the hotel	Guest could disable MAC randomization for this network/these networks	Utilize same SSID in all areas of the hotel Use Hotspot 2.0/Passpoint certificates for laptops or SIM authentication for mobile phones to identify guests
Guest casts personal content	MAC address is often used to establish a relationship between the device casting and the screen to which it is casting	The guest would need to reauthenticate to Wi-Fi and re-pair for each change in MAC address	Guest could disable MAC randomization for this network	Use Hotspot 2.0/Passpoint certificates for laptops to identify guests
Guest multi-day purchase	MAC address is used to identify the purchaser and confirm they are entitled to access on subsequent days	MAC randomization by day would result in the device not being recognized on day two and the guest having to re-authenticate It would not result in an additional charge unless the guest paid by credit card	Guest could disable MAC randomization for this network	Use Hotspot 2.0/Passpoint certificates for laptops or SIM authentication for mobile phones to identify guests

Scenario	Utilization of MAC address	Impact	Mitigation	Alternatives
Staff connect mobile device	MAC address can be used to confirm identity of the staff member and ensure they are given appropriate access	Randomization by SSID could mean the device was no longer recognized (unless the OS doesn't randomize known networks) Randomization by day would mean that the staff device was no longer recognized	Corporate MDM could block MAC randomization for these networks or install profiles for Passpoint 2.0	Use 802.1x on host name
Multi-property staff connect mobile device	MAC address can be used to confirm identity of the staff member and ensure they are given appropriate access	Randomization by day would mean that the staff device was no longer recognized. Different Back of House (BoH) SSIDs by hotel would mean that the device was no longer recognized	Corporate MDM could block MAC randomization for these networks or install profiles for Passpoint 2.0	Use 802.1x on host name
Connect headless device	Headless devices are usually added based on MAC address alone	If the MAC address changes then it would not be possible to connect the headless device without knowing the random MAC to which it had changed	OS for most headless devices is not likely to randomize	Use WPA2-Enterprise 802.1x authentication
Request from authorities	When they choose to, authorities usually request information based on MAC address	Hotel and service provider could provide data on a given MAC address but neither they nor the authorities would be able to link it to an identified guest	Other identifying factors could be utilized to identify a guest	In those countries where authorities require identity verification, guests could verify identity every time MAC address changes OR verify identity using SIM authentication for mobile phones to identify guests or previously verified Hotspot 2.0/Passpoint certificates for laptops (may require enhanced identity verification process for profile installation)

Scenario	Utilization of MAC address	Impact	Mitigation	Alternatives
Guest wants to be recognized	Currently most hotels use MAC address to recognize a guest's device	If the hotel chain has different SSIDs in different hotels, the MAC address will only be recognized where the guest has utilized that SSID before (and the OS doesn't randomize MAC for known networks) OR If MAC randomization by day is operable then the guest will not be recognized	Guests could disable MAC randomization for this network/these networks 1	Use Hotspot 2.0/Passpoint certificates for laptops or SIM authentication for mobile phones to identify guests

3 Selected Solutions

3.1 Do Nothing – Rely on Captive Portal for Authentication

3.1.1 Details

- Guests see a captive portal upon connecting to a network, usually in a Captive Network Assistant browser that offers limited capabilities for cookies and other similar data.

3.1.2 Dependencies

- This requires captive portal experience to be set up (e.g., for a guest to accept terms of use, enter last name/room number, access code, etc.

3.1.3 User Experience

- The guest is presented with a captive portal experience and they must take action (e.g., accept terms of use, enter last name/room number, access code, etc.).

3.1.4 Identity/Credential Types

- Click-and-go approach to agree to terms of use, last name/room number, access code, etc.

3.1.5 Complexity for Implementation/Infrastructure

- This requires an initial software setup to establish captive portal experience.
- Depending on the complexity of experience, this may require ongoing support.

3.1.6 Effort/Costs (not specific costs)

- The cost to maintain existing MAC authentication solution with reduced guest impact and reduced guest satisfaction.

3.1.7 Benefits

- There is no effort required and existing solutions will be left in place.

3.1.8 Drawbacks

- This only works with individual browsers; multiple cookies are needed for different browsers and cookies do not persist through captive portal assistants.
- The captive portal must be revisited any time a MAC address is rotated.
- It is difficult to identify returning devices.

3.1.9 Use Case Support

1	**Multi-location Hotel Brand Provides Guests Internet Access Across Locations**	Yes, but only for 1 day
2	**Guest Roam Between Hotel SSIDs**	Yes, but only for 1 day
3	**Guest Cast Personal Video Content to Hotel Room TV**	Yes, but only for 1 day
4	**A Guest Selects a Multi-day Internet Package**	Yes, but only for 1 day
5	**Staff Connect Provided Mobile Devices to Wi-Fi (single hotel)**	Yes, but only for 1 day
6	**Multi-property Staff Connect Provided Mobile Devices to Wi-Fi (where BoH SSID differs between hotels)**	Yes, but only for 1 day
7	**Hotel Operators Connect Hotel Headless (e.g. IoT) Devices to Wi-Fi Network**	Yes, but only for 1 day
8	**Low Priority – Hotel Management Provides Device Identifiers and Activity to Authorities Upon Request**	Yes, but only for 1 day
9	**Low Priority – A Guest Wants to be Recognized by the Corporate Brand that Operates a Venue**	Yes, but only for 1 day

3.2 Turn Off All Authentication to Your Network

3.2.1 Details

- Open SSID, with no authentication or captive portal.

3.2.2 Dependencies

- None

3.2.3 User Experience

- The user must manually associate with the SSID.

3.2.4 Identity/Credential Types

- None

3.2.5 Complexity for Implementation/Infrastructure

- Low complexity

3.2.6 Effort/Costs (not specific costs)

- Minimal

3.2.7 Benefits

- Likely works on all devices
- Least friction for user
- Lowest level of effort to configure

3.2.8 Drawbacks

- There is a lack of security; the network is open to anyone and wireless traffic is not encrypted.
- There is no way for a user to verify the validity of the network.
- OS warnings are sent to users when connecting.
- This reduces the ability to track and manage traffic by users.
- There is no opportunity for guest engagement.
- Bandwidth management will become more difficult.
- There's a possibility of increased liability for hotels.
- This is not legal in some countries.

3.2.9 Use Cases

1	**Multi-location Hotel Brand Provides Guests Internet Access Across Locations**	Yes
2	**Guest Roam Between Hotel SSIDs**	Yes
3	**Guest Cast Personal Video Content to Hotel Room TV**	It depends on the solution type (some won't work, some will work for 1 day)
4	**A Guest Selects a Multi-day Internet Package**	Yes
5	**Staff Connect Provided Mobile Devices to Wi-Fi (single hotel)**	No
6	**Multi-property Staff Connect Provided Mobile Devices to Wi-Fi (where BoH SSID differs between hotels)**	No
7	**Hotel Operators Connect Hotel Headless (e.g. IoT) Devices to Wi-Fi Network**	Yes
8	**Low Priority – Hotel Management Provides Device Identifiers and Activity to Authorities Upon Request**	Yes, but much more complicated and unreliable
9	**Low Priority – A Guest Wants to be Recognized by the Corporate Brand that Operates a Venue**	No

3.3 Passpoint: Internal Identity or Third Party Owned Identity and Shared with Hospitality Company

3.3.1 Details

- A brand provides identity via a Passpoint profile distributed to guests, loyalty members, staff, vendors, meeting attendees, etc.

3.3.2 Dependencies

- This may require access to a brand identity/loyalty/PMS system.
- User devices must support Passpoint.

- Network hardware must support it, which requires modern enterprise hardware.
- Capabilities depend on the version of Passpoint that is supported (r1, r2, r3).
- FastRoaming/802.11r/Fast BSS Transition should be enabled for the best experience.

3.3.3 User Experience

- The user must install an initial Passpoint profile onto their devices through either a pre-visit web portal, mobile app, captive portal, QR code, OSEN+OSU, or email.
- Once installed, the user's device will detect and connect to the network automatically.
- The user will need to periodically update their profile.
- Guests may need to renew terms of use depending on the program or the geography it is being used in.

3.3.4 Identity/Credential Types

- Username/Password or Certificate-based Passpoint profile (EAP-TTLS, EAP-TLS)
- Can be tied to brand loyalty/identity system or can be a standalone database
- Profiles can be unique to the user identity and roles and can determine network access entitlements

3.3.5 Complexity for Implementation/Infrastructure

- Likely requires a vendor to support the infrastructure
- Need to ensure entitlements are updated as user profiles change (e.g., leaving program, changing status, leaving employment, etc.)
- Requires IT or network operators to be trained in configuring and supporting a Passpoint network configuration

3.3.6 Effort/Costs (not specific costs)

- Requires re-configuring every network
- Initial setup and configuration of program
- Ongoing support and delivery of the program

3.3.7 Benefits

- Enables outbound roaming agreements
- A likely reduction in the number of support calls due to reduced friction to connect
- Improved Wi-Fi Performance/Efficiency
- Encrypted Wi-Fi connection improves security
- Opportunity to identify and engage with guest upon arrival to property or specific area of the property
- Enables bundling Wi-Fi in corporate sales opportunities
- Improved guest experience with r3
- Gives users the ability to trust the network once provisioned
- Improves battery life of mobile device
- Better confidence in the identity of the user

3.3.8 Drawbacks

- Installing a Passpoint profile can seem risky to a user and requires multiple steps.
- This causes added infrastructure and cost.
- This requires ongoing maintenance and support.
- This also requires compatible network hardware and user devices.

3.3.9 Use Cases

1	**Multi-location Hotel Brand Provides Guests Internet Access Across Locations**	Yes
2	**Guest Roam Between Hotel SSIDs**	Yes
3	**Guest Cast Personal Video Content to Hotel Room TV**	Yes
4	**A Guest Selects a Multi-day Internet Package**	Yes
5	**Staff Connect Provided Mobile Devices to Wi-Fi (single hotel)**	Yes
6	**Multi-property Staff Connect Provided Mobile Devices to Wi-Fi (where BoH SSID differs between hotels)**	Yes
7	**Hotel Operators Connect Hotel Headless (e.g. IoT) Devices to Wi-Fi Network**	Depends on device support (not many do)
8	**Low Priority – Hotel Management Provides Device Identifiers and Activity to Authorities Upon Request**	Yes
9	**Low Priority – A Guest Wants to be Recognized by the Corporate Brand that Operates a Venue**	Yes

3.4 Passpoint: External Identity (Not Shared by Third Party)

3.4.1 Details

- A third-party partner (MNOs, Loyalty, Affiliate, etc.) provides identity via Passpoint profile and the brand allows access to these users onto their network.

3.4.2 Dependencies

- User devices must support Passpoint.
- Network hardware must support it, which requires modern enterprise hardware.
- FastRoaming/802.11r/Fast BSS Transition should be enabled for best experience.

3.4.3 User Experience

- Devices with SIM cards from certain carriers or profiles from roaming partners will automatically connect to the Wi-Fi.

3.4.4 Identity/Credential Types

- EAP-TTLS, EAP-TLS, EAP-SIM

3.4.5 Complexity for Implementation/Infrastructure

- Likely requires a vendor to support the infrastructure
- Requires IT or network operators to be trained in configuring and supporting a Passpoint network configuration

3.4.6 Effort/Costs (not specific costs)

- Requires re-configurating every network
- Ongoing support and delivery of the program.

3.4.7 Benefits

- Could generate revenue for the property
- Allows for co-marketing with loyalty partners
- Can provide different experiences based on external partnerships
- Encrypted wireless connection

3.4.8 Drawbacks

- A brand must share ownership of the guest relationship with the external identity provider.

3.4.9 Use Cases

1	**Multi-location Hotel Brand Provides Guests Internet Access Across Locations**	Part
2	**Guest Roam Between Hotel SSIDs**	Part
3	**Guest Cast Personal Video Content to Hotel Room TV**	No
4	**A Guest Selects a Multi-day Internet Package**	No
5	**Staff Connect Provided Mobile Devices to Wi-Fi (single hotel)**	No
6	**Multi-property Staff Connect Provided Mobile Devices to Wi-Fi (where BoH SSID differs between hotels)**	No
7	**Hotel Operators Connect Hotel Headless (e.g. IoT) Devices to Wi-Fi Network**	No
8	**Low Priority – Hotel Management Provides Device Identifiers and Activity to Authorities Upon Request**	It depends on business terms between hotel and authentication provider
9	**Low Priority – A Guest Wants to be Recognized by the Corporate Brand that Operates a Venue**	No

3.5 Instruct Guests or Staff to Turn Off Private Addressing (or manage corporate devices to do that by default)

3.5.1 Details

- Automated or manual approach to manage messaging to guest and staff

3.5.2 Dependencies

- Guests act upon hotel requests
- Hotel group MDM ensures the private address is switched off for relevant SSIDs

3.5.3 User Experience

- Guests will manually disable Private MAC Address option and will be presented with a security warning.
- Staff may need to manually disable, or they may not have to do anything if MDM is in place.

3.5.4 Identity/Credential Types

- MAC Address

3.5.5 Complexity for Implementation/Infrastructure

- Assume already implemented

3.5.6 Effort/Costs (not specific costs)

- May need to update captive portal to include messaging to guests to disable Private Address feature
- Education for guests and support staff
- Possible for additional support calls from users who do not disable

3.5.7 Benefits

- Existing solutions continue to work

3.5.8 Drawbacks

- There is a lack of security; the network is open to anyone and wireless traffic is not encrypted.
- OS warnings are sent to users when connecting.
- There is a possibility of increased liability for hotels.
- There is bad publicity for those that implement this.
- NOT RECOMMENDED

3.5.9 Use Cases

1	**Multi-location Hotel Brand Provides Guests Internet Access Across Locations**	Yes
2	**Guest Roam Between Hotel SSIDs**	Yes
3	**Guest Cast Personal Video Content to Hotel Room TV**	Yes
4	**A Guest Selects a Multi-day Internet Package**	Yes
5	**Staff Connect Provided Mobile Devices to Wi-Fi (single hotel)**	Yes
6	**Multi-property Staff Connect Provided Mobile Devices to Wi-Fi (where BoH SSID differs between hotels)**	Yes
7	**Hotel Operators Connect Hotel Headless (e.g. IoT) Devices to Wi-Fi Network**	Yes
8	**Low Priority – Hotel Management Provides Device Identifiers and Activity to Authorities Upon Request**	Yes
9	**Low Priority – A Guest Wants to be Recognized by the Corporate Brand that Operates a Venue**	Yes

3.6 Capport/Wispr – Application Layer APIs for Network Access

3.6.1 Details

- A mobile device application determines the availability of networks and connects behind the scenes using APIs.

3.6.2 Dependencies

- Application to broker connections occur through a captive portal network. The user may need to log-in to the app to identify themselves.
- Mobile devices must support the standard. DHCP servers must support options.

3.6.3 User Experience

- The guest may have to launch the mobile app and log-in, but will not need to interact with the captive ports.

3.6.4 Identity/Credential Types

- This is determined by a mobile app and could be surrounding loyalty information, room information, roaming credential, etc.

3.6.5 Complexity for Implementation/Infrastructure

- This requires mobile app support, portal servicer support and network configuration.

3.6.6 Effort/Costs (not specific costs)

- Development costs to enhance mobile app
- Requires re-configuring every network
- Initial setup and configuration of program
- Ongoing support and delivery of the program

3.6.7 Benefits

- This allows application-level recognition and authentication to a Wi-Fi network with a captive portal.

3.6.8 Drawbacks

- This requires the user to install a mobile app and log-in to the network to obtain identity information.
- Capport is an evolving standard. Wispr is dated and has security concerns.

3.6.9 Use Cases

1	**Multi-location Hotel Brand Provides Guests Internet Access Across Locations**	Yes
2	**Guest Roam Between Hotel SSIDs**	Yes
3	**Guest Cast Personal Video Content to Hotel Room TV**	Depends on implementation, but likely need to repair every 24 hours
4	**A Guest Selects a Multi-day Internet Package**	No
5	**Staff Connect Provided Mobile Devices to Wi-Fi (single hotel)**	No
6	**Multi-property Staff Connect Provided Mobile Devices to Wi-Fi (where BoH SSID differs between hotels)**	No
7	**Hotel Operators Connect Hotel Headless (e.g. IoT) Devices to Wi-Fi Network**	No
8	**Low Priority – Hotel Management Provides Device Identifiers and Activity to Authorities Upon Request**	Yes
9	**Low Priority – A Guest Wants to be Recognized by the Corporate Brand that Operates a Venue**	Yes

3.7 WPA2 Enterprise/802.1x Various Flavors

3.7.1 Details

- Users must enter a username and password either supplied by the hotel/brand or based on existing credentials known to the hotel (e.g., loyalty credentials).

3.7.2 Dependencies

- Application to validate credentials
- FastRoaming/802.11r/Fast BSS Transition should be enabled for best experience

3.7.3 User Experience

- The guest must have access and then enter credentials at an OS prompt prior to being able to associate with the network.
- Loyalty credentials or a set of standard credentials are supplied by the hotel/brand.

3.7.4 Identity/Credential Types

- Typically, a Username and Password is needed, but these types could be certificate-based.

3.7.5 Complexity for Implementation/Infrastructure

- Setting up validation pathway to validate user credentials
- Supporting and maintaining a large list of user credentials
- Increased dependencies on network configuration (such as 802.11r)

3.7.6 Effort/Costs (not specific costs)

- There is likely a custom solution to build or buy whether it is home-built by the hotel/brand or available to purchase as a proprietary vendor solution.

3.7.7 Benefits

- Encrypted wireless connection

3.7.8 Drawbacks

- Not all devices support WPA2-Enterprise
- Some devices behave differently than others based on implementation

3.7.9 Use Cases

1	**Multi-location Hotel Brand Provides Guests Internet Access Across Locations**	Yes
2	**Guest Roam Between Hotel SSIDs**	Yes
3	**Guest Cast Personal Video Content to Hotel Room TV**	Yes
4	**A Guest Selects a Multi-day Internet Package**	Yes
5	**Staff Connect Provided Mobile Devices to Wi-Fi (single hotel)**	Yes
6	**Multi-property Staff Connect Provided Mobile Devices to Wi-Fi (where BoH SSID differs between hotels)**	Yes
7	**Hotel Operators Connect Hotel Headless (e.g. IoT) Devices to Wi-Fi Network**	Depends on device support
8	**Low Priority – Hotel Management Provides Device Identifiers and Activity to Authorities Upon Request**	Yes
9	**Low Priority – A Guest Wants to be Recognized by the Corporate Brand that Operates a Venue**	Yes

3.8 WPA2 Personal – Unique PSK, Various Flavors; DPSK, mPSK, iPSK, ePSK

3.8.1 Details

- Standard WPA2 Personal SSID where each user gets a unique passphrase to connect and identify themselves.

3.8.2 Dependencies

- An application is needed to validate credentials.

3.8.3 User Experience

- The guest must have access and then enter credentials (that the hotel must provide) at an OS prompt prior to being able to associate with the network.
- Loyalty credentials or a set of standard credentials are supplied by the hotel/brand.

3.8.4 Identity/Credential Types

- Single unique key

3.8.5 Complexity for Implementation/Infrastructure

- Setting up validation pathway to validate user credentials
- Supporting and maintaining large list of user credentials

3.8.6 Effort/Costs (not specific costs)

- There is likely a custom solution to build or buy whether it is home-built by the hotel/brand or available to purchase as a proprietary vendor solution.

3.8.7 Benefits

- Encrypted wireless connection

3.8.8 Drawbacks

- Proprietary to the hardware and key-matching service implementation
- Compute on constraints on the number of keys supported
- Vulnerable to brute force attack

3.8.9 Use Cases

1	**Multi-location Hotel Brand Provides Guests Internet Access Across Locations**	Yes, if enabled on corresponding infrastructure (it depends)
2	**Guest Roam Between Hotel SSIDs**	Yes
3	**Guest Cast Personal Video Content to Hotel Room TV**	Yes, if on the same VLAN
4	**A Guest Selects a Multi-day Internet Package**	Yes
5	**Staff Connect Provided Mobile Devices to Wi-Fi (single hotel)**	Yes
6	**Multi-property Staff Connect Provided Mobile Devices to Wi-Fi (where BoH SSID differs between hotels)**	Yes
7	**Hotel Operators Connect Hotel Headless (e.g. IoT) Devices to Wi-Fi Network**	Yes
8	**Low Priority – Hotel Management Provides Device Identifiers and Activity to Authorities Upon Request**	Yes
9	**Low Priority – A Guest Wants to be Recognized by the Corporate Brand that Operates a Venue**	Yes