Wi-Fi Devices Identification

Confidential for IEEE 802.11 ONLY

A Way Through MAC Randomization

Source: Wireless Broadband Alliance

Author(s): WBA Wi-Fi Devices Identification

Issue date: March 2022

Version: 1.0.0

Document status: Final Draft Pre-Publishing

ABOUT THE WIRELESS BROADBAND ALLIANCE

Wireless Broadband Alliance (WBA) is the global organization that connects people with the latest Wi-Fi initiatives. Founded in 2003, the vision of the Wireless Broadband Alliance (WBA) is to drive seamless, interoperable service experiences via Wi-Fi within the global wireless ecosystem. WBA's mission is to enable collaboration between service providers, technology companies, cities, regulators and organizations to achieve that vision. WBA's membership is comprised of major operators, identity providers and leading technology companies across the Wi-Fi ecosystem with the shared vision.

WBA undertakes programs and activities to address business and technical issues, as well as opportunities, for member companies. WBA work areas include standards development, industry guidelines, trials, certification and advocacy. Its key programs include NextGen Wi-Fi, OpenRoaming, 5G, IoT, Testing & Interoperability and Policy & Regulatory Affairs, with member-led Work Groups dedicated to resolving standards and technical issues to promote end-to-end services and accelerate business opportunities.

The WBA Board includes Airties, AT&T, Boingo Wireless, Broadcom, BT, Cisco Systems, Comcast, Deutsche Telekom AG, Google, Intel and Viasat. For the complete list of current WBA members, click here.

Follow Wireless Broadband Alliance:

www.twitter.com/wballiance

http://www.facebook.com/WirelessBroadbandAlliance

https://www.linkedin.com/company/wireless-broadband-alliance

CONFIDENTIALITY

Privileged/confidential information may be contained in this document and any files attached in it ('WBA Documentation').

Only WBA member companies who have signed the new WBA IPR Policy (Located at: WBA Extranet and are the intended recipient are entitled to receive, review or comment on this WBA Documentation.

If you are not the intended recipient (or have received this WBA Documentation in error), please notify the sender and WBA (pmo@wballiance.com) immediately and delete this WBA Documentation. Any unauthorized copying, disclosure, use or distribution of this WBA Documentation is strictly forbidden.

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

The device MAC (Media Access Control) address was originally a fixed unique hardware address that uniquely identified the device on a network. As a result, Wi-Fi MAC addresses have long been used as if they were a stable invariant identifier to manage Wi-Fi networks. However, that stability started to be deprecated about 10 years ago when operating systems (OS) makers started to take small steps to anonymize, or randomize, the MAC address via firmware or software.

With Wi-Fi, the MAC address is broadcast over the air and in the clear, meaning that 3rd parties can observe it and track the behavior of individual devices. Having the MAC settable in firmware (and now software) also means that devices can be configured to masquerade as others.

Together these features introduced issues for both privacy and authenticity. To address the privacy issue, operating systems such as iOS, Android, and Windows have been progressively introducing anonymization of Wi-Fi client device MAC addresses over the last half a decade. This process started with network discovery probe requests whilst still using the true MAC address when connecting to the network and has now reached the stage of a different MAC address for each Service Set Identifier (SSID) that a device visits. It is expected, though not truly known when, that OS makers will continue to introduce additional randomization techniques over time to further enhance user privacy.

To illustrate the prevalence of MAC randomization, the data below was gathered from open SSIDs in a hospitality context in one large-scale Wi-Fi management system over a period of 15 months to March 2021, and illustrates that the randomization of MAC addresses is increasingly becoming the paradigm and an important feature in mobile devices.

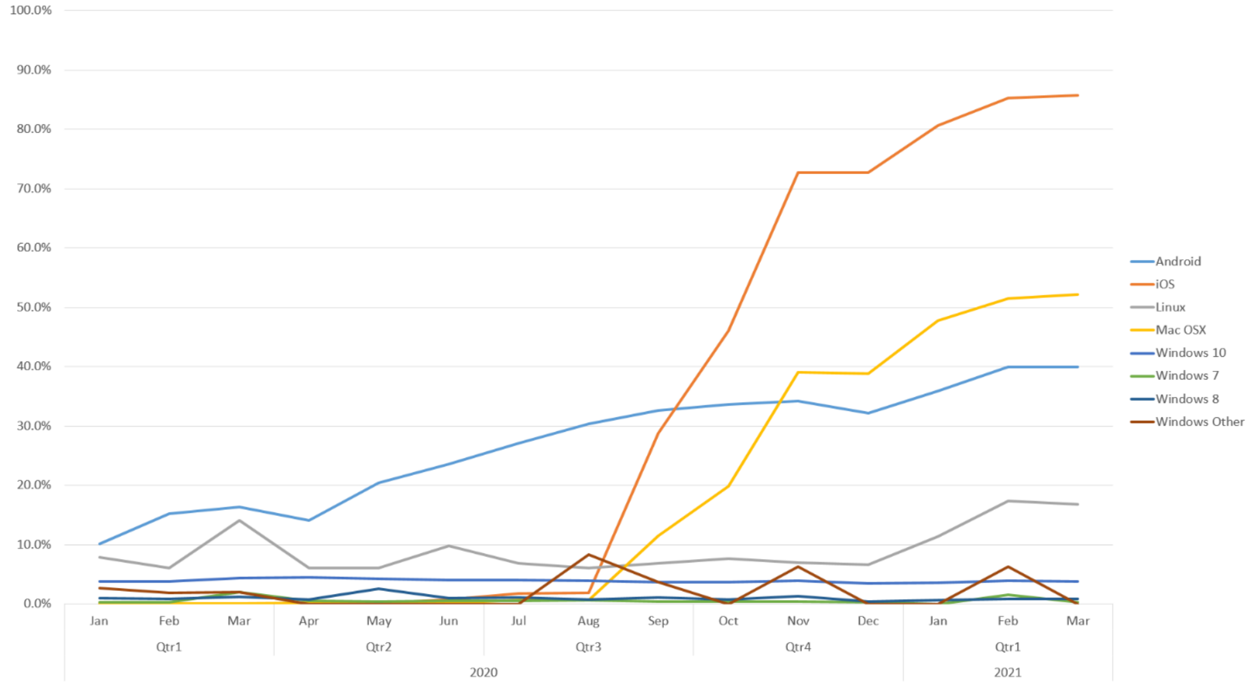


Figure 1 - Percentage of devices by OS type that are now exhibiting MAC randomization behaviour in 2020-21

Randomization has brought with it problems for network operators. MAC-based functions typically no longer work in the manner that was intended and often cause usability issues for the network user, as well as denying the operator network usage metrics and diagnostic data for connectivity issues. While these issues remain relatively minor today, more frequent randomization, such as every 24 hours, will create significant challenges for many network types and use cases.

The WBA community has been looking at the issues of MAC address anonymization for quite some time and has identified a list of potential impacts of these changes to existing systems and solutions that can be explored, instead, to overcome the dependency on MAC address. The WBA hopes this work can help towards defining a mitigation path and the necessary steps required to update the Wi-Fi network ecosystem.

Subsequently, the WBA members have also agreed on a priority set of use cases that a Wi-Fi Identification Standard should address and have performed the market requirements analysis and matching technologies able to scale and achieve longer term sustainability of deployed services.

1 Impacts of MAC randomization and the need for new solutions

This section examines the issues that a randomized or varying MAC address poses to existing networks and functionalities. What does a varying MAC address break, what functionality will be lost if there is no alternative means to identify a device?

1.1 Hospitality and venue networks

MAC usage	Access control – identify devices for guest access
Impact	When the MAC address changes, the user will have to re-authenticate. The network may accumulate a large list of permitted MAC addresses, most of which are redundant device entries. The user may have a restricted number of permitted devices to which obsolete MAC entries will count. This problem is exacerbated in multi-SSID properties, which is still common in the hospitality networking space.
MAC usage	Managing transition and roaming or any activity managing location within a network
Impact	When the private MAC address is used for probing, the device cannot be identified, which has led in some systems to private MACs being discarded as unusable information. Now that associated MACs are being randomized; they are also being discarded as unusable information. Access points cannot identify if a device has transitioned in cases were the SSID/BSSID (Basic Service Set Identifier) is different across access points.

1.2 Operators' public networks (including networks like Eduroam)

MAC usage	Blocking devices that repeatedly and rapidly retry with invalid credentials
Impact	Extra load on Authentication, Authorization, and Accounting (AAA) servers that will have to handle all frequently repeated invalid requests, potentially between continents. This behavior could be detected as 'Denial-of-Service' attacks as the MAC address changes each time.
MAC usage	In Passpoint®, record the acceptance of T&Cs by the AAA, and for 'Certificate Enrolment'
Impact	Users (devices) may appear not to have accepted the T&Cs. Devices may appear to be using a certificate that was not registered to them, OR certificates could be duplicated onto other devices to gain access.
MAC usage	'Certificate Enrolment' tied to MAC to prevent copying
Impact	Device may appear to be using a certificate that was not registered to it and be refused access / have its credentials invalidated.

MAC usage	Responding to requests for ‘Lawful Intercept’ and other law enforcement purposes The MAC is often used to identify a device as a proxy for the user
Impact	The operator will cease to be able to provide useful information to law enforcement. This is likely to lead to demands for legislative changes that would erode user privacy.
MAC usage	Network utilization and performance monitoring MAC addresses have in the past been used to provide basic statistics on the number of devices visiting a network and the number and level of repeat visits
Impact	Network visit data will no longer be available for basic statistics in this way, all devices will appear as new unique visits.

1.3 Private home network

MAC usage	Parental controls (such as restricting access times) address
Impact	Once the MAC address changes, devices will cease to be restricted or denied. Any restrictions in place will stop being applied. Children would be able to use the network at restricted times, or access restricted content.
MAC usage	Quality of Service (QoS) / Quality of Experience (QoE) management
Impact	Once the MAC address changes, devices will cease to be prioritized appropriately.
MAC usage	Internet Protocol (IP) address allocation
Impact	Identification of the device for IP allocation is MAC based, the device may continue or attempt to continue to use an IP lease that it appears not to have been given, or a new IP may be unnecessarily allocated. Table data space and address pools may be exhausted, and duplicated or rogue device detection may be triggered. In general, rogue device identification becomes more complex and less accurate.
MAC usage	Device diagnostics and performance monitoring
Impact	Diagnostic and performance monitoring data will become fragmented. The diagnostic data for a device will not extend beyond the life of the MAC, after which it will appear to be a new device. Long-term device issues will be hard to identify and correlate.
MAC usage	Registration of devices for services
Impact	Some applications or services, such as where websites are provided with network-derived information, may offer reduced sign-on functions by remembering a device. With changing MAC addresses the users would have to go through a full sign-on process every time.
MAC usage	Band steering with split-SSID installations
Impact	The device will not be identified as the same device on both SSIDs and cannot readily be steered between them. There are situations where device behavior can result in devices sticking to 2.4GHz channels where because of the high degree of contention often experienced, they would be much

	better off moving to a 5GHz or 6GHz channel. The AP will not be able to determine the identity of a device between the two (or more) bands.
MAC usage	Firewall, network access, VLAN access and guest network separation
Impact	Settings for firewalls, network access, and VLAN usage based on MAC address would no longer functions requiring constant updating.

1.4 Enterprise networks

MAC usage	Network or device diagnostics and performance monitoring
Impact	A persistent physical layer identifier is required at the physical layer to identify various types of issue such as connectivity and performance issues with individual devices.
MAC usage	Steering between networks (split SSIDs) The network may try to identify the device as it probes for SSIDs; or other behavior, to understand devices' steering responses over time
Impact	Devices cannot reliably be identified as belonging to or having been seen on a particular network.
MAC usage	Certificate Enrolment
Impact	Device may appear to be using a certificate that was not registered to it and be refused access / have its credentials invalidated.

1.5 Pay-per-Use functionality

MAC usage	Identification of complementary and paid-up users or devices
Impact	When the MAC changes, the user may have to re-enter information to regain access or may even lose the paid-for access. The user may have a restricted number of permitted devices to which obsolete MAC entries will count and will find it difficult to identify obsolete device entries in order to release them. A complimentary-access user may be able to obtain unlimited free sessions by forcing a MAC change. In some cases, billing systems will need to be changed or revenue sacrificed.
MAC usage	Network or device diagnostics, utilization, and performance monitoring
Impact	A persistent physical layer identifier is required at the physical layer to identify various types of issues such as connectivity and performance issues with individual devices.

2 Requirements for Wi-Fi identifiers

To replace the MAC Address, alternative identifiers are required. There is not necessarily a 1:1 mapping between the network type, the service, and the identifier. In some situations, the network may require different identifiers with different lifetimes for different services. Some of those identifiers may be essential to providing the service – the device cannot access the service without the identity, others may be subject to consent, or withdrawal of consent by the user – such cases could include not having to log in to every new session, or collecting device behavior over multiple sessions for problem resolution.

Bear in mind some of the features that a good identifier might exhibit when examining the requirements that various networks have for the use of an identity or identities:

- Identifies the correct entity – a user, a device, or an application / service
- Unique to the application / service
- Sufficient only for the application or provision of the service
- Only used for the application / service that it is the identifier of
- Private to the application or service
- Existing for only as long as required
- Unguessable - suitably randomized to reduce attack
- Compatible with local laws and sensibilities (as appropriate)
- Easy to deploy, especially in cases for non-technical users with unmanaged devices
- Require limited user action to authenticate and be as transparent to the user as practicable
- In all cases, the identity being used will have to be cost-effective if the service is to be provided

This next section collects use cases and describes the requirements that various networks and services have for identifiers to support those same use cases:

2.1 Use cases and requirements for an identifier

Application	Private home network access restrictions / privileges (including 'Parental Controls' and per-device or per-user QoS) Pay-per-Use networks - identification of complementary and paid-up users or devices
Identity Requirement	The network must be able to identify each specific device or user-to-device association to which/whom restrictions or privileges are applied. The identity must last for as long as the restrictions or privileges need to be applied. There should not be a way to remove the identity and still obtain service/privilege. The identity is unique to the network and user (or device). Devices not subject to restrictions or privileges do not need to be specifically identified.
Application	IP Address allocation in private, public and enterprise networks
Identity Requirement	The network must be able to identify each specific device to which an IP has been allocated for the duration of that allocation. The identity must last at least as long as the IP lease renewal period and only alter if the IP lease is not renewed, or indefinitely where it is desired to allocate a static IP. The identity is unique to the network and the device. All associated devices need to be individually identified.
Application	Private home network device diagnostics and performance monitoring Enterprise network or device diagnostics and performance monitoring
Identity Requirement	The network must be able to identify each specific device that associates to the network. The identity will ideally last indefinitely for private users but may be time-limited for guest users. The identity is unique to the network, which may consist of more than one Extended Service Set (ESS) in the case of split SSIDs, and to the device. It may be necessary to identify all devices that have associated or attempted to associate with the network in order to identify situations where they try but are unable to (associate).
Application	Private home networks and enterprise networks band steering with multi-ESS networks (e.g., split-SSID installations)
Identity Requirement	The network must be able to identify each specific device that associates to the network. The Identity may need to extend across sessions where the network consists of more than one ESS (such as the case of Split SSIDs). The identity is unique to the network and the device. Devices not using the network do not need to be identified.
Application	Hospitality and venue network access with varying service levels
Identity Requirement	The network must be able to identify each specific user or user's device to whom access is granted and apply the appropriate service level. The identity should last for the duration of the access permission. Loyalty services with a very long identity lifetime are a possibility.

	The identity is unique to a user's device and an individual network or collection of networks – the network may sometimes include multiple venues or brands. Devices or users that are not granted access do not need to be identified.
Application	Pay-per-Use network access
Identity Requirement	The network must be able to identify the user or device for which access has been paid and apply the appropriate service level. The identity should last for the duration of the paid service. Paid updates to the duration are a possibility, as are ongoing subscriptions. The identity is unique to an individual network or collection of networks – the network is likely to include multiple locations and may cover multiple brands. Devices or users that have not paid, or are not in the process of paying, for access do not need to be identified.
Application	Operators' public networks block devices that have expired or invalidated credential and rapidly and repeatedly reattempt to connect
Identity Requirement	The network should be able to identify the user or device for which access has been denied and restrict it at the access network level. The Identity should last for a pre-determined duration to protect the AAA servers and network interconnections from excess load. The identity is unique to the public network or collection of networks – the network is likely to include multiple locations and may cover multiple brands. Devices that are not being blocked are not required to be identified for this purpose.
Application	Network blocks devices due to abusive behavior or upon lawful demand
Identity Requirement	The network should be able to identify the user or device for which access has been denied and restrict it at the access network level. The identity should last indefinitely and not be subject to removal by the user. The identity is unique to the network or collection of networks – the network is likely to include multiple locations and may cover multiple brands. Devices that are not being blocked are not required to be identified for this purpose.
Application	Passpoint networks record the acceptance of T&Cs on the AAA
Identity Requirement	The network should be able to identify the user who has accepted the T&Cs for a particular network. Multiple branded networks with different T&Cs could potentially be operated by the same operator with the same credential. The identity should last for as long as the T&Cs are deemed to be valid. The identity is unique to the network or collection of networks – the network is likely to include multiple locations and may cover multiple brands. Devices do not need to be identified but users do need to be identified to reduce or eliminating having to accept T&Cs on every connection.
Application	Networks - typically using 802.1X - that use the device MAC to tie devices to certificates for Certificate Enrolment

Identity Requirement	The network should be able to identify the user or device and associate the Identity with a specific certificate. The identity is supposed to tie the user or device to the certificate and should only be available to the user or device to which it was granted. The identity should last for as long as the certificate is considered valid or is replaced. The identity is unique to the certificate, which should be tied to a network or collection of networks.
Application	Any network operator responding to requests for communications records, lawful interception, and other law enforcement purposes
Identity Requirement	The network must be able to identify each specific user to whom access is granted and associate this with one or more communications records. It must be possible to determine the user from specifically identified communications. The identity and the association must be retained for the statutory period. The identity is unique to a user and an individual network.

3 Identification and consent

3.1 What needs to be identified, when, and for how long?

Identities of some kind are required in cases where either people or specific devices need to be identified, and, in particular, when those identities are needed for longer than a single Wi-Fi session. MAC addresses have been used by default as identifiers for devices in many scenarios where user identifiers would have been more appropriate. However, there is no longer a need to use a device identity as a proxy for a user, there are solutions that provide user identities. There are cases where a basic device ID continues to be more appropriate and the ability to identify the user of the device is neither necessary nor wanted and there are solutions that can be used to identify just the device, or both the device and the user, and this can be as simple as the manner in which the credential is created and issued.

With identities that last for longer than a session, particular consideration needs to be given to the requirement for consent and the possibility of its withdrawal, and to the lifetime of the identifier / credential that is used, and these aspects are mentioned further in the following sections, and in 5.1.3.

Where the identity only lasts for a single session, or for legacy devices with unchanging MAC, MAC addresses can continue to be used along with any current identification mechanism such as a captive portal and pay-per-use. However, it should be noted that an unchanging MAC on a personal device is itself likely to be regarded as personally identifying for the purposes of data protection regulations. If the device presents a frequently changing MAC address, then it seems unlikely that such a MAC would constitute personal information by itself.

3.2 Is consent needed?

Processing and protecting data that can be personally identifiable is about maintaining the trust of users in the organizations that are handling the data. Many countries have laws controlling the processing of personal data, but even where there is no legal obligation to obtain consent, explaining why the data are needed and asking permission both help to maintain that trust and as more consumers become privacy-aware, explanation and permission will be an increasing expectation from end-users.

With legal requirements for privacy in the processing of personal data (sometimes called Personally Identifying Information - PII), anyone processing personal data should ensure that they comply with the relevant laws. The penalties for failure to comply can be significant – for the European 'General Data Protection Regulation' (GDPR) the limit is the greater of €20M or 4% of annual global turnover, and for the Malaysian 'PDPA' can include up to 3 years imprisonment. The scope of GDPR is wide, it applies to the personal data of anyone within the EU at the time (including tourists visiting Europe), and to the processing of personal data of EU residents anywhere in the world. UK law also implements the EU GDPR, and the e-Privacy directive may also apply with additional consent requirements.

There are data protection laws all around the world. For example, Malaysia, as mentioned above, has its Personal Data Protection Act 2010 (PDPA), and Singapore its PDPA 2012. The scope of both is similar to the GDPR. China has had data protection laws since 1994, and Russia since 2006. In South America, Brazil passed its General Data Protection Law in 2018 and that has recently come into effect.

In the US, the California Consumer Privacy Act (CCPA 2018) provides some similar restrictions to GDPR, but only applies to the personal data of California residents, and generally does not apply to non-profit organizations, or to small businesses (by revenue or number of data subjects). If you process the data of children under the age of 13, then the Children's Online Privacy Protection Act (COPPA 1998) will also apply, and parental consent will be required.

Typically, legal restrictions on the processing of personal data only extend as far as processing the data of identifiable persons. Within the GDPR, where data are not *capable of being* associated to a person, family, etc. then those data do not constitute personal data and the law does not apply. If the information is not available[1] to tie the device identity to an identifiable person, then consent is not needed, though it may still be advisable to ask for it in order to meet user expectations.

Whether the processing of PII requires consent will depend upon the relevant law. As an example, within GDPR there are two main justifications for processing personal data: 'Legitimate Interest', and 'Consent' of the data subject.

Legitimate Interest can be used where data is necessary for the provision of a service. However, what constitutes a legitimate interest is defined and is not as all-encompassing as you might guess, it must also be

1) necessary for the primary purpose – this would also include features such as fraud prevention and IT security,
2) fair and proportionate - data should not be processed in ways that the user would not understand or reasonably expect, nor be excessive for the purpose, and
3) not adversely affect the data subjects' rights and freedoms.

Consent is a more suitable basis for processing data that is not essential for providing the service to the user.

3.3 What is Consent?

To continue with the European example – which will apply if you process the data of European residents -, GDPR defines 'Consent' as needing to be freely given, specific, informed, and unambiguous.

[1] If the means to identify a person subsequently becomes available, consent will be needed to continue processing the data.

In practice, this means that the data subject must be told what data is being collected and what it is to be used for in quite specific terms. The information must be clear and easily understandable for the average person, and the consent must be freely and specifically given. If the user is coerced into providing consent or does not have to take any action to 'consent' - e.g., an opt-out rather than an opt-in setting - then consent will not be considered to have been freely given. Consent is given for the purposes described; the data must not subsequently be used for different purposes without further consent.

Consent can be withdrawn by the data subject at any time, and the data processor must stop processing the subject's data by consent. Consent must also be as easy to withdraw as it is to grant. It is worth noting that GDPR also specifies that data should only be retained for as long as it is needed for the purpose for which it was collected, whatever the basis being used to justify the processing. So, if you no longer have a basis for processing the personal data, and you have no legal obligation to retain it, then you need to delete it.

3.4 Mechanisms for obtaining informed consent

Still continuing with the European example, the GDPR does not define a specific method by which consent should be obtained. This is because, if consent must be obtained, the ways of obtaining this consent may be many, and may be specific to the type of information that is collected. For example, a website may track user actions, and an obvious way to collect consent is therefore to display a form when a user first connects to the website, showing which information is intended to be tracked, how collected data is used, and allowing the user to selectively accept (opt-in) or refuse (keep unchecked) each element that the website proposes to track. "Freely consented" means that the user should not be prevented from accessing the website when declining tracking, but also that the user should be able at any time to modify the consent (e.g., with a privacy menu accessible from any page of the website). This way, consent is obtained, but the user has the choice to modify this consent at any time.

Other technologies do not offer an interactive interface to the user through which consent can directly be managed. However, the controller (the entity collecting data and consent) must be able to demonstrate that consent was obtained prior to data collection. This requirement implies that consent must be obtained in a way that is explicit and trackable in time. Any mechanism that allows such conditions to be fulfilled is acceptable. The easiest and least controversial method is naturally to tie consent with data collection. For example, a shopping mall wishing to track users' location may tie the process to the mall Wi-Fi web portal, asking for consent upon connection, and recording only the position of those devices from which consent was received. When such real time interaction is not possible, the controller needs to design a mechanism to interact with the user prior to the data collection. This mechanism could be a form, e-mail, or any other way to query for the user consent.

In the case of MAC address tracking, however, a strong assumption is that there will be a device in range of a system detecting the device's 802.11 frames. These frames are usually an indication of an interaction between the device and the Wi-Fi infrastructure, and this interaction can be used to send collection consent questions to the device and the user. However, there is no current mechanism to collect such consent outside of an upper layer application (e.g., a web browser).

3.5 How is privacy protected?

Data communication technologies are not concerned with the privacy of persons, but with the privacy of data. This difference is important, because it means that these technologies do not directly address issues related to interaction between people, but address issues related to data collected about a natural person. Privacy in that context relates to data privacy, i.e., how personal data is collected and stored. Privacy is preserved by various means.

During data collection, consent has to be obtained, as described above. Data, in this context, only refers to PII, i.e., data which can be tracked back to a user. In the case of a personal device (e.g., a smartphone, tablet, or laptop), this data includes the MAC address, if it can be mapped back to the device itself, and any other identifying information (directly identifying the device or the user, i.e., PII, or which can be used indirectly to identify the user, i.e., 'Personally Correlated Information' [such as 802.11 scrambler fingerprinting or others]). When consent has not been received, data must not be collected.

In the example of location tracking, such requirement means that the Wi-Fi infrastructure may receive signals from devices whose user has not provided consent for tracking. The detail of their MAC address and radio frequency (RF) parameters is not forwarded to the location engine, or their location is not computed. The infrastructure also does not keep a record of these MAC addresses, deleting them from memory as they are compared to the approved list. This second element is also important, because it means that data privacy is only affected as it relates to PII and PCI. In this context, a parallel action to consent collection can be to anonymize the data. For example, scrambling a particular MAC address before processing or storage, or only collecting concatenated and unidentified elements (e.g., "3 MAC addresses were present in this area", without any data about which addresses these were) is also a mean to preserve privacy.

Privacy is also preserved with data storage. The consent mechanism must also describe data usage, with a physical and time boundaries, defining how data will be used, by which entity (and for which purpose). The controller must ensure that the data is not shared outside (i.e., that it is only accessible by the entity identified in the consent form), and also not kept beyond the duration for which the data is required by the usage described in the consent form. Because this second requirement has implications for security, the controller should store the data in a secured database. It is also a recommended practice to delete the data as soon as it is not directly useful anymore (in particular, to avoid that later security vulnerabilities exposes this data to third parties). Additionally, and because PCI can be obtained by cross-referencing information from multiple sources, the processing of data should be limited to the scope and perimeter defined in the consent form.

4 Examination of existing identification solutions

With the development of randomized and changing MAC address (RCM) for devices when connecting to networks there is a fear that network operators have lost, or will lose, the ability to quickly and efficiently identify devices that are connecting to and utilizing Wi-Fi networks. While this may be the case for some networks in certain scenarios, this isn't the case for all networks in all scenarios. To aid in network operators overcoming the introduction of RCM, there are current standards and solutions that exist that can be used to identify devices on a short-term and long-term basis.

These identifiers and solutions aren't isolated to a single market segment or use case but are mode dependent on factors relating to how network operators wish to operate their network, the capabilities of the network administrators and the devices utilizing the network, and the relationship between the end users and network administrators, i.e., company employee vs guest user in a public venue.

While not as easy as using the MAC address, these pieces of information do exist but many times it requires operators to change their approach to managing the networks to accommodate this change. Networks that already use some of the approaches detailed here will find less of a challenge resulting from RCM than networks that have relied solely on the MAC address of the client device to manage access and the services provided to that user by the network.

Most of the ability of the network to identify devices that will be utilizing a random MAC address today stems from either a pre-existing application, credentials, or certificates that the end user or device utilizes to authenticate to the network. This usually requires prior coordination before the user attempts to access the network, leading to issues in certain scenarios.

4.1 WPA2 & WPA3 Enterprise with 802.1X authentication

WPA2 & WPA3 Enterprise that uses 802.1X authentication has long been the standard for securing networks for many reasons. Increased security and device control is the primary hallmarks of these solutions but, in the case of MAC randomization, using 802.1X authentication offers an additional benefit. Except in the case where networks are using the MAC address of the device as the credentials, 802.1X authentication types, known as Extensible Authentication Protocol (EAP) Types, use other methods to identify the client device and the user of that device, and not the MAC address of the device.

With the ease of MAC spoofing, using MAC Authentication Bypass (MAB) for authentication lost favor with administrators long ago. MAC randomization only reinforces that decision. EAP types can use several methods to authenticate, usually certificate-based or username / password based. Using these methods, networks can assign identity based on these artifacts as they don't change without coordination on both the device and the network.

The issues that administrators face with WPA2 & WPA3 Enterprise stem from the complexity of configuration and operational continuity. Managing certificates for both the network and the client devices can pose challenges that some organizations aren't equipped to deal with and with the extensive list of EAP types, finding the type that is supported by all devices using the network can also pose a challenge. Password methods are also popular but that then requires additional servers to manage the credentials for the end user. For some network administrators this is a good alternative, but not all networks have close coordination between the network operators and the end users.

Issues: Issuance, deployment, and management of credentials and certificates.

4.2 Passpoint and OpenRoaming

Wi-Fi CERTIFIED Passpoint® is an industry-wide solution from the Wi-Fi Alliance designed to enhance and streamline Wi-Fi access for users. WBA OpenRoaming™ is a roaming federation service from the Wireless Broadband Alliance (WBA) to enable automatic, secure experience and seamless roaming between Wi-Fi networks. Both Passpoint and OpenRoaming are based on 'HotSpot 2.0' and fall under the IEEE 802.11u specification. As such, both use WPA2/3-Enterprise and EAP types are used to authenticate the user. In this regard, Passpoint and OpenRoaming both deal with MAC randomization in the same manner as discussed in the previous section.

The difference between the traditional WPA2/3-Enterprise solution and these are the entity that provides the identity portion of the solution. Organizations in these solutions are categorized as "Identity Providers" (IDP) and "Access Network Providers" (ANP). Identity Providers are classified as an organization that will manage the identities of the devices using the network and, in times, can also provide the WLAN to allow service / access. Network Providers are organizations that will only provide the WLAN for users to access the service.

In the majority of cases, networks acting as Network Provider don't manage the identities that are provided to the end users. These identities can be in the form of user credentials, a proprietary application that needs to be downloaded, or digital certificates that need to be installed on the device before users can connect. This approach has led to confusion for networks providers as well as challenges for users that wish to access the network without taking the prior steps needed to configure and ready their device, technically known as provisioning. A final challenge to some older networks can be the lack of support for Passpoint, which would block this service.

Issues: Provisioning and maintenance of subscriptions (containing credentials). Complexity of user interaction.

4.3 Easy Connect – Home Networks

Wi-Fi Easy Connect™ is a simple, secure way to configure a Wi-Fi device with the details needed to authenticate to an access point (AP). It is a more functional and more secure replacement for the insecure and obsolete WPS (Wi-Fi Protected Setup) as widely used in AP push-button pairing.

Easy Connect makes use of a trusted device designated as a 'configurator' to onboard all the other Wi-Fi devices on to the network. The configurator requires a good user interface (UI) and other capabilities such as Near Field Communication (NFC). Typically, the configurator will be a smartphone app but could equally be a web interface on a primary AP, and multiple configurators are allowed. The devices to be provisioned on the network are referred to as 'Enrollees'.

Amongst the main features of Easy Connect are:

- Standard method for onboarding any Wi-Fi device
- Provides for devices with little or no user interface (e.g., IoT devices)
- Simplified device identification (from user PoV) by using QR codes, NFC, human-readable text or downloaded device information
- Uses secure transport and a public key identity for provisioning and network access
- Onboards for WPA2 and WPA3 and other security access methods
- Allows change of SSID or to swap out an AP without needing to re-enroll devices

Easy Connect is implemented using DPP (Device Provisioning Protocol).

Issues: Easy Connect is not yet widely available and will take years to propagate through installed base of home routers. Moderately technical procedures are required. Furthermore, Easy Connect is not designed to provide continually available identities for devices. As designed, Easy Connect provides identity for authentication but has no current specification to provide ongoing identity for other network services. This would not be a significant change to the specification, but it has yet to be made.

4.4 802.1AR Secure Device Identity[2]

The 802.1AR Secure Device Identity standard specifies Secure Device Identifiers (DevIDs). A DevID is an x509 certificate-based identity bound to a device to enable authentication of the device's identity. The identity includes the device certificate chain, public and private keys, and other identifying information (e.g., a unique name and serial number) protected by a secure module (such as a Trusted Platform Module (TPM)) that facilitates signing operations to prove

[2] IEEE Std 802.1AR™-2018 IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity

knowledge of the secret whilst protecting the secret from being exfiltrated for device impersonation.

A device supporting DevID comes with a pre-installed identity and the ability to install one or more local identities. Private certificate authorities (CA) are permitted for both the initial/pre-installed and subsequent local DevIDs.

A DevID can be used in an EAP-TLS (Transport Layer Security) exchange between the DevID module and an authenticator and is intended for facilitating secure device provisioning.

For privacy, care should be taken in the construction and signing of local DevIDs used for different services to avoid fingerprint of the device between local DevIDs.

Where credentials are being used to identify users, DevID offers the additional possibility for identifying individual devices sharing the same user credential, perhaps allowing customization of services for specific devices.

Issues: It is not known how widespread the availability of DevID is on client devices, and as with Easy Connect, the DevID is intended to facilitate provisioning and may not be available to provide an ongoing identity.

4.5 External identifiers / proprietary identifiers

Identifiers provided through a UI, an App, or other side channel.

Identification of the device or user to a back-end service (such as a login name or a unique ID sent from an App to a server). This form of identification is outside of the Wi-Fi network, and can be used for many purposes, including requests from the identifying server to a network to request particular network-level services (e.g., QoS, content filtering).

Solutions are typically proprietary and the methods of doing this are outside of the scope of this paper.

Issues: Solutions are proprietary, therefore not standardized and not interchangeable.

4.6 PPSK – Private/Personal Pre-Shared Key

Private PSK (PPSK), also sometimes called Unique PSK, is the common name for a set of technologies that enable multiple users to connect to networks with their own unique WPA2 Personal pre-shared key (PSK) on a single secure SSID and works with any client device that supports WPA2-PSK. It has various proprietary names based on vendor, such as Private PSK, Dynamic PSK, Identity PSK, mPSK, and ePSK.

A common implementation of PPSK involves some form of initial enrolment process (via email, SMS, or captive portal) where a user is issued a PSK that is unique to them. Many vendors now allow for matching new devices to PSKs without MAC address registration. When a user then enters their PSK on the network with a new device, they exchange EAPoL (Extensible authentication protocol over LAN) messages with the access point and authentication server. This allows them to connect new devices to the network with their own PSK without any additional steps. These EAPOL messages verify that the unique PSK is valid and authenticate/associate the device on the network with an encrypted connection. This process works on any device that supports WPA2 Personal which is the vast majority of client devices (including IoT and browser-less devices).

In many PPSK solutions, the user's PSK becomes their identity and knowledge of the device MAC address is not required for authentication onto the network. These implementations are therefore unaffected by RCM because the PSK is used as a stable user identifier instead of device MAC addresses.

Issues: Solutions are proprietary, therefore not standardized and not interchangeable.

4.7 Device fingerprinting

Device fingerprinting is the collection of data from or on a device, to enable a network operator to create a device model allowing a device to be repeatedly recognized. Typically, a device ID is created for the device in the form of some sort of ID number. A Device fingerprint ID is used to identify a device, fully or partially, to enable network features, network debugging, personalization, targeted marketing or for authentication. The goal is to do this independent of typical device identifiers such as device name, IP address or MAC address. Fingerprinting solutions are almost always proprietary in nature, though many are at least partially based on information that is standardized. No fingerprinting solution is 100% deterministic so accuracy is an important parameter. Other considerations are how long it takes to create a fingerprint, how long it takes to match a fingerprint, does the solution use PII and finally, how much compute power is required.

Broadly speaking there are four types of fingerprinting. Radio fingerprinting, application fingerprinting, browser (or WAN) fingerprinting and Network (LAN) fingerprinting. In the following section each of these is briefly explained, along with some general pros and cons to each method.

Radio fingerprinting is based upon the characteristics of a devices radio transmissions, most frequently Wi-Fi or Bluetooth. A device’s radio waveforms have unique characteristics that result from variations it the manufacturing processes of the semiconductor, the Printed Circuit Board (PCB), other components, and the antenna. Radio fingerprinting is extremely hard to spoof or to disable. It is completely passive and requires no PII from the device owner. However, it is one of the more compute intensive solutions and requires access to lower level “physical layer” data from the receiving radio chip. While this information is commonly available in more recent devices, legacy semiconductors, which are prevalent in the installed base, are less likely to have this information available.

Application fingerprinting is a method of utilizing application level and other data directly from the device in question to create an identity. Parameters such as what applications are on the device, which ones are used, OS version and more are used to create an identity. Historically, this method is highly accurate, is fast, and it does not require much in the way of computer power. However, it does require a program to be running on the user device and it relies on information that is considered to be PII in most parts of the world. This method is quickly declining in general usefulness as OS makers limit access to the information required.

Browser or WAN fingerprinting leverages a device's behavior on the internet, including information that a browser may collect, to create an identity for the device. While not requiring much compute power, it is typically a slower solution in terms of time to recognize a device. As a result, it is more typically used for non-real-time applications. It also is leveraging information that is considered to be PII in most geographies. Private browsing windows have always limited effectiveness, and more recently encrypted Domain Name System (DNS) and Apple's private relay service significantly limit effectiveness for many devices.

Network or LAN fingerprinting leverages information on how a device communicates on the LAN network. This can be done completely passively and without using PII, so deployment does not require anything on the user device. There is not a lot of compute power needed and it can be done quickly within the network. It does however require access to either the layer 3 switch or the wireless access point to extract the appropriate networking management packets. This type of fingerprinting has emerged more recently as device maker changes have limited the usefulness of some of the other types of fingerprinting.

Issues: Solutions are proprietary, therefore not standardized and not interchangeable. Device vendors may take measures in future to thwart fingerprinting.

4.8 Doing nothing

The least effort is to simply do nothing to help identify devices allowing the current issues that have arisen to persist. By natural evolution, standards organizations having identified issues that have arisen from randomizing the device MAC address, will most likely act. If these organization do not act, then individual industry and service provider operators will pursue actions to overcome their unique situations. This is how the use of MAC address as a persistent device identity, and subsequently the various solutions described above, arose in the first place. This scenario will lead to disjointed and fragmented approaches to addressing the various issues, imposing random and burdening solutions on the overall Wi-Fi industry. Having a unified solution will result in enabling the device vendors, operators, and consumer of devices to apply functions which are interoperable and easy to deploy.

Issues: None of the issues caused by RCM will be resolved.

5 Matching solutions against requirements

5.1 Summary of identity requirements from Section 2

In many cases, different networks and service types have different and sometimes conflicting need for device or user Identities. The summary below excludes the requirement for and use of MAC addresses that last for the duration of a session, which are unique and always required for management of the local network.

There are three basic and interrelated features for the identity requirements:

- Uniqueness – whether an identifier needs to be unique, and for which entities (user, device).
- Scope – which devices or users need to be identified, and how widely the identity needs to be available, this depends on the purpose of the identity, and affects the privacy of the user.
- Duration – how long the identity of the device or user needs to be retained.

5.1.1 Uniqueness of the identity

The use of a MAC address as an identifier has resulted in systems that identify devices, even when it would be more appropriate to identify the user. In the use cases in section 2, there are examples where each permutation of the two may be required. Many cases require all devices to be uniquely identified, in others it is the user that should be uniquely identified, and in some cases both unique user and device identities are required. There are also cases where only devices or users meeting specific conditions such as those with specific services or restrictions need to be identified uniquely, other devices do not need to be distinguished for the purposes of providing (or denying) a service (i.e., the session MAC will be sufficient).

5.1.2 Scope of the identity

Except where users need to be personally identifiable (e.g., for law enforcement, which obviously is beyond any network scope), typically the identity is only needed for users or devices that have been authorized for and authenticated onto a specific ESS, network or related group of networks. Whilst an operator may operate different ESSs and brand names on one network, the user may have unrelated (and unrelatable) identities on each network.

A unique user identity does not necessarily imply that the user needs to be personally identifiable[3] to the network operator, or at all, though in most cases they will be personally

[3] It could be sufficient to identify the user as 'the person who gave me the €10 note (or $10 bill) at a coffee bar, kiosk, or vending machine'.

identifiable somewhere in the chain of authorization because of other requirements – payment mechanisms, hotel registration regulations etc.

There are situations where the user may decide to opt into being identified more personally, or for a longer duration than strictly necessary in order to receive a better level of service. Devices might also be identified by traffic characteristics in order to provide a better service – e.g. a gaming device.

For diagnostic, device steering, and network defense purposes, devices that attempt but fail to connect to the network may need to be identified but devices not using the network at all do not need to be and should not be identified.

5.1.3 Duration of the identity

Again, there is a lot of variability in the requirements for the duration of a stable identity.

Multiple possibilities exist as to how long an identity should last, the most common of which are:

- for a fixed pre-determined or variable duration and then expire
- for the duration of the access permission, restriction, privilege, or other validity e.g., session, length of stay, paid period, duration of IP lease, statutory retention period, etc.
- in the case of communications data retention, for as long as the data that it identifies. In this case, the lifetime of the identity may be different from the lifetime of the authorization, or different identities for the same device/person may be used by the data store and the operating network
- indefinitely for user blocking, and not be subject to subversion by the user
- Repeated but scheduled access to the network (e.g., working hours)
- No unique identity is required, session MAC is enough

5.2 Comparison of Requirements vs Existing Solutions

Tables 5.2a & 5.2b outline the comparison of requirements to the existing solutions identified in Sec Error! Reference source not found.

5.2a - Comparison for the first four solutions

	Capability / Solution			
	WPA2 & WPA3 Enterprise +802.1X	Passpoint	OpenRoaming – Additional to Passpoint features	Easy Connect / DPP
What is the identity? Is it unique?	EAP credentials. Can but does not have to be. Depends on EAP type.	Profile containing EAP credentials – CUI can be used to ID the device during the session or as long as the home operator maintains the association with the user	Refer to Passpoint	Easy Connect (EC) has a unique identity per device, typically the public key. It is tied to that device. For now, it is limited to authentication ID.
Identifies All or selected entities	All Associated devices must be identified, but identity need not be unique.	Based on device certificate or SIM could be device (noting that the SIM (ESIM) could be moved to a new device – however the entity is identified	Refer to Passpoint	Ideally an Easy Connect system would ID all devices on the network, However, legacy devices may still be allowed to join via WPA2 etc.
Private to the network?	Private to the authentication service.	Private to the authentication service		Yes, the ID is private to the network.
Lifetime of identity	Until removed or revoked. Network may receive a shorter duration identity from authentication server.	If CUI is used, then it is dependent on the authentication server operator and the lifetime may be less than that specified in the profile	Refer to Passpoint	In theory the ID is valid to the network for lifetime, even if the AP is switched out
ID can be transferred to another device?	Depending on device restrictions, identity may be copyable.	Depending on user ID in use (username/ password, User certificate, SIM)	Refer to Passpoint	No. IDs are unique to a device.

How is the identity revoked / removed?	Revocation or removal from the authentication server, from the device, or on expiry of a one of the credentials	Operator revokes the user ID/ Certificate/SIM	Refer to Passpoint	Via the configurator app used by network admin
Tied to a specific device?	In some cases, identity can be copied. MAC anchoring has been used to tie to a device.	Tied to device if device certificates or SIM are in use	Refer to Passpoint	Yes.
Tied to a specific user	User- or device- specific credentials can be issued, but copying may still be possible	Tied to user based on username / password, certificate, or SIM	As for Passpoint but the user must be personally identified by identity provider to ISO/IEC 29115	No There is no mechanism to associate the device to a user.
How is user consent obtained?	Independently, or at point of installation if the credential is user-installed.	This is based on how the profiles are loaded. If loaded by the user consent may be given by action of the user	Refer to Passpoint	The user has to go through the process to join the network. Any ID use beyond that is not yet comprehended.
Key Features	Secure click-free connection	Secure click-free connection Not dependent on SSID	Use other networks without further user effort	Easy authentication with a variety of onboarding and encryption methods.
Standard / Proprietary	Standard	Standard	Standard	Authentication is standardized but further device ID is not.

5.2a - Comparison for the final four solutions

	Proprietary External Identifiers	PPSK See also - PSK	Non-deterministic IDs / Device fingerprinting	Doing nothing
What is the identity? Is it unique?	Proprietary e.g., Username and password, device id, unique string	WPA2 Passphrase	The identity varies but a common approach is to create a machine learning model of the device behavior. It is non-deterministic but can have accuracy as high as 99.9%. There are also rule based approaches as well that tend to be faster, but with slightly less accuracy.	Session MAC address. Yes.
Identifies All or selected entities	Only registered devices/users	All	Finger printing can identity all devices. In many cases it can do so in a passive manner without the user taking any action.	All
Private to the network?	Yes	Yes, but passphrase can optionally be configured to work on multiple networks	Device fingerprinting can be made private to a location, a given network, or across a broader set of geographies. It is configurable	Yes
Lifetime of identity	Until deleted or revoked	Until removed or revoked	Indefinite for devices periodically on the network. The longer the device is absent, the lower the accuracy, measured in tenths of %. Device recognition accuracy may degrade slowly after 90 days of network absence.	Session or linked to SSID until SSID is forgotten
ID can be transferred to another device?	Easily shared just like a Netflix password	Yes, by entering the passphrase on a new device	No, device fingerprinting is about recognizing a particular device, not a person. As a result, it can have improved privacy protections	Identity can be forged If duplicate random is generated

How is the identity revoked / removed?	Removal of app or account	Passphrase can be invalidated by removing it from the pool. Forgetting it on the device.	Deleting the machine learning model from the data base	Expiry of session or forgetting the SSID based on OS implementation
Tied to a specific device?	Possibly	Not tied to a specific device	Yes, 100%	Yes – but temporary
Tied to a specific user	Usually.	Yes, unless user shares passphrase with another user	No, strictly tied to a device	No
How is user consent obtained?	App or web-page Ts & Cs and consent box.	During the onboarding process, could involve sending a link to obtain consent via email or SMS.	A user consent is optional as there is no PII used, and it is not associated to a user. It is strictly a device identity. In cases where user consent is needed a simple opt in or captive portal can suffice	None The network could still have a captive portal to gain consent. This would have to happen every session.
Key Features	User interaction	As WPA2 personal but unique passphrase per user, works on all devices (even IoT)	No user involvement needed. Can be limited to a specific location or network, low cost if implementation.	No effort
Standard / Proprietary	Proprietary	Proprietary	These are proprietary solutions for applications where the non-deterministic behavior is acceptable. There are proposals for “open” models and techniques although they do not currently exist.	Std

5.3 Legacy clients

With any of these solutions, the possibility needs to be addressed that there are likely to be some legacy devices, probably ones with fixed MAC addresses, that will not work with some of the particular solutions and will still require MAC-based controls unless they are to be made obsolete. A solution could potentially be an addition to the existing network as a hybrid solution rather than a complete replacement, where the equipment is sufficiently modern to do so. MAC addresses will still be required for session management, it is simply that they will no longer be used for authentication and authorization except in a few legacy cases. The operators of networks continuing to use MAC authentication should understand the risk, that has been present for some years now, from devices able to spoof those legacy MAC addresses. Some techniques, such as device fingerprinting, are passive, do not have issues with legacy devices and therefore may be combined with other techniques for a more complete solution. PPSK also does not require device changes and so works with any legacy devices that already work with PSK.

6 Are the requirements of the use cases satisfied by any of the solutions?

Requirements do not usually stand alone. A particular use case is likely to have several requirements, each of which can be met by one or more of the available solutions, but all of which may not necessarily be met by any one solution.

This section first examines all the requirements and will then look again at the combinations of requirements in the use cases to see whether there are any use cases that cannot be met by existing solutions.

The requirements for the following use cases are reflected in the table below:

1. For private home network access restrictions / privileges (including parental controls, per-device or per-user QoS)

   For Pay-per-Use networks - identification of complementary and paid-up users or devices
2. IP Address allocation in private, public and enterprise networks
3. Private home network device diagnostics and performance monitoring Enterprise network or device diagnostics and performance monitoring
4. Private home networks and enterprise networks band steering with multi-ESS networks (e.g., split-SSID installations)
5. Hospitality and venue network access with varying service levels
6. Pay-per-Use network access
7. Operators' public networks block devices that have expired or invalidated credentials and rapidly and repeatedly reattempt to connect
8. Network blocks devices due to abusive behavior or upon lawful demand
9. Passpoint networks record the acceptance of T&Cs on the AAA
10. Networks, typically using 802.1X, that use the device MAC to tie devices to certificates for certificate enrolment
11. Any network operator responding to requests for communications records, lawful interception, and other law enforcement purposes

	Used by cases	Frequent RCM	WPA2/3 Enterprise	Passpoint	Open Roaming	DPP	Proprietary	PPSK	Non-Deterministic
Requirement / Solution	Identify user								
	1 5 6 7 8 9 10 11	N	Y[0]	Y[0]	Y[0]		Y[0]	Y[0]	N
	Identify specific device								
	1 2 3 4 5 6 7 8 10 11	Y	Y[0]	Y[0]	Y[0]		Y	Y	Y
	The Identity must last for as long as certain conditions apply (e.g., QoS, IP lease, subscription, ban or restriction).								
	1 2 3 4 5 6 7 8 9 10 11	N	Y	Y	Y		Y	Y	Y[9]
	There should not be a way to remove the identity and still obtain service/privilege.								
	1 5 6 7 9	Y	Y	Y	Y		Y	Y	Y
	The Identity is unique to the network and device or user								
	1 2 6 7? 8	Y	Y	Y[0]	Y[0]		Y[0]	Y	Y[0]
	All associated devices need to be individually identified.								
	2 3 5? 6?	Y	Y	Y	Y		Y	Y	Y[9]
	Identify all devices that have associated or attempted to associate with the network (even when not associated)								
	1 3 6 7 8	Y	Y[1]	Y[1]	Y[1]		Y[1]	Y	N
	Devices not associated to the network do not need to be identified								
	1 2 4 5 6 9	Y	Y	Y	Y		Y	Y	Y[2]
	Identify all devices that have associated or attempted to associate with the network (even when not associated)								
	3 4	N	N	N	N		N	N	Y[2]
	Identify devices across a collection of networks - more than one SSID								
	3 4 5 6? 7 8 9?	N	Y[3]	Y	Y		Y	Y[3]	Y[3]
	The network should be able to restrict devices from retrying at the access network level.[4]								
	7	N[4]	N	N	N		N	N	Y[5]
	The Identity should not be removable by the user. (In all other cases, it should be.)[5]								
	7 8 11	N	N	N	N		N	N	Y
	The identity should be able to be tied to a device so that it can only be used by that identity								
	10	N	N	N	N		N	N	Y
	The network must be able to identify each specific user to whom access is granted and associate this with one or more Communications Records.								
	11	N	Y[6]	Y[6]	Y[6]		Y[6]	Y[6]	N[8]
	It must be possible to determine the User from specifically identified communications/packets.								
	11	N	Y[6]	Y[6]	Y[6]		Y[6]	Y[6]	N[8]
	The Identity and the association must be retained for the statutory period.								
	11	N	Y[7]	Y[7]	Y[7]		Y[7]	Y[7]	N[8]

Figure 2 - Support for requirements - by use case.

[4] Although it would be better if the device behaviour were modified to prevent this being a problem.

[5] Baring a user from a network is a separate and potentially more difficult issue.

Notes:

- Y[0] - The solution can be configured either to identify each specific device, or each user whose device is associated to the network.
- Y[1] - Devices do still need to be identified, but can share a common credential.
- Y[2] - Depending on the type of fingerprinting, devices may be able to be identified from their radio signature alone.
- Y[3] - Devices may be identified as being the same across networks if the credentials or fingerprints are shared between the networks.
- N[4] - How long the device can be restricted will depend on the duration of the RCM
- Y[5] - Some techniques can only identify associated devices.
- Y[6] - The solution can be configured to identify each specific user whose device is associated to the network. The network operator must maintain the link between the identity, the session MAC, and the Communication Records appropriately.
- Y[7] - The credential can be configured to have a long lifetime, but the user cannot be prevented from removing it, nor generally from acquiring a different new one.
- N[8] - The fingerprint is not guaranteed 100% unique and may alter over time. A device that has not been connected to a network for a long time may not fingerprint as the same device that was previously connected.
- Y[9] - The fingerprint is not guaranteed 100% unique, a device may appear to have more than one fingerprint, and the identity may alter over time.

6.1 Filling in the Gaps

The requirements that are not readily facilitated by the solutions identified in this section are typically also not ones that can reliably be solved by the use of a fixed MAC address where there is the possibility for a user to change that MAC address.

In the domain of network management and statistics:

- identifying and blocking at the access network, devices with invalid or expired credentials is best dealt with by appropriate changes to the device behavior.
- With those authorized devices that are having connection issues prior to association, RCM will obscure repeat behavior of particular devices and device types for which this is happening.
- The expanding use of RCM is resulting in device type identification slowly going dark but whilst device types have typically been identified by the network it is often not the network that needs to know. Endpoints use device type to tailor services, but they may

be able to determine it by other means. One such example application is for the provision of the correct Passpoint R1 profile from a captive portal in the absence of standardized Online Sign-Up (OSU) and in this case the provisioning portal should be able to identify the device type itself.

- Where connection diagnostics are required, the combination of RCM and the loss of the Organizational Unique Identifier (OUI) and even the Hostname, it is increasingly difficult for a network operator to identify devices that a user claims to be having problems with.
- Where a device is exhibiting undesirable behavior (such as a Denial-of-Service (DoS) attack) and needs to be blocked, the device may have the ability to change its MAC whether or not RCM is in use and the obstruction of such behavior is likely to be only short-term.

For credential management and user identification:

- Transferring a credential from one device to another (e.g., WPA2 passwords) has been an issue for a long time, with some device manufacturers even seeing this as a feature and providing mechanisms for the sharing of Wi-Fi access details. This issue is once again best resolved by changes to device behavior, and some devices are now storing credentials in secure areas that the user cannot access in order to copy, share, or transfer them. However, it will never be possible to completely prevent credential sharing and the network operator should take steps to prevent the same credential being used on multiple devices simultaneously.
- Where jurisdictions require that particular devices or users can be blocked from accessing networks the only practical solution is positive identification of all users before providing service. Otherwise, a user can always reset or reflash an existing device to remove all traces of existing IDs or can obtain a new device.

7 How are these solutions used?

For a Wi-Fi network provider currently using MAC-based network management that decides they need to provide something different to overcome issues that arise from RCM, this section is intended to assist in making informed choices by providing some understanding of each of the solutions, its capabilities, advantages, and disadvantages, and what is involved in deploying it. When considering these, it is best to consider the case where the RCM may change every session if we want the solution to be a long-term one.

Note should also be taken of the other issues raised in this document (privacy and consent, security, legal compliance around the world, etc.), what would be needed beyond the MAC-based network in order to use each of these alternatives, how long-term the solution might be, and how legacy devices will be handled.

7.1 WPA2 & WPA3 Enterprise with 802.1X authentication

These methods require the provisioning of a credential to the user's device which can be done in a number of ways including through an app, automatically in the case of SIM-based credentials, and by manual entry on the part of the user. Although this may initially be more work for the user, once provisioned, these methods have the advantage of automatically providing a secure exchange of credentials with an identity provider; which need not be the network provider. Network identification is SSID-based and so the user must still select the network or mark it for auto-connection.

In this configuration, each Access Point needs a connection to an authentication server. Wi-Fi EAPOL messages from the client to the AP carry the EAP transaction destined for the authentication server which then tells the AP whether the client is allowed access to the network.

Based on the types and configuration of use of the method presented to the AP which is forwarded to the authentication server, device or user identity could be collected. In the case of EAP-TLS a certificate is used which could be associated with either the device (i.e., device certificate) or the user (i.e., user certificate). In the case of the device certificate this is assigned to specific device and typically is not meant to be used by other devices, while user certificates are assigned to a user and can be installed in one or more devices. While the certificates are assigned to either a device or user, anonymous is used at the beginning of the EAP exchange to allow for the certificate to be encrypted and unusable by the AP.

EAP-TTLS unlike EAP-TLS makes use of a username/password which would only identify the user not the device. In the case of EAP-TLS the username/password could be sent in a manner that the AP would have access to the username. However, in many cases the username of "anonymous" used to initiate the EAP exchange would result in the actual username / password being encrypted and unusable by the AP.

In the cases of EAP-SIM, EAP-AKA, and EAP-AKA' the exchange is encrypted early in the EAP exchange resulting in the information being unusable by the AP.

In many of the above cases the authentication server may return a Changeable User Identity (CUI). The CUI is maintained over the session and could remain associated with the authentication (device and/or user) over multiple sessions. However, depending on the operator of the authentication server configuration may be short lived limiting the use of the CUI or rendering useless to identify the device or user.

Although this solution provides more secure and more flexible identification of users and/or devices it does require the provision and management of an authentication server.

7.2 Passpoint

Passpoint utilizes 802.1X authenticated parameters as described in section 7.1. above but in addition provides a mechanism for automatic network selection that is not dependent on SSID. It does not in itself provide any direct method of identifying the device or user.

In addition to the requirements for 802.1X, Passpoint R2/R3 also specifies a mechanism (OSU) to deploy and update subscriptions to each device, though this is not yet widely implemented, and a captive portal or mobile app is often used to install a Passpoint R1 subscription. The user process for installing the subscription on the device is limited to visiting the correct source for the subscription and agreeing to the installation. Once the subscription has been installed, Passpoint typically requires little or no user intervention.

The main advantages of Passpoint over 802.1X lie in the automatic detection of APs providing service for a particular subscription, and 'zero-touch' connection to the service. Passpoint removed the dependence on Wi-Fi SSIDs to identify networks and thus facilitates connection to networks with different brands so long as the identification and authentication remain the same. Deployment of a Passpoint service requires a Passpoint-capable AP and firmware. These features have been widely available on most enterprise APs for many years now.

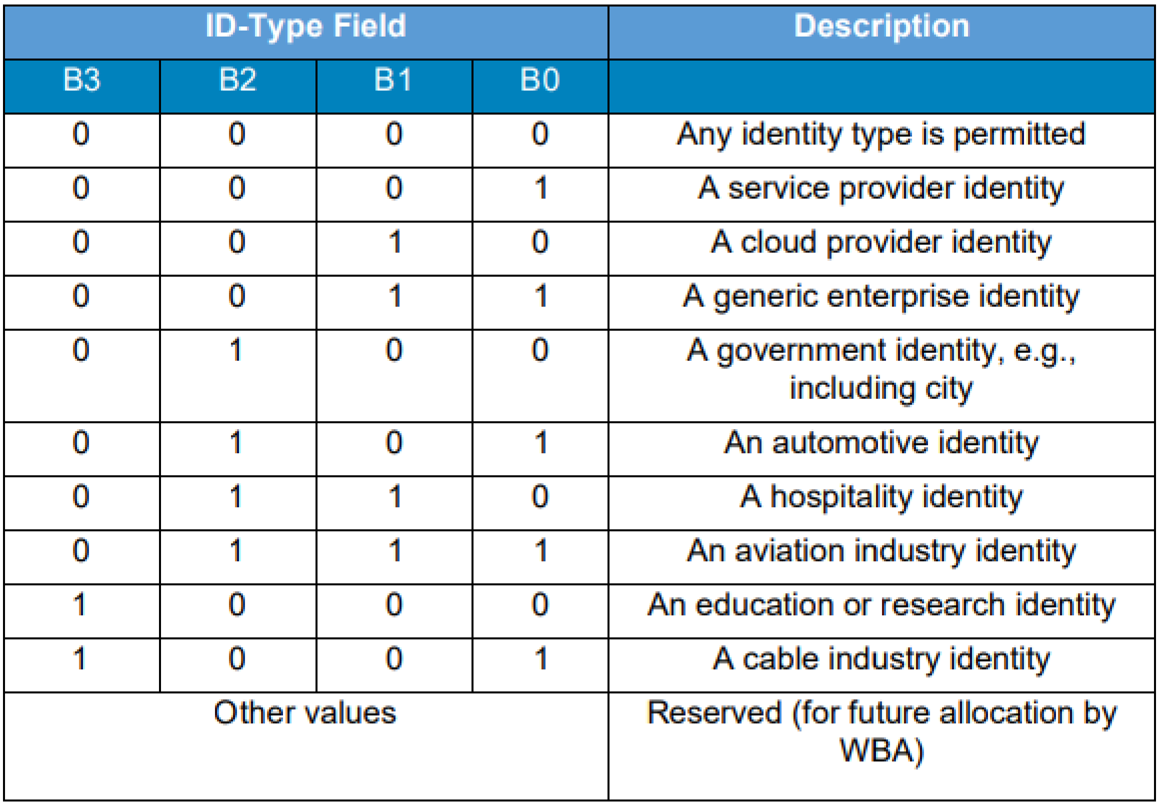
7.3 OpenRoaming – Roaming between Passpoint networks

OpenRoaming enables a federation of operators to have a common method of allowing users to roam and increase the number of networks that a user can roam on. OpenRoaming makes use of Passpoint (7.2) resulting in the same level of device and user identification.

But, in addition, OpenRoaming uses a Roaming Consortium Organization Identifier (RCOI) Policy, that allows for the application of specific RCOI bits that can be used to contextualize the type of identity.

This is an important addition that allow specific identity providers to complement the RCOI they are using with a specific context, bound by an underlying legal framework.

Can be used not only to inform the network that this is an identity focused on a given vertical:



ID-Type Field				Description
B3	B2	B1	B0	
0	0	0	0	Any identity type is permitted
0	0	0	1	A service provider identity
0	0	1	0	A cloud provider identity
0	0	1	1	A generic enterprise identity
0	1	0	0	A government identity, e.g., including city
0	1	0	1	An automotive identity
0	1	1	0	A hospitality identity
0	1	1	1	An aviation industry identity
1	0	0	0	An education or research identity
1	0	0	1	A cable industry identity
Other values				Reserved (for future allocation by WBA)

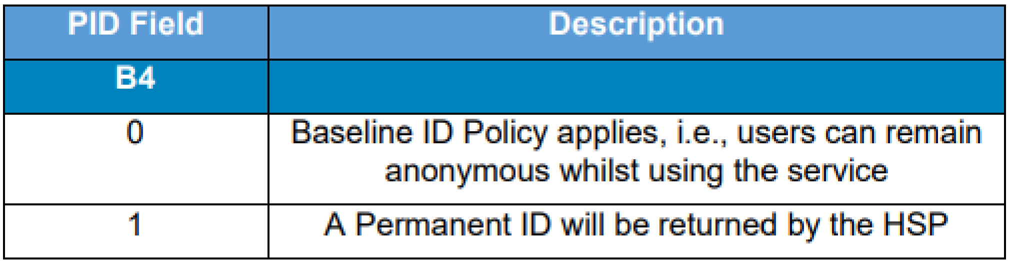
Figure 3 - OpenRoaming R2 RCOI Policy – Verticals

But can also be used to indicate that a given Identity might be returned to the Network Provider in the Access-Response. These are called PID or Permanent IDs.

The PID field can be used to support a policy where the HSP has agreed to return a permanent ID to the VNP in the Access-Response. This can be contrasted with the baseline policy of OpenRoaming which enables the identity of roaming subscribers to remain anonymous when using the service.

Note, the OpenRoaming Terms of Service requires that subscribers have explicitly given their permission for their permanent identity to be shared with the third-party VNP.

The format of the PID field is as follows:



PID Field	Description
B4	
0	Baseline ID Policy applies, i.e., users can remain anonymous whilst using the service
1	A Permanent ID will be returned by the HSP

Figure 4 - OpenRoaming R2 RCOI Policy - Permanent IDs

Therefore, a given Identity Provider – carrier, software company or even network / venue – can decide to issue and provision their credentials, and incorporate a PID bit onto the RCOI, so that the users authenticating with that credential can have their ID returned to the network through the Access-Response exchange.

7.4 DPP / Easy Connect – Home Networks

While the certification for Easy Connect is just starting there are no certified APs or devices on the market at the time of writing. Available implementations require a smartphone to conduct the provisioning. Easy Connect can operate in a similar way to WPS, making it easy for the user to provision devices for connection to the home network.

7.5 PPSK

PPSK solutions have network hardware dependencies and vary greatly across vendors. There are many proprietary names for the PPSK capability, but each vendor-specific version offers a way for multiple users to connect to a single SSID with their own WPA2 Personal passphrase (PSK). Many vendors even support PPSK without prior knowledge or registration of the client device MAC address, which makes these particular PPSK solutions compelling for many use cases.

PPSK is used in apartments, long-term stay hotels/resorts, and other visitor-based Wi-Fi applications where a network operator is managing the network but does not have control of the end-user devices. Because PPSK makes use of WPA2-Personal, end users are able to use their personal PSK on virtually all client devices. This includes gaming consoles, printers, IoT, e-readers, and even older devices without browsers.

A standard implementation involves a single SSID being broadcast for all users and begins with onboarding users via email, SMS, or other channels.

This onboarding process can be triggered manually, based on a schedule, or via integration to the venue's property management system so that when new apartment resident signs a lease, the onboarding process automatically begins.

When a user gets the onboarding email or SMS message, they will be taken to a welcome page to confirm their identity, accept the terms of service, and be issued their PSK. They will not be able to create the PSK themselves, as this would cause security issues and potential collisions. The best practice is to use an easy-to-remember randomly generated PSK that contains multiple words and numbers.

Once the end-user knows their PSK, this becomes their identity on the network. When a device joins the network with the key issued to the end-user, the vendor-specific PPSK solution is able to match that key to the one stored for that user and authenticate that device on the network. Many PPSK solutions also offer the capability to put each device matched to the same key on the same Personal Area Network which allows these devices to securely communicate with one another.

Using the scheduling system or integration to the property management system, notifications can be sent to end-users based on their lease ending or if their Wi-Fi access has been suspended. Users can also communicate via email or SMS if they forget their PSK and offboarding of users can also be done automatically. With this in place, the entire user management process can be automated which has the potential to significantly reduce ongoing support costs for the network operator.

PPSK solutions are only able to identify users (with user-entered PSKs as the primary identifier) and cannot usually identify devices on the network. This is beneficial in that PPSK solutions are unaffected by RCM but can be a limitation if the use case requires device identification (such as blocking access for a single device without blocking access entirely for a specific user).

PPSK solutions can be implemented to offer a simple and efficient end-user onboarding experience that can be fully automated, and they can potentially solve many of the issues that drive support calls for network operators. However, PPSK is not vendor-agnostic, and adopting it will mean a certain degree of vendor lock-in. Finally, PPSK deployment in the home may result in credential sharing, which makes it is nearly useless beyond saying this device is allowed on the network. Parental controls would not work, as an example, when credential sharing happens.

7.6 Separate SSIDs

Guest or alternate Wi-Fi SSIDs offer the possibility of providing networks each with their own PSK that have different constraints from other SSIDs on the same AP(s). Extending this concept further could provide a deployment having a similar effect to PPSK by providing a separate SSID and unique PSK for each person, and thereby provide per-person customization. Potential applications for this technique could include an SSID per family member for an in-home system or highly localized networks for specific office/factory/hospitality functions. Downsides to this technique include the number of SSIDs (and associated air-time) that may need to be broadcast, and the management overhead of each individual SSID.

7.7 External Proprietary Identifiers – Apps and Web-based login

As mentioned in section 4, there are many proprietary solutions which are outside the scope of this paper.

Use of a captive portal on an open Wi-Fi network is the most common example of this and one that will be familiar for most networks that use MAC as an identifier, although with RCM this will only allow access for the duration of the MAC. Where longer-term identifiers are required, an App can be used to provide these from session to session. This would include Apps that automatically make or substitute for the captive portal submission or otherwise use a 'pinhole' to contact an authentication server when a specific Wi-Fi network is detected, Apps implementing WISPr (now obsolete), and Apps implementing challenge-response systems using stored secrets.

The server receiving the information instructs the network access control to allow or deny access to the wider network or services for the device that has a particular (session) MAC.

Where an open network is being used, users should be made aware of the need to always use secure connections such as HTTPS or a VPN.

The main issue with these approaches is universality, in that the solutions are proprietary and unlikely to be interoperable between networks unless they use the same solution/provider, and that Apps are built for particular operating systems, and in some cases versions of operating systems, and a separate one will be needed for each system that the network intends to support.

7.8 Device fingerprinting

Fingerprinting solutions (FPS) come from several different vendors and as a result there is a lot of variability in the specific implementations. It is recommended that interested parties connect with specific vendors for additional details. In this section a generalized approach will be taken to highlight common characteristics of FPS.

The three most common high- level characteristics of FPS are:

1) the solutions are generally passive, living within the network and not requiring anything from a user or the user's device.
2) the solutions are non-deterministic with accuracy in the high 90-99.9% range, and
3) Most FPS use some level of machine learning to improve accuracy over time

The three characteristics defined above helps to define the best use cases in the following three deployment architectures: (i) consumer homes, (ii) enterprise, and (iii) public/retail/hotel/Muni networks. Starting with the home, a generalized system architecture for the home shown in the figure 1.

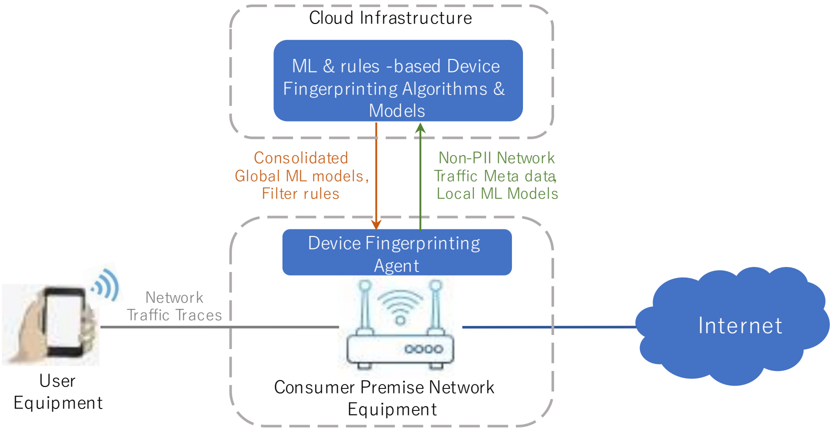

Cloud Infrastructure
ML & rules -based Device Fingerprinting Algorithms & Models
Consolidated Global ML models, Filter rules
Non-PII Network Traffic Meta data, Local ML Models
Device Fingerprinting Agent
Network Traffic Traces
Internet
User Equipment
Consumer Premise Network Equipment

Figure 5 - Generalized system architecture for consumer home networks

Functionally, the system uses a FP agent that runs in the home access point. Network traffic is analyzed with some combination of machine learning and rules-based approaches to create an identification (ID) unique for each device. The CPE generally has a data collection agent, and the cloud is used for ID generation and matching. This agent runs in the user space and in most modern ISP networks can be added over the air (OTA). After a device is learned, a small packet of data is collected each time the device is on the network and the cloud agent then validates the device. Given FPS systems improve accuracy over time and the home has a limited pool of devices, accuracy can be very high. Additionally, the passive nature and the fact that home devices are essentially unmanaged make the FPS a very good match with parental controls and general network device identity.

Potential Solutions

On the enterprise side of things, the use cases of fingerprinting around mac randomization are more limited. The biggest reason is that enterprise networks can professionally control and manage the devices on the network WPA enterprise can be used (amongst other solutions) that can provide for deterministic device and user identity solutions for the network. Fingerprinting may be used in the enterprise environment as a backup method for legacy or IoT devices.

Finally, we look at the general grouping of public/retail/hotel/Muni networks. To generalize, most of the networks are multiple managed APs connecting to a layer 3 switch with the whole network being cloud managed. The devices on the other hand are very much unmanaged consumer devices for the most part. That means installing a cert or an application on the device, or controlling user behavior, is a complex problem. Again, this is a good match with the passive techniques of FPS. Additionally, many of these services rely on MAC based billing systems and changing of MAC IDs can make multiday billing a challenge and can also be used as an avenue for fraud in systems that give a certain amount of time free each day. A generalized architecture is shown Figure 2. In this system, a lean appliance is installed on (virtual machine) or beside (physical appliance) the layer 3 switch. The appliance collects the required network traffic to identify or deduplicate each device, without using any PII from the user whatsoever. This information is forwarded to a cloud-based device identity system which then integrates cloud to cloud with the existing network management system. Given that most of the systems are already cloud managed, the additional data load is small, and it fits well with the existing network architecture. As a result, deployment to the premise can usually be done in a 30-minute service call. The biggest part of the deployment is the cloud-to-cloud integration, but that is typically done through standardized APIs allowing for push and pull operation. Nothing needs to be done by the network users. Depending on geography and the desire of the network owners, simple user opt-in capabilities can be added, and APIs are typically provided.

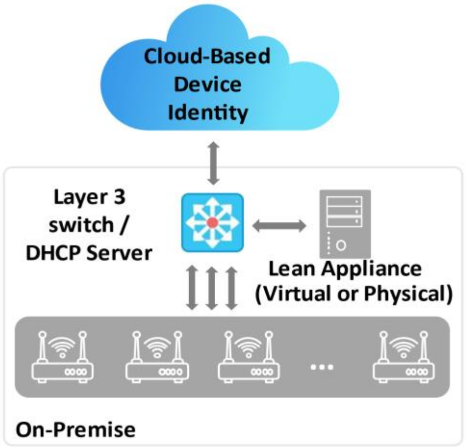

Cloud-Based Device Identity
Layer 3 switch / DHCP Server
Lean Appliance (Virtual or Physical)
...
On-Premise

Figure 6: Architecture for cloud-based fingerprint ID

Recommendations

In summary, finger printing solutions are best deployed in networks where the devices are unmanaged, and the cost of managing those devices are high. Networks, such as in many enterprises, where the devices can be tightly controlled and managed are not the best fit. The ability to deploy OTA, without user involvement, means costs can be very low and time to implementation can be very fast. At the same time, the solution is non-deterministic, so use cases that require 100% accuracy are not a fit, and solutions from different vendors are unlikely to be interoperable.

8 Application of Existing Solutions to Network Types

In this section we consider the main categories of networks that are affected by randomized and changing MAC address and look at some of the more appropriate solutions that can be used with them.

8.1 Hospitality and venue networks

Wi-Fi connectivity is considered the most important guest amenity in hotels. Conference attendees, hotel guests, and dining guests expect a fast, secure, and reliable connection wherever they are on the property. However, this has become increasingly difficult with existing MAC-based solutions. RCM has made it difficult for users to roam from one SSID to another. A guest may move from the lobby to the guest room and then to the meeting space; each of which may have a different network and identity; and may have to reauthenticate to Wi-Fi at each new location. Time-based RCM also significantly impacts the guest experience by requiring guests to reauthenticate their devices to Wi-Fi multiple times during the course of their stay. Lastly, there are increasing security issues with Wi-Fi at hotels. Evil-twin attacks have become so prevalent that the FBI issued a warning specifically about them in hotels.

Potential Solutions

Passpoint can be implemented in hospitality in a variety of ways. A common method is through the hotel brand's loyalty program. Loyalty guests are able to install Passpoint subscriptions via the brand's mobile app or a branded microsite. The hotel brand mandates that a Passpoint-specific SSID is deployed across the footprint and guests with subscriptions are automatically and securely connected at any property. This implementation solves many of the issues caused by RCM for loyalty members and provides better security for guests who opt-in to the program, but it does not address the issues for non-loyalty guests or non-guests.

WBA Open Roaming is a good fit for hospitality and can also be implemented in many ways. Unlike traditional Passpoint, Open Roaming can authenticate users using credentials they already have (such as a SIM issued by an MNO or a TLS certificate from a supported Open Roaming identity provider) and can allow these users to automatically connect. Hotels typically have many transient visitors, and this removes the friction of a device onboarding step for them to get connected. It also provides improved security when compared to traditional MAC-based solutions which is critical. Implementations of Open Roaming also do not rely on device MAC addresses and are not affected by RCM.

802.1X is increasingly important in hospitality due to the growing number IoT devices on hotel networks. While RCM is rarely implemented on these types of devices (staff alert devices, employee devices, point of sale systems, thermostats, door locks, etc.), traditional MAC-based networks have major security limitations for authenticating them. 802.1X allows each device to have a unique credential and to be authenticated by a AAA server that can allow secure access to the right segment of the network.

Device fingerprinting can also be implemented on hospitality networks in order to potentially reduce the impact of RCM. Using a proprietary device fingerprinting solution, guest devices can potentially be identified using the specific characteristics of their Wi-Fi radios, installed applications, browser, and network behavior. Where required, the fingerprint of a device can be associated to its user by indirect means such as captive portal.

Device fingerprints could potentially be shared across deployments to enable tracking of the device, albeit with less than perfect accuracy.

Recommendations

Hospitality networks are complex, and in most scenarios, it makes sense to deploy a hybrid solution using several different technologies.

- It’s recommended to deploy a traditional Passpoint network for loyalty members if this is an important benefit for the hotel brand.
- It’s recommended to deploy Open Roaming to allow users to securely roam on to the hotel network.
- It's recommended to deploy 802.1X for staff and IoT devices that support it.
- Doing nothing is not advisable. RCM will negatively impact the guest experience and there are too many security risks with going this route.

8.2 Operators’ Public Networks (including networks like Eduroam)

Traditionally these have been open Wi-Fi networks with MAC-based captive portals to control access to wider network services and relying on browsers’ TLS for security. There may also be the option of App-based authentication to these networks.

These mechanisms are very simple for user to understand and use, but open to MAC-based attacks to obtain free services etc.

Open networks are slowly being superseded by 802.1X and Passpoint. For those few where EAP-SIM authentication can be used this is very easy for the user, but where a subscription must be installed there is considerable friction in the user sign-up journey, and this is all the more so when the network may only be needed occasionally or for a short time. However, once the user has the subscription installed, the connection experience is much better than that experienced on the previous captive portal-based solutions.

- Operators’ Public Networks may support a very large number of users across wide geographic areas. They may also provide branded solutions for VNOs and partner organizations.

- Where legacy MAC-based authentication is still in use, RCM is degrading the user experience, often causing user to have to re-register for service, as well as increasing resource usage for various network elements (captive portals, user databases etc.).

Potential Solutions

- 802.1X or Passpoint are the natural evolution for these networks
    - Operators usually have the capability and expertise to be able to provide authentication servers and infrastructure for these solutions.
    - These solutions also provide the flexibility to identify devices, groups of devices, individuals, or groups of individuals depending on the service proposition.
    - Customers may find the onboarding experience a little difficult or confusing on some devices, either because of the subscription/credential installation journey or because of device limitations.
    - Once the devices have been onboarded to the network the user experience is usually very good.
    - These networks are unlikely to be supporting the use of IoT or similar devices and Operators should consider whether or not it will be necessary to continue to provide a MAC-based service for legacy devices that are unable to use either 802.1X or Passpoint.
- Open Roaming:
    - OpenRoaming can be added later and increases the possibilities for the services that operators are able to offer their customers

Recommendations

- Passpoint and 802.1X are the recommended solution for these networks, with Passpoint being an ideal addition to an 802.1X network
- Operating a Passpoint network opens up the possibilities for agreements to allow users to roam between networks, and Open Roaming is the recommended method for this enhancement.
- Because of the scale of typical operator networks, neither fingerprinting nor PPSK can be recommended.

8.3 Private home networks

The major identifying feature of home networks is the sheer diversity of devices that may be connecting to the network, from cheap insecure IoT devices and smart home devices, through legacy computers and mobile devices through to Enterprise working-from-home devices.

One major issue introduced by RCM on this type of network are likely to be from personal or mobile devices bypassing MAC-based restrictions. Another is the lack of expertise of the typical user for whom networking technicalities and RCM are completely unknown. A further complication is that when seeking help from the network provider, the RCM will make it more difficult for the help-desk to identify the activities of the device that the user is having problems with, especially if the user cannot get the device to connect at all.

Potential Solutions

For home networks it is going to be necessary to retain the MAC-based capability unless the user is going to scrap many devices and has the knowledge to know which new devices not to buy. This would be an unreasonable expectation because many new low-cost devices will continue not to provide anything better than WPA2-personal authentication, perhaps via WPS.

Most functions that relied on MAC address will continue to work as they always have until more frequent randomization is introduced. Devices that start to randomize may require re-application of authorizations or restrictions, and some restrictions may be bypassed by the user changing the MAC. Ideally if the AP allows, devices should be permitted rather than blocked to prevent restrictions being bypassed.

In the near term, APs could also be updated to support proprietary solutions using Private PSK or Device Fingerprinting though these would require firmware updates to the APs. These solutions should work reliably at the scale of; and within the resources of; a home network, though the user management interface may require extra consideration.

In the longer term, home network providers should look towards providing lightweight self-contained versions of Enterprise solutions such as WPA2/3 Enterprise and Passpoint for their more capable modern devices. A lightweight AAA server would be required either on a master AP/controller or on an external device, but this is not beyond the capabilities of a modern AP processor.

A new home network solution will require considerable resource and effort in what is often a price-sensitive market. Considerable attention will also need to be given to the challenge of how a naïve user is going to manage the connection of devices to the network.

The MAC-based authentication will need to be retained and should be set up to permit devices with certain MACs to perform certain activities.

Private home networks often feature Guest Networks that may not have access to all of the resources of the home network but do provide internet access and may have content restrictions and bandwidth or usage controls. Devices using a guest network may be regular visitors, in which case some onboarding mechanism is desirable; or may be short-term, where a simple and quick management interface to permit a device to use the guest network for a limited period for which a MAC may be sufficient, the ease is more important, and may not be particularly troubled by any effects of RCM.

Recommendations:

A hybrid system will be required in order to support both legacy fixed-MAC devices and RCM devices. There are a wide variety of options available.

- Doing Nothing is a valid choice for Home Networks in the short term and is the best option for legacy devices that do not conduct MAC randomization.

  If choosing this option, network providers should also prepare their next home network offering for the time when frequent RCM is implemented on some devices by choosing and implementing one of the following solutions.

- Home APs may support 802.1X, and in those cases using 802.1X for devices that support it is an option for either the expert user or the service provider of managed home networks
- Device Fingerprinting is an option that could be provided by the Home AP provider – an AP firmware update would be required
- Private PSK is an option that could be provided by the Home AP provider – an AP firmware update would be required
- Easy Connect cannot be recommended in the near term due to the low availability of AP and device support but is an option for authentication and potentially for other use cases in a new AP development because it is at least partially supported by modern mobile operating systems.

8.4 Managed home networks and SMBs

Managed home and small business networks differ from the more common home networks in that they are managed by the homes' Service Providers. Typically, they are multi-AP solutions and as well as the network management being provided for the user, these networks have extra functionality provided by remote systems operated by the network provider that can be used for enhanced features such as dynamic reconfiguration, enhanced security, content filtering, and even AAA, PPSK, and Fingerprinting services. There may also be better management of updates to the APs that will still be required to make use of those kinds of functionality.

The implementation of small managed networks is often a hybrid between a typical home network and some variant of an enterprise network. Typically, it will provide some of the additional management and security functionality found in enterprise networks. The applicable solutions will depend on the functionality required in each specific case and should be chosen from the most appropriate solution in the surrounding sections.

SMBs should not resort to using home network solutions but instead should look for low- to mid-tier enterprise networking solutions which may be available as managed business networks.

8.5 Enterprise networks

While enterprise networks are typically seen as related to business networks such as in an office or business-related industries as hospitals, and factories. However, enterprise networks are in used in other areas such as entertainment venues, conference center, and outdoor or community Wi-Fi. The level of need to know the identity of a device is as varied as the enterprise deployments. These range from no requirement to ID the device based on MAC layer, such as in a factory where IOT devices may be known based on upper layer applications, to the other end of the spectrum where knowing the ID of a device is a critical function, such as to apply unique rules to each device. As the range of knowing the identity devices blankets the full spectrum, the use cases are many and varied. This includes but is not limited to routing of traffic, monitoring network usage, allow-deny lists, and troubleshooting. Without knowing the identity of devices, these functions along with others are limited or not possible.

Potential Solutions

With the lack of a persistent means for identifying devices based on layer 2, there are other means that are potential solutions beyond using upper layer functions. These include making use of 802.1X, Passpoint, and device fingerprinting which are the most prominent as identified within this paper.

Since enterprise networks rely on 802.1X to authentication/authorization a device, the credentials could be used to identify the device or user. There are two basic issues with making use of 802.1X to identify an individual device. The first is that the credentials may be user based and not device based, examples are TTLS and user-based certificates for TLS. In the case of device-based certificates for TLS or SIM/AKA/AKA’, these are device- specific and either cannot be shared between devices or may be restricted for use in only one device at a time. The second is informing the AP of the relationship between the device’s current RCM MAC and the identity of the devices or user. Since 802.1X is forwarded to an authentication/authorization server via Radius messaging, there needs to be a consistent method of return for the identity to be used and which rules need to be applied to the devices. While this is possible within a closed network, in the case of roaming networks this would require extensive inter-partnered agreement. Additionally, with roaming there is a risk of exposing the device/user identification to the visited network. While Passpoint has been offered as a solution, Passpoint relies on 802.1X as well and so has the same issues as 802.1X.

Device fingerprinting could be used; however, vendors are attempting to find ways to thwart this technology. This method has some flaws, either not identifying the device consistently or identifying multiple devices as one device. The resulting case of one device being identified as multiple devices would not allow rules to be applied as needed and possibly over run resources. Likewise, multiple devices being identified as a single device again may result in incorrect rules being applied or even not allowing the other device(s) so identified to access the network.

PPSK use could be more feasible as the enterprise wireless LAN controller typically has the resources to deal with a large pool of PPSKs. The issue with this approach is that PPSK requires that each device has an individual PPSK or at the least each user having an individual PPSK. This would complicate the provisioning of the devices as the PPSK would most likely have to be manually installed on the device(s).

Recommendations

For business, office, and education types of enterprise network where a high degree of security is desirable per-device 802.1X credentials would typically be used.

For the other enterprise uses, based on the ease and endurance of identifying individual devices and/or users, PPSK would be the first method of choice, followed by device finger printing - as the false identifications are less than 1% based on testing. The use and complexity of 802.1X to identify devices places this and Passpoint as the last of the methods recommended for use.

9 Summary

Many network operators have a need to identify either devices or users that are using their network and for many older networks this has been achieved by using device MAC addresses to identify the devices and associating them to the users where a user identity was required. The privacy implications of a fixed, publicly visible identity across all networks resulted in the introduction of randomized and changing MAC addresses (RCMs) which were written into the 802.11 standards in 2016, and into WFA WPA3 certification standards in 2020. RCMs have the potential to cause many issues in those networks where MAC is being used to identify devices or users to higher network or application layers.

9.1 Evolution of the technologies that have led to this point

Since MAC addresses were first used for Wi-Fi device identification, more secure authentication mechanisms have been introduced. For basic authentication, starting with WEP and its WPA-PSK successors, a pre-shared secret is exchanged over a secure connection. This has since been augmented with mechanisms to allow multiple PSKs on the same network, resulting in PPSK. On the enterprise side, the 802.1X protocol used for securing wired networks has been incorporated into Wi-Fi through WPA2/3-Enterprise. In this configuration credentials, often including certificates, are transmitted securely to a trusted authentication server which can even be remote to the network and operated by an independent Identity Provider.

At the same time, mechanisms that can be used in association with a MAC address have been devised to allow a service provider to identify the user. The first of these was the captive portal, where a user must enter some information (such as a username and password) that is then checked before access to the network is granted for a period of time for the device MAC address. With the advent of mobile device that run ‘Apps’, another channel similar to the captive portal has opened up. In this case the device and the network exchange information before granting access to services.

Device fingerprinting technologies have also been developed and evolved to the point where they are reliable for many use-cases. These identify devices by their behavior at radio or network traffic levels without any active participation on the part of the device.

9.2 Improvements in the service provided by networks as a result of these solutions

Amongst the improvements that these newer identification and authentication mechanisms provide are:

Ease of access – once the credentials or subscriptions are installed on the device or within the App, or the fingerprints have been created, they will persist until they are removed or expire. The device can automatically connect to those networks without user intervention (such as was required with a captive portal) and a change in MAC address between sessions will not be of any consequence to the user.

Security of Identity – In addition to being publicly visible, MAC addresses are easily spoofed and are not a reliable identifier. The replacements all provide user or device identities that are not public and are transmitted securely to the identification service.

Privacy – the user or device identities are not visible to the network outside of the identification service and in particular are not publicly visible to 3rd parties. In many cases they will be unique to the network and so tracking between networks will not be practical in the absence of a fixed MAC address. Where personally identifiable information is sought or collected, the user should as far as possible be asked to consent to the collection and without unnecessary information being demanded as a condition of providing service.

Roaming – where an identification service is used, the user may be identified as having access to a consortium of networks with different network identities and operators without any additional provisioning being required to access newly visited networks.

9.3 Brief outline of the verticals and the effects on them of RCM

The issues introduced by RCM are the consequences of the inability to identify a device uniquely beyond an individual session. Any device identified solely by its MAC will appear as a different device on each network and potentially also for each session on the same network.

Any restrictions or privileges based on MAC, such as a premium QoS, or restrictions on access to services (e.g., 'parental controls') will also last only for the session and will have to be re-established every time.

Any diagnostics or device steering relying on seeing an unassociated device or requiring consideration of device behavior over prolonged time periods will also not be able to function.

For any networks using a captive-portal style login page, the user will have to log into the authentication portal each time the MAC changes in order to connect, and potentially every session, which is likely to result in the user having a low opinion of the service.

Particularly in the case of networks where a captive portal and MAC identity was used, replacing it with a credential stored on the device will introduce a device management burden, much of which will fall on the user who may be unfamiliar with the mechanisms and terminology for installing credentials on the device.

For networks where an 802.1X-based solution is already implemented, the consequences of RCM will range between not being able to impose device-specific restrictions (where a user credential is being used) to an absence of continuity of device identification for diagnostic and management purposes. There is also the further issue of associating the AAA response; which may be from a 3rd-party identification service; to any identity required by the network for management purposes – such as offering premium service levels for particular classes of user.

9.4 Brief outline of the menu of solutions

The solutions already available to relieve reliance on MAC addresses all have their particular strengths and weaknesses:

- WPA2 & WPA3 Enterprise with 802.1X authentication is used for systems with the resource to perform network management and where a high level of security and a unique device or user identity is required. Typically for large-scale or corporate networks. Initial installation of the credential may impose a burden on the user and/or support staff.
- Passpoint and OpenRoaming – as above
- Easy Connect will be suitable for home and factory networks and IoT devices but complete implementations are not yet widely available on APs or clients.
- 802.1AR Secure Device Identifier (DevID) – unique, secure device ID. Availability and mechanisms for use are not widely understood.
- External Identifiers / Proprietary Identifiers – not portable between networks. App-based solutions introduce the issue of availability for particular device categories and may face user reluctance if there are many of them.
- PPSK – solutions implemented on the network side, but not yet standardized. Supported by any device that supports PSK.
- Device Fingerprinting - proprietary solutions implemented on the network side. Device support not required but may not deliver a completely unique identity and may sometimes give a device multiple identities, particularly for networks with large numbers of devices that do not connect frequently.
- Doing Nothing – remaining with a MAC-based approach can be an acceptable approach where connections are typically only used for a single session and security is not a significant issue, or where a unique device identity is only needed at a higher layer (any system where the device registers its presence and communicates with a central authority). Where applicable, users should be made aware of any privacy and security issues.

10 Conclusions

The introduction of per-SSID, daily, and per-session MAC randomization to Wi-Fi networks is designed to improve the privacy of the user but it can cause problems for the provision of services that need to uniquely identify the devices; or the users in those cases where the identity of the device is used as a proxy for the identity of the user.

Fortunately, there are several established technologies that are freely available and can remediate these issues in the majority of cases and these not only offer improvements to privacy but also to security and user experience.

The paper details the requirements and the available solutions for many cases and has made recommendations for solutions across different verticals that a network operator may wish to adopt to overcome the issues introduced by MAC randomization. There are a few cases in network diagnostics and management where a network may have a need to identify some unassociated devices persistently, and these are not resolved by any of the methods described in this whitepaper.

The WBA has identified randomized MAC addresses as an impact on deployments of Wi-Fi networks and has been in contact with standards organizations to address the issues surrounding MAC randomization. The WBA has presented and shared the work and findings regarding the situations in which MAC address randomization can cause problems and will to update the other standards organizations with any relevant information. The standards organizations that are addressing MAC randomization are the IETF through its MADINAS workstream, and the IEEE 802.11bh task-group.

Within this paper, also discussed is the need for identities and the legal necessity to consider privacy and consent when identifying people. The requirement for a network operator to establish a true user identity in certain jurisdictions is outside of the domain of Wi-Fi device identities and so it is not addressed directly, but is not diminished, by any of the solutions presented here.

Additional activities that the WBA is doing include the collection of information beyond that which was originally collected to describe device behavior in the presence of a captive portal and which may be useful to its members. These could include recording device support for Wi-Fi Easy Connect, Passpoint R1/2, Capport (rfc8908/rfc8910), and DevID (802.1ar).

The WBA continues to monitor the progress of initiatives by other standards bodies relating to Wi-Fi device and user identification and inform its members of any significant developments.

Consequently, WBA roadmap will include prominent activities addressing these topics and invite the industry to engage, for more information please contact the WBA: contactus@wballiance.com

WIRELESS
BROADBAND
ALLIANCE

REFERENCES

IEEE Std 802.1AR™-2018 IEEE Standard for Local and Metropolitan Area Networks - Secure Device Identity

IEEE SA - P802.11bh - Standard for Information Technology--Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment: *Operation with Randomized and Changing MAC Addresses*

IEEE SA - P802.11bi - Standard for Information Technology--Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment: *Enhanced Service with Data Privacy Protection*

IETF Capport Architecture - **RFC 8908 - Captive Portal API (ietf.org)** and **RFC 8910 - Captive-Portal Identification in DHCP and Router Advertisements (RAs) (ietf.org)**

IETF MADINAS workgroup - MAC Address Device Identification for Network and Application Services

Passpoint® Specification **v3.2** - login required. (or see **Passpoint | Wi-Fi Alliance** for overview)

Wi-Fi Easy Connect™ Specification **Version 2.0** - login required. (or see **Wi-Fi Easy Connect | Wi-Fi Alliance** for overview)

PARTICIPANT LIST

NAME	COMPANY	ROLE
Tim Twell	BT	Project Leader & Chief Editor
Luther Smith	CableLabs	Project Co-Leader
Alex Meub	Eleven Software	Project Co-Leader
Jim Palmer	CommScope	Editorial Team
Tim Colleran	LEVL	Editorial Team
Thierry Van de Velde	Nokia	Editorial Team
Pedro Mouta	WBA	Editorial Team
Irfan Acar	AirTies	Project Participant
Peter Thornycroft	Aruba, an HPE company	Project Participant
Paul Hancock	AT&T	Project Participant
Brian Shields	Boingo Wireless	Project Participant
Kishore Raja	Boingo Wireless	Project Participant
Peter Barany	Boingo Wireless	Project Participant
Sandeep Agrawal	CDOT	Project Participant
Jason Weil	Charter Communications	Project Participant

For other publications please visit:
wballiance.com/resources/wba-white-papers

To participate in future projects, please contact:
pmo@wballiance.com

READ MORE

Loay Kreishan	Charter Communications	Project Participant
Jerome Henry	Cisco	Project Participant
Mark Grayson	Cisco	Project Participant
Deepak Tripathi	CommScope	Project Participant
Mark Hamilton	CommScope	Project Participant
Edmond Sam	Datavalet	Project Participant
Ahmed Hafez	Deutsche Telekom	Project Participant
Hideaki Goto	Eduroam	Project Participant
Karen Quinn	Eleven Software	Project Participant
Hai Shalom	Google	Project Participant
Po-Kai Huang	Intel Corporation	Project Participant
Edward Wincott	Jisc	Project Participant
Olivier Mayor	Meta	Project Participant
Max Riegel	Nokia	Project Participant
Malay Vadher	Plume	Project Participant
Vasudevan Nagendra	Plume	Project Participant
George Hart	Rogers	Project Participant

For other publications please visit:
wballiance.com/resources/wba-white-papers

To participate in future projects, please contact:
pmo@wballiance.com

READ MORE

Michael Sym	Single Digits	Project Participant
Ryan Blossom	Single Digits	Project Participant
Ceyhun Kumus	Turkcell	Project Participant
Anton Monk	Viasat	Project Participant
Bruno Tomás	WBA	Project Participant
Jonah Ross	WBA	Project Participant
Tiago Rodrigues	WBA	Project Participant

For other publications please visit:
wballiance.com/resources/wba-white-papers

To participate in future projects, please contact:
pmo@wballiance.com

READ MORE