Wi-Fi Security Guidelines

Advancing Trust, Privacy, and Seamless Wi-Fi Roaming Across Global Networks

Source: Wireless Broadband Alliance

Authors: Wi-Fi Security Project Group

Issue Date: April 2026

Version: 1.0.0

Status: Public

For other publications, visit our website here

To participate in further projects, contact pmo@wballiance.com

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 WBA is to drive seamless, interoperable Wi-Fi services experiences within the global wireless ecosystem. The WBA's mission is to bring together global industry leaders, collaborating to accelerate the development, integration and adoption of next-generation Wi-Fi and wireless technologies to deliver business growth, through innovation, technical and standards development, and real-world deployment programs. Its key programs include NextGen Wi-Fi, OpenRoaming, 5G, 6G, IoT, Smart Cities, Testing & Interoperability and Policy & Regulatory Affairs.

Membership in the WBA includes major operators, service providers, enterprises, hardware and software vendors, and other prominent companies that support the ecosystems from around the world. The WBA Board comprises influential organizations such as Airties, AT&T, Boingo Wireless, Boldyn Networks, BT, Charter Communications, Cisco Systems, Comcast, HFCL, HPE, Intel, Reliance Jio, RUCKUS Networks, Telecom Deutschland and Turk Telekom.

Follow Wireless Broadband Alliance:

www.twitter.com/wballiance

http://www.facebook.com/WirelessBroadbandAlliance

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

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.

Table of Contents

1. Executive Summary 6
2. Definitions 7
3. Introduction 7
4. Authentication and Access Control 9
5. Strong Encryption and Integrity 13
6. Identity Privacy 15
   - 6.1 EAP-TLS 17
   - 6.2 EAP-TTLS 17
   - 6.3 EAP-SIM 18
   - 6.4 EAP-AKA 19
   - 6.5 EAP-AKA' 19
7. Credential Storage 20
   - 7.1 User Credential Device Storage 20
   - 7.2 User Credential Secure Storage 20
   - 7.3 Securing Data at Rest 21
8. Access Network Providers (ANP) Security 21
   - 8.1 Physical Security 21
   - 8.2 Over-the-wire AP Security 22
   - 8.3 Backhaul Security 23
   - 8.4 RADIUS Transport Security 24
9. Roaming and Hub Security 24
10. Additional Layer 2 (L2) Security Features 25
    - 10.1 L2 Traffic Inspection and Filtering 25
    - 10.2 Deactivation of Broadcast / Multicast Functionality 26
11. Conclusion 26

Appendix 27

A1 - Introduction 27

A2 – EAP Walkthrough 28

A3 – Platform Adoption 29

A4 – An Overview of Other EAP Methods 29

A4.1 EAP-FAST/TEAP 30

A4.2 FIDO-Based EAP Method 30

A4.3 EAP-CREDS 30

A4.4 EAP-PPT 31

A4.5 EAP-TLS as an inner method 31

A5 – Additional Ladder Diagrams 31

A6 – Post Quantum EAP Methods 35

References 36

Participants List 37

1. Executive Summary

Security and privacy are important concepts in any network. There are best practice guides available today to ensure Wi-Fi security - from the client computer to the network equipment and backend servers. It is crucial that service providers, network providers, and identity providers follow these best practices and ensure that customer data is secure.

The WBA has established the OpenRoaming service framework built on top of the Wi-Fi Alliance's Passpoint technical specification. These are leading to the deployment of the most up-to-date, secure, and standards-based protocols for Wi-Fi networks including authentication, encryption, and privacy, particularly relevant to protect Public and Guest experiences. Properly supporting these protocols makes both users and operators resistant to security risks associated with over-the-air wireless communications and network-to-network exchange of authentication credentials and roaming signalling.

There are measures that operators can take to further mitigate risks. Access Network Providers (ANP) can improve the physical security of the Access Points (APs), properly handle the management and authentication of their wireless systems, and be able to circumvent the latest security threats.

Identity Providers (IDP) can take further measures to ensure that the hub and inter-connecting networks between roaming partners are secure. Operators can establish RadSec or VPN connections with roaming partners to protect the exchanged messages.

Other measures can be taken to ensure the Layer-2 communication between the client and the network is secured, by supporting Layer 2 (L2) traffic inspection and deactivating broadcast/multicast functionality.

The objective of the WBA's Wi-Fi Security program and guidelines herein is to ensure that the highest possible security standards are being built into the fundamental design of future Wi-Fi networks and roaming scenarios.

2. Definitions

Acronym	Definition / Context
AAA	AAA refers to Authentication, Authorization, and Accounting, a security framework that controls and tracks user access to network resources by verifying identities, granting permissions, and logging activity.
EAP	Extensible Authentication Protocol (EAP) is an authentication framework that allows for the use of different authentication methods passed over 802.1X and RADIUS for secure network access to wireless networks.
NAI	The Network Access Identifier (NAI), defined in RFC 7542, is a format used in the RADIUS User-Name attribute to describe the routing of authentication requests by a user or client device. [9]
NGH	Next Generation Hotspot (NGH) was a term coined by the WBA that refers to the combination of Passpoint, as an automatic association technology, with the Wi-Fi Roaming principles and best practices defined in the WBA Wireless Roaming Intermediary eXchange (WRIX) framework. The concept was deprecated back in 2020 to avoid terminology confusion and facilitate Passpoint adoption.
Passpoint	Passpoint(R) is a commercial term that refers to a Technical Specification and Certification from the Wi-Fi Alliance - previously known as 'Hotspot 2.0'. Passpoint is based on the IEEE 802.11u standard that defines the mechanism from which a device can attach automatically and securely to a Wi-Fi network without user interaction.
RADIUS	Remote Authentication Dial-In User Service is a protocol for managing network access. It enables centralized Authentication, Authorization, and Accounting (AAA) for users attempting to access a remote network. It operates using a client-server model in which, the server component it validates user credentials and policies and, the client component (e.g., access points, routers, switches, VPN gateways), connects users to the network, but only with the authorization of the RADIUS server. Additionally, the server collects session usage in the form of accounting records.
WBA OpenRoaming	OpenRoaming™ refers to a federative solution and ecosystem that scales the way Passpoint networks and credential holders interact without requiring a custom, peer-to-peer roaming relationship.
Wi-Fi Roaming	Generically speaking, Wi-Fi Roaming refers to the concept of an end-user being able to 'roam' from one Wi-Fi network to another Wi-Fi network (or even another radio access technology) in an automated fashion and without any required manual action.
WPA	Wireless Protected Access (WPA) is a security standard certified by the Wi-Fi Alliance. WPA is used to protect the user data and ensure secure authentication over wireless networks. The standard has evolved to multiple revisions such as WPA2 and WPA3, with specific modes such as Personal and Enterprise. WPA is a core component of Passpoint technology and, thus, OpenRoaming.
WRIX [10]	The Wireless Roaming Intermediary eXchange (WRIX) Framework is a set of Wi-Fi Roaming documents that compile standards and best practices for implementing and conducting a Wi-Fi Roaming business, agnostic to the underlying vendor technologies used.

3. Introduction

Currently, several network operators are leveraging Wi-Fi as a key component of their wireless data strategy, not only because of the characteristics of the technology which makes it one of the most widely deployed, but also because of recent developments that have enhanced Wi-Fi to become more secure and seamless for purposes of offloading 3GPP based public networks and optimizing client connectivity experiences. Properly managed Access Network Provider (ANP) networks also ensure that service

providers can meet any legal and governmental requirements around recordkeeping within a particular market.

This whitepaper covers Wi-Fi Security, taking into consideration a broad and comprehensive perspective, and explores key security features involved in Passpoint & OpenRoaming network deployments. In addition, this paper explores complementary security solutions that service providers can implement to enhance their end-users' security.

Since 2020, a new standards-based Wi-Fi roaming framework has arisen called WBA OpenRoaming™. OpenRoaming refers to a federated solution and ecosystem that scales the way Passpoint networks and user credentials interact with each other without requiring an individual peer-to-peer roaming relationship to be established. OpenRoaming leverages Passpoint as its underlying technology, and includes additional concepts of Dynamic Peer Discovery (DPD) for scalability and RadSec for security and interconnection. OpenRoaming exemplifies an industry comprehensive solution widely deployed in Wi-Fi networks, and used for IOT devices in convergence with cellular networks.

OpenRoaming incorporates the best Roaming and Security principles defined in the WBA Wireless Roaming Intermediary eXchange (WRIX) framework and its accompanying legal framework which aligns the trust agreements between federation players to avoid intrusive behaviors by users.

The WBA OpenRoaming Legal Framework can be downloaded by WBA members via the WBA extranet. (link HERE).

This white paper is organized into chapters which cover the following topics:

- **Authentication and Access Control**. Choosing the most widely demonstrated secure and standard mutual authentication protocols in the industry. Supporting these authentication protocols from an end-to-end perspective enables only valid mobile devices successfully connect to a Wi-Fi network and prevents them from connecting to rogue networks.
- **Strong Encryption and Integrity**. Selecting the most widely demonstrated standards-based secure encryption and integrity protocols used in industry today.
- **Identity Privacy**. Following relevant recommendations to various Extensible Authentication Protocol (EAP) methods such that user identity privacy can be preserved.
- **Credential Storage.** Ensuring the safe and secure storage of credentials in the network, both while in use and at rest.
- **Access Network Providers (ANP) Security**. Guaranteeing the secure operation of Wi-Fi roaming relies on proper AP security management and authentication, as well as backhaul network security.
- **Roaming and Hub Security**. Establishing guidelines for a hub connection between roaming partners to ensure the required security level can be contractually determined and enforced in both cases of a direct network connection between home IDP and visited ANP and where a hub is used.
- **Additional Layer 2 (L2) Security**. Warranting that networks use secure authentication and access control in addition to strong encryption and integrity, including L2 traffic inspection and filtering, and the ability to disable multicast/broadcast traffic.

It is important to state that there may be rules and regulations from regulatory authorities or law enforcement agencies that are applicable in various unique jurisdictions. Where applied, these rules and regulations supersede any information contained herein.

4. Authentication and Access Control

Well-operated network systems require robust authentication mechanisms. Mobile devices must ensure that the network to which they are trying to connect can securely exchange authentication signalling with their credential provider. The access network must, in turn, make sure that the mobile device is authenticated before it uses any network resources. The access network delegates the authorization of services to the mobile device's RADIUS server which is responsible for authenticating the client. Before transmitting its credential, the client validates the server, typically using a certificate. On successful receipt of the client credential, the server validates the client credential prior to authorizing or denying the service. This is called "Mutual Authentication". Mutual authentication is often realized by a combination of "Server Authentication" and "User/Client Authentication".

Access Control is the way to control the accessibility of network resources. Access Control is required to execute the mutual authentication results to ensure that only authenticated devices can access the network resources. Taking advantage of the existing extensible authentication and access control framework defined by the IETF and IEEE and in the WPA2 and WPA3-Enterprise certification programs, modern Wi-Fi networks can provide strong mutual authentication and access control capabilities. Passpoint is an example of a certification that successfully does this.

It is appropriate to have a basic understanding of the EAP authentication process that is leveraged throughout this Document, and the industry in general. Diagram 4-1 displays an overview of the 802.1X/EAP process. This process is critical to enterprise grade secure wireless networking. A client (Supplicant) connects to the AP (Authenticator) using wireless. The client initiates the connection to a wireless port, using 802.1X, and the AP forwards the connection request through to a RADIUS server (Authentication Server).

As seen in the diagram, the RADIUS server does not always store the user credentials, these are typically stored in an external database that may leverage Lightweight Directory Access Protocol (LDAP) or Structured Query Language (SQL).

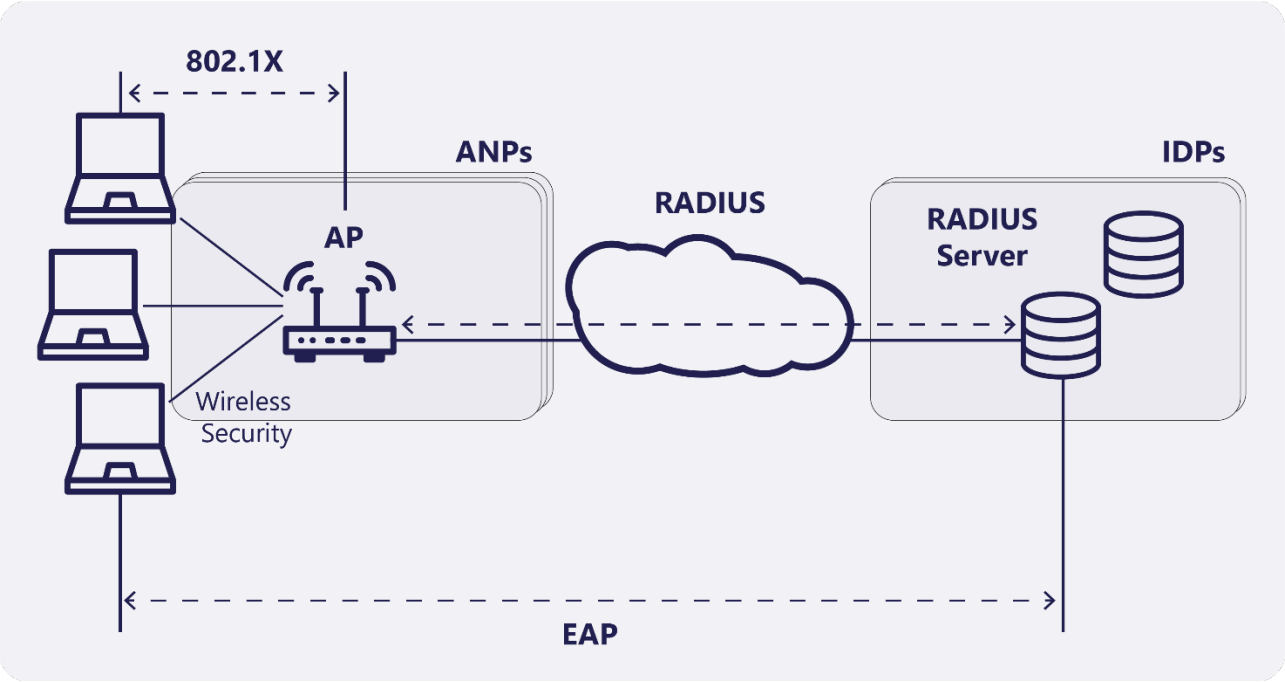

Diagram 4-1 Overview of the 802.1X/EAP Process

Only the most secure EAP authentication method types should be used to convey private credential information during authentication. Modern EAP Authentication Methods have been designed with security in mind, but often there are additional steps which must be performed to ensure trusted communications and identity privacy between the Supplicant and its Home Authentication Server. When choosing a secure method for EAP, the administrator can be faced with many options. The choice that is made should reflect the type of business and type of credential being used for authentication.

Credentials and related EAP methods that are certified by Passpoint are described in Table 4-1. Passpoint-compliant APs should be able to support all EAP methods and credential types listed in Table 4-1.

Credential Type	EAP Method
Certificate	EAP-TLS[4]
SIM/USIM	EAP-SIM [6], EAP-AKA [7], EAP-AKA' [8]
Username/Password (with server-side certificate)	EAP-TTLS [5] with MSCHAPv2 as inner method

Table 4-2 Passpoint Certified Credential Types and EAP Method

It should be noted that this table is not exhaustive since there are other EAP methods available for use with a variety of credential types. While these methods are not specifically tested by the Wi-Fi Alliance for

Passpoint certification, several methods are commonly used and implemented on a variety of devices and recognized by Passpoint-capable systems. There is no prohibition in the use of commonly implemented EAP Authentication Methods if the RADIUS implementation which conveys the end-to-end conversation complies with the required service and security requirements of the Passpoint system, such as Identity Privacy and Key Generation outlined herein.

It is important that mobile devices with SIM/USIM support all EAP methods listed in Table 4-1 and their associated credential types.

Credential and EAP methods that are commonly used, particularly in the Enterprise, but not explicitly certified in Passpoint are described in Table 4-2.

Credential Type	EAP Method
Certificate	EAP-TTLS [5] with EAP-TLS as inner method PEAP with EAP-TLS as inner method
SIM/USIM	PEAP with EAP-SIM, EAP-AKA, EAP-AKA' as inner method
Username/Password	EAP-TTLS [5] with PAP (non-EAP inner method) EAP-PWD PEAP with MSCHAPv2 as inner method)
Token	EAP-TTLS with EAP-GTC as inner method PEAP with EAP-GTC as inner method

Table 4-2 Common Credential Types and EAP Methods

Careful consideration should be given when choosing these commonly implemented methods regarding its security implications, whether over-the-wire or how the credential is stored. Particular attention should be paid to the proper identification and 'binding' of security trust points (Root Certificates, Common Names and Subject Alternative Names) to ensure trusted private communications is used during the authentication process.

There are security implications as to how a credential is delivered and encrypted at rest and in motion when selecting a PAP versus MSCHAPv2 as an inner authentication method. Careful consideration should be given to balance these security implications with any business systems and service requirements.

When selecting a non-certified Passpoint EAP Authentication method, an IDP may have difficulty implementing their vision across all devices as individual vendors may or may not support the method. Other commonly used methods, such as using EAP-GTC, which is essentially an EAP-based version of PAP, involve challenges and prompts to the user in the User Interface and may have a broad variance in device implementation.

New EAP Authentication Methods are being developed by Industry. Emergent and Emerging Credential and EAP methods are under development to support a variety of modern business cases like Internet of Things and 3rd-party connection entitlements. These methods are described in overview in Table 4-3, and in more details in *Appendix A4 – An Overview of Other EAP Methods* – An Overview of Other EAP Methods. These methods are included in this Document as an informational resource and should be considered prototypical at this time without broad adoption on devices and handsets. Careful consideration should be given in the selection of these methods, appropriate to your use case, as its implementation on devices may be severely limited.

Credential Type	EAP Method
Certificate	EAP-FAST with EAP-TLS as inner method EAP-TEAP with EAP-TLS as inner method EAP-CREDS with EAP-TLS as inner method
SIM/USIM	
Username/Password	EAP-CREDS with username/password as inner method
Token	EAP-PPT with attestation blob as inner method
FDO	EAP-FIDO with FIDO-2 credential as inner method [18]

Table 4-3 Emergent and Emerging Credential Types and EAP Methods

All the protocols listed in Table 4-1 Provide the following security features from RFC 3748 [3], (RFC 5448 [8] for EAP-AKA'):

- **Mutual Authentication:** This refers to an EAP method in which, within an interlocked exchange, the authenticator authenticates the peer, and the peer authenticates the authenticator.
- **Integrity Protection:** This refers to providing data origin authentication and protection against unauthorized modification of information for EAP packets (including EAP Requests and Responses).
- **Relay Protection:** This refers to protection against replay attacks on an EAP method or its messages, including success and failure result indications.
- **Confidentiality:** This refers to encryption of EAP messages, including EAP Requests and Responses, and success and failure result indications. A method making this claim MUST support identity protection.
- **Key Derivation:** This refers to the ability of the EAP method to derive exportable keying material, such as the Master Session Key (MSK). The MSK is used only for further key derivation, not directly for protection of the EAP conversation or subsequent data.
- **Fast Reconnect**: The ability, in the case where a security association has been previously established, to create a new or refreshed security association more efficiently, or in a smaller number of round-trips.

- **Session Independence:** The demonstration that passive attacks (such as capture of the EAP conversation) or active attacks (including compromise of the MSK) does not enable compromise of subsequent or prior MSKs.

For tunnel-based EAP authentication methods like EAP-TTLS, additional security properties should be considered:

- **Channel Binding:** is a concept that ties authentication information within a secured EAP channel to ensure that the authentication information cannot be reused or misdirected by a third-party.
- **Cryptographic Binding:** This refers to protection against man-in-the-middle attacks by ensuring that a single entity has acted as the EAP server for all methods executed within a tunnel method, and the resulting keying information from the method are transmitted through separate channels.

Note that these are the original RFCs. Some have been updated since they were first introduced.

For access control, IEEE 802.1X defines two logical port entities: the "controlled port" and the "uncontrolled port". The controlled port is manipulated by the 802.1X PAE (Port Access Entity) to allow (in the authorized state) or prevent (in the unauthorized state) ingress traffic to and egress traffic from the controlled port. The uncontrolled port is used by the 802.1X PAE to transmit and receive EAPOL frames that carry the authentication process messages. In Wi-Fi this is known as WPA2-Enterprise or WPA3-Enterprise.

WBA OpenRoaming builds on this framework. The port-authorized service for an authenticated device is signaled between an Access Network Provider (ANP) and an Identity Provider (IDP) using the RADIUS RFC 2865 [28] defined filter-id attribute to enforce service selection, and RADIUS RFC 3579 [29] defined EAP-Message to conduct a supplicant's EAP authentication method between them.

In summary, these EAP methods combined with Passpoint, enable the most widely demonstrated secure and standard mutual authentication protocols used for Wi-Fi access in the industry today.

Supporting these authentication protocols not only filters out unauthorized or invalid mobile devices, but also protects the mobile devices from connecting to rogue APs and securely encrypts the Wi-Fi link layer to protect against snooping.

5. Strong Encryption and Integrity

Encryption and integrity of the Wi-Fi links is based on the WPA2-Enterprise and WPA3-Enterprise specifications, which provide both a strong standard encryption algorithms and encryption protocols. Passpoint, uses these protocols at its core.

Advanced Encryption Standard (AES) is defined as a Federal Information Processing Standard (FIPS Publication 197) and is the first publicly available encryption mechanism that meets the requirements of the US government for protecting sensitive and classified information. To date, AES has proven to be

extremely resilient in the face of the high number of published attacks triggered by AES's broad adoption. The data travelling across a WPA2/WPA3 network is encrypted by AES to provide the most advanced standards-based data encryption method available today. AES support is required by many protocols and applications used worldwide in enterprise networks.

IEEE 802.11i and WPA2 mandate the use of Counter Mode with CBC MAC Protocol (CCMP), an encryption protocol in which the same key is used for both encryption and integrity protection using AES. AES is used with a block cipher that operates with multiple key lengths and block sizes. IEEE 802.11i and WPA2 mandate the usage of AES with 128-bit keys and 128-bit blocks. The AES encryption keys are derived using the four-way handshake (defined by the IEEE 802.11i key management protocol). These keys are derived from the PTK (Pairwise Transient Key) that, in turn, is derived from the per-session MSK established by the authentication process.

WPA3 extends the key-size to 256 bits and includes Galois/Counter Mode Protection (GCMP). GCM is an alternate block cipher providing authenticated encryption. It can be implemented in hardware to achieve high speeds with low cost and low latency.

The inclusion of AES within WPA2/WPA3 gives Wi-Fi users access to one of the most widely tested and widely applied encryption standards. Today, AES is used across multiple data transport technologies, including 5G, and has withstood extensive scrutiny by cryptographers.

WPA3-Enterprise is an improved specification of WPA2-Enterprise. Wi-Fi uses three different frame categories: Management, Control, and Data. Among these, Protected Management Frame (PMF) protects the management frames containing authentication, de-authentication, association, and disassociation messages, beacons, and probes frames. Without the PMF feature, all management frames are sent unprotected, making the connections vulnerable to aspects of both denial-of-service and man-in-the-middle attacks. The PMF is implemented based on the IEEE 802.11w amendment. WPA3 mandates the PMF feature.

In the 6 GHz band of Wi-Fi 6E and Wi-Fi 7, support of WPA3 is mandatory.

There is a feature prevalent with security called "Transition Mode". This is where a new protocol will still allow the use of an older (and possibly outdated) protocol, so that legacy devices can continue to connect using these older protocols, while connecting to networks that offer newer more robust protocols. Although this is a very convenient feature, allowing for more backwards compatibility, it does suffer from some issues: firstly it slows down the urgency to upgrade; secondly it may compromise security, as the new features are being disabled for convenience; finally, it lulls operators and managers of systems into believing that they are using up-to-date security practices, but they are actually not!

There is another form of Transition Mode, where APs can be configured for backwards compatibility by choosing the WPA2-Enterprise mode and setting the PMF mode to "optional" instead of "required". This setting allows legacy devices supporting WPA2-Enterprise without PMF support to be able to connect, although this connection is not always guaranteed due to client limitations.

WPA3 optionally provides a higher level of security by using the cipher suite originally defined by the NSA as Suite-B or the Commercial National Security Algorithm (CNSA). This mode is known as "WPA3-Enterprise 192-bit mode", because the cryptographic strength is 192 bits. Only EAP-TLS is supported. As of this writing, the user devices supporting WPA3-192 mode are still limited. Hence, WPA3-192 may not be a good choice for Public Wi-Fi use cases that expect a wide range of users and devices. However, this is expected to change as the protocol matures.

One concern moving forward is the oncoming Quantum Computing which, it is feared, may be used to compromise existing security protocols. As of this writing, the NSA has launched CNSA v2 which is intended to develop Quantum Resistant security algorithms. In April 2025, IEEE 802.11 formed a new Post Quantum Cryptography (PQC) study group. The PQC SG is focused on developing encryption algorithms that secure against attacks from quantum computers. The current security protocols (used by Wi-Fi, TLS, certificates) rely on asymmetric key algorithms (e.g., RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography) that become unsecure once quantum computers become a reality. Whereas EAP-TLSv1.3 and EAP-AKA can be enhanced by IETF to support the new quantum resistant Key Encapsulation Mechanisms (KEMs), other 802.11 defined asymmetric key exchanges are vulnerable and need to be enhanced by IEEE:

- Fast Initial Link Setup (FILS): use cases include Carrier Wi-Fi that benefit from reduced setup time, e.g., deployments in crowded train station environments.
- Simultaneous Authentication of Equals (SAE): password-based authentication not used in Carrier Wi-Fi deployments.
- Opportunistic Wireless Encryption (OWE): provides encryption for open networks and not used in Carrier Wi-Fi deployments.

In summary, these protocols provide the most evaluated and widely demonstrated encryption and integrity protection mechanisms. Through the correct use of these protection mechanisms, operators can ensure data confidentiality and integrity.

6. Identity Privacy

Identity privacy ensures that the account information of an end-user's credential is not revealed during the EAP exchange over RADIUS between the ANP and an IDP. Identity privacy is an important consideration in deploying EAP-based authentication over a Wi-Fi network. Mechanisms exist in defined EAP methods to ensure that the identity of the end-user is conveyed only after secure communications is established between the supplicant and its home IDP. This section describes example deployment considerations to ensure that identity privacy is provided, by discussing Passpoint mechanisms which protect identity privacy.

Diagram 6-1 expands on what was seen earlier in Diagram 4-1.

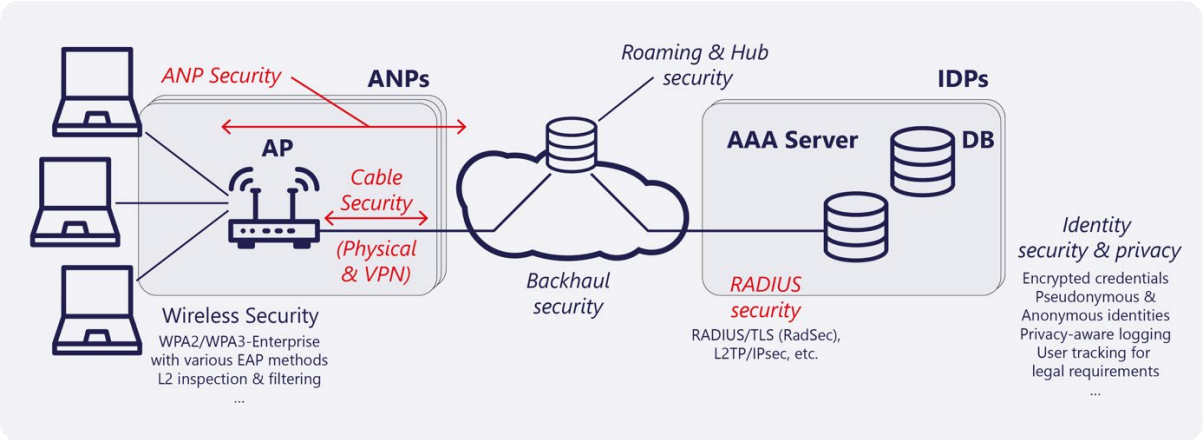

Diagram 6-1 Service Provider view of the 802.1X/EAP

In a typical service provider environment, security considerations must include the connections from the AP (authenticator) to the RADIUS server (also known as the AAA server), as well as the backhaul security. Diagram 6-1 shows the importance of cable security, ANP security, Roaming and Hub security, and backhaul security. These topics are covered in more detail in later Sections.

It is quite possible that the ANP, the backhaul provider, and the IDP may be three separate entities connected in a Roaming framework such as OpenRoaming.

The EAP exchange is expanded further in Appendix A5, including a ladder diagram, and a walkthrough of a simple EAP exchange.

In a Passpoint roaming scenario, the Network Access Identifier (NAI) is a format used in the RADIUS User-Name attribute to describe the routing of authentication requests by a user or client device. The NAI consists of two parts: user identity and realm, delimited by the "@" symbol. Since the EAP Authentication occurs prior to link encryption, this NAI must be transmitted without any Personally Identifiable Information (PII). In Passpoint, the NAI is defined to be transmitted in an anonymized form, where the user identity is replaced with the word 'anonymous', e.g. "anonymous@example.com". The realm portion describes the destination for the authentication request, e.g. the Identity Provider (IDP), and it is required by the Access Network Provider (ANP) and hub operators to discover, and subsequently route, authentication requests to the appropriate IDP's AAA server. This EAP Identity Response in the form of an NAI transmitted as the RADIUS User-Name thus initiates the Challenge/Response Extensible Authentication Method between the client device and IDP AAA which secures the credential information used to further authenticate and ultimately authorize or deny the Wi-Fi session. Using an anonymous EAP identity response to initiate secure client authentication ensures no PII is disclosed over the unsecured 802.1X.

For accounting purposes, or for user tracking and incident handling, the usage of Chargeable-User-Identity (CUI) [12] returned by the IDP is strongly recommended in order to accurately correlate sessions by the same user or device [14]. For privacy protection purposes, the value of the CUI should be unique

for each combination of end-user/ANP and the keys and/or initialization vectors used in creating the content of the CUI should be refreshed at least every 48 hours, but not more frequently than every 2 hours. Use of an opaque user identity returned in an Access-Accept is highly recommended to preserve user privacy, unless the user has agreed to share an immutable permanent identity among all operators involved during roaming use.

Below, you will find additional details of individual EAP methods and their ability to protect Personally Identifiable Information.

6.1 EAP-TLS

EAP-TLS is often recognized as the most secure method. However, some limitations exist. One such limitation is that the details of the client certificate may be disclosed to the ANPs and hubs brokering the authentication exchange, breaking anonymity. For example, the client's identity in the Subject could be used for user activity analysis as it is a persistent value for the connecting client (user). When TLS 1.2 is used, such disclosure is possible. By using TLS 1.3 (RFCs 8446 [34] and 9190 [35]), the client certificate is protected from observation by the ANP. Should TLS 1.2 be required in Public Wi-Fi use cases, you could compromise with a useful solution to combine the transport of an EAP-TLS 1.2 credential within an EAP-TTLS 1.3 tunnel as described later.

When EAP-TLS is used, it is recommended that implementations follow IETF recommendations to support privacy [4].

In a Passpoint scenario, utilization of an anonymous NAI [11] as the EAP-Response/Identity used as the RADIUS User-Name and transmitting the client certificate within a TLS handshake provides confidentiality, and avoids any disclosure of the certificate details. For example, an identity of the form anonymous@example.com can be included in the initial EAP-Response/Identity packet.

6.2 EAP-TTLS

EAP-TTLS is often recognized as a username/password-based authentication method. However, EAP-TTLS allows use of different inner authentication methods including certificates. EAP-TTLS with PAP (Password Authentication Protocol) as the inner method is probably the most widely deployed method used today. One might think that sending password in plaintext to the AAA server is unsecure, but this is offset through the use of a secure tunnel with the password securely transported over an encrypted TTLS application layer. This is known as a two-phase tunnelled EAP method. In EAP-TTLS with PAP, the AAA server must first be authenticated in phase 1 prior to the credential being passed to the server in phase 2.

The server authentication phase and its resulting TLS application layer are essential for providing end-to-end security. Furthermore, it is vital that the supplicant verify the presented server certificate in phase 1, either by Common Name (CN) or Subject Alternate Name (SAN) to ensure any credentials are transmitted to the correct home AAA server during phase 2.

EAP-TTLS with MSCHAPv2 as the inner method is also broadly used. However, MSCHAPv2 requires NThash on the AAA server and thus it is no longer considered secure for storing user credentials.

PEAP is a similar two-phase tunnelled method which was popular when Windows did not have native support of EAP-TTLS. Since most modern OS, including Windows, support EAP-TTLS today, there is little reason to choose PEAP over EAP-TTLS.

When EAP-TTLS is used, it is recommended that implementations follow IETF recommendations to preserve user anonymity [5].

The EAP-TTLS "outer" identity in phase 1 should, for example with Passpoint, use an identity in the form "anonymous@homerealm.com" as the initial EAP-Response packet. ANPs and roaming hub operators can see the Outer-Identity carrying the anonymous NAI used for routing to the IDP. The real identity, also in the form of an NAI is set as the Inner-Identity and securely transmitted to the AAA server via a tunnel protected by TLS.

As explained in the previous section, EAP-TLS has a limitation with respect to privacy protection. A useful compromise is to use EAP-TLS as the inner method of EAP-TTLS. (See also Appendix 4.5 The contents of the client certificate are protected by the TLS transport.

6.3 EAP-SIM

When EAP-SIM is used with Passpoint, it is recommended that implementations follow IETF recommendations to preserve user anonymity using temporary identities (Pseudonym Usernames and Fast re-authentication usernames) as defined in RFC 4186, Sections 4.2 and 12.2. The pseudonym identity is also defined in 3GPP TS 23.003, Section 19.3 [11].

In Wi-Fi roaming scenarios, the realm in the NAI of a supplicating EAP-SIM authentication has the format of @wlan.mncXXX.mccYYY.3gppnetwork.org, where XXX is the three-digit Mobile Network Code (MNC) and YYY the three-digit Mobile Country Code (MCC) used for routing back to the authentication server.

An example of pseudonym delivery using EAP-SIM is illustrated in Appendix A6.

When comparing different mobile SIM card-based EAP methods, EAP-SIM uses the original 2G defined Authentication and Key Agreement (AKA) which is based on a one-way authentication of the SIM card by the network operator. Details of the 2G AKA algorithm implementation were secret. The EAP-SIM authentication method addresses the limitations in the 2G AKA for use in Wi-Fi networks:

- Instead of 2G-AKA based one-way authentication, EAP-SIM specifies the use of mutual authentication by having the device send a random challenge (nonce) to the network and confirming the message authentication code returned by the network is valid.
- The use of a random challenge in the exchange avoids replay attacks.
- The 2G-AKA generated up to 64 bits of keying material. EAP-SIM runs the 2G-AKA algorithm 2 or 3 times and combines the keying material to produce the EAP Master Key (MK).

6.4 EAP-AKA

When EAP-AKA is used with Passpoint, it is recommended that implementations follow IETF recommendations to preserve user anonymity using temporary identities (Pseudonym Usernames and Fast re-authentication usernames) as defined in Section 4.1 of [7] and section 3 of [8]. The pseudonym identity is also defined in 3GPP TS 23.003, Section 19.3.

An example of pseudonym delivery using EAP-AKA is illustrated in Appendix A6.

Mobile devices typically support EAP-AKA as well as EAP-SIM.

For more information, please refer to the WBA document *IMSI Privacy Protection Technical Specification*. https://wballiance.com/resource/imsi-privacy-protection-for-wi-fi/

EAP-AKA uses the 3G defined Authentication and Key Agreement. Compared with 2G and 3G, EAP-AKA introduced mutual authentication between the SIM card and the cellular network. It also shifted to peer review of security algorithms, including the MILENAGE algorithm set for authentication and key agreement that generates up to 128 bits of key material. When comparing EAK-AKA with EAP-SIM, the key differences are:

- Uses native MILENAGE mutual authentication instead of random nonce.
- AKA integrates the use of sequence numbers to prevent replay attacks.
- 128-bit session keys are generated using a single authentication exchange.

6.5 EAP-AKA'

When EAP-AKA' is used with Passpoint, it is recommended that implementations follow IETF recommendations to preserve user anonymity through the use of temporary identities (Pseudonym Usernames and Fast re-authentication usernames) as defined in Section 4.1 of [7] and Section 3 of [8]. The pseudonym identity is also defined in 3GPP TS 23.003, Section 19.3.

A limitation to choosing EAP-AKA' as an authentication method is that it may not be supported by all mobile device manufacturers.

EAP-AKA' is an enhancement to the original EAP-AKA that includes the name of the access network in the key derivation procedures. This enhancement is to limit the effects of a compromised key which is now bound to a use in a particular access network. However, the use of the access network identity varies depending on use case:

- When EAP-AKA' is used in a 5G use case, 3GPP 24.501 specifies the use of serving Public Land Mobile Network (PLMN) network name in the key derivation, e.g., "5G:mnc015.mcc234.3gppnetwork.org".
- When EAP-AKA' is used in a WLAN use case, 3GPP 24.302 specifies that all WLAN exchanges shall use the fixed network name "WLAN" in the key derivation, effectively removing any benefits of the key compromise prevention enhancements in EAP-AKA'.

7. Credential Storage

7.1 User Credential Device Storage

SIM based EAP methods leverage the tamper resistant smart card to store high entropy user credentials (such as those that are difficult to guess or break and offer a high-level of security – usually being longer or made up of a diverse set of characters). Other EAP methods also need to securely store user EAP credentials on end-user devices.

For example, in iOS, user credentials can be stored using the keychain where the credential is encrypted and wrapped with its attribute information before storing. Keychain is a secure storage container provided by Apple that allows an application to store sensitive data such as passwords, encryption keys, and certificates. It is designed to be secure by default and ensures that data stored in it is encrypted.

For Android applications, the Android Keystore lets a Passpoint application store its own credentials, which only that app can access. The Android keystore provides a secure system level credential storage. With the keystore, an app can create a new Private/Public key pair and use this to encrypt application secrets before saving them in the private storage folders.

Other operating systems offer similar features to encrypt and protect stored sensitive information, such as passwords and secrets, and allow applications to securely access the encrypted data.

User credentials MUST NOT be stored as default user data. User credentials MUST be securely stored in an encrypted database, where possible. Access controls MUST prevent unauthorized users from accessing the securely stored user credentials.

7.2 User Credential Secure Storage

The IDP shall store the user credentials in a secure environment. There is a requirement to prevent access to credentials in the terminal, in APs, and in the service provider network. For example, passwords not only should be stored securely with a strong hash value on the user device, but also within the IDP's network including the user database that stores the end-user credentials.

Since IMSI encryption has become more prevalent in Wi-Fi access, specifically with EAP-AKA, EAP-SIM, and Passpoint, there may be a regulatory requirement to be able to identify specific users down to the device level. Specific examples of this could be for user charging, Lawful Intercept, or the ability to identify a user who was flagged for accessing Copyright material/content or conducting other unlawful activities. The IMSI is an identifier that can be used for this purpose.

However, to increase end-user privacy, this information is encrypted over the air when accessing Wi-Fi. The operator may still be required to get this association between the data session and the user and provide it to regulatory platforms either in real time or as part of historic logs. A mechanism to be able to do this should be based on the authentication process to a RADIUS platform that allows the encrypted IMSI to be decrypted. During this authentication, the association between the encrypted IMSI can be

made to the real IMSI and other characteristics of the data session such as the IP address of the user during that specific session. It would be expected that these abilities should be able to accommodate regulatory requirements for the specific region where the Wi-Fi service is being offered.

7.3 Securing Data at Rest

Data at rest refers to all digital information that is stored on physical or virtual media and not actively moving through networks. Security for data at rest is crucial to protect against unauthorized access and security breaches. Future updates to the WRIX framework will address these security measures to ensure protection for stored Wi-Fi session data.

8. Access Network Providers (ANP) Security

8.1 Physical Security

The physical wireless network as deployed in a roaming location can be roughly divided into three classes of equipment: the centralized controller (on-premises or cloud); the access points (APs); and the (communications/network) link between these two types of equipment.

A centralized controller is typically used to manage the network traffic, to monitor and manage APs, and to provide core configuration and authentication services. This entity is either present on-premises in a secure location or is housed in a data centre controlled by the ANP and connected using secure connections.

The network operator must ensure that unauthorized configuration changes cannot take place. This can be accomplished by restricting access to the controller, both physically and using industry standard security best practices.

APs should be deployed in locations that are as physically secure as possible, e.g. high on walls or on ceilings where the physical AP is not easily reachable, and in a tamper-proof enclosure. Lack of physical access makes it more difficult for a malicious entity to physically manipulate the AP. Access Points tend not to store security information locally and rely on a secured controller connection to function. If the physical security of an AP is compromised, it is not practically possible to exploit the stored information on the AP.

The link between the AP and the controller is formed by the in-venue network infrastructure, which can either be a wireless or wired network. It is common in modern deployments for all configuration and management network traffic between the AP and the controller to be encrypted. Even if a malicious entity were to gain access to the physical network, such access would be of no use without access to the controller as well.

8.2 Over-the-wire AP Security

Over-the-wire AP security is a part of Physical Security, intended for protecting user traffic especially, but may also include management and/or RADIUS traffic.

There are many deployment cases where APs are physically accessible by venue owners and/or users. For example, an ANP sends pre-configured, remote-controlled APs to end-users who connect the APs to their home networks. In such a deployment case, communications to and from the AP must be encrypted and protected. In addition, access to the device and its configuration must be protected from the end-user's intrusion. In addition, it may be crucial to protect the physical network wires terminating at the AP so that any end-users will not be able to gain access to the user traffic by eavesdropping on it. Although many protocols over the internet are designed to be secure, e.g. HTTPS, there are still many protocols that are not sufficiently secure or could potentially be vulnerable to privacy-compromising activities such as eavesdropping. Even if the radio communication of a Wi-Fi system is protected by strong encryption mechanisms of WPA2-Enterprise or WPA3-Enterprise, the lack of physical cable protection could jeopardize security and privacy.

It is recommended that APs should support a method to protect management and user data by implementing secure tunnelling of user traffic to its controller or using a fast VPN feature, preferably an open (non-proprietary) solution. AP vendors are strongly encouraged to add secure VPN support.

Special consideration is needed with respect to bandwidth. High bandwidth is especially important for Wi-Fi 6/6E and 7. Use of a VPN to backhaul user data may have significant impact on network bandwidth and performance. To mitigate performance degradation, VPNs over a long-haul network with high latency should be avoided as much as possible. One solution is to deploy a controller or a VPN gateway on-premises and introduce a Local Break-Out (LBO) network architecture. APs and VPN gateways must be equipped with a high-performance processor along with sufficient bandwidth.

These concepts are visualized in Diagram 8-1.

If secure tunnelling cannot be used, the wiring terminating at the AP should be physically protected so that no one can easily tap the wire or perform Man-in-the-Middle (MITM) attacks.

Operators participating in a Wi-Fi roaming system, including OpenRoaming, should take on-the-wire security into consideration to avoid jeopardizing the security and privacy protection of the entire system.

In a managed network environment, security can be enhanced by configuring 802.1X between the Wi-Fi Access Point and its Ethernet Switch. The AP acts as an 802.1X supplicant and is authenticated by the switch using an EAP method, e.g., EAP-TLS, PEAP or EAP-FAST. Beneficially, 802.1X can be used to establish shared MACSec keys, which are then used to secure the Ethernet interface between the Wi-Fi Access Point and the Ethernet switch.

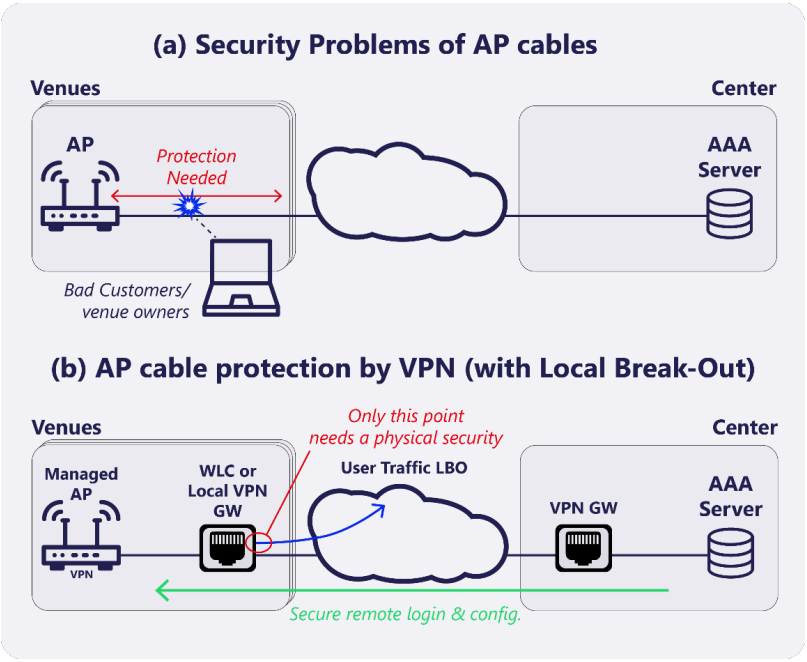

Diagram 8-1 AP Cable Security

8.3 Backhaul Security

Wi-Fi Roaming anticipates the offload of traffic destined for the Internet at the local hotspot, relying on built-in application security to protect this traffic on the Internet at large. The end-user MUST NOT solely rely on the wireless link encryption delivered by Passpoint/OpenRoaming for providing security of services accessed using the ANP's Wi-Fi network. It is recommended that users supplement their connection with VPN or tunnelling software. This approach provides for a generally acceptable level of security.

In certain network deployment scenarios, all network traffic originating from roaming networks is backhauled to a central hub location in a star network topology. Secure links must be deployed to connect the remote networks to the hub.

There is an additional provision for operator-specific traffic that should be backhauled to an operator's home network. For example, operator-specific services such as licensed specific content or traffic destined for a home operator's internal systems may be carried over a VPN tunnel originated from a network gateway and connected directly to the Identity Provider (IDP). Only traffic which meets the criteria and originates from an authenticated user of the IDP will be carried through such a tunnel.

This approach ensures that that the level of security for traffic over the access network is comparable to what the end-user would expect when using a typical cellular network.

In some deployment scenarios such as those using personal home commercial Wi-Fi solutions, the networks of the subscribers need protection. Without sufficient security if a visitor or a passerby connects

to your network and does something unlawful, you could be held responsible. With no security in place, any passerby could attack your local network. Separation of protected subscriber and convenient guest networks is highly recommended to avoid these problems.

8.4 RADIUS Transport Security

Protection of RADIUS traffic is crucial for both security and privacy protection.

Although EAP authentication methods transported by the RADIUS protocol generally have a security mechanism, the use of the original RADIUS (RFC 2865) protocol is considered insecure as much of the information is available in plain text. Furthermore, only certain attribute values are hashed using MD5, which has been shown to be easily compromised. This combined with the unencrypted RADIUS accounting creates privacy issues if sent over untrusted networks. RADIUS/TLS (RFC 6614 [30], also known as RadSec) and RADIUS/DTLS (RFC 7360 [31]) are secure transport protocols for RADIUS and their use is strongly recommended. In case RADIUS/TLS and RADIUS/DTLS are unavailable, the ANP should ensure the security of the RADIUS transport over untrusted networks with a modern secure VPN solution.

Unfortunately, some Wi-Fi equipment does not yet support RADIUS/TLS or RADIUS/DTLS. The Wi-Fi equipment vendors should strongly consider adding support for these RADIUS transport protocols, especially as the IETF is moving towards mandating deprecation of the older protocol. When implementing the RADIUS/TLS and RADIUS/DTLS support, the Wi-Fi equipment vendors should follow both the RFCs for the protocols (e.g. RFC 6614, RFC 7360) as well as RFCs concerning the proper use, configuration and validation of certificates (e.g. RFC 9325 - Recommendations for Secure Use of TLS and DTLS [32], RFC 9525- Service Identity in TLS [33]) to protect the RADIUS transport against attacks like Man-in-the-Middle. ANPs can reduce the risk for these attacks by using private certificate authority issued and strictly validated certificates to secure transport between Wi-Fi equipment and ANP RADIUS servers.

9. Roaming and Hub Security

The primary method of communication between ANPs, hubs and IDPs for AAA traffic is the RADIUS protocol as defined by the IETF. As indicated in the RADIUS Transport Security section above, on its own, this protocol provides limited security, however, the Passpoint specification in conjunction with the WBA WRIX Framework provides the security best practices for a roaming arrangement between two or more parties. The WRIX-I (Interconnect) specification requires that any connection between the ANP's network, any intermediary roaming/offload hub(s) and the home IDPs must be established securely from the ANP's network through to the IDP's AAA. This security is managed with either IPSec tunnels or via RadSec connections between the AP, Network Controller, ANP AAA proxy, Roaming Hub and the IDP. RadSec, based on Transport Layer Security (TLS) is increasingly required and utilized for roaming and offload because of the additional benefits associated with migrating RADIUS UDP signalling to session-based transport. While IPSec and RadSec are recommended and predominantly used, other options are

available and security requirements for other network options are described in more detail in "Section 1 IP Connectivity" of the WBA WRIX-I specification document. [10]

Entities establishing a secure connection over which the RADIUS traffic is exchanged are individually responsible for establishing the point-to-point connections. The IDP will work with the ANP and any hub operators on the security protocols and methods required to protect the AAA traffic. Hub providers are expected to enforce individual IDP security requirements for the connections they manage. For IDPs with many roaming agreements, use of a hub provides an integrated security solution.

In the case of OpenRoaming, the ANP, IDP, and any intermediary Roaming hubs must all adhere to the built-in security requirements of the OpenRoaming Federation. For more information on OpenRoaming's security requirements please refer to the OpenRoaming Technical Specification and the OpenRoaming Contract Framework documents. (link HERE)

10. Additional Layer 2 (L2) Security Features

Modern Passpoint networks support secure authentication and access control (see Section 4) in addition to strong encryption and integrity (see Section 5). They also commonly support L2 traffic inspection and filtering, and the ability to disable multicast/broadcast traffic as described below.

10.1 L2 Traffic Inspection and Filtering

L2 inspection and filtering prevents wireless frames, exchanged between two mobile devices, from being delivered by the Wi-Fi access network without first being inspected and potentially filtered in either the operator network or at its core. Such processing provides protection for mobile devices against some types of malicious attacks.

According to the Passpoint Specification, wireless systems should support inspection and filtering of data frames exchanged between mobile devices connected to the same Wi-Fi network. The inspection is targeted at identifying wireless frames matching a specific set of traffic filters in the entity performing the filtering. Only frames addressed to a certain mobile device from another mobile device that do not match the set of enabled filters are delivered to the addressed mobile device. The aim of the filtering is to provide protection of a mobile device from attacks by other mobile devices.

Proxy-ARP service, as per IEEE 802.11-2012, allows the AP to respond to an ARP request, on behalf of the client. This reduces broadcast traffic over the air. Generally, this is recommended on a Wi-Fi network. It can be used to prevent ARP spoofing attacks to a mobile device from another mobile device belonging to the same BSS or ESS.

It is considered best practice for network operators to deploy a firewall function in their Passpoint access network. The firewall function must either reside in an AP or in an external entity to which the AP is connected. The firewall protects both the AP and mobile devices connected to it from Internet-based attacks as well as protects a mobile device from attacks by other mobile devices.

10.2 Deactivation of Broadcast / Multicast Functionality

Passpoint equipment supports deactivation of Broadcast/Multicast functionality. The purpose of this feature is to mitigate broadcast key attacks.

When multicast/broadcast capability is disabled, the AP can use proxy-ARP service, as per IEEE 802.11-2012, to provide Address Resolution Protocol functionality (ARP).

When multicast/broadcast capability is enabled, the usage of proxy-ARP service is still recommended.

One other feature available in Wi-Fi networks is that of client isolation. This stops WLAN clients from talking to each other, and can help resolve broadcast key attacks, if not stop them completely.

11. Conclusion

Earlier WBA work on Wi-Fi Hotspot security reviewed the security issues with current Wi-Fi Hotspots and recommended some remedies for them [1].

This white paper highlights the security capabilities for Wi-Fi systems, including for roaming. The information herein is equally applicable to Enterprise networks, Passpoint, and OpenRoaming networks. These secure capabilities include adopting a number of existing IEEE 802.11 security features along with WPA2-Enterprise and WPA3-Enterprise security features. This transforms the security positioning of connected devices with guaranteed mutual authentication, over-the-air encryption. and restricted peer-to-peer traffic. Thus, the network security mitigates many of the issues highlighted in earlier WBA security work [1], including Traffic Sniffing and the Man-in-the-Middle Attack, and brings Wi-Fi security on par with cellular security.

The Wi-Fi Alliance Passpoint original documentation was released in Jun 2012. It is constantly being updated. [2].

Additional Wi-Fi security features will be incorporated in the future releases of the Wi-Fi Alliance Passpoint Certification, which will also address some of the security issues surrounding onboarding and the provisioning of subscriber devices with credentials. It will ensure users are communicating with the intended service provider network and utilize only protected communication between the mobile device and network. It will also enable RSN-based secure authorization and access to free public hotspots providing over-the-air encryptions and authentication of a user's identity.

Passpoint solutions like OpenRoaming removes many of the obstacles to simple, seamless, and secure access to public Wi-Fi hotspots and provides a secure cellular-like experience.

Appendix

A1 - Introduction

The Wi-Fi Alliance's Passpoint Specification defines the use of the Per Provider Subscription Management Object (PPS MO) profiles which deliver seamless network selection features. Five EAP methods are included in the Passpoint certification which are required to be supported by "Passpoint certified equipment".

Credential Type	EAP Method
Certificate	EAP-TLS
SIM/USIM	EAP-SIM, EAP-AKA, EAP-AKA'
Username/Password (with server-side certificates)	EAP-TTLS with MS-CHAP-V2

Table 2: EAP Methods defined in the Passpoint Specification

Since the definition of these EAP methods in 2006 (EAP-SIM and EAP-AKA), 2008 (EAP-TLS and EAP-TTLS) and 2009 (EAP-AKA'), there has been continued innovation in the definition of new EAP methods to address a variety of use cases. The IANA registry now includes over 50 defined methods [13]. This appendix describes EAP in more detail and expands on some of the use cases which have led to the development of new EAP methods not covered in the Passpoint certification program.

A2 – EAP Walkthrough

The diagram below displays the interaction between network elements during an EAP authentication method flow. The RADIUS EAP-Message attribute is used to convey EAPoL messages from the connecting supplicant to its routed authentication server to perform its negotiated EAP authentication method in a challenge-response exchange.

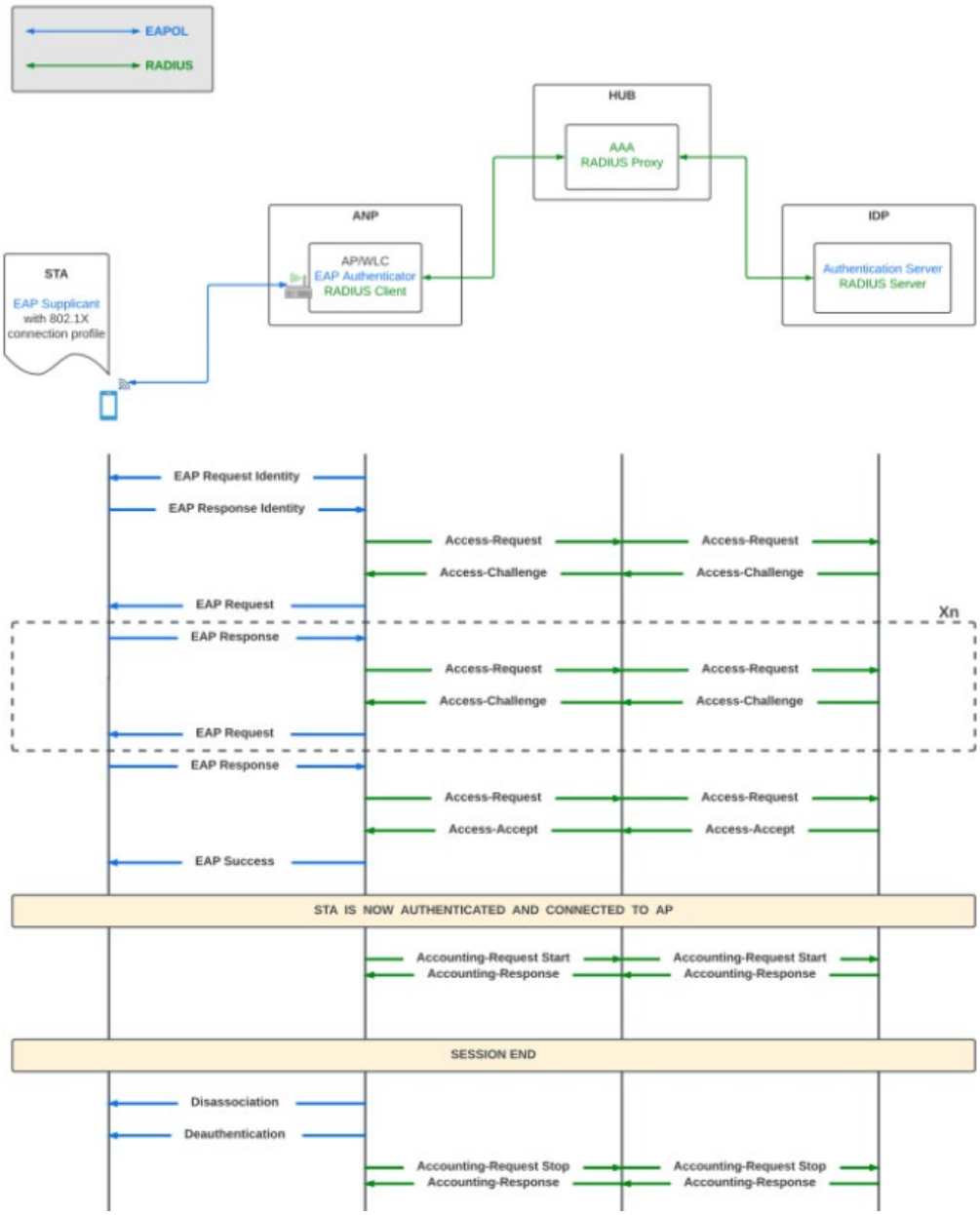

Table 6-1 EAP Ladder Diagram

A3 – Platform Adoption

Today's Passpoint platforms do not limit capabilities to the 5 methods defined and tested by the Wi-Fi Alliance. For example, in addition to the 5 methods listed in the Passpoint specification, Windows 10 and 11 allow Passpoint to be configured with the following EAP methods not defined by WFA [22]:

- PEAP with MS-CHAP-V2
- TEAP with MS-CHAP-V2
- PEAP with EAP-TLS
- EAP-TTLS with EAP-TLS
- TEAP with EAP-TLS

Android, in addition to the 5 methods listed in the Passpoint specification, allows Passpoint to be configured with the following EAP methods [23]:

- EAP-TTLS with PAP
- EAP-TTLS with CHAP
- EAP-TTLS with MS-CHAP

iOS, in addition to the 5 methods listed in the Passpoint specification, allows Passpoint be configured with the following EAP methods [24][25]:

- PEAP with MS-CHAP-V2
- EAP-FAST with MS-CHAP-V2
- EAP-FAST with GTC
- EAP-TTLS with PAP
- EAP-TTLS with CHAP
- EAP-TTLS with MS-CHAP
- EAP-TTLS with MS-CHAP-V2
- EAP-TTLS with an inner EAP method

A4 – An Overview of Other EAP Methods

The Wi-Fi Alliance performs testing of commonly implemented EAP authentication methods as part of its Passpoint certification program. There are no formal restrictions from using alternate EAP method to support your business use cases, although device implementation for these methods may be limited and may not be fully tested by industry for compatibility. There are many emerging (partially implemented)

and emergent (theoretical) EAP methods being proposed by industry and related standards groups. Caution should be used when selecting a non-Passpoint certified method. For more information on these methods please refer to the references section at the end of this Document.

A4.1 EAP-FAST/TEAP

EAP-FAST is an EAP method defined by Cisco in RFC4851 [14] as a replacement for its earlier EAP-LEAP method. EAP-FAST includes an in-band provisioning of a Protected Access Credential (PAC). However, current recommendations are to ensure the PAC provisioning is secured. Following provisioning, the Protected Access Credential (PAC) is used to establish a tunnel for the secure transmission of an "inner" EAP authentication method. RFC5422 describes the dynamic provisioning using EAP-FAST. Inner EAP methods supporting by EAP-FAST include EAP-MSCHAPv2, EAP-GTC and EAP-TLS [15].

TEAP specified in RFC7170 [16] is based on EAP-FAST, with minor changes, in order to meet the requirements outlined in RFC6678 [17] for a standard tunnel-based EAP method. Version 2 of TEAP is currently being defined in IETF EAP Methods Update (EMU) Working Group. Compared to RFC7170 [16], TEAPv1 removes all uses of the PAC, instead replacing it with the NewSessionTicket message as defined in TLS1.3.

Operations for certificate provisioning are defined, whereby a device can send a certificate signing request. After an inner EAP method has completed, the TEAP server can send the issued certificate to the device.

A4.2 FIDO-Based EAP Method

This method [21] is a proposed FIDO-based stand-alone EAP method currently under adoption in the IETF EMU Working Group that aims to improve on existing TLS-based EAP methods by explicitly enforcing TLS 1.3 server certificate and identity validation during tunnel negotiation (which in most TLS-based methods is optionally to be done by the supplicant) and uses a FIDO2-based [26] credential as the inner method to complete authentication. FIDO credentials are passkeys to prove a user's identity without sharing secrets. FIDO supports biometric authentication methods like Face ID and Touch ID.

This method satisfies requirements for protected cipher suite negotiation, mutual authentication, integrity and relay protection, confidentiality, key derivation (at a key strength of >= 128 bits negotiated during the TLS handshake), session independence and cryptographic binding. Dictionary attacks are not possible against this method as it has no password components. The authors are considering the ability for fast reconnection (as part of TLS session resumption).

The name of the method is currently provisional. A proposal for the name EAP-NetAuthn is pending agreement between the authors and the partners in the FIDO2 Project, the W3C and the FIDO Alliance.

A4.3 EAP-CREDS

EAP-CREDS is a draft method designed to be used as an inner method after TLS tunnel establishment [22]. The method is designed to enable access network credentials management. It enables the

encapsulation of existing credential management messages in EAP. The CREDS mechanism can be found in the Release 3 of the CBRS Alliance specifications where EAP-CREDS is used to manage non-USIM based credentials (e.g., username/password or X.509 certificates) for authenticating end-user devices like cell phones [19], [20], [23]

A4.4 EAP-PPT

EAP using Privacy Pass Tokens (EAP-PPT) is a recent published Internet-Draft designed to be used as an inner method after TLS tunnel establishment [21]. The method is designed to protect an individual from the privacy specific threats when operating in public and enterprise environments, including privacy protection against network service providers. Instead of signalling identities in EAP, EAP-PPT carries an attestation from a trusted attester. The authenticator is not linkable to the user and no collusion is possible between the different entities involved in the exchange. Issuance of the privacy pass tokens can be performed ahead of time and cached for use in subsequent EAP dialogues.

A4.5 EAP-TLS as an inner method

This report has identified the benefits of using EAP-TLS as an inner method, ensuring that the client certificate is protected from the ANP during transmission, even when operating using TLS 1.2. Encapsulating EAP-TLS in a TTLS tunnel provides additional functionality by leveraging the EAP-TTLS outer identity for privacy protection. Only some operating systems support this configuration as of this writing. EAP-TLS as an inner method can be used with EAP-TTLS, EAP-FAST or EAP-TEAP.

A5 – Additional Ladder Diagrams

This appendix shows ladder diagrams of different SIM-based EAP types. An example of pseudonym delivery using EAP-SIM is illustrated in Figures 1 and 2. An example of pseudonym delivery using EAP-AKA is illustrated in Figure 3 and the subsequent use of the pseudonym in EAP-AKA authentication is illustrated in Figures 3 and 4.

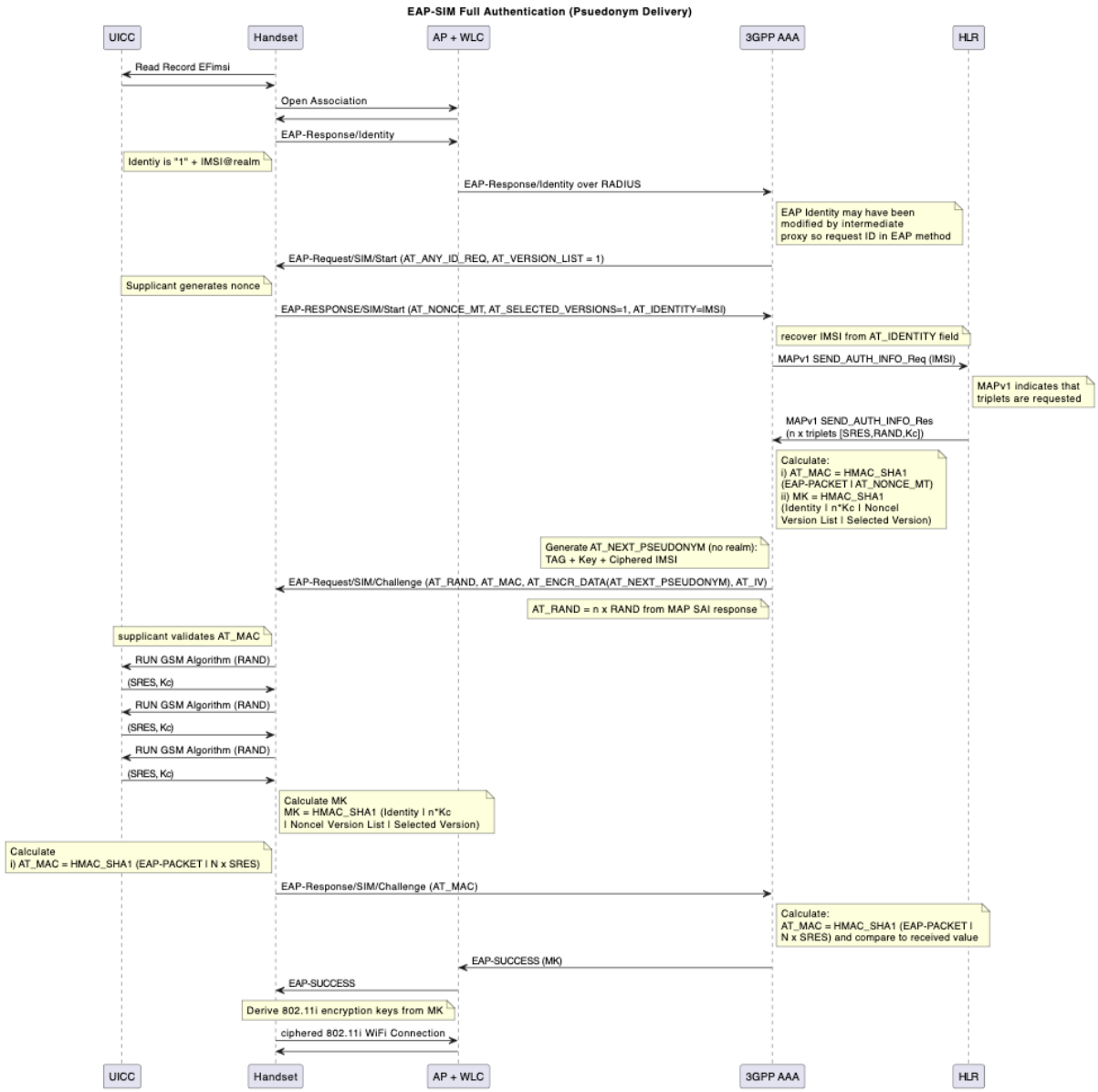

Figure 1 - EAP-SIM Pseudonym generation and delivery

Legend:

- **UICC** – Universal Integrated Circuit Card – used to ensure security and integrity of data that identifies the user
- **AP + WLC** – Access Point + Wireless Lan Controller – refers to the network equipment
- **AAA** – Authentication, Authorization and Accounting – refers to a server that controls access to a network and can enforce policies, auditing usage and provide info necessary for billing services.
- **HLR** – Home Location Register – database in a cellular wireless network that contains users' data, service policies and call-routing info.

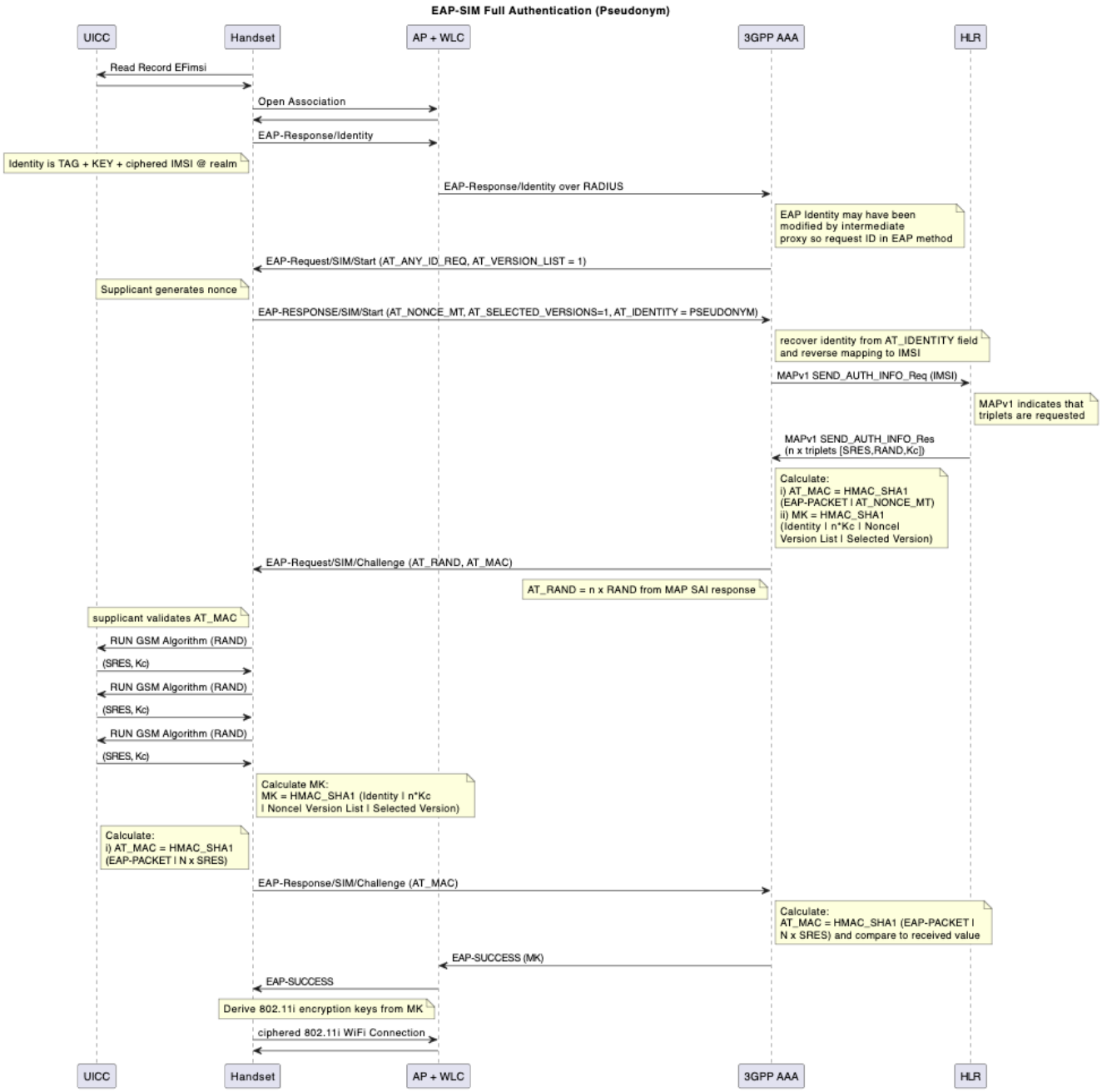

Figure 2 - EAP-SIM Authentication with Pseudonym

In Wi-Fi roaming scenarios, the realm In the NAI looks like @wlan.mncXXX.mccYYY.3gppnetwork.org, where XXX is the three-digit MNC and YYY the three-digit MCC. Hence, MNC/MCC cannot be hidden.

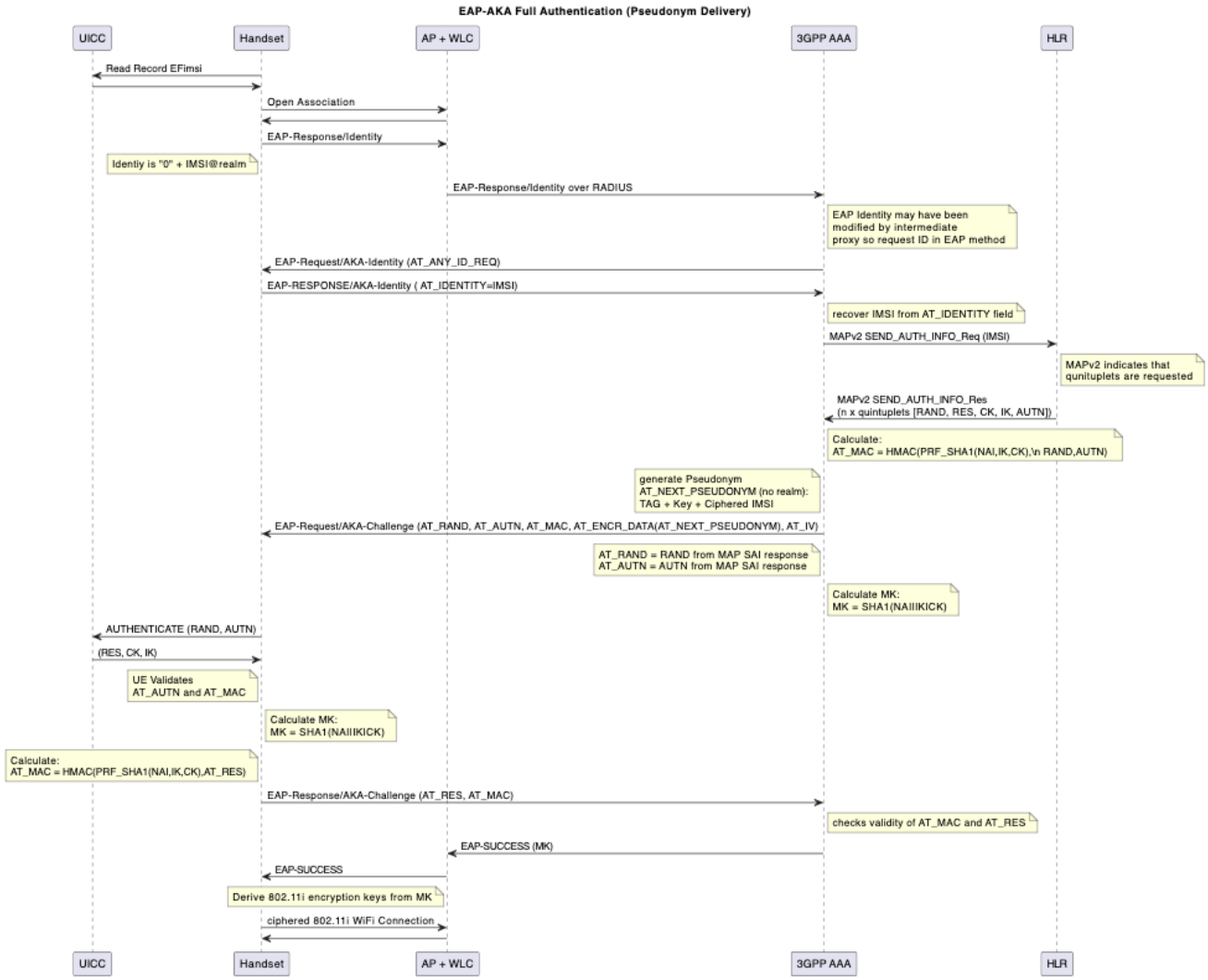

Figure 3 - EAP-AKA Pseudonym generation and delivery

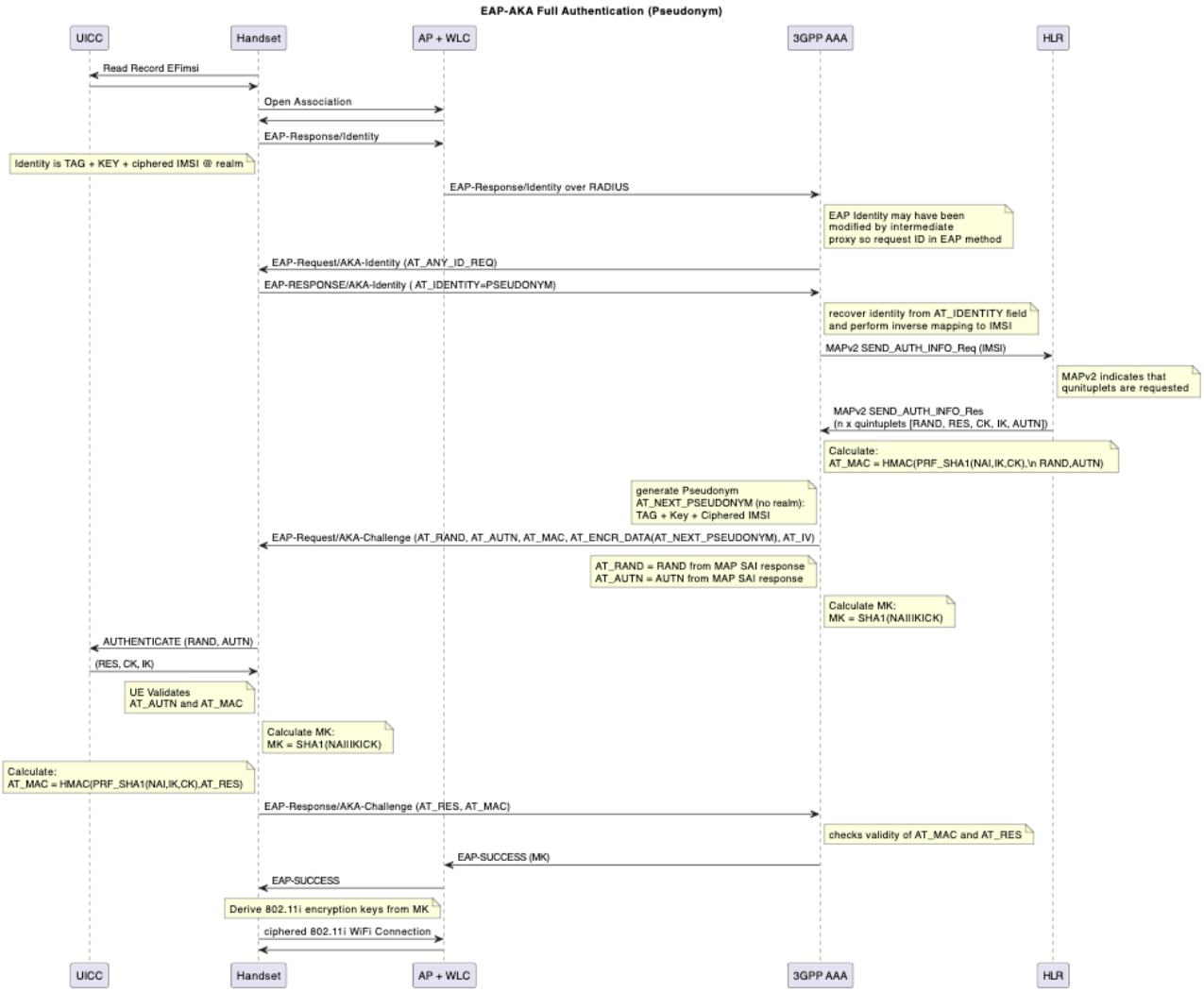

Figure 4 - EAP-AKA Authentication with Pseudonym

A6 – Post Quantum EAP Methods

Post Quantum Computing (PQC) has implications on all TLS traffic, including EAP-TLS. The IETF's focus is on addressing PQC challenges with TLS v1.3 and not TLS v1.2. TLS v1.3 is being enhanced with the ability to negotiate the use of PQC algorithms and hybrid PQC algorithms. Some post quantum Key Encapsulation Mechanisms (KEM) have very large public keys. [27]

EAP-AKA uses the 3GPP defined Authentication and Key Agreement which is based on symmetric cryptography that is less affected by the PQC threats to asymmetric schemes. However, recent enhancements to EAP-AKA in RFC 9048 have added the ability to perform ephemeral key exchange for forward secrecy. These enhancements are vulnerable to post-quantum attacks and hence work is in progress to update EAP-AKA Forward Secrecy to address these limitations in the Internet-Draft draft-ar-emu-pqc-eapaka.

References

[1] Wireless Broadband Alliance, *Next Generation Hotspot Security*, January 26, 2013. Link

[2] Wi-Fi Alliance, *Wi-Fi® Passpoint Release 1 Deployment Guide*, June 25, 2012.

[3] Internet Engineering Task Force, RFC 3748 – *Extensible Authentication Protocol (EAP)*, June 2004. Link

[4] Internet Engineering Task Force, RFC 5216 – *The EAP-TLS Authentication Protocol*, March 2008. Link

[5] Internet Engineering Task Force, RFC 5281 – *Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)*, August 2008. Link

[6] Internet Engineering Task Force, RFC 4186 – *EAP Method for GSM Subscriber Identity Modules (EAP-SIM)*, January 2006. Link

[7] Internet Engineering Task Force, RFC 4187 – *EAP Method for 3G Authentication and Key Agreement (EAP-AKA)*, January 2006. Link

[8] Internet Engineering Task Force, RFC 5448 – *Improved EAP Method for 3G Authentication and Key Agreement (EAP-AKA')*, May 2009. Link

[9] Internet Engineering Task Force, RFC 4282 – *The Network Access Identifier*, December 2005. Link

[10] Wireless Broadband Alliance, *WRIX Standard Service Specification Interconnect Definition*, December 2009.

[11] 3GPP TS 23.003 – *Numbering, addressing and identification*. Link

[12] Internet Engineering Task Force, RFC 4372 – *Chargeable User Identity*, January 2006. Link

[13] IANA – *EAP Numbers*. Link

[14] Internet Engineering Task Force, RFC 4851 – *Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method (EAP-FAST)*, May 2007. Link

[15] Internet Engineering Task Force, RFC 5422 – *Dynamic Provisioning Using EAP-FAST*, March 2009. Link

[16] Internet Engineering Task Force, RFC 7170 – *Tunnel Extensible Authentication Protocol (TEAP) Version 1*, May 2014. Link

[17] Internet Engineering Task Force, RFC 6678 – *Requirements for a Tunnel-Based Extensible Authentication Protocol (EAP) Method*, July 2012. Link

[18] IETF Draft – draft-ietf-emu-eap-fido. Link

[19] IETF Draft – draft-pala-eap-creds. Link

[20] CableLabs – *EAP-CREDS: Enabling Policy-Oriented Credential Management in Access Networks*. Link

[21] IETF Draft – draft-sawant-eap-ppt-02. Link

[22] Microsoft – *Windows Passpoint*. Link

[23] Android – *Wi-Fi Passpoint*. Link

[24] Apple Developer – *NEHotspotEAPSettings/EAPType*. Link

[25] Apple Developer – *NEHotspotEAPSettings/TTLSInnerAuthenticationType*. Link

[26] Wikipedia – *FIDO2 Project*. Link

[27] IETF Draft – draft-ietf-pquip-pqc-engineers. Link

[28] Internet Engineering Task Force, RFC 2865 – *Remote Authentication Dial In User Service (RADIUS)*, June 2000. Link

[29] Internet Engineering Task Force, RFC 3579 – *RADIUS Support for Extensible Authentication Protocol (EAP)*, September 2003. Link

[30] Internet Engineering Task Force, RFC 6614 – *TLS Encryption for RADIUS*, May 2012. Link

[31] Internet Engineering Task Force, RFC 7360 – *Datagram TLS as a Transport Layer for RADIUS*, September 2014. Link

[32] Internet Engineering Task Force, RFC 9325 – *Recommendations for Secure Use of TLS and DTLS*, November 2022. Link

[33] Internet Engineering Task Force, RFC 9525 – *Service Identity in TLS*, November 2023. Link

[34] Internet Engineering Task Force, RFC 8446 – *Service Identity in TLS*, November 2023. Link

[35] Internet Engineering Task Force, RFC 9190 – *Service Identity in TLS*, November 2023. Link

Participants List

Name	Company	Role
Phil Morgan	NC-Expert	Project Leader
Blair Bullock	Boldyn Networks	Roaming Work Group Co-Chair
Erinn Hall	AT&T	Roaming Work Group Co-Chair
Ryan Blossom	Single Digits	Roaming Work Group Co-Chair
Jim Sturges	AT&T	Editorial Team
Loay Kreishan	Charter	Editorial Team
Mark Grayson	Cisco	Editorial Team
Hideaki Goto	Cityroam	Editorial Team
Mark Hamilton	RUCKUS Networks	Editorial Team
Stefan Paetow	JISC	Editorial Team
Rie Morgan	NC-Expert	Editorial Team
Michael Sym	Single Digits	Editorial Team
Sumanth Hallegiri	AT&T	Project Participant
Jessie Manik	Bell Mobility	Project Participant
Prakash Bharti	Boingo Wireless	Project Participant
Pete Casanave	Boldyn Networks	Project Participant
Tooba Faisal	BT	Project Participant
Neeharika Jesukumar	CableLabs	Project Participant
Luther Smith	CableLabs	Project Participant
Darshak Thakore	CableLabs	Project Participant
Ashish Bhargava	Calix	Project Participant
Martin Casey	Calix	Project Participant
Meganathan Pooranan	Calix	Project Participant
Dave Moran	Charter	Project Participant
Bruno Pariseau	Charter	Project Participant
An Ngueyn	CISA	Project Participant
Mir Alami	Cisco	Project Participant
Andy Gowans	Cisco	Project Participant
Jeffry Handal	Cisco	Project Participant
Eva Santos	Cisco	Project Participant
Ruchi Kothari	Comcast	Project Participant
Matt Markel	Comcast	Project Participant
PJ Dhillon	COX	Project Participant
Thomas Liaw	COX	Project Participant
Harpreet Narula	Dell	Project Participant
Lee Harding	Eleven Software	Project Participant
Jonas Anden	ENEA	Project Participant
Haneya Qureshi	General Motors	Project Participant
Mathew George	HPE	Project Participant
Prateek Patni	HPE	Project Participant

Peter Thornycroft	HPE	Project Participant
Necati Canpolat	Intel Corporation	Project Participant
Hassan Yaghoobi	Intel Corporation	Project Participant
Edward Wincott	JISC	Project Participant
Okan Mutgan	Nokia	Project Participant
Tom Van Driessche	Nokia	Project Participant
Stew Goumans	Ekahau	Project Participant
Kevin Hasley	Ookla	Project Participant
Ahmed Elsherif	Qualcomm	Project Participant
José Martinez	RDK Management	Project Participant
Ryan Blossom	Single Digits	Project Participant
Betty Cockrell	Single Digits	Project Participant
Yvette Medina	Single Digits	Project Participant
Lawrence Maddison	TATA Communications	Project Participant
Samson Okulaja	Telus	Project Participant
Pedro Mouta	Wireless Broadband Alliance	Project Participant