# WPA3, Wi-Fi 6E and eduroam

First released 6th September 2022

Updated 7th Feb 2025

**Contents**



### 1. Introduction

Up until now the scope of the eduroam(UK) Technical Specification has been limited to requiring only that WPA2-Enterprise must be adhered to for security/encryption - superseding the originally permitted WPA and WEP. There have been no requirements relating the radio spectrum, so implementers have been free to offer 2.4GHz-only Wi-Fi, 5GHz-only Wi-Fi or as in the majority of cases 2.4GHz and 5GHz Wi-Fi. The specification avoids stipulating 802.11 standards, channels, channel widths or power levels to be used, since all of these fall properly within the domain of the service provider organisation and are best determined for each deployment on the basis of local user needs and local environment.

However with the arrival of WPA3-Enterprise and Wi-Fi 6E, it is possible for the Wi-Fi network to be implemented in such a way, with the intention of providing the best/most secure deployment, that a large swathe of the eduroam user base may be denied service. Therefore an updated service-wide policy is now needed.

The eduroam(UK) Technical Specification will shortly be updated to include:

.

- a) Organisations providing Wi-Fi Visited services in the 2.4GHz or 5GHz RF bands MAY implement WPA3-Enterprise in transition mode; Protected Management Frames (PMFs) MAY be implemented but MUST be set to ‘Supported’ rather than ‘Required’.
- 
- b) Organisations providing Wi-Fi Visited services in the 2.4GHz, 5GHz or 6GHz RF bands MUST NOT enable 192-bit security; organisations providing Wi-Fi Visited services in the 6GHz RF band with WPA3-Enterprise MUST NOT implement WPA3-Enterprise 192-bit mode.
- 
- c) ?Recommendation - WPA3-Enterprise in transition mode SHOULD be implemented in the 2.4GHz and 5GHz RF bands.

What RF bands (2.4GHz, 5GHz and 6GHz) eduroam organisations use to provide Wi-Fi services and how these are set up remains at the discretion of the individual participating member organisations. It is recommended that if organisations deploy 6GHz Wi-Fi, eduroam should in addition continue be provided at least over the 5GHz band.

**2. WPA3 in relation to eduroam**

Wi-Fi CERTIFIED WPA3 was announced by the Wi-Fi Alliance [1] in June 2018. There are some useful benefits for eduroam in the WPA3-Enterprise mode but the biggest difference from WPA2 is in the WPA3-Personal mode (which now leverages Simultaneous Authentication of Equals (SAE), a secure key establishment protocol between devices, to provide stronger protections for users against password cracking).

Of relevance to eduroam is WPA3-Enterprise - which builds upon the foundation of WPA2-Enterprise and includes the later additions to that certification, in particular support for use of Protected Management Frames. Support for validation of server certificate to a root CA, if such root CA is configured, was also included. Deployment of WPA3-Enterprise has significant implications for client devices, the Visited organisation (SP) and the Home organisation (IdP).

### 3. WPA3 Key features

- Authentication: multiple Extensible Authentication Protocol (EAP) methods
- Authenticated encryption: minimum 128-bit Advanced Encryption Standard Counter Mode with Cipher Block Chaining Message Authentication (AES-CCMP 128)
- Key derivation and confirmation: minimum 256-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA256)
- Robust management frame protection: minimum 128-bit Broadcast/Multicast Integrity Protocol Cipher-based Message Authentication Code (BIP-CMAC-128)
- WPA, TKIP and WEP are not permitted on WPA3-Enterprise BSS

### 4. Protected Management Frames (PMF)

Protected Management Frames is a standard defined by Wi-Fi Alliance to enhance Wi-Fi connection safety. It provides unicast and multicast management actions and frames a secure method with WPA2/WPA3, which can improve packet privacy protection. To find out more see:

https://www.wi-fi.org/beacon/philipp-ebbecke/protected-management-frames-enhance-wi-fi-network-security [2]

A WPA3-Enterprise network is identical to a WPA2-Enterprise network that has been configured to support Protected Management Frames (PMF). By setting PMFs as *supported* rather than *required*, backwards compatibility with non-PMF capable WPA2 devices is achieved - older WPA2 devices can continue to connect to the network the same as if it were a WPA2 network. Those devices which do understand PMFs can negotiate use of PMF. In the eduroam environment where it is not uncommon for older devices to still be in use, it is considered essential that devices that do not support PMF should nevertheless be able to be connected.

Regarding network equipment however, manufactures have been building support for PMF into their kit for many years and so enabling PMF on a network should not present a problem nor require investment in new hardware.

### 5. WPA3-Enterprise Modes of Operation

The WPA3 Specification [3] defines three modes of operation – WPA3-Enterprise only; WPA3-Enterprise transition mode; WPA3-Enterprise 192-bit mode.

### A) WPA3-Enterprise only mode

***Protected Management Frames usage is mandatory***.

- When a BSS is configured in WPA3-Enterprise only mode, PMF shall be set to required (MFPR bit in the RSN Capabilities field shall be set to 1 in the RSNE transmitted by the AP)
- A WPA3-Enterprise STA shall negotiate PMF when associating to an AP using WPA3-

Enterprise only mode

**Deployment:** Older devices may not support PMF and so would be excluded from connecting to your eduroam Visitor network. Configuring PMF as ‘required’ is therefore not permitted with eduroam in the 2.4GHz and 5GHz bands. In the 6GHz band, Wi-Fi 6E certification applies which includes the provision that WPA3-Enterprise only is supported so PMF is mandated in that band.

**B) WPA3-Enterprise transition mode**

This mode is effectively WPA2-Enterprise with PMF enabled but not mandatory.

- When WPA2-Enterprise and WPA3-Enterprise transition mode are configured on the same BSS (mixed mode), PMF shall be set to capable (MFPC bit shall be set to 1, and MFPR bit is by default set to 0 in the RSN Capabilities field in the RSNE transmitted by the AP)

- A WPA3-Enterprise STA shall negotiate PMF when associating to an AP using WPA3-Enterprise transition mode

**Deployment:** If you want to enable WPA3-Enterprise Transition mode, then you can set PMF optional in your SSID configuration, so PMF capable clients negotiate it whilst clients that lack capability join the SSID without PMF. This is the practical way of enabling WPA3-Enterprise in today’s network - the alternative would be to create a separate SSID for ‘WPA3-Enterprise only’ which would create difficulties for the eduroam service and is not currently permitted.

It is recommended that eduroam Visited organisations (SPs) activate WPA3-Enterprise transition mode by marking Protected Management Frames as “supported, but not required” in their network equipment. This should be configured for the relevant RF bands 2.4GHz and 5GHz.

**C) WPA3-Enterprise 192-bit mode**

‘WPA3-Enterprise with 192-Bit security’ operation mode enforces CNSA Suite security standards and provides even greater security than WPA3-Enterprise. It is considered an option for govt, defence and industry. PMF must be set to required as for WPA3-Enterprise only. It is based on EAP just like the normal WPA2-Enterprise, but has further constraints regarding the permitted cipher suites - both for group ciphers on the wireless medium (*) and during the TLS negotiation inside of tunnelling EAP methods (**).

(*) The following is advertised and negotiated in beacons, probe response, and association:

**AKM** suite selector as 00-0F-AC:**12** (802.1X with SHA-384).
Pairwise cipher suite selector as 00-0F-AC:9 (**GCMP-256**).
Group data cipher suite selector as 00-0F-AC:9 (GCMP-256).
Group management cipher suite selector as 00-0F-AC:12 (**BIP-GMAC-256**).
Protected Management Frames are mandatory (**MFPR=1 and MFPC=1**).

(**) Permitted EAP cipher suites for use with WPA3-Enterprise 192-bit Mode are:

- **TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 -** ECDHE and ECDSA using

the 384-bit prime modulus curve P-384
- **TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384** - ECDHE using the 384-bit prime modulus curve P-384; RSA ? 3072-bit modulus
- **TLS_DHE_RSA_WITH_AES_256_GCM_SHA384** - RSA ? 3072-bit modulus; DHE ? 3072-bit modulus

**Deployment:** The security requirements of WPA3-Enterprise with 192-Bit security also induce a stringent required feature set on the RADIUS/EAP server equipment of eduroam Home organisations (IdPs). The cipher suite and key length requirements are not met by a majority of eduroam IdPs at this point in time (June 2018). Furthermore, EAP methods not based on TLS – notably EAP-pwd - are not permitted at all on WPA3-Enterprise with 192-Bit Security networks.

WPA3-Enterprise with 192-Bit Security is configured on the access point, but needs compatible EAP servers at the Identity Provider side. With no signalling between the Access Point and the eduroam Identity Provider server, there is a significant risk for interoperability issues within eduroam.

If WPA3-Enterprise with 192-Bit Security is enabled, it must be the only key mechanism on a given SSID. This means that in order to support client devices that are not capable of 192-Bit Security, there would need to be two distinct SSIDs: 'eduroam' with WPA2/WPA3-Enterprise transition mode, and a different SSID for WPA3-Enterprise with 192-Bit Security. As stated above, this would be unworkable for the eduroam service.

The conclusion is that ***WPA3-Enterprise with 192-Bit Security must not be implemented with eduroam***.

Ref: https://eduroam.org/eduroam-and-wpa3/ [4]

Ref: https://arubanetworking.hpe.com/techdocs/aos/wifi-design-deploy/security/modes/wpa3-enterprise/ [5]

### 6. Wi-Fi 6E Overview

The availability of 6GHz for Wi-Fi is for many the most exciting thing to happen for Wi-Fi in the last 15 years. Wi-Fi 6E marks a new beginning for Wi-Fi, promising data rates up to 1GBps, lower latencies and support for much higher device densities that were possible with Wi-Fi 6 and earlier iterations using the 2.4Ghz and 5GHz bands.

In April 2020, nearly 17 years since the last major spectrum allocation, the United States Federal Communications Commission (FCC) approved use of 1200 MHz in the 6 GHz band for unlicensed technologies, (5,925-7,125MHz). And in the UK, the lower part of the 6GHz band (5,925-6,425 MHz, i.e. UNII-5) has been approved for similar use by Ofcom. As of March 2022 Ofcom is considering releasing the upper part (6,425-7,070MHz) under the Shared Access licence framework for low-power, indoor use. So, at the time of writing, in the UK the additional bandwidth benefit is only half of the potential!

Wi-Fi 6E certification [6] for any IEEE 802.11ax (Wi-Fi 6) products supporting 6GHz wireless spectrum was announced by the Wi-Fi Alliance in January 2021. Wi-Fi 6E builds on all the features introduced in Wi-Fi CERTIFIED 6, including:

- **Multi-user multiple input multiple output (MU-MIMO):** allows more data to be transferred at once and enables an access point to transmit data to a larger number of devices concurrently
- **160 MHz channels:** increases bandwidth to deliver greater performance with low latency
- **Target wake time (TWT):** significantly improves battery life in Wi-Fi devices, such as Internet of Things (IoT) devices
- **1024 quadrature amplitude modulation mode (1024-QAM):** efficient modulation - increases throughput in Wi-Fi devices by encoding more data in the same amount of spectrum
- **Transmit beamforming:** enables higher data rates at a given range resulting in greater network capacity
- **Orthogonal frequency division multiple access (OFDMA):** effectively shares channels to increase network efficiency and lower latency for both uplink and downlink traffic in high demand environments
- **Increased symbol duration**: for robust outdoor performance
- **Improved MAC signalling**

The 'E' Extension adds 1200MHz of contiguous spectrum in the 6GHz band, resulting in an additional three times the bandwidth available in the 5GHz range. This can be used to deliver an additional 59 x 20MHz channels, 29 x 40MHz channels or 14 x 80MHz channels - resulting in less co-channel interference and improving support for high device densities. Alternatively 160GHz superwide channels and be implemented (a total of 7 x 160MHz channels) to support very high data rates.

Further benefits in Wi-Fi 6E are more efficient network discovery reducing the need for AP probing through the use of preferred scanning channels and by multiband devices utilising RNR by scanning 2.4 and 5G bands.

Wi-Fi 6E builds on the mechanisms introduced in Wi-Fi 6 to reduce channel contention and collisions between devices. These techniques work exceptionally well in the 6 GHz band, where only Wi-Fi 6E devices with advanced capabilities operate.

Ref: https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6 [7]

Ref: https://www.litepoint.com/wp-content/uploads/2020/06/Wi-Fi-6E-Whitepaper-060220-web.pdf [8]

**7. Security in Wi-Fi 6E**

Alongside the additional bandwidth in the 6GHz spectrum, the Wi-Fi Alliance **mandated WPA3 security certification for Wi-Fi 6E** devices that operate in the 6 GHz band. Of relevance to eduroam, WPA3-Enterprise still uses 802.1X, but WPA3 requires the use of Protected Management Frames (PMF). Moreover, there is ***no backward compatibility support for WPA2 security***. Because there is no backward compatibility for WPA2, there is no need for the WPA3-Enterprise transition mode (or for that matter, the WPA3-Personal transition mode).

WPA3-Enterprise will be the standard of relevance to eduroam, but for sake of completeness, Wi-Fi 6E also includes WPA3-Personal in which PSK authentication is replaced with 'Simultaneous Authentication of Equals' (SAE), which is resistant to offline dictionary attacks –

the passphrase is never sent between Wi-Fi devvices suring the SAE exchange. The other significant development is ‘Enhanced Open’ by which open security guest Wi-Fi hotspots are a thing of the past. Opportunistic Wireless Encryption (OWE) protocol integrates established cryptography mechanisms to provide each user with unique individual encryption, protecting the data exchange between the user and the access point. Data privacy is provided and malicious eavesdropping attacks are mitigated because the 802.11 data frames are encrypted - but there is nil authentication security.

**8. Legacy Devices**

New 6GHz-capable APs and devices will be capable of working with WPA3. But many of the world’s existing 15 billion Wi-Fi clients do not have 6GHz capable radios will never be able to connect to 6 GHz since it  even if their firmware is updated to support WPA3, it appears likely that different levels of security will be used on the different frequency bands in the enterprise. WPA3 will indeed be used in 6 GHz. Yet, despite the support for WPA3 transition mode in the legacy bands, WPA2 will likely remain prevalent in the 2.4 GHz and 5 GHz bands for a very long time.

**9. Implementation / Recommendations**

The deployment of WPA3-Enterprise Transition Mode/optional Protected Management Frames and Wi-Fi 6E is in principle a good move towards better performance and better security. However, as has been described above, the introduction of the latest standards is not without risk.

**Recommendations:**

- When participating service provider organisations introduce Wi-Fi 6E services, eduroam should be provided and this must be via the ‘eduroam’ SSID.
- Spread the implementation - organisations should not implement the introduction of the new band  coincidentally with changes on the existing bands in respect of WPA3-Enterprise transition mode or changes to Protected Management Frames.
- The advice against implementing WPA3-Enterprise 192-Bit security remains - WPA3 Enterprise 192-Bit security must NOT be implemented on the 6 GHz band.
- It is NOT RECOMMENDED to deploy eduroam exclusively on the 6 GHz band. It is expected that Access Points supporting Wi-Fi 6E will at the same time also provide service on the 2.4 and/or 5 GHz bands - both to support best performance in the 6GHz band and  so that existing client devices without support for 6E continue to receive Wi-Fi coverage

Ref:  https://eduroam.org/eduroam-deployment-considerations-on-wi-fi-certified-6e/ [9]

---



**Links**
[1] https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security
[2] https://www.wi-fi.org/beacon/philipp-ebbecke/protected-management-frames-enhance-wi-fi-network-security

[3] https://www.wi-fi.org/file/wpa3-specification
[4] https://eduroam.org/eduroam-and-wpa3/
[5] https://arubanetworking.hpe.com/techdocs/aos/wifi-design-deploy/security/modes/wpa3-enterprise/
[6] https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-delivers-wi-fi-6e-certification-program
[7] https://www.wi-fi.org/discover-wi-fi/wi-fi-certified-6
[8] https://www.litepoint.com/wp-content/uploads/2020/06/Wi-Fi-6E-Whitepaper-060220-web.pdf
[9] https://eduroam.org/eduroam-deployment-considerations-on-wi-fi-certified-6e/