Advice to eduroam® Identity Providers and Service Providers following the release of Wi-Fi CERTIFIED WPA3™ Security

Release Date: 26 June 2018

Executive Summary

The biggest change in Wi-Fi CERTIFIED WPA3™ Security is about pre-shared key deployments, which are not in scope for eduroam IdPs. There are small but useful benefits for WPA3-Enterprise, and there is a new optional operation mode *WPA3-Enterprise with 192-Bit Security* with significant interoperability issues on the deployed base of eduroam WPA-Enterprise hotspots.

The only action, which typically does not require monetary investments at all, is to turn on support for Protected Management Frames (PMFs) and to turn off WPA1 in the existing eduroam SP network deployment.

WPA3-Enterprise with 192-Bit Security MUST NOT be configured.

Changes in WPA3-Personal with pre-shared keys

What was formerly a WPA2-PSK network (one passphrase protects the entire SSID) gets modernised. The passphrase remains as-is, but the algorithm to derive the Wi-Fi master session key from the user-supplied WPA passphrase gets changed and is now based on the "Dragonfly" algorithm. It is called WPA3-SAE (Simultaneous Authentication of Equals). eduroam Identity Providers may know the Dragonfly algorithm for its appearance in the EAP type "EAP-pwd".

Changes in WPA3-Enterprise

Changes for all WPA3-Enterprise deployment modes, including eduroam's WPA-EAP

The changes are very small.

- WPA3-Enterprise includes a roll-up of several late additions to WPA2-Enterprise certification. This ensures that WPA3-Enterprise certified devices are guaranteed to
    - be immune against the KRACK vulnerability
    - support Protected Management Frames (PMF)
    - validate a server certificate to a root CA, if such a root CA is configured. Note: There is still not a requirement to actually *have* a CA certificate configured.
- Support for Protected Management Frames (PMFs) is a requirement

There is no explicit "mixed mode", nor is one required: a WPA3-Enterprise network is identical to a WPA2-Enterprise network which has configured support for Protected Management Frames (PMF). So long as PMFs are only configured as supported, rather than required, older WPA2 devices can continue to connect to the network as if it were a normal WPA2 network.

Only the backwards compatibility to WPA(1) is discontinued, which should not have any significant relevance in the eduroam environment any more. This makes it easy and useful for eduroam Service Providers to activate WPA3-Enterprise by marking Protected Management Frames as "supported, but not required" in their network equipment and by turning off support for WPA1.

Since most equipment supports PMFs since many years, typically, no new investment in Wi-Fi CERTIFIED WPA3™ hardware is required for this.

Considering that a BYOD environment such as eduroam typically has a very diverse set of user devices, including old devices which potentially do not support PMFs, it is considered premature to make PMFs required at this point in time. eduroam operations will revisit this position in due time.

The new operation mode WPA3-Enterprise with 192-Bit security

There is an optional new operation mode in Wi-Fi CERTIFIED WPA3™: WPA3-Enterprise with 192-Bit security. This operation mode is based on EAP just like the normal WPA3-Enterprise mode, but has further constraints regarding the permitted cipher suites; both during the TLS negotiation inside of tunnelling EAP methods [2] and for group ciphers on the wireless medium. The list of cipher suites and key lengths mirrors a regulatory requirement by a committee of various intelligence agencies in the United States of America[1] designed for their local government agencies and military operation ("Commercial National Security Algorithm Suite",CNSA). Despite being part of the Wi-Fi CERTIFIED WPA3™ certification, which suggests that it has an immediate effect only between client devices and access points, its security requirements would also induce a stringent required feature set on the RADIUS/EAP server equipment of eduroam Identity Providers[2]. Early studies in the eduroam IdP landscape indicate that the cipher suite and key length requirements are not met by a majority of eduroam IdPs at this point in time. Furthermore, EAP methods not based on TLS – notably EAP-pwd – are not permitted at all on WPA3-Enterprise with 192-Bit Security networks.

Since 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 inside eduroam.

WPA3-Enterprise with 192-Bit Security, if enabled, must be the only key management on a given SSID. In order to continue to serve client devices which are uncapable of 192-Bit Security, there must be two distinct SSIDs: 'eduroam' with the classic WPA3-Enterprise, and a new SSID for WPA3-Enterprise with 192-Bit Security

To work around those issues, there are three possibilities:

Option A: step-change upgrade sequence: all IdPs -> then SPs

A global upgrade in eduroam infrastructure would need to be done in two phases:

1) **first**, **all** eduroam Identity Providers globally upgrade their RADIUS/EAP servers to meet the IdP-side requirements of WPA3-Enterprise with 192-Bit Security
2) **strictly only after that**, eduroam Service Providers start to upgrade their Access Point configuration to WPA3-Enterprise with 192-Bit Security at their own pace

Option B: per-IdP regime of client configurations

All eduroam Identity Providers individually need to make sure that all their own users' client configurations do not allow the respective device to connect to any WPA3-Enterprise with 192-Bit Security eduroam network until the eduroam Identity Provider has upgraded their authentication server to support the TLS cipher suites required by WPA3-Enterprise with 192-Bit Security (at which point in time its users can be signalled to change their configuration at their own pace).

eduroam Identity Providers not enforcing such a configuration restraint would subject their users to the aforementioned interoperability problems. Given the diverse implementation quality of EAP supplicants, the vastly varying richness of expression of configuration formats, and the fact that a significant fraction of users will not follow configuration advice (including connecting without pre-configuration to non-standard SSIDs), realising this modus operandi appears unrealistic. This option also still needs a **new SSID**, with the same legacy support reasoning as in Option A, above.

Option C: Do not transition to WPA3-Enterprise with 192-Bit Security

eduroam Identity Providers that are interested in the level of security that WPA3-Enterprise with 192-Bit Security brings can upgrade their RADIUS/EAP server to support only the three cipher suites in question at any time, while remaining compatible with the existing eduroam SP setup in WPA2-Enterprise and WPA3-Enterprise.
This will achieve almost the same result as WPA3-Enterrprise with 192-Bit Security by steering and enforcing cipher suite selection from the IdP-side, and without the interoperability problems of the actual change of operation mode. The only minor difference is then the group cipher on the medium.

Advice

Considering that the WPA3-Enterprise with 192-Bit Security operation mode's primary use case is in one country outside its educational community, combined with the fact that option B above is unrealistic, and the significant deployment complexities of option A above, eduroam currently pursues option C above, i.e. does not currently have any plans to engage in any transition in any way.

Due to that, until further notice, **eduroam Service Providers are advised NOT to configure WPA3-Enterprise with 192-Bit Security. Doing so anyway will lead to hard to debug authentication failures for users of the majority of eduroam Identity Providers.**

[1] https://www.cnss.gov – yes, the web site really has a certificate which is not in browser trust stores.

[2] EAP peers and servers need to support TLS1.2 with the cipher suites ECDHE-RSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES256-GCM-SHA384 and/or DHE_RSA_WITH_AES_256_GCM_SHA384. Further to this, where RSA keys are used, they need to be at least 3072 bit long; where ECDSA keys are used, they need to be based on curve P-384.