

JANET Advisory: WPA/TKIP Obsolescence and Change to JRS Tier 2 Requirements

September 2010

Important News from the Wi-Fi Alliance

The Wi-Fi Alliance has endorsed a phased plan for the removal of WEP and WPA/TKIP support from products manufactured by its members. Whilst WEP has not been permitted for use with eduroam services since May 2009, the withdrawal of support for TKIP is of current relevance to organisations participating in JANET Roaming.

The Alliance roadmap phases out TKIP in new products over three years beginning in January 2011.

WPA/TKIP is already disallowed in 802.11n. For 802.11 a/b/g products, the first significant milestone in the withdrawal of TKIP is January 2011. From this date, access points will not be permitted to utilise TKIP alone. Mixed modes, in which an access point can accept either TKIP or AES keys, will however still be allowed and this concession will continue until January 2014.

From January 2012, the TKIP-only ban will be extended to apply to all devices, ie. Wi-Fi adapters. So, from this date, all new products must be able to support AES.

January 2013 sees the final disallowance of WEP on access points, followed in January 2014 by the removal from all other devices (Wi-Fi adapters).

From January 2014, mixed mode will be prohibited in access points, effectively banning TKIP in new access point products (and making it pointless to continue TKIP support in Wi-Fi adapters).

An important step towards improving wireless networking security and the move towards WPA2/AES has been made in allowing manufacturers to ship new products that use WPA2 out of the box. Previously the Wi-Fi certification required access points to be set by default to open and the onus was on the purchaser to configure security – WPA/TKIP, mixed mode or WPA2/AES as required.

Implications for JANET Roaming Participants

JANET(UK) welcomes the Wi-Fi Alliance's intention to withdraw TKIP from its products since we have long recommended the use of WPA2/AES. A useful article has been published by the Wireless Technology Advisory Service describing the problems associated with TKIP:
<http://www.ja.net/documents/services/wtas/WPA-TKIP.pdf>

The withdrawal of TKIP means that eventually users of eduroam networks will have to utilise WPA2/AES. Moreover, there is no good reason for the continuing use of TKIP wherever WPA2/AES is available.

JANET(UK) makes the following recommendations:

1. The requirement for Wi-Fi access points to be able to support WPA2/AES has been in place for some time, so it is unlikely that your wireless LANs will contain TKIP-only equipment. However, to be certain of this, wireless networks should be audited to determine their readiness for WPA2/AES and equipment replacement programmes should be drawn up as necessary.

2. WPA2/AES should be enabled on all Wi-Fi networks (and eduroam in particular) should there be any that do not already support WPA2/AES.
3. Users should receive proactive guidance to adopt the highest possible level of security. This is an important component of the transition away from WPA/TKIP. This can include help-desk technical support, documentation and web-based instructions.

Whilst the current base of Wi-Fi equipment will continue to work using TKIP for a considerable period of time, the writing is clearly on the wall. WPA/TKIP has known vulnerabilities (see article above) and there is no good reason for unnecessarily prolonging its use.

Relaxation of JRS Tier 2 Mandatory Requirement to Support WPA

In light of the Wi-Fi Alliance's endorsement of their plan to remove WPA/TKIP support and the fact that a number of organisations participating in JANET Roaming have expressed the strong desire to turn off WPA/TKIP on their eduroam networks, JANET(UK) has relaxed the mandatory requirement that JRS Tier 2 participants **must** support WPA on their eduroam networks. With immediate effect, participants need not offer WPA; however they **may** offer WPA if they wish to but they **should** provide support for WPA2 on their eduroam networks. A revision to the JRS Technical Specification will be announced shortly.

Edward Wincott
JANET Roaming Service Manager
JANET(UK)