Australian Government
Department of Defence
Intelligence and Security

DSD INFORMATION SECURITY POLICY BROADCAST JUNE 2012

BROADCAST

WIRELESS POLICY: WPA2 NOW A DSD APPROVED CRYPTOGRAPHIC PROTOCOL

The intention of this policy broadcast is to inform Government agencies that:

1. Wi-Fi Protected Access (WPA2) is now a DSD Approved Cryptographic Protocol (DACP) when used in accordance with the advice contained in the *Wireless Local Area Networks* section of the *Network Security* chapter from the August 2012 and successive versions of the *Australian Government Information Security Manual* (ISM).
2. At the time of publication of this policy broadcast, DSD is currently evaluating wireless products for inclusion on the Evaluated Products List (EPL).

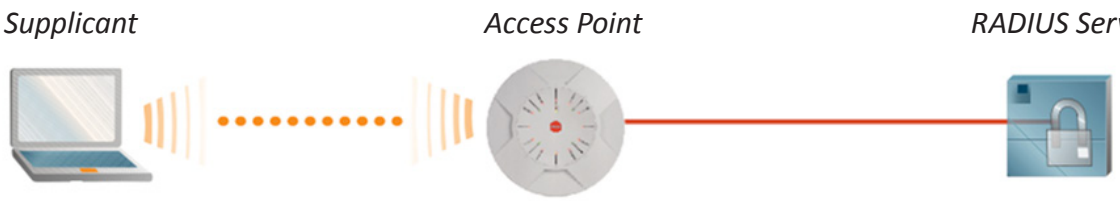
Security requirements for wireless networks

Wireless networks carry inherent vulnerabilities not present in traditional wired networks as traffic is broadcast into uncontrolled public spaces. As such, there are additional security requirements that must be taken into consideration when deploying a wireless network. These additional requirements are detailed in the *Wireless Local Area Networks* section of the *Network Security* chapter of the ISM and the Information Security Publication on Wireless Network Security.

When choosing wireless products, agencies should be aware that the security of any WPA2-Enterprise wireless network is dependent on each of the network components and how they interact with each other.

WPA2-Enterprise wireless networks typically comprise of three main elements:

1. Supplicants: software that supports the 802.1X protocol, and is therefore able to authenticate to a wireless access point (WAP) or Ethernet switch.
2. WAPs: devices that relay data between the supplicant and the Remote Authentication Dial-In User Service (RADIUS) server.
3. RADIUS servers: back-end management servers used for authentication, authorisation and accounting purposes.



Reveal their Secrets – Protect our Own

BROADCAST

WPA2 recognised as a DACP

In revisions of the ISM prior to the August 2012 release, DSD mandated that agencies using wireless networks to communicate sensitive or classified information use an additional layer of encryption on top of the AES-CCMP encryption provided by WPA2.

As WPA2 has now been recognised as a DACP, the requirement for an additional layer of encryption has been removed for the communication of PROTECTED and below information.

However, agencies must use supplicants, WAPs and RADIUS servers that have successfully completed an appropriate evaluation for PROTECTED and above information.

For PROTECTED networks, this entails choosing products that have successfully completed a DSD Cryptographic Evaluation (DCE), while for CONFIDENTIAL and above networks, this entails choosing High Grade Cryptographic Equipment.

Contact

For further information, please email dsd.assist@defence.gov.au.