DRAFT

Sharing workplace wireless networks

1 Introduction

Using office space efficiently helps us provide value to taxpayers whilst working within budget constraints. Desk sharing across different government organisations improves flexibility and ensures we make the best use of building capacity, so network infrastructure should be designed with the ability to share even if it is not an initial requirement.

Wi-Fi is a core enabling technology. Effectively deployed it promotes the flexible and efficient use of building spaces and facilitates the use of a wide range of devices.

The aims of this blueprint are to:

- enable the sharing of infrastructure without significant increase in costs
- make accessing Wi-Fi as straightforward as possible and provide adequate security for government Wi-Fi users
- support universal Wi-Fi provision in government workplaces
- ensure Wi-Fi provision is cost effective

- standardise end user device network access across wired and wireless networks

2 Executive summary

This document defines a recommended set of patterns for workplace networks. It provides:

- an access pattern for a common Wi-Fi network for all government owned and managed devices with a standard Service Set Identifier (SSID) and automatic joining / roaming
- an access pattern for controlled guest access to government workplace Wi-Fi
- the ability to retrofit these patterns to existing Wi-Fi infrastructure and Public Key Infrastructure (PKI)
- advice on coverage, density and radio frequency management for new or upgraded Wi-Fi implementations
- guidance on network separation, security, management, monitoring and migration
- Wi-Fi practices and patterns to avoid for security and performance reasons
- a single converged infrastructure to support wired and wireless devices

3 Wi-Fi technical specification

3.1 Access

Users should access government Wi-Fi networks by either:

1. fully automated joining of trusted networks by trusted devices

   or

2. user enrolled access with minimal staff management overhead

Solution providers must:

- minimise the intervention required by users trying to gain Wi-Fi access
- standardise the process by which access is provided to a specific set of SSIDs
- provide an Acceptable Use Policy (AUP) for users as part of the enrolment process
- ensure there is logging and auditing of Wi-Fi network use and be prepared to respond to Regulation of Investigatory Powers Act (RIPA) requests
- limit the SSIDs broadcast to those outlined here or document any approved exceptions
- add, amend or remove SSIDs as required in a timely fashion

3.2 Network separation

Network separation is required to make the sharing of government Wi-Fi resources a practical reality. The aim is to use industry standard mechanisms to separate traffic allowing each government organisation to deliver their services via their own logical network. We anticipate that further mitigations would be employed at the device layer to further enhance any separation provided by the wireless networks themselves.

Mechanisms are expected to be in place such that wireless Wi-Fi traffic can be isolated:

- by SSID
- by certificate authority, identified by a device certificate

Solution providers should:

- provide a mechanism for separating Wi-Fi network traffic using one of the following methods

1. connecting users of particular classes into separate VLANs at the Wi-Fi AP

   or

2. separating traffic at a central point — traffic should be securely tunnelled from the AP to the tunnel termination point where it can be more easily separated

- employ separate IP addressing, routing and access controls for each Wi-Fi network
- prioritise and manage competing bandwidth requirements between networks
- deploy guest Wi-Fi on a workplace network such that it employs all of the separation methods above
- employ additional isolation of Wi-Fi clients from one another to prevent a compromised device attacking others on the network

Solution providers may consider:

- complementing Wi-Fi with remote access solutions such as client Virtual Private Networks (VPNs) to provide end security for devices connecting back to 'home' organisation networks/platforms
- using encryption tunnelling between access points and controllers
- optionally providing 'home' organisation users access to corporate resources
- implementing location based restrictions such as geofencing tools - eg restricting access to back-end systems to specific locations

3.3 Bandwidth provision and access

It is possible to provide different characteristics to different users but it's important that users understand these different characteristics to avoid confusion.

Solution providers should:

- provide a basic content filtering service (filtered DNS is an appropriate solution)

- provide a minimal default offering that provides internet access to allow users to access their remote access gateways

Solution providers should consider the most cost effective way to manage internet access connectivity and bandwidth at a site which may include:

- transparent caching technologies to minimise the impact of software updates and give a better user experience
- Quality of Service (QoS) however this is unlikely to be a solution to undersized links
- upgrading the link bandwidth using commodity internet services

3.4 Coverage

When deploying workplace Wi-Fi solution providers should:

- deploy centrally managed Access Point (AP) hardware, each with at least 5 GHz frequency band and 802.11ac support (ideally with ac wave 2 and multi-user MIMO support)
- ensure there is sufficient uplink bandwidth from APs to building switch infrastructure
- use 802.11at - Type 2 capable switches to power the access points and allow easier upgrade to future wireless technologies
- disable low-bandwidth Wi-Fi protocols such as 802.11a & 802.11g on the 5Ghz band which should only support 802.11n, 802.11ac or faster - legacy clients can connect using the 2.4Ghz band
- configure a high minimum basic data rate and disable lower data rates — this encourages clients to roam to APs with stronger signals, and increases capacity for all clients
- plan for 50% of the AP vendor's recommended client device count per AP radio — stay well under the vendor's published maximum figure
- if possible not exceed four SSIDs per band per site — each SSID will use up some bandwidth with beaconing, probe requests and probe responses

Solution providers should consider:

- selectively disabling SSIDs at places & frequencies they are not required
- selectively disabling 2.4 GHz radios on around half the APs in large open plan areas with three or more APs — seamless device roaming in large open plan areas may be impossible within the 2.4 GHz space (5 GHz is considerably better at providing non-contending overlapped coverage)
- managing channel width — we recommend that 802.11n/ac be designed using 40 MHz width channels, wider channels (channel bonding) may be enabled on a best effort basis for 802.11ac however they should be configured such that they fall back to a non overlapping channel
- managing channel selection (radio frequency) and reducing power if necessary to minimise contention and overlapping — ideally using the automatic channel selection features present in enterprise Wi-Fi management systems as opposed to manual configuration
- enabling Dynamic Frequency Selection (DFS or 802.11h) for 5 Ghz band, which provides for a larger number of channels to be made available (note that with DFS enabled sudden changes may occur in response to detection of radar signals by Wi-Fi APs)
- enabling 'band steering' — band steering works by regulating probe responses to clients and makes 5 GHz channels appear more attractive to clients by delaying probe responses to clients on 2.4 GHz
- standards based (802.11r) support for smoother roaming for devices on the move
- if voice support is required, solutions supporting on Wi-Fi Voice Enterprise or equivalent

3.5 Administration, availability, security and monitoring

Solution providers must:

- ensure all Wi-Fi equipment and connected infrastructure is well maintained and patched for possible security vulnerabilities
- make reasonable efforts to ensure all users on any network have agreed to an AUP — it can be assumed government users on government devices have already done so
- protect access to all network infrastructure administrative accounts using 2 Factor Authentication (2FA)
- enable detection alerting to respond to potential attacks or electromagnetic interference
- have a process for monitoring and responding to alerts when they are detected
- provide remote monitoring for utilisation management and support purposes — all alert handling should be actioned by the provider, along with detecting trends in utilisation which might require future upgrades or retirements
- ensure any non-anonymised data is used in accordance with the user's agreement through an AUP or agreed explicitly

Solution providers should consider:

- subscribing to CERT UK to understand the types of threat to wireless networks in order to respond to and improve security
- that Wi-Fi networks are vulnerable to deliberate remote Denial of Service (DoS) or accidental interference from other radio frequency equipment (microwave ovens, bluetooth, wireless cameras etc) — processes should be agreed for responding to any events where radio quality is compromised for a significant period
- using tools that show both current and historical network activity — in conjunction with building floor plans and access point locations this can provide a visual insight into coverage and use
- using the location data to aid business operation, such as real time people finder, crowd management and emergency response, queue length reporting, hot desk / meeting room utilisation and path planning

- the impact of Wi-Fi controller infrastructure choices (directly wired on-premises controllers, dedicated on-net controllers or cloud-managed) have on network availability (in the event of component failure) and overall security
- security and privacy implications of devices broadcasting details of previously joined Wi-Fi networks, particularly in high-threat environments — staff using government devices could be identified as such if using their government issued devices away from a managed Wi-Fi network unless Wi-Fi is disabled on the device

3.6 SSIDs and Authentication

The proposal is for two standard SSIDs to be broadcast across all participating government buildings.

user.wifi - user enrolled wifi providing internet access only

device.wifi - wifi automatically joined by policy and authenticated with certificates

Read section 5 for more information on network access profiles.

4 Wired LAN

Solution providers must support client access as well as connectivity for the wireless access points on the same switch fabric to avoid duplication of infrastructure. Organisations with complex or high density wired ethernet requirements for example fixed IP telephony will continue to use their own switches.

Solution providers must ensure that:

- uplinks are suitably sized for the expected level of traffic and implement QoS where appropriate
- an uplink is at least twice the bandwidth of the fastest user access medium to avoid one user impacting the network
- 802.1x certificate based authentication or restriction to an authorised MAC address must be used on every accessible floor port

- appropriate security measures are in place to prevent any access to other VLANs such as dynamic trunking
- the same authentication methods and servers should be used for Wi-Fi and wired LAN ports to give a consistent user experience
- guest access is not provisioned on wired LAN ports as it could encourage undesirable behaviour if non government users are encouraged to plug into floor ports
- VLAN changes such as support for a new organisation are implemented in a timely manner
- a local RADIUS server will need to return Vendor Specific Attributes to allow the client access to the locally allocated VLAN
- VLANs are not spanned between shared and nonshared switches unless detailed agreements are in place between the two parties for spanning tree sharing and broadcast storm mitigation

Solution providers may work with end users to eliminate any requirement for per desk floor ports by moving to laptops, installing wireless cards in desktops and utilising wireless printers however the design should still support a small number of wired clients to allow for future requirements.

5 Network access profiles

5.1 Certificate based access

The authentication architecture of device.wifi is closely modelled on eduroam, with the addition of X509 certificates for device identification. An excellent technical description of eduroam is available in RFC7593.

Government issued and managed devices can have a PKI certificate installed. Depending on the device type and Operating System (OS), this might be done as part

of enterprise device management, mobile device management, or individually by an administrator.

To gain the best user experience and coverage it's crucial that organisations work in a coordinated manner. Each participating organisation must:

- support Online Certificate Status Protocol (OCSP) or Certificate Revocation Lists (CRLs) to ensure compromised or rogue devices are not able to access government Wi-Fi services
- build an IPSEC tunnel to allow two way IP communication between its RADIUS servers and the centrally managed RADIUS proxy infrastructure (detail on specific RADIUS messages can be found in RFC2865 and RFC2866)
- use or install a suitable PKI and Certificate Authority (CA) to provide suitable certificates for device authentication, and ensuring the client certificate Subject Alternate Name (SAN) contains an organisational identifier

The proposed identifier is devicename.unit.organisation.gov.uk

where:

devicename: The computer hostname or asset tag

unit: used if separate PKIs are deployed within an organisation

organisation.gov.uk: their public registered domain name

It may be possible to support existing certificates which do not conform to this standard as long as there is some unique identifier.

To aid the interoperability of different networks we will provide some information on participating networks centrally. Participating organisations should email cts-products@digital.cabinet-office.gov.uk with the CN and SAN of any device certificates you currently have deployed.

To implement access control for devices to access device.wifi Wi-Fi :

- use EAP-TLS as an authentication method

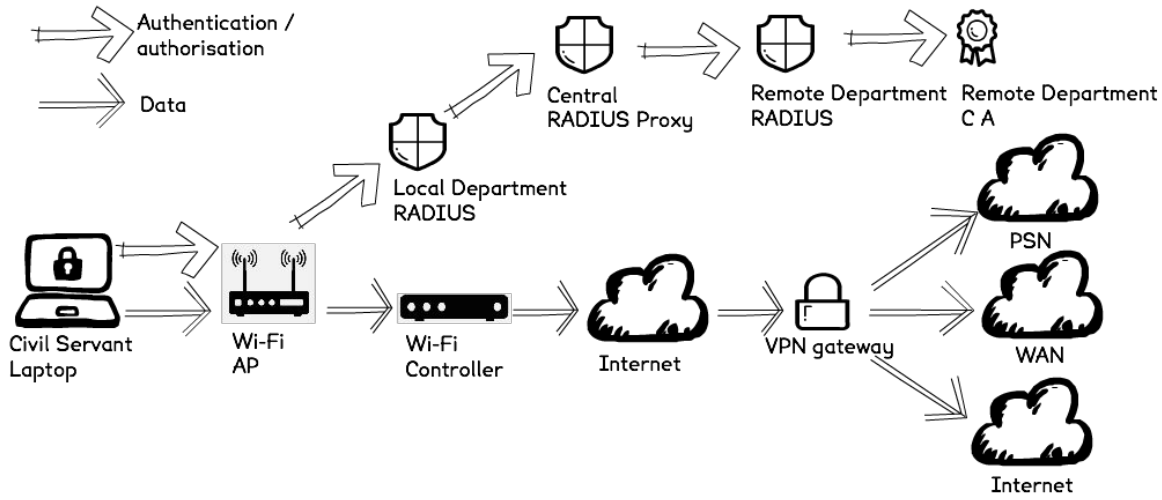
- support IT organisations to roll out device certificates to grant access to the network
- require APs/controllers or switches to check presented certificates against a central RADIUS Proxy (RP) proxied via a local RADIUS server
- provide information in the response from the local RADIUS server so that the network infrastructure can connect the client to the appropriate VLAN
- grant access to the internet to allow connectivity to organisational VPN gateways if no local network exists for that organisation
- provide VLAN separation between certificate based internet access and guest internet access

Organisations wishing to enable their staff and devices to join device.wifi should:

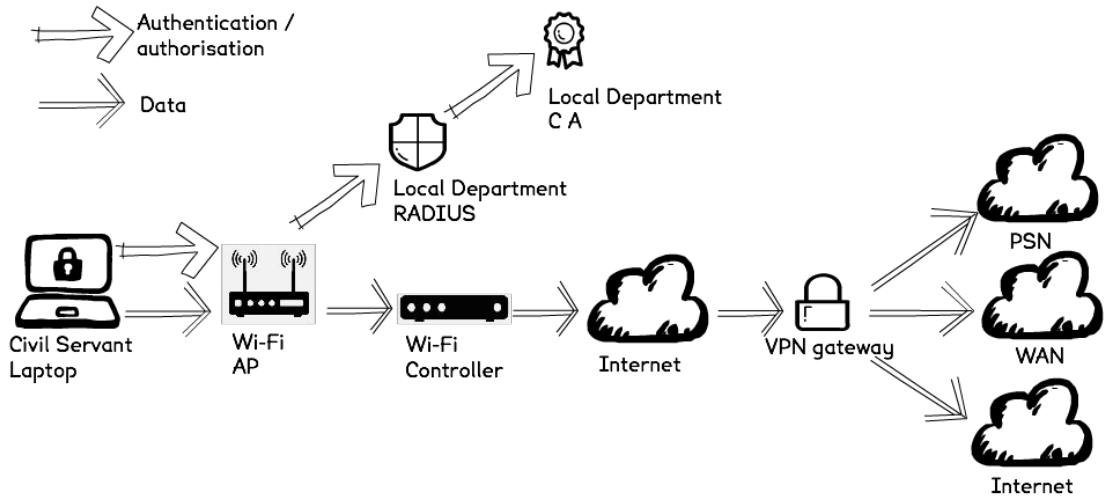
- ensure their devices are issued with a device certificate for 802.1x from their PKI certificate infrastructure
- engage with the central RP operator to allow the service to recognise the organisation or organisation name from the client device certificate SAN field
- ensure their organisational PKI is managed to an appropriate standard (eg observing CAS (CA) or other documented practice)
- provide an adequate RADIUS infrastructure to validate their device certificates
- build an IPSEC VPN to allow connections from the central RADIUS Proxy to their own RADIUS server
- ensure devices join device.wifi automatically where it is present, and refuse to join any other network named device.wifi where the network lacks the correct supporting certificate
- provide device.wifi access to other organisations on your Wi-Fi infrastructure following this blueprint

Diagrams showing example authentication and data flows for device.wifi:

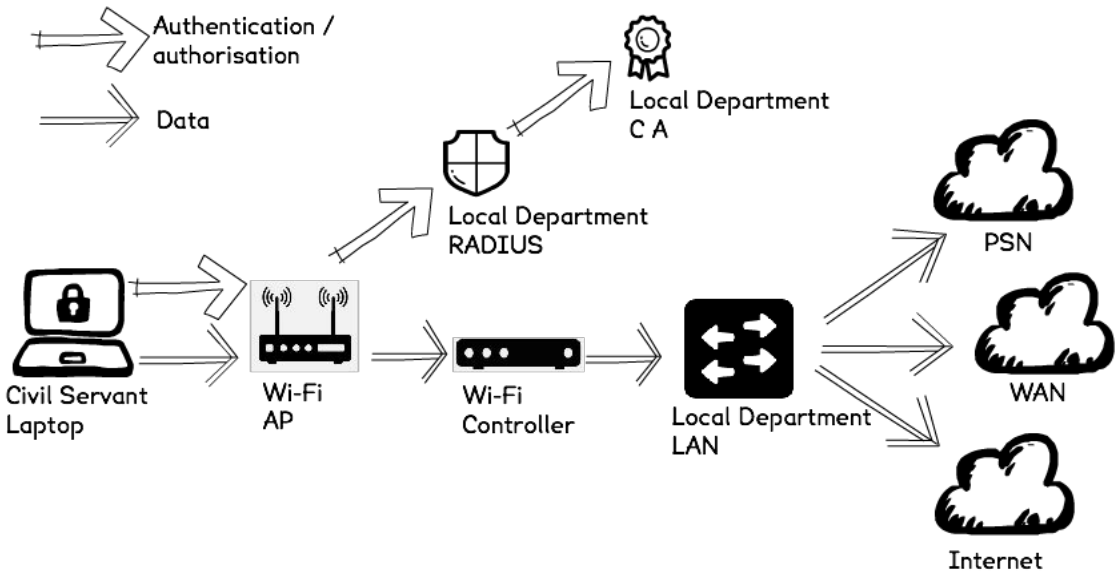
Remote organisation user (default):



Local organisation user (default):



Local organisation user no VPN (optional):



Other networks/SSIDs not shown.

5.2 Access by user enrollment

Unmanaged devices also require access to Wi-Fi services, for example organisations that have not deployed certificates to devices, visitors from outside government, staff with devices without suitable certificates, or staff who bring their own device for work use.

Solution providers must provide:

- this access method on all Wi-Fi installations
- adequate signage to inform users of the service
- sign up facilities for visitors
- different credentials providing a different encryption key per user
- authentication via WPA2-Enterprise , Hotspot 2.0 or WISPr which should all use the (MSCHAPv2 inside PEAPv0) EAP method.
- credentials with a limited lifetime

- the server certificate fingerprint to the user to confirm they are connected to the correct network

Solution providers must not:

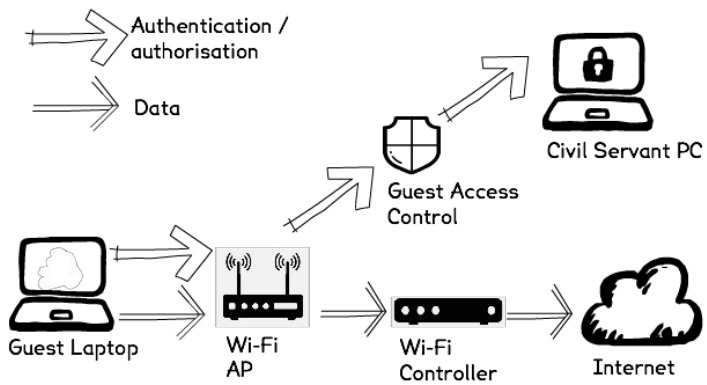
- use unencrypted/open networks – they leak too much information
- use captive portals – these interfere with always on VPNs which are becoming increasingly common
- allow the user to choose their password – they could reuse passwords in use for other Government services
- allow access to internal or privileged networks – these should only be accessible using certificates
- use pre shared keys

Solution providers should consider:

- Using the central user.wifi authentication solution when available to allow the use of the same credentials across government buildings.

SSID name is user.wifi

Diagram showing example authentication and data flows for user.wifi:



5.3 Open public Wi-Fi

The public Wi-Fi blueprint suggests a completely standalone network for public access, with no infrastructure sharing with enterprise networking. It is possible to use enterprise wireless, with appropriate network separation and bandwidth control, to provide free public Wi-Fi by separating the public Wi-Fi network traffic to provide filtered internet access only following the various control measures in the public Wi-Fi blueprint (eg captive portal for agreeing to AUP). If you provide free public Wi-Fi, you may consider managed guest access necessary to protect the data of government visitors. This decision will be informed by a risk analysis on a site by site basis.

6 Implementation

6.1 Migration Planning

For high density enterprise Wi-Fi a site survey before final tendering or implementation is essential. Typically this involves an 'AP-on-a-stick' pre-deployment map of the sites and an AP coverage/positioning plan. A post deployment check survey to ensure performance and coverage is as expected is also recommended. The brief for the survey team should specify that the goal is a a high-capacity Wi-Fi network rather than a coverage-oriented Wi-Fi network, and that there are likely to be multiple Wi-Fi capable devices per person in the building. If location services are required as part of the solution then this should also form part of the survey brief.

Suitable cabling to support the solution may not exist in buildings where all data cable ports are below a raised floor. The cost of providing new or upgraded cabling can be significant. Similarly, existing wired network switches need to support Power over Ethernet (PoE) at a sufficient level to support the required APs, higher power levels (802.11at) should be strongly considered to support future Wi-Fi equipment. We recommend that two cables are installed to each AP location to allow for the higher bandwidths of 802.11ac and future technologies.

The internal structure of each building will play a significant role in Wi-Fi network performance. Thick internal walls may attenuate radio — counter intuitively this can improve Wi-Fi performance by reducing channel contention.

Also asses the extent to which Wi-Fi coverage will extend external to the building fabric, particularly, where the building may be high profile and/or situated within a densely populated public area.

Outside of the wireless network itself, other infrastructure may need upgrading or scaling during a widespread wireless rollout, including internet bandwidth at offices and hosting centres and VPN and firewall systems.

7 Procurement

You can procure this deployment using the Network Services framework. A CCS buyers guide is being created to provide further clarity on the catalogue items required to construct this service.

8 Deprecated practices and patterns to avoid

The following patterns should not be implemented in new locations and should be phased out in favour of the patterns described earlier in this document.

8.1 Multi-tenant government buildings with overlapping networks

Government organisations often share office buildings. In some cases multiple Wi-Fi networks have been deployed by different organisations without sharing or coordination. These networks will tend to overlap, interfere and compete with one another, reducing the availability and speed of the networks for all users. A Wi-Fi survey can be commissioned to discover what problems overlapping networks are creating in an existing shared space.

For shared office buildings we recommend a single Wi-Fi infrastructure managed by an integrated controller system. Differing organisational needs can still be met with multiple VLANs and SSIDs if required. Only a single infrastructure is capable of delivering optimal spectrum efficiency in a shared space in an automated fashion. The alternative to a single managed infrastructure in a shared space is pre-surveying, extensive planning, agreements between all parties on frequency bands and power levels, further surveying, and manual tweaking of AP configs.

Government organisations must not share office spaces without at the very least coordinating their Wi-Fi network deployments.

8.2 PSK for guests

Often guest Wi-Fi is offered based on Pre-Shared Key (PSK). Typically these networks are on an SSID and can also be used for staff Bring Your Own Device (BYOD), or staff working on corporate devices (eg laptops with a VPN).

Access control in these cases should:

- use WPA2 with PSK — also called Personal WPA2 or EAP-PSK — using Advanced Encryption Standard (AES)

- have a long PSK (short PSKs are vulnerable to brute force attacks) — four randomly selected words provides an adequate balance of security and ease of use, see also CESG guidance on passwords
- advise visitors of the SSID and PSK on arrival and building signage can be used to advise staff — but this should not be visible in public areas
- rotate PSKs at regular intervals
- not provide privileged LAN network access — only standard internet access with malware filtering (see free public Wi-Fi)
- force pre-acknowledgement of terms and conditions / acceptable use policy
- not make assumptions about end user device security — devices must be isolated from one another (see free public Wi-Fi)

However, this approach is not recommended due to:

- difficulty of managing PSKs — in practice, despite the best intentions, they are seldom rotated, and when they are this is disruptive to many users
- difficulty in enforcing agreement to AUPs
- inability to distinguish guest traffic from corporate devices preventing traffic prioritisation
- offering an illusion of security which is misleading to end users
- WPA2-PSK based solutions may not support roaming from AP to AP, which may interrupt VPNs and/or break applications as users move around the building

Where deployed this approach should be considered as a legacy stop-gap pending implementation of a more robust solution.

8.3 PSK for legacy devices

There are some devices where enrollment into organisational PKI and/or VPN infrastructure is not feasible, but building LAN or organisational access is required — for instance an environmental monitoring, hand-held barcode scanning or digital signage device. Recommended access control for these devices should:

- use Wireless Protected Access 2 (WPA2) with pre-shared key (PSK) using AES
- use a long PSK — 24 random characters at least which must be rotated at regular intervals
- use hidden SSID comprising random characters
- prevent enrolment of or access to any devices that might share the PSK (eg iOS with iCloud Keychain, Windows 10 with Wi-Fi Sense enabled)
- ensure minimal privileged network access is available from the SSID — access control strictly restricted to the local network services that are required, never provide open LAN/WAN/PSN or internet access
- run at the minimum power level on the AP(s) possible to support the network and disable SSID/radio when not in use
- monitor any unauthorised/unsuccessful attempts to join the network

9 Other patterns to avoid with Wi-Fi

Site and organisation requirements will vary, and organisations will use Wi-Fi in ways not described in this document. In these cases we strongly recommend you do not:

- rely on hidden SSIDs for security
- deploy early versions of WPA (WPA2 is recommended)
- use authentication with 802.1x supported by directory user accounts and passwords (even where mediated via RADIUS and robustly protected using for instance EAP-PEAP) without a supporting PKI infrastructure providing device authentication, and radius server authentication to prevent a rogue network stealing credentials
- use EAP-PSK to provide any form of privileged LAN access except as described above if unavoidable
- encrypt with TKIP
- authenticate with EAP-LEAP or EAP-MD5
- use Wireless Equivalent Privacy (WEP) or Wi-Fi Protected Setup (WPS)
- allow any unmanaged Wi-Fi APs to connect to government networks — all should be centrally managed and monitored