eduroam(UK) Service Technical Specification 1.4

This guide delivers a précis of requirements and recommendations in checklist format with no discussion/history allowing a clear and concise deployment plan.

Requirements

Section 2 - Common Requirements

2.1.1.1. All participating organisations MUST observe the requirements set out in section 2 of this document. ☐

2.1.1.2. Participants that choose to participate as a Home organisation MUST observe the requirements set out in section 3 of this document. ☐

2.1.1.3. Participants that choose to participate as a Visited organisation MUST observe the requirements set out in section 4 of this document. ☐

2.1.1.4. Using the eduroam(UK) Support web portal, participating organisations MUST assert the type of service being provided or being worked towards and the current level of compliance of such a service with this Technical Specification. The current operational level of the service MUST also be asserted. ☐

2.2.1.1 Participants MUST designate a technical contact that can be contacted using e-mail and telephone during normal business hours. The contact may be either a named individual or an organisational unit. Arrangements must be made to cover for absence of a named technical contact owing to eventualities such as illness and holidays. ☐

2.3.1.1 Every log entry MUST state the date and time it was logged, derived from a reliable time source. The timestamp MUST be in UTC. ☐

2.3.1.2 Logs MUST be kept for a minimum period of at least three months ☐

2.4.1.1 Participants' RADIUS (Remote Authentication Dial In Service) clients and servers MUST comply with RFC 2865 [7] and RFC 2866 [8]. ☐

2.4.1.2 Participants' RADIUS clients' and servers' clocks MUST be configured to synchronise regularly with a reliable time source ☐

2.4.1.3 Participants MUST deploy at least one ORPS (organisational RADIUS proxy server). ☐

2.4.1.4 Participants' ORPSs, if operating a Home (IdP) service, MUST be reachable from the eduroam(UK) National RADIUS Proxy Servers (NRPS). ORPS SHOULD be configured to listen on UDP/1812 and SHOULD NOT be configured to listen on UDP/1645. ORPS using RadSec MUST be reachable from the NRPSs on TCP port 2083. ☐

2.4.1.5 Participants using RadSec MUST use X.509 certificates provided by the GÉANT eduPKI service [9] to identify their ORPSs. ☐

2.4.1.6 If the ORPS's RADIUS implementations support it, both the NRPS and eduroam(UK) Support Server MUST be able to receive responses to Internet Control Message Protocol (ICMP) Echo Requests they send to participants' ORPSs. ☐

2.4.1.7 The following RADIUS attributes MUST be forwarded unaltered by participants' ORPSs if present in RADIUS Access-Request, Access-Challenge, Access-Accept or Access-Reject messages. ☐

2.4.1.7.14.1 User-Name ☐

2.4.1.7.14.2 Reply-Message ☐

2.4.1.7.14.3 State ☐

2.4.1.7.14.4 Class ☐

2.4.1.7.14.5 Message-Authenticator ☐

2.4.1.7.14.6 Proxy-State ☐

2.4.1.7.14.7 EAP-Message ☐

2.4.1.7.14.8 MS-MPPE-Send-Key ☐

2.4.1.7.14.9 MS-MPPE-Recv-Key ☐

2.4.1.7.14.10 Calling-Station-Id ☐

2.4.1.7.14.11 Operator-Name ☐

2.4.1.7.14.12 Chargeable-User-Identity ☐

2.4.1.7.1 Participants' ORPSs MUST log all RADIUS authentication requests exchanged with the NRPS; the following information must be recorded. ☐

2.4.1.7.15.1 The value of the user name attribute in the request. ☐

2.4.1.7.15.2 The value of the Calling-Station-Id attribute in the request. ☐

2.5.1.1 Participants MUST publish an eduroam service information website which MUST be generally accessible from the Internet and, if applicable, within the organisation to allow visitors to access it easily on site. The website MUST include the following information as a minimum: ☐

2.5.1.1.16.1 The text of, or a link to, the participant's acceptable use policy (AUP), where applicable. ☐

2.5.1.1.16.2 A link to the eduroam(UK) Policy ☐

2.5.1.1.16.3 The eduroam logo linking to the eduroam website ☐

2.5.1.1.16.4 The type of service offered where the scope of the eduroam service is limited, such as Visited-only or Home-only; and the operational status of the service if the web page is published before the service becomes operational ☐

2.5.1.1.16.5 A link to the eduroam(UK) sites listing and location web page ☐

Section 3 - Home Organisation Requirements

3.1.1.1 Home organisations' eduroam user names MUST conform to the Network Access Identifier (NAI) specification (RFC 4282), i.e. comprise identity name, @ and realm components ☐

3.1.1.2 The realm component MUST conclude with participant's realm name, which MUST be a domain name in the global Domain Name System (DNS) that the Home organisation administers, either directly or by delegation ☐

3.2.1.1 Home organisations MUST log all authentication attempts; the following information MUST be recorded: ☐

3.2.1.19.1 The time that the authentication request was received ☐

3.2.1.19.2 The authentication result returned by the authentication database ☐

3.2.1.19.3 The reason given, if any, if the authentication was denied or failed ☐

3.2.1.19.4 User-Name in the outer-EAP and the User-Name from the inner-EAP (if a tunnelled EAP method is used) ☐

3.2.1.19.5 Chargeable-User-Identity (CUI) if one was generated ☐

3.2.1.19.6 Calling-Station-ID ☐

3.2.1.19.7 Operator-Name if one was present in Access-Request ☐

3.3.1.1 Home organisations MUST configure their RADIUS server to authenticate one or more Extensible Authentication Protocol (EAP) types ☐

3.3.1.2 Home organisations MUST select an EAP type, or EAP types, for which their RADIUS server will generate symmetric keying material for encryption ciphers and encapsulate the keys, following section 3.16 of RFC 3580, within RADIUS Access-Accept packets ☐

3.4.1.1 If the Home organisation has chosen to support PEAP or TTLS type methods, the organisation MUST create an authenticatable test account and the relevant methods MUST be supported by the test account; additionally PAP may be used ☐

3.4.1.2 If the password for this account is changed then the eduroam(UK) Support web portal MUST be updated immediately to reflect this change. If it is believed the password has been compromised then the password MUST be changed immediately and the eduroam(UK) Support portal updated as soon as possible ☐

3.6.1.1 Home organisations MUST attempt to authenticate all authentication requests forwarded from the NRPS ☐

Section 4 - Visited Organisation Requirements

SSID	WPA	WPA2	NAT	Application	Proxy	Port Restrictions	IPv6	Operator-Name	
eduroam	MUST NOT	MUST	MAY	MAY	MAY	MAY	SHOULD	SHOULD	☐

1.1.1.1 Visited organisations MUST implement the base level engineering standards defined in this specification ☐

1.1.1.2 Visited organisations MUST ensure that is not possible for a non-eduroam service to be mistaken by visitors for the participant’s eduroam service ☐

1.1.1.3 The word ‘eduroam’ MUST NOT be used in an SSID for a non-compliant network ☐

1.1.1.4 Visited organisations’ eduroam networks MUST NOT be shared with any other network service ☐

1.1.1.5 Visited organisations that provide access to eduroam for local users, or visitors from organisations not participating in eduroam, MUST ensure that the user has the opportunity to read and has agreed to the eduroam(UK) Policy ☐

1.1.1.6 Visited organisations MUST NOT offer visitors any wireless media other than IEEE 802.11 ☐

1.2.1.1 Visited organisations MUST forward RADIUS requests originating from eduroam Network Access Servers (NASs) which contain user names with non-local realms to a NRPS via an ORPS. A non-local realm name is defined as one that is neither associated with the participant nor the participant's partner where a service is provided in partnership with another organisation. Requests containing local realm names (those associated with the participant or partner organisation) MUST NOT be forwarded to the NRPS ☐

1.2.1.31.1 RADIUS Access-Requests MUST be sent to port UDP/1812 ☐

1.2.1.31.2 Access-Requests using RadSec MUST be sent to port TCP/2083 ☐

1.2.1.31.2.1 Visited organisations MUST NOT forward requests containing user names which do not include a realm nor any which are non-NAI compliant ☐

1.2.1.31.2.2 Visited organisations MUST NOT forward requests that have originated from NASs that do not conform to the requirements of this specification ☐

1.2.1.31.2.3 Visited organisations MAY configure additional realms to forward requests to other internal RADIUS servers, but these realms MUST NOT be derived from any domain in the global DNS that the participant or a partner organisation does not administer ☐

1.2.1.31.2.4 Visited organisations MAY configure additional realms to forward requests to external RADIUS servers in other organisations, but these realms MUST be derived from domains in the global DNS that the participating organisation or partner organisation administers (either directly or by delegation) ☐

1.2.1.31.2.5 In situations where a participating organisation is in partnership with another participating organisation to provide managed Visited services at sites belonging to the partner and where that partner operates its own Home service, the managed Visited ☐

service provider MUST forward requests containing user names with a realm associated with the partner directly to the RADIUS server of that partner and MUST NOT forward those requests to the NRPS

1.2.1.31.2.6 In situations where the organisation providing the managed Visited service is also working as a partner with further participating organisations, the Visited organisation MUST ensure that requests originating from a managed site of such an organisation are NOT forwarded to any other partner ☐

1.2.1.31.2.7 Visited organisations MUST NOT otherwise forward requests directly to other eduroam participants ☐

1.2.1.31.2.8 If an ORPS is not capable of responding correctly to a Status-Server request then the setting to enable Status-Server on the Support server for that ORPS MUST NOT be enabled ☐

1.3.1.1 NASs MUST implement IEEE 802.1X authentication ☐

1.3.1.2 On receipt of a RADIUS Access-Accept, the NAS and network MUST immediately forward traffic to, and from, the visitor according to the requirements set out in section 4.5; no form of local authorisation is permitted that would deny this to the visitor except in the case where network abuse has been detected ☐

1.3.1.3 Wireless IEEE 802.11 NASs MUST support symmetric keying using keys provided by the Home organisation within the RADIUS Access-Accept packet, in accordance with section 3.16 of RFC 3580 ☐

1.3.1.4 A NAS port MUST NOT connect more than one user unless the NAS is not capable of being configured other than to use the same port for the connection of multiple users and the NAS maintains client traffic separation by other means ☐

1.3.1.5 All NASs that are deployed by Visited organisations to support eduroam MUST include the following RADIUS attributes within Access-Request packets: ☐

1.3.1.44.1 Calling-Station-ID attribute containing the supplicant’s MAC address ☐

1.3.1.44.2 NAS-IP-Address attribute containing the NAS’s IP address ☐

1.5.1.1 Visited organisations MAY implement IPv4 and IPv6 filtering between the visitor network and other networks, providing that this permits the forwarding of the following mandatory protocols to external networks: ☐

1.5.1.45.1 IPv6 Tunnel Broker NAT traversal: UDP/3653;TCP/3653 egress and established ☐

1.5.1.45.2 IPv6 Tunnel Broker Service: IP protocol 41 egress and established ☐

1.5.1.45.3 IPSec NAT traversal: UDP/4500 egress and established ☐

1.5.1.45.4 Cisco IPSec NAT traversal: UDP/10000; TCP/10000 egress and established ☐

1.5.1.45.5 PPTP: IP protocol 47 (GRE) egress and established; TCP/1723 egress and established ☐

1.5.1.45.6 OpenVPN: UDP/1194; TCP/1194 egress and established ☐

1.5.1.45.7 NTP: UDP/123 ☐

1.5.1.45.8 SSH: TCP/22 egress and established ☐

1.5.1.45.9 HTTP: TCP/80 egress and established ☐

1.5.1.45.10 HTTPS: TCP/443 egress and established ☐

1.5.1.45.11 LDAPS: TCP/636 egress and established ☐

1.5.1.45.12 IMSP: TCP/406 egress and established ☐

1.5.1.45.13 IMAP4: TCP/143 egress and established ☐

1.5.1.45.14 IMAP3: TCP/220 egress and established ☐

1.5.1.45.15 IMAPS: TCP/993 egress and established ☐

1.5.1.45.16 POP3S: TCP/995 egress and established ☐

1.5.1.45.17 Passive (S)FTP: TCP/21 egress and established ☐

1.5.1.45.18 SMTPS: TCP/465 egress and established ☐

1.5.1.45.19 Message submission: TCP/587 egress and established ☐

1.5.1.45.20 RDP: TCP/3389 egress and established ☐

1.5.1.45.21 VNC: TCP/5900 egress and established ☐

1.5.1.45.22 Citrix: TCP/1494 egress and established ☐

1.5.1.45.23 AFS: UDP/7000 through UDP/7007 inclusive ☐

1.5.1.45.24 ESP: IP protocol 50 egress and established ☐

1.5.1.45.25 AH: IP protocol 51 egress and established ☐

1.5.1.45.26 ISAKMP and IKE: UDP/500 ☐

1.5.1.45.27 SQUID Proxy: TCP/3128 egress and established ☐

1.5.1.45.28 HTTP Proxy: TCP/8080 egress and established ☐

1.6.1.1 Visited organisations deploying application or 'interception' proxies on their eduroam network MUST publish this fact on their eduroam service information website ☐

1.6.1.2 If an application proxy is not transparent, the Visited organisation MUST also provide documentation on the configuration of applications to use the proxy ☐

1.6.1.3 Transport Layer Security (TLS)/Secure Sockets Layer (SSL) interception proxies MUST NOT be used for eduroam visitors ☐

1.7.1.1 In addition to the requirements detailed in section 2.5, Visited organisations' eduroam information websites MUST state: ☐

1.7.1.49.1 Sufficient information to enable visitors to identify and access the service; at a minimum this must include the locations covered ☐

1.7.1.49.2 Where applicable, the information specified in section 4.6 regarding application and interception proxies ☐

1.8.1.1 Operational eduroam Wi-Fi services, as described in this specification, MUST use a broadcast SSID of 'eduroam' in lower case characters only ☐

1.8.1.2 Organisations that are in the process of developing Home or Visited services but are not yet offering operational services MUST limit broadcast of the 'eduroam' SSID to small development environments ☐

1.9.1.1 eduroam networks MAY make use of NAT ☐

1.9.1.2 Visited organisations MUST allocate IPv4 addresses to visitors using DHCP ☐

1.9.1.3 Visited organisations MUST log the IPv4 addresses allocated to visitors and the corresponding MAC addresses ☐

1.9.1.4 Visited organisations MUST log NAT address mappings, if NAT is used as part of an eduroam implementation ☐

1.10.1.1 The WPA specification MUST NOT be supported and the TKIP algorithm MUST NOT be employed in eduroam services ☐

1.11.1.1 Both established and new deployments of eduroam Visited Wi-Fi services MUST implement WPA2 Enterprise with the use of the CCMP (AES) algorithm ☐

Recommendations

Section 2 - Common Recommendations

2.1.2.1 Participants SHOULD observe the recommendations set out in this document ☐

2.4.2.2 Participants SHOULD deploy a secondary ORPS ☐

2.4.2.3 Participants SHOULD NOT forward accounting messages to the NRPS ☐

Section 3 - Home Organisation Recommendations

3.3.2.4 Home organisations SHOULD choose a type, or types, that fulfil all or most of the 'mandatory requirements' section of RFC 4017
3.3.2.4.1 The EAP types TLS, PEAP, and TTLS are recommended ☐

3.4.2.5 The test account SHOULD be created in the organisation's primary user database. If more than one user database exists, it SHOULD be created in the user database that is likely to be most authenticated against ☐
3.4.2.6 Other privileges SHOULD NOT be assigned to the test account ☐

3.4.2.7 The test account SHOULD be configured to allow at least five consecutive failed authentication attempts without the account being locked ☐
3.5.1.8 Home organisations SHOULD educate their users to use protocols that provide appropriate levels of security when using eduroam ☐
3.6.2.9 Where an authentication request is received from a NRPS, as opposed to being received from an internal RADIUS client or NAS, a Home organisation's Access-Accept reply SHOULD NOT contain dynamic VLAN assignment attributes, unless a mutual agreement is in place with the Visited organisation. This may be achieved by the Home organisation filtering out dynamic VLAN assignment attributes if present in Access-Accept packets sent to the NRPS ☐
3.6.2.10 If the Home RADIUS server supports Chargeable-User-Identity (CUI) then Access-Accept replies SHOULD contain the CUI attribute, where CUI is solicited in the authentication request from the Visited organisation, as described in RFC 4372 ☐

Section 4 - Visited Organisation Recommendations

1.1.2.1 Where possible Visited organisations SHOULD implement the enhanced features/advanced level engineering standards in preference to the base engineering standards for their eduroam networks ☐
1.2.2.2 Visited organisations SHOULD configure their ORPS to load balance between the NRPS servers ☐
1.2.2.3 Visited organisations MAY configure their ORPS to fail-over between the NRPS server ☐
1.2.2.3.1 If the fail-over algorithm has a configurable timer that specifies the length of time after which an unresponsive server is considered unreachable, this timer SHOULD be configured to zero seconds (or as low a value as possible) ☐
1.2.2.4 Visited organisation SHOULD configure their ORPS to insert the Operator-Name attribute, accurately composed for their realm, into all Access-Request packets forwarded to the NRPS ☐
1.2.2.5 Visited organisations SHOULD request Chargeable-User-Identity (CUI) in Access-Request packets forwarded to the NRPS if CUI is supported by the ORPS ☐

1.2.2.6 If an ORPS is capable of using Status-Server (RADIUS Code 12) to detect the operational state of the NRPS, then it SHOULD be configured to do so ☐

1.2.2.7 If an ORPS is capable of being queried by Status-Server then that functionality SHOULD be enabled so that the NRPS are able to make a more informed decision on the operational status of the ORPS ☐

1.4.1.8 Visited organisations SHOULD configure the network to prevent a visitor from masquerading as an authorised Dynamic Host Configuration Protocol (DHCP) server or router ☐

1.5.2.9 Visited organisations MAY implement arbitrary IP filtering of packets addressed to other hosts on the Visited organisation's own network ☐

1.5.2.10 Visited organisations SHOULD provide visitors with unimpeded access to the Internet and *vice versa*, where local policy permits ☐

1.6.2.11 Visited organisations SHOULD NOT deploy application or 'interception' proxies on the eduroam network ☐

1.7.2.12 Visited organisations SHOULD ensure that their eduroam information website is accessible using small form-factor devices ☐

1.7.2.13 Visited organisations MAY publish the IP forwarding policies imposed on the visitor network ☐

1.9.3.14 As part of the enhanced features/advanced level standard, participants are recommended to implement IPv6 and allow routing of IPv6 on the eduroam network ☐