eduroam(UK) Technical Specification Appendices

5. Appendices

5.1. Appendix I – Summary of Requirements

5.1.1. Common requirements

1. Participating organisations MUST observe the requirements set out in section two of this document.

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

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

4. 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.

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

6. Logs MUST be kept for at least three months.

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

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

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

10. Participants' ORPSs MUST be reachable from the eduroam(UK) RADIUS Proxy Servers (NRPS) on either port UDP/1812 and port UDP/1813 (recommended), or port UDP/1645 and port UDP/1646 (if required by the participating Organisation). ORPS using RadSec MUST be reachable from the NRPSs on TCP port 2083.

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

12. 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.

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

13.1. User-Name

13.2. Reply-Message

13.3. State

13.4. Class

13.5. Message-Authenticator

13.6. Proxy-State

13.7. EAP-Message

13.8. MS-MPPE-Send-Key

13.9. MS-MPPE-Recv-Key

13.10. Calling-Station-Id

13.11. Operator-Name

13.12. Chargeable-User-Identity

14. The following RADIUS attributes MUST be forwarded by participants' ORPSs if present in RADIUS Accounting messages.

14.1. User-Name

14.2. Acct-Status-Type

14.3. Acct-Session-ID

14.4. Proxy-State

14.5. Class

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

15.1. The value of the user name attribute in the request.

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

16. Participants MUST log all RADIUS accounting requests exchanged with the NRPS; the following information must be recorded.

16.1. The value of the user name attribute in the request.

16.2. The value of the accounting session identifier.

16.3. The value of the request's accounting status type.

17. 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. The website MUST include the following information as a minimum.

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

17.2. A link to the eduroam(UK) Policy [10].

17.3. The eduroam logo linking to the eduroam.org website [11].

17.4. 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.

17.5. A link to the JANET eduroam sites listing and location web page [12].

5.1.2. Home organisation requirements

18. Home organisations' eduroam user names MUST conform to the Network Access Identifier (NAI) specification (RFC 4282 [13]) i.e. comprise identity name @ and realm components.

19. 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.

20. Home organisations MUST log all authentication attempts; the following information MUST be recorded.

20.1. The time that the authentication request was received.

20.2. The authentication result returned by the authentication database.

20.3. The reason given, if any, if the authentication was denied or failed.

20.4. User-ID in the outer-EAP and the User-ID from the inner-EAP (if a tunnelled EAP method is used).

20.5. Chargeable-User-Identity (CUI) if one was generated.

20.6. Calling-Station-ID

21. Home organisations MUST configure their RADIUS server to authenticate one or more Extensible Authentication Protocol [14] (EAP) types.

22. 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 [13], within RADIUS Access-Accept packets.

23. Home organisations MUST create an authenticatable test account. If the Home organisation has chosen to support PEAP or TTLS type methods, these MUST be supported by the test account, else PAP may be used.

24. eduroam(UK) Support MUST be informed immediately if the password for this account is changed. However, if it is believed that the password has been compromised then the password MUST be changed immediately and eduroam(UK) Support informed as soon as possible.

25. Home organisations MUST attempt to authenticate all authentication requests forwarded from the NRPS

5.1.3. Visited organisation requirements

26. Visited organisations MUST implement the base level engineering standards defined in this specification

27. Visited organisations MUST ensure that a non-eduroam service cannot be mistaken by visitors for the participant’s eduroam service.

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

29. Visited organisations’ eduroam networks MUST NOT be shared with any other network service.

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

31. Visited organisations MUST NOT offer visitors any wireless media other than IEEE 802.11.

32. 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.

32.1 RADIUS Access-Requests must be addressed to port UDP/1812.

32.2. RADIUS Accounting-Requests must be addressed to port UDP/1813.

32.3. RADIUS Accounting-Requests MUST be addressed to port UDP/1813.

32.4. Accounting-Requests using RadSec MUST be sent to port TCP/2083.

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

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

35. 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.

36. 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).

37. 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.

38. In situations where the managed Visited service providing organisation is also working as a partner with further participating organisations, the Visited organisation MUST ensure that requests originating from the managed sites of those organisations are NOT forwarded to any other partner.

39. Visited organisations MUST NOT otherwise forward requests directly to other eduroam participants.

40. NASs MUST implement IEEE 802.1X [24] authentication.

41. 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.

42. 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.

43. 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.

44. All NASs that are deployed by Visited organisations to support eduroam MUST include the

following RADIUS attributes within Access-Request packets.

44.1. Calling-Station-ID attribute containing the supplicant's MAC address.

44.2. NAS-IP-Address attribute containing the NAS's IP address.

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

45.1. IPv6 Tunnel Broker NAT traversal: UDP/3653;TCP/3653 egress and established.
45.2. IPv6 Tunnel Broker Service: IP protocol 41 egress and established.
45.3. IPSec NAT traversal: UDP/4500 egress and established.
45.4. Cisco IPSec NAT traversal: UDP/10000; TCP/10000 egress and established.
45.5. PPTP: IP protocol 47 (GRE) egress and established; TCP/1723 egress and established.
45.6. OpenVPN: UDP/1194; TCP/1194 egress and established; UDP/5000-5110 egress and established
45.7. NTP: UDP/123 egress and established
45.8. SSH: TCP/22 egress and established.
45.9. HTTP: TCP/80 egress and established.
45.10. HTTPS: TCP/443 egress and established.
45.11. LDAP: TCP/389 egress and established.
45.12. LDAPS: TCP/636 egress and established.
45.13. IMSP: TCP/406 egress and established.
45.14. IMAP4: TCP/143 egress and established.
45.15. IMAP3: TCP/220 egress and established.
45.16. IMAPS: TCP/993 egress and established.
45.17. POP: TCP/110 egress and established.
45.18. POP3S: TCP/995 egress and established.
45.19. Passive (S)FTP: TCP/21 egress and established.
45.20. SMTPS: TCP/465 egress and established.
45.21. Message submission: TCP/587 egress and established.
45.22. RDP: TCP/3389 egress and established.
45.23. VNC: TCP/5900 egress and established.
45.24. Citrix: TCP/1494 egress and established.
45.25. AFS: UDP/7000 through UDP/7007 inclusive egress and established.
45.26. ESP: IP protocol 50 egress and established
45.27. AH: IP protocol 51 egress and established
45.28. ISAKMP: and IKE: UDP/500 egress
45.29. SQUID Proxy: TCP/3128 egress and established
45.30. HTTP Proxy: TCP/8080 egress and established

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

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

48. In addition to the requirements detailed in section 2.5, Visited organisations' eduroam

service information websites MUST state:

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

48.2. Where applicable, the information specified in section 4.6 regarding application and interception proxies.

49. A broadcast SSID of ‘eduroam’ in lower case characters only MUST be used for operational eduroam wireless network services as described in this specification.

50. 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.

51. eduroam networks MAY make use of NAT.

52. Visited organisations MUST allocate IPv4 addresses to visitors using DHCP.

53. Visited organisations MUST log the IPv4 addresses allocated to visitors and the corresponding MAC addresses.

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

55. Existing eduroam deployments MAY provide WPA with the use of the TKIP algorithm until the end of December 2014.

56. Visited organisations’ eduroam networks MUST implement WPA2 with the use of the CCMP (AES) algorithm. New organisations joining eduroam MUST only implement WPA2/AES..

5.2. Appendix II - Summary of Recommendations

5.2.1. Common recommendations

1. Participants SHOULD observe the recommendations set out in this document.

2. Participants SHOULD deploy a secondary ORPS.

5.2.2. Home organisation recommendations

3. Home organisations SHOULD choose an EAP type, or types, that fulfil all or most of the ‘mandatory requirements’ section of RFC 4017 [14].

3.1. The EAP types TLS [17], PEAP [18], and TTLS [19] are recommended.

4. 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.

5. Other privileges SHOULD NOT be assigned to the test account.

6. The test account SHOUD be configured to allow at least five consecutive failed authentication attempts without the account being locked.

7. Home organisations SHOULD educate their users to use protocols providing appropriate levels of security when using eduroam.

8. 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.

9. Home organisations SHOULD respond with a Chargeable-User-Identity (CUI) attribute in an Access-Accept, if the Home RADIUS server supports CUI, where CUI is solicited in the authentication request from the Visited organisation, as described in RFC 4372 [22].

5.2.3. Visited organisation recommendations

10. Where possible Visited organisations SHOULD implement the enhanced features/advanced level engineering standards in preference to the base engineering standards for their eduroam networks.

11. Visited organisations SHOULD configure their ORPS to load balance between the NRPS servers.

12. Visited organisations MAY configure their ORPS to fail-over between the NRPS servers.

12.1. 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).

13. 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.

14. Visited organisations SHOULD request Chargeable-User-Identity (CUI) in Access-Request packets forwarded to the NRPS if CUI supported by the ORPS.

15. Visited organisations SHOULD configure the network to prevent a visitor from masquerading as an authorised Dynamic Host Configuration protocol (DHCP) [26] server or router.

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

17. Visited organisations SHOULD provide visitors with unimpeded access to Janet, and *vice versa*, where local policy permits.

18. Visited organisations SHOULD NOT deploy application or 'interception' proxies on the

visitor network.

19. Visited organisations SHOULD ensure that their eduroam service information website is accessible using small form-factor devices.

20. Visited organisations MAY publish the IP forwarding policies imposed on the visitor network.

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

22. All networks supporting WPA with the use of the TKIP algorithm should phase out such support as soon as possible and certainly no later than December 2014. WPA2 with the AES algorithm is the recommended cipher for use on eduroam networks.

5.3. Appendix III - Glossary

Term	*Definition*
802.11	See IEEE 802.11.
802.1X	See IEEE 802.1X.
AAA	Authentication, Authorisation, Accounting.
Accounting	The process of reporting the utilisation of a NAS to an accounting server.
Application proxy	An intermediary host which acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests from clients are serviced internally or by passing them, with possible translation, on to other servers. Web proxies, which fetch web pages on behalf of web browser, are amongst the commonest type.
Authentication	The process of a supplicant attempting to confirm its identity to a NAS.
Authorisation	The process of enforcing the privileges accorded to an identity, and restricting access to resources accordingly.

Bluetooth	A specification for seamless wireless short-range communications of data and voice between both mobile and stationary devices.
Broadcast	See Broadcast SSID.
Broadcast SSID	An SSID that is advertised by a WAP.
Credentials	Information, such as a password or user certificate, that is used by an authentication protocol to establish a claimed identity.
DHCP	See Dynamic Host Configuration Protocol.
DHCPv6	See Dynamic Host Configuration Protocol for IPv6.
Dynamic Host Configuration Protocol	A protocol used to assign IP configuration information, such as an IP address, to hosts dynamically.
Dynamic Host Configuration Protocol for IPv6	A protocol used to assign IPv6 configuration information, such as an IP address, to hosts dynamically.
EAP	See Extensible Authentication Protocol.
EAP-PEAP	An EAP type implementing TLS to secure a tunnel in which a second EAP type is used to provide authentication.
EAP-TLS	An EAP type implementing authentication using certificates.
EAP-TTLS	An EAP type implementing TLS to secure a tunnel in which a Diameter-based transaction is performed to provide authentication.

eduroam	An organisation representing a collection of NRENs, mainly European, that promotes inter-NREN roaming.
eduroam(UK)	The UK eduroam federation, governed and supported by Janet which provides technical support services, national RADIUS proxy infrastructure and defines this Technical Specification.
Extensible Authentication Protocol (EAP)	An authentication framework that supports multiple authentication types, including passwords, token cards, and certificates. EAP is specified in RFC2284 [10].
Home organisation	An organisation with affiliated users that can authenticate them when they attempt to authenticate at a Visited organisation.
ICMP	See Internet Control Message Protocol.
IEEE 802.11	A family of specifications for wireless LANs.
IEEE 802.11i	An amendment to the 802.11 standard specifying improved security mechanisms for IEEE 802.11 LANs.
IEEE 802.1X	A specification for port-based network access control, part of the IEEE 802 (802.1) group of protocols. It provides authentication to supplicants attached to a LAN port, establishing a network connection or preventing access from that port if authentication fails.
Internet Control Message Protocol	An IP protocol for reporting errors and other information relevant to IP packet processing.
IPv4	The most commonly deployed version of IP.
IPv6	The next generation version of IP. It includes a much larger address space, amongst other significant improvements.

Janet	Janet manages the operation and development of Janet, the UK’s education and research network.
Janet Roaming Service	The service brand name originally used for eduroam in the UK.
JRS	See Janet Roaming Service.
Man in the middle	An attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised.
NAI	See Network Access Identifier.
NAS	See Network Access Server.
ND	See Neighbour Discovery.
Neighbour Discovery	IPv6 Neighbour Discovery is an IPv6 protocol that determines relationships between other hosts on the LAN.
Network Access Identifier (NAI)	The NAI is used to address a user within a specific realm using the general format user@realm [1]. The NAI is specified by RFC4282 [27] (supersedes 2486).
Network Access Server (NAS)	A router or bridge that provides network access to a locally attached network for authenticated supplicants.
NREN	National Regional Education Network.
NRPS	National RADIUS Proxy Server. A host managed by Janet that forwards packets between eduroam(UK) participants’ ORPSs and the eduroam top-level RADIUS proxies.

ORPS	Organisational RADIUS Proxy Server. A host managed by a participant that forwards RADIUS packets between the NRPS and internal RADIUS clients and servers.
Proxy	See RADIUS proxy or Application proxy.
Public Key Infrastructure	The framework in which digital certificates are created and used, based on a public and private keys.
RA	See Router advertisement.
RADIUS	Remote Authentication Dial-In User Service. A protocol for carrying authentication, authorization, accounting and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server. RADIUS authentication is specified in RFC2865 [4] and RADIUS accounting in RFC2866 [5].
RADIUS proxy	A RADIUS server that can receive RADIUS requests from RADIUS clients and perform a decision to determine which RADIUS server the request should be forwarded onto for processing.
Router advertisement	An ND message used by routers to advertise their presence on the LAN.
Service Set Identifier	An identifier that a WAP and wireless stations use to communicate with each other.
Supplicant	A party requesting authentication from a NAS in order to access a network.
SSID	See Service Set Identifier.
TERENA	See Trans European Research and Networking Association.

Trans-European Research and Networking Association (TERENA)	TERENA carries out technical activities and provides a platform for discussion to encourage the development of computer networking infrastructure for the European research community (see [28]).
Visited organisation	An organisation that provides authenticated visitors with access to a visitor LAN.
WAG	See Wireless Advisory Group.
WAP	See Wireless Access Point.
Wireless Advisory Group	A group which provides advice and dissemination of information on wireless networking technologies to the Janet community, as well as guidance to Janet on work requirements in the wireless area.
Wireless Access Point	A bridge that enables forwarding between its associated wireless stations, and hosts on a directly-connected wired network.
WPA	A subset of the features offered by IEEE 802.11i and profiled by the WiFi Alliance. WPA is a less complete profile of IEEE 802.11i than is WPA2.
WPA2	A subset of the features offered by IEEE 802.11i and profiled by the WiFi Alliance. WPA2 is a more complete profile of IEEE 802.11i than is WPA.

5.4. Appendix IV - Bibliography

1: GÉANT2 JRA5, GÉANT2 eduroam service, http://www.geant.net/Services/UserAccessAndApplications/Pages/eduroam.aspx [2]

2: Janet, Janet Community eduroam website, https://community.jisc.ac.uk/library/janet-services-documentation/eduroam [3]

3: S. Bradner, RFC2119 - Key words for use in RFCs to Indicate Requirement Levels, 1997

4: David L. Mills, RFC 1305 - Network Time Protocol (Version 3), 1992

5: Janet, Janet NTP service, https://www.ja.net/products-services/Janet-connect/ntp [4]

6: Janet, Janet Logfiles technical guide, https://community.jisc.ac.uk/library/Janet-services-documentation/logfiles-technical-guide [5]

7: C. Rigney, S. Willens, A. Rubens, W. Simpson, RFC2865 - Remote Authentication Dial In User Service (RADIUS), 2000

8: C. Rigney, RFC2866 - RADIUS Accounting, 2000

9: GÉANT, GÉANT eduPKI service, https://www.edupki.org/edupki-ca/get-certificates/ [6]

10: Janet, Janet eduroam Policy, https://community.jisc.ac.uk/library/Janet-services-documentation/eduroamuk-policy [7]

11: eduroam, eduroam website, http://www.eduroam.org [8]

12: Janet, Janet eduroam participating organisations listing and sites locations web page, https://community.jisc.ac.uk/library/janet-services-documentation/where-can-i-eduroam-uk [9]

13: B. Aboba, M. Beadles, J. Arkko, P. Eronen, RFC4282 - The Network Access Identifier, 2005

14: B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz, Ed., RFC3748 - Extensible Authentication Protocol (EAP), 2004

15: P. Congdon, B. Aboba, A. Smith, G. Zorn, J. Roese, RFC3580 - IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines, 2003

16: D. Stanley, J. Walker, B. Aboba, RFC4017 - Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs, 2005

17: B. Aboba, D. Simon, RFC2716 - PPP EAP TLS Authentication Protocol, 1999

18: Ashwin Palekar, Dan Simon, Glen Zorn, S. Josefsson, Protected EAP Protocol (PEAP), 2003

19: Paul Funk, Simon Blake-Wilson, EAP Tunneled TLS Authentication Protocol Version 0 (EAP-TTLSv0), 2005

20: IEEE Computer Society, Supplement to 802.11-1999,Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band, 1999

21: Janet, Extensible Authentication Protocol, https://community.jisc.ac.uk/library/advisory-services/extensible-authentication-protocol [10]

22: IETF, RFC 4372 Chargeable User Identity, http://www.ietf.org/rfc/rfc4372.txt [11]

23: P. Mockapetris, RFC1034 - Domain names - concepts and facilities, 1988

24: IEEE Computer Society, Port-Based Network Access Control, 2004

25: Janet, IEEE 802.1X, https://community.jisc.ac.uk/library/advisory-services/ieee-8021x [12]

26: R. Droms, RFC 2131 - Dynamic Host Configuration Protocol, 1997

27: IEEE Computer Society, Medium Access Control (MAC) Security Enhancements, 2004 and IETF, The Network Access Identifier, http://www.ietf.org/rfc/rfc2486.txt [13]

Links
[1] mailto:user@realm
[2] http://www.geant.net/Services/UserAccessAndApplications/Pages/eduroam.aspx
[3] https://community.jisc.ac.uk/library/Janet-services-documentation/eduroam
[4] https://www.ja.net/products-services/Janet-connect/ntp
[5] https://community.jisc.ac.uk/library/Janet-services-documentation/logfiles-technical-guide
[6] https://www.edupki.org/edupki-ca/get-certificates/
[7] https://community.jisc.ac.uk/library/Janet-services-documentation/eduroamuk-policy
[8] http://www.eduroam.org
[9] https://community.jisc.ac.uk/library/janet-services-documentation/where-can-i-eduroam-uk
[10] https://community.jisc.ac.uk/library/advisory-services/extensible-authentication-protocol
[11] http://www.ietf.org/rfc/rfc4372.txt
[12] https://community.jisc.ac.uk/library/advisory-services/ieee-8021x
[13] http://www.ietf.org/rfc/rfc2486.txt