Implementing eduroam Roadmap - Part 1

Page updated 12/09/2022

On this page sections 1 - 7:

1. Concepts and terminology
2. Deciding your service type and planning your eduroam implementation
3. Choose RADIUS server platform and plan network connectivity for ORPS
4. Joining eduroam(UK) and selecting your realm
5. The eduroam Support Server website; input organisation/site details, realm name, test account
6. Install your RADIUS Server (ORPS)
7. Acquire server certificate for ORPS/NAS

See Part 2 for sections 8 - 10: [1]

8. Firewall configuration to permit RADIUS servers to work with NRPS
9. Add your ORPS to the eduroam(UK) RADIUS Infrastructure via support website and acquire your shared secrets
10. RADIUS server proxying to support a Visited service and attributes filtering

See Part 3 for sections 11 - 17: [2]

11. RADIUS Server configuration to support Home user authentication when roaming and when on campus; and attributes filtering
12. Wi-Fi service and establishment of a VLAN/network service for eduroam
13. Firewall configuration to support eduroam network service
14. RADIUS server software configuration and interoperation with user database
15. DNS Name Server Configuration
16. Test facilities on eduroam Support Server / Visitor Test / Testing a new ORPS
17. RADIUS server log keeping and interpretation of logs

See Part 4 for sections 18 - 23: [3]

18. Monitoring your own service
19. Setting up user devices - 'onboarding users'
20. Q.A. test of your eduroam implementation
21. Promote eduroam at your organisation - your eduroam web site
22. Keep your configuration details data on the eduroam Support server up to date
23. Planning Ahead and Developing your eduroam Implementation

Part 1

1. Concepts and Terminology

It is recommended that organisations planning to implement eduroam familiarise themselves with the concepts and terminology described in the eduroam deployment guide [4].
Nb. This guide is now showing its age is due for an update.

Resources:

There are useful summaries of concepts and infrastructure components in the European eduroam wiki, which may of help if there any questions unanswered from this web page: general overview [5] and elements of the eduroam infrastructure [6].

Recommended reading: for an introduction to 802.1X, chapters 1 and 2 of 802.1X Implementation at Janet-Connected Organisations [7]

Janet factsheet: IEEE 802.1X [8]

Janet factsheet: EAP Extensible Authentication Protocol [9]

2. Deciding your service type and planning your eduroam implementation

In the UK, Janet-community organisations generally fund and deploy their network systems independently with the result that there is a wide range of ways in which organisations have implemented network services. To enable disparate networks to interoperate for the purpose of user authentication and to provide a reliable and predicable service for the user, Jisc has produced the eduroam(UK) Technical Specification. This defines the service types and the technical standards that must be adhered to by all participating organisations.

2.1 Decide the type(s) of service you wish to provide

The first step in planning your eduroam implementation is to decide the type(s) of service you wish to offer for visitors and for your own users and that will best suit your organisation. There are several factors which may influence your decision. Most participants choose to deploy both a Home and a Visited service and Janet encourages this approach. Choose from:

a) **Visited only organisation**: you provide an eduroam connectivity service for visitors to your locations. This may be appropriate if you have no eligible users or are providing the service at a venue which only caters for visitors or you are providing a managed service for a client insitution.

b) **Home only organisation**: your members will be able to benefit from eduroam at other sites. Building a Home service is perhaps technically the most challenging component since the RADIUS server must process authentication requests, acting as an EAP end point and performing user database lookups to your AD/LDAP etc. It is worth bearing in mind that if you deploy a Home-only service and want to provide network connectivity for your users at your own site, you'll need to do this via a non-eduroam network service. This would mean that your users would need to have a Wi-Fi profile for eduroam and another for the local service. Nb. you are not under any obligation to provide any eduroam service for all of your network

users - you are at liberty to limit eduroam service to selected users or categories of users).

c) **Home and Visited**: you enable eduroam connectivity for your eduroam-enabled network users for when they roam to other sites and you reciprocate by providing an eduroam connectivity service to support visitors to your site. Your eduroam service can also provide eduroam connectivity for your own users (although you are not under any obligation to provide such connectivity for your own users). If you do authenticate your own users via eduroam on your own site, you may connect them to your eduroam visitors network, but you are not under any obligation to connect them to that. You can connect them to any of your other (non-eduroam) network services - which may be more appropriate since they are at their home site. The means to do this are described later in this guide.

Whilst you need a good idea of the aim of your eduroam deployment programme and need to be able to allocate sufficient resources in terms of server hardware, software and time, you don't need to decide every detail of the implementation of your service at the start of the process. Building of a comprehensive eduroam service can be tackled in stages. Indeed a step by step approach is recommended - the various areas are described in this 'roadmap' guide. Technical Support can provide advice and guidance for your project at each stage of implementation.

Recommended viewing - video of James Hooper's presentation overview of the eduroam deployment at Bristol, 'Challenges for wide scale 802.1X deployment [10]'. For slideset, see 'Resources' at bottom of this section. Although showing it's age now, this is a comprehensive overview of eduroam deployment and can be viewed in parallel with the notes below. eduroam CAT is not covered and references to 'Janet' and 'JRS' should now be understood as 'Jisc' and 'eduroam(UK)'.

2.2 Consider Wi-Fi and Network Architecture if offering Visited Service

A RADIUS service will be required for any eduroam deployment. Ideally this should be built on a resilient platform and comprise two or more servers to provide fail over and load balancing. The servers may be physical or virtual machines or you may opt for a cloud based service. Selection of the RADIUS server software is covered in the following section.

There is the possibility of outsourcing some elements of your eduroam service, but as ever, particularly regarding Home services, a degree of caution is required since eduroam relates to your core network access authentication system - the management of which is best served through in-house skills.

Consider the technological aspects of the network you wish to offer eduroam over. To provide a reasonably standard experience for users and to try reduce the amount of changes to supplicant and application settings required from site to site, the Tech Spec currently defines a single sets of network parameters based on WPA2 'enterprise' authentication with AES encryption.

[Historical note: In eduroam(UK) documentation you might occasionally come across legacy references to 'JRS Tiers'. The JRS1, JRS2, JRS3 system was withdrawn a number of years ago. Authentication now must be based on 802.1X. Captive portal/web redirection methods are no longer permitted for authentication (these used to be permitted in Tier 1 services). The only authentication method permitted now is 802.1X. Captive portal authentication methods

are no longer permitted on 'eduroam' SSID networks, on the grounds of security weaknesses. (It was included in the initial Tech Spec in order to make the service as inclusive as possible). All eduroam tiers used the same national Janet RADIUS infrastructure and users could gain authentication irrespective of the tier of the Home and Visited organisation involved. The differences to the user were simply the wireless cipher options, IPv6 availability and NATing.]

Post-authentication walled-gardens such as where users must click e.g. 'Accept' or load a virus scanner before being admitted to the network are however still permitted. Such systems may be employed for example to assure acceptance of conditions of use or to ensure device patching is up to date or other SoH standards.

2.3 Decide EAP methods to support for Home services

If you decide to offer a Home service, you need to decide what EAP authentication mechanism(s) you want to employ. This is an important decision since it will affect how your user's devices must be configured and the driver/supplicant software and certificates needed. The supplicant requirements may also affect how you support installation/configuration, whether an automated client config system can be used and the provision of instructions for your users. The decision on EAP mechanism will also probably involve a review your WLAN setup - if your site has one (nb. you don't need to have a WLAN on your home network site in order to provide an authentication service for your users when they are visiting other organisations and using the remote site guest WLANs).

Your choice of EAP mechanism will be determined by:

i) the RADIUS platform you choose (see section 3 below) (e.g. Microsoft NPS only supports PEAP/MSCHAPv2 and EAP-TLS)

ii) how the credentials on your authentication backend are held/encrypted,

iii) the authentication backend system (AD/LDAP)

iv) the rate of authentications and the number of simlutanteous authenticated users your system will support (some software engines may lack sufficient performance)

v) the client PC/laptop operating systems you wish to support and

vi) the supplicant software you have or plan to install/use on the client devices and may also be influenced by your wireless LAN (if any) setup/vendor support. This may sound complicated, but for smaller organisations the range of options is limited and the decisions are quite easy to make. Seek advice from our tech support team if in doubt.

Advice on selecting EAP methods: Geant eduroam wiki [11]

Authentication protocol and password storage in your user database: Protocol and Password Compatibility [12](FreeRADIUS HowTo)

Passwords may be stored in a DB in many forms. Clear-text, MD5 hashed, crypt'd, NT hash, or other methods are all commonly used. Authentication protocols used in RADIUS are not always compatible with the way the passwords have been stored. The following table shows which protocol is compatible with what kind of password.

PAP	?	?	?	?	?	
CHAP	?	x	x	x	x	
Digest	?	x	x	x	x	
MS-CHAP	?	?	x	x	x	
PEAP	?	?	x	x	x	
EAP-MSCHAPv2	?	?	x	x	x	
Cisco LEAP	?	?	x	x	x	
EAP-GTC	?	?	?	?	?	
EAP-MD5	?	x	x	x	x	
EAP-PWD	?	x	x	x	x	

2.4 Consider how users devices are to be configured to work with the service

The method of deploying configuration of the supplicants on devices should be given some thought. Whilst it is possible to just let users do this themselves, this approach will inevitably lead to calls to your helpdesk, user frustration and importantly, insecure device configuration due to incomplete setup of authentication server certificate and server name validation. It is a requirement that you provide device setup instructions but some form of automated setup tool/help system for users is strongly recommended. The section below on User Device Setup gives more details. A number of organisations have implemented open access captive portal setup networks which provide access to their automated setup tools for first time users.

2.5 Public IP address and DNS records for your RADIUS server

Since your RADIUS server will be communicating over the internet with the eduroam(UK) National RADIUS Proxy Servers your RADIUS server will need to have an internet facing interface and a fixed publicly accessible IP address. It will need an A (and optionally also an AAAA) record so you will need to be able to manage or request changes to your organisation's DNS space. This IP address will be added into the configuration of the NRPS and will be the registered IP address for RADIUS traffic for your organisation (i.e. realm(s)). In scenarios where you have more than one Organisational RADIUS Proxy Server, which you may decide to implement for resilience and load balancing, each ORPS **must** have its own unique public IP address. For a discussion of DMZ proxy, virtual/load balancers and downstream RADIUS see section below on networking architecture.

DNS NAPTR records - ideally your DNS management service should support NAPTR records, but this is only mandatory for organisations using realm names that do not have .uk at the top level.

2.6 Further Considerations

For participants deciding to offer Visited services (ie most organisations!), a further set of issues must be addressed, particularly the implementation of eduroam VLAN assignment on your wireless access points and wired switches. Also your firewall from the eduroam network/VLAN must permit certain traffic types as detailed in the Firewall Configuration section below.

Without wishing to complicate the process more than necessary, you may wish to consider whether or not you wish to provide guest network services to non-eduroam visitors. These may be visitors from the (very few) UK universities not participating in eduroam, visitors from non-member Further Education colleges, overseas visitors, delegates from outside the community to conferences, alumni and contractors. Some universities only offer eduroam services now! Recommended reading is the Janet guide on provision of network access for guests [14] - the simplest method is through a 'Guests' SSID with a separate non-Janet network feed. You may at the present time however provide guest accounts for use with your eduroam service, but only on strict conditions.

Help is available on all aspects of planning your service from eduroam Technical Support [15]

Resources:

- Challenges for wide scale 802.1X deployment video [10] < highly recommended viewing
- Challenges for wide scale 802.1X deployment slideset [16] < high quality slideset
- Deployment Guide [4]
- Technical Specification [17]
- Comparison of supplicants
- Inter-NREN Roaming Infrastructure & Service Support Cookbook [18] (pdf) (produced and published by GEANT2)
- Consult eduroam(UK) Technical Support for advice [15]

3. Choose RADIUS server platform and plan network connectivity for ORPS

3.1 Choice of Platform

Software - the RADIUS server platform selected will be influenced by the type of credentials employed at your organisation (AD, NDS, LDAP and how certificates are utilised) and consequently the EAP types that you could use. This in turn will affect the choice of supplicant and that may also affect the decision. Other factors will be vendor preference, budget and technical expertise. Most RADIUS platforms however support a wide range of EAP types and authentication back-ends. (Having said that, if considering MS IAS, since this does not at present support EAP-TTLS, the choice falls to EAP-PEAP(MSChapv2) or EAP-TLS (with client certificates).

Options:

- FreeRADIUS (*) [19]
- Radiator (*) [20]

- Microsoft Network Policy Server (NPS) (Windows Server 2008) website1 [21] website2 (*) [22]
- Aruba Clearpass (*) [23]
- Cisco ISE (*) [24]
- Steel-Belted Radius - Funk / Juniper / Pulse Secure [25]
- Fortinet Authenticator [26]
- Extreme Networks ExtremeCloud A3 / ExtremeCloud IQ [27]
- PacketFence [28]
- Cisco ACS (Secure Access Control Server for Windows) - no longer available [29]
- Microsoft IAS (Internet Authentication Service) (Windows Server 2003) - no longer available [30]

(*) mainstream solutions

RADIUS Server Choice Guide - comparison table **[31]** - list of RADIUS server options, costs, pros and cons, why to choose

Server Host/Hardware - Your ORPS may be physical machines or may be VM-based. For most deployments the minimum specification rack-mount server machines available these days (2019) is far more powerful than needed. A perfectly acceptable server would be:

Xeon 4-core processor 3 GHz with 4G DDR memory, RAID1 mirrored 250G hard disk, 2 x 1Gbps network interface, dual power supply.

For a virtual machine on a corporate VM platform: 1vCPU, 4GB memory, 50GB storage.

(Nb. Experience indicates that Solaris-based VM systems, whilst they function, suffer from a latency issue leading to performance limitations).

Separation of RADIUS duties - It is worth considering that the RADIUS proxy server you define as your ORPS does not necessarily need to do any authentication itself. It is perfectly OK to use a relatively simple proxy-only RADIUS server facing eduroam which then forwards any authentication requests received to your NPS server or as needed. One scenario where you might chose to do this is where your chosen RADIUS platform cannot do Operator-Name injection or respond to Status-Server requests or which has poor attribute filtering capabilities and you want to implement these best practice techniques. Another scenario might be that you wish to dedicate an internal RADIUS server to authentication duties and separate the 'proxying' to a second server. FreeRADIUS makes an ideal platform for the proxy-only server in these models.

Resilience - Once your users have experienced eduroam, they will very rapidly come to regard it as an indispensible feature of your network service and your ORPS will become a very important component. Furthermore, once your ORPS have linked into the RADIUS hierarchy of eduroam(UK) the NRPS will normally expect your organisation to be responsive to RADIUS requests sent to your realm. Whilst there is now logic in place to cope with non-responsive ORPS, it is good neighbourly practice to ensure that your ORPS are up and operational 24/7. It is therefore strongly recommened that participants deploy two fault tolerant servers for resilience. The NRPS will communicate with these in the order in which they were configured, but you will be able to adjust the priority.

Your two ORPS will normally be configured with separate unique shared secrets for

communication with the NRPS, but you can opt for the same shared secret to be used on both servers (Support server now offers you the option to 'Copy shared secrets' when you register [Add server] so you no longer need to make a request through JSD). Organisations with Cisco ISE solutions will probably require this.

3.2 Network Architecture

Positioning of your ORPS function in the topology of your network - there is no best practice recommendation as to how you plumb in your ORPS(s). You can connect one interface to your WLAN controller management network with access to your LDAP/AD and a second interface connected to the internet and publicly facing (to the NRPS), alternatively can connect your ORPS into a DMZ. The decision as to where to connect it is up to the organisation and will probably be influenced by exisiting security policy.

Firewall - whatever you choose, the requirements are described in section 8 later in this guide. Note that in the current UDP(*)/RADIUS-heirarchical model for eduroam, only the NRPS and the Support server will communicate with your ORPS so security can be very tight. Unlike, for instance web servers, which need to be open to the wide Internet, your ORPS operates only in a very narrow RADIUS environment.

(*) Technically you could employ RadSec TLS/TCP, (applicable only to Radiator and FreeRADIUS 3), but again the only communications will be with the NRPS, at present) - Nb. this is not an implementation we are currently advocating.

Network Address Translation - your ORPSs must have IP addresses that are reachable and that are resolvable by DNS lookup from the NRPS so if you do wish to employ network address translation, this must be fixed.

Downstream RADIUS servers - you may have any number of downstream RADIUS servers (not to be confused with Organisational RADIUS Proxy Servers), for instance if your organisation is 'collegiate' in structure and you support a number of semi-autonomous downstream colleges/faculties/entities. Note that these will be invisible to eduroam(UK) and we cannot assist with troubleshooting any problems you may encounter. You adopt this model at your own risk.

Proxy server or virtual/loadbalancer appliance - the FQDN/IP address you register with us on Support server is your ORPS and as far as eduroam(UK) is concered is the address that services your eduroam deployment. Implementation of a proxy in a DMZ is a valid solution in cases where such a solution is required to meet security policies - however you should recognise that this can introduce a single point of failure. The deployment of a virtual ORPS/load-balancer with multiple backend RADIUS servers is not a solution endorsed by eduroam(UK) and we cannot provide support in case of problems. You should also recognise that this introduces (unnecessary) complexity and acts as a single point of failure.

Cloud-based ORPS solutions - Azure, AWS etc have not been tested and evaluated by eduroam(UK). Provided that any such solution can meet the Technical Specification they are permitted, but eduroam(UK) does not encourage their use.

IPv6 - is the recommended protocol for providing NRPS connectivity for your ORPS. However please note that the NRPS do not accept RADIUS requests via 6to4 encapsulation. You should either implement IPv6 throughout the network path to Janet or not enable 6to4

tunnelling on your ORPS.

Help:

- Consult Technical Support for advice [15]

FAQs:

Are there any known issues with certain versions of RADIUS server software?

Yes! We of course make the general recommendation that you keep your RADIUS server software updated to the latest releases. There are particular known issues with versions of the popular choices of RADIUS sofware, including the following:

FreeRADIUS - versions prior to 1.1.4 do not support MS Vista clients due to the change in PEAP handling with Vista compared to XP. 1.1.5 and 1.1.6 had further SSL fixes to improve/fix SSL behaviour and stability in general...as well as more than 30 other bug fixes. If you are sticking to 1.1.x code, 1.1.7 was the final version of the 1.1.x product.

However there is no reason to not upgrade to the 2.0.x or preferably the 2.1.x versions of FreeRADIUS. In 2.0.5, many of the issues in 1.1.x were fixed but 2.1.10 is at the time of writing the preferred release (2.1.11 contains a number of service-affecting bugs).

Radiator - in June 2007 the NRPS had to be upgraded to the current version due to several EAP-TLS broken parts. This was leading to failed authentication attempts from visited sites for users from a participating organisation using EAP- TLS with MS IAS.

The problem, which was traced to the RADIUS exchange not completing, was resolved by upgrading our NRPS Radiator software from v 3.13 to 3.17.1. It is likely that if you are running older versions of Radiator on your ORPS and you get a visitor from a site that utilises EAP-TLS then similar problems will be encountered.

We specifically recommend that if you are still running older versions of Radiator, you should upgrade as soon as possible to the latest version. (Radiator 4.12.1 is the latest version, last modified 30 October 2013).

In addition to the above, a compounding problem was that the ipf firewall software configurations on our NRPS were set to discard UDP fragments. The script was therefore changed to pass fragments using the keep frag keyword. If you employ the ipf filewall on your ORPS, you should check this.

What RADIUS server software are eduroam participants using?

Number of ORPS installations by RADIUS software type:

Number of ORPS installations by RADIUS software type

	Dec 2006	July 2007	Dec 2007	Apl 2008	July 2008	Apl 2009	Aug 2010	June 2013	June 2014
FreeRADIUS	27	51	59	64	74	74	106	256	308
Microsoft IAS/NPS	12	15	16	21	24	31	47	119	153
Radiator	13	13	13	15	14	16	16	28	34
Cisco Secure ACS	2	3	4	4	10	15	14	23	37
Cisco IOS	0	1	1	1	1	0	1	1	1
Aruba Clearpass	-	-	-	-	-	-	-	-	7
Juniper Steel-Belted	-	-	-	-	-	-	-	-	1
Other	-	-	-	-	-	-	-	-	8
Typo / not stated	14	9	5	6	4	5	0	17	12

4. Select your Realms and Join eduroam(UK)

4.1 Selecting your realm

An important parameter to decide is your organisational realm name. In eduroam, usernames are of the form 'userID@realm [32]'. The realm name is the '@camford.ac.uk' part of the username. The realm name identifies the organisation the user is affiliated with and is used to determine which RADIUS service the user's authentication request will be processed by. When the user roams to other eduroam member organisations, the RADIUS service at the visited venue recognises that the realm is not supported by the local authentication service and forwards the user's authentication request to the national RADIUS service. The realm is then used by the national and international RADIUS eduroam infrastructure to forward the request to the user's home organisation RADIUS service for authentication.

Your organisation must be entitled to use the requested realm name, i.e. it must be (or be derived from) a DNS name from the organisation's registered DNS namespace. It is expected that most organisations will request their DNS domain name (eg. 'camford.ac.uk') although it is perfectly acceptable to request a sub-domain name (eg. 'computer-science.camford.ac.uk').

More than one realm name can be assigned to your organisatiation - you can request additional realms at any time through Jisc Service Desk / 'Submit a service request' form. Provision of sub-realms is possible by self-service through the Support server portal - see FAQ below.

Internal AD domain container names cannot be used (obviously these won't be configured in remote RADIUS servers nor will they be capable of NAPTR record lookups in DNS).

Hint: Your RADIUS authentication server will need to be able to handle the realm identifier in auth requests. If you have previously only used AD DOMAIN\userID format [33] for usernames in Microsoft AD you can add support for userID@realm [32] format by using a suitable global UPN (user principal name) in the AD. This is docmented in Microsoft Active Directory and NPS technical manuals.

4.2 Complete the application form

The next step is to apply to join the eduroam(UK) federation. This is a very straightforward process - you simply complete the membership application form, which asks for management, technical contact and intended eduroam service deployment details. The online form must be endorsed by a senior member of your organisation.

Complete and submit the eduroam application form [34]. Following a validation check and acceptance of your membership to the eduroam(UK) federation an account will be created for you on Support Server and a 'welcome to eduroam(UK)' e-mail will be sent out. In addition to providing the welcome pack of essential information, this e-mail will contain your account name and a single user token to enable you to access to the Support Server web site. The Support portal provides the self-service tool for managing your eduroam(UK) participation details and allows you to access your organisation service status and alerts, diagnostic tools and view of the NRPS logs relating to your organisation.

Your initial access to Support server will be restricted to read-only for your organisation and you must change your password in order to be access the portal with full admin rights for your organisation. You can change your password via your account settings by clicking on the

person icon on the top right of the page.

Your eduroam(UK) Support account will enable you to manage your participation details including the creation of sub-realms under the primary realm. (If you require an additional primary realm, these may be requested by submiting a support request). Support server allows you to register your organisational RADIUS proxy servers and acquire the requisite shared secrets. You will also be able to carry out tests, view the alerts generated by the Support server monitoring system and access error reports derived from the national proxy server logs. Finally, you will be able to tell us about the service you provide at your site(s), which will then be advertised to the eduroam community. For further details see the section below.

If you require any guidance or help, simply request support by using the request form via the link at the bottom of all Support server web pages or send an e-mail to help@jisc.ac.uk [35].

FAQs:

What support services are available?

To underpin the service and to support organisations joining and participating in the service, a comprehensive, fully resourced support structure has been put in place which provides:

- Pre-deployment support – planning and selection of RADIUS server hardware and software and supplicant systems
- Technical support during implementation
- Post-implementation support on technical issues
- Dedicated eduroam Support server with web front end for eduroam site administrators only
- Participanting organisations RADIUS service monitoring system
- Dedicated e-mailing list for technical and service announcements
- A chargeable consultancy service
- Comprehensive technical and promotional documentation
- eduroam service type and operational status table
- Locations map showing where eduroam is available and the service details at each site

Can individuals join the eduroam from Janet? Is there a way for an individual to obtain an eduroam ID without the user's home institution having to join eduroam?

No. Users must have registered network logon accounts at their home organisations and in order for individuals to use their credentials for authentication at eduroam participating sites, their home organisation has to join eduroam and install a RADIUS server which is peered with the national eduroam proxy servers.

The aim of eduroam is to reduce the amount of administration required both by organisations offering guest access to their networks and for visiting users. This is achieved by users being enabled to use their own usernames and passwords when roaming. Janet has set up the NRPS network and the support service to facilitate this through the eduroam mechanism. There is no facility for users to be issued with independent IDs since this would involve another tier of administration (and defeat the aim of the service).

Do eduroam users have to be registered network logon account users at participating organisations?

Yes. Users must have a network account at their participating home organisation in order for their authentication requests to be validated when they attempt to log on at a visited organisation. They must be registered on their home organisation's AD, LDAP, NetWare etc user database. This is because Janet connected organisations are not permitted to just let anyone onto their guest networks and to access Janet/the Internet via Janet. Furthermore, there is a logging requirement for organisations to record the date and time and user name of eduroam enabled authentications. We have to be able to track down a visiting user if ever there is any security or anti-social usage incident - hence the need to limit the service to registered users.

Can I have a sub-realm for my organisation?

Question a) Does the eduroam spec allow us to configure ORPS to forward user@department.myorganisation.ac.uk [36] RADIUS requests to the department in question's RADIUS server?

Question b) If so, will the NRPS strip off 'department' and forward RADIUS requests to the example-org ORPS?

Answer a) Yes - you can register any number of sub-realms (e.g. 'student.camford.ac.uk') as you like. To create a new sub-realm, click on the Configure tab for your organisation on Support server, scroll down to the grey 'Realms' panel and click the [Add realm] button. Enter the sub-realm name into the 'Realm name' field and enter your test account credentials. Click on the [Save] button.

Answer b) No - the NRPS will forward requests bearing these realms to your ORPS unchanged. Because the realm is left unchanged by the NRPS, you can perform additional proxying within your organisation if you wish (for example, to route the request to a departmental RADIUS server). This permits delegation of authentication to other units within your organisation; alternatively the realm component of inner identity of the user (e.g. during the MSCHAP phase if you are using PEAP/MSCHAPv2) might be utilised as part of the authentication/authorisation process for the user - but note that the phase 1, outer identity of the user MUST NOT be used as the sole basis of user authentication.

Can I request a wild-card realm?

No - however, you are able to define as many "sub-realms" as you require. For example, if your realm is example.ac.uk, you can additionally define bar.example.ac.uk and foo.bar.example.ac.uk.

5. The eduroam(UK) Support Server website; your account, input organisation/site details, realm name, test account

5.1 Welcome to the eduroam(UK) Support Server

Introduction: The eduroam(UK) Support Server (v2) support.eduroam.uk is the primary tool available to you to manage the interoperation of your eduroam service with the national eduroam(UK) infrastructure. Through the web portal you can register your RADIUS server(s) (ORPS) and be provided with the RADIUS shared secrets necessary for peering of your ORPS(s) into the eduroam hierarchy. The portal also gives you access to a wealth of test and monitoring tools, including on-demand and routine service status and error monitoring. The server gives you access to views from the national proxy server authentication and error logs to assist in troubleshooting. Last but not least, the server provides the means for you to provide location and Wi-Fi details of the eduroam service you provide to visitors. This data goes into the European eduroam database allows your service locations to be advertised through the European and UK eduroam service web maps and the eduroam Companion App for smartphones. (The Service Provider Assurance Tool system, which was a feature of Support Server v1 is not available through the current Support Server v2 system).

Credentials for accessing Support Server: When your organisation joins eduroam(UK) a welcome e-mail will be sent to the management and technical contacts listed on the Application form. In addition, an account setup e-mail will be sent to the technical contact, 'Your eduroam support portal password'. The e-mail contains a single-use password reset token which will be valid for one hour. (If this expires, you can request a fresh one by going to the Support portal login page https://support.eduroam.uk/login [37] and click on 'Need help?' underneath the [Sign in] button. In the popup box that appears, click on 'I need a password or token reset', enter your account e-mail address and click [Submit]. This results in a fresh token being e-mailed to you - 'Your eduroam support portal password'). Clicking on the link in the e-mail will log you in with restricited access privileges to Support server and take you to your organisation's home page (monitor). Below the menu bar you'll see the message displayed as below:

> You have logged in with a temporary token and your privileges have been restricted.
> Please (re)set your password – the user menu is in the top right corner. After you have
> set your password, please log out and back in with your password to enable your privileges.

You will be able to access the functions available to Helpdesk level account holders ('Status overview' and 'Troubleshoot' pages). Once you have set your password by following the 'User settings' options on your account menu (**click on the grey person icon on the top right of the page - User settings / Logout**), logged out and logged back in, you will have access to the functions of the Support portal available to Admin users.

If you forget or wish to change your password at any time you can click on Need help? under the [Sign in] button on the login page, or if already logged in, go to 'User settings' via the account icon on the top right of the screen.

If you have newly taken over the role of supporting eduroam at your organisation and have not already been added to the Support server, an account can be created for you by existing Admin account holders. Alternatively you can send a request, which must be authorised by a management level contact at your organisation, to the eduroam(UK) Support team via Jisc

Service Desk. We can also arrange a fresh Joiner's induction for you if you wish.

Additional accounts: You can add additional accounts for your colleagues or IT contractor/consultant to access Support Server - click on [Add user] in the Accounts panel on your organisation's Configure page on the portal. This is useful where a team supports the service or when the lead sys admin or Technical user contact details need to be altered in the event of staff changes. See Responsibilities of the eduroam System Administrator [38] for details of how to do this. With the introduction of Support Server v2, our policy is now that access to Support Server should be through individual user accounts - for reasons of security and accountability.

Managing multiple organisations: Individuals may be authorised to administer the eduroam configurations of more than one organisation - this is useful for instance when multiple college entities are members of larger group, or when mergers are pending; or a consultancy firm is contracted to support multiple eduroam member organisations. Contact help@jisc.ac.uk [35] to request access - network manager/director authorisation will be required.

Service announcements mailing list: The e-mail addresses of all user accounts on the Support Server are automatically added to and maintained on the restricted and moderated jiscmail eduroamUK-support listmail service. The list is used solely for announcements and advisory notices from the Jisc eduroam(UK) team. Postings by mail list members will not be released. Inclusion on this list is a mandatory component of membership of eduroam(UK). Membership of the list is hard-coded to the list of admin account holders in the Support Server database and additional e-mail addresses cannot be added to the jiscmail list. For discussion with other eduroam sys admins and others interested in eduroam topics, the eduroam-uk jiscmail list is available and you are encouraged to join this.

5.2 Assertion of service type and service level

Participation in eduroam is to a large extent based on trust and it is important that you make and keep up to date certain assertions about the service that your organisation provides.

Service Type

Log in to Support Server: via https://support.eduroam.uk/login [37]

Click on the 'Configure' tab.

In the purple 'Organisation settings' panel, click on the 'service type' box. The 'eduroam service type' dialogue box opens.

Click on the type of service that you are implementing

When complete click on [Save]

If you change the type of service your organisation provides, you must update this service type assertion.

Service Deployment status

Click on the 'Configure' tab.

In the purple 'Organisation settings' panel, click on the 'service deployment' box. The 'eduroam deployment' dialogue box opens.

When you have completed your deployment and are ready to provide a live service:

Tick the 'Deployment complete' box

Click on [Save]

...

The section below is due for revision

> Log in to the eduroam(UK) Support web site https://support.eduroam.uk [39] using the credentials supplied during joining/induction. The user name will usually be your organisation's realm name (e.g. 'camford.ac.uk'). Your password is known only to you, but you can reset it if it has been forgotten. The new password will be e-mailed to the primary tech contact address at your organisation; it is to be hoped that this is you(!) If you have newly taken over the role you will need to be registered, please contact Janet service desk.

Once you have logged in, the left hand menu presents the following options:

- General
- **eduroam UK configuration**
- my account
- log out

The first two boxes enable you to assert your service's level of compliance and progress towards full compliance with the eduroam(UK) Technical Specification and your declaration of whether you offer a compliant service yet. Since eduroam is based on a web of trust between participants these are important declarations and in addition determine whether the Nagios monitoring tests are enabled for your ORPS.

Select the relevant 'Compliance level' (Home, Visited, working towards etc.) and 'Service level' (None or Compliant service) from the drop down menus. Click the [Update compliance] or [Update service level] buttons. You must keep these assertions up to date as your eduroam service deployment progresses.

If our Nagios monitoring system detects non-compliance with a mandatory requirement of the Technical Specification, a non-compliance 'Detected issues' box will pop into position as the third box down. Issues triggering this include not having provded the URL of your eduroam service information web site (see later section regardin this).

5.3 Description of Feature Boxes on the Organisation Configuration Page

Normally the third box down will be the 'eduroam(UK) Minor issues' box. Should any issues be detected with your organisation's service an alert will appear here. These will include non-compliance with recommended measures defined in the Tech Spec. These include sending invalid authentication requests to the NRPS, not injecting Operator-Name, no NAPTR entry for RadSec for your realm in DNS. Such omissions are considered as minor issues since not all RADIUS platforms support the measures and therefore these are not mandated. But if you can resolve these issues, please do so.

Also displayed are boxes for:

i) **eduroam CAT invite** - **after** you have asserted that you provide a Home service AND that it is conforms to the Tech Spec, you can request an account on the eduroam (user device) configuration assistant tool which is operated by eduroam Europe. More info [40].

ii) your organisation's **legal name and trading name** (the latter is used for organisation identification on the eduroam participants maps and listings)

iii) **your eduroam test account name** (you will be able to make an entry in this box once you have changed your asserted compliance level from 'none'), test account realm, test account password (which will only ever be seen by eduroam support staff), EAP method to be used by the eduroam monitor test and option for potentially 'poisonous' attributes to be included in Access-Accepts from the Support Server when you run a Visitor Simulation Test (see later section for more details)

iv) the **URL of your eduroam service information web page** - where you publish key information about your eduroam service provision (AUP, locations where eduroam is available, how to use the service/user guide to configure laptops etc.) See later section for more details and Content for eduroam info web page guide [41]. Please keep this information updated if you make any changes.

v) **Problem log files** - 'Examine log files for this organisation by clicking HERE' the HERE link enables you to view files of extracts from the previous day's NRPS error logs relating to your organisation. Each day the NRPS error events log is parsed for errors and sorted for each member organisation and type of error event. There are three types of log file - The error log files are retained on Support for one month after which they are deleted.

vi) **Syslog server** - coming soon. If your organisation operates a syslog server, we can send syslog data to it in real time. If you would like to benefit from this facility, enter the FQDN of your syslog server in the box and when the feature goes online we'll start sending them the data.

vii) **Security auditing** - you can authorise the eduroam Operations Team, eduroam UK or one of our agents e.g. Jisc CSIRT, to perform security assessments of your ORPS server security or ORPS policies via the eduroam infrastructure.

viii) **Primary user** - your Support Server account name and the e-mail address of the primary user we will send new passwords to should you reset the account and to which we will send out service advisory notices.

5.4 Update 'default location'/enter new site details

> Click on **'Site Locations'** from the eduroam Configuration left hand menu:

- RADIUS proxy servers
- Realms
- **Site Locations**
- Test
- Users

Having completed/updated details of your organisation name and post code in the step above, a default site record will have been created. Under 'Site Locations' on the left hand menu, you will see that 'default site' appears and in the right hand pane a blank 'Create a new site location' panel is displayed.

> Click on 'default site' in the left hand menu. The right hand pane now displays the default details for your main site (limited to postcode and default name, note this Site Location name is 'default location', which will stick out like a sore thumb in the internationally published data unless you update it). Please input the details about the service provided in the various fields. These include; site name and post code, site address (optional), the number of APs, number of RJ45 sockets providing eduroam (eduroam is about 802.1X on wired too), wireless ciphers, NAT if implemented, network traffic proxy if implemented, traffic port filtering if implemented, IPv6 avalability, site support contact details (optional).

If you just provide us with a post code, the Support server will automatically generate co-ordinates which will be used in various location dispaly systems. To ensure that your site location is accurately positioned on the eduroam sites locations map and in the eduroam Companion we recommend you input actual co-ordinates (easily determined from web tools such as Streetmap).

The information provided on this site details page will be used to populate UK members sites data tables on the Community and Jisc web sites and is also used by the eduroam organisation to produce the international and UK sites locations map. The information enables organisations to provide a detailed information about their services to visitors and the rest of the eduroam world. Note, *everything* on this page will be published including the site location description and contact details (hence the site contact details are optional).

> Finish site information update by clicking on the [Update Location] button.

5.5 Details about further sites

> If you have multiple sites at which you provide eduroam, you can create records for these by selecting 'Site Locations' on the left hand menu and then complete the necessary details on the blank 'Create a new site location' panel that appears in the right hand pane. By 'site' we

mean a contiguous area of eduroam coverage, so if a campus comprises a number of adjacent buildings in which eduroam service is available, we define this as a singular location. You may provide greater granularity if you wish, but there is a risk that the number of site records will become unmanageable if organisations provide 100s of locations each! Members typically define a handful of sites to upto c.120 for those with faculties/buildings/libraries/halls of residence dispersed throughout city centres.

Use of co-ordinates allows you to get your site much more accurately positioned on the eduroam sites location map and on eduroam Companion. It is therefore recommended that if possible you use co-ordinates (easily determined from web tools such as Streetmap). If you have multiple sites at one post code, to enable the eduroam map to render the locations and for the info you are providing to be of any use in Companion, you **must** use co-ordinates.

If you have a large list of sites which will result in maintaining up to date information becoming an unmanagable administrative burden using the Support portal, you can ask us to update your sites information by sending us a csv file.

> Finish site location creation by clicking on the [Create Location] button. If successful, the new site name will appear in the left hand menu under 'Site Locations.'

5.6 Your Realm(s)

Click on **'realms'** from the eduroam Configuration left hand menu under your organisation name:

- RADIUS proxy servers
- **Realms**
- Site Locations
- Test
- Users

> The realm name(s) that you requested on your application to join will be displayed. You can create and delete additional (sub-)realms for your organisation if you require to. Do not delete your top level domain name (if you do, a request must be made to service@ja.net [15] to have this reinstated).

5.7 Create and register your eduroam Test account

Your eduroam Test User account is an important component of your eduroam implementation and is mandated in the Technical Specification for Home service participants. It is utilised by the eduroam Support server 'Status summary' monitoring system and by the on-demand 'Roaming authentication tests' which you as eduroam Support server site administrators can run to test your deployment. The same password is used by the Support server Visitor simulation test which you can use to verify auth-request forwarding for visitors by your ORPS.

Your test account must be created in the same database that your user authentications are made against i.e. your AD/LDAP database. This will enable the eduroam Support roaming user test to emulate a remote user and to verify your 802.1X authentication setup. It is important that this account is NOT subject to account locking policies (which you may have for general users) that would cause the monitoring tests running on Support server to fail. So, it should allow at least 5 consecutive failed authentication attempts and should not be subject to

password change or account expiry policies – unless you can ensure that refreshes are reliably scheduled. (We recommend against account locking measures in general since there are now alternative measures available).

To make use of your test account you must enter the credentials into the server as described below. If you subsequently change the credentials, whilst on-demand test will work straight away, the Status monitor test will only use the new details after the routine configuration refresh which takes place hourly, on the hour.

Register your eduroam Test account details on the Support server (Home service participants only)

> Click on the **'Configure'** tab and scroll down to the grey 'Realms' panel

The name of the realm(s) that has been assigned to your organisation will be displayed, together with any sub-realms that you may have created. You will also see any test user account-name, if one has previously been registered and the results of the NAPTR record lookup.

Move your cursor to the realm line and you will see the test account password if one has previously been registered.

> Click on the realm line

A popup box will appear. Enter your desired Test account name and password. The test account needs to be in the normal user directory that which you use to register your users. You can edit Test account details at any time if you wish.

You can delete any realms you no longer require, provided that at least one realm remains for your organisation.

> When you have made any changes you wish to, click on the [Save] button.

The [Reset] button discards any changes you have made and keeps you in the popup box.

Using the Roaming user test - once the steps described in sections 8, 9, and 10 have been completed)

This test is useful once you reach the stage of configuring your firewall to permit inbound authentication requests and configuring your RADIUS server to support roaming user authentications.

> Click on the '**Troubleshoot**' tab

The tests available are Certificate Check; ICMP ping; Roaming authentication tests; Visitor authentication test; VSA filtering.

Note that if you have more than one ORPS, an ORPS drop down menu will be visible. You can use this to select which ORPS you wish the test to be directed to.

Note that if you have more than one realm registered, a realm drop down menu will be visible. You can use this to select the realm name to be used by the Roaming user test.

Help is available for the Tests - click on the (?) button on the top right of the Tests panel.

> **Select the test options** you want

On the Tests menu bar the options available are - NRPS; IPv6; RFC; CUI

Choose the source parameters you require:

NRPS to execute the test from - Roaming0,1, 2 can be selected from the drop down list.

IPv6 - selecting this results in the test being run over IPv6; if no AAAA record is present, the test result will be 'DNS' in red.

RFC (applicable to EAP-TTLS and PEAP only) - if the RFC is left unticked, the auth request will use an outer identity which matches the inner identity. This will be the eduroam test account username you registered above. If the RFC box is ticked, the auth request will use an anonymous outer identity, ie the userID part will be blank (e.g. @camford.ac.uk) as specified in RFC 5281. Nb Both versions of the test should succeed if the ORPS is correctly configured.

CUI - will only be relevant if you have configured your RADIUS server to return a CUI in an Access-Accept in response to a request in an Access-Request. (Many RADIUS servers do not support CUI). You'll need to check the debug output for a non-null value of CUI beinf returned by your ORPS.

> Scroll down to the '**Roaming authentication tests**' box

Click on the required EAP method you wish to test. Most deployments support PEAP/MSCHAPv2 (used by Microsoft NPS)

The result can be 'OK', 'Reject', 'Fail', 'NoRpl' or 'DNS'. The 'DNS' status is returned when the target ORPS FQDN fails to resolve to an IP address of the chosen type (default v4 or v6 if selected).

You can click on the result text to view the full eapol_test debug output.

Your organisational firewall must be made ready for the eduroam service at some point. This involves configuring it to permit the passage of required protocols. This can be done now or you can do this after your 802.1X system has been set up and you have tested authentication locally on your campus network.

See: Firewall configuration

6. Install Your RADIUS Server (ORPS)

If you have not already implemented RADIUS on your network, a RADIUS server of your choice must now be deployed. We recommend that software is installed on dedicated

hardware or on a virtual platform. Cloud based solutions (Azure/AWS etc) are also feasible although this introduces complications.

It is strongly recommended that your ORPS is highly fault tolerant and preferrably a resilient dual-ORPS system is put in place. The reason we recommend you depoly a resilient dual-ORPS system is two-fold, a) for your own service continuity b) but most importantly from an eduroam(UK) viewpoint, to ensure that your realm always has an ORPS available to service incoming authentication requests from the NRPS. If your realm for some reason stops responding to auth-requests and these continue to arrive from your users at remote eduroam sites, a huge amount of NRPS resources will rapidly become tied up and the performance of the NRPS will be drastically reduced. This is because since RADIUS uses UDP, each auth-request results in a UDP socket being held open in the NRPS UDP buffer awaiting a reply. If your realm continues to fail to reply, the load on NRPS resources will increase to the point that effectively service will be denied to other operational eduroam sites - which are handling auth-requests properly. To prevent this situation from affecting the performance of the national service, eduroam will have no option but to suspend service to your ORPS.

A multiple ORPS deployment will require configuration of fail-over or load balancing between the two ORPS. Different systems have differing requirements, but normal practice is for each of your ORPS to have a unique set of shared secrets with the NRPS (the shared secret between roaming0 and ORPS1 will be different from the secret between roaming0 and ORPS2). If your configuration requires both ORPS to have the same shared secret for each NRPS, please open a service request ticket with Jisc Service Desk and we will configure the NRPS accordingly.

Internet/Firewall connection

Provide internet connectivity for your ORPS. The internet facing interface will need a fixed publicly accessible IP address. The most usual deployment of servers presenting an interface to the internet involves connection via a firewall. Configuration of the firewall is covered in section 8 and 13.

DNS 'A'/'AAAA' record for your ORPS

Your ORPS must have a unique public-facing IP address and FQDN. The first step is therefore to give your server a DNS name and to create an entry in your DNS zonefile - an A (and optionally also an AAAA) record. Nb. If you are deploying more than one ORPS for resilience/load sharing, each of your ORPS must be given a unique IP address and FQDN. If you are using NAT for some reason you'll need to have static translation in place.

Network connection to Wi-Fi/network controllers

Your ORPS will need a network connection to your Wi-Fi controllers / network switches in order for those 'network access servers' to send RADIUS packets to your ORPSs. This network connection is different from the Wi-Fi service used by user devices to send authentication requests to the APs/WLCs and separate from the VLAN/network service that eduroam user devices will be connected to. Wi-Fi/network service provision is covered in section 12.

Resources:

- Inter-NREN Roaming Infrastructure & Service Support Cookbook [18] - covers various RADIUS platforms (dates from 2008, but still very useful) - 404 error now

FreeRADIUS

- FreeRADIUS official website [19]
- FreeRADIUS website configuration for eduroam guide [42]
- Janet 802.1X Implementation at Janet-Connected Organisations [43] - for an introduction to FreeRADIUS installation and configuration see chapter 4
- FreeRADIUS Demystified Seminar [44] - Alan Buxey's seminal 2012 pre-NWS40 FreeRADIUS Demystified seminar presentation
- FreeRADIUS Best Current Practice Configuration for eduroam [45] - partner material for the FR Demystified seminar
- FreeRADIUS Packet handling; examining the flow [45] - partner material for the FR Demystified seminar
- eduroam.org wiki [46] - FreeRADIUS setup

Radiator

- Radiator official website [20]
- eduroam.org wiki [47] - Radiator setup

Microsoft NPS

- **Microsoft NPS Configuration Guide [48]** - produced by eduroam(UK), step-by-step NPS RADIUS setup guide with screenshots
- **eduroam how to guide - Installing NPS** [49] - web video prodoced by eduroam(UK)
- Using Windows NPS as RADIUS in eduroam [50] - produced by UUINETT (Norway) so beware of country-specific content, but includes content covering AP config and certificates
- Microsoft IAS website documentation [30]
- Installing Microsoft IAS [51]- TechRepublic article
- MS IAS Operations Guide [52]
- Deployment of IEEE 802.1X for Wired Networks Using Microsoft Windows [53]
- Deploying MS IAS with VLANs [54]
- Microsoft TechNet IAS Troubleshooting [55]

Aruba ClearPass

- Guide to Configuring Aruba WLC and ClearPass [56] - written by UUINETT and likely to have Norway-specific config content!

Cisco ACS / ISE

- See material in the Library [57]

7. Acquire and Install Server Certificate for ORPS/NAS

Identity Provider (IdP) organisations i.e. 'Home and Visited' and 'Home-only' participants will generally need to install a suitable server certificate on their RADIUS servers that are used in the authentication process. Visited-only service provider members do not need a server certificate to support authentication of users. For Home service providers, depending upon the EAP method you choose to implement, mutual authentication between client (the user's device) and RADIUS server is generally required and this is based on the use of X509 certificates. The first stage of authentication is for the client device to be able to trust the authenticity of the RADIUS servers and network access servers/APs that they communicate with during the authentication process. The most popular EAP methods require that the authenticating RADIUS server must have a digital certificate. This can be from a legitimate certification authority (CA) or can be self-signed. For information about producing self-signed certificates or for a link to the Jisc Certificate Service (for provision of low cost QuoVadis certificates) see resources section below. Nb The recently defined EAP-PWD method does not require the RADIUS server to have a certificate, however it is not widely supported by suppliants.

eduroam services, being built on 802.1X, are generally implemented using EAP methods that use transport layer security (TLS), such as EAP-TLS, EAP-PEAP and EAP-TTLS - which require the use of a server certificate to authenticate the RADIUS server to the supplicants. In addition EAP-TLS also requires client certificates in order for the clients to be validated by the RADIUS servers. These client certificates may be self-signed, ie. generated by your private CA software.

See Certificates in eduroam [58] for information on: Establishing trust during EAP authentication; How and where to acquire certificates; What certificates to install on the RADIUS server and present during authentication; What certificates to upload into the CAT system.

Self-signed certs/private CA or commercial server certs?

Best practice is to utilise self-signed server certificates or preferrably private CA signed server certificates. These eliminate the potential threat posed by the possibility of a malign agent setting up a RADIUS server masquerading as your ORPS and using a server certificate acquired from the same CA as your legitimate ORPS. The risk is that inadequately set up supplicants, those where server certificate name validation is not enabled, will trust the spoofed ORPS and so will be vulnerable to harvesting of credentials.

You can use a self-signed server certificate, which is one signed with its own private key, but this means that you cannot pre-install trust for it on devices and you will be relying on users to 'click accept' when the certificate alert pops up. This represents poor practice as it conditions users to ignore such alerts - reducing device security. Additionally, having a self-signed cert means that when it expires it you will need to replace it and reconfiguring all client devices - but by having a long expiry date you can balance this effort against the effort of replacing a commercial (e.g. Sectigo through Jisc's Certificate Service [59]) server certificate on the ORPS.

If you have the necessary expertise to set up a private Certification Authority and issue server

certificates you will be able to regate the risk of your ORPS being masqueraded by a credentials harvesting rogue. Use of private CA signed certificates will of course require the CA certificate to be distributed to user's devices and trust of the CA to be pre-configured. But by using CAT, the effort of CA cert distribution and client device reconfiguration can be minimised.

A further benefit of using a private CA is that you will be able to construct a certificate chain without intermediate CA certificates. This results in fewer bytes to be transmitted inside the EAP conversation and hence fewer EAP round-trips and thus faster authentication.

Links
[1] https://community.jisc.ac.uk/library/janet-services-documentation/implementing-eduroam-roadmap-part-2
[2] https://community.jisc.ac.uk/library/janet-services-documentation/implementing-eduroam-roadmap-part-3
[3] https://community.jisc.ac.uk/library/network-and-technology-service-docs/implementing-eduroam-roadmap-part-4
[4] https://community.jisc.ac.uk/library/janet-services-documentation/eduroam-deployment-guide
[5] https://wiki.geant.org/pages/viewpage.action?pageId=121346286
[6] https://wiki.geant.org/pages/viewpage.action?pageId=121346286#eduroaminanutshell(BEGINNER)-Elementsoftheeduroaminfrastructure
[7] http://community.jisc.ac.uk/library/advisory-services/ieee-8021x-implementation-janet-connected-organisations
[8] https://community.jisc.ac.uk/library/advisory-services/ieee-8021x
[9] https://community.jisc.ac.uk/library/advisory-services/extensible-authentication-protocol
[10] http://webmedia.company.ja.net/content/presentations/shared/networkshop300310/hooper_challengesofwidescalede
[11] https://wiki.geant.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus#Howtodeployeduroamon-siteoroncampus-SelectingEAPtypes
[12] http://deployingradius.com/documents/protocols/compatibility.html
[13] http://deployingradius.com/documents/protocols/oracles.html
[14] https://community.jisc.ac.uk/library/advisory-services/guest-and-public-network-access
[15] mailto:service@ja.net
[16] http://webmedia.company.ja.net/content/documents/shared/networkshop300310/hooper_challengesofwidescaledepl
[17] https://community.jisc.ac.uk/library/janet-services-documentation/technical-administratorimplementor-information
[18] http://www.eduroam.org/downloads/docs/GN2-08-230-DJ5.1.5.3-eduroamCookbook.pdf
[19] http://www.freeradius.org/
[20] http://www.open.com.au/radiator/index.html
[21] http://technet2.microsoft.com/windowsserver2008/en/library/9af0667e-aa7d-4b1f-a054-7102a85eb2bc1033.mspx?mfr=true
[22] http://technet.microsoft.com/en-us/network/bb629414.aspx
[23] http://www.arubanetworks.com/products/security/network-access-control/
[24] https://www.cisco.com/c/en_uk/products/security/identity-services-engine/index.html
[25] http://www.juniper.net/products_and_services/aaa_and_802_1x/steel_belted_radius/
[26] https://www.fortinet.com/products/identity-access-management/fortiauthenticator
[27] https://www.extremenetworks.com/product/extremecloud-a3/
[28] https://www.packetfence.org/
[29] http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html
[30] http://technet.microsoft.com/en-us/network/bb643123.aspx
[31] https://jisc365.sharepoint.com/:w:/s/PublicDocumentLinks/EXe5MRALuTdOodkFDRJfpksBJ-T11c-

S3ZWEyoIHIDvQ9g?e=kAnNqx
[32] mailto:userID@realm
[33] http://blog.schertz.name/2012/08/understanding-active-directory-naming-formats/
[34] https://community.jisc.ac.uk/library/janet-services-documentation/how-does-organisation-join-service
[35] mailto:help@jisc.ac.uk
[36] mailto:user@department.myorganisation.ac.uk
[37] https://support.eduroam.uk/login
[38] https://community.jisc.ac.uk/library/janet-services-documentation/what-are-my-responsibilities-eduroam-sys-admin
[39] https://support.eduroam.uk/
[40] https://community.jisc.ac.uk/library/janet-services-documentation/eduroam-cat-configuration-assistance-tool
[41] https://community.jisc.ac.uk/library/janet-services-documentation/content-eduroam-info-web-page-guide
[42] http://wiki.freeradius.org/guide/eduroam
[43] http://www.ja.net/documents/publications/technical-guides/8021x-tg-web.pdf
[44] https://community.jisc.ac.uk/groups/eduroam/document/nws-40-freeradius-demystified
[45] https://community.jisc.ac.uk/groups/eduroam/document/freeradius-best-current-practice-configuration-eduroam
[46] https://wiki.geant.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus#Howtodeployeduroamon-siteoroncampus-FreeRADIUS
[47] https://confluence.terena.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus#Howtodeployeduroamon-siteoroncampus-Radiator
[48] https://community.jisc.ac.uk/library/janet-services-documentation/microsoft-nps-configuration-guide
[49] https://www.youtube.com/watch?v=NR-N65cDzi0&list=PLbKeiLya4JyA_6A10XKhnCzEY4eyApG4M&index=3
[50] http://services.geant.net/cbp/Knowledge_Base/Wireless/Documents/CBP-13_Using-Windows-NPS-as-RADIUS-in-eduroam_final.pdf
[51] http://articles.techrepublic.com.com/5100-1035-6148579.html
[52] http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=5480
[53] http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=7220
[54] http://technet.microsoft.com/en-us/library/cc757645%28v=WS.10%29.aspx
[55] http://technet2.microsoft.com/WindowsServer/en/library/1d497af2-be8a-4e9f-a586-e01bff1862d01033.mspx?mfr=true
[56] https://services.geant.net/sites/cbp/Knowledge_Base/Wireless/Documents/cbp-79_guide_to_configuring_eduroam_using_the_aruba_wireless_controller_and_clearpass.pdf
[57] https://community.jisc.ac.uk/library/janet-services-documentation/cisco-acsise-configuration-eduroam
[58] https://community.jisc.ac.uk/library/network-and-technology-service-docs/certificates-eduroam
[59] http://www.ja.net/products-services/janet-connect/janet-certificate-service