Certificates in eduroam

Updated 25/04/2025

Contents:

1. Scope

This article is relevant to Extensible Authentication Protocol (EAP) methods that use Transport Layer Security (TLS) including PEAP/MSCHAPv2, EAP-TTLS/MSCHAP etc and EAP-TLS.

PEAP/MSCHAPv2, EAP-TTLS/MSCHAP, EAP-TTLS/PAP etc are two-stage authentication methods. In phase 1 TLS is used to establish an encryption tunnel which then carries the user credentials (username and password) for the second phase of authentication. EAP-TLS, in which authentication is based on user certificates, also requires a server certificate. But consideration of the management of user certificates for EAP-TLS solutions is out of scope of this article. EAP/PWD does not require a server certificate.

Platform/OS-specific instructions on generating the certificate signing request CSR is outside the scope of this article due to the wide range of options (openssl, Microsoft mmc certificates snap-in etc). For instructions on using Microsoft Active Directory Certificate Services see the NPS guide and videos on https://community.jisc.ac.uk/library/janet-services-documentation/microsoft-nps-configuration-guide [1]

Similarly, due to the wide range of possible RADIUS platforms, installation/import of certificates into RADIUS servers is not within the scope of this document.

The important question of how and where to source your server certificates - from a

commercial Certification Authority (e.g. Jisc Certificate Service) or to operation your own private CA - is considered in section 6 below.

2. Establishing trust during EAP authentication

An essential step during most EAP authentications is establishing trust between the authenticating RADIUS server and the user's device supplicant. In the early part of the phase one stage of user authentication (e.g. PEAP phase), the RADIUS server presents its server certificate to the user's device. That server certificate may be just the simple server certificate or it may be presented together with the issuing authority's certificate (or even with a longer chain of certification authority certificates). The aim of including the issuing authority certificate with the server certificate is to help the user's device suppliant to establish the trustworthiness of the certificate being presented.

The user's device supplicant needs to validate that server certificate and will check the signature of the authority that issued the certificate against its trust store of issuing authority certificates. The certificate issuer may itself only be an intermediate certification authority, so the suppliant will seek the issuer of the intermediate CA's certificate with the aim of establishing a chain of trust to a root certification authority certificate. Root CA certificates are issued by the relevant certification authority itself and represent the foundation of the public-key infrastructure. Most of the main root CA certificates are shipped with operating systems when devices are built.

Whilst some operating systems permit the user to opt to simply trust a presented server certificate (or issuing CA certificate), this 'trust on first use' option does not represent best security practice. Ultimate trust is only established when the user's device supplicant can establish that the RADIUS server certificate has been issued by a trusted root CA. Opting to not validate the server certificate, which was available on older operating systems, is bad security practice.

3. What certificates to install on the RADIUS server and present during authentication

We recommend that your server certificate chain should comprise:

- the server certificate and
- the issuing Certification Authority (CA) intermediate certificate(s)

i.e. your server cert and e.g. the Geant OV RSA CA 4 intermediate.

4. What certificates should be in the user's device trust store/EAP profile and be used during authentication

We recommend that the user device contains the following:

- the certificate of the intermediate CA that issued the server certificate
- the root CA certificate of the issuer of the intermediate certificate(s)

e.g. the Geant OV RSA CA 4 intermediate and the *root* version of the UserTrust RSA Certification Authority

Nb. Whilst it may technically sufficient for the server to present only the server certificate if the user devices have both the root and intermediate(s) or for the device to only have the root CA certificate if the intermediate CA certificate is presented by the RADIUS server, the ‘belt and braces’ approach above is recommended.

5. What certificates to upload into the CAT system

If you are not familar with the CAT system, see https://community.jisc.ac.uk/library/janet-services-documentation/eduroam-cat-configuration-assistance-tool [2]

When creating the EAP profile(s) for your users' devices, the certificates to the uploaded to CAT are:

- the certificate of the intermediate CA that issued the server certificate (*)
- the root CA certificate of the issuer of the intermediate certificate

e.g. Geant OV RSA CA 4 intermediate and USERTrust RSA Certification Authority CA root

(*) in some cases a second intermediate CA may be involved - one that has issued the cert of the certificate issing CA. The complete chain of intermediate CA certs may be uploaded (e.g. GEANT OV RSA CA 4 intermediate and the USERTRUST RSA CA intermediate). However of you can, it is better to use the CA root version of the USERTRUST RSA CA since this will result in a smaller EAP profile for the CAT/geteduroam download to client devices.

6. How and where to acquire server certificates - private Certification Authority or public Certification Authority

You can operate your own private certification authority or purchase certificates from a commercial / public certification authority. The pros and cons of private vs public CAs for your server certificates are reviewed below. See also Section 7 of the Implementation guide https://community.jisc.ac.uk/library/janet-services-documentation/implementing-eduroam-roadmap-part-2 [3]

Note: if you opt to operate your own CA then you must set it up and configure it carefully to ensure that the certificates it issues comply with the requirements set out in the Generating the CSR section and linked Certificate Properties table as below.

Jisc enables you to purchase public CA certificates at very advantageous rates through a TBA scheme and when used with properly configured CSRs provide server certs that work well with eduroam and you can avoid the complexity and effort of running your own CA.

Which solution to choose depends on individual organisation circumstances - either option is valid, although if the maximum certificate validity period for commercial CA certs is reduced from the current 12 months, the incentive to pite the bullet and operate your own CA will increase!

Whichever option you choose you will first need to generate a certificate signing request on

the server you need the certificate for. How to generate a CSR is outside the scope of this article, however https://wiki.geant.org/display/H2eduroam/EAP+Server+Certificate+considerations [4] provides essential guidance when creating the CSR on your RADIUS server.

Using a certificate from your own private CA

Benefits:

- No need to purchase a certificate from a commercial vendor - saving cost.
- Eliminates the slight inherent security weakness with a commercially provided certificate deployment that exists in the specific case where a client device is not configured to validate the certficate name (CN/SAN:DNS). Note that CAT and geteduroam installers always configure proper cert validation c/w CN checking - which ensures security when a commercial CA is used (hence our strong recommendation to use CAT/geteduroam or similar. How can this configuration error be exploited? A rogue RADIUS server used in a MITM attack could present a valid cert from a commercial CA that would be trusted by the client device if i) the CA is the same as your actual RADIUS server and ii) the client device does not have certificate name validatation set. By you operating your own private CA, an attacker would find it hard to acquire a legitimate certficate - however a user device that is not configured to validate the server certificate/certificate name, e.g. the user clicks to 'trust on first use' will be equally be vulnerable to MITM attack even with an own-CA certificate on the RADIUS server.
- Long certificate expiry date can be applied.

Drawback:

- Since the self-signed ‘root certificate’ of your Certification Authority won't have been installed into user devices at the time of manufacture along with the device operating system, your CA root certificate will generally have to be installed into client devices' trust stores using desktop management systems (e.g. Intune) or by manual installation by the user or by using a device setup provisioning system. This will be essential to enable the client device to trust a server certificate issued by a private CA. This is not a difficult procedure with mobile device management software for corporately managed devices, but may be more of challenge for users own devices. This is where the eduroam CAT system is invaluable.

Using a certificate from a commercial CA

Benefits:

- Avoids the complication of operating your own CA (which includes making CRL URL publicly accessible)
- No need to distribute the CA's root certificate to each client since public CA certificate will generally be recognised by any client, since such certs are distributed with operating systems.
- The correct extension attributes will be present (if requested or needed) - eliminating necessity of configuring openssl etc.

Drawbacks:

- Cost - you usually have to pay an annual fee for each certificate (although Jisc provided certs are very low cost)
- Slight vulnerability to illegal spoofing
- Requirement to renew the certificate annually
- Which solution to choose depends on individual organisation circumstances - either option is valid, although if maximum certificate validity periods for commercial CA certs is reduced from the current 12 months, the incentive to bite the bullet and operate your own CA will increase!

News of confirmation of shortening lifespans of commercially issued server certificates > The CA/Browser Forum – a central body of web browser makers, security certificate issuers, and friends – voted c.12/04/2025 to cut the maximum lifespan of new SSL/TLS certs to just 47 days by March 15, 2029. The reduction will be implemented in steps as below:

- 15/03/2026 - lifespan 200 days
- 15/03/2026 - lifespan 100 days
- 15/03/2029 - lifespan 47 days (with Domain Control Validation at just 10 days)

See: https://www.theregister.com/2025/04/14/ssl_tls_certificates/ [5]

Implication > over the next few years, in order to avoid a heavy server cert renewal workload, eduroam/govroam/RADIUS IT admins currently using commercial CA certificates will need to consider switching to using own CA certificates (e.g. using the guidance on our NPS Guide page)

OR

eduroam/govroam sys admins will need to implement automated systems for handling renewal of SSL/TLS certs

Fortunately the Jisc Certificate Service has published some advice which might be useful for our members in creating a workable solution for **automating certificate renewal** > https://www.jisc.ac.uk/security-certificate-automation/automation-options [6]

https://www.jisc.ac.uk/security-certificate-automation/automation-options/using-acme-protocol-and-certbot [7]

https://www.jisc.ac.uk/security-certificate-automation/automation-options/using-ansible [8]

https://www.jisc.ac.uk/security-certificate-automation/automation-options/using-acme-protocol-and-certbot [7]

and there are further links to useful material on the automation options page.

Cautionary Note - Test Certificates provided in certain RADIUS implementations

Some RADIUS servers such as Radiator and FreeRADIUS, provide a certificate from a self-signed CA for testing purposes. Under no circumstanances should this certificate be used in a production environment.

7. Generating the CSR

Detailed instructions on how to generate a certificate signing request on the varous platforms that exist is outside the scope of this article, however the table below describes the parameters you need to include and the values required when building your CSR and for Microsoft NPS users instructions on how to create your CSR can be found in section 8 of our guide eduroam(UK) Microsoft NPS Configuration Guide [9]

https://wiki.geant.org/display/H2eduroam/EAP+Server+Certificate+considerations [4] provides essential guidance when creating the CSR on your RADIUS server - **the Certificate Properties table** a third of the way down the page is particularly useful; contents summarised below.

- **Certificate type:** you need an X.509v3 certificate.
- **Organisation-Validated (OV)** or Domain-Validated (DV) ideally, although Extended Validation (EV) is usually okay. There is no benefit in the use of an EV certificate and in fact there have been reports of difficulties with ChromeOS. (OV Certs can be acquired more speedily too!)
- **Signature algorithm:** SHA-256 or higher is the recommended secure hash algorithm for signing of the server certificate.
- **The public key:** should be at least 2048 bits and ideally 3072.
- **Common Name: CN name**, the name of the server on the certificate needs to be look like a FQDN; the CN should not be a wildcard name (e.g. *.camford.ac.uk). Whilst the Common Name (CN) does not have to match the host name of the ORPS in DNS (the CN is just 'a name' and the RADIUS server is not a web server) it is best practice to use a fully qualified domain name as the CN for reasons of maximum compatibility with devices. There should be no spaces in the CN.
- **Extension: SubjectAlternativeName:DNS** parameter in the Certificate field must not be empty - the CN and SubjectAlternativeName:DNS must have the same value and there must be an exactly matching value including upper/lower case. Whilst multiple SAN:DNS names can be configured on a certificate (in multiple ORPS deployments to match all hostnames of the servers), there is no necessity for eduroam purposes since SAN:DNS is only used (with geteduroam) to validate the CN name on the server certificate.
- **Extension: Extended Key Usage:** only TLS Web Server Authentication certificates should be used - not to be confused with Extended Validation (EV) certificates.
- **Extension: CRL Distribution Point:** The certificate should include a Certificate Revocation List Distribution Point extension and the (HTTP:/HTTPS:) URI needs to be valid and publicly accessible. If you acquire your certificate from a public CA this will automatically be included on your certificate and the CA will manage the CRL point so you will not need to worry about it. If you operate your own CA, then you will need to identify a publicly accessible location where you can publish the CRL e.g. on a web server. In addition, when setting up your CA you will need to include in the configuration the URI of this CRL Distribution Point and also ensure that the CA is configured to

ensure that the Extension:CRL Distribution Point is included in issued certificates. To learn about Certificate Revocation Lists see: https://www.thesslstore.com/blog/crl-explained-what-is-a-certificate-revocation-list/ [10]

- **Extension: BasicConstraint** (critical): must be CA:FALSE. It is essential that your certificate is marked as **not** being a certification authority certificate. But setting this as 'critical' is not necessary because even if you mark the extension as critical on your CSR, many Cert authorities ignore this when generating your certificate and criticality is not known to be checked by any OS supplicant. In fact if you use MS Windows Certification Authority to generate your own certificates, a bug in the software means that you should NOT tick the 'Make the basic constraints extension critical' box - the bug results in validation failure with Android 12.

If you deploy multiple ORPS servers, since there is no technical requirement for each server to have a different certificate, it is recommended you use one certificate, imported into all your ORPSs, thereby avoiding issues of support and client configuration/certification. The certificate will have just the one CN component in the Subject field - and that is usually a server name, e.g. eduroam.ORPS1.camford.ac.uk. Note that by using just one CN this will allow you to increase the number of ORPSs in your cluster in the future if required by importing a further copy of the certificate. Note that you can use multiple certificates if you wish, but each certificate will need a unique CN/subjectAltName pair.

8. Using the Jisc Certificate Service

This section will be re-written following the re-launch of the Jisc Certificate Service with a new certificate provider Q2 2025

If using the Jisc Certificate Service, you'll be able to upload your CSR and download the server certificate and the TBA intermediate via the TBA portal. (OV certificates are recommended but EV certificates may be used, but add no benefit, take longer to deliver and can cause problems on some devices).

Creating your server certificate:

- Log in to the Sectigo Certificate Manager and navigate Certificates > SSL Certificate page
- Click on the (+) button to add an enrollment request
- Click on the 'Using a Certificate Signing Request (CSR)' option and click 'Next'
- On the 'request SSL Certificate' form scroll down to the Order info section
- Certificate Profile - 'Jisc OV Multi-Domain SSL' is recommended
- Certificate Term - 1 year (no other option)
- Enter your e-mail address and in the Notifications section for 'External Requesters' and click 'Next'
- On the CSR page, populate the CSR box - drag your CSR file into the box and click 'Next'
- (The old interface worked by clicking on the (UPLOAD CSR) button, [Choose File] and select your CSR, then click [Submit])
- On the Domains page, the Common Name is auto-filled (Old interface - click the (GET CN FROM CSR) button)
- Populate the Subject Alternative Names field by clicking the copy icon and pasting into the field, then click 'Next'

- If you wish, select auto renew (old interface required an annual renew passphrase)
- Click on the OK (old interface 'Enroll') button

Acquiring your server certificate, intermediate CA cert and CA root cert:

You will receive an e-mail containing links enabling you to download the server certificate with various options to include the chain to the CA intermediate and root.

Alternatively you can use the Sectigo Certificate Manager portal:

- go to Certificates > SSL Certificates
- Select your server certificate
- Click on [View] button on the menu bar
- Click on the download icon on the top right of the panel
- From the drop down options list, select **Certificate (w/ issuer after), PEM encoded**
- Your certificate bundle will download to your local Downloads folder

Note that if wish you can also download the AAA Certificate Services (Comodo) root certificate along with the UserTrust RSA Certification Authority intermediate cert and the Geant OV RSA CA 4 intermediate cert bundle. Scroll to the bottom of the list and select Root/Intermediates only, PEM encoded. If you need the AAA Certificate Services (Comodo) root certificate you can extract it from the file as described below.

Preparing your certificate for a) importing into your RADIUS server b) uploading to CAT

Assuming you have followed the above and acquired your certificate bundle via Jisc Certificate Service and the Sectigo portal - the file you have downloaded comprises the following:

[Server cert issued by - Geant OV RSA CA 4 intermediate**]**

[Geant OV RSA CA 4 intermediate - issued by USERTrust RSA Certification Authority**]**

[USERTrust RSA Certification Authority intermediate - issued by AAA Certificate Services (Comodo)**]**

You can use the bundle as is for import into your server, but you will need to split it for w hen your create your EAP profile in the CAT system.

However we recommend that you also download the CA root version of the USERTrust RSA Certification Authority certificate.

The Geant OV RSA CA 4 intermediate is issued by USERTrust RSA Certification Authority. There are both root and intermediate CA versions of this USERTrust certificate. And both validate the Geant OV RSA CA 4 intermediate which in turn validates the Sectigo server certificates. But to reduce complexity and eliminate potential issues on certain user devices we recommend that you use the root CA version of the USERTrust certificate.

Download the root CA version via >> https://crt.sh/?id=1199354 [11] <<

Assembling the certificate for your RADIUS server:

The aim at this stage is to concatenate the server and intermediate(s) certificates into one certificate file with the server certificate at the top followed by the intermediate certificates. (i.e. in reverse of the issuing order). You do not need the [Root certificate] to be in the chain. (This will just bloat the certificate and may result in unnecessary additional RADIUS packet exchange).

An example of the order for a root and two intermediate certificates:

[Server certificate - issued by Intermediate certificate 2]
[Intermediate certificate 2 - issued by Intermediate certificate 1]
[Intermediate certificate 1 - issued by Root certificate]

If using Sectigo certificates - for the file bundles you have downloaded from the Sectigo portal - locate your downloaded server certificate bundle file and open it with e.g. Notepad. You will notice that each certificate begins with -----BEGIN CERTIFICATE----- and ends with -----END CERTIFICATE----- The BEGIN and END lines form part of the certificate and must be retained when you cut and paste the certificate components in the bundle files.

Working with the 'Certificate (w/ issuer after), PEM encoded' file, scroll down and delete the third (end) certificate, this is the USERTrust CA intermediate - this is not needed.

You now have a certificate file with the necessary issuing certificate chain (which does not include the CA root certificate).

This can now be imported into your RADIUS servers. And you can then configure your PEAP etc Network Profile/Connection Profile/config file etc to use this.

Preparing the individual certificates for use with CAT:

Using e.g. Notepad open the server certificate chain file you have just edited and select and copy the second certificate, which is the Geant OV RSA CA 4 intermediate certificate. Paste this into a new file and save.

Assuming that you will be using the USERTrust RSA Certification Authority root certificate, this issuing certification authority certificate can be downloaded from https://crt.sh/?id=1199354 [11].

You will now have the following and are ready to upload these to CAT:

[Intermediate certificate (Geant OV RSA CA 4 intermediate cert) - issued by USERTrust RSA Certification Authority]

[Root certificate (USERTrust RSA Certification Authority root)]

9. Uploading certificates into the CAT system when creating your EAP profile

If you are not familar with the CAT system, see https://community.jisc.ac.uk/library/janet-services-documentation/eduroam-cat-configuration-assistance-tool [2]

Certificates to the uploaded to CAT when creating the eduroam EAP profile(s) for your user devices:

- the certificate of the intermediate CA that issued the server certificate e.g. **Geant OV RSA CA 4 intermediate**
- the **root** CA certificate of the issuer of the intermediate certificate e.g. **USERTrust RSA Certification Authority**

However! Note that the Secitgo portal delivers the *intermediate* version of the USERTrust RSA Certification Authority CA certificate. You should use the root version of this certificate in uploads into the CAT system. The root version is available at https://crt.sh/?id=1199354 [11]

When you upload the certificates you will see that the CAT portal detects the certificate type and alongside the certificate file information box displays:

(R) root CA certificate

(I) intermediate CA certificate

(S) server certificate! - do not upload the server certificate

The certificate information box displays useful information about the certificate you have uploaded including the Organisation to which the certificate is issued, and the CN name on the certificate.

10. Renewing your server certificate

Certificates from public CAs are, these days, only valid for one year. You will therefore have to get your certificate renewed and to update your RADIUS systems:

- acquire renewed server certificate and import it into your RADIUS system
- update your RADIUS configuration to use the replacement certificate file

It is recommended that you keep the old certificate in your server's trust store so that the private key is retained.

If you have acquired your certificate from the Jisc Cert Service you can use the Sectigo portal to renew/auto-renew and download your certificate. Log in to the Sectigo portal and navigate to your Certificates > SSL Certificates page. Select the server cert and as above select the certificate and click on the [View] button. A pop out box will apprear and from the download options list on the top right you can select 'Certificate only, PEM encoded'. The Intermediate and CA root certificates will be unchanged so you do not need to download those too, unless these ever change.

11. Changing Certification Authority issuing your server certificate - managing the transition

Correctly set up user devices will have details of the root certificate of the CA that issued the certificate for your RADIUS server configured in their EAP profile and the CA root/inter certificates for your server certificate will be installed in the EAP profile/the device's trust store. When the change is made from your old server cert to the new one, issued by a different CA, user devices must immediately be able to validate and trust the new certificates from the new CA.

The aim is for users to be able to experience secure authentication without interruption when you switch your RADIUS server certificate to a replacement that has been issued by a new CA. Users should not suddenly experiencing authentication failures on change over day and discover that they have to connect to a setup WLAN or rely on 4/5G cellular services to get their eduroam profiles refreshed with an EAP profile for the new server certificate.

Since client devices can be configured to trust multiple CAs you should aim to get the new CA root certificate (and intermediate certs) into your user's devices trust stores/EAP profiles ahead of the switch over. Then on change over day, users' devices will seamlessly validate the new server certificate and authenitcation will proceed as usual. For managed devices this can be accomplished through GPO, Intune or other MDM systems and particularly for BYOD many organisations use CAT to provision device setup.

The GEANT CAT admin guide states
https://wiki.geant.org/display/H2eduroam/A+guide+to+eduroam+CAT+for+IdP+... [12]

"You can upload multiple root CA certificates simultaneously to CAT. This enables CA certificate rollover without a flag day: User devices which were configured with an upcoming new root CA ahead of time will then not even notice the change of server cert from old to new trust root (s***o long as the Common Name of the server certificate remains unchanged*** during the rollover). On the client OSes, all root CAs will be installed and all will be marked trusted."

Once you have installed the new server certificate from the new CA, you can update your CAT profile(s) and device management system by deleting the old CA certificates since these

are no longer needed.

Guidance specifically for the migration from Sectigo/GEANT provided certs to new Jisc Cert Service provided cert partner (tba)

It is assumed that, as we recommended in our Advisory of 20/12/2024, server certs that were due to expire before September 2025 were renewed via the Sectigo portal ahead of the 10th January deadline and if your old certificate has expired you have either installed the renewed certificate already or you have a copy of it ready for when your current cert expires. We're now into the summer term so the options for action are as follows:

If your server cert expires during this summer term you can replace your old cert with the renewed one you acquired from the Sectigo portal in January. You then have until Jan (or in some cases Feb) 2026 to replace your cert with one from the new JCS CA - if you will be sticking with the JCS service (which we recommend). So, you ***could*** leave switching server cert to the new CA until December and run on the old cert during the autumn term. This will mean asking all of your users to refresh their (CAT-installed) EAP profiles twice, once in autumn and again in January. If adopting this approach you should:

1. In the autumn term, upload the new CA root and inter certs into your EAP profile(s) in CAT and into your device management system
2. Request your users to update their EAP profiles via geteduroam or via the CAT website during the term
3. In December, switch server certificate and update your EAP profile in CAT and in your device management system by deleting the old CA certs
4. In the spring term, encourage your users to refresh their EAP profiles via geteduroam or via the CAT website.

Recommendation - ***alternatively*** you could switch to a cert from the new JCS CA during the summer holidays. You would need to prepare for this by updating your EAP profiles in CAT by adding the new CA root and inters as soon as possible and requesting your users to update their EAP profiles too, preferably during term, but certainly before the start of the autumn term. This has the advantage that you will not need to request the new intake of students in the autumn to refresh their EAP profiles via geteduroam or via the CAT website. You will of course still need to request your current users to update their EAP profiles during the autumn term after you have removed the old CA/inter from the EAP profile(s) in CAT.

If your cert expires over the summer holidays and if you are sticking with the JCS service, once the new CA for the service has been finalised, you should

1. upload the new CA root and inter certs into your EAP profile(s) in CAT and into your device management system and
2. encourage your users to refresh their EAP profiles via geteduroam or via the CAT website during this Summer term.

Then when you change your server cert during the holidays your users will immediately be able to continue connecting to eduroam and in particular be ready to connect when they return to campus in the autumn. In the autumn term you can update your CAT profile(s) and device management system by deleting the old CA. And then once again encourage your users to refresh their EAP profiles via geteduroam or via the CAT website.

If your server cert expires during the autumn term, you probably do not have a GEANT/Secitgo certificate but will be able to acquire a server cert from the JCS service issued from the new CA for the service a few days/week ahead of the old cert expiry date. You could replace the with the cert you renewed in January. This will give you until 9th Jan 2026 to replace the cert with one from the new CA.

12. Testing your ORPS certificate installation

Pre-requisite: an eduroam test account should be created in your user directory and registered via the eduroam(UK) Support server - as per section 5.7 of the Implementation guide https://community.jisc.ac.uk/library/janet-services-documentation/implem... [13]

There are two test systems you can use:

1) eduroam(UK) Support server [Certificate Check] button test on your Troublshoot page. This test can be sent from any of the NRPSs. In fact you should conduct the test from each NRPS in turn and target the test at each one of your ORPSs.

Go to the blue Tests panel, select the NRPS you wish to run the auth from, select your target ORPS (many members have multiple ORPSs) and click on the [Certificate Check] button.

The results are: OK, Warn and Fail. Click on the result and scroll to the bottom of the debug output to learn more. The debug output will show you information about the certificates that your ORPS is presenting during the phase 1 part of the PEAP/MSCHAPv2 authentication. An analysis is presented indicating whether it has been possible to verify the certificate chain to a trusted certification authority root certificate and what issues may have been detected by the test.

2) The CAT 'realm reachability' test. This is documented at:

https://wiki.geant.org/display/H2eduroam/A+guide+to+eduroam+CAT+for+IdP+... [14]

Log in to CAT and go to your Identity Provider Overview page. Scroll down to the 'Profiles for this Identity Provider section. In the Profile:eduroam panel click on the [Check realm reachability] button in the top right of the panel. There are 4 tabs, Overview, Static connectivity tests, Dynamic connectivity tests and Live login tests. Click on the Live login tests tab. (Ignore the other tests - except Static connectivity may be useful for a basic test).

Real (inner) username - Enter the full username of the test user you have created for your realm - and registered with eduroam(UK) on your Configure page on Support server.

Anonymous outer ID (optional) - this is optional. If you leave it blank the test will populate it with the inner identity username. You must use a full username if you wish to test an anonymous outerID e.g. 'anonymous@camford.ac.uk [15]'

Password - this is the password of your test user account.

Click on the [Submit credentials] button.

The output is self-explanatory and displays quite a lot of information about the certificate your ORPS is presenting in the authentication request. It also checks against the certificate and CN details you have entered in your eduroam profile on CAT

13. Complete the remainder of your eduroam deployment and you will be 'good to go'

Instruct your users to make use of geteduroam to get their devices correctly configured
Correct use of username and password is essential!

If you find any errors or omissions, wish to add content or have any comments on this page, please e-mail eduroamuk@jisc.ac.uk [16]

Links
[1] https://community.jisc.ac.uk/library/janet-services-documentation/microsoft-nps-configuration-guide
[2] https://community.jisc.ac.uk/library/janet-services-documentation/eduroam-cat-configuration-assistance-tool
[3] https://community.jisc.ac.uk/library/janet-services-documentation/implementing-eduroam-roadmap-part-2
[4] https://wiki.geant.org/display/H2eduroam/EAP+Server+Certificate+considerations
[5] https://www.theregister.com/2025/04/14/ssl_tls_certificates/
[6] https://www.jisc.ac.uk/security-certificate-automation/automation-options
[7] https://www.jisc.ac.uk/security-certificate-automation/automation-options/using-acme-protocol-and-certbot
[8] https://www.jisc.ac.uk/security-certificate-automation/automation-options/using-ansible
[9] http://support.eduroam.uk/files/eduroam(UK)%20Microsoft%20NPS%20Configuration%20Guide.pdf
[10] https://www.thesslstore.com/blog/crl-explained-what-is-a-certificate-revocation-list/
[11] https://crt.sh/?id=1199354
[12] https://wiki.geant.org/display/H2eduroam/A+guide+to+eduroam+CAT+for+IdP+administrators#AguidetoeduroamCAT
Note3-CArolloversupport
[13] https://community.jisc.ac.uk/library/janet-services-documentation/implementing-eduroam-roadmap-part-1
[14] https://wiki.geant.org/display/H2eduroam/A+guide+to+eduroam+CAT+for+IdP+administrators#AguidetoeduroamCAT
VerifyingmyRADIUSsetup
[15] mailto:anonymous@camford.ac.uk
[16] mailto:eduroamuk@jisc.ac.uk