Using Windows® NPS as RADIUS in eduroam

Best Practice Document

Produced by the UNINETT-led working group on campus networking

Authors: P. Dekkers (SURFnet), T. Myren (UNINETT)

February 2015
# Table of Contents

Executive Summary 4

1 Introduction 5

2 Limitations 6

3 Installing NPS 7

4 Server certificate for NPS 14

5 Configuring NPS 15
   5.1 Defining Clients and Servers 16
   5.2 Creating policies 21
      5.2.1 Connection Request Policies 22
      5.2.2 Network Policies. 31

6 Logging / Accounting 42

7 Troubleshooting tips 45

Appendix A Certificates 46
   A.1 Install and configure Windows server as a CA Server 46
   A.2 Distribute CA certificate to clients 65
   A.3 Request and install server certificate for NPS 67

References 76

Glossary 77
Executive Summary

Network Policy Server (NPS) is the Microsoft Windows implementation of a Remote Access Dial-in User Service (RADIUS) server and proxy. An increasing number of institutions in the Norwegian HE sector have chosen to use Windows NPS as their RADIUS server connected to the eduroam infrastructure. This document is provided to explain in some detail how Windows NPS should be configured to best fit in with eduroam.

The examples in this document are collected from a mix of both Windows Server 2008 R2 Enterprise and Windows Server 2012 R2. The dialogue screens differ slightly between the two versions, but the configuration items are very similar.

The instructions in this document assume a basic setup of an Active directory.

For the configuration of related equipment (Access Points, controllers and other RADIUS servers), please see the References section for links to other resources. This includes both other best practice documents and TERENA confluence pages.
1 Introduction

This is a listing of tasks involved in setting up Windows NPS for eduroam as a quick-start for more experienced users. The topics below are covered in more detail through the rest of this document:

- Installing NPS as a server role
- A server certificate suitable for eduroam (and NPS) is required. This could be a self-signed certificate or signed by a public Certificate Agency (CA).
- Configuring RADIUS clients (and shared secrets). Wireless Controllers (or Access points) and the proxy-servers of your National Roaming Operator (NRO) must be defined. Details for national proxy servers must be provided and negotiated (shared secrets) with NRO.
- Configuring RADIUS servers in NPS to allow sending requests to NRO proxy-servers for visiting eduroam users. The proxy-servers will be configured in a server group, with one server preferred and with a secondary configured for failover.
- Connection Request Policies to determine how a request is dealt with. Handle locally or proxy to NRO. For local-accounts create a User Name condition that matches your users with their realms, while preventing usage of unknown / unused sub-realms or no realm in username.
  - Such a Connection Request Policy can use ".\institution\no$" as a match for the User Name attribute, matching your realm and all sub realms. Also configure this policy to override Network Policy authentication settings and configure “Microsoft PEAP” as EAP Type (Add, then Edit to select the server certificate) and deselect all “less secure” mechanisms.
  - A Connection Request Policy to forward requests to the proxy-server group could match a User Name “@+.+$”. Or matching only valid TLD realms “@+.\[a-z][2,6]$”
- Configure one or more Network Policies. These handle all requests that the Connection Request Policies have set to be authenticated locally. These will handle the actual EAP authentication of your users, unless overwritten in the Connection Request Policy. A policy can be duplicated to add VLAN assignment attributes for local use, while travelling users should not receive these attributes.

In the following sections, mainly Windows Server 2012 R2 is used in the examples; configuration in Windows Server 2008 R2 is very similar.
2 Limitations

The Network Policy Server has a few limitations:

- You cannot strip attributes (for instance VLAN attributes assigned by other identity providers (IdPs)), but you can explicitly set values applicable to your environment if you work with VLANs or want to prevent invalid attributes.

- You cannot add attributes in outbound requests: adding an “Operator-Name” attribute to indicate where a user gets online is thus not possible and could be set by the National Roaming Operator instead.

- NPS doesn’t answer to Status-Server requests. It is best-practise for eduroam proxy servers to check your servers’ availability with those requests, and ideally you would do that the other way round too.

- Because of the previous limitations, inform your National Roaming Operator that you’re working with NPS.

- While the outer username (via the Connection Request Policy) can be rewritten, the inner username (often users configure both to be the same) handled by the Network Policy cannot. This means that your users will have to use the registered UPN (User Principal Name) which by convention maps to the e-mail address / user-ID@domain-name.

- Using anonymous outer identities is not possible. Unless “Override network policy authentication settings” is enabled in the Connection Request Policies. This implies that override network policies should be used, but not all consequences of this are known and some functionality (Constraints and Settings) in Network Policies might be lost.

- Logging in Event manager is rather poor (compared to FreeRADIUS) – there is not much detail shown, making the debugging of any connection problems difficult. Be prepared to install Wireshark for this purpose.
3 Installing NPS

In your Windows server open Server Manager, right click Roles and select Add Roles (2008). Or click Add roles and features. The Add Roles Wizard will open – read the information text and accept the default by just clicking Next three times:
Select installation type

Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

- **Role-based or feature-based installation**
  - Configure a single server by adding roles, role services, and features.

- **Remote Desktop Services installation**
  - Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.
Select **Network Policy and Access Services** – then **Next**:
Accept the defaults in the next three windows:
Then **Install**: 

![Add Roles and Features Wizard](image_url)

And wait for the installation to finish – **Close**: 

---

**Best Practice Document:**
**Using Windows NPS as RADIUS in eduroam**
4 Server certificate for NPS

You need to have a Server Certificate in order to use PEAP-authentication with eduroam.

PEAP (Protected Extensible Authentication Protocol) sets up a secure tunnel (just like HTTPS does for websites) in order to protect the credentials, and is an important part of the mutual authentication. Firstly the authentication server needs to prove to the user that he or she will be providing credentials to the right authority, then the users need to prove who they are. So the RADIUS server (NPS in this case) will send its certificate to the client before authentication of the user takes place. The client must have previously installed the public certificate of the Certification Authority (CA) that has issued and signed the NPS server’s certificate. This may be distributed using e-mail, a web page such as eduroam CAT (eduroam Configuration Assistant Tool), or a management system such as AD. The client checks the validity of the RADIUS server’s certificate using the CA certificate. The client should also check the name of the certificate. Using a certificate from local CA, rather than certificates from a larger commercial CA, reduces the possibility of phishing.

Please see the TERENA confluence pages on EAP Server Certificate considerations [TERENA] for good information on this topic.

Without a certificate (self-signed or not) it’s not possible to do local authentication, but NPS can still be used as a proxy to receive requests from Access Points, log, filter, and forward to the eduroam infrastructure.

If you have no certificate installed (or are in doubt about your certificate), please read Appendix A ‘Certificates’.
5 Configuring NPS

Open the NPS console (snap-in):

2012: In Server Manager > Tools > Network Policy Server

2008: Start > Administrative Tools > Network Policy server

A Wizard is available for configuring 802.1X Wireless or wired connections, see the next picture. You may use this for eduroam, but it does not provide all required settings (like realm/username pattern-matching) so you will need to make some changes in the created policies.

In these instructions RADIUS clients and servers, Connection Request and Network policies will be created separately i.e. not using the above Wizard.
5.1 Defining Clients and Servers

Before any policy can be applied to authentication requests we need to create RADIUS clients and servers. This is to allow wireless controllers (or Access Points) and the national proxy servers (they are all clients) to send requests to NPS and the national proxy servers to receive requests (now servers) from NPS.

If you have several controllers or Access Points that need to be defined as clients, it is recommended that you define a shared secret template first (it means you will re-use the same secret for all) and later apply this to each client, in this way avoiding mistyping problems.

Defining shared secret template:

The above screen shows a template for Controllers; in addition you may create one for national proxy servers.
After creating the templates, create the Clients by right-clicking **RADIUS clients** and select **New**.

Enter a friendly name (it can later be referred to and used in pattern matching), IP address or DNS name and a shared secret (use the template if has been created). Details for national proxies must be agreed with your NRO.

Repeat the above until all needed clients are defined, together with at least two national proxies and one wireless controller.
## RADIUS Clients

RADIUS clients allow you to specify the network access servers that provide access to your network.

<table>
<thead>
<tr>
<th>Friendly Name</th>
<th>IP Address</th>
<th>Device Manufacturer</th>
<th>NAP-Capable</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Controller1</td>
<td>CISCO-CAPWAP-CONTROLLER.uninett.no</td>
<td>RADIUS Standard</td>
<td>No</td>
<td>Enabled</td>
</tr>
<tr>
<td>ntr1.eduroam.no</td>
<td>ntr1.eduroam.no</td>
<td>RADIUS Standard</td>
<td>No</td>
<td>Enabled</td>
</tr>
<tr>
<td>ntr2.eduroam.no</td>
<td>ntr2.eduroam.no</td>
<td>RADIUS Standard</td>
<td>No</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
Next, create a server group for the proxy-servers, this will be used to send authentication requests from non-local users via proxies to their home institutions.

Right-click Remote RADIUS Server Groups and select New; enter a name for the server group e.g. “eduroam-proxies” then click Add:

[Image of New Remote RADIUS Server Group dialog]

Enter the name of the server (details from your NRO) and proceed to the Authentication/Accounting tab for the shared secret settings:
Enter the shared secret as agreed with the NRO (manually or by choosing the defined template).
For the secondary server, consider also the last tab “Load Balancing”. It is recommended not to load balance single EAP-sessions across multiple servers, which is what NPS will do when the Load-Balancing Priority is all set to the same level. In many situations it will work, but good practice is setting it to a lower priority meaning it will only be used for failover.

Finish by clicking OK twice.

### 5.2 Creating policies

Two types of policies are used with NPS: “Connection Request Policies” and “Network Policies”. When a request is received, it is first matched against Connection Request Policies, if the resulting match says “local authentication” the request is also matched against “Network Policies”. The order of Policies is important, once conditions are met processing of Policies are stopped. You can move policy
rules up and down, and disable rules. The two policy types can do much of the same condition matching and settings. The following details a set of policies that will work with eduroam, but is not the only possible way to achieve the same result.

5.2.1 Connection Request Policies

The “Connection Request Policies” decide what to do with an authentication request, either by forwarding it to a proxy-server or by authenticating locally. The decision is based on conditions set in a policy such as RADIUS attributes (e.g. User Name), RADIUS client IP-address (or friendly name) and several other options, when conditions are matched to the settings of that particular policy. For eduroam we only need two Connection Request Policies, in this order:

1. Authenticate own realms “your-realm.tld” locally (use Network Policies)
2. Forward eduroam visitors to eduroam proxy-servers.

The following screens show how to create the two Connection Request Policies:

Right click Connection Request Policies – Select New.
Enter a Policy name (e.g. own realms) – click Next

Click Add – to enter a condition, Select User Name and click Add: (in the example below, our realm is win-ng.uninett.no)
Enter the username pattern to match for then press **OK**.

Note: See [PATTERN] for pattern matching syntax. Here we match for any username ending with “win-ng.uninett.no”, this includes possible sub-realms as student.win-ng.uninett.no.

Then click **Next**.
Authenticate on this server – click **Next**.

Select “Override network policy authentication settings” and click **Add** to add PEAP as EAP, select **OK**.

Mark “Microsoft: Protected EAP (PEAP)” and click **Edit ...**.
Select the previously installed server certificate (above is just an example) and deselect “Enforce Network Access Protection”. Then click **OK**, followed by **Next** twice.
Check configuration:

Click Finish.
Next, you need the Connection Request Policy to forward requests to the national proxy servers – Add new policy as above with the following settings:

![New Connection Request Policy](image)

### Policy conditions:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>@.+[a-z][2,6]$</td>
</tr>
</tbody>
</table>

### Policy settings:

<table>
<thead>
<tr>
<th>Condition</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Provider</td>
<td>Forwarding Request</td>
</tr>
<tr>
<td>Authentication Provider Name</td>
<td>eduroam-proxies</td>
</tr>
<tr>
<td>Tunnel-Medium-Type</td>
<td>802 (includes all 802 media plus Ethernet canonical format)</td>
</tr>
<tr>
<td>Tunnel-Type</td>
<td>Virtual LANs (VLAN)</td>
</tr>
<tr>
<td>Tunnel-Pvt-Group-ID</td>
<td>35</td>
</tr>
</tbody>
</table>

To close this wizard, click Finish.

### Note:

Pattern matching used is for any realm of the form “@something.something”, another option is to use “@.+\[a-z][2,6]$” which is a case-insensitive match for realms ending in “@something.tld” where tld is between 2 to 6 letters.

In the above example, eduroam visitors are placed into VLAN 35 by setting the attributes Tunnel-Medium-Type, Tunnel-Type and Tunnel-Pvt-Group-ID. This can be omitted if you would like your eduroam visitors placed in the default VLAN for your eduroam SSID as configured on the wireless...
controller (or Access Points). It is however good practise to also include the VLAN setting here; it will overwrite attributes returned from the IdP. (Some do even if they should not!). For placing local users into specific VLANs we will use Network Policies (see later).
Make sure your Connection Request Policies are processed in this order:

![Connection Request Policies Table]

Note:

The original policy “Use Windows authentication for all users” should be deleted or disabled. Please do not have it enabled! (This policy would catch users without a realm included in their username and could actually work for authenticating your own users, but eduroam will not work for such users at other eduroam locations).

With just the above two policies enabled, a username without a realm will give an entry in your Event Viewer similar to the following example (also revealing the username):

![Network Policy and Access Services]

eduroam visitors should now be able to connect from your site. Check if possible as a guest at your institution.
5.2.2 **Network Policies.**

“Network Policies” are applied to requests that are to be authenticated locally. (As decided in the Connection Request Policy). In a very basic setup, only one Network Policy is needed, so first we create this policy:

Give your policy a name such as “default for own eduroam users”:

Click **Next**

Then click **Add**, to specify the conditions for matching this request.

Here you define the User Group in your AD that are allowed to authenticate. So select **UserGroups** and click **Add**.
Click **Add Groups ... > Advanced > Find Now.** This gives a list to choose from:
Here “All domain users” are selected as an example. You could establish a group just for eduroam users.

Click **OK** three times to get back to Specify Condition for the new Network Policy. Click **Next**.
Click Next.
De-select all “Less secure authentication methods” and Add “Microsoft: Protected EAP (PEAP)”, just as you did for the Connection Request Policy.

**Note:** PEAP (and certificate to use) was configured in **Connection Request Policy to Override Network Policies** for all local realms, so this setting should never be used. However since an authentication method must be set – we choose to select the most secure.

Click **OK** – then **Next**.
Leave this as a default – click **Next**.
This is where VLAN attributes can be set for local users. Leave as default for this policy (we should not set VLAN for our users at remote sites!). Click **Next**.
Check the settings and click **Finish**.

You should now be able to use eduroam at your site. Please check before adding more configurations. Local eduroam users will now all be placed in the VLAN (or possibly interface group) set on your controller or Access Points. Please also note that some Wireless controllers require you to enable “AAA Override” to allow VLAN (or interface group) to be set from RADIUS.

Now to place own users (or perhaps just some of them, e.g. employees) into a different VLAN. First duplicate the above Network Policy:
Then double click on the duplicate to edit:

![Copy of default for own eduroam users Properties](image)

Give the policy a new name and tick **Policy enabled** to enable the policy. Select the **Conditions** tab:
In this example, conditions are set to be Domain Admins and the Client Friendly Name so that request must be from one of the local Controllers. Next select the **Settings** tab:
Add RADIUS attributes as shown above to assign VLAN to users matching this policy. Your VLAN id of course must match your infrastructure. Although at the time of writing this has not been tested; **Tunnel-Pvt-Group-ID** should also be possible to use to set an Interface Group Name.

Click **OK**.

The order of Policies are important – right click on a policy and chose to move it up or down. Make sure the order is as below:

<table>
<thead>
<tr>
<th>Policy Name</th>
<th>Status</th>
<th>Processing Order</th>
<th>Access Type</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>eduroam employees at own institution</td>
<td>Enabled</td>
<td>1</td>
<td>Grant Access</td>
<td>Unspecified</td>
</tr>
<tr>
<td>default for own eduroam users</td>
<td>Enabled</td>
<td>2</td>
<td>Grant Access</td>
<td>Unspecified</td>
</tr>
</tbody>
</table>

You may add more Network Policies for other user groups, Machine Groups or combinations of these – if you have followed this guide you will know how to do this now.
6 Logging / Accounting

To see NPS events open Event Viewer. (Or view events directly in Server Manager)

In Windows 2012: Server Manager > Tools > Event Viewer.


You will find the NPS related log under Custom Views > ServerRoles > Network Policy and Access Services.

Another source of information is accounting, by default accounting is enabled logging to a file:

<table>
<thead>
<tr>
<th>Accounting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting</td>
</tr>
<tr>
<td>Log File Properties</td>
</tr>
<tr>
<td>SQL Server Logging Properties</td>
</tr>
</tbody>
</table>
If you would like to run queries toward your authentication and accounting information and maybe produce some statistics from it, use the “Configure Accounting” Wizard to setup logging to the SQL database. You may combine this with logging to file.

If you choose to keep logging to a file consider these settings, click **Change Log File Properties**:

![Log File Properties](image)

You might want to check that **If logging fails, discard connection requests** is unchecked.

Select the **Log File** tab:
Decide how often you want a new log file created – One month could produce a lot of data to search through.

**Tip:**

To improve the presentation of Log File presentation, a third-party tool like IAS log viewer can be used to track log files, produce statistics and assemble reports for users and accounting purposes. It is also possible to define traps for alarms and filter logs.

7 Troubleshooting tips

- Install Wireshark on your NPS server to be able to see all RADIUS traffic.
- Set up a Linux machine as a RADIUS client and install `wpa_supplicant` on it. This supplicant contains `eapol_test` (a program that communicates directly with the RADIUS server) and `rad_eap_test` (a script that uses `eapol_test`). This provides a lot of information and is a useful tool for testing and troubleshooting. Here is an example command using the script:
- Use the CAT tool to setup clients in your realm / institution – it could save a lot of time doing troubleshooting and also contains a possibility to check your realm from a remote site. Any questions about this tool should be directed to your NRO.
Appendix A Certificates

You need to have a server certificate in order to use PEAP-authentication with eduroam. PEAP sets up a secure SSL tunnel (just like HTTPS does for websites) in order to protect credentials, and is an important part of the mutual authentication. Both the user needs to prove who he or she is, and the authentication server needs to prove to the user that he or she is providing credentials to the right authority.

Without a certificate (self-signed or not) it is not possible to do local authentication. NPS can still be used as a proxy to receive requests from Access Points, log, filter, and forward to the eduroam infrastructure.

The following is showing how to setup your own CA (on your Domain Controller), create a CA certificate, distribute it to your clients and finally request (from your own CA) and install a server certificate for NPS. If you already have a CA set up and a CA certificate, please jump to the relevant section below.

(For an alternative method see [UFS112] “Recommended Security Solution for Wireless Networks” for setting up your own CA and acquire a certificate form your own CA using Linux.)

Prerequisites – Windows Active Directory Domain Controller must be running on this server or this server is part of an AD domain.

A.1 Install and configure Windows server as a CA Server

Add Roles and Features Wizard:
Select **Active Directory Certificate Services**: 

And add required features (as suggested). Select **Add Features**.
Press **Next**:
Select **Review ADCS information text** from the scroll down list. Press **Next**:

Press **Next**:
Select role services

Select the role services to install for Active Directory Certificate Services

- **Certification Authority**

**Description:** Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.

- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Certification Authority Web Enrollment
- Network Device Enrollment Service
- Online Responder

- Previous
- Next
- Install
- Cancel
Select role services

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD CS
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results

Select the role services to install for Active Directory Certificate Services

Role services

- Certification Authority
- Certificate Enrollment Policy Web Service
- Certificate Enrollment Web Service
- Certification Authority Web Enrollment
- Network Device Enrollment Service
- Online Responder

Description
Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.
Then press **Install**: 
Installation – Close once Installation succeeded:
In Server Manager – AD CS – it will notify that configuration is required for AD CS.

Click on More...
Press **Configure Active Directory Certification Services**

Read the text and press **Next**:

Select **Role Certification Authority**:

Then **Next**.
In Setup Type, select **Enterprise CA:**
In CA Type, select Root CA:
In Private Key, select **Create a new private key:**
In Cryptography, accept the suggested cryptographic options:
In CA Name, accept the default Common name for CA (servername-CA.domain):
Choose a long validity period (this is when the CA expires, it is also when all eduroam clients will need new CA cert):
In Certificate Database, accept the default database locations:
Review the configuration and press **Configure:**
Note:

Some clients (Win XP and above) require the certificate extension “TLS Web Server Authentication” (OID 1.3.6.1.5.5.7.3.1) to be present.

This is how to achieve this:

Open MMC on your server – File > Add snap > Certificates.

You will find the CA certificate here:
Right click and choose **Properties** – go to the **Extended Validation** tab, then add the required OpenID (OID):

Click **OK**.

**A.2 Distribute CA certificate to clients**

The CA root certificate must be present as Trusted Root Certification Authorities on all your eduroam clients. The recommended way is to distribute the CA certificate using CAT.

To have the CA transferred to CAT or otherwise to clients:

Right click the **CA** again and choose **Export**.
Next Select file format:
Save the file as for example <institution>_CA.cer – it is then ready for distribution. In a Win AD domain this can be done from the DC.

For clients outside the domain you need to go via CAT, distribute via email, intranet, USB memory stick or other method so that clients can install the CA Certificate.

A.3 Request and install server certificate for NPS

On the server running NPS:

1. Click Start, enter mmc, and press Enter.
2. Click File > Add/Remove Snap-in.
3. Choose Certificates, and click Add.
4. Choose Computer account, and click Next.
5. Select Local Computer, and click Finish.
6. Click OK to return to the Microsoft Management Console (MMC).  
7. Expand the Certificates (Local Computer) and Personal folders, and click Certificates.
8. Right-click in the whitespace beneath the CA certificate, and choose All Tasks > Request New Certificate.

Click Next:
Select (tick) Domain Controller
Or select (tick) **Computer** – in the case of AD running on a separate server (this computer is an AD member running NPS):
Before Clicking **Enroll** – click **Details** and adjust properties according to the screens below:
### Certificate Properties

<table>
<thead>
<tr>
<th>General</th>
<th>Subject</th>
<th>Extensions</th>
<th>Private Key</th>
<th>Certification Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Friendly name:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>NPS eduroam</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Description:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Used for eduroam server authentication</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A friendly name and description will make it easier to identify and use a certificate.
Then **Enroll** – and Finish.

In MMC you should now have both the CA and the server certificate:
<table>
<thead>
<tr>
<th>Issued To</th>
<th>Issued By</th>
<th>Expiration Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>institution-CA</td>
<td>institution-CA</td>
<td>4/4/2039</td>
</tr>
<tr>
<td>tomy-win.institution.no</td>
<td>institution-CA</td>
<td>4/4/2015</td>
</tr>
</tbody>
</table>

![Certificate Window]

- **Certificate Status:**
  - This certificate is OK.

---

**Best Practice Document:**
**Using Windows NPS as RADIUS in eduroam**
References

[PATTERN] Pattern matching syntax for Windows Network Policy Server

[TERENA] EAP Server Certificate considerations
https://confluence.terena.org/display/H2eduroam/EAP+Server+Certificate+considerations

[UFS112] Recommended Security System for Wireless Networks
http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-ufs112.pdf

Other references not directly linked to this document:

Complete guide for deploying eduroam on-site or on campus
https://confluence.terena.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus

Guide to configuring eduroam using a Cisco wireless controller
http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-ufs127.pdf

Best Practice Document on “FreeRADIUS Database Connection”
http://www.terena.org/activities/campus-bp/pdf/gn3-na3-t4-freeradius-db.pdf

FreeRADIUS integration with AD
http://wiki.freeradius.org/guide/FreeRADIUS-Active-Directory-Integration-HOWTO

Cisco example of setting up a Windows server with all components needed for 802.1X authentication
## Glossary

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AD</td>
<td>Active Directory</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority (or Certification Authority)</td>
</tr>
<tr>
<td>EAP</td>
<td>Extensible Authentication Protocol</td>
</tr>
<tr>
<td>EAPoL</td>
<td>Extensible Authentication Protocol over LAN</td>
</tr>
<tr>
<td>EAP-PEAP</td>
<td>EAP - Protected Extensible Authentication Protocol</td>
</tr>
<tr>
<td>EAP-TLS</td>
<td>EAP - Transport Layer Security</td>
</tr>
<tr>
<td>EAP-TTLS</td>
<td>EAP - Tunneled Transport Layer Security</td>
</tr>
<tr>
<td>IdP</td>
<td>Identity Provider</td>
</tr>
<tr>
<td>IEEE 802.1X</td>
<td>Authentication mechanism for wired and wireless networks.</td>
</tr>
<tr>
<td>LDAP</td>
<td>Lightweight Directory Access Protocol</td>
</tr>
<tr>
<td>MSCHAP</td>
<td>Microsoft Challenge-Handshake Authentication Protocol</td>
</tr>
<tr>
<td>NAS ID</td>
<td>Network Access Server IDentifier</td>
</tr>
<tr>
<td>NPS</td>
<td>Network Policy Server</td>
</tr>
<tr>
<td>NRO</td>
<td>National Roaming Operator</td>
</tr>
<tr>
<td>PEAP</td>
<td>Protected Extensible Authentication Protocol</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Remote Authentication Dial-In User Service; a protocol for authentication, authorisation and accounting</td>
</tr>
</tbody>
</table>