radsec certificates

RADIUS/TLS: Obtaining and managing certificates

RADIUS over TLS is a new way of interconnecting federations (and later, if desired, eduroam IdPs and eduroam SPs). It uses TLS encryption instead of IP address and shared secret pairs to authenticate and authorise eduroam servers. When replacing such explicit configuration-based authorisation with a dynamic, automatic provisioning model, it is important to clearly define the rules for issuance of an eduroam server certificate, because the possession of the certificate will enable the holder to participate in eduroam.

In order to make use of this new feature, your FLR server must have acquired an eduroam server certificate. Depending on which federation or world region you are from, the procedures for getting a certificate will differ. The following two subsections are a globally valid description of the eduroam Trust Model. This trust model is currently only implemented by one CA, which operates in Europe. The last subsection provides details for European eduroam participants.

The eduroam server certificate trust model: eduPKI PMA and the eduroam Trust Profile

During the design of the X.509 trust model for eduroam, certain requirements had to be considered.

- It became clear that no single one Certificate Authority (CA) can or should issue all eduroam certificates world-wide. Instead, rules were defined under which multiple CAs can issue eduroam certificates.
- These CAs could possibly be general-purpose CAs that also manage certificates for other services besides eduroam. Consequently, the eduroam trust model had to allow to differentiate eduroam server certificates from other certificates from the same CA in a standardised manner.
- A CA would need to conform to certain quality assurance criteria, which need to be assessed by an oversight committee.

As a result of these requirements, the GEANT project's eduPKI task created a framework for the eduroam trust model:

- an oversight body, the "eduPKI Policy Management Authority" (eduPKI-PMA) was created and produced a document with defined Quality Assurance criteria for CAs which would like to become part of the eduroam trust model. The rules for CA accreditation are set forth in section "CA Accrediation Process" at https://www.edupki.org/edupki-pma/pma-governing-documents/. Note that eduPKI PMA is currently the only PMA, but this doesn't preclude other PMAs in other world regions from emerging.
- a X.509 trust profile for the eduroam service was created, which designates two so-called "policy OID" fields to eduroam IdP and SP servers. The trust profile can be found on this page: https://www.edupki.org/edupki-pma/edupki-trust-profiles/
- this trust profile requires that CAs which use this policy OID will check the authorisation of a certificate applicant whether or not he is actually an eduroam IdP and/or SP server operator.

This way, it can be assured that only authorised eduroam operators get eduroam certificates and can establish connections to other eduroam servers.

Managing accredited CAs in eduroam servers

> As at May 2020, this section may be outdated. The TACAR list of eduPKI eduroam certificates does not include the eduPKI CA certificate described below and does include a certificate that is not widely accepted. There are planned changes that may result in this process being entirely revised. However, in the mean time, use of TACAR will lead to FetchCRL3 errors and including the eduPKI CA certificate manually is required for a functioning eduroam RadSec implementation.

The number of accredited CAs and the list of certificates can change at any time. It is important that all eduroam servers consult an up-to-date list of accredited CAs. The list of currently accredited CAs is maintained in a TERENA repository of the TACAR service. A browsable list can be found here: https://www.tacar.org/cert/list/

Please refrain from manually downloading CAs as a one-time action. Otherwise, your CA list will eventually become outdated and this will create service disruption for some eduroam users!

There is currently one accredited Certification Authority: the eduPKI CA, located at https://www.edupki.org/edupki-ca/ . eduPKI CA acts as a catch-all world-wide for eduroam participant countries which do not have their own accredited CA for the eduroam service. Such further CAs are welcome to apply for eduPKI PMA accreditation.

eduroam operators should request their eduPKI CA eduroam certificate by following the instructions on the eduPKI CA eduroam RA pages at: http://www.eduroam.org/index.php?p=europe&s=edupki

Updating CRLs on your server

Since certificate possibly need to be revoked in case of private key compromise or other reasons, it is important that all RADIUS servers which validate eduroam-accredited CAs consult an up-to-date CRL list for each of the CAs. eduroam suggests to use the script "FetchCRL3" which was developed in the Grid community for this very purpose (download here).

Usage:

- place the .info files of all accredited CAs into one otherwise empty directory (download edupki.info) - let's assume for this example that the path to those files is

  `/path/to/certificates/`

- find out the command which restarts your RADIUS server on your system - let's assume for this example that the command is

  ```
  systemctl restart radiusd.service
  ```

- The following command will attempt to fetch an up-to-date CRL for the CA, and only if successful, will restart your server:
  `fetch-crl -l /path/to/certificates/ && systemctl restart radiusd.service`

- This script should be executed in a cron job on a regular basis (we suggest daily).