GÉANT
Networks • Services • People

Server Certificate Practices in eduroam

Best Practice Document

Produced by the CSC/Funet-led working group MobileFunet

Authors: Tomi Salmi (CSC/Funet), Tuukka Vainio (University of Turku)

September 2015

Document No: FN4.1
Version / date: 14 September 2015
Original language : Finnish/English
Original title: “eduroam ja varmennekäytännöt”
Original version / date: 7 April 2015
Contact: Tomi Salmi, tomi.salmi@csc.fi

CSC/Funet bears responsibility for the content of this document. The work has been carried out by a CSC/Funet-led working group MobileFunet as a part of a joint venture project between the HE sector in Finland.

The research leading to these results has received funding from the European Union’s Horizon 2020 research and innovation programme under Grant Agreement No. 691567 (GN4-1).

Table of Contents

Table of Figures

Table of Tables

Executive Summary

Certificates are extensively used in telecommunications to enable both parties to verify with whom they are communicating. Certificates are also used in the international roaming system eduroam. In eduroam it is important that users can verify that they are communicating with the correct authentication server before submitting their username and password.

Anyone can create a limitless number of self-signed certificates free of charge. Another option is to choose a public Certification Authority (CA) to issue the certificate. A self-signed certificate offers some security advantages in eduroam environment so it is the preferable option for those with CA expertise. The document describes the differences between private and public CAs. When creating and distributing certificates, it is important to pay attention to certificate properties to achieve the best possible compatibility with different end devices.

Using automatic provisioning tools like eduroam CAT makes life easier for eduroam end users. The tool makes end-device configuration and certificate installation a lightweight procedure.

1 Introduction

Certificates help users on the Internet ensure that they are dealing with the correct server and counterparty. However, a certificate alone is insufficient to increase or implement information security – it is just a commonly agreed method of storing information. Although anybody can create a limitless number of certificates, the ability to check a certificate and the information it contains as a whole increases information security.

Certificate verification forms part of the authentication process for the international roaming system eduroam. This document collates the EAP (Extensible Authentication Protocol) certificate practices that have proven successful for eduroam, so that the best possible compatibility can be achieved with a variety of end-user devices, and not forgetting information security and usability. The document is particularly targeted at those who will be administering the eduroam network during its deployment phase.

2 Certificates in eduroam

When a user joins the eduroam network, certificates are used for almost all possible EAP types, so that users can verify that they are communicating with the correct RADIUS (Remote Authentication Dial In User Service) server before submitting their username and password. To do this, an X.509 server certificate must be obtained for the authenticating IdP (Identity Provider) server. This may be either a self-signed certificate from your own Certification Authority (CA) or one obtained from a trusted public CA. The differences between these types of CA are detailed in Section 2.1. If the RADIUS server is merely a proxy that does not require user authentication, there is no need for a server certificate. The user's end device must receive and begin using the public component of the root certificate. Certificate chain administration and distribution is handled in Section 2.2. Section 2.3 covers certificate renewal, and Section 2.4 the technical properties required to ensure the best possible compatibility with end devices.

2.1 Private or public CA?

A certificate must always have an issuer, that is, a Certification Authority. A certificate may be obtained from a trusted public CA, or the administrator may establish a private CA. You can create a limitless number of self-signed certificates free of charge, but CA administration requires knowledge of Public Key Infrastructure (PKI). CA administration also incurs labour costs at the very least. When using EAP-TLS, you will need to authenticate not only the server, but also the end device, each with a separate certificate. Therefore it might be more beneficial to use your own CA as certificate volumes grow. Many RADIUS servers come with a test certificate for test use. This test certificate should not be used when the service goes live.

One downside of using a private CA in eduroam is that no end device automatically recognises this type of CA, so the certificate's public component must be separately installed on every end device. The certificate can, for example, be shared via email or an Intranet, but both the distribution model and user guidelines must be well designed. The use of provisioning software is recommended. If you change the root certificate, the certificate will have to be renewed on all of the end devices that have been configured to use it. It is therefore worth setting a long validity period for certificates when using a private CA. It is also worth paying attention to the size of certificate files when creating your own certificates. You can easily create unnecessarily large certificates that slow down EAP handshakes.

When using a trusted CA, the public component may come preinstalled in at least some end devices. Although the certificate may be found on end devices, the user must be able to choose it during configuration, and this will require operating system-specific instructions. Whether you select a

private or public CA, users must be instructed on how to obtain and install – or at the very least choose – the correct certificate when configuring their network settings.

Using a trusted CA poses an increased risk of Man in the Middle (MITM) attacks compared to using a private CA. The risk arises from the fact that not all end devices perform sufficiently thorough certificate authentications. For example, some end devices only verify that the issuer of the server certificate is the same as that of the root certificate, but do not verify the server's name. A hostile user will, therefore, be able to establish a RADIUS server and obtain a genuine certificate signed by the same trusted CA in order to collect usernames and passwords [1]. Whenever possible, IT support should offer advice and ensure that both the certificates used and the server's name are defined in users' configurations.

Inadequate certificate verification is a particular problem with the Android and Windows Phone operating systems. Although both systems allow configuration of a root authenticator, authentication can be easily by-passed. Neither system allows you to set the name of the authentication server. Android's Jelly Bean (version 4.3) enabled EAP configuration with automatic tools, whereas previously all EAP settings had to be made manually via menus [2].

By using automatic provisioning tools, such as eduroam CAT (Configuration Assistant Tool) or MDM (Mobile Device Management) systems, the installation of certificates on end devices no longer becomes a decisive factor in whether to choose a trusted or self-signed certificate. As a self-signed certificate affords the aforementioned information security advantages, it is the preferable option for those with CA expertise. The pros and cons of using private and public CAs are collated in Table 2.1.

Private CA	Public CA
Advantages	
No cost for creating certificates Information security benefits	Certificate may be preinstalled in end devices
Disadvantages	
Requires PKI expertise Certificates must be distributed to end devices	Usually a fee-based service Greater risk of man-in-the-middle attacks.

Table 2.1: The pros and cons of using private and public CAs

Some organisations belonging to the National Research and Education Networks (NREN) in Europe can also use their local NREN to access the Trusted Certificate Service (TCS), offered through the joint procurement coordinated by the GÉANT Association. This service enables organisations to obtain their own server certificates signed by TERENA (now GÉANT Association). In Finland, the Finnish University and Research Network (Funet) offers services to institutions of higher education and other members [3].

2.2 Certificate chain administration and distribution

The certificate chain used to authenticate the authentication server and the end device consists of a root certificate, potentially intermediate certificates, and a server certificate. The end device must have at least a trusted root certificate before eduroam authentication may begin. End devices come installed with varying selections of trusted CA certificates, but no self-signed certificates will, of course, be preinstalled. The administrator must either organise the distribution of certificates or provide operating system-specific instructions for end users, telling them where and how they can obtain and install a certificate. Whenever possible, it is worthwhile employing the user-friendly provisioning software that has been developed to help end users, such as eduroam CAT.

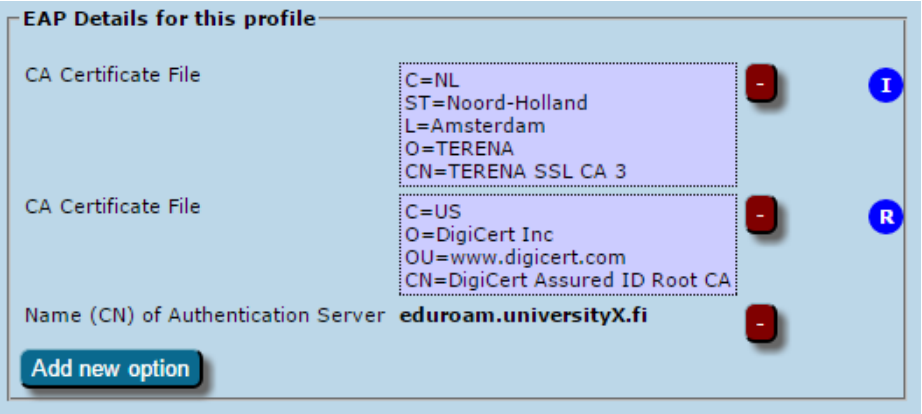

Figure 2.1: Defining the entire certificate chain in an eduroam CAT profile.

During the authentication phase, the RADIUS identification server will send a server certificate at the very least. The certificate chain's intermediate certificates can be transferred during EAP authentication, or then they can be stored in the end device in advance in the same manner as the root certificate. If the intermediate certificates are installed in the end device, this will reduce the need for EAP handshakes and accelerate authentication. A certificate chain may use several intermediate certificates, but the time taken to complete authentication will naturally lengthen with the number of certificates used.

You should also pay attention to the size of certificates, especially when using a private CA. Increasing size not only lengthens handshakes, it may also disconnect them completely. 64 kilobytes is the general maximum size for an end device certificate chain, which will require the back-and-forth transmission of about 60 EAP packets. Many base stations will disconnect EAP handshakes at the 50-packet mark. [4]

In terms of functionality, the surest solution is to store the entire certificate chain on the end device using provisioning software. An example of this are the issues encountered with TCS certificates in the Apple operating system (at least iOS 7 and 8), as the chain's current intermediate certificate was previously a self-signed root certificate. The operating system's preinstalled and trusted certificate is the self-signed version, and iOS will not always approve a new version of the same certificate sent during an EAP handshake. This issue does not occur when certificates are installed using provisioning software. In this CAT screenshot, the service has been correctly linked to both the root certificate

(R=Root) and the intermediate certificates (I=Intermediate), so that they will be installed on the end user's device when the CAT packet is run.

2.3 Certificate renewal

A server certificate should be renewed at the latest when its validity is coming to an end. Certificates signed by a public CA are typically valid for 1–3 years. As long as the CA remains the same, renewing the certificate is a straightforward operation, as the root certificate configured in the end device does not need to be changed. The only changes required will be to the authentication server.

Validity periods for root certificates are typically substantially longer. However, when obtaining a certificate from a public CA, it is still a good idea to check whether the root certificate will still be valid for a decent amount of time. Likewise, you should set a sufficiently long period of validity when setting up root certificates for a private CA. When you set up a new certificate, it is also worth setting up a monitoring for its validity. Certificate providers usually send advance reminders when a certificate's validity is nearing an end. Just make sure what is the email address receiving the notifications in your organization.

If your root certificate changes, all end devices will also have to be reconfigured. The more end devices that have been configured to use this IdP, the tougher and slower this process will be. Choosing a CA is therefore something you should carefully consider as soon as you start planning eduroam deployment.

When revoking a certificate, it is worth noting that, when using eduroam, authentication and certificate verification occur before the actual network connection is established. This means that even a revoked certificate may be authenticated. Although the supplicant will check the Certificate Revocation List after authentication, users will already have submitted their username and password, potentially to a hostile authentication server.

2.4 Certificate properties

The following list contains a number of certificate properties and recommendations. The guidelines seek the best possible compatibility with a variety of end devices and operating systems.

Property	Description
Server name	The server name should be entered into the certificate's Subject field as its Common Name (CN) and as a Fully Qualified Domain Name (FQDN). We recommend that you also use the same name for subjectAltName extensions. You should not use wildcard names.
Signature algorithm	The most highly recommended is SHA-2 (for example, SHA-256). Support for the SHA-1 algorithm will end shortly, and the MD5 algorithm should no longer be used anywhere.
Key length	Some operating systems will not accept keys with fewer than 1,024 bits. It is worth using 2048-bit keys in new environments.
CRL Extension	Windows 8 and Windows Phone 8 require, or can be configured to require, the URL of the Certificate Revocation List (CRL), and this URL must then have the correct syntax. However, neither operating system downloads an actual CRL file, even if a URL is defined.
BasicConstraint Extension	If the BasicConstraint is not defined, issues have been noted with at least OS X Mountain Lion. The setting must be “CA:FALSE (critical)”, that is, the server certificate is not a CA certificate.
X509v3 Extended Key Usage (EKU)	Windows systems require at least one property to be defined. For EAP use in eduroam, this property is “Server authentication”.

Table 2.2: Certificate properties

Sources: [4] [5] [6]

3 IT support

When eduroam is introduced on campuses, as many people as possible need to be informed of its existence. Clear, operating system-specific instructions will also be required to ensure information security when people configure their end devices to use eduroam. We recommend that you produce instructions on how end users should configure their own devices, as people will typically use eduroam on their own devices rather than through the organisation's centrally maintained systems. At institutions of higher education, orientation sessions for new students and personnel should include information on how to start using eduroam safely.

Configuration instructions should highlight the way in which security checks are configured. It is dangerously easy to simplify certificate verification and advise people to bypass it, but this weakens information security and teaches users dangerous habits. It is easy to configure certain operating systems incorrectly, and even so that users can join eduroam in their home network but not when visiting an eduroam network administered by another organisation. For the sake of clarity, home network log-ins without a realm should be prevented. If no realm is included in the configuration, the configuration is ostensibly correct for the home network, yet unusable for roaming when visiting another eduroam network.

Instructions and recommendations for implementing eduroam support can also be found on the eduroam.org [7] and terena.org [8] websites.

The aforementioned eduroam CAT [9] is an excellent tool for helping end users to start using eduroam. Network administrators can use this tool to create user-friendly, organisation-specific eduroam installation packages for their own users. The CAT service will generate complete installation packages – all you need to do is enter your eduroam network details, RADIUS server's name, supported EAP types, and certificate chain. When these settings have been configured, users can obtain installation packages from the CAT website. You can also create a link that will send users directly to the download page for your organisation's installation packet. Using the installation software does not require network expertise. CAT has been proven to reduce the amount of IT support required, as fewer incorrect configurations are made. To start using this free service, simply contact your local NREN.

References

[1] The eduroam architecture for network roaming
https://tools.ietf.org/html/draft-wierenga-ietf-eduroam-05

[2] Elenkov, Nikolay: Android Security Internals: An In-Depth Guide to Android's Security Architecture, 2015, pp. 248-249

[3] Csc.fi: Funet Network Services, Certificate Service
https://www.csc.fi/en/-/varmennepalvelu

[4] Freeradius.org: Certificate Compatibility
http://wiki.freeradius.org/guide/Certificate-Compatibility

[5] Terena.org: EAP Server Certificate considerations
https://wiki.terena.org/display/H2eduroam/EAP+Server+Certificate+considerations

[6] Microsoft.com: Certificate requirements when you use EAP-TLS or PEAP with EAP-TLS
https://support.microsoft.com/en-us/kb/814394

[7] eduroam.org: eduroam Service Definition
https://www.eduroam.org/index.php?p=docs

[8] Terena.org: How to offer helpdesk support to end users
https://wiki.terena.org/display/H2eduroam/How+to+offer+helpdesk+support+to+end+users

[9] eduroam CAT
https://cat.eduroam.org/

Glossary

CA	Certificate Authority
CAT	(eduroam) Configuration Assistant Tool
CN	Common Name
CRL	Certificate Revocation List
EAP	Extensible Authentication Protocol
EKU	Extended Key Usage
FQDN	Fully Qualified Domain Name
IdP	Identity Provider
MDM	Mobile Device Management
MITM	Man in the Middle (Attack)
NREN	National Research and Education Network
PKI	Public Key Infrastructure
RADIUS	Remote Authentication Dial In User Service
SHA	Secure Hash Algorithm
TCS	Trusted Certificate Service

Complete BPDs are available at http://services.geant.net/cbp/Pages/Home.aspx

campus-bp-announcements@geant.org