eduroam Privacy Framework

12.11.2018

CSC – TIETEEN TIETOTEKNIIKAN KESKUS OY
Keilaranta 14 • PL 405 • 02101 Espoo
Puh. (09) 457 2001 • Fax (09) 457 2302 • Y-tunnus 0920632-0 • www.csc.fi

CSC – IT CENTER FOR SCIENCE LTD.
Keilaranta 14 • P.O. BOX 405 • FI-02101 Espoo • Finland
Tel. +358(0)9 457 2001 • Fax +358(0) 9 457 2302 • VAT number FI09206320 • www.csc.fi

Table of Contents

1. INTRODUCTION

1.1 EDUROAM

Funet has set up the eduroam service to ensure optimal collaboration between Funet member institutions. eduroam gives students, lecturers, employees and researchers secure and easy access to the fixed and wireless networks of their own and other institutions both at home and abroad.

At an international level, the umbrella organisation of European research networks, GÉANT, is responsible for managing eduroam. Their privacy notice can be found at . As a European eduroam confederation member, Funet has been authorised by GÉANT to offer and implement the eduroam service in Finland as a **Roaming Operator**. For more information on the (technical) operation of eduroam, see (in Finnish).

Funet aims to provide eduroam at the highest possible quality level. It is important to consider user data integrity and the way institutions and Funet handle users' personal data.

1.2 PURPOSE AND SCOPE OF THIS DOCUMENT

The creation of eduroam involved various parties that process personal data, such as the participating institutions. These parties will have to comply with the current and future privacy regulations, including the General Data Protection Regulation ("**GDPR**"), which came into force on 25 May 2018.

To ensure it is clear to the data subjects (the eduroam end users) whom they can contact with any questions regarding privacy, Funet has published this eduroam Privacy Framework, which further describes the distribution of the parties' roles and provides more information on how personal data are processed. Although eduroam is used internationally, this Privacy Framework primarily intends to clarify the distribution of eduroam roles among the Finnish participating parties.

2. DISTRIBUTION OF ROLES WITHIN EDUROAM

2.1 FEDERATED STRUCTURE

eduroam is characterised by a federal structure in which the institutions involved give their employees and/or guests secure access to each other's network. The key functionality of federated authentication as offered by eduroam is that users with digital identities obtained from their home institutions can access member institutions' networks. In practice, the home and host institutions jointly handle end users' login requests. **Authentication** takes place at the home institution and **authorisation** takes place at the institution to which access is requested (the host institution).

The national RADIUS servers that Funet provide as the Roaming Operator acts as a central hub that correctly directs all login requests. The servers are maintained by Radiator Software Oy and CSC – IT Center for Science Ltd.

The table below describes the parties' roles in more detail.

Funet	The **Roaming Operator** manage the RADIUS servers required to route authentication requests.
Radiator Software Oy	Funet’s subcontractor maintains the RADIUS servers
Home institution	Also referred to as the **Identity Provider**: the institution that handles user authentication for eduroam.
Host institution	Also referred to as the **Service Provider**: the institution that handles user authorisation for eduroam.
eduroam Service Provider	An organisation that is not part of Funet, but still acts as a Service Provider to enable persons with eduroam accounts to use eduroam (for example in conference rooms, cafés, book shops and music centres).

2.2 PRIVACY ROLES

Terminology

The GDPR imposes most obligations on the controller. The controller establishes the purpose (the why) and the means (the how) for personal data processing, either alone or together with others. The controller may outsource the personal data processing to a processor. Processors are parties that process data on behalf of the controller without being under its direct authority. A processor has no control over the data processing and only acts according to the instructions of the controller, who remains responsible.

Privacy roles within eduroam

The parties involved (Funet, home institutions and host institutions) can influence the eduroam overarching policy and the processing taking place within it directly or indirectly and to a greater or lesser extent within the (inter)national cooperation chain. Institutions may act as both Identity Provider and Service Provider within the eduroam system. At the macro level, the various processing operations of the parties involved are more or less integrated with the common goal of enabling access to each other's networks by using jointly established resources.

Within this set-up, it is obvious to consider Funet, the home institutions and host institutions as *sub-controllers*. This means that each of these parties is independently responsible for its own part of the data processing. The parties therefore do not act as each other's mutual processors, so they do not have to sign any processor agreements with each other.

The eduroam Service Provider is an exception. As this party is not part of Funet and can therefore not influence the eduroam policy (including data processing), this party qualifies as a processor and must sign a processor agreement with Funet.

3. THE PROCESSING OF (PERSONAL) DATA WITHIN EDUROAM

3.1 WHAT IS THE PURPOSE OF THE DATA PROCESSING?

The GDPR is based on the principle of purpose limitation: personal data can only be processed if they are necessary to achieve a specific purpose. This purpose must be described in advance. A specific description and justification of the purpose are required by law. The personal data will not be used again for any other incompatible purpose.

The overarching purpose of eduroam for which the required (personal) user data are processed is to enable access to each other's networks. The processing is also necessary to ensure the proper operation of eduroam and to identify the home institution and end user (via the home organisation) in case of unauthorised use.

3.2 WHO DOES WHAT WITHIN EDUROAM?

Funet (Roaming Operator)

In this context, Funet acts as the Roaming Operator by connecting the participating institutions with each other through its RADIUS servers. Funet’s subcontractor Radiator Software Oy maintains the national RADIUS servers required for the authentication within eduroam. In addition to data processing for services, Funet and Radiator Software Oy keep logs of the authentication requests for troubleshooting purposes.

The Home Institution (authentication)

The home institution handles user authentication. In concrete terms, this means that if the user is a guest at another institution, the user's login details are sent to the home institution's authentication server with end-to-end encryption (via Roaming Operator Funet).

The home institution checks that the user's login details are valid with its own Identity Management System and reports this back to the host institution, which can then proceed with the authorisation.

The Host Institution (authorisation)

A user at the host institution can access the network via eduroam. The host institution sends the user's encrypted login details to the home institution's authentication server via the Roaming Operator (Funet). Once the home institution has verified that the user's login data are valid, it will report this back to the host institution. The host institution handles the user authorisation for eduroam.

eduroam Service Provider

A visitor from the eduroam Service Provider logs into the network via eduroam. The eduroam Service Provider sends the user's encrypted login details to the home institution's authentication server via the Roaming Operator (Funet). Once the home institution has verified that the user's details are valid, it will report this back to the eduroam Service Provider. The eduroam Service Provider handles user authorisation for eduroam.

3.3 WHICH (PERSONAL) DATA ARE REGISTERED?

Privacy legislation requires that the quantity and detail of the data collected is limited (not excessive) and the data are accessible (to avoid incorrect/incomplete information) and relevant (not superfluous).

When the parties involved in eduroam process personal data, they always need to ask themselves whether less data can be used to achieve the same goal. The data must be correct and accurate. This means that the user is identified when data are saved for the first time with the home institution. After that, periodic (internal) checks must be performed to ensure the data are still correct.

By the very nature of certain personal data, their processing may constitute a major breach of a data subject's privacy in terms of religion, race, political affiliation, health and criminal history. The law therefore applies a stricter regime for this type of data. The principle of this regime is that these so-called 'special' data must not be processed. Of course, the law provides a number of specific exceptions to this principle. In the case of eduroam, no special data will be processed by any participants.

Funet (Roaming Operator)

Funet and Radiator Software process the following (personal) data with regard to eduroam:

- Users' unique device data (MAC address)
- The identities of the home institution and host institution
- Time of the authentication request
- Username outer identity in EAP message. The username can be sent in anonymised form if the user has configured this.

The above data are also stored in log files.

Home institution

The home institution processes the following (personal) data with regard to eduroam:

- Users' unique device data (MAC address)
- The host institution's identity
- The access point's identity (Wi-Fi access point/network switch)
- Time of the authentication request
- User authentication data (username and password)

The above data are also stored in log files.

Host institution

The host institution processes the following (personal) data with regard to eduroam:

- Users' unique device data (MAC address)
- The home institution's identity
- The access point's identity (Wi-Fi access point/network switch)
- Time of the authentication request
- Username outer identity in EAP message. The username can be sent in anonymised form if the user has configured this.

The above data are also stored in log files.

eduroam Service Provider

The eduroam Service Provider processes the following (personal) data with regard to eduroam:

- Users' unique device data (MAC address)
- The home institution's identity
- The access point's identity (Wi-Fi access point)
- Time of the authentication request
- Username outer identity in EAP message. The username can be sent in anonymised form if the user has configured this.

The above data are also stored in log files.

As already mentioned above, the right configuration (to be determined by the user) will ensure that the Roaming Operator or host institution will not be able to retrieve or view the username of users who logged in in the log files. Funet, the host institution and the eduroam Service Provider will only see 'anonymous@organisation.fi', the so-called *outer identity*, if the user has configured this. The *inner identity* is encrypted (just like the password) and can only be viewed by the home institution.

3.4 HOW LONG ARE THE DATA KEPT?

The GDPR stipulates that organisations must not store personal data for no longer than is necessary for the purposes for which the personal data are processed.

Funet will not keep their processed data for longer than 6 months. Processes in service providers, home institutions and host institutions may vary.

4. THE DISTRIBUTION OF RESPONSIBILITIES WITHIN EDUROAM

4.1 GENERAL INFORMATION

Generally, each of the parties involved is independently responsible for its own part of the data processing. However, taking into account the multitude of parties involved in eduroam, it is important to make clear who does what, so that users are aware whom they should contact with any issues.

4.2 TRANSPARENCY

Transparency is an important goal of the GDPR. To ensure adequate user privacy protection, users must be aware of what their personal data are used for. The more sensitive the user data are, the more reason there is to give the user detailed information on the data's processing.

According to Article 12 and following of the GDPR, the obligation to inform data subjects about the data's processing and to comply with requests from data subjects wishing to exercise their rights under the GDPR rests primarily with the controller. This means that the (sub-)controllers within the eduroam system are each responsible for informing the end users and meeting the end users' privacy requests. From a practical point of view, the parties agree on the following in this regard.

Privacy notice

The first logical point of contact for eduroam users is the home institution. The parties therefore agree that the home institution will primarily ensure that users are informed of how their personal data are processed when they use eduroam. The privacy notice template (**Appendix 1**) can be used for this.

The above does not detract from the fact that each party remains responsible for informing users about their own data processing. To ensure consistent information provision to users, Funet also advises the other parties involved to use the above-mentioned privacy notice template.

4.3 EXERCISING USER RIGHTS

To ensure the transparent processing of personal data, users have various rights under the GDPR. Users can exercise these rights with respect to the controller. For example, users are entitled to access, correct and delete their data.

If users wish to invoke their privacy rights, it is best to contact the ICT help desk of their own home institution. The home institution will then respond within one month, unless it is a complex request. In the latter case, the institution will inform the user that it needs to extend this period within 1 month of receiving the request. The period can be extended by up to 2 additional months.

4.4 SECURITY

Students, lecturers, researchers and institutions all benefit from a secure online environment. Each institution is independently responsible for taking the appropriate technical and organisational protection measures to secure personal data. Security services can help in this regard. They have many benefits.

The institutions can use the security services via Funet. These services are developed especially for and by institutions. For more information, please contact Funet CERT.

The use of eduroam is also subject to certain (technical) conditions to be met by the participating organisations. These preconditions can be found on the eduroam wiki: https://wiki.geant.org/display/H2eduroam/eduroam+SP.

4.5 SECURITY INCIDENTS

The GDPR states that personal data breaches must be reported to the Personal Data Protection Authority and the data subject under certain circumstances. Funet and the institutions are each independently responsible for the timely reporting of data breaches.

Funet member institutions can use Funet CERT, which is Funet's Computer Security Incident Team (CSIRT). Funet CERT investigates and coordinates security breaches at Funet member institutions.

4.6 CENTRAL POINT OF CONTACT FOR USERS

If users have any general questions about this Privacy Framework or how personal data are processed within eduroam, they can send an e-mail to the following central e-mail address: privacy(at)csc.fi.

If users have any specific questions, it is best to contact the home institution's data protection officer (if there is one) or the home institution's ICT help desk.

5. APPENDICES

5.1 APPENDIX 1: PRIVACY POLICY TEMPLATE FOR THE INSTITUTIONS

The most recent template is available online at
https://wiki.eduuni.fi/display/funet/eduroam-verkkovierailu