Norwegian eduroam policy

Revised 15th June 2012

Notation as defined in RFC 2119
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

1.0 Background

1.1 This document defines rules and gives guidelines for Service and Identity Providers of roaming Internet access for educational and research purposes

1.2 eduroam is a TERENA registered trademark and is an abbreviation for "educational roaming" that originated from a European national education and research networks project to deliver a user-friendly, secure and scalable internet access solution for visitors.

1.3 More eduroam information is available at www.eduroam.org and www.eduroam.no.

2.0 Roles and Responsibilities

2.1 eduroam national service provider

2.1.1 UNINETT is responsible for the national eduroam service. UNINETT will act as the federation's eduroam policy authority, in accordance with the European eduroam confederation policy. http://www.eduroam.org/downloads/docs/eduroam_Compliance_Statement_v1_0.pdf

2.1.2 UNINETT's roles are:

a. To coordinate and support the eduroam service to appointed technical contacts of participating organizations only.
b. To maintain links with the European eduroam community and their authentication servers.
c. Contribute to the further development of the eduroam concept.

2.1.3 UNINETT is responsible for maintaining and developing a national authentication server network that connects to participating organizations. The eduroam service provider assumes no liability for any consequence as a result of abuse or a loss or disruption of service. The eduroam identity and resource providers (whether in the same or a different federation or confederation) accept no liability from each other.

2.1.4 UNINETT is responsible for managing a second line technical support function covering pre-connection and

ongoing technical support and maintenance of a dedicated website (www.eduroam.no) containing technical, service, policy and process information, and mailing lists.

2.1.5 UNINETT is responsible for coordinating communications between participating organizations so that policies and procedures contained herein are adhered to in a timely manner and as a matter of last resort has the right to impose technical sanctions.

2.1.6 UNINETT will work with the appointed eduroam technical contact of a participating organization to test one or more of the following aspects
a. initial connectivity
b. authentication and authorization processes
c. the authorized services offered
d. review of the logging activities
e. review the relevant authentication server configuration for compliance with the policy.

2.2 eduroam identity providers

2.2.1 The role of the identity provider (home organization) is to act as the credential provider for registered staff and students. It will also act as technical and service support function for its users who want to access eduroam services at eduroam resource providers (visited sites). Only appointed technical contacts can escalate technical support, service support or security issues on behalf of their users to UNINETT.

2.2.2 Identity providers must assist UNINETT in case of security incidents, misuse etc. in accordance with UNINETT Best-practice for security- and incident handling. See https://www.uninett.no/sites/drupal.uninett.no.uninett/files/webfm/_Produkter%20og%20tjenester/campustjenester/@campus/UFS/pdf/ufs112.pdf and http://cert.uninett.no/

2.3 eduroam resource providers

2.3.1 The role of the eduroam resource providers is to supply Internet access to validated eduroam users. The eduroam resource provider authorizes the use of any service it provides.

2.3.2 Where user activity is monitored, the eduroam resource provider must clearly announce this fact including how this is monitored, stored and accessed.

2.3.3 The eduroam resource provider must abide by this policy and follow UNINETT's service processes and guidelines listed herein.

2.3.4 The eduroam resource provider must cooperate with UNINETT in all matters concerning eduroam.

2.4 User

2.4.1 A user is defined as a person who wants access to the Internet at an eduroam resource provider. The user must abide by their home organization's (identity provider) Acceptable Use Policy (AUP) and the visited organization's AUP. Where regulations differ the more restrictive applies.

2.4.2 The users are responsible for their credentials, their use of it and of any service they might provide.

2.4.3 The user is responsible for taking reasonable steps to ensure that he/she is connected to a genuine eduroam service (as directed by their home organization) prior to entering their login credentials. This means using mutual authentication (authenticate the RADIUS servers certificate before entering login credentials) and only logging on to a 802.1X secured network.

2.4.4 If credentials are thought to have been compromised, the user must immediately report back to his home organization (identity provider).

2.4.5 The user is obliged to inform the visited organization (where possible) and home organization of any faults with the eduroam service or suspicions of the security having been compromised.

3.0 Base service

3.1 Identity providers must deploy an authentication server in accordance with eduroam technical and policy guidelines available at http://www.eduroam.no/eduroam_policy.pdf. (this document) A secondary authentication server is recommended for resilience purposes.

3.2 The eduroam identity provider authentication server(s) must be reachable from the eduroam resource provider's authentication servers for authentication and accounting purposes.

3.3 The identity provider must create an eduroam test account (eduroam username and password credential) that will be made accessible to UNINETT to assist in pre-connection testing, ongoing monitoring, support and fault finding activities. If the test account's password is changed, UNINETT must be notified by the home organization a timely manner. No network services other than authentication should be accorded to the test account.

3.4 The eduroam resource provider may offer any media. As a minimum wireless LAN IEEE 802.11g is required. UNINETT recommendation is to offer wireless IEEE802.11 a/g/n.

3.5 The eduroam resource provider must deploy the SSID 'eduroam' (case sensitive). The SSID ‘eduroam’ should be broadcasted.

3.6 The eduroam resource provider must implement IEEE 802.1X authentication with a RADIUS interface to connect to the eduroam infrastructure. IEEE 802.11i wireless networks must support WPA2 + AES and may additionally support WPA + TKIP as a courtesy to users of legacy hardware.

3.7 The eduroam resource provider must as a minimum offer:
- Standard IPSec VPN: IP protocols 50 (ESP) and 51 (AH) both egress and ingress; UDP/500 (IKE) egress only
- OpenVPN 2.0: UDP/1194
- IPv6 Tunnel Broker service: IP protocol 41 ingress and egress
- IPsec NAT-Traversal UDP/4500
- Cisco IPSec VPN over TCP: TCP/10000 egress only
- PPTP VPN: IP protocol 47 (GRE) ingress and egress; TCP/1723 egress only
- SSH: TCP/22 egress only
- HTTP: TCP/80 egress only
- HTTPS: TCP/443 egress only
- IMAP2+4: TCP/143 egress only
- IMAP3: TCP/220 egress only
- IMAPS: TCP/993 egress only
- POP: TCP/110 egress only
- POP3S: TCP/995 egress only
- Passive FTP: TCP/21 egress only
- SMTPS: TCP/465 egress only
- SMTP submit with STARTTLS: TCP/587 egress only
- RDP: TCP/3389 egress only
- SIP: UDP/5060 ingess/egress
- RTP: UDP/16384 to UDP/16484 ingress/egress

3.8 The eduroam resource provider should provide a dedicated virtual local area network (VLAN) for eduroam-authenticated visitors.

3.9 The visited organization must not charge for eduroam access. This service is based on a shared access model where eduroam resource providers supply and receive Internet access for their users.

4.0 Logging

4.1 eduroam resource providers must log network usage information in such a way that it is possible at a later date to correlate a username with a MAC address and an IP address used at a given time.

4.2 eduroam resource providers must log all RADIUS authentication and accounting requests. The following information must be recorded:
a. The date and time the authentication request was received.
b. The RADIUS request's identifier.
c. The authentication result returned by the authentication database.
d. The reason given if the authentication was denied or failed.
e. The value of the request's accounting status type.

4.3 The eduroam resource provider must keep the logs in accordance with Norwegian laws and the current UNINETT best-practice. Co-operation about the content of these logs will be restricted to the eduroam technical contacts and UNINETT technical contact to assist in resolving specific security or abuse issues that have been reported to UNINETT.

5.0 Support

5.1 The identity provider must provide support to their users requesting access at an eduroam resource provider.

5.2 The eduroam identity provider should provide support to users from other eduroam identity providers that are requesting eduroam services at their eduroam identity provider campus.

5.3 The eduroam resource provider must publish local information about eduroam services on dedicated web pages on their organization website containing the following minimum information:

a. Text that confirms adherence (including a url link) to this policy document published on www.eduroam.no/eduroam_policy.pdf.
b. A url link to eduroam resource providers' Acceptable Use Policy (AUP) or equivalent.
c. A list or map showing eduroam access coverage areas.
d. Details of the broadcasted or non-broadcasted SSID as eduroam.
e. Details of the authentication process and authorized services offered.
f. Details about the use of a non-transparent application proxy including user configuration guidelines (if applicable).
g. A link to the website www.eduroam.no and posting of the eduroam logo and trademark statement.
h. Where user activity is monitored, the eduroam resource provider must clearly announce this fact including how this is monitored so as to meet with applicable legislation, including how long the information will be held for and who has access to it.
i. The contact details of the appropriate technical support that is responsible for eduroam services.

6.0 Communications

6.1 The eduroam identity provider must provide UNINETT with contact details of two appointed technical contacts. Any changes to contact details must be notified to UNINETT in a timely manner.

6.2 The eduroam identity provider must designate a contact and their contact details to respond to security issues, this may be the same person designated as the appointed technical contact.

6.3 Participating organizations must notify UNINETT in a timely manner of the following incidents:

a. Security breaches
b. Misuse or abuse

c. Service faults
d. Changes to access controls (e.g. permit or deny of a user or realm)

UNINETT contact information:
E-mail: drift@uninett.no.
Phone +47 73 55 79 60 (08:00–16:00) and +47 73 55 79 61 (emergency center).

7.0 Authority, Compliance & Sanctions

7.1 The authority for this policy is UNINETT. Local policies must comply. UNINETT implements the national policy.

7.2 Any changes to this policy will be made in consultation with participating organizations and UNINETT.

7.3 Connecting to UNINETT authentication servers will be deemed as acceptance of this policy. Any organization that is currently connected will be given a period of one month's grace from the official ratification date of this policy by UNINETT, to either continue to connect as a statement of acceptance of this policy or the removal of their authentication server connection(s) to indicate an inability to accept this policy at the present time.

7.4 In cases where immediate action is required to protect the integrity and security of the eduroam service, UNINETT has the right to suspend the eduroam service or restrict eduroam access to only those participating organizations that can comply with the required changes. To do so, UNINETT will notify participating organizations of such incidents, outages and remedial.

7.5 UNINETT will notify by email to the nominated technical and/or security contact of the participating organization of any technical or policy breach or incident that requires resolution. Where such notifications are not acted upon in a timely manner, or where the breach or incident may impact on the security and integrity of eduroam, UNINETT has the right to block eduroam access to that organization.

7.6 eduroam resource providers may prevent use of their networks by all users from a particular eduroam identity provider by configuring their authentication server(s) to reject that realm; in some cases a eduroam resource provider may also be able to block a single visiting user.

7.7 eduroam identity providers may withdraw an individual user’s ability to use the eduroam by configuring their own authentication server or removing that user from their authentication database.

7.8 eduroam identity providers must also ensure that their computing regulations enable users who breach this policy to be subject to an appropriate internal disciplinary process irrespective of their location at the time.