Irish *eduroam* policy

Last updated: 6th February 2009

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. Background to this document

1. This document sets out guidelines that cover the control of the supply and receipt of roaming Internet access for educational purposes.

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 userfriendly, secure and scalable Internet access solution for visitors.

3. More information about *eduroam* is available at http://www.eduroam.org

2. Roles and Responsibilities

1. HEAnet Limited (hereafter called “HEAnet”) acts as the *eduroam* National Roaming Operator (NRO) for Ireland.

2. Organisations that participate in *eduroam* by providing their users credentials for authentication against the *eduroam* infrastructure are called Identity Providers, abbreviated as IdP.

3. Organisations that participate in *eduroam* by providing networking equipment that allows users to connect to the Internet using *eduroam* are called Service Providers, abbreviated as SP.

3. *eduroam* National Roaming Operator (NRO)

1. HEAnet is responsible for the national *eduroam* service. HEAnet will act as the federation's *eduroam* policy authority, in accordance with the European *eduroam* confederation policy.

2. HEAnet's role is three fold:
   (1) to coordinate and support the *eduroam* service to nominated technical contacts of participating organisations only, and
   (2) to maintain links with the European *eduroam* community and their authentication servers, and
   (3) contribute to the further development of the *eduroam* concept.

3. HEAnet is responsible for maintaining and developing a national authentication server network that connects to participating organisations. The NRO assumes no liability for any impact as a result of a loss or disruption of service. The *eduroam* IdP's and SP's (whether in the same or a different federation or confederation) accept no liability from each other.

4. HEAnet is responsible for managing a second line technical support function covering preconnection and ongoing technical support and maintenance of a dedicated website containing technical, service, policy and process information, and mailing lists.

5. HEAnet is responsible for coordinating communications between participating organisations 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.

6. HEAnet will work with the nominated *eduroam* technical contact of a participating organisation to test one or more of the following aspects:
   (1) initial connectivity,
   (2) authentication and authorisation processes and,
   (3) the authorised services offered, and review of the logging activities and the relevant authentication server configuration for compliance with the policy.

4. *eduroam* Identity Providers (IdP's)

1. The role of the IdP (home organisation) is to act as the credential provider for registered staff and students. Also it will act as technical and service support function for its users who want to access *eduroam* services at SP's (visited sites). Only nominated technical contacts can escalate technical support, service support or security issues on behalf of their users to the HEAnet.

2. IdPs MUST make their users aware of roaming conditions, especially of the user obligations in section 6. They MUST educate their users to follow security best practices, including how to identify the correct server certificate of the IdP.

3. IdP’s MUST engage cooperatively with HEANet to resolve security incidents involving their users. IdP’s shall not be required to provide logs or other data in response to incidents other than as required by statutory instrument.

4. IdP's MUST deploy an authentication server in accordance with the national *eduroam* technical and policy requirements guidelines available at http://www.eduroam.ie. A secondary authentication server is recommended for resilience purposes. The network equipment MUST comply to RFC 2865 (RADIUS) and SHOULD comply to RFC 2866 (RADIUS Accounting).

5. The IdP authentication server(s) MUST be reachable from HEAnet's national authentication and accounting servers for authentication and accounting purposes.

6. The IdP MUST create an *eduroam* test account (*eduroam* username and password credential) that will be made accessible to HEAnet to assist in preconnection testing, ongoing monitoring, support and fault finding activities. If the test account's password is changed, HEAnet MUST be notified by the home organisation in a timely manner. No authorised services should be accorded to the test account.

5. *eduroam* Service Providers (SP's)

1. The role of the SP's is to supply Internet access to users via *eduroam* (based on trusting that the user's IdP (home organisation) authentication check and response is valid). The SP authorises the use of any service it provides.

2. Where user activity is monitored, the SP MUST clearly announce this fact including how this is monitored, stored and accessed so as to comply with legislation.

3. The SP MUST abide by this policy and follow HEAnet's service processes and guidelines listed herein.

4. The SP may offer any media; however as a minimum, the SP MUST provide wireless LAN IEEE 802.11b whilst 802.11g is also recommended.

5. The SP MUST deploy the SSID '*eduroam*' and IEEE 802.1X Extensible Authentication Protocol (EAP) authentication (excluding EAPMD5) to promote a consistent service and minimum level of security. The SSID ”*eduroam*'' SHOULD be broadcasted.

6. The SP MUST as a minimum implement IEEE 802.1X and WPA/TKIP, or better.

7. The SP SHOULD, as a minimum, permit the following traffic to/from users of their *eduroam* service:
    - Domain Name Service: UDP/53 egress only; TCP/53 egress only
    - 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 NATTraversal 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 (S)FTP: TCP/21 egress only

- SMTPS: TCP/465 egress only
- SMTP submit with STARTTLS: TCP/587 egress only
- RDP: TCP/3389 egress only

8. The SP SHOULD implement a visitor virtual local area network (VLAN) for *eduroam* authenticated users that is not to be shared with other network services.

9. The SP SHOULD give public IP addresses to its visitors. Where available, Ipv6 connectivity SHOULD be provided.

10. The SP MUST NOT charge for *eduroam* access. This service is based on a shared access model where SP's supply and receive Internet access for their users.

6. Users

1. A user's role is in principle always a visitor who wants Internet access at an SP. The user MUST abide by their IdP's AUP or equivalent and respect the visited organisation's AUP or equivalent. Where regulations differ the more restrictive applies. Users MUST as a minimum abide by relevant law of the country where (s)he is physically situated while using the service, home or abroad.

2. The user is responsible for taking reasonable steps to ensure that (s)he is connected to a genuine *eduroam* service (as directed by their home organisation) prior to entering their login credentials. The primary means to achieve this is to validate the server certificate that is presented to the user upon login.

3. The user is responsible for their credentials and the use of any service they might provide.

4. If credentials are thought to have been compromised, the user MUST immediately report back to their IdP.

5. The user is obliged to inform the SP (where possible) and IdP of any faults with the *eduroam* service.

7. Logging

1. Both SP's and IdP's MUST log all authentication and accounting requests; the following information MUST be recorded
   (1) The date and time the authentication request was received;
   (2) The authentication result returned by the authentication database or upstream server;
   (3) For IdP's: The inner identity of the request;
   (4) The value of the request's accounting status type;
   (5) The value of the User-Name attribute in accounting requests;
   (6) The value of the Accounting-Session-Id in accounting requests.

2. The SP MUST log all DHCP transactions; including
   (1) The date and time of issue of the client's DHCP lease;
   (2) The MAC address of the client;

(3) The client's allocated IP address.

3. The SP MUST keep a log of DHCP transactions for a minimum of three months and a maximum of six months. Cooperation about the content of these logs will be restricted to the *eduroam* technical contacts and HEAnet technical contact to assist in resolving specific security or abuse issues that have been reported to HEAnet.

4. All relevant logs MUST be timestamped with accurate dates and times.

8. Support

1. The IdP MUST provide support to their users requesting access at an SP.

2. The SP SHOULD provide support to users from other IdP's that are requesting *eduroam* services at the SP site.

3. The SP MUST publish local information about *eduroam* services on dedicated web pages on their organisation website containing the following minimum information:
   (1) Text that confirms adherence to this policy document as published on http://www.eduroam.ie;
   (2) A url link to the SP's acceptable use policy or equivalent;
   (3) A list or map showing *eduroam* access coverage areas;
   (4) Details of the broadcasted or nonbroadcasted SSID as *eduroam*;
   (5) Details of the authentication process and authorised services offered;
   (6) Details about the use of a nontransparent application proxy including user configuration guidelines (if applicable);
   (7) A url link to the website http://www.eduroam.ie and posting of the *eduroam* logo and trademark statement;
   (8) Where user activity is monitored, the SP MUST clearly announce this fact including how this is monitored so as to meet with state or national legislation, including how long the information will be held for and who has access to it;
   (9) The contact details of the appropriate technical support that is responsible for *eduroam* services.
   (10) The IP traffic (protocols/port numbers/services) which the site will permit to be passed to/from the client of an *eduroam* user once successfully authenticated.

9. Communications

1. Both IdP's and SP's MUST provide HEAnet with contact details of two nominated technical contacts. Each contact may be either a named individual or a defined role. Any changes to contact details MUST be notified to HEAnet in a timely manner.

2. The IdP MUST designate a contact and their contact details to respond to security issues, this may be the same person designated as the nominated technical contact.

3. Participating organisations MUST notify HEAnet in a timely manner of the following incidents; (1) security breaches; (2) misuse or abuse; (3) service faults; (4) changes

to access controls (e.g. permit or deny of a user or realm).

10. Authority, Compliance & Sanctions

1. The authority for this policy is HEAnet who will implement this policy.

2. Any changes to this policy will be made in consultation with participating organisations and HEAnet.

3. Connecting to the national *eduroam* national authentication server network will be deemed as acceptance of this policy. Any organisation that is currently connected will be given a period of one month's grace from the official ratification date of this policy by HEAnet, 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.

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

5. HEAnet will notify by email to the nominated technical and/or security contact of the participating organisation 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*, HEAnet has the right to block *eduroam* access to that organisation.

6. SP's may prevent use of their networks by all users from a particular IdP by configuring their authentication server(s) to reject that realm; in some cases a SP may also be able to block a single visiting user.

7. IdP's may withdraw an individual user's ability to use *eduroam* by configuring their own authentication server or removing that user from their authentication database.

8. IdP's 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.

Participating organisation:

document

participating as ☐ Service Provider (SP)
☐ Identity Provider (IdP) for the following realm(s):

_____

_____

Technical Contact 1: Name: _____

E-Mail: _____

Tel: _____

Technical Contact 2: Name: _____

E-Mail: _____

Tel: _____

Security Contact (IdP only):
☐ same as technical contact ☐ dedicated contact below

Name: _____

E-Mail: _____

Tel: _____

Signatures & dates:

- for the participating organisation - - for HEAnet Limited -