Slovak eduroam policy draft

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 to this document

1.1 This document sets out guidelines that cover the control of the supply and receipt 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 information about *eduroam* is available at www.*eduroam.org*.

2.0 Roles and Responsibilities

2.1 *eduroam* service provider

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

2.1.2 SANET's role is three fold, (1) to coordinate and support the *eduroam* service to nominated technical contacts of participating organizations 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.

2.1.3 SANET 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 impact 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 SANET is responsible for managing a second line technical support function covering pre-connection and ongoing technical support and maintenance of a dedicated website containing technical, service, policy and process information, and mailing lists.

2.1.5 SANET 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 SANET will work with the nominated *eduroam* technical contact of a participating organization to test one or more of the following aspects (1) initial connectivity, (2) authentication and authorization processes and (3) the authorized services offered, and review of (1) the logging activities and (2) the relevant authentication server configuration for compliance with the policy.

2.2 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. Also it will act as technical and service support function for its user's who want to access *eduroam* services at *eduroam* resource providers (visited sites). Only nominated technical contacts can escalate technical support, service support or security issues on behalf of their users to the SANET.

2.2.2 Identity providers must cooperate with **SANET** in case of security incidents, misuse etc.

2.3 *eduroam* resource providers

2.3.1 The role of the *eduroam* resource providers is to supply internet access to validated *eduroam users* (based on trusting that the user's identity provider (home organization) authentication check and response is valid). 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 so as to comply with legislation.

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

2.3.4 The *eduroam* recourse provider must cooperate with SANET in all matters concerning *eduroam*.

2.4 User

2.4.1 A user’s role is in principle always a visitor who wants internet access at an *eduroam* resource provider. The user must abide by their identity providers (home organisation's) Acceptable Use Policy (AUP) or equivalent and respect the visited organization's AUP or equivalent. Where regulations differ the more restrictive applies. Users must as a minimum abide by relevant law of the country where he is physically situated, home or abroad.

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

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

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

2.4.5 The user should inform the visited organization (where possible) and home organization of any faults with the *eduroam* service.

3.0 Base service

3.1 Identity providers must deploy an authentication server in accordance with *eduroam* technical and policy guidelines available at www.sanet.sk/eduroam/policy.pdf. 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 SANET to assist in pre-connection testing, ongoing monitoring, support and fault finding activities. If the test account's password is changed, SANET must be notified by the home organisation in a timely manner. No authorised services should be accorded to the test account.

3.4 The eduroam resource provider may offer any media; however as a minimum, wireless LAN IEEE 802.11b is required whilst 802.11g is also recommended.

3.5 The eduroam resource provider must deploy the SSID '*eduroam*' and IEEE 802.1X Extensible Authentication Protocol (EAP) authentication (excluding EAP-MD5) to promote a consistent service and minimum level of security. The SSID "*eduroam*" should be broadcasted.

3.6 The eduroam resource provider must as a minimum implement IEEE 802.1X and WPA/TKIP, or better.

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 (S)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 both egress and ingress
- RTP: UDP/16384 to UDP/16484 both egress and ingress

3.8 The eduroam resource provider should implement a dedicated virtual local area network (VLAN) for *eduroam*-authenticated visitors that is not to be shared with other network services.

3.9 The visited organisation 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 Both eduroam resource providers and identity providers must log all authentication 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;

(3) For identity providers: The inner identity of the request;

(4) The value of the user name attribute in the request ('outer EAP-identity').

(5) The value of the Calling-Station-Id attribute in the request.

4.2 Both eduroam resource providers and identity providers must log all accounting requests; the following information must be recorded

(1) The date and time the accounting request was received;

(2) The value of the user name attribute in the request;

(3) The value of the accounting session ID;

(4) The value of the request's accounting status type.

4.3 The eduroam resource provider 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.

4.4 The eduroam resource provider or identity provider must keep a log of authentication requests, accounting requests and DHCP transactions for a minimum of six months and a maximum of twelve months. Co-operation about the content of these logs will be restricted to the *eduroam* technical contacts and SANET technical contact to assist in resolving specific security or abuse issues that have been reported to SANET.

4.5 All relevant logs MUST be created with synchronization to a reliable time source.

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,

(1) Text that confirms adherence (including a url link) to this policy document published on www.*eduroam*.sk;

(2) A url link to eduroam resource providers' acceptable use policy or equivalent;

(3) A list or map showing *eduroam* access coverage areas;

(4) Details of the broadcasted or non-broadcasted SSID as *eduroam*;

(6) Details of the authentication process and authorized services offered;

(7) Details about the use of a non-transparent application proxy including user configuration guidelines (if applicable);

(8) A url link to the website www.eduroam.sk and posting of the *eduroam* logo and trademark statement;

(9) Where user activity is monitored, the eduroam resource provider 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.

(10) 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 SANET with contact details of two nominated technical contacts. Any changes to contact details must be notified to SANET 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 nominated technical contact.

6.3 Participating organizations must notify SANET 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)

7.0 Authority, Compliance & Sanctions

7.1 The authority for this policy is SANET who will implement this policy.

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

7.3 Connecting to SANET 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 SANET, 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, SANET 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, SANET will notify participating organizations of such incidents, outages and remedial .

7.5 SANET 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*, SANET 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 an 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.