The Danish *eduroam* policy

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. The full text of RFC 2119 is given in appendix.

The purpose of the Danish eduroam federation is to provide mutual roaming Internet access to its members: the participating institutions and the end users. The federation MAY peer with other roaming infrastructures. The appropriate policy rules SHALL be defined in a confederation peering document. Danish eduroam is open to institutions connected to Forskningsnettet.

Content

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 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 Forskningsnettet

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

2.1.2 Forskningsnettet's role is three fold:
1) to coordinate and support the *eduroam* service to nominated technical contacts of participating organizations only

2) to maintain links with the European *eduroam* community and their authentication servers

3) contribute to the further development of the *eduroam* concept

2.1.3 Forskningsnettet is responsible for maintaining and developing a national authentication server network that connects to participating organizations. Forskningsnettet assumes no liability for any impact as a result of a loss or disruption of service.

2.1.4 Forskningsnettet 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, process information etc.

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

2.1.6 Forskningsnettet SHALL work with the nominated *eduroam* technical contact of participating organizations to test one or more of the following aspects:

1) initial connectivity
2) authentication and authorization processes and
3) the authorized services offered

2.2 eduroam identity providers

2.2.1 *eduroam* identity providers (the users' home organisation) MUST act as the credential provider for registered staff and students. Also it SHALL act as technical and service support function for its' users.

2.2.2 Each participating organisation MUST provide a written statement telling that the following is in place:

a) logging activities (see below)
b) proper authentication server configuration

2.2.3 Identity providers MUST cooperate with Forskningsnettet in case of security incidents, misuse etc. Only nominated technical contacts MAY escalate technical support, service support or security issues on behalf of their users to Forskningsnettet.

2.2.4 **User name format requirements**

2.2.4.1 All *eduroam* user names must conform to RFC4282 (Network Access Identifier specification). The realm component must conclude with the *eduroam* identity providers' realm name, which must be a domain name in the global DNS that the identity provider administers, either directly or by delegation

2.2.5 **EAP authentication general requirements**

2.2.5.1 *eduroam* identity providers MUST configure their Extensible Authentication Protocol (EAP) server to authenticate one or more EAP types

2.2.5.2 *eduroam* identity providers MUST select a type, or types, for which their EAP server will generate symmetric keying material for encryption ciphers, and configure their RADIUS authentication server to encapsulate the keys, in accordance with section 3.16 of RFC3580 (IEEE 802.1X RADIUS Usage Guidelines), within RADIUS Access-Accept packets

2.2.5.2.1 *eduroam* identity providers MUST log all authentication attempts; the following information MUST be recorded:
- the authentication result returned by the authentication database
- the reason given if the authentication was denied or failed

2.3 **eduroam resource providers**

2.3.1 **Contact information**

2.3.1.1 Federation members MUST designate a technical contact that can be contacted using email and telephone during working hours. The contact MAY be either a named individual or an organisational unit. Arrangements MUST be made to cover for absence owing to eventualities such as illness and holidays.

2.3.2 Each participating organisation MUST provide a written statement telling that the following is in place:

a) logging activities (see below)
b) proper authentication server configuration

2.3.3 **RADIUS servers**

2.3.3.1 RADIUS clients and servers MUST comply with RFC2865 (RADIUS) and RFC2866 (RADIUS accounting)

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

2.3.3.3 Federation members' RADIUS proxy servers MUST be reachable from the Federation RADIUS proxy servers on ports UDP/1812 and UDP/1813, or ports UDP/1645 and UDP/1646, for authentication and accounting respectively

2.3.3.4 Federation members' RADIUS proxy servers MUST respond to ICMP Echo Requests sent by the Federation RADIUS proxy servers

2.3.3.5 Federation members SHOULD ensure that logs are kept of all eduroam RADIUS authentication requests exchanged; the following information SHOULD be recorded:

- 2.3.3.5.1 The time the authentication request was exchanged
- 2.3.3.5.2 The value of the user name attribute in the request ('outer EAP-identity')
- 2.3.3.5.3 The value of the Calling-Station-Id attribute in the request

2.3.3.6 Federation members SHOULD log all eduroam RADIUS accounting requests; the following information SHOULD be recorded:

- 2.3.3.6.1 The time the accounting request was exchanged
- 2.3.3.6.2 The value of the user name attribute in the request
- 2.3.3.6.3 The value of the accounting session ID
- 2.3.3.6.4 The value of the request's accounting status type

2.3.4 RADIUS forwarding

2.3.4.1 *eduroam* resource providers MUST forward RADIUS requests containing user names with unknown realms to the national *eduroam* federation server

2.3.4.2 *eduroam* resource providers MAY configure additional realms to forward requests to other internal RADIUS servers, but these realms MUST NOT be derived from any domain in the global DNS that the participant does not administer

2.3.4.3 *eduroam* resource providers MAY configure additional realms to forward requests to external RADIUS servers in other organisations, but these realms MUST be derived from domains in the global DNS that the recipient organisation administers (either directly, or by delegation)

2.3.4.4 *eduroam* resource providers MUST NOT otherwise forward requests to other *eduroam* participants.

2.3.5 Resilience

2.3.5.1 *eduroam* ressource providers SHOULD deploy a secondary *eduroam* RADIUS server for resilience purposes

2.3.6 Network addressing

2.3.6.1 eduroam resource providers MUST keep sufficient logging information to be able to correlate between a client's layer 2 (MAC) address and the layer 3 (IP) address that was issued after login. They SHOULD log all DHCP transactions; if they do, the following information MUST be recorded:

- 2.3.6.1.1 The time of issue of the client's DHCP lease
- 2.3.6.1.2 The MAC address of the client
- 2.3.6.1.3 The IP address allocated to the client

2.3.7 **802.1X Network access server (NAS)**

2.3.7.1 eduroam resource providers MUST deploy NASes that support IEEE 802.1X and symmetric keying using keys provided within RADIUS Access-Accept packets, in accordance with section 3.16 of RFC3580

2.3.7.2 eduroam resource providers MUST assign a single user per NAS port

2.3.7.3 eduroam resource providers MUST deploy NASes that include the following RADIUS attributes within Access-Request packets: The users' MAC address within the Caller-Station-ID attribute

2.3.8 **Application and interception proxies**

2.3.8.1 eduroam resource providers deploying application or interception proxies MUST publish information about application- and intercept proxies on their eduroam website

2.3.8.2 If an application proxy is not transparent, the resource provider MUST also provide documentation on the configuration of applications to use the proxy

2.3.9 **IP filtering**

2.3.9.1 *eduroam* resource providers SHOULD provide open network access to *eduroam* users

2.3.10 **EAP proxying**

2.3.10.1.1 *eduroam* resource providers MUST transparently proxy any EAP-type for visiting users

2.3.11 **Website**

2.3.11.1 Every *eduroam* ressource provider MUST publish an eduroam website, which MUST be generally accessible from all hosts on the Internet on TCP/80. The website MUST include the following at a minimum:

2.3.11.1.1 information and links to the local federation participants
2.3.11.1.2 local acceptable use policy (AUP)
2.3.11.1.3 the *eduroam* logo and link to www.eduroam.org
2.3.11.1.4 local installation guide for network clients

2.3.12 **Service Set Identifier (SSID)**

2.3.12.1 All *eduroam* resource providers SHOULD implement the SSID 'eduroam'. The SSID SHOULD be broadcasted.

2.3.12.2 Overlapping IP-subnets with same SSID is known to be a problem. If this situation occurs the SSIDs of those institutions involved can be changed to 'eduroam-[inst]' (where [inst] is an easily understandable indication of institutions name). If this solution is applied the SSIDs MUST be broadcasted.

2.4 **Users**

2.4.1 The users are responsible for usage of their credentials.

2.4.2 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) 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.

2.4.3 The user SHOULD take reasonable steps to ensure that he is connected to a genuine *eduroam* service (as directed by his home organization) prior to entering his 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.

As participating institution

Name and address:

Date and signature

Forskningsnettet

Sekretariatschef
Steen Pedersen

27.04.07

Date and signature

Addendum January 2011

Politik for kryptering i trådløs adgang til eduroam i Danmark

Beskyttet adgang (WPA) er obligatorisk ved udbydelse af trådløs adgang til eduroam. TKIP (Temporal Key Integrity Protocol) har her haft sin plads, men anses nu for kompromiteret, og er derfor ikke ønsket. Dansk eduroam sigter mod at brugerskaren forlader brugen af TKIP hurtigst muligt, og senst i første kvartal 2012. Hvor eduroam udbydes trådløst (i adgangspunkterne) tilstræbes i resten af 2011 at tilgængeliggøre såvel WPA/TKIP som dens afløser (WPA2/AES). Dette af hensyn til besøgende, der har udstyr, som er indstillet til den gamle form (WPA/TKIP).

Appendix RFC 2119

RFC2119 as given in: http://www.ietf.org/rfc/rfc2119.txt

```
Network Working Group                                          S. Bradner
Request for Comments: 2119                          Harvard University
BCP: 14                                                        March 1997
Category: Best Current Practice


        Key words for use in RFCs to Indicate Requirement Levels

Status of this Memo

   This document specifies an Internet Best Current Practices for the
   Internet Community, and requests discussion and suggestions for
   improvements.  Distribution of this memo is unlimited.

Abstract

   In many standards track documents several words are used to signify
   the requirements in the specification.  These words are often
   capitalized.  This document defines these words as they should be
   interpreted in IETF documents.  Authors who follow these guidelines
   should incorporate this phrase near the beginning of their document:

      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.

   Note that the force of these words is modified by the requirement
   level of the document in which they are used.

1. MUST   This word, or the terms "REQUIRED" or "SHALL", mean that the
   definition is an absolute requirement of the specification.

2. MUST NOT   This phrase, or the phrase "SHALL NOT", mean that the
   definition is an absolute prohibition of the specification.

3. SHOULD   This word, or the adjective "RECOMMENDED", mean that there
   may exist valid reasons in particular circumstances to ignore a
   particular item, but the full implications must be understood and
   carefully weighed before choosing a different course.

4. SHOULD NOT   This phrase, or the phrase "NOT RECOMMENDED" mean that
   there may exist valid reasons in particular circumstances when the
   particular behavior is acceptable or even useful, but the full
   implications should be understood and the case carefully weighed
```

before implementing any behavior described with this label.

5. MAY This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

6. Guidance in the use of these Imperatives

   Imperatives of the type defined in this memo must be used with care and sparingly. In particular, they MUST only be used where it is actually required for interoperation or to limit behavior which has potential for causing harm (e.g., limiting retransmisssions) For example, they must not be used to try to impose a particular method on implementors where the method is not required for interoperability.

7. Security Considerations

   These terms are frequently used to specify behavior with security implications. The effects on security of not implementing a MUST or SHOULD, or doing something the specification says MUST NOT or SHOULD NOT be done may be very subtle. Document authors should take the time to elaborate the security implications of not following recommendations or requirements as most implementors will not have had the benefit of the experience and discussion that produced the specification.

8. Acknowledgments

   The definitions of these terms are an amalgam of definitions taken from a number of RFCs. In addition, suggestions have been incorporated from a number of people including Robert Ullmann, Thomas Narten, Neal McBurnett, and Robert Elz.

9. Author's Address

Scott Bradner
Harvard University
1350 Mass. Ave.
Cambridge, MA 02138

phone - +1 617 495 3864

email - sob@harvard.edu