09.07.08

# Deliverable DS5.4.1: Report on RadSec Integration

**Deliverable DS5.4.1**

| | |
|---|---|
| Contractual Date: | 29/02/08 |
| Actual Date: | 09/07/08 |
| Contract Number: | 511082 |
| Instrument type: | Integrated Infrastructure Initiative (I3) |
| Activity: | SA5 |
| Work Item: | WI4 |
| Nature of Deliverable: | R (Report) |
| Dissemination Level | PU (Public) |
| Lead Partner | RESTENA |
| Document Code | GN2-08-143v2 |

**Authors:** Stefan Winter, Miroslav Milinovic, Ian Thomson

**Abstract**

This document summarises the current state of deployment of the RadSec protocol within the eduroam infrastructure. It describes the current situation for the development, implementation and standardisation of the RadSec protocol. It also describes the eduroam RadSec server trust model necessary for the identification and authorisation of RadSec servers in the eduroam closed roaming environment.

# Table of Contents

# 0 Executive Summary

RADIUS is a cornerstone of the eduroam infrastructure. RadSec is an extension to the RADIUS protocol, and this document summarises the current state of the development, implementation and standardisation of the RadSec protocol by JRA5 within the eduroam infrastructure. It also describes the opportunities and realities of actual protocol deployment within this infrastructure.

In addition to the technical deployment of the protocol, a trust model for identification and authorisation of RadSec servers is needed in a coherent and closed roaming environment like eduroam. Therefore, this document also describes the eduroam RadSec server trust model, which consists of a common trust root (eduGAINCA and other accredited CAs) and the naming conventions in certificates that these CAs must follow to allow proper authorisation determination.

# 1 Introduction

The GN2 Joint Research Activity 5 (JRA5) has been evaluating alternatives to the classic RADIUS based eduroam infrastructure since 2005. Both Diameter and RadSec were originally considered to be good alternatives, but the lack of usable implementations of the Diameter protocol led to the decision to use RadSec to enhance the RADIUS infrastructure in a simple, non-intrusive way.

JRA5 has developed several independent implementations of the RadSec protocol and is striving for standardisation in the IETF.

These implementations have grown mature enough to be considered for rollout within the eduroam infrastructure.

This deliverable gives an overview of the efforts regarding RadSec and its implementation so far. It consists of:

- 2 “Technical Background”: This provides a short technical background to the RadSec protocol, its available implementations and the state of standardisation in the IETF.
- 3 “Current Deployment Details”: This describes the deployment within eduroam, which is a special use-case of the more general RadSec specification. This section includes the trust model used in eduroam and gives a short breakdown of which NROs have already deployed RadSec, and to what extent.
- 4 “Support for RadSec in eduroam service”: This describes the support for RadSec in the eduroam services.
- 5 “Future Deployment Plans”: This provides the outlook regarding standardisation for RadSec and also gives information for NROs who wish to deploy RadSec within their infrastructure.

# 2 Technical Background

When the eduroam architecture was created in 2003, the RADIUS protocol was used to create the proxy hierarchy that routes the authentication and accounting requests in national and international roaming sessions. This decision has proven to be the correct one as the RADIUS protocol has worked well, and allowed increases in the scale of the eduroam service, with only minor shortcomings.

However, as eduroam continues to grow and increasing numbers of users rely on the stability of the service, these shortcomings become more and more important and must be addressed. Therefore, JRA5 committed significant effort into identifying these shortcomings and evaluating alternatives. This evaluation was described in DJ5.1.4 and DJ5.4.1. The overall outcome was that the RadSec extensions to RADIUS appear to be the most promising option for a future infrastructure upgrade.

JRA5 carried out field tests of the first implementation (Radiator), and initiated and funded a second implementation (radsecproxy). After experiencing promising results, especially of the advanced feature set in radsecproxy (proactive failover discovery with Status-Server packets), a third software project was started for FreeRADIUS (the RADIUS server with the largest installed base in eduroam community).

## 2.1 Standardisation Status

RadSec was originally implemented by Open System Consultants and described in their whitepaper [www.open.com.au/radiator/radsec-whitepaper.pdf]. The specification was refined by JRA5 and turned into an Internet Draft for the Internet Engineering Task Force (IETF), currently in its second revision [http://www.ietf.org/internet-drafts/draft-winter-radsec-01.txt]. This draft has been outside of the relevant IETF working group charter, and significant effort has been put into persuading the gremium to accept RadSec as a work item for standardisation. See 5.1 “Standardisation” for the future roadmap of RadSec standardisation.

# Implementation Status

Current RADIUS Server implementations are:

- Radiator: This implementation is the original, first implementation of RadSec. RadSec support has been in Radiator since 2005. The implementation is based on the manufacturer's RadSec whitepaper, which is different to the current IETF internet draft. It allows configurations for RadSec that are not in-line with the current internet draft, but can be configured to behave according to the internet draft. Until recently, it was the only implementation on the market. Because of this lack of competition, the implementation does not offer some of the optional advanced features that were introduced in the internet draft (most notably proactive failure detection with the use of Status-Server packets and reactive failure detection by examining the TCP link state). Negotiations with the manufacturer are underway to introduce the advanced features into this implementation.
- Radsecproxy: This implementation [http://software.uninett.no/radsecproxy/] was funded by JRA5 and contains a rich feature set, according to the RadSec internet draft. It is complete for most current use cases of eduroam, with two notable exceptions:
  - The support for RADIUS accounting packets is incomplete.
  - Dynamic server discovery is not yet implemented.

  These features are on the roadmap for the next production release of radsecproxy, version 1.2. radsecproxy supports both proactive and reactive failure detection.
- Lancom LCOS: Lancom Systems is a vendor of Access Points and “All-in-one” Router solutions. All devices are operated with the Lancom Operating System, LCOS. LCOS version 7.5 supports RadSec in all parts of the operating system; the client code in Access Points for 802.1X authentications as well as the server code for the built-in RADIUS server in router products. The implementation does not yet offer any of the advanced features (for example, proactive failure detection).
- FreeRADIUS: This implementation does not currently offer RadSec support, but is scheduled to provide such support by the end of 2008. The contract includes proactive and reactive failure detection, dynamic server discovery and full accounting support.

The following table contains a feature overview of the existing server implementations:

| Implementation | V. | Proactive failure detection (Status-Server) | Reactive failure detection (TCP state) | dynamic server discovery (DNS/arbitrary) | RADIUS Accounting | eduGAIN certificate validation options |
|---|---|---|---|---|---|---|
| Radiator | 4.2 | no | no | yes/no | yes | yes |
| Radsecproxy | 1.1 | yes | yes | planned/planned | yes | yes |
| FreeRADIUS | 2.0 | contracted | contracted | no/contracted | contracted | contracted |
| Lancom LCOS | 7.5 | no | no | no/no | yes | no |

# 3 Current Deployment Details

## 3.1 eduroam trust model

The RadSec deployment uses X.509 certificates instead of the traditional IP address and shared secret trust model. In order to protect the infrastructure from unauthorised sites using the eduroam authentication fabric, a two-step peer validation model is used.

### Step 1

The certificates presented by the peers when establishing a new connection need to be valid, not revoked and issued by a Certification Authority (CA) that is trusted for eduroam usage. Currently the trusted certification authorities are:

- eduGAIN CA.
- eduGAIN SCA [https://sca.edugain.org].

A policy with requirements for acceptance into this list of CAs is in progress.

### Step 2

The certificate needs to contain a subjectAltName of type URI with the correct value for identifying the peer as either an eduroam Service Provider, Identity Provider, proxy or confederation root server.

The URNs are issued within the GEANT2 branch of the URN space (urn:geant). The following base values are used:

| **Peer Type** | **URN prefix** |
|---|---|
| confederation root (TLRS) | urn:geant:eduroam:component:confederation-root: |
| FLRS | urn:geant:eduroam:component:proxy: |
| IdP | urn:geant:eduroam:component:idp: |
| SP | urn:geant:eduroam:component:sp: |

These URNs are suffixed with " Europe:" for members of the European eduroam confederation. Other confederations will receive a different suffix and can be identified by that suffix.

Validation of certificates therefore uses the following ruleset:

- Server-side RadSec check: Is URN one of sp, proxy or confederation-root?
- Client-side RadSec check: Is URN one of idp, proxy or confederation-root?

### Deployment notes

It is possible to add multiple subjectAltName:URI identifiers to a certificate. This is particularly useful, and is in fact encouraged for institutions that are both IdP and SP simultaneously.

Sample configuration snippets for Radiator and radsecproxy will be included in JRA5's Roaming Cookbook, 3rd edition [DJ5.2.3,3].

URN registrations in the branches below the branch roots above follow the convention described below:

| Peer Type | URN prefix |
|---|---|
| confederation root (ETLRS) | urn:geant:eduroam:component:confederation-root:Europe:<role><br><br>(registered by OT) |
| FLRS | urn:geant:eduroam:component:proxy:Europe:<Federation-Name>:<identifier><br><br>(registered by Federation NRO personnel) |
| IdP | urn:geant:eduroam:component:idp:Europe:<Federation-Name>:<realm name><br>(registered by Federation NRO personnel; any <realm name> includes subdomains of this realm) |
| SP | urn:geant:eduroam:component:sp:Europe:<Federation-Name>:<descriptive-name><br>(registered by Federation NRO personnel) |

## 3.2 Field deployment

The current deployment status of RadSec in the eduroam infrastructure is as follows:

- Confederation level (ETLRS):
  - etlr1.eduroam.org: fully operational, static setup (Radiator).
  - etlr2.eduroam.org: fully operational, static setup (Radiator).

- Federation level (FLRS):
  - LU: fully operational, static setup, dynamic server-side setup (Radiator, radsecproxy).
  - NL: operational toward selected institutions (Radiator).
  - CZ: operational toward selected institutions.
  - DE, CH: in trial phase.
- Institutional level:
  - CZ: current state: 11 institutions on RadSec, 50 on RADIUS over IPSec.
  - NL: several connected institutions.

Note: Currently no comprehensive, overall view is available. We expect that the majority will use FreeRADIUS and will need to wait for the appropriate implementation.

# 4 Support for RadSec in eduroam service

As explained in DS51.1 "eduroam Service Definition and Implementation Plan", the eduroam service consists of:

- Technology infrastructure: TLRS, FLRS, IdP and SP RADIUS servers, network access elements.
- Supporting infrastructure: Monitoring and diagnostics, eduroam database, eduroam web site, TTS, mailing lists.

While the deployment of RadSec in the technology infrastructure is explained in section 3 "Current Deployment Details", and future plans in section 5.2 "Deployment in eduroam", in this chapter we concentrate just on the supporting elements for RadSec in eduroam.

The monitoring system should be capable of monitoring RadSec servers using proper RadSec requests/responses.

The design of the monitoring system and the eduroam database allows the identification and status tracking of RadSec installations in the monitored infrastructure (currently ETLRSs and FLRSs).

The monitoring system is equipped with an appropriate client probe that can act as a RadSec client and provide similar test results as the ones provided for native RADIUS servers. In order to follow the established trust model explained in section 3 "Current Deployment Details", the monitoring probe has a certificate based on the following URN registration:

urn:geant:eduroam:component:confederation-root:Europe:Monitoring .

# 5 Future Deployment Plans

## 5.1 Standardisation

RadSec is currently not standardised at the relevant gremium (the IETF) but there are significant efforts underway to that end. The goal is to create a standard that ensures all implementations of RadSec interoperate easily.

So far, an Internet Draft was issued by GN2 JRA5 and the TERENA TF-Mobility that describes the existing implementations, including the advanced features that are not yet present in the Radiator implementation.

Furthermore, a discussion at the IETF was started regarding adoption of the RadSec work in the official work-plan of the RADIUS Extensions (radext) working group. This turned into a lengthy process as the radext group was not formally allowed to work on this topic (their charter explicitly forbids working on new transports and security measures in RADIUS).

However, in the 71st IETF meeting in Philadelphia there was a broad consensus that the current charter is insufficient and a re-chartering process was launched to include RadSec into the working group's charter. The rechartering process is now complete and numerous restrictions on the permitted scope of the radext working group have been lifted. As a consequence, RadSec was adopted as a future milestone for the working group.

The new charter of this working group lists the components of RadSec as milestones:

- Reliable Transport for RADIUS: TCP (Milestone: Jan 2009).
- Description of Status-Server operation for proactive failure detection (Milestone: Mar 2009).
- RadSec (TLS over TCP) (Milestone: Mar 2009).

The RadSec work item is to be turned into an Experimental Standard (EXP) document, while the TCP transport is going to be a Standards Track document. These standards are to be based on JRA5's Internet Draft. It will be progressed during the coming months and in upcoming IETF meetings.

## 5.2 Deployment in eduroam

Since the ETLR servers are already configured for RadSec in production use, here we need only look at the federation servers (FLRS) and institutional servers - that is, Identity Providers (IdP) and Service Providers (SP). Since it is possible to combine RADIUS and RadSec operation on the same server, it is not necessary to do the switch on a special “flag day” as all IdP and SP connections can be migrated to RadSec at their own pace.

### 5.2.1 Radiator-based installations

It is envisaged that all FLRS that use Radiator as server software migrate to a RadSec configuration as soon as possible. The only required prerequisite for the move is issuance of an eduGAIN CA certificate for the servers, which depends on the eduGAIN CA process. If a sufficiently new version of Radiator is used, the migration can be done without significant server software downtime by a simple configuration change. As soon as the advanced failure detection features are implemented in Radiator, they become available to the installed base in FLRS by a routine software upgrade. It is not necessary to migrate connected institutions at the same time, as Radiator can function as a RADIUS and RadSec server simultaneously. Any institution upgrades can be planned and executed at the administrator's convenience.

### 5.2.2 FreeRADIUS-based installations

Federations that use FreeRADIUS as server software will probably not migrate to RadSec before the corresponding code is available in a released version of FreeRADIUS. Before production rollout of FreeRADIUS with RadSec, extensive testing should take place on a non-production system and/or on lower layers of the infrastructure. In case a federation plans to migrate earlier, the use of radsecproxy as a conversion entity is encouraged; see 5.2.3 “Other installations”.

### 5.2.3 Other installations

Federations that are neither based on FreeRADIUS nor on Radiator can make use of radsecproxy. This software can act as a standard RADIUS client towards the existing FLRS and can itself maintain the outbound connections to the root servers.

It is also possible to replace a FLRS completely with radsecproxy. radsecproxy can mix arbitrary numbers of RADIUS and RadSec clients and servers, and broker requests between them. If a FLRS is only used for proxying RADIUS requests anyway, all functionality can be taken over by radsecproxy. Given its small memory footprint, federations are encouraged to explore this alternative.

# 6 Conclusions

RadSec has proven to be a good candidate for enhancing the existing RADIUS infrastructure within eduroam. A lot of development effort has led to new implementations, bug fixing in the existing implementation and a candidate specification for use in the general internet.

The existing field deployment of RadSec proves that the specification is operating as expected and is backward-compatible .

Its future deployment is still hindered by the lack of support in the FreeRADIUS software, since this is the implementation with the largest installed base in eduroam, but this issue is currently being addressed by JRA5.

The prospect for future implementations, standardisation and deployment appears promising. The relevant standardisation gremium Internet Engineering Task Force (IETF) is committed to advance RadSec to a ratified standard solution with the ambitious goal to publish corresponding RFC documents by March 2009. The last remaining cornerstone for large-scale field deployment, an implementation of RadSec in FreeRADIUS, has already been started and is expected to be ready for production use by the end of the year.

# 7 References


| | |
|---|---|
| [DJ5.1.4] | Inter-NREN roaming Technical Specification |
| [DJ5.2.3,3] | Best Practice Guide - AAI Cookbook - Third Edition |
| [DJ5.4.1] | Advanced Technologies Overview |
| [eduGAIN SCA] | https://sca.edugain.org |
| [Radsecproxy] | http://software.uninett.no/radsecproxy/ |
| [Whitepaper ] | www.open.com.au/radiator/radsec-whitepaper.pdf |

# 8 Acronyms

| | |
|---|---|
| CA | Certification Authority |
| ETLRS | European Top level RADIUS Server |
| FLRS | Federation Level RADIUS Server |
| IdP | Identity Provider |
| IPsec | Internet Protocol Security |
| IETF | Internet Engineering Task Force |
| JRA5 | Joint Research Activity 5 |
| LCOS | Lancom Operating System |
| NRO | National Roaming Operator |
| RADIUS | Remote Authentication Dial-In User Service |
| RadSec | RADIUS Security |
| SP | Service Provider |
| TLRS | Top level RADIUS Server |
| TTS | Trouble Ticketing System |
| URI | Uniform Resource Identifier |
| URN | Uniform Resource Name |