Achieving a trust relationship model in eduroam – the case of an RadSec pilot implementation in Portuguese Higher Education Institutions

Pedro Simões[1], António Rio-Costa[2], Fernando Reis[3], Rui Ribeiro[4], Alberto Vasconcelos[2], Elsa Justino[2]

[1]FCNN FCT, Av. do Brasil n.º 101, 1700-066 Lisboa, Portugal, psimoes@fccn.pt
[2]UNiversidade de Trás-os-Montes e Alto Douro UTAD, Quinta de Prados, 5001-801 Vila Real, Portugal, acosta@utad.pt, albertov@utad.pt, ejustino@utad.pt
[3]Instituto Politécnico de Castelo Branco IPCB, Av. Pedro Álvares Cabral, nº 12 6000-084 Castelo Branco, Portugal, fereis@ipcb.pt
[4]Instituto Universitário de Lisboa (ISCTE-IUL), Av.ª das Forças Armadas, 1649-026 Lisboa, Portugal, Rui.Ribeiro@iscte.pt

Keywords
Eduroam, security, trust, hierarchy, Radius, RadSec, mobility, DNS.

1. ABSTRACT

Eduroam or Education Roaming, is a RADIUS-based (Remote Authentication Dial In User Service) infrastructure that uses 802.1X security technology to allow for inter-institutional roaming.
Since its origin in 2002, eduroam has rapidly spread across the world and now students and researchers from over 85 countries can benefit from free, secure and reliable wifi access. Making this initiative probably the major success story for Research and Education mobility in the past few years.
Being part of eduroam, allows users visiting another member institution to log on to the WLAN using the same set of credentials (username/password) that the user would use if he were at his home institution. All this with a minimum administrative overhead.
The current RADIUS hierarchy protocol implementation of eduroam works well. However, due to the constantly growing number of users and organizations around the world, issues related to timing, security and reliability of communication started to appear. The goal of a RadSec is to handle these issues, add features and more management flexibility.
The current paper intents to describe and report of a Portuguese RadSec pilot implementation between the FCCN - a branch of FCT – the Portuguese Foundation for Science and Technology, with the aim of planning and managing the RCTS – the Science, Technology, and Society Network, UTAD – University of Trás-os-Montes and Alto Douro, IPCB- Polytechnic Institute of Castelo Branco and ISCTE-IUL University of Lisbon. Each of these institutions implemented different technological approaches in order to enable a heterogenic multi-domain RadSec infrastructure aiming to enable a good practice approach to a wither national implementation.

2. EDUROAM AND AUTHENTICATION INFRASTRUCTURE

Eduroam or Education Roaming, is a RADIUS-based infrastructure that uses 802.1X security technology to allow for inter-institutional roaming. Being part of eduroam, allows users visiting another member institution to log on to the WLAN using the same set of credentials (username/password) that the user would use if he were at his home institution. All this with a minimum administrative overhead (Belnet Eduroam.be website, 2011).
Eduroam supports over 5 million access authentications every day with over 500,000 international authentications daily. Eduroam is truly supporting the vision of a global village for Research and Education. Only in 2016, eduroam expanded with a 23% increase in international authentications and a 26% increase in national authentications. Now 86 countries now take part in eduroam around the world with Tajikistan being the latest country to join the eduroam (Figure 1) (Eduroam.org website).

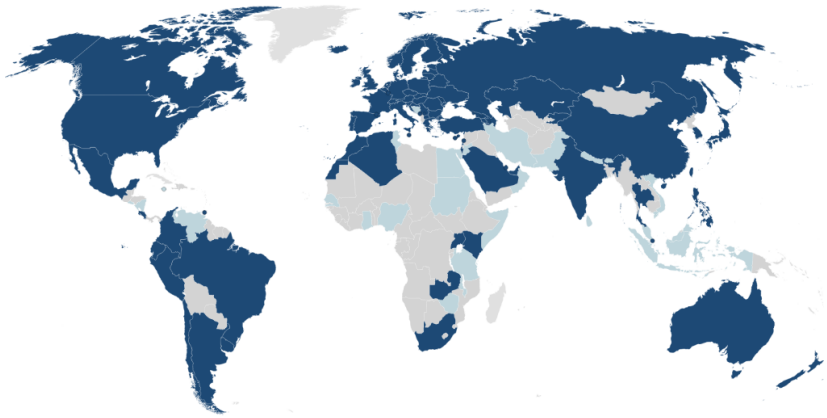

Figure 1 – Worldwide eduroam distribution (source https://eduroam.org).

In total, the eduroam Authentications systems recorded over 2.6 billion national authentications (where users from another institution in the same country authenticate their WiFi access via eduroam) and more than 592 million international authentications (Eduroam.org website).
In Portugal, eduroam is present in 61 Higher Education Institutions scattered all over the the country and also with external coverage outside of the campus environment. In some cities, public parks, libraries and museums, are also covered.
In 2006, the Portuguese eduroam network was initially designated as the e-U network. The e-U network was created under the e-U Virtual Campus initiative, a project partially funded by the Portuguese government through the Program of Action for the Knowledge Society (POSC), coordinated by the Agency For the Knowledge Society (UMIC) and developed and maintained technically by the Foundation for National Scientific Computation (FCCN). The e-U "Campus Virtual" initiative aimed to increase the online access to researchers and students also to promote the online presence of academic contents, which sought to encourage and facilitate the production, access and sharing of scientific Knowledge (Eduroam.pt website, 2015).
Also in 2006, the e-U network was the third, and long-standing, largest national university network to join the European mobility network eduroam. With the emergence of the eduroam brand at the European level, security updates and other configurations were carried out in order to fully comply with the European mobility service (Eduroam.pt website, 2015).
Eduroam is based on 802.1X and a linked hierarchy of RADIUS servers containing users' data (usernames and passwords).
Participating institutions must have operating RADIUS infrastructure and agree to the terms of use.

802.1X is an IEEE Standard for port-based Network Access Control and provides an authentication mechanism to devices wishing to attach to a LAN (local area network) or Wireless LAN.
RADIUS which stands for "Remote Authentication Dial In User Service", is a network protocol which controls user network access that serves three primary functions:

- Authenticates users or devices before allowing them access to a network;
- Authorizes those users or devices for specific network services;
- Accounts for the usage of those services.

The RADIUS protocol is generally hidden inside of the management core of the networks, and is not seen directly by end users. i.e. it is run between trusted systems in the network.
The simplicity, efficiency, and usability of the RADIUS system led to its widespread adoption by network equipment vendors, to the extent that currently, RADIUS is considered an industry standard and is also positioned to become an Internet Engineering Task Force (IETF) standard (Network Radius Website).
The RADIUS client-server protocol has advantages, some of them including (Network Radius Website):

- An open and scalable solution;
- Broad support by a large vendor base;
- Easy modification;
- Separation of security and communication processes;
- Adaptable to most security systems;
- Workable with any client device that supports the protocol;
- Very simple client implementation, usually only a few hundred lines of code;

In eduroam implementation, the RADIUS hierarchy (Figure 2) forwards users credentials securely to the users' home institutions, where they are verified and validated. To protect the privacy of the traffic from the user's device over the wireless network, the latest up-to-date data encryption standards are used. The user's home institution is responsible for maintaining and monitoring user information, even when the user is at a guest campus. Thus, this data is not shared with other connected institutions (Eduroam.org website).

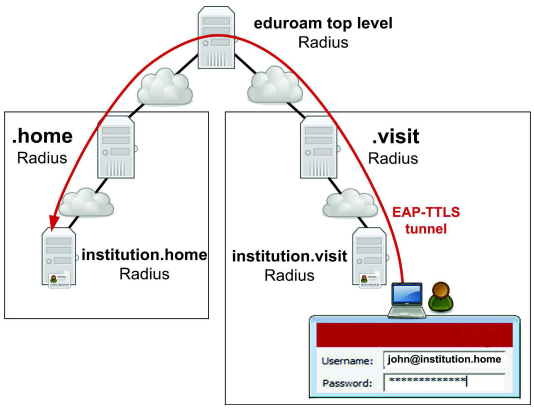

Figure 2 – 802.1X Radius architecture (source: eduroam.org).

As already stated, one of the fundamental bases of the eduroam is the high security standards that are applied and the confidentiality of the users' data. This is done using the most modern protocols of authentication and data transmission. Thus, there is a constant need to improve and maintain in a state of the art all the authentication mechanisms of the eduroam network, ensuring the best possible levels of security in the network and its use. This means that it is necessary to carry out periodic updates in the infrastructure.

The higher incidence of these updates had been centred on the mechanisms and protocols of communication between access points and users' equipment, since these are the most vulnerable points and with a lower degree of control on the entire authentication process.

Most of the authentication and authorization mechanisms currently in use on the eduroam network are based on the RADIUS protocol. This protocol has identified some limitations that may contribute to the emergence of problems in maintaining its use.

One of the biggest problems in data transmission between Radius servers is in the communication protocol used, UDP. This protocol does not use any transmission control mechanisms, which means that in authentication processes that pass through several Radius servers, packets can be lost and they are not forwarded. This loss of data impairs the authentication process, forcing it to be repeated, which generates unnecessary traffic on the network and, in certain situations, the passage of large volumes of data in the eduroam authentication structure (RadSeC WhitePaper).

Second, the data in conventional RADIUS access requests is mostly plaintext, including the user name, IP address, login times and other data. The user's password is encrypted with a shared secret, but using a fairly weak encryption algorithm. This means that eavesdroppers can gain valuable information by listening in on conventional RADIUS requests. This is not usually a problem where the RADIUS requests travel over an otherwise secure or private network, but it is a security problem when the RADIUS requests travel across the internet or any other insecure or shared network (RadSeC WhitePaper).

Furthermore, conventional RADIUS uses the unreliable User Datagram Protocol (UDP) for transport. UDP does not guarantee to deliver messages. The RADIUS protocol permits a limited number of retransmissions, but it does not guarantee the delivery of requests. Therefore, conventional RADIUS requests can sometimes be lost or dropped, especially on a congested network. This can cause inconvenience for users trying to log in, and lost accounting messages can mean lost income for operators (RadSeC WhitePaper).

Other problem that should be pinpointed is that the RADIUS protocol does not always provide a reliable indication of whether the RADIUS server where you are connected to is the one that it should be expected, or that the client that sends a request is really who it he claims to be. This means that it is relatively easy to spoof RADIUS clients and servers when using conventional UDP based RADIUS proxying. This can be used by attackers to gain valuable information about an operator's network and users.

To overcome these problems, RadSec was developed. RadSec stands for Secure RADIUS protocol. This is a protocol which implements the radius protocol on top of TLDv3 transport layer as defined in the ietf draft "draft-ietf-radext-radSec-12" and is a protocol for transmitting Radius authentication and authorization data natively based on the use of TCP and TLS.

The main advantages of the RadSec protocol are as follows (Figure 3):

- TCP - Guarantee of control mechanisms of data transmission;
- TLS - Ensuring inter-server communication security;

- The use of these two methods gives Radius more reliable transport mechanisms with data transmission control while adding to this process an additional layer of data transmission security between Radius servers.

The TCP protocol guarantees the existence of control mechanisms in the data transmitted between the different servers of Radius involved in an authentication process and in case of failure to deliver a package to a certain server, it is resent, avoiding the repetition of the whole process of authentication.
The use of TLS and server certificates, based on a single authorized CA, ensures authenticity and security in the communication process between RADIUS servers.
In RadSec the introduction of TLS also allows direct communication between Radius servers through the use of Domain Name System (DNS) mechanisms, guaranteeing an optimization of the entire authentication process.
The process of discovering the authentication servers relies on DNS mechanisms that provide, via SRV registers, the name/IP of their server.
RadSec as an hierarchical model provides a good trust relationship between each participant. With RadSec you need to transmit digital certificates between RADIUS servers. Also, the digital certificates need to be conform with a certificate policy.

Radius UDP implementation RadSec TCP and TLS implementation

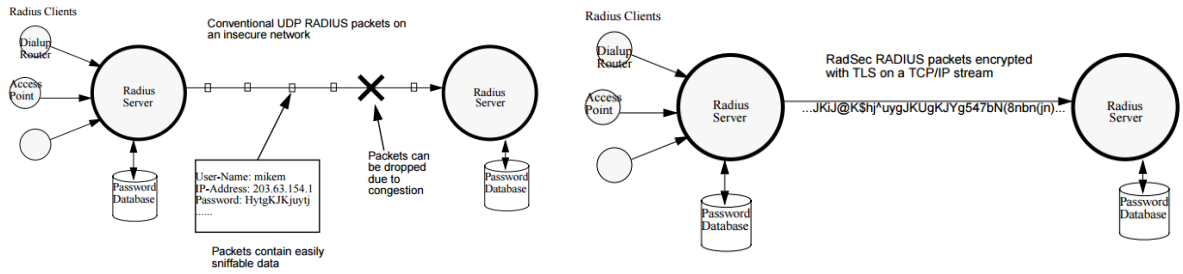

Figure 3 – Radius Vs RadSec security (source RadSec White paper)

3. THE INVOLVED INSTITUTIONS

FCCN is a branch of FCT – the Foundation for Science and Technology, with the aim of planning and managing the RCTS – the Science, Technology, and Society Network (FCCN Website), a digital research infrastructure covering all areas of knowledge, offering national education and research institutions a set of advanced digital services that allows them to work on national projects and also to integrate with or access international research projects and resources.
This ability to access international content is provided through the European network GÉANT, which interconnects with and provides advanced digital services to the European networks for national education and research, of which the FCCN is a National member.
The role of FCCN in the eduroam infrastructure is to operate a Federation Level RADIUS (FLR). It manages and maintain the national radius proxy infrastructure, being a peering point

between the different Portuguese eduroam institutions and also provide an uplink from the federation to all other eduroam federations.
On the traditional Radius model these Federation Level RADIUS servers receives the authentication and accounting request from the different roaming users, forwarding them to the home institutions, and also manages the answers from that servers.

At the University of Trás-os-Montes and Alto Douro (UTAD Website), the 802.1X/eduroam infrastructure is based on Cisco APs (220 aprox.) and Meru Access Points (50 aprox.). The authentication service is provided by an open-source FreeRADIUS implementation, with dynamic Vlan assignment, is connected to a central LDAP server for the authentication processes, and using MySQL and Mongo DB for accountability proposes.

At ISCTE-IUL (ISCTE-UIL Website)University, the 802.1X/eduroam infrastructure is based on 225 Meru/Fortinet Access Points, working in with 802.11n on the 2.4GHz band and 802.11ac on the 5GHz band. The models used are mainly the AP1020 and AP832i.
The authentication service is provided by a in-house customised open-source FreeRadius since 2013.
The current FreeRADIUS implementation is:

- a 3.0.x version in a Debian 8 server active master, and a 3.1.x version a Debian 9 stand-by slave;
- connected to the Active Directory services for authentication and user VLAN selection;
- supporting the PEAP-MSCHAPv2 and EAP-TTLS-MSCHAPv2 for client authentication;
- using a MySQL DB for authentication logging and accounting purposes;
- monitored by the NAGIOS platform;
- directly connected to the PT eduroam federation since 2005;
- sending statistics/logs for the PT federation.

The IPCB (IPCB Website) is a public higher education institution with administrative, scientific and pedagogical autonomy. Its mission is to give citizens a high standard of qualification, the production and dissemination of knowledge, as well as the cultural, artistic, technological and scientific teaching of its students in an international frame of reference.
The 802.1X/eduroam infrastructure in IPCB is composed of 125 Extreme Networks (formerly Enterasys Networks) access points connected to two virtualized wireless controllers making that in the radius server point of view appears only one access point. For authentication and authorization and accounting IPCB uses Radiator (https://www.open.com.au/radiator/) service and user credentials are provided by a central OpenLDAP Server.

4. THE PILOT IMPLEMENTATION

Taking into concern the demonstrated issues related to security, efficiency and manageability that the implementation of RadSec can drive from the success of eduroam, the Portuguese NREN jointly with 3 Higher Education institutions (UTAD; IPCB and ISCTE), started a pilot project aiming to implement RadSec in the eduroam authentication infrastructure.
All of these institutions have different infrastructures and RADIUS authentication methodologies or roles in the national RADIUS federation.

On the new RadSec model, the Federation Level RADIUS servers will act only as a backup connection to the different institutional eduroam radius servers. The communication between these servers will still be made using RadSec.
If the destination institution is still in the traditional Radius model, then the Federation Level RADIUS servers will communicate using the old protocol, acting as a dual stack server. It can also act as a RadSec endpoint if any institution don't want to use RadSec, using just the DNS dynamic discovery.
The implemented pilot, also permitted a seamless evolution to RadSec without any disruption to users in manner that the original radius implementation stayed as backup and redundancy.

Figure 4 shows the evolution made for the RadSec Proxy implementation in the institutions.

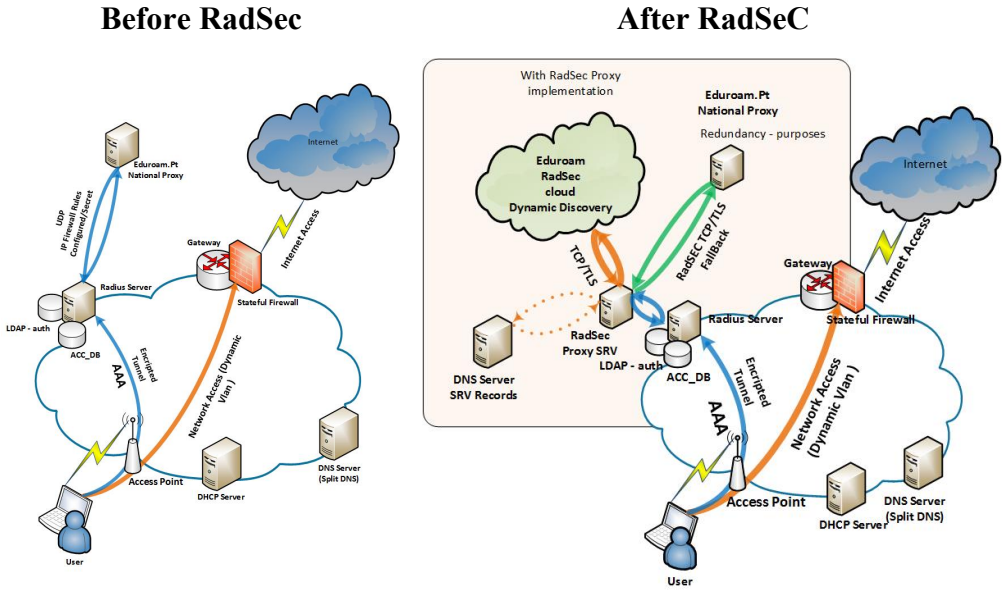

Figure 4 – RadSec Pilot – Before and After

UTAD RadSec Proxy configuration examples:

Initial Scenario

- Ubuntu 14.04.5 LTS
- Freeradius 3.0.10+git
- Firewall accept TCP port 2083

DNS SRV configuration example

zone utad.pt
IN NAPTR 100 10 "s" "x-eduroam:radius.tls" "" _radsec._tcp.utad.pt._radsec._tcp.utad.pt.
IN SRV 0 0 2083 radius.utad.pt.

/etc/radsecproxy.conf file

#External requests over TLS
ListenTLS <proxy Public IP >:2083

```
#Local requests Radius (dual stack)
ListenUDP               127.0.0.1:1830
```

```
#redirections for local Radius l
SourceUDP               127.0.0.1:33000
#redirections for outside
SourceTLS               < proxy Public IP >:33001
LoopPrevention          on

tls default {
        CACertificateFile       eduPKICAG01.crt
        CertificateFile         cert-server.pem
        CertificateKeyFile      key-server.pem
        }

#  Remove Vlan's attributes
rewrite defaultclient {
      removeAttribute    64
      removeAttribute    65
      removeAttribute    81
         }

#Clients Configurations

#Accept via outsider radsec (Dynamic Discovery)
client any {
      type tls
      host 0.0.0.0/0
      certificatenamecheck on
}

#Configuração dos servidores

#Freeradius local (auth)
server  act-local {
      host 127.0.0.1
      port 1812
      type udp
      secret XXXXXXXXX
}

#Freeradius local (accounting)
server  acc-local {
      host 127.0.0.1
      port 1813
      type udp
      secret XXXXXXX
}
```

```
#From outside to  @utad.pt  freeradius
realm utad.pt {
        server act-local
        accountingServer acc-local
}

# Server dynamic
server dynamic {
        type tls
        secret radsec
        dynamicLookupCommand /usr/share/doc/radsecproxy/examples/naptr-eduroam.sh
}

#From inside to outside dynamic RadSec redirection

realm * {
        server dynamic
}
```

File /etc/freeradius/proxy.conf

```
(…..)
#From outside for  local proxy
home_server EDUROAM_Radsec {
        type    = auth+acct
        ipaddr  = 127.0.0.1
        port    = 1830
        secret  = XXXXXXX
}

home_server_pool EDUROAM_RadSec_POOL {
        home_server = EDUROAM_Radsec
}

realm TO_EDUROAM_RadSec {
        pool = EDUROAM_RadSec_POOL
        nostrip
}
```

Debug exemple

root@radius:~# tail -f /var/log/radsecproxy.log

```
Mar 16 16:47:11 2017: createlistener: listening for udp on 127.0.0.1:1830
Mar 16 16:47:11 2017: createlistener: listening for tls on 193.136.40.148:2083
(…)
Mar 16 16:49:36 2017: connecttcphostlist: trying to open TCP connection to radius01.fccn.pt
port 2083
Mar 16 16:49:36 2017: connecttcphostlist: TCP connection to radius01.fccn.pt port 2083 up
Mar 16 16:49:36 2017: verifyconfcert: certificate name check ok
Mar 16 16:49:36 2017: tlsconnect: TLS connection to dynamic_radsec.id.fccn.pt up
```

Mar 16 16:49:36 2017: Access-Accept for user teste@id.fccn.pt stationid 02-00-00-00-00-01 from dynamic_radsec.id.fccn.pt to 127.0.0.1 (127.0.0.1)
Mar 16 16:49:36 2017: replyh: passing Access-Accept to client 127.0.0.1 (127.0.0.1)

5. CONCLUSIONS AND FUTURE WORK

The pilot implementation in the involved institutions was successful regarding the objectives that where initially aimed. The pilot als implementation brought an extra level of security and redundancy to the institutions.
Accomplishing the RadSec implementation lead to the awareness that not only the technology upgrade is needed but security and manageability must thrive in the concerns of the IT staff and in the Administrations of the Institutions.
Also, DNS is a crucial component to the RadSec implementation and security concerns should be applied into the future of the pilot implementation.
The final goal of the pilot aims to create a best practice implementation ensuring that the technological knowledge can be shared with all of the institutions that want to have RadSec in eduroam.

Note: The implementation of RaSec at UTAD was founded was part of one of the objectives of the Project "SMS@UTAD - Information Security and Information Management Systems" co-financed by the European Regional Development Fund (ERDF) through COMPETE 2020 - Competitiveness and Internationalization Operational Program (POCI).

6. REFERENCES

Eduroam.be website (2011). Belnet Eduroam Service -What is eduroam?. Retrieved march 16, 2017, from: https://www.eduroam.be/node/1.

Eduroam.org Website. Eduroam continues to grow in 2016. Retrieved march 16, 2017, from: https://www.eduroam.org/2017/03/07/2016-a-record-breaking-year-for-eduroam/.

Eduroam.pt Website (2015). Sobre o eduroam. Retrieved march 16, 2017, from: https://eduroam.pt/pt/sobre/descricao.

RadSeC White Paper (2012), *RadSec a secure, reliable RADIUS Protocol*, Copyright (C) 2012 Open System Consultants Pty. Ltd. Retrieved march 15, from: http://www.open.com.au/radiator/radsec-whitepaper.pdf.

Network Radius Website. FreeRADIUS Documentation. Retrieved march 16, 2017, from: http://networkradius.com.

Radiator Website. Radiator, Retrieved march, 17, 2017, from: https://www.open.com.au/radiator/

FCCN Website. FCCN- Unidade da FCT – Fundação para a Ciência e a Tecnologia, Retrieved march, 17, 2017, from: https://www.fccn.pt.

UTAD Website, UTAD - Universidade de Trás-os-Montes e Alto Douro, Retrieved march, 17, 2017, from: http://www.utad.pt.

ISCTE-IUL Website. ISCTE-IUL - Instituto Universitário de Lisboa, Retrieved march, 17, 2017, from: https://www.iscte-iul.pt/.

IPCB Website. IPCB - Instituto Politécnico de Castelo Branco, Retrieved march, 17, 2017, from: http://www.ipcb.pt/.

7. AUTHORS' BIOGRAPHIES

Pedro Simões -Working in FCCN for more than 15 years, I have been connected to the eduroam project for since 2006. In these years, I have managing and maintained the Federation Level RADIUS servers and helped the Portuguese institutions on several levels, from the access points to the Radius software. I have also been involved in the different processes of the actualization and upgrade of the eduroam network to the different technologies.

António Costa - ICT specialist at (UTAD), Vila Real, Portugal, and is responsible for the coordination the areas of core infrastructure and communications, computer security areas, data center, VoIP and communications networks. He collaborates in teaching on different degrees of Computer Courses, as well as in research, extension and development projects. Holds a degree in Electrical Engineering (specialization in Electronics, Instrumentation and Computation) and a post-graduate degree in engineering area. Currently, he is in the final research stage to complete the PhD in Computer Sciences. He made several made courses or specializations which includes the Upper Course Director for Public Administration; Diploma of specialization of the Information Society for Public Administration, SIP Masterclasses and a OpenStack specialization. Further information is available at www.linkedin.com/in/ariocosta.

Fernando Reis – Has a Post-Graduation in Software Development and Interactive Systems (2010 2011) by Instituto Politécnico de Castelo Branco (ISCED 6), Engineer (5 years degree) in Information Technologies and Multimedia (1997-2002) by Instituto Politécnico de Castelo Branco (ISCED 5). From 2004 to present IT Manager at Instituto Politécnico de Castelo Branco. From September 2011 to February 2012 Invited teacher in Escola Superior de Tecnologia de Castelo Branco (School of

Engineering) lecturing Programming Languages III at Computer Science Engineering Degree. From April 2006 to March 2007 Information systems consultant at Hospital Amato Lusitano.
https://www.linkedin.com/in/fereis/

Rui Ribeiro - Senior network/Linux/security integrator/consultant working for ISCTE-IUL with more than 20 years of experience, 8 of which in the Education IT services field and an Internet Service Provider services background. He has International experience of more than 6 years in Africa, and was an Eramus student in the UK.
His specialties are Unix architecture/network/IP services/Cisco technology coupled with associated support services/automation and monitoring with a heavy use of open source software, and a strong inclination to mix network concepts with open source-based Unix technology.
His linked.in is https://pt.linkedin.com/pub/rui-ribeiro/16/ab8/434/

Alberto Vasconcelos - Senior network/Linux/security integrator/consultant working in UTAD with more than 14 years of experience. His specialties are Linux architectures/server security/database admin coupled with associated support services/automation and monitoring with a heavy use of open source software, and a strong inclination to mix network concepts with open source-based Unix technology.

Elsa Justino – Currently she is the Administrator of UTAD and of the SASUTAD under the system of accumulation of Functions. In the scope of higher education was also, Representative of the Associations of Students the National Council for Social Action in Higher Education (1994-1996), President of Portuguese Commission for the realization of the Eurostudent Report (on the Socioeconomic status of students in Europe) and representative of the Ministry of Science, Technology and Higher Education in the Education Committee with the European Commission Socrates). He has regularly participated in several studies on students, social work Higher education and scientific articles.