20 May 2021

European eduroam Technical Service Definition

Version 3.0

Table of Contents

0 Executive Summary

eduroam is a secure international roaming service for users affiliated with the academic, research and education communities around the planet. eduroam is governed by the Global eduroam Governance Committee. The European eduroam Confederation is a subset of this global community in Europe and consists of a set of Identity Providers (enabling the aforementioned user communities to access eduroam) and Service Providers (making available Wi-Fi infrastructure for these communities). Identity Providers and Service providers are grouped together by Roaming Operators according to their geographical position in Europe. The European eduroam Confederation is based on a set of defined organisational and technical requirements that each member of the Confederation must agree to (by signing and following the eduroam policy declaration). [1]

The European eduroam service is managed by the eduroam Steering Group (SG). The eduroam Operations Team (OT) carries out the day-to-day operations of eduroam, and runs the European eduroam Confederation service.

This document describes the technical architecture and requirements for Roaming Operators, Identity Providers and Service Providers that are part of the European eduroam Confederation.

[1] European eduroam Confederation Policy Declaration, ver. 2.0 (May 2012).

1 Introduction

eduroam (EDUcation ROAMing) allows users from participating academic, research and education institutions (“eduroam Identity Provider”, IdP) secure Internet access at any eduroam-enabled Wi-Fi hotspot (“eduroam Service Provider”, SP). The architecture that enables this is based on a number of technologies and agreements, which together provide the eduroam user experience: “open your device and be online”.

The basic principle underpinning the security of eduroam is that the authentication of a user is carried out at his/her IdP using the institution’s specific authentication method. The authorisation for local network resource use is defined by the eduroam SP.

The European eduroam service provides the necessary roaming infrastructure as a confederated service, built in a peer-to-peer manner where possible. Roaming Operators connect their IdPs and SPs internally with a structure of their preference, and provide endpoints for outbound and inbound roaming authentications towards the other Roaming Operators. Destinations of a roaming authentication request from one RO’s SP to another RO’s IdP are determined by looking up DNS records of the IdP in question. The central core roaming infrastructure is limited to a PKI which provides certificates to accredited Roaming Operator endpoints, and last-resort servers for IdPs which can not set up the required DNS records.

The protocol used for the authentications of a user is RADIUS. Inside an RO, any RADIUS transport can be used; for RO-to-RO authentication transactions, RADIUS over TLS is used. Typically, IdPs deploy local RADIUS server infrastructure that is connected to a local user database; the RADIUS server is either discoverable and reachable via RADIUS/TLS or is connected to the RO’s RADIUS server. Alternatively, IdPs can make use of various cloud solutions provided by eduroam OT or their RO.

Because users have usernames in the format “user@realm” (where realm is the institution’s DNS domain name, often in the form of institution.TLD, where TLD is the country code), the RADIUS servers can use this information and the DNS responses to route the request to the IdP’s RO and, ultimately, the IdP itself. The last-resort servers operated by eduroam OT can dispatch realms ending in a ccTLD with a static routing table at scale, for one RO per ccTLD. Last-resort routing of realms in generic top-level-domains (gTLD) (for example, geant.org) or ROs that can not be associated to a ccTLD require careful negotiation between RO and the eduroam-OT and MUST be requested only as a rare exception via the eduroam OT.

Access points or switches use the WPA2-Enterprise / WPA3-Enterprise / WPA3-Enterprise with 192-Bit Security / IEEE 802.1X standards that enable the use of the Extensible Authentication Protocol (EAP). Using the appropriate EAP method, either a secure tunnel is established (through which the actual authentication information - username/password, etc. - is carried) from the user’s computer to his/her IdP (EAP-TTLS, PEAP, EAP-TEAP), or mutual authentication by public X.509 certificates is used (EAP-TLS), or zero-knowledge proof algorithms are carried out (EAP-EKE, EAP-pwd). All of those EAP methods have in common that a users' private credentials are not subject to eavesdropping by intermediate parties. Other EAP methods may be designed in the future and they may depend on security mechanisms other than TLS exchange. Those methods may be used as long as they provide effective protection against eavesdropping for critical user data (such as passwords).

The architecture, technical elements, requirements, technology profiles, and trust establishment are described in more detail in the following sections.

2 Infrastructure Description

This section describes the infrastructure elements of the European eduroam service. This includes the technology infrastructure and supporting elements (for example, monitoring and diagnostic facilities, central data repository, eduroam website and the trouble ticketing system).

2.1 Protocols and Participants

The confederation infrastructure relies on a distributed set of RADIUS servers. There are various transport protocols to carry RADIUS payloads. As of May 2021, the following protocols exist: RADIUS/UDP, RADIUS/TCP, RADIUS/DTLS and RADIUS/TLS.

eduroam supports end-to-end connections over any combination of RADIUS transports, but requires the use of RADIUS/TLS for legs of communication that leave any one RO. Routing of RADIUS messages is based on DNS service discovery, with a last-resort uplink for RADIUS realms which are not in DNS.

The routing models and infrastructure elements are described in more detail in the following sections.

2.1.1 Routing Model

eduroam Identity Providers (IdP) announce their responsible RADIUS server over DNS. The DNS record points either directly to an endpoint at the IdP, or to a RO-operated server that accepts the request on behalf of the IdP and forwards the request to the IdP. This forwarding inside the RO is the default case, as it spares the IdP from deploying a rather high-complexity RADIUS/TLS endpoint and retains visibility of authentication transactions for the RO. At its discretion, the RO may also add legacy IdPs that are not able to announce their presence in DNS to a static routing table inside the RO.

eduroam Service Providers (SPs) which need to authenticate a user look up the appropriate RADIUS server by querying the Domain Name System (DNS) for a special eduroam server record. SPs may also send their requests to a dedicated RO-operated server that performs the lookup for them. This forwarding on behalf is the default case, as it spares the SP from deploying a rather high-complexity RADIUS/TLS endpoint and retains visibility of authentication transactions for the RO.

Even eduroam SPs that do deploy RADIUS/TLS endpoints and perform their own dynamic discovery always need to have a last-resort route to their RO's servers configured as a "default" fallback routing mechanism, because there are still legacy eduroam IdPs that do not announce their presence in DNS. So, the default route needs to be available should DNS not yield the routing information.

2.1.2 eduroam top level RADIUS Servers (ETLR)

There are several geographically and administratively distributed eduroam top level RADIUS servers (etlr) within the European Confederation, interconnecting with RO servers across the globe. The purpose of these servers is to provide legacy routing based on static routing tables: These servers have a routing table mapping ccTLDs to one RO each, and also maintain exception rules for domains whose federation membership is not immediately identifiable in the realm (typically gTLD realms such as '.edu', '.eu', '.net', etc.). Finally, a realm-lookup is done in DNS for last resort routing.

The servers accept requests for the ccTLDs they are responsible for, subsequently forward them to the associated RO, and finally transport the response (i.e. result of the authentication request) back. Requests for ccTLDs that the servers are not responsible for are forwarded to other last-resort servers of other world regions.

2.1.3 Roaming Operator RADIUS Servers (ROS)

A Roaming Operator RADIUS server has a list of connected eduroam IdP servers and their associated realms, as well as the connected eduroam Service Providers within the RO. It performs DNS lookups for outbound authentication requests, accepts incoming authentication requests over RADIUS/TLS, and is connected to the ETLR as a last resort.

The purpose of the ROS is to receive requests from the ETLR, other ROS and eduroam SPs performing a direct dynamic lookup, and forward these requests to the responsible eduroam IdP (either inside their RO, or by performing DNS lookups for dynamic request routing, or by sending to the ETLR).

2.1.4 eduroam Identity Providers (IdPs)

An eduroam IdP’s RADIUS server is responsible for authenticating its own users at arbitrary eduroam SPs, including its own local Wi-Fi deployment, by checking the credentials against a local Identity Management System. The Identity Management System contains information on end users (for example, usernames and passwords). It must be kept up-to-date by the eduroam Identity Provider.

Note that the eduroam Identity Provider's RADIUS server has the most complex task of all. Whereas the other RADIUS servers merely proxy requests, the Identity Provider's server also needs to actually authenticate users, and therefore, needs to be able to terminate EAP requests and perform identity management system lookups.

eduroam Identity Providers can alternatively make use of various cloud solutions. They then do not have local RADIUS infrastructure, but remain responsible for their user base; they need to keep the cloud solution’s remote user database as up-to-date as they would a local one.

2.1.5 eduroam Service Providers (SPs)

An eduroam Service Provider (SP) is responsible for forwarding requests from users visiting this SP to the responsible eduroam IdP, either by forwarding the request to their RO, or by discovering the responsible IdP server with DNS. Upon proper authentication of a user, the eduroam SP may assign a VLAN to the user.

Small SPs that do not require VLAN assignment do not necessarily need their own RADIUS server, and can instead connect their network access elements (see below) directly to their RO infrastructure.

In most cases, an educational institution participating in eduroam acts as an IdP and SP at the same time.

2.1.6 Network Access Elements

eduroam is not dependent on access technologies. Users of eduroam can access the service, either by IEEE 802.11 Wi-Fi, IEE 802.3 wired connection, or any other compatible future access medium.

However, the active network equipment required for each method is different. For a IEEE 802.11 Wi-Fi infrastructure, access points are needed, while for a IEEE 802.3 wired infrastructure, managed switches are required.

In both cases, specific supplicant software is required on the user’s machine.

The elements mentioned above are described below.

2.1.6.1 *Supplicants*

A supplicant is software on an end-user's computing device that uses the IEEE 802.1X protocol to send authentication information, using the EAP protocol. Supplicants are often built into the operating system, but can also be a separate program.

In order to use the eduroam service and access the network, the supplicant software on users' devices must be appropriately configured. This configuration is valid throughout the eduroam confederation.

2.1.6.2 *Access Medium IEEE 802.11 - Wi-Fi Access Points*

Access points need to be capable of WPA-Enterprise (WPA2/AES as a minimum). They must also be able to forward access requests coming from a supplicant to the SP or RO RADIUS server, to allow network access upon proper authentication. Access points may also optionally assign users onto specific VLANs based on information received from the RADIUS server. Furthermore, access points exchange keying material (initialisation vectors, public and session keys, and so on) with client systems to prevent session hijacking and to ensure encryption of user payload data on the wireless medium.

2.1.6.3 *Access Medium IEEE 802.3 - Managed Switches*

Wired infrastructures can be configured to provision IEEE 802.1X (and therefore eduroam). This means that eduroam users can access the network through wired technology, but in order to do this, the switches that are used to connect end users’ computers need to be IEEE 802.1X capable and enabled on the ports used for eduroam access.

These switches need to be able to forward access requests coming from a supplicant to the SP or RO RADIUS server, to grant network access upon proper authentication and optionally to assign users to specific VLANs based on information received from the RADIUS server.

2.2 RADIUS Attribute Monitoring

As described above, VLAN assignment is typically done locally inside the SP infrastructure.

The existence of VLAN assignment attributes in authentication responses at any other point in the forwarding chain is almost always a sign of a misconfiguration on the sending (IdP) side. It can be the source of hard to trace problems at the SP side, and ultimately lead to a complete denial of service (a service malfunction) to the affected end user.

However, it cannot be completely ruled out that a given pair of IdP and SP have an agreement about common VLAN tags. This makes it imperative that VLAN attributes are not filtered automatically on any level of the infrastructure.

To minimise possible malfunctions due to VLAN attributes, the OT monitors packets en route for the existence of VLAN tagging attributes, namely:

- Tunnel-Type.
- Tunnel-Medium-Type.
- Tunnel-Private-Group-ID.

The OT notifies the RO from where these packets originate. ROs are encouraged to do the same, and to investigate whether the sender is sending these attributes inadvertently or not, and then take appropriate action.

2.3 Confederation Member Requirements

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" used in this chapter are to be interpreted as described in RFC 2119.

Each RO joining the eduroam service MUST establish the necessary infrastructure for eduroam, and ensure that it is maintained according to the eduroam service requirements and best practices.

2.3.1 eduroam Security Requirements

The basic security principle that governs the eduroam infrastructure is:

The security of the user credentials MUST be preserved when travelling through the infrastructure, and all partners providing the service MUST observe privacy regulations.

All eduroam participants (OT, Roaming Operators, Identity Providers, Service Providers) MUST:

- Always provide trustworthy and secure transport of all private authentication credentials (i.e. passwords) that are traversing the eduroam infrastructure.
- Ensure that user credentials stay securely encrypted end-to-end between the user's personal device and the identity provider when traversing the eduroam infrastructure. See Appendix A for further details.
- Ensure that eduroam servers and services are maintained according to the specified best practices for server build, configuration and security, with the purpose of maintaining a generally high level of security, and thereby trust in the eduroam Confederation.

An additional task for Roaming Operators is to ensure that the participating institutions are fully aware of their responsibility to establish an appropriate level of security.

The OT guarantees that the necessary infrastructure to run the eduroam service is operational and maintained according to server build, configuration and security best practices. The OT also ensures that it will start resolving reported incidents no later than two (2) working hours after the incident has been discovered. All such incidents will be logged, aggregated and presented to the eduroam steering group.

2.4 Technical Requirements for Confederation Members

All the components in eduroam need to have, or provision, access to the Internet. Therefore, in general, the equipment needs to provide all the functionalities for standard Internet access (for example, an IP stack, optional VLANs, etc.). In addition to the general networking requirements, eduroam makes use of a number of protocols for user authentication and service provisioning. These authentication-specific and service-specific requirements are listed below. Details regarding the extent of usage of these specifications are also given.

2.4.1 Specifications and Operational Requirements: Roaming Operator Level

Adherence to the following specifications is REQUIRED:

- AAA Servers:

RADIUS datagram processing to and from the ETLRS, as per RFC 2865 or any other of the recommended transports
. RADIUS/TLS).
server MUST be able to proxy RADIUS datagrams to other servers based on contents of the User-Name attribute.

RFC 3580 (EAP over RADIUS).
server MUST proxy EAP-Message attributes unmodified, in the same order as it received them, towards the appropriate
tination.

F-Ticks [F-Ticks].

The server MUST generate F-Ticks and send them to the monitoring infrastructure. If dynamic RADIUS routing is in

use by an SP, the NRO SHOULD make sure that the SP sends F-Ticks statistics via the NRO or directly to eduroam
(see Section 2.1.1.2).

The server MUST be set up to allow monitoring requests from the monitoring service.

All relevant logs MUST be created with synchronisation to a reliable time source (GPS or in its absence NTP/SNTP).

The server(s) MUST respond to ICMP/ICMPv6 Echo Requests sent by the confederation infrastructure and
federation monitoring service.

- Web server:

NRO MUST set-up a web server in order to publish information about the eduroam service. The address of that server
OULD be www.eduroam.<tld>.

An NRO’s web server MUST provide data in XML format, based on the specification defined by the SG, and available at http://monitor.eduroam.org/database.

Adherence to the following specifications is RECOMMENDED:

- AAA Servers:
  - RFC 2866 (RADIUS Accounting).
    The server SHOULD be able to receive RADIUS Accounting packets if a service provider opts to send that data.
    If RADIUS Accounting is supported, RADIUS Accounting packets with a destination outside the federation MUST NOT be forwarded outside the federation, and MUST be acknowledged by the FLRS.
  - A RADIUS/TLS endpoint open for connections from all other eduroam participants to enable the receiving end of RADIUS/TLS dynamic discovery.
  - A DNS-based discovery module for outgoing RADIUS/TLS dynamic discovery.
  - Servers SHOULD be highly available, for example, by deploying multiple separate servers in a failover configuration in different IP subnets on different physical locations.
  - Logs of all authentication requests and responses SHOULD be kept. The minimum log retention time is six months, unless national regulations require otherwise. The information in the requests and responses SHOULD as a minimum include:
    - The time the authentication request was exchanged.
    - The value of the User-Name attribute in the request ('outer EAP-identity').
    - The value of the Calling-Station-Id attribute in authentication requests.
    - The result of the authentication.

        - The value of Chargeable-User-Identity (if present in Access-Accept message).

2.4.2 Specifications and Operational Requirements: Identity Providers

Adherence to the following specifications is REQUIRED:

- AAA Servers:
    - RADIUS datagram processing as per RFC 2865 or any other of the recommended transports (e.g. RADIUS/TLS). The server MUST be configured to receive authentication traffic from its FLRS and send appropriate replies.
    - EAP server endpoint as per RFC 3580.
    - A well-managed identity management backend system.
    - All relevant logs MUST be created with synchronisation to a reliable time source (GPS or in its absence NTP/SNTP).
    - At least one EAP type, which is capable of mutual authentication and capable of generation of keying material for use with IEEE 802.1X in accordance with Section 3.16 of RFC 3580 (IEEE 802.1X RADIUS Usage Guidelines).
    - The outer EAP identities (and with it, RADIUS User-Name attributes) for the IdP MUST be in the format of arbitrary@realm, The realm component MUST be a domain name in the global DNS (without the trailing . sign) that the identity provider administers, either directly or by delegation. The part to the left of the @ sign is arbitrary; in particular, anonymity support is possible and encouraged.
    - The server-side EAP credentials MUST be communicated to the user base, and end-user documentation needs to be precise enough to allow users the unique identification of their EAP server.
    - The appearance of the Operator-Name attribute (RFC 5580) in Access-Requests MUST NOT cause these requests to be treated as invalid.
    - Logs of all authentication requests and responses MUST be kept. The minimum log retention time is six months, unless national regulations require otherwise. For a rationale and further considerations, please refer to Appendix B. The information in the requests and responses MUST, as a minimum, include:
        - The time the authentication request was exchanged.
        - The value of the User-Name attribute in the request ('outer EAP-identity').
        - The value of the Calling-Station-Id attribute in authentication requests.
        - If tunnelled EAP types are used, the actual user name in the request ('inner EAP-identity').
        - If the IdP opts to generate a Chargeable-User-Identity, the value of this attribute.
        - The result of the authentication.

- Every IdP MUST provide sufficient configuration instructions for their end users so that a unique identification of the IdP is possible for the end user at all times.
- These configuration instructions SHOULD be conveyed to their end user devices with onboarding tools that automate the installation and reduce the mental load for end users.
- IdPs MAY use the corresponding tooling provided by eduroam Operations Team for this purpose (eduroam CAT).

Note: the list of supported EAP types as configured by the IdP in Section 6.3.2, and the list of supported EAP types in the supplicant software in Section 6.3.4 MAY have an empty intersection. In such cases, the combination of end-user device and IdP configuration will leave the user without service. To minimise the probability of this, eduroam IdPs are encouraged to configure as many EAP types as they can possibly support, and to announce the full list of supported EAP types to their end users.

Adherence to the following specifications is RECOMMENDED:

- AAA Servers:

- Generation of a Chargeable-User-Identity (RFC 4372) response if solicited by a Service Provider and on the condition that the Service Provider's Access-Request contains a non-empty Operator-Name attribute. The value of Chargeable-User-Identity attribute returned in the response MUST have a constant value for one user and one Operator-Name attribute value. The value of Chargeable-User-Identity attribute MUST be generated in a way which ensures that the matching of this value to the actual user identity is possible only at the Identity Provider.

2.4.3 Specifications and Operational Requirements: Service Providers

Adherence to the following specifications is REQUIRED:

- Network Access Servers (NAS):
    - Construction and processing of RADIUS datagrams as per RFC 2865 or any other of the recommended transports.
      The NAS MUST send its RADIUS datagrams either to the SPs local RADIUS server or, in its absence, to the federation's FLRS.
      The generated RADIUS datagrams MUST include the attribute Calling-Station-Id, and the attribute value MUST contain at least the MAC address of the connecting end-user device.
    - RFC 3580 (EAP over RADIUS).
    - IEEE 802.1X.
    - All relevant logs MUST be created with synchronisation to a reliable time source (GPS or in its absence NTP/SNTP).
    - Wi-Fi Access Points MUST support WPA2/AES. Wireless NASes provisioned after 2021 MUST additionally support WPA3/AES Transition Mode.
    - For participating organisations which are both IdP and SP, Wi-Fi Access Points MUST deploy the SSID "eduroam" and MUST broadcast the SSID "eduroam", unless there is more than one eduroam SP at the same physical location and the signal overlap would create operational problems. In this case, by preference usage of Wi-Fi Certified Passpoint with RCOI <eduroam> and an appropriate home domain is RECOMMENDED, otherwise an SSID starting with "eduroam-" MAY be used.
    - For SP-only organizations it is recommended to also use the SSID eduroam; as an alternative, Wi-Fi Certified Passpoint with RCOI <eduroam> can be configured instead. This deployment mode offers a service for only a subset of eduroam users though.
- local AAA Servers (in its absence, NAS or the FLRS):
    - Authentication requests MUST be forwarded towards the responsible eduroam Identity Provider via the eduroam infrastructure.
    - The server MUST proxy EAP-Message attributes unmodified in the same order as it received them towards the appropriate destination.
    - Sufficient logging information MUST be kept to be able to correlate between a client’s layer 2 (MAC) address and the layer 3 (IP) address that was issued after login if public addresses are used. This requirement is void if NAT is used.
    - It is in the interest of the SP to keep log files of authentication transactions. For a rationale and further considerations, please refer to Appendix B.
    - If dynamic RADIUS routing (see Section 2.1.1.2) is used, appropriate F-Ticks MUST be sent to the monitoring infrastructure, either directly or through the NRO services (see Section 6.3.1).
- Network:
  At the very least, the following set of ports MUST be made available to roaming visitors:

Service	Protocol / Port	Note
Standard IPSec VPN Client Connection	IP protocol 50 (ESP) IP protocol 51 (AH) UDP port 500 (IKE)	
OpenVPN Client Connection	UDP port 1194	
IPSec NAT-Traversal Client Connection	UDP/4500	

Wireguard VPN Client Connection	UDP/51820	grandfathered for hotspots installed before 2022
Cisco IPSec VPN over TCP Client Connection	TCP/10000	
SSH	TCP port 22	
HTTP	TCP port 80 TCP port 443 TCP port 8143	8143 grandfathered for hotspots installed before 2022
Mail sending	TCP port 465 TCP port 587	
Mail reception	TCP port 143 TCP port 993 TCP port 110 TCP port 995	
DNS over TLS	TCP port 853	grandfathered for hotspots installed before 2022

Adherence to the following specifications is RECOMMENDED:

- NAS or local AAA Servers:
  - Inclusion of hotspot location information with the Operator-Name attribute in authentication requests as per RFC 5580.
  - Requesting a Chargeable-User-Identity value from the IdP, as per RFC 4372.

- local AAA Servers (in its absence, FLRS):
  - Logs of all authentication requests and responses SHOULD be kept. The minimum log retention time is six months, unless national regulations require otherwise. The information in the requests and responses SHOULD, as a minimum, include:
    - The time the authentication request was exchanged.
    - The value of the User-Name attribute in the request ('outer EAP-identity').
    - The value of the Calling-Station-Id attribute in authentication requests.
    - If present, the value of the Chargeable-User-Identity attribute.
    - The result of the authentication.

- Network:
  - network access to roaming visitors SHOULD not be port-restricted at all (i.e. in addition to the minimum list of open ports from above, allow all outgoing communication). Where this is not possible, the number of filtered protocols SHOULD be kept as low as possible.
  - The use of NAT SHOULD be avoided.
  - IPv6 connectivity SHOULD be supplied.
  - Service providers SHOULD NOT deploy application or interception proxies. Service providers deploying application or interception proxies MUST NOT use the proxy to require users to submit personal information before gaining access to the Internet, and MUST publish information about these proxies on their eduroam website. If an application proxy is not transparent, the service provider MUST also provide documentation on the configuration of applications to use the proxy.
  - Service providers SHOULD NOT assign hostnames to the IP addresses handed out to their users which are in the same principal domain as the organization.

Adherence to the following specifications is OPTIONAL:

- NAS equipment MAY support Wi-Fi Certified PASSPOINT technology.

2.4.4 Specifications and Operational Requirements: End-user Devices

- Requirements for user devices:
  - IEEE 802.1X.
  - Supplicant software with support for at least one EAP type capable of mutual authentication.

3

References

[eduroam]	http://www.eduroam.org
[eduroam Database]	http://monitor.eduroam.org/database.
[IEEE 802.1X]	http://www.ieee802.org
[F-Ticks]	http://monitor.eduroam.org/f-ticks/howto.php http://monitor.eduroam.org/f-ticks/
[GeGC]	http://www.eduroam.org/downloads/docs/eduroam_Compliance_Statement_v1_0.pdf
[Monitoring]	http://monitor.eduroam.org/.
[Security Incidents]	http://www.geant.net/service/multidomainsecurity/Security_Incidents/Pages/
[TTS]	http://tts.eduroam.org

Glossary

AAA	Authentication, Authorisation and Accounting
AH	Authentication Headers
CERT	Computer Emergency Response Team
CET	Central European Time
DNS	Domain Name Server
EAP	Extensible Authentication Protocol
EAP-TLS	Extensible Authentication Protocol Transport Layer Security (StB IETF)
eduroam	EDUcation ROAMing
ESP	Encapsulating Security Payloads
ETLRS	European Top-Level RADIUS Server
FLRS	Federation-Level RADIUS Server
FTP	File Transfer Protocol
GeGC	Global eduroam Governance Committee
GPS	Global Positioning System
gTLD	generic Top Level Domain
HI	Home Institution
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IdP	Identity Provider
IKE	Internet Key Exchange
IPSec	IP Security (StB IETF)
MAC	Media Access Control
NAS	Network Access Servers
NAT	Network Address Translation
NREN	National Research and Educational Network
NREN PC	National Research and Educational Network Policy Committee
NRO	National Roaming Operators
NTP	Network Time Protocol
OT	Operations Team
PPTP	Point-to-Point Tunneling Protocol
RADIUS	Remote Authentication Dial-In User Service (StB IETF)
RI	Remote Institution
RI	Remote Institution
SA5	Service Activity 5
SG	Steering Group
SNTP	Simple NTP
SSH	Secure Shell
TCP	Transmission Control Protocol
TLD	Top-Level Domain
TLRS	Top-Level RADIUS Server
TLS	Transport Layer Security
TTS	Trouble Ticketing System
UDP	User Datagram Protocol

VLAN	Virtual Local Area Network
WPA2	Wi-Fi Protected Access, version 2

Appendix A End-to-end Encryption of User Credentials

This ensures that no intermediate party, be it an eduroam infrastructure operator or external parties, can steal the digital identity of an eduroam user. This enables the eduroam service to make an important assertion: using eduroam never exposes the credentials to anyone in the infrastructure except the home institution, which makes sure that the confederation infrastructure operators are neither responsible nor liable for password theft.

Since no AAA infrastructure available today provides end-to-end encryption in itself, end-to-end security has to be established by the two ends of the authentication chain: the end-user device (notebook, PDA, smartphone, tablet, etc.) and the home authentication server. This is achieved by using mutual-authentication protocols such as EAP-TTLS, PEAP or EAP-TLS. Most notably, authentication methods in use by web-redirect portals such as PAP do NOT provide end-to-end security.

Appendix B Logging of Authentication and Accounting Packets

Authenticating a user and the subsequent establishing of the user session is a transaction between the identity provider and the resource provider. The intermediate infrastructure acts only as conveyor of their data. As such, no liabilities for the confederation members or the Operations Team are involved. Still, logging this data provides an audit trail that may help connected institutions resolve conflicts. Furthermore, the data is useful if debugging a problem is required. Because of that, it is recommended that confederation members, and the confederation infrastructure itself, keep logs of the data flowing through the infrastructure. Since national regulations may require time frames for data retention, it is not possible to give a general recommendation on the duration.