

18-04-2013

Deliverable DJ3.1.2,3: Report on the roaming developments, including recommendations for long- term work



Deliverable DJ3.1.2,3

Contractual Date: 31-01-13
Actual Date: 18-04-2013
Grant Agreement No.: 238875
Activity: JRA3
Task Item: Task 1
Nature of Deliverable: R (Report)
Dissemination Level: PU (Public)
Lead Partner: RESTENA
Document Code: GN3-13-101

Authors: Stefan Winter (RESTENA, editor), Scott P. Armitage (Loughborough University, UK), Wenche Backman-Kamila (CSC/Funet), Maja Gorecka-Wolniewicz (PSNC/UMK), Zbigniew Ołtuszyk (PIONIER), Marko Stojakovic (AMRES), Marina Vermezovic (AMRES), Tomasz Wolniewicz (PSNC/UMK), with contributions from JRA3 T1 team members

© DANTE on behalf of the GÉANT project.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7 2007–2013) under Grant Agreement No. 238875 (GÉANT).

Abstract

This deliverable provides an update to DJ3.1.2,2 and to research and development activities undertaken by JRA3 T1 to support the eduroam® service in its mission of supplying roaming access to wireless networks. The Task includes monitoring developments in the network industry, contributing to standards bodies, producing software to improve eduroam® operations, and liaising with third parties as necessary.

Table of Contents

Executive Summary	1
1 Introduction	2
2 Standardisation	4
2.1 Watching Briefs: Update	4
2.1.1 IETF	4
2.1.2 IEEE	9
2.2 Active Contributions	17
2.2.1 RADIUS/TLS: Specification Complete	17
2.2.2 Dynamic Discovery Options for RADIUS/TLS	18
2.2.3 Common EAP Metadata Definition File Format	19
2.2.4 eduroam Consortium and Architecture Description	25
2.2.5 Cryptographic Enhancements to the EAP-PWD EAP Type	26
3 eduroam Infrastructure Enhancements	27
3.1 Usability Study of the Diameter Protocol	27
3.1.1 Available Implementation Overview	27
3.1.2 Evaluation of freeDiameter, Radiator	29
3.1.3 Open Diameter and WIRE Diameter	32
3.1.4 Summary	32
3.2 RADIUS/TLS Deployment	32
3.3 eduroam Configuration Assistant Tool (CAT)	33
3.3.1 Start Page	33
3.3.2 Federation Administrator Management Pages	35
3.3.3 Integration with eduroam Database	36
3.3.4 Federated Authentication (including eduGAIN)	38
3.3.5 Integration with and Expansion of Dynamic Discovery Test Tool	39
3.3.6 EAP-PWD Support Added	40
3.3.7 Linux Installers	40
3.3.8 Streamlined Access to Installers	41

3.3.9	Resolution of Open Issues from DJ3.1.2,2	42
3.3.10	IdP Administrators Manual	42
3.3.11	Transfer to Production Use	42
3.3.12	Further Plans	43
4	Coordination with Other Activities	44
4.1	Eduroam Finland: Case Study on Statistics of Reasons for Failed Authentications on a National Level	44
4.1.1	Introduction	44
4.1.2	Investigation of Failed Authentication Attempts and their Reasons	44
4.1.3	Summary	47
4.2	World-Wide eduroam Community	47
4.2.1	Scalable Routing of Realms in Generic Top-Level Domains	48
4.2.2	Alternatives to the Use of PKI for eduroam Dynamic Peer Discovery	48
5	Recommendations for Long-Term Work	49
5.1	eduroam Operations Support Services (OSS)	49
5.1.1	Introduction	49
5.1.2	Problem Statement	49
5.1.3	An Operations Support System (OSS) for eduroam	50
5.1.4	Recommendation	52
5.2	Extending On-Site Hotspot Monitoring	52
5.2.1	Introduction	52
5.2.2	Problem Statement	53
5.2.3	Requirements for an On-Site eduroam Monitoring Probe	53
5.2.4	Recommendation	56
6	Conclusions	57
Appendix A	Configuration	58
Appendix B	Generic EAP Metadata Profile	61
B.1	Generic EAP Metadata XML Schema Definition	61
B.2	Sample Generic EAP Metadata Configuration File	68
Appendix C	Discussion Paper on Scalability of RADIUS Realms	73
References		78

Table of Figures

Figure 3.1: Setup for Scenario 2	31
Figure 3.2: Setup for Scenario 3	31
Figure 3.3: CAT: new home page	34
Figure 3.4: CAT: detailed instructions for MS Windows 7 installer	35
Figure 3.5: CAT: Federation administrator interface	36
Figure 3.6: CAT: registering a new institution – unmapped and mapped options	37
Figure 3.7: CAT: management page for mapping an institution at any time	38
Figure 3.8: CAT: integrated Dynamic Discovery test tool	39
Figure 3.9: CAT: expanded TLS connectivity checks	40
Figure 3.10: CAT: Linux installer #1	41
Figure 3.11: CAT: Linux installer #2	41
Figure 3.12: CAT: per-profile download counter	42

Table of Tables

Table 2.1: Features and potential benefits of Interworking	13
Table 2.2: Hotspot/Passpoint additions to Interworking	14
Table 2.3: Recommended parameters for hotspots capable of Interworking	17
Table 2.4: Authentication dictionary: server-side credentials	23
Table 2.5: Authentication dictionary: client-side credentials	24
Table 3.1: Diameter implementations: servers	28
Table 3.2: Diameter implementations: APIs/libraries	29
Table 4.1: Successful and failed authentications	45
Table 4.2: Authentication attempt failure classes	46
Table 4.3: Numbers of failed authentication attempts per class	46
Table 4.4: Analysis of failed authentication attempts by class	47
Table 5.1: eduroam internet access connection factors	52

Executive Summary

This deliverable provides a summary update of the research and development activities undertaken by Roaming Developments, GN3 Joint Research Activity 3 Multi-Domain User Application Research, Task 1 (JRA3 T1) since the publication of the second edition of this document (DJ3.1.2,2) in January 2012. JRA3 T1 supports eduroam Operations (GN3 Service Activity 3 Multi-Domain User Applications, Task 2 (SA3 T2)), whose core business is the supply of roaming access to wireless data networks. Activities of JRA3 T1 include monitoring developments in the network access industry, contributing to standards bodies, supporting and seeking new possible support services for eduroam Operations, and liaising with other GN3 activities.

The core results covered in this deliverable are:

- An in-depth analysis of new features of the latest edition of the Wi-Fi standard, which bring exciting new ways of defining access to networks through grouping hotspots by Roaming Consortium identifiers (as opposed to the previous method of relying exclusively on the network name “eduroam”).
- Active work in the IETF, including, but not limited to, more streamlined user authentication (EAP-PWD and enhancements to it that are of importance to eduroam) and standardised discovery of RADIUS servers, which eliminates routing errors for eduroam realms, which are based in a generic top-level domain.
- Enhancements and the transition to service of the eduroam Configuration Assistant Tool (CAT) tool.
- Work in the Global eduroam Governance Committee to solve scalability questions for eduroam as it expands globally.
- A look ahead to GN3plus, particularly regarding important pending development work on an eduroam Business/Operations Support System (B/OSS) and improved monitoring of eduroam hotspots by developing hardware devices that monitor the quality of service at the actual premises.

This deliverable concludes the work of JRA3 T1. The development work that has, up to now, been done in JRA3 T1, particularly the items identified in the outlook in Chapter 5 of this deliverable, will be continued as an integral part of eduroam Operations in GN3plus; readers who are interested in further eduroam developments should consult the deliverables of this new GN3plus Activity.

1 Introduction

This deliverable provides a summary of the efforts undertaken in Roaming Developments (JRA3 Task 1) from November 2011 to December 2012 (M31–M45), but also includes key events until project end (March 2013, M48). It is intended to provide an update on the research and development activities undertaken to support eduroam Operations (SA3 Task 2).

eduroam has been an operational service since the launch of GN2 (September 2004). Its core focus is on the supply of roaming access to wireless networks, but it has also been deployed on other media, such as IEEE 802.3 wired networks. It is vital that eduroam is in step with the latest advances in the wireless LAN industry, and it should also strive to influence the development of the industry in order to evolve the service, and provide the best possible user experience to customers in the research and education community.

Task 1 of JRA3 assumes the role of research and development (R&D) for eduroam in Europe, and its aim is to increase the security and usability of eduroam's architecture. The Task also seeks to investigate and propose a solution to providing more seamless authentication and authorisation in the current eduroam infrastructure. The activities pursued in JRA3 T1 include:

- Establish a watching brief on standardisation organisations that produce standards in the sphere of interest of eduroam.
- Influence and create standards that are relevant for eduroam in the Internet Engineering Task Force (IETF).
- Develop solutions that improve the eduroam operational infrastructure.
- Liaise with third parties inside and outside of Europe for the benefit of eduroam in Europe.

This document provides a 12-month update on network industry developments, new service elements and software to support and link eduroam to other GÉANT activities. Since this is the last deliverable of JRA3 T1, which coincides with the end of GN3 as a whole, the document exceptionally also provides recommendations for future work, to be taken up in the successor project GN3plus or other projects as appropriate.

The deliverable is structured as follows:

- Chapter 2 provides updates in the standardisation space; Section 2.1 lists passive watching briefs while Section 2.2 details active contributions.
- Chapter 3 contains a number of possible improvements to the eduroam infrastructure.

- Chapter 4 lists the activities with third parties.
- As an extra feature of this last edition of the deliverable, Chapter 5 identifies a number of areas for future development which should be tackled in GN3plus.

Please note that some of JRA3 T1's efforts have already been set out in detail as part of the previous editions of this document [DJ3.1.2,1, DJ3.1.2,2], and have not been repeated here.

2 Standardisation

Following the developments of standardisation bodies like the IEEE and IETF is a vital part of eduroam R&D: new standards change the way the network login process works; new Wi-Fi amendments, Extensible Authentication Protocol (EAP) types and infrastructure elements can all either deliver an operational benefit – or hamper the operational model of eduroam. It is important to identify the upcoming changes, and, if possible and needed, to influence them so that they fit well into the operational model of eduroam.

2.1 Watching Briefs: Update

2.1.1 IETF

2.1.1.1 *IETF: Network Endpoint Assessment (NEA)*

The IETF Network Endpoint Assessment (NEA) Working Group (WG) has worked for a long time on a set of standards that enable the state of “health” (called “posture”) of a client device to be determined before it is granted access to a network.

Readers with an interest in the history of NEA in the IETF so far should consult the previous editions of this deliverable (DJ3.1.2,1 Section 2.1.1; DJ3.1.2,2 Section 2.1.1). The remainder of this section describes the updates of the state of the art regarding NEA.

As of March 2013, the NEA working group has finally completed a full set of specifications for creation and transport of posture information from a client to a posture assessment server.

While the definitions of single Posture Attributes (PAs), and of a collation format which binds one or more PAs together, the Posture Broker (PB) format, were already completed by the time the previous deliverable edition was written, the working group had yet to decide on a format for transportation of PB messages from a client device to a server.

Transport: Inside EAP or Outside EAP

One point to decide on was whether the data should be transported inside an EAP conversation (coinciding with the initial network authentication), or whether Posture Assessment should happen after the network authentication is completed, e.g. inside the browser.

The working group could not decide on one single way of transporting PB data. Two specifications were developed, one for transport inside a Transport Layer Security (TLS) tunnel (PT-TLS [RFC6876]) and one for transport inside EAP (PT-EAP [PTEAP]).

Having two independent ways of performing Posture Assessment leaves a number of questions open.

With the EAP transport, posture data is always transported to the user's EAP (authentication) server. When roaming, this means that the data is available at the Identity Provider (IdP), but not the Service Provider (SP), even though the service provider has the most significant interest in evaluating the client posture.

It remains an open question how, if at all, the PB data can be transported from the IdP to an external entity, e.g. the SP. However, when using the EAP transport, the user always communicates to the deterministically same entity – his IdP – which receives and evaluates the PB information.

When doing posture assessment via PT-TLS though, the posture information is evaluated directly at the SP. For the user, this has the significant disadvantage that the way PT-TLS is executed is determined by the SP, which means that different networks query the client in different ways. One example would be browser plugins (ActiveX, Java, etc.), which collect the posture information and send it via PT-TLS. Other deployments might require the download of a specific executable which then sends the data via PT-TLS. For users, it would mean that whenever they roam to a new network, a new way of posture assessment may be encountered, which is potentially extremely confusing for them. It is also questionable from a security perspective: the user is then trained to install and execute “arbitrary” code on his machine because a third party demands so.

These aspects of NEA make its use in a roaming Internet Service Provider (ISP) environment like eduroam very questionable. If deploying a NEA solution at all, probably the most useful way is to enable it only for an IdP's users on the local (“home”) network, while disabling it on visitor VLANs.

2.1.1.2 IETF: Alternative RADIUS Transports

The IETF is in the process of specifying multiple new transports for Remote Authentication Dial-In User Service (RADIUS). The development of RADIUS/TLS was the original trigger, as it needed Transmission Control Protocol (TCP) as a new underlying transport. In addition to that transport, work is ongoing for RADIUS / Datagram Transport Layer Security (DTLS). The status of these transports is as follows:

- RADIUS/TCP: This specification is complete and was published as [RFC6613]. It is the underlying transport for the (now also completed) RADIUS/TLS (see Section 2.2.1). The RFC recommends not using “bare” RADIUS/TCP, but only to use it in conjunction with RADIUS/TLS encryption.

- RADIUS/DTLS: Work on this transport (User Datagram Protocol (UDP) with a variant of TLS for encryption) is still ongoing as a chartered work group item of the RADIUS Extensions working group. The current draft (version -04) is available at [RDTLS].

2.1.1.3 IETF: Internationalisation Challenges

Since the previous edition of this deliverable, a draft of a revision document to the flawed RFC4282 has been submitted to the IETF's RADIUS Extensions working group and is being actively discussed. It is accessible at [RADNAI].

The document's primary way of addressing the problem is threefold:

- Bind the syntax of valid Network Access Identifiers (NAIs) to the syntax of valid domain names.
- Require all intermediate systems to abstain from manipulations of the representation of the username.
- Take all packet handling decisions on the bit-by-bit representation of the User-Name attribute.

The first of these points maps directly into normal eduroam operations: the eduroam Service Definition requires eduroam realms to be registerable (but not necessarily registered) Domain Name System (DNS) domain names. Once eduroam decides to permit non-ASCII realm names, it should be easy to extend the eduroam Service Definition.

The second point is necessary for at least two reasons. One reason is that intermediate systems (e.g. Access Points, RADIUS proxies) do not have enough information about the username to be able to make deterministic alterations to it. This is because the EAP supplicant sends a byte stream which is the EAP identity to the authenticator; but it does not send encoding information along with it. Without encoding information, it is not possible to make deterministically working transformations of that string. The second reason is that the RADIUS User-Name is in correlation to the EAP Identity inside the EAP-Message attribute; if one is altered, but not the other, the resulting mismatches can be confusing to the final IdP server; i.e. with a manipulation, the proxy might cause the authentication to fail further down in the proxy chain.

This second point, by inference, requires that the EAP supplicant and the IdP's EAP server both have knowledge about the different encodings for their realm; i.e. the eduroam IdP server needs to be configured to terminate EAP sessions for the internationalised realm in all encoding and normalisation variants that supplicants might choose to use. If a supplicant uses an encoding or normalisation variant that the IdP does not recognise as representing the realm, authentication may fail, and no intermediate system will be able to rectify the misrepresentation.

The third point probably has the most significance for the eduroam infrastructure because it applies not only to the "ends" of the EAP conversation, but to proxies and forwarding decisions. First, eduroam's practice of dissecting realms into a "federation" (Top-Level Domain (TLD)) suffix and the "institution" second-level part of the domain assumes that a) the (ASCII) dot, 0x2E, is recognisable as a separator; an assumption that is likely to be true in almost all character sets and thus realm representations; and b) that the TLD suffix matches the proxy's configuration, an assumption that may or may not be true in an internationalised (UTF-8) context.

Example:

- A user uses the identity string “user@restena.lu”.
- The supplicant chooses to use UTF-8 as character encoding, and to intersperse the TLD characters between the “l” and the “u” with the unicode character <U+FEFF>, which is a zero-width, non-breaking blank space (i.e. indistinguishable from “nothing”), printed as: “user@restena.lu” but with a binary representation “7573 6572 4072 6573 7465 6e61 2e6c feff 75”.
- The IdP server operator knows that this particular string representation is in use and configures the server to consider the realm “restena.l<U+FEFF>u” as his own realm; he authenticates the user successfully in a local-use context.
- The user roams with this – valid – RADIUS User-Name, sent by an international eduroam SP via intermediates to the European Top-Level Servers (ETLRs).
- The ETLRs inspect the TLD field, do have a known target for “lu”, but do not have a target for “l<U+FEFF>u”.
- The request gets rejected.

Such a rejection due to routing table string representation differences is unfortunate. It is still subject to discussion in the IETF, with involvement of JRA3 T1 personnel. One approach that might be adopted is: instead of requiring byte-by-byte comparisons, perform normalisation of the realm and of the routing tables entries, and do a comparison of the normalised strings.

Unusual representations of the realm also have an impact on dynamic peer discovery and have led to a revision of the discovery algorithm. See Section 2.2.2 for further details.

2.1.1.4 IETF: EAP Types

The watching brief on the IETF EAP Method Update (EMU) working group still has the same focus as in the previous edition of this deliverable: certificate-less (“zero-knowledge”) EAP types, and the development of a common tunnelled EAP method.

EAP-PWD / EAP-EKE

There are no notable developments regarding implementations and deployment of EAP Encrypted Key Exchange (EAP-EKE).

There are, however, several notable updates to EAP authentication using only a password (EAP-PWD). Since the last edition of this deliverable:

- Supplicant software supporting EAP-PWD has been released for Microsoft Windows (all versions from Vista onwards) and UNIX-like operating systems, e.g. Linux and Android.
- Server-side support for EAP-PWD has been added to the RADIUS servers Radiator from Open System Consultants, Inc., and for FreeRADIUS (GIT code for the upcoming version 3.0).

- eduroam Configuration Assistant Tool (CAT) now includes support for EAP-PWD in the IdP administrator configuration interface; if EAP-PWD is the preferred EAP type, eduroam installers are created for the supported Windows and Linux installers.

Furthermore, deployment and discussion of this EAP type has shown several of its strengths and weaknesses, namely:

- EAP-PWD does not support anonymous outer identities. This means that the end user's input into his EAP supplicant will always be revealed to intermediate parties when he tries to log in. These intermediate parties include the Access Point / Controller, the eduroam SP RADIUS server and any proxies between the SP and the user's IdP. It may also include any IP hop in between these entities if transport encryption with RADIUS/TLS is not used. The level of sensitivity regarding the release of their users' true username to intermediate parties varies among eduroam IdPs. Some find this fact prohibitive to using EAP-PWD because they advocate the heavy use of anonymous outer identities in other EAP types; others embrace it because they enforce the use of the real username in other EAP types as well.
- Currently, EAP-PWD terminates the EAP session without further notice if the username was not found. A passive attacker can learn from these aborted sessions that a username was invalid (as opposed to that the password was incorrect). This is a minor information leakage that some IdP administrators may find displeasing. It also has the side-effect that EAP supplicants which started the session will not learn of the failure. Their authentication session will appear to "hang"; which leads to a suboptimal user experience. However, work is currently ongoing (see Section 2.2 *Active Contributions* below) to revise the EAP-PWD standard so as not to reveal this fact and to send fake data to the supplicant instead; this prevents attackers from learning by the absence of a response and it enables EAP supplicants to detect that the authentication session cannot terminate successfully.
- Due to the lack of an encrypted TLS tunnel during the EAP authentication, EAP-PWD does not support EAP-based exchange of posture information with NEA (see Section 2.1.1.1 above). Since EAP-based NEA was standardised only very recently, this is probably not currently a significant hindrance to using EAP-PWD, but should be considered by potential deployers.
- EAP-PWD needs to be able to do local cryptographic calculations on a representation of the password; this need not be a cleartext representation of the password, it can be an NT-Hash of the password. The need to have a representation at all rules out all deployments of Microsoft Active Directory, because ActiveDirectory only works as an authentication oracle; i.e. It doesn't reveal the password but merely acts on artifacts of an authentication session and reveals whether a correct password was used to create the artifact or not.
- When the available password representation is neither cleartext nor an NT-Hash, EAP-PWD cannot currently authenticate users, because these two representations are the only ones specified in an enumeration of compatible representations. However, work is currently ongoing (see Section 2.2 *Active Contributions* below) to revise the EAP-PWD standard to include many more popular and contemporary password representations, e.g. salted variants of SHA1 and SHA2.

In summary, EAP-PWD is useful in all situations where:

- The release of the true username to intermediates is not a concern AND
- NEA is not in use (or is in use with TLS-based transport instead of EAP transport) AND
- Microsoft Active Directory or other password storage that only works as an authentication oracle is not in use AND
- The representation of passwords in the identity management system is either cleartext or NT-Hash (further representation formats may be supported by EAP-PWD at a later stage) AND
- The minor information leakage about non-existing usernames is not a concern (this may be rectified by EAP-PWD at a later stage).

Tunnelled EAP Method (TEAP)

As reported in the previous edition of this deliverable, the IETF is in the process of standardising one EAP type that provides a TLS tunnel for user authentication, with the goal of unifying the existing similar, but slightly different, tunnelled EAP types (EAP Tunnelled Transport Layer Security (EAP-TTLS), Protected Extensible Authentication Protocol (PEAP), EAP Flexible Authentication via Secure Tunnelling (EAP-FAST)).

The EAP type that was selected for standardisation was originally called EAP-FASTv2. As work on the final standard progressed, it was renamed because the old name was seen as an unfair advantage: EAP-FAST is widely recognised as being an EAP type proprietary to Cisco, while the new standard is supposed to obsolete all other tunnelled EAP types as well, not just EAP-FAST.

The standardised EAP type will be called “Tunnel EAP Method (TEAP) Version 1” [TEAP].

The operational differences between this EAP type and the established tunnelled EAP types are minor. One of the advantages is that TEAP will probably require fewer round-trips to perform an authentication, leading to faster authentication time. Another advantage is that it will always terminate the EAP state machine, even if a client is not accepting a server certificate. In PEAP, such a situation simply meant that the client would not reply to the server at all – meaning that the server unnecessarily reserves state for a potentially ongoing conversation, and is not able to log that there was an authentication failure due to the user rejecting the server’s identity.

As of the date of issue of this deliverable, the specification is nearing completion. It has completed a Working Group Last Call (WGLC) in the EAP Method Update working group.

2.1.2 IEEE

2.1.2.1 IEEE 802.1X-2010

Even though the IEEE 802.1X-2010 standard was ratified more than a year ago, there is no significant momentum in terms of available devices that support the new beaconing features of IEEE 802.1X-2010. This is true both for authenticators (i.e. switches) and for supplicants.

The situation should continue to be monitored, albeit with a low priority.

2.1.2.2 IEEE: Network Discovery with IEEE 802.11u and Hotspot 2.0

Background

IEEE 802.11u was originally introduced as an amendment to the IEEE 802.11 protocol specification [80211u-2011]. It later became part of the IEEE 802.11-2012 protocol specification as “Interworking with External Networks” [80211-2012]. Its purpose is to advertise properties of a wireless network to the clients in its vicinity before the clients try to establish a connection to the wireless network. The advertised properties are intended to help the client device to select the “best” network to connect to.

Related to Interworking is the Hotspot 2.0 specification, created by the Hotspot 2.0 working group and published by the Wi-Fi Alliance [HS20]. The Wi-Fi alliance has created the Passpoint™ Certification program to certify wireless devices that have implemented Hotspot 2.0 [PP-DEPLOY]. Interworking and Hotspot 2.0 / Passpoint provide pre-association information allowing client devices to make more intelligent decisions about which wireless access point (AP) they associate to.

IEEE 802.11 Interworking: Advertisement of Network Properties

Interworking uses two protocols to provide this pre-association information. The first protocol is Generic Advertisement Service (GAS) for communication between the service provider’s infrastructure and the client. The second protocol is Access Network Query Protocol (ANQP), which is the query / response protocol providing the information about the access network. ANQP is delivered over GAS. In addition to the ANQP elements defined in the IEEE 802.11-2012 standard, the ANQP protocol also allows additional pieces of information in a “Vendor-Specific” range to be transmitted. Hotspot 2.0 / Passpoint make use of this Vendor-Specific extension to send more network metadata (see Section 0.0.0.0).

Interworking provides a number of features which are of potential benefit to eduroam, as summarised in Table 2.1 below:

Element Name	Purpose
Roaming Consortium	<p>Generic</p> <p>The roaming consortium element is part of Interworking and allows networks that support multiple IdPs to be identified to client devices (irrespective of the Service Set Identifier (SSID)). This identification is achieved through the use of IEEE-registered Organisation Identifiers (OIs) [IEEE-RA]. Three roaming consortium OIs can be directly included in the beacon (further OIs must be queried for using ANQP). The roaming consortium OI identifies a roaming network and therefore a client with a binding between the OI and a configuration / set of credentials will automatically join the network. As the network selection is performed based upon the roaming consortium OI, the SSID is somewhat irrelevant.</p> <p>Benefit for eduroam</p> <p>eduroam has a chronic deficiency when it comes to network names: client</p>

Element Name	Purpose
	<p>configuration pre-Interworking depends entirely on the SSID. Where overlapping eduroam SSIDs require one deployment to move to a different SSID, re-configuration of client devices is required. Also, business agreements with other roaming consortia are hampered by the requirement to broadcast the eduroam SSID for network identification purposes.</p> <p>For eduroam purposes, the ability to identify an eduroam hotspot via a consortium OI provides much more flexibility in terms of simpler device configuration. It may become possible to ease the rather strict requirement of using the SSID “eduroam” in all cases.</p> <p>In anticipation of the future widespread availability of Interworking-capable client devices and Access Point hardware, TERENA has registered the OUI-36 Organisation-Unique Identifier 00-1b-c5-04-6 and has in turn assigned the Consortium Identifier 00-1b-c5-04-60 for eduroam purposes. This Consortium Identifier can be used as a roaming consortium OI to identify a hotspot as being an eduroam hotspot, regardless of the SSID used on that hotspot.</p>
NAI Realm List	<p>Generic</p> <p>The intention of the realm list is to advertise the realms supported by a network and also, optionally, the EAP types supported by that realm. The NAI realm list is transmitted over ANQP to the client and lists all authentication realms supported by this network.</p> <p>Benefit for eduroam</p> <p>For roaming networks with a small number of IdPs, advertising every single realm works as intended. However, this doesn’t appear to scale to roaming networks that have large numbers of IdPs such as eduroam. For eduroam this is a very large number, which can change on a daily basis, and it is therefore unlikely to be useful to the eduroam community.</p>
Venue Information	<p>Generic</p> <p>Interworking provides the ability for an AP to provide information about the service provider and location of the AP. The Interworking element in the network broadcast can indicate the availability of venue information. This information includes a group identifier indicating the function of the organisation that is operating the AP; e.g. 3 indicates Educational. The group code can then be combined with a type code to indicate the type of organisation; e.g. under group 3, type 3 indicates University or College.</p> <p>Benefit for eduroam</p> <p>The consequences of setting information into the Venue Information GAS field are not clear. Furthermore, eduroam hotspots may want to indicate venue information at their discretion. The types 3 (“Educational”) and 5 (“Institutional”) seem appropriate for most eduroam networks; types 7 (“Residential”), 10 (“Vehicular”) and 11 (“Outdoor”) may also have frequent applicability. Hotspot operators should consult the tables 8-52 and 8-53 of IEEE 802.11-2012 for further classification information.</p>

Element Name	Purpose
Venue Name	<p>Generic</p> <p>ANQP provides the Venue Name element which allows service providers to enter a UTF-8 string (together with an ISO-639 language code), e.g. “TERENA Secretariat, Amsterdam, 1017 AW, T:+31(0)20 5304488” “eng”. ANQP allows multiple venue names and therefore a service provider could have their organisation name in one venue name field and the location in another field or have their name in multiple languages. Depending upon implementation in the client device, this information could be used to indicate to the client exactly which service provider’s infrastructure they are connected to.</p> <p>Benefit for eduroam</p> <p>It remains to be seen whether supplicants will expose this information to the end user. If so, this field could be used to convey points of contact for the hotspot in question to the end user; e.g. to report problems while using the hotspot.</p>
Domain	<p>Generic</p> <p>Using Interworking, a service provider’s access points can advertise one or more fully qualified domain names to indicate the operator of the access points. Clients configured with a domain that matches one advertised by the AP will consider the service provider as its “home” service provider. Likewise, clients configured with a domain that is not advertised by the access point will consider the network a roaming network. Devices implementing Passpoint should prefer their home service provider over roaming service providers [PP-DEPLOY].</p> <p>Benefit for eduroam</p> <p>This functionality is probably going to be useful in two scenarios:</p> <ol style="list-style-type: none"> 1) Organisations whose eduroam coverage overlaps with another eduroam site. eduroam sites implementing Interworking could advertise their realm in the domain field and clients could configure their eduroam profile on their device with their home realm. The user’s device would then prefer the APs belonging to their home organisation. 2) Indication of service availability to own users. In pre-Interworking eduroam, the privilege level and services offered to an eduroam user differ from hotspot to hotspot, without an indication for the user of which services he can come to expect. Users without a background in IT may be confused if a service that was available in their “home” eduroam network becomes unavailable when roaming. If supplicants allow display of a “Home Zone” identifier if logged into their home network (as is customary in several cell phone provider networks), users might be less surprised to find a different level of service when roaming.
IP address type availability	<p>Generic</p> <p>Interworking allows service providers to advertise their IP protocol ability and some basic characteristics. Service providers can indicate whether IPv4 or IPv6 is available, and whether their IPv4 offering is using public addresses or Network Address Translation (NAT). The presence of carrier-grade NAT can also be indicated. This provides useful pre-association information to client devices. The</p>

Element Name	Purpose
	<p>values to use for this information element are described in Table 8-186 and 8-187 of IEEE 802.11-2012.</p> <p>Benefit for eduroam</p> <p>eduroam currently uses an out-of-band means to collect (eduroam DB) and display (eduroam coverage maps) information regarding the availability of IPv6 and presence of NATs. This information element is as useful in eduroam as in any other network and should be set according to the actual setup of the access point, which might ultimately obsolete the need to collect and display the information out-of-band.</p>
Access Network Type	<p>Generic</p> <p>Interworking provides an enumerated list of network types, which gives client devices an indication of whether or not they should try to connect at all. For example, a network that is not configured on the client device and which advertises its Access Network Type as “private network” (type 0) is not likely to be a usable network. It also provides basic billing information with type identifiers “Chargeable Public Network” (type 2) and “Free Public Network” (type 3).</p> <p>Benefit for eduroam</p> <p>eduroam networks can use this element to indicate their semi-closed nature by selecting “Private network with guest access” (type 1).</p>

Table 2.1: Features and potential benefits of Interworking

IEEE 802.11-2012 defines more information elements, most of which are not useful or only marginally useful for eduroam.

It is noteworthy that neither the IEEE 802.11-2012 standard nor the Hotspot 2.0 / Passpoint certification documents make clear which identification method (Roaming Consortium vs. NAI realm list) should take priority when a client device makes its access decision. To avoid problems with implementations, this document recommends that only one of the two be set, i.e. Roaming Consortium.

Should the hotspot Access Points / Controller allow specifying Interworking information elements, it is advisable for the hotspot operator to populate all of the above fields with meaningful information. See also the recapitulation section *Recommendations for eduroam Hotspots*.

Hotspot 2.0 / Passpoint: Additional Vendor-Specific Network Metadata

Passpoint makes use of the ANQP protocol to provide information to client devices in an industry-recognised format – ANQP elements of type Vendor-Specific with the Wi-Fi Alliance’s vendor ID – which is supported by all devices carrying the Passpoint certification.

Hotspot 2.0 Vendor-Specific additions to Interworking are summarised in Table 2.2 below:

Element Name	Purpose
Operator Friendly Name	In addition to Interworking's Venue Name, Hotspot 2.0 also provides the Operator Friendly Name. Operator Friendly Name allows the network operator to enter their service provider name, e.g. "TERENA Offices" or "eduroam@Loughborough". Hotspot 2.0 allows multiple Operator Friendly Names [PP-DEPLOY].
WAN metrics	Hotspot 2.0 also provides the ability to provide WAN metrics to clients. This includes whether the WAN link for the network is up or down, and the speed and loading of the WAN link. Client devices can then move between service providers either to avoid loaded links or WAN links that are down, or to prefer networks with more bandwidth available.
Connection Capability	This element allows the hotspot operator to communicate a list of network ports that are usable by clients connecting to the hotspot.

Table 2.2: Hotspot/Passpoint additions to Interworking

While all this information is useful for clients when making a decision about which hotspot to access, it is much less crucial than the elements included in 802.11 Interworking. eduroam hotspots may make use of these fields as they see fit.

Using its registered OUI-36, TERENA could create its own vendor-specific ANQP content. In theory this could allow an eduroam SP to provide information through an ANQP element. However, unless a client / supplicant on the device was configured so that it could interpret the element, this feature is somewhat redundant.

Field Evaluation

eduroam participants from Janet(UK) have conducted early field tests with the new Interworking features, based on the implementations available at the time.

Setup

The following equipment was used during the tests:

Client Side: Laptop running Ubuntu 12.10 with a recent development version of wpa_supplicant [WPA_S], which is capable of Interworking.

Access Point: Linksys SOHO Access Point running openWRT firmware image capable of Interworking.

For the tests a minimal wpa_supplicant configuration file was created using the credential block. The credential block was introduced for use with Interworking network selection and provides a credential set that can be used with Interworking / Hotspot 2.0 wireless networks. A key feature to note with the credential block is the lack of an SSID, as network selection is based upon Interworking features. This is the crucial part of the configuration used for the tests (the full configuration file can be found in Appendix A):

wpa_supplicant.conf

```
interworking=1
auto_interworking=1

cred={
    ...
    username="user@lboro.ac.uk"
    roaming_consortium=001bc50460
    domain="lboro.ac.uk"
    ...
}

hs20=1
```

Test 1: Simulating Overlapping Service Provider Networks

For the test, two wireless networks were created using the SSIDs “11u Test” and “HS2 Test”. Both networks were WPA2/AES with Interworking and Hotspot 2.0 enabled. Both networks advertised the eduroam roaming consortium OI (001bc50460) and the same Hotspot 2.0 profile (e.g. WAN data rate etc.). The two networks did, however, advertise different domain names, “lut.ac.uk” and “lboro.ac.uk”, while the user’s credential was of the realm user@lboro.ac.uk.

The expected outcome was that wpa_supplicant will connect to either of these two networks (but no other networks in the vicinity) and that it would prefer “lboro.ac.uk” over “lut.ac.uk” because it matches the home domain of the user.

Below is an annotated and abbreviated log output from wpa_supplicant on the test client:(see Appendix A for the full debug output).

Initially the client begins by scanning for wireless networks.

```
nl80211: Received scan results (12 BSSes)
wlan0: BSS: Start scan result update 1
wlan0: BSS: Add new id 0 BSSID 1c:17:d3:ca:ea:75 SSID '11u Test'
wlan0: BSS: Add new id 1 BSSID 1c:17:d3:ca:ea:71 SSID 'eduroam'
wlan0: BSS: Add new id 4 BSSID 1c:17:d3:ca:ea:74 SSID 'HS2 Test'
```

As the configuration file does not contain any SSID-based profile and thus no configuration for any of the networks is known, wpa_supplicant begins an ANQP fetch from all Interworking-enabled networks.

```
wlan0: No suitable network found
wlan0: Interworking: start ANQP fetch since no matching networks found
```

After querying all Interworking-enabled networks, the returned information is processed against the credential block from the configuration (coloured emphasis added).

```
wlan0: ANQP fetch completed
Interworking: Search for match with home SP FQDN lboro.ac.uk
Interworking: AP domain name - hexdump_ascii(len=9):
    6c 75 74 2e 61 63 2e 75 6b                lut.ac.uk
wlan0: INTERWORKING-AP 1c:17:d3:ca:ea:75 type=roaming
Interworking: Search for match with home SP FQDN lboro.ac.uk
Interworking: AP domain name - hexdump_ascii(len=11):
    6c 62 6f 72 6f 2e 61 63 2e 75 6b        lboro.ac.uk
wlan0: INTERWORKING-AP 1c:17:d3:ca:ea:74 type=home
Interworking: Highest roaming consortium matching credential priority 0
Interworking: Connect with 1c:17:d3:ca:ea:74 based on roaming consortium match
```

The client matches the Roaming Consortium ID from both “11u Test” and “HS2 Test”. However, these networks are advertising different domains. The client recognises “HS2 Test” (1c:17:d3:ca:ea:74) as having a matching domain (lboro.ac.uk) to that in the credential block. This network is therefore recognised as the preferred network over the roaming 1c:17:d3:ca:ea:75 “11u Test” with the domain lut.ac.uk.

Subsequently, wpa_supplicant creates an ad hoc SSID configuration block for this network and connects to the network with the credentials as configured in the “cred” block.

```
wlan0: WPA: Key negotiation completed with 1c:17:d3:ca:ea:74 [PTK=CCMP
GTK=CCMP]
wlan0: Cancelling authentication timeout
Removed BSSID 1c:17:d3:ca:ea:74 from blacklist
wlan0: State: GROUP_HANDSHAKE -> COMPLETED
wlan0: CTRL-EVENT-CONNECTED - Connection to 1c:17:d3:ca:ea:74 completed
```

The connection is complete.

This early field test shows that the concept can indeed be used for network selection. As at the time of writing this deliverable, several major vendors have already implemented Interworking and Hotspot 2.0 into their Access Point / Wi-Fi Controller products, either in production or beta firmware; among them Cisco Systems, Aruba, Meru Networks, Aerohive, Ruckus Wireless, Lancom Systems. Also, more vendors have announced future support for this feature set (e.g. Juniper Networks). It can therefore be expected that Interworking will gain significant traction in the wireless access industry.

Recommendations for eduroam Hotspots

With IEEE 802.11's Interworking becoming more and more available in client devices, it is RECOMMENDED that all hotspots that are capable of Interworking set up their equipment with the following parameters:

Setting	Value	Description
Roaming Consortium	00-1B-C5-04-60	TERENA Organisation Identifier for eduroam
Access Network Type	1	Private network with guest access
NAI Realm List	<leave empty>	Number of realms too high, unmanageable
Domain	<hotspot's DNS domain>	If also IdP, use identical string as IdP realm
IP Address Type Availability	For applicable values, see IEEE 802.11-2012, tables 8-186 and 8-187	IPv4 and/or IPv6, is NAT used, etc.
Venue Name	Fill with contact information for hotspot	Examples include a mail address, office location, telephone number
Venue Information	For applicable values, see IEEE 802.11-2012, tables 8-52 and 8-53	Classification of the type of hotspot, e.g. "educational/university"

Table 2.3: Recommended parameters for hotspots capable of Interworking

It should be noted that the above settings will fail to make the hotspots "Hotspot 2.0 Certified", the most striking reason being that this certification requires the NAI realm list to be populated with the supported realms. Future developments (such as being able to make real-time queries about the available NAI realms in a consortium to an external ANQP server) may rectify this situation.

2.2 Active Contributions

2.2.1 RADIUS/TLS: Specification Complete

JRA3 T1 and, previously, GN2 JRA5 have been working on the specification of RADIUS over TLS (previously called "RadSec") for over five years. The work was fruitful and led to the release of RFC6614: "Transport Layer Security (TLS) Encryption for RADIUS" [RFC6614].

The specification includes only the encryption of RADIUS servers; it does not include an answer to the question of how these peers find each other. As such, it is limited to the traditional static configuration of RADIUS servers based on the user's realm. The use of DNS to discover RADIUS servers dynamically, "Dynamic Peer Discovery", is the subject of a follow-up specification – see the next section (2.2.2) for details.

2.2.2 Dynamic Discovery Options for RADIUS/TLS

The specification of RADIUS Dynamic Peer Discovery based on Network Access Identifier (NAI) realms is progressing as planned. The current revision is -06 [DYN]. eduroam Operations has deployed Dynamic Discovery based on the content of this draft already, and is in fact feeding the lessons learned from operational experience back into new revisions of the draft.

The document has already undergone a Working Group Last Call (WGLC) in the RADIUS Extensions working group of the IETF. The document received very thorough reviews in WGLC and is currently being revised to address these comments. As soon as the outstanding issues are resolved, it can be advanced towards publishing. The main aspects that need revision at this point are:

- Even though the discovery algorithm is finished, IETF participants require that the subsequent server and client authentication and authorisation checks are standardised as well; in particular, the draft should have at least one mandatory-to-implement (MTI) mechanism for verifying discovered peer identity and authorisation. The eduroam mechanism in that regard (checking the presented server certificate for two criteria: is it issued from an eduroam-accredited Certification Authority (CA), and does it carry a Policy OI designation for “authorised eduroam SP / IdP”) is not seen as sufficient in the general internet because it does not allow identification of the exact IdP authorisation, only that the discovered server is part of eduroam. In principle, this creates an opportunity for an impersonation attack, where one IdP captures the traffic of another IdP. In eduroam, this is not a significant issue, but, in more hostile roaming environments, it may well be. There are several approaches to this problem, which are currently being actively discussed in the working group:
 - Require the use of DNS Security Extensions (DNSSEC) during the discovery algorithm execution and only use trusted results.
 - Introduce a certificate property that contains the exact realm (or set of realms) that a server is authorised to act for.
- Internationalisation and its side-effects. The discussion on the structure and exact permissible content of Network Access Identifiers (see Section 2.1.1.3 *IETF: Internationalisation Challenges* above) also has consequences for the work on Dynamic Peer Discovery. When using discovery, the algorithm is executed on the attribute User-Name in the RADIUS packet – which is unvetted end-user input and does not necessarily conform to any specification. There are multiple possible inputs to consider:
 - The user input is not valid UTF-8 or does not contain a realm separator (“@”). This case is relatively easy: simple parsing of the User-Name content will reveal both of these conditions. The dynamic discovery algorithm is rightfully not executed.
 - The user input is valid UTF-8 and contains the realm name in the so-called “Normalised Form C” (NFC) – a canonical presentation of the realm as used in DNS. This is also a relatively easy case, as the server can compare the string with its own RADIUS configuration (which is ideally also in NFC). If the realm should be routed statically, the configuration will reveal that and, rightfully, no dynamic discovery is executed. If the realm is not in the static routing table, dynamic discovery will be rightfully triggered, and the input is guaranteed to be converted to a DNS label for the subsequent lookup.

- The user input is valid UTF-8, but the realm name is not normalised in NFC. This is a rather problematic case. The RADIUS server needs to check the incoming realm name against its configuration to determine whether the request should be handled locally or forwarded to another server. Regardless whether or not dynamic discovery is configured, there is a recognition problem: if the realm is configured in normalised form, and the input is not in the exact same form, simple checks for equality will fail, which will ultimately lead to the server making a wrong decision about the packet. This is the general problem with internationalisation as described in Section 2.1.1.3. The speciality that is adding complexity for dynamic discovery is the possible introduction of routing loops; these are described below.
- Routing loops. Under unusual circumstances, it may be possible that a server does not recognise that a realm is already configured in static configuration, and consequently will trigger Dynamic Peer Discovery. DNS might then yield the information that the server itself is responsible for the realm. Example:
 - User input (realm) is in an international character set, but not in normalised form.
 - Server configuration is in normalised form and advertises that it is responsible for the (normalised) realm in DNS.
 - The lookup for the realm in static configuration will not produce a result.
 - Dynamic Discovery is used to find the responsible server in DNS.
 - DNS normalises the realm on its own, looks up the normalised realm.
 - The result of discovery is that the server that triggered Dynamic Discovery is itself the responsible server.
 - The server will send its own request to itself.

Such a routing loop can be prevented. In IETF discussions, two options are being considered:

- From the set of servers that are discovered, remove the entry that represents the querying server itself; send to another host in the set.
- Declare the discovery process failed; use static routing for the realm.

It remains to be seen which of two options is favoured; both of them prevent the “forward-to-self” problem.

2.2.3 Common EAP Metadata Definition File Format

2.2.3.1 Problem Description

The implementation of the Configuration Assistant Tool (CAT) (see Section 3.3) has led to an interesting observation: many operating systems store or process their EAP configuration data in a structured way which can be exploited to create automatic installers that feed this information into the device. However, all these operating systems use different ways of representing the information. Examples include:

- Apple: an XML file in Apple's own "plist" style schema describes the EAP properties and the WLAN for which the EAP credentials are valid.
- Microsoft: each EAP type has its own XML schema for specifying EAP properties, WLAN properties, and many Microsoft-proprietary extensions. Most notably, the XML tag names differ between EAP types, even if they contain conceptually the same piece of information.
- Linux: various supplicants use their own configuration files, most being flat-file (`wpa_supplicant.conf`), some being XML-based (openSUSE "`sysconfig`").
- Other supplicants create files with opaque binary "blobs" that contain the EAP configuration information (e.g. Intel Pro/SET Wireless).

Furthermore, the richness of what can be expressed in these configuration formats varies widely between the various operating systems. One popular shortcoming is that an EAP identity is often tied to a specific network.

The Apple format, for example, requires the creation of a strict 1:1 mapping: one EAP configuration per SSID. It is not possible to define one EAP identity and express that it is valid for a whole set of wireless networks, or that it is also usable in a wired IEEE 802.1X context. This is not just a hidden nuisance: in Apple's case, it means that the user is asked for his username and password for each of the SSIDs in the profile, instead of typing it once for it to be applied to all those SSIDs automatically.

All major operating systems have developed these description languages for their internal purposes, but it is quite hard to observe similarities between them. One is under the impression that schema designers were interested in finding a quick solution to a given problem rather than a systematic and well-organised approach.

eduroam CAT was designed to cope with these many variants, and achieves that goal successfully. However, it was a natural thought to try and formalise the definition of EAP identities and their applicable uses in a well-thought-out and structured way, superior to the individual-device vendor approaches. A first attempt towards such a definition has been undertaken mainly as a proof of concept and basis of future work. The resulting XML Schema document definition is called the Generic EAP Metadata Profile.

2.2.3.2 Overall Approach

The minimal goal (as pursued by the proprietary approaches outlined above) would be to pass enough information so that an 802.1X network can be configured on the user's device. However, the developers' experience with CAT shows that more general needs should be covered.

Since installers configure the network for a particular institution, and possibly for a particular user group within the institution, the profile should be able to carry additional information that may be used during the installation process in an interaction with the user. For instance, an installer should tell the user that it is only meant to work for a particular group; the installer may display Terms of Use and require that the user accepts them; the installer may also use a logo image embedded in the profile to customise its appearance, etc.

Generic profiles could also be used as metadata for transporting configurations between configurations access systems like CAT.

2.2.3.3 *Specification Details*

Central to any 802.1X configuration is the EAP method setup. EAP has been defined in [RFC3748] in an abstract way, leaving specifics to definitions of particular EAP methods. Formally, each EAP method defines its own vocabulary and its semantics is strictly local, but in practice, many EAP methods employ similar concepts that can be easily mapped between them.

The current version of the Generic EAP Metadata Profile defines a vocabulary that covers all methods currently within the interest of eduroam. This vocabulary should be used to describe EAP configurations. It is recognised, however, that new EAP methods will be defined and they may require new concepts. It is therefore possible to add EAP method-specific terms to a configuration described by the Generic EAP Metadata Profile definition without the need to extend the original vocabulary. The preferred approach for a new method would be to use the existing vocabulary to the maximum and propose new terms only whenever really necessary. Subsequent methods could make use of this extended dictionary. Uncontrolled usage of method-specific vocabulary could quickly lead to the situation observed currently, and should be avoided.

Another container for uncontrolled vocabulary is the VendorSpecific tag. This will allow some additional options to be set which only make sense for particular devices or systems.

The proposed definition of the Generic EAP Metadata Profile is derived from CAT work, but is not limited to the functionality required by CAT. In particular, it is possible to pass full user credentials for each of the supported EAP methods. This, together with profile encryption, will allow full-scale enterprise user management and is expected to be useful far beyond eduroam.

The Generic EAP Metadata Profile is expected to be of use for several purposes, including:

- Setting up a predefined device (when the optimal EAP method can be pre-set before the interaction with the particular device).
- Setting up multiple types of devices, or devices that can appear under the same name but with differing requirements concerning EAP methods (leaving the selection of the optimal EAP method during the runtime of the installation).
- Transporting configuration parameters for one or many IdPs.

The Profile can carry information in various language variants. Depending on a particular scenario, the Profile can be crafted for a single or multiple languages.

2.2.3.4 *Usage Scenarios*

Immediate Installation of a Preselected Profile Directly onto a Device

Currently CAT supports devices in two ways. The first is to produce an installer program (an executable in the case of MS Windows or a combination of bash and Python scripts for Linux); the second (for Apple systems) is to produce an XML profile, which is automatically recognised and installed by the system. These installers are

prepared for a single institution or possibly even a single user group within an institution. The user downloads the entire installer and either executes it or lets the system use a default action.

Installation via External Application; Profile Selection via XML Download

The user needs to download a general installer “app” (possibly from an application store specific to a given operating system, e.g. Google Play store or Apple App Store). The installer app registers the Generic EAP Profile’s MIME type and/or file extension to itself. Then the user accesses the CAT Web interface to collect the generic profile customised for his institution. The installer should be executed automatically after the download of the profile completes and 802.1X connectivity will be configured.

Installation via Operating System; Profile Selection via XML Download

In this situation the operating system already recognises the Generic EAP Metadata Profile and it is enough to download the profile from CAT. The workflow is then similar to the current configuration of Apple systems via the mobileconfig configuration profiles. This approach requires that the Generic EAP Metadata Profile gains traction in the industry and will be integrated into typical operating systems.

2.2.3.5 File Format Details

The full XML Schema profile definition and an example of a resulting XML file are provided in Appendix B of this document.

The root element is the <EAPIdentityProviderList> tag, which contains a sequence of <EAPIdentityProvider> elements; these carry the actual installer information. In most practical applications, the <EAPIdentityProviderList> will contain only a single element; a longer list can be used for metadata transfers between systems.

As described above, the <EAPIdentityProvider> contains a number of general information tags such as <DisplayName> or <Description>, <ProviderLogo>, <TermsOfUse> and <Helpdesk>.

The <Helpdesk> element can list contact information via email, Web or phone, and can be marked with a language, so that the user can pick the best option (if provided by the home site).

The <ProviderLocation> element can store geographical coordinates of the Identity Provider. This can be used together with geolocation by systems like CAT to help find the best-guess institution for the current user. This element is therefore defined to carry this part of metadata but is not going to be used by the actual configurators.

The <VendorSpecific> tag can carry certain information which can be useful for a given operating system (or device), but most likely would be irrelevant for others. The <VendorSpecific> element may also appear at the <EAPMethod> level, which is discussed later in this section.

The <CompatibleUses> element is used to specify where the EAP identity can be used. Examples include which SSIDs are supposed to be configured and which encryption protocol, TKIP (WPA/TKIP) or CCMP

(WPA2/AES), should be used. The schema also supports the recent additions of IEEE 802.11u and can carry 802.11u consortium-related information. Further uses include the ability to specify that the identity is usable on wired IEEE 802.1X networks, and with further extensions can also cover more advanced uses like ABFAB / Moonshot authentication.

The key element is <AuthenticationMethods>, defined to be a sequence of <AuthenticationMethod> elements.

The <AuthenticationMethod> element specifies the EAP method and all of its parameters, such as trusted certificate authorities (for the server certificate), accepted RADIUS server names, outer identity, inner authentication method (EAP or non-EAP), etc. The set of configuration parameters depends on a particular EAP method. For instance, EAP-PWD [RFC5931] does not require any parameters at all; EAP-FAST is the only one supporting Protected Access Credential (PAC) provisioning. On the other hand, properties such as anonymous identity are common to several EAP methods.

<EAPMethod> specifies the EAP method identifier (according to the IANA EAP Numbers Registry [IANA-EAP]) and can additionally also specify method-specific and vendor-specific information.

The <InnerAuthenticationMethod> element defines the inner method for tunnelled EAP methods. It shares the property dictionary with the <AuthenticationMethod>.

The current complete dictionary related to authentication is shown in Table 2.4 and Table 2.5 below.

Server-Side Credentials

Property	Description	Used in EAP methods	Remarks
CA	CA certificate (root or intermediate) – server certificates issued within this tree will be trusted	ALL except PWD	
ServerID	Server name as in the server certificate – these names will be trusted	ALL except PWD	

Table 2.4: Authentication dictionary: server-side credentials

Client-Side Credentials

Property	Description	Used in EAP methods	Remarks
AnonymousIdentity	User name used for RADIUS request routing	TTLS, PEAP, FAST	Optional; if not present, the actual user name will be used
ProvisionPAC	Method of provisioning PAC files to clients	FAST	

Property	Description	Used in EAP methods	Remarks
UserName	The actual user identity, for tunnelled EAP methods used inside the protected tunnel, this parameter is usually provided by the user at installation or login time, but may also be supplied within a configuration profile	ALL	Only used in per-user configurations
Password	Either the user password for password-based EAP methods or personal private key password for TLS, this parameter is usually provided by the user at installation or login time, but may also be supplied within a configuration profile	TTLS, PEAP, FAST, PWD, TLS	Only used in per-user configurations
PAC	Protected Access Credential token, specific to EAP-FAST	FAST	Only used in per-user configurations
ClientCertificate	Client Certificate and private key pair specific to EAP-TLS	TLS	Only used in per-user configurations

Table 2.5: Authentication dictionary: client-side credentials

2.2.3.6 Internationalisation Considerations

Several elements within the Generic EAP Metadata Profile may have multiple language variants. <DisplayName>, <Description>, <TermsOfUse> are obvious examples, but elements of <Helpdesk> can also point to different information resources depending on the language setting.

When the Generic EAP Metadata Profile is used within CAT, it is expected that the user will select a language and then the profile will be prepared for this setting. It may happen that the system does not contain values for a particular selected language; in this case, default values will be used instead. The most likely situation is that institution administrators will configure specific values for all languages that are common in their country, and additionally a default value in English. A user may pick the installer language from a wider selection, and when a non-configured language is picked, the default (most likely English) values will be used. For instance, a Polish student studying at a German university will probably pick a Polish version of an installer. Most likely, the institution administrator has not defined Polish variants. As a result, the installer downloaded by the user will show nearly all text in Polish; only some local names may appear in English. The user experience will be much better in comparison to being forced to use an installer in a foreign language.

2.2.3.7 Security Considerations

The Generic EAP Metadata Profile is a crucial security setting. Tricking a user into installing a manipulated profile could result in exposure of user credentials. This is why the profiles must be signed, the signature must be checked by the user system, and the result must be displayed in a comprehensible way.

At the moment, signing of the profile has not yet been introduced or defined. Future work regarding the Generic EAP Metadata Profile includes specifying mandatory-to-implement signature checking (either via S/MIME document signatures or XMLDSig signatures).

2.2.3.8 Further Plans for Implementation, Deployment and Wider Industry Support

The specification of the Generic EAP Metadata Profile has been developed entirely inside GN3 JRA3 T1 and has not yet been submitted to a standardisation body. However, the general concept of it has been discussed in private conversations at IETF meetings. The result is that while such a format is useful, there is likely to be some resistance from some parts of the wireless access industry, most importantly from consulting services that currently derive business from making the “complex” EAP / IEEE 802.1X configuration “simple” in a Bring Your Own Device (BYOD) context. A configuration format that simply makes things simple will have a detrimental effect on the profitability of such consulting businesses.

Because of that, the action plan includes the creation of at least two device implementations that make use of the Generic EAP Metadata Profile, to prove that the concept works and can be implemented with little effort on real-world devices. The two targeted platforms to demonstrate the client side (consumption of Generic EAP Metadata Profiles) are:

- An Android 4.0 application, which will be made available on the Google Play store.
- A Linux installer; which will be lobbied to be included in mainstream Linux releases.

Simultaneously, the implementation of the server side (creation of Generic EAP Metadata Profiles) will be demonstrated by CAT; the development branch of the CAT system already contains an implementation of a “generic” device which produces Generic EAP Metadata Profiles in various configurations. This is a nucleus, enabling more installer implementations.

Finally, the file format will be submitted to the IETF in its Operations & Management (O&M) area, either directly in its O&M discussion slots or in the more specific Operations & Management Area working group (OPSAWG).

2.2.4 eduroam Consortium and Architecture Description

In terms of participating IdPs, eduroam is the biggest roaming consortium utilising IEEE 802.1X, EAP and RADIUS in the world. eduroam operators have repeatedly been asked to create a summary document listing the principal architecture, lessons learned, and future plans for the consortium. Since most of the technologies used in eduroam are IETF ones, such a document should naturally be published within the IETF.

Following these arguments, an individual draft has been submitted to the IETF, “The eduroam architecture for network roaming” [EDU-IETF]. When finished, it is going to be a concise summary description and starting point for external entities wanting to learn about eduroam.

The document also includes the various design decisions taken by eduroam, as reported in earlier editions of this deliverable, particularly the use of Operator-Name, Chargeable-User-Identity and the privacy-preserving combination of the two (see also Chapter 3 of [DJ3.1.1] and Section 2.2.2 of [DJ3.1.2,1]).

2.2.5 Cryptographic Enhancements to the EAP-PWD EAP Type

As mentioned in Section 2.1.1.4, the EAP type EAP-PWD has potential for improvement in a few areas. In cooperation with the original authors of EAP-PWD, members of JRA3 T1 are seeking to explore which improvements are useful, and to work on a specification that will update the original RFC [RFC5931].

The areas under investigation include:

- Which password storage representations are in common use?
- Are improvements to the problem of information leakage regarding non-existing usernames useful?

A draft specification is currently being worked on, but has not been released at the time of writing this deliverable.

3 eduroam Infrastructure Enhancements

3.1 Usability Study of the Diameter Protocol

eduroam Operations is exclusively using the RADIUS protocol (in various transport profiles, e.g. RADIUS/ User Datagram Protocol (UDP) [RFC2865] and RADIUS/TLS [RFC6614]) for inter-domain authentication communication. However, as per the IETF specifications, the Diameter protocol (originally specified as [RFC3588], later revised as [RFC6733]) was intended to replace RADIUS as a more efficient and more secure transport protocol for EAP and IEEE 802.1X.

eduroam R&D has evaluated and kept monitoring the landscape of Diameter implementations to find possible upgrade paths from RADIUS to Diameter since the early days of the eduroam service. An enthusiastic early evaluation of the protocol itself was conducted in Chapter 2.1 of [GN2-DJ5.4.1]; a later, much more sober, evaluation of the then-available implementations followed in Chapter 2.1 of [GN2-DJ5.1.6] in April 2008. The conclusion at the time was that the protocol would very likely not be of any use during the GN2 lifetime and probably for some time after, but that the situation should continue to be monitored.

During the fourth year of GN3, five years after the initial evaluation, another round of tests of available implementations took place. The idea of this activity was to identify and test evolved Diameter protocol implementations for potential future use in the eduroam service.

3.1.1 Available Implementation Overview

The Diameter protocol is adopted most by 3rd Generation Partnership Project (3GPP) and 3GPP2 standardisation bodies for Authentication, Authorisation and Accounting (AAA) in IP Multimedia Subsystems (IMSs) of mobile networks. A lot of commercial implementations of Diameter have a main goal to fulfill the requirements for mobile IMS functions and interfaces. Therefore, just a few of these have support for RFC 4072 – EAP [RFC4072]. Since eduroam is built with EAP as a cornerstone, an evaluation of Diameter servers without EAP support does not make sense.

Table 3.1 and Table 3.2 below summarise the Diameter implementations identified to date that support EAP.

Servers

Server	EAP Support
freeDiameter	Supports EAP
WIRE Diameter (based on Open Diameter)	According to the product documentation, supports EAP: EAP-TLS, EAP-TTLS, PEAP. However, not yet/could not be tested by JRA3 T1.
Radiator	Supports EAP; functions as Diameter to RADIUS gateway
Lucent AAA Server	According to the product documentation, supports EAP. However, not yet/could not be tested by JRA3 T1.
Novi diam tieto	According to the product documentation, supports EAP [TIETO]. However, not yet/could not be tested by JRA3 T1.
Traffix – sdc server variant	According to the product documentation, supports EAP. However, evaluation not available.

Table 3.1: Diameter implementations: servers

Out of those, freeDiameter and Radiator were the only implementations that could be evaluated thoroughly. The other implementations were either commercial and did not supply evaluation versions of their product, or were largely defunct. The following implementations may have EAP support, but could not be verified to have it: Diametriq Routing Engine, Novi Diameter AdvOSS.

APIs / Libraries

In addition to fully-featured server implementations, a number of Diameter libraries and APIs are also available:

Server	Type	EAP Support
Open Diameter	API	According to the product documentation, supports EAP. However, compilation failed due to ancient libACE requirement.
Marben	API	According to the product documentation, supports EAP. However, not yet/could not be tested by JRA3 T1.
Radvision IMS	Diameter Protocol Stack	Does not support EAP
Signalware Diameter	API	Does not support EAP (judging by data sheet)

Server	Type	EAP Support
Metaswitch networks Diameter	Stack	Does not support EAP
Calsoft Diameter NASREQ and SIP Applications	API	According to the product documentation, supports EAP. However, not yet/could not be tested by JRA3 T1.
Traffic Openblox	API (free)	Minimal EAP support
Diametriq accelero	API	According to the product documentation, supports EAP; free trial possible
Jboss communication platform	Stack	EAP support unclear
CdiameterPeer module	API	No EAP support

Table 3.2: Diameter implementations: APIs/libraries

To send Diameter requests to a Diameter server, it is necessary either to use RADIUS devices and a RADIUS-to-Diameter translation agent, or to find native Diameter Network Access Server (NAS) devices.

Network Access Server Devices

No NAS devices with Diameter support were found.

Implementation Conclusions

Of all Diameter implementations, freeDiameter, Radiator and Lucent AAA 8950 servers provided a promising list of features that could be useful in an eduroam context. Therefore, further evaluations focused on these servers.

3.1.2 Evaluation of freeDiameter, Radiator

3.1.2.1 Installation

Dependencies

- flex
- bison
- lksctp-tools* (i.e. lksctp-tools, lksctp-tools-devel)
- libgcrypt, libgcrypt-devel
- gnutls, gnutls-devel
- mercurial

- cmake
- gdb
- python-devel
- swig
- libidn* (i.e. libidn11, libidn-devel, libidn-tools)

Compilation

```
hg clone http://www.freedometer.net/hg/freeDiameter
mkdir fDbuild
cd fDbuild
cmake <flags> ../freeDiameter/
```

3.1.2.2 Configuration and Testing

Starting the service:

```
freeDiameterd -c putanja_do_conf_fajla
```

If the following error occurs during the first start of the service:

```
freeDiameterd: error while loading shared libraries: libfdproto.so.4: cannot
open shared object file: No such file or directory
freeDiameterd: error while loading shared libraries: libfdcore.so.4: cannot
open shared object file: No such file or directory
```

Then a soft link of this library in /lib/ needs to be created.

3.1.2.3 Scenario 1: Echo Test

This is a test of simple communication between two servers with echo messages, as described in [freeDiameterTest1].

This test was executed and succeeded.

3.1.2.4 Scenario 2: RADIUS-to-Diameter, Proxy to Backend Server

This is a more complex test case where two instances of freeDiameter are involved: one acts as a RADIUS-to-Diameter gateway and proxies the request to the second instance, which performs the EAP authentication and sends the result back. This test case is described in [freeDiameterTest1].

To initiate the (RADIUS) EAP conversation, the open source tool “eapol_test” (part of “wpa_supplicant”) was used.

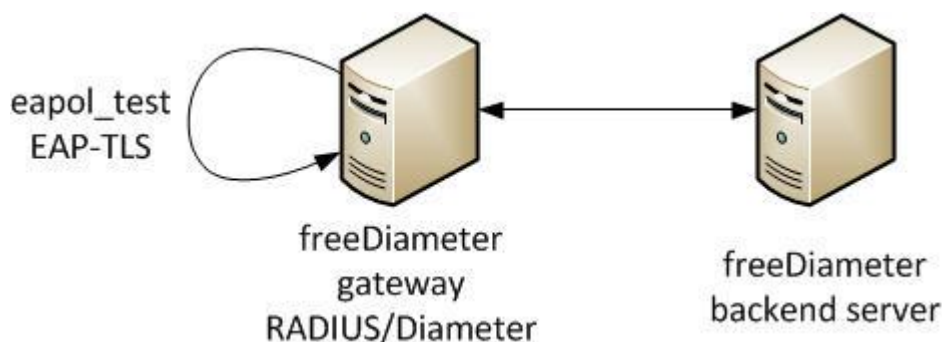


Figure 3.1: Setup for Scenario 2

The following command starts the server:

```
freeDiameterd -c /root/conf/freeDiameter/freediameter.conf
```

(where /root/conf/freeDiameter/freediameter.conf is the path to the freediameter.conf file).

During the tests, it surfaced that EAP-TLS was the only authentication that was successful. After querying, the freeDiameter developers claimed that an EAP-TTLS implementation exists (student work). However, an evaluation of that EAP-TTLS module was not possible, because it required undocumented configuration directives in the configuration file, which could not be determined.

3.1.2.5 Scenario 3: Radiator Proxy between Two Diameter Servers

Radiator software is an implementation of the RADIUS protocol, and it is used widely in the eduroam community. Radiator has support for Diameter as a gateway to RADIUS. However, testing of the following scenario (proxy chain freeDiameter -> Radiator -> freeDiameter) was not successful. The reason is that in the initial communication between Radiator and freeDiameter, Radiator does not advertise support for the EAP protocol in the Diameter “Capability Exchange Request” (CER) exchange. As a consequence, EAP authentication requests are not transmitted between freeDiameter and Radiator.

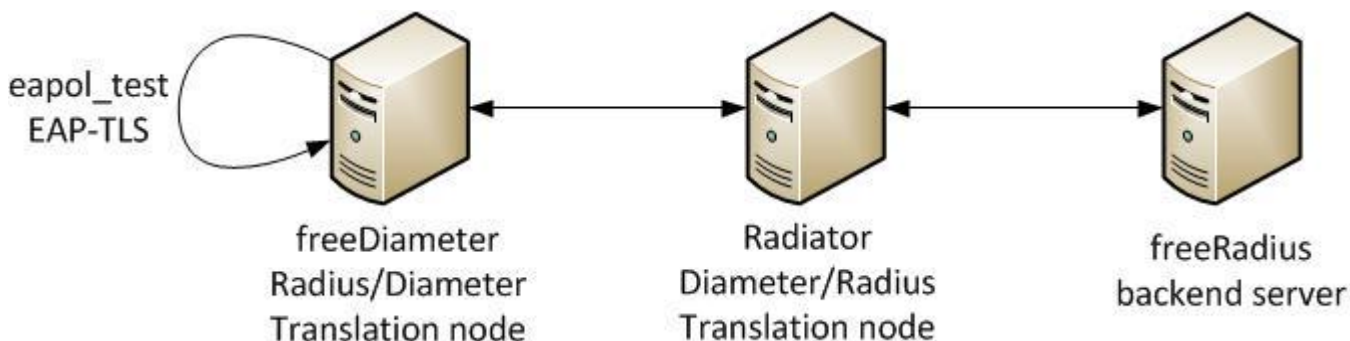


Figure 3.2: Setup for Scenario 3

3.1.3 Open Diameter and WIRE Diameter

Open Diameter is merely an API for Diameter functions. This API is used by WIRE Diameter to build an actual Diameter server. According to its specifications, this server then has support for EAP-TLS, EAP-TTLS, PEAP, etc. However, installation of Open Diameter was not successful as the project ended in 2005 and the last version only works with specific old versions of libraries (ACE, boost, etc.) that cannot be installed any more on contemporary Linux/Unix systems with a reasonable effort.

3.1.4 Summary

Several years have passed since the last evaluation, and the implementation landscape of Diameter has had much time to improve the existing products, and to create new ones. And yet, no single Diameter server could be identified that provides the essential functionalities for eduroam: support for a few popular EAP types, and the ability to proxy EAP authentication requests among several servers.

It appears that the use of Diameter for EAP authentication in general and eduroam in particular is a dead end for the immediate and mid-term future, and that Diameter remains a protocol with exclusive use in the 3GPP/LTE provider area.

However, it may well be possible that these providers will, at some point, push for improved usability of Diameter with EAP due to the rollout of data offload with IEEE 802.11 Interworking (see Section 2.1.2.2 above) and Hotspot 2.0, which is currently beginning and which would result in more usable implementations.

In the light of the possibility of more positive developments, the Diameter implementation landscape should continue to be monitored with a low priority.

3.2 RADIUS/TLS Deployment

RADIUS/TLS, meanwhile, is in widespread use in eduroam. There are more than ten countries that use a RADIUS/TLS uplink to the European top-level RADIUS servers; about ten countries perform dynamic discovery with DNS Name Authority Pointer (NAPTR) lookups; and at least four countries are known to publish the corresponding NAPTR records for a significant fraction of their IdPs.

These deployments use Education Public Key Infrastructure (eduPKI) certificates, as reported in previous editions of this deliverable. An investigation of alternatives to using a PKI, including the possible use of DNS-based Authentication of Named Entities (DANE), is currently ongoing. The first results of this investigation will be presented at the TERENA Networking Conference 2013 (TNC2013).

3.3 eduroam Configuration Assistant Tool (CAT)

For a general discussion on the purpose and scope of the eduroam Configuration Assistant Tool (CAT), see Chapter 3.5 of the previous edition of this deliverable [DJ3.1.2,2].

At the time of writing the previous edition of this deliverable (Q4 2011), many of the core functionalities of eduroam CAT were already developed, but significant amounts of work were still required for full integration into the eduroam operational environment. The following areas were worked on and completed since DJ3.1.2,2:

- Start page.
- Federation administrator management pages.
- Integration with eduroam database.
- Federated authentication (including eduGAIN).
- Integration with and expansion of Dynamic Discovery test tool.
- EAP-PWD support added.
- Linux installers.
- Streamlined access to installers.
- Resolution of open issues.
- IdP Administrators Manual.
- Transfer to production use.

Each of these is described below. The section ends with a summary of further plans.

3.3.1 Start Page

The CAT start page received a new user-centric look. Several layouts were proposed and the winning design (Figure 3.3) was chosen in a vote.

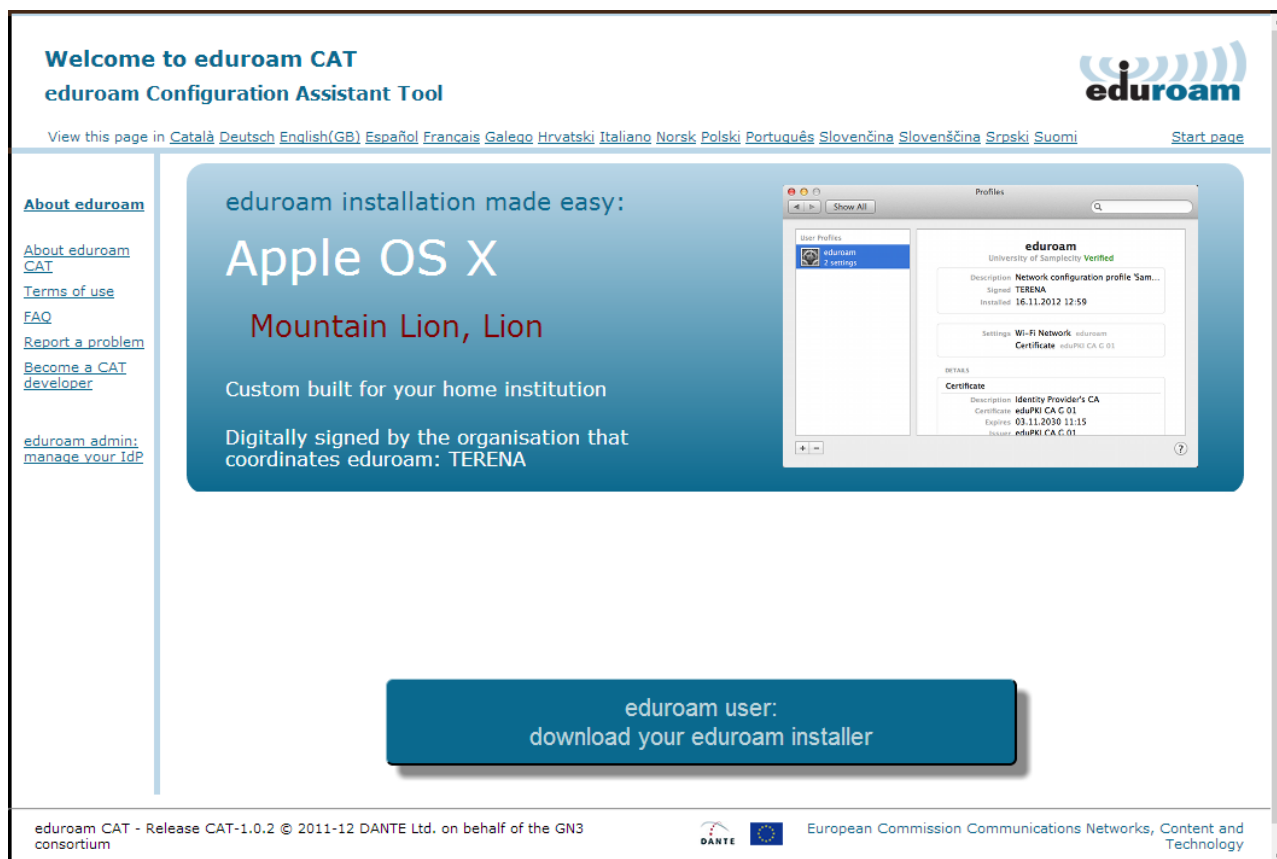


Figure 3.3: CAT: new home page

eduroam configuration is not just about running an installer. The user should be told which username and password to use, and in some cases more detailed instructions may be required. It is possible to configure such additional instructions, both EAP-type specific and device specific, and display them to the user just before the download. Figure 3.4 shows how such instructions are displayed after the user has clicked the MS Windows 7 download.

Select the user group


NCU temporary staff members

If you encounter problems, then you can obtain direct assistance from you home organisation at

WWW: <http://eduroam.umk.pl>

email: eduroam@umk.pl

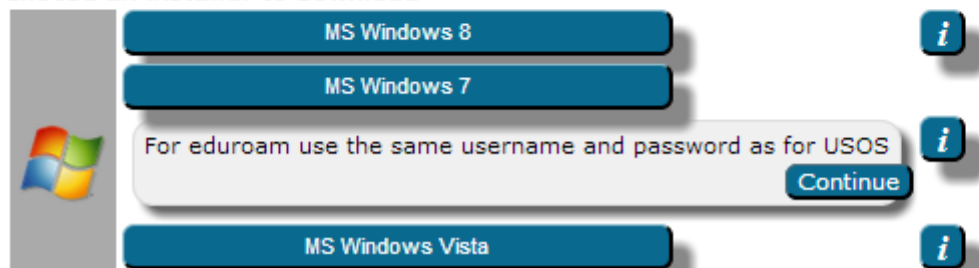
Choose an installer to download


Figure 3.4: CAT: detailed instructions for MS Windows 7 installer

3.3.2 Federation Administrator Management Pages

A separate overview is provided for eduroam CAT users who have the privilege of being a federation administrator for one or more federations. Federation administrators can create new IdPs and invite the primary administrator, add further administrators, and take control of orphaned IdPs if need be. The process of invitation by the federation administrator obsoletes the initial self-service enrolment page that was shown in DJ3.1.2,2.

The federation administrator is also responsible for maintaining the mapping of eduroam CAT data to the official eduroam database data (see Section 3.3.3 below).

Figure 3.5 illustrates the federation administrator interface.



Figure 3.5: CAT: Federation administrator interface

3.3.3 Integration with eduroam Database

The eduroam database is the authoritative source of participant information, on both a technical and an administrative level. eduroam CAT required tight integration with the existing eduroam database to be of maximum use for eduroam administrators, and avoid duplication of information.

One of the issues to overcome was the fact that the eduroam database does not contain unique and persistent identifiers for registered IdPs and SPs. The lack of such identifiers made it difficult to identify the same participant in the eduroam database vs. the eduroam CAT database. This required a mapping between participants in both databases by the federation administrator (who can use manual verification means, such as comparing the names of participants). The eduroam CAT federation administrator interface thus now contains two means to explicitly link CAT data to the corresponding eduroam database entry:

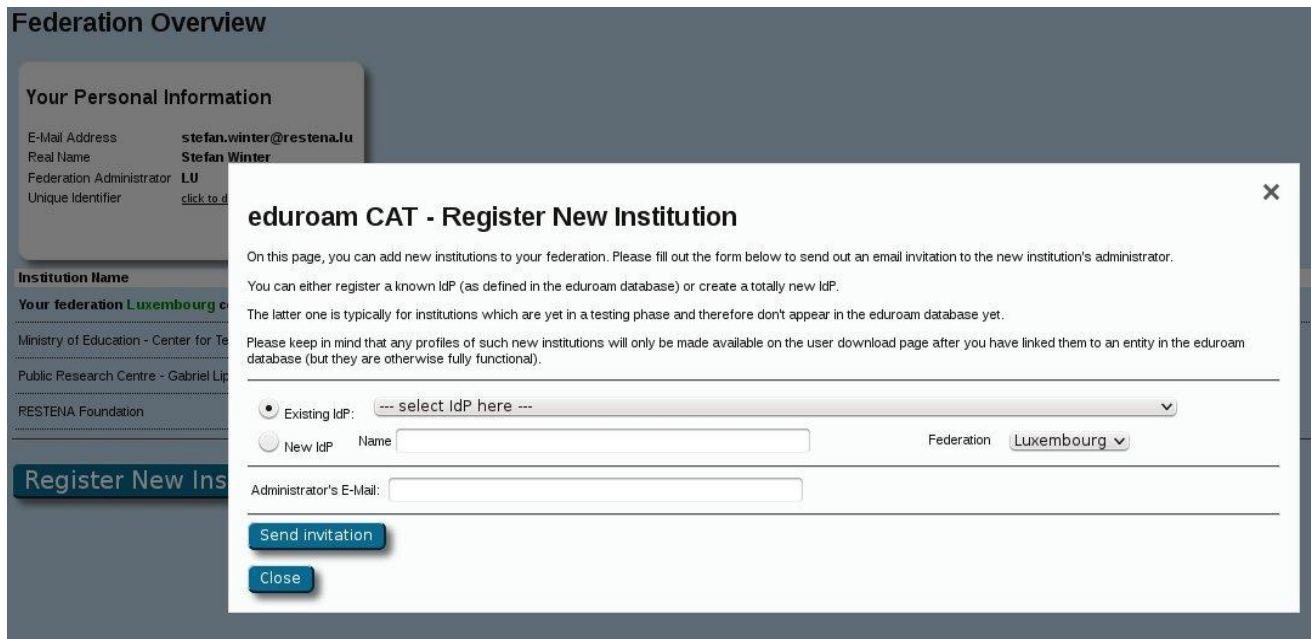
- Specify the institution mapping when inviting a new IdP administrator.
- Create a separate management page to map details at any time.

Each of these is described below.

3.3.3.1 Specify the Institution Mapping when Inviting a New IdP Administrator

When sending out an invitation to a new administrator, the federation administrator can either type in a new free-text name for an institution (no mapping to an existing eduroam database entry) or select a known institution from the eduroam database's list of IdPs in the federation. The ability to create unmapped, new

entries was seen as a vital option: eduroam CAT's installers are probably most useful while a new IdP is in the process of bootstrapping its service. However, it will not be listed in the official eduroam database until the bootstrapping process is complete, hence the requirement for the federation administrator to be able to add unlisted institutions manually. Figure 3.6 below shows the Register New Institution window, where both options are available.



Federation Overview

Your Personal Information

E-Mail Address: stefan.winter@restena.lu
 Real Name: Stefan Winter
 Federation Administrator: LU
 Unique Identifier: [click to d](#)

Institution Name

Your federation Luxembourg c

Ministry of Education - Center for Te

Public Research Centre - Gabriel Lip

RESTENA Foundation

Register New Institution

On this page, you can add new institutions to your federation. Please fill out the form below to send out an email invitation to the new institution's administrator.

You can either register a known IdP (as defined in the eduroam database) or create a totally new IdP.

The latter one is typically for institutions which are yet in a testing phase and therefore don't appear in the eduroam database yet.

Please keep in mind that any profiles of such new institutions will only be made available on the user download page after you have linked them to an entity in the eduroam database (but they are otherwise fully functional).

☒ Existing IdP: --- select IdP here ---

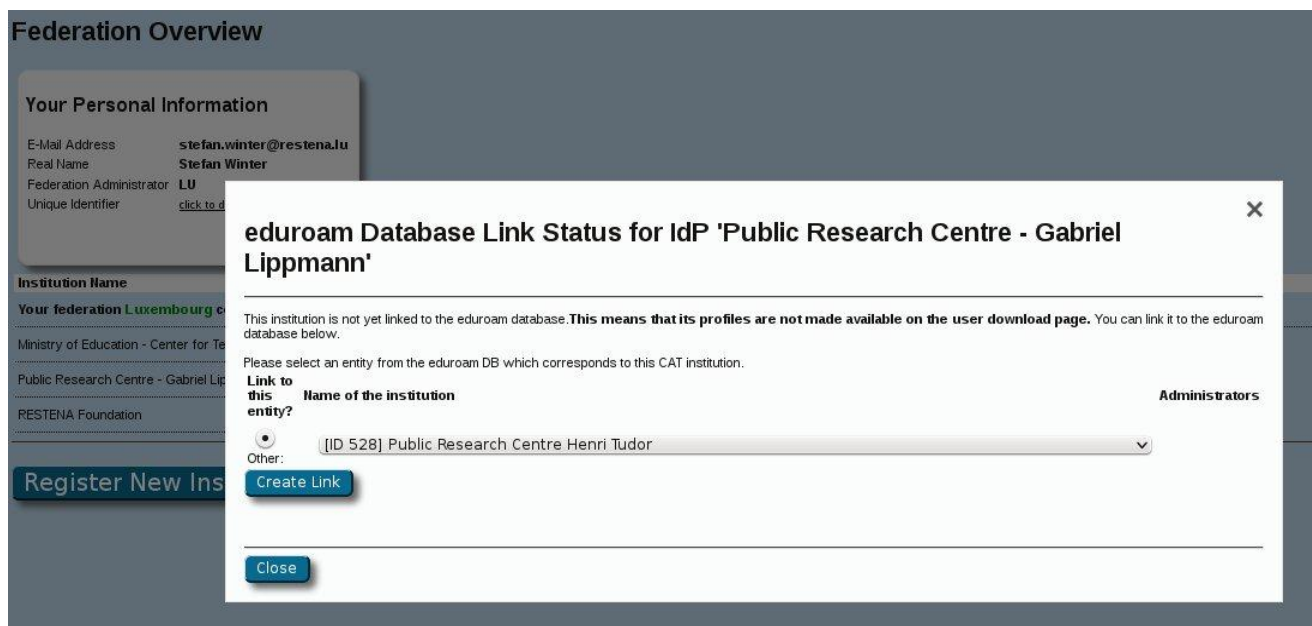
☐ New IdP Name: Federation: Luxembourg

Administrator's E-Mail:

Figure 3.6: CAT: registering a new institution – unmapped and mapped options

3.3.3.2 Create a Separate Management Page to Map Details at any Time

For institutions for which no mapping is known, the federation administrator can create a separate management page which allows the institution details to be mapped at any time. This is typically useful if a bootstrapping IdP has completed the eduroam joining process and is now listed in the eduroam database. Figure 3.7 below shows an example of the management page.



Federation Overview

Your Personal Information

E-Mail Address: stefan.winter@restena.lu
 Real Name: Stefan Winter
 Federation Administrator: LU
 Unique Identifier: click to d

Institution Name

Your federation Luxembourg c
 Ministry of Education - Center for Te
 Public Research Centre - Gabriel Lip
 RESTENA Foundation

Register New Ins

eduroam Database Link Status for IdP 'Public Research Centre - Gabriel Lippmann'

This institution is not yet linked to the eduroam database. This means that its profiles are not made available on the user download page. You can link it to the eduroam database below.

Please select an entity from the eduroam DB which corresponds to this CAT institution.

Link to this entity? **Name of the institution** **Administrators**

Other: [ID 528] Public Research Centre Henri Tudor

Create Link

Close

Figure 3.7: CAT: management page for mapping an institution at any time

3.3.4 Federated Authentication (including eduGAIN)

Even though eduroam CAT has a public download area for end users (where they can download their installers), access to the administrator area of eduroam CAT is restricted, and administrative users need to be authenticated.

eduroam CAT also needs to determine proper authorisation in the administrative interface: some users are federation administrators and are authorised to enter more sensitive areas than other users.

In consultation with the eduroam Operations Team (OT), it was decided that the authentication and authorisation of administrative users should happen on a more generic level than for eduroam CAT only: various other resources (such as the Web interface to the eduroam database, various on-demand test tools, etc.) also have the same authentication and authorisation needs.

As a consequence, eduroam OT created a federated authentication endpoint (“eduroam SP proxy”) which serves as a front end for all services in need of administrative user authentication. eduroam CAT makes use of that SP proxy by using the SAML 2.0 protocol and by using the eduroam SP as the single Identity Provider. The eduroam SP proxy in turn has multiple authentication sources configured, among them being the official eduGAIN IdP list, several experimental IdPs, and numerous social identity providers (Google, Facebook, etc.) for those who do not have an eduGAIN credential. Determining authorisation levels is a task for eduroam OT; the authorisation level can be extracted by eduroam CAT from an authorisation database.

The eduroam SP proxy follows best practices for federated authentication; in particular, it requires only an opaque unique identifier of a user, not any personal data. The release of further personal data such as email

address is beneficial for the user though. For further details about the eduroam SP proxy authentication system, readers are encouraged to contact eduroam OT.

3.3.5 Integration with and Expansion of Dynamic Discovery Test Tool

DJ3.1.2,2 reports on the Dynamic Discovery test tool in Section 3.3. This tool has now been integrated into eduroam CAT: since the RADIUS realm is among the information that administrators are asked to provide inside eduroam CAT anyway, and since that realm information is the only input required for the test tool, it is easy to link an eduroam IdP profile with the corresponding test page.

The test tool is now tightly integrated into IdP management (see Figure 3.8 below).

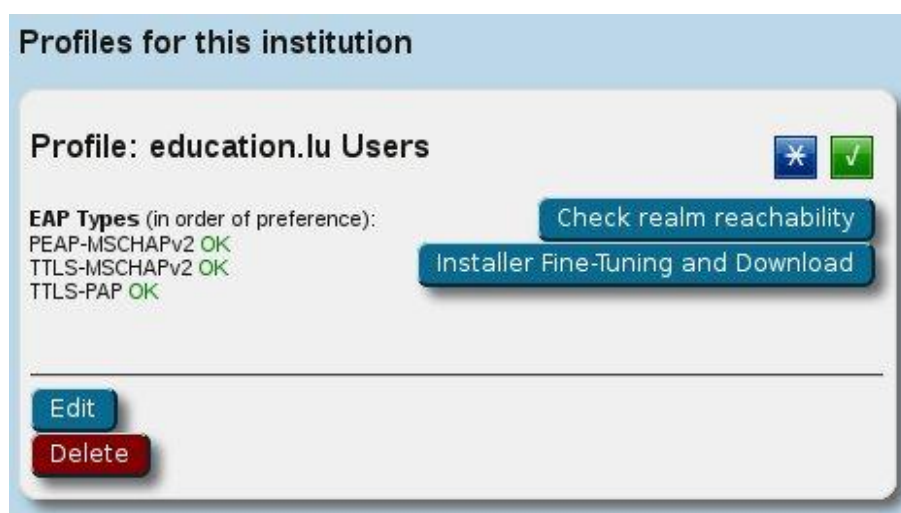


Figure 3.8: CAT: integrated Dynamic Discovery test tool

The tool was also expanded significantly in terms of the thoroughness of the checks that are performed. Since eduroam CAT is in possession of more information than the mere realm of an IdP, it can perform a number of checks by faking a login operation and seeing whether it succeeds, or at which points the login fails.

For the dynamic discovery tests, the TLS connectivity checks were expanded so that eduroam CAT will present a number of client certificates, a mix of good and bad ones, and will check whether the contacted server will only accept all the valid and accredited certificates, and reject all invalid and not accredited ones. An example output of these very thorough TLS checks is shown in Figure 3.9 below.

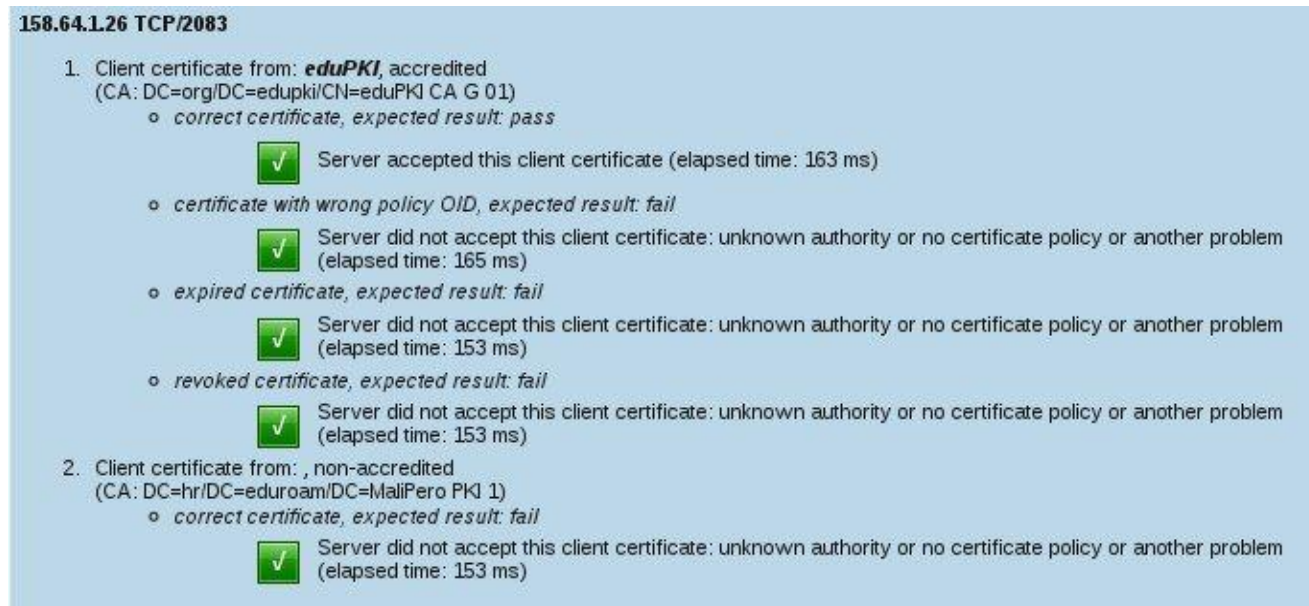


Figure 3.9: CAT: expanded TLS connectivity checks

3.3.6 EAP-PWD Support Added

With the release of a Windows supplicant for EAP-PWD by Aruba Networks, and an accompanying licence which allows eduroam Operations redistribution, it was possible to add support for EAP-PWD in eduroam CAT. IdP administrators who have enabled EAP-PWD in their RADIUS server can now create Windows installers for that EAP type with eduroam CAT.

3.3.7 Linux Installers

Linux installers have been fitted with a simple Graphical User Interface (GUI). They have been tested in all major distributions and work properly in most of them. The installer interfaces with Network Manager, and therefore is currently restricted to systems that base their network management on this tool. Two sample screenshots are provided in Figure 3.10 and Figure 3.11 below.

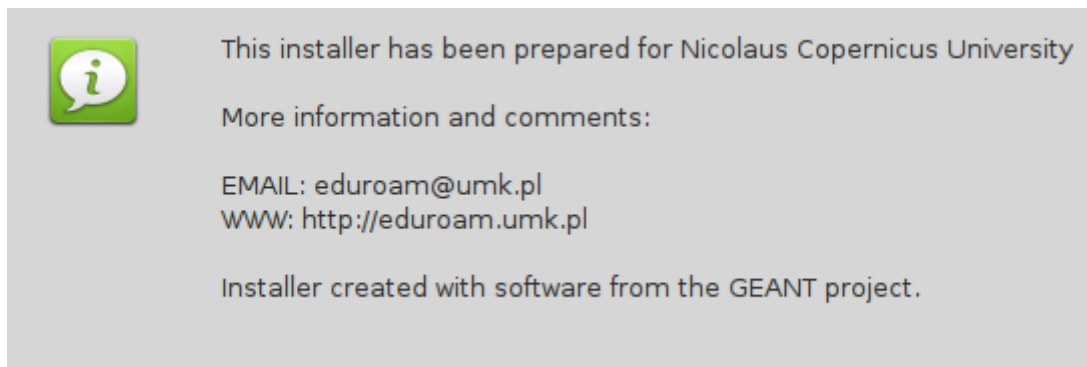


Figure 3.10: CAT: Linux installer #1

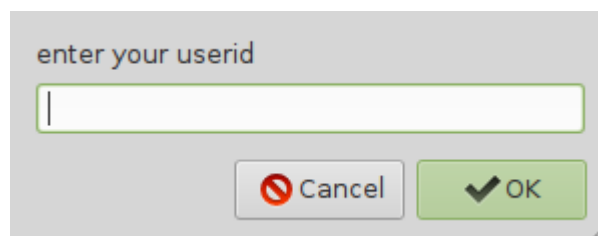


Figure 3.11: CAT: Linux installer #2

3.3.8 Streamlined Access to Installers

The IdP administrator interface of eduroam CAT now generates links that point directly to the end-user download area of a given profile. This is beneficial for institutions that want to send users from their local support pages to the download area, but want to avoid the user-interactive discovery process. The link is presented both as a simple plain-text https link and also as a Quick Response (QR) tag for administrators who want to include the installation instruction download link in promotional material for direct consumption with smartphones (e.g. in posters).

The interface also includes a per-profile download counter, which enables an administrator to see how many end users have actually downloaded an installer from eduroam CAT's Web page. Figure 3.12 illustrates this new functionality.



Figure 3.12: CAT: per-profile download counter

3.3.9 Resolution of Open Issues from DJ3.1.2,2

DJ3.1.2,2 Section 3.5.9 lists three significant open issues to be resolved before a release. All of these issues have since been resolved.

- EAP-TLS is now a supported EAP type. Users are NOT expected to upload their private key, in either encrypted or cleartext form. Instead, installers expect either that the client certificate is already installed on the target system (e.g. the browser certificate store) or that the client certificate is stored on the target system in a specific filename. These assumptions may fail, and investigations on how to improve EAP-TLS inside eduroam CAT are ongoing.
- Installer caching. eduroam CAT now keeps all previously generated installers on file. Installers are generated for 3-tuples: language, device, profile. If a user selects a previously generated installer for this 3-tuple, the cached installer is served immediately. For the CAT installation administrator, there is a minimal interface that allows cached installers to be flushed if something goes wrong or if the code base is updated.
- User instructions. The end-user download page now features an “Information” button in addition to the download button, which explains installation details to the users.

3.3.10 IdP Administrators Manual

With the growing complexity of the eduroam CAT software, it became important to provide good documentation for eduroam IdP administrators. A complete eduroam IdP administrator manual for eduroam CAT was created and is available at [CAT-MAN].

3.3.11 Transfer to Production Use

eduroam CAT was officially transferred to production use on 25 March 2013. It is now accessible for eduroam administrators and end users at the following URL: <https://cat.eduroam.org>.

The version that is currently in use on the production instance is running software version CAT-1.0.2 with three hotfixes (eventually to become CAT-1.0.3). The developers of eduroam CAT are standing by for maintenance of this version and for development of subsequent new feature releases. Manpower for these maintenance and development activities has been secured for the GN3plus project.

3.3.12 Further Plans

The development of eduroam CAT has shown that there is a significant need for support tools that help eduroam federation operators, Identity Providers, Service Providers and end users in their day-to-day activities. eduroam CAT can serve as the nucleus for a larger support system. See Section 5.1 *eduroam Operations Support Services (OSS)* in Chapter 5 *Recommendations for Long-Term Work* below for further details.

4 Coordination with Other Activities

4.1 eduroam Finland: Case Study on Statistics of Reasons for Failed Authentications on a National Level

4.1.1 Introduction

eduroam authentication servers, particularly the national and regional proxy servers, process a mix of successful and failed authentications. The rate of success vs. failure is approximately 1.5 : 1. While this may look suspicious to a casual observer, it is not an alarming state: devices that are misconfigured will attempt to connect with the wrong settings over and over again, while a successful login is just one transaction, i.e. the failed authentications, whatever their cause, are significantly over-represented in statistics.

However, there may still be something to be learned from examining the pool of failed authentications. One national eduroam operator, CSC/Funet in Finland, has conducted an in-depth examination of failed authentication traffic.

4.1.2 Investigation of Failed Authentication Attempts and their Reasons

The failed authentication attempts from the Finnish RADIUS root servers were analysed in order to better understand how many users suffer from not being able to log into eduroam smoothly while visiting another campus. The idea was also to try to categorise why the authentication attempt failed.

The maintenance of the Finnish RADIUS root servers, `ftlr.funet.fi` and `ftlr2.funet.fi`, is outsourced to a company named Arch Red. For this investigation, Arch Red provided the log files from 13.5.2011 to 16.4.2012. This dataset is the basis for the observations below.

First the numbers of successful and failed authentication attempts were checked; the result is shown in Table 4.1.

Time Period	Successful Authentications	Failed Authentication Attempts	All
13.05.2011-16.04.2012	1,033,942	613,768	1,647,710

Table 4.1: Successful and failed authentications

The total number of failed authentication attempts does not show how many different devices tried to authenticate without success, and how many times. Failed authentication attempts from one user, over a short period of time, can be considered as one failed authentication “session”, although it generates several individual failed authentications in the log files. It is not possible to determine deterministically how many different users were failing to authenticate; this is because anonymous outer identities may conflate several different users into one observed identity. However, a look at the dataset reveals that anonymous outer identities are very rarely used – in almost all cases the real username is used also as outer identity.

By removing duplicates (by counting the same outer identity as one single user) it can be seen that during the observed time period only 88,809 different outer identities failed authentication attempts. Compared with the overall failure count of 613,768, this means that one single misconfigured user device generated an average of approx. 7 failed authentication attempts.

Further drilling down into the dataset revealed that very few misconfigured devices can generate much more than this average: one outer identity, xyz@ad.pax.fi, had generated a total number of 63,041 failed authentication attempts during the observed time period. The misconfiguration for this case could be identified rather easily: the correct realm to use would be @pax.fi, not @ad.pax.fi.

In a second phase, the complete set of failed authentications was then analysed to find possible reasons for the failed authentication. In cases like the above, the failure reason is the use of a wrong realm by the end user; other, more sophisticated failure reasons could also be identified. Table 4.2 below shows the full set of failure reasons – or classes – evaluated.

Failure Class	Explanation
unknown/timeout	This class conflates two cases: for Finnish realms, a known realm is trying to be contacted, but does not reply (timeout); for non-Finnish realms, international authentication indicates authentication failure due to unknown realm.
loop	An organisation sends authentication attempts with one of their own realms to the server.
proxied	The authentication was proxied to a known destination, and rejected. This class includes realms like 3gppnetwork.org which are not eduroam members.
malformed-1	The RADIUS User-Name attribute contains invalid characters (not proper UTF-8 text).
malformed-2	The username does not contain invalid characters, but is otherwise malformed. This class includes, for example, authentication attempts with “guest@guest” given as

Failure Class	Explanation
	username, and usernames without any realm (no @ sign).
malformed-3	The authentication attempt has included spaces or other forbidden characters, for example “=”.
unknown-FI	The realm part ends with .fi but no Finnish organisation with that realm exists in eduroam.

Table 4.2: Authentication attempt failure classes

Out of these classes, two deserve particular attention.

- loop, because it is a genuine infrastructure error (i.e. not caused by wrongly configured supplicants in end-user devices, but caused by one or more RADIUS servers that transport the authentication).
- unknown/timeout, particularly timeouts from known organisations within the own country. These should be contacted because their infrastructure is not responding (“down”).

The numbers of failed authentication attempts per class is shown in Table 4.3.

unknown/ timeout	loop	proxied	malformed-1	malformed-2	malformed-3	unknown-FI
124,867	7,8091	255,549	6,469	13,943	37,905	96,944

Table 4.3: Numbers of failed authentication attempts per class

The failed authentication attempts were then further analysed per class.

Class	Investigation Results
unknown/timeout	96% of failed requests turned out to originate from the servers of one single organisation (Organisation A) in Finland. The organisation has been contacted to fix a misconfiguration.
loop	73% of failed requests originated from the same Organisation A, which has been contacted to fix their misconfiguration. Another 17% could be attributed to organisations that did not treat the use of different capitalisations in their realm correctly (e.g. if the realm is university.fi, the server would not recognise University.fi as a local authentication).
proxied	26% of the failed attempts were due to the fact that the supplicant of a mobile phone was wrongly configured: The string “@...3gppnetwork.org” was sent as realm. For the remainder, it was hard to observe specific patterns. Possible reasons include: the supplicant security settings may be wrongly configured, the chosen EAP method may not

Class	Investigation Results
	be supported by the home organisation, the configured certificate information may be wrong or the password may be wrong.
malformed-1	Such severe misconfigurations suggest a bug in the software or firmware of the supplicant used.
malformed-2	Most of these failed authentication attempts seem to be caused by wrongly configured supplicants or wrongly entered usernames. Quite common is that the realm part is missing from the username.
malformed-3	94% of failures are due to the fact that the username has included the string "==" . A further investigation revealed that the username had been of the form "ZrJODsEQ7mjnSKPGBIm+Yg=="@Sonera Class2 CA," "5Jh8tFQ9UFUSsBZeGSHFJQ=="@AddTrust External CA Root" or something similar. It looks as though raw certificate information was sent instead of usernames and realms. Some Nokia cell phone firmwares are known to exhibit this erroneous behaviour.
unknown-FI	66% of failed authentications had been made with the same outer identity: xyz@ad.pax.fi.

Table 4.4: Analysis of failed authentication attempts by class

4.1.3 Summary

Summarising the findings above, it turned out to be true that single entities can generate a very significant proportion of failure. In the dataset above, one case involves a single organisation generating a six-digit number of failed authentication attempts due to a RADIUS server misconfiguration; another case involves a high five-digit number of failed authentication attempts due to a single misconfigured device.

Further to this, it can be seen that the analysis of failed authentication datasets is a very valuable tool to quickly identify the few entities in the infrastructure that are misconfigured. It is advisable to conduct a similar analysis on national proxy servers regularly, or even on a continuous basis, and to notify misbehaving RADIUS entities as soon as they are identified.

4.2 World-Wide eduroam Community

JRA3 T1 personnel regularly participate in the Global eduroam Governance Committee (GeGC). While most of the topics discussed in GeGC are of an administrative nature, there are some topics related to technology, including:

- Scalable routing of realms in generic top-level domains.
- Alternatives to the use of PKI for eduroam dynamic peer discovery.

Each of these is described below.

4.2.1 Scalable Routing of Realms in Generic Top-Level Domains

The most notable technology topic was the scalability of RADIUS realms that are not based on a country-code top-level domain (TLD). The discussion was triggered by the observation that the current practice of adding exception rules for those realms, and subsequent synchronisation of routing tables, does not scale well. A discussion paper on possible ways to overcome this problem was prepared by JRA3 T1 participants and was sent to GeGC for consideration. The document is included as Appendix C.

4.2.2 Alternatives to the Use of PKI for eduroam Dynamic Peer Discovery

RADIUS/TLS, both with and without Dynamic Discovery, is already in somewhat widespread use in Europe. Its uptake outside of Europe is still negligible, though, the reason being that the use of PKI for server-to-server authentication introduces a lot of administrative overhead. This is mostly because a) server certificates are only issued to previously vetted identities (which is difficult when the recipient is physically located on another continent) and b) the alternative to one CA that vets all identities is the use of a set of CAs (i.e. multiple trusted root anchors) with a more local scope; but this requires trust anchor management globally on every RADIUS/TLS-enabled server, and requires the local CAs to be set up and operated in the first place.

GeGC is investigating several other means of establishing trust between servers, including the use of:

- DNSSEC to secure server discovery.
- DNSSEC+DANE to securely derive communication keys for server discovery.
- Moonshot Trust Router architecture.

GeGC members from Canada and Europe are going to present first findings on this topic at the TERENA Networking Conference 2013 [TNC2013].

5 Recommendations for Long-Term Work

The GN3 project ends on 31 March 2013, and the separate eduroam R&D activity that was JRA3 T1 will be discontinued. Instead, R&D for eduroam will become an integral part of the eduroam Operations Team (eduroam OT) in the GN3plus project.

This section describes two of the major pieces of work that have been identified as being important to implement in the future, but which have not yet been tackled during the GN3 lifetime.

5.1 eduroam Operations Support Services (OSS)

5.1.1 Introduction

The work on eduroam CAT was the first instance of delivering a service to the user groups of eduroam Identity Providers (IdPs) and end users. This was innovative, in that eduroam Operations is defined as being the overarching coordination body for cross-national coordination; the layers of national eduroam management and service delivery for eduroam IdPs and eduroam SPs was previously regarded as strictly the “local business” of the eduroam federation concerned.

5.1.2 Problem Statement

The enormous success of eduroam CAT, which already had more than 100 participating IdPs during its beta phase, shows that there is significant opportunity to enhance the eduroam service across national deployments (i.e. within the scope of eduroam OT) by catering for the needs of individual IdPs/SPs/other user groups inside the connected federations, throughout the GÉANT service region and beyond.

eduroam CAT is beneficial (and, consequently, popular) for IdPs across eduroam because it aggregates into one central place business intelligence that was previously distributed. Distribution created workload for every single IdP: each IdP had to learn how to create installers for devices or at least screenshots for end-user self-service provisioning; this was time consuming, had a steep learning curve, and was executed with varying amounts of success. Aggregating this work into a single Web service that automates all these tasks using current best practice saves duplicated work for all the IdP administrators, leaving them time for other work.

Following the acknowledgement that de-duplication, automation of tasks and aggregation of best practices would be a useful endeavour, JRA3 T1 examined more parts of typical eduroam day-to-day workflows and investigated how some of those could be automated in the same way. The result of this investigation is that there are indeed many tasks that are still executed by human interaction and non-real-time communication (predominantly email) but which could in large part be automated.

5.1.3 An Operations Support System (OSS) for eduroam

As a consequence, JRA3 T1 suggests that a more comprehensive Business and Operations Support System is created, for which eduroam CAT can form the nucleus. This follows existing practice in the mobile communication sector, where such systems are commonly called OSS (Operations Support System) or B/OSS (Business/Operations Support System) [B/OSS]. It appears that there are few standards to adhere to (only a vague abstract model defined by the TMForum), so designing an own, customised system for eduroam appears to be a good way forward.

JRA3 T1 preliminarily identified the following concrete use cases for an OSS; the use cases are organised by user group.

- End users.
 - Provisioning eduroam: eduroam CAT already provides end users with ready-made installers for eduroam provisioning.
 - Debugging eduroam: requesting remote assistance when a roaming login does not work. The OSS could include a harmonised Web form that only requires a user's realm name as an input, and which could perform automated reachability checks for that realm and, if unable to isolate the source of the problem automatically, could allow the user to submit a problem description to his eduroam IdP.
 - Compliance enforcement: sending complaints about underperforming eduroam SPs to their IdP (e.g. a mandatory open port is closed, no IP address was obtained post-authentication, WPA/TKIP encryption, etc.). The OSS could help the user identify the eduroam SP by providing a list of SPs nearby if location services are available, and could send the complaint to the eduroam SP and/or his eduroam IdP without disclosing the actual contact data of the SP to the user.
- Identity Providers.
 - Provisioning eduroam: eduroam CAT already provides IdPs with ready-made installers for eduroam provisioning.
 - Verifying RADIUS setup: eduroam CAT already provides IdPs with a real-time test tool to check RADIUS setup correctness.
 - Assistance for configuration of RADIUS: an Operations Support System could generate sample (skeleton) configurations for popular RADIUS servers that match the EAP deployment details as indicated by the IdP and which follow all known best practices.
 - Problem reports: an OSS could provide Web forms where IdPs can make direct contact with an SP, e.g. if a user has reported a problem with a specific hotspot.

- Service Providers.
 - Debugging roaming-guest problems: eduroam CAT already allows another realm's reachability to be checked. This is useful if a hotspot operator has an incoming helpdesk request from a roaming user and needs to be able to determine whether the user's IdP has a globally affecting problem (e.g. RADIUS server down), or whether the problem is pertinent only to his own hotspot.
 - Verifying hotspot setup: an OSS could include an on-demand facility for logging into the hotspot as an "end user", which could then verify whether the hotspot performs well in all the important metrics of eduroam hotspots. This topic is large enough to be addressed in a separate section; please see Section 5.2 *Extending On-Site Hotspot Monitoring* for details.
 - Assistance for configuration of RADIUS: an OSS could generate sample (skeleton) configurations for popular RADIUS servers that match a typical eduroam SP RADIUS deployment and which follow all known best practices.
 - Abuse/problem reports: an OSS could provide Web forms where SPs can make direct contact with an IdP. There are many reasons for such communication. Examples include an abuse report if an IdP's user is in breach of the SP's Acceptable Use Policy (AUP) and should be blocked; or a technical problem report if, e.g., the SP detects that an IdP erroneously sends VLAN assignment attributes for its users.
- Federation Operators.
 - Real-time information about the status of their IdPs and SPs: examples for this include a dashboard showing whether all required information about participants has been submitted to the authoritative eduroam database.
 - Assistance for configuration of RADIUS: an OSS could generate sample (skeleton) configurations for popular federation RADIUS servers that match a standard RADIUS deployment on a federation level. Such a tool would be particularly useful for new federations or small federations that cannot spend a lot of time and effort on a custom setup.
 - Monitoring: currently, eduroam Monitoring checks only whether the international uplinks between federations work. With an OSS, the realm checks for IdPs could be leveraged to provide real-time monitoring for federation administrators.
- General public.
 - Usage statistics: this use case is partly fulfilled with the introduction of the Federated Ticker System (F-Ticks) into eduroam, although only on an international roaming level. However, the system easily allows the creation of statistics for roaming inside a federation (see [DJ3.1.2,1] Section 3.5). An OSS could integrate F-Ticks into federation management more tightly: statistics data for an IdP/SP/federation could be linked and be made visible to that participant; visibility settings for that slice of data, as well as live "widgets" with current usage data for inclusion into promotional material for the participant, could be provided.
- PR professionals.
 - Providing customised and localised marketing material: eduroam CAT has already demonstrated that localisation of texts is achievable in a scalable way. An OSS could leverage this by providing generic marketing material, in all supported languages, pre-filled with data and information for an IdP, SP, or federation. The marketing material would then be ready to use for all these participants.

This would aid uniformity in eduroam advertisements because all material would follow a common look and feel.

5.1.4 Recommendation

JRA3 T1 strongly suggests that work on such an OSS should be carried out in GN3plus, using eduroam CAT as a nucleus for the work.

5.2 Extending On-Site Hotspot Monitoring

5.2.1 Introduction

A successful eduroam internet access connection depends on many factors, under the control of many different parties, as summarised in Table 5.1 below.

Party	Internet Access Connection Factor
eduroam infrastructure	RADIUS request forwarding to the IdP
eduroam IdP	EAP server setup, server uptime and redundancy
eduroam SP	Wi-Fi setup, DHCP server, firewall settings
End user	Supplicant setup, working Wi-Fi device

Table 5.1: eduroam internet access connection factors

Over time, eduroam operators have created tools to monitor their part of the setup on all these points, which leads to end users' very high satisfaction with the overall eduroam service. For example:

- RADIUS request forwarding: eduroam OT has created two tools to verify that forwarding paths are working as expected:
 - eduroam Monitoring regularly checks whether the ETLRS and FLRS servers are forwarding international roaming requests as required (national roaming, and the forwarding of generic Top-Level Domain (gTLD) realms, are not covered).
 - The on-demand testing tool allows federation administrators to check whether the specific combination of "any" FLR server and their own server is working properly in real time (again, only international roaming with country-code Top-Level Domain (ccTLDs) is covered).
- Many (but not all) national eduroam federations have established regular monitoring with specific test accounts to verify the IdP setup and reachability.

- Some (but not all by far) national eduroam federations also test the reachability and request forwarding of their SPs (which works only for SP setups with their own RADIUS server).
- Very few national eduroam federations have hardware testing probes on-site at hotspots to verify the actual login, DHCP lease and service availability at their hotspots (typically using the username/password of a special-purpose test IdP in their federation).

5.2.2 Problem Statement

Two things about these monitoring approaches are noteworthy:

- None of the above monitoring approaches covers the entirety of eduroam; they lack either coverage in terms of realms (gTLD realms, national roaming) or lack penetration in terms of the number of federations deploying that type of monitoring.
- Some of the possible problems and incompatibilities with eduroam equipment on all these interaction points are only surfacing in certain constellations with some equipment and are very hard to debug.

JRA3 T1 has identified that an automated testing suite of hotspots, which ideally works in real time and can be triggered for immediate debugging, would be a very useful addition to the eduroam OT service portfolio. A set of the requirements that such a system would need to satisfy was specified; these are summarised in Section 5.2.3 below.

5.2.3 Requirements for an On-Site eduroam Monitoring Probe

5.2.3.1 Requirements for Physical Deployment

The probe would need to be a field-installable hardware device that establishes connections to a given hotspot in the same way an end user does. This first overarching requirement has many logistical implications, which are not detailed in this deliverable; may it suffice to say that at least the following conditions need to be taken into account. Devices need:

- To be field-upgradeable (new firmware to fix bugs, change set of tests to be run).
- To be capable of having their test credentials revoked if the device is stolen.
- To be replaced if broken.
- To be shipped and their target physical location mapped to eduroam database SP participant data.
- Test EAP credentials, which should be rotated at regular intervals to prevent leakage.
- To be able to report the test suite even if wireless connectivity does not work, i.e. they need to be equipped with a secondary out-of-band communications mechanism.

5.2.3.2 Requirements for a Set of Regular Automatic Tests

The device should be able to perform a set of tests in its physical vicinity regarding the presence and properties of eduroam hotspot(s) nearby:

- Is there a hotspot with SSID: eduroam (plus variants) in the vicinity?
- Is there a hotspot with the IEEE 802.11-2012 Interworking Consortium OI of eduroam in the vicinity?
- For all these hotspots:
 - Does the hotspot offer login with IEEE 802.11i “Enterprise security” (WPA2/AES with IEEE 802.1X)?
 - Is the hotspot EAP-type agnostic?
 - If a login was possible, are all the ports that are required to be open in the eduroam policy actually open?

5.2.3.3 Technical Details for Test Setup of Automatic Tests

In a more detailed description, these checks could be executed as follows:

1. Test suite to be executed at regular time intervals, e.g. every 30 minutes.
2. SSID:
 - Scan for SSIDs in the vicinity; store list of all SSIDs, their channels and signal strengths for later reporting.
 - Extract BSSIDs of networks whose SSID conforms to the regular expression `/.*eduroam.*/i` plus all BSSIDs who emit the consortium OID 00-1B-C5-04-60.
 - Examine beacons of extracted BSSIDs; store list of BSSIDs that support IEEE 802.11i (WPA2/AES with IEEE 802.1X) for later reporting as compliant; store list of remaining BSSIDs as NOT compliant for later reporting.
3. Login:
 - Connect to all SSIDs that have BSSIDs in the previously determined set of compliant BSSIDs using the device’s test EAP credential(s).
 - Measure duration and result of login operation; store list of test EAP credential usernames, EAP types, their respective duration, and their respective result for later reporting.
4. Connectivity:
 - Wait for a DHCP lease for a configurable amount of time (e.g. 10 seconds); store outcome of DHCP request process for later reporting.
 - If DHCP lease was successful, verify that IPv4 connectivity exists (ping defined sample address(es) outside the hotspot area, e.g. an eduroam monitoring host of choice); store outcome of test for later reporting.
 - Check whether IPv6 connectivity exists (DHCPv6 or global-scope SLAAC address, ping6 reference address(es)); store outcome of test for later reporting.

- Verify that the minimum set of ports is open (the list of ports is defined in the eduroam Policy Service Definition) by contacting defined sample hosts for each service; for each port, store outcome of the connection attempt for later reporting.
- Check whether further ("all") ports are open by contacting defined sample hosts for a number of TCP ports; store outcome of the connection attempt for later reporting.
- Connect to a defined sample host on port TCP/80 for Web traffic and determine whether a transparent Web proxy is used (it remains to be specified how such a detection would work).
- Optionally: test available bandwidth if network utilisation with production traffic is low; store outcome of the test for later reporting.

5.2.3.4 Requirements for Real-Time Tests On Demand

Further to the automatic tests outlined in the previous sections, it should also be possible for any eduroam IdP to make use of the probe for real-time debugging. For example, if one user of the IdP reports problems at a certain eduroam SP location, the IdP could create a temporary test credential, and trigger tests on the probe in question. To facilitate this use case, the following requirements are added:

- Probes must be able to receive instructions for immediate execution of real-time tests from a remote entity; such requests need to be authenticated. The probe may accept such requests only from a central point; in that case, it only needs to be able to authenticate this central entity.
- Since the probe's Wi-Fi uplink is not always online, the probes need to be equipped with a non-Wi-Fi communications channel and to listen for the real-time test instructions on that channel; e.g. a wired network port (which requires physical deployment of the probe near a wired network socket) or a broadband data dongle for reporting over 3G (which requires placement in an area with GPRS/3G/LTE coverage).
- Probes must be able to perform the tests from Section 5.2.3.3 *Technical Details for Test Setup of Automatic Tests* above, with the following alterations:
 - The EAP type to be used is not taken from the probe's own configuration, but is part of the instructions from the remote entity.
 - The EAP credential to be used is not taken from the probe's own configuration, but is part of the instructions from the remote entity.
 - The tests are not run at intervals, but are instead executed immediately and once only.

5.2.3.5 Requirements for Result Reporting

All the results from the above tests need to be communicated from the monitoring probe to a collection facility that can archive and display the results to authorised eduroam operators. The reporting process has the following requirements:

- Probes always need to be able to send results, even if the wireless login is not working. In practice, this means that they need to be equipped with a non-Wi-Fi communications channel; e.g. a wired network

port (which requires physical deployment of the probe near a wired network socket) or a broadband data dongle for reporting over 3G (which requires placement in an area with GPRS/3G/LTE coverage).

- The set of results as obtained from the tests above should be sent to the collection facility immediately. In the case of a real-time test, the results **MUST** be sent immediately after completion to the entity that triggered the test.
- All test results must be accessible for the hotspot operator in full, unfiltered detail.
- All test results should be accessible for the national eduroam operator of which the hotspot operator is part in full, unfiltered detail.
- eduroam OT should have access to a summary of statuses per federation. The details of the wealth of data being made available is still subject to discussion.

5.2.4 Recommendation

eduroam participants have repeatedly voiced the opinion that an extension of eduroam monitoring to individual hotspots is becoming more and more important to assure service quality. JRA3 T1 recommends that an on-site hotspot monitoring facility, as described above, should be made available as soon as possible. This may either be achieved by procuring such testing equipment from a third-party vendor, by leveraging some of the national monitoring probe projects, or by designing a hardware probe from scratch.

6 Conclusions

GN3 JRA3 Multi-Domain User Application Research, Task 1 Roaming Developments has been active throughout the lifetime of the GN3 project and has produced three editions of the “Roaming Developments” deliverable.

This iteration of the deliverable has continued to provide summaries of activities within the relevant standardisation bodies for eduroam – IETF and IEEE – and has included both passive watching briefs on upcoming standards of interest as well as active contributions in the IETF. The most notable of these has been the conclusion and final publishing of RFC6614 as a direct consequence of GN3 involvement in the IETF. This standard is now in active use in eduroam and elsewhere, creating a significant impact in the network access niche of the IT industry.

The deliverable has also taken a close look at the eduroam infrastructure and identified areas that have benefited from further development. The most significant of those was the finalisation of eduroam CAT and its transition to production service. Together with the F-Ticks concept for enhanced statistics, two of the major software projects that were designed in JRA3 T1 have been widely adopted and put to good use by eduroam Operations.

In addition to this direct architecture improvement work, JRA3 T1 has also provided insights into two areas: eduroam federation-specific work, with an example analysis of failed authentication traffic on a federation-level RADIUS server; and topics of interest on a beyond-European level, by actively participating in the Global eduroam Governance Committee.

Lastly, since this iteration of the deliverable is the final one in the GN3 project, the deliverable has also provided an outlook for areas that deserve further R&D work, and which should be worked upon in GN3plus or other projects as appropriate.

This deliverable concludes the work of JRA3 T1. Looking back at the history of three editions of this deliverable and also DJ3.1.1, the group believes it has created significant value for eduroam in these four years. All the authors of all the deliverables would like to thank the project for the continued support of this Task.

The development work that has, up to now, been done in JRA3 T1, particularly the items identified in Chapter 5 of this deliverable, will be continued as an integral part of eduroam Operations in GN3plus; readers who are interested in further eduroam developments should consult the deliverables of this new GN3plus Activity.

Appendix A Configuration

This is the full configuration file as used for the Interworking field test:

```
ctrl_interface=/var/run/wpa_supplicant
eapol_version=1
ap_scan=1
fast_reauth=1

# Interworking (IEEE 802.11u)
# Enable Interworking
interworking=1

# 1 = perform Interworking network selection if one or more
#   credentials have been configured and scan did not find a
#   matching network block
auto_interworking=1

cred={
    username="user@lboro.ac.uk"
    password="Password"
    ca_cert="/home/user/11utesting/ca.pem"
    roaming_consortium=001bc50460
    domain="lboro.ac.uk"
    eap=TTLS
    phase2="eapauth=MSCHAPV2"
}

# enable Hotspot 2.0
hs20=1
```

This is the full debug output as produced by wpa_supplicant while connecting:

```
nl80211: Received scan results (12 BSSes)
```

```

wlan0: BSS: Start scan result update 1
wlan0: BSS: Add new id 0 BSSID 1c:17:d3:ca:ea:75 SSID '1lu Test'
wlan0: BSS: Add new id 1 BSSID 1c:17:d3:ca:ea:71 SSID 'eduroam'
wlan0: BSS: Add new id 2 BSSID 00:24:97:f1:8d:a1 SSID 'eduroam'
wlan0: BSS: Add new id 3 BSSID 1c:17:d3:ca:ea:73 SSID 'YST'
wlan0: BSS: Add new id 4 BSSID 1c:17:d3:ca:ea:74 SSID 'HS2 Test'
wlan0: BSS: Add new id 5 BSSID d0:c2:82:06:d8:f1 SSID 'eduroam'
wlan0: No suitable network found
wlan0: Interworking: start ANQP fetch since no matching networks foundwlan0:
ANQP fetch completed
Interworking: Search for match with home SP FQDN lboro.ac.uk
Interworking: AP domain name - hexdump_ascii(len=9):
    6c 75 74 2e 61 63 2e 75 6b                                lut.ac.uk
wlan0: INTERWORKING-AP 1c:17:d3:ca:ea:75 type=roaming
Interworking: Search for match with home SP FQDN lboro.ac.uk
Interworking: AP domain name - hexdump_ascii(len=11):
    6c 62 6f 72 6f 2e 61 63 2e 75 6b                        lboro.ac.uk
wlan0: INTERWORKING-AP 1c:17:d3:ca:ea:74 type=home
Interworking: Highest roaming consortium matching credential priority 0
Interworking: Connect with 1c:17:d3:ca:ea:74 based on roaming consortium match
wlan0: 4: 1c:17:d3:ca:ea:74 ssid='HS2 Test' wpa_ie_len=0 rsn_ie_len=20
caps=0x1431 level=-39
wlan0:    selected based on RSN IE
wlan0:    selected BSS 1c:17:d3:ca:ea:74 ssid='HS2 Test'
wlan0: Request association: reassociate: 1  selected: 1c:17:d3:ca:ea:74  bssid:
00:00:00:00:00:00  pending: 00:00:00:00:00:00  wpa_state: SCANNING
wlan0: Automatic auth_alg selection: 0x1
RSN: PMKSA cache search - network_ctx=(nil) try_opportunistic=0
RSN: Search for BSSID 1c:17:d3:ca:ea:74
RSN: No PMKSA cache entry found
wlan0: RSN: using IEEE 802.11i/D9.0
wlan0: WPA: Selected cipher suites: group 16 pairwise 16 key_mgmt 1 proto 2
wlan0: WPA: clearing AP WPA IE
WPA: set AP RSN IE - hexdump(len=22): 30 14 01 00 00 0f ac 04 01 00 00 0f ac 04
01 00 00 0f ac 01 28 00
wlan0: WPA: using GTK CCMP
wlan0: WPA: using PTK CCMP
wlan0: WPA: using KEY_MGMT 802.1X
WPA: Set own WPA IE default - hexdump(len=22): 30 14 01 00 00 0f ac 04 01 00 00
0f ac 04 01 00 00 0f ac 01 00 00
FT: Stored MDIE and FTIE from (Re)Association Response - hexdump(len=0):
wlan0: Cancelling scan request
wlan0: SME: Trying to authenticate with 1c:17:d3:ca:ea:74 (SSID='HS2 Test'
freq=2462 MHz)
wlan0: No keys have been configured - skip key clearing

```

```

wlan0: State: SCANNING -> AUTHENTICATING
EAPOL: External notification - EAP success=0
EAPOL: Supplicant port status: Unauthorized
EAPOL: External notification - EAP fail=0
EAPOL: Supplicant port status: Unauthorized
EAPOL: External notification - portControl=Auto
EAPOL: Supplicant port status: Unauthorized
nl80211: Authenticate (ifindex=3)
  * bssid=1c:17:d3:ca:ea:74
  * freq=2462
  * SSID - hexdump_ascii(len=8):
    48 53 32 20 54 65 73 74                HS2 Test
  * IEs - hexdump(len=0): [NULL]
  * Auth Type 0
nl80211: Authentication request send successfully
SSL: SSL_connect:SSLv3 read server hello A
TLS: tls_verify_cb - preverify_ok=1 err=0 (ok) ca_cert_verify=1 depth=1
buf='/C=GB/ST=Leicestershire/L=Loughborough/O=Loughborough
University/emailAddress=it.services@lboro.ac.uk/CN=Loughborough University
Network Services Certificate Authority'
wlan0: CTRL-EVENT-EAP-PEER-CERT depth=1
subject='/C=GB/ST=Leicestershire/L=Loughborough/O=Loughborough
University/emailAddress=it.services@lboro.ac.uk/CN=Loughborough University
Network Services Certificate Authority'
EAP: Status notification: remote certificate verification (param=success)
TLS: tls_verify_cb - preverify_ok=1 err=0 (ok) ca_cert_verify=1 depth=0
buf='/C=GB/ST=Leicestershire/O=Loughborough
University/CN=radius.lboro.ac.uk/emailAddress=it.services@lboro.ac.uk'
wlan0: CTRL-EVENT-EAP-PEER-CERT depth=0
subject='/C=GB/ST=Leicestershire/O=Loughborough
University/CN=radius.lboro.ac.uk/emailAddress=it.services@lboro.ac.uk'
EAP: Status notification: remote certificate verification (param=success)
wlan0: WPA: Key negotiation completed with 1c:17:d3:ca:ea:74 [PTK=CCMP
GTK=CCMP]
wlan0: Cancelling authentication timeout
Removed BSSID 1c:17:d3:ca:ea:74 from blacklist
wlan0: State: GROUP_HANDSHAKE -> COMPLETED
wlan0: CTRL-EVENT-CONNECTED - Connection to 1c:17:d3:ca:ea:74 completed [id=0
id_str=]
```


Appendix B Generic EAP Metadata Profile

B.1 Generic EAP Metadata XML Schema Definition

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema version="1.0" xmlns:xs="http://www.w3.org/2001/XMLSchema"
elementFormDefault="qualified">
  <xs:simpleType name="EAPNumbers">
    <xs:restriction base="xs:int">
      <xs:enumeration value="13">
        <xs:annotation>
          <xs:documentation>TLS</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="21">
        <xs:annotation>
          <xs:documentation>TTLS</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="25">
        <xs:annotation>
          <xs:documentation>PEAP</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="26">
        <xs:annotation>
          <xs:documentation>MSCHAPv2</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
      <xs:enumeration value="52">
        <xs:annotation>
          <xs:documentation>PWD</xs:documentation>
        </xs:annotation>
      </xs:enumeration>
    </xs:restriction>
  </xs:simpleType>
</xs:schema>
```

```

</xs:simpleType>

<xs:complexType name="VendorSpecificExtension">
  <xs:sequence>
    <xs:any namespace="##other"/>
  </xs:sequence>
  <xs:attribute name="vendor" type="xs:int" use="required"/>
</xs:complexType>

<xs:complexType name="TypeSpecificExtension">
  <xs:sequence>
    <xs:any namespace="##other"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="EAPMethod">
  <xs:sequence>
    <xs:element name="Type" type="EAPNumbers" minOccurs="1" maxOccurs="1"/>
    <xs:element name="TypeSpecific" type="TypeSpecificExtension" minOccurs="0"
      maxOccurs="1"/>
    <xs:element name="VendorSpecific" type="VendorSpecificExtension" minOccurs="0"
      maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<xs:simpleType name="NonEAPAuthNumbers">
  <xs:restriction base="xs:int">
    <xs:enumeration value="1">
      <xs:annotation>
        <xs:documentation>PAP</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="2">
      <xs:annotation>
        <xs:documentation>MSCHAP</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="3">
      <xs:annotation>
        <xs:documentation>MSCHAPv2</xs:documentation>
      </xs:annotation>
    </xs:enumeration>
  </xs:restriction>
</xs:simpleType>

```

```

<xs:simpleType name="IEEE80211-RSN-Protocols">
  <xs:restriction base="xs:string">
    <xs:enumeration value="TKIP">
      <xs:annotation>
        <xs:documentation>
          Temporal Key Integrity Protocol (if used, crypto settings
            "WPA/TKIP", "WPA2/TKIP" and "WPA2/AES" and possible future
            protos are acceptable).
        </xs:documentation>
      </xs:annotation>
    </xs:enumeration>
    <xs:enumeration value="CCMP">
      <xs:annotation>
        <xs:documentation>
          CTR with CBC-MAC Protocol (if used, only crypto setting
            "WPA2/AES" and possible future protos are acceptable).
        </xs:documentation>
      </xs:annotation>
    </xs:enumeration>
  </xs:restriction>
</xs:simpleType>

<xs:complexType name="NonEAPAuthMethod">
  <xs:sequence>
    <xs:element name="Type" type="NonEAPAuthNumbers" minOccurs="1" maxOccurs="1"/>
    <xs:element name="TypeSpecific" type="TypeSpecificExtension" minOccurs="0"
      maxOccurs="1"/>
    <xs:element name="VendorSpecific" type="VendorSpecificExtension" minOccurs="0"
      maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="CertData">
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute name="format" type="xs:string" use="required"/>
      <xs:attribute name="encoding" type="xs:string" use="required"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:complexType name="LogoData">
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute name="mime" type="xs:string" use="required"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

```

```

        <xs:attribute name="encoding" type="xs:string" use="required"/>
    </xs:extension>
</xs:simpleContent>
</xs:complexType>

<xs:complexType name="ClientCredentialVariants">
    <xs:annotation>
        <xs:documentation>
            Not all EAP types and non-EAP authentication methods need or
            support all types of credentials in the list below. While the
            Schema allows to put all kinds of credential information inside
            every AuthenticationMethod, even where the information is not
            applicable, tags which are not applicable for an authentication
            EAP or non-EAP type

            SHOULD NOT be included in the corresponding instance of
            AuthenticationMethod or InnerAuthenticationMethod when
            producing the XML file, and

            MUST be ignored by the entity consuming the XML file if
            present in the XML file.
        </xs:documentation>
    </xs:annotation>
    <xs:sequence minOccurs="1" maxOccurs="1">
        <xs:element name="AnonymousIdentity" type="xs:string" minOccurs="0" maxOccurs="1"/>
        <xs:element name="UserName" type="xs:string" minOccurs="0" maxOccurs="1"/>
        <xs:element name="Password" type="xs:string" minOccurs="0" maxOccurs="1"/>
        <xs:element name="ClientCertificate" type="CertData" minOccurs="0" maxOccurs="1"/>
        <xs:element name="PAC" type="xs:string" minOccurs="0" maxOccurs="1"/>
        <xs:element name="ProvisionPAC" type="xs:boolean" minOccurs="0" maxOccurs="1"/>
    </xs:sequence>
    <xs:attribute name="allow_save" type="xs:boolean" use="optional"/>
</xs:complexType>

<xs:complexType name="ServerCredentialVariants">
    <xs:annotation>
        <xs:documentation>
            Not all EAP types and non-EAP authentication methods need or
            support all types of credentials in the list below. While the
            Schema allows to put all kinds of credential information inside
            every AuthenticationMethod, even where the information is not
            applicable, tags which are not applicable for an authentication
            EAP or non-EAP type

            SHOULD NOT be included in the corresponding instance of
            AuthenticationMethod or InnerAuthenticationMethod when
            producing the XML file, and

            MUST be ignored by the entity consuming the XML file if

```

```

        present in the XML file.
    </xs:documentation>
</xs:annotation>
<xs:sequence minOccurs="1" maxOccurs="1">
    <xs:element name="CA" type="CertData" minOccurs="0" maxOccurs="unbounded"/>
    <xs:element name="ServerID" type="xs:string" minOccurs="0" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>

<xs:complexType name="IEEE80211-Properties">
    <xs:annotation>
        <xs:documentation>
            The conditions inside this element are considered AND conditions.
            It does e.g. not make sense to have multiple SSIDs in one
            IEEE80211-Properties field because the condition would never
            match. To specify multiple ORed network properties, use multiple
            IEEE80211-Properties instances.
        </xs:documentation>
    </xs:annotation>
    <xs:sequence minOccurs="1" maxOccurs="1">
        <xs:element name="SSID" type="xs:string" minOccurs="0" maxOccurs="1"/>
        <xs:element name="ConsortiumOID" type="xs:string" minOccurs="0" maxOccurs="1"/>
        <xs:element name="MinRSNProto" type="IEEE80211-RSN-Protocols" minOccurs="0"
            maxOccurs="1"/>
    </xs:sequence>
</xs:complexType>

<xs:complexType name="LocalizedInteractive">
    <xs:simpleContent>
        <xs:extension base="xs:string">
            <xs:attribute name="lang" type="xs:string" use="optional"/>
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>

<xs:complexType name="LocalizedNonInteractive">
    <xs:simpleContent>
        <xs:extension base="xs:string">
            <xs:attribute name="lang" type="xs:string" use="optional"/>
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>

<xs:element name="EAPIdentityProviderList">
    <xs:complexType>

```

```

<xs:sequence minOccurs="1" maxOccurs="unbounded">
  <xs:element name="EAPIdentityProvider">
    <xs:complexType>
      <xs:sequence minOccurs="1" maxOccurs="unbounded">
        <xs:element name="NameIDFormat" type="xs:string" minOccurs="1"
          maxOccurs="1"/>
        <xs:element name="DisplayName" type="LocalizedNonInteractive"
          minOccurs="0" maxOccurs="unbounded"/>
        <xs:element name="Description" type="LocalizedNonInteractive"
          minOccurs="0" maxOccurs="unbounded"/>
        <xs:element name="AuthenticationMethods" minOccurs="1" maxOccurs="1">
          <xs:complexType>
            <xs:sequence minOccurs="1" maxOccurs="unbounded">
              <xs:element name="AuthenticationMethod">
                <xs:complexType>
                  <xs:sequence minOccurs="1" maxOccurs="unbounded">
                    <xs:element name="EAPMethod" type="EAPMethod"/>
                    <xs:element name="ServerSideCredential"
                      type="ServerCredentialVariants" minOccurs="0"
                      maxOccurs="1"/>
                    <xs:element name="ClientSideCredential"
                      type="ClientCredentialVariants" minOccurs="0"
                      maxOccurs="1"/>
                    <xs:element name="InnerAuthenticationMethod"
                      minOccurs="0" maxOccurs="unbounded">
                      <xs:complexType>
                        <xs:sequence minOccurs="0"
                          maxOccurs="unbounded">
                          <xs:element name="EAPMethod"
                            type="EAPMethod" minOccurs="0"
                            maxOccurs="1"/>
                          <xs:element name="NonEAPAuthMethod"
                            type="NonEAPAuthMethod"
                            minOccurs="0" maxOccurs="1"/>
                          <xs:element
                            name="ServerSideCredential"
                            type="ServerCredentialVariants"
                            minOccurs="0" maxOccurs="1"/>
                          <xs:element
                            name="ClientSideCredential"
                            type="ClientCredentialVariants"
                            minOccurs="0" maxOccurs="1"/>
                        </xs:sequence>
                      </xs:complexType>
                    </xs:element>
                  </xs:sequence>
                </xs:complexType>
              </xs:element>
            </xs:sequence>
          </xs:complexType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:sequence>

```

```

        </xs:sequence>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="CompatibleUses" minOccurs="1" maxOccurs="1">
  <xs:complexType>
    <xs:sequence minOccurs="1" maxOccurs="1">
      <xs:element name="IEEE80211" type="IEEE80211-Properties"
        minOccurs="0" maxOccurs="unbounded"/>
      <xs:element name="IEEE8023-NetworkID" type="xs:string"
        minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="ProviderLocation" minOccurs="0"
maxOccurs="unbounded">
  <!-- this specification still lacks the richness to express the
most important coordinate: bearing 112, carom 365, dist 365321. -->
  <!-- Welcome to the planet Earth, Fabian! -->
  <xs:complexType>
    <xs:sequence minOccurs="1" maxOccurs="1">
      <xs:element name="Longitude" type="xs:string" minOccurs="1"
        maxOccurs="1"/>
      <xs:element name="Latitude" type="xs:string" minOccurs="1"
        maxOccurs="1"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="ProviderLogo" type="LogoData" minOccurs="0"
maxOccurs="1"/>
<xs:element name="TermsOfUse" type="LocalizedNonInteractive"
minOccurs="0" maxOccurs="unbounded"/>
<xs:element name="Helpdesk" minOccurs="0" maxOccurs="1">
  <xs:complexType>
    <xs:sequence minOccurs="1" maxOccurs="1">
      <xs:element name="EmailAddress" type="LocalizedInteractive"
        minOccurs="0" maxOccurs="unbounded"/>
      <xs:element name="WebAddress"
        type="LocalizedNonInteractive" minOccurs="0"
        maxOccurs="unbounded"/>
      <xs:element name="Phone" type="LocalizedInteractive"
        minOccurs="0" maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>

```

```

        </xs:complexType>
    </xs:element>
    <xs:element name="VendorSpecific" type="VendorSpecificExtension"
        minOccurs="0" maxOccurs="1"/>
</xs:sequence>
<xs:attribute name="ID" type="xs:string" use="optional"/>
<xs:attribute name="lang" type="xs:string" use="optional"/>
<!--
If the optional attribute "lang" for the EAPIdentityProvider
tag is specified, then all user-displayable strings inside
this tag are to be considered suitable for use in user
interfaces in that language. Individual lang tags for the
sub-tags inside EAPIdentityProvider then SHOULD NOT be used.

If the optional attribute "lang" for the EAPIdentityProvider
tag is not set, individual sub-tags which contain user-
displayable strings SHOULD be marked with the language they
are written/available in.
-->
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>

```

B.2 Sample Generic EAP Metadata Configuration File

```

<?xml version="1.0"?>
<EAPIdentityProviderList
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="generic-data-strawman.xsd">
  <EAPIdentityProvider ID="urn:RFC4282:realm:education.lu">
    <NameIDFormat>urn:RFC4282:realm</NameIDFormat>
    <DisplayName>RESTENA Foundation - education.lu Users</DisplayName>
    <DisplayName lang='de'>Stiftung RESTENA - education.lu Benutzer</DisplayName>
    <Description>This profile is for all users with a mailbox @education.lu</Description>
    <AuthenticationMethods>
      <AuthenticationMethod>
        <EAPMethod>
          <Type>25</Type>
        </EAPMethod>

```



```
<ServerSideCredential>
  <CA format="X.509" encoding="base64">
```

```
MIIDxTCCAy6gAwIBAgIJAOfXed1VHiJFMA0GCSqGSIb3DQEBAUAMIGeMQswCQYDVQQGEwJMVTETMBEGA1UEBxMKTHV4ZW1ib3V
yZzEaMBGGA1UEChMRMR9uZGF0aW9uIFJFU1RFTkExGzAZBgNVBAsTElJFU1RFTkEgZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4
VOQSB1ZHVyb2FtIGF1dGhvcml0eTEdMBsGCSqGSIb3DQEJARYObm9jQHJlc3RlbmEubHUwHhcNMDYwMTE5MTI1MzA5WhcNMTYwM
TE3MTI1MzA5WjCBnjELMAkGA1UEBhMCTFUXEzARBgNVBAcTCkxleGVtYm91cmcxGjAYBgNVBAoTEUZZvbmRhdGlvbiBSRVNURU5B
MRswGQYDVQQLExJSRVNURU5BIGVkdXJvYW0gQ0ExIjAgBgNVBAMTGJFU1RFTkEgZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4
G9w0BCQEWdm5vY0ByZXN0ZW5hLmx1MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBQC576jFDDKeS9Lq5vf6WGxjTWK1dMw08B
RGMJ8/VVj3b59Bmm6qHuxrQ4V48SIG8i6q/bxuCgusG/FGvnIcxiYchCDF0ggGx17XBje0EmqAi4c1nViQhMVQnCN3rG5jr5e/r
U1HvzvVF/zFeEgD6NGGyJsodiVWuXyGcfjK1NcyYQIDAQABo4IBBzCCAQMWHQYDVR0OBByEFNKjQqCmSOBRgDvmVOEAqkZVH3y4
MIHTBgNVHSMegcswgciaFNKjQqCmSOBRgDvmVOEAqkZVH3y4oYgkpiGHMIGeMQswCQYDVQQGEwJMVTETMBEGA1UEBxMKTHV4ZW1
ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4
VTVEVOQSB1ZHVyb2FtIGF1dGhvcml0eTEdMBsGCSqGSIb3DQEJARYObm9jQHJlc3RlbmEubHUwHhcNMDYwMTE5MTI1MzA5WhcNM
TADAQH/MA0GCSqGSIb3DQEBAUAA4GBAEyFwxhGxGtKjDrcG6TLh5CORjpEdtOe5Poq5g02y64xFKgVn2mtpfOtOrN5C0zk8vkh
A4X5rb91hiTSpI2bzS5q/pbNbwqVUJe3W6ZG+rdokkBP0pfQV3vq8xDS322MHkxmdAybRizIx24Sv5T4y0aEaMtQt+wnFxLFU6H
Ck3X3
```

```
</CA>
<ServerID>eduroam.restena.lu</ServerID>
<ServerID>server2.restena.lu</ServerID>
</ServerSideCredential>
<ClientSideCredential>
  <AnonymousIdentity>@education.lu</AnonymousIdentity>
</ClientSideCredential>
<InnerAuthenticationMethod>
  <EAPMethod>
    <Type>26</Type>
  </EAPMethod>
  <ClientSideCredential allow_save="false">

  </ClientSideCredential>
</InnerAuthenticationMethod>
</AuthenticationMethod>
<AuthenticationMethod>
  <EAPMethod>
    <Type>21</Type>
  </EAPMethod>
<ServerSideCredential>
  <CA format="X.509" encoding="base64">
```

```
MIIDxTCCAy6gAwIBAgIJAOfXed1VHiJFMA0GCSqGSIb3DQEBAUAMIGeMQswCQYDVQQGEwJMVTETMBEGA1UEBxMKTHV4ZW1ib3V
yZzEaMBGGA1UEChMRMR9uZGF0aW9uIFJFU1RFTkExGzAZBgNVBAsTElJFU1RFTkEgZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4
VOQSB1ZHVyb2FtIGF1dGhvcml0eTEdMBsGCSqGSIb3DQEJARYObm9jQHJlc3RlbmEubHUwHhcNMDYwMTE5MTI1MzA5WhcNMTYwM
TE3MTI1MzA5WjCBnjELMAkGA1UEBhMCTFUXEzARBgNVBAcTCkxleGVtYm91cmcxGjAYBgNVBAoTEUZZvbmRhdGlvbiBSRVNURU5B
MRswGQYDVQQLExJSRVNURU5BIGVkdXJvYW0gQ0ExIjAgBgNVBAMTGJFU1RFTkEgZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4
G9w0BCQEWdm5vY0ByZXN0ZW5hLmx1MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBQC576jFDDKeS9Lq5vf6WGxjTWK1dMw08B
RGMJ8/VVj3b59Bmm6qHuxrQ4V48SIG8i6q/bxuCgusG/FGvnIcxiYchCDF0ggGx17XBje0EmqAi4c1nViQhMVQnCN3rG5jr5e/r
U1HvzvVF/zFeEgD6NGGyJsodiVWuXyGcfjK1NcyYQIDAQABo4IBBzCCAQMWHQYDVR0OBByEFNKjQqCmSOBRgDvmVOEAqkZVH3y4
MIHTBgNVHSMegcswgciaFNKjQqCmSOBRgDvmVOEAqkZVH3y4oYgkpiGHMIGeMQswCQYDVQQGEwJMVTETMBEGA1UEBxMKTHV4ZW1
ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4
VTVEVOQSB1ZHVyb2FtIGF1dGhvcml0eTEdMBsGCSqGSIb3DQEJARYObm9jQHJlc3RlbmEubHUwHhcNMDYwMTE5MTI1MzA5WhcNM
TADAQH/MA0GCSqGSIb3DQEBAUAA4GBAEyFwxhGxGtKjDrcG6TLh5CORjpEdtOe5Poq5g02y64xFKgVn2mtpfOtOrN5C0zk8vkh
A4X5rb91hiTSpI2bzS5q/pbNbwqVUJe3W6ZG+rdokkBP0pfQV3vq8xDS322MHkxmdAybRizIx24Sv5T4y0aEaMtQt+wnFxLFU6H
Ck3X3
```

G9w0BCQEWDm5vY0ByZXN0ZW5hLmx1MIGfMA0GCSqGSIB3DQEBAQUAA4GNADCBiQKBgQC576jfDDKeS9Lq5vf6WGxjTWK1dMwO8BRGMJ8/VVj3b59Bmm6qHuxrQ4V48SIG8i6q/bxuCgusG/FGvnIcxIychCDF0ggGx17XBje0EmqAi4c1nViQhMVQnCN3rG5jr5e/rU1HvzvVF/zFeEgD6NGGyJsodiVWuXyGcfjK1NcyYQIDAQABo4IBBzCCAQMwHQYDVR0OBByEFNKjQqCmSOBRgDvmVOEAqkZVH3y4MIHTBgNVHSMGcswgcIAFNKjQqCmSOBRgDvmVOEAqkZVH3y4oYgkpiGhMIGeMQswCQYDVQQGEwJMVTETMBEGA1UEBxMKTHV4ZW1ib3VyZzEaMBGGA1UEChMRRm9uZGF0aW9uIFJFU1RFTkExGzAZBgNVBAsTElJFU1RFTkEgZWRLcm9hbSBDQTEiMCAGA1UEAxMZUkVTVEVOQSBlZHVyY2FtIGF1dGhvcml0eTEdMBsGCSqGSIB3DQEEJARYObm9jQhJlc3RlbnEubHwCCQDn13ndVR4oxTAMBgNVHRMEBTADAQH/MA0GCSqGSIB3DQEBAQUAA4GBAEyFwxhGxGtKjDrcG6TLh5CORjpEdtOe5Pq5g02y64xFKgVn2mtpfOtOrN5C0zk8vkhA4X5rb91hiTSpI2bzS5q/pbNbwqVUJe3W6ZG+rdokkBp0pfQV3vq8xDS322MHkxmdAybRIzIx24Sv5T4y0aEaMtQt+wnFxLFU6HCk3X3

```

    </CA>
    <ServerID>eduroam.restena.lu</ServerID>
    <ServerID>server2.restena.lu</ServerID>
  </ServerSideCredential>
  <ClientSideCredential>
    <AnonymousIdentity>@education.lu</AnonymousIdentity>
  </ClientSideCredential>
  <InnerAuthenticationMethod>
    <NonEAPAuthMethod>
      <Type>1</Type>
    </NonEAPAuthMethod>
    <ClientSideCredential allow_save="false">

    </ClientSideCredential>
  </InnerAuthenticationMethod>
</AuthenticationMethod>
<AuthenticationMethod>
  <EAPMethod>
    <Type>13</Type>
  </EAPMethod>
  <ServerSideCredential>
    <CA format="X.509" encoding="base64">

```

MIIDxTCCAy6gAwIBAgIJAOfXed1VHiJFMA0GCSqGSIB3DQEBAQUAA4GNADCBiQKBgQC576jfDDKeS9Lq5vf6WGxjTWK1dMwO8BRGMJ8/VVj3b59Bmm6qHuxrQ4V48SIG8i6q/bxuCgusG/FGvnIcxIychCDF0ggGx17XBje0EmqAi4c1nViQhMVQnCN3rG5jr5e/rU1HvzvVF/zFeEgD6NGGyJsodiVWuXyGcfjK1NcyYQIDAQABo4IBBzCCAQMwHQYDVR0OBByEFNKjQqCmSOBRgDvmVOEAqkZVH3y4MIHTBgNVHSMGcswgcIAFNKjQqCmSOBRgDvmVOEAqkZVH3y4oYgkpiGhMIGeMQswCQYDVQQGEwJMVTETMBEGA1UEBxMKTHV4ZW1ib3VyZzEaMBGGA1UEChMRRm9uZGF0aW9uIFJFU1RFTkExGzAZBgNVBAsTElJFU1RFTkEgZWRLcm9hbSBDQTEiMCAGA1UEAxMZUkVTVEVOQSBlZHVyY2FtIGF1dGhvcml0eTEdMBsGCSqGSIB3DQEEJARYObm9jQhJlc3RlbnEubHwCCQDn13ndVR4oxTAMBgNVHRMEBTADAQH/MA0GCSqGSIB3DQEBAQUAA4GBAEyFwxhGxGtKjDrcG6TLh5CORjpEdtOe5Pq5g02y64xFKgVn2mtpfOtOrN5C0zk8vkh

A4X5rb91hiTSpI2bzS5q/pbNbwqVUJe3W6ZG+rdokkBp0pfQV3vq8xDS322MHkxmdAybRIzIx24Sv5T4y0aEaMtQt+wnFxLFU6H
Ck3X3

```

    </CA>
    <ServerID>eduroam.restena.lu</ServerID>
    <ServerID>server2.restena.lu</ServerID>
  </ServerSideCredential>
  <ClientSideCredential>
    <AnonymousIdentity>@education.lu</AnonymousIdentity>
    <ClientCertificate format="PKCS12" encoding="base64">

```

MIIDxTCCAY6gAwIBAgIJAOfXed1VHiJFMA0GCSqGSIb3DQEBAUAMIGEMQswCQYDVQQGEwJMVTETMBEGA1UEBxMKTHV4ZW1ib3V
yZzEaMBGGA1UEChMRM9uZGF0aW9uIFJFU1RFTkExGzAZBgNVBAsTElJFU1RFTkEgZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4
VOQSB1ZHVyb2FtIGF1dGhvcml0eTEdMBsGCSqGSIb3DQEJARYObm9jQHJlc3RlbnEubHwHcNMDYwMTE1MzA5WmcNMTYwM
TE3MTI1MzA5WjCBnjELMAkGA1UEBhMCTFUXEzARBgNVBAClTCkxleGVtYm91cmcxGjAYBgNVBAoTEUZZbWV4ZW1ib3V4ZW1ib3V4
MRswGQYDVQQLEwJSRVNURU5BIGVkdXJvYVY0gQ0ExIjAgBgNVBAMTGVJFU1RFTkEgZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4
G9w0BCQEWdm5vY0ByZXN0ZW5hLmx1MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC576jfDDKeS9Lq5vf6WGxjTWK1dMw08B
RGMJ8/VVj3b59Bmm6qHuxrQ4V48SIG8i6q/bxuGgusG/FGvNcIychCDF0ggGx17XBje0EmqAi4c1nViQhMVQnCN3rG5jr5e/r
UlHvzvVF/zFeEgD6NGGyJsodiVWuXyGcfjK1NcyYQIDAQABo4IBBzCCAQMwHQYDVR0OBYYEFNKjQqCmSObRgDvmVOEAqkZVH3y4
MIHTBgNVHSMGcswgcIAFNKjQqCmSObRgDvmVOEAqkZVH3y4oYgkPIGhMIGEMQswCQYDVQQGEwJMVTETMBEGA1UEBxMKTHV4ZW1
ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4ZW1ib3V4
VTVEVOQSB1ZHVyb2FtIGF1dGhvcml0eTEdMBsGCSqGSIb3DQEJARYObm9jQHJlc3RlbnEubHwHcNMDYwMTE1MzA5WmcNMTYwM
TADAQH/MA0GCSqGSIb3DQEBAUAA4GBAEyFwxhGxGtKjDrcG6TLh5CORjpEdtOe5Poq5g02y64xFKgVn2mtpfOtOrN5C0zk8vkh
A4X5rb91hiTSpI2bzS5q/pbNbwqVUJe3W6ZG+rdokkBp0pfQV3vq8xDS322MHkxmdAybRIzIx24Sv5T4y0aEaMtQt+wnFxLFU6H
Ck3X3

```

    </ClientCertificate>
  </ClientSideCredential>
</AuthenticationMethod>
</AuthenticationMethods>

<CompatibleUses>
  <IEEE80211>
    <SSID>eduroam</SSID>
    <MinRSNProto>CCMP</MinRSNProto>
  </IEEE80211>
  <IEEE80211>
    <SSID>foobar</SSID>
    <MinRSNProto>TKIP</MinRSNProto>
  </IEEE80211>
  <IEEE80211>
    <ConsortiumOID>00-1B-C5-04-60</ConsortiumOID>
    <MinRSNProto>CCMP</MinRSNProto>
  </IEEE80211>
  <IEEE8023-NetworkID>testnet</IEEE8023-NetworkID>
</CompatibleUses>

```

```
<ProviderLocation>
  <Longitude>10.7218382</Longitude>
  <Latitude>59.9399477</Latitude>
</ProviderLocation>

<ProviderLogo mime="image/jpeg" encoding="base64">
  klasjdfh7wa04564wlsaiurrrxvyjkgh
</ProviderLogo>

<TermsOfUse>
  Do whatever you want!
</TermsOfUse>

<Helpdesk>
  <EmailAddress lang="any">stefan.winter@restena.lu</EmailAddress>
  <WebAddress lang="fr">
    http://www.restena.lu/restena/fr/FR-eduroam-setup-main.html
  </WebAddress>
  <Phone lang="fr">+352 424409 1</Phone>
  <Phone>+352 424409 99</Phone>
</Helpdesk>

</EAPIdentityProvider>
</EAPIdentityProviderList>
```

Appendix C Discussion Paper on Scalability of RADIUS Realms

Evolved handling of non country-code-routed domains in global eduroam

- Proposal for GeGC consideration -

Background

eduroam infrastructure RADIUS servers inspect an incoming access request to determine how to reach the authoritative eduroam IdP server. The inspection dissects the attribute User-Name and determines the realm part (everything right to the “@” sign).

Example: User-Name = stefan.winter@education.lu

-> Realm = education.lu

The eduroam request routing of a realm is based on the fact that realms have the format of domain names in DNS; in particular that they have a top-level domain (TLD) behind the last “.” character. Eduroam authentication authority is partitioned by TLD.

Example: Realm = education.lu

-> responsible server: Luxembourg federation server

In the eduroam traditional “hierarchy” routing model, there is a well-defined destination for most top-level domains (that is, for all TLDs which map to a geographic region/country, the so-called country-code TLDs (ccTLD), plus the .cat domain); requests are routed to the responsible server for that TLD, and then delivered to the IdP server by that TLD server.

There are no well-defined destinations for TLDs which are not ccTLDs or .cat. This is hereafter referred to as generic TLDs, (gTLD), even though it excludes the .cat domain.

Example: education.lu -> ccTLD realm

 institute.net -> gTLD realm

Problem statement

There are educational institutions which use gTLD domains as their primary domains and who want to use these same domains as user identifiers for eduroam use. By inspection of such realms, it is not possible to determine which federation's TLD server to route the request to. Such domains will thus by default fail to work in international roaming. They will work in national roaming contexts because then the request never leaves the TLD server which knows where to send the request to. Users will typically not notice any problems until international roaming is attempted.

Historical workaround

The current practice regarding gTLD realms involves the creation of exceptions in the international RADIUS request routing tables. The aggregation servers which handle traffic beyond national scale (regional proxy servers) need to maintain and synchronise with each other a list of gTLD realms and the ccTLD servers which are able to authenticate users from that realm. This has proven to work in principle; there are currently numerous entries in the exception list.

However, several incidents of non-working international roaming recently serve as evidence that the complexity and synchronisation need for these entries is getting out of hand; this workaround does not scale with the number of exception entries.

Numerous other approaches of handling these realms can be imagined; some have been used in a sparse way in practice.

Solution 1: assign gTLDs to ccTLD servers in a fixed mapping

Part of the complexity of the routing table stems from the fact that the gTLD domains by nature don't always map to the same federation (ccTLD) server; e.g. The ".net" and ".org" domains have RADIUS realms in a number of different federations. This translates into the synchronisation need between the regional servers; they basically need to know which .net to route to which world region proxy server; and these regional servers in turn need to know which country to route the request to.

One possible mitigation of the problem is to treat gTLD like ccTLD domains: each gTLD is handled by one server as if it was part of a federation; all requests worldwide for the corresponding gTLD would be routed through that server; only the operator of that server would need to know how to reach the IdP that can ultimately handle the request.

This approach has downsides on both the efficiency and the administration scale though:

- Requests for gTLD realms would possibly take sub-optimal paths through the routing infrastructure because the server responsible for the gTLD might reside in a different world region than both the SP and IdP server. This introduces longer roundtrip times for the authentication requests in question.
- Even though the gTLDs in question are part of numerous federations, and bound by differing national policies, their technical handling would need to be handled by the one server serving this gTLD. As a consequence, whoever operates the gTLD server would do a service for other federations without immediate benefit for itself. It would require administrative signalling by federations to the gTLD operator to add or remove entries.
- If a federation usually imposes specific policies for its own national SPs or IdPs by e.g. filtering attributes for its federation members, it could not do so if that IdP is routed not via its own servers but the gTLD server.

Solution 2: Discontinuing the use of gTLD realms for int'l roaming

Another possible solution is to try and force newly participating institutions not to use gTLD realms. This has been tried in the past but usually raises sensitivities and does not appear to work well.

A slightly different, but equally unsatisfying approach, which unfortunately defeats the purpose of eduroam in large parts, would be to officially state: gTLD realms can be used, but are only guaranteed to work in national roaming.

Such an approach would in case need to preserve the existing exceptions and would only apply to newly joining organisations.

There is a significant risk that organisations would be appalled by either of the two consequences (giving up their well-known domain name for eduroam or not having international roaming).

Solution 3: Offloading routing information to DNS (“Dynamic Discovery”)

A recent addition to eduroam, RADIUS over TLS with Dynamic Discovery, does not rely on static routing tables inside a RADIUS server configuration to route requests to their proper destination. Instead, the participating institution adds one single DNS resource record to their own domain's DNS zone which states, paraphrased: “eduroam authentication for this domain is handled by server X”.

Several countries in Europe have consistently rolled out this DNS entry for their participating institutions; about 10 countries in Europe already query this information and use it for request routing. The approach has proven to be more efficient than the static “hierarchy” routing for international roaming, mostly because it bypasses the need to send the request from the SP country to the regional proxy server and back to the IdP's country; instead, the two countries get into direct contact.

For ccTLD realms, dynamic discovery merely improves efficiency of the request routing as stated in the previous paragraph. However, for gTLD realms, it offers the promise of completely obsoleting all exception routing entries because the mapping of the realm to a responsible ccTLD server is then a self-service operation for the IdP, not requiring any aggregation.

The steps to enable dynamic discovery are twofold:

1) the institution needs to add a DNS resource record of type Network Authority Pointer (NAPTR); the structure of this entry is slightly more complex than a typical “A” record but can be configured on many DNS server implementations just fine. Example of a NAPTR for the realm “education.lu” (live data):

```
swinter@aragorn:~> dig education.lu NAPTR
;; QUESTION SECTION:
;education.lu.          IN NAPTR
;; ANSWER SECTION:
education.lu. 43200 IN NAPTR 100 10 "s" "x-eduroam:radius.tls" ""
_radsec._tcp.eduroam.lu.
```

2) the national ccTLD server which is pointed to by this record needs to be able to process incoming RADIUS/TLS requests; which means it needs to be in possession of an accredited eduroam operator X.509 certificate and needs to be configured to enable incoming RADIUS/TLS connections. This is only a single server (or a few, if the national deployment has multiple failover servers); it is not of any concern for the IdP.

Note that:

- the institution server does not need any RADIUS/TLS certificates, and in fact does not need to be aware of the existence of that protocol at all. The institution creates a normal RADIUS uplink to its national server.
- the national server only needs to accept incoming connections, not do dynamic discovery itself. However, since both ways (incoming and outgoing) use the same certificate, and it is a simple configuration matter to enable the outgoing part, it is most practical to enable both directions.

Since this concept is in actual production use for some (but not all) gTLD realms with a “home” in Europe, there is already some information about a possible drawback:

Some gTLD realm IdPs have reported that their DNS server implementation does not permit to add resource records of type NAPTR. Such IdPs would obviously not be able to announce their routing over DNS then, making them incompatible with this deployment option.

It remains to be discussed how such IdPs should be handled. One suggestion is

- for gTLD IdPs already connected today, keep their exceptions entry in the static routing (principle of least surprise); however recommend adding NAPTRs so that the static exceptions can be deleted when possible
- for gTLD IdPs newly trying to join but with no suitable DNS server:
 - add an exception anyway? -or-
 - deny admission to eduroam? -or-
 - inform that they will only have national roaming then?

This one drawback is probably the biggest obstacle.

For the certificate matters, a CA is in place and it can issue certificates to all eduroam national servers world-wide.

RADIUS/TLS on the national server requires RADIUS software which is capable of RADIUS/TLS; two such products are available (commercial: Radiator; open source: radsecproxy) and a third one is in late stages of development (FreeRADIUS 3.0). This covers a vast majority of national proxy servers.

References

- [80211-2012]** IEEE Standard for Information technology – Telecommunications and information exchange between systems Local and metropolitan area networks – Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Standard 802.11-2012, 2012
<http://standards.ieee.org/getieee802/download/802.11-2012.pdf>
- [80211u-2011]** IEEE Standard for Information technology – Telecommunications and information exchange between systems Local and metropolitan area networks – Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 9: Interworking with External Networks
<http://standards.ieee.org/getieee802/download/802.11u-2011.pdf>
- [B/OSS]** Wikipedia, “Operations support system”
http://en.wikipedia.org/wiki/Operations_support_system
- [CAT-MAN]** Stefan Winter, et al., “A guide to eduroam CAT for institution administrators”
<https://confluence.terena.org/display/H2eduroam/A+guide+to+eduroam+CAT+for+institution+administrators>
- [DJ3.1.1]** S. Winter, T. Wolniewicz, I. Thomson, “Deliverable DJ3.1.1: RadSec Standardisation and Definition of eduroam Extensions”
https://geant3.archive.geant.net/Media_Centre/Media_Library/Media%20Library/GN3-09-213-DJ3_1_1_RadSec_Standardisation_and_Definition_of_eduroam_Extensions_20091106091343.pdf
- [DJ3.1.2,1]** Stefan Winter, Ed., Zbigniew Oltuszyk, Tomasz Wolniewicz, Gunnar Bøe, Gurminder Singh, “Deliverable DJ3.1.2,1: Roaming Developments”
https://geant3.archive.geant.net/Media_Centre/Media_Library/Media%20Library/GN3-10-304%20DJ3.1.2-1%20%20Roaming%20Developments%2024FEB11.pdf
- [DJ3.1.2,2]** Stefan Winter, Ed., Zbigniew Oltuszyk, Tomasz Wolniewicz, Gunnar Bøe, Gurminder Singh, “Deliverable DJ3.1.2,2: Roaming Developments, Second Edition”
https://geant3.archive.geant.net/Media_Centre/Media_Library/Media%20Library/GN3-11-354_DJ3-1.2-2_Roaming_Developments_v1.0.pdf
- [DYN]** Internet Engineering Task Force – Work in Progress, “NAI-based Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS”, S. Winter, M. McCauley
<http://datatracker.ietf.org/doc/draft-ietf-radext-dynamic-discovery/>

- [EDU-IETF]** Internet Engineering Task Force – Work in Progress, “The eduroam architecture for network roaming”, K. Wierenga, S. Winter, T. Wolniewicz
<http://tools.ietf.org/html/draft-wierenga-ietf-eduroam-00>
- [freeDiameterTest1]** <http://www.freediameter.net/trac/wiki/TBSimple>
- [freeDiameterTest2]** <http://www.freediameter.net/trac/wiki/TBEAP>
- [GN2-DJ5.1.6]** S. Winter et al, “Deliverable DJ5.1.6: Evaluation of New Roaming Technologies and Possible Integration into AAI”
http://www.geant2.net/upload/pdf/GN2-08-051v2-DJ-5-1-6-Evaluation_of_New_Roaming_Technologies_and_Possible_Integration_into_AAI.pdf
- [GN2-DJ5.4.1]** T. Kersting, Ed., et al, “Deliverable DJ5.4.1: “Advanced Technologies Overview”
http://www.geant2.net/upload/pdf/GN2-07-142v3-DJ5-4-1_Advanced_Technologies_Overview_20071009174112.pdf
- [HS20]** Hotspot 2.0 Technical Specification v1.0.0, Wi-Fi Alliance, 2012
<https://www.wi-fi.org/knowledge-center/published-specifications>
- [IANA-EAP]** Extensible Authentication Protocol (EAP) Registry
<http://www.iana.org/assignments/eap-numbers/eap-numbers.xml>
- [IEEE-RA]** <http://standards.ieee.org/develop/regauth/general.html>
- [PP-DEPLOY]** Wi-Fi CERTIFIED Passpoint™ (Release 1) Deployment Guidelines Version 1.0, Wi-Fi Alliance® Hotspot 2.0 Technical Task Group, 2012
<https://www.wi-fi.org/knowledge-center/published-specifications>
- [PTEAP]** Internet Engineering Task Force – Work in Progress, “PT-EAP: Posture Transport (PT) Protocol For EAP Tunnel Methods”, N. Cam-Winget, P. Sangster
<http://datatracker.ietf.org/doc/draft-ietf-nea-pt-eap/>
- [RADNAI]** Internet Engineering Task Force – Work in Progress, “The Network Access Identifier”, A. DeKok
<http://tools.ietf.org/html/draft-ietf-radext-nai-02>
- [RDTLS]** Internet Engineering Task Force – Work in Progress, “DTLS as a Transport Layer for RADIUS”, A. DeKok
<http://tools.ietf.org/html/draft-ietf-radext-dtls-04>
- [RFC2865]** Network Working Group, RFC 2865, Standards Track, Draft Standard, “Remote Authentication Dial In User Service (RADIUS)”, C. Rigney, S. Willens, A. Rubens, W. Simpson
<http://tools.ietf.org/html/rfc2865>
- [RFC3588]** Network Working Group, RFC 3588, Standards Track, Proposed Standard, “Diameter Base Protocol”, P. Calhoun, J. Loughney, E. Guttman, G. Zorn, J. Arkko
<http://tools.ietf.org/html/rfc3588>
- [RFC3748]** Internet Engineering Task Force – ISSN 2070-1721 * RFC3748, “Extensible Authentication Protocol (EAP)”, B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz
<http://tools.ietf.org/html/rfc3748>
- [RFC4072]** Network Working Group, RFC4072, Standards Track, “Diameter Extensible Authentication Protocol (EAP) Application”, P. Eronen, Ed., T. Hiller, G. Zorn
<http://www.ietf.org/rfc/rfc4072.txt>
- [RFC5931]** Internet Engineering Task Force – ISSN 2070-1721 * RFC6613, “Extensible Authentication Protocol (EAP) Authentication Using Only a Password”, D. Harkins, G. Zorn
<http://tools.ietf.org/html/rfc5931>

- [RFC6613] Internet Engineering Task Force – ISSN 2070-1721 * RFC6613, “RADIUS over TCP”, A. DeKok
<http://tools.ietf.org/html/rfc6613>
- [RFC6614] Internet Engineering Task Force – ISSN 2070-1721 * RFC6614, “Transport Layer Security (TLS) Encryption for RADIUS”, S. Winter, M. McCauley, S. Venaas, K. Wierenga
<http://tools.ietf.org/html/rfc6614>
- [RFC6733] Internet Engineering Task Force – ISSN 2070-1721 * RFC6733, Standards Track, Proposed Standard, “Diameter Base Protocol”, V. Fajardo, Ed., J. Arkko, J. Loughney, G. Zorn, Ed.
<http://tools.ietf.org/html/rfc6733>
- [RFC6876] Internet Engineering Task Force – ISSN 2070-1721 * RFC6876, “A Posture Transport Protocol over TLS (PT-TLS)”, P. Sangster, N. Cam-Winget, J. Salowey
<http://tools.ietf.org/html/rfc6876>
- [TEAP] Internet Engineering Task Force – Work in Progress, “Tunnel EAP Method (TEAP) Version 1”, H. Zhou, N. Cam-Winget, J. Salowey, S. Hanna
<http://tools.ietf.org/html/draft-ietf-emu-eap-tunnel-method-06>
- [TIETO] <http://www.tieto.com/industries/telecom-0/tietos-solutions-network-equipment-providers/tieto-signaling-solutions-services-and-products/signaling-routers/diameter-signaling-controller>
- [TNC2013] Trans-European Research and Education Networking Association, “Looking into the Future: Exploring Enhancements to the eduroam Infrastructure”, C. Phillips, S. Winter
<https://tnc2013.terena.org/core/presentation/65>
- [WPA_S] Linux WPA/WPA2/IEEE 802.1X Supplicant
http://hostap.epitest.fi/wpa_supplicant/

Glossary

3GPP	3 rd Generation Partnership Project
3GPP2	3 rd Generation Partnership Project 2
802.11	A set of standards for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5GHz frequency bands
AAA	Authentication, Authorisation and Accounting
ABFAB	Application Bridging for Federated Access Beyond Web
ACE	Adaptive Communication Environment
AD	Active Directory
ANQP	Access Network Query Protocol
ANT	Access Network Type
AP	Access Point
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
AUP	Acceptable Use Policy
B/OSS	Business/Operations Support System
BSSID	Basic Service Set Identification
BYOD	Bring Your Own Device
CA	Certification Authority
CAT	Configuration Assistant Tool
CCMP	Counter Cipher Mode with Block Chaining Message Authentication Code Protocol
ccTLD	Country-Code Top-Level Domain
CER	Capability Exchange Request
CI	Consortium Identifier
DANE	DNS-based Authentication of Named Entities
DB	Database
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNSSEC	DNS Security Extensions
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
EAP-EKE	EAP Encrypted Key Exchange
EAP-FAST	EAP Flexible Authentication via Secure Tunnelling
EAP-FASTv2	EAP Flexible Authentication via Secure Tunnelling version 2 a derivate of EAP-FAST
EAP-PWD	EAP Authentication using only a password

EAP-TLS	EAP Transport Layer Security
EAP-TTLS	EAP Tunnelled Transport Layer Security
eduroam	Roaming confederation aiming to provide mutual roaming network access to its members – users from the education and research sector world-wide
eduPKI	Education Public Key Infrastructure
EMU	EAP Method Update Working Group
ETLRS	European Top-Level Server
F-Ticks	Federated Ticker System (eduroam's advanced statistics tool)
FLRS	Federation Top-Level RADIUS Server
FreeRADIUS	Open Source version of RADIUS
GAS	Generic Advertisement Service
GÉANT	Gigabit European Advanced Network Technology 2 is the main European network for research and education purposes, successor to the pan-European multi-gigabit research network GÉANT
GIT	A free and open source distributed version control system
GN2	Second GÉANT Project, September 2004 – March 2009
GN3	Third GÉANT Project, April 2009 – March 2013
GeGC	Global eduroam Governance Committee
GNU	GNU's Not Unix – a Unix-like computer operating system developed by the GNU project
GTC	Generic Token Card
gTLD	Generic Top-Level Domain
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
IdP	Identity Provider
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISO/OSI	International Organisation for Standardisation/Open System Interconnection Reference Model
ISP	Internet Service Provider
Janet(UK)	UK National Education and Research Network
JRA3	GN3 Joint Research Activity 3 Multi-Domain User Application Research
JRA3 T1	JRA3 Task 1, Roaming Developments
LAN	Local Area Network
LTE	Long-Term Evolution
M	Month
MAC	Media Access Control address
MIME	Multipurpose Internet Mail Extensions
Moonshot	Project Moonshot is a JANET(UK)-led initiative, in partnership with GN3 and others, to develop a single unifying technology for extending the benefits of federated identity to a broad range of non-Web services, including Cloud infrastructures, High Performance Computing & Grid infrastructures and other commonly deployed services including mail, file store, remote access and instant messaging.
MS IAS	Microsoft Internet Authentication Service (Microsoft's implementation of a RADIUS server)

MS NPS	Microsoft Network Policy Server (Microsoft's implementation of a RADIUS server, renamed from MS IAS in Windows Server operating systems later than Windows Server 2003)
MTI	Mandatory to Implement
NAI	Network Access Identifier
NAPTR	Name Authority Pointer
NAS	Network Access Server
NASREQ	Network Access Server Requirements
NAT	Network Address Translation
NEA	Network Endpoint Assessment
NEA WG	Network Endpoint Assessment Working Group
NFC	Normalised Form C
NORDUnet	Nordic Infrastructure for Research & Education
NREN	National Research and Education Networks
NSIS	Nullsoft Scriptable Install System
O&M	Operations and Management
OI	Organisation Identifier
OPSAWG	Operations & Management Area Working Group
OSS	Operations Support System
OT	Operations Team
OUI	Organisation-Unique Identifier
PA	Posture Attribute
PAC	Protected Access Credential
PB	Posture Broker
PEAP	Protected Extensible Authentication Protocol
PHP	Personal Home Page
PKI	Public Key Infrastructure
PT	Posture Transport
PT-EAP	Posture Transport Protocol for EAP Tunnel Methods
PT-TLS	Posture Transport Protocol over TLS
QR	Quick Response
R&D	Research and Development
RADIUS	Remote Authentication Dial-In User Service
RadSec	Protocol for transporting RADIUS datagrams over TCP and TLS.
RFC	Request for Comments
S-NAPTR	Straightforward Name Authority Pointer
SA3	GN3 Service Activity 3 Multi-Domain User Applications
SA3 T2	SA3 Task 1 eduroam
SAML	Security Assertion Mark-up Language
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SLAAC	StateLess Address Auto-Configuration
S/MIME	Secure/Multipurpose Internet Mail Extensions
SOHO	Small Office, Home Office
SP	Service Provider
SQL	Structured Query Language

SSID	Service Set Identifier
TCP	Transmission Control Protocol
TEAP	Tunnelled EAP Method
TERENA	Trans-European Research and Education Networking Association
TKIP	Temporal Key Integrity Protocol
TLD	Top-Level Domain
TLS	Transport Layer Security
TNC2013	TERENA Networking Conference 2013
TTLS-PAP	Tunnelled Transport Layer Security with Password Authentication Protocol
TNC	Trusted Network Connect
UCS	Universal Character Set
UDP	User Datagram Protocol
UNIX	A Multitasking, Multi-user Computer Operating System
URL	Uniform Resource Locator
UTF-8	UCS Transformation Format—8-bit
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WAN	Wide Area Network
WG	Working Group
WGLC	Working Group Last Call
Wi-Fi	A trademark of the Wi-Fi Alliance and the brand name for products using the IEEE 802.11 family of standards
WIRE	Wireless Internet Research & Engineering
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access – security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks
WPA2	Wi-Fi Protected Access II – security protocols and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. A derivate of WPA.
WPA2/AES	Advanced Encryption Standard used by WPA2
WPA/TKIP	Temporal Key Integrity Protocol used by WPA
X.509	Public Key Infrastructure Certificate and Certificate Revocation List
XML	Extensible Mark-up Language
XMLDSig	XML syntax for digital signatures