24-02-2011

Deliverable DJ3.1.2,1: Roaming Developments

Deliverable DJ3.1.2,1 v1.0

Contractual Date:	31-10-2010
Actual Date:	24-02-2011
Grant Agreement No.:	238875
Activity:	JRA3
Task Item:	T1
Nature of Deliverable:	R
Dissemination Level:	PU
Lead Partner:	RESTENA
Document Code:	GN3-10-304
Authors:	Stefan Winter (RESTENA, ed.), Miroslav Milinovic (Srce/CARNet), Dubravko Penezic (Srce/CARNet), Wenche Backman (CSC/Funet), Tomasz Wolniewicz (PIONIER), Maja Gorecka-Wolniewicz (PIONIER), Zbigniew Ołtuszyk, (PIONIER), Paul Dekkers (SURFnet), Shannon Milsom (DANTE)

Abstract

This deliverable covers research and development activities undertaken by JRA3 T1 to support new and emerging eduroam® services supplying roaming access to wireless networks. The task includes monitoring developments in the network industry, producing software to improve eduroam operations, and contributing to standards bodies.

Table of Contents

Table of Figures

Table of Tables

Executive Summary

This deliverable provides a summary of research and development activities of Roaming Developments (JRA3 T1). It covers tasks that support new and emerging eduroam® services. JRA3 T1 supports eduroam Services (SA3 T2), in which the core business is the supply of roaming access to wireless data networks.

Activities include monitoring developments in the network access industry, contributing to standards bodies, supporting and seeking new possible services for eduroam operations, and liaising with other GÉANT activities. This document describes the activities undertaken by JRA3 T1 for this task.

Advances in wireless and wired network services provide new challenges and opportunities by way of changes, developments, threats and problem resolution. JRA3 T1 is tasked with producing and implementing software to support eduroam operations in such developments. Additional features such as CUI support to RADIUS and F-Ticks to collect usage statistics are included in this task.

JRA3 T1 influences the network access industry's evolution by participating and contributing to technology standards bodies such as IEEE and IETF. Key areas for input are in standardisation and internationalisation of protocols.

JRA3 T1 works to improve authentication. It monitors developments in eduroam core authentication protocol (EAP) to determine the benefit to eduroam operations, tests newly developed EAP methods such as EAP FAST, reviews speed and reliable performance. It watches and investigates interesting technology developments such as 3G mobile access to spread network coverage beyond campus bounds.

Liaising with other GÉANT activities, JRA3 T1 works with:

- SA3 T2 to improve eduroam operations.
- SA3 T1 eduPKI to define server certification for eduroam servers.
- SA2 T4 Considering how to report to Computer Security Incident Response Teams in case of network abuse by authenticated eduroam user.

1 Introduction

This deliverable provides a summary of the efforts undertaken in Roaming Developments (JRA3 Task 1) from the beginning of the project until October 2010 (M1-M19). It is intended to provide a thorough insight into the research and development activities. The results of these activities serve as support actions towards eduroam® operations (SA3 Task 2).

eduroam has been an operational service since GÉANT2. Its core focus is in the supply of roaming access to wireless networks, but it has also been deployed on other media, such as IEEE 802.3 wired networks. There are significant advances in the wireless LAN industry segment and eduroam requires to be informed of and, if applicable, to influence the industry development to evolve the service and provide the best possible user experience to the customers in the education and research community. JRA3 T1 assumes the role of the R&D unit for eduroam in Europe. The activities pursued in JRA3 T1 include:

- Monitoring developments in the industry.
- Providing active input into the industry.
- Investigating new possible eduroam service elements.
- Producing software for eduroam operations.
- Liaising with other GÉANT activities.

Given the technical nature of industry standard investigation, the activities also need to go into depth where necessary.

The document is structured as follows:

- Section 2 contains a summary of interactions with Standards Bodies, both regarding passive participation (watching briefs) and active participation.
- Section 3 describes specific software implementations carried out by JRA3 T1 to support SA3 T2.
- Section 4 looks at the core protocol for eduroam authentication: the Extensible Authentication Protocol (EAP) to determine whether newly developed EAP types can provide a benefit for eduroam operations.
- Section 5 lists various developments which are either carried out by individual federations (and which are merely monitored as interesting technologies by JRA3 T1), and conceptual outreach topics.
- Section 6 details the liaison activities which were carried out by JRA3 T1.

Some of JRA3 T1's efforts have already been covered in detail in *RadSec Standardisation and Definition of eduroam Extensions* [DJ3.1.1] and are not described here in detail.

It is understood that the relatively long reporting period for this deliverable, 19 months, makes the document somewhat bulky. The next edition of this deliverable is scheduled for M30, covering only 11 months of developments, which is expected to be easier to digest.

2 Contribution to Standards Bodies

eduroam is based exclusively on widespread IT industry standards; mostly those of the Institute of Electrical and Electronics Engineers (IEEE) for the lower ISO/OSI layers and Internet Engineering Task Force (IETF) for the higher ISO/OSI layers. These standards naturally evolve over time. It is important to:

- Monitor the standards which are in use to evaluate whether any changes introduce either a threat to operations or provide new opportunities for service enhancement.
- Actively influence the development of these standards to make them a better fit to eduroam operations.

JRA3 T1 maintains watching briefs on several technologies to address:

- Case a: These are described in section 2.1. Personnel of JRA3 T1 personnel actively contribute to standards bodies and/or trials of new concepts that might eventually be picked up for standardisation to address
- Case b: These are described in section 2.2.

2.1 Watching Briefs

2.1.1 IETF: NEA/Federated TNC

Trusted Network Connect (TNC) is an open architecture for Network Access Control with the aim of providing a means to evaluate terminals (endpoints) before they are allowed on the network. This way, the security configuration of the terminal can be evaluated in advance, e.g. it can be verified that the firewall is on and a virus scanner with recent antivirus definitions is active, etc. The TNC architecture has been defined by the Trusted Computing Group (TCG), which is an international industry consortium.

Since the TCG is an industry consortium and not a standardisation body, the TNC specifications could be more widespread if they were approved as standards. The NEA (Network Endpoint Assessment) working group of the IETF have similar standardisation efforts as the TCG. As of March 2010, two of the TCG documents have been accepted:

- PA-TNC (Posture Attribute) protocol, which transports information between a Posture Collector in an NEA client and a Posture Validator in an NEA server.
- PB-TNC (Posture Broker) protocol, which aggregates posture attributes and carries the PA protocol.

One further protocol, the PT (Posture Transport) protocol will be defined, but it will likely be a protocol which wraps the PB-TNC to fit into an existing standard transport protocol. Two candidates for this transport protocol are:

- EAP, which carries NEA PB after the actual authentication has taken place. This is a mechanism known as method chaining.
- TLS

The TCG have expanded their efforts to provide a means for terminal assessment before network connection also within a federation. The corresponding concept is called Federated TNC and it provides a mechanism to represent and transport information about users and machines between security domains. In Federated TNC, in the roaming case, there are three main players:

- The endpoint to be connected to the network.
- The Asserting Security Domain (ASD), which has knowledge of the endpoint's security posture information (SPI) and which is located at the home organisation of the user (for eduroam, the Identity Provider).
- The Relying Security Domain (RSD) which requires knowledge of the endpoint's SPI. This is the hotspot operator, i.e. the organisation that the endpoint user is visiting (for eduroam, the eduroam Service Provider).

In addition to security information, user attribute information can be requested using the three players. Since Federated TNC is an expansion of TNC, the same transport protocols will be used, i.e. the PA-TNC and PB-TNC protocols that were recently standardised within IETF, as well as the forthcoming PT protocol.

Federated TNC provides several possibilities for eduroam. In particular, the following two separate use cases are of interest:

- Security: Federated TNC can be used to enhance the level of security inside eduroam. The security policy of own and visiting users' terminals can be checked at network access along with the authentication.
- Authorisation with user attributes: The identity provider can provide information regarding the position held by the person. For example, is he a student, a member of the staff or a manager? The service provider can assign services based on the value of the attribute.

However, there are no known implementations of Federated TNC to date. JRA3 T1 has monitored several emerging projects around federated TNC to be able to test early implementations as they become available.

2.1.1.1 *OpenTC*

The Open Trusted Computing (OpenTC) consortium, which was a research and development project financed by the European Commission through the 6th framework programme, planned a follow-up project but the project preparations failed because of disagreements. In addition, the German research organisation Fraunhofer Society has been planning projects related to Federated TNC, but so far no funding has been secured.

2.1.1.2 *FreeRADIUS*

eduroam is expected to be the first or one of the first federations to implement and utilise Federated TNC. A starting point for this scenario is to implement Federated TNC in FreeRADIUS, but as of this writing, there is no production-ready implementation. However, this situation is expected to improve in the future because Janet(UK) has been working on the (non-federated) Microsoft variant "Statement of Health". JRA3 T1 is making RADIUS attributes from the TERENA Enterprise Object Identifier (OID) space available to Janet(UK) to permit extension of TNC to a federated scenario.

2.1.1.3 *IETF NEA Working Group*

There is a chance that the NEA working group within IETF will pick up Federated TNC, as it has done with TNC. This requires a re-charter of the working group and is seen as an option by the working group chairs. Even in this case, a real standardisation of Federated TNC is many years ahead.

2.1.2 IEEE 802.1X Revision

The IEEE 802.1X standard is the major cornerstone of the eduroam concept. The first edition of this standard is from 2001 and predates the beginning of eduroam (2003). The standard saw a minor revision in 2004. That revision only contained clarifications to the original issue and had little to no impact on actual equipment behaviour.

During the timeframe which coincided with GN3's Year 1, the IEEE worked on a major conceptual overhaul of IEEE 802.1X. JRA3 T1 investigated the draft of the new standard in various stages of completion and has fed critical opinions on various details of the upcoming standard into the IEEE balloting process by proxy via a voting member.

Three of the major changes in the standard are particularly noteworthy and deserve inclusion in this deliverable. They are described in the next three sections.

2.1.2.1 *Changes of Behaviour on Wired Networks*

With IEEE 802.1X-2004 and previous standards, user experience on wired networks was substantially different from wireless networks.

Wireless networks use IEEE 802.11 beacon frames to announce the exact properties of a network. One of those properties is the network name. In eduroam, the brand name "eduroam" is also used as the network name throughout the infrastructure, enabling users to recognise that a given network is part of eduroam. The network name is only a string and can be used by any other party, but for these cases the mutual authentication will enable a user to verify that he is connected to a genuine eduroam network. If a user connects to multiple wireless networks and has different digital identities, he can configure these identities on a per-network-name basis.

On wired networks, no such beacon frames exist. Consequentially, there is no in-band hint for a user that a given network plug belongs to any roaming consortium or that it is enabled for IEEE 802.1X authentication in the first place. Users must connect a network cable on a trial and error basis to find out whether or not they are connected to an IEEE 802.1X network, and to determine whether this network might be eduroam or a different network. In addition, it is not easily possible to configure multiple digital identities on a wired port. There is usually the IEEE 802.1X wired configuration on a client device, making switching between multiple networks very cumbersome.

For this reason, until now eduroam on wired networks was not heavily advertised. Several countries do use the concept though and it is expected that a five-digit number of wired IEEE 802.1X eduroam ports is set up. Communicating that a port is wired eduroam is done out-of-band, for example using leaflets or stickers.

IEEE 802.1X-2010 introduces the beacon concept into wired networks. When supplicants get equipped with the appropriate features, very similar mechanisms for detecting networks and selecting digital identities as in wireless networks can be used in wired networks. This makes a wide-spread adoption of wired eduroam more probable.

It remains to be seen how old and new versions of supplicants and authenticators can interoperate. JRA3 T1 is planning to conduct field tests on actual hardware to assess compatibility.

2.1.2.2 *Introduction of Out-of-Band Authentication*

Prior to IEEE 802.1X-2010, the standard stood for one, well-defined way of attaching a device to a network and included a lock-step protocol (EAPoL) to perform the authentication of the user/computing device.

With the beacon frames, IEEE 802.1X-2010 enables communication that an authentication is not happening with the established EAPoL mechanism, but instead via an out-of-band solution. This means that a network port is opened immediately, an IP address is assigned and the user is subsequently redirected to a website to authenticate against. This operation mode allows for a tighter integration between web-based captive portals and the traditional IEEE 802.1X EAPoL mechanisms.

This development is perceived as dangerous to eduroam, since the term IEEE 802.1X could previously be used unambiguously to identify the secure, enterprise-level authentication that is eduroam. The term may very well lose that strict meaning over time, leading to user and administrator confusion. At that point, eduroam's authentication type should rather be communicated as “IEEE 802.1X / EAPoL”.

2.1.2.3 *Encryption on the Medium*

IEEE 802.1X-2004 and previous standards do not encrypt user's payload data on wired networks. Eavesdropping on wired networks can be considered a much smaller threat than on wireless networks because it is not a broadcast media and traffic typically does not pass by other connected stations.

However, the threat of exposing payload traffic is not zero. In 2006, the IEEE created the standard IEEE 802.1AE, Media Access Control Security (MAC) to encrypt and secure data. With IEEE 802.1X-2010, the

mechanisms of that standard have been integrated into IEEE 802.1X. For IEEE standards publications in electronic format, see [802STAN].

2.1.2.4 *Conclusion*

The new revision of IEEE 802.1X provides interesting opportunities for a larger roll-out of wired eduroam. However, the new standard also raises questions regarding usability. JRA3 T1 will continue to monitor the development of supplicants and authenticator hardware and conduct interoperability tests. If the new beacon mechanisms turn out to provide substantial benefit for the eduroam target audience, it is envisaged to report the corresponding results to SA3 T2 for consideration to deploy.

2.1.3 IETF: Alternative RADIUS Transports

Despite the active contributions in the IETF regarding the protocol RADIUS/TLS (see section 2.2.1), JRA3 T1 also keeps a watching brief on upcoming alternative transports for RADIUS.

The only candidate at present is RADIUS/DTLS, which uses very similar encryption to RADIUS/TLS to encrypt RADIUS packets, but still transmits the packets over UDP. Author Alan DeKok proposed this in the IETF several years ago and submitted a preliminary version of an internet-draft. Until the 78th IETF meeting in July 2010 in Maastricht, The Netherlands, it was an individual submission only. The draft leans heavily on the RADIUS/TLS draft in an attempt to keep most characteristics of secure transport identical. It only highlights the necessary differences in operation when transporting encrypted data over an unreliable transport.

A call for adoption was made to consider RADIUS/DTLS as an IETF effort. After successful completion of the call for adoption, a revised draft was published on 8 Oct 2010. See [RADDTLS]. For a further overview of alternative RADIUS transports, see section 2.1.2 in [DJ3.1.1].

2.1.4 Internationalisation Challenges

Many protocols which have been developed for use on the internet did not initially consider characters from outside the ASCII character table. Examples for such protocols include the Domain Name System (DNS), and email. Retrofitting such protocols with support for non-ASCII characters often turns out to be a complex and error-prone task.

The DNS has been redefined to include Internationalised Domain Names (IDNs) and has recently been revised to address flaws in the original IDN specification.

Email has been redesigned in several stages to include non-ASCII characters in the local part of the address (for example, jürgen@tu-muenchen.de) and subsequently for the domain names themselves (for example, jürgen@tu-münchen.de).

As the use of internationalised domain names becomes commodity and users gain familiarity in using them, there is an increasing probability that site administrators will also want to use these identifiers as eduroam realms for their users. Research conducted near the end of GN2 (March 2009) in JRA5 revealed that the use of

internationalised names in eduroam realms leads to unpredictable results. As a result, their use was temporarily discouraged in the Admin Advisory 002. For more information, see [ADV002].

JRA3 T1 is charged with monitoring the situation in the IETF and, where possible, to influence the development towards a working internationalisation framework in the chain of protocols involved in eduroam authentication: IEEE 802.1X, EAPoL, RADIUS.

Unfortunately, there is not yet a clear path towards working internationalisation. The weakest link in the process is the IEEE 802.1X supplicant. Several implementations, including Microsoft Windows (up to at least Windows Vista), are known to produce invalid character encodings during authentication (sending in the system locale instead of UTF-8) or perform no input validation of the contents of configured identities (NetworkManager).

It is also unspecified how internationalised realms are to be encoded within UTF-8. There are several encodings for the same domain name, semantically identical, but bitwise different. This makes comparison operations difficult.

The active contributions which are carried out by JRA3 T1 in the IETF take internationalisation into consideration. This affects primarily the Dynamic Discovery part of RADIUS/TLS. For more information, see section 2.2.1).

2.2 Active Contributions

2.2.1 Ongoing RADIUS/TLS (RadSec) Standardisation

A wrap-up of the work undertaken in this work item up until October 2009 is in section 2 of [DJ3.1.1] and is not repeated here.

In the meantime, two major comments were raised that need a resolution.

Firstly, a question about the use of UDP and TCP ports was raised. RADIUS/UDP uses three distinct ports for RADIUS Authentication (UDP/1812), RADIUS Accounting (UDP/1813) and Change of Authorisation (UDP/3799). RADIUS/TLS uses one single port for all three types of packets (TCP/2083).

The discussion evolved around failure scenarios if a server supports only one of the packet types. In RADIUS, for example, attempts to send an accounting packet to an authentication-only server leads to an ICMP error message because the accounting port is then closed. If all packets are sent to one port, but the server is not configured to process accounting packets, there is no indication of this to the sender. Unfortunately, there is no negative acknowledgement of accounting packets. It is simply not foreseen in the RADIUS Operational Model to reject Accounting packets on the application level.

This discussion is still ongoing and its outcome will be incorporated into future revisions of the internet draft. Possible solutions include selecting three distinct ports for RADIUS/TLS; or to require administrators to watch out for unanswered Accounting packets as a symptom which reveals their misconfiguration.

Secondly, a question about re-use of existing ports emerged. Table 2.1 defines port usage in the current draft for alternative RADIUS transports.

Type of Packet	RADIUS/UDP	RADIUS/TCP	RADIUS/DTLS	RADIUS/TLS
Authentication	UDP/1812	TCP/1812	UDP/1812	TCP/2083
Accounting	UDP/1813	TCP/1813	UDP/1813	TCP/2083
CoA	UDP/3799	TCP/3799	UDP/3799	TCP/2083

Table 2.1: Provisional port allocations for RADIUS transports

As Table 2.1 shows, the DTLS transport is set to share ports with plain UDP transport. It needs to employ a technique known as application-layer demultiplexing. Every single incoming UDP packet must be inspected whether it is a well-formed RADIUS packet (in which case the traditional UDP processing is executed) or not (in which case it is assumed to be a DTLS fragment). This approach has several caveats. A failure in the detection heuristics can lead to unpredicted behaviour.

The discussion around this point concentrates on consolidating the approaches between DTLS and TLS. Either both transports should do application-layer demultiplexing or none (the consequence being that DTLS gets a new port assignment). This discussion is still ongoing and its outcome will be incorporated into future revisions of the internet draft.

2.2.2 Standardisation of per-SP CUI

The eduroam use of the attribute Chargeable-User-Identity in conjunction with the attribute Operator-Name as described in [DJ3.1.1] is unprecedented; mainly due to the fact that Operator-Name is a very recent attribute. Personnel in the IETF have indicated that documentation of the eduroam use-case in an Informational RFC would have good chances of publication.

Due to the current work of RADIUS/TLS still pending, there is no work yet to craft and publish this document. It is planned to start work on that document when the core RADIUS/TLS document is published.

2.2.3 RADIUS and SAML

eduroam uses RADIUS as an authentication protocol. In the past, much work was directed at how to convey specific user attributes with the authentication request. The RADIUS way of defining RADIUS attributes was seen as insufficient because the attributes were sent in the clear, which may have serious privacy implications (depending on the content of these attributes).

The protocol Security Assertion Markup Language (SAML) is usually seen as a much more flexible means to transport information about users and is widely used in web browser-based federations.

It is a complex task to integrate SAML into EAP authentication exchanges. The corresponding work moved to a newly created sub-task of JRA3 T2 (Moonshot), where substantially more expertise regarding SAML is present.

JRA3 T1 monitors the progress of this subtask. Personnel from JRA3 T1 provide active contribution to the parts of Moonshot which are related to RADIUS and RADIUS/TLS.

2.2.4 Authenticated DHCP

The DHCP protocol assigns IP addresses to new computing devices when they enter a network and refreshes the IP information at configurable intervals. It is crucial for IP guest access networks such as eduroam to provide the DHCP service, because guests would otherwise need to go through an administrative procedure of manually requesting an IP address for temporary use.

The DHCP is used widely in access networks. There are some well-documented weaknesses in the protocol which apply to any access network and are not eduroam specific. In eduroam, DHCP addresses are assigned to client devices after they have authenticated to the eduroam infrastructure, i.e. only after a successful authentication. There is no possibility for a non-community adversary to abuse DHCP. There is a possibility that a properly authenticated user can try to do harm in his surroundings or has malware installed that tries to do so. This section discusses possible extensions to DHCP to deal with such authenticated adversaries who attempt to exploit one of the weaknesses of DHCP.

This weakness is described in section 2. A possible extension to DHCP which can eliminate this weakness in IEEE 802.1X networks is described in section 3. Other approaches for problem mitigation are described in section 4. Section 5 provides a conclusion.

2.2.4.1 *Problem Description*

One of the weaknesses in the DHC protocol is that requesting and issuing DHCP addresses is typically done in an unauthenticated way. The new computing device sends a broadcast to the network, asking for an IP address. The DHCP replies to the device with the address to use for subsequent IP communication (among other pieces of information).

This unauthenticated use of DHCP provides some attack vectors for adversaries on the network. The following scenario describes the attack vector called rogue DHCP Server which is present on many DHCP networks.

In this scenario, an eduroam access network has a legitimate router and a legitimate DHCP server. A malintended eduroam user (or malware-infected device) connects to the network, authenticates, requests an IP address from the legitimate DHCP server and connects to the internet. His communication is properly encrypted through the Access Point (AP).

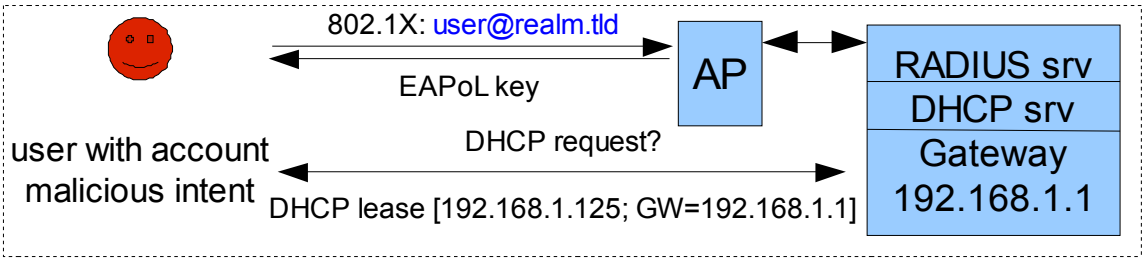


Figure 2.1: Login of valid user with malicious intent

The user then sets up a NAT gateway, which maps from its own IP address range of choice to his obtained IP address; and an own DHCP server, which announces his new NAT address as default gateway and hands out its own IP addresses in his own address range.

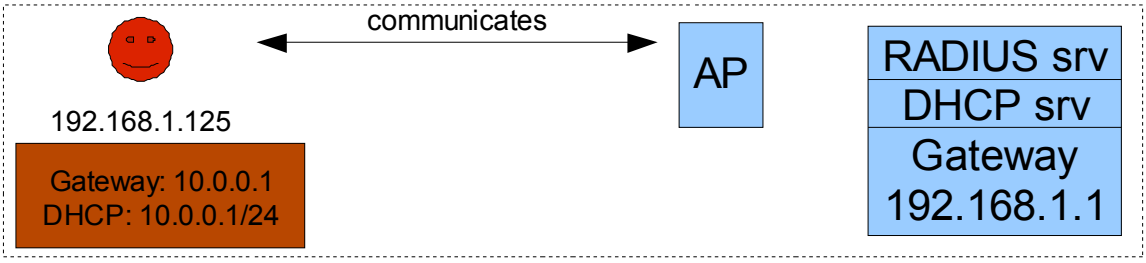


Figure 2.2: User with malicious intent sets up fake subnet

When a second, benign, eduroam user connects to the same network, he will authenticate and ask for a DHCP address. Currently there are two DHCP servers on the network, the legitimate one and the malicious one. Both of them can reply to the DHCP request. This creates a race condition. If the benign user is first contacted by the legitimate DHCP server, IP communication functions normally. But if the response from the malicious server arrives first, the benign user gets an IP address and default gateway, which points him to the malicious user; while the user is still communicating via the Access Point as he expects.

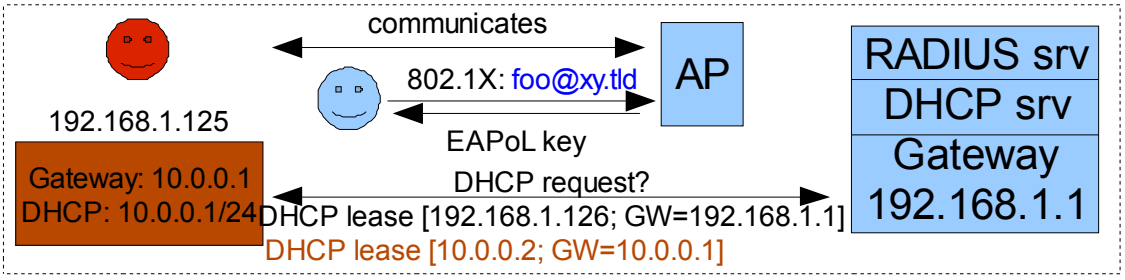


Figure 2.3: Conflicting DHCP announcements for benign user

From this point on, communication on ISO/OSI layer 2 diverges from the one on layer ISO/OSI layer 3. The attachment point for the benign user is the Access Point, but the next IP hop is the device of a different user on the same LAN (which is itself connected to the Access Point). Even though there is an encrypted communication on layer 2, the encapsulated IP traffic is sent to the malicious device and is visible unencrypted on that device. All IP communication towards the internet flows via the malicious device, which provides ample opportunity for the malicious user to sniff out the benign user.

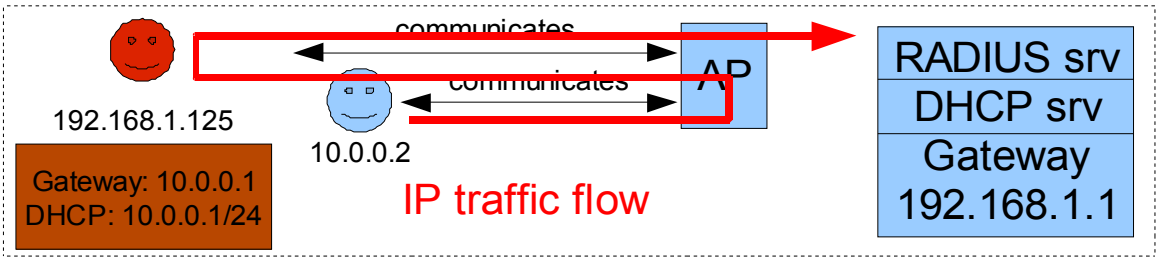


Figure 2.4: IP traffic flow after successful attack

A recent example of an actual attack based on rogue DHCP servers can be found at the Internet Storm Center, ISC: [MAL6025].

2.2.4.2 *Mitigation Approach: Authenticated DHCP*

Basis for Mitigation Approach: RFC 3118

[RFC3118] describes an optional protocol field for DHCP which provides authentication of DHCP messages. Since its inception in 2001, there is little practical value in this specification. The main problem with it is that it does not describe any key distribution mechanism. It assumes that a network administrator has manually exchanged a key with the user prior to connecting to the network. Requiring a manual administrative step is contrary to the stated goals of DHCP, namely seamless network configuration.

Unfortunately, in most networks it is not possible to dynamically distribute keys at runtime because the user does not have any knowledge of the network. If the key distribution occurs in-band, it can be faked by an adversary.

Proposed Extension of DHCP for IEEE 802.1X-based Networks such as eduroam

In IEEE 802.1X-based networks, the situation is different. There is an out-of-band channel that can be used to exchange confidential information between the supplicant and the network infrastructure, namely the IEEE 802.1X keying material which is generated during the authentication exchange. In the final stages of GN2, participants of JRA5 envisaged an extension to the DHC protocol as follows:

A DHCP system can take advantage of the presence of (unrelated) keying material which is known both to the device and the network infrastructure to:

- Derive a DHCP from the keying material on both sides.

- Send DHCP requests which are authenticated with this key.
- Reply in an authenticated manner with DHCP addresses.

A DHCP server can verify that the incoming request is genuine and tied to a recently authenticated client. The client can verify that his leased IP address was issued by the legitimate DHCP server and that all the transmitted information is correct.

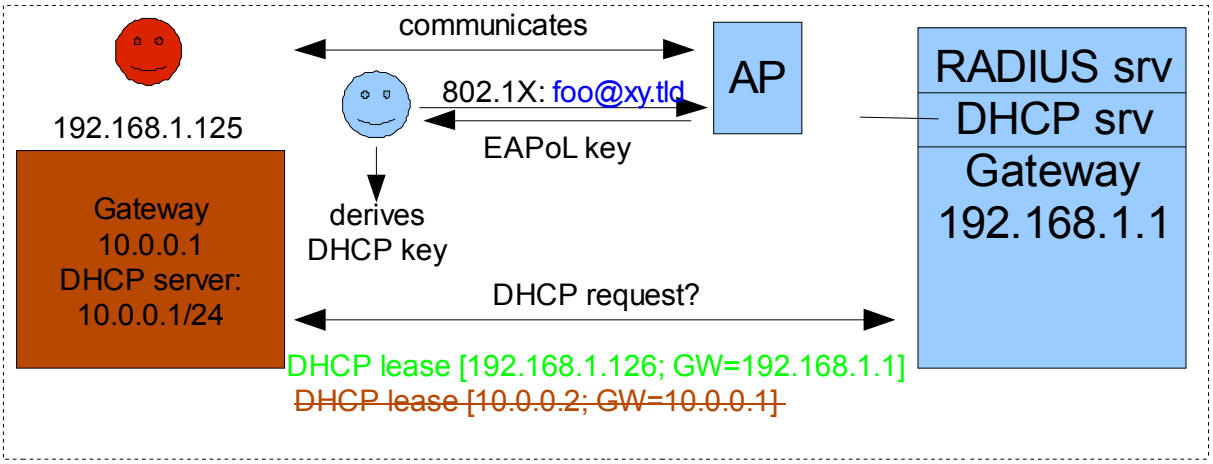


Figure 2.5: Malicious DHCP announcement prevented

Following are several hurdles to an actual implementation of this concept:

- After authentication, the 802.1X keying material resides at the IEEE 802.1X authenticator (the Access Point, Switch or Wireless LAN Controller). The authenticator is not necessarily colocated with the DHCP server for this network. It is undefined how the keying material is to be transferred to the DHCP server.
- All involved entities (DHCP client, DHCP server, IEEE 802.1X authenticator) need to support the mechanisms to ensure an authenticated transaction.
- Backwards compatibility in networks with an authenticated DHCP server must be preserved.
- The definition of this mechanism must work across vendors.

These hurdles make it paramount that any design or implementation happens in the Internet Engineering Task Force (IETF) to ensure industry-wide deployment and interoperability.

The concept was introduced to the IETF's Dynamic Host Configuration Working Group (dhc wg) at the 73rd IETF Meeting in July 2008 in Minneapolis, MN, USA. It created interest and was subsequently introduced as an item for further work in GN3 JRA3 T1.

2.2.4.3 *Other Approaches*

Operators of wireless networks and participants in the dhc wg proposed alternate ways around the rogue DHCP problem.

Client Isolation

The most popular approach to deal with this problem is to enable a feature called client isolation in the wireless network. On wired networks, this feature is often called port security. This feature prohibits all direct communication between two stations in the same LAN, except for communication with the router towards the outside world.

This enables users to use the internet, but protects them from any other users who are concurrently logged in. The diverted IP traffic flow in Figure 2.4 is prohibited. The Access Point will not forward an IP packet from 10.0.0.2 to 10.0.0.1 because the station that owns 10.0.0.1 is not the administratively configured router for the subnet.

While this is a relatively simple countermeasure, there are drawbacks associated with it. Direct communication between stations is a requirement for some protocols (such as SIP phone calls between two handsets in the same LAN) and it may be a desired feature in some situations (such as two users who want to share a folder via Windows Networking on the same LAN).

IDS and Disconnecting Rogue DHCP Server

Another way to overcome the problem is to use intrusion detection systems (IDS) which actively scan the network for anomalies, for example with DHCP snooping. When such an IDS discovers a rogue DHCP server, it can trigger a disconnection of that rogue DHCP server. However, there is a drawback to this. If the DHCP announcement is inadvertent (accidental misconfiguration), the client will not get any service and will not know why.

2.2.4.4 *Conclusion*

Authenticated DHCP is superior because it can exploit a property of 802.1X, while the other approaches have minor drawbacks. However, the other approaches are more convenient and are considered good enough. The possibility of an industry-wide advancement of the technology described herein is very low. No further effort to this end is planned. It is proposed as a best practice to eduroam operations to adopt either of the two approaches if rogue DHCPs are a concern.

3 Implementations of New Concepts

3.1 Chargeable-User-Identity

Chargeable-User-Identity (CUI), as defined in [RFC4372], was designed primarily for accounting support. In eduroam, its main use is to provide a persistent User ID support. The main concepts and use cases are described in *RadSec Standardisation and Definition of eduroam Extensions* [DJ3.1.1]. This document presents the details of actual implementations.

The general concepts were developed during work on the FreeRADIUS implementation, which has served both as a proof-of-concept and testing ground for new ideas.

The main goals of the implementations are as follows:

- The final RADIUS packet of a successful authentication (Access-Accept) should carry a CUI RADIUS attribute, containing an identifier which can be used by the visited eduroam site to recognise the user on return.
- CUI values, while being persistent, should not be traceable to a particular person without cooperation from the user's home institution.
- CUI values should be different for every visited institution, so it is not possible to create behavioural profiles of users.
- CUI support should include RADIUS-Accounting. Upon receipt of an Accounting-Request packet from a Network Access Server, the server can supplement it with a proper value of a CUI, making accounting much more meaningful.

CUI support clearly differentiates between both co-operating parties, the visited institution (acting as SP) and the authenticating institution (acting as IdP). The SP is interested in being able to merge various user sessions and requests the IdP to supply CUI values. The IdP responds to these queries, generating CUI responses. In spite of the fact that most eduroam institutions are at the same time both and SP and IdP, it makes sense to clearly separate these roles in software implementation.

Note one particular case: when an institution uses eduroam as its local network and authenticates its own users. This is conceptually different from eduroam used for guest access for two reasons: no packet proxying appears in this process and, more importantly, the institution is able to recognise its own users, since it is responsible for authentication (and does not require CUI for that).

However, the functionality brought by CUI can be a very welcome addition for local administrators. One use of the attribute is in local RADIUS accounting support, which will become more valuable because the accounting packets are then immediately linked to the actual user.

Another use is in local blacklisting of users. Even though the operator could achieve the same blacklisting without CUI (he is in possession of the IdP-side logs and could look up the actual user), CUI allows creation of local blacklists with less back-office correlation of log files. Such an addition will make CUI support more attractive to eduroam institutions and, as a result, help to introduce CUI on the pan-eduroam scale.

The IdP side of the implementation is quite straightforward. The IdP recognises a CUI request (an Access-Request packet containing a CUI attribute) and uses a hashing algorithm to scramble the real User-Name concatenated with a unique SP identifier (supplied as the value of Operator-Name attribute) and an additional secret value (the "salt"). The addition of the salt is a safeguard against dictionary attacks to retrieve the actual User-Name value. The presence of the attribute Operator-Name is required to maintain user privacy. See section 3.3 for further considerations regarding the Operator-Name attribute.

The SP side must generate CUI requests (add a NUL CUI value to its Access-Request packets), receive corresponding CUI responses and be able to match obtained CUI values to authenticated devices. Without accounting support, it is sufficient to log incoming Access-Request packets. Accounting is more complicated, because the source of accounting information is Network Access Servers (NAS), which do not have CUI support built in. Network Access Servers generate Accounting-Request packets that must be correlated to CUI values known to the RADIUS server. The RADIUS server keeps a temporary database of authenticated CUI values and corresponding MAC addresses of user devices. Upon receipt of an Accounting-Request packet, it then can find the appropriate CUI value and add it to the Accounting-Request packet.

It is worth noting that adding CUI-based accounting support requires adding a session persistence, which is somewhat foreign to the RADIUS server concept. RADIUS servers typically only keep sessions to support each individual authentication process, but treat each authentication and each Accounting-Request as completely isolated events. In addition, a connection is not normally required between the server responsible for authentication and the server used for accounting. The two servers are usually separately configured Network Access Servers. CUI accounting support, as implemented by us, requires that accounting and authentication servers have access to the same temporary database.

A standard Accounting session consists of Accounting-Request realising Start, Interim Update and Stop functions. In real life, it has been observed that the Stop packets are quite frequently missing. For this reason, a garbage collection process must be run regularly to remove stale records from the temporary database.

3.1.1 FreeRADIUS

The FreeRADIUS implementation of CUI support was first done as a proof-of-concept. It has served as a basis for tests and resulting work on further extensions.

This implementation has been tested within the GN3 project by several participating institutions. The implementation is also running on a busy production server in Nicolaus Copernicus University in Torun, Poland.

FreeRADIUS permits extensive amounts of configuration. It has been found that all CUI related support can be done exclusively using those configuration capabilities. No code modifications have been necessary on the side of the GN3 project. The developers of FreeRADIUS added a feature in the server core to streamline the GN3 implementation.

Stating that the implementation is merely configuration should not give the impression that this is a trivial task. FreeRADIUS configuration is very complex and utilises a special internal language. As in our case, the configuration language can be used to create new modules.

GN3 implementation has been done in a form of a tar file which can be unpacked on top of a production server installation. A detailed README file is provided and all files are extensively commented. It has been tested that adding CUI support to a running server is not difficult and can be done quickly.

The temporary database is implemented as a MySQL database. The communication between this database and the FreeRADIUS server is done as an additional module, being an instance of the generic MySQL FreeRADIUS module.

3.1.2 Radiator

Radiator is licensed software from Open System Consultants. Although its source code is available, no changes are allowed to be made to it. As in the FreeRADIUS case, there is a mechanism of functionality extensions by hooks. These are external Perl procedures which can be added to the configuration and do not violate the software license.

An external MySQL database is used to hold temporary state records.

The hooks provided for CUI have the following functionality:

- cui_hook: As the PostProcessingHook, it is called for each Access-Request after all authentication methods have been called and before the reply is sent back. It adjusts the Access-Accept reply creating the MD5 hash from the User-Name, received Operator-Name and the local salt and placing it as the CUI value. It also inserts the appropriate record to the temporary database. As the PreProcessingHook for the Accounting-Request, it checks for a matching record in the temporary database and, if it finds it, adds the appropriate CUI value to the packet and updates the temporary record with the last accounting time.

- cui_attr_hook: This hook should be called for each proxied request. If a CUI attribute is not present in an Access-Request, then the hook adds the CUI attribute with the NUL value and the Operator-Name attribute with the value defined in cui_operator_name.

eduroam CUI for the Radiator package is available as a tar file, which should be unpacked in the Radiator working directory. An enclosed README file contains simple instructions for configuration.

The package was installed in the GN3 test installation and tested by several project partners prior to implementation.

3.2 New Features in radsecproxy

radsecproxy is a JRA3 T1 reference implementation of RADIUS/TLS (it was previously in GN2 JRA5). At the beginning of the GN3 project, radsecproxy was already at version 1.3 and was mostly feature complete; requiring few changes to the implementation.

Two notable features were added for version 1.4:

- The server's loop detection can be configured per server. Previously, it was a global setting, which was inadequate for some deployments. In particular, eduroam monitoring uses an artificial loop in its testing cycle. This means that the feature should be turned off at least for this client/server combination.

- Improved support for Vendor-Specific attributes. Version 1.4 allows adding Vendor-Specific attributes to any incoming packet.

radsecproxy is available from http://software.uninett.no/radsecproxy. Note that a major rewrite of radsecproxy's core is currently in progress under the auspices of JRA3 T2 (Moonshot sub-task). The goal is to create a standalone library, libradsecproxy, to enable the RADIUS/TLS transport for arbitrary applications. JRA3 T2 will present a detailed report on these modifications in a future edition of the deliverable.

3.3 Introduction of Additional RADIUS Attributes into eduroam

When using the RADIUS protocol as a transport layer, IEEE 802.1X networks require a set of RADIUS attributes to be present during the authentication (most notably User-Name, EAP-Message, Proxy-State and others). The absence of a required attribute leads to an authentication failure.

On the other hand, there are attributes which are usually neither needed nor prudent to put into RADIUS requests (such as the group of VLAN assignment attributes). The presence of such attributes often leads to a reduced level of service for the user.

Authentication failures which are introduced by such infrastructure misconfigurations are very unsatisfying for end users because there is no way to communicate to them that it was not their fault. Such cases are also very difficult for network administrators to debug. As a consequence, eduroam administrators are trained to restrict their sending of attributes to the required minimum, while at the same time to filter out unexpected incoming attributes.

It is sensible to add (or support deployment of) new RADIUS attributes to the eduroam infrastructure, as long as they provide a tangible benefit and do not produce undesired side-effects. Several such attributes have been considered. The following sections describe these attributes.

3.3.1 Operator-Name

The Operator-Name attribute is defined in [RFC5580]. It allows an eduroam Service Provider to announce the administrative entity by which it is operated, revealing its approximate location. It does so by adding this attribute into RADIUS Access-Requests to communicate them to the eduroam Identity Provider (IdP). The attribute provides several benefits:

- It allows an eduroam IdP to produce per-SP CUI attributes (as described earlier in the document).
- It allows an eduroam IdP to look up from where a possible end user problem originates to streamline any necessary debugging.

The RFC 5580 format of Operator-Name places some restrictions on the content of the attribute. It defines four modes of operation:

- 0. TADIG (Transferred Account Data Interchange Group) codes
- 1. REALM (registered domain names)
- 2. E.212 namespace (Mobile operator's Mobile Country Code (MCC) and Mobile Network Code (MNC))
- 3. ICC (ITU Carrier Codes)

Out of these, only the REALM mode can be used by eduroam, since eduroam is not registered in any of the other namespaces. eduroam operators typically possess a registered domain name and can make use of namespace 1 without any additional efforts. There is a possibility that the granularity of a domain name is insufficient for an eduroam SP. The provider may not possess a domain name (namespace is too granular), or may have many distinct deployed sites, all belonging to the same organisation and domain name (namespace is not granular enough). Such cases, if they occur often enough, can be subject to further research in JRA3 T1 if necessary; but there are no current plans to do so because these cases are believed to occur rarely.

The on-the-wire format for a domain name is Operator-Name = 1<domain> (the namespace identifier is encoded in the string).

For example, the eduroam Service Provider RESTENA Foundation domain name, “restena.lu”, puts the following attribute into its RADIUS Access-Requests:

```
Operator-Name = “1restena.lu”
```

Initial tests by JRA3 T1 participants showed that the presence of Operator-Name does not produce any side-effects, except for the default risk associated with adding attributes. It enlarges the RADIUS packet on the wire, potentially causing problems with misconfigured firewalls when the threshold of the 1500 byte size altogether is exceeded.

There is, however, one notable caveat. Although Operator-Name is a standard IETF attribute which did not exist prior to the issuance of RFC 5580, it has been observed that its attribute number has been defined and used by commercial vendors. This is an unauthorised use of IETF namespace, but the attribute definitions still found their way into popular RADIUS servers’ attribute definitions (known as dictionaries). This did not create any problems in the past because these vendors’ definitions did not clash with any existing attribute. However,

with the issue of [RFC5580], a RADIUS dictionary that contains the old third-party definitions clashes with the IETF definition.

Two such clashes have been observed. The dictionaries of two former companies, Ascend and U.S. Robotics, defined the attribute to be an integer (4 bytes in length). The IETF definition is a string (up to 253 bytes in length).

Despite being undocumented and unexpected, some RADIUS servers cut the contents of Operator-Name down to 4 bytes if they have listed the attribute as an integer. This severely hampers the use of the attribute on such servers. In the example above, the content is garbled to Operator-Name = “1res”. The impact is particularly large for national and international proxy servers, because they will render an entire country's usage of Operator-Name useless.

This situation warranted invention of a new infrastructure checking mechanism which allows checking for and alerting operators when truncation of this attribute occurs on a proxy server. JRA3 T1 participants from Srce produced such a tool. For more information, see section 3.4.

Another manifestation of the same issue (conflicting or missing dictionary entries) has proven to be more serious in specific RADIUS server implementations: Microsoft IAS, NavisRADIUS and, to a limited extent, Microsoft NPS. These servers mistakenly discard authentication requests when the requests carry Operator-Name. Deployers of these servers have worked out defined ways to prevent this issue from happening. JRA3-T1 will issue an appropriate advisory to that effect. An infrastructure checking mechanism to find affected realms is currently being developed.

Despite the deployment problem of possibly having to fix RADIUS server dictionaries, JRA3 T1 believes this attribute adds value and suggests that eduroam Service Providers add this attribute as an extra piece of information into their RADIUS Access-Request packets, and that they do not filter this attribute because it provides valuable information. The eduroam Operational Team (OT) monitors the proper processing of the Operator-Name attribute for federation-level servers. See section 3.4.

3.3.2 Chargeable-User-Identity

The IETF attribute CUI (attribute number 89) has been studied extensively and is a useful addition to the service. A detailed report about this attribute is in section 3 of [DJ3.1.1]. Its concrete implementations are described earlier in section 3.1.

3.3.3 Attributes for Experimentation

In addition to the previous IETF standard attributes, several attributes for eduroam-only use were discussed. JRA3 T1 secured a namespace for such attributes in the Vendor-Specific-Attributes (VSA) section of the RADIUS standard. The namespace used is the TERENA Enterprise Number.25178.

Discussions in JRA3 T1 included defining a more fine-grained attribute for eduroam Service Provider location, visited country and user attributes. While all suggestions seemed feasible, there was no compelling reason for

including them on a wide-spread scale into eduroam operations. No recommendation towards SA3 T2 was made.

One contentious point was whether or not to create own attributes for federated NEA checks (see section 2.1), since an IETF standard solution will not likely emerge in the foreseeable future. The biggest interest in NEA-style solutions seemed to be in Janet(UK). Consequently, parts of the TERENA RADIUS namespace was delegated to Janet(UK) for experimentation with such attributes, with the prospect of leveraging the attributes to a European scale at a later stage.

3.4 Extending eduroam Monitoring for Additional Attribute Checks

The eduroam monitoring service (later referred to as monitoring service) was developed and deployed as a supporting service for the European eduroam service portfolio. See [DS5.3.1]. One of its strong points is its modularity and extensiveness. It is easy to extend current monitoring workflows with new tests or even add new workflows according to the further development of the eduroam service and related technologies.

This section explains how the monitoring service has been successfully extended to support the monitoring of the new RADIUS attributes CUI and Operator-Name in the eduroam service.

3.4.1 Monitoring Probe

The idea is to extend the already implemented server monitoring work flow (see [DS5.3.1]) to test if the RADIUS attributes CUI and Operator-Name (ON) are handled correctly by the federation level RADIUS servers (FLRS). The monitoring database and web pages have been modified to store and display this additional piece of information.

The CUI monitoring probe is based on the probe used in server monitoring work flow so the basic concepts remain the same as explained in [DS5.3.1]:

- Usage of EAP-TTLS/PAP authentication mechanism.
- The monitoring probes takes on two roles:
  - eduroam SP (sending authentication requests).
  - eduroam IdP (receiving this authentication request and replying to it appropriately).
- In one test round, the monitoring probe issues two distinct authentication requests (one of which is replied to with an Access-Reject and one with Access-Accept) and analyses the responses from the monitored FLRSs.

In the first phase, the set of attributes used by the eduroam SP side of the probe is extended to the following:

- NAS-IP-Address = 161.53.2.204
- NAS-Port = 8484

- Calling-Station-Id = eduroamMON
- Called-Station-Id = eduroamSCH
- NAS-Identifier = SA-EAP-TTLS
- Connect-Info = Smonitoring
- Chargeable-User-Identity = 0

This first phase can detect if the FLRSs are proxying the CUI value unaltered (a literal 0; not a NULL).

In the case of the Accept probing run, the eduroam IdP part of the monitoring system checks if the CUI attribute has remained unchanged (equal to 0). It then generates a CUI using the following data:

Operator-Name = “eduroamMonitoring”
local_salt = “12345”
CUI = `md5(concat(“${user.LocalSalt}”,”${reply.Operator-Name}”, “${user.uid}@${user.realm}.${user.country}”))`

Finally the eduroam SP part of the monitoring probe analyses that response to check the correctness of the ON and CUI attributes. Based on that final test, the FLRS is marked as OK or with some error status.

One of the most important results of these tests is that almost 50% of the FLRSs in eduroam are not forwarding the ON and CUI attributes correctly. The most common error is that the ON attribute value is being stripped to 4 bytes only (see section 3.3.1). This can be resolved easily by making the proper changes in the FLRS configuration.

The detected errors can be rectified rather easily with a simple configuration change in the RADIUS servers. This issue is currently being dealt with in eduroam operations.

The results of the tests are available in the standard form. See [DS531] and the following web pages:

- http://monitor.eduroam.org//eduroam/test_cui.php
- http://monitor.eduroam.org/genhtml/cui.html

3.5 Support Services for eduroam Next Generation Architecture: F-Ticks

The introduction of dynamic discovery based on RADIUS/TLS is a change of paradigm in the eduroam infrastructure. Static, manually configured uplinks from institutions (SP and IdP servers) to countries (FLR servers) and a central root server (ETLR server) get replaced by more direct SP-to-IdP connections.

One of the implications of this change is that it becomes considerably harder to generate statistics regarding international service usage.

On the old RADIUS hierarchy, every single authentication that involved crossing country borders went by the ETLR server; which made it possible to extract the statistics by retrieving the information from its log file. On the other hand, intra-country roaming usage is concealed from this central server instance, since intra-country authentications do not pass the ETLR server.

With dynamic discovery, neither intra-country nor international authentication traffic necessarily passes through a central intermediate, making the central generation of statistics impossible.

Discussions in SA3 T2 (eduroam operations) led to the conclusion that loss of international statistics is deemed unacceptable, both by the GN3 project's funding body and project management. Loss of intra-national statistics is seen as having a serious impact on the funding and justification of existence of national operators.

JRA3 T1 was consequently tasked with the creation of an alternate, decentralised statistics collection system which works both in the presence and in the absence of a central root server infrastructure.

3.5.1 Alternative Approaches

In the late stages of GN2 (Q2 2008), SA5 (eduroam operations), the first solution to this emerging problem was created: National operators were supposed to collect statistics regarding their own infrastructure on their own to supply eduroam database content, then report the monthly summary of authentication traffic via an XML file which would be polled by the eduroam database collector. See the corresponding tool documentation [DBASE].

Unfortunately, uptake of this mechanism was rather poor. The database collection mechanism was widely accepted for static data, such as locations of access points, contact details of local administrators etc. On the other hand, constantly changing data, such as the requested statistics, was much less accepted and used. The reasons for that remain unclear; but it may be that the extraction, collation and creation of an XML file, then export of this file to a web server was too complex and fragile to be executed on a regular basis by many.

Consequently, an alternative, more lightweight mechanism was required. Section 3.5.2 details the requirements that form the basis of a solution which is likely to be accepted.

3.5.2 Requirements

A statistics collection tool suitable for eduroam in a dynamic discovery scenario must:

1. Allow receipt of statistics events in a decentralised manner (i.e. from arbitrary, but legitimate sources).
2. Support semantics of established eduroam statistics collection, in particular:
   a. Quantify number of authentications carried out, noting source country of user and country visited.
   b. Quantify number of roaming days (total number of distinct MAC addresses seen roaming on a given day).
   c. Separate actual user traffic from automatically generated probe traffic (monitoring traffic).
3. Be implementable by participants (FLR or SP/IdP servers) in a lightweight manner; ideally completely stateless for the participant.

4. Contain a reliable duplicate detection.
5. Require only the bare minimum of information about users to satisfy the quantification goals in requirement 2.
6. Enable participants to opt in to receive more detailed statistics than those stated in requirement 2 (at the expense of giving away more information).
7. Be extensible enough to allow for future adaptation if changes are made to the eduroam infrastructure.
8. Be independent of the server software used by participants.

3.5.3 F-Ticks: Solution Architecture Overview

F-Ticks (Federated Ticker System) is a modular solution to the problem space above. It consists of a small software package, configuration instructions for participants, SQL schemata, a standardised message syntax for event reporting and a sample PHP-based website for visualisation of data (an authentication event is called a tick).

F-Ticks contains the following components:

3.5.3.1 *Standardised Event Reporting Syntax*

In order to work across server software boundaries, a simple string is defined which needs to contain all the required information about a tick, and which can optionally contain more information if a federation wants to send that additional information. The basic format is:

```
F-TICKS/eduroam/1.0#REALM=%R#VISCOUNTRY=LU#
      CSI=%{Calling-Station-Id}#RESULT=OK#
```

The # character does not typically appear in eduroam realms or Calling-Station-Id information, and is suited as a field separator. The information contained in this string is not the absolute minimum required for logging in purposes. It exceeds the minimum in two ways:

- The REALM field as used in the authentication (for example “@education.lu”) contains the user’s country of origin and the institution of origin.
- The Calling-Station-Id Field contains the full MAC address of a user’s device.

This extra information may be considered privacy-invading by some national operators. In these cases, it is suggested that senders of the tick do the following:

- Replace institution information with the string “undisclosed”. In the example above, “education.lu” becomes “undisclosed.lu”.
- Garble the second half of the Calling-Station-Id by hashing it in a one-way manner. It is important that the same MAC address results in the same garbled string since the Calling-Station-Id field is used for extraction of the roaming days figure. The reason for suggesting that the first half of the MAC address is untouched is because that part of the MAC address can, in any case, be used to generate service-relevant data (the distribution of hardware vendors in the eduroam user base).

With the information contained in the basic format, F-Ticks can collate the same statistics as the status quo system. This is sufficient for international roaming statistics.

If a participant wants to generate more detailed statistics for his national branch, the participant can optionally let F-Ticks generate more detailed statistics by providing national roaming details as an optional parameter. The string then looks like the following:

```
F-TICKS/eduroam/1.0#REALM=%R#VISCOUNTRY=LU#VISINST=SP-Name#CSI=%{Calling-
Station-Id}#RESULT=OK#
```

Note the additional parameter VISINST (visited institution). Also note that if a participant wants these fine-grained intra-country statistics, it makes less sense to obscure the realm, since the extra granularity of statistics requires the full user institution name to be present.

The string format is considered to be sufficiently extensible since it contains a service tag, F-TICKS/eduroam, to clearly separate it from other services. It contains a version number 1.0 to provide for possible changes in the string syntax. The tick content itself contains clearly separated attribute value pairs which provide the ability to supply additional optional parameters without the need to increment the version number.

The F-Ticks distribution contains configuration samples on how to generate correctly formatted strings for the three main servers used in eduroam:

- FreeRADIUS
- Radiator
- radsecproxy

The separation of actual user authentications vs. monitoring traffic can be achieved by adding one operational requirement for senders of ticks. The Calling-Station-Id for monitoring traffic needs to be set to a special vendor tag, so that this vendor tag can be used as a separation criterion.

The vendor tag to be used must not conflict with MAC addresses in actual use. This means that either a registration at IEEE must be done to reserve a MAC address space or to use a MAC space in the locally administered space. It was decided to go for a locally administered region. eduroam monitoring traffic must carry the vendor prefix “22-44-66” in the MAC addresses used.

3.5.3.2 *Data Export from RADIUS Servers: syslog*

It is crucial that data export from participants works as painlessly as possible. The old system’s prerequisite of maintaining state of authentications over extended periods of time and the construction of a schema-compliant XML file has proved to be difficult to use.

F-Ticks uses syslog [RFC5424] as the transport mechanism for the messages described in the previous section. Syslog is a commodity function in many, if not all, RADIUS servers. It can usually be activated via a simple configuration change. A RADIUS server typically triggers a syslog message as soon as an authentication operation completes. The message is to be sent at that instant to the F-Ticks server component. This makes

the statistics generation a “fire and forget” operation for the participant. All further processing is done for the participant on the F-Ticks server side.

The F-Ticks distribution contains instructions on how to configure the three main RADIUS servers used in eduroam for using syslog:

- FreeRADIUS v2 (+syslog-ng HOWTO for sending the syslog message to a remote server)
- Radiator
- radsecproxy (+ conversion script and HOWTO for sending to a remote server)

The prototype implementation of F-Ticks uses classic syslog over UDP for delivering the messages. Syslog/UDP is unauthenticated and not integrity-protected. This means that unauthorised third-parties can send ticks to the server component without an actual authentication event having taken place.

However, the incentive for such an action is believed to be low, since an attacker would not be able to achieve a monetary benefit from such an action, and would, at worst, skew the statistics so they indicate that eduroam is used more extensively than it actually is.

When the tool is carried over to eduroam operations, it can easily be reconfigured to use the newer syslog modes of operation such as Signed syslog, defined in [RFC 5848], syslog over TLS [RFC5425], or syslog over DTLS, [RFC6012] instead. When used with eduPKI, eduroam SP certificates (see SA3-T1 activities), this can authenticate and integrity-protect the sender and message.

Note that a decentralised system such as F-Ticks will always allow an authorised eduroam SP to generate more ticks than it has actual authentications. This has not been addressed as an issue in the eduroam operational community, since it is viewed as an artificial threat.

A second note about eduroam operations concerns potential RADIUS servers which do not support syslog. If such a server is encountered, it is quite likely that it also does not support the new feature of dynamic discovery. If that is the case, the server needs to make use of an upstream dynamic discovery server, which can then send the tick. Should eduroam operations encounter a server which does support dynamic discovery, but does not support syslog, JRA3 T1 requests notification of that situation, so statistics collection options for such a server can be researched.

3.5.3.3 *Data Collection and Conversion: syslog and f_ticks.py Script*

The server side of F-Ticks naturally uses a syslog server instance to accept incoming ticks. Since a syslog port which is open to the general intranet can also receive unsolicited (junk) messages, the syslog instance provides some initial rudimentary parsing with incoming syslog/UDP messages (and can authenticate and verify the integrity of messages with syslog/DTLS if so configured).

Any syslog message conforming to basic sanity check requirements is subsequently written to a UNIX pipe. The pipe’s contents are consumed by the parsing and collating script f_ticks.py.

f_ticks.py does in-depth parsing of the incoming message and checks every attribute-value pair for sanity and consistency. Messages passing the detailed sanity check are:

- Sorted to separate monitoring from actual payload.
- Entered into the F_TICKS_eduroam database for international traffic.
- Entered into the F_TICKS_eduroam database for intra-national traffic. If a country opts not to send the detailed tick format, the VISINST attribute is set to UNKNOWN.
- The MAC address of the tick is noted in a separate table for:
  - Duplicate detection: if later a tick with same realm, same visited country, same visited institution and same MAC address arrives within a configurable amount of time, it is considered a duplicate.
  - Roaming days: if later a tick with same realm, different tuple (visited country, visited institution) arrives on the same calendar day, it is only considered a re-authentication, and does not increment the roaming day figure.

F-Ticks is designed with agility in mind regarding realms and visited countries. There is no pre-defined set of REALM and VISCOUNTRY attributes. If a new tick arrives which has not been observed before, the database schema automatically accommodates that and creates new tuples to hold the incoming data. This means that by design, F-Ticks is not (and cannot be) a European eduroam support service element only. It is intended to be a world-wide service. It is able to hold non-European visitors in European countries (i.e. REALM is outside the EU, VISCOUNTRY is in the EU), European visitors in non-EU countries (i.e. REALM is inside the EU, VISOUNTRY is not in the EU) or completely international traffic (neither REALM nor VISCOUNTRY are in the EU) without handling them as special cases if only the corresponding visited country opts to send its ticks to the F-Ticks server.

There is one category of ticks which does create a special case. Some eduroam realms are not immediately able to be mapped into participant countries: those residing in generic top-level domains (gTLDs). During the implementation phase, the question arose whether to list these entries on their own (e.g. “REALM=foo.net”, in which the country of origin of the user is not known and would be listed as the country “NET”) or to list them within the country where the realm’s institution is located. The latter approach was chosen; which implies manual F-Ticks server administrator action, because the system cannot automatically derive the affiliated country from a generic top-level domain. Ticks with gTLDs are by default discarded and their appearance is merely logged into the unknownrealms table, until the F-Ticks server administrator takes action and enlists the realms in the specialrealms table. From that moment on, corresponding ticks get logged into the affiliated country as if their REALM attribute were the corresponding source country.

Note that .cat corresponds to the Catalan linguistic and cultural community (a gTLD as per IANA assignment [IANA]) and, as such, is not geographically locatable. However, as an approximation, the F-Ticks system assumes that institutions with a .cat domain ending are attributable to the country Spain. As a consequence, ticks for ".cat" realms are mapped into ES.

Finally, tick-like messages which fail the detailed parsing (for example, the CSI attribute is empty) can either be discarded or be written to a separate table for later inspection and/or troubleshooting. By default, they get written to the table “malformed”. See section 3.5.3.4 for the schema definition.

3.5.3.4 *Data Storage: MySQL*

The F-Ticks schema contains tables for real-time storage of:

- daily: international daily summaries (successful authentications, successful roaming days, monitoring, failed authentications, failed roaming days)
- monthly: international monthly summaries (successful authentications, successful roaming days, monitoring, failed authentications, failed roaming days)
- intrafed_daily: intra-national daily summaries (successful authentications, successful roaming days, failed authentications, failed roaming days)
- intrafed_monthly: intra-national monthly summaries (successful authentications, successful roaming days, failed authentications, failed roaming days)
- Observed MAC addresses
- Unknown realms
- gTLD realm mappings
- Comprehensive list of MAC vendor prefixes
- Table for pretty-print aliases of some vendors in the MAC vendor prefix list

Appendix A lists the full database schema definition.

3.5.3.5 *Database Support Components*

In addition to the major components in the previous section, two small helper programs need to be executed on a regular basis:

- A script to purge the observed MAC addresses is executed at midnight to reset statistics for the new roaming day.
- A script to sum up the daily statistics of the previous month is executed on the first day of each month.

3.5.3.6 *Data Presentation: PHP-based Web Frontend w/ AJAX for Dynamic Updates*

The database content can be queried with a multitude of tools since it is a MySQL database in an open format. As one example visualisation, a website based on PHP was created to show the results of data collection to web users.

The website possesses the following features:

- Separate web pages for daily and monthly international roaming summaries.
- Both web pages contain the roaming days and authentication count figures.
- Both web pages can show either successful authentication events (“the light side of the force”) or failed authentication attempts (“the dark side of the force”) and default to the successful event view.
- The daily web page contains a date selector (calendar style) to select and view arbitrary dates in the past and the present day.
- When the daily web page is set to display the current day, it features real-time updates to the tables and marks recent updates with a green background colour (resembling a typical stock ticker).

- The monthly web page contains a drop-down list of months for which monthly summaries exist (full months in the past only).
- In all views, it is possible for a national administrator to zoom into intra-national statistics by clicking on his country. This results in a view where FROM shows individual realms (instead of countries) and TO displays the visited institutions within his country (instead of countries). The access to these intra-national statistics contains sensitive data so it is access-protected.

At the time of this writing, the prototype implementation is available at the website http://ticker.eduroam.lu/. Figure 3.1 through Figure 3.4 show several views from the website. The data was collected during the development phase and the actual numbers shown may be skewed. The development prototype also monitors only 6 out of approximately 50 countries, which means that the grand totals of eduroam altogether are significantly higher than the numbers shown in the following figures.

eduroam usage statistics for 2010-09-24

Do you want to see the dark side of the force?

Devices (by Calling-Station-Id)

Last updated Thu, 30 Sep 2010 08:49:00 +0200.

FROM -> VISITED	DE	ES	LU	NL	PL	UK	User Agility
AT	18	13	2	1	1	3	38
AU	4	1	1	3	0	6	15
BE	3	2	4	1	0	3	13
BG	0	2	0	0	0	0	2
CA	0	0	0	2	0	3	5
CH	23	2	0	1	1	4	31
CZ	6	14	0	2	3	6	31
DE	1725	67	8	19	1	43	138
DK	7	1	0	4	0	4	16
EE	2	0	0	1	0	1	4
ES	47	924	0	12	5	40	104
FI	1	0	0	0	0	1	2
FR	6	3	8	0	0	6	23
GR	3	2	0	1	0	8	14
HK	0	0	0	2	0	9	11
HU	4	3	0	0	0	0	7
IE	1	0	0	0	0	0	1
IT	0	1	0	0	0	1	2
LT	0	0	0	0	1	0	1
LU	4	4	577	3	0	0	11
NL	47	20	1	1743	0	22	90
NO	7	13	0	5	0	4	29
PL	6	5	0	2	13	3	16
PT	8	56	0	8	1	18	91
SE	10	14	0	4	0	13	41
SI	2	0	0	0	0	1	3
TR	0	0	0	0	0	2	2
UK	35	21	6	12	2	1325	76
Hotspot Popularity	244	244	30	83	15	201	

That is a grand total of **6307** national roaming and **817** international roaming events.

Figure 3.1: Screenshot: International daily summary of roaming days 24 SEP 10

eduroam usage statistics for 2010-07

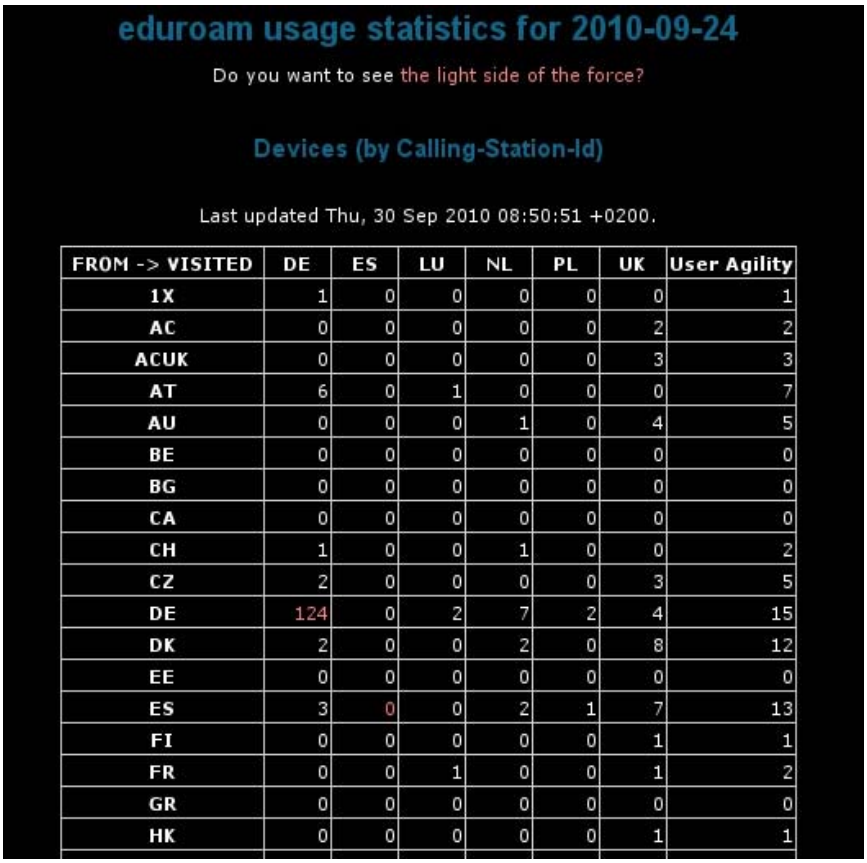
Devices (by Calling-Station-Id)

Last updated Thu, 30 Sep 2010 08:53:00 +0200.

FROM -> VISITED	DE	ES	LU	NL	PL	UK	User Agility
AD	0	1	0	0	0	0	1
AT	226	61	28	28	1	253	597
AU	31	6	1	19	2	167	226
BE	20	35	47	48	1	88	239
BG	0	24	0	0	0	1	25
CA	9	12	0	11	0	190	222
CAT	0	1	0	0	0	1	2
CH	69	32	40	52	0	37	230
CZ	151	46	15	48	9	147	416
DE	18843	334	109	306	35	748	1532
DK	58	81	15	22	3	201	380
EE	13	1	1	3	0	8	26
ES	466	13822	10	177	16	999	1668
FI	6	5	1	23	0	17	52
FR	105	122	198	38	6	350	819
GR	8	11	2	7	2	17	47
HK	22	0	2	35	0	238	297
HR	7	14	0	7	4	2	34
HU	16	4	0	0	0	7	27
IE	11	0	0	4	0	14	29
IT	22	11	0	2	3	26	64
JP	0	0	0	0	0	10	10
LT	0	7	0	0	0	3	10
LU	73	4	6071	16	0	5	98
LV	0	0	0	9	0	0	9
NL	421	176	78	11330	11	424	1110
NO	72	80	6	31	7	137	333
PL	107	36	0	31	361	123	297
PT	111	783	20	61	34	378	1387
RO	1	0	0	0	0	0	1
SE	94	79	4	48	16	196	437
SI	24	28	0	29	12	52	145
SK	11	1	23	0	0	2	37
TR	7	13	0	0	0	1	21
UK	493	228	64	221	44	20871	1050
US	2	0	0	217	0	1	220
Hotspot Popularity	2656	2236	664	1493	206	4843	

That is a grand total of **71298** national roaming and **12098** international roaming events.

Figure 3.2: Screenshot: International monthly summary of roaming days July 2010



eduroam usage statistics for 2010-09-24

Do you want to see the light side of the force?

Devices (by Calling-Station-Id)

Last updated Thu, 30 Sep 2010 08:50:51 +0200.

FROM -> VISITED	DE	ES	LU	NL	PL	UK	User Agility
1X	1	0	0	0	0	0	1
AC	0	0	0	0	0	2	2
ACUK	0	0	0	0	0	3	3
AT	6	0	1	0	0	0	7
AU	0	0	0	1	0	4	5
BE	0	0	0	0	0	0	0
BG	0	0	0	0	0	0	0
CA	0	0	0	0	0	0	0
CH	1	0	0	1	0	0	2
CZ	2	0	0	0	0	3	5
DE	124	0	2	7	2	4	15
DK	2	0	0	2	0	8	12
EE	0	0	0	0	0	0	0
ES	3	0	0	2	1	7	13
FI	0	0	0	0	0	1	1
FR	0	0	1	0	0	1	2
GR	0	0	0	0	0	0	0
HK	0	0	0	0	0	1	1

Figure 3.3: Screenshot: daily summary of failed authentications 24 SEP 10 (abbreviated)

eduroam LU usage statistics for 2010-09-24

Do you want to see the dark side of the force?

Devices (by Calling-Station-Id)

Last updated Thu, 30 Sep 2010 08:51:56 +0200.

FROM -> VISITED	EPF	EPMC	EPSA	FOYER	HOTCITY	IAM-CTE-WRONGIF	LAML	LCD	LCE	LGE	LHCE	LMRL	LRSL	LTAM
ALUNOS.IPCA.PT														
CAM.AC.UK														
EDUCATION.LU														
EPMC.LU														
GOLD.AC.UK														
GRIFFITH.EDU.AU														
HS-ESSLINGEN.DE														
IAM.EDUCATION.LU														
LBMCC.LU														
LEEDS.AC.UK														
LOD.LU														
LTETT.LU														
MWN.DE														
RWTH-AACHEN.DE														
STUDENT.UNI.LU														
SUSSEX.AC.UK														
TUDOR.LU														
U-STRASBG.FR														
UHP-NANCY.FR														
ULB.AC.BE														
ULG.AC.BE														
UNET.UNIVIE.AC.AT														
UNI-KL.DE														
UNI.LU														
UNIMAAS.NL														
UNISTRA.FR														
UNIV-NANCY2.FR														
UNIVIE.AC.AT														
Hotspot Popularity														

That is a grand total of **1398** intra-national events and **87** international events.

Figure 3.4: Screenshot: daily summary of roaming days within Luxembourg Federation, 24 SEP 10 (abbreviated; details blinded)

3.5.4 Possible Data-Mining Uses

The data collected by F-Ticks is for statistical purposes only. Having the aggregate of authentications at hand, coupled with the ability to perform arbitrarily sophisticated queries on the data allows for more information to be extracted from the raw data set. Examples of such uses follow.

3.5.4.1 *Country Popularity*

Calculating the sum of users from any country visiting a given country shows the influx of foreign users into that country in a day. This immediately allows for comparison of absolute popularity of a country among roaming users for any given day.

However, that data set is not very meaningful, since a number of factors play into that figure, including:

- Size of the country (bigger countries tend to have longer border lines, creating more opportunity for casual near-border roaming).
- Number of eduroam Service Providers in the country (countries with more eduroam Service Providers create more opportunity for roaming users to use the network).
- Location of eduroam Service Providers in the country (countries with eduroam Service Providers in popular tourist locations attract more casual users).
- Reachability of and cost of travel to the country (better reachability tends to lower the barrier of entry for roaming users).
- Shape and position of the country (landlocked countries provide more opportunity for casual near-border roaming; the shape of a country can have significant impact on the length of the border line to its neighbouring countries).

In the course of development of the F-Ticks tool, the idea of normalising these absolute numbers by crafting a metric out of the decisive factors to gauge relative popularity of a country compared to other participant countries was deemed to be too complicated and necessarily inaccurate and was dismissed.

However, since F-Ticks also keeps a record of past statistics, the popularity of a country can be plotted over time and provide a national administrator with information on the general direction of service adoption in his country. Extracting these figures from F-Ticks can be done using simple SQL queries; however a visual display of such data on the website is not implemented yet. If it is deemed useful by eduroam operations, this feature can be added in a future release.

3.5.4.2 *User Agility*

Calculating the sum of countries visited by a given country of user origin shows the outflow of users from that country to the rest of the world on a given day. This immediately allows for comparison of how active users from a country are.

However, that data set is not very meaningful, since a number of factors play into that figure, including:

- Number of eduroam IdPs in the country (countries with more eduroam IdPs create a larger pool of possibly roaming users).
- Cost/Convenience of travel for leaving the country (high cost of leaving a country is a disincentive, particularly to a sub-group of student users).
- Relative size of the educational sector compared to the total population of the country (a higher ratio yields more potential roaming users).
- Median distance to the border of a neighbouring country (shorter distances generate more opportunity for casual usage).
- Incentive to leave the country (countries with mandatory foreign semesters or good student exchange programs tend to generate more roaming users).

In the course of development of the F-Ticks tool, the idea of crafting a metric out of these decisive factors to normalise the absolute numbers and gauge relative agility of a country's users compared to other participant countries was deemed to be too complicated and inaccurate. It was dismissed.

However, since F-Ticks also keeps a record of past statistics, the agility of a country's user base can be plotted over time, and provide a national administrator with information on the general direction of service adoption in his country. Extracting these figures from F-Ticks can be done using simple SQL queries; however a visual display of such data on the website is not implemented yet. If deemed useful by eduroam operations, this feature can be added in a future release.

3.5.4.3 *Hardware Distribution of Devices*

Since F-Ticks keeps a short-term record of observed MAC addresses on a given day, and since MAC addresses are globally registered and can be attributed to a hardware vendor, it is possible to derive the relative distribution of device vendors among eduroam users. This can yield valuable information for user support, since it can give a national administrator an idea on which part of end user documentation to place emphasis.

The current version of F-Ticks contains sample SQL queries to generate the data for all of eduroam and for national use. However, a visualisation of these results is not implemented yet. If deemed useful by eduroam operations, this feature can be added in a future release.

Table 3.1 shows the distribution of hardware vendors on a typical day (data collected on the prototype with 6 out of approximately 50 countries). It is particularly noteworthy that the same data, analysed on a per-country basis, shows big differences (example: Apple ranges between approximately 30% and 80%).

Absolute count	Percentage (Total absolute count was 7592)	Vendor
4439	58.5%	Apple
1152	15.2%	Intel
599	7.9%	Hon Hai Precision (also known as. Foxconn)
319	4.2%	AzureWave
257	3.4%	HTC Corporation
152	2.0%	Askey Computer
124	1.6%	Research in Motion
113	1.5%	Liteon
102	1.3%	GemTek Technology Co Ltd
94	1.2%	Nokia

Table 3.1: Client device hardware vendor distribution (abbreviated)

3.5.5 Summary

The implementation of F-Ticks shows that it is possible to generate relevant statistics in a decentralised way. With the data collation and storage being implemented on the server side, the burden for national eduroam administrators can be kept at a minimum. The resulting statistics data can be used in a real-time fashion and can be leveraged to produce insightful data into national deployment and uptake situations.

It is planned to transfer the F-Ticks 1.0 release into the eduroam OT and to promote the tool's usage for all eduroam operators. It is expected, but remains to be seen whether or not the uptake of F-Ticks will vastly exceed the previous XML-polling way of collecting statistics.

4 Investigations Regarding the EAP Layer

In eduroam, EAP is the central component as it carries the actual user credentials from an end-user's device (via the IEEE 802.1X supplicant software) to his authentication server. There are many EAP methods from which to choose. eduroam requires that IdPs deploy only EAP types which enable mutual authentication. Even with this restriction, there are numerous EAP types remaining. Until recently, the use of PEAP, EAP-TTLS and EAP-TLS was advocated on the various eduroam setup instructions. This section gives a few recommendations regarding EAP configuration and investigates some alternative EAP types.

4.1 General EAP Optimisations

The EAP peer (supplicant) and the EAP server (eduroam IdP) need to negotiate one EAP type to use for the authentication. This negotiation is carried out during every authentication. Supplicants are configured to maintain a list of EAP types which they find acceptable. The IdP likewise maintains a list of EAP types which can be used with its identity management backend.

The negotiation happens during the EAP conversation. The IdP proposes an EAP method. If the proposal is acceptable to the supplicant, the actual EAP authentication begins immediately. If the proposed method is not acceptable, the supplicant denies the proposal and sends his list of accepted types; from which the IdP then chooses one.

It is important to note that the first case (proposed choice is acceptable) saves the authentication a packet round-trip, because the (send list to Identity Provider) -> (Identity Provider chooses method) step does not need to take place. Further no harm is done if a supplicant includes more authentication methods in his acceptable list than the IdP can support.

Section 4.2.5 describes performance testing EAP-FAST tests

Observations regarding the time needed for authentications which were carried out during the EAP-FAST tests revealed that the amount of round-trips is a significant factor in overall authentication speed, much more than the computation time needed on the EAP peers. It is useful to configure authentication servers to save round-trips where possible.

This leads to two recommendations in the following sections.

4.1.1 Default EAP Type Selection (eduroam Identity Providers)

If only one EAP type is configured and supported on the IdP server, it will be the default and no other considerations are necessary.

If more than one EAP type is configured and supported on the IdP server, it is recommended to make the most commonly used type the default for the EAP negotiation.

As an example, an eduroam IdP offers TTLS-PAP for most of its users, but it also supports the use of PEAP for client devices which do not support TTLS-PAP. The IdP should then configure TTLS-PAP as the default EAP type to save most of its users one extra round-trip time.

The corresponding configuration directives in popular RADIUS server software are:

FreeRADIUS

```
eap {
    ...
                default_eap_type = peap
    ...
}
```

Radiator

```
EAPType         <list of types>
```

(The first entry in the list is the default EAP type.)

4.1.2 Generic Client Profiles

Supplicants are sometimes suitable for one EAP type only. There are no particular considerations for these supplicants.

When deploying a supplicant which can serve multiple EAP types, an eduroam IdP has the choice of deploying it with a narrow configuration (enable only the one supported EAP type) or a wider one (enable as many EAP types as possible for the type of credential).

Both of these choices are viable. The IdP should consider that on the server-side, it might be necessary for operational reasons to switch from one EAP type to another (for example, if the type of identity management backend changes). Supplicants with a wide configuration (such as those configured to perform both a PEAP and an EAP-TTLS-PAP authentication) can be used unmodified, regardless of the server-side EAP type change. If configured in a narrow way, interaction with end users may be necessary in the case of an EAP type change. IdPs should assess whether they think it is necessary to provide this flexibility.

Note that there have been multiple requests to unify the eduroam client-side configuration so the burden on end users and site administrators can be lessened. A wide configuration can allow for a better supplicant

compatibility. However, since eduroam EAP methods require a proof of identity from the network (IdP identity), client configuration remains a per-IdP configuration with specific preconfigured server-side credentials (such as acceptable CAs and server names). This situation may change in the future if EAP methods which do not need a server-side credential to be configured become commodity. For more information, see section 4.3.

4.2 EAP-FAST

EAP-FAST is a relatively new EAP type defined in RFC 4851. It is natively supported in several operating systems (including MacOS X, but excluding MS Windows). For MS Windows, a Cisco client is available on commercial terms. EAP-FAST is another version of a tunnelled EAP type, such as EAP-TTLS or PEAP, with one major difference. The TLS tunnel established to protect the credentials exchange can be re-established without the typical TLS handshake. This difference significantly lowers the number of packets needed to perform authentication, which is of interest for eduroam. The TLS session resumes with the use of a Protected Access Credential (PAC) file. The need for provisioning this file to clients is seen as one of the problems of EAP-FAST. The PAC can be provided out-of-band, but there is no clear mechanism described. The best alternative is to provide a PAC via a TLS tunnel setup similar to PEAP with a full TLS handshake and MSCHAPv2 authentication. Another problem with EAP-FAST is the relatively narrow support of EAP-FAST in existing implementations on both client and server sides.

JRA3 T1 testing concentrated on three areas:

- Protocol overview and its applicability for eduroam
- Support for EAP-FAST in popular RADIUS servers
- Performance tests with these servers

4.2.1 Overview

EAP-FAST is thoroughly documented in [RFC4851], which users are encouraged to read for details of the protocol. JRA3 T1 studied how useful EAP-FAST could be for distributed authentication infrastructures such as eduroam, considering factors such as the speed of authentication and the ease of potential adoption.

One of the strengths of eduroam's design is that it is transparent to EAP methods. The decision to deploy a new EAP method is completely with the eduroam IdP. An IdP must set up a server which supports that EAP method and supply its users with proper client software. Then its users can benefit from the fast method, regardless of where they use eduroam. The fact that EAP-FAST can be deployed in a closed environment of a single institution makes it possible to overcome the weakness of a relatively small implementation base. Even the narrow client support may not be an obstacle. An institution may support other EAP methods at the same time, providing extra speed for some and availability for everyone.

In regard to protocol security, it is important to note that an operation mode called Anonymous PAC provisioning is part of the EAP-FAST specification. This mode of operation is not considered suitable for use in eduroam, because it does not verify the server identity in the provisioning phase. It receives and accepts

credentials from an unknown server. When deploying EAP-FAST for eduroam purposes, eduroam IdPs are solicited not to use anonymous PAC provisioning.

4.2.2 Support in Popular RADIUS Servers

As of October 2010, the server side implementation works well on the Cisco ACS server and Radiator from Open System Consultants. With a substantial amount of patching, FreeRADIUS can be retrofitted to provide at least a partially working implementation of EAP-FAST.

4.2.3 EAP-FAST in FreeRADIUS

Since EAP-FAST is an interesting solution, JRA3 T1 evaluated an experimental EAP-FAST implementation for FreeRADIUS. This implementation was created by the FreeRADIUS author and was an experiment in adding an external library taken from the source of the wpa_supplicant project. As both FreeRADIUS and wpa_supplicant have changed since the original implementation, significant code modifications to the source code were needed to get the implementation working. This has been done successfully, but only for wired network connections.

In wireless networks the EAP-FAST support in FreeRADIUS does not include support for fragmentation of the EAP messages. FreeRADIUS was sending RADIUS packages with EAP-Message contents that exceeded the link-layer MTU of the supplicant. Due to EAPoL protocol limitation, EAP messages cannot be fragmented and reassembled by the link layer. Consequently, it is not possible to deliver the EAP conversation to the supplicant if the EAP message exceeds the MTU and authentication fails. In the absence of EAP fragmentation support, the only chance of successfully authenticating lies in the question of whether each and every EAP message fragment is below the supplicant LAN's MTU.

Since JRA3 T1 efforts were intended as basic testing only, no effort was spent in trying to improve the implementation to support EAP fragmentation. The setup was still sufficient for authentication speed testing, which is described in section 4.2.5.

Note that FreeRADIUS' EAP-FAST support is not reliably usable in a real-life authentication scenario until EAP fragmentation support is added.

4.2.4 EAP-FAST in Radiator

Open Systems Consultants Radiator product comes with built-in support for EAP-FAST and can be easily configured like any other EAP type. During the initial testing phase, an unusual behaviour was detected in the implementation: it stored the PAC secrets in memory during run-time only. In case of a server restart, the authentication context to all clients was lost and a new PAC had to be exchanged.

JRA3 T1 team members informed the vendor of this anomaly, and the functionality of persistent storage for PACs was added by the vendor in a subsequent software release.

4.2.5 Performance Testing

The performance tests for authentication speed have been done by using eapol_test from wpa_supplicant package on the client side and a combination of servers (OSC Radiator, Cisco ACS and FreeRADIUS). EAP-FAST has also been tested with wireless clients and supplicants from Cisco (for MS Windows) and native supplicants in Mac OS X, iPhone, and Nokia Symbian. Testing of wireless clients was limited to confirm that the authentication was successful and that the user perception of the time was favourable.

Performance testing of actual wireless connections is extremely difficult. The shared medium character introduces more variance regarding transmission speed and it is difficult on many client platforms to separate the authentication phase from the network setup phase. On the other hand, eapol_test measures exclusively the authentication phase and provides good, repeatable results.

Measurements were done locally at two different local networks and provided very similar results. Long distance testing was done by authentication with eapol_test client from Torun (Poland) to Utrecht (The Netherlands) across the standard eduroam infrastructure.

The tests were carried out on the following platforms:

- Cisco ACS Server: Version 4.2, Windows 2003 (spec: 1 vCPU of Intel 5520 CPU, 2G RAM, VMWare ESX 4)
- Radiator (Netherlands): Version 4.7, FreeBSD // CentOS 5.4 (spec: 1 vCPU of Intel 5520 CPU, 1G RAM, VMWare ESX 4)
- Radiator (Poland): Version 4.4
- eapol_test client: FreeBSD (spec: 1 vCPU of Intel 5520 CPU, 512MB RAM, VMWare ESX 4)

There are two kinds of measurements for EAP-FAST:

- Automatic PAC provisioning (where a TLS tunnel is set up like PEAP to provision the PAC file).
- Successive EAP-FAST authentications While the PAC provisioning seems slow, this only happens during the initial configuration and after expiration of the provisioned PAC.

The first EAP-FAST session with PAC provisioning exchanges credentials, but will always result in an authentication failure on the wire. A second, consecutive authentication is always required to use the PAC and successfully authenticate.

Table 4.1 and Table 4.2 show measurements for EAP-FAST. It appears that there are differences in the defaults between RADIUS servers. While both Radiator and Cisco ACS used MSCHAPv2 for the PAC-provisioning phase, the tunnelled authentication on Cisco ACS was always done using EAP-GTC and was on Radiator by default EAP-MSCHAPv2. The use of GTC is optional, but as the server suggests MSCHAPv2 first, it is not used by most clients. This results in fewer packet exchanges for the GTC variant on Cisco ACS:

	PAC provisioning	Tunnelled authentication	Packets
Radiator	MSCHAPv2	MSCHAPv2, GTC optional	14
Cisco ACS	MSCHAPv2	GTC	10

Table 4.1: Variants of EAP-FAST

In addition, there is a small difference in authentication-times between these RADIUS servers. Though locally the differences in authentication times seem small, this indicates again that mostly the remote authentications differ because of the number of packets (and not the time needed on the server).

	Local FAST average	Remote FAST average
Radiator	27 – 41 ms	228 ms
Cisco ACS	23 ms	163 ms

Table 4.2: Average time-to-authenticate for EAP-FAST variants

Table 4.3 shows all the measurements taken for the most popular EAP types in eduroam:

	FAST Radiator	FAST Cisco ACS	FAST-PAC	TTLS	PEAP	TLS
Number of packets	14	10	18 / 18	10	18	12
Total conversation length	2479	2136	3785 / 4193	3391	4649	5420
Average packet size	184	213	210 / 233	339	258	451
Max packet size	178	406	670 / 699	1460	1460	1472 frag 1549(*)
Average time (ms) - intl. roaming -	228	163	-	300 ms	518 ms	369 ms
Average time (ms) - local -	27	23	264 / 375	41 ms	53 ms	46 ms
Time / pkt	16	16	-	30 ms	29 ms	31 ms

Table 4.3: Time measurements for various EAP types

(*) client to server side of communication exceeded the 1500 byte MTU; server to client stayed below.

There are several interesting conclusions drawn from these measurements. First, this shows the least efficient EAP mechanisms.

It is no surprise that EAP-TLS has the largest packets to be sent over the wire, since it uses client certificates that must be sent over the wire. While the packet size on the server is controlled by a server configuration setting, the clients decide this for themselves. This can cause UDP fragmentation of the RADIUS packet when the client sends EAP fragments near its MTU size and the RADIUS message adds additional overhead. This

condition occurred during the tests several times. It is important to note that the total amount of data exchanged varies with the size of the server and client certificates.

The worst EAP mechanism regarding number of packets appears to be PEAP. While it is perceived as the easiest type for end users because of client-software support (it is natively supported in Windows), it is definitely not the most efficient. Because of this, it is also the slowest of the tested mechanisms. For tunnelled authentication, TTLS appears to do a much better job compared to PEAP.

EAP-FAST is clearly the winner when it comes to the number of packets and the packet-size. This results in faster authentications, but also smaller chances of failing authentications because of packet-loss.

4.2.6 New Technologies and Their Impact on Performance

There are alternatives for solving the problems addressed with EAP-FAST. First, the problems related to packet-loss (because of the packet-size, fragmentation and/or UDP reliability in general) can be solved by using TCP as a transport via RadSec.

RadSec does not make remote authentications faster, but with newer wireless deployments (especially the controller based implementations) there are ways to make local roaming faster, preventing re-authentications (full and slow).

The Pairwise Master Key (PMK) caching solves the re-authentication problem at a (single) Access Point. The master key negotiated during the full authentication is cached, and can be used when a user roams back to this specific Access Point. In environments with centralised controllers, the PMK cache can be shared across Access Points, replacing the full re-authentication with just a few packets handshake.

There is another option that is somewhat less efficient, especially in large environments. As soon as a client authenticates to a certain Access Point, the Access Point pre-authenticates the client over the wire to other Access Points.

These solutions deliver more performance and reliability when roaming with solutions such as eduroam, but do not replace the benefits of EAP-FAST. There are many locations where PMK caching or centralised controllers are not in place. In addition, RadSec is relatively new and is not widely deployed. It still makes sense to have the most efficient authentication for clients (at least trying to prevent over-sized packets that need fragmentation).

4.3 EAP-EKE/EAP-PWD: Strong Password-based Authentication

The IETF recently approved an RFC, “EAP Authentication Using Only a Password” [RFC5931], in the informational sub-series. It is on the verge of issuing an informational RFC, “EAP Authentication Method based on the EKE Protocol” [IRFCEAP].

While both technologies differ in implementation, they share a similar concept. They make it possible to mutually authenticate (the user proves his identity to the network and the network proves its authenticity to the user), using only a simple user password. There is no server certificate involved, consequently no PKI.

This is a fundamental difference to the widely deployed EAP methods in eduroam: PEAP, EAP-TTLS, EAP-TLS. All these traditional methods achieve mutual authentication by the network's authentication server providing an X.509 certificate, which the end user (his computing device) can verify to be genuine before sending his password to that authentication server.

The algorithms around these EAP methods are still protected by patents and are not easy to license. Two patents in question are:

- U.S. Patent 5.241.599 [USP599]
- U.S. Patent 5.440.635 [USP635]

There are no publicly known implementations of them, but there may be proprietary implementations. The patents around EAP-EKE expire in mid-2011, which enables a more widespread deployment. JRA3 T1 will continue to investigate the standards and any upcoming implementations. As implementations become available, lab tests and performance analysis of these implementations will be carried out (similar to those of EAP-FAST, section 4.2.5).

The following sections describe the approach taken, and the advantages and disadvantages.

4.3.1 Schematics of PKI-less Mutual Authentication

The user's password is the only secret component to the protocol handshake. Achieving mutual assurance that the two connecting entities are the expected ones can only be achieved by exploiting the knowledge of the password on both sides, while never disclosing the password to the respective other party.

This is achieved by a multi-phased protocol exchange which:

- Establishes an anonymous cryptographic exchange (so no additional intermediate parties can intercept any subsequent communication).
- Negotiates cryptographic parameters to derive a session key for a subsequent proof of identity, calculated independently and offline on both sides of the communication.
- Uses the derived session key to prove the identity.

Figure 4.1 gives a rough outline of the phases of the protocol handshake involved.

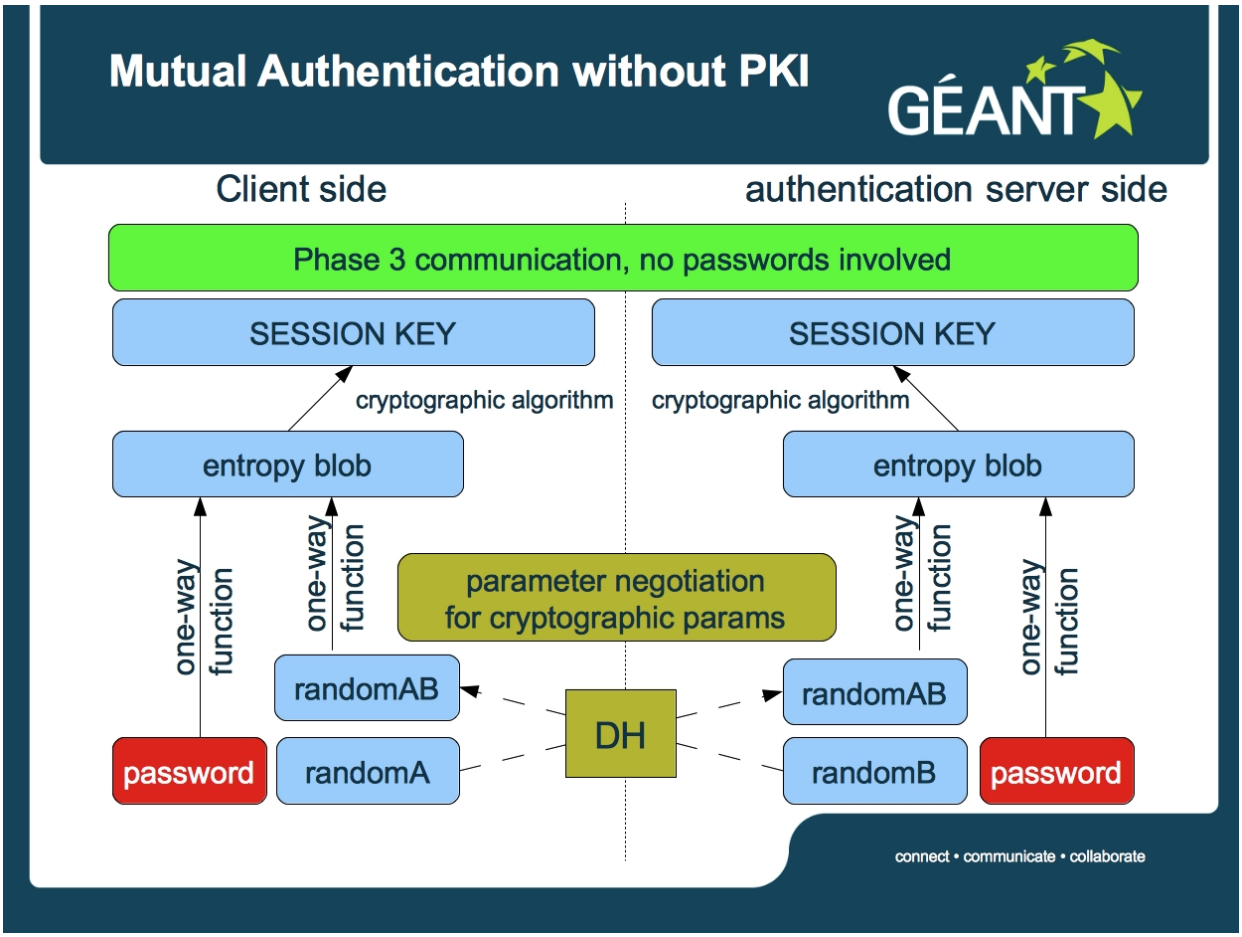


Figure 4.1: Mutual Authentication without PKI

As a general rule, whenever packets between client and server are transmitted, the identifier for the communication is the user's EAP identity. Note that the user identifier was left out of Figure 4.1 for readability.

In Phase 1, (dark yellow, exchanges between client and server), neither the identity of client nor server is established. The client connects to a (yet unauthenticated) entity and performs a Diffie-Hellman (DH) key exchange. This exchange does not require knowledge or any computation related to the password. The result is that both sides of the communication are in possession of a shared, secret key to protect further communication.

In Phase 2, both (yet unauthenticated) entities negotiate a set of cryptographic one-way functions and parameters which are to be applied to the password.

If the client is in possession of the password, he uses the password with the DH session key as input to these cryptographic functions. The result is a master key for all subsequent communication ("entropy blob" in Figure 4.1). That master key is safe against replay attacks (since the DH key is different for each protocol run) and cannot be used to derive the password. This is because cryptographically strong one-way functions have been used to scramble the password and the resulting master key also uses the DH key as a non-password input).

The server performs the exact same calculations with the same algorithms and parameters, using the same input. As a result, it arrives at the same master key.

In Phase 3, both sides use the master key to derive a session key for their subsequent communication. They then exchange defined protocol datagrams, which are not connected to the password in any way. The proof of identity lies in the fact that these datagrams can be exchanged at all: only if both sides were able to calculate the same session key, the phase-3 communication can be carried out. This in turn means that all the required inputs to the cryptographic functions existed on both sides of the communication. The password is one of the inputs to these functions. Both sides must be in possession of the password. Since only the user and his genuine authentication server are in possession of the password, the client side (user) can be sure that it is communicating with its genuine authentication server and vice versa.

This is a fundamental difference compared to established EAP types. PEAP, EAP-TTLS, EAP-TLS all explicitly verify the server's identity prior to sending user credentials. EAP-EKE infers the identity of the server from the fact that it is able to communicate with it.

Failure to communicate in phase 3 means that both sides differ on what the user's password is, because all the other inputs are openly available to both ends and cannot have been the source of the miscalculation. The reason could be on either side. The user may simply have mistyped his password or the server end of the communication may have been a malign intruder. From the protocol point of view, it is indistinguishable which side was the offending one. Either way, it does not matter since no valuable information was transmitted at any time. The only information related to the user which was visible on the network throughout the authentication process is the username.

4.3.2 Advantages of PKI-less Mutual Authentication

The first and foremost advantage of these authentication methods is that they require no parameters on the client side for the verification of the server's identity. Client misconfiguration is a common problem for eduroam helpdesks. Reducing the amount of configuration options that must be set correctly can immediately translate into higher user satisfaction and fewer support costs for an eduroam IdP.

A more technical advantage is that the EAP methods may work with any credential storage in identity management backends. This is superior to PEAP, for example, where the credential must be stored either as an NT-Hash or in clear text.

With the server verification options becoming obsolete and the independence of the hash format on the IdP side, it may be possible to generate the eduroam client profile for some supplicants which are completely independent of the IdP configuration details (as long as that IdP supports EAP-EKE). For example, a corresponding profile can be included in default Linux distributions and make eduroam work out of the box on these distributions.

4.3.3 Disadvantages of PKI-less Mutual Authentication

As of this writing, the technologies in question are still patented. It is not yet possible to work with a freely available implementation on both the client and the server sides. It is believed that contributions to popular RADIUS servers exist and a production-quality implementation will emerge soon after the patent expiry date in 2011.

With the server identity being inferred from the communication, it becomes more difficult to debug connection problems. The reason for a failure to connect cannot be pinpointed to either side of the communication. It can be that both ends disagreed about the password. This can be the user's fault (mistyped/forgotten password), the actual server's fault (glitch in identity management system), a malicious user trying to guess an actual user's password or a malicious server trying to hijack user connections. Helpdesks must be trained to respond accordingly.

The user's actual username must be communicated to the server side of communication before the identity of the server is established. It is not possible to conceal the true user identity from anyone. In the case Chargeable-User-Identity, this means that CUI's main value (concealing the actual username) will not be possible any more. It is possible to compute a CUI value for the user, but his true identity will always be revealed to the SP regardless. Other established EAP methods provide anonymous outer identities, which means deploying EAP-EKE will be a step back in that direction. Some believe that this is a major problem. Brute force attacks on user passwords become easier, since the force works in one dimension only (known username; unknown password). EAP methods with anonymity require an attacker to use brute force in two dimensions: unknown username and unknown password).

4.4 EAP-TTLS-GTC: Circumventing Supplicant Restrictions in Nokia Phones

Nokia mobile phones are popular devices used on GSM/GPRS/3G networks. Some models have a wireless adapter to connect to a wireless network and support a set of authentication protocols to authenticate the user on the wireless network.

The Symbian OS supports several EAP mechanisms which are in common use in eduroam, such as EAP-TLS and PEAP. It does not support another popular EAP mechanism, TTLS-PAP. This section describes how to circumvent supplicant restrictions on selected Nokia/Symbian-based devices by deploying support for EAP-TTLS-GTC on the IdP side.

4.4.1 Problem Description

eduroam IdPs use data storage (directories, databases, etc.) to store their users' credentials. There are different technical ways to store user passwords in a secure, non-reversibly encrypted way. When using PEAP, the only option to store the credentials in this way is by employing the NT-Hash function to the password, which is a variant of the MD4 hash function.

Many IdPs opt not to use NT-Hashes, but different forms of hashes which provide greater cryptographic strength than MD4. Popular choices are SHA1, SHA256 or their salted derivatives. Such hashes have the drawback that they are not compatible with PEAP. IdPs which use such hashes are forced to deploy EAP-TTLS with cleartext transmission of the user password within the TTLS tunnel (usually PAP).

The EAP authentication combination EAP-TTLS+PAP is based on the creation of a secure communication channel using a certificate (EAP-TTLS) and sending user name and password in clear text inside the established tunnel from the user device to the IdP. The secure tunnel extends from the user device to the IdP (authentication server).

Although the EAP-TTLS-PAP authentication combination is a common solution, Nokia phones that are able to connect to the wireless network use Symbian OS, which does not support EAP-TTLS+PAP. For more information on this topic, see the Nokia forum thread, *EAP-TTLS/PAP support* [NOKIAFORUM].

4.4.2 Approach

Since software modifications on the Nokia phone are impossible without vendor assistance, a solution is to use a supported EAP type on the Symbian OS. The solution should not break the security standards and policy requirements of eduroam. Table 4.4 lists the supported EAP types in Symbian OS:

EAP Type	Inner Authentication
EAP-PEAP	EAP-MSCHAPv2 EAP-AKA EAP-SIM EAP-TLS EAP-GTC
EAP-AKA	N/A
EAP-SIM	N/A
EAP-TLS	N/A
EAP-TTLS	EAP-MSCHAPv2 EAP-AKA EAP-SIM EAP-TLS EAP-GTC MSCHAPv2
EAP-LEAP	N/A
EAP-FAST	EAP-MSCHAPv2 EAP-AKA EAP-SIM EAP-TLS EAP-GTC

Table 4.4: Supported EAP types in Symbian OS

Of the supported EAP types in Table 4.4:

- EAP-AKA, EAP-SIM and EAP-TLS do not use passwords at all.
- EAP-LEAP has major known security issues.
- MSCHAPv2 is incompatible with non-NT-Hash passwords.

The remaining viable choices are:

- EAP-PEAP with EAP-GTC
- EAP-TTLS with EAP-GTC
- EAP-FAST with EAP-GTC

These three EAP types are candidates for further investigation. The differences between PEAP/GTC and TTLS/GTC are very minor and, for practical purposes, can be considered equal. EAP-FAST, as an outer EAP method, is rather uncommon and needs specialised server software on the IdP side to support it. It is not readily available in FreeRADIUS. After further investigation, it is suggested to try with the authentication combination EAP-TTLS with EAP-GTC.

EAP-GTC is the authentication protocol for Generic Token Card. It carries information about the user and a challenge-token (not necessarily a password) in clear text. GTC assumes that the token may be different for each authentication session. A small drawback of this for the user is the fact that every authentication session needs a manual user interaction (entering the challenge-token/password). Conceptually the token can change every time, so the implementation does not offer to store it on the device.

EAP authentication combination EAP-TTLS with EAP-GTC is based on the creation of a secure communication channel using a server certificate (EAP-TTLS) and sending the user name and challenge-token in clear text inside that tunnel to the IdP (EAP-GTC). This satisfies the eduroam requirements for mutual authentication.

As in the more common solution (EAP-TTSL+PAP), the secure tunnel extends from the user device to the IdP (the challenge-token is interpreted by the IdP's RADIUS server as the user's password). This satisfies the eduroam policy requirement that user credentials need to remain encrypted all the way to the IdP.

The IdP needs to reconfigure the authentication process in its RADIUS server and add EAP-GTC support to EAP-TTLS authentication mechanism for gathering user credentials. Successful tests have been carried out by Srce, Croatia, on their organisation's IdP (srce.hr). Results show that using the EAP-TTLS with EAP-GTC workaround can indeed be used on Nokia devices.

Section 4.4.3 provides configuration examples in various RADIUS server implementations and Symbian OS that are known to work.

4.4.3 Configuration Examples

All examples assume that TTLS-PAP support is already configured on the server.

4.4.3.1 *FreeRADIUS*

Add the following lines in eap.conf file under eap group:

```
gtc {
        challenge = "Password: "
        auth_type = LDAP
}
```

The value of auth_type must correspond with the usual Auth-Type definition in the authentication stanza in the server (in this example it is ldap).

In the ttls group add:

```
ttls {
        default_eap_type = gtc
        ...
}
```

It is required that EAP-TTLS is the default EAP type and that the default_eap_type variable in the main eap block is set to ttls.

4.4.3.2 *NavisRadius*

Add the following plug-in in the policy flow:

```
CheckNewEAP    Method-Type=Compare Method-Next=<first_method> Method-On-
Fail=EAPGTC Method-Disabled=FALSE
               Compare-Input1 = "${packet.EAP-Identity}"
               Compare-Input2 = ""
               Compare-Operator = "=="
EAPGTC Method-Type=AuthEapGtc Method-Next=<first_method> Method-On-
Fail=<first_method> Method-Disabled=FALSE
               AuthEapGtc-TunnelMethod = "GTCInfo"
               AuthEapGtc-TunnelWriteMap = <<
${request.*}:=${request.*};
DELETE ${request.EAP-Message};
${request.Password}:=${tunnel.Password};
>>
               AuthEapGtc-TunnelReadMap = "${request.*}:=${request.*};"
               AuthEapGtc-Message = "Upisite lozinku: "
               AuthEapGtc-UseReplyMessage = "TRUE"

GTCInfo Method-Type=WriteDebug Method-Disabled=FALSE
   WriteDebug-Map = <<
${Request Variable Group}=${request.*};
${Packet Variable Group}=${packet.*};
${User Variable Group}=${user.*};
${Check Variable Group}=${check.*};
${Reply Variable Group}=${reply.*};
>>
```

Check if the inner tunnel method in authEapTTLS is CheckNewEAP and change <first_method> with the method that was selected as the inner tunnel method in authEapTTLS before the change.

4.4.3.3 *Setting Up Nokia Mobile Phone*

To be able to connect to eduroam, the Nokia phone must have support for wireless network and the proper root CA certificate (from the authority which provides RADIUS certificates for EAP-TTLS) in its certificate store.

The exact procedure for configuring the Nokia phone may differ from phone to phone. The following example is generic:

1. Define the Access Point using eduroam SSID.
2. Edit the Access Point under WLAN Security Settings > EAP Plug-in Settings.
3. Select EAP-TTLS and unselect all other EAP types
4. Edit EAP-TTLS and leave everything set by default except the following.
5. Change Authority Certificate to root CA, which provides RADIUS certificate for EAP-TTLS on the user's IdP server.
6. Set "Username in use" to "User defined".
7. For Username enter the full userid, possibly made anonymous (anonymous@realm.xy)
8. Set "Realm in use" to "User defined".
9. Leave the Realm field empty.
10. Select the right arrow to edit the inner protocol (upper right corner).
11. Select EAP-GTC and unselect all other EAP types.
12. Edit EAP-GTC and write full, non-anonymous userid (e.g. pero@realm.xy).

At every authentication request, the Nokia phone will ask for a user challenge-token. In this case, it is the user's password.

5 Combining 3G and eduroam: Theory and Possibilities

Operators providing third generation (3G) mobile telecommunications services are having problems providing enough capacity for mobile phones connected to their network. WLAN access points providing eduroam are connected to the NREN networks in which capacity is not an issue. eduroam coverage, on the other hand, is usually limited to campus areas while 3G networks usually cover most parts of the country. It is worth investigating if the NREN networks could take care of some of the 3G operators' traffic using eduroam and, in return, university students and staff could be allowed access to the 3G networks outside of campuses using their eduroam credentials.

The first motivation behind producing this kind of survey report within the Roaming Developments task of the GN3 project is to investigate if there is a win-win situation for NRENs and 3G operators in which they both can serve their end-users better.

The second motivation, if the first one results in a negative outcome, is to investigate circumstances in which it is possible for the NRENs to provide more widespread coverage than the present campus-wide coverage. In other words, how 3G access could be provided to students and staff on campus as well as outside the campus, utilising as much as possible the current eduroam infrastructure.

Fruitful cooperation between 3G operators and NRENs in this area is most likely to be achieved if the end user terminals, in addition to WLAN, also support UMTS (Universal Mobile Telecommunication Service), a popular mobile communication system included in the 3G brand. A technology is needed for the UMTS and WLAN wireless systems to collaborate. One technology that can achieve this is UMA (Unlicensed Mobile Access). However, this technology requires that the terminal supports not only UMTS and WLAN, but UMA as well.

The UMA technology is illustrated in Figure 5.1. The main element is the UMA Network Controller, which handles connections from networks using technologies other than UMTS or GSM, and makes the connections appear as normal UMTS/GSM connections to the mobile core network. The UMA controller may also be referred to as the GAN (Generic Access Network) controller (GANC).

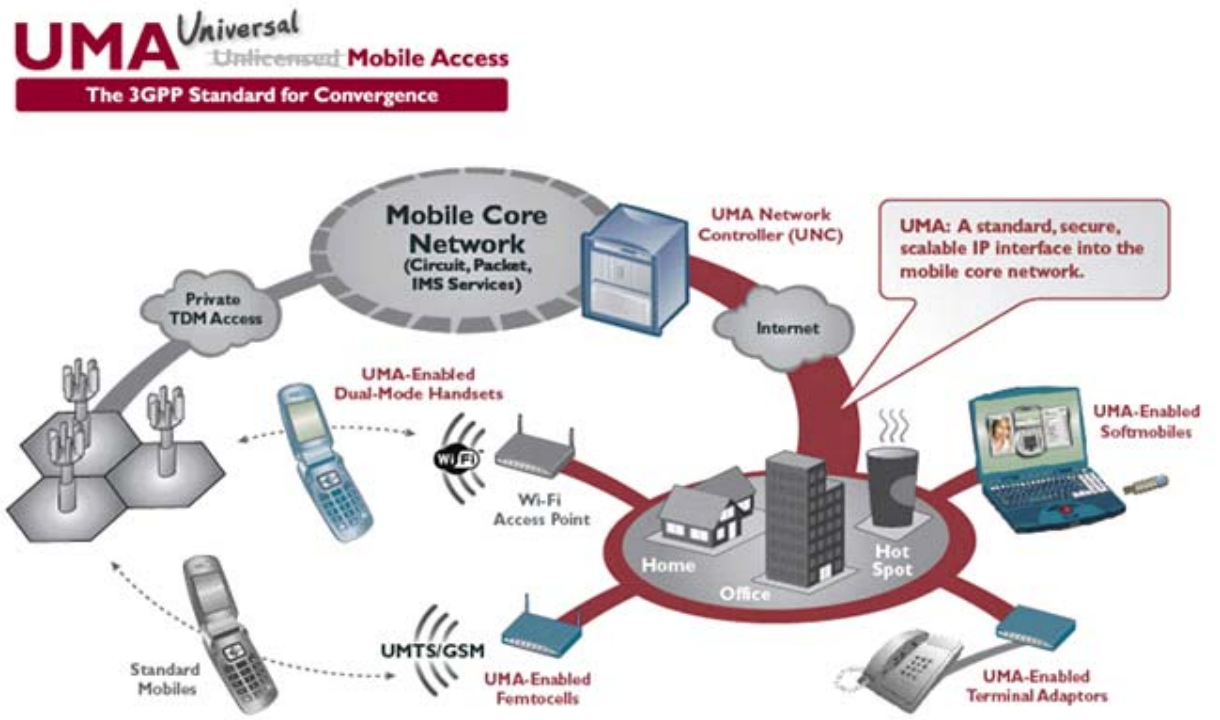


Figure 5.1: UMA technology [UMA/GAN]

In many of the white papers on the UMA website [UMAWP], the home is considered the area in which moving traffic from the mobile network to the Internet is most needed. The reason for this is the large amount of data-intensive traffic that is transmitted to and from the home. The office is also mentioned as an opportunity for UMA. This should also apply to university campuses.

As an example, the NREN network in Finland is equipped with a UMA Network Controller (UNC) and is connected to the network of a Finnish mobile operator. How can authentication and authorisation be handled securely without compromising the identity and integrity of the eduroam user?

To find a way to accomplish secure authentication and authorisation of the eduroam user, white papers (as well as the standards in which UMA is defined [3GPPSTAN]) were reviewed. The white papers and the standards are all written from the 3G/2G operator's point of view. In all cases it is considered how the UNC/GANC can let terminals in other networks connect to the mobile core network and not the other way around.

The mobile core network is constantly enhanced and one of the focus areas is to deal with growing amounts of traffic. Small base stations for home use which connect to the operator's mobile core through broadband, such as DSL or cable, have already been launched. They provide a coverage area with a radius of about 10 m called femtocells. By introducing femtocells, the mobile operator can increase the capacity of his own network. The traffic within these cells can be offloaded in several ways and the most promising solutions at the moment are LIPA (Local IP Access) and SIPTO (Selective IP Traffic Offload). In LIPA, access to the user's private LAN can be offered at the same time as access to the mobile core and its services. With LIPA the device can be

connected directly to a local printer. SIPTO, on the other hand, offers seamless IP traffic offloading between 3G/4G and Wi-Fi networks. LIPA and SIPTO will be part of LTE-Advanced, which is a developed version of LTE (Long-term Evolution), which in turn was developed from UMTS. However, all development work within mobile communication networks is done from the mobile operator's point of view (not directly applicable to combining eduroam and 3G on equal terms).

It is vital for the NREN community to think of ways in which they can provide more widespread coverage than the present campus-wide coverage. The next phase of this work will focus on coverage and how roaming between the eduroam wireless networks and other networks can be implemented.

6 Coordinating with Other Activities

6.1 SA3-T2 (eduroam Operations)

eduroam has been in operational service since before the start of GN3. Its policy and service descriptions:

- *European eduroam Confederation Policy* [GN207328]
- *eduroam Service Definition and Implementation Plan* [GN207327]

originated in GN2 JRA5 and GN2 SA5. It is an ongoing activity to verify that the service description is still appropriate, and to propose changes where appropriate.

In the course of GN3 Year 1, JRA3 T1 and SA3 T2 cooperated to identify several small shortcomings with the current service description, mostly related to technological advances which cannot possibly be covered in the original service description because they did not exist at the time (for example, IEEE 802.11n networks) or which were less well understood than they are today (for example, WPA/TKIP security flaws). The major topics are covered in this section; but the full list of proposed changes is maintained by the SA3 T2 task leader. It will be released as a revision to the service description later in the project.

6.1.1 IEEE 802.11n networks

The IEEE 802.11n standard is an extension of the wireless LAN standards series in IEEE 802.11. The specification defines a network with higher throughput than was possible with the predecessors IEEE 802.11g/IEEE 802.11a (which are in turn faster than their predecessor IEEE 802.11b and the original IEEE 802.11 standard). The theoretical maximum throughput of IEEE 802.11n networks can be as high as 600 Mbit/s. This is as long as a set of assumptions is met, such as the ability to transmit independent data channels over several spatial streams simultaneously. There is no networking equipment on the market yet which supports full spatial multiplexing and it remains to be seen how much actual throughput can be reached in real-life situations. However, the increase in throughput is very significant compared to the previous standards.

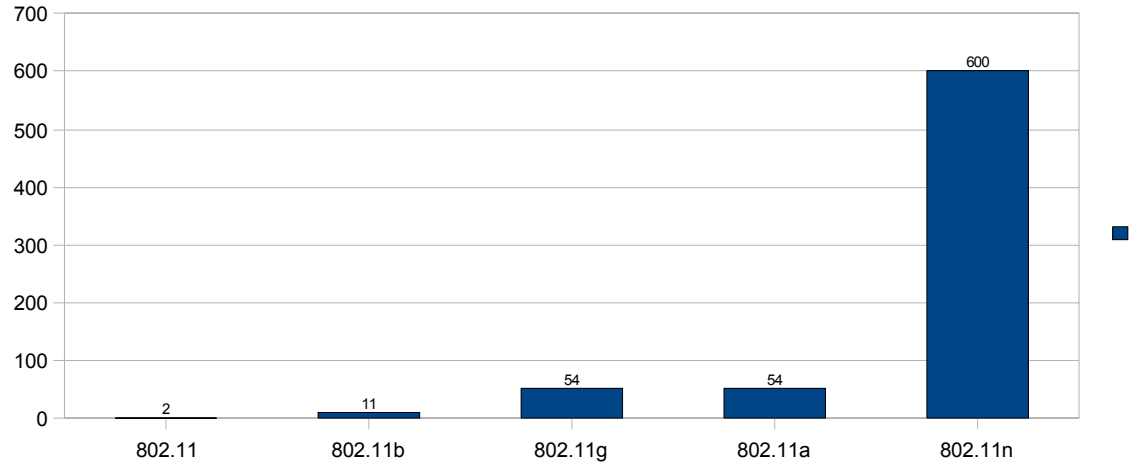


Figure 6.1: Maximum theoretical throughput on ISO/OSI Layer 2

IEEE 802.11n also deprecates older wireless LAN encryption types. A network which is operating at IEEE 802.11n speeds is not allowed to announce and process the older encryption types WEP/56, WEP/128, WPA/TKIP, WPA/AES and WPA2/TKIP; making WPA2/AES the only supported encryption type.

The current version of the eduroam Service Definition states that: eduroam Service Providers MUST support IEEE 802.11b and SHOULD support IEEE 802.11g.

The requirement to support IEEE 802.11b was quickly agreed to be outdated and is not enforced any more. However, hotspots that want to maintain an IEEE 802.11b service for a small fraction of users with old networking hardware are free to do so. It is understood and accepted that this small fraction of users will experience a degraded eduroam experience when travelling abroad. Their networking devices may not sense an eduroam hotspot because that hotspot does not support the slow data rates any more.

A more contentious point is whether or not to require IEEE 802.11n support as a MUST, and whether or not to maintain support for IEEE 802.11g as a MUST.

Note that an eduroam Service Provider which deploys only IEEE 802.11n will de facto lock out users with contemporary wireless networking hardware. Currently, IEEE 802.11n client devices are not very common yet. Therefore, a large portion of users will be left with no service at all on such a hotspot.

Subsequently, it was agreed to make IEEE 802.11g support as a baseline a MUST. Service providers are free to offer IEEE 802.11n service in addition to that baseline support.

6.1.2 WPA2 Hole 196

During the reporting period of this deliverable, one particular perceived vulnerability of the WPA2 standard hit general media coverage. It was reported that the WPA2 standard contains a hole which cannot easily be fixed. It is believed that the hole affected WPA2-Enterprise encryption in particular. For more details see the announcement from AirTight networks [HOLE196].

Since eduroam relies on Enterprise encryption and suggests the use of WPA2 as current best practice, such vulnerability affects the core operations of eduroam. JRA3 T1 monitored the situation and analysed the vulnerability following its complete disclosure at the conferences DEFCON 18 and Black Hat Arsenal (both in July 2010). The intention is to create a service advisory with possible workarounds and background information, and with possible consequences for new versions of the eduroam Service Description.

It turned out that the importance and impact of the reported vulnerability was far less significant than feared at first. The core of the so-called vulnerability is that broadcast traffic in wireless LANs is sent using one single key for all authorised users (the Group Temporal Key, GTK), and that the sender address used to send the broadcast traffic is not verified. This very fact is well-known because it is documented in the IEEE 802.11i security standard on page 196.

Since an attacker must have the GTK prior to launching malicious activity, the vulnerability is immediately reduced to an insider attack. The attacker needs to hold a valid eduroam account and be logged in with that account.

A second important point to note is that every authenticated user in a WPA2 network must be able to send broadcast traffic and have it received by all other stations in the LAN, since broadcast is part of basic operations in any IP network. This is not at all an attack. AirTight however emphasised the fact that an attacker can send malicious broadcast traffic to conduct ARP spoofing attacks or to act as a rogue DHCP server (as explained in section 2.2.4). It is very important to note that such spoofing attacks are a general problem for any IP network; whether or not it is encrypted or wireless.

The only actual point in AirTight's disclosure is that a maliciously intended insider user who wants to conduct broadcast-traffic-based attacks can do so in complete anonymity, because he can change his sender MAC address at his discretion. In particular, he can disguise himself as being the Access Point when he sends the malicious broadcast traffic. Even though all users of the wireless LAN are properly authenticated with their eduroam identities, it is impossible to tell which user is the source of the broadcast traffic-based malicious activity. All malicious activity which requires unicast two-way communication does not provide this anonymity.

The media coverage and conference presentation coincided nicely with the announcement that AirTight's wireless LAN IDS is the only one to spot this particular source address forgery; making the WPA2-Hole-196 announcement a good sales opportunity for that company.

JRA3 T1 has decided not to work towards a specific service Advisory for this problem. On a more general note, it was considered a good idea to produce an eduroam Service Provider advisory for best security practices for hotspots, detailing ARP spoofing and similar general threats, and to propose countermeasures. Work is currently ongoing on this advisory.

6.2 SA2-T4 (and Wider CSIRT Community)

Another part of the ongoing eduroam Service Definition review process relates to the procedural interface between eduroam operators and Computer Security Incident Response Teams (CSIRTs) in the event of a network abuse by an authenticated eduroam user.

An eduroam security incident may involve at least three parties and correspondingly three affected CSIRT teams:

- CSIRT of the victim of the attack
- CSIRT responsible for the eduroam Service Provider subnet
- CSIRT responsible for the institution of the authenticated user

The current eduroam Service Definition states "Whenever necessary and appropriate, incidents should be handled by the respective CERT(s)". This is considered rather unspecific and does not reflect GN3 Multi-Domain Security procedures as set in *Security Standards for Multi-Domain Incident Resolution and Reaction* [MS2.4.3].

As soon as the GN3 multi-domain virtual security team is in place, all incidents where both the eduroam SP and the eduroam IdP are located within the GÉANT service region should be handled according to the procedures defined therein. Since eduroam is present world-wide and spans more than the GÉANT service region, generic rules for CSIRT coordination for eduroam security incidents must be defined.

JRA3 T1 was asked to present a typical workflow of incident resolution to the CSIRT community and to seek advice how specifically CSIRT teams want to be involved in the incident resolution.

A presentation at the 31st TERENA TF-CSIRT meeting in Istanbul included a generic workflow in any IEEE 802.1X network and solicited advice for the concrete case of eduroam. The presentation is available at [TERENA802X].

The meeting attendees voiced the opinion that:

- Tracing the source of an incident in IEEE 802.1X networks is a very sophisticated action that is best performed by the network operators themselves, as they are the subject-matter experts.
- The affected CSIRT teams want to be informed that an incident happened and that steps taken to identify the source.
- Where it is necessary to communicate between the eduroam Service Provider (hotspot) and the eduroam IdP (source of user), the communication should happen via the established eduroam communication channels (eduroam database, eduroam Operational Team) and not via the corresponding CSIRTs.

Reporting incidents in IEEE 802.1X networks, such as eduroam to CSIRTs, requires more information to be transmitted than is typically requested in the popular "CERT/CC" Incident Report template.

When an eduroam SP reports an incident to his CSIRT, the following information should be supplied in addition to the standard form:

- MAC address of the device that caused the incident (this can be extracted from the IP to MAC address binding logs, which are mandatory to implement for eduroam SPs).
- Outer EAP identity of the infringing user (which can be extracted from the RADIUS authentication logs).
- RADIUS realm of the infringing user (the part behind the first "@" in the outer EAP identity).
- Timestamp of authentication of the session that created the incident.

The eduroam SP can use his access to the eduroam database in combination with the known RADIUS realm to find out contact details of the IdP administrator. He can then contact this IdP administrator. The SP may also want to include this contact information in its report to its CSIRT.

The information listed above is vital for the eduroam IdP to find the true inner EAP identity of the user in question. After being informed by the eduroam SP, the IdP can use the submitted information to extract the inner EAP identity of the user. After doing this, the eduroam IdP should report to his own CSIRT the following information:

- Timestamp of authentication of the infringing user.
- Any reference to the eduroam SP's report, if available.
- Report about the incident response measures undertaken.

The report should only additionally contain the inner EAP identity of the infringing user if the data is submitted via a secure channel and if the release of this information is in line with the eduroam IdP's privacy policy.

6.3 SA3-T1: eduPKI

The deployment of RADIUS/TLS and dynamic discovery requires the presence of a PKI to manage the server certificates. During the initial pilot phase of RADIUS/TLS (RadSec at that time), certificate management was provided by project partner RedIRIS in the form of the eduGAIN-SCA. This pilot CA is about to be phased out and requires replacement by a production level Policy Management Authority (PMA) to accredit NREN CAs. It also requires a catch-all Certification Authority (CA) for those NRENs without their own CA.

JRA3 T1 is working closely with the eduPKI task to define the server certificate profile for eduroam servers. As of October 2010, there is a near-final draft version of the Certificate Policy and Certificate Practice statement and a web interface to the eduPKI catch-all CA. Testing of the web interface and procedures is ongoing. It is expected that eduPKI will be operational by February 2011.

7 Conclusions

This deliverable provides a summary of actions undertaken in GN3 JRA3 T1, Roaming Developments. It covers the participation in standardisation bodies, own developments and liaisons with other activities within and outside of GN3.

The participation in standardisation organisations, both active and passive, shows that there are significant developments surrounding eduroam's technology foundations (IEEE 802.1X, RADIUS and EAP). These developments either lead to an improvement in roaming experience and/or infrastructure, or can at other points threaten the deployment model of eduroam. It is important to maintain the established watching briefs and, if possible, to steer developments in a desirable direction.

JRA3 T1's own developments provide additional functionality for the existing eduroam infrastructure. They improve debugging possibilities (the Operator-Name attribute work), enable blacklisting misbehaving users (the CUI work) and provide detailed service usage statistics even when dynamic discovery is turned on in eduroam. Pieces of work such as these can be expected to be necessary infrequently, but they can be recurring. It is deemed important to keep personnel ready for such possibilities.

Liaisons with other activities are necessary and are exercised extensively, particularly with SA3 T2 (eduroam operations) and SA3 T1 (eduPKI). It has proven fruitful to interact with these two activities in particular. It is expected that SA3 T2 will continue to make requests for service enhancements to JRA3-T1. In turn, JRA3 T1 will continue to provide SA3 T2 with solutions to perceived challenges in the eduroam infrastructure.

As a general rule, all the topics covered in this deliverable will continue to be followed and reported upon in the next edition. More specifically, the roadmap for JRA3 T1 in the upcoming Project Year 3 includes:

- Continuing the established Watching Briefs on IETF and IEEE technologies.
- Guiding and supervising the transition of RADIUS/TLS with dynamic discovery into service.
- Performing a field test of promising technologies, such as IEEE 802.1x-2010 (for wired eduroam) and new EAP methods (for streamlined authentication), as soon as implementations become available.
- Leveraging interesting intra-NREN eduroam support tools toward a European scale.

The next edition of this deliverable will be DJ3.1.2,2 *Roaming Developments, 2nd edition*. It is currently scheduled for October 2011.

Appendix A SQL Tables

A.1 SQL Table: csi

This table stores information about seen devices. It is purged at midnight.

ID	Integer, auto-increment (Row identification)
viscountry	String (visited country)
visinst	String (visited institution)
csi	String (Calling-Station-ID; device identification)
count	Integer (number of occurrences)
lastchanged	Timestamp (of last occurrence, for dupe detection)

Table A.1: csi SQL table

A.2 SQL Table: daily

This table stores accumulated information about international roaming events.

ID	Integer, auto-increment (Row identification)
date	Date
source	String (Country of origin)
dest	String (Visited country)
count_raw_ok	Integer (Total successful authentications for this country pair on date)
count_raw_lastchanged_ok	Timestamp (Last change of previous datapoint)
count_csi_ok	Integer (Total successful roaming days for this country pair on date)
count_csi_lastchanged_ok	Timestamp (Last change of previous datapoint)
count_testtraffic	Integer (Total monitoring traffic for this country pair on date)
count_testtraffic_lastchanged	Timestamp (Last change of previous datapoint)
count_raw_fail	Integer (Total failed authentications for this country pair on date)
count_raw_lastchanged_fail	Timestamp (Last change of previous datapoint)
count_csi_fail	Integer (Total failed roaming days for this country pair on date)
count_csi_lastchanged_fail	Timestamp (Last change of previous datapoint)

Table A.2: daily SQL table

A.3 SQL Table: intrafed_daily

This table stores accumulated information about roaming per federation.

ID	Integer, auto-increment (Row identification)
date	Date
country	String (country of event)
source	String (Institution of origin)
dest	String (Visited institution)
count_raw_ok	Integer (Total successful authentications for this country pair on date)
count_raw_lastchanged_ok	Timestamp (Last change of previous datapoint)
count_csi_ok	Integer (Total successful roaming days for this country pair on date)
count_csi_lastchanged_ok	Timestamp (Last change of previous datapoint)
count_raw_fail	Integer (Total failed authentications for this country pair on date)
count_raw_lastchanged_fail	Timestamp (Last change of previous datapoint)
count_csi_fail	Integer (Total failed roaming days for this country pair on date)
count_csi_lastchanged_fail	Timestamp (Last change of previous datapoint)
is_national	Boolean (to check if traffic was pure national)

Table A.3: intrafed_daily SQL table

A.4 SQL Table: monthly

This table stores monthly aggregates of international roaming events.

ID	Integer, auto-increment (Row identification)
date	Date
country	String (country of event)
source	String (Country of origin)
dest	String (Visited country)
count_raw_ok	Integer (Total successful authentications for this country pair on date)
count_csi_ok	Integer (Total successful roaming days for this country pair on date)

Table A.4: monthly SQL table

A.5 SQL Table: intrafed_monthly

This table stores monthly aggregates of per-federation roaming events.

ID	Integer, auto-increment (Row identification)
date	Date (month; in the form YYYY-MM-00)
country	String (country of event)
source	String (Institution of origin)
dest	String (Visited institution)
count_raw_ok	Integer (Total successful authentications for this country pair on date)
count_csi_ok	Integer (Total successful roaming days for this country pair on date)
is_national	Boolean (to check if traffic was pure national)

Table A.5: intrafed_monthly SQL table

A.6 SQL Table: specialrealms

This table stores maps gTLD realms into countries of origin.

ID	Integer, auto-increment (Row identification)
realm	String (end of realm; sub-realms are also considered automatically)
country	String (corresponding country of origin)

Table A.6: specialrealms SQL table

A.7 SQL Table: unknownrealms

This table stores lists all observed gTLD realms which are not mapped to countries of origin.

ID	Integer, auto-increment (Row identification)
realm	String realm
count	Integer (number of observations of this realm)
eversuccess	Integer (number of successful authentications for that realm)

Table A.7: unknownrealms SQL table

A.8 SQL Table: malformed

This table dumps malformed ticks.

ID	Integer, auto-increment (Row identification)
time	Timestamp (of observed tick)
text	String[255] (beginning of malformed tick text)

Table A.8: malformed SQL table

A.9 SQL Table: oui

This table lists the IEEE MAC address prefix.

ID	Integer, auto-increment (Row identification)
oui_prefix	String (first six digits of MAC address as per IEEE database)
vendor	String (name of vendor as per IEEE database)

Table A.9: oui SQL table

A.10 SQL Table: oui_aliases

This table lists friendly names for some vendor names.

ID	Integer, auto-increment (Row identification)
vendor	String (name of vendor as per IEEE database)
alias	String (friendly name of vendor)

Table A.10: oui_aliases SQL table

References

[3GPPSTAN] for 3GPP TS 43.318 and 44.318 standards
http://www.3gpp.org/specification-numbering
Also:
http://www.3gpp.org/ftp/Specs/html-info/43318.htm
http://www.3gpp.org/ftp/Specs/html-info/44318.htm

[802STAN] http://standards.ieee.org/getieee802/download/802.1AE-2006.pdf

[ADV002] http://www.eduroam.org/downloads/docs/advisory/eduroamOT-admin-advisory-002.pdf]

[DBASE] http://www.eduroam.org/database.php

[DJ3.1.1] *RadSec Standardisation and Definition of eduroam Extensions*
S. Winter, T, Wolniewicz, I. Thomson
www.geant.net/Media_Centre/Media_Library/Media%20Library/GN3-09-213-DJ3_1_1_RadSec_Standardisation_and_Definition_of_eduroam_Extensions_20091106091343.pdf

[DS5.3.1] *Report on Introduction of Monitoring System and Diagnostics Tools*
http://www.geant2.net/upload/pdf/GN2-09-008v2-DS5-3-1-Report-on-Introduction-of-Monitoring_System_and_Diagnostics_Tools_Final.pdf

[GN207328] *European eduroam Confederation Policy*
http://www.eduroam.org/downloads/docs/GN2-07-328-eduroam-policy-for-signing-Final2-2.pdf

[GN207327] *eduroam Service Definition and Implementation Plan*
http://www.eduroam.org/downloads/docs/GN2-07-327v2-DS5_1_1-eduroam_Service_Definition.pdf

[HOLE196] AirTight networks knowledge centre
http://www.airtightnetworks.com/WPA2-Hole196]

[IANA] Internet Assigned Numbers Authority
http://www.iana.org/domains/root/db/

[IEEE] Institute of Electrical and Electronics Engineers
http://www.ieee.org

[IETF] The Internet Engineering Task Force
http://www.ietf.org/

[IRFCEAP] EAP Authentication Method based on the EKE Protocol
http://tools.ietf.org/html/draft-sheffer-emu-eap-eke-08

[MAL6025] new rogue-DHCP server malware
http://isc.sans.edu/diary.html?storyid=6025

[MS3.7.5] *Report on Passive Monitoring Pilot*
S. Ubik, V. Smotlacha, S. Trocha, S. Leinen, V. Jeliazkov, A. Friedl
http://www.geant2.net/upload/pdf/GN2-08-191-MS3-7-5_Report_on_Passive_Monitoring.pdf

[MS2.4.3] *Security Standards for Multi-Domain Incident Resolution and Reaction*
https://intranet.geant.net/sites/Services/SA2/T4/Documents/GN3-10-139-MS2-4-3_Security_Standards_for_MD_Incident_Detection_and_Reaction.pdf

[NOKIAFORUM] Forum.Nokia: EAP-TTLS/PAP support
http://discussion.forum.nokia.com/forum/showthread.php?p=622919#post622919

[RADDTLS] DTLS as a Transport Layer for RADIUS
http://www.ietf.org/id/draft-ietf-radext-dtls-01.txt

[RADSECPROXY] generic RADIUS proxy
http://software.uninett.no/radsecproxy/

[RFC2865] Remote Authentication Dial In User Service (RADIUS). The RADIUS protocol.
http://www.ietf.org/rfc/rfc2865.txt

[RFC3118] Authentication for DHCP Messages
http://tools.ietf.org/html/rfc3118

[RFC4372] Chargeable-User-Identity (CUI)
http://www.ietf.org/rfc/rfc4372.txt

[RFC4851] The Flexible Authentication via Secure Tunneling Extensible Authentication Protocol Method (EAP-FAST)
http://tools.ietf.org/rfc/rfc4851.txt

[RFC5424] SYSLOG The Syslog Protocol (Obsoletes: 3164 March 2009)
http://www.rfc-editor.org/rfc/rfc5424.txt

[RFC5425] Transport Layer Security (TLS) Transport Mapping for Syslog
http://www.rfc-editor.org/rfc/rfc5425.txt

[RFC5426] For further information: Transmission of Syslog Messages over UDP
http://www.rfc-editor.org/rfc/rfc5426.txt

[RFC5580] Carrying Location Objects in RADIUS and Diameter
http://tools.ietf.org/search/rfc5580

[RFC5848] Signed Syslog Messages
http://www.rfc-editor.org/rfc/rfc5848.txt

[RFC5931] EAP Authentication Using Only a Password
http://tools.ietf.org/html/rfc5931

[RFC6012] Datagram Transport Layer Security (DTLS) Transport Mapping for Syslog
http://www.rfc-editor.org/rfc/rfc6012.txt

[TNC] Trusted Network Connect (TNC)
http://www.trustedcomputinggroup.org/developers/trusted_network_connect

[TCG]	Trusted Computing Group (TCG) http://www.trustedcomputinggroup.org
[TERENA802X]	Tracing individual users in IEEE 802.1X networks, presentation at the 31st TERENA TF-CSIRT meeting in Istanbul http://www.terena.org/activities/tf-csirt/meeting31/winter-802.1X-tracing.pdf
[USP599]	Cryptographic Protocol for Secure Communications http://www.freepatentsonline.com/5241599.pdf
[USP635]	Cryptographic Protocol for Remote Authentication http://www.freepatentsonline.com/5440635.pdf
[UMA/GAN]	http://www.smart-wi-fi.com/applications.php
[UMAWP]	UMA white papers http://www.smart-wi-fi.com/whitepapers.php

Glossary

2G	2nd generation mobile telecommunications services
3G	3rd generation mobile telecommunications services
802.11	IEEE 802.11 standards for wireless networks operating on the 2.4 GHz Industrial, Scientific and Medical (ISM) band.
ACS	Access Control Server (from CISCO)
AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
ASD	Asserting Security Domain
CA	Certification Authority
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Teams
CUI	Chargeable-User-Identity
dhc wg	Dynamic Host Configuration Working Group (of the IETF)
DH	Diffie-Hellman (key exchange)
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DTLS	Datagram Transport Layer Security
E.212 namespace	Mobile operator's Mobile Country Code (MCC) and Mobile Network Code (MNC)
EAP	Extensible Authentication Protocol
EAPoL	Extensible Authentication Protocol over Local Area Network
EAP-GTC	Authentication protocol for Generic Token Card
eduroam®	Federation of organisations mutually providing their users access to the Internet connectivity.
EKE	Encrypted Key Exchange
ETLR Server	Central root eduroam server
FLR Server	Country eduroam server
F-ticks	Federated Ticker System
GAN	Generic Access Network
GANC	Generic Access Network Controller
GPRS	General packet radio service
GSM	Global System for Mobile Communications
GTC	Generic Token Card
GTK	Group Temporal Key
gTLDs	generic top-level domain
IANA	Internet Assigned Numbers Authority
IAS	Internet Authentication Service
ICC	ITU Carrier Codes

ICMP	Internet Control Message Protocol
IDNs	Internationalised Domain Names
IdP	Identity Provider
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISC	Internet Storm Center
ISO	International Organisation for Standardisation
ITU	International Telecommunication Union
LAN	Local Area Network
ldap	Lightweight Directory Access Protocol
LIPA	Local IP Access
LTE	Long term Evolution
MAC	Media Access Control address
MCC	Mobile operator's Mobile Country Code
MD4	Message-Digest algorithm 4
MNC	Mobile Network Code
MS-CHAP v2	Microsoft Challenge Handshake Authentication Protocol v2
MTU	Maximum Transmission Unit
NAS	Network Access Server
NAT	network address translation
NEA	Network Endpoint Assessment
NEA PB	Network Endpoint Assessment Posture Broker
NPS	Network Policy Server
NREN	National Research and Education Network
OID	Object Identifier
ON	Operator-Name
openTC	Open Trusted Computing
OSI	Open Systems Interconnection
OT	Operational Team
PAC	Protected Access Credential
PAP	Password Authentication Protocol
PA-TNC	Posture Attribute Trusted Network Connect
PB-TNC	Posture Broker Trusted Network Connect
PEAP	Protected Extensible Authentication Protocol
PKI	Public Key Infrastructure
PMA	Policy management Authority
PMK	Pairwise Master Key
PT	Posture Transport
PWD	EAP-PWD
RADIUS	Remote Authentication Dial-In User Service
REALM	Registered domain name
RSD	Relying Security Domain
SAML	Security Assertion Markup Language
SIP	Session Initiation Protocol
SIPTO	Selective IP Traffic Offload

SP	Service Provider
SPI	Security Posture Information
SQL	Structured Query Language
TADIG	Transferred Account Data Interchange Group
TCG	Trusted Computing Group
TCP	Transmission Control Protocol
TERENA	Trans-European Research and Education Network Association
TKIP	Temporal Key Integrity Protocol
TLDs	Top-level Domain
TLS	Transport Layer Security
TTLS	Tunnelled Transport Layer Security
TNC	Trusted Network Connect
TTLS-PAP	Tunnelled Transport Layer Security with Password Authentication Protocol
UDP	User Datagram Protocol
UMA	Unlicensed Mobile Access
UMTS	Universal Mobile Telecommunication Service
UNC	UMA Network Controller
VISINST	Visited Institution
VLAN	Virtual LAN
VSA	Vendor-Specific-Attributes
Wi-FI®	Wireless Fidelity
WLAN	wireless local area network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access, version 2
XML	Extensible Markup Language