24.04.08

Deliverable DJ5.1.6: Evaluation of New Roaming Technologies and Possible Integration into AAI

Deliverable DJ5.1.6

Contractual Date:	31/12/07
Actual Date:	24/04/08
Contract Number:	511082
Instrument type:	Integrated Infrastructure Initiative (I3)
Activity:	JRA5
Work Item:	WI1
Nature of Deliverable:	R
Dissemination Level	PU
Lead Partner	RESTENA
Document Code	GN2-08-051v2

Authors: S. Winter (RESTENA), J. Rauschenbach (DFN), J.M. Macias Luna (RedIRIS), S. Neinert (University of Stuttgart), J. Howlett (JANET(UK)), M. Gast (Trapeze Networks), M. Milinovic (Srce/CARNet), Óscar Cánovas Reverte (University of Murcia), S. Venaas (UNINETT), D. Fernandes (FCCN), I. Thomson (DANTE)

Abstract

New and developing technologies relevant to roaming and authentication are examined in this document. Developments in the areas of infrastructure, support technologies, client configuration, IPv6, and Network Admission Control are discussed. Conclusions are given to the relevance of any developments, and whether they should be considered for inclusion in the eduroam project.

Table of Contents

Table of Figures

0 Executive Summary

This Deliverable examines the progress in new and developing technologies relevant to roaming and authentication and authorisation since the publication of deliverables DJ5.1.4 “Inter-NREN Roaming Architecture: Description and Development Items” and DJ5.4.1 “Advanced Technologies Overview”.

In particular, the areas reviewed are:

- Improvements to the Roaming Infrastructure: This section examines developments in Diameter and RADSEC, and the progress of the sub-project DAMe.
- Administrative and User Support Technologies: This reviews the development of systems for capturing information on relevant personnel and services.
- Client Configuration: This section describes the existing situation for supplicant software on client devices, and investigates a new Configuration API that may make the process more usable.
- IPv6: A review of developments in IPv6 is given.
- Network Admission Control: This section evaluates the impact of new control technology designed to give a “state of health” evaluation of a device.

Detailed conclusions for each research area are given at the end of each relevant section. These summaries are collated in section 7. In brief, they are:

- Roaming Infrastructure Technologies: Diameter is not deemed to be usable for the eduroam infrastructure, however, RadSec has proven to be a valuable addition to the eduroam infrastructure. The DAMe sub-project has also proved invaluable in defining an architecture for the authorisation of network properties in eduroam, and for unified Single Sign On.
- Administrative and User Support Technologies: OpenLayers is clearly the best solution for providing the graphical representation of PoP and hotspots.
- Client Configuration technologies: The “Wireless Native API” might provide an eduroam-compatible supplicant configuration simply and efficiently. The OpenSEA project is discussed, and needs to be monitored for its future applicability to eduroam.
- IPv6: There is no requirement.

- Network Admission Control: The analysis suggests that this technology shows great potential for ensuring the security of local campuses and their administrators. However, it introduces a new layer of deployment complexity for roaming use. Compatibility with eduroam needs to be ensured, and so this topic needs to be followed closely.

1 Introduction

The development of new technologies that might have an impact on roaming in general and eduroam specifically has been monitored continuously during the GN2 project time (in the JRA5 work items 1 – Roaming and 4 – New Technology). The first results of this research were published in DJ5.1.4 “Inter-NREN Roaming Architecture: Description and Development Items” and in DJ5.4.1 “Advanced Technologies Overview”. These deliverables contained several important design choices, along with the conclusion that some technologies were not mature enough to be used within eduroam. The documents also stated that these immature technologies were to be re-evaluated at a later stage. This deliverable presents the results of this re-evaluation.

Furthermore, other areas of technology that were only of a secondary importance during the pilot phase of eduroam are now becoming increasingly important. Therefore, this deliverable also provides an initial evaluation of these new fields of interest.

This deliverable addresses the following points:

- Improvements to the Roaming Infrastructure
  The two protocols Diameter (advanced designated successor of RADIUS) and RadSec (increased security and reliability for the existing RADIUS infrastructure) are examined with regard to the progress that has been made recently in terms of usability and broad deployment.

  The results so far of the DAMe sub-project within JRA5 are evaluated. This sub-project aims to augment the RADIUS admission decisions with additional authorisation decisions that may enable privileged users the use of more resources on the network, compared to users without those extra authorisation attributes.

- Administrative and User Support Technologies
  Maintaining information about such things as the appropriate responsible personnel at IdP and SP locations, the technical personnel available to assist in debugging problems, the usage of the service, and the location of hotspot areas is becoming increasingly important to the operation of the service. This information has to be collected and stored in a decentralised manner by the NRENs, but routinely aggregated by the SA5 Operational Team in a central database. A mechanism for collecting, storing and distributing the information is described.

  During the pilot phase, there was no consistent map with exact locations of eduroam hotspots. As eduroam moves into service, the user experience is of utmost importance. Therefore map technologies that give users easy access to hotspot information need to be investigated and put to use in a timely manner. Thus, a number of mapping technologies are evaluated.

- Client Configuration
  For end users, the configuration of their computing device is the most important point of contact with the technologies in use by eduroam. While an appropriate solution for most devices exists (SecureW2 supplicant, explained in DJ5.1.5,2), some use cases may require the use of different supplicants. Particularly the MS Windows Built-in supplicant is difficult to configure in a secure way. A new Configuration API for this operating system shows a good promise and is described in section 4.

  Efforts are also underway to write a new cross-platform supplicant with a feature set and user interface superior to those currently in existence. This is done by the OpenSEA alliance. An overview of their work is included here.

- IPv6
  IPv6 is a topic of continuous evaluation. While it is not a pressing subject, it becomes of more significance as time passes and the IPv4 address space is diminishing. This deliverable evaluates whether or not the eduroam infrastructure is prepared for a phased switch to IPv6.

- Network Admission Control
  This chapter evaluates the impact of a new control technology that is able to check whether a device is properly maintained (patches, anti-virus, etc.) and makes it possible to allow or disallow network admission based on that information. When the technology was designed, roaming was not seen as a relevant topic for design choices, so the impact of it in a roaming scenario is unclear. This section evaluates the possible impact on roaming users.

2 Roaming Infrastructure Technologies

Previous deliverables in the roaming work item, most notably DJ5.1.4, have identified various possible improvements for the eduroam infrastructure. For the transmission of authentication messages, two of these options were selected for further investigation and testing

- Diameter [RFC3588]
- RadSec [RADSEC]

Additionally, the possible infrastructural improvements for differentiation of authorisation levels have been developed in the JRA5 sub-project DAMe. This chapter re-evaluates these three technologies.

2.1 Diameter

2.1.1 Protocol specification

The Diameter protocol has not seen significant improvements for the use case of Wireless LAN roaming in the last 18 months.

The main focus of further advancements of the specification was in the use case of 3GPP and 3GPP2 networks, defining so-called “Diameter Applications” on top of the Diameter Base Protocol [RFC3588] that accommodate validation of SIM credentials, credit control, and accounting of pre-paid cards. Consequently, almost all implementations of the protocol focused on implementing these Diameter applications.

While the Diameter Base Protocol initially was supposed to provide better support for roaming scenarios, it didn't achieve this goal. In the course of re-working the protocol, this failure was acknowledged by the authoritative working group, stating that Diameter does not offer any significant advantages in roaming scenarios than RADIUS [ref: http://www1.ietf.org/mail-archive/web/dime/current/msg02197.html]. However, even though that problem exists and is known by those involved, no specific actions to rectify this issue are being undertaken.

2.1.2 Implementation

The Diameter Base Protocol is not implemented at all in WLAN Access Points to date, and neither are the most important applications for Wireless LANs (the “Diameter NAS Application” [RFC4005] and the “Diameter EAP Application” [RFC4072]).

While most implementations of Diameter servers implement the Diameter EAP application, they do not usually offer out-of-band connections to authentication backends that would allow verification of credentials not based on EAP-SIM or EAP-TLS (these two EAP payloads do not require any backends for verification).

Unfortunately, the development of the most promising Open Source Diameter implementation, OpenDiameter [ref: www.opendiameter.org] has stalled. In a conversation with the main developer at the 69th IETF Meeting in Chicago, US, it turned out that the project was initially started as a Diameter client only, was later widened in scope but the developer base could not stem the task of building a full-featured Diameter server, which consequently led to an abandoned project. Significant fresh manpower would be needed to revive the activity. For the time being, OpenDiameter is not in a usable state as a Diameter server.

2.1.3 Conclusions

It appears unlikely that Diameter will be usable for the eduroam infrastructure, at least during the remaining GN2 lifetime. Further progress on protocol development and implementations should be monitored though.

2.2 RadSec

At the time of DJ5.1.4, RadSec existed only as a single implementation in one RADIUS server implementation, with only a vendor white paper as a rough specification.

In JRA5, it was decided to pursue the concept of RadSec further and develop it to a more widespread solution. To that end, the following activities have taken place:

- An advanced specification of the RadSec protocol (due to on-the-wire changes labelled as “Version 2”) was developed within JRA5 and presented to the Internet Engineering Task Force. The document in its initial version is available at: http://www.ietf.org/internet-drafts/draft-winter-radsec-01.txt and is constantly being refined according to the outcome of discussions in IETF.
- JRA5 created a second, independent implementation of RadSec based on the specification above. The software, “radsecproxy”, was developed by UNINETT and is available at: http://software.uninett.no/radsecproxy/.
- Contacts with the makers of various brands of Access Points were established and led to the integration of RadSec in two separate types of devices so far:
    - Linux-based Access Points: Using the radsecproxy implementation, client-side RadSec could be deployed easily (examples: Fon, Linksys).

- LANCOM Access Points and Routers: The company LANCOM has decided to adopt RadSec in their devices' firmware with their own implementation. The firmware is currently in an alpha stage; RadSec will be included in the next production release.

2.2.1 Conclusions

RadSec has proven to be a good addition to the current infrastructure, even with only the static peer connections. The ability to enable Access Points for RadSec opened new possibilities of eduroam deployments: it has become possible to provide ad-hoc eduroam deployments behind NAT networks, unknown-beforehand IP addresses or even behind network address translation (NAT) networks, firewalls or arbitrary IP networks in the internet.. This feature could be very valuable for provisioning the eduroam service in environments without pre-installed eduroam-capable equipment, during such events as working group meetings or small conferences. The feature of dynamic peer discovery is as of yet only implemented in Radiator, but is on the roadmap for radsecproxy 1.2 and will probably be part of the FreeRADIUS implementation.

RadSec has seen significant attention from the "Operations & Management Area" within the IETF and its working group "RADIUS Extensions" (radext). The contents of the RadSec specification are currently out of radext's working scope. In the IETF's most recent meeting (IETF70, Vancouver, Canada) it was proposed to monitor the implementation and deployment of RadSec and then decide upon a re-chartering of radext to include RadSec in the scope, or alternatively to find an alternate location for roaming work.

2.3 DAMe

DAMe stands for Deploying Authorization Mechanisms for Federated Services in the eduroam Architecture. The DAMe sub-project was created to define and validate an architecture (DAMe architecture) providing two value-added services:

- Determination of network properties based on user attributes to be added to the eduroam infrastructure.
- A unified Single Sign On mechanism to bootstrap the application-level authentication from network authentication.

2.3.1 Network Authorization and Determination of Network Properties

The first goal of the DAMe sub-project is to add mechanisms for network authorization to the eduroam infrastructure. This authorization will be based on attributes of the roaming user that are managed by his home institution, and on access policies that are controlled by the visited institution. These attributes can be any of those defined in the eduPerson, SCHAC or other schema. Examples would be the affiliation "student" or the entitlement "common-lib-terms".

eduroam is a running infrastructure that connects hundreds of institutions in 33 GÉANT2 members currently. It is therefore essential that any changes do not disrupt the eduroam service, and that a seamless introduction of new functionality is possible in some places now and in other places later. Because of this it was decided to keep authentication using the RADIUS hierarchy unchanged. If the additional components of the DAMe architecture are deployed at the home and at the visited institution, attribute-based authorisation can be performed for additional network properties, such as Quality of Service (QoS). These new components are from the NAS-SAML architecture and the eduGAIN architecture.

NAS-SAML (Network Access Service based on SAML) is an approach for network access control based on attributes that are expressed in SAML (Security Assertion Markup Language), and on access policies expressed in XACML (eXtensible Access Control Markup Language). Both SAML and XACML are highly flexible languages based on XML and standardised by OASIS. The use of SAML also allows for easy integration with other federation middleware, such as Shibboleth and eduGAIN. Preliminary designs of NAS-SAML are based on Diameter, so protocol translators from RADIUS to Diameter and vice-versa would be required for connecting those parts directly to eduroam's RADIUS infrastructure. Because of this, the component responsible for authorisation decisions (Policy Decision Point, PDP) is used only, and the requesting and delivery of attributes is done via the eduGAIN infrastructure based on HTTP instead of Diameter.

eduGAIN is used in this architecture for the exchange of user attributes. There are Bridging Elements (BE) for interconnecting different kinds of federation middleware, and there is the Meta Data Service (MDS) for managing information about what eduGAIN components are located where. One DAMe enabled home BE sits between the home RADIUS and the home Identity Provider (IdP). This allows including a handle (identifying a specific user), which is sent to the remote RADIUS in case of successful authentication. The remote RADIUS can be extended with a module that contacts a remote BE (using the LDAP protocol), and that R-BE can request user attributes for the handle using the eduGAIN infrastructure. The remote RADIUS then gives the received user attributes to the Policy Decision Point (PDP), where local policies are applied and network properties for the current user are returned. Figure 1 shows all main elements of this proposed architecture.

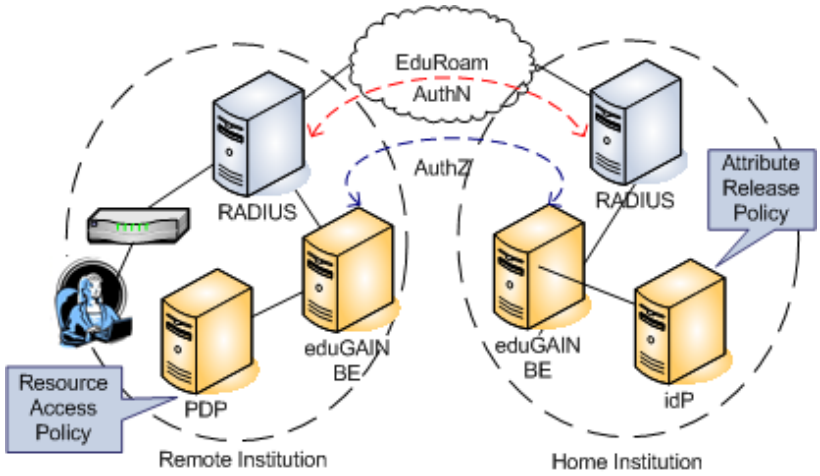

Figure 2.1: Proposed Architecture

The components for network authorization are developed. Adaptors for connecting the RADIUS servers to the PDP and the eduGAIN parts are implemented as FreeRADIUS modules: a modified LDAP module for contacting the remote RADIUS to the PDP, and a modified PEAP-module for the home RADIUS to IdP connection. Adaptors for a Shibboleth IdP and for a PAPI IdP are implemented.

2.3.2 Unified Single Sign On

The goal of unified Single Sign On (uSSO) is to use authentication information from the network authentication phase to bootstrap the authentication for services. Therefore a token called “eduToken” is delivered from the home institution to the user’s supplicant. The token is a SAML authentication statement in XML format. It is in itself not relevant for roaming, but it is transported via eduroam’s RADIUS infrastructure. It is put in a vendor-specific EAP-TLV (Type Length Value). The token will possibly be fragmented and be split into a few more messages than with usual authentication methods. No modification of the remote RADIUS is needed for uSSO. The home RADIUS needs a modified module that is connected to an adaptor, that is then connected to an Identity Provider (IdP). The home RADIUS is still responsible for performing the authentication, but additionally a token is requested from the IdP and sent to the user. If the user has a modified supplicant installed that understands the new TLV, it can receive, encrypt and store the token so that it can be used for uSSO afterwards. If another supplicant is used, the unknown TLV is ignored.

The components for connecting the home RADIUS to an IdP are the same as described above, and are available for Shibboleth and PAPI IdPs. The xsupplicant was chosen as a suitable supplicant, which has been extended for receiving and encrypted storage of the token.

2.3.3 Conclusions

DAMe is mainly a research sub-project that defined an architecture for the authorisation of network properties in eduroam, and for unified Single Sign On. Additionally, a prototypical implementation of the architecture was created, deployed and tested in an experimental setup.

More extensive testing in a larger test federation would be required to collect practical experiences and further develop the software also in terms of reliability and performance. This is valid not only for the DAMe specific components but also for those of eduGAIN that are also not yet ready for production.

A finer granular authorisation scheme based on attributes of the users would allow the institutions providing the network to get more information on the users and decide that selected user groups are entitled to extended sets of services.

A unified Single Sign On would provide an improved user experience, requiring less interaction. Additionally both eduroam and eduGAIN are interlinked, thereby leading towards a more integrated infrastructure for federated identity management combining the advantages of both.

3 Administrative and User Support Technologies

3.1 eduroam Database

The eduroam database is introduced in order to provide necessary information needed for operation of the eduroam service. The eduroam database will be built as a central database but with a mechanism that enables automatic data collection from NROs. It is the task of the SA5 group to finalise the design of eduroam database and ensure it is properly implemented and duly filled with respective information.

eduroam OT will provide proper maintenance and tools in order to ensure day to day operations of the eduroam database as well as its connection with other elements of the eduroam service (for example, the web site).

The information stored in the eduroam database includes:

- NRO representatives and respective contacts.
- Local-institutions (both SP and IdP) official contacts.
- Information about eduroam hotspots (SP location, technical info).
- Monitoring information.
- Information about the usage of the service.

The access to the database will be provided through the eduroam web site with different access rights being applied according to the use cases.

The eduroam database model is illustrated in Figure 3.1:

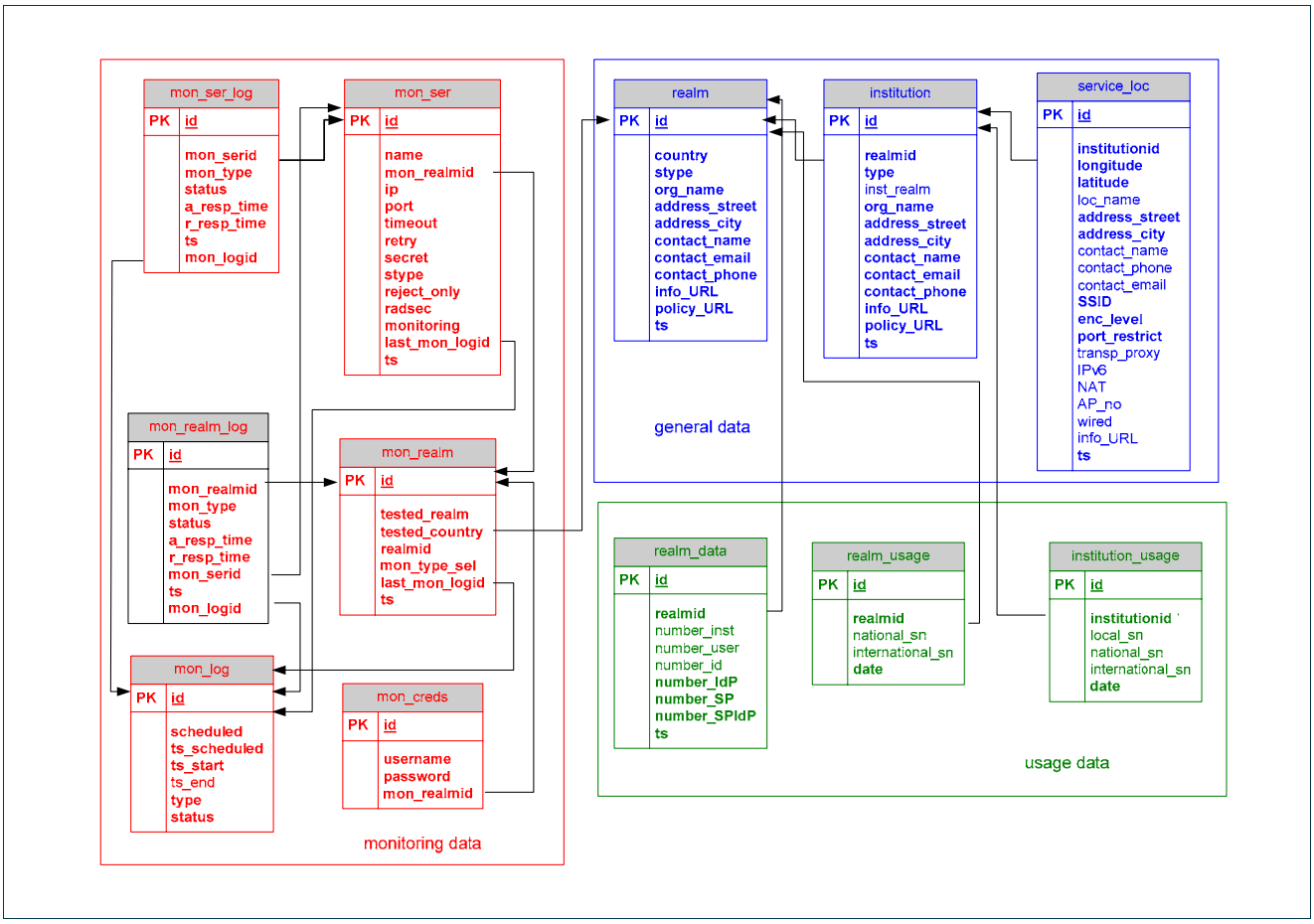

Figure 3.1: eduroam database structure.

Note: Bold items are required items, non-bold items are optional.

The eduroam database can be divided into three main parts:

- General data.
- Monitoring data.
- Usage data

The general data part is used to store information about the:

- NRO representatives and respective contacts.
- Institutions (both SP and IdP) official contacts.
- eduroam hotspots (SP location, technical info).

The database does not contain any end-user related personal data. Contact information and server IP addresses are necessary to provide the service. To avoid abuse, parts of the database will not be publicly available.

More detailed information about the proposed database model is provided in Appendix (please note that refinement work is still in progress, and the final version will be published by SA5 when the work is complete).

The general and usage data will be collected from the NROs on regular basis. It is envisaged that the usage data will be collected monthly, while general data will be refreshed weekly or on NRO's demand. Monitoring data will be automatically acquired from the monitoring system.

NROs should provide general and usage data in the defined XML format. The data should be available at the specified URL (http://www.eduroam.<tld>/usage/ for usage data and http://www.eduroam.<tld>/general/ for general data), which should be accessible only from the eduroam database server site. SA5 will develop detailed proper tools for data collection. See **Error! Reference source not found.**.

3.2 Hotspot Dissemination

The original model of announcing eduroam hotspots provided a map with participating federations in various colours depending on the committed level of participation of that federation, but no detailed deployment information. This is currently the only map, see Figure 3.2.

Figure 3.2: Root Layer Map

This sort of map will be referred to as the “political” map later on.

The political map is of importance for administrative personnel only, because it does not convey the vital information for end users: the location of PoP to determine whether one can expect to get roaming service at a given destination.

Up to now, this information was provided heterogeneously on a per-federation basis after clicking on the geographical area in question. There is no defined model for dissemination of PoP information within federations, so the results after clicking into a country vary greatly, from resizable, zoomable (scalable) maps with exact geographical coordinates to simple lists of connected institutions without geographic reference.

The SA5 meeting in Zurich (27 September 2007) decided to collect information about available PoP in a way that a Europe-wide map could be built. This map will later be referred to as the "geographical" map. The database model to collect and store the information was discussed in section 3.1 "eduroam Database", the options for visual presentation of this data are discussed here.

3.2.1 Google Maps

The company Google, Inc. operates a well-known map and satellite photo service on the Internet, generically accessible at http://maps.google.com. Apart from enabling access to this service from that web page, Google also provides the service on other sites. Owners of web space can register at Google to embed maps and satellite views on their own web space.

The terms and conditions of that embedded maps service are quite liberal - as long as the site is publicly accessible and non-commercial, the site owner is eligible for the free service. Google then reserves the right to

- Advertise for itself in the lower-left corner by injecting the logo "powered by Google" into the map.
- Place advertisements into the map space.

Option #2 is currently not in use, but this may change at any time. The paid Google service ("Google Maps Enterprise") is different in that it will not display non-Google advertisements, the site owner has an SLA to guarantee availability and may use the service on non-public web pages. Pricing for this high-availability service starts in the five-digit EUR range per year and depends on the click count on the web site.

The terms of the free edition of Google seem sufficient for displaying eduroam maps, since the geographical eduroam map will be on the public part of the web site and eduroam is a non-commercial undertaking.

Adding hotspots to the map service is done by using a JavaScript(R) based Application Programming Interface (API). It can either be fed with the coordinates of all PoP using a listing in the JavaScript code, or by referencing an external file that contains all these coordinates (in Google's publicly specified KML format). Practical tests with the API showed that embedding KML PoP is somewhat unreliable; not all points are shown on all occasions. This hinders the use for a hotspot map significantly.

Listing the hotspots in JavaScript works more reliably. The API allows to selectively transmit only a portion of the PoP data, namely the part that is currently visible on the map.

For the duration of the tests, a demo page was set up with the hotspots of the signed members of the European eduroam confederation at the time of the Zurich meeting. It is accessible at http://www.eduroam.lu/files/eduroam-map-new.html for the time being, but will be discontinued after the decision is made of which mapping provider to use.

The following screenshots show the Google Maps solution at various zoom levels:

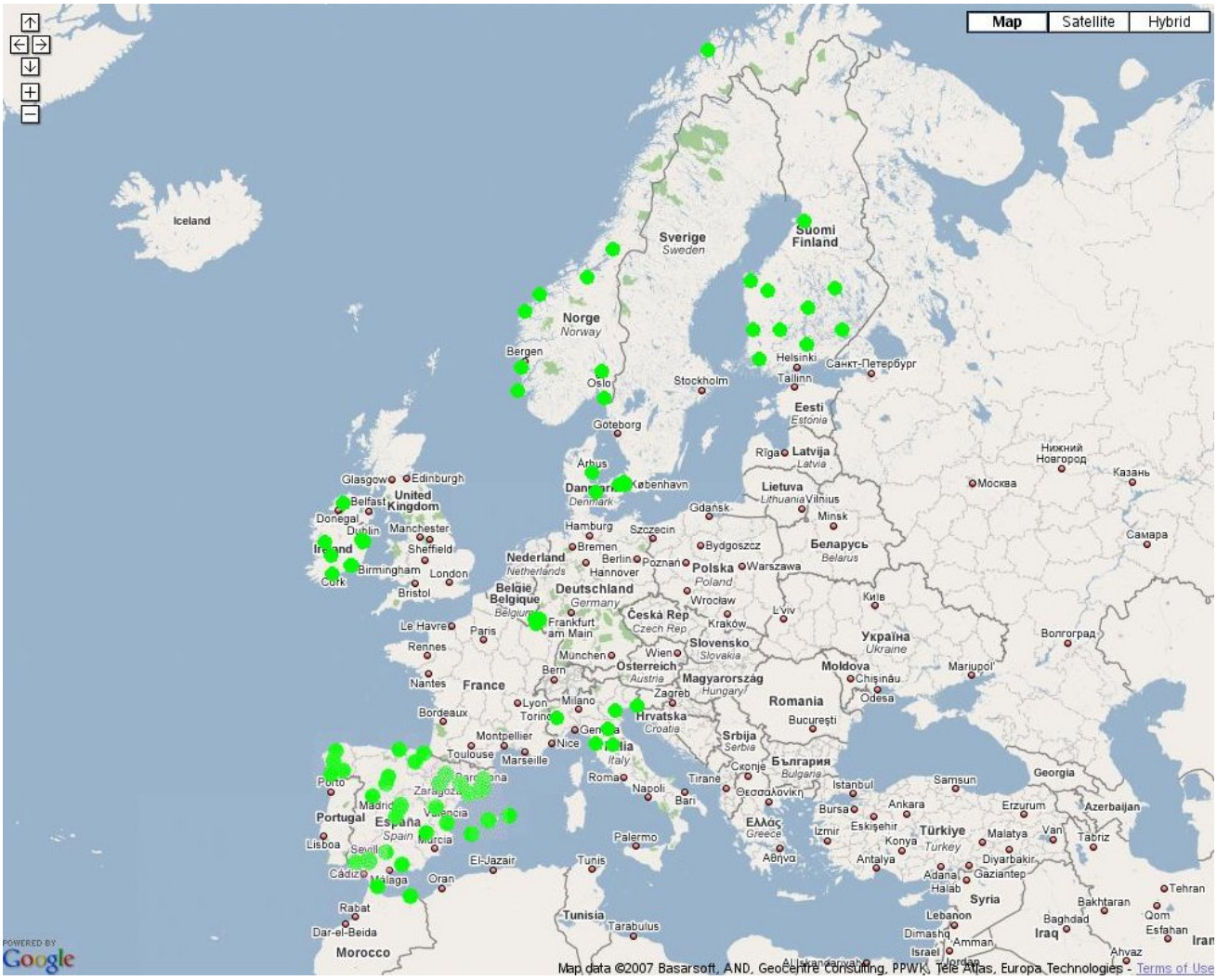

Figure 3.3: Example Google Map, Europe

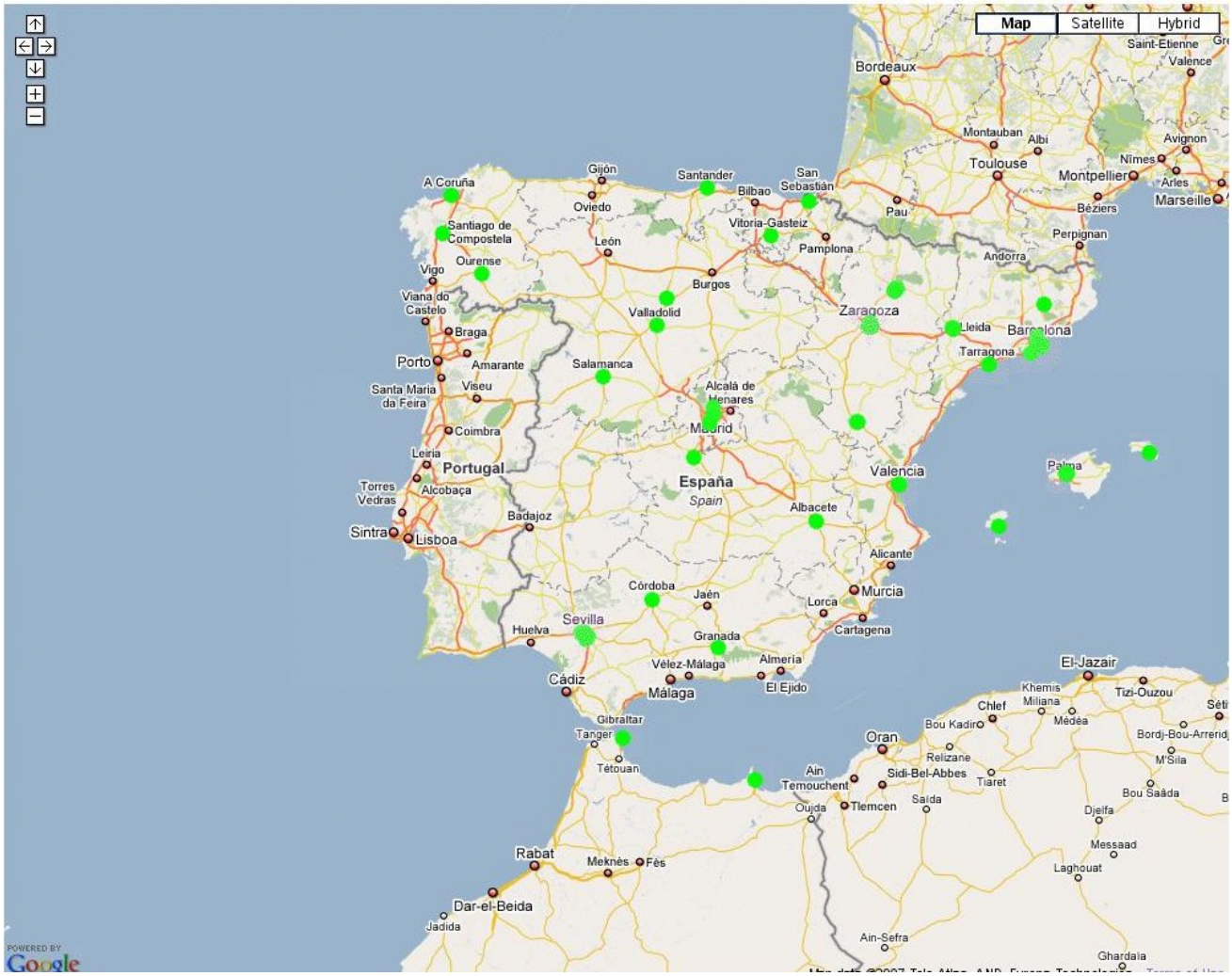

Figure 3.4: Example Google Map, Spain

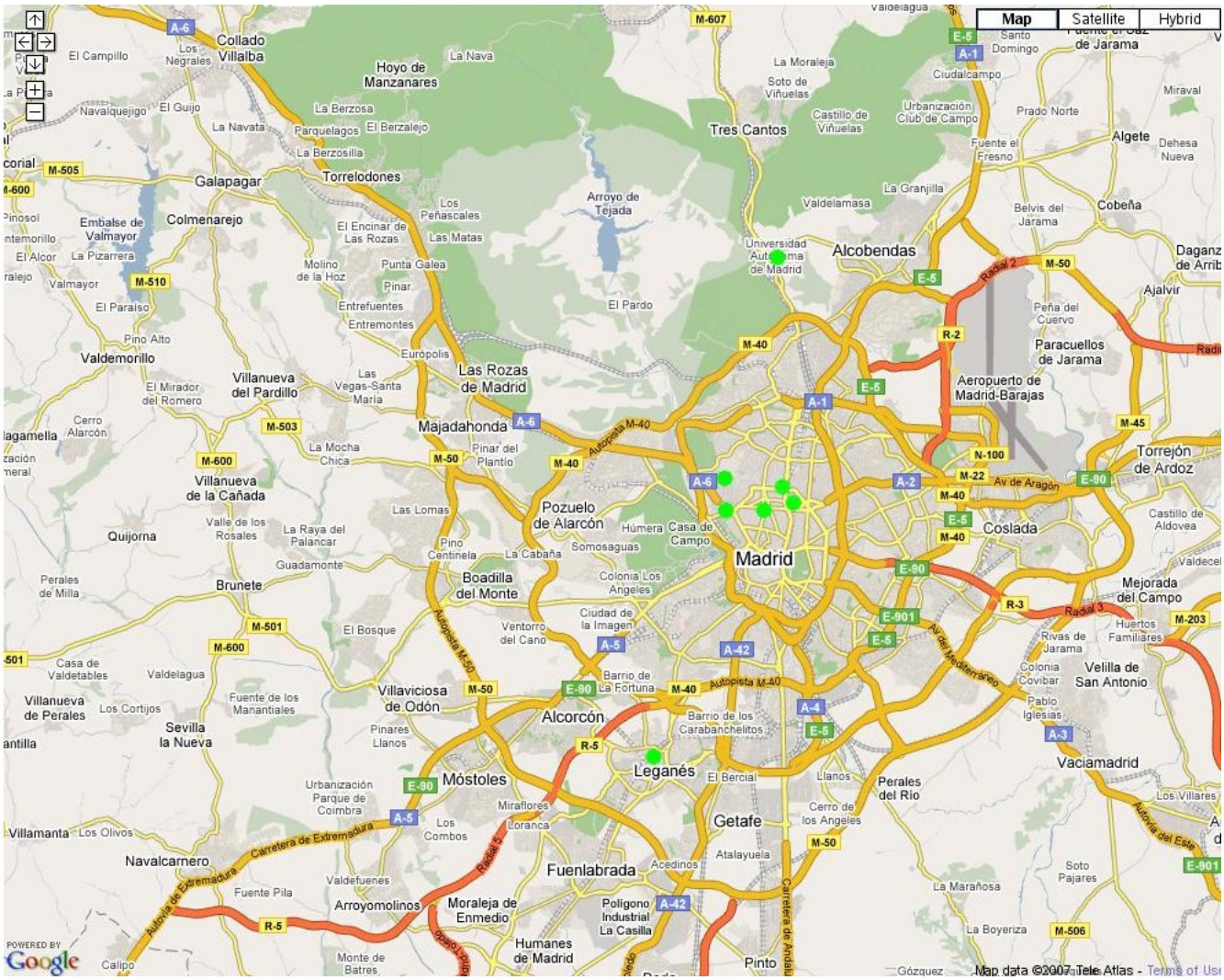

Figure 3.5: Example Google Map, Madrid

Figure 3.6: Example Google Map, eduroam institute detail

3.2.2 Microsoft Live Maps

Microsoft Live Maps offers a very similar service as Google. The API is vendor-specific from Microsoft. Since OpenLayers is able to use Microsoft Live Maps as a base layer with the exact same API that it can also use for Google Maps, no further investigation has been carried out regarding the specific capabilities of the Microsoft Live Maps API.

3.2.3 Yahoo! Maps

Yahoo! Maps offers a very similar service as Google. The API is vendor-specific. Since OpenLayers is able to use Yahoo! Maps as a base layer with the exact same API that it can also use for Google Maps, no further investigation has been carried out regarding the specific capabilities of the Microsoft Live Maps API.

3.2.4 OpenLayers

OpenLayers [openlayers] is a JavaScript API that can be used for creating dynamic maps in a web page. It allows the creation of overlays of public and private map databases and APIs to create fully customised maps.

The code was initially developed by Metacarta [metacarta], and then made open source under a BSD license. Since then it has evolved and now offers a very complete solution.

3.2.4.1 *Main features of OpenLayers*

OpenLayers is not different in essence from other JavaScript map APIs. It offers methods for creating a map object, and then adding different objects to that map (points, lines, polygons, and so on). Accessing these JavaScript methods is done by including the OpenLayers.js in the page that will include the map.

Maps can be configured to use any of the available commercial map databases; at the moment of writing this, it supports Google Maps, Yahoo! Maps, and MSN Virtual Earth. OpenLayers also supports Open Geospatial Consortium's [opengeo] Web Mapping Service (WMS) and Web Feature Service (WFS) protocols.

Maps created with OpenLayers can be fed with points stored in KML [kml] or GeoRSS [georss] files. Points can be generated also dynamically by using any scripting language that creates the corresponding JavaScript code after querying a database.

Modifying the behaviour or aspect of the map is quite easy. It can be done through the plethora of controls that can be added to a map. Adding own controls is also possible if needed.

3.2.4.2 *OpenLayers drawbacks*

OpenLayers is not completely free of limitations.

If the philosophy behind using OpenLayers is to avoid showing the Copyright notice of a commercial solution, then perhaps an open server should be used (such as OpenLayer's WMS service, or NASA's OnEarth service). However, the quality of the images/maps from these services is not as good as the commercial ones. There is also the possibility of creating a dedicated map server, but this is considered to be not affordable.

Another disadvantage is that using OpenLayers to process KML or GeoRSS files needs the user's browser to parse them, and this will not scale as well as drawing the maps directly from a database containing geographical coordinates.

3.2.4.3 *eduroam map preview*

A preview of a possible implementation of the eduroam map is currently available at http://www.eduroam.es/openlayers/, but may be discontinued after the decision of which mapping technology to use is made. The following two screenshots show two zoom levels of the Spanish federation, using Google Maps as the base layer:

Figure 3.7: Google Map, Spanish Federation (Zoom level 1)

Figure 3.8: Google Map, Spanish Federation (Zoom level 2)

3.3 Conclusions

While a plethora of providers for map data exists, each has its own API, meaning that specific development work has to be done to add eduroam hotspots onto the base map. If a change from one provider to another is required for whatever reason (for example, the provider introduces targeted advertising in their map), switching away from this provider would be a lengthy process (including writing new code in a different and unfamiliar API, and not possible in a short timeframe).

OpenLayers offers a “meta” map service, with an API that is independent of the map itself. This enables switching from one provider to another on short notice, and thus prevents vendor lock-in. JRA5 suggests to the eduroam Service Activity that OpenLayers be used as a scripting API.

The base layer to use with OpenLayers should be Google Maps for the moment, since this service has proven to be highly available and can scale to a large number of visitors easily. Note that no information is delivered to Google in this process, as only the maps are used to present information about the hotspots - all drawing on the maps is done by OpenLayers without any interaction with Google at all. However, these maps will be publicly accessible.

4 Client Configuration Technologies

4.1 Microsoft Wireless Native API

The built-in supplicant in MS Windows operating systems is known to have usability problems. It requires a lot of user interaction, and so far there has been no easy way of pre-configuring an installable package.

Recently, Microsoft released the “Wireless Native API”. It allows for a scripted configuration of the wireless settings using DLL calls to that API.

This API is available as a hotfix for MS Windows XP Service Pack 2. The same functionality is also available without installing a hotfix in MS Windows Vista. MS Windows XP Service Pack 3 will likely include the functionality, so that its installation base will be significant.

The API is documented at http://msdn2.microsoft.com/en-us/library/ms706556%28VS.85%29.aspx. A set of API calls is used to obtain access to the configuration store:

- WlanOpenHandle (to open the connection to the store).
- WlanEnumInterfaces (to enumerate the available interfaces).
- WlanSetProfile (to set a new profile).
- WlanCloseHandle (to close the connection).

WlanSetProfile expects an XML description of the network as an input. Sample XML profiles can be found in the API documentation (example: PEAP-MSCHAPv2 profile: http://msdn2.microsoft.com/en-us/library/aa370030(VS.85).aspx) and only need to be slightly adapted for use with eduroam.

Once an executable program with the abovementioned API calls is created, the only action needed by local campus administrators is to configure the XML file to their local setup and distribute the program along with the XML file to their users.

Users then only need to execute this program to have a fully configured eduroam system.

This technology will be described in the next release of the Roaming Cookbook.

4.2 Other advances in eduroam clients – OpenSEA

The OpenSEA Alliance was formed in early 2007 by a number of vendors and end-user organisations, including the UK NREN, JANET. The OpenSEA Alliance supports research related to user identification, link control, and management of network connections, and the development of open source code that implements those protocols.

The most concrete output of the work done by the OpenSEA Alliance is the development of open source supplicant software code for client devices. As its first major project, the OpenSEA Alliance began working with the Open1X project to create a cross-platform supplicant suitable for deployment on desktop computers. This has focused on the creation of an easy-to-use cross-platform GUI across the major desktop operating system platforms (Linux, Windows, and Mac OS X). The resulting GUI offers full control over all available options and complete status reporting. The GUI is written using the Qt toolkit to ensure portability to additional platforms and is fully customisable using the Qt Designer program. This allows an organisation to easily develop its own supplicant skin.

The structure of the GUI source code mirrors the underlying engine. A modular architecture allows "plug-ins" to use an API in order to extend the functionality of the supplicant; plug-ins can also create additional tabs in the GUI. For example, plug-ins are being used to provide posture support using existing libraries such as libtnc. To aid in debugging, a logging plug-in retains full debug-level data in a ring buffer for automatic reporting to a trouble ticket system. A plug-in is also in development to support automatic supplicant updates so that the software will update itself when a new version is available.

The modular code base also assists in enabling new classes of devices. Small devices such as PDAs and phones have limited memory, and so it is only possible to implement a subset of the functions that a fully functional portable computer requires. Separation of the GUI from the engine over a message-passing channel is well-suited to small-resource devices because many of them have their own GUI systems.

To enable new applications, the Open1X project plans to implement the new 802.11r and 802.11w security standards. 802.11r enables faster transitions between 802.11 access points by expanding the key hierarchy to cover multiple access points, and defining new handoff messages to exchange keys before the 802.1X exchange. 802.11w further extends the 802.11 security model by providing security for management frames.

The Open1X Project is also researching automatic configuration mechanisms; these will probably be enabled by the forthcoming 802.11u and 802.21 standards. The current draft of 802.11u includes a Generic Advertising Service (GAS) protocol. GAS is a generic transport protocol that provides communication between a client device and a network server prior to the completion of 802.11 authentication and 802.11 association. As this occurs prior to the establishment of an 802.11 security association, the development of application-layer mechanisms for the integrity of the file will be important.

The Open1X Project is actively seeking volunteers to work on testing, and on the development of EAP methods and GUI design.

For information, please see:

http://open1x.sourceforge.net/
http://www.openseaalliance.org/

4.3 Conclusions

The Wireless Native API appears to be a good way to configure the built-in supplicant.

OpenSEA's progress should be monitored as its implementation progresses.

5 IPv6 Support

IPv6 (Internet Protocol Version 6) is the "next generation" protocol, designed by the IETF, to replace the current version Internet Protocol, IP Version 4 (IPv4).

Analysis shows that IPv6 is supported by Radiator, radsecrpoxy, and FreeRADIUS2.0 servers. NAS support for IPv6 is, however, mixed.

All of the above technologies support dual-stack, meaning that they support both IPv4 and IPv6 at the same time. This means that incoming requests can be successfully sent over a mixed path of protocols. For example, a request could be sent from Point A to Point B using IPv4, but then could be sent from Point B to Point C using IPv6. Also, NAS IPv4 traffic is translated into IPv6 backbone traffic.

5.1 Conclusions

Although eduroam's back-end infrastructure could be configured to support IPv6 easily (in fact, radsecproxy could even be used to bring IPv4-only RADIUS devices to IPv6), there has been no requirement to do this, and no such requirement is envisioned in the near future. Therefore, no more work is planned.

6 Network Admission Control

Network Admission Control (NAC), sometimes called Network Endpoint Assessment (NEA), is a technology that enables network administrators to regulate admittance of a device to a network based on information related to the security status of this device (commonly known as the device's *posture* towards the network).

The basic idea is to first check whether the host seeking admittance to the network is at an appropriate security level (checking on the patch level of the operating system, the presence of antivirus software, the state of the firewall, and so on), evaluate this state and decide whether or not the host should be:

- Allowed access to the network.
- Diverted to a remediation network to raise its security level.
- Denied access.

There are various software stacks and solutions for this concept, but there is no standard way of doing this currently. Among the major vendors/consortia offering such solutions is Cisco Systems, Inc. with its NAC portfolio and a consortium named Trusted Computing Group (TCG), where a working group led by Juniper is developing a solution for the consortium members. TCG's goal is to provide an open solution that will eventually be standardised so that competing products can interoperate.

One common element in NAC products is that a piece of software needs to be installed on the client device. This software evaluates the device configuration and sends a Statement Of Health (SoH) to the network infrastructure. The way in which this information is exchanged between device and network varies from vendor to vendor. One notable approach is using an EAP conversation that adds the SoH information after the authentication. I.e. first a user authenticates to the network using one of the usual EAP payloads (EAP-TTLS, PEAP, EAP-TLS or others) and subsequently sends the SoH information in a second payload element of the EAP conversation. The container protocol for this information exchange carries the name EAP-TNC (Trusted Network Computing).

The approach of tying the authentication with the health status in one EAP conversation has its challenges. In a roaming scenario such as eduroam, the designated entities for authentication and health assessment are separate: authentication information is verified at the Identity Provider, whereas the device's security status is mainly of interest for the Service Provider to whom the device is trying to connect to. However, using the EAP conversation, the SoH payload will travel in an opaque way to the Identity Provider, and the Service Provider cannot evaluate the posture information itself. In this case a federated trust fabric is necessary so that the

Identity Provider evaluates the SoH statement and only sends a summary state to the Service Provider that the Service Provider needs to trust.

The lack of vendor interoperability has challenges in itself: a device roaming from one Service Provider to another may find that different clients are needed to satisfy different Service Provider NAC solutions. This makes roaming very inconvenient, and a situation like this should be avoided at all costs in eduroam. After confronting Cisco with these challenges, short-term advice given to the participants of TERENA TF-Mobility was to disable posture validation on eduroam networks.

The long-term solution should be to influence the market in a way that interoperable solutions and protocols are developed, and to establish a means to enable trust fabrics regarding roaming posture assessments from Identity Providers to Service Providers.

6.1 Conclusions

The topic of NAC should be followed closely, and solutions to the before mentioned challenges should be sought proactively. This is mainly to protect the eduroam service development from any harm resulting from the NAC technology.

7 Conclusions

Conclusions for the different research areas are given below.

Roaming Infrastructure Technologies: Diameter is not deemed to be usable for the eduroam infrastructure, at least during the remaining GN2 lifetime, although progress on protocol development and implementations should be monitored. However, RadSec has proven to be a valuable addition to the eduroam infrastructure. The DAMe sub-project has also proved invaluable in defining an architecture for the authorisation of network properties in eduroam, and for unified Single Sign On. Additionally, a prototypical implementation of the architecture was created, deployed and tested in an experimental setup. However, more extensive testing is required.

Administrative and User Support Technologies: The eduroam database is described in this section. From the analysis of available mapping technologies, OpenLayers is clearly the best solution for providing the graphical representation of PoP and hotspots.

Client Configuration technologies: The “Wireless Native API”, available as a hotfix for MS Windows XP Service Pack 2 and as an integral part of MS Windows Vista, allows administrators to configure an XML file to the settings required for their local setup. Running this file produces an eduroam-compatible supplicant configuration simply and efficiently, and this is clearly a good solution. The OpenSEA project is discussed, and needs to be monitored for its future applicability to eduroam.

IPv6: There is no requirement as yet to support IPv6.

Network Admission Control: Although the concept of NAC is definitely valuable, the challenges involved in incorporating such a system into eduroam make it unfeasible. A future solution might be to influence the market in a way that interoperable solutions and protocols are developed, and to establish a means to enable trust fabrics regarding roaming posture assessments from Identity Providers to Service Providers. This activity should be monitored closely.

8 References

DJ5.1.1,2 “Glossary of Terms”
DJ5.1.4 “Inter-NREN Roaming Architecture: Description and Development Items”
DJ5.4.1 “Advanced Technologies Overview”
[openlayers] OpenLayers http://www.openlayers.org/
[metacarta] Metacarta http://www.metacarta.com
[opengeo] Open Geospatial Consortium http://www.opengeospatial.org/
[kml] KeyHole Markup Language http://code.google.com/apis/kml/documentation/
[georss] GeoRSS: Geographically Encoded Objects for RSS feeds http://www.georss.org/

9 Acronyms

API	Application Programming Interface
BE	Bridging Element
DAMe	Deploying Authorization Mechanisms for Federated Services in the eduroam Architecture
eduGAIN	GÉANT Authorisation INfrastructure for the research and education community
IdP	Identity Provider
GeoRSS	Geographically Encoded Objects for RSS feeds
GUI	Graphical User Interface
KML	KeyHole Markup Language
MDS	Meta Data Service
NAC	Network Admission Control
NAS-SAML	Network Access Service based on SAML
NEA	Network Endpoint Assessment
NRO	National Roaming Operator
OT	Operations Team
PDP	Policy Decision Point
PoP	Point of Presence
SAML	Security Assertion Markup Language
SP	Service Provider
TCG	Trusted Computing Group
TLV	Type Length Value
uSSO	unified Single Sign On
XACML	eXtensible Access Control Markup Language

Appendix A eduroam Database

This Appendix lists the database tables and respective fields, with basic information describing them. Note that mandatory fields are shown in **bold typeface**.

A.1 General data part

A.1.1 table: realm

Contains general information about the NROs i.e. member federations:

Field Name	Field Description
id	Automatically generated identifier
country	Federation's two letter country code; (e1 and e2 may be used to save info about TLRSs and respective OT members)
stype	0= FLRS, 1=(E)TLRS
org_name*	NRO's corporate name
address_street	NRO's address
address_city	NRO's address
contact_name**	NRO's representative: name
contact_email**	NRO's representative: e-mail
contact_phone**	NRO's representative: phone no.
info_URL***	NRO's web page
policy_URL***	NRO's Policy
ts	Date: last changed

- * Multiple names can be specified via respective XML file; note that it is mandatory to provide language info; name in English is required.
- ** Multiple contact info can be specified via respective XML file.
- *** Multiple URLs can be specified via respective XML file; note that it is mandatory to provide language info.

A.1.2 Table: institution

Contains information about the institutions inside federations:

Field Name	Field Description
id	Automatically generated identifier
realmid	id of respective realm (i.e. federation); handled by central application
type	1=IdP, 2=SP, 3=IdP&SP
inst_realm****	Institution's realm (for IdPs only)
org_name*	Institution's corporate name
address_street	Institution's address
address_city	Institution's address
contact_name**	Institution's representative: name
contact_email**	Institution's representative: e-mail
contact_phone**	Institution's representative: phone no.
info_URL***	Institution's web page with the information related to the service
policy_URL***	Institution's Policy
ts	Date: last changed

- * Multiple names can be specified via respective XML file; note that it is mandatory to provide language info; name in English is required.
- ** Multiple contact info can be specified via respective XML file.
- *** Multiple URLs can be specified via respective XML file; note that it is mandatory to provide language info.
- **** Multiple realms can be specified via respective XML file; for type 2 no realms should be specified.

A.1.3 Table: service_loc

Contains information about the eduroam service locations:

Field Name	Field Description
id	Automatically generated identifier
institutionid	id of respective institution; handled by central application
longitude	Geographic coordinates
latitude	Geographic coordinates
loc_name*	Location's name
address_street	Location's address
address_city	Location's address

contact_name**	On-site support: name
contact_email**	On-site support: e-mail
contact_phone**	On-site support: phone no.
SSID	SSID must be specified
enc_level	List of supported encryption levels separated by **,** (example: WPA/TKIP, WPA/AES, WPA2/TKIP, WPA2/AES)
port_restrict	0=default, 1 if there are port restrictions
transp_proxy	0=default, 1 if there is a transparent proxy
IPv6	0=default, 1 for IPv6 support
NAT	0=default, 1 for NAT
AP_no	Number of APs (number of enabled sockets for wired access)
wired	0=default, 1 if wired access is provided
info_URL***	Additional info page (e.g with additional restrictions if port_restrict set to “1”)
ts	Date: last changed

- * Multiple names can be specified via respective XML file; note that it is mandatory to provide language info; name in English is required.
- ** Multiple contact info can be specified via respective XML file.
- *** Multiple URLs can be specified via respective XML file; note that it is mandatory to provide language info.

A.2 Usage data part

A.2.1 Table: realm_data

Contains basic demographic data related to the eduroam service inside a federation:

Field Name	Field Description
id	Automatically generated identifier
realmid	id of respective realm (i.e. federation); handled by central application
number_inst	Total number of institutions that are eligible to participate in eduroam service
number_user	Total number of users (individuals) that are eligible to participate in eduroam service
number_id	Total number of issued e-identities (credentials) that may be used for authentication in eduroam service
number_IdP	Total number of institutions that act only as IdP
number_SP	Total number of institutions that act only as SP
number_SPIdP	Total number of institutions that act both as IdP and SP

ts	Date: last changed

A.2.2 Table: realm_usage

Contains basic numbers related to the eduroam service usage at a federation (NRO) level:

Field Name	Field Description
id	Automatically generated identifier
realmid	id of respective realm (i.e. federation); handled by central application
national_sn	Total number of successfully authenticated sessions per day – national level (inside the federation); monitoring requests must be filtered out
international_sn	Total number of successfully authenticated sessions per day – international level; monitoring requests must be filtered out
date	Date (gggg:mm:dd)

A.3 Table: institution_usage

Contains basic numbers related to the eduroam service usage at an institution level:

Field Name	Field Description
id	Automatically generated identifier
institutionid	id of respective institution (institution table); handled by central application
local_sn	Total number of successfully authenticated sessions per day – local level (same institution / RADIUS server); monitoring requests must be filtered out
national_sn	Total number of successfully authenticated sessions per day – national level (inside the federation); monitoring requests must be filtered out
international_sn	Total number of successfully authenticated sessions per day – international level; monitoring requests must be filtered out
date	Date (gggg:mm:dd)

A.4 Monitoring data part

A.4.1 Table: mon_realm

Contains information related to federation monitoring:

Field Name	Field Description
id	Automatically generated identifier
tested_realm	Realm used for testing (usually eduroam)
tested_country	Country code used for testing (usually respective realm's country code)
realmid	id of the monitored realm (i.e. federation)
mon_type_sel	Coded type of tests to be preformed (0 = PAP, 1=EAP-TTLS, 10= PAP & EAP-TTLS, ...)
last_mon_logid	id of the last successful monitoring job for this realm
ts	Date: last changed

A.4.2 Table: mon_ser

Contains information related to RADIUS server monitoring:

Field Name	Field Description
id	Automatically generated identifier
name	Server's (host) name
mon_realmid	id of respective realm used for testing (mon_realm table)
ip	Server's IP address
port	RADIUS server: port number
timeout	RADIUS server: timeout
retry	RADIUS server: number of retries
secret	RADIUS server: secret
stype	0=TLRS, 1=FLRS, ...
reject_only	0=default, 1 if only reject logic tests are performed
radsec	0=default, 1 if it is RadSec server
monitoring	0=default, -1 if this server should not be tested
last_mon_logid	id of the last successful monitoring job for this server
ts	Date: last changed

A.4.3 Table: mon_ser_log

Contains results of RADIUS server monitoring:

Field Name	Field Description
id	Automatically generated identifier
mon_serid	id of respective server
mon_type	Coded type of performed tests (0 = PAP, 1=EAP-TTLS, ...)
status	RADIUS server status: 0=OK, -1=reject logic test failed, -2= accept logic test failed, -3= both tests failed
a_resp_time	Response time for accept test
r_resp_time	Response time for reject test
ts	Date: created
mon_logid	id of the respective monitoring job

A.4.4 Table: mon_realm_log

Contains results of infrastructure monitoring:

Field Name	Field Description
id	Automatically generated identifier
mon_realmid	id of respective realm (mon_realm table)
mon_type	Coded type of performed tests (0 = PAP, 1=EAP-TTLS, ...)
status	Federation status: 0=OK, -1=reject logic test failed, -2= accept logic test failed, -3= both tests failed
a_resp_time	Response time for accept test
r_resp_time	Response time for reject test
mon_serid	id of TLRS used for test
ts	Date: created
mon_logid	id of the respective monitoring job

A.4.5 Table: mon_log

Contains internal monitoring information (e.g. info on scheduled tasks):

Field Name	Field Description
id	Automatically generated identifier
scheduled	0=automatic; 1=manual
ts_scheduled	Scheduled time
ts_start	Start time
ts_end	Stop time
type	Job type (10=all servers; 11=single server; 20=all realms; 21=single realm)
status	Job status (0=END, 1=RUNING, 2=START, -1=ERROR)

A.4.6 Table: mon_creds

Contains credentials used for monitoring:

Field Name	Field Description
id	Automatically generated identifier
username	Test username
password	Test password / automatically generated
mon_realmid	id of respective realm used for testing (mon_realm table)

Appendix B Data Collection

As explained in section 1, NROs should provide general and usage data in the defined XML format. The data should be available at the specified URL (http://www.eduroam.<tld>/usage/ for usage data and http://www.eduroam.<tld>/general/ for general data), which should be accessible only from the eduroam database server site.

The data collection mechanism will allow both pull (standard) and push data collection method. Pull method will be used by the central server according to the agreed schedule. Push method will provide NROs with the ability to select the time for data collection and initiate the process regardless of the agreed schedule. This might be used in case of massive changes in the data or when an urgent correction is needed.

B.1 The XML specification for general and usage data

In this subsection we list appropriate XML Schemas (XSD files) – one per database table with exception of institution.xml that covers tables institution and service_loc.

B.1.1 Schema for http://www.eduroam.<tld>/general/realm.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:simpleType name="eduroam_realm_stype">
<xs:restriction base="xs:int">
<xs:enumeration value="0">
<xs:annotation>
<xs:documentation>FLRS</xs:documentation>
</xs:annotation>
</xs:enumeration>
<xs:enumeration value="1">
<xs:annotation>
<xs:documentation>(E)TLRS</xs:documentation>
</xs:annotation>
```

```
</xs:enumeration>
</xs:restriction>
</xs:simpleType>
<xs:element name="realms">
<xs:complexType>
<xs:sequence>
<xs:element name="realm">
<xs:complexType>
<xs:sequence>
<xs:element name="country" type="xs:string"/>
<xs:element name="stype" type="eduroam_realm_stype"/>
<xs:element name="org_name" maxOccurs="unbounded">
<xs:complexType>
<xs:simpleContent>
<xs:extension base="xs:string">
<xs:attribute name="lang" type="xs:string" use="required"/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>
</xs:element>
<xs:element name="address">
<xs:complexType>
<xs:sequence>
<xs:element name="street" type="xs:string"/>
<xs:element name="city" type="xs:string"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="contact" maxOccurs="unbounded">
<xs:complexType>
<xs:sequence>
<xs:element name="name" type="xs:string"/>
<xs:element name="email" type="xs:string"/>
<xs:element name="phone" type="xs:string"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="info_URL" maxOccurs="unbounded">
<xs:complexType>
<xs:simpleContent>
<xs:extension base="xs:anyURI">
<xs:attribute name="lang" type="xs:string" use="required"/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>
```

```
</xs:element>
<xs:element name="policy_URL" maxOccurs="unbounded">
<xs:complexType>
<xs:simpleContent>
<xs:extension base="xs:anyURI">
<xs:attribute name="lang" type="xs:string" use="required"/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>
</xs:element>
<xs:element name="ts" type="xs:dateTime">
<xs:annotation>
<xs:documentation> Format: 2008-02-29T12:00:00 </xs:documentation>
</xs:annotation>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>
```

B.1.2 Schema for http://www.eduroam.<tld>/general/institution.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:simpleType name="eduroam_institution_type">
<xs:restriction base="xs:int">
<xs:enumeration value="1">
<xs:annotation>
<xs:documentation>IdP</xs:documentation>
</xs:annotation>
</xs:enumeration>
<xs:enumeration value="2">
<xs:annotation>
<xs:documentation>SP</xs:documentation>
</xs:annotation>
</xs:enumeration>
<xs:enumeration value="3">
<xs:annotation>
<xs:documentation>SPIdP</xs:documentation>
</xs:annotation>
```

```
</xs:enumeration>
</xs:restriction>
</xs:simpleType>
<xs:element name="institutions">
<xs:complexType>
<xs:sequence maxOccurs="unbounded">
<xs:element name="institution">
<xs:complexType>
<xs:sequence>
<xs:element name="country" type="xs:string"/>
<xs:element name="type" type="eduroam_institution_type"/>
<xs:element     name="inst_realm"     type="xs:string"     maxOccurs="unbounded"
minOccurs="0"/>
<xs:element name="org_name" minOccurs="1" maxOccurs="unbounded">
<xs:complexType>
<xs:simpleContent>
<xs:extension base="xs:string">
<xs:attribute name="lang" type="xs:string" use="required"/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>
</xs:element>
<xs:element name="address">
<xs:complexType>
<xs:sequence>
<xs:element name="street" type="xs:string"/>
<xs:element name="city" type="xs:string"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="contact" maxOccurs="unbounded">
<xs:complexType>
<xs:sequence>
<xs:element name="name" type="xs:string"/>
<xs:element name="email" type="xs:string"/>
<xs:element name="phone" type="xs:string"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="info_URL" minOccurs="1" maxOccurs="unbounded">
<xs:complexType>
<xs:simpleContent>
<xs:extension base="xs:anyURI">
<xs:attribute name="lang" type="xs:string" use="required"/>
</xs:extension>
```

```
</xs:simpleContent>
</xs:complexType>
</xs:element>
<xs:element name="policy_URL" maxOccurs="unbounded">
<xs:complexType>
<xs:simpleContent>
<xs:extension base="xs:anyURI">
<xs:attribute name="lang" type="xs:string" use="required"/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>
</xs:element>
<xs:element name="ts" type="xs:dateTime">
<xs:annotation>
<xs:documentation> Format: 2008-02-29T12:00:00 </xs:documentation>
</xs:annotation>
</xs:element>
<xs:element name="location" maxOccurs="unbounded" minOccurs="0">
<xs:complexType>
<xs:sequence>
<xs:element name="longitude" type="xs:string"/>
<xs:element name="latitude" type="xs:string"/>
<xs:element name="loc_name" minOccurs="0" maxOccurs="unbounded">
<xs:complexType>
<xs:simpleContent>
<xs:extension base="xs:string">
<xs:attribute name="lang" type="xs:string" use="required"/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>
</xs:element>
<xs:element name="address">
<xs:complexType>
<xs:sequence>
<xs:element name="street" type="xs:string"/>
<xs:element name="city" type="xs:string"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="contact" maxOccurs="unbounded" minOccurs="0">
<xs:complexType>
<xs:sequence>
<xs:element name="name" type="xs:string"/>
<xs:element name="email" type="xs:string"/>
<xs:element name="phone" type="xs:string"/>
```

```
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="SSID" type="xs:string"/>
<xs:element name="enc_level" type="xs:string"/>
<xs:element name="port_restrict" type="xs:boolean" default="0"/>
<xs:element name="transp_proxy" type="xs:boolean" default="0" minOccurs="0"/>
<xs:element name="IPv6" type="xs:boolean" default="0" minOccurs="0"/>
<xs:element name="NAT" type="xs:boolean" default="0" minOccurs="0"/>
<xs:element name="AP_no" type="xs:int" minOccurs="0"/>
<xs:element name="wired" type="xs:boolean" default="0" minOccurs="0"/>
<xs:element name="info_URL" minOccurs="0" maxOccurs="unbounded">
<xs:complexType>
<xs:simpleContent>
<xs:extension base="xs:anyURI">
<xs:attribute name="lang" type="xs:string" use="required"/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>
```

B.1.3 Schema for http://www.eduroam.<tld>/usage/realm_data.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name="realm_data_root">
<xs:complexType>
<xs:sequence maxOccurs="unbounded">
<xs:element name="realm_data">
<xs:complexType>
<xs:sequence>
<xs:element name="country" type="xs:string"/>
<xs:element name="number_IdP" type="xs:int"/>
```

```
<xs:element name="number_SP" type="xs:int"/>
<xs:element name="number_SPIdP" type="xs:int"/>
<xs:element name="number_inst" type="xs:int" minOccurs="0"/>
<xs:element name="number_user" type="xs:int" minOccurs="0"/>
<xs:element name="number_id" type="xs:int" minOccurs="0"/>
<xs:element name="ts" type="xs:dateTime"/>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>
```

B.1.4 Schema for http://www.eduroam.<tld>/usage/realm_usage.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name="realm_usages">
<xs:complexType>
<xs:sequence maxOccurs="unbounded">
<xs:element name="realm_usage">
<xs:complexType>
<xs:sequence maxOccurs="unbounded">
<xs:element name="usage">
<xs:complexType>
<xs:sequence>
<xs:element name="national_sn" type="xs:int" minOccurs="0"/>
<xs:element name="international_sn" type="xs:int" minOccurs="0"/>
</xs:sequence>
<xs:attribute name="date" use="required" type="xs:date"/>
</xs:complexType>
</xs:element>
</xs:sequence>
<xs:attribute name="country" use="required" type="xs:string"/>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>
```

B.1.5 Schema for http://www.eduroam.<tld>/usage/institution_usage.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name="institution_usages">
<xs:complexType>
<xs:sequence maxOccurs="unbounded">
<xs:element name="institution_usage">
<xs:complexType>
<xs:sequence maxOccurs="unbounded">
<xs:element name="usage">
<xs:complexType>
<xs:sequence>
<xs:element name="local_sn" type="xs:int" minOccurs="0"/>
<xs:element name="national_sn" type="xs:int" minOccurs="0"/>
<xs:element name="international_sn" type="xs:int" minOccurs="0"/>
</xs:sequence>
<xs:attribute name="date" type="xs:date" use="required"/>
</xs:complexType>
</xs:element>
</xs:sequence>
<xs:attribute name="inst_realm" type="xs:string" use="required"/>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>
```